Comp 2207: IPv6

Graeme Bragg
  g.bragg@ecs.soton.ac.uk
Electronics & Computer Science
University of Southampton
24th of October 2017
Topics

- Why we need IPv6
- IPv6 History
- IPv6 Overview
- IPv6 Header
- Neighbour discovery & autoconfiguration
- Deploying IPv6
- IPv6 Usage
- Security Issues
IPv4 Address Exhaustion

- We are running out of IPv4 addresses:
  - << 3.7 bn useable addresses,
  - >> 8 bn devices in 2017 [1],
  - >> 20 bn devices by 2020.
- NAT and CIDR have only helped so much.
- IANA have no unallocated address blocks (Feb 2011):
  - APNIC was the first RIR to run out, other RIRs soon followed,
  - Only AfriNIC are left (predicted depletion in H1 2018)

1. [https://www.gartner.com/newsroom/id/3598917](https://www.gartner.com/newsroom/id/3598917)
   Image by By Mro - Own work, GFDL,
   [https://commons.wikimedia.org/w/index.php?curid=10593349](https://commons.wikimedia.org/w/index.php?curid=10593349)
IPv6 History

- 1998: Draft standard (RFC 2460),
- 1999: IPng Tunnelbroker (precursor to SixXS) started,
- 2003: DHCPv6 (RFC 3315),
- 2004: First IPv6 records visible in DNS root servers,
- 2008: IANA add AAAA records for 6 root name servers,
- 2008: Google IPv6 support (www.ipv6.google.com),
- 2011: All major PC operating systems support IPv6,
- 2011: World IPv6 Day,
- 2012: World IPv6 Launch Day,
- 2016: Sky at 80% IPv6 coverage, BT beginning deployment,
- June 2016: All apps submitted to Apple App store must support IPv6 only networking
- June 2017: SixXS shuts down,
IPv6 Features

128-bit addresses

- $3.4 \times 10^{38}$ IPv6 addresses – more than enough to give every grain of sand on Earth a global address.
- Current public pool is confined to addresses beginning with 2xxx and 3xxx ($4.2 \times 10^{37}$ addresses)

Addresses represented in colon hexadecimal format:

- e.g. 2001:0630:00d0:f102:0000:0000:0000:0022
- Leading 0s in a block can be omitted:
  - 2001:630:d0:f102:0:0:0:22,
- A single set of repeated 0 blocks can be replaced by “::”
  - 2001:630:d0:f102::22,
IPv6 Features

- Subnets represented in CIDR notation:
  - e.g. 2001:630:d0:f102::/64

- Not as easy to remember as IPv4 addresses!
  - Users shouldn’t care
  - Especially in home networks
  - DNS, NetBIOS and service discovery are well established

- Multicast is an inherent part of IPv6:
  - Used within subnets instead of broadcast.

- IPv4 and IPv6 can co-exist in dual-stack deployments
IPv6 Address Scopes

Various scopes of addresses defined:

- Loopback: ::1/128
- Unspecified (equivalent to 0.0.0.0) ::/128
- Link-local addresses – used only on local link
  - fe80::/10
- Unique Local Addresses (ULA) – used within a site
  - fc00::/7
- Global Unicast:
  - 2000::/3
- Multicast:
  - ff00::/8

Hosts can (and usually do) have multiple IPv6 addresses!

RIPE reference sheet: http://www.ripe.net/ipv6-address-types
IPv6 Address Conventions

- /127 can be used for inter-router links (RFC 6164)
- Smallest subnet is a /64 (RFC 4291)
  - 18 quintillion addresses
- Home/small business users should be given a /56 (RFC 6177)
- A “site” is commonly given a /48
- Minimum IPv6 allocation from RIR is /32

N.B.: IPv6 still uses CiDR: for the routing prefix so any size of subnet larger than /64 can be used
Technical Benefits

→ Removes the need for NAT:
  ➔ Restores end-to-end connectivity,
  ➔ Remove the need for NAT traversal,

→ More plug-and-play than IPv4:
  ➔ Stateless auto configuration (SLAAC) works,

→ Streamlined header,
  ➔ More efficient routing and packet processing.

→ Fragmentation only occurs at sender:
  ➔ Hosts should use Path MTU Discovery (RFC 8201),
  ➔ Links must support an MTU of at least 1280,
  ➔ Simpler for routers.
Reasons to Deploy Now

→ Gain familiarity before IPv6 becomes “mandatory”:
  - Some sites/services are ONLY available on IPv6,
  - E.g. Mythic Beasts Raspberry Pi hosting,
  - More services will become IPv6 only.

→ Securing IPv6 in your own “IPv4 only” network:
  - Deploy to be able to manage it – modern OSes have IPv6 by default,
  - Windows automatically uses Teredo if there is no native IPv6 – bypasses firewalling/content filtering.

→ Enabling innovation/teaching/research,
→ Enable early-adopters to access your services,
→ Support new applications: e.g. IoT.
IPv6 Header

- **Fixed size (40 bytes):**
  - Large than IPv4 but simpler,
  - Uses extension headers rather than options.

- **8 fields, Version, source address & destination address plus:**
  - Traffic Class: 6-bits for differentiated services, 2-bits for ECN,
  - Flow Label: Give routers a hint that packets should stay on the same path,
  - Payload Length: Size of the payload, including any extension headers,
  - Next Header: Indicates the next header. Could be transport header or extension header,
  - Hop Limit: Equivalent to TTL in IPv4.

![IPv6 Header Diagram](image)
Extension Headers

- Sit after the IPv6 header but before the transport layer header in the packet:
  - Effectively implements the Options fields from IPv4,
  - Fragmentation is moved to an extension header,
  - Extension headers can be daisy chained but need to be placed in a specific order.
  - Each extension header includes a “Next Header” field

- Each extension header is a multiple of 8-bytes
Neighbour Discovery

- Functionally replaces ARP and ICMP Router Discovery

- Defines five ICMPv6 packet types:
  - **Router Solicitation:** Host request for router information
  - **Router Advertisement:** Router information
  - **Neighbour Solicitation:** Equivalent to ARP “who has”
  - **Neighbour Advertisement:** Equivalent to ARP reply
  - **Redirect:** Router informing host of a better first-hop
Router Advertisements

A host sees or solicits a Router Advertisement (RA):
- The RA message carries the IPv6 network prefix (/64) to use,
- The RA’s source address implies the default router address,
- DNS server information can be included in a RA.

Prefix information is sent by multicast:
- Periodically (typically every 600 seconds)
- On request (in response to a Router Solicitation)
StateLess Address AutoConfiguration (SLAAC)

- Hosts can autoconfigure basic network settings without a DHCPv6 server (RFC 4862).

- A host using SLAAC builds its address from:
  - A 64-bit prefix determined from a Router Advertisement
  - A 64-bit host part is generated based on MAC address

- Alternative method in RFC 7217:
  - Does not embed MAC address,
  - Mitigates many of the security/privacy issues of RFC 4862
For example:

- Host’s Ethernet (MAC) address is 08:00:20:9c:14:66
- The network prefix in the RA is 2001:630:80:200::/64

Address is 2001:630:80:200:0a00:20ff:fe9c:1466
- A MAC address is 48-bits, hence the ‘fffe’ 16-bit ‘padding’
- The “0a” is the globally unique EUI-64 bit being set

So an IPv6 host can get its address and default gateway through the Router Advertisement
- The subnet prefix length or ‘netmask’ is fixed at /64.
Privacy Extensions

- Embedding the MAC address in the autoconfigured *global* address causes a privacy issue:
  - Host part stays the same across networks,
  - Makes it easier to track users.

- IPv6 Privacy Extensions (RFC 2941) added that use a random 64-bit host part:
  - Random IPv6 generated periodically (e.g. hourly) and used for outbound connections,
  - Host still has SLAAC-configured address for inbound connections.
Privacy Extensions

A host can have multiple temporary addresses
Expired addresses are retained for a while

<table>
<thead>
<tr>
<th>Ethernet adapter Ethernet:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection-specific DNS Suffix</td>
<td>ecs.soton.ac.uk</td>
</tr>
<tr>
<td>Description</td>
<td>Intel(R) Ethernet Connection I217-LM</td>
</tr>
<tr>
<td>Physical Address</td>
<td>08-62-66-48-5A-75</td>
</tr>
<tr>
<td>DHCP Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Autoconfiguration Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Temporary IPv6 Address</td>
<td>2001:630:d0:f118:592b:660e:463b:b672 (Deprecated)</td>
</tr>
<tr>
<td>Temporary IPv6 Address</td>
<td>2001:630:d0:f118:ac79:35b5:b90e:eed4 (Deprecated)</td>
</tr>
<tr>
<td>Temporary IPv6 Address</td>
<td>2001:630:d0:f118:d5c0:bd77:8e29:e745 (Deprecated)</td>
</tr>
<tr>
<td>Temporary IPv6 Address</td>
<td>2001:630:d0:f118:fd85:60ad:b042:f06f (Preferred)</td>
</tr>
<tr>
<td>Temporary IPv6 Address</td>
<td>fe80::28e7:401a:757b:bd79%3 (Preferred)</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>152.78.67.9 (Preferred)</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.254.0</td>
</tr>
<tr>
<td>Lease Obtained</td>
<td>18 October 2017 12:32:58</td>
</tr>
<tr>
<td>Lease Expires</td>
<td>24 October 2017 14:03:23</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>fe80::214:1bff:fe3d:2c00%3</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>152.78.67.254</td>
</tr>
<tr>
<td>DHCPv6 IAID</td>
<td>152.78.111.198</td>
</tr>
<tr>
<td>DHCPv6 Client DUID</td>
<td>50081126</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>00-01-00-20-62-ED-59-08-62-66-48-5A-75</td>
</tr>
<tr>
<td>NetBIOS over Tcpip</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
Deploying IPv6

- Current Internet is (mostly) IPv4
  - New IPv6 services will be introduced but everything needs to keep working

- One approach is to run both protocols, known as ‘dual stack’

- We might have IPv6-only systems so:
  - IPv4-only systems need to access IPv6-only services
  - IPv6-only systems need to access IPv4-only services

- We can also have isolated IPv6 networks (or isolated IPv4)
  - Need to use an IPv4 network to carry IPv6 traffic from one site to another
Dual stack systems

- Run both protocols on the same equipment
  - Used in this university and by BT/Sky

- May need to rewrite/update existing applications

- Need to choose when to use IPv4 or IPv6
  - Current “preference” is IPv6 if available

- Requires IPv4 address space going forward
  - Can use NAT/CGNAT with global IPv6 addresses

- Need to secure (e.g. firewall) both protocols
Translation Mechanisms

- Translate from IPv6-only to/from IPv4-only
- Can re-write IP header information as best as possible
  - Stateless IP/ICMP Translation (SIIT) uses IPv4 translated addresses in the range ::ffff:0:0:0/96
  - e.g. 152.78.130.145 Can be written as ::ffff:0:152.78.130.145
- Or use Application Layer Gateways (ALGs)
- NAT64: Single IPv4 address NATed to IPv6 network
- DNS64: “fabricates” AAAA record for non-IPv6 sites that points to an IPv6/IPv4 translator
**Tunneling**

- **6in4**: encapsulates IPv6 packets in IPv4 packets
  - Uses “Protocol 41” as Protocol field in IPv4 header
  - Used by tunnelbrokers such as Hurricane Electric and (formerly) SixXS

- **Teredo**: encapsulates IPv6 in UDP IPv4
  - Uses a well-known IPv4 host on the Internet to relay IPv6 traffic
  - Work with no co-operation of local network – bypasses security

- **DS-Lite**: encapsulates IPv4 packets in IPv6 packets
  - Customer CPE is only given IPv6 addresses
  - CPE uses IPv6 addresses to send IPv4 traffic to CGN

- **Can also use VPN to distribute IPv4 over IPv4**:
  - tunnelbroker.ecs.soton.ac.uk does this
Best transition method?

→ We have a ‘toolbox’ of methods
  → Some suited to certain scenarios
  → No best solution for all scenarios

→ The topic is covered in more detail in COMP3210

→ IPv4 hosts will be around for a long time, with transition ongoing for many years (10-20+ ??)
  → Initial focus is on dual-stack deployment
  → But use of IPv6-only is growing, esp. with mobile operators
IPv6 Deployment

In November 2016:

- 98.2% of TLDs supported IPv6 access to DNS servers
- 97.8% of zones contained IPv6 glue records
- ~4.6% of domains had IPv6 address records in zone

Today Many major sites have IPv6:

- All varieties of Google
- Youtube
- Facebook
- Netflix
- Yahoo

Dropbox
- LinkedIn
- Instagram
- Blogspot
- Wikipedia

Major ISPs beginning to support IPv6
> 20% of global Google users currently use IPv6:

- 32.99% in Greece
- 32.85% in USA
- 31.77% in Germany
- 26.39% in India
- 18.94% in UK

> Up from ~11% from a year ago

Barriers to Deployment

- Many home routers lack IPv6 support,
- Network administrators lack understanding/desire to understand IPv6,
- Regular users don’t want to learn something new,
- Chicken and egg situation with ISPs and content providers:
  - ISPs are being slow to deploy IPv6 to customers because the content is not there,
  - Content providers are being slow to adopt IPv6 because the users are not there:
IPv6 Security Issues

- IPSEC (encryption...) is baked into IPv6,
- Sheer number of addresses makes scanning less feasible:
  - It would take ~500,000 years to scan a single /64 at one million probes per second.
- Transition mechanisms (Tunnelling, Teredo) can bypass network security mechanisms,
- IPv6 implementations still have undiscovered flaws:
  - e.g. Windows is susceptible to Router Advertisement flooding.
IPv6 hosts can essentially pick their own addresses
  - May use many privacy addresses over time

To track which devices are used where, we can poll switches and routers for MAC table and ARP table information
  - Build a database of mappings
  - Switch port : device MAC
  - MAC address : IPv4/IPv6 address

In ECS, an open source network monitoring package called NAV supports this…
UoS IPv6

➤ UoS has 2001:630:d0::/48
➤ UG Labs use 2001:630:d0:f110::/64
➤ ECS have been allocated 2001:630:d0:f000::/52
➤ SOWN use 2001:630:d0:f700::/56
➤ Tunnelbroker uses 2001:630:d0:f300::/56
➤ Deployment in a dual-stack setup
➤ Currently being deployed to whole University
IPv6 Myths

→ We don’t need IPv6, CGNAT and address recovery means we have a lot more addresses:
  → NAT and CGNAT only go so far. We already have IPv6-only services.

→ IPv6 replaces IPv4:
  → IPv6 and IPv4 will co-exist for years to come.

→ IPv6 is more complicated than IPv4:
  → Addresses look daunting but the concepts are similar or simpler.

→ IPv6 is less secure because there is no NAT:
  → NAT is NOT a security mechanism and IPv6 still has firewalling/ACLs.
Will we run out of IPv6 addresses?

- Only if the Nanobots take over…
Reading

- Tanenbaum Chapter 5
  - IPv6, pp. 473-483

- Wikipedia articles on:
  - IPv4 address exhaustion
  - IPv6
  - IPv6 Deployment
  - IPv6 Packet