A Path Towards IP-V6 Transition Strategies for Scientific Research: An Overview

M. Junaid Arshad, Amjad Farooq, S. Ahsan, M. Shahbaz, M. Aslam, Tanvir Ahmad

Department of Computer Science and Engineering, University of Engineering and Technology, Lahore
junaidarshad@uet.edu.pk

Abstract: This research work explores various aspects regarding the introduction and analysis of transition strategies to the Internet Protocol Version 6 (IP-v6). We firstly analyze the different ways of transition as of IP-v4 to IP-v6. These ways are not integral parts of IP-v6 itself, rather they have administrative nature or they reside on lower layers of ISO/OSI model. We give an overview of non-technical issues and layer-2 options (targeted to distinct types of organizations and networks) which will aid in implementing the transition strategies supporting the Internet Protocol Version 6 (IP-v6). We also present a transition roadmap for each of these strategies in terms of addressing scheme; layer-2 technologies; routing, application and tunneling protocols; security problems relevant to transition and network protocols. Moreover, a comparative analysis of these strategies are presented using different criteria such as scalability, methods used for transition to native IP-v6 connectivity, degree of deployment difficulty and others. We hope this work will be found useful by both network operators and designers, and will be used to design strategies for transition to IP-v6 protocol based on the presented strategies, or at least as a reference.
[M. Junaid Arshad, Amjad Farooq, S. Ahsan, M. Shahbaz, M. Aslam, Tanvir Ahmad. **A Path Towards IP-V6 Transition Strategies: An Overview.** Life Science Journal. 2012;9(1):599-602] (ISSN:1097-8135). http://www.lifesciencesite.com. 88

Keywords: BGP-Border Gateway Protocol; IP-v6; QoS-Quality of Service; VPN-Virtual Private Network

1. Introduction and Problem Statement

The most visible drawbacks of IPv4 (Perkins, 2002) in regard to current demand are insufficient security support and lack of end-to-end reach-ability. We will try to analyze these drawbacks in following sections by presenting arguments why they are harmful to different aspects of the current Internet growth. Some of these issues are as follows:

1.1 Address Space Shortage

The main reason why IP-v6 (Internet, 2001) was designed, the answer is because increasing scarcity of IP addresses (Srisuresh et al., 2001). With more and more organizations deploying NAT (Network Address Translation) (Rosenberg et al., 2003) as a measure to reduce this overhead, next generation application layer protocols which require end-to-end reach-ability and inherent security are harder to implement. Currently, it is clear that most of the predictions about when IPv4 address space will run out of allocate-table address prefixes were wrong.

The main reason why is that they primarily focused on density of address space population and not on how allocation process has changed over the years. Nowadays, the main constraint for Internet growth regarding address space is not its practical capacity, but rather overhead linked to allocation and assignment process. There is roughly 30% of address space left which can be used for allocation of global unicast IPv4 addresses to Regional Internet Registries (RIRs). In practice however, IPv4 address blocks are hard to get because of strict policies imposed by RIRs.

1.2 End-to-End Reach-ability

NAT (Rosenberg et al., 2003) is widely deployed on current Internet. This technique breaks the initial idea of Internet saying that every two hosts connected to Internet should be able to reach each other directly. This brokenness is being softened by using additional mechanisms such as proxy servers, protocol extensions such as NAT detection and NAT traversal added to software logic, but in fact they only add another level of complexity - for both users and programmers/protocol designers.

1.3 Ad-hoc Mobility

The presence of IP-enabled mobile devices is more and more frequent. Since network stack implementations cannot cope with IP address changes, support for mobility in IP protocol (Perkins, 2002) is needed. The Support for IP mobility in IPv4 protocol was retrofitted and this affects the possibility to deploy it. On the other hand, IPv6 protocol was designed with mobility support in mind (Johnson et al., 2003). The most serious problems of mobility support in IPv4 are the following:

1). No end to end reach-ability: The implementation of IP mobility in IPv4 would have to solve NAT traversal problem – this is too big obstacle compared to transition to IPv6 (Bi et al., 2007).

2). Not coherent with IP protocol features: The design of mobility support in IPv6 was built upon inherent features of IPv6 protocol (Deering et al., 1998) such as Neighbour Discovery (Narten et al., 1998), auto-configuration (Narten et al., 1998) and mandatory IPsec support, whereas in IPv4 it was not. This can bring some issues when implementing IPv4 mobility, mainly weaker security and greater complexity.

3). Lack of implementations: Mobility support for IPv6 has already (as of beginning 2005) (Johnson et al., 2003) working implementations of entities needed for IPv6 mobility. Some of these implementations are distributed with source code. Contrary to the state of mobility for IPv6, IPv4 mobility support can be found mostly in proprietary form made for specific deployment cases.

4). IPv4 mobility support mandates: This entity is necessary for mobile node to receive packets sent from its home-agent. On the contrary, in IPv6 mobility support, foreign agent is not necessary and thus infrastructure does not need to be upgraded in order to accept mobile IPv6 nodes.

5). IPv4 address space restricts (Report, 2002): The mobile IP deployment on a very large scale.

Efficiency: IPv4 stores data needed for routing a packet to destination node in one header. Format of IPv4 header (Perkins, 2002) has two main disadvantages - its length is not fixed and it contains Header checksum field which has to be recomputed on each router along the path to destination node. IPv6 solves this problem by splitting the data needed for routing into basic header and several extension headers (Deering et al,. 2003). The size of basic header is constant which should theoretically result in faster packet processing in hardware. IPv6 also pushes checksum computation to upper layer protocols.

Security: For mobility support, IPsec (Internet Protocol Security) support is crucial because mobile node needs to secure the maintenance of bindings with its Home Agent which represents them while its absence in home network (Johnson et al., 2003). IPv4 specification does not provide any reference to whether IPsec should be included in IPv4 stack implementation or not. In this sense, IPv6 specification is more demanding and security aware. Enhanced security in IPv6 also coheres with end-to-end reach-ability; because nodes are able to communicate without an intermediary who would provide realization of security services for them (e.g., IPsec gateway), they are able to indulge in end-to-end, authorized, tamper-proof, private communication (Narten et al,. 2001). IPv6 offers these services by specifying IPsec support as mandatory. It is important to note that although support for IPsec is mandatory in IPv6, it does not mean that any IPv6 implementation not doing IPsec extension headers processing is not compliant to basic IPv6 RFC documents (Deering et al,. 2003). Therefore there can be nodes implementing only small subset of IPv6 protocol without IPsec support.

2. Comparison of Transition Strategies

Although strategies presented in this section differ from each other they can be eventually modified and applied even to networks of different size than those on which these strategies were presented. Thus it is important to create a methodology for comparing the strategies in general. The methodology should provide information about how much effort will be needed to implement given strategy, what performance characteristics will it show, what services will be provided and how long it is sustainable to continue using this strategy.

Progress: Tunnel Broker strategy (Cisco, 2005) progresses slowly to the core and the transition to native connectivity are completed when it reaches core of the network. Similar approach was applied in IPv6 over MPLS Strategy (Rosen et al,. 1997), which makes transport of IPv6 packets without any form of layer 3 encapsulation possible first in the backbone network and at the same time it proceeds from CPE devices to the edge of native backbone.

In Tunnel mesh strategy, the upgrade of network into native one was done in all phases with the emphasis on providing IPv6 connectivity to end users. If ordering all described strategies according to the time when native connectivity was first deployed in backbone network, the list would be as follows:

- IPv6 over MPLS Strategy
- Tunnel Mesh Strategy
- Tunnel Broker Strategy

Scalability: Scalability of given system is usually defined as ability of a system to adapt to increasing number of input variables. This definition holds as well for a strategy.

The scalability of a strategy can be thought of in following terms:

- Network performance
- Limit of difficulty of administration

The first point conveys how overall performance of a network is to change when the strategy is implemented in increasingly bigger part of the network. Each step of a strategy could be taken into account but usually generic strategy can be divided into two stages - proliferation of interim means of transmission of IPv6 packets and replacement of these means by native IPv6 connectivity.

Estimation of scalability could be only done for the first stage because the limiting factors are not present in the second stage. For the second point, some

coefficient analogous to HD-ratio can be specified, which would reflect how much ”pain” will be endured by administrators when number of elements (tunnels, tunnel server, AAA servers, etc.) will grow above bound from which the coefficient would be computed (Durand et al,. 2001).

Dual-Stack Backbone versus 6-PE: Deploying IPv6 in MPLS network can be solved by one of following four proposals:

- Use manually configured (static) tunnels between PE routers by creating a” tunnel mesh”
- Deploy IPv6 natively in the whole backbone
- Upgrade whole signalling plane (P routers) to support IPv6
- Deploy 6PE

The idea behind 6PE technology was that most of MPLS operators would not be willing to perform upgrade of P routers, which constitute the core of MPLS network. The other reason is that by disrupting the service of the fast forwarding in the core, the operation of whole MPLS would be lowered.

The first option would create a” static tunnel mesh” between 6PE routers. Its negatives are apparent – first, its performance compared to common operation of MPLS packet transport is low.

Second, creating another layer of boundaries between PE routers would lead to additional layer of complexity, which could make debugging network problems very difficult, especially in dense MPLS cloud. Thus, deploying IPv6 in MPLS network by setting up static tunnels is far worst solution for deploying IPv6 in MPLS-enabled network because its scalability is very limited - static tunnels have very low performance limit.

The comparison of dual-stack operated backbone and 6PE regarding performance is such as that in middle-sized network, these solutions should prove equal. However, on large scale, MPLS could perform better because it will probably take an advantage in fast forwarding in the core of MPLS network. Also, 6PE is a lot easier to deploy - only PE routers need to be upgraded, compared to every router in the path when upgrading backbone to dual-stack.

Degree of Deployment Difficulty: In regard to deployment difficulty each strategy can be looked at from two points of view:

- How much difficult is to deploy the techniques used in individual steps of the transition
- Overall efficiency of a strategy

There can be another issue of technical difficulties when implementing transition strategy: Looking at IPv6 over MPLS strategy, it is very straightforward and painless strategy regarding 6PE deployment for networks already using MPLS in backbone network. However, it is not very reasonable to deploy MPLS in backbone just for the reason of transition to IPv6 using 6PE. In this case, this strategy will be technically difficult to implement.

Vicious Cycle: In most of the strategies described in this chapter it is presumed that customers will demand IPv6 connectivity by themselves which would start the next stage of transition strategy. While this might be true in some of the networks used for illustration of the strategies, in reality where ISP provides connectivity especially directly to end users, it is not likely the ISP will get big number of requests for IPv6 connectivity.

These obstacles cause kind of vicious cycle - until the users will be motivated they would not demand IPv6 connectivity from the providers and on the contrary, until providers will come up with technical solution users will not be motivated to proceed with transition. In order to make the transition to IPv6 as smooth as possible the providers should push native IPv6 connectivity to the edges of their networks because with the help of integral components such as auto configuration end users would not notice they are using IPv6 in ideal case. Therefore, the activity should be on provider’s side.

Transition to Native Connectivity: The goal of each transition strategy is not only to provide IPv6 connectivity to all nodes which actually make some use of it but rather to provide native IPv6 connectivity to all end nodes in the network capable of using it.

Clear winner in this category is IPv6 over MPLS strategy because it incorporates only very limited number of tunnels during the whole process of transition to IPv6 connectivity. As opposed from other strategies, there is no tunnel present in the backbone of the network in every step of the transition roadmap.

The Tunnel mesh strategy can be put on same level because their approach to transition of core of the network is almost the same, although Tunnel Mesh Strategy does not push the transition of the core much forward in list of steps needed to complete the transition.

The Tunnel Broker strategy keeps tunnels in the network longest of all described strategies, but this is merely result of assumptions imposed on the particular network type, on which the strategy was shown. On the other hand, it is at least designed so that transition from tunneled to native connectivity should be gradual.

Addressing Schemes: The addressing scheme used in Tunnel mesh strategy can be called” classical” because it tries to map addressing scheme to network topology as close as possible. This allows greater aggregation but less conservation. Since it is presumed that the ISP mentioned in this strategy will get subsequent prefix allocation of the same size as initial allocation, the degree of aggregation will decrease because e.g. in one POP there will be prefixes from

initial as well as subsequent allocation, which cannot be aggregated at the POP level. At highest level, the aggregation imposed by a RIR will be preserved, thanks to the way how RIRs allocate prefixes.

The IPv6 over MPLS Strategy (Awduche et al,. 1999) for addressing scheme construction is similar to that used in Tunnel Mesh Strategy because it also maps network topology to addressing scheme. The difference is merely in structure of the networks.

The addressing scheme constructed for Tunnel Broker strategy resigned on creating addressing scheme after 38th bit boundary. This decision was done mainly for two reasons – because of the transition technique used and also because of the assumption that the network will expand internally.

3. Conclusions

In the most of the current networks, the transition to IPv6 is yet to be accomplished on many fronts. Not only technical issues such as ISO/OSI layers or application-development perspective need to be refined but also administrative procedures for transition and business cases for IPv6 will have to be developed. This work aimed at both technical and strategic aspects of the transition.

At first, we have presented a motivation to the development of IPv6 protocol and transition to IPv6. We have also discussed basic concepts of IPv6, IPv4, OSI/ISO Model, and TCP/IP etc.

In the next, we have given an overview of non-technical issues and layer 2 options which will aid in implementing a transition strategy.

Finally, we have described several transition strategies, targeted to distinct types of organizations and networks. Each of these strategies was described in terms of addressing scheme, layer 2 technologies and network protocols. Also, a transition roadmap for each particular strategy was given. Moreover these strategies were compared using different criteria such as scalability, methods used for transition to native IPv6 connectivity, degree of deployment difficulty and others.

We hope this work will be found useful by both network operators and designers, and will be used to design strategies for transition to IPv6 protocol based on the presented strategies, or at least as a reference.

Acknowledgments

This research was supported by the Directorate of Research Extension and Advisory Services U.E.T., Lahore-Pakistan.

References

Perkins, C., Ed, IP Mobility Support for IPv4, RFC 3344, (August, 2002).

Internet Architecture Board, Internet Engineering Steering Group, IAB/IESG Recommendations on IPv6 Address Allocation to Sites, RFC 3177, (September, 2001).

Srisuresh, P., and Egevang, K., "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, (January, 2001).

Rosenberg, J., Weinberger, J., Huitema, C., and Mahy, R., STUN - Simple Traversal of User Datagram Protocol (UDP) Through NATs, RFC 3489, (March, 2003).

Johnson, D., Perkins and C., Arkko, J., Mobility Support in IPv6, RFC 3775, (June, 2004).

Bi, J., Wu, J., and Leng, X., IPv4/IPv6 Transitions and Univer6 Architecture, IJCSNS, Vol. 7, No. 1, (January, 2007).

Deering, S., and Hinden, R., Internet Protocol Version 6 (IPv6) Specification, RFC 2460, (December, 1998).

Narten, T., Nordmark, E., and Simpson, W., Neighbor Discovery for IP Version 6 (IPv6), RFC 2461, (December, 1998).

Narten, T., and Thomson, S., IPV6 Stateless Address Auto-configuration, RFC 2462, (December, 1998).

IPv4 Address Report, http://bgp.potaroo.net/ipv4/

Deering, S., and Hinden, R., Internet Protocol Version 6 (IPv6) Addressing Architecture, RFC 3513, (April, 2003).

Narten, T., and Draves, R., Privacy Extension for Stateless Address Auto configuration in IPv6, RFC 3041, (January, 2001).

Durand, A., and Huitema, C., The H-Density Ratio for Address Assignment Efficiency an Update on the H ratio, RFC 3194, (November, 2001).

Rosen, E., Viswanathan, A., and Callon, R., A Proposed Architecture for MPLS, Internet draft, (July, 1997).

Awduche, D., MPLS and Traffic Engineering in IP Networks, IEEE Commun. Mag., vol. 37, no. 12, 42-47, (December, 1999).

Cisco IOS Release 12.0 (7) T, MPLS Virtual Private Network enhancements, Cisco, (2005).

2/12/2012