Request to move Connection of IPv6 Domains via IPv4 Clouds (6to4) to Historic status
draft-ietf-v6ops-6to4-to-historic-04.txt

Abstract

Experience with the "Connection of IPv6 Domains via IPv4 Clouds (6to4)" IPv6 transitioning mechanism has shown that the mechanism is unsuitable for widespread deployment and use in the Internet. This document requests that RFC3056 and the companion document "An Anycast Prefix for 6to4 Relay Routers" RFC3068 are moved to historic status.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 8, 2011.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must
1. Introduction

There would appear to be no evidence of any substantial deployment of the variant of 6to4 described in [RFC3056]. Its extension specified in "An Anycast Prefix for 6to4 Relay Routers" [RFC3068] has been shown to have severe practical problems when used in the Internet. This document requests that RFC3056 and RFC3068 be moved to Historic status as defined in section 4.2.4 [RFC2026].

6to4 was designed to help transitioning the Internet from IPv4 to IPv6. It has been a good mechanism for experimenting with IPv6, but because of the high failure rates seen with 6to4 [HUSTON], end users may end up disabling IPv6 on hosts, and content providers are reluctant to make content available over IPv6.

[I-D.ietf-v6ops-6to4-advisory] analyses the known operational issues and describes a set of suggestions to improve 6to4 reliability, given the widespread presence of hosts and customer premises equipment that support it.

The IETF sees no evolutionary future for the mechanism and it is not recommended to include this mechanism in new implementations.

6rd [RFC5969] utilizes the same encapsulation and base mechanism as 6to4, and could be viewed as a superset of 6to4 (6to4 could be achieved by setting the 6rd prefix to 2002::/16). However, the deployment model is such that 6rd can avoid the problems described here. In this sense, 6rd can be viewed as superseding 6to4 as described in section 4.2.4 of [RFC2026]

2. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. 6to4 operational problems

6to4 is a mechanism designed to allow isolated IPv6 islands to reach each other using IPv6 over IPv4 automatic tunneling. To reach the native IPv6 Internet the mechanism uses relay routers both in the
forward and reverse direction. The mechanism is supported in many IPv6 implementations. With the increased deployment of IPv6, the mechanism has been shown to have a number of fundamental shortcomings.

6to4 depends on relays both in the forward and reverse direction to enable connectivity with the native IPv6 Internet. A 6to4 node will send IPv4 encapsulated IPv6 traffic to a 6to4 relay, that is connected both to the 6to4 cloud and to native IPv6. In the reverse direction a 2002::/16 route is injected into the native IPv6 routing domain to attract traffic from native IPv6 nodes to a 6to4 relay router. It is expected that traffic will use different relays in the forward and reverse direction. RFC3068 adds an extension that allows the use of a well known IPv4 anycast address to reach the nearest 6to4 relay in the forward direction.

One model of 6to4 deployment as described in section 5.2, RFC3056, suggests that a 6to4 router should have a set of managed connections (via BGP connections) to a set of 6to4 relay routers. While this makes the forward path more controlled, it does not guarantee a functional reverse path. In any case this model has the same operational burden as manually configured tunnels and has seen no deployment in the public Internet.

List of some of the known issues with 6to4:

- Use of relays. 6to4 depends on an unknown third-party to operate the relays between the 6to4 cloud and the native IPv6 Internet.
- The placement of the relay can lead to increased latency, and in the case the relay is overloaded packet loss.
- There is generally no customer relationship or even a way for the end-user to know who the relay operator is, so no support is possible.
- In case of the reverse path 6to4 relay and the anycast forward 6to4 relay, these have to be open for any address. Only limited by the scope of the routing advertisement. 6to4 relays can be used to anonymize traffic and inject attacks into IPv6 that are very difficult to trace.
- 6to4 may black hole traffic in the case where protocol (41) is blocked in intermediate firewalls. Even if a firewall sent an ICMP message unreachable back, an IPv4 ICMP message rarely contains enough of the original IPv6 packet so that it can be relayed back to the IPv6 sender. That makes this problem hard to detect and react upon by the sender of the packet.
- As 6to4 tunnels across the Internet, the IPv4 addresses used must be globally reachable. RFC3056 states that a private address [RFC1918] MUST NOT be used. 6to4 will not work in networks that employ other addresses with limited topological span.
4. Deprecation

This document formally deprecates the 6to4 transition mechanism and the IPv6 6to4 prefix defined in [RFC3056], i.e., 2002::/16. The prefix MUST NOT be reassigned for other use except by a future IETF standards action.

It is expected that disabling 6to4 in the IPv6 Internet will take some time. The initial approach is to make the 6to4 a service of "last resort" in host implementations, ensure that the 6to4 service is disabled by default in 6to4 routers, and deploy native IPv6 service. In order to limit the impact of end-users, it is recommended that operators retain their existing 6to4 relay routers and follow the recommendations found in [I-D.ietf-v6ops-6to4-advisory]. When traffic levels diminish, these routers can be decommissioned.

1. IPv6 nodes SHOULD treat 6to4 as a service of "last resort" as recommended in [I-D.ietf-6man-rfc3484-revise]
2. Implementations capable of acting as 6to4 routers SHOULD NOT enable 6to4 without explicit user configuration. In particular, enabling IPv6 forwarding on a device, SHOULD NOT automatically enable 6to4.

Existing implementations and deployments MAY continue to use 6to4.

The references to 6to4 should be removed as soon as practical from the revision of the Special-Use IPv6 Addresses [RFC5156].

Incidental references to 6to4 should be removed from other IETF documents if and when they are updated. These documents include RFC3162, RFC3178, RFC3790, RFC4191, RFC4213, RFC4389, RFC4779, RFC4852, RFC4891, RFC4903, RFC5157, RFC5245, RFC5375, RFC5971, and RFC6071.

5. IANA Considerations

IANA is requested to mark the 2002::/16 prefix as "deprecated", pointing to this document. Reassignment of the prefix for any usage requires justification via an IETF Standards Action [RFC5226].

IANA is requested to mark the 2.0.0.2.ip6.arpa domain [RFC5158] as "deprecated", pointing to this document. Redelegation of the domain for any usage requires justification via an IETF Standards Action [RFC5226].

IANA is requested to mark the 192.88.99.0/24 prefix [RFC3068] as
6. Security Considerations

There are no new security considerations pertaining to this document. General security issues with tunnels are listed in [I-D.ietf-v6ops-tunnel-security-concerns] and more specifically to 6to4 in [RFC3964] and [I-D.ietf-v6ops-tunnel-loops].

7. Acknowledgements

The authors would like to acknowledge Tore Anderson, Dmitry Anipko, Jack Bates, Cameron Byrne, Gert Doering, Ray Hunter, Joel Jaeggli, Kurt Erik Lindqvist, Jason Livingood, Keith Moore, Tom Petch, Daniel Roesen and Mark Townsley, James Woodyatt, for their contributions and discussions on this topic.

Special thanks go to Fred Baker, Geoff Huston, Brian Carpenter, and Wes George for their significant contributions.

Many thanks to Gunter Van de Velde for documenting the harm caused by non-managed tunnels and to stimulate the creation of this document.

8. References

8.1. Normative References


[ RFC5226 ] Narten, T. and H. Alvestrand, "Guidelines for Writing an

8.2. Informative References


[I-D.ietf-v6ops-6to4-advisory] Carpenter, B., "Advisory Guidelines for 6to4 Deployment", draft-ietf-v6ops-6to4-advisory-01 (work in progress), April 2011.


Author’s Address

Ole Troan
Cisco
Oslo,
Norway

Email: ot@cisco.com