Title:	***NAv6TF NTIA IPv6 RFC Response***
Editor(s):	***Jim Bound and Latif Ladid***
Date:	***03/01/04***
Version:	***FINAL***

Contents

Executive Summary

This is the North American IPv6 Task Force's (NAv6TF) www.nav6tf.org response to the NTIA IPv6 RFC.This response leads to the suggestion that the U.S. Government begin a plan to adopt IPv6 as a core network infrastructure technology for National Business, Economic, Social, and Political reasons, in addition to the formal NAV6TF response to this RFC. The response will also make a set of recommendations how the U.S. Government could help lead the deployment for IPv6 within the U.S.

The emergence of the Internet as a fundamental technology for commercial and social activity has been most apparent since the creation of the World Wide Web in the mid 90's. The Internet has grown rapidly in the past five years, to a scale well beyond that which the original Internet designers envisaged over twenty years ago. It is imperative that the U.S. Internet be able to grow to meet the future demands of commerce and society, for business, for learning, to enable new markets to be realized, and to enrich the lives of U.S. citizens. The Internet has been a significant driver for innovation in the US industry, which is an important impact on the economy.

IPv6 is also important to the U.S. Department of Defense as a network infrastructure and as a technology enabler to support secure and robust state of the art military operations tomorrow, and likewise for the U.S. Department of Homeland Security from a NAv6TF perspective.

The Internet relies on a data communication method called the Internet Protocol (IP) to transfer data between machines on the network, be that data Web pages, e-mail, online gaming or otherwise. All Internet applications communicate using IP; it is the basic enabler of every service on the Internet; it is thus critical that IP is able to scale on the Internet.

Future network growth requires that Internet-enabled devices can be assigned and use a globally unique IP address, in a similar way to the telephone numbers that identify individual phones. The current version of IP, IPv4, has been in existence for over twenty years, but has a limited address space, not even enough for one IP address per person on the planet. Its successor, IPv6 core specifications, in development by the IETF for eight years, offers relatively unlimited address space. The IPv6 core standards were completed in 1999, and vendors started shipping commercial IPv6 products in earnest in 2000. As a result a number of early IPv6 deployments already exist, notably in Japan **www.ipv6style.jp/en/**.

The scarcity of IPv4 address space, for example for both commercial and home users, restricts the applications that can be run for both business and home networks. A technique known as Network Address Translation (NAT) allows multiple devices to be "hidden" behind one or more real IPv4 addresses, but NAT breaks the end-to-end principle of the Internet, preventing the evolution of next generation applications that demand IP address space, and connectivity into business premises and home networks (e.g. from IP-enabled mobile handsets). IPv6 delivers that address space, insures the option of Mobile IPv6 devices, and is thus a key factor for the well being of the future U.S. Internet.

This response overviews IPv6, describing the features of IPv6 that will be key enablers for new applications and services. It describes the road forward for IPv6, including the requirement to integrate IPv4 and IPv6 services as the gradual overall transition to IPv6 occurs. There is no IPv6 "flag day" as there was for Y2K, but the earlier that IPv6 transition is begun, the less costly that transition will be in the long run, and the sooner IPv6's benefits can be exploited in the U.S.

IPv6 is the only solution that provides the vastly increased IP address space and enhanced features that will allow the U.S. Internet to grow and to scale into the next decades. The base IPv6 protocols are ready now, but deployment, which should be lead by market forces, requires a number of factors to be addressed, as recommended in our response.

The US leadership in Internet technologies should be sustained as its mega-engine and foundation for new job and wealth creation, transforming and enhancing society life and work styles cementing thereby the US as the most innovative and advanced technology nation in the world with greater positive impact on the entire planet.

The response is formatted so the NTIA RC questions are first in *italics* and the NAv6TF indented below the questions in **bold.**

1. Potential Benefits and Uses of IPv6 (NTIA RFC Section II)

We seek comment on the potential benefits and uses of IPv6. As described below, some of the potential benefits commonly associated with IPv6 include a significant increase in the number of available Internet addresses, a proliferation of new applications building on peer-to-peer communications, and improved security. We request comment on these and other possible benefits related to widespread adoption of IPv6. We request comment on the benefits accruing to both end users and system providers.

1.1. Increased Address Space (NTIA RFC Section II-A)

One of the most commonly cited benefits of IPv6 is the vastly expanded number of individual addresses that IPv6 will enable. IPv4 uses a 32-bit IP address scheme that allows more *than 4 billion individual addresses to be identified on the Internet. With the explosive growth rate of Internet users and new applications over the last decade, concerns have been raised that the currently defined IPv4 address space may not be sufficient to meet the needs of the growing Internet user base. By expanding the existing IP address field to 128 bits, IPv6 offers a vast pool (3.4 x 10^{38}) of assignable Internet addresses. As a result, IPv6 can enable an enormous number of new nodes and users to be connected to the Internet using their own unique Internet addresses.*

The task force requests comment on the adequacy of IPv4 address space. Specifically, we seek estimates (and underlying assumptions) of how many IPv4 addresses have been allocated, how many are still *available, and how long the remaining addresses will be sufficient to meet the needs of users in the United States, as well as users in other countries around the world. We recognize that, because a large portion of the available IPv4 addresses have been allocated to North America, concerns regarding address availability may differ depending on the commenter's perspective. We therefore ask commenters to discuss how the purported limitations on IPv4 addresses will affect different geographic regions (e.g., North America, Europe, Asia) and customer markets (e.g., private sector, government, academia).*

There are many ongoing debates regarding the IPv4 address space remaining worldwide.

There are different positions based upon the formula, weights, and metrics used to analyze the IPv4 address space phenomena. Endless debates have already been published regarding the number of global IPv4 addresses that are either dependent upon the proponents' view of allocated or unallocated, used or unused, with or without the H-Ratio address space, but so far most if not all of these addresses were consumed by the IT industry. Allocation of IPv4 address space restricts the availability of the address space, disabling US enterprises and home networks to get sufficient address space for their needs. The non-accessibility of address space disables the deployment of new innovative applications. This view also does not look at an innovative model to enable every country without distinction of its population or economy to become a member of what the NAv6TF references as the e-Nation.

The NAv6TF position and projections for IPv6 addresses can be found at NAv6TF web site:

http://www.nav6tf.org/RIR_eNations/RIR_eNations.html

http://www.nav6tf.org/slides/IPv6ImpactReport.doc

The world population counts now over 6 billion people and might grow to 9 billion by 2050. The threshold of 4 billion IP addresses was crossed back in 1980 prior to the launch of the Internet in 1983. Any new design of the Internet protocol should cater for servicing equitably the world population and its devices. India has 2 million IP addresses for a population of over 1.0 billion. China has 30 million IP addresses for a population of over 1.2 billion. The fact that IP addresses have to be unique worldwide is by itself a constraint and renders the address space a limited and scarce resource to share equitably among the world population. Dependent on the country you live in, one could not name the Internet an open model?

Without sufficient global IP address space, applications are forced to work with mechanisms that provide local site addressing, loosely the equivalent of the early days of telephony where users had to interact with one (or more) operators to place a call. Such mechanisms (i.e. Network Address Translation or NAT) restrict the end-to-end transparency of the Internet. While NAT has to some extent delayed the pressure on IPv4 address space for the short term, it places severe restrictions on application communication. While a client behind a NAT device can communicate out to servers on the Internet (the "client-server" communication

model), that same client cannot be guaranteed to be accessible when external devices wish to establish a connection to the client (as typified by the "peer-to-peer" communication model).

The need for always-on environments (such as residential Internet through broadband, cable modem, or Ethernet-to-the-Home) to be globally reachable precludes NAT-style IP address conversion, pooling, and temporary allocation techniques, and the "plug and play" always-on consumer Internet appliance requirements further increases the address pressure. IPv6 will remove the requirement for the use of NAT because global addresses are widely available.

IPv6 reintroduces the ability to provide end-to-end security that is not always readily available through a NAT-based network. The plug and play feature of IPv6 makes IP device deployment, for example in the home, much easier for vendors, end users should not need to configure their network appliances (and with IPv4, users would have to configure NAT routers, which is unacceptable for commodity deployment). IPv6 introduces prefix delegation which permits home users to configure their network as its own network domain; this capability with plug and play will provide home users the ability to manage their own network with less reliance on their ISP.

The important point to note about IPv4 address space is that many users are behind a NAT and this prohibits the use of End-2-End (E2E) security and networking. There are not enough IPv4 addresses to permit businesses or society to move to mobile E2E computing world wide today, as one example. Mobile devices will be a disruptive technology and strain the current IPv4 NAT model and IPv4 address space beyond its capabilities.

Basing the decision of the adoption of IPv6 simply on the number of the remaining IPv4 address space is solely a reasoning of an accountant depleted of any long term strategic and innovation vision. Accountants are forced to adopt a frozen view of the future to sustain a good meaning of their projections, but they arrogantly eliminate the unexpected and unforeseen events that change the world. Restricted IPv4 addressing means wider deployment of NAT even in the US which is supposed to have the lion's share of the address space. NAT is definitely a showstopper to Internet innovation. The Internet is designed to cater to multiple large scale applications of the size of the web today. If we had to make a copy of the web today with the same amount of addressing needed to make it work, we would not be able to obtain this IP resource. So, the Internet is condemned to be used only for the web and any new large scale application won't get this resource and will fail to scale and will sadly be downscaled to niche applications.

The Internet model based on IPv6 would cater for ten more large scale applications even larger than the web of today. VoIP, Grid Computing, 3G, P2P (gaming, file sharing, ..), Remote sensing, Smart Homes, Ad hoc networks, Mobile devices, Intelligent Transport Systems (ITS), Consumer Electronics, Home appliances and networked RFIDs are some of the applications that will see the light with IPv6 and dwarf current network concepts into oblivion.

The task force also seeks comment on the potential uses for this greatly expanded pool of addresses. What new products, services, features, applications and other uses are likely to result from the additional addresses

offered by IPv6? To the extent possible, commenters should provide estimates and underlying assumptions of the economic impact of these new uses and should identify which market segments will be affected by these uses.

The IPv6 address space permits many devices to be attached to an Internet with a globally routable IPv6 address, which permits E2E communications between two devices. The NAv6TF definition of E2E is as follows: the ability for two devices to communicate with each other, where a device sending an IPv6 packet, has the property that the IPv6 source and destination within the IPv6 header of the packet are both globally routable addresses on the Internet, and because those addresses are globally unique, can be used to assist E2E IPv6 security between devices using the IPsec protocol, which is mandatory for compliance to IPv6.

The NAv6TF does not state projections for markets that will use IPv6. This is not one of our functions or skill sets, as a vendor neutral body. We do believe new markets will emerge because of the inherent advantages of IPv6, well documented in our literature on the NAv6TF web site. We also believe that IPv6 will bring back the restoration of the E2E model for the Internet and for businesses to evolve to a new communications model that does not exist today, for many, within the current Internet or for businesses using Network Address Translation (NAT) within their enterprise.

IPv6 is infrastructure. The transition to this infrastructure from IPv4 is an evolutionary paradigm shift from one IP infrastructure to the other. The end result of the move to IPv6 is revolutionary, because it is the restoration of the E2E model for networking, which can be used by enterprises and individuals that cannot be done by most currently with IPv4 when using NAT. Initial emerging market segments will be able to use the paradigm shift to provide new and improved services and functions to users and within devices that require an E2E networking infrastructure. These initial markets will stimulate the use of IPv6 and the transition to IPv6 across all markets. These markets will help stimulate building a new Next Generation Internet highway with IPv6, similar to the reasons our U.S. Interstate highways were built by President Eisenhower in the 1950's.

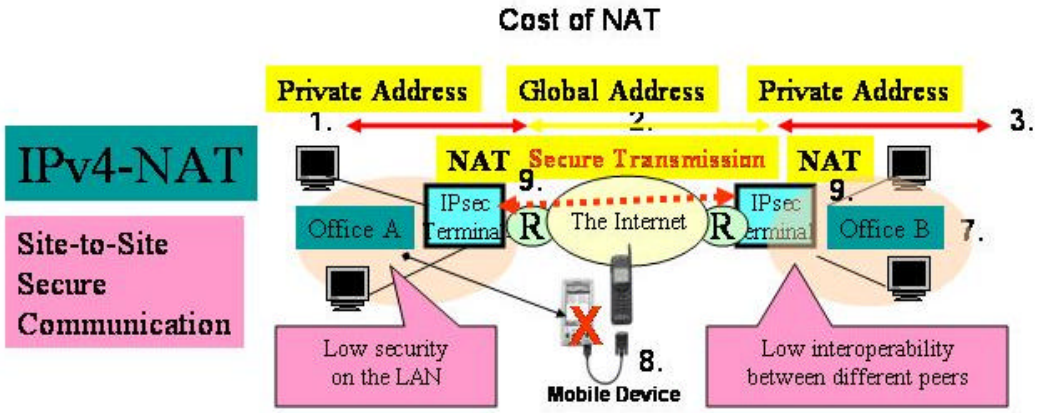
The initial emerging markets that will use the benefits of IPv6 are as follows:

- **Military Net-Centric Operations**
- **Homeland Security Net-Centric Operations**
- **Multimedia Applications and Network Infrastructure**
- **Mobile Applications and Network Infrastructure**
- **Satellite, Cellular, and Wireless Communications Network Infrastructure**
- **Online Gaming and Network Infrastructure**
- **Wearable devices**
- **Nano Sensor Technology**
- **Grid Computing**
- **Peer-2-Peer Computing**

The wireless Internet will most likely lead the IPv6 evolution. Wireless devices with IPv6 will be used in the home, the workplace, in cars, and in consumer electronic devices. As IPv4 lead to wired networks in business and in homes, leaving mainframes behind, likewise IPv6, in relative terms, will leave the wired Internet behind in time too. IPv4 has been in use for over twenty years, yet the World Wide Web did not exist until ten years after the introduction of IPv4. By deploying IPv6, new, innovative applications will be realized, some that can be developed now, but many will follow in years to come, as the U.S. Internet evolves. This will provide a foundation for innovation within the U.S. as the web did in the mid 1990's. If the

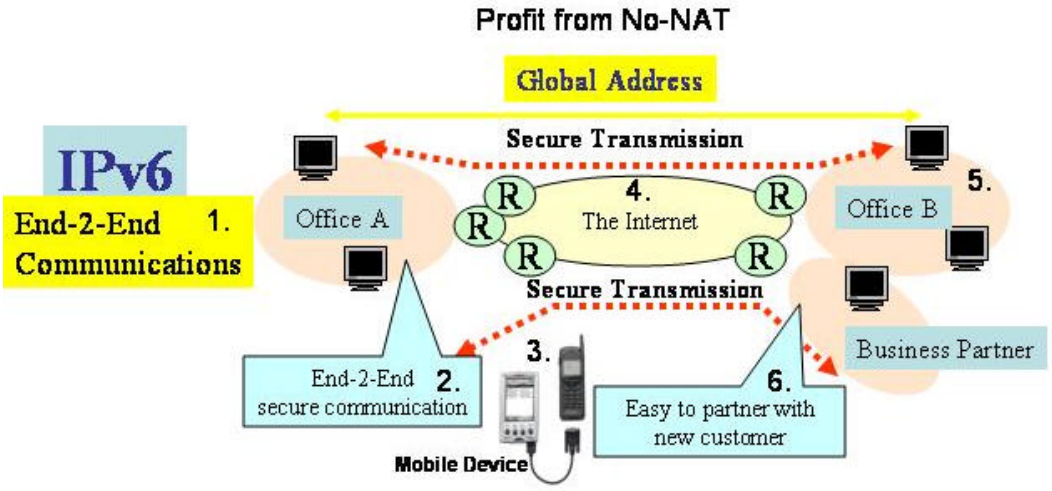
US does not provide that foundation, risks are that other countries might lead that innovation, creating a disadvantage for the US economy.

The task force understands that the use of Network Address Translation devices (NATs) and the adoption of address conservation practices, such as Classless Inter-Domain Routing (CIDR), have slowed the consumption of available IPv4 addresses. We seek comment on the accuracy of this understanding. While the adoption of NATs over the last decade has apparently slowed the consumption of IPv4 addresses, we understand that NATs have contributed to the development of separate, privately addressed networks that are interconnected with the public Internet. Because NATs act as gateways between the public Internet and users with private network addresses, each NAT device could potentially represent a single point of failure for traffic moving between a privately addressed network and the public Internet. We seek comment on the effects that NATs (as well as CIDR and other address conservation strategies) may have on network performance and network reliability.



1. Node can only communicate out of site with peer through a NAT and has reduced capability of applications.
2. Communications has only one entry point to Office A node through one router and single point of failure.
3. Attacker only has to masquerade the packet between the NATs and they will be able to enter either network.
4. Peer-to-Peer communications and security can only be done within a site behind a NAT.
5. Security on the LAN is only by NAT once attacker gets passed the NAT it can attack a node on any LAN.
6. Interoperability between peers out of the site, suppliers, partners, or other vendors has greater cost, if even possible.
7. A node not within the site cannot initiate a connection with a node behind a NAT site reducing communications.
8. Mobile Nodes cannot roam out of a site with a private address because it does not exist out of the site.
9. NAT state for translation, namespace, security, and routing must be maintained at all entry/exit points to the network.

All of these points are a cost to an entity deploying networks who need for their business or operation to communicate out of the site to peers or applications. Not being able to perform communications and not having true security associations with peers out of the site for one-way communications has a significant cost. Each of these points also causes extra software and state to be maintained and administered by the network operations within the entity.



1. End-2-End communications permits nodes to communicate in the site or out of the site without NAT additions.
2. End-2-End security methodology and architecture permits pervasive security in the site, and out of the site.
3. Global Addresses and End-2-End communications and security permit nodes to roam and be mobile out of the site.
4. Entry into to out of the network does not have to be a single point of failure and provide redundancy and failover.
5. A node in another site can initiate a peer-2-peer communications session with a node in another site.
6. Partners, Suppliers, or Applications can now be accessed as peer-2-peer nodes or applications.

Profit from No-NAT can be realized with greater application support and availability which cannot run in a NAT Environment, communications with peers can be initiated by a site or peers out of the site, security is based on security within the node and provides End-2-End secure communications trust and privacy model, and the business options are greater for communications and the cost of managing all the NAT state is removed.

NAT is not a security mechanism and networks that use NAT require other security mechanisms to secure the perimeters of the Network. NAT also does not permit E2E networking, and thus it does not permit E2E security, and more importantly for government operations peer-2-peer security, as E2E is defined previously in this response. The two figures above depict the cost of using NAT and the single point of failures, and then the profit from not using NAT.

NAT has no traceability to the source of a packet, and in the case of twice NAT the destination either. This is another security and operational problem from NAT.

Please see further discussions regarding NAT below in End User Applications section

1.2. Purported Security Improvements (NTIA RFC Section II-B)

The task force seeks comment on the ability of IPv6 to improve the security of information transmitted over IP networks. In general, we ask commenters to address any characteristics of IPv6 that directly or indirectly enhance network security compared to IPv4. Conversely, we also seek comments on any features of IPv6 that may degrade network security compared to IPv4.

There are no known features in IPv6 that will degrade network security. However, as any new technology, new software introduces new possible security holes.

We also seek specific comment on Internet Protocol Security Architecture, or IPsec, as it relates to an examination of the relative merits of IPv4 and IPv6. IPsec is a data security specification that is designed to protect the integrity and confidentiality of data traffic carried over the Internet. We understand that while IPsec in IPv4 is functionally equivalent to that available in IPv6, IPsec support is optional in IPv4 networks. Because IPsec is a standard feature of IPv6, will IPsec be easier to use with IPv6 than with IPv4 and, therefore, more widely used? If IPv6 adoption leads to the elimination of NAT devices on the Internet, is it more likely that IPsec will work better as a widely used, end-to-end security mechanism? Are there critical IPsec implementation issues that are independent of the version of IP employed? To what extent will a successful IPsec implementation depend on the development of workable trust models that deal adequately with issues such as public-key management and the adoption of effective security policies? The task force requests comment on these and any other issues involving IPsec, relevant to the growth of IPv6.

IPsec will not work better with IPv6, but will become more widely deployed.

IPsec will not be easier or more difficult to use with IPv6, it will be equivalent to IPv4 only when using unique and permanent IPv4 global addresses at end nodes. The issue is if you want to build a clean network with a billion nodes using globally routable addresses, IPv4 cannot provide the addresses required. This is the case for China, seen from a bigger picture point of view, as one well known example.

Because IPsec is mandatory for IPv6 it can be assumed by users of networks planning to adopt IPv6 for its operational advantages over IPv4, and that cannot be assumed for IPv4 because it is optional. IPv6 can make IPsec pervasive as a network security method providing the first barrier to intrusion of the IP payload by attackers.

The use of IPsec requires the use of PKI trust models and PKI management absolutely for both IPv4 and IPv6. It is imperative that some entity foster and support the strategy and implementation of PKI within the U.S. and the most likely candidate to lend that hand of support is the U.S. Government.

IPsec implementation issues of IPv6 and IPv4 are equivalent.

We understand that IPsec also permits address authentication, thereby assuring the recipient that a particular message is actually coming from the purported addressor. We seek comment on whether this feature could potentially deter "spoofing" attacks or could facilitate tracing of undesirable messages. Specifically, interested parties should explain how implementation of IPv6 or IPsec will accomplish those ends. As noted, moreover, IPsec is also available in IPv4. To what extent would deployment of IPv6 further national security and law enforcement interests over and above the security features and capabilities available via IPv4? The task force also understands that persons sending messages via the Internet can attempt to conceal their identities and addresses by, for example, operating through anonymous servers and relays operating at multiple protocol layers (e.g., NATs, mailrelays, proxies). Assuming that "network traceability" is an important objective in cyber security, to what extent would adoption of IPv6 improve the ability of network operators and law enforcement officials to identify accurately the true source of malicious or illegal network activity?

IPsec uses the IP address as a Security Parameter Index identifier for IPsec operations. If the key management is not compromised then the assumption that a particular message is actually coming from the purported address is a correct assumption.

The security advantage of IPv6 is that it permits an E2E secure model for Law Enforcement, as one example, personnel so the trust model is peer-2-peer, and there is no intermediate party that

can determine the contents of the packet. The reason this is not an advantage of IPv4 is that IPv4 is now widely deployed with NAT. NAT destroys the properties of E2E and a peer-2-peer security trust model. This is not acceptable for highly secure operations such as Law Enforcement, and other network operations such as a life support wearable device, which only the patients doctor can communicate with over a network or the Internet. It is not an issue of IPsec, but the pervasive use of NAT with IPv4.

The use of IPsec with PKI will reduce the ability for attackers to enter networks far greater than currently on networks. The model requires packets entering a network to have obtained a security method to encrypt or authenticate the packet to enter another network. IPsec requires in implementation that every packet that enters the receiving node must be checked that a packet has an IPsec header or a policy can reject that packet or send to an Intrusion Detection monitoring system, as one example.

Regarding proxies and relays in less trusted secure environments they can simply forward the packet, or in a highly trusted environment the packet can be verified with IPsec on those nodes. In either case the packet cannot do harm from its content unless the key has been compromised. The key and algorithms supported by IPsec are beyond the scope of this response.

For additional issues regarding Security with IPv6 please see reference below at our NAv6TF web site:

http://www.usipv6.com/2003arlington/presents/Renee_Esposito_and_Rich_Graveman.pdf

1.3. End User Applications (NTIA RFC Section II-C)

Apart from its expanded addressing capabilities and purported security improvements, we understand that IPv6 has also been designed to address other important user needs, including reducing network management burdens, simplifying mobile Internet access, and meeting quality of service needs. We ask commenters to explain whether and how IPv6 accomplishes these and other functions in a manner superior to IPv4. We also request that commenters explain the importance or value of the improved capabilities afforded by IPv6. To the extent possible, we ask that commenters provide examples of how these improved capabilities of IPv6 could benefit current users of IPv4 (e.g., cost savings, time savings).

IPv6 has technology advantages over IPv4, and most of them will not be seen by the end user any more than users see features added to other extensions to the Internet Protocol suite, sensors on their automobiles, or from any infrastructure technology evolution. This is important to note when discussing IPv6 benefits to end user applications, and again IPv6 and IPv4 are infrastructure components. This section provides an overview of some of the advantages of IPv6 that will benefit End User Applications deployment with IPv6.

These are also some of the operational advantages of IPv6 that are of benefit to the Department of Defense and part of the reason for the IPv6 mandate in June 2003.

IPv6 is an essential catalyst for the Next-Generation Internet, which will provide an evolution to a more pervasive use of the Internet and networking in general. The current Internet, using IPv4, is insufficient to support the business and operational preconditions for peer-to-peer applications and security, billions of mobile devices, sensor networks, and the requisite distributed computing infrastructure to support a mobile society. The IPv4 "band aids"

applied to permit the current Internet to keep it operating has created additional operational costs and reduced operational capabilities for users and networks.

IPv6 Supports End-2-End Applications Security

There are several schools of thought and opinions on the issue of address space and all project different results, depending on one's mathematical view and philosophy regarding use models, as previously stated. There is also the effect of disruptive technology, which can make moot any projections of IPv4 address space. In that sense, rationing is justified and intelligent. The NAv6TF believes we already are experiencing the initial quake of disruptive technology, and that there is a need for users and markets to evolve further with a basic tenet that E2E applications and security are a priori for that evolution to begin. The NAv6TF believes that *Network Address Translation* (NAT) is about control, but that control comes at a cost of the freedom to use peer-2-peer computing over client to server-only computing.

Two users on the Internet today generally cannot each initiate peer-2-peer communications with each other because their location and identity are not available to each other from two disparate networks. In addition, security between them must trust a third party, and absolute private communications is impossible. The reason is that the Internet has evolved so that users are generally behind NATs that preclude peer-2- peer communications, or the exchange of private security credentials. Some will say this affords users security on the Internet. Although NAT does provide a denial-of-service perimeter, it also provides a denial of service to a direct trust relationship between peers. IPv6 is the only way to have peer-to-peer security for the Next-Generation Internet at a reasonable cost and a true privacy trust model on the Internet.

In the field of network computer science when engineers and architects implement translation functions in a solution, a cost is incurred that would not exist without translation. This is due to the need to keep *state* before, during, and after the translation. In software engineering terminology, these *state machines* add time and space costs to the entire operation. In addition, a NAT box is a single point of failure, because it is the only point on the network where a user can exit or enter when translation exists. Translation also does not permit the use of all functions possible without translation because too many participants need to know the mappings, and each function requires a separate state to be maintained, and the time + space costs increase exponentially. The time + space costs of NAT to keep the Internet operational have been passed on to every part of the current Internet business, consumer, and government market sectors, and cannot even support the original functions of the Internet before NAT. The current Internet has no hope of supporting the functions of the Next-Generation Internet required or of offering a solution to the great digital divide that exists currently and is increasing daily.

The good news is that IPv6 is evolving, early adopter deployment has begun, and vendors have delivered initial IPv6 products to the market. IPv6 will not require NAT, and the infrastructure supports a stateless architecture for the Internet, using stateful properties only where they can be used without a translation attribute or policy. IPv6 inherently supports mobile communications, billions of devices, and sensor networks that will be pervasive at a reasonable cost and provide the option to eliminate the digital divide within the current Internet.

IPv6 Supports a Stateless Node Discovery Architecture

A Next-Generation Internet base technology advantage for mobile user devices, ad hoc networks, mobile network providers, and generally for all users is the *Stateless Node Discovery Architecture* inherent within IPv6.

IPv6 nodes can discover each other and form IPv6 addresses to communicate on a network using what is called *Neighbor Discovery* and *Stateless Autoconfiguration*. IPv6 supports an extensible stateless node discovery paradigm, which provides the following:

- **Discover presence of nodes on the network**
- **Discover Datalink Layer nodes on the network**
- **Discover routers on the network**
- **Discover link configuration parameters on the network**

These features permit an IPv6 node to obtain and maintain information about the accessibility of another node on the network for communications. Node Discovery is the predecessor to the node obtaining an address from IPv6 autoconfiguration. This core IPv6 technology framework also permits nodes to communicate on networks where there are no routers within an ad hoc network.

A host, when booted on an IPv6 link, first creates a *link-local* address by taking the architecturally defined prefix in Neighbor Discovery FE80, and appending an *End User Identifier* (EUI), determined by the host, to that prefix. This link-local address is then verified on the link that it is not duplicated with other link-local addresses on that host's link. This host communication is performed using link IPv6 multicast packets, to avoid duplicate link-local addresses, which are not permitted on an IPv6 Link.

The host then uses the link-local address to send on the IPv6 link *Neighbor Solicitations* and all other hosts on that link see those multicast solicitations, and then return *Neighbor Advertisements* to the host. After this communications process, all nodes on the IPv6 link can now communicate and communication was accomplished without the use of servers or routers in a stateless manner.

The host also listens for *Router Advertisements* on the IPv6 link (or sends *Router Solicitations*), which provide address prefixes, link configuration parameters, and information as to whether or not to use a stateless or stateful method for address assignment, and additional network configuration parameters using the *Dynamic Host Configuration Protocol* for IPv6 (DHCPv6).

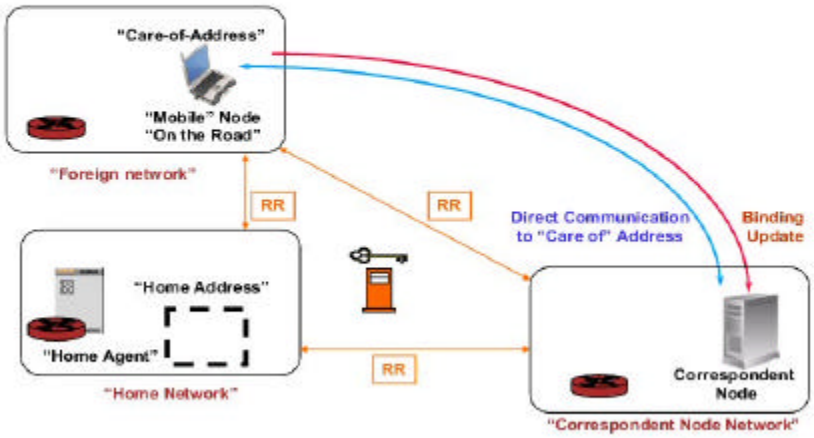
If the host is instructed to use the stateless method for address configuration, then it can use the router prefixes announced to form IPv6 addresses from those prefixes by appending the EUI determined from the link-local address to that prefix to create an IPv6 Address. IPv6 supports multiple address types within the address architecture. If the host is instructed to use the stateful method for address configuration, then DHCPv6 can be used to configure additional hosts' addresses.

Users will benefit from the IPv6 stateless advantages for network communications, and they

will exist behind the wall of the user to provide a new and improved set of mechanisms for Node Discovery and Address Autoconfiguration far more robust and efficient than using the current IP Version 4 (IPv4) protocol. The IPv6 Stateless Architecture for Node Discovery permits a new model for node communications on links.

The Mobile IPv6 Technology Value Proposition

Mobile IPv6 offers many improvements over Mobile IPv4. Mobile IP as a technology permits users to remain connected across wireline (for example, Ethernet, xDSL) and wireless (for example, 802.11, cellular, satellite) networks, while roaming between networks. This permits users to stay connected while on the way to the airport from home, rather than shutting down their personal digital assistant (PDA)/laptop at home, and reconnecting at the WiFi location at the airport.



The figure above depicts the multiple phases of a mobile IPv6 connection. On the home network, a mobile node receives its home address as any IPv6 node. The mobile node registers that address with the *Home Agent,* which is a router that keeps the location information for the mobile node when it moves to a foreign network, stores the mobile-node *careof address* when the mobile node is away from home, and performs other functions on behalf of the mobile node when it is away from home. A peer node that the mobile node communicates with is defined as the *Correspondent Node* (which may be stationary or mobile).

Security between the mobile node and home agent can be accomplished using the *IP Security Protocol* (IPsec) architecture. This permits secure communications between the mobile node and the home agent. When a correspondent node receives a packet from a mobile node, it first checks its binding caches to see if it has a cache of the mobile-node care-of address, and if it does not, the correspondent node sends the packet to the mobile-node home address. The home agent receives all packets sent to the mobile node when it is away from home and then tunnels the packets to the mobile-node care-of address

To permit a mobile node and correspondent node to communicate directly, without going through a home agent, requires the use of *Mobile IPv6 Route Optimization*. First the connection

to the correspondent node needs to be secure from the home agent and directly from the mobile node. In the figure, that is done using a procedure defined as *Return Routability* (RR) within the Mobile IPv6 protocol. The network path between the mobile node and correspondent node is secured through the RR procedure.

Mobile IPv6 uses the extensibility of the IPv6 protocol defining new Neighbor Discovery messages and types, *Routing Header*, and the use of the *Destination Option* in an IPv6 packet, which does not exist in IPv4. Discussion of those extensions is beyond the scope of this article, and is left as an exercise for readers to read the actual Mobile IPv6 specification.

Mobile IPv6 has core technical operational advantages over Mobile IPv4, as follows:

- **There is no need to deploy special routers as "foreign agents," as in Mobile IPv4. Mobile IPv6 operates in any location without any special support required from the local router.**
- **Support for route optimization is a fundamental part of the protocol, rather than a set of nonstandard extensions.**
- **Mobile IPv6 route optimizations can operate securely even without prearranged security associations. It is expected that the route optimizations can be deployed on a global scale among all mobile-node correspondent nodes.**
- **Support is also integrated into Mobile IPv6 for allowing route optimizations to coexist with routers that perform ingress filtering.**
- **The IPv6 *Neighbor Unreachability Detection* assures symmetric reachability between the mobile node and its default router in the current location.**
- **Most packets sent to a mobile node away from home in Mobile IPv6 are sent using an IPv6 routing header rather than IP encapsulation, reducing the amount of resulting overhead compared to Mobile IPv4.**
- **Mobile IPv6 is decoupled from any particular link layer because it uses IPv6 Neighbor Discovery instead of IPv4 *Address Resolution Protocol* (ARP). This also improves the robustness of the protocol.**
- **The use of IPv6 encapsulation (and the routing header) removes the need in Mobile IPv6 to manage tunnel soft state.**
- **The dynamic home-agent address discovery mechanism in Mobile IPv6 returns a single reply to the mobile node. The directed broadcast used in IPv4 returns separate replies from each home agent.**

Also see the following NAv6TF brief on IPv6 Advantages:

http://www.usipv6.com/2003arlington/presents/Yanick_Pouffary.pdf

http://www.usipv6.com/2003arlington/presents/Carl_Williams.pdf

One potential benefit of IPv6 is that its increased address space may further an original vision of the Internet. The task force understands that the Internet address space was originally designed to be a unified open scheme, connecting all users and nodes (each with its own unique address), as defined by the IPv4 addressing convention. A central idea was to allow users to communicate and run applications (e.g., Voice over IP (VoIP), gaming, or file exchange) with each other, across the Internet, on a peer-to-peer basis. Interested parties are encouraged to comment on the desirability and potential effort required to return the Internet to a unified open scheme as originally designed.

All of the applications listed above require the previous advantages discussed from IPv6 and more importantly they will be deployed using mobile networking as an assumption.

The combination of VoIP and WiFi promises to have an exciting future by enabling a new class of wireless enterprise mobility applications. Enterprises are now beginning to deploy VoIP-WiFi as an alternative to private radio in campus and industrial environments. For enterprises customers unhappy with the limited connectivity of private radio the ability of VoIP-WiFi to enable PSTN and IP access using inexpensive PDAs is a major step up. Unfortunately when users compare the seamless mobility of cellular with WiFi's hard hand off and dropped connections, VoIP-WiFi a step down! Thus before VoIP-WiFi can become a main stream solution WiFi's poor mobility needs to be addressed - and that is where IPv6 can come in.

IPv6 incorporates a number of mobility features that make it a natural fit for VoIP-WiFi solutions. By embedding IPv6 routers into Access Points and switches vendors can create fast hand off solutions that can equal the capabilities of their more expensive cellular cousins at a fraction of the cost. Leveraging a set of features grouped under Mobile IPv6 (or MIPv6) WiFi vendors can leverage IPv6's ability to track and forward traffic to users as the move from Access Point to Access Point. The advantages of a Mobile IPv6 powered VoIP-WiFi solution includes:

- **Unlike conventional WiFi switch solutions that can only provide mobility within one network, a Mobile IPv6 solution could provide connectivity across multiple networks and sites (even in different countries). For enterprises and (more importantly) multi-national corporations the ability to deploy a single connectivity solution can be a major cost saver and productivity enhancer. For example a plant operator in Italy could use his WiFi PDA to call a co-worker in Malaysia on a similar device. Moreover because WiFi is a global standard when the Italian manager went to Malaysia his WiFi PDA would still be "on-net".**
- **Mobile IPv6 provides WiFi vendors with intelligent mesh routing logic that can be used to build over-the-air Wireless Distribution System (WDS) trunks. Leveraging a feature call stateless node discovery MIPv6 enhanced Access Points could discover adjacent nodes and automatically provision an over-the air trunk. For industrial sites where Ethernet interfaces are difficult to come by (like a shipping dock) the ability to provide WiFi coverage with only power is an important benefit.**
- **And finally, when users are outside campus sites they could still use their WiFi PDAs to talk to co-workers (though without the mobility benefits they enjoy in their enterprise networks). Traveling employees could leverage public hot spot services to enable connectivity back to their facility without the cost of long distance charges.**

With the availability of <$50 Access Points with high powered CPUs from Taiwan, building an IPv6 Access Point is quite easy. Thus the harder task is to develop an interface to VoIP system

as well as providing connectivity between enterprise sites. Fortunately there is good availability of VoIP developer solutions with SDKs as well as a number of IPv6 connectivity solutions that enable site to site connectivity over IPv4. Given that all the components for a MIPv6 powered VoIP-WiFi solution are available off-the-shelf, vendors and even system integrators could easily prototype a solution within a few months. Also see the paper below that enters more depth for use of IPv6 with WiFi and VoIP as enabler application for IPv6.

www.nav6tf.org/slides/IPv6ApplicationNote3rdgenerationWiFi-Oct9-2003.pdf

VoIP has grown exponentially over the past few years as ISPs and competitive carriers deploy SIP based solutions to enable toll by-pass services. Unfortunately customer churn and emergence of inexpensive enterprise gateways has meant that VoIP toll by-pass services have turned into a commodity business for nearly every operator. Thus the key to survival is to identify potential VoIP applications that are unique enough to discourage customer churn and offer operators the ability to charge premium rates.

By provisioning IPv6 to end customer sites (either through trunks or tunnels) service providers have the ability to create secure VoIP services that can be offered as a compliment to a VPN service or on a stand alone basis. The advantage of an IPv6 based VoIP service includes:

- **Ability to deploy end-to-end signaling and encryption that enables customers to have a highly secure voice communications solution that is deployable on a global basis. For multi-national firms like financial companies the ability to protect client information can be an important competitive edge and business necessity.**
- **Ability to provide secure VoIP connectivity to mobile users via the use of IPv6 tunnels. This would facilitate enabling traveling executives to have a secure call with their office even if using a public hot spot or in-room hotel service.**
- **Ability to support other services such as Instant Messaging within the same network infrastructure. Once a laptop or desk top is connected, users could launch multiple clients even though they are not integrated.**
- **Operators also have the ability to associate services with address ranges - thereby restricting communications within specific groups of employees.**

The primary challenge the deploying an IPv6 based VoIP solution will be PSTN access and its inter-operability with existing SIP applications. For customers who want PSTN connectivity the appropriate solution would be to deploy a SIP gateway at the client site (eliminating a carrier hole in the middle). For customers who want to leverage existing SIP applications but do not need PSTN connectivity moving all of the existing SIP devices to inside the IPv6 cloud is the best option.

For further study: There is a new generation of codec's that enables high quality audio even across high lossy networks like WiFi. Operators may also wish to explore the availability of IPv6 based SIP devices (with/without encryption). Longer term operators may wish to explore pure software based end-to-end client solutions that probably offer the best cost structure and security.

The online gaming business is enabling new types of shared entertainment experiences as faster desktops, networked consoles like Playstation 2 and Xbox Live and inexpensive broadband access becomes ubiquitous. Based on current market, IDC estimates that online gaming will be a $2.3 Billion business by the year 2005. However one challenge developers are having is deploying server architectures which can cost effectively handle the computation load that many of today's immersive games demand (i.e. many games cost as much as $100/seat in compute power). Another challenge developer's face is providing connectivity

between teams of players on different servers. Simply moving more players to bigger servers doesn't work as the costs climb faster than the revenue – thus the solution is to develop a more cost effective distributed computing and connectivity solution between players and servers.

By marrying the persistent connectivity benefits of IPv6 with the computational power of GRID computing, online game developers have new powerful tools to create the next generation of online games. First, by connecting players to GRID servers via native or tunneled IPv6 connections clients can have unique and addressable network interfaces from which they can interact with the servers as well as other players. Second, as requests to join a game come in the GRID engine, player traffic can be routed to the most appropriate server based on the load as well type of game. Some of the benefits of this type of connectivity model include:

- **-Even though player connectivity is based on IPv6, native v6 connectivity is not required for clients via the use of 6-4 tunneling. The persistent IPv6 client address enables game primitives to be delivered to players irrespective of what server they may be on or where in the world they are calling in from. Thus two friends in different battle fields will be able to share their experience even though they are on separate servers (i.e. environments). Moreover as the calls are inbound players even on NAT connections will be able to participate.**
- **-The large swings in computational power can be softened by sharing GRID computing resources globally. Thus late night games in California could leverage unused capacity in Asia where people would be working during the day (we hope). Moreover a single network could also support multiple games (i.e. be a shared resource between different online companies) to improve the economics.**
- **-And finally, the networked GRID solution could even allow gamers themselves to donate their machines when they are away from their homes in exchange for game credits. The increase of residential broadband and dedication of gamers to always buy the fastest machine possible makes them ideal compute resources!**

The biggest challenge in leveraging an IPv6 enhanced GRID network is that the online game software would have to re-designed so that to work in a distributed computing environment. For example tasks which are serialized may need to be re-written so that they can be distributed by a GRID engine. Additional the users' clients would have to be enhanced to support connectivity from multiple processes (i.e. players or environments). While the work is non-trivial, it does open up a new world of possibilities in terms of what is possible.

These applications depicted for IPv6 cannot be pervasive unless the Internet is restored to an E2E model with IPv6.

As noted above, the use of NATs has contributed to the development of separate, privately addressed networks that are interconnected with the public Internet. At the same time, various other devices are apparently being deployed throughout the Internet to increase network functionality. Such devices, often referred to as "middleboxes," appear to be proliferating in response to demand for capabilities that may include not only network address translation, but also firewall protection, intrusion detection systems, and other features. There is some concern that use of NATs and other middleboxes may block or inhibit the growth of peer-to-peer applications. Some observers assert that deployment of IPv6, by vastly increasing the available address space, will eliminate the need for NATs in particular, which, in turn, could lead to a proliferation of new peer-to-peer applications. On the other hand, NATs and other middleboxes may persist in an IPv6 environment because they may be useful for other reasons, including affording users some protection from hackers launching attacks

across the public Internet. We request comment on these and any other issues involving NATs (or their equivalents) and middleboxes, related to the growth of IPv6.

The assumptions above are in fact true and IPv6 does restore the E2E model required for applications to be peer-2-peer, but IPv6 can support the use of Network Address Filters (NAF), which can be viewed similar to the functions of current Firewalls. The advantage of IPv6 is that NAF's will not have to also perform address translation as part of its function as a middle box. This permits a deployment model where networks can permit E2E but with a 3rd party additional trust model. Bob and Alice can talk but they communicate through Jane who speaks to Bob and Alice. The NAF is Jane and the removal of Jane is the trust model between only Bob and Alice. IPv6 can support both models and also likewise for proxy servers and relays.

But, all of the failure modes and loss of E2E security from NAT will have been removed.

Notwithstanding the criticisms of NATs, some have argued that NATs will not preclude peer-to-peer devices and applications. The task force requests comment on the accuracy of this assertion. Similarly, we seek comment on the effects of middleboxes on the availability and efficacy of peer-to-peer devices and applications. If NATs or middleboxes do interfere with peer-to-peer interactions, can "work arounds" be developed for particular applications? If work arounds can be developed, to what extent will they adversely affect the performance of the associated applications? Will those work arounds scale well (i.e., continue to function seamlessly and efficiently as the number of applications and users increases)? As importantly, what additional costs (in time, money, and complexity) will firms incur to develop work arounds for particular applications in order to accommodate NATs and middleboxes?

Please see previous response and see RFC 2993 Architectural Implications of NAT below URL:

ftp://ftp.rfc-editor.org/in-notes/rfc2993.txt

Also there is not one type of NAT deployment model, but many models. Workarounds for NAT increase cost, failure modes, require custom code to applications, and it has not been proven by implementation to work in the market to support E2E or peer-2-peer.

1.4. Network Evolution (NTIA RFC Section II-D)

Although the task force requests comments on the potential benefits of IPv6, we understand that IPv4 networks can incorporate many of the features and capabilities commonly associated with IPv6. Thus, some observers have claimed that the increase in address space afforded by IPv6 is the only compelling reason for adopting the new protocol, not the availability of other capabilities. The task force seeks comment on this assertion. Specifically, the task force requests comment on the ease with which each feature and capability associated with IPv6 can be implemented over IPv4 networks and whether IPv4 implementations will perform as effectively as IPv6 networks. Will IPv4 networks providing IPv6-associated features and capabilities suffer a performance penalty as compared to IPv6 networks? We request comment on whether any IPv6 feature or capability cannot be readily implemented over IPv4 networks. We ask commenters to identify the cost of implementing such features or capabilities on IPv4 networks, as compared to the cost of implementing IPv6 alternatives? We request comment on whether any IPv6 feature or capability, or set of features or capabilities is markedly superior to its IPv4 alternative, in terms of implementation cost or relative performance, such that an IPv6 implementation would be the clearly preferred choice over IPv4.

IPv4 cannot possibly do what has been presented in this response by the NAv6TF. We stand by our responses to the Huston ISP "Waiting for IP version 6" by our parent organization the IPv6 Forum, in the NTIA footnote for this section of the document. IPv4 is not an alternative to IPv6 in any way, shape, or form technically. It is impossible to achieve the operational advantages discussed in this response with IPv4.

Another Australian effort for IPv6 to note, The Australian Higher Education Bandwidth Advisory Committee (HEBAC), which was established jointly by the Commonwealth Minister for Education, Science and Training, Dr Brendan Nelson, and the Minister for Communications, Information Technology and the Arts, Senator Richard Alston, made a series of recommendations which resulted in Dr Nelson announcing that the Commonwealth would allocate $42.5 million over three years to support the recommendations. Dr Nelson said that the Queensland project is a concrete example of the way in which collaboration between the Commonwealth, AARNet and the private sector can produce an Australian research and education network which is of benefit to all. State and Territory governments have expressed their willingness to be involved in such initiatives. With co-operation from all parties, Australia can build an advanced network which will serve the education and research communities well both now and in the future and ensure that our research strengths remain globally competitive.

www.aarnet.edu.au/engineering/wgs/ipv6/charter.html

The recommendation by AARNet is to say a clear no to NAT and yes to IPv6, see the presentation of the Executive Director of AARNet (se slide 38):

http://www.gu.edu.au/conference/questnet2003/docs/Jonathon_Potter.ppt

Most significantly IPv6 can help bridge the digital divide that currently exists between the developed world (in particular the US, where IPv4 address space was in good supply in the early years of the Internet) and emerging Internet nations in Eastern Europe, India, South America, Mid-East, Africa and Asia. IPv6 promises a level playing field for Internet Protocol application development and deployment where IP addresses are readily available the world over, not a luxury for a privileged minority. The NAT technology, business model, and the implications discussed in RFC 2993 are an inhibitor to worldwide Internet global E2E communications.

Bridging this divide is now a global objective. But the uneven diffusion of technology is nothing new. There have long been huge differences among countries. The bitter irony of the Internet phenomenon is that while in theory the global network of networks is open to all, the vast majority of the world's populations remain cut off from its economic and educational benefits. Only 8% of the world population has access to the Internet, compared to 20% for the phone system. Likewise not all of our U.S. citizens have access to the U.S. Internet either, especially the poor.

Affordable technologies more appropriate to developing economies could include solar-rechargeable batteries that would allow mobile phones to be used even in areas lacking electricity lines. The Internet could achieve a far better penetration through wireless access technologies, due to their dual benefit of being faster to deploy in any area (wide-scale cabling is not required) and of "giving wings" to the Internet with their mobility.

The PC era will be overtaken by the non-PC world (PDAs, Smart Cell Phones, personal network devices, etc). The Docomo I-Mode advanced mobile data communication initiative in

Japan achieved more than 30 Million users in just two years of deployment and is perceived by its users as the Japanese Internet. Now, adding IPv6 to it would give the developing world immediate access to not only the Internet, but to many next generation applications currently under development. If we fail to provide access to digital technology to countries in the developing world we are, essentially, denying them an opportunity to participate in the new economy of the 21st century. The precepts apply to the U.S. choice to evolve or not to evolve to IPv6 and if the U.S. is to benefit from IPv6 and the global economy and Internet communications advantages from a restoration of E2E.

The task force also seeks comment on whether there are any potential performance impairments associated with the adoption of IPv6. For example, would the increased size of the IPv6 header have a significant impact on voice quality in VoIP applications, which are generally sensitive to latency? If, for example, IPv6 header compression schemes are used to mitigate potential performance issues (e.g., increased transmission latency), do such schemes require more router processing effort resulting in increased end-to-end latency? To be widely implemented, does IPv6 require new routing technologies (e.g., new versions of BGP-4) that could result in significant end-to-end system design and operational challenges? Are there any drawbacks due to inherent limitations of the IPv6 protocol design? Are there drawbacks resulting from immature or (currently) impractical hardware and software IPv6 implementation technologies?

There are no performance penalties from IPv6 for networking that the NAv6TF has seen from extensive interoperability events and testing, most recently on the new North American IPv6 semi-commercial test bed Moonv6 www.moonv6.org and see the following report at that site.

ftp://ftp.iol.unh.edu/pub/ipv6/Moonv6PhaseI_wp.pdf

An objective met by vendors shipping IPv6 products is no performance degradation of IPv6 over IPv4 performance.

We understand that the deployment of IPv4 networking infrastructure continues to evolve in ways that can effectively use existing and emerging transport and transmission system infrastructures (e.g., multi-protocol label switching (MPLS), asynchronous transfer mode (ATM), Frame Relay, optical, wireless, digital subscriber line (DSL), ethernet). Does IPv6 deployment depend on modifications to these underlying networks or require new transport and transmission systems to be implemented? Will IPv6 be able to utilize presently underused capabilities of transport and transmission networks to support new types of applications or to provide more efficient networking services for existing applications? We also seek comment on any spectrum management issues that might arise when IPv6-based wireless and hybrid networks are used to support mobile and fixed applications. Because IPv6 offers new capabilities, do the transport layers (e.g., transmission control protocol (TCP), user data protocol (UDP)) need to be modified to support both existing and new applications? Further, we request comment on whether and to what extent the transport layers need to be modified in order to realize the full capabilities of IPv6, including the potential for significantly improved IP network performance.

These concerns are transparent to IPv6 or IPv4 and concerned with the upper and lower virtual layers of the IP protocol suite. IPv6 as IPv4 is transparent to link technology.

1.5. Other Benefits and Uses (NTIA RFC Section II-E)

The task force seeks comment on the range, attractiveness, and potential economic impact of new services that will emerge with the growth of IPv6. Specifically, what new service possibilities does IPv6 provide

beyond those available using IPv4? We also ask commenters to identify other benefits and uses of IPv6 and to describe the potential economic and other impacts of such developments. For example, does VoIP represent the kind of application that could drive IPv6 adoption, and if so, how? Will IPv6 improve the performance of VoIP? Please identify other applications that could drive or benefit from the adoption of IPv6. Are there applications that could thrive with only a partial implementation of IPv6?

Viewed from a technical perspective, IPv6 has many benefits which enhance its use model, including the following:

- **Larger address space for end-to-end global reach ability and Internet scalability.**
- **Simplified IPv6 data packet header for extensibility and performance**
- **Support for routing and route aggregation, making Internet backbone routing more streamlined and efficient (the IPv4 Internet backbone contains data routing information for over 130,000 networks; with IPv6 this number could be dramatically reduced).**
- **Serverless ("stateless") IP autoconfiguration, easier network renumbering, and much improved plug and play support. This is the most important future benefit for the Department of Defense and Home Land Defense communications.**
- **Prefix Delegation of IPv6 addresses to support renumbering and autoconfiguration.**
- **Security with mandatory implementation of IP Security (IPsec) support for all fully IPv6-compliant devices (IPsec implementation is not mandated in IPv4). The *use* of IPsec is not mandatory, but the mandatory implementation requirement of IPsec permits the user to have the option for secure communications.**
- **Improved support for IP Mobility inherent in IPv6**
- **Enhanced Multicast Networking Support**
- **Enhanced Anycast Networking Support**

IPv6 also enhances the vision and properties of Net-Centric Operations with the following benefits:

- **The Defense Department is leading industry in moving to the new IPv6 version. Future Defense systems must be IPv6 compatible.**
- **Secure and available communications**
- **Trusted sharing of network resources**
- **One-time handling of information, posted by authoritative sources**
- **Data posted as it is created**
- **Applications encourage discovery of data when and where it is needed**
- **Data is separate from applications**
- **Applications are posted for use**
- **Data is timely, accurate, complete, and easy to use.**

The future of network services lies in convergence, of voice, video and data to a unified IP architecture. Such integration will have significant benefits, and open up new opportunities for business and to offer services for residential users in the U.S. For example, the combination of VoIP, wireless LAN and SIP (Session Initiation Protocol) technologies could have a significant business impact: In the near future, a user will be able to run VoIP through an IP-enabled handset over a wireless local area network to a local SIP gateway which communicates via IP to another SIP gateway at the recipient's site. In such an environment there is no conventional "phone call" that has to be billed and paid for; the communication is purely IP-based.

With IPv6 everywhere, mobile users can get a seamless Internet experience and wireless operators will be just another type of ISP, albeit one that carries a significant proportion of voice traffic. Users can connect to whatever web sites they choose, log in to their corporate intranet (and be reached from that network), do VoIP, get streaming audio/video, and use whatever network applications they need. They will not be constrained to the limited set of value added network services the wireless operators will offer through their own portals. As a base protocol for a converged network, IPv6 is a significant enabler.

In the initial phase of GPRS/UMTS with a few millions of terminals, IPv4 is a perfectly reasonable solution, but to offer a scalable service that will cater for hundreds of millions of terminals, IPv6 is an imperative. By rapidly adopting IPv6, the U.S. Mobile industry has a unique chance to investigate and pioneer the future, together with all other Internet related players, whether they are fixed, cable, xDSL, ISPs etc. In so doing they will acquire a competitive edge which can be explored and exported.

There should be no reason for address space exhaustion in IPv6, and no need to resort to expensive and inefficient, non-scalable workarounds like schemes based on NAT. With simplified network renumbering methods, IPv6 will make network mergers easier to achieve, and the availability of the global address space of IPv6 will reduce the pressure for sites to use local private addressing and NAT (which can cause problems when two sites merge that use the same private IP address space).

While wireless operators may be the leading IPv6 adopters, IPv6 will also reach into all aspects of social life – the home, the workplace and schools and universities. It will enable end-to-end user services that have as big an impact on society as the business services will have on commerce. However, IPv6 is only an enabler. For the full social benefit broadband access to the home must become commonplace; at present xDSL and Cable Modem deployment is in its infancy, but combinations such as xDSL with wireless LANs in the home will – in conjunction with IPv6 addressing – open up avenues for consumer-electronics manufacturers and household appliance vendors to offer innovative new services.

While end-user and business requirements for advanced network services expand exponentially, IPv4 will not be able to cope. In the IPv4 world severe problems and limitations exist with band-aids such as NAT, and although these band-aids and extensions may prove valuable in the very near term, they ultimately will limit connectivity, interoperability, and performance in the long term for enterprises that are increasingly network-dependent.

As the transition to IPv6 takes place progressively and at different speeds by different industrial sectors, the need will arise to develop IPv6 transition and integration guidelines that will recognize that the coexistence of IPv4 and IPv6 will last many, many years, that the phasing out of IPv4 will be soft and gradual and that there will not be a magic date imposed on any particular industry (as was the case with Y2K) to move to IPv6, but rather that there will be an incentive to act before it becomes *too* late and *too* expensive.

It is now widely recognized – as exemplified by the position statements of the vast majority of router, host and mobile operators - that IPv6 will become critical to the operations and continued efficiency of day-to-day business activities in the new economy, and that there is ultimately no substitute for IPv6 when emerging multimedia, interactive, and transaction-oriented network applications start requiring high levels of connectivity.

The requirement for IPv6 implies a need for coordinated trials and tests of new IPv6-enabled devices – routers, hosts, PDAs, etc – which are more likely to succeed via both harmonization of standards and readily available interoperability events (such as those offered by University of New Hampshire, TAHI, and ETSI). The trials and roadmap processes are critical for IPv6 systems developers and implementers.

For IPv6-enabled services to be deployed in a timely manner, it is of key importance to structure, consolidate and integrate U.S. efforts on IPv6, to ensure that the necessary base of skilled human resources are available, that the research effort is sustained, that standards and specifications work is accelerated and that all sectors of the new economy likely to be impacted by IPv6 are fully aware of potential benefits accruing from the adoption of IPv6. U.S. Government funding towards advanced test bed deployment should be made available, and advertised appropriately. Where secure networks require cryptographic key exchange, the avenues for PKI deployment should be explored.

A concerted effort is hence required that will enable the competitiveness of the U.S. to be strengthened. Standards activity needs to be harmonized, while application developers, and organizations tendering for new IP-based services, should consider the IPv6-ready status and future proofing of the services they intend to deploy. Regulation frameworks need to be investigated, such that IPv6 deployment is allowed to proceed unhindered via natural market forces.

We will address the business and economic benefits and IPv6 as a stimulus for the U.S. economy in the next section.

2. Cost of IPv6 Deployment and Transition from IPv4 to IPv6 (NTIA RFC Section III)

The task force seeks information on the factors that may cause individuals and organizations to adopt IPv6 and, most importantly, the costs of doing so and the transitional issues presented. We encourage interested parties to provide us with specific detail, to the extent possible, on their IPv6 deployment strategies. What factors influence an organization's decision to adopt IPv6? For example, is there a certain level of IPv6-based traffic that will cause network operators or ISPs to convert their facilities to IPv6? Is there a critical point at which consumers' acquisition and use of IPv6-capable terminal equipment and applications will drive deployment of IPv6-capable infrastructure? To what extent, if at all, do these factors vary by provider (e.g., network operator, ISP, equipment vendors, applications providers) and by market segment (e.g., small and medium enterprises, large enterprises, academia, civilian government, military, individual users, and any other relevant segments)? As importantly, why are certain organizations choosing not to implement IPv6 at this time?

The NAv6TF as an entity does not deploy IPv6.

We do see markets for IPv6: Enterprise, Provider, Home Users, and Mobile Pedestrians.

An IPv6 device connected to the IPv6 Internet is theoretically capable of communications with any other IPv6 device. This enables any-to-any communication, but also favors the creation of community of interest focusing on business services and security. This is true all over the

world. Today, only about 8% of the world population has access to the Internet while 20% have access to the telephone network. This is a huge and growing market opportunity. U.S. companies and businesses need to expand the size and diversity of their markets. IPv6 enables a robust and scaleable e-commerce capability and opens new worldwide markets to U.S. businesses. IPv6 enables new applications and services which for one reason or another are not practical or scaleable with the IPv4 Internet. These include but are not limited to remote sensing and control, VoIP, peer-to-peer gaming, mobile internet, and home networking. US vendors and businesses will develop these and other new and innovative applications for the commercial and government markets.

An enterprise like the Department of Defense, General Motors, Dupont, or Chase Manhattan Bank will be able to extend their operational capabilities for their business from the advantages of IPv6, including but not limited to the previously stated applications for IPv6.

A Provider can extend peer-2-peer services in many creative ways that are not possible today with NAT and potentially provide PKI for IPv6 at their sites and distributed location and through their sub-Providers to the public and businesses. The Providers will be able to expand their business with incremental steps and be able to have revenue at each step. The reason is that the IPv6 infrastructure can provide new services and uses for their customers that do not exist today with IPv4 and NAT, as discussed in the previous sections.

Home users will flock to peer-2-peer gaming and other uses for entertainment and IPv6 will permit them to enter Cyberspace with others using an E2E trust model. This will be a market specifically for the providers above.

Mobile Pedestrians with IPv6 will be able to remain connected and not have to disconnect and connect, because Mobile IPv6 will be able to be used not just in WiFi hotspots but across a state or even an entire country.

The task force seeks specific data on the hardware, software, training, and other costs associated with implementation of IPv6. In responding to the questions below, we ask commenters to discuss the extent to which any of these costs may vary by market segment. They should also discuss whether and to what extent the costs might vary depending on the nature of the IPv6 implementation (e.g., a "greenfield" implementation versus one that overlays or replaces an embedded IPv4 base)? To what extent do the IPv6 costs vary with the size of the embedded IPv4 base? In instances where IPv6 capabilities are already deployed, what factors must be present to "turn on" existing IPv6 functionality?

Responses below for the cost, but the NAv6TF will address the variance that will exist across markets here. The costs across markets or deployment scenarios can be extrapolated from the responses below. Each deployment scenario can use the responses to this NTIA RFC and for each cost type apply that cost to the deployment requirements to use IPv6. In all cases some training costs will be required for every deployment scenario, for some time. At the low end a Home User today must know which operating system releases have to support IPv6 and then what applications on that platform have been ported, at the high end an enterprise will have to define a strategy to transition some applications to IPv6 and leave other applications as legacy that must be able to interoperate with a dual IPv4 and IPv6 node. Hence, for initial deployment across any segment today there will be some training cost to all. Overtime IPv6 for the Home User as one example will just exist as IPv4 does today and be pervasive.

Regarding other specific costs below, the responses below can be used to extrapolate to the scope of nodes and systems integration required for an IPv6 deployment scenario. Clearly the Department of Defense will have a greater cost than a Dentist office, but the Hardware, Software, Training, and Transition costs below will apply equivalently to both. The point is that IPv6 cost can be defined in list form and then applied to a cost matrix for any deployment scenario, as part of any entity planning and cost analysis to deploy IPv6.

2.1. Cost of Deploying IPv6 (NTIA RFC Section III-A)

1. *Hardware costs*

Deploying IPv6 on a national scale will require a substantial replacement and/or upgrading of existing IPv4 equipment. The task force solicits comments on the nature and magnitude of the costs of deploying IPv6, including the likely time period over which those costs will be incurred. For example, routers, hosts, servers, and terminal equipment presumably will have to be replaced or modified in order to originate, transport, and receive IPv6 traffic. If only modifications are required, will they involve hardware changes (e.g., router line cards)? What are the likely costs of those changes? What additional costs will be incurred (e.g., training/retraining costs, transition testing on operational functionality and performance)? Will the premises equipment that enables broadband transmission services (e.g., DSL and cable modems) need to be replaced or modified in order to carry IPv6 traffic and, if so, at what cost?

The software to support IPv4 or IPv6 on a platform is orthogonal to the replacement of the hardware, in most cases, except in cases where the software has been integrated into a processor or circuitry of the hardware. Most platforms in the market today support both IPv4 and IPv6 in software and when procuring those platforms there is no additional charge for IPv4 or IPv6. Today vendors are not requesting a layered software charge for IPv6 being added to their software. For most platforms it is an upgrade of the operating system or installation of a patch upgrade for the network software subsystem on the platform. Additional response on cost analysis is provided below for other costs.

As embedded IPv4 equipment reaches the end of its useful life, users will presumably need to acquire replacements. What are the useful lives of the various categories of such equipment (e.g., routers, servers, premises equipment) and how has the duration of those lives changed over time? Are there differences between the technical and economic lives of particular equipment that may have a bearing on the decision to move from IPv4 to IPv6? When the time comes to replace existing IPv4 equipment, will the relative costs be such that users will tend to purchase IPv6-capable equipment? Or will the added direct and indirect costs (e.g., operating, and administrative costs) of purchasing IPv6 equipment induce users to stay with IPv4-compatible equipment and applications? Will manufacturers continue to produce equipment and applications that can handle only IPv4 packets? What market conditions would persuade manufacturers to cease offering IPv4 equipment?

The NAv6TF is a vendor neutral body and cannot respond to the replacement projections of platforms, that really is a question that must be asked of each platform provider. But, we can respond from our knowledge that we do not know of any platforms except embedded systems that do not support IPv6. IPv6 is an integral part to the networking subsystem of any IP protocol stack and suite on a platform. Once, IPv6 is added to that software on any platform it is part of the product. Whether IPv6 is used or not will be an option that must be selected on a platform for sometime until IPv6 is more pervasive as IPv4 today and ubiquitous. Manufactures will not remove IPv4 from their platforms for a very long time anymore than they removed TELNET or FTP from platforms when the Web was created. There could be new markets for appliances in

the future where embedded systems could deploy IPv6 only new devices that did not implement IPv4. Examples would be monitoring, mini cameras, or intelligence gathering sensors.

A user today would actually have to search very hard to find any new platform that did not support IPv6 with IPv4, as most platforms today are IPv6 capable currently in the market.

2. *Software costs*

To what extent will the modifications to routers, hosts, servers, and terminal equipment mentioned above involve only software changes? What is the likely magnitude of those costs? Will various applications and Internet services (e.g., search engines, content delivery networks, DNS) have to be modified to make them compatible with IPv6 transmission? What are the estimated costs of those changes? Will the necessary modifications to software and applications require extensive changes in the underlying coding and, if so, at what cost? Are there differences in the useful life and cost of software, as compared to hardware, that make it likely that firms will acquire and implement IPv6 software and applications before IPv6 hardware, or vice versa?

The modification question for hardware because of software costs were addressed in the response for the Hardware costs. Applications being ported to IPv6 will be transparent to link media and transmission media. If the Application over IPv4 supports link and media type X then when the application is ported to IPv6 will also support link and media type X too.

The extent the application has to change is relative to the complexity of the applications middleware use of accessing the communications layer (IP protocol suite in this case) for applications that send and receive packets over a network. An application that uses simple BSD UNIX or Linux sockets, or equivalent with the Java.net programming interfaces to access the communications layer it really is quite straight forward. This cost will vary on the number of lines of code required to locate where and what IPv6 approach the software code change will use, and will be the most time consuming effort to port to IPv6. Please see below URLs for this case:

http://www.nav6tf.org/slides/trans_ipv6_v013.pdf

http://www.usipv6.com/2003arlington/presents/Eva_Castro.pdf

When the application has a complex middleware architecture and custom network APIs to the communications layer, and did not isolate the information services layer to the communications layer then that becomes more complex and costly, because all the dependencies assumed about IPv4 (e.g. address size, header information, etc) must now be considered in a port to IPv6. The cost in this case is directly proportional to the complexity of the application's code that requires the use of the communications layer on the platform.

It is not possible for applications to be ported unless the platform first supports IPv6.

The lifetime of software is related to how well it was designed for extensibility, and any patches for quality or performance done over time. The code changes to port an application to IPv6 so that application executes over a network as IPv4 are not typically a software subset in an application that requires changes once written. The exception to that case is when the application wants to take advantage of the new features within IPv6 like address scoping, use of the flow label, supporting multiple address space types on a node, and others.

The cost of porting applications is also directly proportional to the programming skills of the software engineers use to port the applications too.

3. *Training costs*

An organization's personnel will have to be trained in how to install, operate, maintain, and service IPv6 hardware and software. How much will that training cost? How do training costs compare (e.g., in percentage terms) to the costs of IPv6 hardware and software? To what extent does the likely costs of training influence an organization's decision to adopt IPv6?

The NAv6TF suggests NTIA issue RFP to Systems Integrators, Platform Vendor, Consulting Firms, and others that are in the business of training to get actual dollar costs and then contrast and compare those responses.

For organizations or home users that turn their router and embedded hardware over to new models often, the only cost will be training costs. If a firm recently in 2004 purchased a new set of routers, servers, and client nodes there is a good chance IPv6 is already within those nodes and it is just a matter of knowing how to use IPv6, thus the training costs.

Training costs can vary and clearly any adoption for new infrastructure technology like IPv6 must be considered and planned by an organization or it cannot possibly deploy IPv6. Hence, if an organization cannot plan for that training immediately it will have to add that infrastructure training into their future plans to adopt the new technology as any other technology to evolve their business or operational capabilities. IPv6 is merely new infrastructure technology.

The IPv6 Forum with support from the key players of the NAv6TF has contributed with following major actions worldwide, which assists with the training requirements:

Organized 32 Global IPv6 Summits over the last 5 years in 20 countries (Asia, Europe, Africa, Australia and the Americas) 7 new IPv6 Summits are planned for 2004 around the world

Trained a total of more than 6000 engineers worldwide with deep technical content and commercial deployment

Introduced the IPv6 Ready Logo Program to create a worldwide quality and interoperability platform to win confidence of vendors and users.

Members of the IPv6 Forum worked on multiple research projects in different geographies:

Europe: over 180 million Euros have invested in research on projects with the European Commission

The Japanese IPv6 promotion Council has won direct support from the Japanese government for multiple research projects

The Chinese government has contracted the first large scale China Next Generation Internet project for 170 million dollars to become the largest commercial IPv6 native network.

Ten IPv6 Forum Chapters have been created around the world (Australia, Japan, China, Korea, Taiwan, India, Malaysia, Tunisia, Russia, Slovakia, Brazil) www.ipv6forum.com/navbar/ipv6forum/worldsites.htm

Twenty National Task Forces have been created to address the national political and business opportunities and challenges: www.ipv6tf.org

- **NAv6TF**
- **China IPv6 Council**
- **India IPv6 Task Force**

- **Taiwan IPv6 Task Force**
- **Iranian IPv6 Task Force**
- **Asia Pacific IPv6 Task Force www.ap.ipv6tf.org/**

European IPv6 Task Force, which includes www.ec.ipv6tf.org/in/i-enlaces.php

- **French IPv6 Task Force**
- **Spanish IPv6 Task Force**
- **Portuguese IPv6 Task Force**
- **Belgian IPv6 Task Force**
- **UK IPv6 Task Force**
- **German IPv6 Task Force**
- **Danish IPv6 Task Force**
- **Swedish IPv6 Task Force**
- **Swiss IPv6 Task Force**
- **Italian IPv6 Task Force**
- **Finnish IPv6 Task Force**
- **Luxembourg IPv6 Task Force**
- **Irish IPv6 Task Force (under formation)**
- **Austrian IPv6 Task Force (under formation)**
- **Dutch IPv6 Task Force (under formation)**

4. Other costs

What are the opportunity costs of waiting to deploy IPv6? To what extent 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)? 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? For example, will costs and prices decrease over time as a function of the worldwide IPv6 installed base? Could waiting for international development and deployment of IPv6 lead to reduced R&D costs and fewer security problems for U.S. adopters? Would the U.S. benefit from lessons learned by early adaptors or will there be minimal knowledge spillovers? Conversely, will late entry into global IPv6 markets by U.S. firms have a significant long-term negative effect on market shares and economic performance? What is the impact of slow IPv6 deployment on the development of native IPv6 applications?

The other cost is the overall planning cost. IPv6 for organizations cannot be deployed without planning. That means and organization has network architects, systems engineers, and system operational engineers that are able to provide a plan to transition to IPv6. This implies that these persons are trained or hired by the organization to know the details of IPv6 to add this new infrastructure to the organizations network infrastructure. These persons will also have to design an IPv6 deployment roadmap for each part of the network that will be affected by the transition and how that will be accomplished at what rate. For application vendors or organizations that build their own applications, the software engineers will have to understand enough about IPv6 to make decisions in the software as to approach, extensibility, and where to add IPv6 to the application code base. This is another form of training cost.

IPv6 has a very severe cost and that is the cost of waiting to long to deploy IPv6. That cost has several penalty costs. The first penalty cost is the longer an organization waits to deploy IPv6, implies more of the band-aids for IPv4 created are implemented into the infrastructure, which will continue to affect the complexity and time-to-market to have the benefits of IPv6. This

penalty cost also can increase the planning costs exponentially. Another penalty cost is a competitive parity cost and loss of opportunity cost with IPv6, if the market or product the organization is participating evolves to IPv6. Another cost is lost customers and influence because an organization is unable to interoperate with business partners or other organizations. There are penalty costs for not deploying IPv6 from the NAv6TF's perspective. This is one reason why waiting for international development and deployment is not a wise strategy for the U.S. Government, firms, or providers, it will cost all more later than to begin deployment today of IPv6.

IPv6 native applications, assuming that IPv6 is only used not IPv4, is dependent on a core IPv6 infrastructure being deployed within the network domain and scope required for that application. If that IPv6 infrastructure does not exist then those applications cannot execute and thus cannot be deployed. The U.S. economies as all world geographies are dependent on a global economy. The Internet phenomenon is a backbone infrastructure to support a global economy and if the U.S. becomes isolated from that backbone supporting only IPv4, it will be isolated from participating in that economic growth. The U.S. Government and Businesses must ask themselves what is the cost of not deploying IPv6? NAv6TF suggests to NTIA that this cost is great.

Regarding the U.S. influencing the costs of IPv6 internationally, the NAv6TF believes that without U.S. participation in the global deployment of IPv6 that the costs to all will be greater, because U.S. involvement can help make IPv6 a commodity technology infrastructure . The U.S. deploying IPv6 would assist to keep the deployment and eventual products costs lower than if the U.S. is late to support IPv6 widely. The NAv6TF believes that the time-to-market window for IPv6 from the U.S. will significantly influence and reduce the overall costs of IPv6 in the global economy. This will benefit U.S. businesses and our economy both short term and long term. U.S. deployment of IPv6 would also benefit the social evolution of our citizens and people worldwide to continue to use the Internet beyond the social class digital divide that exists currently in the U.S. The U.S. has the opportunity to assist worldwide the ability for people to communicate with the new model for E2E within IPv6, presented in this response, and at a reduced cost affordable to all, not just those with wealth, which is the current situation for the Internet.

2.2. Transition Costs and Considerations (NTIA RFC Section III-B)

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

As our nation migrates from IPv4 to IPv6, there will be a period of time during which IPv4 and IPv6 operate simultaneously. The task force seeks comment on the costs and any other issues related specifically to this migration from IPv4 to IPv6. For example, what are the costs, burdens, and potential problems of ensuring interoperability between IPv6 and IPv4 networks? What are the incremental costs resulting from operating IPv6 and IPv4 concurrently? To what extent will various interoperability solutions continue to function efficiently and effectively as traffic increases? Does the operation of dual IPv4/IPv6 equipment impose significant costs relative to IPv4 or IPV6-only equipment? To what extent do measures to ensure interoperability reduce the performance of network routers, increase routing tables, or have other adverse effects?

The NAv6TF suggest in this response that the U.S. Government not use the word migration when referencing IPv6. It will not be a migration as was Y2K. It will be a gradual transition, and IPv4 will continue to exist for a long time.

The base incremental costs because of transition as an overview are as follows:

- **Analysis of what transition mechanism should be used for IPv6 deployment. This will define how the interoperability between IPv4 and IPv6 will occur and their will be multiple choices to select that support ones objective. A one-size-fits-all strategy will not exist or support the diverse requirements for a particular deployment model in the market. Understanding in depth the supplier and IETF standards body transition mechanisms to implement transition is also another training cost curriculum.**
- **Analysis of ones network requirements for performance must be done to select the appropriate transition strategy to deploy IPv6. The NAv6TF has not seen any performance degradation of networks or platforms that support IPv6. Transition mechanisms will have minimal network performance degradation, but all transition mechanisms will require some management and configuration costs. The NAv6TF is completely supportive of the IETF current thinking that whenever possible the use of dual IPv4/IPv6 methods be used as the essential transition mechanism for initial deployment. Discussing those methods is beyond the scope of this response, but the NAv6TF has the deployment and technology expertise to perform such analysis as input to NTIA and the U.S. Government if that would be useful in another document at some later time. We would want to agree to any time frames for such document as it would very involved.**

The other costs and issues raised will be responded to in the responses below for this section of the RFC.

Many observers assume that, regardless of the pace of IPv6 deployment, there will be significant "islands" of IPv4 for the foreseeable future. There appear to be several transition mechanisms to allow interoperability among IPv4 and IPv6 hosts and networks, including dual stack, tunneling IPv6 over IPv4 networks, and IPv6-only to IPv4-only translation. What are the costs and benefits of each of these mechanisms? Is there a "best" or accepted approach that will provide for interoperability between islands of IPv4 and/or IPv6 and the Internet at large? What factors may determine whether and where alternative transition mechanisms will be available and applicable? Can alternative transmission mechanisms co-exist while still providing end-to-end interoperation among IPv6 and IPv4 networks? 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 testbeds?

The NAv6TF views all transition mechanism are valuable and all can be used. The time frame for this response precludes the NAv6TF from a deep analysis of the transition mechanisms for the many variant deployment scenarios that exist and will exist in the market today. Each deployment scenario will require a specific transition strategy there is no one-size-fits-all transition strategy to transition to and deploy IPv6.

Alternative transmission mechanisms can interoperate between IPv4 and IPv6 E2E, and see previous response on link and media operations for IPv6.

The embedded base of IPv4 equipment does not preclude the U.S. from the benefits of foreign IPv6 deployments, as long as there is means to connect IPv4 to that equipment when legacy application support is required. That is inherent in all transition mechanism as a base architecture precept for developing a transition mechanism. But, if an organization has no way to receive and IPv6 packet then it cannot participate in IPv6 communications. It is not a function

of the current equipment, but rather a function of deploying IPv6 within the organization and initializing a transition strategy.

The task force recognizes that industry groups have worked hard to ensure interoperability between IPv4 and IPv6 networks and applications. 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? If government intervention is needed, what form should it take?

Government intervention should be used with caution for all cases in the U.S. as a precept, per the U.S. constitution. Interoperability will be insured from the many test beds and network pilots worldwide, and within the U.S. like Moonv6. Please see responses below on Monopoly and What government can do further down in this response.

What problems, if any, may arise when existing IPv4 networks convert hardware, appliances and middleware to IPv6? Will applications that use IP services migrate easily? Are there estimates of the cost associated with these issues? On the other hand, implementation of IPv6 (as distinct from gains anticipated via the definition of the new protocol) could also yield substantial hardware and software advances. Currently, IPv4 operates on top of several protocol layers (e.g., MPLS, ATM, frame relay, ethernet and wireless). Commenters are requested to explain how the technical requirements for these protocol layers and dependencies of protocol layers supported by IPv4 (e.g., UDP and TCP) may be impacted by the use of IPv6.

We have responded to this concern previously in the response and it should not be a concern.

The task force seeks comment on the adequacy of the existing set of IETF standards for IPv6. 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? Would it be helpful for the IETF standards-track RFCs to define "mandatory" services (e.g., protocol capabilities) and "optional" services? What problems, if any, may arise in implementing IPv6, as embodied by the IETF standard set, in various types of equipment and software? Will the standards create undue hardship on equipment and software providers? Are additional industry or government specifications required to successfully realize the potential benefits of IPv6?

The IETF is now a large complex body with much work to be done besides IPv6. The time-to-market delivery for specifications for transition and many other Internet Protocol specifications is not optimal at this time within this standards body. The IETF is addressing this problem currently and NAv6TF believe in time it will be fixed.

The IETF should continue to build specifications and not implementation mandates. The NAv6TF and most vendors will completely reject any form of mandate for deployment of IPv6 whether it be for transition or an emerging protocol extension for IPv6.

The market will adopt the transition mechanisms that work and request them from their vendors. If the IETF does not meet the time-to-market requirements for transition mechanisms when needed for deployment then industry will form consortia's and develop those standards for the industry as a market requirement.

The NAv6TF and other bodies in industry are now looking at the possibility of developing a support infrastructure that would ratify existing transition mechanisms and developing new ones as required until the IETF problem is fixed. The NAv6TF would be open to working with NTIA and the U.S. Government to determine what else is required for transition mechanisms, and from that a solution can be determined. A possible thought is for NTIA to

work with the NAv6TF and parent organization the IPv6 Forum to develop a working group to build additional transition deployment mechanisms, as a future discussion.

2. Security in Transition

Among the IPv6-related issues that the National Strategy to Secure Cyberspace directs us to study is "security in transition," the need to ensure that security interests are protected during transition from IPv4 to IPv6. 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?

In addition to the references provided in Section II for security it is important first to verify that IPv6 supports all that IPv4 does today with security infrastructure. For example IPv6 must support IPsec (mandated), SSL/TLS, DNS Security, Firewalls, etc. So the defense is verify that security infrastructure and components for IPv4 have been ported or now support IPv6. That is mandatory for legitimate security and Law Enforcement.

Many of the concerns for transition are illogical and simply misinformed technically. For example lets discuss a manual configured tunnel where IPv6 is encapsulated within an IPv4 packet.

When the node encapsulates the IPv6 in IPv4 the node has the option of first encrypting the IPv6 packet, thus the packet cannot be decrypted while being routed, and only decrypted on the end node after the IPv6 packet is decapsulated on the end node (assuming in this case its done by two end nodes). There is no compromise of security (assuming the encryption is strong from network attackers which is not indicative to IPv6) because of this operation.

Most of the concerns in this area are fear, uncertainty, and doubt. If the IPv6 path (or IPv4 path) of data does not support the current security components and infrastructure that are available today for the Internet Protocol suite then IPv6 can be compromised in that situation.

IPv4 and IPv6 are at the IP layer in the communications model and infrastructure. The IPv6 transition mechanisms known today do not cause new security problems that do not exist native with IPv4 and IPv6.

What must be done for IPv6 transition is to verify the trust relationship assumptions between nodes using the transition mechanisms, in addition to the basics of IPv4 and IPv6 supporting the current security infrastructure and components available. This exercise must be part of the transition planning for the deployment of IPv6.

In addition to the Graveman and Esposito reference previously in our response within the security section all transition specifications in standards bodies like the IETF or future efforts to define new mechanisms must contain a security considerations section, that must be understood by any deploying IPv6. The NAv6TF will provide at our technology summits security sessions and workshops periodically that specifically discuss and present the issues around security for IPv6.

3. Other Transition Concerns

Proper Internet address allocation is achieved through a network of national (i.e., the American Registry for Internet Numbers (ARIN)) and international (i.e., Reseaux IP Europeens Network Coordination Centre (RIPE-NCC) and Asia Pacific Network Information Centre (APNIC)) organizations that are authorized by the Internet Corporation for Assigned Names and Numbers (ICANN) to administer numbering and

addressing. Does the deployment of IPv6 create address allocation issues for any market segment? How will allocations to end users and end-user devices be affected by IPv6 deployment? Will small and mid-sized ISPs and IT firms have equitable access to the addresses they need? Are the existing national and international registries technically capable of handling administrative tasks required for IPv6 numbering and addressing? If not, identify the tasks and the costs for registries to be made capable of handling IPv6 related administrative tasks.

IPv6 changed the model of how IP addresses are provided. NAv6TF suggests that the registries must respond to this in the RFC, and the NAv6TF supports the registries and believe they are capable of supporting the deployment of IPv6.

The one problem we have seen recently reported to the NAv6TF are cases in the U.S. where an organization was not able to get IPv6 address space, because their provider did not support IPv6 and was unable to give the organization an IPv6 address. This is a problem and could require Government intervention or a policy to avoid any Provider preventing the early adoption of IPv6 by an organization.

3. Current Status of Domestic and International Deployment (NTIA RFC Section IV)

3.1. Appropriate Metrics to Measure Deployment (NTIA RFC Section IV-A)

Efforts to deploy IPv6 commercially are relatively recent phenomena. Notwithstanding the nascent nature of the IPv6 market, the task force seeks to develop an understanding of how the market is evolving across regions (both domestically and internationally) and among user groups (e.g., government, industry, academia). What are the most appropriate metrics to gauge IPv6 deployment? Is 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 carried sufficient to properly define the IPv6 market? Are there other metrics or some combination of metrics best suited to characterize the domestic and international penetration of IPv6?

These are exactly the metrics to use, but not all are accessible.

The task force is interested in an assessment of the total domestic and international deployment of IPv6. What is the known current volume of deployed native IPv6 and IPv4 network equipment (e.g., hosts, routers, switches)? 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)? How is that equipment deployed by market segment? What is the approximate domestic and global value of all deployed IPv4 and IPv6 equipment? What is the percentage (and proportion as compared to IPv4) of known IPv6 deployments by market segment?

NAv6TF or the IPv6 Forum does not have this data. This would be a big help if some government entity could gather such information. Possibly some vendors may have this information.

3.2. Private Sector and Government Deployment Efforts (NTIA RFC Section IV-B)

1. Overall Domestic Effort

The task force seeks specific comment on the status of IPv6 deployment efforts in the United States. First, we seek comment on the availability of IPv6 products and services. 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? We ask commenters to identify the relevant product and service categories and to describe 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? To the extent any relevant products and services are not available or are in limited supply, we seek information about their projected availability in the future, including analysts' estimates and suppliers' business plans.

The NAv6TF cannot respond and we will assume suppliers and vendors are responding to the RFC with this information. What NAv6TF can say from what we have seen from Network Pilots and other activities is that we know of no box vendor not supporting IPv6. What is missing now are applications being ported, and systems integrators supporting IPv6 with solutions.

But what must be noted is that by deploying dual stack networks (co-existence), it will avoid the "urgency" for porting everything, of course, not being able to exploit all the IPv6 advantages initially, in some applications, until they are not just ported, but improved. This was the brilliance and advantage of the DoD mandate requiring IPv6 capable systems now as it provides a path to begin IPv4 and IPv6 coexistence.

Second, the task force seeks comment on the actual deployment of IPv6 products and services in the United States. To the extent possible, we ask commenters to provide specific information on the status of IPv6 deployment across product and service categories (e.g., hardware, software) and across customer segments (e.g., private sector, government, academia). For example, how many enterprise network routers are currently IPv6-capable? How many public or backbone network routers are IPv6-capable? How does U.S. router deployment compare with other countries? How many ISPs are currently capable of handling IPv6 traffic? What percentage of Internet access customers receive IPv6 capable 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? To the extent that such capability is only provisioned in such devices, how easy/costly will it be for users to activate that capability? How many of the critical functions within an enterprise are IPv6 enabled (e.g., DNS, wireless firewalls)?

Third, we seek comment on the projected growth of IPv6 products and services in the United States. We ask commenters to provide all relevant assumptions and underlying data that support their growth projections. To the extent possible, we ask commenters to provide growth projections for specific products and services, as well as projections among customer segments.

The NAv6TF cannot respond and we will assume suppliers and vendors are responding to the RFC. What we can say is our Network Pilots do show that most of the Internet Application Infrastructure has been ported and running (e.g. DNS, Web, Mail, etc), but then we still are missing some like the Network Time Protocol (NTP) has not been ported to IPv6. The NAv6TF is currently determining a list of applications we believe important for IPv6 deployment and initial target markets. NAv6TF other concern is we have seen very few implementations support IPsec

and other security infrastructure and components for our Network Pilots. In addition, we have not seen the PKI suppliers in the industry come on board to support IPv6, which is a problem too.

2. Domestic Government Efforts

The task force seeks comment on federal, state, and local government efforts to deploy IPv6 in the United States. For example, the Department of Defense (DoD) has announced plans to migrate its existing Global Information Grid Network to IPv6 by 2008. Additionally, DoD recently initiated a multivendor testbed, known as "Moonv6," to examine the interoperability of IPv6 equipment, software, and services under real-world conditions. Involving more than 30 networking vendors, testing vendors, and service providers, the project purportedly will be the most substantial test of the IPv6 standard set in North America. We seek comment on any lessons learned to date from DoD's efforts to deploy IPv6 that could be applied to federal civilian agencies, state and local governments, academia, and the private sector. We seek similar comment on other IPv6 research efforts and testbeds, including IPv6 deployments in federal research networks (Fednets), the Abilene backbone network, and any other similar efforts. We ask commenters to identify the costs of these efforts and the expected effects these activities may have on the deployment of IPv6 within the United States?

NAv6TF is the overseer of the Moonv6 project and initiated Moonv6 with the DoD and Interne2. Please see www.moonv6.org for status and updates to the Moonv6 Network Pilot. NAv6TF is also working now worldwide within the IPv6 Forum to connect Moonv6 to test beds across all geographies. The NAv6TF Moonv6 project also assisted the verification of U.S. vendors to meet the requirements of the IPv6 Forum Logo Certification Program. www.ipv6ready.org

What is the current state of IPv6 deployment by other federal, state, and local government agencies? What factors have various agencies considered in deciding whether and at what pace to deploy IPv6? 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? 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? The task force encourages states and local governments to describe any initiatives or studies that they have undertaken regarding the deployment of IPv6. What is the current state of IPv6 deployment by state and local government agencies? What factors have various agencies considered in deciding whether and at what pace to deploy IPv6? 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?

No Comment.

3 International Efforts

In addition to domestic IPv6 deployments, the task force seeks comment on international efforts to deploy IPv6. For example, we understand that governments and companies in Asia have been aggressively promoting and adopting IPv6, purportedly because of the growing demand for public Internet addresses in their countries. Japan and Korea plan to have IPv6 fully deployed before the end of this decade. The European Union has developed substantial IPv6 plans and programs to ensure readiness and competitiveness when IPv6 is widely deployed. Additionally, we understand that other countries such as Tunisia are engaged in substantial IPv6 deployments.

Please see www.ipv6tf.org for IPv6 efforts around the world. This is a list of IPv6 Forum task forces working on IPv6 deployment as the NAv6TF.

Here is a comprehensive report on the status of all IPv6 Task Forces around the world:

www.ipv6tf-sc.org/html/public/ipv6tf-sc_pu_d3_4v1_3.pdf

Key players of the NAv6TF contributed to the European launch event of the IPv6 services organized in Brussels January 15-16, 2004. The minutes and results of this event can be found in this report:

www.eu.ipv6tf.org/PublicDocuments/ipv6-global-service-launch-03.pdf

We have a world wide team in place to support the deployment of IPv6.

The task force requests comment on the current and projected levels of IPv6 deployment across the globe, on both a regional basis (e.g., Europe, Asia, South America) and on a country specific basis, where available. To the extent possible, we ask commenters to provide such information by product category (e.g., hardware, software) and by customer segment (e.g., government, private sector, academia). We also ask commenters to explain how particular initiatives or programs by foreign governments or foreign suppliers have 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? Are governments devoting significant funding for IPv6 deployment efforts? Have government initiatives (of lack thereof) interfered with normal market forces and what are the consequences of those actions or inactions?

Same as previous response.

4. Government's Role in IPv6 Deployment (NTIA RFC Section V)

The task force seeks to build a public record that addresses two fundamental questions: (1) should government be involved in fostering or accelerating the deployment of IPv6; and (2) if so, what actions should government undertake? In answering these questions, we ask commenters to build upon their responses to the questions above and to provide specific, empirical evidence, where possible, to support their assertions regarding the proper role of government in IPv6 deployment.

4.1. Need for Government Involvement in IPv6 Deployment (NTIA RFC Section V-A)

1. *Reliance on Market Forces*

As a general matter, government policymakers in the United States prefer to rely on market forces for the large-scale deployment of new technologies. In most cases, reliance on the market tends to produce the most efficient allocation of resources, the greatest level of innovation, and the maximum amount of societal welfare. Accordingly, we seek comment on whether market forces alone will be sufficient to drive a reasonable and timely level of IPv6 deployment in the United States. For example, 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? We ask commenters to identify the specific reasons for their positions.

The NAv6TF supports the market should drive IPv6 deployment, but at the same time if IPv6 is being stalled or prevented so that the market cannot adopt IPv6 because of any self-vested-

interest force then that is a potential government issue to support the evolution of technology within the U.S. per Anti-Trust rule of law.

2. Potential Market Impediments

Notwithstanding the government's general preference for relying on market forces, there may be impediments in a particular market that warrant corrective action by the government. In this section, the task force seeks comment on whether some of the more common forms of impediments are present in the market for IPv6 products and services.

a. Technological Interdependencies and the "Chicken and Egg" Problem

The task force requests comment on whether a "chicken and egg" problem exists that could hinder efficient deployment of IPv6 (i.e., disincentives for investment in supporting infrastructure until applications are deployed, matched by disincentives for investment in applications until supporting infrastructure is in place). In the case of IPv6, firms may be reluctant to build IPv6 networks (or to install IPv6 capability in existing IPv4 networks), or to develop and market IPv6 devices, if there are no IPv6 applications that prompt consumer demand for the underlying transmission infrastructure. Similarly, Internet service providers may be reluctant to install IPv6 in the absence of sufficient IPv6 applications. Applications providers, on the other hand, may hold off until the infrastructure is in place to make those applications usable by consumers. We seek comment on whether such a "chicken and egg" relationship exists between IPv6 applications and supporting infrastructure, and if so, how that relationship is manifesting itself in the market for IPv6 products and services.

This problem should be left to market forces and the evolution of IPv6.

The "chicken and egg" problem seems to be most acute when the interrelated products are costly to develop and are highly interdependent (i.e., the end product is a complex and capital intensive system). We seek comment on whether those characteristics are present for IPv6 infrastructure and applications. We also seek comment on how the expected degree of interoperability between IPv6 and IPv4 networks will affect this potential chicken and egg problem. 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? In some instances, government has responded to concerns over potential "chicken and egg" problems by playing an active role in the introduction of certain products and services, such as FM radio and HDTV. We request comment on how the deployment of IPv6 compares to other standards-based technology transitions and whether IPv6 presents the same or similar concerns that warrant government action.

This should be left to market forces. The only case today that the government may want to view is the availability of wireless spectrum to support Providers to supply the market with the spectrum to support IPv6 peer-2-peer Mobile IPv6 Pedestrian devices.

b. Monopoly Power

The presence of a firm or group of firms, with monopoly power in the market for IPv6 products or services could create a potential impediment to the efficient deployment of IPv6 in the United States. Although we are not currently aware of any concerns regarding monopoly power, such a situation could arise from the existence of a dominant firm or group of firms in the relevant markets with the incentive to impede normal dissemination

of IPv6, either by directly suppressing the technology or by setting excessive prices for IPv6 products and services. We therefore seek comment on whether any firm or firms have monopoly power for IPv6 products and services, and how the exercise of such monopoly power will affect IPv6 deployment in the United States.

To aid in this analysis, we seek comment on the extent to which IPv4 and IPv6 are direct substitutes. If IPv4 and IPv6 are direct substitutes (e.g., if IPv6 equipment and applications compete directly with IPv4-based counterparts for market share), it may be unlikely that providers of IPv6 equipment, applications, and services will be able to charge excessive prices for their products (i.e., prices that exceed any performance differential). Alternatively, if IPv6 builds on IPv4, enabling related but different applications, early entrants into the market may be able to establish sufficient market power to impede adequate competition. Economists, however, generally consider such temporary monopolies to be a normal phase of new technologies' evolution and thus such a pattern may represent an efficient deployment of a new technology and not a market failure. We request comment on these issues.

There are enough platforms and systems' already supporting IPv6 and the NAv6TF does not see a product monopoly here, and the evolution of IPv6 to support applications should only happen for business reasons from within the market. But, if IPv6 is prevented from being on the U.S. Internet superhighway across the U.S. from any entity or economic infrastructure then it would be wise for the government to determine what is the problem and is there something they can do to help, because NAv6TF believes that the wide spread deployment of IPv6 is important to U.S. national interests.

There are no performance penalties from IPv6 for networking that the NAv6TF has seen from extensive interoperability events and testing, most recently on the new North American IPv6 semi-commercial test bed Moonv6. Please read the extensive report of the Moonv6 project under www.moonv6.org.

c. *Network Externalities*

The presence of network externalities or networking effects could also impede efficient deployment of IPv6. The task force requests comment on whether and to what extent deployment of IPv6 is characterized by network externalities. If so, what is the magnitude of those externalities? In this regard, most observers believe that IPv6-based networks will be interoperable to a considerable degree with embedded IPv4 networks and, therefore, IPv6 users will be able to communicate with IPv4 users in many instances. To what extent does that affect the size or scope and timing of any network externalities associated with deployment of IPv6? 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)? 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? How important are network externalities in the U.S. market for domestic firms who want to compete in global markets?

As previously stated verifying enough wireless spectrum will be important. Satellites for public Internet communications may be useful to help support public sector application availability for the Mobile IPv6 pedestrian.

Network externalities increase uncertainty (and thereby deter efficient investment decisions) because the returns on a company's investment are dependent on the investment decisions of other companies. In addition, if related applications, or applications and infrastructure are highly complementary, early entrants

into a market that is not mature may not be able to realize returns on investment in an acceptable time frame. These factors increase market risk and impede the development and deployment of technologies. A lack of information and documentation regarding benefits and costs also increases market risk. The task force seeks comments on the importance of coordinating the timing of IPv6 migration for achieving efficient market penetration.

See NAv6TF Additional Recommendations below.

d. Other Impediments

In addition to the potential market impediments described above, we seek comment on any other potential market impediments that may hinder IPv6 deployment in the United States. To the extent possible, we ask commenters to provide specific, factual examples of any such impediments and to describe how those impediments are affecting IPv6 deployment.

No comment.

3. Public Goods

An important role of government is to ensure the adequate provision of "public goods," which market forces alone commonly cannot do. Examples of public goods include national defense, law enforcement and clean air. Infrastructures, to varying degrees, also have the characteristics of public goods. Because standards are by definition used collectively by competing and partnering economic agents, they have infrastructure characteristics. In this section, the task force seeks comment on the public good characteristics of IPv6-capable products and services.

See NAv6TF Additional Recommendations below.

a. Security

In section II.B above, we seek comment on the potential security benefits of IPv6. To the extent that commenters believe IPv6 may directly or indirectly facilitate improved IP security, we seek comment on whether security benefits from IPv6 exist that can significantly further the delivery of public goods. For example, could the deployment of IPv6 advance important national security, national defense, and law enforcement interests, which are commonly understood to be public goods? We understand that certain features of IPv6 (e.g., expanded address space, auto-configuration) could enable the military to provide soldiers with equipment that could improve command and control capabilities in the field. Improved auto-configuration could also enable first responders to establish vital communications systems in the event of disaster or national emergency. Does the furtherance of those and any other security-related interests require government action to speed the deployment of IPv6 in the United States? In responding to theses questions, interested parties should explain the specific security interests to be furthered and how they would be advanced by wide scale deployment of IPv6.

For the DoD and other government agencies it is possible to mandate PKI within that enterprise and that will most likely be classified and not available to the public. But the open market cannot create similar mandates. To deploy the pervasive use of the absolute trust model of E2E will require PKI and within the public sector. It would be worth an investigation for the government to determine how to motivate PKI vendors to support IPv6 in the interest of the greater public good.

The task force also seeks comment on whether the private sector may fail to sufficiently implement IPsec or other security mechanisms, and whether government action to accelerate the deployment of IPv6 could aid private sector security efforts. For example, what conditions could hinder private sector efforts to fashion key management systems and trust mechanisms needed to implement IPsec in an IPv6 environment? To what extent would federal government intervention be useful or necessary to overcome such obstructions?

If PKI is motivated in the public sector it will also appear in the private sector and definitely PKI would benefit from some government support.

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? In this regard, we understand that U.S. firms are currently major providers of IP equipment, services, and applications. We also understand that many have developed or are developing IPv6 capabilities for their products and services. We further understand that some U.S. firms appear to be selling equipment in many of the countries (e.g., Korea, Japan, China) that ostensibly are most committed to IPv6 deployment. Given these understandings, we seek comment on how the competitiveness of U.S. equipment firms and service providers would be adversely affected by slower deployment of IPv6 domestically?

See NAv6TF Additional Recommendations below.

We also understand that use of IPv6-capable networks and applications may increase the efficiency of users of IPv6 infrastructure, potentially allowing them to produce and market their goods and services at lower cost or with higher quality – both domestically and in international markets. Thus, lagging deployment of IPv6 in the United States (with consequent loss of economies of scale and scope) could conceivably reduce the competitiveness of American firms in various export markets vis-à-vis companies from countries that have deployed IPv6 more aggressively. We request comment on this supposition and, particularly, on 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.

No comment other than previous comments on the benefit from the global economy.

4.2. Nature of Government Actions (NTIA RFC Section V-B)

In light of commenters' answers provided to the preceding questions, we now seek comment on the type of action or actions, if any, that the government should take regarding IPv6 deployment. Traditional government support for new technologies and technology infrastructures have included R&D support, incentives for investment in equipment, government procurement, and facilitation roles with respect to standards development and deployment. We emphasize that the list of government actions discussed below is not exhaustive, nor are such actions mutually exclusive. We therefore request that commenters provide specific details for any course(s) of action they propose, together with the estimated costs of such action(s).

1. <u>No Government Action</u>

To the extent commenters believe the aforementioned trends and potential market conditions suggest a timely deployment of IPv6 in the U.S., one possible U.S. government action would be to let market forces guide the diffusion of IPv6 into existing and future markets. The task force requests comment on the appropriateness of

this non-intervention approach. Commenters should address the potential costs to the U.S. economy if government inaction results in a domestic implementation of IPv6 that lags other industrialized nations.

Government for IPv6 should lend a helping hand as identified in the preceding paragraph, to help stimulate innovation that is supportive of technology evolution, to stimulate to help keep the U.S. competitive in the global economy, and enforce Anti-Trust that prevents markets, but the market must be the reason for a technology to proliferate. We also provide in recommendations below some leadership actions as suggestion that the government could support.

2. Options for Government Action

We discuss below specific actions that government could take to further deployment of IPv6. As noted above, the approaches discussed are not exhaustive, however, and interested parties are encouraged to identify and outline other potential avenues for government action. If the federal government should elect to spur deployment of IPv6 within the U.S. economy, we also request comments regarding how, when and in what form such action should take. What factors and market information should government consider in order to determine that the market-driven rate of IPv6 deployment in the U.S. is insufficient, thereby necessitating government intervention? Should government intervene early to stimulate deployment? Should it allow the market to drive deployment forward, and concentrate government efforts on assisting or encouraging those individuals and enterprises that are the slowest to adopt IPv6? To what extent, if at all, should the timing of government intervention differ with respect to private sector deployment of IPv6, as compared to its adoption by federal, state and local government?

a. Government as Information Resource

Rather than actively promoting deployment of IPv6, the government could establish programs to assist public and private sector entities in making their deployment decisions. It could, for example, create an information clearinghouse that gathers and disseminates IPv6-related information among government agencies and interested private sector firms. Such information could include data concerning the potential benefits and costs of deploying IPv6, the purchasing decisions made by other public and private actors, and guidelines to aid interested parties in making IPv6 procurement decisions. What would be the costs and benefits of such an approach? What would be the essential elements of an effective clearinghouse program?

This would be very useful, but the cost and elements to do this would require further analysis beyond the time frame for this response.

b. Government as Consumer

We seek comment on whether the government should use its position as a large consumer of information technology products to help spur IPv6 deployment. For example, working through its procurement process, should the federal government purchase only IPv6-compatible products and services? Should state and local governments adopt similar procurement policies? What would be the cost to the government of adopting IPv6 procurement policies compared to not adopting such policies? Could the government's adoption of IPv6 procurement policies have any unintended, adverse effects on the market for IPv6 products and services? If so, please define and assess the likelihood and magnitude of such effects?

In the U.S. the government is a business and all agencies are in fact a business too. If the government believes IPv6 adds value to their business and it clearly does for the DoD and DHS, then agencies should follow the lead of the DoD. If the U.S. government widely adopted IPv6 for

business and national leadership reasons it would greatly influence the adoption rate of IPv6 worldwide. The NAv6TF believes all businesses should move to IPv6, hence; believe that the U.S. Government should move to IPv6. The NAv6TF also believes the DoD method and declaration of IPv6 adoption is very supportive of a good IPv6 transition deployment strategy, permitting the use of test beds to define the requirements and adoption rate.

To the extent commenters support government IPv6 procurement policies, we seek specific comment on how they should be implemented. For example, when should such policies become effective? Should such policies apply to all government entities, or are there specific classes of agencies that should adopt these policies before others? How should government fund any additional costs (if any) associated with the adoption of IPv6 procurement policies.

How the U.S. Government performs business funding trade-offs is beyond our capabilities. If the Federal Government believes IPv6 is imperative to its evolution adopting it across all departments and agencies are a prudent decision. The NAv6TF will support the U.S. Government as best we can as a body if that in fact is the decision.

c. Government Support for Research and Development

As discussed above, testbeds and experiments by the Fednets and Abilene have provided early working experience relating to the deployment and use of IPv6. Those activities have also helped to train a corps of IPv6 technicians that could be available to facilitate private sector deployment of IPv6. Furthermore, the Internet2 program has established an IPv6 Working Group that interacts with users, university networks, and Fednets to explain IPv6 deployment and transition issues and to provide hands-on experience to those entities concerning implementation, maintenance, and use of IPv6. In light of these activities, we seek comment on whether the government should provide additional support for IPv6 research and development. Are current research and development efforts sufficient? Does the government possess research and development tools or resources for IPv6 that are not readily available to the private sector? 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)?

NAv6TF suggest that the government built a similar test bed as the DoD is doing and mirror the Internet2 and Moov6 sites and participate in the Moonv6 North American IPv6 backbone network as a site portal. Most likely the model would be different departments and agencies would have their own subnet portals and access to the Moonv6 backbone.

d. Government Funding of IPv6 Deployment

Aside from research and development projects, we also seek comment on whether the federal government should attempt to spur the growth of IPv6 networks, applications, and services through direct funding of IPv6-related activities. For example, the government could provide direct assistance to entities desiring to purchase IPv6-capable equipment, whether in the form of tax incentives, matching grants, or direct funding. The task force seeks comments on the need, feasibility and wisdom of these approaches. How should such programs be structured and how much would they cost? Could existing policies and programs be used to provide such funding, or would new legislative authorization be required? Where the federal government provides funding to state and local governments for emergency communications equipment and networks, should the federal government require state and local agencies to purchase IPv6-capable equipment to ensure interoperability among equipment and networks in neighboring communities?

The government should fund projects that support the further evolution of IPv6 as a technology and for deployment at the federal, state, and local level. See below for example of project that could be funded called MetroNet. If this proposal is interesting the NTIA or DHS NAv6TF would be interested in discussing it further and in more detail. But, it is an example in this response where funding by the government could support an R&D project with real benefits to the U.S. community at large, and the proliferation of IPv6 as an infrastructure technology important to the national interests of the nation.

A required technology capability within the U.S. for Homeland Security is communications between multiple forces 24x7x365 for prevention, at the point of engagement during a 911 event, and the ability for those forces to be commanded at any point in time in an Ad Hoc manner. This requires the integration of multiple technologies, 911 communications platforms, and access to an Internet Infrastructure within a Homeland Security geography, and to the Office of Homeland Security in Washington D.C. The technology capability should support multiple simultaneous events engaged across the U.S. geography from a single command control selected by the National Homeland Security Office.

An example of the above is as follows. In a U.S. city or town the State Police, Fireman, Hospital 911 Personnel, Local Police, and any other required Local Authorities would have Handheld Devices that would have their own Metropolitan Network (MetroNet) for Voice, Video, Graphics, Intelligence, Medical, and other forms of data through multimedia communications 24x7x365. This MetroNet would be connected over the Internet to the National Homeland Security Office securely for communications updates. The MetroNet would support both wireless and wireline technology as the physical medium for communications and the integration of wireless and wireline so either can be used on the MetroNet. The MetroNet would support the ability for a command center to be established in an Ad Hoc manner to communicate with the MetroNet Homeland Security force and National Homeland Security Office using wireless or wireline communications. In addition, the MetroNet should be able to add additional Ad Hoc Sub-Networks in as required such as the National Guard, Air Command, or other U.S. Agencies that must connect to the MetroNet during a 911 disaster.

Most of the technology to develop this communications exists today, but the core technology requires further testing and integration as a complete solution. The backbone technology to support a MetroNet effort is the underlying Internet Protocol Layer that will permit the transmission and reception of communications, and in an Ad Hoc manner. The Internet Protocol version 6 (IPv6) is the Next Generation Internet Protocol to support communications over the Internet and private networks into the 21st century. IPv6 is able to provide the necessary infrastructure to support the MetroNet and National Homeland Security Office, and the Department of Defense (DoD) in June 2003 declared IPv6 as a required technology on all DoD platforms as of October 1, 2003.

IPv6 is the core technology to build a MetroNet communications network, but requires other technologies to be integrated, below is an overview of core technology integral components that require analysis:

- **Mobile IPv6 Routing which permits MetroNet nodes to connect and re-connect while moving across the MetroNet and any Ad hoc Sub-Networks joining the MetroNet.**
- **Large Scale network formation of new Ad Hoc Sub-Networks to join MetroNet.**
- **Security using a Public Key Infrastructure at the IPv6 layer that supports absolute trust model between two peers on the MetroNet, Ad Hoc Sub-Networks, or to National Homeland Security Office.**

- **Integration of Homeland Security applications required for 911 operations and MetroNet forces.**
- **Network Management of MetroNet operations and security infrastructure.**

The proposal is to build a prototype MetroNet in the State of XXXX in XXXXX County. Project control would be in the hands of the non-profit neutral body and provide coordination with the National Office of Homeland Security. The MetroNet R&D project would benefit the residents of XXXX as the end result of MetroNet would provide a Homeland Security analysis that is needed to enhance the capabilities of dealing with Homeland Security prevention and events should they occur. MetroNet will also be useful for non Homeland Security objectives from the network communications capabilities to support other catastrophic events within a town or city required daily (e.g. Law Enforcement, Fires, Accidents, and Natural Disasters).

The project would require hardware platforms, services, hands-on network engineering expertise, Internet communications lines, and software engineering development for integration. The deliverable of the project would provide a complete prototype of MetroNet, the Internet communications to support communications with Ad Hoc Sub-Networks and the National Homeland Security Office, and a report of the results with a recommendation for MetroNet use as infrastructure to support Homeland Security and a deployment model of MetroNet in XXXXXX and across cities in the U.S.

The proposed budget for this project over an 18 month period is 15 million dollars.

An additional investment by the US Government would to be invest in the further development of the Moonv6 project with initial funding directly to UNH and DoD Moonv6 sites, working with the NAv6TF to determine what such funding would be used for to benefit the Moonv6 network evolution.

e. Government IPv6 Mandates

Although imposing government mandates on the private sector to deploy IPv6 is perhaps the least preferred role for government, the task force nonetheless seeks comment on this option to ensure that we develop a complete record. Specifically, we seek comment on whether the government should require suppliers of IP products and services to provide those products and services in an IPv6-compatible version by a date certain. To the extent commenters support such an approach, we ask them to explain the specific authority under which such a mandate could be imposed (legislative or administrative), the timeline under which the mandate would operate, and the benefits and costs of imposing such a mandate.

NAv6TF does not support the use of U.S. wide government mandates, but does believe the government should protect and stimulate technology that is in the interests of our nation. IPv6 is a critical technology that should be adopted in the U.S. widely with many benefits to the U.S. economy and the nation.

4.3. NAv6TF Additional Government Recommendations List

- **A call to application providers to support a Dual IPv4/IPv6 stack to begin to deliver IPv6 services coexistent with IPv4. Though the goal should be that applications are agnostic regarding IPv4 or IPv6.**
- **Determine funding required by the DoD to begin fast track to assist IPv6 deployment..**

- **Increase U.S. support towards the integration of IPv4 and IPv6 in the networks and services associated with the public sector, in the context of public applications requiring the use of new Internet next generation tools and technologies. The integration of IPv6 in existing e-government, e-learning and e-health services and applications towards IPv6, will notably offer users greater reliability, enhanced security and privacy, and user friendliness, in a more open and dynamic environment. IPv6 future-proofing should be considered in application procurements**
- **Establish and launch educational programs on IPv6 tools, techniques and applications, so as to significantly improve the quality of training on IPv6 at professional level, and create the required base of skills and knowledge.**
- **Promote the adoption of IPv6 through awareness raising campaigns and co-operative research activities, by small and medium size enterprises, ISPs, wireless service providers, and network operators, so as to educate the stakeholders, boosting their technological know-how and strengthening their ability to operate on a U.S. if not International basis.**
- **Continue to stimulate the wide spread use of Internet across the U.S. and encourage the integration of IPv6 through the creation of a favourable, stable and government support programs and by avoiding fragmented approaches, mandatory deployment time-lines or excessive fees. Broadband access to the home and to small and medium size enterprises is a key requirement to maximize the benefit of future end-to-end, converged network services.**
- **Strengthen the financial support towards national and regional research networks, with a view to enhance their integration in U.S. IPv6 wide networks and increase the operational experience on novel Internet services and applications based on the use of IPv6. It should be understood that the move towards native IPv6 is a major step for the U.S. to keep its dominant position in the Network Communications Industry.**
- **Provide the required incentives towards the development, trials and testing of native IPv6 products, tools, services and applications in the new economy sectors such as consumer electronics, telecommunications service provisioning, IT equipment manufacturing, construction, transportation, public education and health, banking, insurance and trade.**
- **A formal statement or release from the Department of Commerce and/or from the President regarding IPv6 within the context of technology evolution as was done in Europe and Asia would be very beneficial as a catalyst for IPv6 momentum in the U.S. within government, and in the private sector. IPv6 benefits all as a national interest.**
- **Establish a National IPv6 Council tasked with:**
  - **The assessment, at national, state, and local municipality level, of current developments and rate of adoption with IPv6, as well as with the formulation of guidelines and dissemination of best practices relating to the efficient transition towards IPv6. The IPv6 Council should be guided by the imperative need for harmonization and by the economical benefits achievable through the wide spread IPv6 technology in all ICT sectors and should duly take into account the requirements for an all inclusive information society as well as the digital divide dimension.**
  - **Developing measures aiming at the alignment of IPv6 integration schedules favouring a cohesive IPv6 adoption and ensuring that the U.S. gains a competitive advantage on the Next Generation Internet.**

- **Ensuring the active participation of national experts in the work of U.S. and International standards and specification bodies tasked with IPv6 matters.**
- **Drawing the attention of potential IPv6 systems or application developers to funding opportunities available through a U.S. research and development incentive.**
- **Lead from the Council IPv6 and Security Interest Groups at the State and Local municipality levels for consumers to access for support and education.**
- **Government Web sites that are IPv6 enabled for IPv6 users to access.**

NAv6TF Organization, Acknowledgements, and Contact Information

Organization History

In July of 2001, at U.S. Navy SPAWAR IPv6 Seminar in Charleston, SC, and then again in December 2001, at a U.S. Army Seminar at FT. Monmouth, NJ, the initial creation of the North American IPv6 Task Force (NAv6TF) www.nav6tf.org was solidified. The NAv6TF is a Task Force under the auspices the IPv6 Forum www.ipv6forum.com and provides for the promotion, consultation, a center of technical expertise, white papers, business and marketing support, educational support, and guidance on for the adoption and deployment for IPv6. Additional information can be found at the side bar regarding the Steering Committee, Objectives, Target Industries, and Workgroups.

The NAv6TF supports and drives the IPv6 US Summits in North America, promotes IPv6 with industry and government, provides a technical and business center of expertise for the deployment of IPv6, provides white papers, briefings, and presentations for public consumption, and works with the IT sector to understand the effects of IPv6 transition on the enterprise.

The NAv6TF and others developed the idea for Moonv6 www.moonv6.com during its work to support the U.S. Government Cyberspace Security Office and Department of Defense as two entities the NAv6TF worked with in the IT sector to promote, consult, and define IPv6 technology deployment issues and objectives as a Task Force. The NAv6TF provided volunteer resources that participated in the Moonv6 technology and network requirements to assist the University of New Hampshire and Department of Defense to design the Moonv6 network, developed the Moonv6 Web Page, provided an initial vendor base within the NAv6TF to support Moonv6, provided engineers to support the Moonv6 U.S. sites and test centers, worked with Internet2 community to support Moonv6, and has been an IPv6 conduit for all entities across the North American geography for Moonv6 and IPv6 in general, and fulfill the role of overseer as a body for Moonv6.

The actual definition of Moonv6 was defined at the previous mentioned NAv6TF meeting with the Cyberspace Security Office and Department of Defense participants during discussions to determine how serious should the U.S. take IPv6 as a mission. The question posed to the participants was should we treat IPv6 as we did going to the Moon in 1969? Later when it was decided to investigate how to deploy a U.S. wide IPv6 Network Pilot at a meeting at the University of New Hampshire in March of 2003, including NAv6TF, University of New Hampshire, and Department of Defense principals, the term Moonv6 was selected to name this Network Pilot.

The NAv6TF is also working with other IPv6 Forum Task Forces around the world to support the adoption and deployment of IPv6. NAv6TF has signed a Memorandum of Understanding with the China IPv6 Council as one example.

Acknowledgements:

The editors would like to thank the NAv6TF membership who have many significant contributions to IPv6 with papers, briefs, and presentations from which much of the material for this response came from in this response. Specifically we want to acknowledge significant NAv6TF subject matter experts contributions used for this response: Mike Brig, Randy Runkles, Yurie Rich, Yanick Pouffary, Carl Williams, Steve Pollock, Patrick Grossetete, Tony Hain, Rich Graveman, Renee Esposito, Junaid Islam, Eva Castro, Ben Schultz, Major Roswell Dixon USMC, Marc Blanchet, and Jessica Little. The editors would also like to thank the NAv6TF Steering Committee and NAv6TF Members List for reviewing this response. We also want to thank all vendors worldwide who have shipped IPv6 products to support the deployment of IPv6.

Contact Information and Editors

Jim Bound

Chairman NAv6TF

Chair IPv6 Forum Technical Directorate

Hewlett Packard Fellow

Jim.Bound@nav6tf.org

Latif Ladid

President IPv6 Forum

Vice Chairman NAv6TF

Internet Society Board of Trustees

Latif.Ladid@ipv6forum.com

Glossary

3G	Third generation mobile communications system.
ADSL	Asynchronous Digital Subscriber Line. Offers high-speed connectivity to the Internet over existing copper telephony wiring.
Always-on	Devices remain connected to the Internet when powered up (e.g. ADSL), rather than establishing temporary connections (e.g. dialup). Because devices need a unique IP address continuously, the rise in always-on devices demands more IP address space.
APNIC	The Asia-Pacific regional registry (equivalent of RIPE NCC).
ARIN	The Americas regional registry (equivalent to RIPE NCC).
Broadband access	High-speed Internet connection technologies, e.g. xDSL and cable modems
Cable modem	High-speed Internet access via cable television service line.
Client-server	A communication model where connections are initiated one-way, from clients to servers.
DNS	Domain Name Service. Used to map between Internet domain names (e.g. www.ipv6forum.org) and IP addresses (for use by the network).
End-to-end model	Devices communicating on the Internet do so directly without any intervening translation devices; such devices fate-share their connection.
GPRS	General Packet Radio Service. Allows Internet access from a mobile device running IP(v4) over the wireless telephony network.
IETF	Internet Engineering Task Force. Define global Internet standards,
I-Mode	Popular interactive Internet telecommunications system in Japan
Interoperability	The ability of two devices, usually from different vendors, to work together.
IP	Internet Protocol. The underlying technology by which all Internet data communication is carried out.
IPv4	Internet Protocol version 4. The current protocol.

IPv6	Internet Protocol version 6. The new protocol.
IPv6 prefix	A block of IPv6 addresses that may be used by an ISP or a site network
ISP	Internet Service Provider. Provides network/access services.
ITU	International Telecommunications Union.
LAN	Local Area Network. A local data network.
NAT	Network Address Translation. Allow multiple computers to connect to the Internet via a limited number of global IPv4 addresses. Restricts end-to-end principle of the Internet.
PDA	Personal data assistant, e.g. a handheld PC.
PKI	Public Key Infrastructure. Used to exchange keys used for data encryption.
Peer-to-peer	Communication model in which client devices may communicate directly, initiating the data exchange in either direction, without a server system.
RFC document	The document format used by the IETF to describe Internet standards.
RIPE NCC	The organisation (regional registry) that assigns IPv6 top-level prefixes in Europe.
SIP	Session Initiation protocol. Used for VoIP.
Static IP address	An IP address allocated to a device that does not change, thus allowing the device to be consistently found at that address. Important when running Internet services to that device.
Tunneling	Using one version of IP to carry (deliver) data from another version of IP, currently most usually IPv6-in-IPv4 to link two IPv6 networks over the commodity IPv4 Internet.
UMTS	The third generation mobile communications system.
VoIP	Voice over IP. Using an IP network to carry voice data.
Wireless LAN	A local network communication over an air interface. The current 802.11b standard allows 11Mbit/s maximum throughput over a wireless LAN.
xDSL	The set of Digital Subscriber Line technologies, including ADSL.