Chicago, Illinois - USA
29 May – 2 June 2006

SOURCE: **ATIS**

TITLE: **ATIS IPv6 Report and Recommendation - May 2006**

AGENDA ITEM: **GSC11 OPENING; 4.3**

DOCUMENT FOR:

Decision	
Discussion	
Information	**XX**

1 DECISION/ACTION REQUESTED

N/A

2 REFERENCES

N/A

3 RATIONALE

ATIS Internet Protocol Version 6 (IPv6) Report & Recommendation - May 2006 provides an initial survey of deployment drivers and challenges that service providers may face when considering their deployment of commercial IPv6 services. It also outlines transition strategies to mitigate those deployment challenges

Aspects noted in this report include the key reasons for or drivers behind the transition to IPv6; the impacts a transition will or will likely have on an existing Internet IPv4 infrastructure; the identification of respectable transition methods available; and, finally, transition recommendations and strategies worth consideration.

4 CONSEQUENCES AND IMPLICATIONS

N/A

5 ISSUES FOR DISCUSSION

N/A

ATIS INTERNET PROTOCOL VERSION 6 (IPV6) REPORT & RECOMMENDATION

May 2006

ATIS is a technical planning and standards development organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. Over 1,100 participants from more than 350 communications companies are active in ATIS' 22 industry committees, and its Incubator Solutions Program.

< http://www.atis.org/ >

ATIS Internet Protocol version 6 (IPv6) Report & Recommendation

This is an ***ATIS Report*** developed by the **IPv6 Task Force** for the **TOPS COUNCIL**.

This document is a *work in progress* and subject to change.

Published by
Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

TABLE OF CONTENTS

LIST OF FIGURES

EXECUTIVE SUMMARY

Given the ever-increasing international deployment of Internet Protocol version 6 (IPv6), the ATIS Technology and Operations (TOPS) Council agreed that the industry -- as represented by ATIS member companies -- would be well served by assessing the various aspects of IPv6 and communicating a consensus view on aspects of deployment, transitioning, and drivers with respect to its perspective. In answering this need, the TOPS Council commissioned the IPv6 Task Force to assess various aspects of IPv6, such as key reasons for or drivers behind the transition to IPv6, and the impacts a transition will or will likely have on the existing Internet Protocol version 4 (IPv4) infrastructure.

The deployment and availability (from service providers) of new services, features, and functions in the North American marketplace for IP network services is typically driven by one of the following rationales:

a. Customer interest reflecting new network services enabled by IPv6 (e.g., IP Multimedia Subsystem (IMS), peer-to-peer applications, or mobility enhanced services); although these demands are, as yet, untested;
b. Customer interest reflecting a change in the characteristics required by an existing customer demand (e.g., enterprise networks migrating from IPv4 to IPv6 may require IPv6 support in their Virtual Private Networks (VPN), the United States government's deadline of June 2008 as the date by which all agencies' infrastructure (network backbones) must be using IPv6);
c. Service provider concerns may include efficiency improvements; however, these do not accrue until after the transition costs are incurred. (i.e., leading to potential reductions in operational costs) ; or
d. Service provider concerns may be responses to emergent problems (e.g., service providers unable to obtain sufficient public address space) in service delivery.

Since some academic and international organizations have already deployed IPv6, it could be argued that the transition has already begun. Although organizational-specific factors will drive the pace at which networks are eventually transitioned to IPv6, it is generally accepted that transitioning to IPv6 is a matter of *when*, not *if*; though it is likely that some IPv4-only networks will survive. It is partially for this reason that transition technologies have been specifically designed to enable an evolutionary path reflective of normal life-cycle updates in order to minimize deployment and operational interdependencies and cost. However, it is recognized that a uniform transition plan will likely never be adopted by industry, as each organization's needs differ. To ensure end-to-end interoperability during the transitional phase, however, the IPv6 Task Force recommends the general adoption of a dual-stack transition approach complemented with tunneling technologies.

As the transitioning of existing networks occur, technical and operational challenges will surface. For example, there is no certainty whether Network Address Translators (NAT) usage will decrease, increase, or remain constant over time since many NAT users may not wish to "expose" their private addresses. While in theory it would be preferable to encourage the "elimination" of NAT, it is unlikely that in the future transition to a dual-

stack environment this would easily occur as NAT devices will remain an important address amplification and security mechanism for IPv4 only sites and requirements in the dual-stack scenario. This, as well as equally important challenges noted in this report, need further study. In this context, additional focus by ATIS or its committees may be necessary.

Also, as enumerated in this report, setting a timeline under which existing networks should transition or when native IPv6 networks should be deployed is not practical, as demands will differ across various organizations. With this boundary in place, the IPv6 Task Force does highly recommend that certain initiatives in preparation for this event start now, if they are not already underway. Namely, in preparation for transitioning to IPv6 and eventual IPv6 dominance, the following events (in no particular order) are recommended to start as soon as possible:

- Train operators and designers (personnel) for IPv4 to IPv6 knowledge and interworking skills.
- Begin internal planning and lab trials and offer a limited launch of IPv6 to gain experience. A limited launch could consist of offering a tunnel or initiating trial peering.
- Acquire /32 addresses from the American Registry for Internet Numbers (ARIN).
- Inventory every aspect of an existing IPv4 operating system to include routers, applications, servers, and hosts.
- Inventory IPv6 compatible equipment, and inventory deployed dual-stack equipment to include routers, applications, servers, and hosts.
- Assess current inventory of IPv4 addresses and determine a timeframe for address exhaustion.
- Provide feedback to vendors on ascertaining requirements.

1 INTRODUCTION

Amid the growing interest in North America to transition communication systems to Internet Protocol version 6 (IPv6), the TOPS Council -- a standing committee of the ATIS Board of Directors -- agreed that industry (as represented by ATIS member companies) would be well served by assessing the various aspects of IPv6 and communicating a consensus view with respect to its perspective. The intent of this report is to provide that viewpoint.

1.1 Purpose

This report is intended to provide an initial survey of deployment drivers and challenges that service providers may face when considering their deployment of commercial IPv6 services. It also outlines transition strategies to mitigate those deployment challenges.

In order to develop the rationale for those challenges, it is necessary to first start with some consideration of what factors may be potential drivers for a service provider to offer a commercial IPv6 service. Indeed, establishing a rational commercial basis for that decision may be the largest deployment challenge.

1.2 Scope

Produced by the TOPS Council's commissioned IPv6 Task Force, this report touches on various aspects of IPv6 at a high-level. This report is not intended to be all inclusive and does not attempt to address the multiplicity of issues around IPv6. For details regarding the opportunities and challenges around IPv6, or for an in-depth comparison of IPv4 to IPv6, readers are encouraged to pursue the vast amount of information referenced in this report, as well as that information generally available on the Internet.

Aspects noted in this report include the key reasons for or drivers behind the transition to IPv6; the impacts a transition will or will likely have on an existing Internet IPv4 infrastructure; the identification of respectable transition methods available; and, finally, transition recommendations and strategies worth consideration.

2 DRIVERS/REASONS FOR TRANSITION

2.1 Business Factors

Service providers are driven by the demands of their customers. Therefore, a likely scenario for service providers to evolve to IPv6 would assume sufficient demand and interest of IPv6 applications and services in the customer space to create demand for networked IPv6 services. Such applications would need to provide sufficient value for customer adoption without Wide Area Network (WAN) IPv6 capabilities, but still be enhanced by the availability of such WAN services. An application involving the ad-hoc networking of customer electronic devices may provide such a driver. Given the paucity of infrastructure for connectivity and the inconvenience of cabling in such environments, wireless technologies may predominate. Predicting the commercial availability and

market success of wireless IPv6-enabled customer electronics devices is, however, somewhat speculative.

In spite of these uncertainties, it is widely anticipated that industry's initial push to wide scale deployment of IPv6 will come from large enterprises, such as in response to government contract requirements for an all IPv6 backbone. As stated before the United States' House Committee on Government Reform, the Office of Management Budget (OMB) has set June 2008 as the date by which all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must interface with this infrastructure[1].

In a recently released government report, five general categories of benefits associated with IPv6 have been identified:[2]

a) *Increased Address Space* – While considered a potentially large benefit, the report also indicated that this was not a near term issue in the U.S.
b) *Simplified Mobility* – It is believed that IPv6 can better support mobile device applications than current available options in IPv4. While this may also be a large benefit, new applications may be driven from other markets.
c) *Reduced Network Administration Costs (e.g., auto-configuration)* – A modest benefit that may not occur until some indeterminate future time when the transition is complete.
d) *Improved Network efficiency (by the removal of NATs, firewall, etc.)* – A modest benefit that may not occur until some indeterminate future time when the transition is complete.
e) *Improved Quality of Service (QoS) capabilities with the newly introduced flow label* - A modest benefit that may not occur until some indeterminate future time when the transition is complete.

The second push to wide-scale deployment will be driven largely by wireless base networks looking to offer a variety of peer-to-peer multimedia services. More specifically, with the adoption and eventual deployment of the IMS architecture, wireless service providers may transition to IPv6 to offer IMS services like push to talk, inter-carrier roaming of applications, and Internet-based applications.

A third push to wide-scale deployment of IPv6 will result from consumer and home networking demands.

2.1.1 Large Enterprises

A leading driver for the North America's transition to IPv6 will be the adoption of IPv6 by large enterprises such as federal and state governments, corporations, and universities. Government agencies within the U.S. have already set June 2008 as its date

[1] Executive Office of the President, Office of Management and Budget (OMB), "Memorandum for the Chief Information Officers, M-05-22, August 2, 2005."
[2] US Dept of Commerce/NIST/NTIA - "Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)" January 2006.

by which all agencies must be using IPv6. The result of the government's mandate, which in and of itself will not drive wide-scale IPv6 deployment, is expected to have a cascading effect within the industry as other large enterprises rapidly transition to IPv6 to interoperate with or in support of existing or future government contracts and business. Such networks are typically private networks from the perspective of the service provider and in many cases require dedicated infrastructure. Initial deployment approaches also seem likely to be biased towards various tunneling mechanisms to minimize the impact on the existing network infrastructure, where these services must be provided over shared infrastructure.

While it may be tempting to assume that such networks are only concerned with a relatively few high speed links (e.g., GigE) between major government installations, such networks typically involve a plethora of lower speed links (e.g., "Business x - Digital Subscriber Lines (xDSL)"). As such, in practice it can be difficult to distinguish such networks purely on the basis of "speeds and feeds."

2.1.2 Residential (Consumer) Networking

As outlined in a recent Internet Society briefing, the use of IPv6 in the home is expected to meet the home networking needs of simple configuration, simple application development and security. The widespread adoption of IPv6 is dependent on support of IPv6 in popular operating systems and standards under development, for instance, in the areas of name service in the home using stateless Domain Name Server (DNS) server discovery or multicast DNS and transporting IPv6 through simple IPv4 NAT. Home networks today are predominantly comprised of PCs running IPv4, perhaps behind a home gateway. The scope of home networking, however, is undergoing a paradigm shift whereby there is a trend away from the PC-only household towards a much richer set of devices and applications involving entertainment media, conferencing, and command and control that will see the rise of significantly more complex home networking scenarios.[3]

Today, IPv6 enablers are beginning to emerge in Operating Systems (OS) and router technology in the current home networking scenario. In the near future, home networks running new versions of the Microsoft OS will have IPv6 built in. Both Microsoft Windows Vista and Windows Server "Longhorn" include the Next Generation Transmission Control Protocol/Internet Protocol (TCP/IP) stack: a redesigned TCP/IP protocol stack with an integrated version of both IPv4 and IPv6. Microsoft Corporation. is making IPv6 the foundation of its next major operating system release. When released, Windows Vista and Windows Server Longhorn will be fully compatible with IPv6, with the new version of the Internet protocols turned on by default and used as the preferred transport. Although users will be able to turn off IPv4 and run Vista with IPv6 only, it is more likely that in the near term a dual protocol stack will be used to ensure connectivity with existing IPv4 networks. EarthLink Research and Development has reworked the open source firmware of the popular Linksys model WRT54G™ home gateway to support IPv6. The firmware rework enables the WRT54G using Tunnel Set-up Protocol (TSP) to work with a network-based Tunnel Broker to: a) acquire a publicly

[3] Reference materials at: < www.isoc.org >.

routeable /64 IPv6 prefix; b) provide IPv6 addresses from that prefix to hosts on the home network; and c) route IPv6 home network traffic to the greater IPv6 Internet.

2.2 Technology Factors

2.2.1 Wireless Internet Applications

Mobility is quickly becoming an important feature in networks and a major driver in the need for more IP addresses. Mobile IP –specifically Mobile IPv6-- is a routing technique deployed when a user's IPv6 device is connected at a location distant from its home location. This technique allows nodes to remain reachable while moving around in the IPv6 network.

When a user roams outside the home network and registers at a foreign link, IPv6 auto-configuration is used to identify a local "care-of" (i.e., forwarding) address. This IPv6 care-of address is sent back to the user's home network and a binding (association) is established between the mobile device's home address and the care-of address. As packets arrive for the user in the home network, the "home agent" function, now established, will respond to the routing queries and forward the packets directly to the foreign link.

Due to the enhancements inherent in IPv6 (i.e., auto-configuration, route optimization, improved header), Mobile IPv6 requires less overhead than Mobile IPv4, where the home network must establish a home agent and the visited network must establish a foreign agent so that packets can be tunneled from the home network to the foreign network.

Mobile IPv6 enables packets addressed to the home address of the mobile device to be routed directly to the foreign link by caching the binding of the home address with the care-of address.

Utilizing route optimization, most packets forwarded to the mobile device are sent using the improved IPv6 header, rather than IP encapsulation (as in Mobile IPv4). This reduces overhead and makes Mobile IPv6 more efficient.

Security concerns do exist in Mobile IPv6. For instance, it is imperative that packets forwarded from the home network are forwarded to the correct IPv6 address and device. To address this concern, periodic binding updates are sent to ensure that binding information is current and IP-security (IPsec) is utilized for securing packets (especially binding updates). It is also critical that both the mobile device and the home agent support and use the Encapsulating Security Payload (ESP) header in transport mode and must use a non-null payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

The benefits associated with the use of mobile IPv6 include:

a) No need to deploy special "foreign agents." Standard IPv6 address auto-configuration features perform all the tasks that a foreign agent did in IPv4 mobility;

b) Route optimization is a fundamental part of the protocol rather than a non-standard set of extensions;
c) Mobile IPv6 route optimization can operate securely even without pre-arranged security associations;
d) Use of the destination options header allows route optimization to coexist efficiently with routers that perform 'ingress filtering';
e) Sending packets to a Mobile Node (MN) while away from home is more optimal because the routing header is used instead of IP encapsulation;
f) The use of the routing header removes the need to manage 'tunnel soft state';
g) Global address availability removes the need for NATs, address salvaging procedures and allows subscribers to have permanent address that can have a registered domain name.

Additional information on IPv6 Mobility is provided in Appendix C of this report.

Service providers should consider whether IPv6 mobility is considered a basic network capability in the context of NGN services (i.e., provided to all users). Current IPv4 networks typically do not provide mobile IPv4 support for all network users. If this is provided as a service provider function, then the potential interactions between Mobile IPv6 and mobility management procedures should be studied further.

2.2.2 IPv6 Specific Applications and Services

IPv6 provides the ability to enable new types of services and allows many new and different enterprise and customer assets to join the network. This opens the door to provide novel ways of offering service, managing resources, monitoring systems in real time, sharing data and deploying distributed applications.

These new services and applications often take advantage of more than one of the following IPv6 enablers:

- No restrictions on address availability
- Peer-to-Peer (P2P) enabled services
- Auto-configuration, auto-joining, plug and play networks, devices and services
- End-to-end (E2E) enabled security
- IP Mobility

The North American v6 Task Force has issued a document outlining a whole host of applications and services enabled by IPv6. Provided are a few examples.[4]

2.2.2.1 Machine-to-Machine (M2M) applications

IPv4 applications mainly provide service where a person is directly involved in receiving, sending, or posting information. The availability of IPv6 addresses, together with the other benefits of IPv6, will create an environment where IP enabled Machine-to-Machine (M2M) applications are widely deployed to manage, model, control, service,

[4] < http://www.nav6tf.org/documents/arin-nav6tf-apr05/3.Road_to_Revenue_Opportunities_YP.pdf >

and report on all manner of systems from the health of an individual, to the state of an automobile engine, to the atmospheric conditions of the world.

Many of these services are possible using IPv4, but addressing restrictions and the complexities of traversing private addressing domains create significant hurdles to the development, deployment, and operation of the services.

Examples of IPv6 enabled applications and services:

1. *Building monitoring and control systems*:
    a. Adaptive environmental control over heat, cooling, and humidity delivery.
    b. Security monitoring and alarming.
    c. System monitoring, diagnostics-automated servicing, and service dispatching (i.e., elevators, water systems, mechanical units, etc.):
        i. For example, a museum in Japan is deploying an IPv6 enabled building control system that will require approximately 20,000 sensors and controllers.
2. *Product Tethering*:
    a. Products are equipped with IP enabled monitoring, alarming, and servicing devices.
    b. Supplier or manufacturer can diagnose and in some cases service product remotely.
3. *Telematics* (Mobile networks within a vehicle):
    a. First responder vehicles fully equipped with voice/video/data services to communicate to and from central station or hospital.
    b. Taxi systems used for billing, dispatching, traffic monitoring, event detection.
        i. For example, a taxi company in Japan has IPv6 enabled sensors that detect windshield wiper activity. Taxis are automatically dispatched to the areas experiencing rain.
4. *Personal health monitoring systems*:
    a. Medial information is logged, reported, and alarmed.
    b. First responders can be dispatched when alarm is raised.
5. *Environment sensing, modeling and alarming*:
    a. Sensors can be deployed to monitor atmospheric or oceanic conditions that allow for more accurate meteorological monitoring.
    b. Extreme events such as tornados and tsunamis can be sensed and alarmed early.
6. *Distributed applications*:
    a. Distributed web-service applications rely on P2P communication.
    b. Distributed applications with public Application Programming Interfaces (APIs) are easily built over IPv6, allowing the application to be implemented by multiple organizations and deployed across disparate platforms.
7. *RFID inventory, shipping and delivery tracking*:
    a. Radio Frequency Identification (RFID) tracked entities are essentially mobile devices that can move within a building, region or around the world.

b. IPv6 mobility is ideally suited for this application.

2.2.2.2 IPv6 Mobility

The North American v6 Task Force has also identified possible benefits associated with IPv6 mobility to include:

1) *Better spectrum utilization* -- Due to the triangulation requirements of IPv4 mobility, IPv6 mobile devices use 50% less of the scarce spectrum.[5]
2) *Better battery life for mobile devices* -- It was noted that mobile devices running IPv6 had twice the battery life of IPv4 devices. Devices with IPv4 private addressing are constantly processing 'heartbeats' sent from the carrier that want to reclaim the address and re-assign it. This processing drains the battery.
3) It was also predicted that there will be 3 billion mobile subscribers in 2008.

2.2.3 IP Multimedia Subsystems (IMS)

The adoption of IP Multimedia Subsystem (IMS) is expected to drive the adoption of IPv6, as it will provide a standard communications infrastructure based on the ubiquitous IP transport layer to converge voice, data, and multimedia services via a Session Initiated Protocol (SIP) infrastructure. It is a key enabler for the support of advanced mobile multimedia services and convergence of both fixed and mobile communications services available on 3rd generation networks. IMS will provide for increased peer-to-peer communication and integration of different IP based services over both fixed and mobile networks.

IMS was specified to exclusively use IPv6 by 3rd Generation Partnership Project (3GPP) Release 5 and 3GPP2. However 3GPP Release 6, while remaining formally IPv6 exclusive, does include a technical report that provides for IPv4 and private address scheme support by early IMS implementations and deployments.[6] The use of IPv6 by IMS not only allows for the additional capabilities offered by IPv6 extended address space and "always on" paradigm, but adoption from the outset also mitigates future migration problems. While Global System Mobile (GSM) and Universal Mobile Telecommunications System (UMTS) mobile network operators may be implementing some IP-based services such as General Packet Radio Service (GPRS) initially using IPv4, GPRS is also IPv6 capable. IMS operating over GPRS can co-exist with IPv4 GPRS deployments, although operators who have deployed IPv4 GPRS networks will incur migration costs as IPv4 will not be capable of meeting the anticipated growth and address space need and could slow the development of global IPv6 IMS.

IPv6 is needed in order to make peer-to-peer services work between operators' networks, as these services only work well with public IP addresses. The SIP/IMS user plane is real-time peer-to-peer in nature. Thus SIP/IMS sessions between private IPv4 addresses become highly complicated, requiring client-server interaction. In the client-server service delivery model, commonly found today for Internet services, information is accessed via Web pages or information on or collected by one or more servers. P2P services such as content sharing, VoIP applications, conferencing, and gaming are E2E in

[5] < http://www.larta.org/lavox/articlelinks/2004/041129_ipv6.asp >
[6] Specifications for IMS support of IPv4 can be found in clause 5.1 of TS 23.221[3] (October 4, 2005).

nature and are most effective and robust without the intervention of intermediate servers.

The convergence of IMS increases the value proposition for applications and services, now offered to end users via a variety of networks. Standards based IMS enables interoperability of services between fixed, mobile, and IP-based networks, and network operators and service providers are working to integrate and package various service offerings (telephony, VoIP, Internet, television, cable entertainment, IPTV). IMS, with its converged multimedia network architecture, offers flexibility in the delivery of services from a variety of content sources to a variety of user access appliances.

IPv6, with its advantages over IPv4, can be the catalyst for the expansion of network service access and creation of new peer-to-peer applications (such as interactive gaming). The IMS architecture model is also closely integrated with an Open Service Access (OSA) architecture that allows for access to third-party applications -- thus allowing increased access to services that utilize the advantages of peer-to-peer capabilities.

2.3 Depletion of IPv4 Addresses

The most often quoted reference for IPv4 address depletion is a report authored by Geoff Huston at the Asia Pacific Network Information Centre (APNIC).[7] Until recently, the conclusion of that report has been that IPv4 address depletion would not be an issue until sometime beyond 2020. The latest release of that report, however, predicts that the Internet Assigned Numbers Authority (IANA) will actually exhaust its addresses by 2013, and total exhaustion will occur around 2022. Even with this revised prediction, there is some evidence that the conclusions of that report do not reflect what is likely to happen over the next decade.

A recent report published by Tony Hain at Cisco System concludes that IANA will actually exhaust its addresses before the end of this decade.[8] It was predicted that by November 2005 somewhere in the order of 140/8 IPv4 addresses would have been allocated by IANA. The reality of what has happened, however, is very different from what was predicted. As of November 2005, 156/8 addresses have been allocated.

Hain makes the case that a five (5) year bias (2000-2005) should be used to predict what will happen as opposed to a 10 year bias used by Huston. He argues that between 1995 and 2000, Classless Inter-Domain Routing (CIDR), NAT, and the technology downturn created irregularities that should not be included in the predictive model.

After IANA runs out of IPv4 addresses, the five (5) Regional Internet Registries (RIRs) are suspected to have about 12-18 months worth of addresses to allocate to Internet Service Providers (ISPs). Both reports agree on that buffer of addresses; but disagree on what will happen after IANA and the RIRs have exhausted their addresses.

[7] < http://www.potaroo.net >
[8] < http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_8-3/ipv4.html >

Huston predicts that an address trading market will emerge where addresses that have been allocated but never used (~46/8s) will be bought and sold on the open market. Huston suggests that this will extend the life of IPv4 for many years. Hain argues that this market will not produce a significant supply of addresses and the world will effectively run out of IPv4 addresses by sometime around 2010.[9]

From the arguments noted, the best that can be said about IPv4 address exhaustion, timeframes is the following:

- It is reasonably certain that the IPv4 address space will be exhausted by 2016;
- It is probable that the IPv4 address space will be exhausted by 2012; and
- It is possible that the IPv4 address space will be exhausted by 2009.

It is likely that the IPv4 address space will effectively be exhausted well before the actual depletion of the addresses. As addresses become scarce, IPv4 address allocation fees and administrative policy restrictions will make IPv6 only solutions more attractive.

At the time of effective IPv4 address exhaustion there will be three types of connected customers and services:

- *IPv4-only sites:* These sites will not have access to the new emerging IPv6 services and clients.
- *IPv6-only sites*: These sites will not have access to the large body of existing IPv4 services and sites.
- *Dual-stack IPv4 & IPv6 connected sites*: These sites will have access to everything.

The ISP community plays a critical role in determining how the IPv6 Internet will emerge and how converged or isolated the IPv4 and IPv6 worlds will be.

In view of the uncertainty regarding IPv4 addresses, it is recommended that service providers consider their IPv4 address inventory, historical IPv4 address consumption rates, and planned service deployment initiatives to determine when they expect to reach IPv4 address exhaustion.

2.4 Political Factors

2.4.1 U.S. Government Direction

The United States Government, in particular the Department of Defense (DoD), has provided much of the initial push towards the use and direction of IPv6 deployment in the United States.

The 2003 DoD announcement of the Department's decision to complete a transition to IPv6 by fiscal year 2008 included a requirement that, beginning October 1, 2003, all network assets developed, procured, or acquired by the Department were to be IPv6 capable. With a $25B per year budget for information technology, the DoD's embrace of

[9] http://www.apnic.net/docs/apster/issues/apster12-200412.pdf and
http://www.circleid.com/posts/twenty_myths_and_truths_about_ipv6_and_the_us_ipv6_transition/

IPv6 in 2003 has had a significant impact on the development of a government-wide adoption and transition strategy.

In support of the DoD's plan for IPv6, the OMB and House Committee on Government Reform have also taken active roles in leading the U.S. government towards IPv6 adoption.

As stated before the United States' House Committee on Government Reform, OMB has set June 2008 as the date by which all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must interface with this infrastructure. Following the June 20, 2005 hearing on "To Lead of Follow: The Next Generation Internet and the Transition to IPv6" held by the House Committee on Government Reform, the OMB issued *Memorandum for the Chief Information Officers (M-05-22, August 2005)* that outlined the plan for government agencies' transition from IPv4 to IPv6.

This *Memorandum* requires that by June 2008, all federal agency network backbones must be using IPv6 and that all federal agency networks must interface with the IPv6 network. The "meaning of network backbone," as defined by OMB in the *Memorandum*, is either operating a dual-stack network core or it is operating in a pure IPv6 mode -- i.e., IPv6-compliant and configured to carry operational IPv6 traffic.

The *Memorandum* also acknowledges the roles of the National Institute for Standards and Technology (NIST) to develop a standard to address IPv6 compliance for the federal government and the General Services Administration (GSA) and the Federal Acquisition Regulation (FAR) Council to develop a suitable FAR amendment for use by all agencies in their reporting requirements. However, in the report published by NIST and National Telecommunications and Information Administration (NTIA), the NIST IPv6 Task Force states that it "believes that aggressive government action to accelerate private sector deployment of IPv6 is unwarranted at this time."[10,] In terms of the public sector, the record indicates that IPv6 is increasingly being incorporated into Internet hardware and software. Consequently, the Task Force believes that federal agencies should initiate near-term, focused efforts to plan and operationally prepare for the increasing availability and use of IPv6 products and services in both internal and external networks.

The U.S. government is an important client to most of the major IPv6 network equipment vendors and Internet service providers. In positioning the federal government to be a leader in the transition from IPv4 to IPv6 in the U.S., NTIA and other agencies responsible for creating transition plans are working closely with vendors to evaluate current IPv6 feature capabilities against U.S. government requirements.

2.5 Interoperable Global Communications

With the increase of IPv6 only clients (e.g., network infrastructures, services, and enterprises) in Asia and the increasing deployment of IPv6 infrastructures in Europe, North America is faced with a compelling driver to deploy IPv6: ensuring interoperable

[10] US Dept of Commerce/NIST/NTIA, "Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)" January 2006 (Page 8).

service-transparent offerings to their consumers. More precisely, by maintaining IPv4-only sites, users are locked out of using IPv6 only services. As such, the existence of IPv6-only services will further tip the scales to wide spread transition to IPv6.

2.6 Mergers & Acquisitions

Often when companies using IP networks are involved in mergers or acquisitions, there is a requirement to integrate -- at a minimum – the data communications networks for applications such as email and common corporate data servers. Depending on the size of the companies and their business focus, there may be several IP networks with various ranges of both public, globally-routable registered IP addresses and private RFC 1918 addresses. It is also not uncommon that these multiple networks will have different exposure to the public Internet as well as to other internal private networks, due to cost, security, routability, or other factors. In many cases, there is a large possibility that each of the previously independent companies are using the same ranges of RFC 1918 private IP address. In these situations of overlapping IP address ranges, the network operators must either renumber one of the ranges prior to integrating the networks or maintain the networks individually and employ a NAT or ALG between the two networks.

Renumbering an existing network using private IP addresses in the RFC 1918 range can present some challenges as well as expenses. Finding unused private addresses that are available in both networks is not always possible, and in situations where more than two networks need to be integrated, the complexity increases. Assuming common addresses can be negotiated between the networks, the level of difficulty increases when there is a requirement for future integration of still another private network. In addition to the challenge of finding common available space, there is the expense involved in "visiting", either physically or remotely, each device that requires readdressing, as well as updating and testing any applications that may be dependent on the use of those specific addresses. Although there is an acknowledgement in the ARIN Number Resource Policy Manual that allows for the use of public registered addresses on private networks not connected to the Internet, there is time and expense involved in applying for and justifying the use of globally unique addresses.[11] Additionally, assuming the application is granted, there is still the associated expense with the actual renumbering and testing of devices.

The use of NATs and Application Layer Gateways (ALGs) as a mechanism to interconnect networks of merged companies introduces its own level of complexity and expense. Instead of using an addressing solution to solve the network integration issue, this approach uses a routing solution. The long-term problem is that the goal of integrating the networks is avoided, not addressed, and that the routers managing the interconnection must be maintained on an ongoing basis as changes are made to both individual networks.

Section 5.5 of this document discusses Unique Local IPv6 Unicast Addresses as defined in RFC 4193. If IPv6 private unique local addressing were used in situations where

[11]< http://www.arin.net/policy/nrpm.html >, Section 4.3.5, Non-connected Networks.

public addresses are not required or justified, there would be a high probability of uniqueness of private IPv6 address. This would totally avoid the problems associated with the limited availability of IPv4 private addresses.

3 TRANSITION TECHNOLOGIES

Transitioning from IPv4 to IPv6 will take years, and organizations or groups within organizations will likely continue to use IPv4 indefinitely. Therefore, while native IPv6 is the long-term goal, equal consideration must be given to the interim coexistence of IPv4 and IPv6 nodes, as well as the eventual roadmap to native IPv6. To this end, several transition plans are available for consideration.

- Dual Stack
- IPv6 over IPv4 Tunneling
  - 6to4 Tunneling
  - Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
  - TEREDO
  - Tunnel Set-Up Protocol (TSP)
- 6PE Deployment
- IPv4-IPv6 Interworking (Translation)

The *Recommendation for the IP Next Generation Protocol* specification from IETF (RFC 1752) defined the following transition criteria:

- Existing IPv4 hosts can be upgraded at any time, independent of the upgrade of other hosts or routers.
- New hosts using only IPv6 can be added at any time, without dependencies on other hosts or routing infrastructure.
- Existing IPv4 hosts with IPv6 installed can continue to use their IPv4 addresses and do not need additional addresses.
- Little preparation is required to either upgrade existing IPv4 nodes to IPv6 or deploy new IPv6 nodes.

3.1 Dual-stack

Dual-stack consists of a separate implementation of the TCP/IP and User Datagram Protocol (UDP) suite of protocols that includes both an IPv4 Internet layer and an IPv6 Internet layer. This is the mechanism used by IPv6/IPv4 nodes so that communication with both IPv4 and IPv6 nodes can occur. All upper layer protocols in a dual-stack implementation can communicate over IPv4, IPv6, or IPv6 tunneled in IPv4.

3.2 IPv6 over IPv4 Tunneling

IPv6 over IPv4 tunneling is the encapsulation of IPv6 packets with an IPv4 header so that IPv6 packets can be sent over an IPv4 infrastructure.

3.2.1 6to4 Tunneling

6to4 is an address assignment and router-to-router automatic tunneling technology that is used to provide unicast IPv6 connectivity between IPv6 sites and hosts across the IPv4 Internet.

3.2.2 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

ISATAP is an address assignment and host-to-host, host-to-router, and router-to-host automatic tunneling technology that is used to provide unicast IPv6 connectivity between IPv6 hosts across an IPv4 intranet. ISATAP hosts do not require any manual configuration and create ISATAP addresses using standard address auto-configuration mechanisms.

3.2.3 TEREDO

TEREDO, also known as *IPv4 NAT traversal for IPv6*, provides address assignment and host-to-host automatic tunneling for unicast IPv6 connectivity across the IPv4 Internet when IPv6/IPv4 hosts are located behind one or multiple IPv4 NATs. To traverse IPv4 NATs, IPv6 packets are sent as IPv4-based UDP messages.

6to4 provides a similar function as TEREDO; however, 6to4 router support is required in the edge device that is connected to the Internet. 6to4 router functionality is not widely supported by IPv4 NATs. Even if the NAT were 6to4-enabled, 6to4 would still not work for configurations in which there are multiple NATs between a site and the Internet.

3.2.4 Tunnel Setup Protocol (TSP) and Tunnel Broker

Another automatic tunneling approach is a *tunnel broker-based TSP*. In the simple model, a single network device sits on the IPv4 network and the IPv6 network and acts as both the tunnel-broker and tunnel gateway. (For a dual-stack TSP client, an IPv6 tunnel is established to the tunnel broker over the IPv4 network.) The client then uses that tunnel for all IPv6 communications. TSP clients can run on single user devices (i.e., Windows PCs) or devices that could act as gateways to a sub-network of users (i.e., Unix, Linux). The broker could be configured to allow all users, or provide RADIUS-based authentication.

3.3 6PE Deployment

A *6PE* RFC 4364 based solution involves turning on one or more IPv6 Virtual Router Forwarding (VRF) on the edge devices. Packets are transported over IPv4/MultiProtocol Label Switching (MPLS) across the core of the network. For general Internet access, one VRF can be used to aggregate many customer connections. For enterprise Layer 3 Virtual Private Network (VPN) service, an IPv6 VRF or dual-stack VRF can be turned on for each customer connection.

4 DEPLOYMENT CHALLENGES

It has been frequently stated that deployment of IPv6 will allow the original philosophical vision of the Internet for P2P addressability to be realized. While this may

have been true, private addresses and NAT have been widely deployed without alarm to this original philosophy. Returning the Internet to this original philosophy, therefore, would require a considerable amount of effort and resources. Furthermore, many users and enterprises do not care about the original philosophy, such that it is not a driving issue worthy of expending scarce resources. Instead they merely want peer-to-peer applications to work. Enabling these applications to work does not require returning the Internet to the originally envisioned philosophy, but instead can be achieved by work-arounds and incremental designs and implementations that are considerably more manageable and affordable.

4.1 Security

During industry's transition to IPv6 and -- subsequently -- the proliferation of dual-stack IPv6-capable software and devices, focus must be given to properly configuring and managing these offerings, as abuse by attackers can occur. Additionally, even though IPsec is widely used in IPv6, NAT will likely continue to be desired by many for IPv4 environments. However, IPsec and NAT tend to be incompatible and problems are likely to occur in a dual-stack network.

In April 2005, the United States Computer Emergency Response Team (US-CERT) at the Department of Homeland Security (DHS) issued an IPv6 cyber security alert to federal agencies based on testing and discussions with DHS officials. The alert warned federal agencies that unmanaged, or rogue, implementations of IPv6 present network management security risks. Specifically, the US-CERT notice informed agencies that some firewalls and network intrusion detection systems do not provide IPv6 detection or filtering capability, and malicious users might be able to tunnel IPv6 traffic through these security devices undetected. More specifically, as many host and router stacks today have IPv6 capabilities that may be turned on by default without any knowledge of the user, it is possible to connect to dynamic tunnel concentrators using static any-cast addresses. Consequently, the upstream provider does not have to support IPv6 for a user to get connected to the IPv6 Internet tunneling over IPv4. Organizations, as such, need to start implementing IPv6 security strategies today to protect valuable resources.

Different transition paths and choices will come with different security concerns, as organizations transition to IPv6. As examples, when using a dual-stack approach, IPv4 addresses may be private while IPv6 will be global. For a static tunneling approach, malicious IPv6 packets can be carried within valid IPv4 tunnels and, finally, with dynamic tunneling, end points can be easily spoofed. It is also important to note that IPv4 security policies are not adequate for IPv6. As such, many aspects of IPv6 will require different policies, for instance:

- Anycast addresses
- Scoped addresses
- New extension headers
- Tunneling protocols
- Transport headers and deep packet inspection
- Privacy addresses
- ICMP options

A different approach to security is required if users within an organization are permitted to connect peer-to-peer to other users. Therefore, dynamic security policies need to be driven from the trusted user. Standards and product for defining and deploying host-based security architectures are in their infancy and need to mature. Such distributed dynamic architectures are likely to be more complicated than more centralized static systems and, until then, static perimeter security needs to be deployed and enhanced to support IPv6.

One of the key values of IPv6 is that there are many new automation features that can reduce operational overhead. However, inherent with increased automation are increased vulnerabilities. Namely: malicious users can spoof solicitation, advertisement, and binding messages. To combat this problem, mechanisms have been developed to provide securer automated capabilities.

Given the current stability of IPv6 relative to IPv4, it is expected that many security "holes" are likely to be found in IPv6, especially as it continues to be deployed. However, as IPv6 evolves, the robust security features associated with IPv6 will improve as a result of increased use of end-to-end security functions. In the near-to-short-term, it is anticipated that IPv6 will deliver minimal value-add to security than what is realized in IPv4-only networks today.

4.1.1 Security Issues around 6to4: Request for Comment 3964

The IPv6 interim mechanism 6to4 (RFC 3056) uses automatic IPv6-over-IPv4 tunneling to interconnect IPv6 networks. The architecture includes 6to4 routers and 6to4 relay routers, which accept and de-capsulate IPv4 protocol-41 ("IPv6-in-IPv4") traffic from any node in the IPv4 Internet. This characteristic enables a number of security threats, mainly Denial of Service (DoS). It also makes it easier for nodes to spoof IPv6 addresses. RFC 3964 discusses these issues in more detail and suggests enhancements to alleviate the problems. In the interim, configured tunnels are the recommended secure practice for external transition methods.

When automatic tunneling is used, strong ingress filtering and route policies on both IPv6 and IPv4 environments is required and products need to execute proper security and process checks -- i.e., checking that the IPv4 and IPv6 addresses are conversion matched.

4.2 NAT Gateways and Security

In the IPv4 environment, the use of NAT to map single IP addresses to multiple nodes within a private or home network has extended the lifespan of IPv4 through address conservation. In addition, when used in a pure IPv4 environment, NATs are also perceived to provide some security due to the anonymity of the private address to the public Internet beyond the gateway, which cannot be reached except through mapping. These firmly held beliefs that NAT devices not only provide an address amplification function but also a security function are the biggest challenges to the widespread deployment and usage of IPv6.

As industry transitions to a dual-stack IPv4/IPv6 environment and then beyond to a pure IPv6 environment, NATs may present significant challenges to the achievability of true end-to-end applications. Wide spread deployment of NAT devices, as seen today, do not support bi-directional communication, global addressing, always on systems, peer to peer networking, and push technologies -- all of which are inherent to the design of IPv6.

There is no certainty whether NAT usage will decrease, increase, or remain constant over time, since many NAT users may not wish to "expose" their private addresses. While in theory it would be preferable to encourage the "elimination" of NAT, it is unlikely that in the future transition to a dual-stack environment this would easily occur, as NAT devices will remain an important address amplification and security mechanism for IPv4-only sites and requirements in the dual-stack scenario. In addition, some analysts supporting private networks consider the lack of support for NATs and private address space in IPv6 a design deficiency in IPv6, rather than a desirable architectural objective.[12]

4.3 Product Availability

4.3.1 Host & Clients

With Microsoft's implementation of an IPv6 dual-stack architecture in their Windows XP and Windows Server 2003 Windows Vista™ (a.k.a. Longhorn) application due to be released in 2007, IPv6-capable applications are likely to become the norm rather than the exception. The separate IPv4 and IPv6 protocol components used by Microsoft support separate Transport layer that include TCP, UDP, and framing layer. In addition, the stack has both IPv4 and IPv6 enabled by default, thereby eliminating the need to install a separate component to obtain IPv6 support.

IPv6 applications support by Windows includes:

- *FTP Client*: The File Transfer Protocol (FTP) client, Ftp.exe, can be used to establish FTP sessions with IPv4 and IPv6 FTP servers.
- *Telnet client*: The Telnet client, Telnet.exe, can be used to establish Telnet sessions with IPv4 and IPv6 Telnet servers.
- *Internet Explorer*: The new Internet extensions dynamic link library, Wininet.dll, enables Web browsers to access IPv6-enabled Web servers. For example, Wininet.dll is used by Microsoft Internet Explorer to make connections with a Web server to view Web pages. Internet Explorer uses IPv6 to download Web pages when the DNS query for the name of the Web server in the Uniform Resource Locator (URL) returns an IPv6 address.

Although very few application developers are actually selling IPv6-capable products today, many developers have been testing IPv6 and planning to integrate IPv6 into their products. Expectations are that IPv6-capable products will be introduced as early as 2007.

Examples of Host Operating System support for IPv6 include:

[12] Burton Group, D. Golding, "IPv6: Unmasked", version 1, February 8, 2006.

- *Microsoft Windows*:
  - XP supports IPv6
    - Service Pack 2 embeds IPv6 functionality. The TCP/IP protocol suite includes both IPv4 and IPv6. However, the IPv4 and IPv6 versions of TCP and UDP are not integrated, as is the case with a typical dual-stack implementation.
    - IPv6 is available once Service Pack 2 is installed.
  - Vista
    - Vista is currently in Beta trial and due to be released in 2006. Vista fully supports an integrated dual-stack operating system. All Microsoft applications delivered with Vista will be IPv6 capable.
    - IPv6 is on by default.
- *Sun Workstation with Solaris 8*:
  - Solaris 8 and later versions fully support IPv6. IPv6 is enabled during the installation process.
  - Once installed, IPv6 is on by default.
- *FreeBSD*:
  - FreeBSD has kernel support for IPv6.
  - IPv6 is enabled by adding an enabling command to the /etc/rc.conf file.
- *Linux*:
  - Linux 2.4 supports IPv6. However, enabling IPv6 requires either recompiling the kernel with IPv6 support or loading an IPv6 module.
- *MAC OS X*:
  - Starting with Jaguar (a.k.a. 10.2, released mid 2002), Mac OS X supports IPv6. Includes server edition.

Essentially, with infrastructure hardware and software apparently already IPv6 "capable" today, over the next four or five years it is anticipated that the vast majority of network hardware, operating systems, and network-enabled software packages will be sold with IPv6 capabilities.

4.3.2 Other Network Equipment

Other categories of equipment in operators' networks that will also be impacted by the eventual transition to direct support of IPv6 include:

- Access equipment -- e.g., Digital Subscriber Line Access Multiplexers (DSLAM).
- Service Specific Equipment – e.g., Session Border Controllers.
- Network Measurement Infrastructure -- e.g., Deep Packet Inspection Equipment.
- Maintenance & Diagnostic equipment – both permanently connected and portable.

4.4 Cost

Transition costs have many variables and each operator will have different ratios of costs. Some networks' operators are expected to have very small associated hardware and software costs, since networks are IPv4 plus IPv6 featured out of the box. Other larger scale networks, such as service provider networks, must assess transitioning to IPv6 based on the economic and operational benefits -- e.g., their return on investment

(ROI). It is anticipated that the majority of the cost associated with the transition will center on:

1. Retraining operators and designers for IPv4 to IPv6 knowledge and interworking skills;
2. Upgrading end stations to dual-stack and testing applications (Oracle or web services by example);
3. Hardware or software changes to network;
4. Security or authentication testing of upgrades;
5. Operations Support Systems (OSS);
6. Upgrading end-user applications; and
7. Creating a suite of IPv6 services and upgrading network services such as DNS, Dynamic Host Configuration Protocol (DHCP), and Network Time Protocol (NTP).

Hardware devices such as high end routers, switches, and firewalls are beginning to offer dual-stack implementations using advanced memory and processor technologies as vendors move to "future-proof" their offerings. Software-based devices also generally provide IPv6 support and, therefore, do not require replacement. As equipment and software continue to include IPv6 capabilities, the CAPEX for IPv6 in most cases will be addressed through the normal product and/or software upgrade cycles. More precisely, assuming a gradual transition to IPv6, the cost of development can be amortized over the rest of a development cycle.

The costs of investing in IPv4 infrastructure, NAT devices, ALGs, and Proxies over time, however, will increasingly outweigh the benefits of retaining an IPv4 infrastructure and services. Additionally, it is anticipated that services and applications will continue to be developed that do not work with IPv4 or are very difficult to use with IPv4. Accordingly, the cost savings achieved by fully switching over to and operating an IPv6-only network will trigger a transition to an IPv6 dominant network.

It has also been stated that the operating costs of managing NATS and ALGs in an IPv4 network with private addresses is not cost-effective. It is estimated that in the range of 30% of IT budgets are allocated to the management of private addresses, NAT devices, ALGs, and proxies. The scarcity of global IPv4 addresses has created an environment where obtaining addresses can be expensive.

4.5 Quality of Service (QoS)

Where signaling authorizes the transmission of session based traffic, a mechanism will be required to identify that a particular data flow is indeed the flow that has been authorized and not belonging to some other session.

IPv4 assumes all bearer traffic treats on an interface as an aggregate and does not distinguish between flows. Flows in IPv4 are typically identified using a tuple of packet header information including source and destination addresses and port numbers. Many application protocols use dynamic port allocation which makes flow identification difficult in IPv4. IPv6 headers provide for improved flow identification (with the

definition of a flow id field), but no standard mechanisms are yet in place for the use of this information. A single value in the flow "ID" field could enable the network to identify as a single coherent flow what would appear to be multiple flows in an IPv4 network – e.g., the control and data channels used for an ftp transfer.

Standardized mechanisms to identify a particular data flow, as such, are required.

4.6 Operations Support Systems (OSS)

Introduction of IPv6, especially in a mode where the network supports both protocols for an extended period of time, will require extensive modifications to the OSS systems that support the current IPv4 network. Essentially, any system that has an IPv4 address field will be a candidate for modification to support both address fields.

4.7 Coexistence with IPv4

Coexistence occurs when the majority of the network's nodes communicate using an IPv4 infrastructure, an IPv6 infrastructure, or an infrastructure that is a combination of IPv4 and IPv6. True transition is achieved when all IPv4 nodes are converted to IPv6-only nodes. For the foreseeable future, practical transition is achieved when as many IPv4-only nodes as possible are converted to IPv6/IPv4 nodes. IPv4-only nodes can communicate with IPv6-only nodes only when using an IPv4-to-IPv6 proxy or translation gateway[13].

Since supporting two effectively different protocols (i.e., IPv4 and IPv6) has an inherent higher associated cost, some networks operators will look to stop supporting IPv4 sooner rather than later. The eventual decision as to when this will occur, however, will be based on independent and individual assessments. Contributors to this decision include the finite scalability of IPv4 due to security and stateful configuration models, as well as the deployment of new IPv6-only services like Mobility for IPv6 (MIPv6)[14] and Network Mobility (NEMO),[15] and their interoperability and compatibility with an IPv4 network.

In a network infrastructure supporting two different protocols, ensuring continued interoperability and compatibility across applications and services is a considerable concern among network operators. Network applications built on or around new IPv6-only services may not be IPv4 compatible at all. It is also widely promoted that IPv6 is a better protocol for E2E/P2P applications. As such, E2E wireless services may be born IPv6 only due to its IPv6 capabilities, or from other significant drivers like the lack of IPv4 available address space.

4.8 Vendor/Equipment Interoperability

IPv6 protocols are less mature than IPv4. As a result, different vendors may interpret the standards in a slightly different way. Different implementations of the standards by different vendors can lead to interoperability problems.

---

[13] "IPv6 Transition Technologies," updated September 2005, Microsoft Corp.
[14] < http://www.ietf.org/html.charters/mip6-charter.html >
[15] < http://www.ietf.org/html.charters/nemo-charter.html >

Conformance tests that measure how a product adheres to the standards exist for most of the major protocols, and most vendors will have certified their products against the conformance tests. However, the conformance tests rarely measure every nuance of a protocol, and vendors often implement enhancements that go beyond the standards to provide improved efficiency or features.

4.9 Site Multi-Homing

Site multi-homing is an important issue that is yet to be resolved in IPv6. *Site multi-homing* allows a site to connect to multiple service providers for Internet connectivity. The primary purpose is to provide redundancy in the event that there is an outage in the connection to any one service provider or there is an outage somewhere within the service provider's core network that interrupts connectivity from the site.

The solution used today in the IPv4 Internet of having the 'alternate' service provider (SP) advertise the specific prefix allocated from the primary SP is not feasible in IPv6. For instance, if this solution was used in IPv6, the alternate would have to advertise the specific /48 provider allocated address issued by the primary SP. The alternate SP does not own the larger aggregate that includes the specific address and therefore it must advertise the specific /48 to all of its peers. This /48 must be advertised throughout the Default Free Zone (DFZ) of the Internet and breaks the rule of strong aggregation.[16]

To address this challenge, the IETF is working on a protocol based solution called Shim6.[17] However, if Shim6 is not accepted as a viable solution, other solutions need to be further developed such as network/routing-based solutions and provider-independent addressing solutions. The general consensus about the routing-based solutions, however, is that they are too complicated for both the service provider and site to manage.

4.9.1 SHIM6

Shim6 is in the definition phase and there is a fair amount of controversy regarding its viability. Assuming that Shim6 is the ultimate solution for IPv6 multi-homing, it is not expected to be mature and widely implemented for several years. Widespread deployment will take even longer.

[16] Typically, service providers are allocated a /32 prefix from their Regional Internet Registry (RIR) from which they allocate /48 prefixes to each of their customers. The SP can then advertise the single /32 prefix to its peers. This provides a 64K:1 aggregation ratio. This is known as the rule of strong aggregation. Given the scope of the IPv6 address space, this rule must be achieved, otherwise performance and memory scaling problems will cause Internet core routers to become overwhelmed. The rule of strong aggregation must be preserved when considering site multi-homing issues and solutions.

[17] http://www.ietf.org and http://www.ietf.org/html.charters/shim6-charter.html

4.9.2 Routing-based Solutions

Routing-based solutions to site multi-homing are being proposed in the IETF.[18] This solution requires that each service provider create an IP in IP tunnel into the site using an address from the other service provider at the tunnel end point within the site.

The degree to which it provides redundancy depends on how the tunnel is engineered within the service provider. Greater degrees of redundancy require greater degrees of complexity. This solution is criticized in that it can not provide redundancy in the failure case where the service provider has a complete outage.

4.9.3 Provider Independent Addresses

Provider Independent (PI) addressing is another proposal designed to solve the multi-homing solution. PI addresses are derived from a site's geographical location, which -- along with a site's longitude and latitude -- determines the global prefix portion of its address. With this prefix, the site can then connect to multiple service providers using the same address. The address is then aggregated at some regional Internet Exchange (IX) point mutually agreed to by the organizations that can affect the policy at the IX points.

This solution is by far the simplest for end users, and it is certainly simpler than the routing solution for both end user and service providers. However, there is no guarantee that service providers within a larger geographical area, such as North America, will come together and cooperate and agree on continental aggregation policy. There is also a proposal under consideration in ARIN and the IETF for PI addresses that are not geographical dependent.[19]

4.9.4 Site Multi-homing Proposal

With various methods being explored to resolve site multi-homing (each with its pros and cons), ATIS member companies are encouraged to further explore the topic and proposed solutions, and reach consensus on the most appropriate approach. Of the possible approaches presented, PI addressing must be socialized amongst ATIS members in order to further understand its values and challenges. In addition, further work must be done to determine if a regional and a North American aggregation policy can be agreed to.

4.10 Dual-stack with DNS

A DNS infrastructure is needed for successful coexistence because of the prevalent use of names (rather than addresses) to refer to network resources. Upgrading the DNS infrastructure consists of populating the DNS servers with records to support IPv6 name-to-address and address-to-name resolutions. After the addresses are obtained using a DNS name query, the sending node must select which addresses are used for communication.

[18] < http://www.ietf.org/rfc/rfc3178.txt?number=3178 >
[19] < http://www.ietf.org/internet-drafts/draft-hain-ipv6-pi-addr-09.txt >

When transitioning to dual-stack IPv4/IPv6, one has to consider the implications on the applications using the IP layer. Managing applications in a dual-stack environment is anticipated to increase complexity and costs. Coordinating the transition of co-resident applications likewise is going to add complexity to the transition process.

Many applications are not Layer 3 independent and may need to be modified to support IPv6. For example, dual-stack IP support is independent of dual-stack application support. As such, not all applications have been converted to IPv6.

On a particular device, all the applications may not have been transitioned, even though the stack supports both IPv4 and IPv6. If a server has been transitioned to dual-stack, it will register both the IPv4 and IPv6 address with DNS.

The device requesting the service will receive both addresses from the DNS. Most implementations will choose IPv6 address first. In addition, if server applications have not been converted to IPv6, the session may fail.

An approach would be to upgrade all applications on a particular server before turning on IPv6 in the stack. However, due to timing, stability, testing, and availability, it may not be feasible to upgrade and transition all applications at once.

4.11 Impacts to Services

The choice of how NAT is used for IPv6 has the potential to impact the pace of the IPv6 transition. A primary motivator to transition to IPv6 is the availability of IPv6 specific services, many of which do not work or have limited capabilities over IPv4 and NAT. For the business case and widespread use of IPv6, the development of IPv6 services depends upon the anticipated availability of IPv6 ready devices and their ability to access applications and services.

The widespread deployment of NATs in the IPv4 environment has placed architectural restraints on the design and functionality of new IPv6 services, which result in added cost and complication to new service development and deployment. IPv6 specific services will: 1) not be designed for and implemented to work across NATs; 2) require "always on" addresses; 3) result in applications requiring large numbers of IP addressable devices; and 4) drive user applications and end devices to be the recipient of session connections.

IPv6 networks also do not need the address amplifying capabilities of NAT. Many applications that were not designed to run over NAT require complicated and expensive ALGs. New application development is inhibited by the constraints imposed by NATs and many E2E type services are severely limited or do not work across a NAT. Application development also is restrained by the ubiquitous deployment of NATs and IPsec/Internet Key Exchange (IKE) is difficult and not often used across a NAT.

In the initial deployment of IPv6, many IPv6 addresses are private -- i.e., internal to private enterprise networks. These addresses are then translated to allow access to public sites. Even though the devices in the private networks are IPv6 capable, the

translation of their IPv6 addresses to IPv4 addresses prevents them from accessing services created for IPv6.

The characteristics of private addresses hidden behind NAT devices create problems for IPv6 enabled services. Private addresses are only publicly visible once a NAT mapping is established. Mapping of private addresses to a public address is initiated from the private side; however, these mappings are removed after a period of inactivity. The Network Address Port Translation (NAPT) multiplexing of ports limits many services as well.

Some of the implications running applications across a NAT are that services require a DNS-ALG and a Dynamic DNS (DDNS) to register a domain name and address with DNS. Devices and users on the public side in general cannot initiate session to addresses behind a NAT. Applications that retain addresses across sessions usually break and services that connect to well known ports do not work across NAPT. IP packet reassembly also does not work across a NAPT.

NAT devices and ALGs add infrastructure and operational costs that add complexity to a site, and impact its services. As such, many applications are more difficult and costly to employ when a NAT transversal is required. Consequently, devices not hidden behind NATs can be more active in providing service or content for peer-to-peer services.

While NATs do allow sites to switch service providers relatively easily, the IETF IPv6 Working Group is progressing on IPv6 site renumbering which will allow a site to change service providers with relative ease.

Should NATs be deployed in an IPv6 environment, the use of TEREDO transition mechanisms can allow those devices behind the NAT to access the IPv6 public Internet through IPv4/UDP packet tunneling.[20] However, it should be noted that TEREDO has very little scalability and should only be viewed as a last resort transition mechanism.

4.12 Impact to IP Settlement

With initiatives ongoing to address inter-carrier settlement issues (e.g., ordering, billing, and provisioning) in an IP environment, impacts to the network as a result of transitioning to IPv6 can be minimized provided existing standards development efforts for the exchange of necessary IMS or IP-based billing information take this eventual transition into account.

If the IPv6 service is to be commercially available, then procedures and tools will be required to support the ordering, provisioning and billing of those services. Most operators have systems to support these functions today. Therefore, changes are likely to be required to these support systems in order to support the new services and their associated data fields.

[20] TEREDO was developed for the purposes of a NAT device processing native IPv6 or IPv6 tunneled over IPv4 packets.

IPv6 will also allow subscribers of P2P services to communicate directly with each other, whereby user data traffic will bypass the server, except perhaps for management functions such as call setup and teardown. Any billing solution that is based on per-packet or per-byte accounting may have to change to alternate models such as flat monthly rate, per call, per time, and so on.

IPv4 Internet access services today typically provide a single address for a consumer service instance. Additional IP addresses and static IP addresses may result in additional consumer charges. Business Internet services also commonly charge based on the size of the public address space provided. In IPv6, the consumer would typically be provided a group of addresses. The size of the service bundle for Internet access would therefore need to change compared to IPv4.

If mobile IPv6 is supported as a network service, the address of the roaming device is partially static and partially dynamic. Service providers typically implement anti-spoofing controls to prevent unauthorized traffic entering the network. The authentication mechanisms to support valid address allocation for mobile IPv6 services require further study.

4.13 Privacy Issues/Legal Challenges

Network operators will need to support legal obligations -- such as Lawfully Authorized Electronic Surveillance (LAES) -- on the IPv6 network as well as on the IPv4 network. Additionally, the existence of unique identifiers in certain types of IPv6 addresses provide the potential to track network activity. Network operators must therefore be cognizant of any legal requirements to safeguard the privacy of their users. These and other legal and privacy issues are discussed in the paper "Legal Aspects of the New Internet Protocol", edited by Euro6IX with the support of the European Commission.[21]

4.14 Address Allocation Policies

ARIN policy states that within six months of IPv6 allocation, /32 must be announced to the global IPv6 networks.[22] In addition, within five (5) years the service provider must have 200 /48 networks allocated to customers in order to retain its IPv6 allocation. This will become a major challenge to service providers given that upon allocation of IPv6 address space, typically 6-12 months of internal testing is required prior to development of an implementation plan, and actual deployment of IPv6 services may take an additional two to three years.

As outlined by ARIN, an enterprise is to receive a /48 global address from their service provider. Home networks are also to receive a /48 address from their service provider; although ARIN is proposing to amend their assignment guidelines to provide /56.[23] A

[21] < http://www.ipv6tf.org/pdf/ipv6legalaspects.pdf >
[22]< http://www.arin.net/policy/nrpm.html#six52 >
[23]"Policy Proposal 2005-8: Proposal to amend ARIN IPv6 assignment and utilization requirement" now under discussion found at < http://www.arin.net/policy/proposals/2005_8.html >. Define an additional end site assignment size of /56. This /56 assignment should be considered the general case, intended for small office, household, and personal networks, and other small and medium-sized deployments where the number of potential subnets exceeds 1, but is not expected to exceed 256.

/64 can be allocated if only one address is assigned to that link, such as an Asynchronous Transfer Mode (ATM) link.

This essentially means that service providers need to allocate the address per the above guidelines as part of the service offerings. Customers also would be required to allocate their addresses to their links within their site appropriately. If a customer required additional address space, most likely this would have to be received from their service provider based on their business relationship.

4.15 Impact on Infrastructure Reliability

The operation of a network infrastructure supporting both IPv4 and IPv6 is likely to be less reliable than that of a network operating an IPv4 or IPv6 alone. Possible failures include DoS attacks, or software immaturity in one network that propagates to the other through the unavailability of shared nodes or links.

The IPv6 features are largely implemented in software, and the large scale deployment of this software will create challenges in maintaining infrastructure reliability. While prototype and commercial systems are operating successfully, there is a risk of error due to human interaction (i.e., "hands in the plant"), and the size of the software changes. The reliability risks of operationalizing large software changes are not specific to IPv6. Where hardware reliability risks can be readily quantified, the system reliability risks of operationalizing software are harder to quantify. There are no standard industry-accepted mechanisms for this.

4.16 Impact on Traffic & Routing

Transition strategies inherently call for an extended period of operation with both IPv4 and IPv6 protocols – either explicitly supported or indirectly supported by various tunneling mechanisms. While these tunnels are in effect, the network operator now has to manage essentially two different networks with different topologies. Any traffic engineering activities -- e.g., manipulation of routing administrative weights, use of MPLS terminating equipment (TE) tunnels, etc. -- also need to be duplicated to include changes in traffic patterns, since not all peering relationships will transition to supporting IPv6 at the same time.

Routing policies at peering points will need to be developed for IPv6 as well as the existing IPv4. It may be expected that these peering arrangements will have to also act as tunneling/conversion points in the case where operators have chosen anything other than native IPv6 support.

4.17 Impacts to Access Networks

Service providers are currently in the process of upgrading facilities for consumer Internet access from "dial-up" to broadband access with various service speeds (e.g., xDSL). These are typically capital intensive, multiyear investments based on standard architectures (e.g., DSL Forum TR59) that impact millions of consumers. These architectures are based on IPv4 and NAT deployments and typically involve devices with some degree of IPv4 awareness beyond a standard router (e.g., DSLAM, BRAS,

Residential Gateway). For instance, DSL Forum standards currently do not address IPv6 migration in access networks. Premature introduction of IPv6 would introduce additional project risks for current deployment programs and potentially premature obsolescence of newly deployed equipment. This creates significant drivers against IPv6 deployment.

4.18 Partitioned Internet

As presented in Section 2.3 of this report, there continues to be a lot of speculation and debate with respect to the timeframes around which the IPv4 address space will be exhausted. While there is much uncertainty over when IPv4 addresses will be depleted, two things are known: (1) the IPv4 address space is a finite resource and thus will exhaust; and (2) the IPv4 address space will almost certainly be exhausted sometime between 2009 and 2016.

At some point in time before total IPv4 address exhaustion occurs, IPv6 only sites will emerge, resulting in IPv6 only enterprises that cannot access IPv4 services, IPv6 services that cannot access IPv4 only enterprises, and vice-versa.

The only reasonable approach to healing a partitioned Internet is the widespread transitioning of the existing IPv4 Internet to dual-stack capabilities. For some, this transition will start to happen as either a strategic initiative to avoid future loss of connectivity or in hopes of realizing an opportunity in an emerging IPv6 market. For many, this transition will only occur once market drivers are clearly visible, or in reaction to the impending loss of a market or loss of connectivity.

For medium to large organizations, transitioning to dual-stack capabilities is a multi-phase, multi-year endeavor. The degree to which the Internet becomes partitioned will depend on how early or late the global IPv6 transition planning begins relative to the effective exhaustion of IPv4 addresses. Today, solutions such as Network Address Translator-Protocol Translator (NAT-PT) are being developed as stop-gap measures to proactively prepare for this event. However, NAT-PT is viewed as a short-term bridging function between two incompatible Internets (i.e., IPv4-only vs. IPv6-only applications, hosts, clients, and/or servers), and is subjected to inherent limitations and restrictions.

The full effect of a partitioned Internet will not be known, nor a more long-term solution developed, until such time that ISPs start to deploy native IPv6 Internets as a result of IPv4 address depletion, consumer demands and/or strategic business decisions. Only when these types of occurrence start to fully materialize in numbers or frequency can focus be given to developing better approaches, as industry continues its transition from a dominant IPv4 Internet to dual-stack.

5 TRANSITION RECOMMENDATIONS & DEPLOYMENT STRATEGY

While various organizational-specific factors will drive the pace at which networks are transitioned, it is generally accepted that industry's transition to IPv6 is a matter of *when*, not *if*. It is partially for this reason that transition technologies have been specifically designed to enable an evolutionary path reflective of normal life-cycle updates in order

to minimize deployment and operational interdependencies and cost. The replacement of IPv4 only hardware and software to dual-stack (IPv4 and IPv6) offerings, as such, should occur through normal life-cycle updates. Once critical mass of IPv6 enabled replacement technology and training is achieved, native IPv6 should be turned on for routine use.

5.1 Transition Recommendation

Different service providers and (large) enterprises will deploy IPv6 at varying paces and using different strategies. Adding to this complexity is the fact that traversal of IPv6 packets across the NAT may be different depending on the stage and method of transition.

It is recognized that a uniform transition plan will likely never be adopted by industry, as each organization's needs differ. Although this may be the case, for assured end-to-end interoperability during the transitional phase, the ATIS TOPS Council–commissioned IPv6 Task Force highly recommends the general adoption of dual-stack transition approach complemented with tunneling technologies. The IPv6 Task Force also recommends, to the extent possible, a coordinated transitional timeline for the industry's service providers. One possible approach for this coordination may be via the industry's adopted feature-rich IPv6 IMS architecture.

When transitioning to IPv6, three fundamental steps are recommended:

- *Experimentation*: Gain experience with IPv6 and transition mechanism.
- *Production dual-stack dominance*: Transition to one or more core services use IPv6.
- *IPv6 dominant*: Ascertain "critical mass" for switching to native IPv6 and decommission IPv4- only services and devices.

In general, the primary recommendations of the IPv6 Task Force are:

a) *Incremental, dual-stack approach to transitioning should be used*: Transitioning to dual-stack capabilities is a multi-year endeavor that affects just about every aspect of networking and service infrastructures. The recommended approach to transitioning is multiple cycles of planning and deployment that allows experience and capacity to be built up over the various phases. The dual-stack approach to transitioning is the best method of introducing IPv6, preserving the enabling values provided by IPv6 with the least impact to existing IPv4 services.

b) *Early phase planning for a very limited launch should begin now*: It is important that a limited launch phase of deployment be initiated sooner rather than later. This phase provides the data required to plan subsequent deployments. A limited experimental launch can provide input into decisions regarding products, versions, transition mechanism, security strategies, and many aspects of operational requirements that will be used during a production phase of deployment. It also provides the information needed to develop any operational or management tools, and to provide feedback to vendors for required feature development.

c) *Wider spread transitioning should take place during the normal refresh period of software and hardware upgrades*: For most products, enabling IPv6 requires a software or hardware upgrade. The most efficient way to deploy IPv6 is to incorporate it into

a network and service infrastructure during the next upgrade cycle. IPv6 features can then be turned on gradually to meet demand.

d) *At some point, the conditions will be right for new and expanding sites to deploy IPv6 only networks and services*: The degree to which the Internet becomes fragmented will depend on how early or late the global IPv6 transition planning begins relative to the time when IPv6 only sites become common. The service provider community needs to play a leadership role in minimizing the fragmentation and/or partitioning of the Internet. As such, some time before native IPv6 becomes common: (1) The service provider community should promote IPv6, encouraging the wide spread transition to dual-stack capabilities in all aspects of the Internet; and (2) Service Providers should offer production native IPv6 service to all customers.

5.2 Deployment Strategy

5.2.1 Experimentation Phase

With this understanding that performance and scalability will be limited, the proposed experimentation phase offers the opportunity to gain critical exposure and experience in IPv6. It is also an easy, low risk, low cost starting point for the transition process.

Some selective hosts, servers, and possibly routers should be transitioned to dual-stack devices. Experience will be gained using intra-site tunneling mechanisms such as ISATAP, as well as experience in transitioning over servers, host applications, and using network applications (DNS, DHCP). Experience will also be obtained from accessing IPv6 services external to the site using 6to4 tunnels.

5.2.2 Production Dual-stack Dominance

Wide spread usage of IPv6 services will require more server capacity and more native IPv6 forwarding. In this phase, core routers, edge routers, servers, and hosts are transitioned to be dual-stack capable, as IPv6 capable software (and possibly new hardware) releases are deployed. During this phase, pockets of legacy IPv4-only devices and applications are expected to remain.

Throughout this phase of deployment, the existence of NAT devices will not impact early deployments. As deployment progresses towards dual-stack dominant and production networks, IPv6 NAT traversal choices could have some impact on widespread IPv6 service deployment timelines. One of the primary motivators for transitioning to dual-stack is to gain access to IPv6-only capable services. The motivation for developing and deploying IPv6-specific services depends on the anticipated and real availability of devices that can access them. If most sites choose to translate private IPv6 addresses into public IPv6 addresses: (1) the available market for IPv6 only services will be diminished; (2) motivation for developing IPv6 only services will be diminished; and (3) this could decelerate the wide spread transition to IPv6.

To achieve dual-stack dominant and IPv6 dominant phases, two options are possible:

1. *Translate private IPv6 addresses to public IPv6 addresses*:
   - Requires enhanced NAT capability.

- Existing ALGs have to be upgraded to support IPv6.
- New IPv6 capable applications may be optimized or not capable of working across a NAT.
- Devices cannot participate as content provider participants.

2. *Bypass the NAT or NAT routes IPv6 natively*:
   - NAT has to be enhanced to support native IPv6 or deploy a separate router/link to SP for IPv6 traffic.
   - If SP does not support native IPv6, define configured tunnel to IPv6 Internet router or use 6to4.
   - If SP supports native IPv6, route natively.

From an (large) enterprise viewpoint, initially, IPv6 devices behind a NAT may access the public IPv6 Internet using the TEREDO transition mechanism. TEREDO -- developed because most NAT devices today will not process native IPv6 packets or IPv6 tunneled over IPv4 packets -- tunnels IPv6 in IPv4/UDP packets. The IPv6 addresses are not translated when using TEREDO. TEREDO addresses are globally unique and routable. Because of its limited scalability, it is important to note that TEREDO is a "last resort" transition mechanism. For scalability, it is recommended that native IPv6 followed by 6to4 be used.

5.2.3 IPv6 Dominance

At some point in time, the economical and operational savings achieved in switching to a fully native IPv6 core will overcome the need to maintain dual-stack devices and services. Under this phase, IPv6 dominance will occur.

To implement a native IPv6 core, IPv4 applications, interfaces, and dual-stacks on servers, host and routers will be turned off. To maintain interoperability, however, some nodes may need to support IPv4/IPv6 tunneling. Under this scenario, organizations may be required to deploy an IPv6/IPv4 translation protocols to access some legacy IPv4 equipment.

5.3 Transition Options

When transitioning to IPv6, the home, enterprise Internet, enterprise VPN and mobility markets may require different strategies. For this situation, there are four basic transition options that can be considered for service provider transition:

1. *Tunnel Concentrator* -- Deploy one or more tunnel concentrators using one or more tunneling mechanisms: configured tunnels, 6to4, TEREDO, or Tunnel Broker.
2. *Dual-stack Edge* -- Transition edge routers to dual-stack capabilities as required, transported over IPv4, Layer 2, MPLS, or tunnel of choice between the edge routers
3. *Dual-stack Edge and Core* -- Transition edge routers to dual-stack capabilities as required and transition enough core routers to dual-stack to allow native IPv6 forwarding between the edge routers.

4. *IPv6-VPN* -- Transition edge routers to dual-stack VRFs, transport over IPv4 MPLS in the core.

5.3.1 Tunnel Concentrator

A tunnel concentrator allows the end user to tunnel from within the site, over IPv4 or IPv4/UDP, using one of the recommended tunneling mechanisms to a fixed relay point in the service provider network. Refer to *Appendix B*, Figure B.13, for a diagram.

On the core side of the tunnel concentrator, there is a connection to the native IPv6 network. The connection on the core side can be native IPv6 or IPv6 over some tunneling mechanism (IPv4, GRE, L2, MPLS).

Each tunneling mechanism offers different values. A fuller description of the different tunneling mechanism can be found in *Appendix A: Transition Strategies*.

Tunnel concentrator deployments can be valuable, as an initial IPv6 offering where access requirements are sparse, or where IPv6 access is required before a particular edge (PE) router has been transitioned to dual-stack. However, many of the tunneling mechanisms do not support multicasting.

A device within the customer premise must be capable of initiating the tunnel. This device is the logical IPv6 customer edge (CE) device for the site.

5.3.2 Dual-stack Edge

In a dual-stack edge deployment, edge routers are transitioned to dual-stack capabilities as required. The core routers, for the most part remain IPv4 only. The edge routers are inter-connected over a mesh of tunnels. The service provider can choose their tunnel of choice to provide the required service and performance. Some core routers may be transitioned to dual-stack to reduce meshing requirements. Refer to *Appendix B*, Figure B.14, for a diagram.

A dual-stack edge deployment allows the service provider to offer native IPv6 service to customers without impacting the core of the network. Multicasting is also supported with this solution.

CE devices route native IPv6 to the dual-stack edge device. The connection to the CE can be over a physical link or any L2 or L3 tunnel. Most implementations support both IPv4 and IPv6 on the same link.

5.3.3 Dual-stack Edge and Core

In a dual-stack edge and core deployment, edge routers are transitioned to dual-stack capabilities as required. The core routers are also transitioned to dual-stack as required to connect transitioned edge routers. Refer to *Appendix B*, Figure B.15, for a diagram.

Transitioning the core routers to dual-stack may provide improved performance and scalability over a dual-stack edge only configuration for multicast traffic.

CE devices route native IPv6 to the dual-stack edge device. The connection to the CE can be over a physical link or any L2 or L3 tunnel.

5.3.4 IPv6-VPN

A 6PE RFC 4364 based solution involves turning on one or more IPv6 VRFs on the edge devices. Packets are transported over IPv4/MPLS across the core of the network. For general Internet access, one VRF can be used to aggregate many customer connections. For enterprise L3 VPN service, an IPv6 VRF or dual-stack VRF can be turned on for each customer connection. Refer to *Appendix B*, Figure B.16, for a diagram.

This solution may be the most viable for a native IPv6 service offering on RFC 4364 capable networks. There is no impact on the core of the network, and performance and operational considerations for this solution may be favorable over other strategies. Solutions for Multicast MPLS native support have been developed in the IETF MPLS Working Group, which are available now: *draft-ietf-mpls-rsvp-te-p2mp-03.txt* and *draft-ietf-mpls-ldp-p2mp-00.txt*

CE devices connect to the VRF using IPv6. The connection can be over a physical link or any L2 or L3 tunnel. If a dual-stack VRF is used for connectivity to the CE, a single link to the CE can be used. Any other configuration would require a separate link for IPv4 and IPv6 from the CE.

5.3.5 Wireless Transition Options

The transition strategy provided in this report outlines the options for a GSM network (based on specifications developed by the 3GPP) to transition to support dual-stack and IPv6 only mobile subscribers and services. Transitioning from a mobile IPv4 solution is not considered. Figures illustrating this strategy are provided in *Appendix B*.

Starting with a view where all network elements and mobile terminals are IPv4 only, as illustrated in *Appendix B*, Figure B.17, deployment of IMS will be one of the first IPv6 services offered that will drive mobile terminals to be dual-stack and the Gateway GPRS Support Node (GGSN) transitioned to support IPv6 Application Points (AP) and dual-stack Gi interfaces. This will allow the GGSN to tunnel IPv6/IPv4 to the IMS. The tunneling mechanism can be dynamic, configured, or 6PE. Packets between the mobile terminal and the GGSN are native IPv6 over the standard GSM tunneling protocols. The Serving GPRS Support Node (SGSN) can remain IPv4, as it is only providing a transport tunnel to the GGSN. Refer to Figure B.18, for an illustration.

In circumstances where a dual-stack subscriber is to connect to IPv6 Internet services and the immediate upstream service provider does not offer native IPv6 service, a device within the operator's network has to establish a tunnel to a tunnel concentrator somewhere in the Internet. One option is to have the GGSN provide this tunneling service, as illustrated in Figure B.19. Another option is to transition an edge router to dual-stack capabilities, as shown in Figure B.20. The GGSN would tunnel to the edge router and the edge router would tunnel to the tunnel concentrator.

Should the core routers in the operator's network be transitioned to dual-stack, IPv6 packets can be forwarded natively from the mobile terminal through to any service within the operator's network, as shown in Figure B.21. Due to the rapid growth in the mobility market and the scarcity of IPv4 addresses, it is probable that mobile terminals will be one of the first network elements deployed as IPv6 only. Before this event occurs, it is recommended that operators support dual-stack GGSNs, and all internal services be transitioned to dual-stack. Otherwise roaming support for IPv6 only terminals will be inconsistent. Figure B.22 illustrates this option.

Where service exists that cannot be transitioned to dual-stack, it is recommended that an application proxy (HTTP, TCP) be used to provide the conversion, as illustrated in Figure B.23. Due to security and other reasons, the use of NAT-PT is no longer recommended by the IETF.

IPv6 Mobility is a complementary service that can be added to the services offered by a GPRS/CDMA operator. It does not replace the GGSN or any other element; rather, it enhances the connectivity options while the mobile subscriber is outside of its home region. The home agent can be co-located with the GGSN or separate as illustrated in Figure B.24.

5.4 Security Measures

5.4.1 Personnel Training

With the continued proliferation of dual-stack IPv6-capable software and devices, personnel must be trained to properly configure and manage these offerings, as abuse by attackers can occur. Accordingly, training of personnel should begin now, if it is not already underway.

5.4.2 Native IPv6

IPv6, together with a firewall, can provide all of the real and perceived benefits of a NAT and previous IPv4 supported security applications. IPv6 features, and the inherent capabilities of IPv6, provide the same or better security as provided by a NAT alone. When considering site security, three types of addresses and communication need to be considered:

1. Addresses that are only used for intra-site communication.
2. Addresses that are used to initiate sessions to services outside of the site.
3. Addresses that are used to provide service to users and devices outside of the site.

Unique Local Addresses (previously site local) should be used for all intra-site communication. These addresses are private addresses and by definition can not be advertised or forwarded in or out of the site. Packets from outside the site cannot be forwarded to these unique local addresses. This provides the same protection as private addresses in IPv4 behind a NAT for which there is no mapping.

5.4.3 Enterprise

In the enterprise environment, running 6to4 configured tunnels is the recommended secure practice for external transition methods.

When automatic tunneling is used, strong ingress filtering and route policies on both IPv6 and IPv4 environments and products need to execute proper security and process checks -- i.e., checking that the IPv4 and IPv6 addresses are conversion-matched.

5.4.4 Security Recommendation

Some of the recommendations outlined in this section will assist in enhancing a secure network. However, a more comprehensive and thorough study along with detailed recommended actions to mitigate network vulnerabilities and threats is highly recommended. More precisely, although it is anticipated that security holes are likely to be found in IPv6 as it continues to be deployed, efforts should be undertaken now to identify and resolve these security gaps before, versus after, a malicious attack occurs.

5.5 Enable Globally Unique IP Address

There are currently two modes of assigning addresses: *private* and *public*. The IP address space assigned by ARIN to any organization must be reachable and visible. In an MPLS network, the CE router acts as a gateway between the ISPs' public MPLS network and the customers' private network. Figure 5-1 shows a CE setup consisting of the customer network, the ISP MPLS network, and the Network Management LAN (NML).

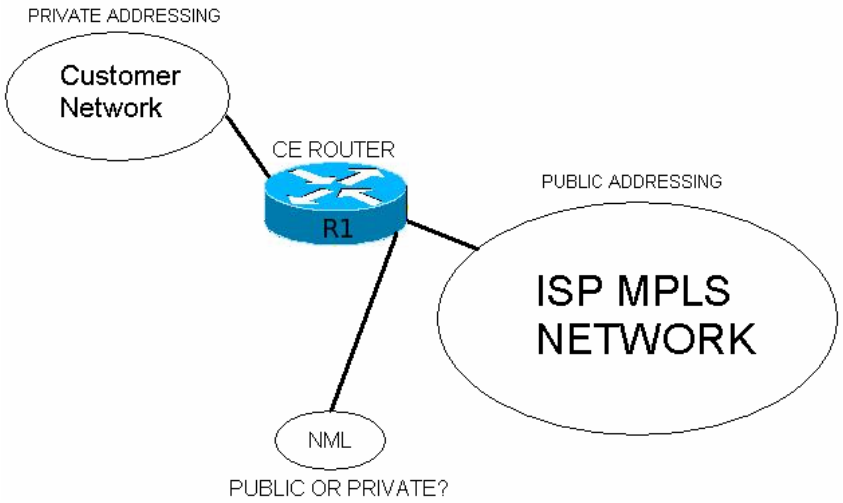


Figure 5-1: CE Management

The NML is a separate carrier-provided network that is responsible for managing IP VPN services as well as for provider maintenance of CE routers. Since this is a management LAN, public and customer traffic should not be able to traverse through the NML. As a result, NML's specific requirements require a network address allocation that is separate from both the customer's and carrier's MPLS network. This is difficult to accommodate under current ARIN guidelines, due to the unavailability of a proper IP address allocation.

Although the customer network uses a private address space and the ISP MPLS core is using public address space, it is not clear what address space will be used for the NML. Currently different organizations are using registered public IP addresses from their own allocations to compensate. However, this method does not promote the efficient use of the IP addresses and potentially conflicts with the ARIN IP guidelines. As a result, an industry solution needs to be established to correct this issue as soon as possible.

To meet the NML requirements for managed MPLS-based IP VPN services, it is recommended that ARIN reserve IPv6 address blocks specifically for routing within and among private networks for applications like network management. For service provider management of CEs, it is further recommended that these address blocks be globally unique in order to ensure that conflicts arising from IP Address allocations for NMLs are avoided, as service provider consolidation (industry trend) occurs.

Until these addresses are assigned by ARIN, or in case the assignments do not happen, use of Unique Local IPv6 Unicast Addresses (RFC 4193) are recommended. RFC 4193 defines the generation of a prefix for use inside a network. The addresses generated are not designed to be routed in the global routing table. While not truly unique, the algorithm used to generate the network portion of this address block creates an address that is very highly likely to be unique with regards to any other given network. The calculated probability of collision with any other given network is $1.81*10^{-12}$.

5.6 Timeline

As enumerated within this report, the rate at which an organization (e.g., service provider and/or enterprise) transitions to supporting a fully dual-stack or native IPv6 infrastructure will be driven primarily by market demands. Each organization should carefully assess the costs associated with the transition to IPv6, and justify the timing for it. Therefore, setting a timeline under which an existing network should transition or when a native IPv6 network should be deployed is not practical. However, also outlined in this report are key market drivers and adopted timelines that should influence an organization's transition timelines, in efforts to avoid future loss of connectivity or opportunities. Examples of these drivers include:

a) U.S. government's deadline of June 2008 as the date by which all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must interface with this infrastructure.
b) Industry's adoption and deployment of IMS based on IPv6 to deliver true peer-to-peer converged voice, data, and multimedia services, as well as IPv6 mobility (when IPv4 no longer provides support for such applications).
c) The rate at which new specialized networking applications, such as using remote sensors and controllers (see section 2.2.2.1), are adopted at a wide scale.
d) IPv4 address exhaustion timeframes which, based on published reports (see section 2.3), predicts the possibility that ARIN and RIR assigned IPv4 addresses will be exhausted as early as 2009.

e) Most network hardware, operating systems, and network-enabled software packages will likely include IPv6 capabilities within the next five years.

In preparations for transitioning an existing infrastructure to IPv6 to support these drivers, and to meet these timelines, the following events should start as soon as possible (in no particular order):

- Train operators and designers (personnel) for IPv4 to IPv6 knowledge and interworking skills.
- Finalize internal planning and lab trials and offer a limited launch of IPv6 to gain experience. A limited launch could consist of offering a tunnel or initiating trial peering.
- Acquire /32 addresses from ARIN.
- Inventory every aspect of an existing IPv4 operating system to include routers, applications, servers and hosts.
- Inventory IPv6 compatible equipment and inventory deployed dual-stack equipment to include routers, applications, servers, and host.
- Assess current inventory of IPv4 addresses and determine a timeframe for address exhaustion.
- Provide feedback to vendors on ascertaining requirements.

5.7 Next Steps & Follow-on Actions

Based on industry's current state of affairs with respect to transitioning to IPv6 and the numerous deployment challenges noted in Section 4 of this report, follow-on initiatives towards resolving these challenges need to be undertaken to ensure interoperability. Thus, further study by ATIS or its committees is necessary to identify specific actions and timelines in support of this objective. External organizations noted in this report (as well as potential other organizations), should also be made of aware of this report's findings and conclusion as they continue their work-programs to develop industry specifications in support of IPv6.

APPENDIX A: TRANSITION STRATEGIES

A.1 Dual-stack

A *dual stack* network element supports both IPv4 and IPv6 protocol stacks. These stacks are completely independent. Applications can choose to use one or the other depending on the session requirements. A dual stack network implies that most network elements support both stacks. This allows the creation of an independent IPv4 network and an independent IPv6 network.

A.2 IPv6 Tunneling

RFC 2893 defines two types of tunnels: *configured tunnels* and *automatic tunnels*.

A.2.1 Configured tunnels

Configured tunnels are those in which the endpoints are manually configured. The IPv4 addresses of tunnel endpoints are not derived from IPv6 SA or DA or the next hop prefix route. These are most often used for router to router tunnels.

A.2.2 Automatic tunnels

Automatic tunnels are those that do not require manual configuration. Tunnel endpoints are determined by the use of logical interfaces, routes, IPv6 SA or DA. Examples of automatic tunnels are 6to4, ISATAP, and TEREDO.

A.2.2.1 Tunnel Setup Protocol (TSP) and Tunnel Broker

Another automatic tunneling approach is a *tunnel broker-based TSP*. In the simple model a single network device sits on the IPv4 network and the IPv6 network and acts as both the tunnel broker and tunnel gateway. A dual-stack TSP client "sets-up" an IPv6 tunnel to the tunnel broker over the IPv4 network. The client then uses that tunnel for all IPv6 communications. TSP clients can run on single user devices (i.e., Windows PCs) or devices that could act as gateways to a sub-network of users (i.e., Unix, Linux). The broker could be configured to allow all users, or provide RADIUS-based authentication.

A.2.2.2 6to4

6to4 is an address assignment and router to router automatic tunneling technology that is used to provide unicast IPv6 connectivity between IPv6 sites and hosts across the IPv4 Internet. (Ex. Global prefix 2002:WWXX:YYZZ::/48) 6to4 is described in RFC 3056 and defines the following terms:

6to4 host
Any IPv6 host that is configured with at least one 6to4 address (a global address w/ the 2002::/16 prefix). 6to4 hosts do not require any manual configuration and create 6to4 addresses using standard address auto-configuration mechanisms.

6to4 router
A router that supports the use of a 6to4 tunnel interface and is typically used to forward 6to4 addressed traffic between the 6to4 hosts within a site and other

6to4 routers or 6to4 relay routers on an IPv4 network. 6to4 routers require additional processing logic for proper encapsulation services and might require additional manual configuration.

6to4 relay router
An IPv6/IPv4 router that forwards 6to4 addressed traffic between 6to4 routers on the IPv4 Internet and hosts on the IPv6 Internet.

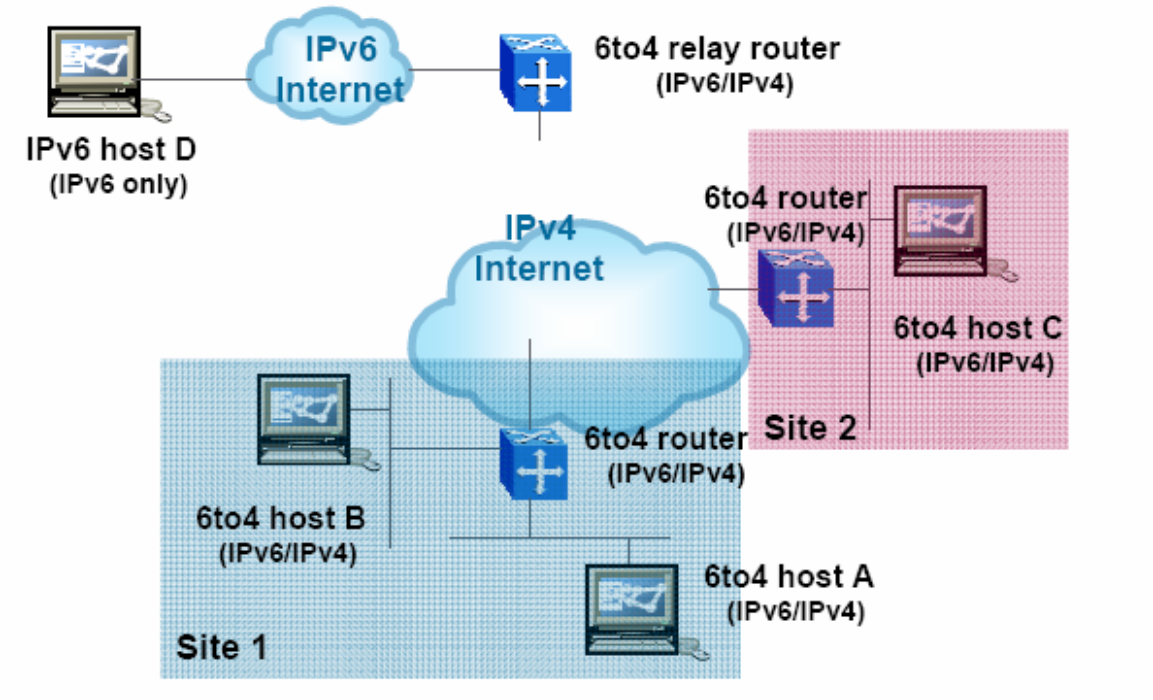


Figure A.1: 6to4 System Components

A.2.2.3 ISATAP: Intra Site Automatic Tunnel Addressing Protocol

ISATAP provides IPv6 connectivity to hosts and routers within IPv4 sites. It allows incremental deployment of IPv6 by treating the site's IPv4 infrastructure as a link layer for IPv6 and by treating an IPv4 infrastructure as a single link. ISATAP enables the usage of IPv6 without the requirement of IPv6 routers and offers an effective host-to-host and host-to-router tunneling method. It can work in conjunction with 6to4 and configured tunnels to provide routed connectivity. When working in conjunction with 6to4, ISATAP works as a host-to-router/router-to-host tunneling method.

ISATAP addresses
Standard IPv6 Prefix + 16 bits (0) + 16 bits (5EFE) + 32 bits (IPv4 address)
[*64-bit prefix*]:0:5EFE:*w.x.y.z*

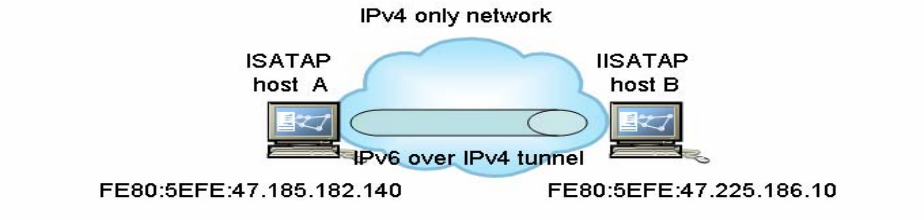


Figure A.2: ISATAP IPv4 Only Network

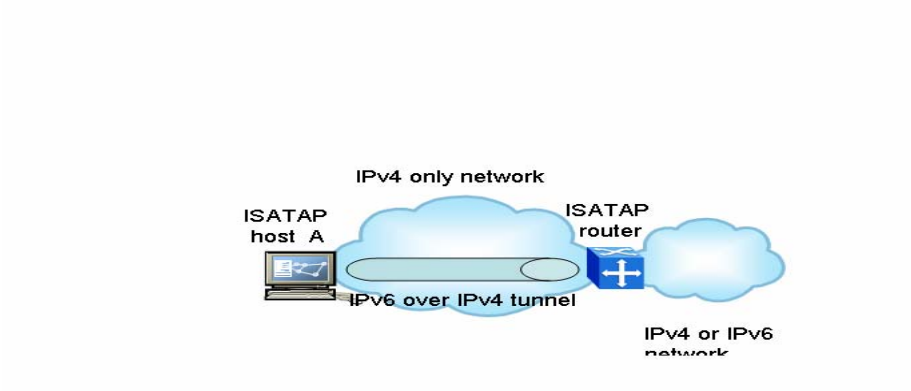


Figure A.3: ISATAP Router

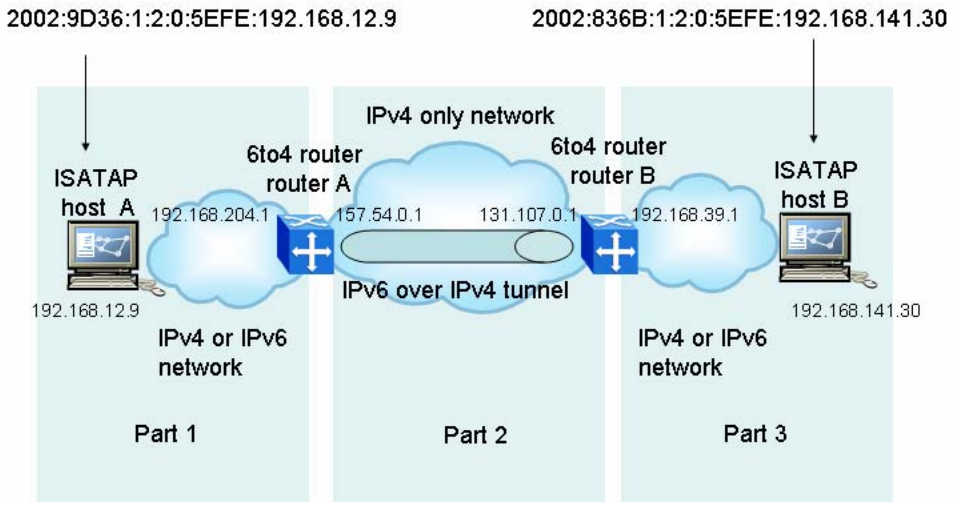


Figure A.4: ISATAP Addresses 6to4 Router

A.2.2.4 TEREDO

TEREDO is in draft experimental status as an automatic tunneling method. An address assignment and host-to-host automatic tunneling technology, TEREDO provides unicast IPv6 connectivity when IPv6/IPv4 hosts are located behind one or multiple IPv4 NATs by sending tunneled packets as IPv4 UDP messages. Communication is facilitated by TEREDO servers and TEREDO relays.

A TEREDO host-specific relay in an IPv6/IPv4 does not use TEREDO addresses, but can communicate with TEREDO clients without having to use a TEREDO relay in the communication path. TEREDO is intended as a transition method, and it is expected that the use of TEREDO will decrease over time as IPv4 NATs begin to disappear.

TEREDO System Components

TEREDO client
A TEREDO client is an IPv6/IPv4 node that supports a TEREDO tunneling interface through which packets are tunneled to either other TEREDO clients or nodes on the IPv6 Internet (via a TEREDO relay).

TEREDO server
A TEREDO server is an IPv6/IPv4 node that is connected to both the IPv4 Internet and the IPv6 Internet and supports a TEREDO tunneling interface over which packets are received.

TEREDO relay
A TEREDO relay is an IPv6/IPv4 router that can forward packets between TEREDO clients on the IPv4 Internet (using a TEREDO tunneling interface) and IPv6-only hosts.

TEREDO host-specific relay
Communication between TEREDO clients and IPv6 hosts that are configured with a global address must go through a TEREDO relay. This is required for IPv6-only hosts connected to the IPv6 Internet.

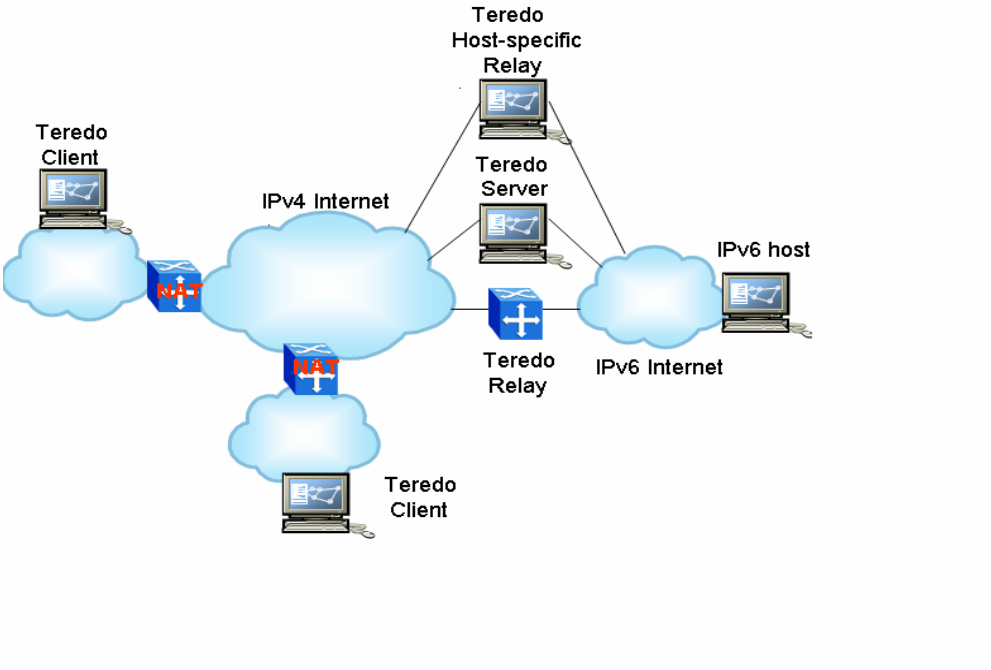


Figure A.5: TEREDO Configuration

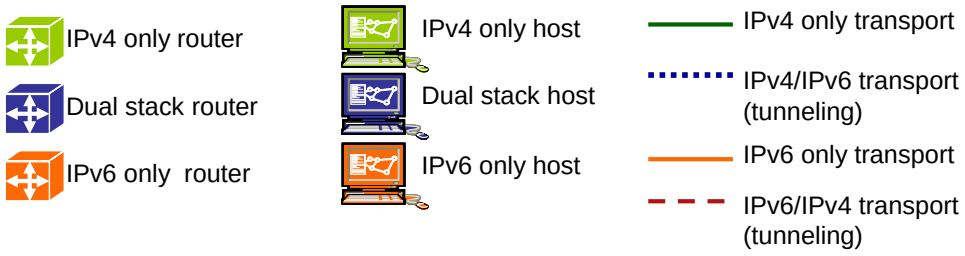
TEREDO Addresses

TEREDO addresses are used as a tunneling method to traverse cone and restricted IPv4 NAT boundaries. (Prefix 3FFE:831F::/32 (not yet IANA assigned). Address contains colon hexadecimal representations of TEREDO servers as well as obscured (XORed) external addresses. Addresses have interoperability with native IPv6, 6to4 ,and ISATAP as if either method is present, host will not use TEREDO.

Teredo Prefix	Teredo Server IPv4 address	Flags	Obscured External Port	Obscured External Address
32 bits	32 bits	16 bits	16 bits	32 bits

APPENDIX B: DUAL-STACK TRANSITION TO NATIVE IPV6

B.1 Enterprise Transition Perspective



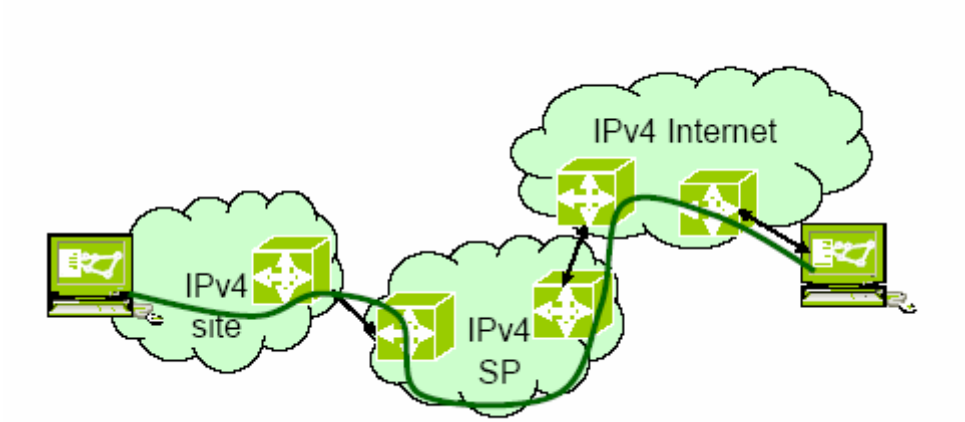


Figure B.1: IPv4 Only Connection

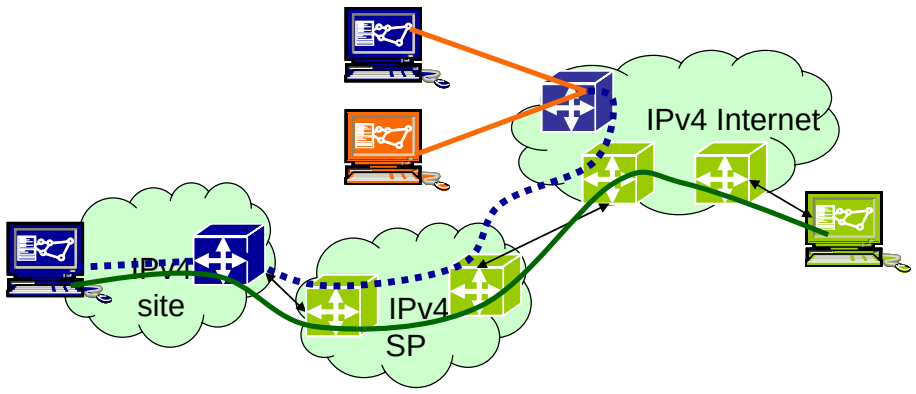


Figure B.2: Dual-stack Host Connectivity: Sparse IPv6 Internet

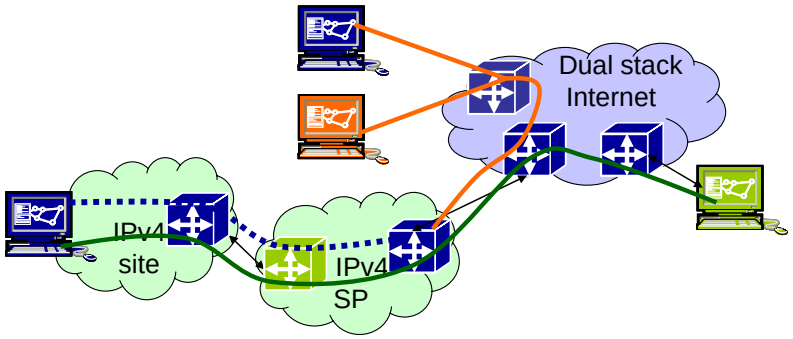


Figure B.3: Dual-stack Host Connectivity: Dual-stack Internet

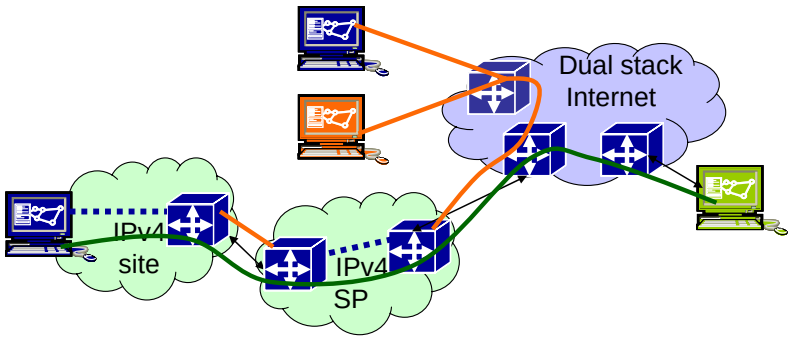


Figure B.4: Dual-stack Host Connectivity: SP Tunneling

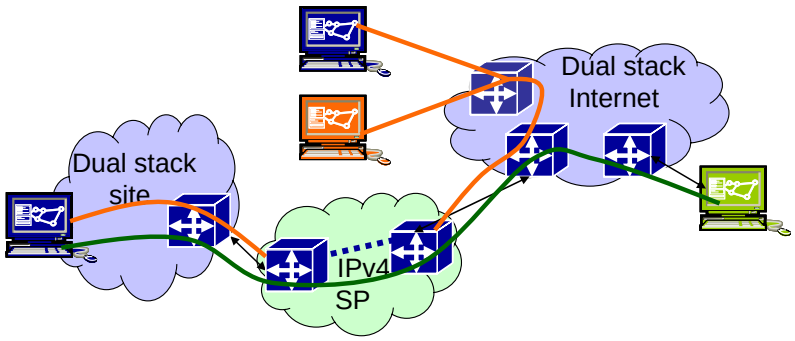


Figure B.5: Dual-stack Host Connectivity: Dual-stack Site

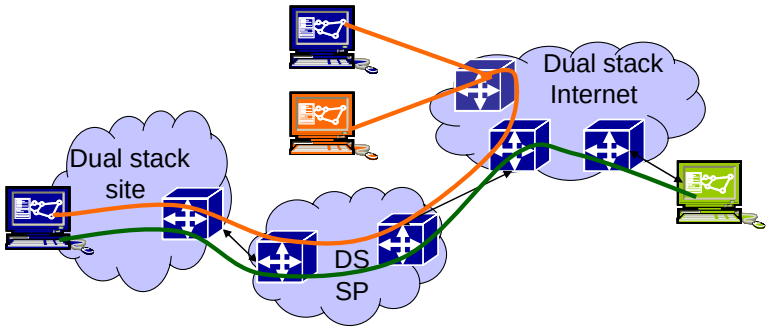


Figure B.6: Dual-stack Host Connectivity: Dual-stack SP

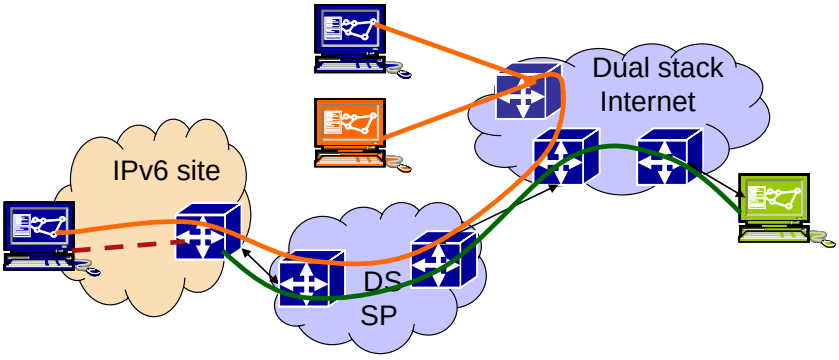


Figure B.7: Dual-stack Host Connectivity: IPv6 Dominate Site

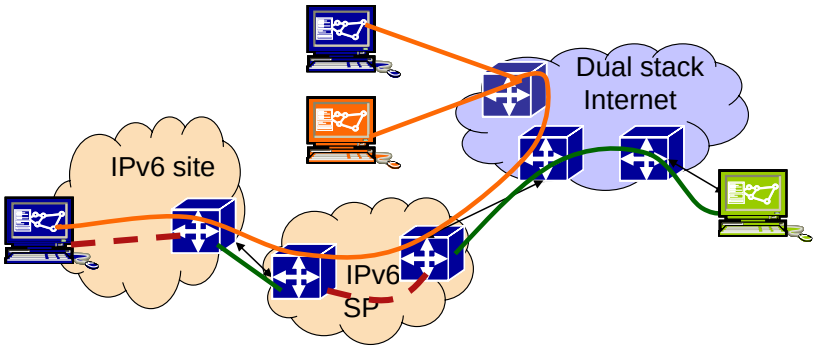


Figure B.8: Dual-stack Host Connectivity: IPv6 Dominate SP

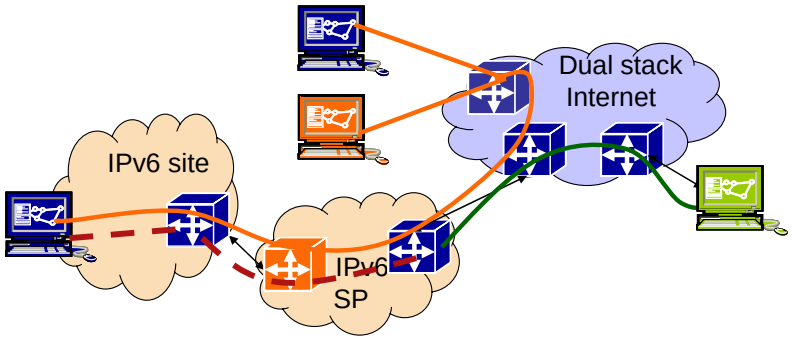


Figure B.9: Dual-stack Host Connectivity: SP Transitioning to IPv6 Only

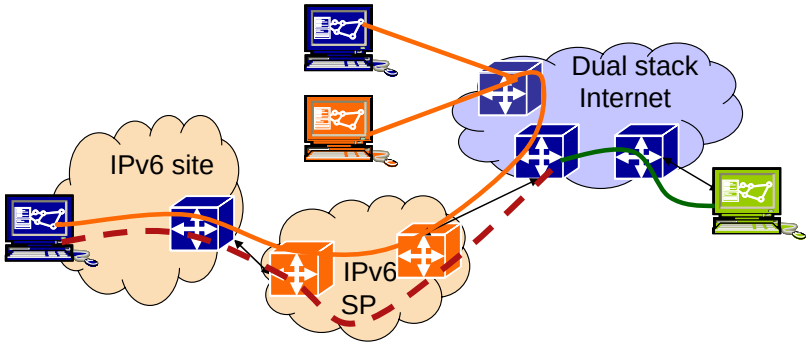


Figure B.10: Dual-stack Host Connectivity; IPv6 Only SP

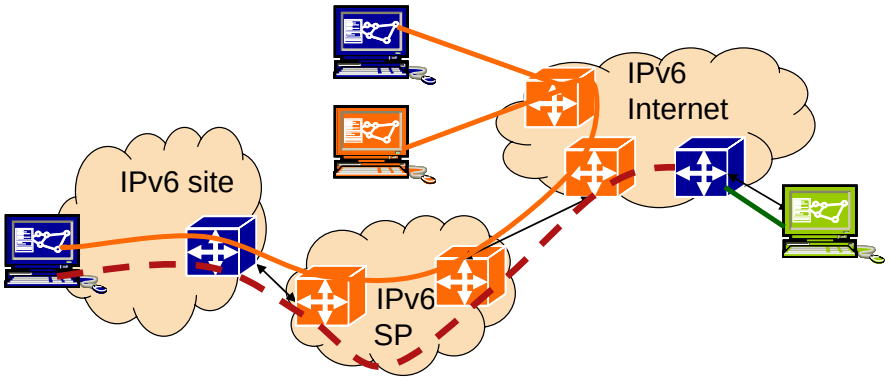


Figure B.11: Dual-stack Host Connectivity; IPv6 Dominate Internet

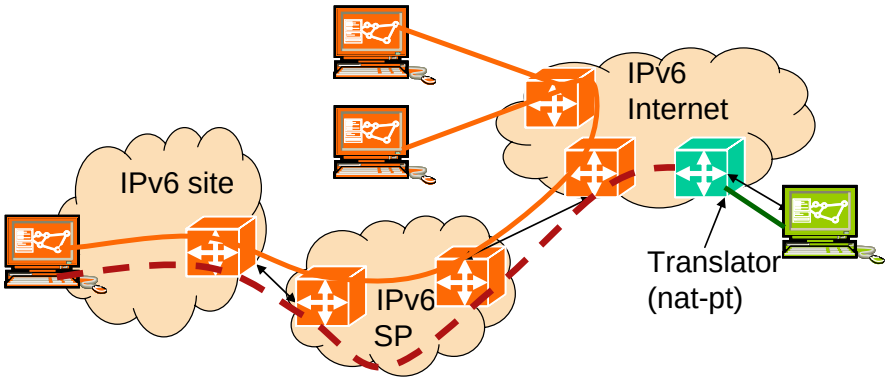


Figure B.12: Only Legacy IPv4 Equipment Remains

B.2 Service Provider Transition Perspective

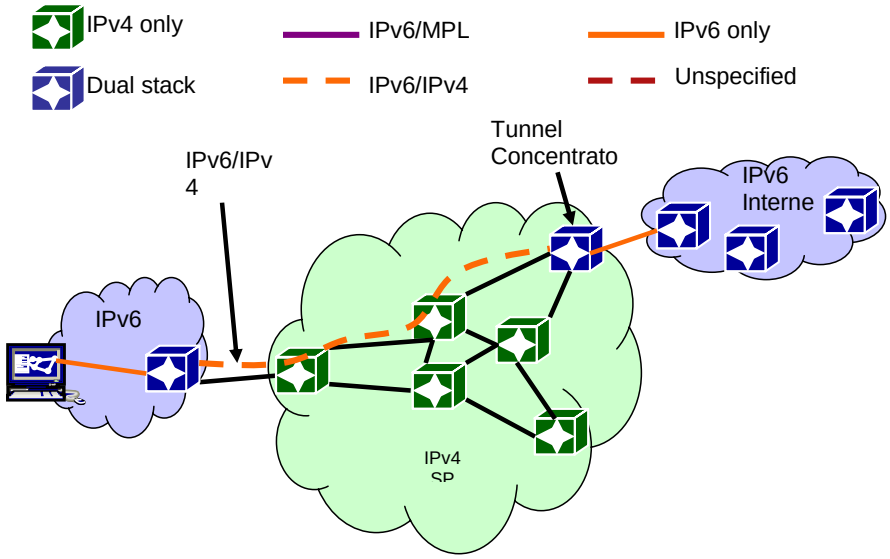


Figure B. 13: Tunnel Concentrator

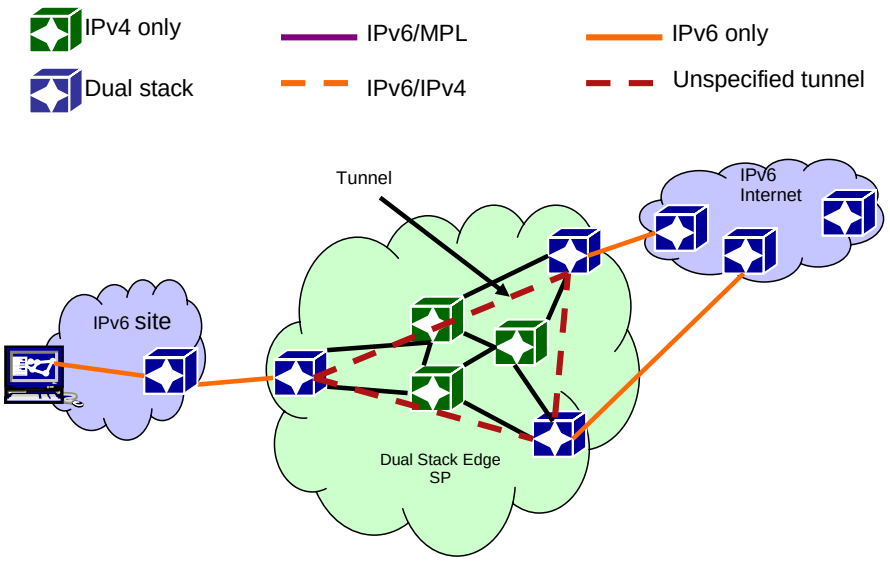


Figure B.14: Dual-stack Edge

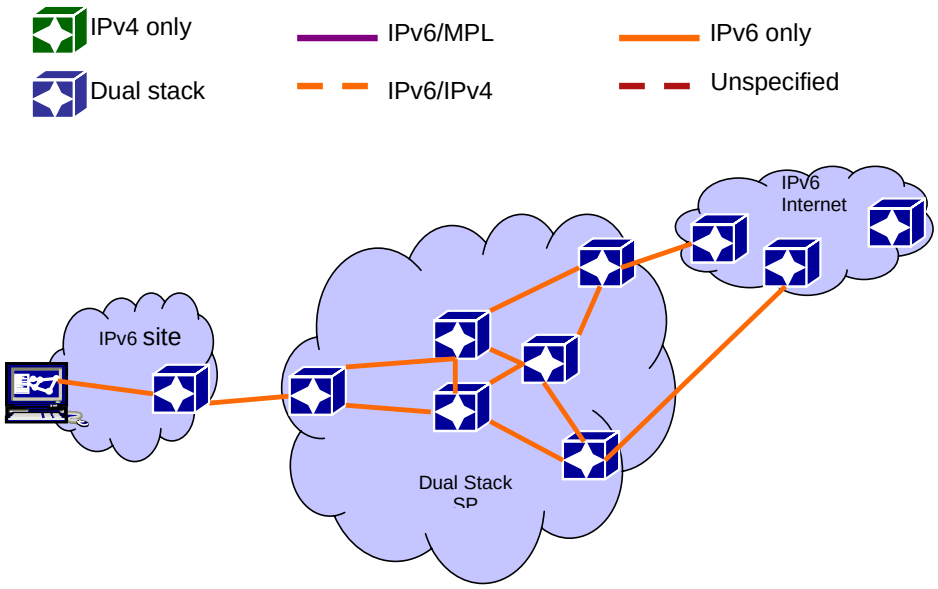


Figure B.15: Dual-stack Edge & Core

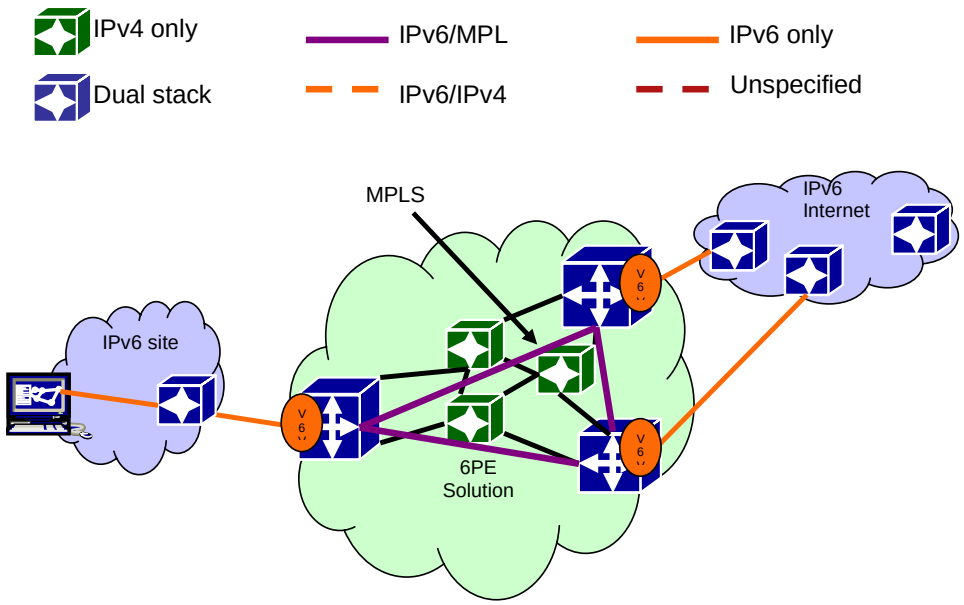
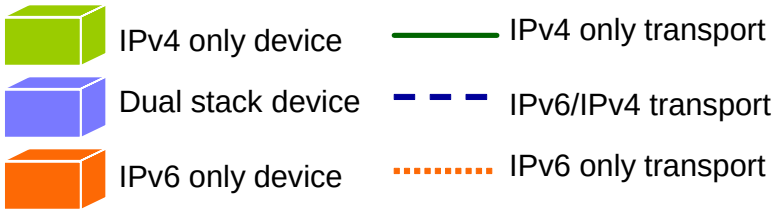


Figure B.16: 6PE Deployment

B.3 Wireless/Mobile Transition Perspective



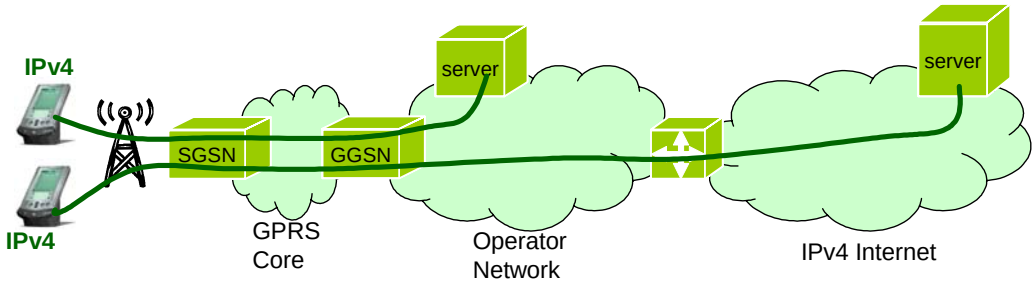


Figure B.17: IPv4 Only Mobile Network

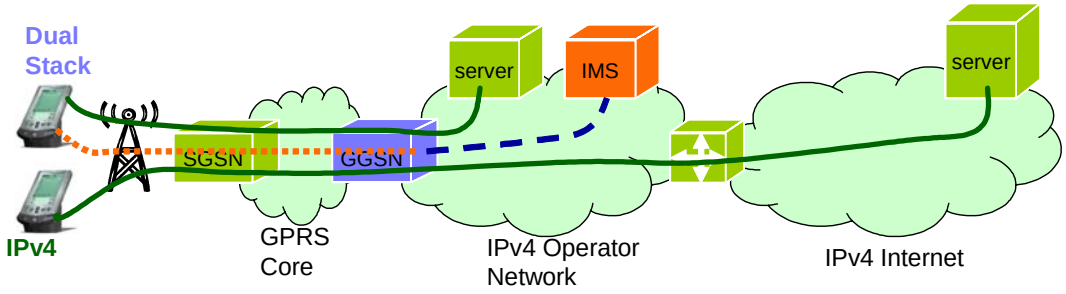


Figure B.18: Dual-stack Network (IMS)

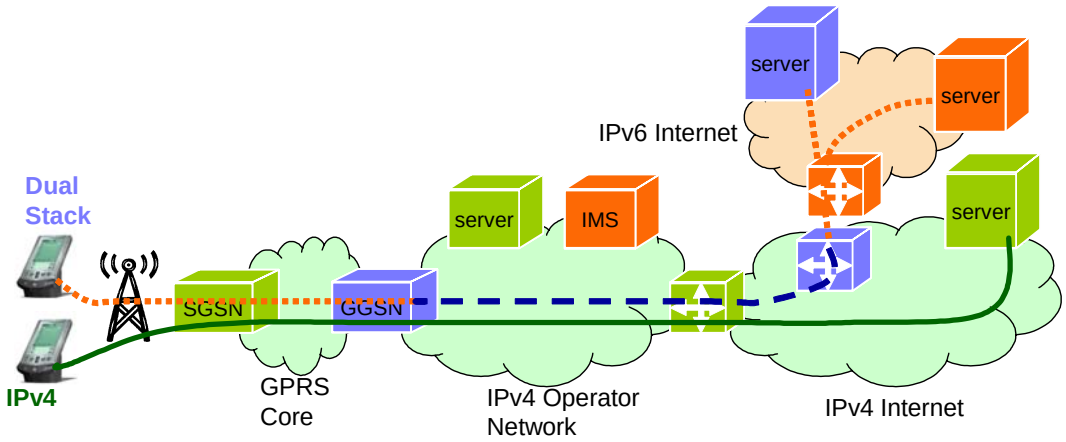


Figure B.19: Dual-stack Device Tunnel to Native IPv6 Application

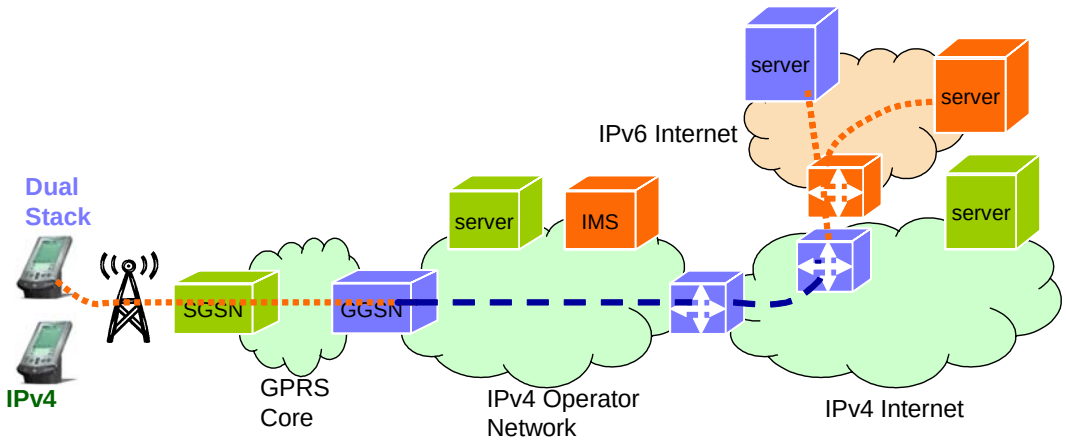


Figure B.20: Edge Router Dual-stack Enabled

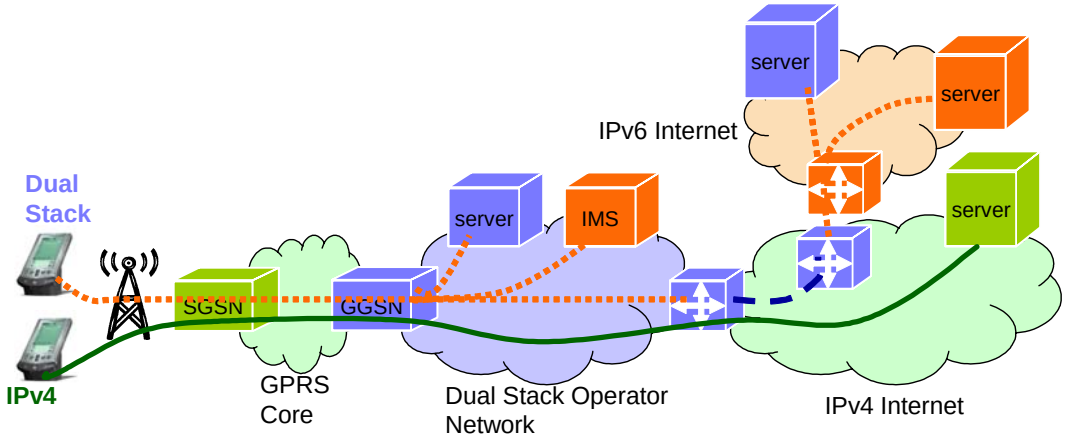


Figure B.21: Network Core Router Dual-stack Enabled

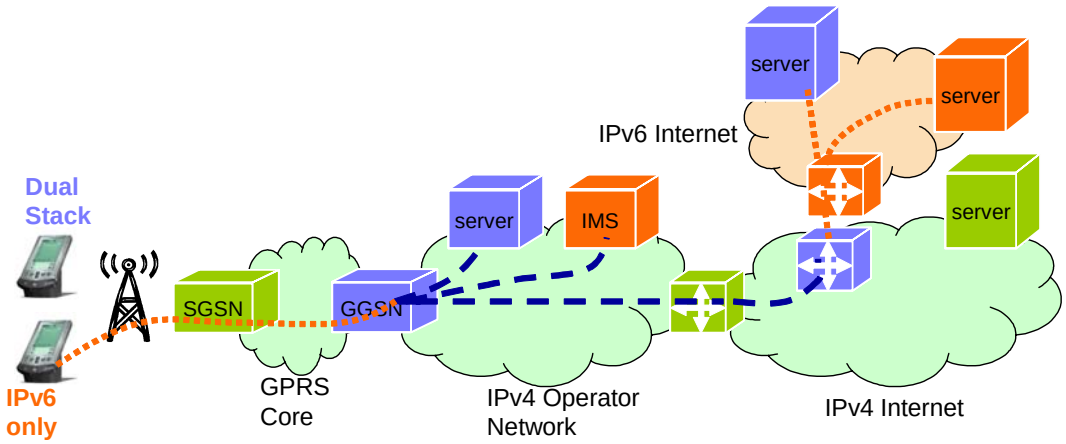


Figure B.22: Dual-stack GGSN for IPv6 Only Devices

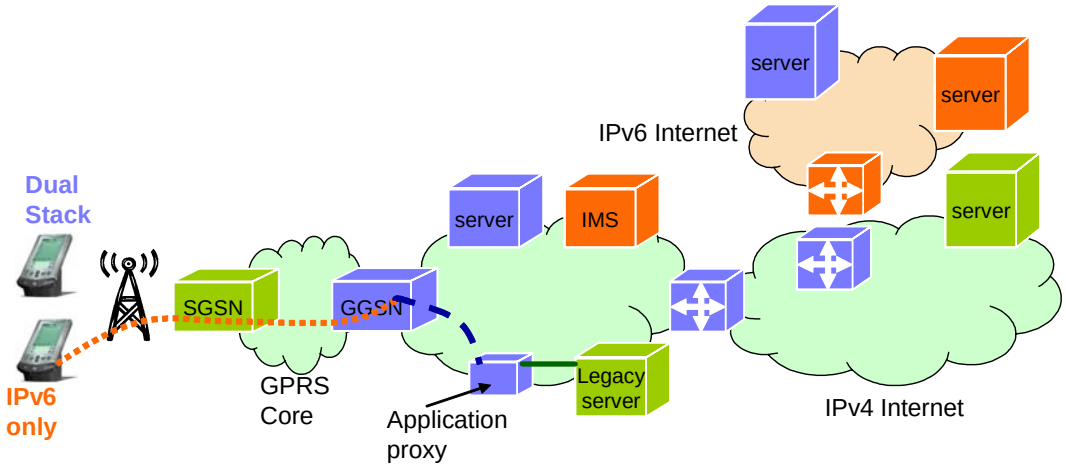


Figure B.23: Application Proxy Translation

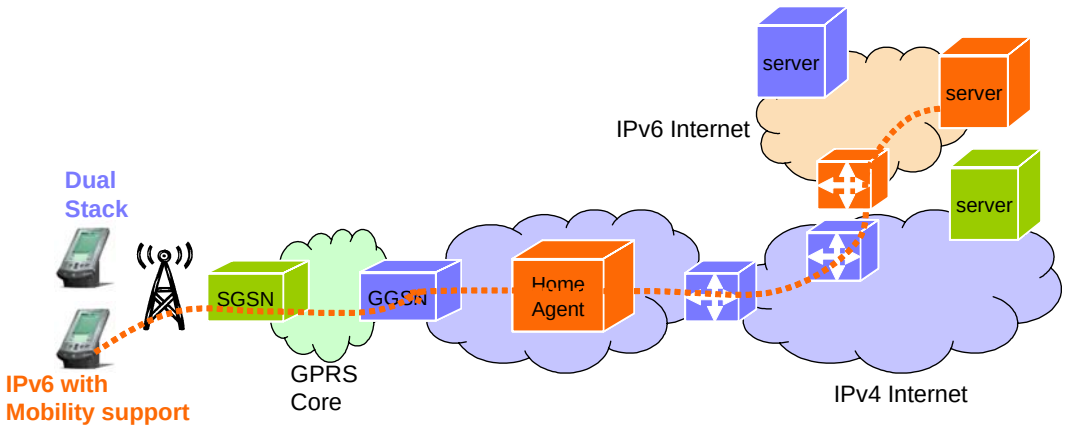


Figure B.24: IPv6 with Mobility Support

APPENDIX C: IPV6 MOBILITY

C.1 IPv6 Mobility: Concept

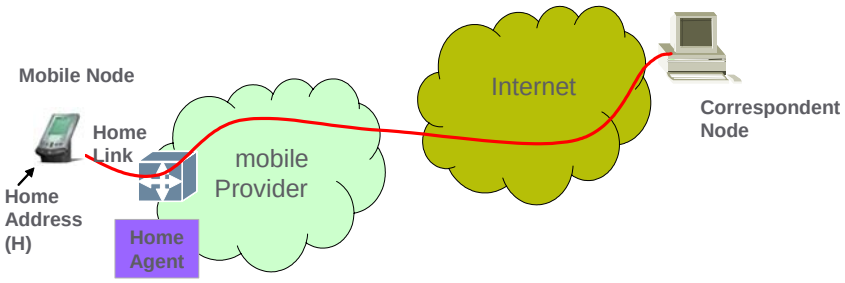


Figure C.1: IPv6 Mobility Concept

- *Home Address*: A unicast routable address assigned to a mobile node used as the permanent address of the MN. This address is within the mobile node's home link.
- *Home Link*: The link on which the mobile node's home subnet prefix is defined.
- *Mobile Node*: A node that can change it point of attachment from one link to another while still being reachable via its home address.
- *Correspondent Node (CN)*: A peer node with which a MN is communicating. The CN may be mobile or stationary.

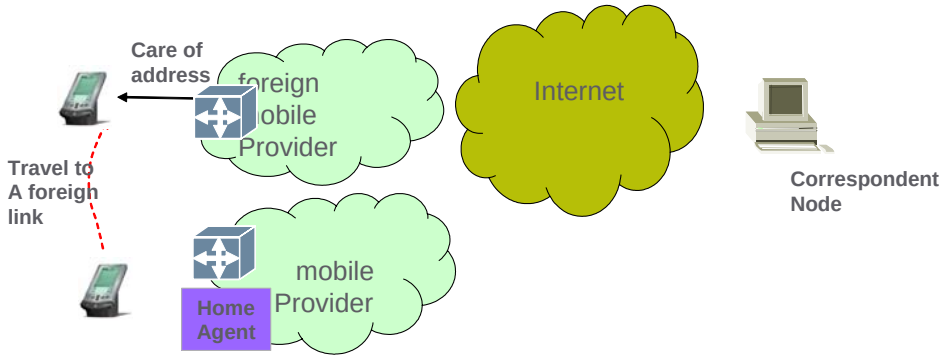


Figure C.2: IPv6 Mobility: Care of Address

- *Foreign Link*: A link other than the mobile nodes home link.
- *Care of Address*: A unicast address associated with a Mobile Node (MN) while it is visiting a foreign link. The subnet prefix of this IP address is a foreign subnet prefix.
- The care of address can be assigned using standard neighbor discovery and auto-configuration mechanisms.

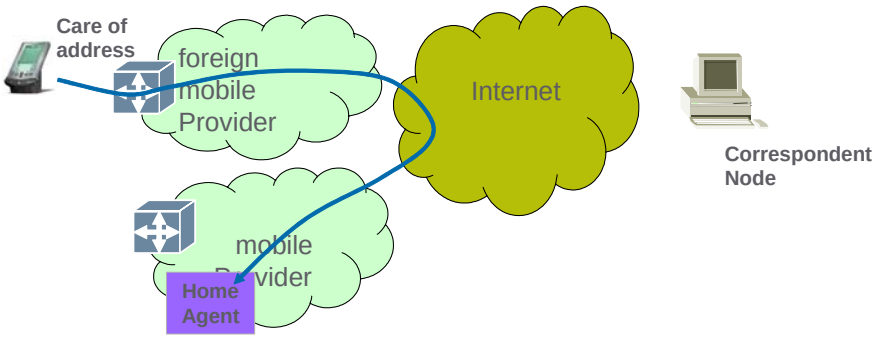


Figure C.3: IPv6 Mobility: Home Agent Router

- *Home Agent:* A router on a mobile node's home link with which the MN has registered its current care of address.
- *Binding*: The association of the home address of a mobile node with a care of address for that MN.
- *Registration*: The process during which a MN sends a binding update to its home agent.
- IPsec must be used in binding updates to the home agent. MN and HA must support and should use the ESP header.

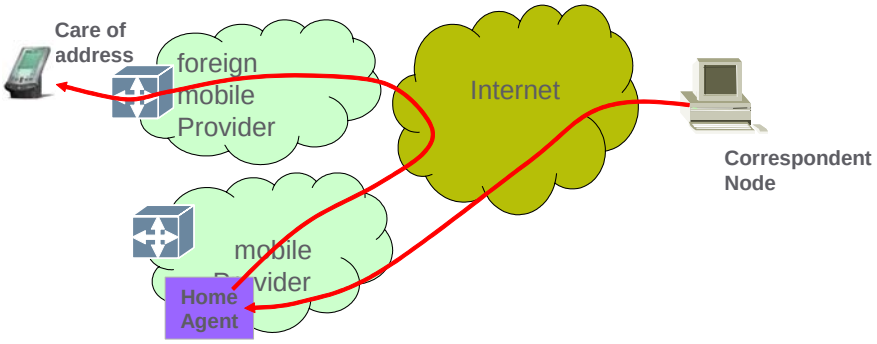


Figure C.4: IPv6 Mobility: CN to MN Using Care of Addressing

- While the MN is away from home, the HA intercepts packets on the home link destined to the MN's home address, encapsulates them and tunnels them to the MN's care of address.
- These packets are tunneled to the care of address associated with the MN.

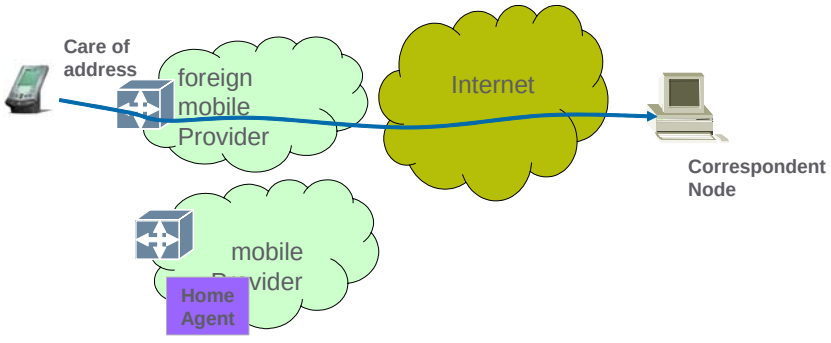


Figure C.5: IPv6 Mobility: Binding Updates

- The mobile node also sends a binding update to the correspondent node, registering its care of address with the CN.
- This requires that the CN, even if stationary, supports mobile IPv6 correspondent node functionality.

C.2 IPv6 Mobility: Bind Update Security

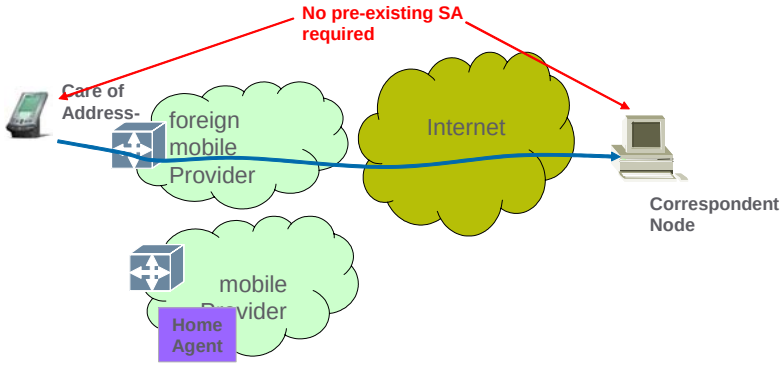


Figure C.6: IPv6 Mobility: Bind Update Security

- Protection of binding updates to correspondent nodes does not required the configuration of security associations between the MN and CN.
- Instead, a return routability procedure is used to assure that the right MN is sending the bind update.

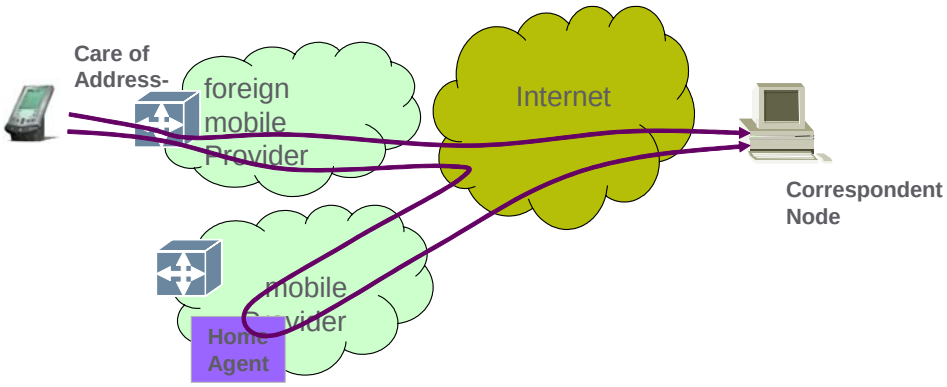


Figure C.7: IPv6 Mobility: CN Bind Update Step 1

- Prior to sending a bind update to the CN, the MN and CN establish a trust relationship via a series of messages:
  - The MN sends a Home Test Init (HoTi) to the CN via the home agent containing its home address.
  - The MN sends a Care-of test init (CoTi) to the CN directly containing its care of address.

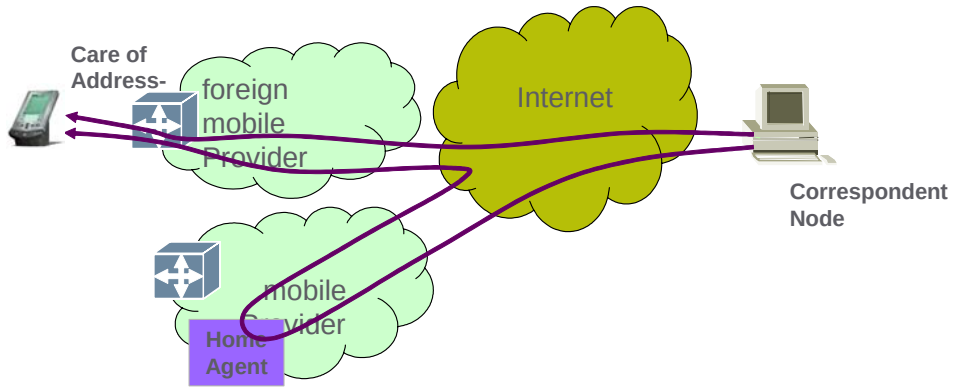


Figure C.8: IPv6 Mobility: CN Bind Update Step 2

- The CN sends a Home Test (HoT) to the MN via the home agent containing a special key only known to the CN.
- The CN sends a Care-of test (CoT) to the MN directly containing a special key only known to the CN.

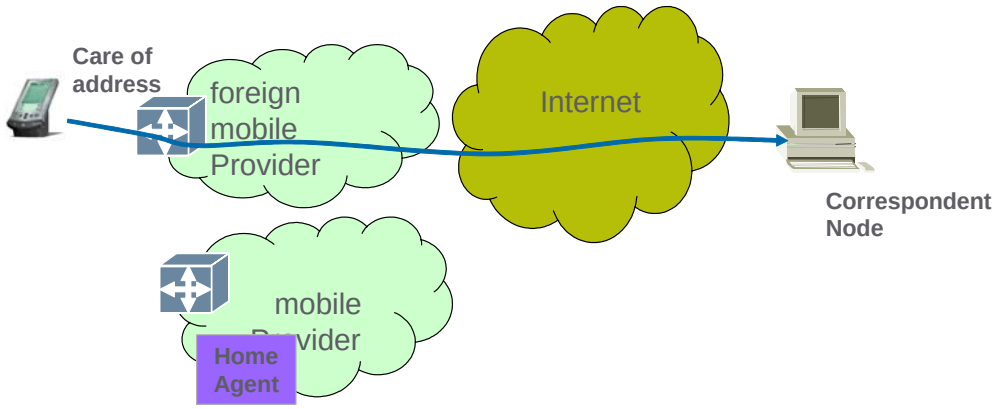


Figure C.9: IPv6 Mobility: CN Bind Security Step 3

- The mobile node can finally send the bind update; it contains a value that can only be derived from the combination of the keys received via the HOT and COT messages.
- This returned value provides the trust that CN needs to accept the bind update request.

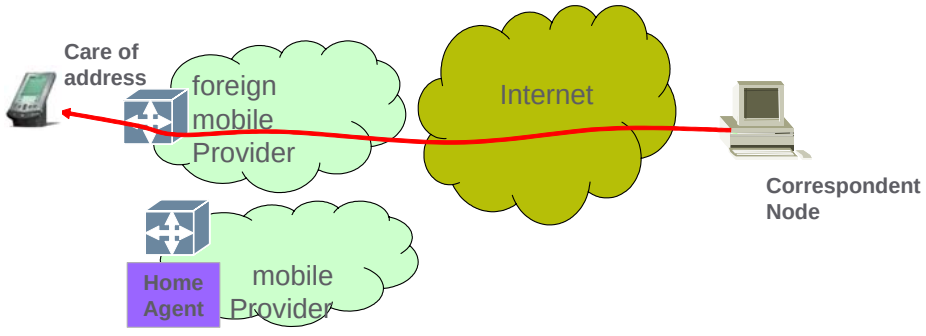


Figure C.10: IPv6 Mobility: CN to MN Direct Link

- The correspondent node can then send packets directly to the MN using the care of address and using the shortest communications path.
- This also limits congestion at the MN's home agent and home link.
- The CN uses a new type of IPv6 routing header to send the packet which is more optimal than encapsulating IP in IP encapsulation.
- The home address is swapped into the IPv6 header destination address field in the MN, allowing all transport connections to be maintained.

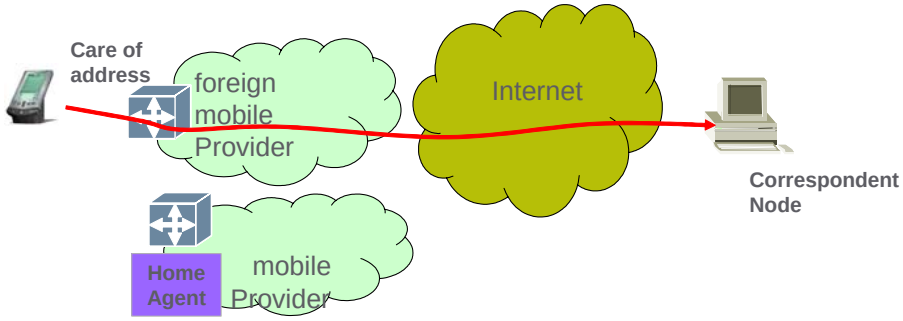


Figure C.11: IPv6 Mobility: MN to CN Direct Link

- The MN also sends packets directly to the CN.
- The MN sets the source address to the care of address and adds a 'home address' destination option extension header to the packet.
- Setting the source address to the care of address avoids any ingress filtering issues with the foreign mobile provider while maintaining transport layer connections.

APPENDIX D: ACRONYMS & ABBREVIATIONS

Acronym	Section	Definitions
3GPP	(2.2.3, 5.3.5)	Third Generation Partnership Project
ALG	(2.6, 4.9)	Application Layer Gateways
AP	(5.3.5)	Application Points
API	(2.2.2.1, A.1)	Application Programming Interface
APNIC	(2.3)	Asian Pacific Network Information Centre
ARIN	(2.5)	American Registry for Internet Numbers
ATM	(4.14)	Asynchronous Transfer Mode
CAPEX	(4.4)	Capital Expenditures
CDMA	(5.3.5)	Code Division Multiple Access
CE	(5.4)	Customer Edge
CIDR	(2.3)	Classless Inter-Domain Routing
CIO	(2.4.1)	Chief Information Officers
DDNS	(4.11)	Dynamic DNS
DFZ	(4.9)	Default Free Zone
DHCP	(4.4, 5.2.1)	Dynamic Host Configuration Protocol
DHS	(4.1)	Department of Homeland Security
DNS	(2.1.2, 3.4, 4.8)	Domain Name System
DoD	(2.4.1, Appendix C)	Department of Defense
DoS	(4.1.1)	Denial of Service
DSL	(2.1.2)	Digital Subscriber Line
DSLAM	(4.3.2)	Digital Subscriber Line Access Multiplexer
E2E	(2.2.2)	End-to-End
ESP	(2.2.1)	Encapsulating Security Payload
FAR	(2.4.1)	Federal Acquisition Regulation Council
FTP	(4.3)	File Transfer Protocol
GGSN	(5.3.5)	Gateway GPRS Support Node
GIG	(Appendix C)	Global Information Grid
GPRS	(2.2.3, 5.3.5)	General Packet Radio Service
GSM	(2.2.3)	Global System for Mobile communications
HTTP	(5.3.5)	HyperText Transfer Protocol
IANA	(2.3, Appendix A2-TEREDO)	Internet Assigned Numbers Authority
IETF	(3, 4.9.2, 5.3.5)	Internet Engineering Task Force
IKE	(4.11)	Internet Key Exchange
IMS	(2.1, 2.2.3)	IP Multimedia Subsystem
IPSec	(2.2.1, 4.9)	IP Security
Ipv6 SA or DA	(Appendix A2–)	Source Address/Destination Address
ISATAP	(3, 3.2.2, 5.2.1)	Intra-Site Automatic Tunnel Addressing Protocol
ISP	(2.3)	Internet Service Provider
IX	(4.9.3)	Internet Exchange
LAES	(4.13)	Lawfully Authorized Electronic Surveillance
M2M	(2.2.2.1)	Machine-to-Machine
MIPv6	(4.7)	Mobility for IPv6
MN	(2.2.1, C.1)	Mobile Node
MPLS	(3.3, 4.16, 5.4)	MultiProtocol Label Switching
NAPT	(4.11)	Network Address Port Translation
NAT	(2.1.2, 4.9)	Network Address Translator
NAT-PT	(4.18)	Network Address Translator – Protocol Translator
NEMO	(4.7)	Network Mobility
NIST	(2.4.1)	National Institute for Standards and Technology
NML	(5.5)	Network Management LAN (Layer)
NTIA	(2.4.1)	National Telecommunications and Information Administration
NTP	(4.4)	Network Termination Point OR network Time Protocol
OMB	(2.1,2.4.1)	Office of Management and Budget
OSA	(2.2.3)	Open Service Access
OSS	(4.4)	Operations Support System
P2P	(2.2.2, 4.12)	Peer-to-Peer

Acronym	Section	Definitions
PE	(5.3.5)	Processing Equipment
PI	(4.9.3)	Provider Independent
QoS	(2.1, 4.5)	Quality of Service
RFC	(3)	Request for Comment
RFID	(2.2.2.1)	Radio Frequency Identification
RIR	(2.3)	Regional Internet Registries
SGSN	(5.3.5)	Serving GPRS Support Node
SIP	(2.2.3)	Session Initiated Protocol
SP	(5.2.2)	Service Provider
TCP	(4.3, 5.3.5)	Transmission Control Protocol
TCP/IP stack	(2.1.2)	A redesigned TCP/IP protocol stack with an integrated version of both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (Ipv6)
TE	(4.16, 5.5)	Terminating Equipment
TOPS	(1, 5.1)	Technology and Operations Council
TSP	(3.0)	Tunnel Set-up Protocol
UDP	(3.1, 3.3)	User Datagram Protocol
UMTS	(2.2.3)	Universal Mobile Telecommunications Service
URL	(4.3.1)	Uniform Resource Locator
USCERT	(4.1)	United States Computer Emergency Response Team
VPN	(3.3, 5.4)	Virtual Private Network
VRF	(3.3, 5.3.4)	Virtual Routing and Forwarding
WAN	(2.1)	Wide Area Network

APPENDIX E: LIST OF REFERENCES

Note: At the time of publication the following website links (URL) were active; however, it is not anticipated that all identified links will remain static.

1: Executive Office of the President, Office of Management and Budget (OMB), "Memorandum for the Chief Information Officers, M-05-22, August 2, 2005" (2.1.1)

2: US Dept of Commerce/NIST/NTIA, "Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)" January 2006 (2.1.1)

3: "IPv6 Transition Technologies". www.isoc.org/breifings/007 (2.1.2)

4: "The Ipv6 Road to uncharted territories of revenue opportunities." http://www.nav6tf.org/documents/arin-nav6tf-apr05/3.Road_to_Revenue_Opportunities_YP.pdf (2.2.2)

5: http://www.larta.org/lavox/articlelinks/2004/041129_ipv6.asp (2.2.3)

6: "IPv6 – Extinction, Evolution or Exhaustion?" http://www.potaroo.net/ (2.3)

7: "A Pragmatic Report on IPv4 Address Space Consumption." http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_8-3/ipv4.html

8: "IP addressing in China." http://www.apnic.net/docs/apster/issues/apster12-200412.pdf (2.3)

and

"Twenty Myths and Truths About IPv6 and the US IPv6 Transition" http://www.circleid.com/posts/twenty_myths_and_truths_about_ipv6_and_the_us_ipv6_transition/ (2.3)

9: US Dept of Commerce/NIST/NTIA, "Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)" January 2006 (Page 8) (2.4.1)

10: "Subsequent allocation." http://www.arin.net/policy/nrpm.html (2.6)

11: Burton Group, D.Golding, "IPv6: Unmasked", version 1, February 8, 2006 (4.2)

12: Reference "IPv6 Transition Technologies," updated September 2005, Microsoft Corp.

13: "Mobility for IPv6 (mip6)." http://www.ietf.org/html.charters/mip6-charter.html (4.7)

15: "Network Mobility (nemo)." http://www.ietf.org/html.charters/nemo-charter.html (4.7)

16: "Multihoming L3 Shim Approach." http://www.ietf.org/Internet-drafts/draft-ietf-shim6-l3shim-00.txt (4.9)

and

"Site Multihoming by IPv6 Intermediation (shim6)." http://www.ietf.org/html.charters/shim6-charter.html (4.9)

17: "IPv6 Multihoming Support at Site Exit Routers."
http://www.ietf.org/rfc/rfc3178.txt?number=3178 (4.9.2)

18: http://www.ietf.org/Internet-drafts/draft-hain-ipv6-pi-addr-use-08.txt
http://www.ietf.org/Internet-drafts/draft-hain-ipv6-pi-addr-08.txt

19: "Euro 6IX; IPv6: The New Internet; 'Legal Aspects of the New Internet Protocol.'"
http://www.ipv6tf.org/pdf/ipv6legalaspects.pdf (4.13)

20: "Subsequent allocation." http://www.arin.net/policy/nrpm.html#six52 (4.14)

21: "Policy Proposal 2005-8: Proposal to amend ARIN IPv6 assignment and utilization requirement." http://www.arin.net/policy/proposals/2005_8.html. (4.14)

22: "IPv4 Address Report." http://www.potaroo.net/tools/ipv4/ (4.18)

and

"A Pragmatic Report on IPv4 Address Space Consumption."
http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_8-3/ipv4.html (4.18)

APPENDIX F: IPV6 TASK FORCE MEMBERS

Name	Company
Convener	
Tim Jeffries	ATIS
Members	
Chuck Bailey	AT&T (SBC Laboratories)
Phyllis Anderson	AT&T (SBC Laboratories)
Connie Hunt	AT&T (SBC)
Joe Houle	AT&T (SBC)
Anik Sane	Bell Canada
Jack Trimmer	Bell Canada
Steven Wright	BellSouth, Inc.
Robert Streijl	BellSouth, Inc.
David Meyer	Cisco Systems
Asok Chatterjee	Ericsson, Inc.
Kurt Melden	Juniper Networks
Andy Heffernan	Juniper Networks
Wayne Zeuch	Lucent Technologies
Dwight Jamieson	Nortel, Inc.
Chris Garner	Qwest, Inc.
Mike Fargano	Qwest, Inc.
Sean Mentzer	Qwest, Inc.
Mark Desterdick	Verizon, Inc.
Nabil Bitar	Verizon, Inc.
ATIS Support	
Meghan Ewell	ATIS
Martha Ciske	ATIS