IPv6 Now

Easy IPv6

The Lookup Book

Second Edition

Kate Lance

Index

Easy IPv6

The Lookup Book

Second Edition

Kate Lance

Lancewood

The Author

Kate Lance PhD is the Communications Manager of IPv6Now. She has worked in Internet technical services since 1988, and in the IPv6 area since 2005. She is also an award-winning author.

Acknowledgements

Special thanks for suggestions and proof-reading are due to my IPv6Now colleagues, Karl Auer, Tony Hill, Kevin Karp, Michael Biber and George Fong. All remaining errors are the responsibility of the author.

Published by Lancewood Research for IPv6 Now Pty Ltd

First edition 2010
Second edition 2011

ISBN 978-0-9872113-0-9

Lancewood Research
www.lancewood.net
Please contact *lookup@lancewood.net* with any comments

Printed in Australia by Landmark Printing, Melbourne

1. Introduction

What is IPv6?

When we read email or browse a website we're really seeing a host of electrical signals broken into packets by the sending computer, transported in milliseconds through networks across the world, and re-assembled perfectly at our end.

This magic only succeeds if the sender, receiver, and everyone in between agrees on the format of those packets and how to handle them. To navigate through the networks every packet needs a header with sender and destination addresses, and the blueprint for that header is called the Internet Protocol.

The old version of the Internet Protocol, IPv4, has been the foundation of the Internet's success for over thirty years, but the total number of addresses IPv4 can use has a hard limit, already surpassed by today's massive diversity of connected devices.

IPv6 (Internet Protocol version 6) is a vastly improved addressing system for Internet-connected devices. It is not only the glue for an almost inconceivably larger Internet, but helps build safer and more resilient network infrastructure, which in turn drives efficiency, economy and innovation for both business and society.

IPv6 adoption world-wide is essential so that the Internet may continue to expand and innovate into the future. This book provides a quick reference to the technical definitions of IPv6.

IPv6 Review

The year 2011 brought some extraordinary moments in the global transition to IPv6 addressing. On 3 February, the Internet Assigned Numbers Authority (IANA) allocated its final remaining free blocks of IPv4 addresses. While this milestone had been anticipated for years, the timing so early in 2011 came as a surprise.

Even more startling was the announcement on 15 April by the Asia Pacific Network Information Centre (APNIC) that it had reached its final remaining block of IPv4 addresses sooner than expected, due to a 'gold rush' of applications for the dwindling resource. The next registry in line for IPv4 depletion, Europe's RIPE NCC, will probably reach the same point in 2012.

A positive step forward was World IPv6 Day on 8 June, organised by the Internet Society together with major sites such as Facebook, Google, Yahoo!, Akamai and Limelight Networks. This international focus on IPv6 encouraged many others to implement or accelerate their own efforts.

IPv6 offers advantages that underpin the fundamentals of success in business and communications. For some years, governments world-wide have had timetables in place for their transition to IPv6: the Australian government has mandated that its own systems be IPv6-compliant by the end of 2012.

However, until recently, large-scale IPv6 adoption has been gridlocked by the lack of IPv6 transit from Internet Service Providers. Although this situation is improving it is still far from ideal, and the benefits of IPv6 are not yet even close to being realised.

Unfortunately, IPv6 is too often regarded as simply a technical issue which will eventually be solved by 'someone'. But it's not just for techies and the solution is in everyone's hands – and we who enjoy the benefits of the global Internet today need to consider how to facilitate its transition to IPv6 tomorrow.

2. 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 simpler, flatter and more manageable architectures, including auto-configuration capabilities. Greater simplicity and manageability lead to greater reliability, security and economy.

Return of End-to-End Connectivity

IPv6's vast address space means direct peer-to-peer addressing, which is better for performance, security and troubleshooting, and removes the need for stopgap NAT techniques.

Mandated Security Features

IPSec support is mandatory in IPv6, providing authentication and encryption capabilities for use with a suitable key infrastructure. (In IPv4, IPSec support was an optional feature.)

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.)

A Platform for Innovation and Scaleability

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.

3. IPv6 Addresses

IPv6 addresses are written in the hexadecimal number system. Below, from 0 to 31 in binary (machine) format, decimal (IPv4) and hexadecimal:

Binary	Decimal	Hex	Binary	Decimal	Hex
0000	0	**0**	0001 0000	16	**10**
0001	1	**1**	0001 0001	17	**11**
0010	2	**2**	0001 0010	18	**12**
0011	3	**3**	0001 0011	19	**13**
0100	4	**4**	0001 0100	20	**14**
0101	5	**5**	0001 0101	21	**15**
0110	6	**6**	0001 0110	22	**16**
0111	7	**7**	0001 0111	23	**17**
1000	8	**8**	0001 1000	24	**18**
1001	9	**9**	0001 1001	25	**19**
1010	10	**a**	0001 1010	26	**1a**
1011	11	**b**	0001 1011	27	**1b**
1100	12	**c**	0001 1100	28	**1c**
1101	13	**d**	0001 1101	29	**1d**
1110	14	**e**	0001 1110	30	**1e**
1111	15	**f**	0001 1111	31	**1f**

Bit (binary digit) = `0` or `1`
Nibble = 4 bits, e.g. `1011`
Byte = 8 bits, 1 octet, e.g. `00010110`
Word = 32 bits, 4 bytes

IPv4 Addresses: 32 bits in 4 bytes

32 bits in 4 binary bytes = `11000000 10101000 00000001 00000000`
Same IPv4 address in decimal format = `192.168.1.0`
Maximum number of IPv4 addresses possible: **4,294,967,296**

IPv6 Addresses: 128 bits in 16 bytes

128 bits in 16 binary bytes = `00100000 00000001 00001101 10111000`
`00000000 00000000 00000000 00000000 00010010 00110100 00000000`
`00000000 00000000 00000000 00000000 00000001`

Same 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

Representing IPv6 Addresses in Hexadecimal

An IPv6 binary address in 128 bits –

```
001000000000000100001101101110000000000000000000000000000
000000000010010001101000000000000000000000000000000000000
00000000000001
```

Convert the binary to hex – `20010db8000000001234000000000001`

Break into eight groups of 4 hex digits –
`2001:0db8:0000:0000:1234:0000:0000:0001`

(Optional) drop the leading zeros in a group –
`2001:db8:0:0:1234:0:0:1`

(Optional) collapse ONE series of zero groups to `::` –
`2001:db8::1234:0:0:1` or `2001:db8:0:0:1234::1`

4. Prefixes, Subnets and Hosts

The high-order (left-side) bits of an IPv6 address specify the network *prefix*, and all of the addresses in a network have the same prefix. '/N' is used to denote that the prefix is N bits long, e.g. the shorthand for all addresses in the network with the 32-bit prefix `2001:0db8` is `2001:db8::/32`

A typical IPv6 address might have 48 bits of prefix and 16 bits of subnet:

`2001:db8:0:`	`abcd:`	`1234:0:0:7`
48 bits of prefix +	*16 bits of subnet* +	*64 bits of host*

Network `2001:db8:0::/48`
Subnet `2001:db8:0:abcd::/64`
Host `2001:db8:0:abcd:1234::7`

- A standards-compliant subnet size is /64, with 1.8×10^{19} addresses
- Typical enterprise assignment size is /48, containing 65,536 /64 subnets
- Typical ISP assignment size is /32, containing 65,536 /48 subnets

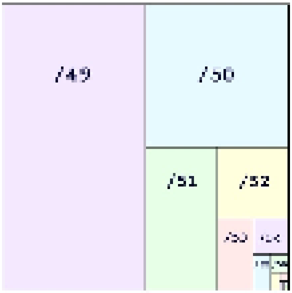
To calculate the number of subnets in a network prefix, take the difference between network and subnet sizes and raise it to the power of 2.

e.g. to calculate how many /48 subnets in a /32 –

32 - 48 = 16 and 2^{16} = 65,536

– so there are 65,536 /64 subnets in a /48 network.

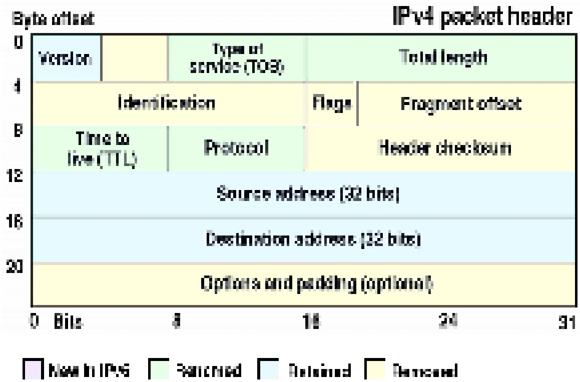
The first allocation from any network halves the largest size allocatable from the remainder, e.g. progressively subnetting a /48 (*right*):

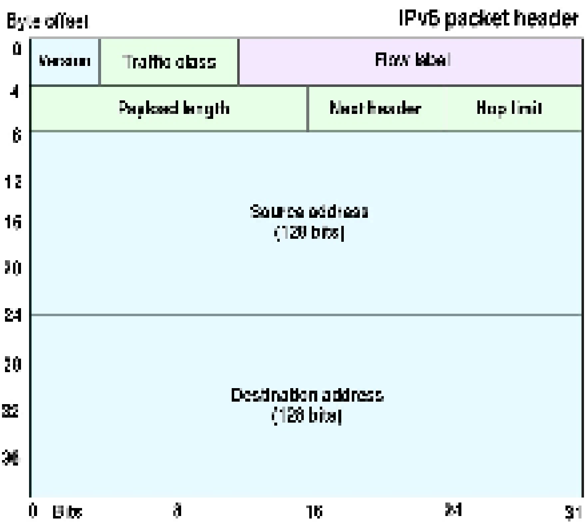


The larger the prefix the smaller the actual network, because it can hold fewer hosts. A /96 prefix network is tiny in IPv6 terms, but is the size of the entire existing IPv4 Internet (*below*):

IPv6 Prefixes and Numbers of Addresses		
Prefix	**Addresses**	**Equivalent 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	

5. IPv6 Packet Headers





IPv6 Header Structure

Unlike IPv4's variable header length, the IPv6 header has a *fixed* 40-byte length. It is simpler, no checksums, has extension headers, & packets are fragmented only at source and reassembled only at destination. Fields are:

- **Version**: 6
- **Traffic class**: to identify different classes or priorities of IPv6 packets.
- **Flow label**: for a packet sequence requesting special handling by routers, e.g. for quality-of-service.
- **Payload length**: length of the packet following the IPv6 header, including extension headers.
- **Next header**: type of header following the current header.
- **Hop limit**: decremented by 1 by each forwarding node. Packet is discarded if hop limit falls to zero.

Next Header Field

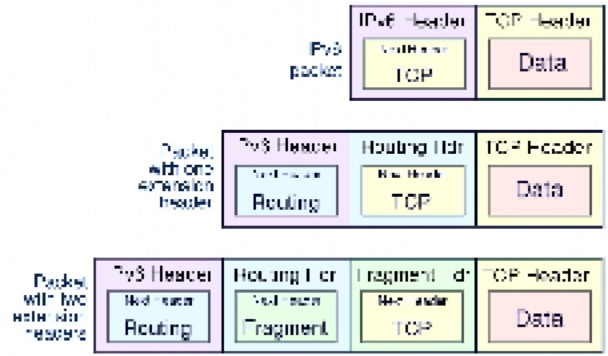
Defines the type of header immediately following the current header. Usually the protocol of the data payload such as TCP or UDP, but may also be one or more Extension Headers, with routing and format options.

Next Header Common Protocol Numbers

002 – ICMP	047 – GRE
004 – IP-in-IP	055 – IP Mobility
006 – TCP	058 – ICMPv6
017 – UDP	089 – OSPFv3
041 – IPv6	103 – PIM
046 – RSVP	

Next Header Extension Headers – in required order of use

000	**Hop-by-hop** – must be examined by every node on path to destination
043	**Routing header** – list of nodes that should be visited on path
060	**Destination options** – processed by routers along path
044	**Fragment header** – packet has been fragmented at source if too large for path
051	**Authentication header** – part of IPSec
050	**Encapsulated security payload** – IPSec
060	**Destination options** – processed at final destination



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 is defined in the Hop-by-Hop Options header.

6. IPv6 Address Types

Unicast – single address, uniquely receives traffic.
Anycast – unicast address on multiple interfaces, any one receives traffic.
Multicast – address for multiple interfaces, all of which receive traffic.

Reserved Address Ranges

Default route	`::/0`
Unspecified address	`::/128`
Loopback/localhost	`::1/128`
Unique-local unicast	`fc00::/7`
Link-local unicast	`fe80::/10`
Multicast	`ff00::/8`
Global unicast	`2000::/3`
Documentation	`2001:db8::/32`
Benchmarking	`2001:0002::/48`
Teredo	`2001:0000::/32`
6to4 space	`2002::/16`
IPv4-mapped IPv6	`::ffff/96`

Unicast Addresses

Unique-local (ULA): IPv6 equivalent to RFC1918 private space. Uses address range `fc00::/7`. Must choose a good random prefix, voluntary registry is at *sixxs.net/tools/grh/ula*. See RFC 4193.

Link-local: automatically generated by any IPv6-capable interface, uses address range `fe80::/10`, never routed outside network. See RFC 4291.

Multicast Addresses

Replaces broadcast in IPv4 and performs many other functions as well. Uses subscription model: listeners join a multicast group and hosts send only to that group – saves bandwidth, CPU.

All link-local nodes have the predefined multicast address: `ff02::1`
All link-local routers have the predefined multicast address: `ff02::2`

Multicast Flags and Scopes

`ff` (8 bits)	**Flag** (4 bits)	**Scope** (4 bits)	**Group ID** (112 bits)

Flag	Scope
0 Well-known 1 Temporary	1 Interface-local 2 Link-local 3 Subnet-local 4 Admin-local 5 Site-local (deprecated) 8 Organisation-local e Global

Well-known Multicast Scopes

Interface-local	`ff01:: /64`
Link-local	`ff02:: /64`
Global	`ff0e:: /64`

Multicast Hosts

`::1`	All nodes	`::a`	EIGRP routers
`::2`	All routers	`::b`	All mobile agents
`::3`	unassigned	`::c`	Simple Service Discovery Protocol
`::4`	DVMRP router	`::d`	All PIM routers
`::5`	OSPF IGP	`::e`	RSVP-encapsulation
`::6`	OSPF IGP DR	`::101`	NTP servers
`::7`	ST router	`::1:1`	Link name
`::8`	ST hosts	`::1:2`	DHCP relay agents & servers
`::9`	All RIP routers	`::1:3`	Link-Local Multicast Name Resolution

Solicited-Node Addresses

A node joins a special multicast group for each unicast address it has. The solicited node address is formed from the link-local scope prefix **`ff02`**, the all-nodes address **`::1`** and the constant value **`ff`**, plus the last 24 bits of the IPv6 unicast address, i.e. **`ff02::1:ffxx:xxxx`**

e.g. Given the unicast address **`2001:db8:0:100::7`**, a node should form the solicited-node address **`ff02::1:ff00:0007`**.

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 Protocol

- Uses ICMPv6 message types 133-137. (More on NDP in Section 16.)
- 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.

7. Internet Control Message Protocol v6

ICMPv6 must be fully implemented in all IPv6 nodes. It is essential for troubleshooting, 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

ICMPv6 Informational Messages: Types 128-255

No.	Type	Description
128 129	Echo Request Echo Reply	RFC 4443 – ping
130 131 132	Multicast Listener Query Multicast Listener Report Multicast Listener Done	RFC 2710 – Multicast group management
133 134 135 136 137	Router Solicitation Router Advertisement Neighbour Solicitation Neighbour Advertisement Redirect Message	RFC 4861 – Neighbor Discovery and autoconfiguration

138	Router Renumbering for IPv6	RFC 2894
139 140	ICMP Node Information Query ICMP Node Information Response	RFC 4620 – IPv6 Node Information Queries
141 142	Inverse Neighbor Discovery Solicitation Inverse Neighbor Discovery Advertisement	RFC 3122 – Extensions to Neighbor Discovery
143	Version 2 Multicast Listener Report	RFC 3810 – MLDv2
144 145 146 147	Home Agent Address Discovery Request Home Agent Address Discovery Reply Mobile Prefix Solicitation Mobile Prefix Advertisement	RFC 3775 – Mobility Support
148 149	Certification Path Solicitation Certification Path Advertisement	RFC 3971 – Secure Neighbor Discovery
151 152 153	Multicast Router Advertisement Multicast Router Solicitation Multicast Router Termination	RFC 4286 – Multicast Router Discovery

8. Address Autoconfiguration

Stateless Address Autoconfiguration (SLAAC)

Major benefit for IPv6 devices: plug in, switch on, globally routable! Stateless Autoconfiguration occurs when a host configures its own address: the address is *generated*, not allocated.

- Router multicasts route advertisements, or host solicits advertisements
- Advertisement contains the prefix
- Host responds *only* to /64 prefixes!
- Host creates address from prefix and generated interface ID
- Interface ID from MAC address, or temporary, random or cryptographic
- Easy network renumbering: just advertise a different prefix
- Address lifetimes in advertisements, hosts must honour lifetimes
- Address expires depending on advertised lifetime of prefix
- Preferred lifetime: how long address *should* be used (can extend)
- Valid lifetime: how long address *can* be used: after this, address invalid

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 and completely on error, no policy hooks, no event logging, little address control, little ancillary information.

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) identifiers simply complement bit 7, then the EUI-64 identifier is appended to the prefix.

Dynamic Host Configuration (DHCPv6)

Stateful Autoconfiguration: DHCP is a protocol that allows a server to supply addresses to hosts in a network: the address is *allocated*, not generated.

- DHCP servers manage and *control* address ranges
- Not limited to /64 subnets
- Can do dynamic DNS, distribute nameserver information
- Can delegate prefixes, allocate multiple addresses at once
- Uses DUID (DHCP Unique Identifier), not MAC address
- All client messages are multicast - uses well-known address `ff02::1:2` (all relay agents & servers)
- Address expires depending on server specification, as with SLAAC

DHCPv6 benefits: Allows control of addresses. DHCPv6 fails more gracefully on error, has policy hooks and event logging.

DHCPv6 drawbacks: not secure – snooping possible, doesn't have boot server, some dual-stack issues getting information from two sources, DUID is tied to host, not an interface.

DHCPv6 Relays

Relays use two special messages with the DHCPv6 message as payload: RELAY-FORWARD (from relays) and RELAY-REPLY (from servers).

- Client multicasts SOLICIT to `ff02::1:2` (all relays and servers).

- Server unicasts ADVERTISEMENT to client, including server DUID.
- Client multicasts REQUEST to `ff02::1:2`, specifying server DUID.
- Server unicasts REPLY back to client, confirming allocation.
- If client sends 'rapid commit' in SOLICIT, all servers REPLY, one used.

9. Domain Name System

See RFC 3596 on the extensions to DNS to support IPv6.

Domain Name-to-Address Mappings (Forward Lookups)

A new AAAA (quad-A) IPv6 record type has been defined. eg:

`dig ipv6now.com.au aaaa` or

`nslookup -type=aaaa ipv6now.com.au` returns:

```
ipv6now.com.au.   521   IN   AAAA  2406:a000::29
```

Address-to-Name Mappings (Reverse Lookups)

- each subdomain represents 4 bits (1 nibble) of the 128-bit address
- ip6.arpa instead of in-addr.arpa
- least significant nibble to the left
- no abbreviations – all nibbles must be shown

e.g. the AAAA record above would have the corresponding PTR record:

```
9.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.6.0.4.2.ip
6.arpa IN PTR   ipv6now.com.au
```

IPv6 DNS Issues

DNS *responses* returned by nameservers can be IPv4 or IPv6 addresses – they are independent of whatever protocol the server itself uses. But IPv4 nameservers and clients can communicate only via IPv4, and IPv6 nameservers and clients only via IPv6, so for full functionality, nameservers should be dual-stacked, i.e. running both protocols.

As IPv6 addresses are physically larger, fewer DNS replies fit into a single packet, so EDNS0 (Extension Mechanisms for DNS) essential for IPv6. See *dns-oarc.net/oarc/services/replysizetest*.

An IPv6-only lookup is only possible if all levels of the recursive lookup chain refer to IPv6-capable nameservers. It is impossible to pre-populate the reverse domain for an IPv6 network, which may affect IP address management systems.

Applications are supposed to try an IPv6 lookup first, and fall back to IPv4, but if nameservers return NXDOMAIN (non-existent domain) for all IPv6 lookups, they will block this fallback process.

10. IPv6 Transition

Today: If IPv6 is available on end-user systems, a variety of transport techniques over IPv4 can be used to access the IPv6 Internet.

Transition : the ideal is full dual-stacking (IPv4 and IPv6 on all devices, and OSs and applications choose preferred protocol), but in practice a mixture of techniques will probably remain during transition.

Future: IPv6 will be the standard everywhere, transport techniques will deal with legacy IPv4 systems as they are phased out.

Dual-Stacking

Dual-stacking means that hosts and servers have both IPv4 and IPv6 protocol capabilities. It is an essential transition method, widely supported, allows staged deployment of IPv6 infrastructure.

It requires an audit and overhaul of logical and physical network elements, e.g. routing, peering, websites, databases, operations support, user access, authentication, accounting, customer premises equipment, etc. See RFC 4213. Drawbacks include:

- Need to manage and troubleshoot two logically distinct protocols.
- Increased CPU and memory demands for two stacks on devices.
- May need different firewall rules for IPv4 and IPv6.
- Dual-stacking still requires a pool of IPv4 addresses.
- Costly in time/staff/resources for large or complex networks.

Transport Techniques

IPv6 and IPv4 are incompatible, although they can coexist on the same physical infrastructure. An IPv4 network cannot deliver IPv6 packets, or vice versa, unless they are either *translated* or *encapsulated*.

Translation

Translation is the stateful mapping of one kind of address protocol to another. Currently widely used in NAT (network address translation) devices to map between public IPv4 addresses and private IPv4 space, translation can also map between IPv6 and IPv4 addresses, e.g. NAT64. Problems with NAT techniques include:

- Loss of end-to-end transparency
- Difficulties with security protocols like IPSec
- Single point of failure of stateful devices
- Complexity, scaleability, performance issues
- Still require a pool of IPv4 addresses

Encapsulation

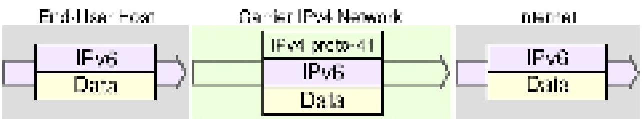
Packets of one protocol are wrapped (encapsulated) inside packets of another protocol for delivery, and unwrapped (decapsulated) at the other end. The process is also called *tunnelling*, and is used widely in telecommunications and IPv6 transition. In the case of IPv6, packets are encapsulated within IPv4 packets (protocol 41) or IPv4-UDP packets (protocol 17), and sent across the IPv4 Internet.

Encapsulation is often used with address prefixing – the construction of an IPv6 address from an IPv6 prefix and the value of an IPv4 address, often with special prefixes to denote specific protocols. See RFC 4213.

11. End-User IPv6 Tunnels

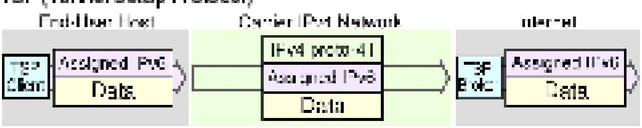
End-users may want IPv6 but their ISP/carrier has not implemented it: hence techniques for bypassing IPv4-only carriers. Techniques have limitations, e.g. *configured tunnels* (6in4, TSP) need high levels of expertise and infrastructure control. *Automatic tunnels* (6to4, Teredo), enabled by default in some Microsoft operating systems, have high failure rates due to DNS shortcomings and dependence on often-blocked protocols. The major end-user techniques are:

6in4



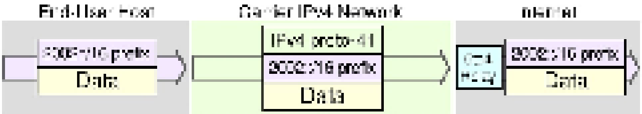
Configured tunneling: IPv6 packets are wrapped inside IPv4 with protocol 41, then at the tunnel endpoint the IPv4 header is stripped and the packet sent to the IPv6 destination. Requires user to configure static address endpoints. See RFC 4213.

TSP (Tunnel Setup Protocol)



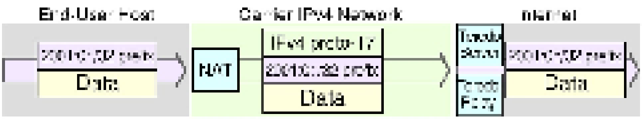
Configured tunneling: Tunnel Setup Protocol – client software makes request to a TSP tunnel broker device to assign IPv6 address. Uses 6in4 encapsulation, relies on 3rd-party tunnel broker. See RFC 5572.

6to4



Automatic tunneling: IPv6 addresses are built up of special prefix 2002::/16 plus the value of the IPv4 address. Outgoing packets are encapsulated with protocol 41. IPv4-to-IPv6 routers/relays strip off IPv4 headers and send IPv6 packets to destination. Problems: relies on 3rd-party relaying servers, and protocol 41 is sometimes blocked by firewalls or filters. See RFC 3056.

Teredo



Automatic tunneling: Uses special prefix 2001:0::/32 plus IPv4 server & host addresses. For hosts behind NATs allowing only IPv4 TCP/UDP. IPv6 packets are encapsulated inside IPv4-UDP packets (protocol 17), then Teredo servers and relays pass IPv6 traffic to destination. Problems: relies on 3rd-party Teredo services, needs (sometimes-blocked) ICMP to negotiate NATs. See RFC 4380.

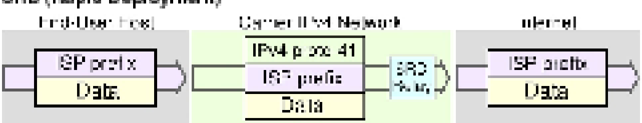
ISATAP

Intra-Site Automatic Tunneling Protocol: used within trusted sites. Runs between dual-stack hosts on IPv4 network. see RFC 5214.

12. Carrier-Grade IPv6 Tunnels

Usually operated by service providers, spanning networks from incoming client systems to border relays. Benefits: providers do not need to immediately dual-stack entire infrastructure – they can run IPv4 internally and also support IPv6 users over transition period. Major techniques:

6RD (Rapid Deployment)

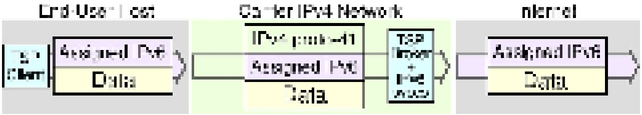


Similar to 6to4 but with major improvement – 6RD routers use the service provider's own prefix rather than 2002::/16, so outgoing and incoming relays are under the service provider's routing control. Removes unreliability of 3rd-party relays or protocol blocking, but still requires additional provider IPv6 services for security, monitoring, DNS, access, accounting, etc. RFC 5569.

MPLS-6PE (Multiprotocol Label Switching – Provider Edge)

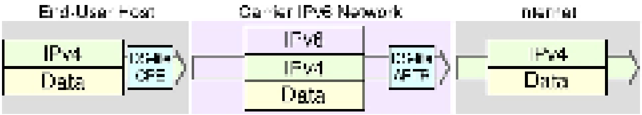
MPLS routers encapsulate packets of any network protocol, creating end-to-end circuits across any type of transport medium. For IPv6 traffic, an IPv4 header is added then packet is directed to a Provider Edge router, where encapsulation is stripped and original packet sent to IPv6 destination. Also requires provider IPv6 services – security, DNS, etc. See RFC 4798.

TSP (Tunnel Setup Protocol – Carrier-Grade)



Carrier's tunnel broker device assigns IPv6 address to authenticated client software endpoints. Runs on stand-alone brokers using provider's own IPv6 address space. Brokers usually have *integrated* security, monitoring, access, authentication, accounting, forward and reverse DNS, NAT functions, multiple encapsulation techniques, etc. See RFC 5572.

DS-Lite (Dual Stack-Lite)



For IPv4 tunnelling inside IPv6. Uses dual-stack CPE (customer premises equipment). Carrier runs IPv6 on own internal networks, so IPv6 traffic simply transits to IPv6 Internet. IPv4 traffic is tunneled inside IPv6 to an Address Family Translation Router (Carrier-Grade NAT), then to IPv4 Internet. DS-Lite is an efficient use of remaining IPv4, but equipment is costly. See RFC 6333.

13. Security and IPv6

IPv6 shares its basic structure with IPv4 so many issues are the same, but it also has features that are specific to IPv6. Most security mechanisms will need overhauling to deal with IPv6, which can pass through IPv4 firewalls unless filters are set to recognise it.

There is more IPv6 traffic on the Internet than generally recognised – some OSs default to IPv6 under certain conditions, and much P2P traffic uses IPv6 – so businesses must monitor IPv6 for internal and external security. See RFC 4942 for IPv6 security problems, transition mechanisms, and IPv6 deployment. Areas to note:

Newness

- IPv6 is young in operational terms, may be issues not yet imagined.
- Affects internal personnel: network administrators, system administrators, support staff, management, users.
- Affects IT component suppliers: vendors, application programmers, operating systems programmers.
- Affects external partners: peering, ISPs and carriers, business partners, outsourcing providers.

Automatic tunnelling

Microsoft Windows Vista has automatic tunnelling mechanisms enabled out of the box – 6to4, Teredo, ISATAP. Not all will actually work – may need external servers, globally routable IPv4 addresses etc. But if they do work it creates a new path direct to the host, and hosts and firewalls are probably unprepared.

Tunnels are useful, but not if they are unexpected or unwanted. Automatic tunnelling can be prevented by firewalling, e.g. block 2002::/16 (6to4) and the well-known 6to4 relay address 192.88.99.1. Non-automatic tunnelling, i.e. configured TSP clients (static tunnels to tunnel brokers) can be prevented by blocking default ports or protocol 41.

Dual stacking

Remember that two protocols are in play: security steps like firewalls must be taken for both. Automation and management software that abstracts policy is safer than manual configuration.

Autoconfiguration

In IPv4, DHCPv4 can use autoconfiguration with external support, but SLAAC is available by design in IPv6 and requires nothing but a router – the connected host is *immediately* reachable! Privacy and security issues: hardware (MAC) addresses are exposed to the world – permits tracking of a host via unchanging interface ID, exposes NIC vendor, possibly host vendor. MAC exposure can prevented by using random, temporary, or cryptographically generated addresses (CGA).

Hosts with Multiple Addresses

Multiple addresses always possible in IPv4, but rare. But very common with IPv6: SLAAC, DHCPv6, link-local, multiple prefixes, overlapping lifetimes, *plus* IPv4 addresses. Need to be aware of all possible address links.

Scans and IPv6

With 18 billion billion addresses in a /64 subnet, sequential scanning becomes pointless; it would take 500,000 years to scan a single /64 at a million probes per second. However, hinted scanning (using other sources to gain information on address ranges to profitably scan) may still be effective: could leverage a compromised host with Neighbor Discovery, routing table, whois, reverse DNS.

14. IPv6 Packet Security

IPsec defines cryptography-based security for both IPv4 and IPv6, see RFC 4301. IPsec support is optional in IPv4, but *mandatory* in IPv6 – however, IPsec is not automatically set up, it must be configured and properly used.

IPsec Headers

IPsec has two security headers which can be applied separately or together: Authentication Header (AH) and Encapsulating Security Payload (ESP). Both AH and ESP are regarded as end-to-end payloads, so can be fragmented.

Authentication Header: provides connectionless integrity, data origin authentication and protection against replay attacks. It authenticates with an Integrity Check Value (ICV) calculated over the payload, the header, and unchanging fields of the IPv6 header and options. AH does *not* provide privacy/confidentiality of packet contents. Its IPv6 next header extension number is 051. See RFC 2402.

Encapsulating Security Payload: also provides connectionless integrity, data origin authentication, protection against replay attacks, limited traffic flow confidentiality, *plus privacy/confidentiality* through encryption of the payload. Next header extension number is 050. See RFC 2406.

Security Association: is a record of the authentication algorithm, encryption algorithm, public/private/secret keys, mode (transport or tunnel), sequence number and overflow flag, lifetime/expiry of SA and anti-replay window. The SA is held in a database at each endpoint, indexed by outer destination address, IPsec protocol (AH or ESP), and Security Parameter Index value.

Selection of SA can be by manual configuration (pre-shared keys), but it is preferable to automate with Internet Key Exchange (IKE, IKEv2). IKE uses Diffie-Hellman techniques to create a shared secret encryption key used to negotiate SA data. For key exchange IKE depends on Public Key Infrastructure (PKI), which is not yet widespread. The framework and syntax for key exchange is ISAKMP (Internet Security Association and Key Management Protocol). See RFC 2408.

IPsec Modes

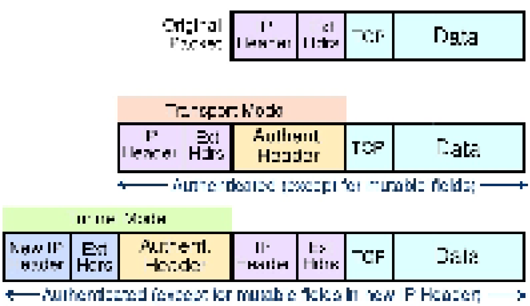
IPSec operates in two different *modes*: Transport mode (host-to-host) and Tunnel mode (gateway-to-gateway or gateway-to-host).

Transport mode: the IPv6 header of the original packet is used, followed by the AH or ESP header, then the payload.

Tunnel mode: a new IPv6 header encapsulates the AH or ESP header and the original IP header and payload.

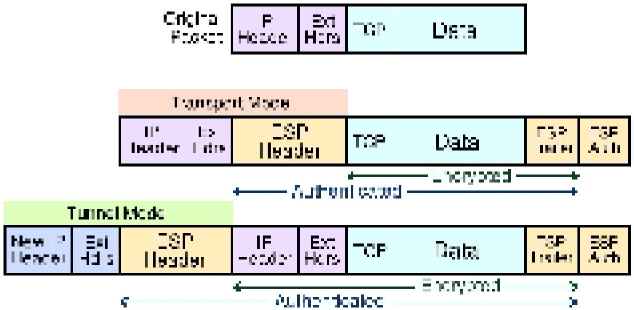
Extension headers (Hop-by-Hop, Routing, Fragmentation) immediately follow their IP headers, except for Destination Options, which can appear before or after AH or ESP. ("TCP" below indicates any upper layer protocol.)

Applying IPv6 AH in Transport and Tunnel Modes



AH authenticates the packet and the outermost IPv6 addresses (except for mutable fields), but does not encrypt payloads. AH cannot be used to traverse NATs as it calculates the integrity check value over source and destination addresses: NATs translate addresses, so would invalidate ICVs.

Applying IPv6 ESP in Transport and Tunnel Modes



ESP authentication does not include the outermost IPv6 headers, but in Tunnel mode it protects the original headers. ESP is used to build virtual private network tunnels between sites. It permits NAT traversal, as it does not use the outermost address values in the ICV calculation. If AH and ESP are used together, ESP is applied first, then AH authenticates the entire new packet.

15. IPv6 Routing Protocols

Internal Gateway Protocols

RIPng – IPv6 version of RIP (Routing Information Protocol)

- Distance-vector protocol, hop count as metric. Maximum of 15 hops.
- Has 128-bit addresses, uses UDP port 521.
- Uses Authentication Header and Encapsulated Security Payload.
- Dual-stack sites need to run both RIP (IPv4) and RIPng.

OSPF3 – IPv6-modified OSPF (Open Shortest Path First)

- Adaptive routing protocol, uses link-state and shortest path first.
- Link-state advertisements (LSA) do not carry prefix information.
- Runs on per-link basis, not per subnet.
- Neighbour ID information based on 32-bit router ID.

IS-IS (Intermediate System To Intermediate System)

- Link-state routing protocol, floods link-state information over network.
- Same as IPv4, but with IPv6 address family running on top.

- Uses ISO Network Service Access Point.
- Problems running IS-IS over tunnels.

External Gateway Protocol

BGP4+ – Extensions in BGP4 (Border Gateway Protocol)

- Path vector protocol, maintains table of autonomous system reachability.
- Runs over TCP/IP, better security, finer-grained control.
- Backwards compatible with BGP4. Need to run separate BGP4 and BGP4+ sessions, but can be on same router.

16. IPv6 Routing Security

Neighbor Discovery Protocol

NDP is new and integral to IPv6, see RFC 4861. It defines five main ICMPv6 packet types which do inverse neighbor discovery: Router Solicitation, Router Advertisement, Neighbor Solicitation, Neighbor Advertisement, and Redirect, see RFC 3122. NDP provides:

- Router discovery: hosts can locate routers on attached links.
- Prefix discovery: hosts can discover prefixes on-link for attached links.
- Parameter discovery: hosts can find link parameters (e.g. MTU).
- Address autoconfiguration: stateless configuration of network interfaces.
- Address resolution: mapping between IP and link-layer addresses.
- Next-hop determination: hosts find next-hop routers for a destination.
- Neighbor unreachability detection (NUD).
- Duplicate address detection (DAD).
- Redirect: router can inform a node about better first-hop routers.
- Recursive DNS Server (RDNSS) and DNS Search List (DNSSL) assignment via router advertisement (RA) options.

NDP has weaknesses – if spoofed, it can redirect to a non-existent router, redirect traffic to wrong hosts, allow denial of service from attackers on-link, advertise a non-existent router, advertise but not route, deprecate prefixes, block autoconfiguration by spoofing DAD responses, spoof 'neighbour unreachable' responses. RFC 4861 discusses NDP security issues, advises Secure Neighbor Discovery (SEND).

Secure Neighbor Discovery

SEND secures NDP – fairly heavy-duty so most useful in high-value networks, see RFC 3971. Works in similar way to SSL – certificates held, verifiable via a trust anchor. Adds NDP messages to handle certificate checks. Uses CGA (cryptographically generated addresses) to secure endpoints.

Cryptographically Generated Addresses

CGA was developed for SEND, see RFC 3972. For IPv6 addresses, interface identifier is generated by computing a cryptographic one-way hash function from public key and auxiliary parameters.

CGAs are not certified, so attackers can create new CGAs from any subnet prefix and public key but can't forge a CGA created by someone else. Protection works without a certification authority or any security infrastructure – only need an address and an algorithm, so also useful as a privacy tool.

Neighbor Discovery Flood

ND Flood is denial of service from off-link attackers, *not* addressed by SEND. Fills router with incomplete ND entries – similar to SYN flood, but worse because one subnet has so many possible hosts. Attackers do not send the ND packets themselves, they trigger them by sending to non-existent addresses – connection attempts are real, but malicious.

Solutions: block access to inappropriate subnets, use smaller subnets on router links. Requires firewall and router awareness, rate limiting, fast flushing of incomplete entries, etc. – needs vendors to address problem!

Rogue Router Advertisements

Rogue RA may be from unauthorised routers, or spoofed RA from other hosts. Not necessarily malicious – perhaps unintentional or misconfiguration.

Communication is interrupted because hosts have incorrect information about where to route packets. Problem is usually local to a subnet – WANs unlikely to be relying on RA. Host-level filters help, accept RA only from known routers, but requires filters on all hosts.

RA-Guard

RA-Guard is lighter-weight than SEND, understands and complements SEND. Sits in switches between routers and hosts, acts as an 'authorisation proxy'. RA-Guard drops bad RAs before they reach hosts, simplifies SEND structure – only need certificates on routers and switches, not all hosts.

Stateless RA-Guard uses static information configured into switch. Stateful RA-Guard collects information about acceptable RAs. However, fragmented RA packets are hard or impossible for a Layer 2 device to inspect.

BGPSEC

BGPSEC (Border Gateway Protocol Security) is an extension to BGP to improve security for routing information exchange. Resource Public Key Infrastructure (RPKI) certificates provide a binding between cryptographic keys to verify digital signatures and Autonomous System (AS) numbers & IP address prefixes.

RPKI also specifies a Route Origination Authorization (ROA), which determines if a route came from an AS authorised to originate it. BGPSEC also adds a BGPSEC router certificate to verify the validity of the AS Path in update messages. BGPSEC can be negotiated separately for IPv6 and IPv4.

17. Mobility in IPv6

Mobile IP: connections remain up as a computing device roams from network to network, like a mobile phone. Definitions in both IPv4 and IPv6 Mobile IP:

Mobile node – the moving device.
Home network – provides the mobile node's identifying home address.
Home agent – router on home network, tunnels packets to mobile node.
Foreign network – where the mobile node operates outside home network.
Foreign agent – router on the foreign network that stores information about visiting mobile nodes and advertises care-of addresses.
Care-of address – the IP address of the mobile node in a foreign network.

The home agent is globally reachable. It supplies the mobile node with a home address. Home and foreign agents broadcast advertisements and respond to solicitations, so the mobile node knows whether it is at home or 'abroad'.

When in a foreign network, the mobile node solicits a foreign agent and registers itself and its home agent's address. The foreign agent supplies a care-of address and tells the home agent. Traffic to the mobile node goes to the home agent, which encapsulates it and sends it to the care-of address of the mobile node.

Improvements in Mobile IPv6:

- Mobile IPv6 does not require a foreign agent.
- Support for route optimisation is built into IPv6.
- Mobile IPv6 has less routing bandwidth overhead, is faster.
- Has dynamic home agent address discovery – ICMPv6 Informational Messages 144-147 define Home Agent Address Discovery Request/Reply, Prefix Solicitation and Prefix Advertisement.

18. Useful Information

Firefox Plugins that Show IPv6 Addresses

ShowIP displays IP address of the current webpage in the bottom corner.

ExternalIP shows the IP address the world sees you coming from.

Unix Tools for IPv6

`ip -6` – show/manipulate routing, devices, tunnels etc
`ifconfig -a` – to see all network interfaces on a host
`ping6` – host and network reachability
`traceroute6` – traces route to a host
`tracepath6` – traces route to host discovering MTU along path
`route -6` – the current routing table
`netstat` – network connections, routing tables, interface statistics etc.
`tcpdump` – shows packet contents on network interfaces
`wireshark` – GUI network protocol analyzer
See **`man`** pages for command options.

Windows Tools for IPv6

Options below in square brackets. Use `/?` to get a list of usage options.

```
ipconfig /all
ipconfig /flushdns
route [print add delete]
ping [-4 -6 -i -R -S]
tracert [-4 -6 -R -S]
pathping [-4 -6]
netstat
netsh interface ipv6 show [interface address route
neighbors destination cache]
```

Address Testing

Check for IPv6 and IPv4 connectivity: **`http://www.ipv6-test.com`**

Looking glasses: publicly accessible servers for routing queries, used to troubleshoot routing issues. List of IPv6-capable looking glasses:

`http://www.bgp4.as/looking-glasses`

IPv6 Addresses in URLs

To use a website's IPv6 address rather than its URL, the address must be enclosed in square brackets, e.g., `http://[2001:db8::2e:0:7348]`
Port numbers go outside the brackets – `http://[2001:db8::2e:a0:57ab]:80`

19. Useful IPv6 Sites

IETF RFCs – *ietf.org/RFC.html*
IPv6 Forum – *ipv6forum.org*
IPv6 Forum Australia – *ipv6forum.org.au*
ISOC-AU IPv6 Resources – *ipv6.org.au*
APNIC IPv6 Program – *apnic.net/community/ipv6-program*
Asia-Pacific IPv6 Forum – *www.ap-ipv6tf.org*
Australian IPv6 Summit – *ipv6.org.au/summit*
IPv6 Portal News – *ipv6tf.org*

RIPE NCC IPv6 Statistics – *v6day.ripe.net/cgi-bin/index.cgi*
ARIN Tools – *getipv6.info/index.php/IPv6_Management_Tools*
IPv6 Status Survey - *mrp.net/IPv6_Survey.html*
List of IPv6 websites – *sixy.ch*

SixXS, free IPv6 tools, information and services:
IPv6 tools – *sixxs.net/misc*
IPv6 routing table statistics – *sixxs.net/tools/grh*
IPv6-enabled devices & facilities – *sixxs.net/misc/coolstuff*

Subnet Online, IPv6 network tools:
ping, traceroute, tracepath, port scanner, dig –
www.subnetonline.com/pages/ipv6-network-tools.php
Subnet calculators –
www.subnetonline.com/pages/subnet-calculators.php
Number system converters –
www.subnetonline.com/pages/converters.php

Potaroo, IPv6 deployment and performance:
In-depth articles – *www.potaroo.net*
IPv6 routing statistics: BGP table, CIDR, BGP Update reports, address allocations by ISO-3166 (country) code –
bgp.potaroo.net/index-v6.html

Easy IPv6: The Lookup Book

The Internet is undergoing a quiet revolution. One of its most fundamental elements, the Internet Protocol, is being gradually upgraded from version 4 to version 6. Internet Protocol version 6 offers new benefits:

- ✔ Almost unlimited address abundance
- ✔ Easier and cheaper network management
- ✔ Return of end-to-end connectivity
- ✔ Mandated security features
- ✔ Integrated mobility and interoperability
- ✔ A platform for innovation and scaleability

The Lookup Book is a quick reference to technical definitions in IPv6. It covers addresses and prefixes, packet structure, address types, multicast, ICMPv6, autoconfiguration, DNS, transition, security, mobility, useful tools and websites.

This expanded Second Edition has new sections on tunnel techniques for end-users and service providers, and IPv6 packet and routing security.

Lancewood

ISBN 978-0-9872113-0-9