

SAMPLE PAGES from The Lookup Book

1. Six Benefits of IPv6

Almost Unlimited Address Abundance

IPv6 has 3.4×10^{38} possible IPv6 addresses = 340 trillion trillion trillion – about 670 quadrillion addresses per square millimetre of the Earth's surface. (IPv4 has only 4.29×10^9 addresses = 4.3 billion – far less than even a single IP address per person on the planet.)

Easier and Cheaper Network Management

IPv6 networks have auto-configuration capabilities. Networks are simpler, flatter and more manageable, especially large installations. Greater simplicity provides greater reliability and security.

End-to-End Connectivity

IPv6's vast address space means direct peer-to-peer addressing. The need for NAT is effectively eliminated, better for performance, security and troubleshooting. (NAT devices mask thousands of connections, and can hide spammers, crackers and cyberbullies.)

Integrated Mobility and Interoperability

Interoperability and mobility capabilities are improved in IPv6 and are already widely embedded in network devices. (In IPv4, constraints from network topologies limit such capabilities.)

Improved Security Features

IPSec is built into the IPv6 protocol for use with a suitable key infrastructure. (IPv4 was not designed with security in mind, so IPSec was optional.)

Platform for Business Innovation and Processes

Huge size, together with scalability and flexibility of IPv6 networks, fosters innovation, collaboration, streamlined processes and massive-scale real-time reporting of environmental or business conditions.

IPv6 Addresses: 128 bits in 16 bytes

IPv6 address in binary bytes = 00100000 00000001 00001101 10111000 00000000
00000000 00000000 00000000 00010010 00110100 00000000 00000000
00000000 00000000 00000000 00000001

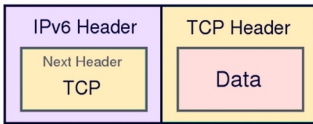
IPv6 address in hexadecimal format = 2001:db8:0:0:1234:0:0:1

Maximum number of IPv6 addresses possible:

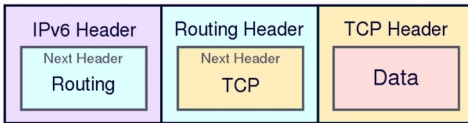
340,282,366,920,938,463,463,374,607,431,768,211,456

IPv6 Prefixes and Numbers of Addresses

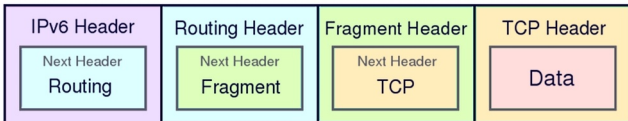
Prefix	Addresses	Quantity
/0	3.4×10^{38}	All possible IPv6 addresses
/8	1.3×10^{36}	1/3 of the luminosity in watts of the Milky Way
/16	5.2×10^{33}	Sun's energy output in joules in half a year
/24	2.0×10^{31}	20 times the number of bacteria on Earth
/32	7.9×10^{28}	42 times the mass of Jupiter in kilograms
/40	3.1×10^{26}	3 times the diameter of the Universe in metres
/48	1.2×10^{24}	20 times the number of stars in the Universe
/56	4.7×10^{21}	Twice the number of grains of sand on Earth
/64	1.8×10^{19}	Eighteen times the number of insects on Earth
/72	7.2×10^{16}	From Earth to the nearest star and back in metres
/80	2.8×10^{14}	The number of leaves on all the trees on Earth
/88	1.1×10^{12}	Three times the number of stars in the Milky Way
/96	4.3×10^9	All possible IPv4 addresses
/104	1.6×10^7	
/112	65,536	
/120	256	
/128	1	



IPv6 packet



IPv6 packet with one extension header



IPv6 packet with two extension headers

Path Maximum Transmission Unit Discovery

Routers do not fragment too-large packets as in IPv4. Instead:

- Host sends packet with MTU set the same as the first hop.
- If packet is too large for a router to forward, it discards the packet.
- Router sends host back an ICMPv6 *Packet Too Big* message, which includes the MTU size of next hop link.
- Host now uses this lower size as MTU and retransmits packet.
- **Essential that firewalls handle ICMPv6 with care!**

IPv6 Packet Sizes

- Minimum packet size is 1280 bytes: 40 bytes header + 1240 bytes of payload.
- Payload Length field is 16 bits, so supports payloads up to 65,535 bytes.
- Packets between 65,536 and 4,294,967,295 bytes = Jumbograms.
- In a Jumbogram, Payload Length is set to 0 and size defined in the Hop-by-Hop Options header.

Ethernet Multicast

The destination link-layer multicast address is 0x3333 plus the last 32 bits of the destination IPv6 multicast address. e.g. Ethernet multicast address for ff02::1:ff54:9b80 is 33:33:ff:54:9b:80

Neighbor Discovery

- Uses ICMPv6 message types 133-137.
- Router Solicitation and Advertisement: routers send regular route advertisements on attached links, or nodes solicit (request) advertisements. Route advertisements carry information about the router and the prefix on the link.
- Neighbor Solicitation and Advertisement: to find out link-layer addresses (equivalent to ARP in IPv4), reachability of neighbours, and to do Duplicate Address Detection.
- ICMP Redirect: routers use Redirects to inform nodes of better first-hop nodes on path to destination.

5. ICMPv6

Internet Control Message Protocol – *must be fully implemented in all IPv6 nodes*. Essential for diagnostics, error messages, path MTU discovery, multicast group management, Neighbor Discovery. See RFC 4443.

ICMPv6 Error Messages: Types 0-127

No.	Type	Code
1	Destination Unreachable	0 = no route to destination 1 = communication prohibited 3 = address unreachable 4 = port unreachable
2	Packet Too Big	0
3	Time Exceeded	0 = hop limit exceeded in transit 1 = fragment reassembly time exceeded
4	Parameter Problem	0 = erroneous header field 1 = unrecognised Next Header type 2 = unrecognised IPv6 option

6. Address Autoconfiguration

Stateless Address Autoconfiguration (SLAAC)

- Stateless Autoconfiguration: host configures its own address
- Address is *generated*, not allocated
- Routers send out route advertisements, or nodes solicit advertisements
- Advertisement contains prefix
- Nodes respond only to /64 prefixes!
- Address lifetimes included in advertisements
- Easy network renumbering: just advertise different prefix
- Host creates address from prefix and generated interface ID
- Suffix from MAC address, or temporary, random or cryptographic
- Address expires, depending on advertised lifetime of prefix

Autoconfigured Address from 48-bit MAC address (EUI-48)

MAC address is expanded to 64 bits by complementing (1 to 0 or 0 to 1) the **seventh bit** and inserting **fffe** after the third octet:

bbbbbb0b bbbbbbbb bbbbbbbb bbbbbbbb bbbbbbbb bbbbbbbb is changed to:
bbbbbb1b bbbbbbbb bbbbbbbb 11111111 11111110 bbbbbbbb bbbbbbbb bbbbbbbb
then appended to advertised prefix to create autoconfigured address. e.g.

Advertised prefix: **2001:db8:0:100::/64**
48-bit MAC: **00:22:fb:54:9b:80** → **0022:fb54:9b80**
Complement bit 7: **0222:fb54:9b80**
Insert **fffe**: **0222:fbff:fe54:9b80**
Autoconfigured address: **2001:db8:0:100:0222:fbff:fe54:9b80**

Devices with EUI-64 (64-bit MAC) addresses simply complement bit 7 then are appended to the prefix.

Autoconfiguration benefits – low cost, huge scalability, fast, no host configuration needed, universally supported, no servers required, can assign globally routable addresses.

Autoconfiguration drawbacks – not secure (but secure Neighbor Discovery available), fails rapidly on error, no policy hooks, no event logging, little address control, no ancillary information.

8. IPv6 Transition Techniques

See RFC4213 on dual-stack and tunnelling techniques.

1. Translation

Uses devices to translate addresses and/or protocols, but has substantial drawbacks. There are a variety of NAT (network address translation) techniques, e.g. NAT444, DS-Lite, 464NAT. Carrier Grade NAT (or Large Scale NAT) has been proposed as a stopgap solution to IPv4 address exhaustion, but problems with all NAT techniques include:

- Loss of end-to-end transparency
- Difficulties with security protocols like IPSec
- Difficulties with address lookups
- Limited flexible routing, single point of failure
- Complexity, scalability, performance issues
- Still require a pool of IPv4 addresses

2. Dual-Stacking

Running hosts and servers with both IPv4 and IPv6 protocol capabilities. Essential transition technique, widely supported, easily implemented, allows staged IPv6 infrastructure and application deployment. When dual-stack servers look up an IPv6 address, if it is not available they fall back to an IPv4 address. Compared to NAT, dual-stacking has only minor drawbacks:

- Two protocol stacks running increases CPU and memory demands
- Need to manage, administer and troubleshoot two networks, not one
- Need different firewall rules in some cases for IPv4 and IPv6
- Still require a pool of IPv4 addresses

3. Tunneling

IPv6 packets are encapsulated within IPv4 packets (protocol 41) or UDP packets (protocol 17), and sent across the IPv4 Internet as usual (IP in IP). Tunneling is the most flexible means of transition, and techniques are continually improving. Major tunneling mechanisms include:

	6in4	6to4	6rd	L2TP	Teredo	ISATAP	TSP
Protocol	41	41	41	udp	udp	udp	udp
Address space	any	2002::/16	any	any	2001::/32	any	any
RFC	4213	3056	5569	2661	4380	5214	5572