

IPv4 to IPv6 Transition

1.0 EXECUTIVE SUMMARY

As expected, the major groups handling the inner-workings of the internet had announced on Thursday, 3 Feb 2011, that the final unassigned IPv4 address blocks have been handed over to the five regional internet registries (RIR) [ARIN]. This marks the official, albeit symbolic, end of IPv4 and the groups focused more on the future, IPv6, rather than dwindling in the past. This highlighted the urgent need for companies and organizations to move to a new system amid the ever increasing number of net-connected devices.

This paper explains and discusses the current transition mechanisms to IPv6 and their applicability to different network scenario. Also discussed is the evolutionary work being done in different IETF working groups to address new realities in the IPv6 deployment. Security and routing aspects are not discussed in this paper.

IPV4 TO IPV6 TRANSITION – APPROACHES AND CHALLENGES

1.1 IPv6 Standard Profile

DoD Information Technology Standards Registry (DISR) technical and standards based definition of interoperability requirements for IPv6 Capable Products, provides a reference point for selecting the protocols for IPv6 capable devices and supporting acceptable transition strategy to IPv6 [DISRIPV6]. IPv6 Standard profile requires support of Dual Stack to ensure interoperability with the IPv4-Only End Node. It defines several IPv6 capable product classes according to their architectural and functional role in an IPv6 network. The set of product classes defined herein as “End Nodes” are a range of devices that embody “Host” behavior as defined in RFCs; the set defined as “Intermediate Nodes” embody “Router” behavior. Specific product classes incorporate nuances about compliance with various RFCs appropriate to products of that class [DISRIPV6]. DoD has also published a generic test plan for conformance, interoperability and performance testing of IPv6-capable under different product class [DODIPV6TP].

1.2 Transition to IPv6 - Generic Approach

The long-established strategy for IPv6 transition depends on “IPv6 dominance”. In an IPv6-dominant network the preponderance of end nodes would be IPv6 Capable, all routers would be Dual Stack, and the majority of the traffic would be IPv6 [DISRIPV6]. Transition mechanisms are dependent on, deployment and architectural factors. These mechanisms include Dual Stack operation, configured and automatic tunneling and translation.

RFC 4213, Transition Mechanisms for IPv6 Hosts and Router, describes several general transition strategies. Mechanisms in this document are designed to be employed by IPv6 hosts and routers that need to interoperate with IPv4 hosts and utilize IPv4 routing infrastructures. A new resource record type named “AAAA” defined for IPv6 addresses [RFC3596] and IPv4 “A” record is used by the Dual Stack node to detect the IP version of the peer node. Configured or automatic tunneling is used for routing IPv6 over IPv4 routing infrastructure. RFC 2766, Network Address Translation - Protocol Translation (NAT-

PT1) specifies an IPv4-to-IPv6 translation mechanism through transparent routing to end-nodes in V6 realm trying to communicate with end-nodes in V4 realm and vice versa. This is achieved using a combination of Network Address Translation and Protocol Translation deployed at the exit node such as edge router or Layer 3 aggregator. Exit node assigns IPv4 or IPv6 address, depending upon the destination realm, to the incoming flow as though flow is originating from it. It interconnects the incoming flow to outgoing flow through Application Level Gateways to translates IP address embedded within the application payload. RFC 2765, Stateless IP/ICMP Translation Algorithm (SIIT), provides translation between IPv4 and IPv6 packet headers (including ICMP headers) in separate translator "boxes" in the network without requiring any per-connection state in those "boxes". This algorithm can be used as part of a solution that allows IPv6 hosts, which do not have permanently assigned IPv4 addresses, to communicate with IPv4-only hosts. IPv4 source address is converted to IPv6 source address using IPv4-mapped prefix (::ffff:0:0/96) and IPv4 destination address is converted to IPv6 destination address using IPv4-translated prefix (0::ffff:0:0/96). IPv6 source address is an IPv4-translated address then the low-order 32 bits of the IPv6 source address is copied to the IPv4 source address. Otherwise, the source address is set to 0.0.0.0. IPv6 packets that are translated have an IPv4-mapped (IPv6 prefix: ffff: 0:0/96) destination address.

RFC 5969, IPv6 Rapid Deployment on IPv4 Infrastructures (6rd2), defines an IPv6-IPv4 mechanism in which IPv6 traffic to or from can be ensured to traverse a gateway node (e.g. ISP gateway). Service Provider selects an IPv6 prefix to be use in 6rd domain. The 6rd delegated prefix for use at a customer site is created by combining the 6rd prefix and all or part of the customer edge (router) IPv4 address. From these elements, the 6rd delegated prefix is automatically created by the customer edge router for the customer site when IPv4 service is obtained. This 6rd delegated prefix is used in the same manner as a prefix obtained via DHCPv6 prefix delegation [RFC3633].

1.3 IPv6 Support in Enterprise Network

RFC 4852 – IPv6 Enterprise Network Analysis – IP Layer 3 focus, provides analysis of the transition to IPv6 Enterprise Network Scenarios [RFC4057]. Enterprise networks are characterized as having multiple internal links and one or more router connections to one or more Providers, and as being managed by a network operations entity. A transition strategy in such an environment should consider IP-capability of the end points (Application/OS), IP capability of the enterprise 'network segment' end point is connected to, and IP-capability of service provider network. Typically enterprise will upgrade its network segment wise and all end points (hosts) OS and middleware will also be upgraded together. However, Dual Stack operation will be needed on enterprise service nodes during transition. Coexisted IPv4 and IPv6 network (i.e. parallel IPv6 infrastructure) can we implemented using VLANs [RFC4554]. Enterprise proxy/firewall will implement site specific IPv6 security policies.

1.4 IPv6 Support in Packet Centric Wireless Networks

RFC 4215, Analysis on IPv6 Transition in Third Generation Partnership Project (3GPP) Networks, analyzes different transition scenarios and applicable transitions mechanisms in 3GPP packet networks to IPv6. In a Dual Stack UE scenario, it recommends to activate an IPv6 PDP context when communicating with an IPv6 peer node and an IPv4 PDP context when communicating with an IPv4 peer node. If the 3GPP network does not support IPv6 or IPv6 PDP contexts, and an application on the UE needs to communicate with an IPv6 (-only) node, the UE may activate an IPv4 PDP context and encapsulate IPv6 packets in IPv4 packets using a tunneling mechanism. Tunneling mechanisms can be configured tunnel or auto tunneling options such as [RFC 5214 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)], [RFC5969]]. When UE is not a Dual Stack UE (IPv6-only), it will always activate IPv6 PDP context and tunneling of IPv6 traffic through IPv4 (-only) segment of the routing path is handled by the network.

¹ Translation based on RFC 2766, Network Address Translation – Protocol Translation (NAT-PT) has been rendered *Historic* by the publication of RFC 4966 primarily for security concerns.

² IPv6 Rapid Deployment

Dual stack implementation requires management of both IPv4 and IPv6 networks, and one approach is that "legacy" applications keep using IPv4 for the foreseeable future and new applications requiring end-to-end connectivity (for example, peer-to-peer services) use IPv6. Due to this reason IPv4-only UE connecting to an IPv6-only UE will be a very common scenario in the 3GPP network. However, this will require either generic-purpose translator (e.g. SIIT [RFC2765], NAT-PT [RFC2766]) in the local network or specific-purpose protocol relays/proxies (e.g. IPv6-to-IPv4 Transport Relay Translator [RFC3142]) in the local network or in the foreign network. Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers is being defined by the IETF Behave working group. Stateful NAT64 translation allows IPv6-only clients to contact IPv4 servers using unicast UDP, TCP, or ICMP. This also avoids the pitfalls (DNS-ALG) that doomed NAT-PT.

1.5 Dual Stack – A Challenge

Dual Stack is core to any transition strategy. This condition can be met with the Dual Stack operation on the platform and dual stack support in the application or via translation method internal to the node or provided in an external translation device [DISRIPV6].

However, dual stack may not be feasible for some network deployments (e.g. broadband access, large enterprise networks) since requirement of routable IPv4 address space to support large numbers of Dual stack nodes. There is significant new effort is in progress in the IETF IPv6 Operations (v6ops) working group to define viable alternatives for interconnecting IPv6 Nodes with legacy IPv4-only Nodes.

IETF Softwire working group is chartered to develop the Dual-stack Lite (DSlite) solution (draft-ietf-softwire-dual-stack-lite). DSlite is primarily targeted for broadband service providers to quickly transition to IPv6. DSlite defines two elements namely B4 (Basic Bridging Broadband) and AFTR (Address Family Transition Router). B4 is located in the customer premises in dual stack capable home gateway or customer device such as desktop. An AFTR element is the combination of an IPv4-in-IPv6 tunnel endpoint and an IPv4-IPv4 NAT implemented on the same node and located in service provider network. B4 and AFTR are connected through point-to-multipoint IPv4-in-IPv6 tunnel. In order to setup IPv4-in-IPv6 tunnel, B4 discovers AFTR IPv6 address using DHCPv6 option (ietf-softwire-ds-lite-tunnel-option). IPv4 traffic from home network is forwarded by B4 element to AFTR. IPv6 traffic from home network is forwarded using IPv6 routing table.

1.6 Enabling Application for IPv6

Any transition strategy has to also consider the transition of applications. Applications have to be upgraded to support coexistence of IPv4 and IPv6, Dual Stack operation and eventually IPv6-only. RFC 4038, Application Aspects of IPv6 Transition, specifies scenarios and aspects of application transition. However, one has to consider and exploit the application operating environment such as platform (Operating System, Middleware, Control protocol, Management support), intended use and deployment before adopting one approach over the other. Most of the operating systems provide IPv6 support natively. However support for other tunneling and translation mechanisms to realize transition strategies is still lacking and being made available on demand by the OS vendors.

2.0 SUMMARY

Dual Stack operation, 6-to-4 tunneling and 6-to-4 translation are the key elements of IPv4 to IPv6 transition mechanisms. Implementations of these elements in IPv6 products are dependent on, deployment and architectural factors. Vendors and network operators should consider transition of applications, control plane and IP transport in forming transition strategy. When IPv6 assumes dominance, supporting sparse IPv4 networks and legacy services should also be considered.

3.0 ABOUT HSC

HSC provides professional services in IPv4 and IPv6 Network transition, Co-existence of IPv4 and IPv6 nodes and mobility across IPv4/IPv6 networks. HSC focuses in Metro and Broadband Access (Wireless – 802.11, 802.16, 3GPP, LTE, satellite; Wireline – FTTx, DSL) part of the current internet architecture. HSC IP Team has deep understanding of IPv6 and IPv4 network architecture and deployment. Some the work done in the past includes

- Development of dual mode Applications on Linux, VxWorks and NetBSD
- Evaluation of NAT-PT as an option for transition to IPv6 in enterprise network.
- ISATAP Intra-Site Automatic Tunnel Addressing Protocol for V4 and V6 coexistence
- Migration of Legacy satellite data path (PEP) to dual mode
- IPv6 Protocols support in edge router
- Proprietary (stateless) IPv6 header compression to conserve bandwidth on satellite hop
- Usage of IPv6 Protocols – ND, ICMPv6, DNSv6, IPfilter-v6
- Legacy code review of a IP access gateway from coexistence point of view – code size 40KSLOC
- IPv6 test lab to test coexistence cases – under construction

CONTACT INFORMATION:

phone: +1.301.527.1629

fax: +1.301.527.1690

email: whitepaper@hsc.com

web: www.hsc.com

4.0 REFERENCES

[ARIN] [The IANA IPv4 Address Free Pool is Now Depleted.](#)

[DISRIPV6] DoD IPv6 Standard Profiles For IPv6 Capable Products Version 5.0

[DODIPV6TP] DEPARTMENT OF DEFENSE INTERNET PROTOCOL VERSION 6 - GENERIC TEST PLAN VERSION 4

[RFC 4057] J. Bound, Ed, "IPv6 Enterprise Network Scenarios", June 2005

[RFC3596] Thomson, et al., "DNS Extensions to Support IP Version 6", October 2003

[RFC3633] O. Troan, R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", December 2003

[RFC4554] T. Chown, "Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks", June 2006

APPENDIX A ABOUT HUGHES SYSTIQUE CORPORATION

HUGHES Systique Corporation (HSC), part of the HUGHES group of companies, is a leading Consulting and Software company focused on Communications and Automotive Telematics. HSC is headquartered in Rockville, Maryland USA with its development centre in Gurgaon, India.

SERVICES OFFERED:

Technology Consulting & Architecture: Leverage extensive knowledge and experience of our domain experts to define product requirements, validate technology plans, and provide network level consulting services and deployment of several successful products from conceptualization to market delivery.

Development & Maintenance Services: We can help you design, develop and maintain software for diverse areas in the communication industry. We have a well-defined software development process, comprising of complete SDLC from requirement analysis to the deployment and post production support.

Testing : We have extensive experience in testing methodologies and processes and offer Performance testing (with bench marking metrics), Protocol testing, Conformance testing, Stress testing, White-box and black-box testing, Regression testing and Interoperability testing to our clients

System Integration : As system integrators of choice HSC works with global names to architect, integrate, deploy and manage their suite of OSS, BSS, VAS and IN in wireless (VoIP & IMS), wireline and hybrid networks.: NMS, Service Management & Provisioning .

DOMAIN EXPERTISE:

Terminals

- Terminal Platforms : iPhone, Android, Symbian, Windows CE/Mobile, BREW, PalmOS
- Middleware Experience & Applications : J2ME , IMS Client & OMA PoC,

Access

- Wired Access : PON & DSL, IP-DSLAM,
- Wireless Access : WLAN/WiMAX / LTE, UMTS, 2.5G, 2G , Satellite Communication

Core Network

- IMS/3GPP , IPTV , SBC, Interworking , Switching solutions, VoIP

Applications

- Technologies : C, Java/J2ME, C++, Flash/lite,SIP, Presence, Location, AJAX/Mash
- Middleware: GlassFish, BEA, JBOSS, WebSphere, Tomcat, Apache etc.

Management & Back Office:

- Billing & OSS , Knowledge of COTS products , Mediation, CRM
- Network Management : NM Protocols, Java technologies,, Knowledge of COTS NM products, FCAPS, Security & Authentication

Platforms

- Embedded: Design, Development and Porting - RTOS, Device Drivers, Communications / Switching devices, Infrastructure components. Usage and Understanding of Debugging tools.
- FPGA & DSP : Design, System Prototyping. Re-engineering, System Verification, Testing

Automotive Telematics

- In Car unit (ECU) software design with CAN B & CAN C
- Telematics Network Design (CDMA, GSM, GPRS/UMTS)

BENEFITS:

- **Reduced Time to market :** Complement your existing skills, Experience in development-to-deployment in complex communication systems, with key resources available at all times
- **Stretch your R&D dollars :** Best Shore” strategy to outsourcing, World class processes, Insulate from resource fluctuations

PROPRIETARY NOTICE

- All rights reserved. This publication and its contents are proprietary to Hughes Systique Corporation. No part of this publication may be reproduced in any form or by any means without the written permission of Hughes Systique Corporation, 15245 Shady Grove Road, Suite 330, Rockville, MD 20850.
- Copyright © 2006 Hughes Systique Corporation