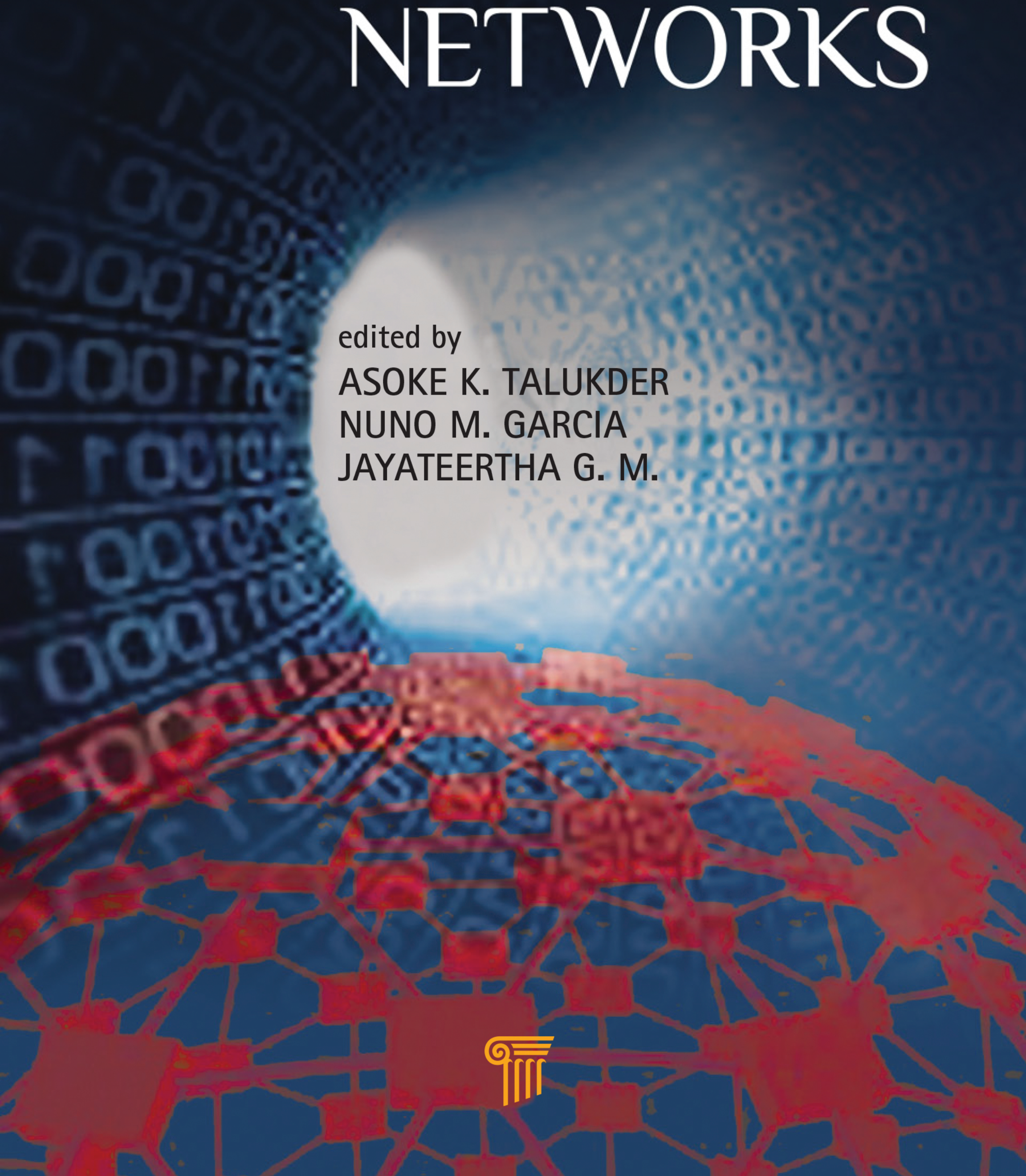
CONVERGENCE THROUGH ALL-IP NETWORKS



edited by

ASOKE K. TALUKDER
NUNO M. GARCIA
JAYATEERTHA G. M.

CONVERGENCE THROUGH ALL-IP NETWORKS

CONVERGENCE THROUGH *ALL-IP* NETWORKS

edited by
ASOKE K. TALUKDER
NUNO M. GARCIA
JAYATEERTHA G. M.

PAN STANFORD PUBLISHING

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

No claim to original U.S. Government works
Version Date: 20131021

International Standard Book Number-13: 978-981-4364-64-5 (eBook - PDF)

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Contents

Preface

The success of a technology is measured by how invisible the technology is to a user. The 21st century is the century of anywhere communication—anybody can communicate, anytime, anywhere in the world, so easily, so seamlessly, be it voice, data, multimedia, or even video. Though it looks trivial to a user, from the science and engineering point of view there is a complex fabric of networks and technologies that work in tandem in the background to orchestrate these synergy and wonders. A book to explain the interworking of these wonders was the motivation behind the title *Convergence through All-IP Networks*.

On April 28–30, 2009, we had the 6th IEEE and IFIP International Conference on Wireless and Optical Communication Networks (WOCN2009) at Cairo. In the said conference, Dr. Talukder offered a tutorial on next-generation networks (NGNs). The foundation of the book started then—Dr. Talukder and Dr. Garcia met each other at that conference, and Mr. Stanford Chong of Pan Stanford Publishing approached Dr. Talukder to author a book on the said topic. Dr. Jayateertha joined the team later.

Our goal was to bring out a volume with the entire technology spectrum of NGNs from a backbone to varied network elements with myriads of end-user devices. We wanted a volume that exposes all IP and its convergence that otherwise remain invisible. In this regard, this book encompasses a variety of topics, including specialized services and applications scenarios. In doing this, our main endeavor was to introduce these complex topics to the reader at large without losing simplicity and legibility in presentation. We wanted a comprehensive handbook for the industry and a reference book for students, professionals, and researchers.

To achieve the above goals of convergence and NGN, we included topics starting from a fiber-optic backbone to the wireless last mile, including routing. We included the "Internet of Things," low-power wireless personal area networks (LoWPANs), and extended networked homes. We included mobility and worldwide interoperability for microwave access (WiMAX). We included routing, extensively including IPv6 routing. We included the network for vehicles on highways and intravehicle and intervehicular communication. In the 21st century a book on networks is incomplete without addressing security issues; therefore, we included security issues in NGNs as well.

Having a book with such a wide spectrum of topics that covers the next generation of the Internet and convergence has its own challenges. The most difficult part of the challenge was to get the right mix of experts and authors who could contribute. Though it took us time, we have been lucky to get some of the world leaders to participate as authors in this volume. We tried to make the volume error free and respect the original creators as well as trademarks and copyright; however, any unintended errors or omissions are regretted.

We would like to sincerely acknowledge all the contributors and specially thank Pan Stanford Publishing for coming forward to publish this volume. We appreciate the efforts of the reviewers and the editorial team for coming up with an excellent edition. We also would like to thank all the family members of each and every author and editor for their support.

Asoke K. Talukder
Nuno M. Garcia
Jayateertha G. M.
August 2013

Chapter 1

All-IP Networks: Introduction

Asoke K. Talukder,[a,b,*] **Nuno M. Garcia,**[c,d,e,**] **and Jayateertha G. M.**[f,g,†]

[a]*InterpretOmics, Bangalore, India*
[b]*Indian Institute of Information Technology & Management, Gwalior, India*
[c]*Universidade da Beira Interior, R. Marquês D'Ávila e Bolama, Covilhã, Portugal*
[d]*Lusophone University of Humanities and Technologies, Lisbon, Portugal*
[e]*Instituto de Telecomunicações, R. Marquês D'Ávila e Bolama, Covilhã, Portugal*
[f]*Department of Telecom Engineering, R. V. College of Engineering, Bangalore, India*
[g]*Xavier Institute of Management and Entrepreneurship, Bangalore, India*

[*]asoke.talukder@interpretomics.co, [**]ngarcia@ubi.pt, and [†]jayateertham@gmail.com

1.1 Introduction

The birth of the term "internet" dates to 1969, when the Internet Engineering Task Force (IETF) released the first Request for Comments (RFC 1), a publicly available document that summarizes the contributions of the Internet community on a particular topic. It can also be termed the birth of first-generation Internet—the data communication protocol for researchers. RFC 1 was entitled

Convergence through All-IP Networks
Edited by Asoke K. Talukder, Nuno M. Garcia, and Jayateertha G. M.

ISBN 978-981-4364-63-8 (Hardcover), 978-981-4364-64-5 (eBook)
www.panstanford.com

“Host Software” and dealt with interface message processor (IMP) and host-to-host protocols. The IMP was the packet-switching node used to interconnect participant networks to the Advanced Research Projects Agency Network (ARPANET) from the late 1960s to 1989. The official name for ARPANET was ARPA Network. ARPANET was founded in the United States Department of Defense (DoD) to encourage and fund advance scientific and engineering research to establish the United States as a leader in science and technology. After about 50 years, and after more than four decades of evolution, the Internet became one of the most disruptive technologies that has touched everybody’s life across the world, from infant to old, rich to poor, and woman to man. It is now the main vehicle for data communication, be it in the context of simple e-mail communication, social networking, or even a tool to organize political mass movements.

1.1.1 Generations of the Internet

IMP was the first generation of gateways, which are known today as routers. This is where the foundation of interconnection of data networks was built. Ray Tomlinson, while working as a computer engineer for Bolt Beranek and Newman (BBN) Technologies, invented Internet-based electronic mail in late 1971, which became one of the most popular applications in the Internet. The file transfer protocol (FTP) was introduced through RFC 113 in 1971. Telnet specification RFC 137 was also released in 1971. Then in the following year, in 1972, through RFC 360, remote job entry (RJE) was introduced, which integrated telnet and FTP. Also, in October 1972, Larry Roberts and Robert Kahn demonstrated ARPANET at the International Conference on Computer Communication (ICCC) held in Washington, DC. In the spring of 1973, Vinton Cerf, the developer of the existing ARPANET network control program (NCP) protocol, joined Kahn to work on open-architecture interconnection models with the goal of designing the next protocol generation for ARPANET. ARPA then contracted with BBN Technologies, Stanford University, and the University College at London, England, to develop operational versions of the communication protocol on different hardware platforms. Four versions of the transmission control protocol (TCP) were developed: TCPv1, TCPv2, a split into TCPv3 and IPv3 in the spring of 1978, and then stability with

TCP/IPv4—the standard protocol still in use on the Internet [1]. This protocol was published through RFC 760 in January 1980.

Some researchers suggest 1971 to be the year of the birth of the Internet. In fact, it can be said that internet with lowercase i was born in 1969 and Internet with uppercase I was born in 1971. However, the Internet reached its adulthood in 1980 with the introduction of IPv4 in the Internet protocol (IP) stack. Unlike the internet, which included only the communication protocol of TCP and IP for the data network, the Internet covered both network and applications protocol stacks, including e-mail, telnet, FTP, and RJE. Irrespective of the internet or the Internet, this generation of packet-switching networks and applications on these networks were used by the research community only. On the contrary, in those days, the industry was using its own set of proprietary protocols, such as system network architecture (SNA) from IBM and DECnet from DEC, which included a suite of products comprising both applications and data communication protocols.

Soon the Internet evolved—we can call this the second-generation (2G) Internet. The 2G Internet was the generic data communication protocol; it can be dated to 1989, when interdomain routing was included in the Internet with specifications such as the open shortest-path-first (OSPF) protocol (RFC 1131), the border gateway protocol (BGP) (RFC 1105), and IP multicasting (RFC 1112). These network protocols helped acceptance of the Internet beyond the United States; it became an interworking protocol and spread its influence across the world. Australia, Germany, Israel, Italy, Japan, Mexico, the Netherlands, New Zealand, and the United Kingdom joined the Internet [2]. The number of hosts doubled from 80,000 in January 1989 to more than 160,000 in November 1989.

Then came the emergence of the third-generation (3G) Internet with the invention of the hypertext transfer protocol (HTTP) by Tim Berners-Lee. He wrote the first web client and server in 1990. His specifications of a uniform resource identifier (URI) through RFC 1738, hypertext markup language (HTML) (RFC 1942), and HTTP (RFC 1945) helped the common man use the Internet for general information access. Soon voice was integrated into the Internet in 1995 through the voice over IP (VoIP) protocols. Convergence of these two pathbreaking technologies in the Internet helped it graduate and become a generic media for communication—be it data or information or be it voice, image, or multimedia. By the turn of the century, the domain of the Internet started expanding as more and more services were integrated into the Internet; it took 27 years for the RFC database to reach from RFC 1 to RFC 1945, but following the release of HTTP, in just 13 years more than 4,000 RFCs were added to the Internet specification suite. From this evolution, the emergence of the next-generation Internet (NGI) became apparent; NGI will overcome most of the current shortfalls of the Internet to allow it to become the technology platform for general communication and services.

1.1.2 Wireless Internet

Freedom from being confined in a determined space is a powerful driver to make researchers and industry want to integrate wireless communications into the target technology. The Internet was no exception—research and industry have constantly been working to make communication mobile through innovative wireless technologies. In the last decade or so, the exponential increase of Internet use (as its evolution traced in the previous pages) has had a tremendous impact on wireless communication. Wireless Internet has undergone phenomenal growth in the sense of technology evolution and development from providing voice services to providing data services, at present, leading to online real-time multimedia connectivity. The evolution of the market of wireless networks can be traced logically, dividing it into three classes: voice-oriented market, data-oriented market, and online multimedia connectivity.

The voice-oriented market has evolved around wireless connection to the public switched telephone network (PSTN). These services further evolved into local and wide-area markets. The local voice-oriented market is based on low-power, low-mobility devices with higher quality of voice. The local voice-oriented applications started with the introduction of the cordless phone (in the 1970s), which uses similar technology used in walkie-talkies that existed since the Second World War. The first digital cordless telephone was the CT-2 standard developed in the United Kingdom in the early 1980s. Then the next-generation cordless telephone was a wireless private branch eXchange (PBX) using the Digital

European Cordless Telephone (DECT) standard. Both CT-2 and DECT had minimal network infrastructure to go beyond the simple cordless telephone and over a larger area and multiple applications. These local systems soon evolved into a personal communication system (PCS), which was a complete system with its own infrastructure, very similar to cellular mobile networks. However, all together, none of the PCS standards became a commercial success and, hence, in the later 1990s were merged with the cellular telephone industry, which was a big commercial success. The idea of cellular networks was very old—in 1947, AT&T Bell Labs came up with an idea of frequency reuse by dividing the coverage area into smaller cells. However, due to various licensing and commercial issues, the cellular mobile telephone technology did not take off at that time [3, 4].

The wide-area voice-oriented market evolved around cellular mobile telephony services that are using terminals with high power consumption, comprehensive coverage, and low quality of voice. The first generation of wireless mobile communication was based on analog signaling. Analog systems implemented in the United States were known as Analog Mobile Phone Systems (AMPSs), while the systems implemented in Europe and the rest of the world were identified as Total Access Communication Systems (TACSs). Analog systems were primarily based on circuit-switched technology and solely designed for voice, not data. The 2G mobile network was based on low-band digital data signaling. The most popular 2G wireless technology is known as the global system for mobile communication (GSM). GSM [5] was first implemented in 1991. GSM technology is the combination of frequency division multiple access/time division multiple access (FDMA/TDMA) and is now operating in about 140 countries. A similar technology called personal digital communications (PDC) using TDMA technology emerged in Japan. Since then, several other TDMA-based systems have been deployed worldwide. While GSM was being developed in Europe, code division multiple access (CDMA) was being developed in the United States. CDMA uses spread spectrum technology to break speech into small digitized segments. CDMA technology is recognized as providing clearer voice quality with less background noise, fewer dropped calls, enhanced security, and greater reliability and network capacity. The 2G systems are based on circuit-switched technology. The 2G wireless networks are digital and expand the range of applications to more advanced voice services. Although 2G wireless technologies can handle some data capabilities, such as fax and short message service (SMS), the data rate only goes up to 9.6 kilobits per second (kbps).

The wireless data-oriented market evolved around the Internet and computer communication network infrastructure. The wireless data-oriented services may be divided into broadband local, ad hoc, and wide-area mobile data markets. Wireless local networks support higher data rates and ad hoc operations for a low number of users. The wireless local networks are usually referred to as wireless local area networks (WLANs). The major WLAN standard is IEEE802.11; it was first introduced in 1980 and took nearly a decade to complete. Since then, this technology has evolved from IEEE 802.11 to IEEE 802.11 a/b/g/e/n, becoming a powerful wireless technology that supports data rates from 2 Mbps, 11 Mbps, 54 Mbps, up to 600 Mbps. It operates in the industrial, scientific, and medical (ISM) 2.5 GHz band and uses direct sequence spread spectrum (DSSS), orthogonal frequency division multiplexing (OFDM), and multiple input multiple output (MIMO) technologies. Ad hoc networks include wireless personal area networks (WPANs) such as Bluetooth, infrared, and near-field communication (NFC). The coverage of WPANs is smaller than that of WLANs, and they are designed to allow personal devices, such as laptops, cell phones, headsets, speakers, and printers, to connect together without any wiring. Bluetooth is the technology for ad hoc networking and was introduced in 1998. Like a WLAN, Bluetooth operates in ISM but in lower data rates and uses the voice-oriented wireless access method, which provides a better environment for the integration of voice and data services. NFC or radio frequency tags work in very close proximity of only a few centimeters [3].

The wide-area wireless data market provides for Internet access for mobile users. The technologies belong to this category are 2G+ and worldwide interoperability for microwave access (WiMAX). GSM, PDC, and other TDMA-based mobile system providers and carriers have developed 2G+ technology, which is packet based and increases the data communication speed to as high as 384 kbps. These 2G+ systems are based on the following technologies: high-speed circuit switched data (HSCSD), general packet radio service (GPRS), and enhanced data rates for global evolution (EDGE). HSCSD, a circuit-switched technology, improves data rates up to

57.6 kbps by introducing 14.4 kbps data coding and by aggregating four radio channel time slots of 14.4 kbps. GPRS is an intermediate step that is designed to allow the GSM world to implement a full range of Internet services without waiting for full-scale deployment of 3G systems. GPRS technology is packet based and designed to work in parallel with the 2G GSM, PDC, and TDMA systems that are used for voice communications and to obtain GPRS user profiles from the location register database. GPRS uses multiples of one to eight radio channel time slots in 200 kHz frequency band allocation for a carrier frequency to enable data speeds up to 115 kbps. The data is packetized and transported over public land mobile networks (PLMNs) using an IP backbone so that mobile users can access services on the Internet, such as the simple mail transfer protocol (SMTP)/post office protocol (POP)-based e-mail, and FTP- and HTTP-based web services. The EDGE standard improves the data rates of GPRS and HSCSD by enhancing the throughput per time slot [4].

The wireless real-time multimedia market has evolved around high-speed Internet connectivity and real-time multimedia communications. The major technologies in this domain are 3G, WiMAX, and Wi-Fi. The 3G technology represents a shift from voice-centric services to multimedia-oriented (voice, data, and video). 3G mobile devices and services have transformed wireless communications into online real-time connectivity providing location-specific services that offer information on demand. 3G wireless technology represents the convergence of various 2G wireless communication systems into a single global system that includes both terrestrial and satellite components. 3G uses three air interfaces to accomplish this: wideband CDMA, CDMA2000 (also known as International Mobile Telecommunications (IMT)-multicarrier, or IMT-MC), and Universal Wireless Communications (UWC)-136. Through these technologies, 3G systems provide good quality of voice, higher data rates for mobile service users to get high-speed Internet, and multimedia connectivity.

WiMAX technology is developed as a broadband wireless communication standard to provide wireless data services with high data rates with high-speed Internet connectivity. Within a few years, it has emerged as the de facto standard for broadband wireless communication, providing stiff competition to 3G systems.

WiMAX enables ubiquitous delivery of wireless broadband service for fixed/mobile users. Current mobile WiMAX technology is mainly based on the IEEE 802.16e standard, which specifies an orthogonal frequency division multiple access (OFDMA) air interface and provides support to mobility. WiMAX provides flexible bandwidth allocation, multiple built-in types of quality of service (QoS) support, and a nominal data rate up to 100 Mbps with a covering range of 50 km. Also, WiMAX has a provision for the deployment of multimedia services such as VoIP, video on demand (VOD), videoconferencing, multimedia chats, and mobile entertainment.

Adding to this, as traced in earlier paragraphs, the exponential growth of the number of Internet users with high-speed connectivity due to permanent development in IPv4 applications, building over the TCP/IP suite of protocols, the engineering of high-speed routers, and built-in QoS mechanisms, has made IP the unquestioned standard for transportation and routing multimedia real-time packets. Hence, from a network carrier perspective, multimedia access wireless technologies 3G, WiMAX, and WiFi have leveraged IP as a method of transporting and routing their packets. Considering the exponential growth of the wireless industry, in turn, introducing various wireless devices in recent times, this convergence of wireless and Internet technologies through IP connectivity has opened up possibilities for a plethora of devices (wireline and wireless) to be connected through IP. Hence, providing high-speed Internet connectivity over wireless communication is the main commendable task for the convergence of emerging technologies.

Thus, we see that the next-generation network is not merely a network of computers but a connected conglomeration of various networks with diverse Physical layer properties, with a plethora of network elements and devices such as personal computers, laptops, tablets, mobile devices, and personal digital assistants (PDAs), using a variety of applications ranging from voice and data to realtime multimedia communications with mobility.

Obviously, this expansion and usage scenario soon exposed the limitations of IPv4, namely, in terms of its address space, limitation on QoS handling, security, and scalability. Soon, too, became apparent the need for an IP that not only can support large-scale routing and addressing but also is able to impose a low overhead on such tasks (the requirement originated from the wireless media communications area) and that also supports autoconfiguration, built-in authentication and confidentiality, and interworking with current-generation devices, including mobility as a basic element.

To solve this problem, IPv6 was designed to replace IPv4. IPv6 extends the IP address length from 32 bits to 128 bits, that is, IPv6 supports 2^{128} addresses, or approximately 3.4×10^{38} addresses. This allows the allocation of approximately 5×10^{28} addresses for each person on Earth in 2010 (expectedly 6.8 billion people). Along with this, IPv6 is designed to handle the growth rate of the Internet and to cope with demanding requirements on data rates, services, mobility, and end-to-end security, with its built-in QoS and security features.

1.1.3 All-IP Networks

In this volume, we have included chapters on next-generation networks that offer all kinds of multimedia services, in which connectivity and communication happen through the common network-level protocol IPv6. For the reader's convenience, the topics in this volume are divided into three groups: networking, specialized services, and advanced communications. The topics on networking, in general, discuss the connectivity features of next-generation networks, like addressing, switching, routing, multihoming, mobility, and security. The topics on specialized services deal with specific network services and applications. The topics on advanced communications deal with IPv6 on specific Physical layer technologies.

Networking Topics: We have included three chapters in this category: "Addressing and Routing in IPv6" by Jayateertha and Ms. Ashwini B., "Routing inside the Internet Cloud" by Dattaram Miruke, and "Mobility and Security" by Asoke K. Talukder.

Addressing and Routing in IPv6: This chapter discusses five topics: addressing, IPv4 to IPv6 transition, touting, multihoming, and mobility. The Addressing section comprehensively deals with all about IPv6 addressing, like representation, classification, allocation, and assignments. The IPv4 to IPv6 Transition section mainly discusses three main transition techniques to coexist within the IPv4 infrastructure and to provide eventual transition to an IPv6-only infrastructure. The Routing section describes the routing phenomenon in IPv6. After explaining routing essentials like routers, routing algorithms, and routing tables, the section describes in detail three main routing protocols in the context of IPv6: RIPv2, OSPFv3, and BGP-4. The Multihoming section describes multihoming in IPv6 as its key feature, elaborating the concepts of host multihoming and site multihoming. Lastly, the Mobility section describes the basic operation of mobility in IPv6 without going into advanced-level discussions.

Routing inside the Internet Cloud: This chapter exhaustively discuss switching and routing in next-generation networks. It starts with a discussion of routing protocol algorithms and data structures. It discusses routing protocols in detail, which includes multicast routing, policy-based routing, routing, and switching in wireless networks and sensor networks. The chapter also deals with router and switching platform architectures.

Mobility and Security: This chapter discusses mobility in IP for both IPv4 and IPv6. It also deals with advanced mobility features like roaming, handover in IPv6, handover mobile IPv6 over 3G CDMA networks, and security in mobile IPv6. In rgw security section, this chapter describes the inbuilt IPsec protocol of IPv6. It also touches upon the IPsec services provided at the Network layer.

Specialized Services: We have included three chapters in this category: “Transforming Extended Homes” by Jose Bilbao and Igor Armendariz, “Wireless Vehicular Networks: Architecture Protocols and Standards” by Prof. Rola Naja, and “Next-Generation IPv6 Network Security: Toward Automatic and Intelligent Networks” by Artur M. Arsénio, Diogo Teixeria, and João Redol.

Transforming Extended Homes: This chapter analyzes the incipient problem in present home and extended home scenarios in adapting the user’s infrastructure to the revolution of multimedia services, highlighting an all-IP architecture. Toward this end chapter discusses the IP extended home architecture, including challenges involved in adopting the most suitable architecture for new IP services.

Wireless Vehicular Networks: This chapter develops some insight into the design of future broadband vehicular networks capable of adapting to varying vehicle traffic conditions and variable mobility patterns. It also brings the focus on vehicular network standards, vehicular applications, and QoS mechanisms aiming at improving critical dissemination of safety information.

Next-Generation IPv6 Network Security: This chapter presents different works in the area of monitoring traffic for user profiling and security purposes. It provides, as well, a solution for next-generation IPv6 networks, which uses selective filtering techniques combined with an engine traffic deep packet inspection (DPI) to identify applications and protocols that customers use most frequently. Thus it becomes possible to get ISPs to optimize their networks in a scalable and intelligent manner.

Advanced Communications: We have included four chapters in this category dealing with IPv6 on different Physical layer technologies: "The Internet of Things" by Mr. Syam Madanpalli, "6LoWPAN: Interconnecting Objects with IPv6" by Gilberto G de Ameida, Joel Rodrigues, and Lui's M.L. Oliveira, "IP over Optical Fibers" by Nuno M. Garcia, and "IPv6 over WiMAX" by Jayateertha G. M. and and Ashwini B.

The Internet of Things: This chapter introduces the "Internet of Things," that is, a low-power wireless personal area network (LoWPAN) over the Internet. The chapter describes its network architecture, protocol stacks, and applications. It also deals with transmission of IPv6 over LoWPAN and describes the need for IPv6 in realizing the Internet of things.

6LoWPAN: This chapter discusses LoWPANs and devices, the IEEE 802.15.4 standard, the 6LoWPAN specification, and the Adaptation layer, including proposed 6LoWPAN neighbor discovery optimization.

IP over Optical Fiber: This chapter describes issues related to IP over the Physical layer and, in particular, describes the architecture and control of IP over optical networks implementing wavelength division multiplexing (WDM). This chapter also discusses, from an agnostic point of view, the concept of data aggregation, introducing an IP packet aggregation and converter machine. Finally it describes a possible architecture for all-IP optical networks implemented using optical burst switching.

IPv6 over WiMAX: This chapter throws light on the feasibility of the deployment of IPv6 on WiMAX, considering the Network Working Group (NWG)-proposed solution model and issues involved. The main hitch in deployment is due to the fact that WiMAX technology is based on point-to-multipoint architecture, where no direct communication is authorized at the media access control (MAC) layer between two stationary station (SSs)/mobile stations (MSs) but all communication starts and ends at the base station (BS), the impact of this being nonsupportive of multicast communication at the MAC layer in WiMAX, while the stateless autoconfiguration feature of IPv6 requires MAC-level multicast implementation.

References

1. Computer History Museum, http://www.computerhistory.org/internet_ history/internet_history_80s.html.
2. Raj Jain, "Internet 3.0: ten problems with current internet architecture and solutions for the next generation," Military Communications Conference, Washington, DC, October 23–25, 2006, http://www1.cse.wustl.edu/~jain/papers/gina.htm.
3. Asoke K Talukder, Hasan Ahmed, and Roopa R Yavagal, Mobile Computing Technology, Applications and Service Creation (2nd Edition), McGraw-Hill, 2011.
4. Kaveh Pahlavan and Prashant Krishnamurthy, *Principles of Wireless Networks, a Unified Approach*, Prentice Hall of India, 2008.
5. GSM 05.05, GSM Technical Specification, Version 5.1.0: May 1996, www.etsi.org.

Chapter 2

Addressing and Routing in IPv6

Jayateertha G. M.[a,b,*] and B. Ashwini[c]

[a]*Department of Telecom Engineering, R. V. College of Engineering, Bangalore, India*
[b]*Xavier Institute of Management and Entrepreneurship, Bangalore, India*
[c]*ECI Telecom, Bangalore, India*

[*]jayateertham@gmail.com

2.1 Introduction

Currently the Internet protocol version 4 (IPv4)-served computer market has been the driver of the growth of the Internet. It comprises the current Internet and countless other smaller internets. This market has been growing at an exponential rate. The computers that are used at the endpoints of Internet communications range from personal computers to supercomputers. Most of them are attached to local area networks (LANs), and the vast majority is not mobile.

The next phase of growth may not be driven by the computer market alone but the market influenced by the convergence

Convergence through All-IP Networks
Edited by Asoke K. Talukder, Nuno M. Garcia, and Jayateertha G. M.
Copyright © 2014 Pan Stanford Publishing Pte. Ltd.
ISBN 978-981-4364-63-8 (Hardcover), 978-981-4364-64-5 (eBook)
www.panstanford.com

of networks: wireless, wireline, data, voice, and video through all-IP networks. These markets will fall into several areas and are extremely large, apart from having a new set of requirements that were not evident in the early stages of IPv4 deployment. The numerous personal computing devices appear certain to become ubiquitous as their prices drop and their capabilities increase, as the convergence of voice, data, video, and mobile networks into IP networks becomes a reality. A key capability of these computing devices is that they will be networked and will support a variety of types of network attachments, such as radio frequency (RF) wireless networks, infrared attachments, and physical wires. Hence, all of them require internetworking technology and need a common protocol that can work over a variety of physical networks.

Another outcome of this convergence of networks and data is the emergence of a networked entertainment market, viz., quadruple play, video on demand, etc. As the world of digital high-definition television approaches, the difference between a computer and a television will diminish. Hence, there is a need of an IP that not only can support large-scale routing and addressing but also imposes a low overhead (requirement that originates from the wireless media area) and supports autoconfiguration, built-in authentication and confidentiality, interworking with current-generation devices, and mobility as a basic element. Internet protocol version 6 (IPv6) is designed to provide scalability, flexibility, and needs of markets due to the convergence of voice, data, video, and mobility into IP networks in an evolutionary step from IPv4.

Hence, in the following sections, we focus on these design features of IPv6 in terms of addressing, routing, multihoming, and mobility, along with transitional technological challenges.

2.2 Addressing

The rapid growth of the Internet across the world, reaching the remotest places in recent times, has almost exhausted the public 4-byte IPv4 address space. Hence, there is an impending necessity to expand the IP address space. IPv6 is perceived as the next-generation networking protocol, which has been standardized to replace the current IPv4 and was specified in RFC 2360 dated from the mid-1990s to address, among other things, the rapidly diminishing IP address space. This not only ignited the development of IPv6 but also stimulated the development of other technologies that prolonged the life expectancy of IPv4 address space, such as:

- classless interdomain routing (CIDR), enabling regional Internet registries (RIRs);
- allocation of Internet service provider (ISP) address space;
- allocation of private address space using network address translation (NAT) technologies; and
- development of dynamic host configuration protocol (DHCP), with its ability to share addresses among a number of uses on an as-needed basis.

Despite these schemes to better utilize IPv4 address space, the growing Internet subscriber base, due to convergence not only in voice, data, video, and mobility but also in network interfaces and network equipment, has led to a plethora of IP-enabled devices in the market. These, in turn, can increase IPv4 address space consumption, hence diminishing its available capacity [15, 19].

According to industry estimates, in the wireless domain, more than a billion cellular phones, personal digital assistants (PDAs), and other wireless devices will require Internet access, and each will need its own unique IP address. IPv6 supports a 128-bit address space and can potentially support about 3.403×10^{38} unique IP addresses. With this large address space scheme, IPv6 has the capability to provide unique addresses to each and every device or node attached to the Internet.

2.2.1 Addressing Overview

IPv6 increases the size of the IP address from 32 bits to 128 bits. This results in a very large pool of IP addresses, which allow for a broader range of addressing hierarchies and a much larger number of addressable nodes. This eliminates IP address scarcity and, hence, the NAT deployment. Getting rid of NAT results in a simplified network configuration and reduces hardware/software complexity. The large IPv6 address space also fits well with the future vision of networked homes, in which various appliances and gadgets will be networked and managed over the Internet. Hence, now onward, the deployment of wireless and mobile devices will not be hampered because of IP address scarcity.

We begin this section with a discussion on IPv6 address representation and then look into the IPv6 header format, which contains IPv6 addresses of the source and the destination. We also discuss the classification of IPv6 addresses and end the section with a discussion on some special types of IPv6 addresses.

2.2.1.1 Address representation

A 128-bit (16 bytes) IPv6 address is represented by a sequence of eight components separated by colons as follows:

< comp.0>: < comp.1>: ...< comp.7>

Each component <comp.*i*> consists of 16 bits (0 or 1), represented as four hexadecimal digits. Each hexadecimal digit represents 4 bits as per the mapping of each hexadecimal digit (0 to F) to its 4-bit binary mapping as follows:

0 = 0000	4 = 0100	8 = 1000	C = 1100
1 = 0001	5 = 0101	9 = 1001	D = 1101
2 = 0010	6 = 0110	A = 1010	E = 1110
3 = 0011	7 = 0111	B = 1011	F = 1111

Note that hexadecimal letters in IPv6 address are not case sensitive (Request for Comments (RFC) 2373 [2]). The following are some IPv6 address examples:

4FDE:0000:0000:0002:0022:F376:FF38:AB3F
3FFE:80F0:0002:0000:0000:0010:0000:0000
2001:0660:3003:0002:0a00:20ff:fe18:964c

To represent an IPv6 address more succinctly, RFC 4291 [12] gives the following rules:

- Drop the leading zeros within any 16-bit component.
- Represent any consecutive set of zero components into a double-colon but use only one.

Applying these two rules to the above IPv6 address examples, they can be written as follows:

4FDE::2:22:F376:FF38:AB3F
3FFE:80F0:2::10:0:0 or 3FFE:80F0:2:0:0:10::
2001:660:3003:2:a00:20ff:fe18:964c

Note that there are always eight components in an IPv6 address representation.

Hence, it is easy to calculate how many of them are zeros with a single double-colon. However, with more than one double-colon, it becomes ambiguous.

Consider an IPv6 address, for example, 4C62:0:0:56FA:0:0:0:B5.

We can abbreviate this address as either 4C62::56FA:0:0:0:B5 or 4C62:0:0:56FA::B5 but not as 4C62::56FA::B5, since we cannot decode this unambiguously as it could represent any of the following:

4C62:0:0:0:56FA:0:0:B5, 4C62:0:0:56FA:0:0:0:B5.

2.2.1.2 IPv6 header format

To get an intuitive feeling of an IPv6 address, which forms one of the fields of each IPv6 packet header, we need to understand the format of the IPv6packet header. Hence, here we briefly touch on the IPv6 packet header format, explaining its salient features [4].

IPv6 has a different packet header structure compared with IPv4. This is best illustrated by Figs. 2.1 and 2.2. As shown in the illustration, the IPv6 packet header is simplified compared with IPv4. The Options fields have been restructured to follow the header and are no more part of the IPv6 packet header.

This makes IPv6 packet header processing at intermediate nodes much easier. The Header Length and Total Packet Length fields of the IPv4 header are replaced by the Payload Length field. The (Type of Service (TOS)) field in the IPv4 header is replaced by the Traffic Class (TC) field. The Time to Live (TTL) field in the IPv4 header is replaced by the Hop Limit field in the IPv6 header. The Protocol field of the IPv4 header is replaced by the Next Header field in the IPv6 header. Finally, a new Flow Label field has been added to provide the quality of service (QoS).

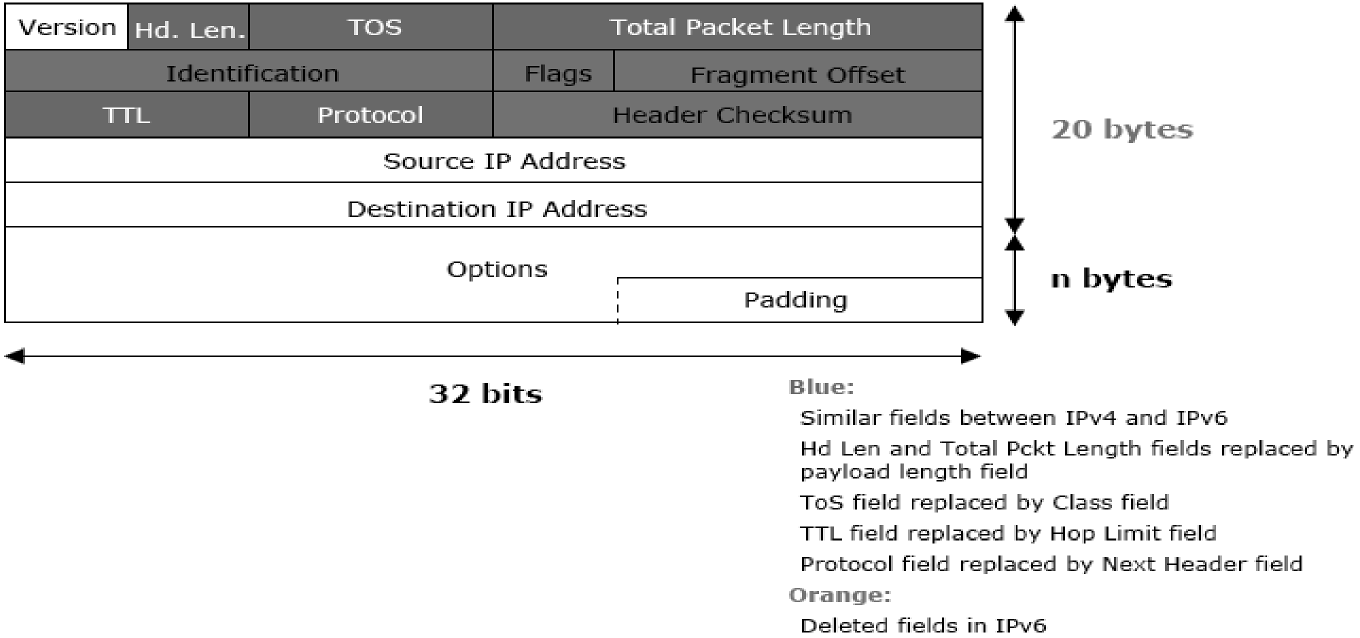

Version
Hd. Len.
TOS
Total Packet Length
Identification
Flags
Fragment Offset
TTL
Protocol
Header Checksum
Source IP Address
Destination IP Address
Options
Padding
20 bytes
n bytes
32 bits
Blue:
Similar fields between IPv4 and IPv6
Hd Len and Total Pckt Length fields replaced by payload length field
ToS field replaced by Class field
TTL field replaced by Hop Limit field
Protocol field replaced by Next Header field
Orange:
Deleted fields in IPv6

Figure 2.1 IPv4 packet header format.

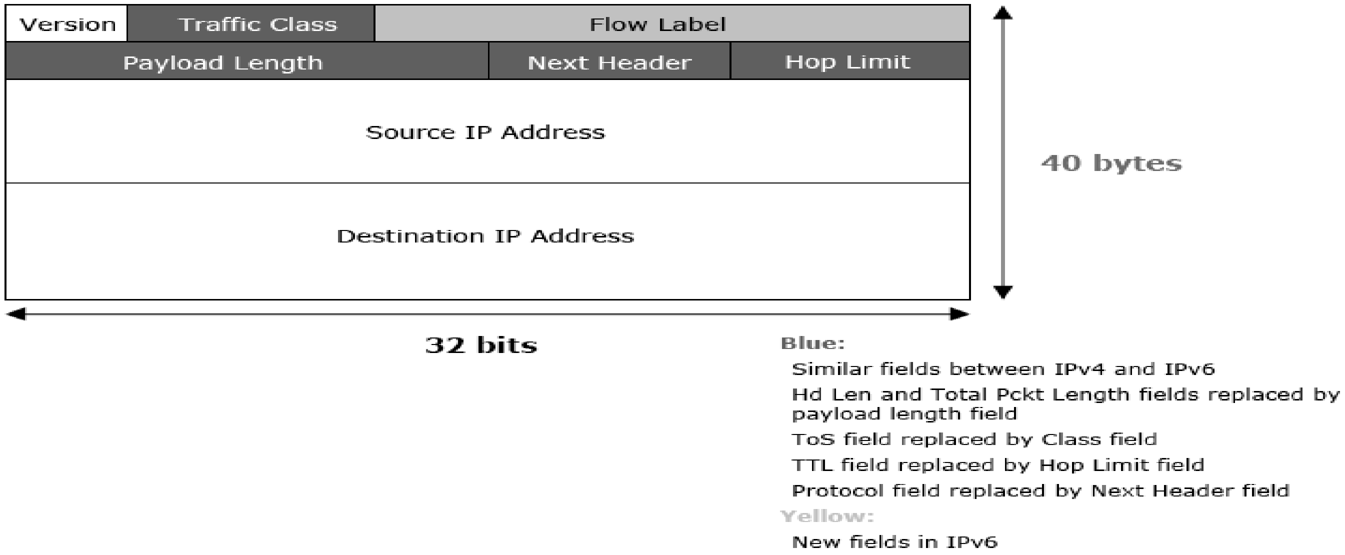

Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source IP Address
Destination IP Address
40 bytes
32 bits
Blue:
Similar fields between IPv4 and IPv6
Hd Len and Total Pckt Length fields replaced by payload length field
ToS field replaced by Class field
TTL field replaced by Hop Limit field
Protocol field replaced by Next Header field
Yellow:
New fields in IPv6

Figure 2.2 IPv6 packet header format.

2.2.1.3 IPv6 address prefix representation

An IPv6 address prefix representation is a combination of the IPv6 address prefix (or an IPv6 address) and its prefix length. This takes the following form:

IPv6 prefix (or IPv6 address)/prefix length

where the IPv6 prefix variable follows the general IP address rule specified in RFC 4291 [2, 12] and the prefix length is a decimal value that indicates the number of contiguous higher-order bits of an IP address that makes the network portion of the IPv6 address.

Note that the IPv6 prefix representation can be used to represent a block of address space (network address range or network) and also the unique IPv6 address. IPv6 address prefix representation, used to denote a network of addresses, is also called classless interdomain routing notation. We explain this by considering the following examples:

Example 1: Consider the IP address 2001:CB8E:2A::D15/64. Expanding the IPv6 address we get:

2001:CB8E:002A:0000:0000:0000:0000:0D15

Expanding the IPv6 address into complete binary format, and since the prefix length is 64, we can identify the network portion by putting the slash after 64 bits as follows:

0010 0000 0000 0001 1100 1011 1000 1110 0000 0000 0010 1010 0000
0000 0000 0000/0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 1101 0001 0101

We can write this in the IPv6 prefix format, which represents the network as follows:

2001:CB8E:2A:: /64 is a network.

Example 2: Consider another example: 2002:3F0E:102A::7/48.

2002:3F0E:102A:0000:0000:0000:0000:0007 (expanding the IPv6 address)

0010 0000 0000 0010 0011 1111 0000 1110 0001 0000 0010 1010/0000

0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000 0000 0111 (fully expanding in complete binary format)
2002:3F0E:102A::/48 is a network.

Example 3: Consider one more example: 3FFE:10C2:43EE:D0C:F::C15/126

3FFE:10C2:43EE:0D0C:000F:0000:0000:0C15 (expanding the IPv6 address)

We can also identify the network address just expanding as follows and putting the slash after 126 bits:

3FEE: 10C2: 43EE:0DOC:000F::0000 1100 0001 01/01
3FEE:10C2:43EE:0DOC:F::0C14/126 is a network.

From these examples, it is clear that the smaller the network prefix, the larger the block of addresses.

2.2.1.4 Address types

Three main types of IPv6 addresses have been defined in the literature by primary addressing and routing methodologies used in networking, viz., unicast addressing, anycast addressing, and multicast addressing.

A unicast address identifies a single unique network interface. The IPv6 delivers a packet sent to a unicast address to that specific interface.

An anycast address is assigned to a group of interfaces usually belonging to different nodes. A packet sent to an anycast address is delivered to just one of the members of the group, typically the nearest host, according to the routing protocol definition of the distance. An anycast address has the same format as a unicast address and differs only by its presence in the network at multiple points.

A multicast address is used by multiple hosts, which acquire a multicast address destination by participating in the multicast distribute protocol among network routers. A packet sent to a multicast address is delivered to all interfaces that have joined the multicast group. IPv6 does not implement the broadcast address. The broadcast's traditional role is subsumed by multicast addressing to all-nodes local link multicast groups. We study these IPv6 addresses in detail in the following sections.

2.2.2 Unicast Addressing

A unicast IPv6 address is a single unique address identifying an IPv6 interface. ISPs assign these addresses to organizations. Unicast addressing offers globally unique addresses. With the appropriate unicast routing topology, packets addressed to a unique address are delivered to a single interface.

There are several types of unicast addresses in IPv6, viz., aggregatable global unicast addresses, local-use addresses, special addresses, compatibility addresses, and network service access point (NSAP) addresses. Additional address types may be defined in the future. We will discuss these unicast addresses in the following sections. Before starting the discussion on these addresses, let us understand first the general unicast address format, which will help us understand various unicast address types.

2.2.2.1 Unicast address format

Unicast and anycast addresses are typically composed of two logical parts, a 64-bit network prefix (global network prefix + subnet identifier (subnet ID)) used for routing and a 64-bit interface identifier (interface ID) used to identify the host's network interface. The network prefix is contained in most significant 64 bits of the address. RFC 6177 [18] recommends that 56 bits of a routing prefix be allocated to normal users such as home networks, but a 48-bit routing prefix is also possible. In this scenario 8-bit Subnet ID fields are available to the network administrator to define subnets within the given network. The 64-bit interface ID is either automatically generated from the interface media access control (MAC) address using the modified extended unique identifier-64 (EUI-64) format obtained from the dynamic host configuration protocol v6 (DHCPv6) [10] server automatically or assigned manually (Fig. 2.3).

Bits	56	8	64
Fields	Global routing prefix	Subnet ID	Interface ID

Figure 2.3 Unicast address format.

2.2.2.2 Local-use unicast addresses

There are two types of local-use unicast addresses, viz., link-local-use addresses, which are used between on link neighbors, and site-local-use addresses, which are used between the nodes that communicate with other nodes in the same site.

2.2.2.2.1 *Link-local-use addresses*

These are based on an interface ID with a typical format for the network prefix (fixed prefix + zeros), as shown in Fig. 2.4. They are used to reach neighbor nodes attached to the same link and self-configured by the interface. All IPv6 addresses have a link-local-use address.

Bits	10	54	64
Fields	Fixed prefix	Zeros	Interface ID

Figure 2.4 Link-local-use address format.

The prefix fields contain the binary value 1111 1110 10. The 54 zeros that follow make the total network prefix as FF80::/64, the same for all link-local addresses, rendering them nonroutable. Link-local-use addresses are equivalent to automatic private IP addressing (APIPA) IPv4 addresses using the 169.254.0.0/16 prefix. The scope of the link-local-use address is the local link. A link-local-use address is required for neighbor discovery protocol (NDP) procedures and is always automatically configured. For details, the reader is referred to the IPv6 Address Autoconfiguration section.

2.2.2.2.2 *Site-local-use addresses*

Site-local-use addresses are also based on the subnet ID and the interface ID with the first 48 bits of the network prefix (10 bits fixed prefix + zeros), as shown in Fig. 2.5. They are assigned to interfaces within an isolated intranet. This can be easily migrated to a provider-based address and are equivalent to the IPv4 private address space (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16). Site-local-use addresses are not reachable from other sites, and routers do not forward site-local traffic outside the site. The scope of the site-local-use address is the site.

Bits	10	38	16	64
Fields	Fixed prefix	Zeros	Subnet ID	Interface ID

Figure 2.5 Site-local-use address format.

The first 48 bits are always fixed for the site-local address. The fixed prefix has the binary value 1111 1110 11, and the 38 zeros that follow form the first 48 bits of each site-local-use address: FEC0::/48. After these 48 fixed bits is a 16-bit Subnet ID field, with which one can create subnets within the site. After the Subnet ID field is the 64-bit Interface ID field that identifies a specific interface on the network. The aggregatable global unicast addresses and site-local-use addresses share the same structure beyond the first 48 bits of the address.

2.2.2.3 Special unicast addresses

There are some unicast addresses with a special meaning in IPv6. We discuss them here.

2.2.2.3.1 *Unspecified address*

This is an address with all zero bits, represented as 0:0:0:0:0:0:0:0 or :: or ::/128. It is used only to indicate the absence of an address and is equivalent to the IPv4 unspecified address 0:0:0:0. The unspecified address is typically used as the source address for packets that are attempting to verify the uniqueness of the tentative unicast address. The unspecified address is neither assigned to any interface nor used as the destination address.

2.2.2.3.2 *Loop-back address*

This is a unicast local lost address, represented as 0:0:0:0:0:0:0:1 or ::1 or ::1/128. It is typically used to identify a loop-back (virtual) interface, and hence, packets sent to this addresses are looped back to the same host or node and are never sent to any interface. Thus, this address enables a node/host to send packets to itself and is equivalent to the IPv4 loop-back address of 127.0.0.1.

2.2.2.4 Compatibility unicast addresses

These types of unicast addresses are defined to aid in migration from IPv4 to IPv6 and facilitate the coexistence of both IPv4 and IPv6 hosts.

2.2.2.4.1 *IPv4-compatible address*

This address holds an embedded global IPv4 address. This address has the format 0:0:0:0:0:0.w.x.y.z or ::w.x.y.z, where w.x.y.z is the dotted decimal representation of a public IPv4 address, for example, ::129.144.52.38 (the same in IPv6 compressed format would be :: 8190:3426). These addresses are used by dual-stack hosts to tunnel IPv6 packets over IPv4 networks. Dual-stack hosts are hosts with both IPv4 and IPv6 stacks. When an IPv4-compatible address is used as an IPv6 destination, the IPv6 traffic is automatically encapsulated with an IPv4 header and sent to the destination over an IPv4 infrastructure.

2.2.2.4.2 *IPv4-mapped address*

This also holds an embedded global IPv4 address. This address has the format as 0:0:0:0:0:FFFF.w.x.y.z or ::FFFF.w.x.y.z, where w.x.y.z is the dotted representation of a public IPv4 address, for example, ::FFFF.129.144.52.38 (in IPv6 compressed format as ::FFFF:8190:3426). This address is used to represent the address of public IPv4 hosts as an IPv6 address to IPv6 applications that are using AF_INET6 sockets. In this way, these IPv6 applications always deal with the IP address in IPv6 format, regardless of the communication occurring over IPv4 or IPv6 networks. It is important to note that the IPv4-mapped address is used for internal representation only. The IPv4-mapped address is never used as the source or destination address. IPv6 doesn't support the use of IP-mapped addresses.

2.2.2.4.3 *6to4 address*

This address is used by the 6to4 tunneling technique to identify 6to4 packets and tunnel these packets on IPv4 networks. For more information on 6to4 tunneling techniques, the reader is referred to Section 2.3. The 6to4 address is formed by combining the prefix 2002::/16 with the 32 bits of the public IPv4 address of the host, forming a 48-bit prefix. For example, for the IPv4 address of 129.144.52.38, the 6to4 address prefix is 2002:8190:3426::/48.

2.2.2.4.4 *Teredo address*

This address is used in the Teredo tunneling technique [13], which enables the NAT traversal of IPv6 packets over IPv4 networks. A Teredo address has the format shown in Fig. 2.6.

Bits	32	32	16	16	32
Fields	Teredo prefix	Teredo server IPv4 address	Flags	Client port	Client IPv4 address

Figure 2.6 Teredo address format.

The Teredo Prefix field has the value 2001::/32. Flags indicate the type of NAT as either full cone (value = 0 × 8000) or restricted or port restricted (value = 0 × 0000). The client port and the client IPv4 address field represent obfuscated values of their respective values reversing each bit value.

2.2.2.5 NSAP unicast address

This address provides a means for mapping an NSAP address to an IPv6 address. A NAP address uses the fixed prefix of 0000001 and maps the last 121 bits of IPv6 bits of an IPv6 address to an NSAP address. For details of address mapping, the reader is referred to Refs. [1, 14].

2.2.2.6 Aggregatable global unicast address

This address defined in RFC 2374 [3] is globally routable and reachable on IPv6 networks. This address is equivalent to a public IPv4 address. Hence, the scope of an aggregatable global unicast address is the entire IPv6 Internet. As the name indicates, these are designed to be aggregated or summarized to produce an efficient routing infrastructure. This address is identified by its format prefix (FP) 001. The aggregatable global address format is shown in Fig. 2.7.

Bits	3	13	8	24	16	64
Fields	FP	TLA ID	RES	NLA ID	SLA ID	Interface ID

Figure 2.7 Aggregatable global unicast address format. *Abbreviations*: TLA ID, top-level aggregation identifier; NLA ID, next-level aggregation identifier; SLA ID, site-level aggregation identifier.

The fields in the aggregatable global unicast address can be described as follows:

- The Format Prefix field indicates the FP for the aggregatable global unicast address, and its value is 001.
- The Top-Level Aggregation Identifier field indicates the TLA ID for the unicast address. The TLA ID identifies the highest level in the routing hierarchy. TLA IDs are administered by the Internet Assigned Numbers Authority (IANA) and allocated to RIRs, which, in turn, allocate individual TLA IDs to large global ISPs. A 13-bit field allows up to 8,192 different TLA IDs. Routers in the highest level of the IPv6 Internet routing hierarchy are called default-free routers, since they do not have default routes. As a matter of fact, they only route with the 16-bit prefix that corresponds to allocated TLA IDs.
- The RES field is reserved for future use in expanding the size of either the TLA ID or the (NLA ID) fields.
- The Next-Level Aggregation Identifier field indicates the NLA ID for the unicast address. A 24-bit field is used to identify a specific customer site. The NLA ID allows an ISP to create multiple levels of addressing hierarchy to organize addressing and routing and identify sites. The structure of an ISP's network is not visible to default-free routers.
- The Site-Level Aggregation Identifier field indicates the SLA ID for the unicast address. A 16-bit SLA ID is used by an individual organization to identify subnets within its sites. An organization can use these 16 bits to create 65,536 subnets or multiple levels of addressing hierarchy and an efficient routing infrastructure. The structure of a customer network is not visible to the ISP.
- The Interface ID field, a 64-bit field, indicates the interface of a node on a specific subnet.

The aggregate global unicast address creates a three-level topology structure, as shown in Fig. 2.8.

The public topology is a collection of larger and smaller ISPs that provide access to the Internet. The site topology is a collection of subnets within an organization's site. The interface ID identifies a specific interface on a specific subnet within an organization's site.

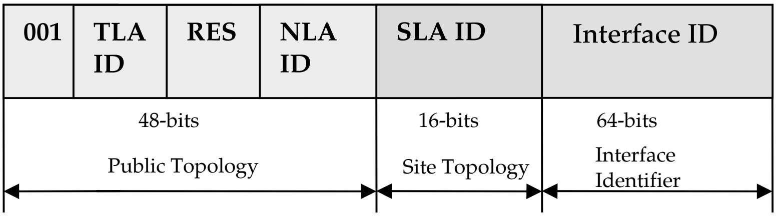


Figure 2.8 Three-level topology structure of global unicast address format.

2.2.2.7 Unique local IPv6 unicast address

The unique local IPv6 unicast address (ULA) is defined in RFC 4193 [11] intended for local communication usually inside a site. It has a globally unique prefix with the probability of uniqueness but is not expected to be routable on the global Internet. ULAs are routable within a limited area such as a site or a limited set of sites. As such they are ISP independent and can be used for communication inside a site without any permanent or intermittent Internet connectivity. It is interesting to note that even if they are accidentally leaked outside a site via routing or the domain name service (DNS), there is no conflict with any other addresses. In fact, applications may treat these addresses like global scoped addresses. or otherwise, assignments of prefixes to these addresses can be both locally as well as centrally assigned local unicast addresses. The unique local unicast address has the format shown in Fig. 2.9.

Bits	7	1	40	16	64
Fields	Prefix	L	Global ID	Subnet ID	Interface ID

Figure 2.9 Unique local unicast address format.

The Prefix field indicates the ULA and has the value FC00::/7.

L = 1 if the prefix is locally assigned.

L = 0; it may be defined in the future but in practice is used for centrally assigned prefixes.

A ULA is created using a pseudorandom allocated global ID, which means there is a relationship between the allocations. Hence, these prefixes are not intended for global routing.

2.2.2.8 EUI-64 address-based interface identifier

RFC 2373 (4291) [2, 12] states that all unicast addresses that use the prefixes 001 through 111 must use a 64-bit interface ID that is derived from an EUI-64 address. The 64-bit EUI address is defined by the Institute of Electrical and Electronics Engineers (IEEE). The EUI-64 address is either assigned to a network interface card or derived from the IEEE 802 MAC address of the network interface card. The IEEE defines mechanism to create an EUI-64 address from an IEEE 802 MAC address. An EUI-64 address is compatible with IEEE 1394 (fir wire specification) and also eases out the autoconfiguration process.

2.2.2.8.1 *IEEE 802 MAC address*

Traditional network interface cards use a 48-bit address called an IEEE 802 MAC address. This address consists of two parts, a 24-bit company ID and a 24-bit extension ID, also called board ID (Fig. 2.10).

Bits	24	24
Fields	cccccug cccccccc cccccccc	xxxxxxxx xxxxxxxx xxxxxxxx
	IEEE-administered company ID	Company-selected extension ID

Figure 2.10 IEEE MAC address format.

The meaning of some special bits within the IEEE 802 address is as follows:

- *Universal/local* (*U/L*) *bit*: This is the seventh bit of the first byte and is used to determine whether the address is universally or locally administered. If U/L = 0, this means the address is universally administered by the IEEE. and if U/L = 1, this means the address is locally administered.
- *Group/individual* (*G/I*) *bit*: It is the low-order bit of the first byte and is used to determine whether the address is an individual (unicast) address or a group (multicast) address. If G/I = 0, the address is unicast, and if G/I = 1, the address is multicast.

For a typical 802 network interface card address, U/L and G/I are set to 0, corresponding to a universally administered unicast address.

2.2.2.8.2 *IEEE 802 EUI-64 address*

The IEEE EUI-64 address represents a new standard for network interface card addressing. It consists of a 24-bit company ID and a 40-bit extension ID, creating a much larger address space. The EUI-64 address uses U/L and G/L bits in the same way as the IEEE 802 address (Fig. 2.11).

Bits	24	40
Fields	cccccug cccccccc cccccccc	xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx
	IEEE-administered company ID	Company-selected extension ID

Figure 2.11 EUI-64 address format.

2.2.2.8.3 *Mapping an IEEE 802 address to an EUI-64 address*

To create an EUI-64 address from an IEEE 802 address, 16 bits 1111 1111 1111 1110 (0xFFFE) are inserted into the IEEE 802 address between the company ID and the extension ID. Figure 2.12 shows the conversion of an IEEE 802 address to an IEEE EUI-64 address.

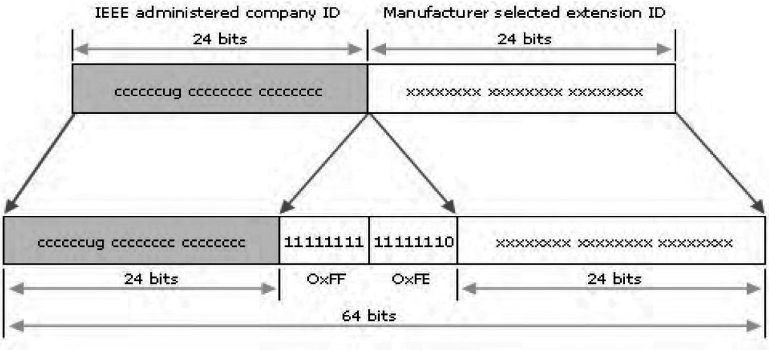

IEEE administered company ID
Manufacturer selected extension ID
24 bits
24 bits
ccccccug cccccccc cccccccc
xxxxxxxx xxxxxxxx xxxxxxxx
ccccccug cccccccc cccccccc
11111111
11111110
xxxxxxxx xxxxxxxx xxxxxxxx
24 bits
0xFF
0xFE
24 bits
64 bits

Figure 2.12 Mapped EUI-64 format.

2.2.2.8.4 *IPv6 interface identifier from mapped EUI-64*

To obtain a 64-bit interface ID for an IPv6 unicast address, the U/L bit in mapped EUI-64 bit address is complemented, that is, the U/L bit is set to 1. Figure 2.13 shows the universally administered unicast EUI-64 bit address to an IPv6 interface address.

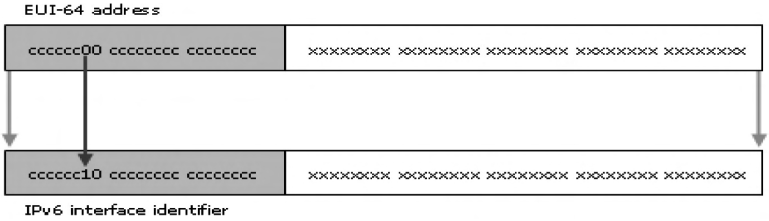

EUI-64 address
cccccc00 cccccccc cccccccc
xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx
cccccc10 cccccccc cccccccc
xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx
IPv6 interface identifier

Figure 2.13 IPv6 interface ID.

Hence, to obtain the IPv6 interface ID from the IEEE 802 address, one should first map the IEEE 802 address to the EUI-64 bit address and then complement the U/L bit. Figure 2.14 shows all steps involved to obtain the IPv6 unicast address interface ID.

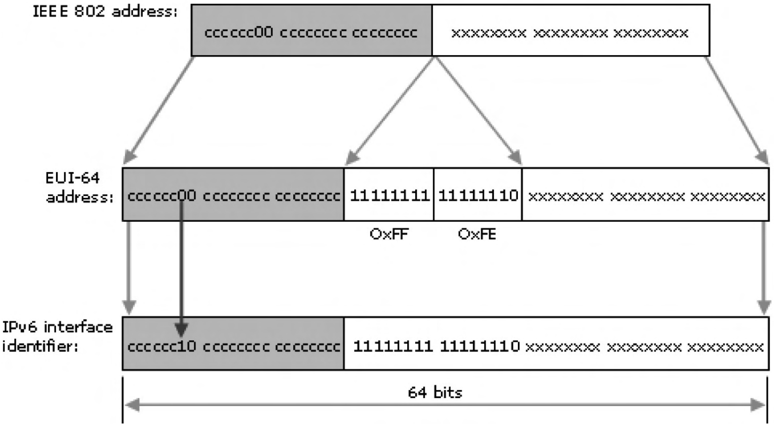

IEEE 802 address:
cccccc00 cccccccc cccccccc
xxxxxxxx xxxxxxxx xxxxxxxx
EUI-64 address:
cccccc00 cccccccc cccccccc
11111111
11111110
xxxxxxxx xxxxxxxx xxxxxxxx
OxFF
OxFE
IPv6 interface identifier:
cccccc10 cccccccc cccccccc
11111111 11111110 xxxxxxxx xxxxxxxx xxxxxxxx
64 bits

Figure 2.14 IPv6 interface ID from an IEEE 802 address.

2.2.3 Multicast Addressing

A multicast address identifies multiple interfaces, and it is used for one-to-many communications. As such, a multicast address cannot be used as a source address. With an appropriate multicast routing topology, packets addressed to a multicast address are delivered to all interfaces that are identified by the address. A multicast address is identified by its FP of 1111 1111 (FF in hexadecimal). It is formed according to several specific formatting rules depending on the applications. In general a multicast address has the format as shown in Fig. 2.15.

Bits	8	4	4	112
Fields	Prefix	Flag	Scope	Group ID

Figure 2.15 Multicast address format.

The fields in a multicast address are described as follows:

- The Prefix field holds the binary value 1111 1111 (FF in hexadecimal) for any multicast address.
- The Flags field indicates the flags that are set on the multicast address. Currently, three of four flag bits are defined. The most significant bit is reserved for future use.
- Flag bits: 0 R P T
- 0 = Reserved for future use
- T = 0, permanent addresses managed by the IANA
- T = 1, transient multicast addresses
- P = 1, derived from unicast prefix
- R = 1, embedded rendezvous point addresses
- The scope field indicates the scope of the internetwork for which the multicast is intended. In addition to the information provided by the multicast routing protocols, routers use the multicast scope to determine whether the multicast traffic can be forwarded. Table 2.1 gives scopes and their respective scope field values.

Table 2.1 IPv6 multicast address scopes and their values

Scope field values	Scopes
1 (0001)	Interface/node local
2 (0010)	Link local
4 (0100)	Admin local
5 (0101)	Site local
8 (1000)	Organizational local
E (1110)	Global

Values 0, 3, and F are reserved, and values 6, 7, 9, A, B, C, and D are not assigned. For example, traffic with the multicast address of FF02::1 has a link-local scope. The router never forwards this traffic beyond the local link.

The Group ID field identifies the multicast group and is unique within the scope. Permanently assigned group IDs are independent of the scope. Transient group IDs are only relevant to a specific scope.

2.2.3.1 Multicast assignments

In this section, we provide main multicast address assignments depending on the scope level of the multicast address. Table 2.2 enumerates IPv6 multicast address assignments based on the address scope.

Table 2.2 IPv6 multicast address assignments based on address scopes

Multicast address	Comp	Assignments
Node-local scope: 1111 1111 0000 0001 FF01		
FF01:0:0:0:0:0:0:1	FF01::1	All nodes address
FF01:0:0:0:0:0:0:2	FF01::2	All routers address
Site-local scope: 1111 1111 0000 0005 FF05		
FF05:0:0:0:0:0:0:2	FF05::2	All routers address
FF05:0:0:0:0:0:0:3	FF05::3	All DHCP servers
FF05:0:0:0:0:0:0:4	FF05::4	All DHCP relays
FF05:0:0:0:0:0:0:8	FF05::8	Service location
Link-local scope: 1111 1111 0000 0002 FF02		
FF02:0:0:0:0:0:0:1	FF02::1	All nodes address
FF02:0:0:0:0:0:0:2	FF02::2	All routers address
FF02:0:0:0:0:0:0:3	FF02::3	Unassigned
FF02:0:0:0:0:0:0:4	FF02::4	DVMRP router
FF02:0:0:0:0:0:0:5	FF02::5	OSPFIGP
FF02:0:0:0:0:0:0:6	FF02::6	OSPFIGP DR
FF02:0:0:0:0:0:0:7	FF02::7	ST routers
FF02:0:0:0:0:0:0:8	FF02::8	ST hosts
FF02:0:0:0:0:0:0:9	FF02::9	RIP routers
FF02:0:0:0:0:0:0:A	FF02::A	EIGRP routers
FF02:0:0:0:0:0:0:B	FF02::B	Mobile agents
FF02:0:0:0:0:0:0:D	FF02::D	All PIM routers
FF02:0:0:0:0:0:0:E	FF02::E	RSVP encapsulation

(*Continued*)

Table 2.2 (*Continued*)

Multicast address	Comp	Assignments
FF02:0:0:0:0:0:1:1	FF02::1:1	Link name
FF02:0:0:0:0:0:1:2	FF02::1:2	All DHCP agents
FF02:0:0:0:0:0:FFXX:XXXX		Solicited node
Global scope: 1111 1111 0000 0001 FF01		
FF0E:0:0:0:0:0:0:101	FF0E::101	NTP server
FF0E:0:0:0:0:0:0:102	FF0E::102	SGI dogfight
FF0E:0:0:0:0:0:0:103	FF0E::103	Rwhod

Abbreviations: DVMRP, distance vector multicast routing protocol; OSPFIGP, open shortest-path-first interior gateway protocol; DR, designated router; RIP, routing information protocol; EIGRP, enhanced interior gateway routing protocol; PIM, protocol-independent multicast; RSVP, resource reservation protocol; NTP, network time protocol; SGI, Silicon Graphics Inc.

2.2.3.2 Solicited node multicast addresses

For each unicast address or unicast address that is assigned to an interface, the associated solicited node multicast group is joined on that interface. The solicited node multicast address has the following format (Fig. 2.16).

Bits	8	4	4	79	9	24 bits
Fields	Prefix	Flag	Scope	Zeros	Ones	Unicast address

Figure 2.16 Solicited node multicast address format.

The Prefix, Flag, and Scope fields hold the binary values 1111 1111, 0000, and 0010, respectively. The Group ID field of a solicited node multicast address is computed as a function of a node unicast address or anycast address. As shown in Fig. 2.16, the scope field of a solicited multicast address is followed by 79 zeros and 9 ones and the last 24 bits are created by coping the last 24 bits of a unicast address or an anycast address. For example, for a node with a link-local unicast address FE80::2AA:FF:FE28:9C5A, the corresponding solicited node multicast address is FF02::1:FF28:9C5A.

The solicited node multicast address facilitates the efficient querying of network nodes during address resolution. In IPv4 address resolution protocol (ARP), the protocol message is sent to MAC-level broadcast for address resolution. But in IPv6, instead of disturbing all IPv6 nodes on the local link by using a local link scope all nodes address, the solicited node multicast address is used as the neighbor solicitation (NS) message destination.

2.2.4 Anycast Address

An IPv6 anycast address is an identifier for a set of interfaces typically belonging to different nodes. A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the nearest interface) according to the routing protocol's measure of distance, as shown in Fig. 2.17. It uses the same format as a unicast address. So one cannot differentiate between a unicast and an anycast address simply by examining the address. Instead, anycast addresses are defined administratively.

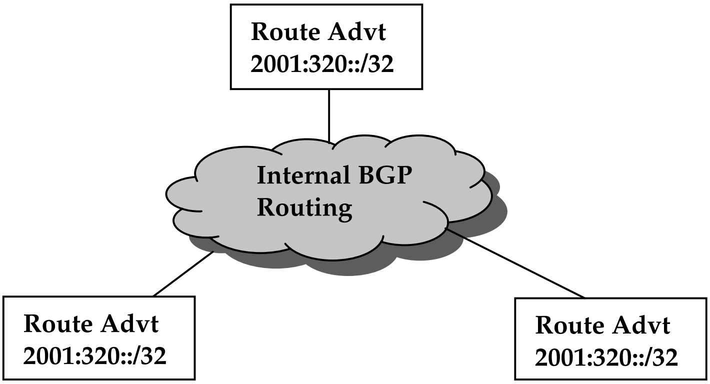


Figure 2.17 Anycast example.

Anycast addresses are taken from the unicast address spaces of any scope and are not syntactically distinguishable from unicast addresses. Anycast is described as a cross between unicast and multicast. Like multicast, multiple nodes may be listening on an anycast address. Like unicast, a packet sent to an anycast address will be delivered to one (and only one) of those nodes. Thus, while a multicast address is used for one-to-many communications, with delivery to multiple interfaces, an anycast address is used for one-to-one of many communications, with delivery to a single interface. The exact node to which it is delivered is based on the IP routing tables in the network.

Also, to facilitate delivery to the nearest anycast group member, the routing infrastructure must be aware of the interfaces that are assigned anycast addresses and their distances in terms of routing metrics. At present anycast addresses are used only as destination addresses and are assigned to only routers. The reserved anycast addresses are defined in RFC 2526 [6] and RFC 4291 [12].

Anycast addressing originally was known as clustering addressing. Motivation for such addressing arises from a desire to allow replication of services. For example, a corporation that offers a service over a network assigns an anycast address to several computers that all provide the service. When a user sends a datagram to the anycast address, IPV6 routes the datagram to one of the computers in the set (cluster). If another user sends a datagram to an anycast address, IPV6 can choose to route the datagram to a different member of the set, allowing both computers to process requests at the same time.

2.2.4.1 Subnet-router anycast address

A subnet-router anycast address is predefined and mandatory for all routers. The format of a subnet router anycast address is shown in Fig. 2.18.

Bits	N	128-*n*
Fields	Subnet prefix	Zeros

Figure 2.18 Subnet-router anycast address format.

It is created from the subnet prefix for a given interface. The bits in the subnet prefix are fixed at their values, and the remaining bits are set to zero. All router interfaces attached to a subnet are assigned the subnet router anycast address for that subnet.

2.2.5 Addresses for Hosts and Routers

In IPv4, generally a host with a single network interface has a single IPv4 address and a router with multiple network interfaces has multiple IPv4 addresses. IPv4 also defines multihoming hosts