IPv6 Maintanence (6man)
Internet-Draft
Intended status: Informational
Expires: May 8, 2008

F. Baker
Cisco Systems

November 5, 2007

Multiprefix IPv6 Routing for Ingress Filters
draft-baker-6man-multiprefix-default-route-00

Status of this Memo

Copyright Notice

Abstract

This note addresses routing in a network that supports multiple prefixes and has different DMZs, in the context of BCPs 38 and 84 (ingress filtering). It proposes a change to the way IPv6 forwarding occurs, and so should be considered carefully by the Internet community.

Requirements Language

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 [RFC2119].

Table of Contents

1. Introduction

BCP 38 [RFC2827] recommends that routing systems protect themselves against spoofed source addresses by the application of ingress filtering. In short, this means discarding datagrams that purportedly come from addresses that the routing system does not believe are reachable from the direction whence they have arrived. BCP 84 [RFC3704] discusses the problems this raises in a multihomed network that uses multiple prefixes internally. In short, it recommends that a routing system route in such a way that datagrams are only presented to an upstream routing system if and only if that upstream routing system will not discard them in accordance with BCP 38.

In IPv6 [RFC2460] networks, this poses several problems. The IPv6 Addressing Architecture [RFC4291] leads one to assume that on any interface, a system is likely to have at least two addresses - its link local address and its address in the relevant prefix. If Privacy addresses [RFC4941] are in use, it might have many addresses in the same prefix. In a routing system with multiple prefixes overlaid, an interface might have numerous addresses even if it has only one per prefix.

It is this last situation that causes the present concern. Is there a way that we can ensure that routing to the egress router is optimal while ensuring that traffic sent upstream uses the right upstreams without forcing the host to be involved in datagram routing?

2. Proposal

In short, the author suggests that datagrams should be sent in a direction that will avoid ingress filtering, starting from the originating host. This section discusses the ramifications of that policy.

2.1. Host selection of an address

[RFC3484] describes an architecture by which a network administrator can define which source address prefixes should be used on datagrams sent to various destination prefixes. This proposal assumes that if remote non-default prefixes are propagated within a network, this technology governs the choice of address. As such, traffic headed to destinations for which there is routing other than the default route will never be sent to an upstream that will discard them.

2.2. Host selection of a router

Having selected a source address, the host must now determine what router to send its datagram to.

If Neighbor Discovery [RFC4861] or SEcure Neighbor Discovery [RFC3971] are in use, the prefix that the host is using will have been advertised to it in a Router Advertisement. In either case, the host SHOULD send the datagram to the router from which it learned the prefix.

if DHCP [RFC3315] is in use, it may be possible to rely on the Router Advertisements bring broadcast periodically. This case requires further thought.

2.3. Selection of a multipath route by a router

Once a datagram has been handed to a router, the router has two possible options: either it has a single route to that prefix, or it has a multipath route. If it has a single route or an internal route, it SHOULD of course use it.

If the chosen route is a multipath route to an external network, the router SHOULD use the path that was advertised into the network by the DMZ that injected the prefix used in the datagram's source address. This can be determined, for example, by observing the OSPF [RFC2740] inter-area-router-LSA, which will contain at least one interface using the prefix of the relevant upstream and will have a companion AS-external-LSA indicating a default route. This would generally apply t default routes, but may also apply to more specific aggregated routes advertised into the network via multiple DMZs.

3. IANA Considerations

This memo adds no new IANA considerations. The presence of this template text indicates that the author/editor has not actually reviewed IANA considerations.

Note to RFC Editor: This section will have served its purpose if it correctly tells IANA that no new assignments or registries are required, or if those assignments or registries are created during the RFC publication process. From the author"s perspective, it may therefore be removed upon publication as an RFC at the RFC Editor"s discretion.

4. Security Considerations

One could argue that hist note addresses a security concern raised in BCP 84, that the communications between two systems may be inhibited or obstructed by a poor choice of source address in a poorly thought through routing system. At this writing, the security issues have not been fully thought through, so this section needs to be updated.

5. Acknowledgements

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

6.2. Informative References

[RFC2740] Coltun, R., Ferguson, D., and J. Moy, "OSPF for IPv6", RFC 2740, December 1999.

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3484] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, March 2004.

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman,

"Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.

Author's Address

Fred Baker
Cisco Systems
Santa Barbara, California 93117
USA

Phone: +1-408-526-4257
Fax: +1-413-473-2403
Email: fred@cisco.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).