Advisory Guidelines for 6to4 Deployment

draft-carpenter-v6ops-6to4[-teredo]-advisory-03

Brian Carpenter

March 2011

Acknowledgements

- Very useful and practical input from at least 20 people:

  Emile Aben, Tore Anderson, Jack Bates, Cameron Byrne, Remi Despres, Jason Fesler, Wes George, Geoff Huston, Eric Kline, Victor Kuarsingh, Martin Levy, David Malone, Martin Millnert, Keith Moore, Gabi Nakibly, Michael Newbery, Pekka Savola, Mark Smith, Nathan Ward, James Woodyatt

Why?

- Because there is quite a lot of 6to4 out there.
- Because it is responsible for quite a lot of operational issues, and in some cases for help desk advice to just switch IPv6 off.
- Because advising operators how to mitigate these issues is a lot more use than moaning.

Background

- Router 6to4 (RFC 3056) was not designed as an unmanaged solution.
  - routing and relays need to be well managed
- Anycast 6to4 (RFC 3068) was aimed at unmanaged hosts but still needs well-managed relays.
- Empirically, 10-20% of connection attempts received from 6to4 clients at IPv6 servers fail [Aben, Huston]
  - translates into a fraction of 1% of “lost sessions” for content providers.
  - indirect evidence suggests that filtering of protocol 41 (IPv6-in-IPv4) is the major reason.

Summary of issues

- Outbound Black Hole: 192.88.99.1 unreachable
- Inbound Black Hole: protocol 41 filtered
- No Return Relay: content server has no 2002::/16 route, or the relay it reaches drops its traffic
- Large RTT: 6to4 path exists but is far too slow
- PMTUD Failure: and actual PMTU is 1280
- Reverse DNS Failure
- Bogus Address: ISP assigns bogons to subscribers
- Faulty 6to4 Implementations
- Difficult Fault Diagnosis (given all of the above)
- 6to4 observed to be implicated in rogue RA

Advice to vendors

- Do not enable 6to4 by default
- Do not activate 6to4 for RFC 1918 addresses
- Adopt draft-ietf-6man-rfc3484-revise
- Do not emit rogue RAs for 6to4 prefix

Advice to consumer ISPs & enterprise networks that do not support IPv6

- Find a transit provider willing to offer your users a route to a working 6to4 relay at 192.88.99.1
  - Be aware that 6to4 cannot work behind CGN
  - If impossible, arrange to return ‘destination unreachable’ for 192.88.99.1
- In any case, allow inbound protocol 41 through firewalls.
  - Necessary for 6to4, and allows users to use a configured IPv6 tunnel service if they want
- Never use "bogon" address space such as 1.1.1.0/24
- Consider operating a 6to4 relay as a first baby step towards IPv6

Advice to consumer ISPs & enterprise networks that do support IPv6

- Advise users to disable 6to4; do not create DNS records for any 6to4 addresses.
- Ensure that no routers are unintentionally or by default set up as active 6to4 relays.
- Defend against rogue RA messages (RFC 6105).

Advice to transit ISPs and IXPs that support IPv6

- Run an Anycast 6to4 relay service for users
  - 192.88.99.0/24 announced only towards IPv4 nets whose outbound 6to4 packets will be accepted
  - 2002::/16 announced towards native IPv6. The relay must accept all traffic to 2002::/16 that reaches it
  - when the relay sends 6to4 packets back to a 6to4 user, use 192.88.99.1 as the IPv4 source address
  - ICMPv6 *echo request* and *packet too big* must work
  - IPv4 Protocol 41 not filtered
  - Performance must be adequate
  - No NAT in sight

Advice to IPv6 content providers and their ISPs

- Run a 6to4 relay service announcing 2002::/16 towards the content servers
  - dedicated to return traffic, not offering 192.88.99.1
  - scope advertisements for 2002::/16 so that content servers have a short path to the relay
  - if ingress filtering allows, relay should use 192.88.99.1 as the IPv4 source address
  - may embed a relay directly in the content server. Done by enabling a local 6to4 interface and using it to route 2002::/16 for outbound packets
  - other recommendations as above
- Don’t rely on reverse DNS.

Security considerations

- draft-ietf-v6ops-tunnel-security-concerns
- draft-ietf-v6ops-tunnel-loops
- RFC3964
- However, if an operator provides well managed 6to4 relays, non-encapsulated IPv6 packets will pass through well defined points (the native IPv6 interfaces of the relays) at which IPv6 security mechanisms may be applied.
- A blanket recommendation to block Protocol 41 is not compatible with mitigating the 6to4 problems.

Discussion?

Adopt the draft?

Push to finish it by IPv6 Day?

•

•

•

•

•

•