INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

THE FUTURE CONFIGURATION VERSION PROTOCALS OF GLOBAL AND PRIVATE IP - IPv6 SECURIT FEATURS

Mr. P Ravindra Reddy [*], Mr. Dr.V.V.Krishna, MS .P.Madhavi, Mr. B. Ramakantha Reddy, MS. D.Mallika Reddy
[1*] Department of Computer Science and Engineering, S.V Collage of Engineering Tirupathi.
Principal, Professor, Department of Computer Science and Engineering, GITE, Engineering Collage
Department of ECE, GITE, Engineering Collage
Department of Computer Science andEngineering, S.V College of Engineering TIRUPATHI
Department of CIVIL Engineering, GITE STUDENT M_TECH, ASST.PROF GITE, Engineering Collage
*Correspondence Author: pulimiravi.ravi256@gmail.com

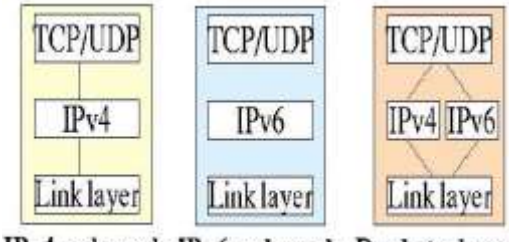
Keywords: IPv6 transition, heterogeneous network connectivity, tunneling, translation.

Abstract
In the process of Internet evolution, the transition from IPv4 to IPv6 has become inevitable and fairly urgent. Internet Assigned Numbers Authority has finally exhausted the global IPv4 address space, which leaves the community no choice but pushes forward the IPv6 transition process. IPv4 and IPv6 networks both will exist during the transition period, while the two are not compatible in nature. Therefore it is indispensable to maintain the availability, as well as to provide the inter-communication ability of IPv4 and IPv6. Years ago a series of transition techniques were actually proposed. However, because of their technical immatureness, they failed to cover the solution space well. Some of these techniques were even obsoleted by IETF due to their flaws. This paper reconsiders the basic problems and key difficulties in IPv4-IPv6 transition, and introduces the principles of tunneling and translation techniques. Then the paper surveys the mainstream tunneling and translation mechanisms raises since 1998.

Introduction
IPv6 is coming, whether we like it or not. It isn't a matter of new features or "killer applications," although those may come with time. Rather, it is the rapid depletion of the remaining IPv4 addresses that is leaving IPv6 as the only feasible alternative for the continued growth of networks beyond the next few years. Governments and service providers in many regions of the world have been cognizant of this fact for years, and are currently in various stages of planning for IP6 deployment in their networks. With thorough, clear planning IPv6 can be deployed safely and within acceptable costs. Understanding the elements of a good deployment plan is essential, however, as is an understanding of the various mechanisms and methodologies available for IPv6 implementation.

It is probably obvious the driving force behind the push to IPv6 – we're running out of IP address space! The current 32-bit addressing scheme used by IPv4 allows for a whopping 4.3 billion unique addresses. Although that sounds like a lot, consider that there are approximately 6.4 billion individuals on our planet. Certainly everyone doesn't have an IP address, but those that do might have multiple between home and work systems, IP-enabled phones and other network-aware devices. The rapid explosion of technology in emerging markets, especially in the Asian-Pacific region, demands a new supply of IP address space. IPv6 solves this problem by using 128-bit addressing. That allows for a total of 3.4 x 1038 addresses; a quantity that should keep us from running out for a long time.

Literature Review
IPv6 is receiving escalating attention within the networking industry. Where only a few years ago there was widespread doubt as to whether IPv6 would ever be adopted, the meetings of network operators forums such as the North American Network Operators' Group, the Asia Pacific Regional Internet Conference on Operational Technologies and Roseau IP Europeans now devote substantial portions of their agendas to discussions of how to best implement the new protocol.



IPv4-only node IPv6-only node Dual stack node

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

Fig: Layer structure of IPs

Where a few years ago resistance to IPv6 centered on the lack of a business case, organizations worldwide are now devoting significant financial and engineering resources to IPv6 planning. And where a few years ago even those who advocated IPv6 were casual about transition timelines, there is now a growing sense of urgency around its deployment.

Most of the standards that comprise the IPv6 protocol suite have been around for since the mid 1990s. What, then, is behind the suddenly intense interest in its deployment and the growing stress on deploying sooner rather than later? Is this interest justified, and should you also be thinking about deployment? How do you determine whether IPv6 is important for your own network? If you conclude that you should be concerned, how do you begin planning an IPv6 deployment? What factors and considerations comprise a research deployment? How do you identify – and avoid – pitfalls?

This paper begins by examining the current drivers for IPv6: The answer to why people are suddenly excited – or concerned – about IPv6. An overview of IPv6 deployment status around the world is then provided. With that foundation, the value of a well-considered deployment plan and the elements of such a plan are considered. Finally, the research work will examines the major mechanisms, tools, and approaches available for deploying IPv6 in accordance with the needs of network and the global goals of secured networks.

Problem Statement

The IPV6 would come to solve many known problems but as it is generally observed with new technological solutions it would also introduce so many security issues. The issues that would be introduced are variants. So, what does the emergence of IPv6 mean to security practitioners, engineers, IT Administrators and everyone who uses the internet? The problems expected amongst many others that will impact all networks are:

Security practitioners need education/training on IPv6.

IPv6 will come to the networks – it's only a matter of time. As with any new networking technology, it's essential that the basics of IPv6 is learned, especially the addressing scheme and protocols, in order to facilitate incident handling and related activities. This will be handled in detail during this research work and recommended training layout will be provided.

Security tools need to be upgraded.

IPv6 is not backwards compatible. This means that after switching or migrated to IPV6, then IPV4 would be dead. The hardware and software used to route traffic across networks and perform security analyses won't work with IPv6 traffic unless they are upgraded to versions that support the protocol. This is especially important to remember when it comes to perimeter-protection devices. Routers, firewalls and intrusion-detection systems may require software and/or hardware upgrades in order to "speak" IPv6 languages. Many manufacturers already have these upgrades available.

Existing equipment will require additional configuration.

The devices that do support IPv6 typically treat it as an entirely separate protocol. Therefore, the access control lists, rule bases and other configuration parameters will need to be reevaluated and translated to support an IPv6 environment.

Tunneling protocols will create new risks.

The networking and security communities have invested time and energy in ensuring that IPv6 is a security-enabled protocol. However, one of the greatest risks inherent in the migration is the use of tunneling protocols to support the transition to IPv6. These protocols allow the encapsulation of IPv6 traffic in an IPv4 data stream for routing through non-compliant devices. Therefore, it's possible that users on the internet and networks can begin running IPv6 using these tunneling protocols before organizations and managers are ready to officially support it in production. The summary solution to this problem would be to block IPv6 tunneling protocols (including SIT, ISATAP, 6to4 and others) at the perimeter of the network. The detail of this procedure would also be presented in this research work.

IPv6 auto configuration creates addressing complexity.

Auto configuration, another interesting IPv6 feature, allows systems to automatically gain a network address without administrator intervention. IPv6 supports two different auto configuration techniques. Stateful auto configuration uses DHCPv6, a simple upgrade to the current DHCP protocol, and doesn't reflect much of a difference from a security perspective. On the other hand, keep an eye on stateless auto configuration. This technique allows systems to generate their own IP addresses and checks for address duplication. This decentralized approach may be easier from a system administration perspective, but it raises challenges for those of us charged with tracking the use of network resources. System administrators and integrators would have to face new challenges of monitoring IP activities.

Intended Solution

1. Dual Stacks
2. Manually Configured Tunnels

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

3. Automatic Tunnels and Translators

Dual Stacks

Dual-stack refers to side-by-side implementation of IPv4 and IPv6. That is, both protocols run on the same network infrastructure, and there's no need to encapsulate IPv6 inside IPv4 (using tunneling) or vice-versa. Dual-stack is defined in RFC 4213.

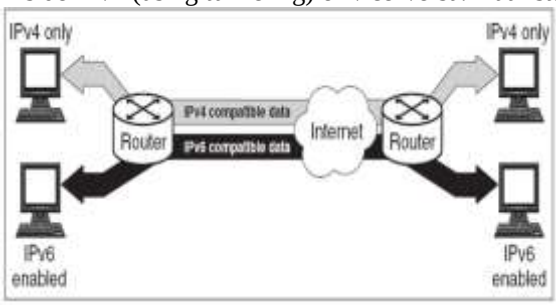


Fig: Dual Stack Network

Although this is the most desirable IPv6 implementation during the transition from IPv4 to IPv6, as it avoids the complexities and pitfalls of tunneling such as security, increased latency, management overhead, and a reduced path maximum transmission unit (PMTU), it is not always possible, since outdated network equipment may not support IPv6. A good example is cable TV-based internet access. In modern cable TV networks, the core of the Hybrid fiber-coaxial (HFC) network such as large core routers is likely to support IPv6. However, other network equipment such as a Cable Modem Termination System (CMTS) or customer equipment like cable modems may require software updates or hardware upgrades to support IPv6. This means cable network operators must resort to tunneling until the backbone equipment supports native dual-stack.

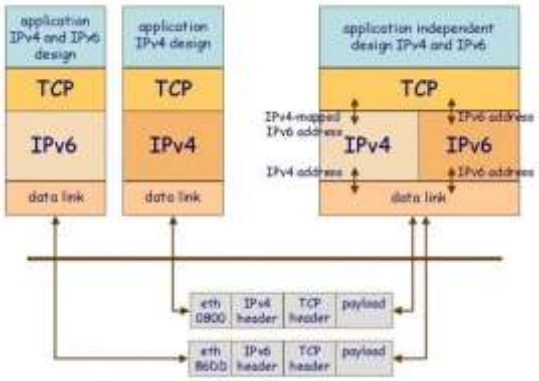


Fig: Dual Stack guidelines.

The dual-stack should only be considered as a transitional technique to facilitate the adoption and deployment of IPv6, as it has some major drawbacks and consequences: it will not only more than double the security threats from both IPv4 and IPv6 for the existing network infrastructure, but also ultimately overburden the global networking infrastructure with both dramatically increased Internet traffic. The ultimate objective is to deploy the single stack of IPv6 globally.

Manually Configured Tunnels

Many current internet users do not have IPv6 dual-stack support, and thus cannot reach IPv6 sites directly. Instead, they must use IPv4 infrastructure to carry IPv6 packets. This is done using a technique known as tunneling, which encapsulates IPv6 packets within IPv4, in effect using IPv4 as a link layer for IPv6.

IP protocol 41 indicates IPv4 packets which encapsulate IPv6 datagrams. Some routers or network address translation devices may block protocol 41. To pass through these devices, UDP packets may be used to encapsulate IPv6 datagrams. Other encapsulation schemes, such as Anything In Anything (AYIYA) or Generic Routing Encapsulation, are also popular.

Conversely, on IPv6-only internet links, when access to IPv4 network facilities is needed, tunneling of IPv4 over IPv6 protocol occurs, using the IPv6 as a link layer for IPv4.

Automatic tunneling

Automatic tunneling refers to a technique by which the routing infrastructure automatically determines the tunnel endpoints. Some automatic tunneling techniques are below.

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

6to4 is recommended by RFC 3056. It uses protocol 41 encapsulation. Tunnel endpoints are determined by using a well-known IPv4 any-cast address on the remote side, and embedding IPv4 address information within IPv6 addresses on the local side. 6to4 is the most common tunnel protocol currently deployed.

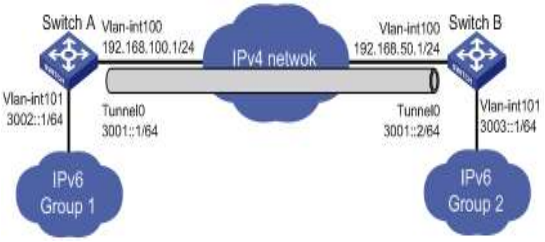


Fig: Automatic Tunneling

Treed is an automatic tunneling technique that uses UDP encapsulation and can allegedly cross multiple NAT nodes. IPv6, including 6to4 and Treed tunneling, are enabled by default in Windows Vista and Windows 7. Most Unix systems implement only 6to4, but Treed can be provided by third-party software such as Mired.

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) uses the IPv4 network as a virtual IPv6 local link, with mappings from each IPv4 address to a link-local IPv6 address. Unlike 6to4 and Treed, which are inter-site tunneling mechanisms, ISATAP is an intra-site mechanism, meaning that it is designed to provide IPv6 connectivity between nodes within a single organization.

Configured and automated tunneling (6in4)

6in4 tunneling requires the tunnel endpoints to be explicitly configured, either by an administrator manually or the operating system's configuration mechanisms, or by an automatic service known as a tunnel broker; this is also referred to as automated tunneling. Configured tunneling is usually more deterministic and easier to debug than automatic tunneling, and is therefore recommended for large, well-administered networks. Automated tunneling provides a compromise between the ease of use of automatic tunneling and the deterministic behavior of configured tunneling.

Raw encapsulation of IPv6 packets using IPv4 protocol number 41 is recommended for configured tunneling; this is sometimes known as 6in4 tunneling. As with automatic tunneling, encapsulation within UDP may be used in order to cross NAT boxes and firewalls.

Translation for IPv6-only hosts

After the regional Internet registries have exhausted their pools of available IPv4 addresses, it is likely that hosts newly added to the Internet might only have IPv6 connectivity.

For these clients to have backward-compatible connectivity to existing IPv4-only resources, suitable IPv6 transition mechanisms must be deployed. One form of address translation is the use of a dual-stack application-layer proxy server, for example a web proxy.

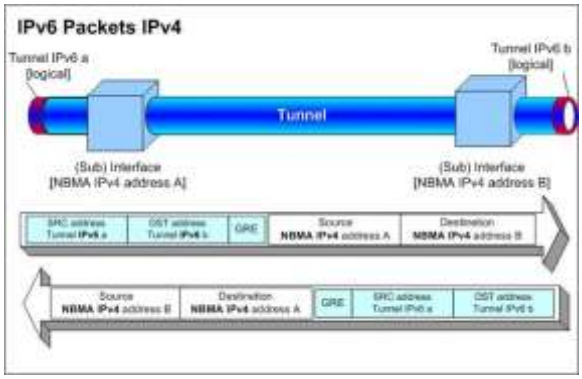


Fig: Tunneling Addresses

NAT-like techniques for application-agnostic translation at the lower layers in routers and gateways have been proposed. The NAT-PT standard was dropped because of criticisms; however, more recently, the continued low adoption of IPv6 has prompted a new standardization effort of a technology called NAT64.

Recent Developments

The implementation mechanisms discussed in this paper are by no means the only tools that will ever be available. New mechanisms continue to be proposed; some will not gain enough interest to be developed, some will be developed but proven impractical, and some will become useful additions to the IPv6 implementation toolbox.

Among the newer proposals currently being discussed are:

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

1. A stateless address mapping mechanism called IVI, which uses IPv4 addresses embedded in IPv6 addresses as a scalable alternative to NATPT. IVI has been used in CERNET2, the CNGI-sponsored Chinese academic and research network, for over two years.
2. The IETF Software's Working Group is presently proposing new solutions for interconnecting IPv4 and IPv6 networks, with a focus on tunneling IPv4 over IPv6.
3. Comcast has proposed a mechanism called Dual-Stack Lite that addresses both the growing scarcity of IPv4 addresses and the need for existing IPv4 devices to communicate with new IPv6 devices. Rather than have traditional NAT devices at each site, IPv4 would be tunneled to more centralized carrier-grade NATs which both assign IPv4 to dual stacked devices and de-capsulate IPv4 packets from IPv6 packets.

The success of these and other proposals is yet to be seen, but they serve as an assurance that means for overcoming the currently recognized challenges of IPv6 implementation continue to be developed.

Conclusion

Given that IANA has eventually run out IPv4 address space, the Internet is bound to enter the IPv6 era. Nevertheless, IPv4 networks will coexist with IPv6 networks for a long time during the transition. The IPv6 transition process should be steady and smooth. Therefore, the IPv4-IPv6 coexisting networks should sustain the availability of both IPv4 and IPv6, and support IPv4-IPv6 interconnection as well. This paper analyzes the basic problem of heterogeneous traversing and heterogeneous interconnection in IPv6 transition, introduces the principle of tunneling and translation techniques, and reviews the mainstream tunneling and translation mechanisms. The aspects of address scheme and routing, heterogeneous addressing, data forwarding, performance, security and scalability are studied for these mechanisms. The paper also summarizes the pros and cons, and subsequently application scenarios of every mechanism. A series of mechanisms including Software Mesh, 6RD, DS-Lite, 4over6, MAP, IVI and NAT64 are recommended as feasible solutions to filling in their respective application scenarios. Based on these recommendations, this paper studies the characteristics and transition requirements of practical ISP networks, and proposes the transition strategies for both
backbone and edge networks by selecting and deploying the recommended mechanisms.

The transition techniques are still facing challenges and require further research efforts. For translation techniques, the most critical issue is the lack of feasible, shameful IPv4→IPv6 translation mechanisms. Unfortunately, based on the current understanding of IPv4-IPv6 translation, this problem seems unlikely to be solved. We need to find a new angle to develop a solution. As for the existing translation mechanisms, there are still the issues of scalability, heterogeneous addressing and application layer translation.

For tunneling techniques, mechanisms like 4over6 and MAP-E change the provisioning granularity from a full address into a port set. New address resource management models are required to achieve good address resource utilization. During the IPv6 transition process, the above problems are the essential challenges that need to be overcome. They are all non-neglect able problems in promoting IPv6, and hopefully they are solvable with the combination of techniques and business means.

References

1. G. Huston, "IPv4 Address Report," Tech. Rep., Sep. 2010.
2. M. Tatipamula, P. Grossetete, and H. Esaki, "IPv6 integration and coexistence strategies for next-generation networks," IEEE Commun.Mag., vol. 42, no. 1, pp. 88 – 96, jan 2004.
3. J. J. Amoss and D. Minoli, Handbook of IPv4 to IPv6 Transition: Methodologies for Institutional and Corporate Networks. Auerbach Publications, 2007.
4. M. Mackay and C. Edwards, "A Managed IPv6 Transitioning Architecture for Large Network Deployments," IEEE Internet Computing, vol. 13, no. 4, pp. 42 –51, july-aug. 2009.
5. P. Wu, Y. Cui, M. Xu, J. Dong, and C. Metz, "Flexible Integrationof Tunneling and Translation for IPv6 Transition," Networking Science, vol. 1, pp. 23 – 33, 2012.
6. Connecting to 6bone with dynamic IPv4 address,
7. Y. Cui, J. Wu, X. Li, M. Xu, and C. Metz, "The Transition to IPv6, Part II: The Softwire Mesh Framework Solution," IEEE Internet Computing, vol. 10, pp. 76 – 80, 2006.
8. M. Townsley and O. Troan, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)," 2010, IETF RFC 5969.
9. Y. Cui, P. Wu, M. Xu, J. Wu, Y. Lee, A. Durand, and C. Metz, "4over6:network layer virtualization
10. J. Wu, Y. Cui, X. Li, and C. Metz, "The Transition to IPv6, Part I: 4over6 for the China Education and Research Network," IEEE Internet Computing, vol. 10, pp. 80 – 85, 2006.
11. R. Despres and R. Penno and Y. Lee and G. Chen and S. Jiang , "IPv4 Residual Deployment via IPv6 - a unified Stateless Solution (4rd)," 2012, IETF draft.

12. M. Mawatari and M. Kawashima and C. Byrne , "464XLAT: Combination of Stateful and Stateless Translation," 2012, IETF draft.