



CCBOOTCAMP's CCIE® IPv6 Lab Guide version 1.0

Email :
sales@ccbootcamp.com

Toll Free :
(877) NLI-CCIE (654-2243)
Int: +1 (702) 968-5100

WebSite :
www.ccbootcamp.com
www.routerie.com
www.securityie.com
www.voiceie.com



CCBOOTCAMP's CCIE IPv6 Lab Guide

WRITTEN BY:

ASHWIN KOHLI

CCIE # 8877

NLI's CCIE PRACTICE LABS – IPv6

Ashwin Kohli, CCIE #8877

Published by:

Network Learning Inc.

1997 Whitney Mesa Dr.

Henderson, NV 89014 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America

Warranty and Disclaimer

This book is designed to provide information about the Cisco CCIE lab examination. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The author, and the publisher, Network Learning Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Feedback Information

Feedback should be submitted to the following URL: www.securityie.com and www.routerie.com

That site is monitored daily by our staff. Should you have any comments, suggestions, or complaints feel free to post them on that site.

Trademark Acknowledgments

CCNA™, CCNP™, and CCIE™ are registered Trademarks of Cisco Systems, Inc

Sincerely,

Marc Russell

CEO, Network Learning, Inc.

About the Author

ASHWIN KOHLI, is a dual CCIE #8877 (Routing/Switching and Security). He is currently a Architect for one of the top financial companies, and is responsible for architecting enterprise solutions. He has worked at many of the top financial companies for over 10 years. Ashwin also holds the CCNP®, CCDP® and a BSc in Computer Science & Accounting form Manchester University, United Kingdom. He has more than 10 years experience in Cisco® networking and security including planning, designing, implementing, and troubleshooting enterprise multi-protocol networks. Ashwin also writes Cisco® training material for Network Learning, Inc.

Table of Contents

LEARNING THE BASICS OF INTERNET PROTOCOL	9
Brief History of IP: ARPAnet.....	9
Brief History Of IP:DARPAAnet.....	9
TCP/IP Was Born	10
TCP/IP Layering	10
IP Layer Features	10
IP Versions And Version Numbers.....	11
IPv4 Packet Format.....	12
What Is An IP Address?.....	13
IPv4 Address Format	13
IPv4 MASK	13
IPv4 Addressing.....	13
Classful v Classless.....	13
Variable Length Subnet Mask (VLSM).....	14
IPv4 Address Allocation.....	14
Limitations Of IPv4	15
Why has NAT not solved the address allocation problem?.....	16
IPv6 HISTORY	17
History Of IPv6.....	17
IPv6 HEADER FORMAT	18
IPv6 Architecture	18
Comparison of IPv4 And IPv6 Header	19
IPv6 Packet Format.....	20
Extension Headers	21
IPv6 ADDRESSING ARCHITECTURE	23
IPv6 Address Pool.....	23
IPv6 Text Representations	23
Text Representation Of Address Prefixes.....	24
Illegal IPv6 Prefix Length Representations	24
Address Type Representation	26
Types Of Addressing	28
Aggregatable Global Unicast Address.....	29
Site-Local Address.....	33
Link-Local Address	35
EUI-64 Address-Based Identifier	36

Mapping An 802 Address To EUI-64 Address.....	37
Special IPv6 Addresses.....	38
Compatible Addresses	40
Anycast Address	41
Multicast Address	43
Solicited-node Multicast Address	46
IPv6 Address Assignment.....	47
Summary of IPv4 and IPv6 comparison	48
IPv6 CONFIGURATION FOR WINDOWS XP	49
Installing IPv6 On XP Machine.....	49
Removing IPv6 On XP Workstation.....	51
Configure Interface Attributes	52
View Interface Attributes.....	53
IPv6 Address Configuration Methods	54
Manually Configure IPv6 Addresses.....	55
Pinging Options On XP Workstation.....	56
Pinging The Loopback Interface.....	56
Pinging The Local Interface Of Node.....	57
Pinging Between Two Hosts On Same Subnet.....	57
Other Pinging Options	58
Traceroute	58
IPv6 Routing.....	59
IPv6 Routing Tables	59
IPv6 Node Local Routing Table Details.....	59
View IPv6 Routes On XP Workstation	61
To Add A IPv6 Route Manually On XP Workstation	61
To Remove A IPv6 Route Manually On XP Workstation.....	61
IPv6 Utility On XP Workstation.....	62
IPv6.exe Utility.....	62
IPsec6.exe Utility.....	65
Ping6.exe Utility	65
Tracert6.exe Utility.....	66
Windows IPv6 Applications	67
Troubleshooting IPv6 Configuration	68
ICMP VERSION 6	69
ICMP Overview	69
ICMPv4.....	71
ICMPv6.....	72
Neighbor Discovery (ND).....	73
ICMPv6 Router Solicitation Message (RS).....	73
ICMPv6 Router Advertisement Message (RA)	74

AutoConfiguration	76
Stateless Autoconfiguration Of Link-Local Address (Routers & Hosts)	77
Stateless Autoconfiguration Of Site-Local Address (only Hosts)	77
Stateless Autoconfiguration Of Global Address (only Hosts)	78
States Of AutoConfigured Address	78
Stateful Autoconfiguration.....	80
DHCPv6 Components.....	80
DHCPv6 Ports.....	80
DHCPv6 Multicast Addresses	80
DHCPv6 Client / Server Identification	81
DHCPv6 Server Configuration Parameters	81
DHCPv6 Client / Server Operation On Same Link	81
DHCPv6 Client / Server Operation On Different Links	82
Summary Comparison Between Stateless & Stateful AutoConfiguration	83
ICMPv6 Neighbor Solicitation Message (NS)	84
ICMPv6 Neighbor Advertisement Message (NS)	84
NeighborUnreability Detection.....	86
Redirect Messages	88
Maximum Transmission Unit (MTU) Path Discovery	89
ICMPv6 Security	90
IPv6 ROUTING	91
Introduction.....	91
Static Routes	91
Types of Static Routes	91
IPv6 RIP (RIPng).....	92
OSPFv3	93
Similarities with OSPFv2	93
OSPF Packet Header Comparison	94
OSPF Link State Advertisement Message Format Comparison.....	95
OSPF LSA Type Comparison.....	96
LSA flooding scope Comparison.....	98
Other Major Comparions Between OSPFv2 And OSPFv3	99
OSPFv3 support for IPv6.....	99
OSPFv3 protocol processing per link rather than per subnet	99
Multiple OSPFv3 protocol instances	99
OSPFv3's use of link-local addresses.....	99
Multicast Addresses	99
Unknown LSA types.....	100
Removal Of Authentication	100
Routing Process Not Necessary	100
Interface Configuration Mode.....	100
NBMA Networks	100
Force SPF in OSPFv3	100
OSPFv3 Load-Balancing	101
OSPFv3 Route Authentication.....	101

IS-IS Protocol Overview.....	102
IS-IS For IPv6.....	103
IS-IS Multi-Topology Support For IPv6.....	103
BGPv4.....	104
BGP Path Attributes.....	109
BGPv4 Support For IPv4.....	110
BGPv4 Support For IPv6.....	111
MP_REACH_NLRI Attribute	112
MP_UNREACH_NLRI Attribute.....	112
CISCO IPV6 ROADMAP	113
Cisco IPv6 IOS Roadmap.....	113
12.3T IPv6 Feature Overview.....	117
Cisco Hardware.....	118
Layer 2 Switches.....	119
IPv6 Security Features	120
IPv6 Network Management Features.....	121
IPV6 INTEGRATION & COEXISTENCE WITH IPV4	122
Introduction.....	122
IPv6 Deployment Planning Assumptions	123
IPv6 Transition Planning	123
How Do I Start?	124
Where do I start?.....	125
When Do I start.....	125
How Do You Do It?.....	125
Tunneling IPv6 Over IPv4 Tunnels	126
a) Manual Tunneling.....	128
IPV6 SECURITY	131
IOS Code To Implement IPv6 Security	131
IPv6 Access-Lists.....	131
CONFIGURING IPV6.....	134
Labs Structure	134
Equipment Required	134
Practicing the labs.....	134
Enabling Basic IPv6 On A Router	135
Enable Only IPv6 Address On An Interface.....	138
Configuring IPv6 Address On An Interface	140
Manually Converting Router's Mac Address to EUI-64 Address	146

Configuring IPv6 Address On An Interface – Using EUI-64.....	149
Configuring IPv6 Unnumbered Address	153
Configuring IPv6 Loopback Interface	155
Configuring IPv6 CEF	157
Configuring IPv6 On Ethernet Local Subnet.....	160
Duplicate Address Detection (DAD)	165
Duplicate Address Detection (DAD) Options	168
IPv6 Frame-Relay Point-To-Point Configuration.....	170
IPv6 Frame-Relay Full Mesh Configuration	173
IPv6 Static Routes – Directly Attached IPv6 Static Route	177
IPv6 RIP – Basic Enabling	183
IPv6 RIP – Maximum Paths	192
IPv6 RIP – RIP Timers	195
IPv6 RIP – Default Route	199
IPv6 RIP – Redistribute static.....	204
IPv6 RIP – Route Tagging.....	211
IPv6 RIP – Route Filtering (Incoming)	217
IPv6 RIP – Summary-Route	222
IPv6 RIP – Metric-offset.....	227
IPv6 OSPFv3 – Basic Enabling	232
IPv6 OSPFv3 – Type1 Router LSA.....	245
IPv6 OSPFv3 – Type2 NETWORK LSA.....	259
IPv6 OSPFv3 – Type3 Inter Area Prefix LSA.....	268
IPv6 OSPFv3 – Type4 Inter Area Router LSA	278
IPv6 OSPFv3 – Type5 External LSA	285
IPv6 OSPFv3 – NSSA - Type7 Link-LSA	292
IPv6 OSPFv3 – Type8 Link-LSA.....	301
IPv6 OSPFv3 – Type9 INTRA-AREA-PREFIX-LSA.....	314
IPv6 OSPFv3 – AREA IPSEC Authentication.....	327
IPv6 OSPFv3 – INTERFACE IPSEC Authentication.....	333
IPv6 OSPFv3 – Timer Changes.....	339
IPv6 OSPFv3 – Inter Area Route Summarization	345
IPv6 OSPFv3 – Advertise Default Route	357
IPv6 OSPFv3 – Distribute-List.....	366
IPv6 OSPFv3 – Reference Bandwidth.....	375
IPv6 OSPFv3 – STUB AREA	381
IPv6 OSPFv3 – TOTAL STUB AREA (TSA).....	397
IPv6 OSPFv3 – NOT-SO-STUBBY-AREA (NSSA).....	412
IPv6 OSPFv3 – NOT-SO-STUBBY-AREA (NSSA) – Totally Stubby Area.....	429
IPv6 OSPFv3 – Point-To-MultiPoint.....	447
BGPv4 Support For IPv6 – EBGP Peer Relationship	456
BGPv4 Support For IPv6 – EBGP Peer Relationship – Using Local-Link Addresses	465
BGPv4 Support For IPv6 – IBGP Peer Relationship	472
BGPv4 Support For IPv6 – Redistribution Using A Route-Map	479
BGPv4 Support For IPv6 – Weight Attribute.....	502
BGPv4 Support For IPv6 – EBGP Load Sharing Over Multiple Paths.....	508

BGPv4 Support For IPv6 – ADVANCED LAB.....	514
IPv6 Tunnel – Manual Configuration.....	531
IPv6 Tunnel – GRE Configuration.....	547
IPv6 Tunnel – 6to4 Relay.....	563
IPv6 Access-List – Standard.....	577
IPv6 ICMP - ICMPAccess-Lists.....	583
ISDN - Legacy Dial.....	590
ISDN – Dialer Profile.....	596
Configuring ATM with IPv6 Connectivity On Physical Interface.....	605
Enabling IPv6 QOS – Rate-Limiting Per IPv6 Traffic.....	611
Enabling IPv6 QOS – Low Latrncy Queuing with Marking & Queuing.....	614
Enabling IPv6 NAT-PT (One-To-One Address Translation).....	618
Enabling IPv6 NAT-PT (Pooling).....	621
APPENDIX A- IPv6 RFCs.....	624
APPENDIX B- LAB SETUP & PREPARATION.....	628
Minimum CCIE Rack Setup for R&S and Security.....	628
LAB Topology.....	629
Configuring a Typical Frame Relay Switch.....	630
Configuring a Terminal Server.....	633
Template Configuration.....	635

Table of Figures

Figure 1 - TCP/IP Layering	10
Figure 2 - Format of an IPv4 packet	12
Figure 3 - Field description of IPv4 packet	12
Figure 4 - IPv4 Class Boundaries	14
Figure 5 - Growth of IPv4 Address usage	15
Figure 6 - Growth in devices requiring an IP address	15
Figure 7 - IPv6 Architecture	18
Figure 8 - IPv4 to IPv6 packet header comparison	19
Figure 9 - IPv6 packet format	20
Figure 10 - Field description of IPv6 packet	20
Figure 11 - IPv6 Packet Extension Header	21
Figure 12 - Examples of IPv6 Packet Extension Headers	22
Figure 13 - IPv6 Preferred Format addressing architecture	23
Figure 14 - IPv4 to IPv6 address representation	24
Figure 15 - IPv6 legal address format	24
Figure 16 - IPv6 illegal address format	25
Figure 17 - IPv6 Unicast Address	28
Figure 18 - IPv6 Anycast Address	28
Figure 19 - IPv6 Multicast Address	28
Figure 20 - Aggregatable Global Unicast Address Format	29
Figure 21 - Site-local address format	33
Figure 22 - Single network subnet	35
Figure 23 - Link-local Address Format	35
Figure 24 - IEEE 802 MAC address format	36
Figure 25 - EUI-64 Address Format	37
Figure 26 - Example of mapping 802 address to EUI address	38
Figure 27 - Multiple hosts on different subnets advertised same Anycast address	41
Figure 28 - Anycast address format	41
Figure 29 - Multicast Address Format	43
Figure 30 - Solicited-node Address Format	46
Figure 31 - Converting Ethernet Macc Address to Solicited Node Address	47
Figure 32 - IPv6.exe Utility on an XP workstation	62
Figure 33 - IPsec6.exe Utility on XP Workstation	65
Figure 34 - Ping6.exe Utility on XP Workstation	65
Figure 35 - Tracert6.exe Utility on XP Workstation	66
Figure 36 - ICMP packet encapsulation	69
Figure 37 - ICMPv4 packet format	71
Figure 38 - ICMPv6 Header Format	72
Figure 39 - ICMPV6 Router Solicitation Message	73
Figure 40 - ICMPv6 Router Advertisement Message	74
Figure 41 - Link-local address format	77
Figure 42 - Site-Local Address Format	77

Figure 43 - Global Address format	78
Figure 44 - States of Autoconfigured address.....	78
Figure 45 - DHCPv6 Client and Server Operation on same local link.....	81
Figure 46 - DHCPv6 Client and Server on different subnets	82
Figure 47 – ICMPv6 Neighbor Solicitation Message.....	84
Figure 48 - ICMPv6 Neighbor Advertisement Message	84
Figure 49 - Solicited-node Multicast NS Message for IPv6 Address Resolution.....	85
Figure 50 - Unicast Neighbor Advertisement Message for Address Resolution.....	86
Figure 51 - Steps involved in an ICMPv6 redirect message.....	88
Figure 52 - Steps involved in ICMPv5 MTU Path Discovery.....	89
Figure 53 - OSPFv2 packet header	94
Figure 54 - OSPFv3 Packet Header.....	94
Figure 55 - OSPFv2 LSA packet format.....	95
Figure 56 - OSPFv3 LSA packet format.....	95
Figure 57 - New LSA Type field format	96
Figure 58 - OSPFv2 LSA flooding scope	98
Figure 59 - IS-IS Router types	102
Figure 60 - External Border Gateway Peering between different Autonomous Systems	104
Figure 61 - Comparison between EBGP and IBGP.....	104
Figure 62 - Fixed states a BGP peer progresses through.....	107
Figure 63 - Figure: Courtesy of Cisco © - IOS Roadmap	117
Figure 64 - Innovation Adoption Curve.....	122
Figure 65 - Tunneling IPv6 over IPv4 tunnels.....	126
Figure 66 - Manual Tunneling	128
Figure 67 – IPv6 packet through dual stack router for Manual Tunnel	128
Figure 68 – GRE Tunnel.....	129
Figure 69 - IPv6 packet through dual stack router for GRE Tunnel	130

LEARNING THE BASICS OF INTERNET PROTOCOL

BRIEF HISTORY OF IP: ARPANET

The United States Government commissioned the creation of an organization called the "Advanced Research Projects Agency" or ARPA for short. Work began on researching a decentralized system that would be robust enough to survive and function even if most of the network were destroyed.

Paul Baran of Rand Corporation first conceived the idea for a distributed packet switching network, built on the premise that communication on the network would be unreliable. The network was designed to be able to operate after a nuclear attack had wiped out large portions of the network. After tons of statistical analysis, Paul figured out that by breaking messages up into pieces and sending them via various redundant paths to the destination, messages would be difficult to destroy and hard to intercept. A system with no centralized control point would be difficult to target, let alone destroy. Even if some of the data were to be destroyed, as well as some of the communications points, the message would still get through, and the network would continue to function even when crippled.

After Paul Baran presented his findings, a testbed network was set up. The first machines connected to this experimental communications system (without packet switches between) were a TX-2 located at MIT and an AN/FSQ-32 at System Development Corporation in Santa Monica, CA; and a DEC computer at ARPA. The devices were attached to 1200bps connections (circa 1965). This formed the first 'Experimental Network'.

The government awarded a Packet Switch contract to build Interface Message Processors (IMP) to Bolt Beranik and Newman (BBN) in 1968. BBN chose Honeywell DDP-516's with 12K memory as the connection and interface device. The Interface Message Processor (IMP) devices they built were placed on each of the four designated research sites. These sites were colleges who had won research grants from the US government. UCLA, Stanford, UCSB and University of Utah were the first Universities to interconnect their supercomputers (hosts) via the new ARPAnet IMP's. BBN purchased AT&T 50Kbps dedicated lines for the connections between sites.

BRIEF HISTORY OF IP:DARPANET

As the network was deployed and more government and research institutions were connected to it, the Defense Department took over the project ARPA. The Defense Department administrated the network for several years, and so, the name was changed to DARPAnet (Defense Advanced Research Projects Network) in the early to mid 70's.

The DARPAnet eventually expanded beyond the Defense Department's willingness to sponsor it. More than half the connected sites were Universities receiving government funding, however the networks were in use by more than just the researchers. Around 1971, Ray Tomlinson, originally of BBN, wrote an application to send electronic mail back and forth and later modified it to use the @ symbol (user@host).

It wasn't long before 75% of the traffic on the network was private and personal e-mail. Many of the Defense Department connections were thus dismantled, and the network was handed over to the National Science Foundation (NSF).

TCP/IP WAS BORN

Early on in the 1980's, the Network Control Protocol (NCP) was used to move packets over the ARPANET. This protocol was eventually split into two protocols to isolate functions in separate pieces of software, thus simplifying future software development efforts. The first of the two new protocols was to handle addressing (IP), the second was to ride over it and was designed to handle transport and make it reliable (TCP). Thus was born TCP over IP (TCP/IP).

TCP/IP LAYERING

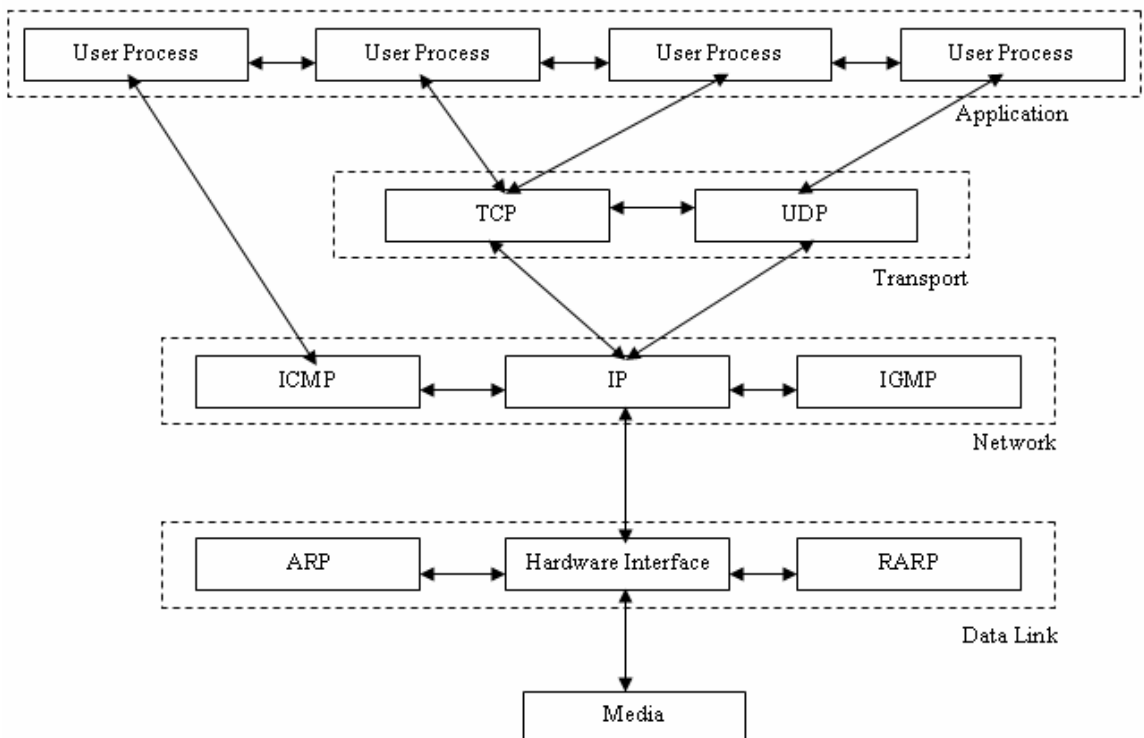


Figure 1 - TCP/IP Layering

TCP and UDP are the two predominant transport layer protocols. Both use the IP as their network layer. Every piece of TCP and UDP data that gets transferred around the Internet goes through the IP layer at both end systems and at every intermediate router.

IP LAYER FEATURES

The following are some of the features that the IP layer provides:

- Connectionless service

- IP addressing

- Data Forwarding

- Fragmentation and reassembly of packets

Best-effort delivery: Delay, out-of-order, corruption, and packet loss are possible. Higher layers should handle this.

IP provides the frame work to encapsulate other protocols like TCP, UDP etc, as shown in figure 1.

IP VERSIONS AND VERSION NUMBERS

IP was created when its function was split from an earlier version of TCP, which combined both TCP and IP functions. TCP evolved through three earlier versions, and was split into TCP and IP for version 4. Confusion arises when most think that there were earlier versions of IP i.e. 1, 2 and 3. However, IP version 4 which was the first version!

Given that it was originally designed for an internetwork a tiny fraction of the size of our current Internet, IPv4 has proven itself remarkably capable. Various additions and changes have been made over time to how IP is used, especially with respect to addressing, but the core protocol is basically what it was in the early 1980s.

IP version 4 is abbreviated IPv4. Unless otherwise qualified, it's safe to assume that "IP" means "IP version 4"—at least for the next few years! Or is it?

Despite how well IPv4 has served us, it was recognized that for various reasons a new version of IP would eventually be required. Due to the difficulties associated with making such an important change, development of this new version of IP has actually been underway since the mid-1990s. This new version of IP is formally called Internet Protocol version 6 (IPv6) and also sometimes referred to as IP Next Generation or IPng.

A natural question at this point of course is: what happened to version 5 of IP? The answer is: it doesn't exist. While this may seem confusing, version 5 was in fact intentionally skipped to avoid confusion, or at least to rectify it. The problem with version 5 relates to an experimental TCP/IP protocol called the Internet Stream Protocol, Version 2, originally defined in RFC 1190. This protocol was originally seen by some as being a peer of IP at the Internet Layer in the TCP/IP architecture, and in its standard, these packets were assigned IP version 5 to differentiate them from "normal" IP packets (version 4). This protocol apparently never went anywhere, but to be absolutely sure that there would be no confusion, version 5 was skipped over in favor of version 6.

IPv4 PACKET FORMAT

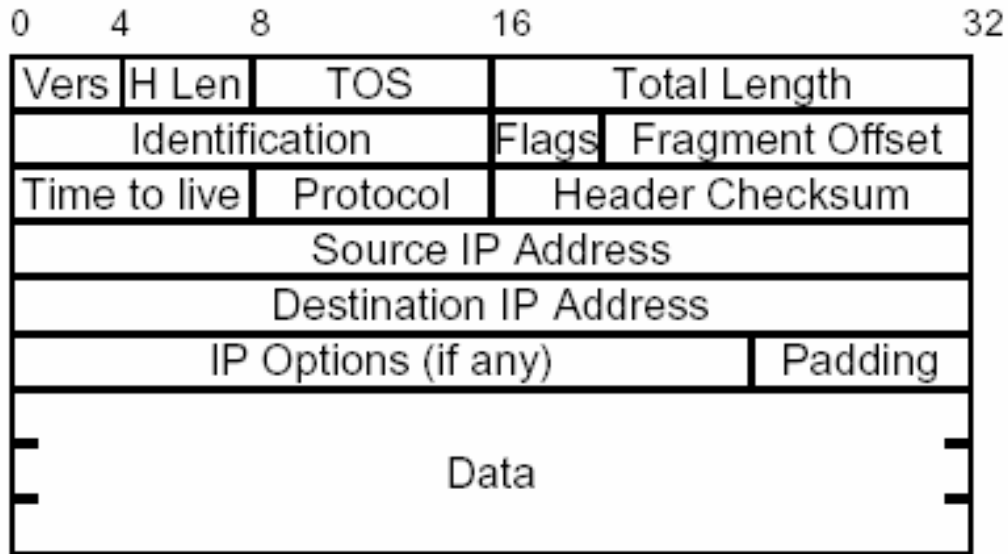


Figure 2 - Format of an IPv4 packet

Field	Explanation	Size (bits)
Version	Version of IP currently used i.e. 4	4
Header Length	Datagram Header Length	4
TOS	Assigns various levels of importance to the datagram e.g. priority	8
Total Length	Length of packet (including data and header). Max size = $2^{16} = 65,535$	16
Identification	If packet size > MTU of data link it is fragmented. The router marks each packet with an identified field	16
Flags	This field indicates whether the datagram can be fragmented or not	3
Fragment Offset	Because fragments may not arrive in the correct order, this field allows the fragments to be reassembled in the right order	5
Time to live	As packets are passed from router to router, each router decrements this field. If the field value reaches zero, the packet is discarded and error message sent to the source. This keeps packets from looping endlessly.	8
Protocol	Indicates which upper layer protocol of the OSI model receives the packet after the IP processing of the packet is complete. Examples of the upper layer protocols are - TCP, UDP, ICMP, OSPF, GRE etc	8
Header Checksum	Helps ensure IP header integrity only and not on the encapsulated data (that is done by TCP)	16
Source IP Address	IP address of the source node	32
Destination IP Address	IP address of the destination node	32
IP Options	It is of variable length. It allows IP to support various options, such as, security, timestamps, route record, loose source routing, etc	
Padding	Extra zero's added to end the field to fill up the 32 bit boundary	
Data	Contains upper layer information	

Figure 3 - Field description of IPv4 packet

WHAT IS AN IP ADDRESS?

Humans work with names. Computers work with numbers. To identify a specific logical connection to a network, a unique number called an 'IP address' is assigned to the network interface of a host. When the IP address is assigned by the network administrator manually, this is called a 'fixed' or 'static' IP address. When the network software assigns the IP address on bootstrap, it's called a 'dynamic' IP.

IPV4 ADDRESS FORMAT

An IP v4 address is a 32-bit binary number, composed of four, 8-bit numbers and is used to identify the logical connection of a host to a physical network. IP v4 addresses are represented as four decimal numbers between 0 and 255 separated by dots; (eg. 172.16.1.1). This is referred to as dotted-decimal notation. Any host attached to an IP network can be assigned an IP address. IP addresses are always unique to each host. Because IP addresses are software configured, it is easy to move hosts from one network to another simply by changing the IP address or the network mask. This process is called renumbering

IPV4 MASK

The mask is a value that is stored in the configuration of a computer along with the IP v4 address. The mask gives the computer a simple way to figure out whether the IP address of another computer is on the same local network, or on a different local network.

IPV4 ADDRESSING

When looking at an IPv4 address, the left-most portion of the address identifies which network the machine (host) belongs to. The right-most portion is used as the address of the host itself.

All hosts on the same network will have the same network address (the network portion will be the same for all hosts). Only the host portion will be different and unique for each host on the network.

CLASSFULL V CLASSLESS

To find a particular host, you first find the network that host is on, then ask that network to find the host. There are two main ways to find a host:

Classless Addressing treats the IPv4 address as a 32 bit stream of ones and zeroes, where the boundary between network and host portions can fall anywhere between bit 0 and bit 31.

Classfull Addressing divides the entire IP address space (0.0.0.0 to 255.255.255.255) into 'classes', or special ranges of contiguous IPv4 addresses. Classfull addressing makes it possible to determine the network portion of the IP address by looking at the first four bits of the first octet in the address. These first sets of four bits are referred to as the 'most significant bits' of the first octet. The value of the first four bits determines the range of actual numerical values of the first octet of the IP addresses in that Network class. From this information, a receiving host can determine which part of the IP address is network, and which is host.

There are 4 main IPv4 classes:

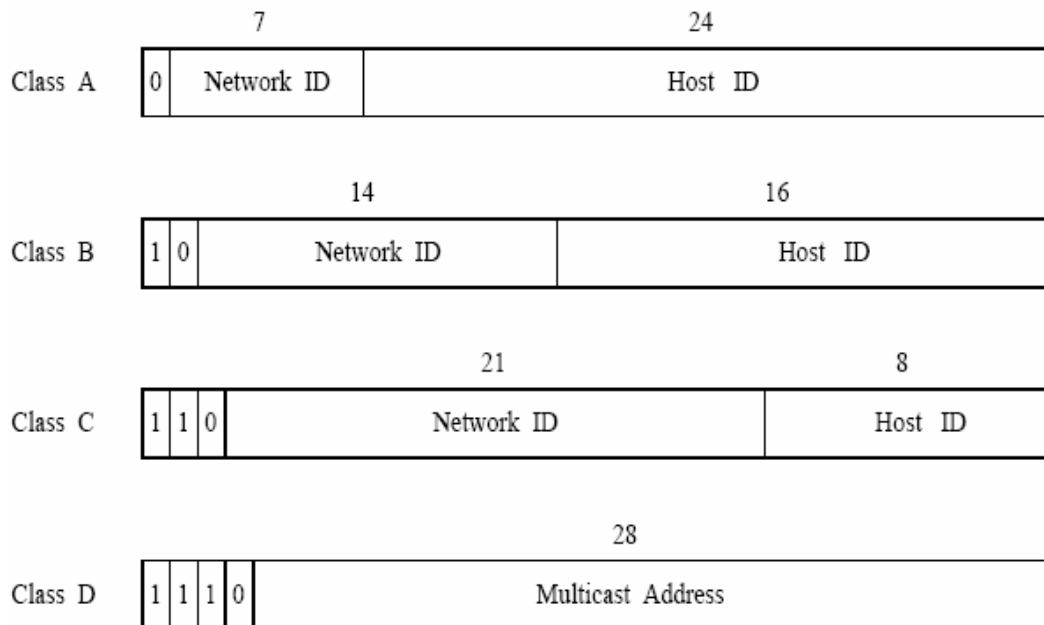


Figure 4 - IPv4 Class Boundaries

VARIABLE LENGTH SUBNET MASK (VLSM)

The Internet's explosive growth eventually required the more efficient use of the IP address space. A technique was developed to carve the Classful address blocks into smaller blocks, to conserve and waste fewer addresses. This process of carving out smaller blocks from larger blocks is known as Subnetting. VLSM is often referred to as subnetting.

Many organization's networks started very small blocks and were assigned class C addresses. A class C address range contains 256 addresses. Soon, these organizations grew and so did their networks. Networks that needed to expand beyond their original class C range used a technique called Supernetting to allow them to turn two contiguous IP address blocks into one network.

IPv4 ADDRESS ALLOCATION

The IPv4 address pool consists of a maximum of 2^{32} addresses or approximately 4.5 billion addresses. The pool of IP addresses is managed by the Internet Assigned Numbers Authority (IANA) <http://www.iana.org/assignments/ipv4-address-space>. The IANA assigned blocks of Class A i.e. /8 addresses to Regional Internet Registries (RIRs) e.g. ARIN, who in turn allocate smaller blocks to local Internet Service Providers (ISPs) e.g. AT&T, UUnet etc.

There are a possible 256 Class A addresses available. Of these:

221 /8 - Class A's are allocated to RIRs i.e. total of 3.7 billion possible addresses.

16 /8 - Class A's are reserved for multicast addresses

16 /8 - Class A's are reserved for future use

3 /8 - Class A's are not use for Internet use.

LIMITATIONS OF IPV4

Of the 221 /8 Class A's possible allocated addresses, 130 /8 Class A blocks have actually been allocated, 89 /8 Class A's blocks are still unallocated and remaining 2 /8 Class A blocks reserved for other use.

With the explosion of the Internet since 1995, it is being predicted that the remaining 89 /8 Class A blocks will be fully exhausted by August 2018. This is shown by Figure 5

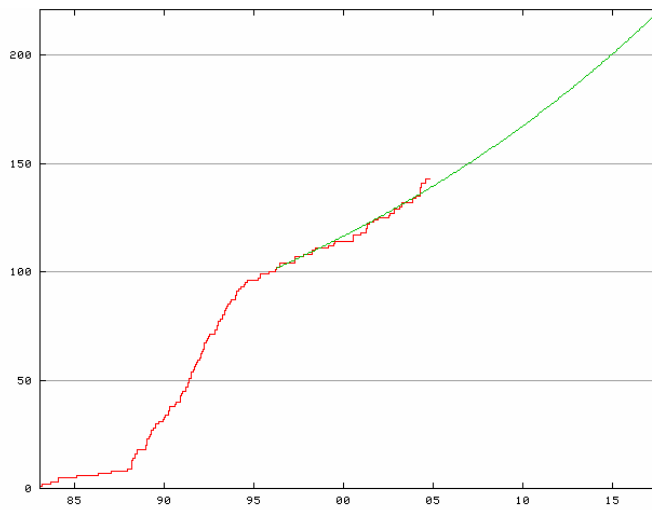


Figure 5 - Growth of IPv4 Address usage

To get the latest projection analysis visit - <http://bgp.potaroo.net/ipv4/>. If all the possible 256 /8 Class A's were allocated to the internet, it is predicted that the complete IPv4 address pool would be completely exhausted by April 2040.

Internet has been the main reason for the explosion of addresses since 1985. However, mobile phones, PDA, home area networks and IP telephony services have expedited the problem.



Figure 6 - Growth in devices requiring an IP address

The IETF first recognized the problem of eventual IPv4 address exhaustion around the 1990s and tried to solve the problem using a number of techniques:

- Network Address Translation
- Classless Inter Domain Routing (CIDR)
- DHCP

These techniques appear to increase the size of the IPv4 address pool, however, they fail to meet the requirements of many peer-to-peer and server-to-client applications.

WHY HAS NAT NOT SOLVED THE ADDRESS ALLOCATION PROBLEM?

NAT is used to translate IANA allocated address to private address space, described by RFC 1918. NAT only delays the exhaustion of the IPv4 address pool and does not solve the problem. Some of the common problems associated with NAT are:

NAT breaks security

NAT requires a state table to be kept of the translation. If the device performing the NAT fails, state connections are lost and routing problems occur.

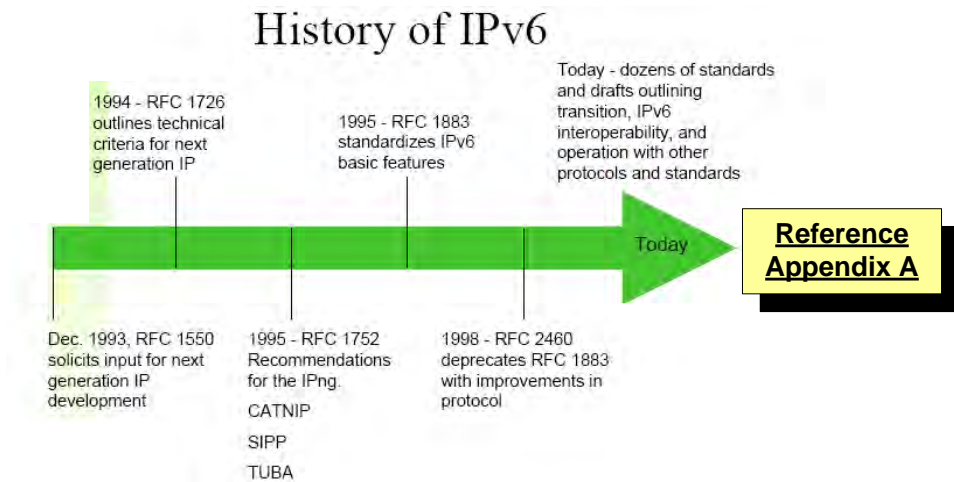
Not all applications are "NAT friendly".

When companies are merging and they have the same internal address space, "double NAT'ing" can cause communication problems between the companies.

IPv6 HISTORY

HISTORY OF IPv6

The following shows a brief timeline of the development of IPv6 RFCs:



IPv6 FORUMS

The following lists some of the important IPv6 forums that can be visited to learn more about the protocol:

- IPv6 Forum - <http://www.ipv6forum.com/>
- 6Bone - <http://www.6bone.net/>
- Cisco IPv6 - <http://www.cisco.com/warp/public/732/Tech/ipv6/>
- Microsoft IPv6 Overview - <http://www.microsoft.com/downloads/details.aspx?FamilyId=27B1E6A6-BBDD-43C9-AF57-DAE19795A088&displaylang=en>

IPv6 STANDARDS

There are various IPv6 standards and these are listed in Appendix A.

IPv6 HEADER FORMAT

IPv6 ARCHITECTURE

As you can see from Figure 7, the architecture of IPv6 is very similar to that of IPv4. The only difference is that the Internet layer which used version 4, has now been replaced by version 6.

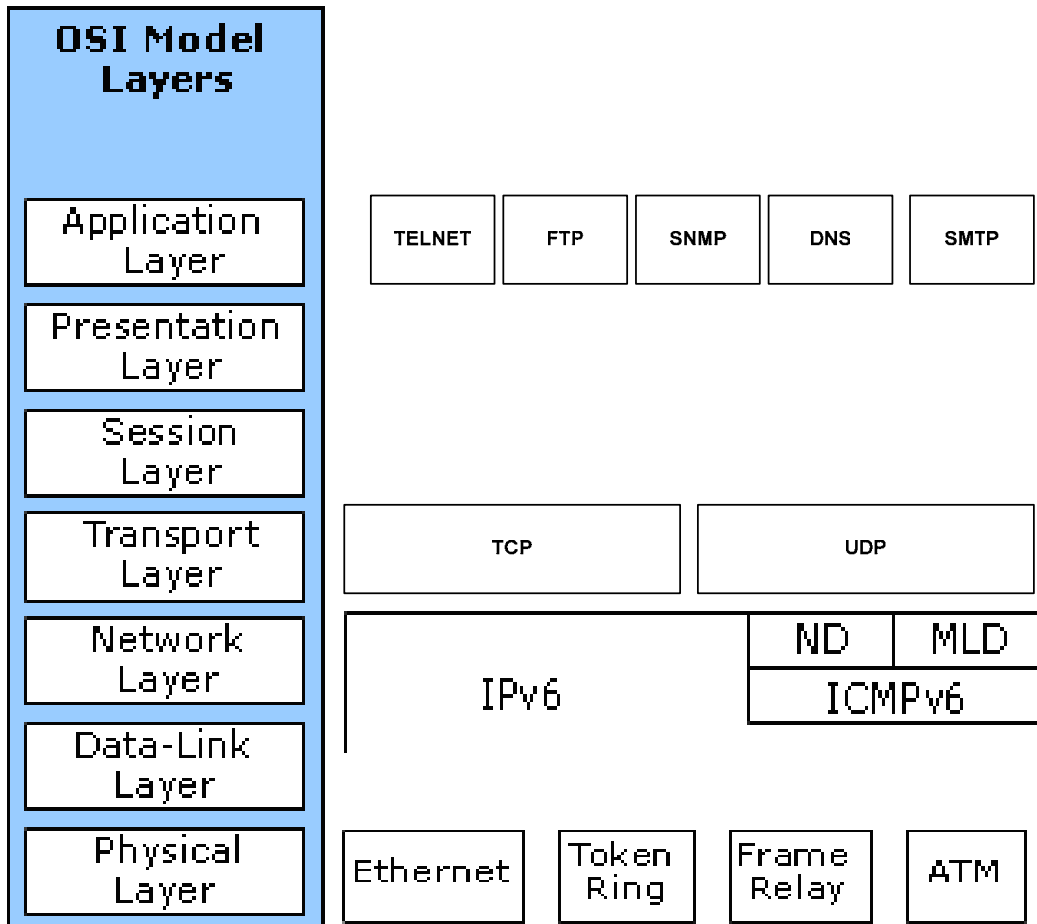


Figure 7 - IPv6 Architecture

COMPARISON OF IPv4 AND IPv6 HEADER

Figure 8 shows the main comparisons between an IPv4 header and an IPv6 header:

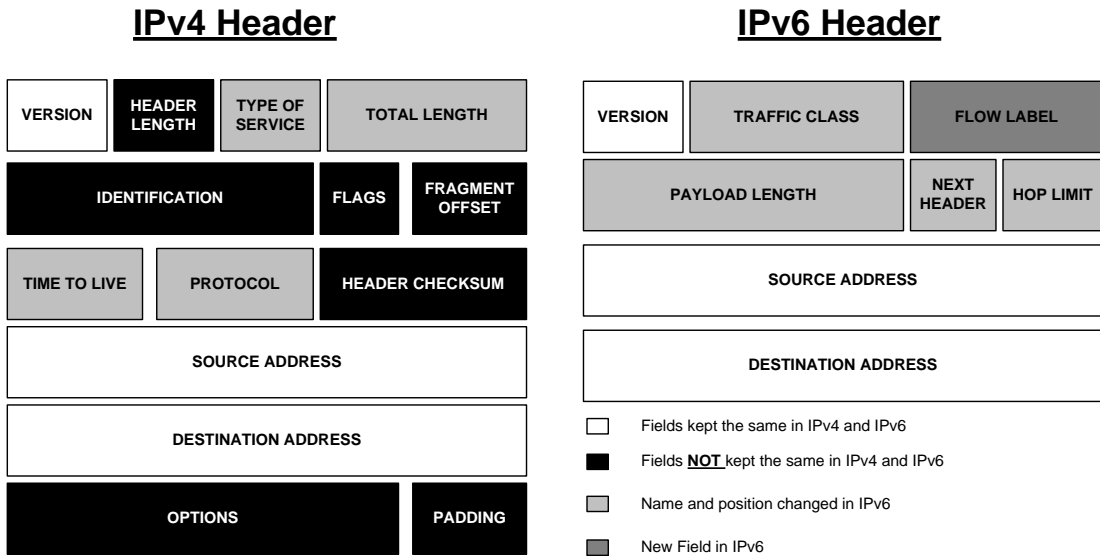


Figure 8 - IPv4 to IPv6 packet header comparison

IPv6 PACKET FORMAT

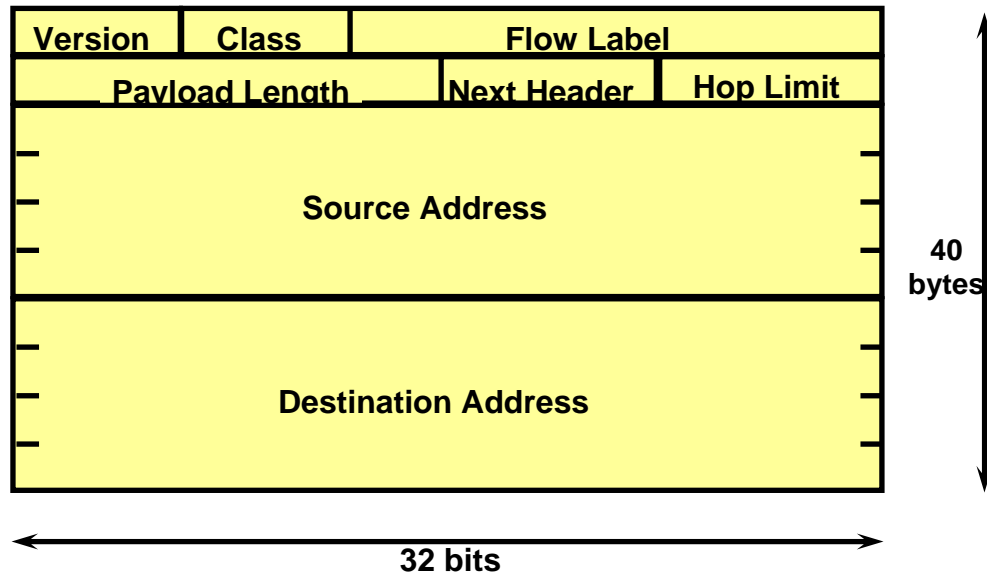


Figure 9 - IPv6 packet format

<u>Field</u>	<u>Length</u>	<u>Description</u>
Version	4 bits	This indicates version 6
Class	8 bits	Similar to IPv4, indicates traffic "class" or priority, so that packets can be forwarded at different priorities to ensure QOS
Flow Label	20 bits	Packets that belong to a specific traffic class, are labeled to identify to which "flow" they belong to. A flow is based on 5 fields: source / destination address, source / destination port and protocol type
Payload Length	16 bits	Length of the remainder of the packet, including extension header
Next Header	8 bits	Identifies the type of header following the packet header.
Hop Limit	8 bits	Number of hops the packet can travel, before it gets discarded
Source Address	128 bits	Sender's IPv6 address
Destination Address	128 bits	Destination's IPv6 address

Figure 10 - Field description of IPv6 packet

EXTENSION HEADERS

Following the IPv6 packet header, there can be more than one header. These additional headers are called Extension Headers. Each header is 8 octets long. Only the destination node must evaluate and process all the headers.

Each header contains a field called Next Header. This field helps continuity to identify the next header if there is one. If this field contains a value of "59", this indicates that there are no subsequent headers.

Figure 11 shows the structure of an IPv6 packet containing extension headers:

IPv6 header	Hop-by-Hop Options header	Destination Options header	Routing header	Fragment header	Authentication header	Encapsulating Security Payload header	Destination Options header (2)	TCP header and data
Next header: Hop-by-Hop Options	Next header: Destination Options	Next header: Routing	Next header: Fragment	Next header: Authentication	Next header: Encapsulating Security Payload	Next header: Destination Options	Next header: TCP	

Figure 11 - IPv6 Packet Extension Header

Packets can include none, some or all of the extension headers. The extension headers are always implemented in the order shown. Each extension header should not occur more than once in a packet.

These extension headers contain information, such as:

Hop-by-Hop Header - The next hop on the path specified by the sender. Each node along the delivery path must examine this header.

Destination Option Header – This is almost identical to the Hop-by-Hop header, except that it is only examined by the destination node. This header appears twice. When it appears last, it is only examined by the destination node, otherwise it is examined by each node defined in the routing header.

Routing Information Header – lists one or more IPv6 nodes to be “visited” on the way to the packet destination. The IPv6 header contains the first node to be visited, and the Routing header contains the list of the remaining nodes, including the final destination.

Fragmented Header - Whether the packet has been formatted. Only the source node can fragment a packet and the packet sent are no more than the paths MTU. IPv6 requires a minimum link of 1280 octets and if a link has a smaller MTU then it must provide link fragmentation and assembly below the IPv6 layer.

Authentication Header – provides data origin authentication and connectionless integrity and is used in conjunction with the ESP header.

Encapsulation Security Payload (ESP) header – provides encryption security and confidentiality. ESP encrypts the data to be protected and places it in the Data portion of the ESP header. There are two encryption modes – Tunnel and Transport mode. In Tunnel mode, the ESP header encrypts the entire IPv6 packet and places it in the encrypted field. In Transport mode, the ESP encrypts transport layer and above (i.e. TCP, UDP, ICMP), and places the encrypted data in the encrypted field.

TCP Header – Defines TCP options.

The following figures show three example of how header options could be stacked up:

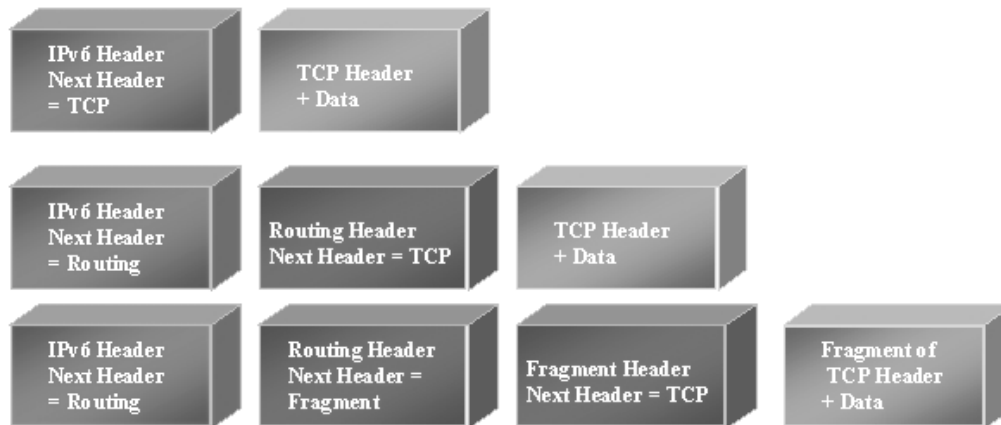


Figure 12 - Examples of IPv6 Packet Extension Headers

IPv6 ADDRESSING ARCHITECTURE

IPv6 ADDRESS POOL

IPv6 uses a 128 (binary - 2^{128}) bit addressing format. If we presume the current population of earth is 10 billion, then each person on earth could possibly have - $3.4 * 10^{27}$ addresses for themselves. No more IP addressing issues☺.

IPv6 TEXT REPRESENTATIONS

There are three different possible text representations of an IPv6 address:

1. **Preferred format** – **x:x:x:x:x:x:x:x**, where each “x” is a hexadecimal value, therefore, each x is 16 bits long. To represent 16 bits using hexadecimal, it is broken down into four sets of hex digits. The values are not case sensitive.

1	2	3	4	5	6	7	8
X:	X:	X:	X:	X:	X:	X:	X
16 bits	16 bits	16 bits	16 bits	16 bits	16 bits	16 bits	16 bits

Figure 13 - IPv6 Preferred Format addressing architecture

An example is:

1	2	3	4	5	6	7	8
FEDC:	BA98:	7654:	3210:	FEDC:	BA98:	7654:	3210
16 bits	16 bits	16 bits	16 bits	16 bits	16 bits	16 bits	16 bits

2. **Multiple Zeros** - IT MAY BE COMMON FOR SOME ADDRESSES TO CONTAIN LONG STRINGS OF ZERO BITS. IN ORDER TO MAKE WRITING SUCH ADDRESSES EASIER, IT IS POSSIBLE TO COMPRESS THE ZEROS, BY USING “::” TO REPRESENT MULTIPLE 16 BITS OF ZEROS. HOWEVER, THE “::” CAN ONLY APPEAR ONCE IN AN IPv6 ADDRESS. THE “::” CAN ALSO BE USED TO COMPRESS LEADING OR TRAILING ZEROS IN AN IPv6 ADDRESS.

For example the following addresses:

Address Type	IPv6 address	Compressed format
Unicast address	1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A
Multicast address	FF01:0:0:0:0:0:0:101	FF01::101
Loopback address	0:0:0:0:0:0:0:1	::1
Unspecified address	0:0:0:0:0:0:0:0	::

3. **IPv4 to IPv6 representation** – In a mixed environment of IPv4 and IPv6 nodes, an alternative format can be used: x:x:x:x:d:d:d:d, where “x” represents the hexadecimal fields of an IPv6 address and the “d” represents the IPv4 address

1	2	3	4	5	6	7	8
X:	X:	X:	X:	d:	d:	d:	d
16 bits	16 bits	16 bits	16 bits	16 bits	16 bits	16 bits	16 bits

Figure 14 - IPv4 to IPv6 address representation

For example:

IPv6 format	Compressed format
0:0:0:0:0:13.1.68.3	::13.1.68.3
0:0:0:0:FFFF:129.144.52.38	::FFFF:129.144.52.38

TEXT REPRESENTATION OF ADDRESS PREFIXES

The text representation of an IPv6 address prefix is similar to that of an IPv4 prefix. It is written as:

IPv6 address / prefix-length

The “/ prefix-length” is a decimal value that indicates the number of contiguous bits that comprise the prefix.

For example, the correct representation of the node address 12AB:0:0:CD30:123:4567:89AB:CDEF and its prefix length /60 is - 12AB:0:0:CD30:123:4567:89AB:CDEF /60.

ILLEGAL IPv6 PREFIX LENGTH REPRESENTATIONS

The following shows example of illegal representations of the node address 12AB:0:0:CD30:123:4567:89AB:CDEF /60.

Legal format
12AB:0000:0000:CD30:0000:0000:0000:0000/60
12AB::CD30:0:0:0/60
12AB:0:0:CD30::/60

Figure 15 - IPv6 legal address format

Illegal format	Reason
12AB:0:0:CD3/60	You may drop leading zeros, but not trailing zeros, within any 16-bit chunk of the address
12AB::CD30/60	address to left of "/" expands 12AB:0000:0000:0000:0000:000:0000:CD30
12AB::CD3/60	address to left of "/" expands to 12AB:0000:0000:0000:0000:000:0000:0CD3

Figure 16 - IPv6 illegal address format