

IPv6 - Coexistence and Integration with Next Generation Networks

Pradeep Monga

Ishtiaq Ahmed

Indranil Gupta

*Faculty of Computer Science
Dalhousie University
{monga,ishtiaq,igupta}@cs.dal.ca*

1. Introduction

The basic rationale behind IPv6 development was to provide an extended address space so that the growing future networking needs could be fulfilled. The uninterrupted progressive growth of the global internet requires that its overall architecture evolve to accommodate new technologies, to support the growing number of users, applications, appliances and services [1]. Among IPv6's unique benefits over IPv4 are increased address space, simpler "plug and play", network security, improved mobility and Quality of Service. These benefits are mutually interrelated. Increased address space lets networks globally address more and new types of devices, and removes the need for Network Address Translator (NAT). This provides host-to-host IPsec and allows other novel services to run within network previously hidden behind NAT. IPv6 was intended to be an evolutionary approach to global internet as opposed to a revolutionary approach. In IPv6 approach the existing IPv4-based technologies are integrated to form a unified whole. In response to the increasing address need, IPv6

has been developed to provide an extremely large number of addresses, guaranteeing supply well into the future [4, 7].

2. Problem Definition

In the future, internet networks are expected to use IPv6 rather than IPv4. This is mainly due to the limitations of IPv4 in terms of addresses, routing and security. Since a huge amount of sub-networks are already installed for the IPv4, it is difficult to imagine ISPs starting deploying the IPv6 without some assurance that old legacy networks will still be able to connect to the internet. The expected transition phase between IPv4 networks to IPv6 will certainly need some set of mechanisms to insure a transparent communication bearing the two protocols. We believe that a variety of methods will coexist until a global unique IPv6 network will dominate. These mechanisms vary in their complexity and may in some cases violate the usual end-to-end Internet model by using application level proxies like firewalls and network address translators (NAT) [7].

In what concerns IPv6 deployment, any interconnection mechanism where IPv6 and IPv4 networks can be separated, but where IPv6 and IPv4 applications can transparently exchange information should be welcomed. We can consider the challenge of introducing IPv6 from two angles. First, when introducing IPv6 to an existing IPv4 infrastructure, we must have transitioning mechanisms that enable the protocol's seamless introduction, minimizing any impact on existing network users. Second, when introducing a new IPv6 network, we clearly must ensure that all components (network devices, host operating systems, applications, and so on) support the new protocol [3].

3. Coexistence Strategies

Focussing on the primary goal, to enable IPv6 applications on hosts to communicate, many network designers recommend deploying IPv6 at the edge first, where the applications and hosts reside, and then moving towards the core to reduce the cost. Also, the migration of IPv6 into the edge or user site is relatively easier, as major operating systems are already IPv6-capable.

Several Important Transition mechanisms are discussed in the following sections [1]:

3.1 Dual-stack backbones

The dual IPv4/IPv6 stack is very important and most straight forward transition

mechanism. This technique allows IPv4 and IPv6 applications to coexist in a dual IP layer routing backbone. All routers in the network need to be upgraded to be dual-stack, with IPv4 communication using the IPv4 protocol stack and IPv6 communication using the IPv6 stack. This method is currently used in the early phase of the transition. On the network side, implementation of the dual stack, like, GGSN is vital to enable both IPv4 and IPv6 access points and to perform IPv6 in IPv4 tunneling. In addition, the edge router at the border of the operator's IP network and the public Internet should also be a dual stack router [2]. Mobile terminals need dual stacks in order to access both IPv4 and IPv6 services without additional translators in the network. Besides, an IPv4 address has to be allocated for all equipments. Routers must be configured for the two protocols and IPv4 applications must be slightly modified and recompiled to be adapted to the IPv6 API.

3.2 IPv6 over IPv4 tunnels

Tunneling tools aim at to simplify IPv6-to-IPv6 communication both within and between sites. Such tools will be very important in IPv6's early deployment period, as network operators can use intra-site tools to test IPv6 before full site migration and inter-site tools to obtain connectivity to other IPv6-aware sites across the IPv4 Internet. These tunnels encapsulate IPv6 traffic within IPv4 packets and decapsulate at the other end, and

are meant primarily for communication between isolated IPv6 sites. Tunneling requires dual IPv4/IPv6 stack functionality in the encapsulating/decapsulating nodes. In configured tunneling, the endpoint of the tunnel is manually configured to a certain IPv4 address. In automatic tunneling, the encapsulation is done automatically in the encapsulating router/host, and the tunnel endpoint IPv4 address is included in the IPv6 destination address of the packet. An example of such a tunneling mechanism is so-called 6to4 tunneling. Other techniques include generic routing encapsulation tunnels, semiautomatic tunnel mechanisms such as tunnel broker services, and intra-site automatic tunnel addressing protocol (ISATAP) for the campus environment. The aim of this mechanism is at connecting IPv6 hosts/routers within IPv4 networks when there is no IPv6 backbone provided by the ISP (Internet Service Provider). This is an easy scenario for network managers who want to get familiar with IPv6 technology.

3.3 Protocol Translation Mechanisms

None of dual-stack and tunneling mechanisms works for communication between an IPv6-only node and an IPv4-only node. Such communication requires a translation mechanism either at the network, transportation, or application layer. A variety

of IPv6-to-IPv4 translation mechanisms are available, which are as follows:

- NAT-Protocol Translation (NAT-PT),
- TCP-UDP relay,
- Bump-in-the stack (BIS),
- SOCKS- based gateway

These protocols translation mechanisms become more relevant as IPv6 becomes more prevalent, and as IPv6 becomes the protocol of choice to allow legacy IPv4 systems to be part of the overall IPv6 network. NAT-PT is required to allow communication between applications using IPv4 and those using IPv6. The SOCKS based IPv4/IPv6 gateway mechanism is based on a mechanism that relays two “terminated” IPv4 and IPv6 connections at the application layer. The translation mechanisms tend to fall into two categories; those that require no change to either the IPv4 or IPv6 hosts and those that do. An example of former is the TCP-UDP relay mechanism that runs on a dedicated server and sets up separate connections at the transport level with IPv4 and IPv6 hosts, and then simply transfers information between the two. An example of the latter is the BIS mechanism that requires extra protocol layers to be added to the IPv4 protocol stack.

4. New research on IPv6 Coexistence

We have already discussed a number of well-accepted and proven ideas for the coexistence of IPv6 and IPv4. It is reasonable to assume that a variety of mechanisms will exist until the migration from IPv4 to IPv6 is completed. Routers and hosts in the global network encounter multiple cases where the need for efficient coexistence methodology is still being felt very frequently. The new techniques dedicated in this task have common goal of improving performance rating in the complex issues including routing, DNS, error handling, etc. The basic ideas like tunneling and dual stack are now getting more dynamicity and robustness leaving behind the

inherent weakness. In this section we will discuss some relatively new strategies developed in this purpose.

4.1 DTTS – Dynamic Tunneling Transition Solution

DTTS [5] is designed mainly to provide transparent end-to-end IP communication between IPv4 and IPv6 nodes, to enable scalable deployment of IPv6 and at the same time to offer seamless service of IPv4 based applications in IPv6 networks. As this is mainly IPv6 based method, each host in the IPv6 network has dual stack facility. Border routers also support dual stack and work as connector between two generation networks. Figure 1 depicts the network architecture for DTTS deployment.

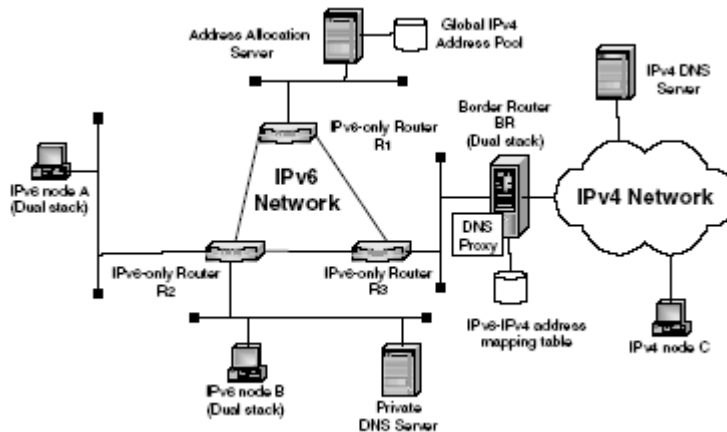


Figure 1: Components in DTTS

The tunneling method dynamically encapsulates IPv4 packet into IPv6 packets and continues the flow over the network.

Border routers serve as the tunnel end points. They forward the packet in the destination network. For a packet to run from IPv6 to

IPv4, border router decapsulates the tunnel header of the packets and forward them to the IPv4 network. In case of the reverse scenario, when border router receives the IPv4 packets to transmit into the IPv6 network, it encapsulates them with IPv6 header and forwards toward the destination. Whether the address type is private or public IPv4, dynamic tunneling only allows IPv6 packet over the network and so reduces network management issues. Dual stack facility in each host gives the ability to run an IPv4 application on them. Dynamic tunneling also allows communicating between two hosts for an IPv4 application even though they remain in the v6 network.

4.1.1 Dynamic Tunneling and Hosts' Address Allocation

Each host has a private IPv4 address to run IPv4 application. An Address Allocation Server (AAS) can help in dynamically allocation such address. Each interface can contain multiple IPv6 address like link local address, site local address and aggregatable global unicast address. In DTTS each host is assigned an IPv4-compatible address which is used for IPv6-IPv6 communication. A site local address is used for IPv6-IPv4 transfer or IPv4-IPv6 scenario.

The system is entitled 'dynamic tunneling' as unlike traditional tunnelling it need not know the tunnel endpoint address before setting up the tunnel. In this way, it

improves scalability and flexibility features in the network.

4.1.2 Different kind of tunneling scenario

a. Host-to-host tunneling: This is used during transfer of an IPv4 packet between two IPv6 hosts. As each host is assigned an IPv4 compatible address, the receiver host need to just pad 96 bit zeros before the 32 bit IPv4 address and pass it through the network.

b. Host-to-router tunneling: It happens when IPv4-IPv6 or IPv6-IPv4 communication is needed. At the sending host of IPv6 network, the host transforms the destination address as an IPv6 site local address. The source address is just the site local address of the host and destination address is constructed by putting 32 bit zero and 32 bit IPv4 address in the last 64 bit. Site local address prefix (FEC0) is in the both case. The merit of this method is that, sender does not need to determine the tunnel end point. The packet just traverse like a normal IPv6 packet until it reaches one of the border routers.

c. Router-to-host tunnelling: This scenario occurs subsequently after the previous scenario. The router receives the tunnelled packet and determines the destination IPv6 address. The destination address is determined by the 'IPv6-IPv4 address mapping table' maintained by the

border router. The source is the router's own site local address.

4.1.3 DNS and ICMP issue

Generally, IPv4 address mapping are held as 'A' records and IPv6 records are taken as 'AAAA' or 'A6' records in DNS server. In DTTS, the BIND server which is a private DNS server is a dual stack IPv6 node. It resolves both private and public IPv4 and IPv6 DNS queries. For the IPv6 to IPv4 and IPv6 to IPv6, there is no need to special DNS handling as IPv4 applications use private DNS resolver library to do this over IPv6.

But when a request for an IPv6 host from an IPv4 network comes, it is resolved by consulting AAS for the pool of public IPv4 for the IPv6 nodes.

In case of ICMP error messages, if it is generated outside the tunnel, it is treated as normal IPv4 packet. In case of IPv6-IPv4 and vice versa scenario and if the message is generated in the IPv6 network, the tunnel entry point converts it to ICMPv4 and in the second case the border router does the conversion task.

4.2 SIIT

This method resembles like the NAT (Network Address Translation) in IPv4 to exchange a private IPv4 to public IPv4 address. But, SIIT protocol does not ease in applications sending addresses like FTP and RTP. Some application level gateways acting

as proxies are needed in that case. If an IPv6 host in IPv6 network wants to communicate with an IPv4 host, it uses an automatic address allocation from the dual stack. Router administers both routing tables. It is a one way translation. So outside IPv6, IPv4 hosts cannot commence a communication.

4.3 NAT-PT

NAT-PT provides transparent end-to-end [6] solution. A collection of IPv4 addresses are reserved at the boundary to provide IPv4 address to any IPv6 host when a packet needs to leave the boundary. This proposal allows both way address translation as the transition context is done by the DNS. But it carries the problem of applications sending IP addresses in the payload.

4.4 AIIH

The AIIH proposal [6] combines DHCPv6 and DNS to provide transition from IPv6 to IPv4 and vice versa. It is also complementary to SIIT and NAT-PT [6]. It focuses on network topology when both type of network exist in the same domain. DHCP is used in this method which does the task of assigning temporary IPv4 address to an IPv6 host. On the other hand, the task is more difficult when an IPv4 host wants to talk with an IPv6 host. There is no protocol currently available to do such automatic assignment [6]. The weakness of this method is two fold. First, the routers need to be configured for

both networks. Again, assigning IPv4 is difficult due to frequent change of network topology.

5. IPv6 deployment in next generation networks

It is imperative that the next generation IPv6 networks must support current IPv4 format since IPv4 networks will exist for quite a number of years before it can be totally transformed into IPv6 network connectivity. The future networks will be mostly wireless mobile networks seamlessly connected to the internet each having a unique IP address of its own. Current IPv4 technology is unable to resolve this unique addressing issue and client reachability information. Thus it is necessary to deploy IPv6 for a necessary solution.

5.1 IPv6 support on MPLS Networks

Multiprotocol label switching (MPLS) is a flexible solution for addressing present-day network problems speed, scalability, quality-of-service and traffic engineering. It can exist over existing asynchronous transfer mode (ATM) and frame-relay networks and remains independent of the Layer-2 and Layer-3 protocols. The paper [9] emphasizes on the IPv6 support on MPLS architecture for future networks using the Protocol Tunnel technique

or '6PE technology'. In MPLS, data transmission occurs on label-switched paths (LSPs). The labels are distributed using label distribution protocol (LDP), RSVP. An LSR is router device in the core of an MPLS network that participates in the establishment of LSPs. A Label Edge Router (LER) is a device that operates at the edge of the access network and MPLS network.

IPv6 support on MPLS network can be classified under following deployment strategies [9,1].

- IPv6 using tunnel on Customer edge routers: Has the advantage that it can be deployed over the current infrastructure easily and requires dual stack CE routers.
- Circuit transport over MPLS: can be used by providers having ATM or Ethernet links to CE routers can use this but it needs layer 2 transport layer over MPLS
- 6PE model: only extend the edge LSR's (LER) for IPv6 compatibility and the rest IPv4 routing & signaling should be on done on core LSR's
- IPv6 MPLS VPN's to 6PE: We extend the routing and signaling protocols on all LSR's for IPv6 support and adding IPv6 MPLS VPN to 6PE. It requires software upgrades for PE routers.

- Native IPv6 MPLS based backbone: All the LSR's are allowed to support IPv6 completely.

5.1.1 6PE model

The paper [9] examines the characteristics of the 6PE model by implementing it in the MPLS research platform AYAME.

In this model the IPv4 packets transit the MPLS network through the LSP's. The LSP's are setup by the IPv4 routing and signaling mechanism. In the second phase BGP session is established between edge LSR's using IPv4 through the LSP's and the routing information in IPv6 is carried by MP-BGP. The BGP next hop attribute for the IPv6 route information is the IPv4 mapped IPv6 address of the router. When an LSR receives an IPv6 route, the LSR uses IPv4 IGP route table to look for the next hop.

This model provides minimal change needed for the transition from IPv4 to IPv6 over the existing MPLS network. Thus it is the most realistic model for supporting the IPv6 on MPLS at the current situation. In the future, MPLS signaling protocol must be able to handle the IPv6 addresses exhaustively. Although the Label Distribution Protocol

already addresses this issue but the IPv6 specification does not match with the IPv6 routing information. This is the problem that is to be resolved in the days to come.

5.2 Transition to IPv6 in GPRS and WCDMA Mobile Networks

5.2.1 Mobile IPv6

Mobility is an important feature supported in IPv6 networks [11]. The problem is if a station moves it must change its IP but then it would change its ID that uniquely identifies the terminal. So as a solution there are two IP numbers static one called 'home address' and a variable one called 'care of address'. Each mobile node is identified with its home address stored by its 'home agent'. After attaching itself to another network the mobile host first binds to home agent it sends a binding update, to which the home agent sends a binding acknowledgement and thus 'bind'. When another host tries to connect to the mobile host it transmits to the home address of mobile host in turn the home agent takes the packet and starts tunneling to the mobile host the mobile host transmits direct back. Now the mobile host sends a binding update to the host and packets are transmitted directly to the 'care of address' of the mobile host.

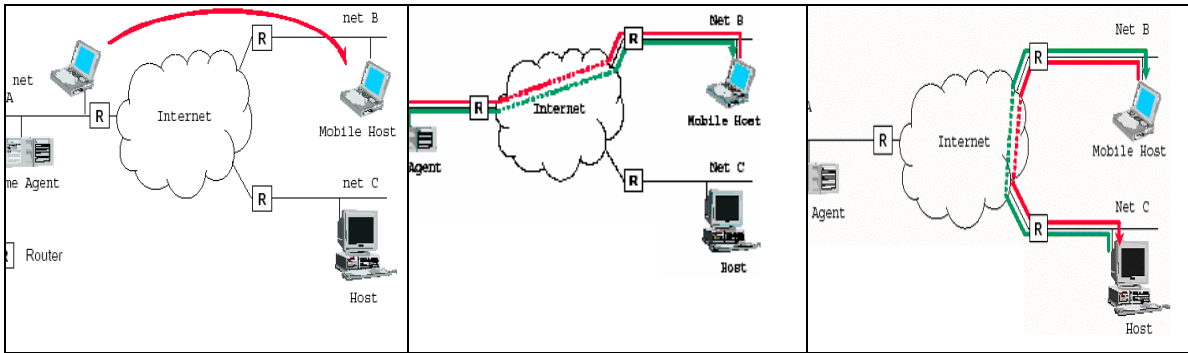


Fig 3. Address binding in mobile IPv6 network

Mobile IPv6 avoids triangular routing of packets via the home address thus reducing delay and increasing performance. The address auto configuration (stateless and stateful) of IPv6 [11] simplifies the care of address assignment for mobile node. In stateless auto configuration the addresses are assigned by Gateway GPRS Support Node in the mobile network whereas in stateful auto configuration, external DHCP servers assign addresses.

Mobile IPv6 can be used by the terminals having non cellular interfaces like WLAN when they need to maintain session while moving from different transition technologies. Moreover, mobility can also be achieved by technologies like GTP (GPRS Tunneling Protocol) in GPRS and WCDMA networks.

5.3.2 IPv6 in GPRS and WCDMA networks

IPv6 is standardized by IETF as a support for GPRS/WCDMA mobile networks and terminals. The Global System for Mobile

Communication (GSM) networks uses the General Packet Radio Service (GPRS) technology (2.5 G networks) for packet switched IP services. GPRS is an extension of the GSM network that enables data packets to be transmitted at high speed [11, 10]. The network offers virtually instantaneous connection. Each GPRS core network consists of Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN) network elements.

Moreover, The Wideband Code Division Multiple Access (WCDMA) in 3G networks (3G Partnership Project) [10] aims to provide packet-switched data to a mobile terminal with high data speeds. GGSN elements in GPRS core network are needed to be updated for transition from IPv4 to IPv6 since they have to support the IPv6 services.

Three strategies can be used for the transition.

- Dual IPv4/IPv6 stack: Dual stacks in edge routers, GGSN elements to enable IPv6 in IPv4 tunneling. Mobile terminals too need dual

- stacks for IPv4/IPv6 service access without additional translators.
- Tunneling: Requiring the encapsulation and decapsulation capabilities on terminal nodes.
 - Translators: Its use is transparent to the mobile terminals. The Network Address Translator – Protocol Translator (NAT-PT) is used during Header Conversion, most important translation mechanism.
 - User IP Layer: It is the application layer having the protocol stacks.
 - Network Model: This demonstrates the mobile terminal connection to the GPRS core network. Packet Data Protocol (PDP context) is the connection between mobile terminal and GGSN access point as shown in the figure. The IP address of the mobile is assigned by it.

As per the report [11], three transition scenarios can be considered:

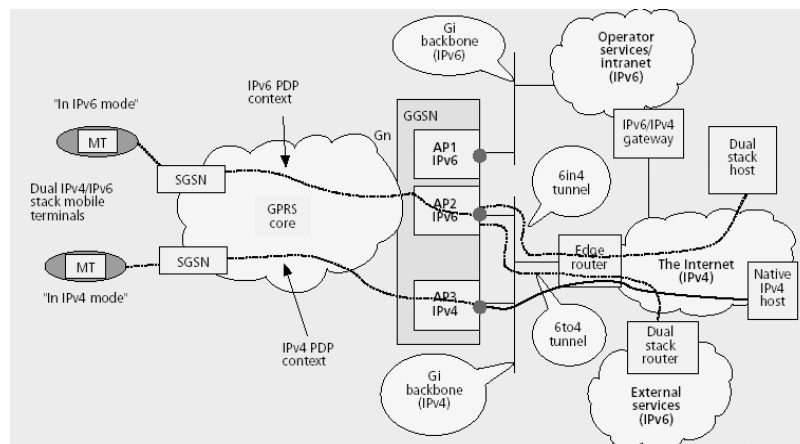


Fig 4. MT connection to the GPRS core and network connection

Access Point AP1 [11] is connected to all IPv6 networks. Access Point AP3 is connected to all IPv4 networks and provides a service to them. AP2 provides IPv6 connection through IPv4 networks by tunneling (dotted lines). This may be of two types ‘6 to 4: where other end is an external IPv6

cloud’ and ‘6 in 4: where the other end is a dual stack host’.

- The Reference Network: NAT is used to map the private IPv4 addresses of the mobile terminals to public IPv4 addresses. IPv4 hosts can be reached through IPv4 networks, IPv6 hosts can be reached through IPv4 networks (tunneling) or IPv6

intermediate networks to IPv6 hosts. In tunneling the start point can be Mobile terminals (that support dual stacks), GGSN and edge routers whereas the end point being the host itself or the edge routers.

To define the design we can take some typical examples of transition scenarios [11]

- Native IPv4 terminal: IPv4 services are provided to all IPv4 terminals. NAT (in the operator network) is used for connecting a mobile terminal using a private address to the public IPV4 internet else in case of intranets nothing else is needed to be done.
- Dual Stack terminal: IPv6 packets from MT to host can be tunneled via IPv4 network or directly through IPv6 network through edge routers. When dual stack MT is connected to a native host the IPv4 is used.
- Native IPv6 terminal: It differs from the Dual stack in a way that IPv4 intranet also requires NAT-PT translator for access. Dual stack MT will enhance the functionality in this case since NAT-PT is not necessary that time.

Currently IPv6 services are gaining ground in applications like Voice over IP (VOIP), Wireless Application Protocol (WAP) and other real time mobile support applications

[11, 10]. So for the proper deployment in present network scenario, the following points should be always stressed upon as discussed earlier.

- Use of Dual IPv4/v6 stack in GGSN, edge routers and MT's
- Protocol translators NAT-PT for each operator network

6. Evaluation of coexistence strategies

In this section we will present a comparison scenario of different basic tunneling approaches in terms of some common metric. In general we can classify tunneling mechanisms in two broad class – host-to-host tunneling and router-to-router tunneling [8]. In a study in [8] it is found that the throughput is surprisingly better in host-to-host tunneling than simple IPv6 packet transfer mechanism! But the host-to-host mechanism incurs most CPU utilization other than IPv6 routing. Nonetheless, router-to-router has only 1%-7% data overhead over the top of IPv6 packets. The TCP latency for host-to-host tunneling (30 ms) is smaller than that of straight IPv6 (40 ms) and router-to-router tunneling (42) taking 64kb packet size. In terms of TCP connection time, host-to-host is the winner taking the least time where router to router comes out as worst in this case. In another experiment that counts number of client-server connection in a

second, all these three methods perform almost equally [8]. Router –to- router tunneling is slightly better though.

Apart from this, there are some indubitable criteria for evaluating transition tools in current time as well as in future times. The criteria should include but not limited to Scalability, Security, Performance, Functionality, Host and router requirements, IPv4 and IPv6 address requirements, application requirements, Ease of use and Ease of management [3].

7. Phases in transitioning from IPv4 to IPv6

The solution for the transitioning from IPv4 to IPv6 being followed is to incrementally deploying it in a phased manner. In the first phase, there are separate IPv6 islands in the network connected by IPv4 internet using automatic and/or configured IPv6 in IPv4 tunneling. Most IPv6 services provided to mobile users in this phase are in the operator network (intranet). Other mobile services, such as connection to an IPv6 corporate access network, are reachable by configured/automatic tunnels over the IPv4 Internet. In the Second phase, IPv6 is widely deployed and numerous services are implemented on the IPv6 platform. IPv6 is widely deployed but tunnelling is still sometimes needed since IPv6 Internet does not yet have full

connectivity. The pace of deployment of IPv6 has though increased because IPv6 deployment is already widespread. In the third phase, IPv6 has achieved a dominant position. IPv6 Internet has global connectivity, and all services work on IPv6 platform. No dual stack functionality or address or protocol translators are vitally needed in mobile networks [2].

8. IPv6 – issues concerning global deployment

It is substantiated from our discussion that IPv6 is definitely is a better choice for next generation networks. Still some factors exist which are holding the fast adoption of this method. Big names in communication industry have started releasing products that support IPv6. But still lack of user and an oscillating egg-hen phenomenon due to this reason is pulling back the rate of transition. Some other factors that directly influence the deployment process include higher cost of IPv6 product, new technicians and extensive effort needed for the purpose. Finally, IPv6 will not gain ground until the future technology products like PDA, wireless terminals and mobile devices are deployed extensively.

9. Conclusion

In this document, we have looked into some existing and future possible ways of incorporating IPv6 network protocol into

current networks and future generation networks. As a next generation protocol IPv6 is still a strategic issue and making its own scope in the global network system. This is obvious that IPv6 is not something that can change the way world runs in an overnight. It is experiencing its needs and at the same time research community is working on its perfection. That is why IPv6 is perfectly hailed as *evolutionary* not *revolutionary*. It is fairly acceptable to state that the world of communication is on its way to a matured and reliable network system through all these entailments.

References

- [1] Tatipamula M., Grossetete P, Esaki H., "IPv6 integration and coexistence strategies for next-generation networks", *Communications Magazine, IEEE, Volume: 42, Issue: 1, Jan. 2004 Pages: 88 – 96*
- [2] Wiljakka, J., "Transition to IPv6 in GPRS and WCDMA mobile networks", *Communications Magazine, IEEE, Volume: 40, Issue: 4, April 2002 Pages: 134 - 140*
- [3] Mackay M., Edwards C., Dunmore M., Chown T., Carvalho G., "A Scenario-Based Review of IPv6 Transition Tools", *IEEE Internet Computing, May - June 2003*
- [4] Lee D.C., Lough D.L., Midkiff S.F., Davis N.J., Benchoff P.E, "The next generation of the Internet: aspects of the Internet protocol version 6", *Network, IEEE, Volume: 12, Issue: 1, Jan.-Feb. 1998 Pages: 28 – 33*
- [5] Kai Wang; Yeo, A.-K., Ananda, A.L, "DTTS: a transparent and scalable solution for IPv4 to IPv6 transition", *Computer Communications and Networks, 2001.*
- [6] Afifi H., Toutain L., "Methods for IPv4-IPv6 transition", *Computers and Communications, 1999. Proceedings of IEEE International Symposium on, 6-8 July 1999 Pages: 478 - 484*
- [7] Hui Huang, Jian Ma, "IPv6 - future approval networking", *Communication Technology Proceedings, 2000. WCC - ICCT 2000. International Conference on, Volume: 2, 21-25 Aug. 2000 Pages: 1734 - 1739 vol.2 Proceedings. Tenth International Conference, 15-17 Oct. 2001 Page:248 – 253.*
- [8] Raicu I., Zeadally S., "Evaluating IPv4 to IPv6 transition mechanisms", *Telecommunications, 2003. ICT2003. 10th International Conference, Volume: 2, 23 Feb.-1 March 2003 Pages: 091 - 1098 vol.2*
- [9] Uda, S., Ogashiwa, N., Uo, Y., Shinoda, Y., "IPv6 support on MPLS networks: experiences with 6PE approach", *Applications and the Internet Workshops, 2003. Proceedings.*

2003 Symposium on, 27-31 Jan. 2003: Pages:
226 – 231.

[10] Worrall K.P., “The impact of IPv6 in wireless networks”, *3G Mobile Communication Technologies, 2001. Second International Conference. Pages 324-329.*

[11] Wiljakka, J., “Transition to IPv6 in GPRS and WCDMA mobile networks”, *Communications Magazine, IEEE, Volume: 40, Issue: 4, April 2002: Pages: 134-140.*
