

Using IPv6

Daniel Hagerty
hag@linnaean.org

6to4 connectivity on this laptop

- Included since OS-X 10.3 or so.
- Works anywhere you have a public IP that can send/receive IP protocol 41.
- Could give v6 transit to everyone on this wireless subnet if asked to, but IS might not appreciate this (more on this later).

IPv6 Ups and Downs: Ups

- It's a network protocol. When it does its job, you don't think about it.
- My wife uses it and doesn't notice.
- Can directly address house internal machines from IPv6 networks, including my roaming laptop.
- 30-40% of incoming email received over v6.
- Access to google sites is using v6, including youtube.

IPv6 Ups and Downs: Downs

- Google hit a bad spot that caused me to revert to v4 with them for a month.
- 6to4 is famed for a particular failure mode that I've experienced three times:
 - Reading python documentation
 - Reading debian documentation
 - Receiving mail from netbsd.org
- You won't like web browsing affected sites.

What's new for the v4 clued

- IPv6 is mostly IPv4 with bigger addresses, however:
 - Link local addresses
 - Extensive use of multicast
 - Link scoping to help target the above
 - Stateless address auto configuration (SLAAC)
 - Router advertisements
- This isn't a complete list, but are the differences I see all the time.

Bigger Addresses

- 128 bits long, 4 times bigger than IPv4
- Verbosely represented as
2001:0db8:b009:0000:0000:0000:0000:006a
- Some tricks to make them smaller, but the real world still gives you addresses like
2002:425c:49d9:8:216:cbff:feb7:ae2b

Address Compression

- You can leave off leading zeros of digit groups: “fd00::0123” and “fd00::123” are equivalent.
- You can compress a run of zeros with “::” ONCE, and the run has to be 16 bit aligned. For example, the fd00:: example above. If you have “2001:db8:0:0:0:1:0:0”, “2001:db::1:0:0” is valid, “2001:db8:0:0:0:1::” is legal, but “2001:db8::1::” is not.
- You can use IPv4 notation for the last 32 bits of an address, e.g. 2001::128.52.32.80 is legal.

Prefixes you'll see a lot

v4 Address	v6 Address	Notes
0.0.0.0	::	Unspecified Address
127.0.0.1	:::1	Loopback
	::ffff:0.0.0.0/96	v4 mapped onto v6 sockets
192.0.2.0/24	2001:db8::/32	Documentation Prefix
10/8, 172.16/12, 192.168/16	fc00::/7	Local Unicast (ULA)
169.254.0.0/16	fe80::/10	Link Local
224.0.0.0/4	ff00::/8	Multicast space

- No broadcasts!

Routable Unicast Space

Prefix	Usage
2000::/3	Global unicast
2001:0::/32	Teredo
2001:db8::/32	Documentation Prefix
2002::/16	6to4
3ffe::/16	6bone (deprecated)

- 4000::/3 through c000::/3 are reserved, as are several other smaller holes. We have 5 tries at address allocation before we need to do IP over again.

Link Local Addresses (fe80::/10)

- Like IPv4's 169.254.0.0/16 prefix, but used extensively.
- Every single IPv6 interface has one as part of configuration.
- Link scoped, meaning the address is relative to an interface. fe80::1 on one link might be a different host than fe80::1 on another link.
- Routing protocols often use them.

Multicast (ff00::/8)

- IPv6 does away with broadcast entirely.
- ff02::1 is the multicast equivalent of an IPv4 broadcast.
- Like link local addresses, they require link scoping.
- Propagation scoping is encoded in the 4th octet: e.g. the “2” in ff02:: addressed packets confines them to the link they were sent on (like 224.0.0.0/24 in IPv4).

Link Scoping

- You need to specify an interface for link local and multicast addresses.
- Append “%” and an interface name to the address.
- For example, “ping6 ff02::1%eth0” should get ping responses from everything in eth0's broadcast domain.

Autoconfiguration

- All hosts can use link local addresses to communicate across a single subnet with no central planning.
- The main ingredient for inventing unique addresses is the EUI-64, a 64 bit hardware identifier. Firewire uses it natively.
- Ethernet MACs can be promoted to EUI-64 by inserting “ff:fe” into the middle, after the OUI.
- Only works with /64 prefixes.

Router Advertisements

- Routers tell clients the prefixes in use and clients build themselves addresses with them.
- Clients route to the routers they see, even if it's a broken laptop somebody has been experimenting with.
- This isn't anything like DHCP.

DHCPv6

- There is one.
- It's late to the party.
- Not everyone is on board, notably Apple.
- Vista and subsequent MS OSes are the only I'm aware of shipping with support out of the box.
- Nothing in my house supports it without me doing a lot of work, so I haven't run it.

DHCPv6 vs RA

- Religion. Different constituents want different things.
- Purists hate the DHCP model and implementation. Pragmatists want the purists to suggest something that meets their needs, as RA doesn't do it yet.
- For example, stock RA can't configure DNS servers for a client. RFC5006 extends RA to do this, but support isn't very broad yet.

Unique Local Addresses (ULA)

- More or less RFC1918 for IPv6.
- Much less likely to collide than RFC1918 addresses when used for private interconnect, mergers, etc.
- There's a “registry” where a further hint that a prefix is in use can be shared.

IPv6 info in DNS

- Works roughly the same as it did in v4: there's an address record for forward, and a PTR record for reverses.
- Reverses are split by each hex digit. Use host!

- Forward:

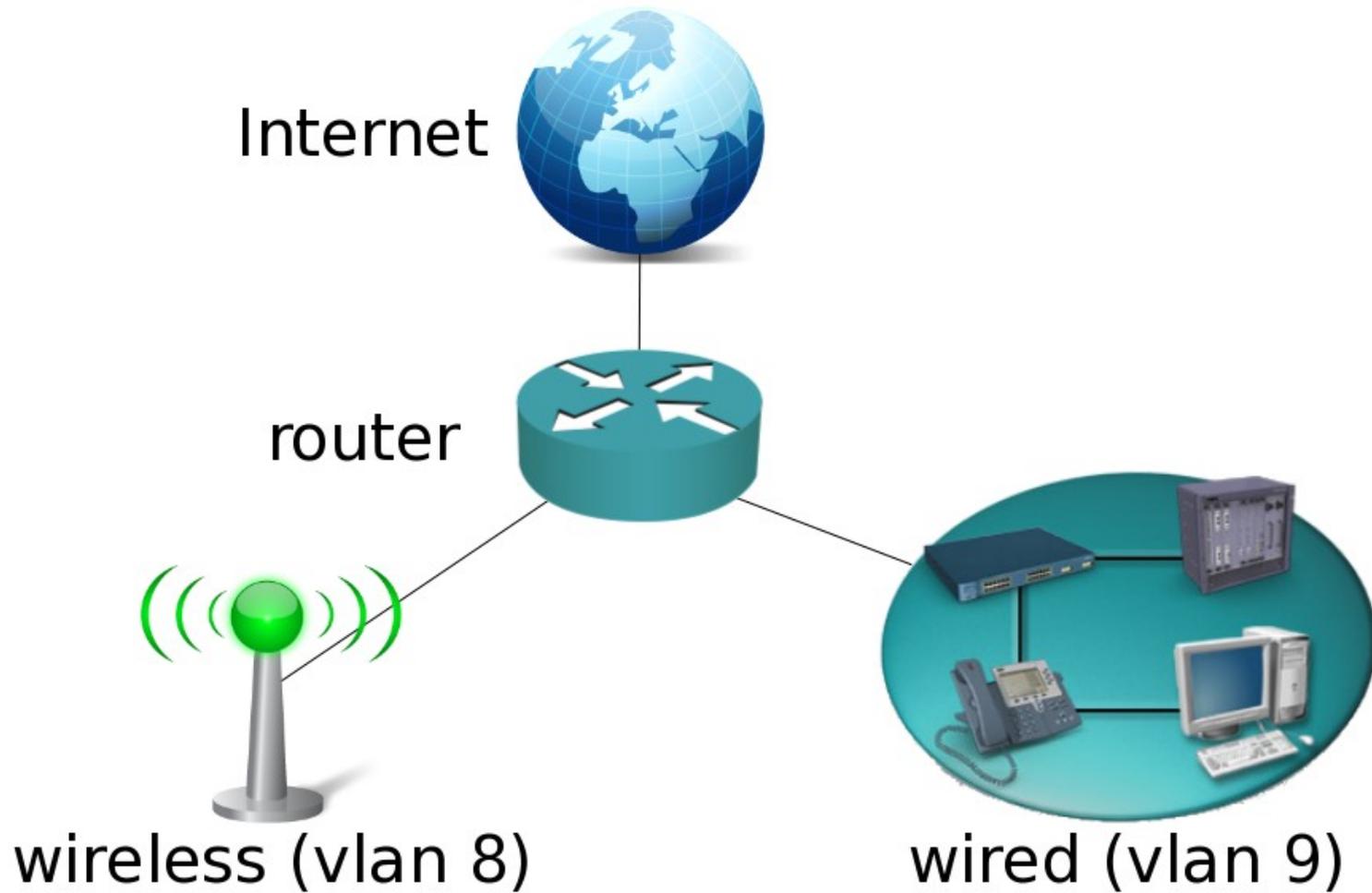
```
perdition IN AAAA 2002:425c:49d9:1::1
```

- Reverse:

```
$ORIGIN 9.d.9.4.c.5.2.4.2.0.0.2.ip6.arpa.
```

```
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0 IN PTR  
perdition.linnaean.org.
```

Home Network



Home Network

- I picked 6to4 as my connection method, mostly because I like its routing properties between multiple 6to4 sites.
- Configuring the router to speak 6to4 was a non-event.
- Router advertisements required configuring addresses on the subnets, and starting a daemon with no options. There was a surprise, in that all v6 hosts IMMEDIATELY using it.

Home Network

- Initially, I didn't expose my v6 DNS to the public, but eventually I exposed individual services over the course of a couple of months.
- Google doesn't offer their services over v6 without your DNS resolver being on a whitelist.
 - But it's an open secret that Hurricane Electric's resolvers are on this whitelist, and will resolve for anybody. So my internal DNS server forwards google's domains through them.

IPv6 Connection Methods

- Native; stop here if you can get it.
- Static tunnel providers like Hurricane or Sixxs
- 6to4
- Teredo

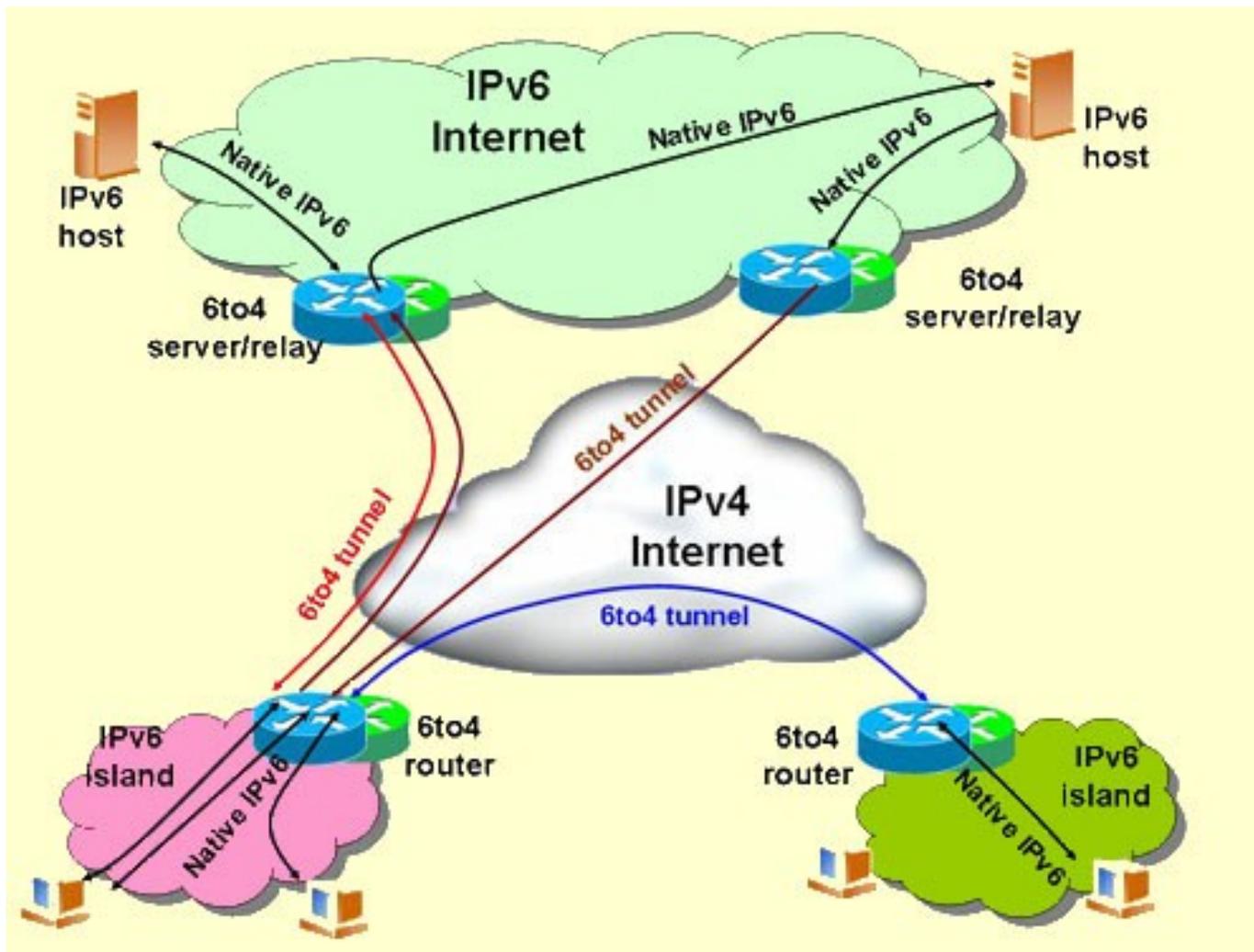
Static Tunnel Providers

- Hurricane Electric's tunnelbroker.net
 - Simple IP Protocol 41 tunnels.
 - They hand out /48s with a click.
 - Will speak BGP.
- Sixxs
 - Requires tunneling software, available for most any OS you care to name.
 - Can traverse most NATs.
 - Some POPs only offer /64 prefixes (1 subnet).

6to4 Tunneling

- Requires a public IP address that will pass IP protocol 41.
- Gives you a prefix `2002:xxxx:xxxx::/48` where `xxxx:xxxx` is your 32 bit IPv4 address in hex.
- Can offer control of reverse DNS.
- The IP address `192.88.99.1` is an anycast address for public 6to4 relays.
- Can directly reach other 6to4 users using v4.
- Build in support on all majors OSes.

6to4, visualized



Teredo

- Works through typical NATs that will pass UDP traffic with the help of a “teredo server”.
- Only provides a single /128 address
- Can directly reach other teredo users over v4.