Encyclopedia of Internet Technologies and Applications

Mario Freire
University of Beira Interior, Portugal

Manuela Pereira
University of Beira Interior, Portugal

Information Science REFERENCE

INFORMATION SCIENCE REFERENCE
Hershey · New York

Acquisitions Editor: Kristin Klinger
Development Editor: Kristin Roth
Senior Managing Editor: Jennifer Neidig
Managing Editor: Sara Reed
Copy Editor: Larissa Vinci and Mike Goldberg
Typesetter: Amanda Appicello and Jeffrey Ash
Cover Design: Lisa Tosheff
Printed at: Yurchak Printing Inc.

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue, Suite 200
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com/reference

and in the United Kingdom by
Information Science Reference (an imprint of IGI Global)
3 Henrietta Street
Covent Garden
London WC2E 8LU
Tel: 44 20 7240 0856
Fax: 44 20 7379 0609
Web site: http://www.eurospanonline.com

Library of Congress Cataloging-in-Publication Data

Encyclopedia of Internet technologies and applications / Mario Freire and Manuela Pereira, editors.
p. cm.
Summary: "This book is the single source for information on the world's greatest network, and provides a wealth of information for the average Internet consumer, as well as for experts in the field of networking and Internet technologies. It provides the most thorough examination of Internet technologies and applications for researchers in a variety of related fields"--Provided by publisher.
Includes bibliographical references and index.
ISBN 978-1-59140-993-9 (hardcover) -- ISBN 978-1-59140-994-6 (ebook)
1. Internet--Encyclopedias. I. Freire, Mário Marques, 1969- II. Pereira, Manuela.
TK5105.875.I57E476 2007
004.67'803--dc22
2007024949

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

The IPv6 Protocol

Christos Bouras
Research Academic Computer Technology Institute and University of Patras, Greece

Apostolos Gkamas
Research Academic Computer Technology Institute and University of Patras, Greece

Dimitris Primpas
Research Academic Computer Technology Institute and University of Patras, Greece

Kostas Stamos
Research Academic Computer Technology Institute and University of Patras, Greece

This article provides a description of the IPv6 protocol. It briefly covers the reasons that make IPv6 a necessary upgrade, describes the most important methods for transitioning networks, applications, and hosts from IPv4 to IPv6, and the possibilities that IPv6 opens up. It finally also examines the current status of IPv6 deployment and vendor, protocol, and application support.

INTRODUCTION

In order to address the limited address space of **IPv4** and other concerns regarding its age and ability to support future needs for the Internet, the Internet Engineering Task Force (**IETF**) has developed a suite of protocols and standards known as IP version 6 (IPv6).

The principal problem with IPv4 was the fact that its 32-bit address space allows only about four billion unique addresses, which are not enough to accommodate the rapid growth of the Internet. Moreover, because of inefficient allocation and parts of the address space that cannot be used for unique address allocation, the IPv4 address space is even smaller, and techniques such as NAT, which, however, break the Internet's end-to-end architecture, have to be used. IPv6 solves this problem by providing 128 bits of address space which provides a huge amount of addresses available for every person or device in the world in the foreseeable future.

The design of IPv6 (Deering, 1998) is intentionally targeted for minimal impact on upper- and lower-layer protocols by avoiding the random addition of new features. More than simply increasing the address space, IPv6 offers improvements like built-in security support, plug and play support, no checksum at the IP header, and more flexibility and extensibility than IPv4. IPv6 also facilitates efficient renumbering of sites by explicitly supporting multiple addresses on an interface. The widespread adoption of the new Internet Protocol will fuel innovation and make possible the creation of many new networking applications. It will also allow the replacement of the NAT solutions that have been implemented today in order to work around the lack of IPv4 addresses. NAT introduces a number of problems to network applications that need knowledge of the IP address of the host machine or want to take advantage of Quality of Service mechanisms like VoIP implementations.

BACKGROUND

The proposal for a next generation Internet protocol was first discussed within IETF in 1993, while the final proposal for the IPv6 protocol was defined in 1995. Although in the following years a lot of the parameters of the IPv6 technology were defined, refined, analyzed, and reviewed, the fact that IPv4 is still the dominant protocol well within the 21st century has led many people to either regard IPv6 as a technology that will never gain wide adoption, or has taught them to be cautious in trying to guess when it will start overshadowing IPv4.

However, IPv6 usage is gaining significant support and wide adoption in countries such as China and Japan,

where IPv4 address allocation has been scarce because of historical factors (Wang, 2005).

In addition, IPv6 support in most networking vendor equipment, operating systems, and applications has been elevated to a production-quality level, with several years of experimentation, research, and improvement of the product's IPv6 support.

IPV6 DESCRIPTION

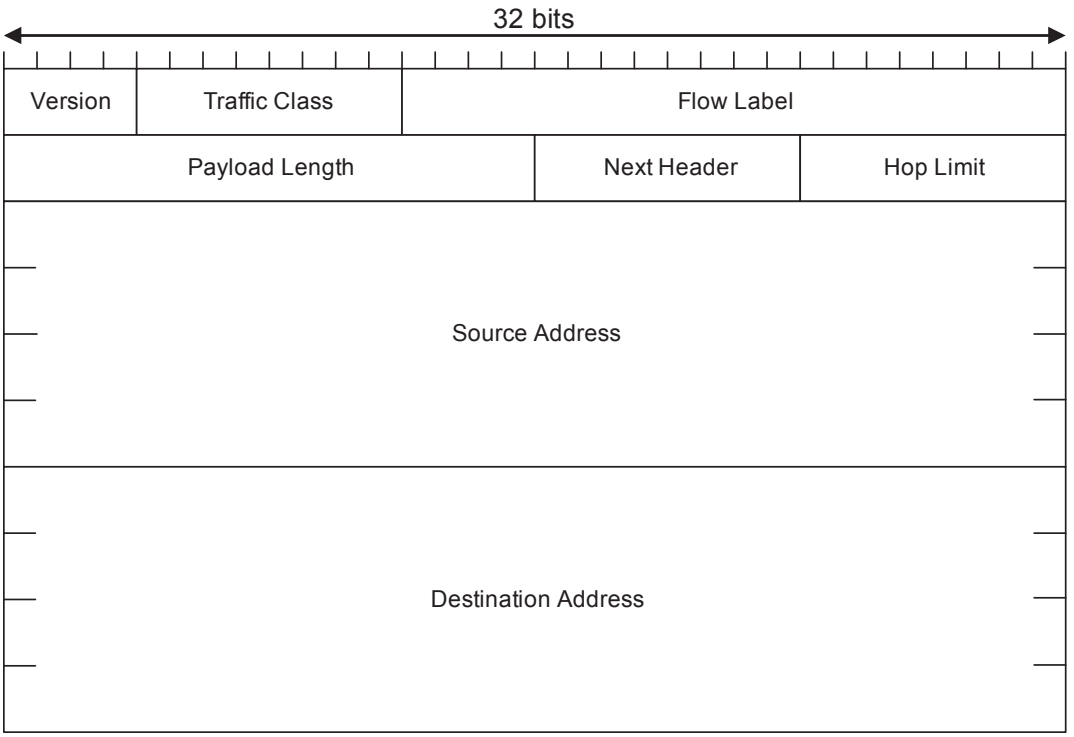
The IPv6 protocol has a different header than IPv4, removing some fields and adding others. It also introduces the notion of optional extension headers that are responsible for handling situations that are not always common, in order to spare the forwarding equipment in the network (routers) from complicated processing that would be in most cases unnecessary.

IPv6 has a number of benefits over IPv4, which are explained in more detail.

Enormously Larger Address Space

The number of IP addresses available with IPv6 is huge (2^{128}, which is about 3.4×10^{38} addresses) and will not be exhausted in the foreseeable future. The address space of IPv6 is so enormous that, as a thought experiment, one could allocate 670,000 trillion addresses for each square millimeter of the earth's surface. The large address space of IPv6 opens up new possibilities for easier Internet connectivity to all kinds of devices. Practically, it means that any electronic device, from computers to cell phones, automobiles, and household appliances, can have its own address. As a result, it is no longer required to come up with complex solutions to bypass **NAT** (network access translation) mechanisms which will no longer be necessary. The IPv6 approach of assigning a unique routable address to any device that is connected to the Internet restores the original simplicity of the Internet peer-to-peer architecture. It also makes possible the hassle-free emergence of new

Figure 1. IPv6 header



applications, whose deployment is complicated and hindered by NAT's lack of peer-to-peer connectivity.

Furthermore, because of the abundance of IPv6 addresses, their assignment can be made in a hierarchical manner that was not possible for IPv4, and therefore increase the efficiency of routing equipment (Hinden, 2003).

Simplified Packet Header for Routing Efficiency and Performance

IPv6 also improves the efficiency of the Internet by simplifying and optimizing the IP header (Deering, 1998). Unlike IPv4, the IPv6 header has a fixed size, and the 14 header fields of IPv4 have been reduced to eight for IPv6. Simplified packet header information allows for more straightforward and efficient routing of Internet packets. More unusual header fields are handled in a more efficient way through IPv6 header extensions, which combine the benefit of accommodating new features and the efficiency of a fixed and quickly processible standard header. The use of IPv6 also results, as mentioned, in shorter routing tables because most Internet service providers (ISP) can now receive address space in adjacent blocks.

Deeper Hierarchy and Policies for Network Architecture Flexibility

At the enterprise level it is also possible to rapidly define a complete addressing plan (Router Renumbering) by constructing step by step: (1) the prefixes on different router interfaces from the access router, (2) the prefix of the operator network, the service provider network, or that of the network administrator. This approach avoids problems that arise from managing combined private networks on IPv4.

Serverless Autoconfiguration, Easier Renumbering, Multihoming, and Improved Plug and Play Support

IPv6 is "auto-configurable," which means that devices like laptops, PDAs, and mobile phones can be given their own unique IP addresses easily and without delay. This will simplify the installation and maintenance of home, vehicle, and small office networks. IPv6 supports two types of automatic configuration, stateful and stateless. The "stateless" address auto-configuration mechanism that is introduced by IPv6 (Thomson et al., 1998) does away with the need for a **DHCP** server (Droms et al., 2003). With stateless address configuration, hosts on a link automatically configure themselves with IPv6 addresses for the link and with global addresses derived from prefixes advertised by local routers. Even in the absence of a router, hosts on the same link can automatically configure themselves with link-local addresses and communicate without manual configuration.

Security with Mandatory IP Security (IPSec) Support for All IPv6 Devices

IPv6 improves security by facilitating network-level security. It has security services at the IP-layer as a native feature. Also, allowing each communications device to have its own unique IP number facilitates end-to-end security, meaning that an entire communication session can be conducted securely rather than just the parts that use a virtual private network. IPv6 introduces two header extensions (authentication and encapsulating security payload headers) which can be used separately or in combination in order to provide authentication and confidentiality for the data transmitted at the network layer.

Improved Support for Mobile IP and Mobile Computing Devices

Managing **Mobile IP** consists of defining protocols to convey information to a device, wherever it is connected without interruption. Mobile IP solutions exist today on IPv4. However, their implementation creates a number of obstacles that inhibit mass deployment, which is now being addressed by Mobile IPv6. For example, with the use of IPv6 there is need for triangular communication via a home agent. A key factor is the possibility for a mobile node to keep the same unique IPv6 address while moving between different networks.

QoS Support in IPv6

The QoS problems remain the same as IPv4 but IPv6 is a more streamlined protocol (Nichols et al., 1998). Its key benefit over IPv4 is scalability, and many features of IPv6 are IPv4 "add ons." The IPv6 header has two

QoS-related fields, the new 20-bit Flow Label field which can be used for the implementation of IntServ-based QoS schemes, and an 8-bit Traffic Class indicator which can be used for the implementation of DiffServ-based QoS schemes (Bouras et al., 2004). The Flow Label can be used in order to identify specific flows in the network and allows intermediate nodes in the flow path to recognize the flow and treat it appropriately.

Transitioning to IPv6

A large variety of mechanisms have been proposed in order to facilitate the transition from IPv4 to IPv6. The most common approach is the implementation of a dual IPv4/IPv6 stack at hosts, so that they are able to communicate using both protocols. Depending on the network infrastructure used by an IPv6-enabled host (an IPv4 network, an IPv6-enabled network, an MPLS backbone, etc.), several techniques have been developed, such as ISATAP (if the IPv6 host resides in an IPv4 network), 6to4 (if the IPv6 host resides in an IPv6 local network but wants to communicate to another remote host over IPv4 infrastructure), 6PE (if there is available MPLS infrastructure), etc., in order for the IPv6 host to be able to communicate with other IPv6 hosts. These mechanisms are going to be useful for the long period of transitioning from IPv4 to IPv6, when most IPv6 nodes will have to traverse at least part of IPv4-only infrastructure in order to reach each other.

An important part of the proper operation of the dual IPv4/IPv6 stack is the way the DNS service influences whether the IPv4 or the IPv6 host will be used. Upon a DNS request, a DNS server can either return only an IPv6 address, an IPv4 address, or both. It is recommended that the choice of the address used should be made by the requesting host and not the DNS server.

Tunneling mechanisms are used when IPv6 hosts want to communicate over an infrastructure that is partly IPv4. IPv6 packets are then encapsulated as payload in IPv4 packets, transferred over the IPv4 network infrastructure and decoded at the other end of the tunnel for delivery. The encapsulation and the decoding of IPv6 packets can be performed in either a router or a host, and the tunneling procedure can be configured either manually with the intervention of an administrator or automatically.

A widely-used technique for automatic tunneling is called 6to4 (Carpenter et al., 2001), and is particularly useful when an IPv6 host inside a local IPv6 network wants to communicate with another remote host over IPv4 infrastructure. For the 6to4 mechanism to work, the border router at the end of the IPv6 network has to be properly configured in order to support the 6to4 tunneling mechanism.

Another mechanism is 6over4 (Carpenter et al., 1999), which is useful when the underlying IPv4 infrastructure supports multicast. The 6over4 mechanism utilizes the multicast infrastructure in order to make an isolated IPv6 host with no native IPv6 support from its network become a fully functional IPv6 node.

If the IPv4 network provides an **MPLS**-enabled core, it is possible, through the use of the 6PE mechanism (developed by Cisco Systems; Clercq, 2004), to forward IPv6 packets over the MPLS network without enabling IPv6 in the intermediate routers. Furthermore, MPLS also provides the possibility of L2VPNs (Layer 2 Virtual Private Networks) that can connect two remote IPv6 hosts over an intermediate MPLS network, as if they were directly connected at Layer 2.

While 6to4 is suitable for connecting IPv6 hosts in IPv6-enabled local networks over IPv4 infrastructure, another tunneling mechanism called **ISATAP** (Templin et al., 2005) is designed in order to connect isolated IPv6 hosts residing in a network that does not support IPv6.

In cases where none of the above mechanisms is available, a last resort mechanism can be the **Teredo** (Huitema, 2004) mechanism. It is useful when there is no suitable border router with 6to4 support, but there is NAT support available. In such cases, Teredo encapsulates IPv6 packets as IPv4 UDP ones that can traverse NAT.

Apart from communication between IPv6 hosts, there is also a number of translation techniques that enable the communication of hosts using different IP protocols. Techniques such as Bump-in-the-stack (Tsuchiya et al., 2000) or Bump-in-the-API (Lee et al., 2002) are used in order to translate IPv4 traffic generated by an application into IPv6 traffic by the time it reaches the network, and vice versa. Another mechanism called SOCKS, uses an application level gateway (ALG) node, which is responsible for relaying traffic in a TCP or UDP session between an IPv4 and an IPv6 host.

FUTURE TRENDS

IPv6 support is currently widespread among vendors of network equipment and operating systems. All major modern operating systems offer dual stack implementations, and IPv6 support is standard in most new networking equipment and software. Also, the majority of new applications come with a capability to communicate over IPv6, and many legacy applications have been ported to support the new protocol. Overall, the pieces of the transition to IPv6 seem to be in place and the transition is moving forward.

Countries that did not play a large part in the original development of the Internet, such as China and Japan, were not allocated IP addresses proportional to their constantly increasing number of Internet users in the last years. Despite having over half of the world's population, Asia only controls about nine percent of the allocated IPv4 addresses. Therefore, the scarcity of unique routable IP addresses is more intense in these countries than in the U.S., where institutions and enterprises were allocated much larger IP address blocks because of their early adoption of the Internet. As a result, IPv6 adoption in Asia is much larger and growing faster than in Europe and the U.S. (Barnard, 2006).

A significant incentive for the adoption of IPv6 in the United States has been that the U.S. Government has specified that all federal agencies must deploy IPv6 by 2008 (GovExec.com 2005), with the Department of Defense being the most advanced agency in the deployment.

In Europe, the European Union has helped advance IPv6 knowledge and adoption by funding large-scale projects such as 6NET, which have contributed to the promotion of IPv6 as a technology that can be considered at the production stage instead of the research stage.

CONCLUSION

IPv6 has been proposed by IETF in order to overcome the scarcity of unique globally routable addresses in IPv4. It enhances network layer connectivity by offering a number of additional improvements over IPv4. Although techniques such as NAT have reduced the urgency of the situation, most experts in the field foresee a gradual transition to IPv6 within the next years, aided by the maturity of the support for the new protocol at most new hardware vendor and software implementations coming out today.

REFERENCES

6NET project. (2006). Retrieved March 2006, from http://www.sixnet.org

Barnard, P. (2006). Recent Internet2 land speed records show that IPv6 is almost on par with IPv4. *TMCnet*. Retrieved March 2006, from http://news.tmcnet.com/news/2006/03/09/1444997.htm

Bouras, C., Gkamas, A., Primpas, D., & Stamos, K. (2004). Performance evaluation of the impact of quality of service mechanisms in an IPv6 network for IPv6-capable real time applications. *Journal of Network and Systems Management, 12*(4), 463-483.

Carpenter, B., & Moore, K. (2001). *Connection of IPv6 domains via IPv4 clouds*. RFC 3056.

Carpenter, B., & Jung, C. (1999). *Transmission of IPv6 over IPv4 domains without explicit tunnels*. RFC 2529.

Conta, A., & Deering, S. (1998). *Internet control message protocol (ICMPv6) for the Internet protocol Version 6 (IPv6) Specification*. RFC 2463.

Clercq, J. (2004). *Connecting IPv6 islands over IPv4 MPLS using IPv6 provider edge routers (6PE)*. draft-ooms-v6ops-bgp-tunnel-03

Deering, S., & Hinden, R. (1998*). Internet protocol, version 6 (IPv6) specification.* RFC 2460.

Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., & Carney, M. (2003). *Dynamic host configuration protocol for IPv6 (DHCPv6)*. RFC 3315.

Hinden, R., & Deering, S. (April 2003). *IP version 6 addressing architecture*. RFC 3513.

Huitema, C. (2004). *Teredo: Tunneling IPv6 over UDP through NATs.* draft-huitema-v6ops-teredo-02.

Lee, S., Shin, M-K., Kim, Y-J., Nordmark, E., & Durand, A. (2002). *Dual stack hosts using "Bump-in-the-API" (BIA).* RFC 3338.

Nichols, K., Blake, S., Baker, F., & Black, D. (1998). *Definition of the differentiated services field (DS field) in the IPv4 and IPv6 headers*. RFC 2474.

Rajahalme, J., Conta, A., Carpenter, B., & Deering, S. (2004). *IPv6 flow label specification*. RFC 3697.

Templin, F., Gleeson, T., Talwar, M., & Thaler, D. (2005). *Intra-site automatic tunnel addressing protocol (ISATAP)*. RFC 4214.

Thomson, S., & Narten, T. (1998). *IPv6 stateless address autoconfiguration*. RFC 2462.

Thomson, S., Huitema, C., Ksinant, V., & Souissi, M. (2003). *DNS extensions to support IP version 6*. RFC 3596.

Tsuchiya, K., Higuchi, H., & Atarashi, Y. (2000). *Dual stack hosts using the "Bump-In-the-Stack" technique (BIS)*. RFC 2767.

U.S. government agencies must use advanced Internet by 2008. Retrieved March 2006, from http://www.govexec.com/dailyfed/0605/062905tdpm2.htm

Wang, T. (2005). China is deploying IPv6 to generate enough IP addresses for billions of internet users. Retrieved March 2006, from http://blog.loaz.com/timwang/index.php/2005/04/12/china_is_deploying_ipv6_to_generate_enou

KEY TERMS

DHCP (Dynamic Host Configuration Protocol): A protocol used for dynamic assignment of IP addresses to devices in a network.

DNS (Domain Name Service): A distributed database service developed in order to match IP addresses to human-readable names for easier location and retrieval of Internet services.

Internet Engineering Task Force (IETF): The organization comprised of a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

IPv4 (Internet Protocol, version 4): The version of the Internet protocol that has been used throughout the existence of the Internet.

IPv6 (Internet Protocol, version 6): The new version of the Internet protocol designed to replace IPv4, with the motivation of solving the address scarcity problem and improving protocol efficiency in additional areas.

MPLS (Multi-Protocol Label Switching): A data-carrying mechanism which emulates some properties of a circuit-switched network over a packet-switched network and was designed in order to provide a unified data-carrying service for both circuit-based clients and packet-switching clients which provide a datagram service model.

Quality of Service (QoS): The ability to provide specific guarantees to traffic flows regarding the network characteristics, such as packet loss, delay, and jitter experienced by the flows.

TCP (Transmission Control Protocol): A connection-oriented, reliable protocol of the TCP/IP protocol suite used for managing full-duplex transmission streams.

UDP (User Datagram Protocol): A connectionless, unreliable protocol of the TCP/IP protocol suite used for sending and receiving datagrams over an IP network.