

**Department of Commerce
Response to Notice of Inquiry**

Prepared by:

**NTT/VERIO
8005 S. Chester St, Suite 200
Englewood, CO 80112**

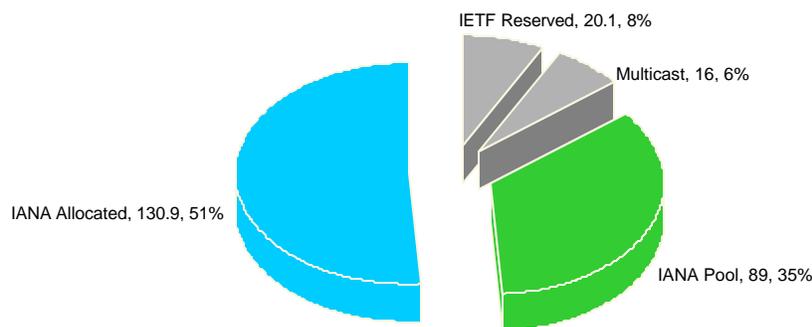
March 8, 2004

Please comment on the adequacy of IPv4 address space.

In accordance with a United Nation (UN) 2002 report, the Earth's population is estimated to be 6.3 billion. Without considering the H-ratio, the IPv4 32 bit address space is inadequate to support 1/3 of the Earth's population after factoring in the unusable IPv4 space such as the RFC 1918 private address block (10/8, 172.16/12, 192.168/16), the loopback address block (127/8) and reserved address space for uses such as multicast (224/3). Further, this UN report expects the population to increase by 2.6 billion during the next 47 years, to 8.9 billion in 2050 from 6.3 billion in 2002. The Internet architecture will need to accommodate growth in population and the quantity of devices which will be "naturally" connecting to the Internet; such as PDAs, cell phones and eventually, appliances.

China suffers from serious IP address shortages. Statistics show that currently, China has more than 60 million Internet users, but only 30 million-odd IPv4 addresses to be used by their populace, approximately two users for each IP address. Meanwhile, this nation's 240 million mobile phone users are turning into potential Internet surfers and as a result, need their own IP addresses. This inadequate supply of IP address is causing a bottleneck for Internet development within China.

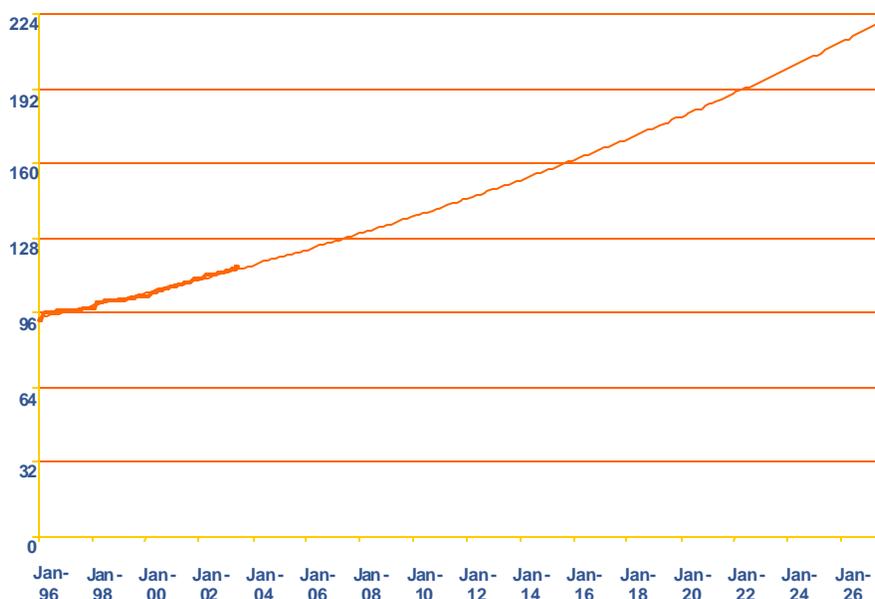
The TCP/IP protocol suite was developed under DARPA in the late 60s and early 70s. The lion's share of IPv4 address space was allocated within the United States. Other countries received a disproportionate and smaller blocks of IPv4 space. The Internet Engineering Task Force (IETF), through standards actions, defined the IPv4 standard that created the 32-bit addressing scheme yielding 4.4 Billion IP addresses. Of total address space, the IETF allocated a portion of the total address space (256/8s) for Unicast 86.3% (220/8s), Multicast, 6.2% (16/8s), and reserved 7.5% (20/8s) address space. The Unicast IP address allocation was delegated to Internet Addressing and Numbers Authority (IANA). The Regional Internet Registrars (RIRs – American Registry for Internet Numbers (ARIN) [US], (Réseaux IP Européens Network Coordination Center - RIPE NCC) [Europe], and Asia-Pacific Network Information Center (APNIC) are the organizations who allocate the address space to ISPs.



IANA Allocations

As of December 2003, IANA has allocated 51% (51 /8s) of the Unicast address space. This address space is in use by numerous organizations globally. IANA has a reserve pool of 35% - 89/8s, for future allocation to the RIRs. The balance of the IP space is reserved by the IETF, 7% -19/8s, for experimental or other specialized uses and 6% - 16/8s for Multicast uses. With estimated current growth rates, the IANA and RIPE studies predicts IPv4 address space will be exhausted between the years, 2019 and 2045. Further, this study targets a depletion window of 2019-2045, while the IANA is predicting it will exhaust it's pool of IPv4 address in the year 2020, and the RIRs will exhaust the pool of IP space allocated by IANA in the year 2027. However, this data is based on historical growth and does not take into account the population growth mentioned in the UN study, the China study nor the global growth of Ground Services Mobile (GSM), other wireless or mobile IP services, and other types of mobile hardware devices. The RIPE study acknowledges that predicted dates of exhaustion are wide because of poor initial data collection and analysis.

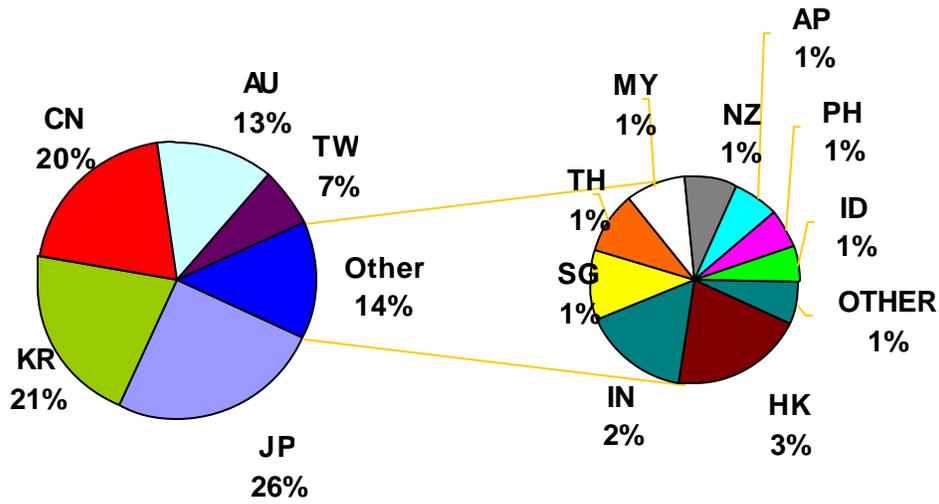
Total Allocations – Projection of “/8s”



Based IPv4 historical data, IPv4 address space will be exhausted by the year 2047. Including the growth of cell phones, PDAs, mobile IP and other devices, estimations are closer to 2025.

The following IP space under APNIC allocation authority has been allocated to the countries as depicted in the chart below:

IPv4 Allocations – Distribution by Nation



Country Codes:

AU – Australia
AP – Other Asia Pacific
CN – China
HK – Hong Kong
ID – Indonesia

IN – India
JP – Japan
KR – South Korea
MY – Malaysia
NZ – New Zealand

PH – Philippines
SG – Singapore
TH – Thailand

Estimate (and underlying assumptions) how many IPv4 addresses have been allocated, how many are still available, and how long the remaining addresses will be sufficient to meet the needs of users in the United States, as well as users in other countries around the world.

Current estimates for IPv4 address “exhaustion” range from the year 2005 to 2010 and beyond. Estimates are very sensitive to factors such as 3G service addressing architecture, 3G service growth, xDSL and cable modem adoption. The important fact is IPv4 addresses will continue to become harder to obtain, especially where new services such as streaming video and mobile PC phones require large numbers of addresses for initial deployment. The data below factors in anticipated growth rates of subscribers utilizing GSM, cable modems and DSL.

As of April 18, 2001, the IPv4 address space currently allocated to RIRs for further allocation to customers are:

- RIPE – 7 x /8s
- ARIN – 13 /8s
- APNIC – 6 x /8s

Total remaining IPv4 space available for allocation to RIRs is 103/8s.

Demand Forecast for IPv4 space for GSM service:

The table below shows the total number of GSM Subscribers (in Millions) broken down by regions:

	Actual			Forecast			
	2001	2002	2003	2004	2005	2006	2007
Total	627.8	796.0	941.3	1080.0	1204.1	1309.6	1393.0
Africa	26.2	36.9	51.1	70.4	94.4	121.2	146.0
South America	4.5	8.4	11.9	17.5	24.0	30.8	37.2
Asia Pacific	226.1	313.9	381.5	447.5	505.6	552.5	587.0
Eastern Europe	48.5	73.4	97.1	119.1	135.0	144.6	150.0
Western Europe	298.6	328.4	355.2	370.4	379.4	385.0	388.9
Middle East	11.4	17.4	23.8	31.5	39.3	46.8	53.0
USA/Canada	12.5	17.6	20.6	23.7	26.4	28.7	30.9

Source: EMC World Cellular Database, May 30, 2003

Global Cellular IP address (Millions)

IPv4 address demand (based on terminal demand)

01/02	02/03	03/04	04/05	05/06	Exhaustion Scenario
759	919.	1060	1177	1274	Worst Case
531.6	643.9	742.2	823.6	891.5	Most Likely
80	92	106	118	150	Best Case

Source: RIPE, April 2001 estimate

DSL + Cable Modem (Millions) Global Growth Forecast

01/02	02/03	03/04	04/05	05/06	Exhaustion Scenario
88	182	266	329	408	Worst Case
44	91	133	165	204	Most Likely
9	18	27	33	41	Best Case

Note: Carriers and industry analysts are significantly increasing their estimates of DSL deployments. These figures need to be revised upwards.

Summary of Exhaustion dates (based on projections for terminal and lines, not IP addresses):

Best Case (late exhaustion):

- 2014 (for 84 x /8s)
- 2018 (for 103 x /8s)

Most Likely Case:

- End 2010 (for 84 x /8s)
- End 2012 (for 103 x /8s)

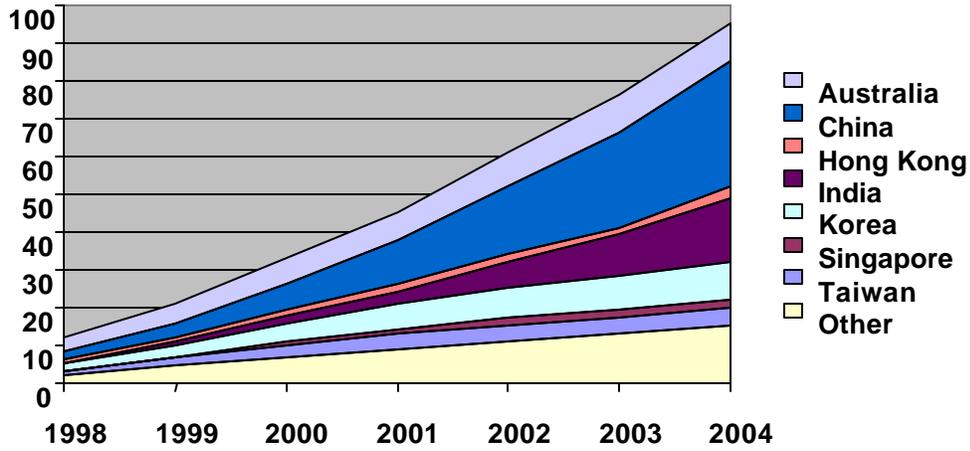
Worst Case (early exhaustion)

- Mid 2005 (for 84 x /8s)
- Mid 2006 (for 107 x /8s)

Note: NAT proxy servers and DHCP (dynamic addressing) are factored into estimates above.

Over the past four years, both China and India have started an explosive user growth rate:

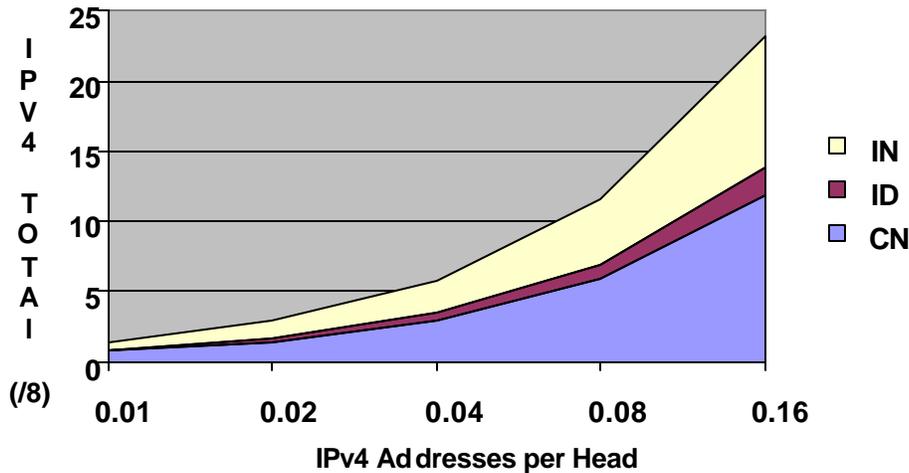
Asia Pacific Internet User Population



Source: Morgan Stanley Dean Witter

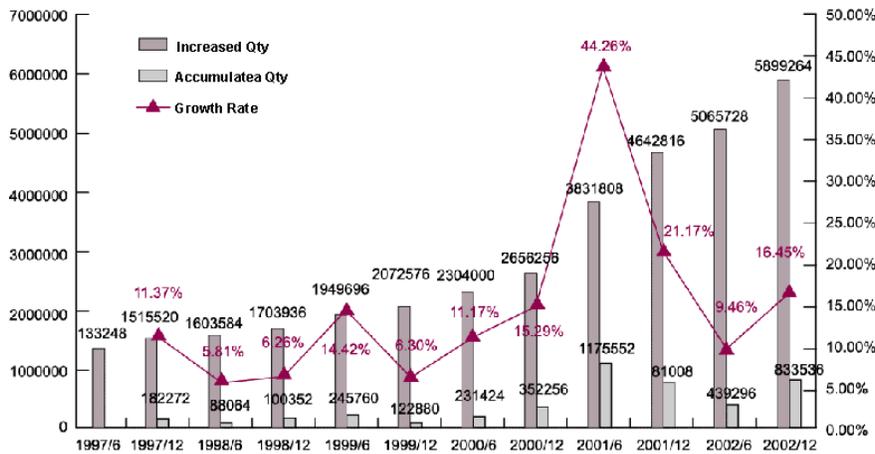
Discuss how the purported limitations on IPv4 addresses will affect different geographic regions (such as North America, Europe and Asia) and customer markets (such as the private sector, government and academia).

For the Asia Pacific region, the potential growth of population (per head) for China (CN), India (IN) and Indonesia (ID) are shown in the graph below:



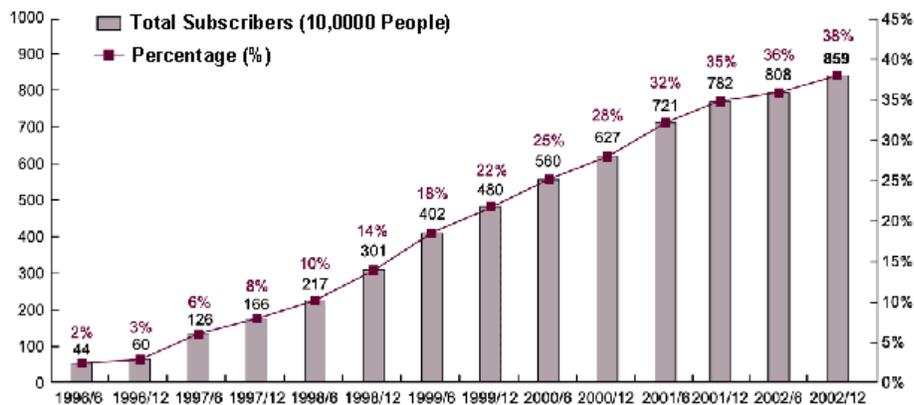
Taiwan's IPv4 growth rate

◀ TWNIC Issues IPv4 Address Growth Statistics. ▶



Source: TWNIC

◀ Taiwan Internet Subscribers Growth ▶



Source: Ministry of Economic Affairs, Department of Industrial Technology Internet Technology Project, ECRC FIND.

Discuss potential uses for the greatly expanded pool of addresses. What new products, services, features, applications and other uses are likely to result from the additional addresses offered by IPv6?

According to an IDC report, worldwide shipments of mobile telephones and personal digital assistants (PDAs) with digital imaging capabilities will increase to 151 million by the year 2006.

Comment: This report is a little old at this point– can we find updated info or delete the date of the report? Should be less than 12 months old

The global wireless market has exploded beyond expectation and the market is hungry for new and innovative services. In Japan for instance, emailing and database browsing from mobile phones have been rapidly penetrating the Internet market and the number of such users has exceeded 3.5 million. Introducing competitive services in this market space apparently requires an infrastructure that easily extends from the wireless network to the Internet," said Hideo Okinaka, of DDI Corporation, General Manager, Strategic Business Development) and a member of the Board of Directors for the Interim Mobile Wireless Internet Forum (MWIF) "MWIF represents a global voice of operators and service providers to enable this change."

Comment: Where does the quote begin?

Drivers for IPv4 to IPv6 transition include but are not limited to:

Near term:

- Cellular IP / mobile (the major consumer)
- DSL
- Cable modems
- Users in China and India gaining Internet connectivity

Long term:

- 3GT/UTMS (mobile)
- Multimedia
- E – commerce applications
- IP enabled devices in the consumer, transportation, manufacturing industries
- IP telephony
- Global IP VPNS (publicly registered addressed needed)

The need for more IP address space for mobility and security are the main drivers to move to IPv6. Utilizing IPv6 with IPsec would eliminate the need for the NAT feature used in IPv4, allowing direct secure connections in a peer-to-peer fashion. DSL and cable modem subscribers would not necessarily need to deploy firewalls as IPv6 connections can be made secure in point-to-point fashion. Utilization of IPv6 with mobile IP would allow for a simpler mobile network architecture eliminating the need for foreign agents, and eliminating the triangular routing issue that exists when using IPv4 with mobile IP. With IPv6, a mobile subscriber could move from subnet to subnet and from service provider to service provider without manual intervention or reconfiguration. IPv4 does not currently

allow mobile IP technology to function in this fashion. As a result, mobile users are tied to their home service provider network. If the subscriber wants to move from one provider to another, the IP address must be manually moved from one service provider's IP block to another service provider's IP block, a lengthy process. Typically, service providers will give each enterprise customer a /48 address block. End users will receive a sub-allocation of the enterprises /48, contingent on the need and the number of embedded host(s) in the mobile platform such as cell phones, automobiles and commercial aircraft.

Comment on the effects that NATs (as well as CIDR and other address conservation strategies) may have on network performance and network reliability.

IPv4 has traditionally utilized NAT with the RFC 1918 private address space (10/8, 172.16/12, and 192.168/16), primarily for address conservation and secondarily as a simple security method of hiding hosts behind a firewall. Classless Inter-domain Routing (CIDR) and "supernetting" have been traditionally utilized to minimize the explosive geometric route table growth and the related demand of increases in physical memory that is required in a router to store rout table information since the mid-1990's. Introduction of CIDR technology has made it possible to segment old class "A" address blocks into many small fragments. This increased the size of the internet routing table and led to long-term instabilities. Because once an inter-connection occurred between large ISPs, many routers needed to re-calculate the entities of the routing table and consume a huge amount of CPU time.

Port Address Translation (PAT) has also been used in conjunction with NAT to redirect inbound traffic to the appropriate host behind the NAT boundary.

The fact that IPv6 addresses are unique and globally routable is very significant. Growing numbers of popular applications, such as file-sharing and instant messaging, are built on a peer-to-peer model requiring end nodes to have unique, globally-routable addresses. Nodes addressed in this way are able to establish unmediated communications with each other, between any two points on the Internet (between 'peers', hence 'peer-to-peer'). Users whose ISPs provide them with connectivity via NAT will have difficulty using these popular applications with precision because they do not have unique addresses. It also may be impossible to merge an IPv4 privately-addressed network with another IPv4 privately-addressed network, requiring instead, a complex and costly network renumbering operation. Choosing IPv4 private addressing also closes the door to deploying peer-to-peer applications or any other end-to-end services, such as IPsec, in the future.

The methods mentioned above have a minimal impact on network performance and reliability of an operational network, but add complexity to an organization's network. There are significant labor cost issues in merging IPv4 networks if the merging organizations utilize the same RFC 1918 private address space. Additionally, there are potential performance and reliability issues which could directly impact an organization if, during the migration, duplicate IPv4 address were inadvertently assigned and/or used. For example, parts of the organization would be isolated without Internet connectivity or intermittent connectivity if assigned the same IP space. Potential routing loops could develop causing connectivity to be blocked at an unexpected time if routing issues are not examined closely before integration of networks.

Address any characteristics of IPv6 that directly or indirectly enhance network security compared to IPv4. Conversely, we also seek comments on any features of IPv6 that may degrade network security compared to IPv4.

IPsec is integrated into IPv6, whereas in IPv4, is offered as an add-on, typically requiring some form of NAT to occur with either private or public IPv4 space. In both IPv4 and IPv6, different algorithms can be utilized for authentication (MD5, SHA-1) and encryption (DES, triple DES, and AES). Utilizing IPv6 allows direct end-to-end connections to be established in a peer-to-peer fashion eliminating the need for NAT.

This allows for more granular control of connections that can be permitted or denied in a secure policy enforcement point, thereby reducing the risk of address spoofing that can be performed in IPv4.

At this time, there are no known vulnerabilities to the IPv6 protocol that might degrade network security as compared to IPv4. However, as in IPv4, there will most likely be undiscovered vulnerabilities in host operating systems and applications that use IPv6. This being said, it will allow vulnerabilities to potentially be exploited when discovered. The two leading router providers, Cisco Systems, Inc. and Juniper Networks, Inc. do an excellent job of providing reliable, stable and secure routing code for their respective product lines.

Several features of IPv6 could be exploited by hackers in an attempt to gain access into a network or hosts on an IPv6 network. For example, the address auto configuration feature could be used by attackers to announce rogue routers if necessary security precautions to prevent this exploit are not taken. In addition, some of the designed transitioning mechanisms will allow easier interaction between IPv6 and IPv4 networks. Unfortunately, attackers can misuse these mechanisms. Transitioning tools create a way for IPv4 applications to connect to IPv6 services, and IPv6 applications to connect to IPv4 services. Since many firewalls allow User Datagram Protocol (UDP) traffic, IPv6 over UDP can get through those firewalls without system/firewall administrators realizing it is taking place. In addition, attackers can use 6 over 4 tunnels to evade Intrusion Detection software. If IPv6 is tunneled over IPv4, this method of exploitation effectively bypasses some or all IPv4 security devices that have been implemented to protect an organization's network.

The IPv6 protocol has been designed with security in mind, making it inherently more secure than the IPv4 protocol; which does not have any security fields integrated into the protocol.

NAT for IPv4 has some functionality as an anonymizer. Hosts behind NAT-boxes could mix their packets with packets generated by other hosts in the same private network space; when the packets go through the NAT-boxes. Although inspectors could isolate each stream and determine its origination point through, TCP, UDP ports, it's still difficult to gather the streams which have the same origin and be able to determine the

source. This would be applicable when the number of active hosts behind the NAT-boxes is more than two.

Using IPv6 global address makes it possible to track it's origin and collect activity of the packet's origin; even though IPv6 has a privacy extension specification.

Since IPsec is a standard feature of IPv6, will IPsec be easier to use with IPv6 than with IPv4 and, therefore, more widely used?

The IPsec protocol is an add-on to IPv4 and not integrated into the IPv4 protocol itself. IPv6 was designed with new extended packet headers to allow for newer encryption and authentication algorithms to be incorporated into IPv6. This allows for easier management of secure connections and keying material for those secure connections. This will be especially important for mobile IPv6 which allows more efficient routing (elimination of triangular routing) of packets to mobile nodes than IPv4. When IPsec is utilized in conjunction with mobile IPv6, E-commerce can occur from a mobile node in a secure fashion. For example, many Japanese companies are working on location based applications that allow consumers to have a text message sent to them while walking by a store offering them a promotional discount or other method of increasing foot traffic into the store to effectively target the consumer. The consumer enters the store, shows the ad to the vendor, receives their product and pays for the transaction securely using the E-commerce capability integrated into their PDA or cell phone. IPv6 will make this type of transaction much easier than with IPv4 protocol.

With either protocol, a good public key infrastructure (PKI) will be required to issue, manage and expire digital certificates or pre-shared keys on a regular, timely basis.

To what extent would deployment of IPv6 further national security and law enforcement interests over and above the security features and capabilities available via IPv4?

The IPv6 protocol is somewhat inherently more secure than IPv4, supporting 56-bit DES in nearly all IPv6 stacks. IPv6 was designed in a modular way with new extended packet headers to allow the utilization of various encryption algorithms, such as 3DES, AES, and others, be utilized in IPv6 in place of 56-bit DES encryption. The extended packet headers will also allow other new features to be incorporated into IPv6 as they become more developed.

From the government's perspective, the establishment of IPv6 IPsec encrypted VPNs, may make it more difficult to monitor for terrorist activity, especially used in conjunction with IP mobility. This will create a need for new tools to be developed in order to monitor malicious activity targeted by the various government agencies such as the CIA or FBI, while following the traditional processes and procedures to obtain permission to deploy wiretap(s) of suspected individuals.

Additional training will be required at the federal, state, county, and local law enforcement levels. For example, during a raid on a suspected terrorist or drug dealer, the cell phone would not only yield contact information based on it's telephone number, but also obtain it's IP address and encryption keys for other peers it has "engaged." This would allow law enforcement personnel the unique ability to identify the instrument(s) utilized during the transmissions. Newer cell phones currently being shipped, contain an operating system similar to a PDA or a PC, which allows the device to store more information that could be potentially valuable to a criminal investigation.

Provide examples of how these improved capabilities (reducing network management burdens, simplifying mobile Internet access, and meeting quality of service needs) of IPv6 could benefit current users of IPv4.

In general, there are no reasons to rely on NAT (Network Address Translator) compatibility: Recent IPv4 NAT-boxes have Universal Plug and Play capability to support the NAT traversal technique. Peer-to-Peer applications, such as Voice over IP of the Windows Messenger, require this functionality if they are behind NAT-boxes. Application developers/providers need to test new devices or applications on IPv4 with various NAT-boxes to check their compatibility. From a user's perspective, one needs to make sure that his/her NAT-box is compatible with any new application(s). On the other hand, with IPv6, a NAT box is no longer required because users and application developers do not need to concern themselves about compatibility issues.

Route Optimization of Mobile IP:

According to the specifications for Mobile IPv6, it already has a route optimization functionality built into it. Though an initial packet exchange goes through Home-Agent (HA), Mobile Node (MN) and Corresponding Node (CN) begins to exchange packet directly after that. This route optimization offers better quality for jitter sensitive applications and peer-to-peer applications such as Voice over IP. Please see Exhibits A and B.

Easy subnet provisioning:

Due to the large number of addresses that could be assigned for each customer (/48), users can assign a fixed length subnet, such as a /64, for all subnets. As a result, Network Administrators do not need to worry about the prefix length assigned for each subnet.

Is the increase in address space afforded by IPv6 the only compelling reason for adopting the new protocol?

According to an IDC report of August 2002, worldwide shipments of mobile telephones and PDAs with digital imaging capabilities will increase to 151 million by the year 2006. Adding to the address demands will be the millions of new users in countries such as China and India, as well as millions of new devices such as, Internet-connected automobiles, home theater PCs and home based appliances such as the refrigerator and microwave. The improvements of IPv6 over IPv4 yield a more intelligent packet for Internet access with high security and better quality of service. The driver for additional IP space for IP mobility based products are much greater in Europe and Asia than in the United States; as they do not have very much IPv4 space allocated to these regions.

The principal benefit of IPv6, and the main reason for its initial deployment is the increased address space compared with its IPv4 predecessor. IPv4 has a 32-bit address space, theoretically providing for 2^{32} (approximately 4 billion) unique Internet node addresses. On the other hand, IPv6 has a 128-bit address space, providing 2^{128} ($2^{32} \times 2^{32} \times 2^{32} \times 2^{32}$) unique addresses. To put this in perspective, if the population of China and India were each given one IPv4 address, over 50% of the IPv4 address pool would be consumed by these two countries without taking into account any other constraint. This is the major driver for the Asia-Pacific and European nations to migrate to IPv6 before the US, especially before the use of mobile wireless devices vastly expands in these countries.

A very significant second factor for migrating to IPv6 is the fact that IPv6 addresses are unique and globally-routable. Growing numbers of popular applications, such as file-sharing and instant messaging, are built on a peer-to-peer model that requires end nodes to have unique, globally-routable addresses. Nodes addressed in this way are able to establish unmediated communications with each other, between any two points on the Internet in a peer-to-peer fashion. A user's ISP provides them with connectivity via Network Address Translation (NAT), a commonly deployed solution to overcome IPv4 address shortages, will have difficulty in precisely using these popular applications because they do not have unique addresses. Another issue that will arise from using IPv4 versus IPv6 is that it may be impossible to merge an IPv4 privately addressed network with another IPv4 privately addressed network, requiring instead a complex and costly network renumbering operation. Choosing private addressing would close the door to deploying peer-to-peer applications or any other end-to-end services, such as IPsec in the future.

One specific example of wireless mobility products and services is from Cisco's October 2003, press release stating that Cisco Systems Technology Center and Renault Prospect & Research Division jointly worked on a revolutionary IPv6 e-Vehicle project, equipping a Renault Laguna 2 car with a router and a set of emergent applications, such as vehicle remote diagnostic, centralized support, and off-road navigation system. These features were easily enabled by IP technologies. This is an example where many IPv6 addresses are consumed on one mobile platform.

Comment on the ease with which each feature and capability associated with IPv6 can be implemented over IPv4 networks and whether IPv4 implementations will perform as effectively as IPv6 networks.

When enough IPv4 addresses are supplied, problems caused by NAT-boxes may be ignored, allowing for easier network management. Fundamental differences such as the extension header mechanism and the route optimization function of Mobile IPv6 cannot be implemented with IPv4.

Because IPv6 offers new capabilities, do the transport layers (e.g., transmission control protocol (TCP), user data protocol (UDP)) need to be modified to support both existing and new applications?

TCP and UDP are not significantly impacted by IPv6. In fact, the impact of IPv6 on all upper layer protocols is minimal because the datagram service is not substantially modified. One exception is check summing. Unlike IPv4, the IPv6 header does not include a checksum. This checksum is important to the transport layer (TCP and UDP) and other upper layer protocols. With IPv4, a checksum in the UDP header was optional. However, with IPv6, the computation of a UDP checksum is mandatory. IPv6 nodes will discard UDP packets with checksum field values of zero. (Checksums have always been mandatory for TCP). TCP and UDP use a pseudo-header to calculate their checksums. Because the IPv6 address is longer than the IPv4 address, a new version of the pseudo-header was created. The new IPv6 pseudo-header accommodates the longer IPv6 addresses and takes into account extension headers that can impact payload length. Below is the format for the pseudo-header built and used to calculate TCP and UDP checksums in IPv6:

- Source Address (16 bytes): IPv6 packet source address
- Destination Address (16 bytes): IPv6 packet final destination
- Upper Layer Packet Length (4 bytes): length of upper layer protocol header plus data
- Reserved (3 bytes): must be zero
- Next Header (1 byte): identifies header type

The task force seeks specific data on the hardware, software, training, and other costs associated with implementation of IPv6.

As with any emerging technology, the costs for implementing IPv6 will largely be based on the amount of strategic planning an organization does early on to control costs associated with integrating this technology into an operating enterprise. IPv6 has been available in a production form from all the major routing vendors for at least a year. Prior to that, vendors were already disclosing their roadmap on the support of IPv6 so those choosing to deploy it would be able to integrate the use of IPv6 along with any other strategic improvements. In fact, deploying IPv6 may be easier than many other such technologies since the basic mandates in the standards bodies for supporting IPv6 have required that it co-exist with IPv4 from the outset.

So, if the enterprise is using a strategic planning approach when determining how to integrate new technologies into their network capabilities, it is strongly believed that these costs are very small relative to those that relate to the basic upkeep of the network. This has certainly been the case for NTT/VERIO. Because of the strategic planning done early on for the support of IPv6, MPLS and other technologies, NTT/VERIO made purchasing decisions and provided training to our staff using existing budgets and existing processes. As a result, the costs of deployment have been incremental and by relative terms, gradual.

NTT/VERIO uses routers and servers from different manufacturers in their network. All of the equipment mentioned, support IPv6 and are being used for that purpose.

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

The network layer should experience few, if any, issues migrating from IPv4 to IPv6 when utilizing router hardware and software from the major router vendors. Typically, only the software image needs to be upgraded. If an older router is used, a memory upgrade will most likely will be needed in addition to a software image upgrade. In some instances, a newer software image may dictate that the router hardware may need to be upgraded or replaced, depending on the age of the device. On older hardware appliances and middleware that had IPv4 addresses specifically hard coded into the firmware or software could cause problems, especially if the devices, firmware or software have not been reviewed for IPv6 compatibility. For example, a Point of Sale (PoS) terminal, commonly used in hundreds of thousands of businesses worldwide was reviewed for the Y2K date issue may be functioning correctly, but it may not have network capability. If it does have network capability, it may not be able to speak with the IPv6 protocol. If the PoS terminal cannot be upgraded, it will need to be replaced. Overall, a majority of the newer hardware appliances should be capable of being upgraded to IPv6 by a vendor's firmware or software upgrades. Older hardware appliances may need to be phased out or replaced if there is no upgrade path available. For example, if there is a Cisco or Juniper router is being considered, the user needs to make sure that a fairly recent release of IOS is used. Caution must be exercised to ensure the platform supports IPv6. For instance, Cisco's 6509 Supervisor1 and Supervisor2 still do not have an IOS release that supports IPv6. Supervisor1 may not have IPv6 support at all. Supervisor2 support is approximately one-month away.

Middleware should be capable of being upgraded to IPv6 if the vendor of the product is still conducting business. However, it should be noted that the customer is reliant on the vendor for upgraded availability.

Once a vendor's hardware and OS has been confirmed to support ipv6, implementation is very similar to IPv4 and should not be difficult.

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

IPv6 standards are complete enough to enable widespread commercial deployment. Operating Systems, routers, firewalls, and other types of network appliances are mature enough to support IPv6 in a commercial fashion. There are numerous IPv6 research networks established at the regional, national and global levels to determine the stability, reliability and maturity of the IPv6 protocol suite. The web site www.ipv6forum.org has much more detail regarding the deployment and implementation of IPv6 research networks on the regional, national and global level.

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

RIRs (ARIN, APNIC, RIPE, LACNIC) have strict rules on Provider Independent (PI) IPv6 address block assignment for applicants than with IPv4 to suppress total number of routes on the Internet. Some people say that it might hard to apply for academics and middle size enterprises because of these rules. The prefix length of initial assignment is now 32 bits (65536 customers). Current IPv6 network allow announcements of only aggregated sTLA.

RIR mentioned that these conditions make it difficult to use its own PI address blocks for customers in this market segment for redundancy using BGP. Further, some development is in progress within IETF's multi6 working group to solve this problem. The DNS discovery mechanism remains an open item for IETF. There are three proposed mechanisms to discover recursive DNS servers that support IPv6 transport between its clients, (i) DHCPv6-lite, (ii) embedded information to RA, (iii) and well-known address mechanism. The "DNSOP" working group is working on these proposals.

But, the prefix length of 32 bits is same as only one IPv4 address, so it is thought there are no foreseen issues for any market segment obtaining an allocation of IP space from a technical perspective.

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

The United States is behind in the deployment of IPv6 as compared to other nations. As of June 2000, the allocation of IPv6 sub-TLAs is as follows:

- RIPE NCC (Europe): 17
- APNIC (Asia-Pacific): 12
- ARIN (US): 5

More updates are needed for sTLA allocation status. Currently, North America has more sTLAs.

Japan in particular has already deployed IPv6 in a commercial environment. Due to the explosion of DSL cable and cellular technology, the shortage of IPv4 addresses has pushed both Asia and Europe ahead of the US in using IPv6. For example, some large academic institutions in the US and Europe have more IPv4 addresses than mainland China, driving the Chinese to look at IPv6 for their current and new Internet users.

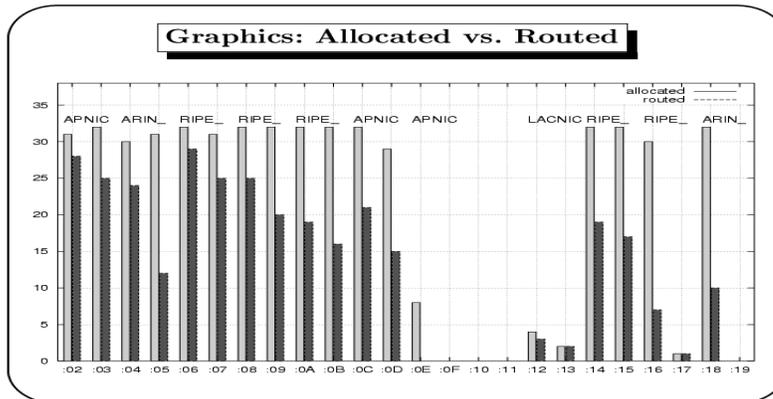
On March 22, 2000, NTT Communications, announced it was the first ISP to offer commercial Internet service supporting IPv6 in Japan. On April 26, 2001, NTT Communications and Verio Inc. launched operation of the world's first commercial global IPv6 backbone, which spans Japan, the U.S. and Europe. And on December 11, 2003 NTT Communications and Verio Inc., announced commercial native IPv6 services globally to the customer premise. IJ, Japan's competitor to NTT Communications launched a national IPv6 commercial service on September 1, 2000, in Japan.

In Europe, Telecom Italia Laboratory announced on July 27, 2001, that it was the first to offer commercial IPv6 services. The diagram below depicts the number of IPv6 addresses that has been allocated and is currently being routed by the three RIRs.

IPv6 routing table

Numbers

14



In addition to the Asia-Pacific and European regional drivers for IPv6 deployment, certain services will require IPv6. Standards mandate use of IPv6 for connections to new multimedia services. Essentially, any service with significant IP addressing requirements will benefit by adopting IPv6. IT outsourcing companies that currently have issues managing multiple networks with overlapping, private address space will find the expanded address space offered by IPv6 to be a great benefit.

Comment on the availability of IPv6 products and services in the US.

The following list is a sample representative of vendors who currently support IPv6 with products available. This list is by no means exhaustive nor is any vendor recommended over another vendor.

- Routers:
 - Cisco (IOS)
 - Juniper (JunOS)

- Operating Systems:
 - HP (HP-UX, Openview)
 - Sun Microsystems (Solaris)
 - Linux (all variations)
 - BSD, (All variations)
 - Microsoft XP
 - IBM AIX
 - Windriver's VxWorks

- Security Devices:
 - Nokia (IP series of firewall platforms)
 - Checkpoint (firewall vendor)

- Microsoft Windows2003 server

Please see Appendix A for more details.

Currently, only one vendor, NTT/VERIO, commercially offers native IPv6, tunneling and dual stack services globally over the NTT/VERIO Global Tier One IPv6 Network. For more information, please see Exhibit C.

How many ISPs are currently capable of handling IPv6 traffic?

At the time of this response, NTT/VERIO is currently the only global provider that can offer commercial IPv6 services in the US. Austria, Belgium, Canada, Czech Republic, Denmark, European Union, France Germany, Hungary, India, Italy, Korea, Mexico, Netherlands, Norway, Poland, Russia, Singapore Spain, Switzerland, Tunisia, USA, and the United Kingdom all have IPv6 research networks to varying degrees of development, primarily in the academic realm. The following URL depicts in more detail, IPv6 development status by other nations with respect to their regional and national deployments:

<http://www.ipv6forum.com/>

Click on the IPv6 Deployment menu item / National Deployments hyperlink.

IPv6 products and services are both in the early stages of adoption in the US. Products are slightly ahead of services with several companies having IPv6 compatible CPE, such as routers and switches on the market. For IPv6 access services, the market is very limited. Currently there are two major test beds for IPv6 within the US, Moonv6 and 6bone. Both are simply test environments for the protocol and do not offer commercial service to customers. NTT/VERIO launched it's Native, Tunneling and Dual Stack IPv6 Gateway Services in October 2003.

What percentage of Internet access customers receive IPv6 capable services?

While IPv6 is more prevalent globally, especially in Asia Pacific countries, a very small percentage of US customers receive IPv6 capable services. Due to the limited availability of commercial services, less than 1% of customers in the US currently have IPv6 services.

Explain how particular initiatives or programs by foreign governments or foreign suppliers have helped (or hindered) IPv6 deployment.

Japan's Case Study:

(1) Policy setting

- Support from the Japanese Government started in September 2000, when Prime Minister Yoshiro Mori spoke at the Diet about the importance of IPv6 research. (For more information on Prime Minister Mori's speech go to: <http://www.kantei.go.jp/foreign/souri/mori/2000/0921policy.html>)
- His speech turned into a tangible strategy of "e-Japan" which outlined support from the Japanese Government for IPv6 transition. (For more information go to: http://www.kantei.go.jp/foreign/it/network/0122full_e.html)
- According "e-Japan" strategies, the Japanese Government (particularly the Ministry of Public Management, Home Affairs, Post and Telecommunications) launched various projects promoting IPv6.

(2) IPv6 Core Technology Development:

- Information Appliance Projects: IPv6 promotions focused on information appliances including the creation of various prototypes of IPv6 based Information Appliances.
- E! Project: Apply the leading edge of IPv6 technologies into six different areas of applications which show the potential of IT usage. These six areas were; Education, Agriculture, Tourism, International cultural exchange, Social welfare, and local government operations. (For more information, go to: http://www.kantei.go.jp/foreign/policy/2001/1204yosan_e.html)
- JGN (Japan Gigabit Network): R&D network, which mandated IPv6 requirements. This project stimulated vendor's into developing IPv6 ready routers.
- IPv6 Transition Project: Created the guidelines for System Integration Vendors dealing with the IPv4 to IPv6 transition. (For more information , go to <http://www.v6trans.jp/en/index.html>)

Newly launched projects were focused on IPv6 technology rather than development of cutting edge innovation.

(3) Support of IPv6 proliferations

- Special Tax exemptions were awarded to those ISP's evaluating the application of IPv6 in their network. The purchase of IPv6 "ready" routers were tax exempted
- The Ministry of Public Management, Home Affairs, Post and Telecommunications sponsored an "IPv6 promotion council." Because of

the Ministry's sponsorship and support, the participation fee for council members was waived; encouraging the participation from many different areas (currently 350 companies and organizations are council members). Recent council activities include:

- Establishment and promotion of a IPv6 Ready Logo
- IPv6 demonstrations at various IPv6 conferences and summits
- Establishment of various working groups to discuss areas of IPv6 technologies, including Building Automation, Information Appliance, and Sensor Networking.
- Collaboration with foreign organizations also promoting IPv6.

(For more information on the Promotion Council and recent activities, please go to: <http://www.v6pc.jp/en/index.htm>)”

Appendix A: Detailed Listing of Hardware, Host Operating Systems and Software Applications Supporting IPv6

Applications:

Application database:

- [IPv6 applications](#) - Contains over 100 IPv6 packages/patches

Chat software:

- [RAT and SDR](#) - Windows versions of the UCL conferencing ports

DNS:

- [BIND 9.1.2](#) - Uses A6 records and offers IPv6 transport
- [toto](#) - DNS proxy to support IPv4/IPv6 translation
- [IPv6 transport for BIND8](#) - Patch for BIND8.2.3 by Stig Venas

Firewalls:

- [CheckPoint](#) - Plans for IPv6 in FireWall-1
- [Firewalling in OpenBSD](#) - Guide from the SANS institute
- [ipfilter](#) - Supports IPv6 filtering
- [IPFW](#) - Included within the FreeBSD 4.0 release
- [netfilter](#) - IPv6 patches for Linux's packet filter

FTP:

- [LFTP](#) - Supports IPv6 "as is"
- [NcFTP \(Windows\)](#) - Available from MSR
- [NcFTP \(BSD\)](#) - From the KAME project site

Games:

- [Quakeforge](#) - FreeBSD port by Viagenie

IPsec:

- [IPv6 FreeS/WAN for Linux](#) - Developed by IABG as part of the 6INIT project
- [IPv6 IPsec in KAME](#) - KAME IPv6 supports IPsec with Racoon

Java:

- [IPv6 Java for Windows](#) – Note: This is not a Sun Javasoft product
- [Sun JDK](#) - Java(TM)2, Standard Edition 1.4.1 FCS includes IPv6 support

Mail:

- [Exim](#) - Has built-in IPv6 support
- [qmail](#) - V1.03 patch by Kazunori Fujiwara
- [Public Sendmail](#) - Version 8.10 officially supports IPv6.
- [WIDE Sendmail](#) - Version 8.9.1 from KAME.
- [Fetchmail](#) - Supports IPv6 and IPsec.

Mobile IPv6:

- [MIPL Mobile IPv6 for Linux](#) - Developed at HUT. Finland, and available freely under GPL.

Monitoring Tools:

- [ASPath-tree](#) - Tool to monitor BGP4+ routing
- [COLD](#) - An IPv6-aware packet sniffer.

News:

- [INN v2.2.2](#) - IPv6 patch from the Japanese NORTH site
- [mnews](#) - IPv6 enabled news client

Patch Sites:

- [IPv6 Meat](#) - Linux patches
- [IPv6 patches](#) - Maintained by Hajimu Umemoto
- [KAME patches](#) - From the Japanese KAME project site
- [KAME patch list](#) - List of patches for many apps
- [Linux IPv6 apps](#) - From the Linux Japanese user group
- [Linux IPv6 apps list](#) - By Peter Bieringer
- [University of Tromso](#) - Patches from the Norwegian site
- [WIDE patches](#) - From the Japanese WIDE project site
- [Zama Networks](#) - Patches for a variety of applications

Socket software:

- [IPv6 socket 1.1](#) - By the University of Tromso

Video and conferencing:

- [ISABEL](#) - Collaborative working and conferencing system
- [mpeg4ip](#) - Just run './bootstrap - enable-ipv6' before making
- [Vic and Rat](#) - UCL MICE tools
- [Vic/Rat for WinXP](#) - Plus other Microsoft multicast information

Web servers and clients:

- [Apache \(Linux\)](#) - From the Japanese Linux users group
- [Apache \(BSD\)](#) - From the KAME project site
- [Apache + mod_ssl](#) - Patches from Zama Networks
- [Apache 2.0](#) - Currently beta code, but supports IPv6
- [Fnord!](#) - Windows web server from MSR
- [lynx](#) - Port of the text-based browser by Tromso
- [mini_hhttpd](#) - Web server with IPv6 support
- [Mozilla](#) - Port of the browser by KAME
- [that'd](#) - Web server with IPv6 support
- [w3m](#) - Text-based browser that supports IPv6
- [w3m](#) - Text-based browser that supports IPv6

Host Operating System Support:

Apple:

- [Jaguar](#) - MacOS X v10.2 has a production IPv6 stack and supports IPsec

BSD:

- [FreeBSD 4.0](#) - Includes the KAME IPv6 stack
- [KAME](#) - various BSD versions are being united here
- [INRIA](#) - Development appears to have ceded to KAME
- [NRL's IPv6](#) - Distributed from MIT (v7.1 Dec'98)
- [IPv6-DRET](#) - French implementation

Compaq:

- [Compaq IPv6 Information](#) - Concerning IPv6, and Tru64/OpenVMS implementations

Elmic Systems:

- [Dual Stack Suite](#) - Aimed at embedded systems

FTP/NetManage:

- [OnNet Host Suite](#) - IPv6 support for Windows 95/98/NT

Future Software :

- [FutureIPv6 Host](#) - Portable source code product from Future Software Limited

Hitachi:

- [Toolnet6](#) - Provides IPv6 connectivity for your Windows PC

HP:

- [HP-UX 11i](#) - IPv6 Release (August 2001)

IBM:

- [AIX 4.3](#) – Built-in IPv6 support for the RS6000
- [Next Generation Internet](#) - IPv6 and much more
- [OS/390](#) - Working prototype

Integrated Systems Inc (ISI):

- [IPv6 in embedded systems](#) - First company to achieve this

Linux:

- [IPv6 Users Group JP](#) - Japanese site, but lots in English
- [IPv6 HowTo](#) - By Peter Bieringer
- [USAGI Project](#) - Universal Playground for IPv6, liaising with WIDE, KAME and TAHI
- [IPv6 Meat](#) - Linux patches
- [Debian IPv6 Project](#) - IPv6 for Debian Linux
- [Linux IPv6 RPM Project](#) - IPv6 in RPM packages

Microsoft:

- [Microsoft and IPv6](#) - General product information
- [Windows XP IPv6 FAQ](#) - XP ships with IPv6
- [Microsoft IPv6 Technology](#) - For .NET, WinCE .NET and WinXP
- [Corona](#) - Streaming with IPv6 support
- [Official Windows 2000 press release](#) - IPv6 and Win 2000 information (dated)

NTT/VERIO

- [Windows 2000 preview version](#) - Available for Win2K SP1
- [Microsoft Research and IPv6](#) - General MSR information (dated)

Mentat:

- [Mentat TCP](#) - TCP/IP stack including IPv6 and IPsec support

Mistral Software:

- [MistIPv6](#) - Modular, compact, portable and robust implementation designed for high performance

SCO:

- [UnixWare 7](#) - With IPv6 API support

Sun:

- [Solaris 8](#) - Ships with IPv6 support

Trumpet:

- [Winsock 5.0](#) - IPv6 stack for Win 9x/NT

Hardware:

3Com:

- [6com.net](#) - 3Com's IPv6 info site
- [Technology info](#) - General information
- [Enterprise OS Software v11.4](#) - Reference manual with IPv6 information

6WIND:

- [IPv6 Access and Edge Routers](#) - Providing Security/VPN/Firewall, QoS Management, IP Mobility, Multicast and IPv4/v6 migration features

Cisco:

- [Cisco IP Version 6 Solutions](#) - General information
- [Configuring IOS Software](#) - Notes on 12.2 series
- [Cisco IOS Software Release](#) - Specifics for IPv6 features
- [IPv6 IOS](#) - Cisco IPv6 for IOS, with many links
- [6NET](#) - European project coordinated by Cisco

Ericsson Telebit:

- [IPv6 modules](#) - Telebit routers support IPv6 commercially

Fujitsu:

- [GeoStream R900 Series](#) - IPv6 product deployable from core to edge.

Future Software:

- [FutureIPv6 Router](#) - Portable source code product from Future Software Limited

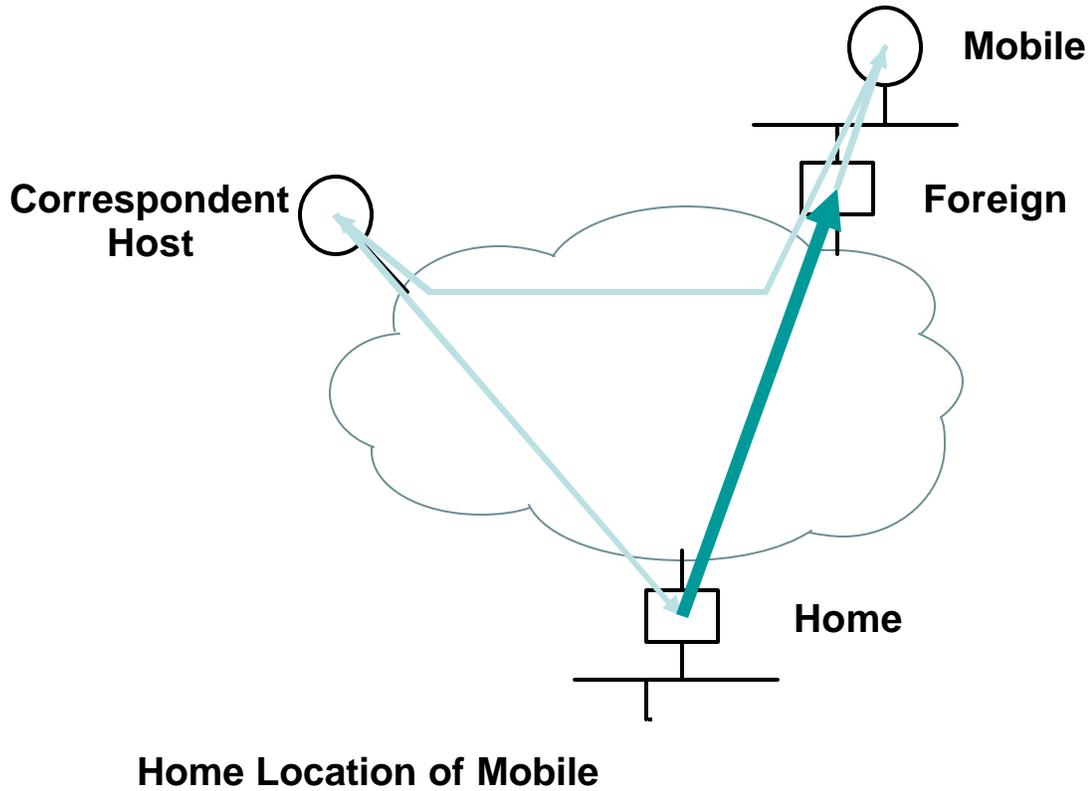
Hitachi:

- [Hitachi Internetworking](#) - Supports IPv6 in GR2000 product
- [NR60 Router](#) - Supported IPv6 since 1997 (dated)
- **IP Infusion:**
- [ZebOS Advanced Routing Suite](#) - Includes advanced IPv6 functions
- **Juniper:**
- [JUNOS](#) - Supports IPv6 in version 5.2 - Configuration guide
- **Multi-threaded Routing Toolkit (MRT):**
- [MRT-2.2.0a](#) - Developed by the University of Michigan
- [MRT at Sourceforge](#) - Latest version of MRT is here
- **Nortel Networks:**
- [Nortel IPv6 technology](#) - Information on IPv6 support

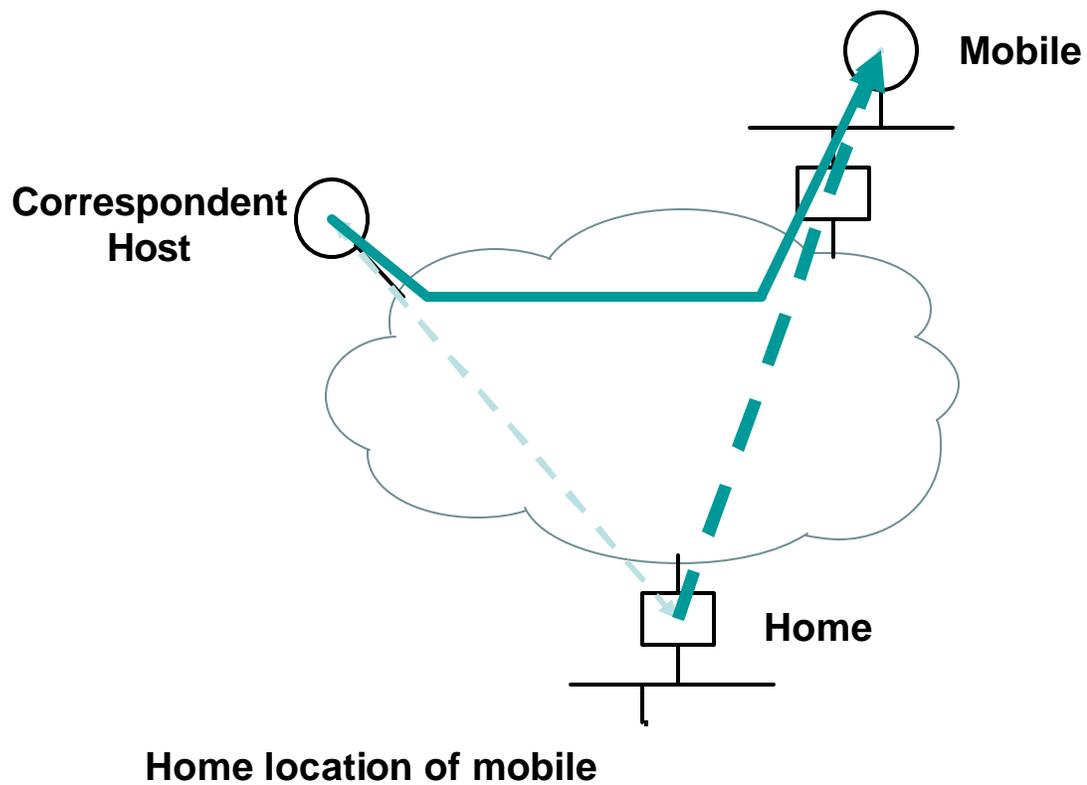
Zebra:

[Zebra](#) - GNU router product supports IPv6

Mobile IP (v4 version)



Mobile IP (Version 6)



NORTH AMERICAN NTT/VERIO IPv6 GATEWAY SERVICES



UNLEASH NETWORKS OF ANY SIZE OR SCOPE

Here's your opportunity to put NTT/VERIO IPv6 through its paces:

- NTT/VERIO has configured our network in the United States for IPv6 Gateway Services. All you need is an IPv6-capable router for your premises and you're able to connect to the world's only commercial-grade Global Tier One IPv6 Backbone operating in Asia, Europe, North America and Australia.
- Join over 500 NTT/VERIO customers already enjoying the limitless potential of IPv6 Gateway Services.
- Count on the strength, stability and experience of our Global Tier One IPv6 and IPv4 networks.

Take a Competitive Leap Forward with NTT/VERIO IPv6 Gateway Services

NTT/VERIO operates the world's largest tier one IPv6 backbone, spanning Asia, Europe, North America and Australia. Be on the forefront of technology in the United States with NTT/VERIO IPv6 Native, Tunneling, and Dual Stack Gateway Services.

THE FIRST LARGE-SCALE IPv6 SERVICE IN THE US

Our globally tested and proven NTT/VERIO IPv6 Native, Tunneling, and Dual Stack Gateway Services are now available on a commercial basis here in the US.

We have configured our network in the United States for NTT/VERIO IPv6 Gateway Services. All you need is an IPv6-capable router for your premises and you're able to connect to the world's only commercial-grade Global Tier One IPv6 Backbone operating in Asia, Europe, North America and Australia.

So get a major jump on your competition, and accelerate the future of IPv6 in the United States by choosing NTT/VERIO IPv6 Gateway Services.

WHAT IS IPv6 AND HOW DOES IT AFFECT MY BUSINESS?

IPv6 is a replacement for the current network layer IP protocol. The current IP protocol is version 4 and is now referred to as IPv4. IPv6 is short for IP version 6 and represents a significant change from the old IPv4 protocol.

IPv4 has some limitations, and it is to overcome these limits that IPv6 has been developed. The chief limit is that the address space IPv4 provides only allows for 4 billion nodes on the network, and with the global internet, this is rapidly becoming depleted. IPv6, in contrast, allows for 340 undecillion addresses; this is anticipated to be enough to accommodate future expansion of the network to include every electronic and electrical device in the world.

NTT/VERIO

NORTH AMERICAN NTT/VERIO IPv6 GATEWAY SERVICES

As well as the much larger network address space, IPv6 has other improvements over IPv4. A big problem for IPv4 network administrators is the chore of renumbering their entire network if they change ISPs. IPv6 embodies the concept of prefix propagation which makes renumbering entire networks considerably easier. IPv6's addressing includes more flexible support for mobile computing devices (laptops, PDAs, cellphones, wristwatch computers, GPS tracking devices, etc) and supports automatic transparent address reconfiguration while the device is in use. There is also better support for secure communications. And, IPv6 improves on QoS support, allowing applications which are dependent on specific delivery characteristics (e.g., voice over IP) to request and obtain the characteristics they need.

IPv6 is designed to eventually replace IPv4. During the transition, IPv6 and IPv4 will co-exist, with traffic steadily moving to IPv6.

TEAM WITH THE RECOGNIZED LEADER

All NTT/VERIO IPv6 US customers are fully supported by our highly experienced IPv6 engineers. How experienced? We and our parent company, NTT Communications, have been on the forefront of IPv6 development and implementation worldwide since 1996. The timeline on the back page highlights some of our more significant milestones.

After all, the move up to IPv6 might be a big step, but with NTT/VERIO's global expertise and infrastructure on your side, there's no reason for it to be a risky one.

Verio is a leading provider of global IP solutions and one of the world's largest operators of Web sites for businesses. We are a wholly owned subsidiary of NTT Communications, part of the largest and most financially secure telecommunications company in the world.

There are currently over 500 customers around the world enjoying the benefits of NTT/VERIO IPv6 Gateway Services. They have chosen to team with a company that's been directly involved with the development and deployment of IPv6 technology since 1996.

The company that the World Communication Awards recognized as having the Best Technology Foresight for its work in the field of IPv6 (in addition to offering the Best Carrier Service in Asia-Pacific). The company that Boardwatch magazine recognized for excellence in customer service and customer satisfaction.

NTT/VERIO

NORTH AMERICAN NTT/VERIO IPv6 GATEWAY SERVICES

NTT/VERIO IPV6: EXPERIENCE THAT STRETCHES FROM THE RESEARCH LAB TO GLOBAL TIER ONE BACKBONE DEPLOYMENT

- **1996** NTT Labs started one of the world's largest global IPv6 research networks.

- 1997** CICNet and NWNnet, later acquired by Verio, started operating major nodes of 6bone.

- 1998** Verio began participating in PAIX native IPv6 IX.

- 1999** NTT Communications obtained sTIA registry from APNIC.

- 1999** NTT Communications began IPv6 tunneling trial for its domestic ISP "OCN" customers in Japan (200 trial customers).

- 2000** Verio obtained sTIA from ARIN.

- 2000** NTT MCL established the world's first commercial IPv6 IX in San Jose.

- 2001** NTT Communications plays key roles in Japan's National Project "IPv6 Home Appliance Trials."

- 2001** NTT Communications began commercial IPv6 services.

- 2001** NTT Communications participated in European Union "6net" Project.

- 2001** NTT/VERIO Global IPv6 Backbone in place.
 - > The world's first commercial quality Asia-US-Europe IPv6 backbone.
 - > 24x7 monitoring and operation by both NTT Com NOC in Japan and Verio NOC in US.

- 2001** Global IPv6 Gateway Service offered — native IPv6 global transit for ISP, ASP and IDC.

- 2001** IPv6 Tunneling Service for OCN — IPv6 over IPv4 tunneling service for IPv4 dedicated address services.

- 2002** IPv6 Dual Service for OCN — both IPv4 and IPv6 service is available to customers.

- 2002** Verio receives Boardwatch magazine's prestigious Service Provider Excellence Award for customer service and support.

- 2002** NTT Com receives two World Communications Awards — Best Technology Foresight and Best Carrier, Asia-Pacific.

- 2002** NTT MSC began commercial IPv6 services in Malaysia.

- 2003** NTT Europe began IPv6 commercial services in Europe.

- 2003** NTT Korea, NTT ComAsia, NTT Taiwan and NTT Australia began IPv6 services.

- 2003** NTT/VERIO IPv6 Pre-Commercial Service in the United States.

- 2003** NTT/VERIO IPv6 Commercial Service in the United States.

TO LEARN MORE ABOUT PUTTING THE IPV6 SOLUTIONS TO WORK FOR YOU, CONTACT ONE OF OUR CONSULTANTS AT 1-800-438-8374 OR VISIT www.verio.com.

NTT/VERIOVerio and the Verio logo are trademarks and/or service marks of Verio Inc. in the United States and other countries. All other names are trademarks or registered marks of their respective owners. ©2003 Verio Inc. All rights reserved.