IPv6 Address Design
Practical Considerations

Jeff Doyle
Principal Architect
FishNet Security

SECURELY ENABLING YOUR BUSINESS
Obligatory IPv4 Depletion Slide

Source: http://www.potaroo.net/tools/ipv4/
Public IPv6 Traffic

It’s All About the Address Space

Some Perspective:

1 picometer = $10^{-12}$ (one trillionth) meter

$2^{32}$ picometers = 4.29 millimeters
    - length of a small ant

$2^{128}$ picometers = $3.4 \times 10^{23}$ kilometers
    - 34 billion light years
    - Furthest visible object in universe: 13.2B LYs
Abandon IPv4 Thinking!

Foremost IPv4 design consideration: Conservation

Balancing act between:
– Number of available subnets
  – Number of hosts per subnet

Result: VLSM
  – Complex
  – Difficult to manage

2001:0db8:1234:abcd:5401:473c:0015:ea85/64
Global IPv6 Unicast Address Structure

- 64 bits
- \( n \) bits
- 64 - \( n \) bits

<table>
<thead>
<tr>
<th>Global Unicast Prefix</th>
<th>Subnet</th>
<th>Interface ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Topology</td>
<td>Site Topology</td>
<td>Network (Location)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>First 3 bits = 001</td>
</tr>
</tbody>
</table>
Global IPv6 Prefix Allocations

Reserved for Global Unicast: 2000/3

Total IPv6 Space

5 /12s assigned to RIRs*

<table>
<thead>
<tr>
<th>RIR</th>
<th>IPv6 Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>AfriNIC</td>
<td>2C00::/12</td>
</tr>
<tr>
<td>APNIC</td>
<td>2400::/12</td>
</tr>
<tr>
<td>ARIN</td>
<td>2600::/12</td>
</tr>
<tr>
<td>LACNIC</td>
<td>2800::/12</td>
</tr>
<tr>
<td>RIPE NCC</td>
<td>2A00::/12</td>
</tr>
</tbody>
</table>

*Plus numerous /23s and shorter

Source: [http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xml](http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xml)
## IPv6 Prefix Assignments

### Typical IPv6 prefix assignments:

- Service provider (LIR): /32  \(\rightarrow\) \(2^{32}\) /64 subnets
- Large end user: /48  \(\rightarrow\) 65,536 /64 subnets
- Medium end user: /56  \(\rightarrow\) 256 /64 subnets
- Small/ Home/ SOHO: /64 or /60  \(\rightarrow\) 1 or 16 /64 subnets

### Address Conservation

- Is this really practical?
- Yes!

If you don’t have enough subnets, you don’t have the right prefix allocation.
What Prefix Size is Right for You?

ARIN Number Resource Policy Manual:

2.10. End Site

“The term End Site shall mean a single structure or service delivery address, or, in the case of a multi-tenant structure, a single tenant within said structure (a single customer location).”

6.5.8.2.1. Standard Sites

“An organization may request up to a /48 for each site in its network, and any sites that will be operational within 12 months.”
Are You Ready for IPv7?

All current IPv6 global unicast prefixes start with 001
This is 1/8 of the entire IPv6 address space
$2^{45} = 35$ trillion /48 prefixes

UN projections for 2100 world population:
Median figure 10 billion
High end: 16 billion

$2^{45} / 16$ billion = 2199 /48s per person
And, we still have 85% of the IPv6 space held in reserve

Opinion:
IP will become obsolete before IPv6 is depleted
What About Subnet Assignments?

RFC 4291 specifies that Interface-IDs are 64 bits
- Several IPv6 functions depend on this

All subnets should be /64
- Including point-to-point links
- Simplifies address management
- Random addressing improves security

Trend is to use stateful (DHCPv6) addressing
What About Point-to-Point Links?

18 million trillion addresses in a /64 link
– And I will only ever use 2 of them?
– Are you kidding???

People have a very hard time accepting this
– Again: This is not IPv4!
– What else are you going to do with those addresses?

It’s a matter of comprehending the scale
– 5000 out of $2^{64}$ is not really any bigger than 2 out of $2^{64}$
Point-to-Point Subnets (Battling RFCs)

**Reasons for using /64**
- RFC 3627
- RFC 5375 => /64 usage endorsed and encouraged
- Design consistency
- Anycast problems are not significant on PtP links
  - Subnet-Router Anycast
  - MIPv6 Home Agent Anycast

**Reasons for using /127**
- RFC 6164
- Ping-pong vulnerability
  - This is an issue with older version of ICMPv6 (RFC 2463)
  - Issue is corrected in newer version of ICMPv6 (RFC 4443)
  - Vendors: Upgrade your code!
- Neighbor cache exhaustion vulnerability
Point-to-Point Subnets (cont.)

Insist that your vendors use current ICMPv6!

Don’t use /126
– This is IPv4 thinking
– “Subnet number” is meaningless in IPv6
– IPv6 does not use broadcast addresses

Potential compromise:
– Assign /64 per PtP subnet
– Address /127 out of the /64
What Do I Get in Exchange for “Waste”?

**Simplicity**
– One-size-fits-all subnets

**Manageability**
– Hex is much easier to interpret (binary) than decimal

**Scalability**
– Room to grow

**Flexibility**
– Room to change
Designing for Simplicity

Start by mapping “working” bits
Generally the bits between assigned prefix and Interface-ID

Group by hex digit (nibble)
4 bits per hex digit

Define “meanings” you need to operate
Geographic area? Logical topology? Type designation? User ID?

Try to keep “meanings” on hex boundaries
Defined meanings will then be some multiple of $2^{4n}$
Ex: 16, 256, 4096, 65536…

Don’t get carried away with meanings
No need for 10 layers of address hierarchy if 4 will do
Designing for Simplicity (cont.)

Use zero space as much as possible

– Which address is easier to read?
  • 2001:DB8:2405:C::27

Benefit: Operations quickly learns to focus on meaningful bits

– Ignore public prefix (usually)
– Ignore Interface-ID (usually)
– A few hex digits tell operations most of what they need to know

2001:DB8:2405:C::27

Region  Office  Subnet
**Designing for Scale**

---

**Leave “zero” space whenever possible**

Designate as Reserved
Both vertical and horizontal

**Insert between “meaningful” digits or bits**

Allows future expansion in two directions
Designing for the Future

Do not integrate IPv4 into an IPv6 design!

– Reading IPv4 in hex is (almost) meaningless
– IPv4 will (eventually) go away
Other Issues

DNS design and management is critical
DNS issues are well documented

IP Address Management is critical
IPv6 design is not easy to manage via spreadsheets
IPAM deployment tends to be a part of IPv6 deployments

Abandon IPv4 thinking!
Thank You

Jeff Doyle
Principal Architect
FishNet Security
Jeff.Doyle@FishNetSecurity.com