v6ops Working Group	N. Hilliard
Internet-Draft	INEX
Intended status: Informational	October 26, 2011
Expires: April 28, 2012	

A Discard Prefix for IPv6
draft-ietf-v6ops-ipv6-discard-prefix-01

Abstract

Remote triggered black hole filtering describes a method of militating against denial-of-service attacks by selectively discarding traffic based on source or destination address. Remote triggered black hole routing describes a method of selectively re-routing traffic into a sinkhole router (for further analysis) based on destination address. This document explains why a unique IPv6 prefix should be formally assigned by IANA for the purpose of facilitating IPv6 remote triggered black hole filtering and routing.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

Remote triggered black hole (RTBH) filtering describes a class of methods of blocking IP traffic either from a specific source or to a specific destination on a network. Remote triggered black hole (RTBH) routing describes a class of methods of re-routing IP traffic destined to the attacked/targeted host to a special path (tunnel) where a sniffer could capture the traffic for analysis. These methods operate by setting the next-hop address of an IP packet with a specified source or destination address to be a unicast prefix which is wired locally or remotely to a router's discard, null or tunnel interface. Typically, this information is propagated throughout an autonomous system using a dynamic routing protocol. By deploying RTBH systems across a network, traffic to or from specific destinations may be selectively black-holed or re-routed to a sinkhole device in a manner which is efficient, scalable and straightforward to implement. For IPv4, some networks configure RTBH installations using [RFC1918] address space or the address blocks reserved for documentation in [RFC5737].
However RTBH configurations are not documentation, but operationally important features of many public-facing production networks.
Furthermore, [RFC3849] specifies that the IPv6 documentation prefix should be filtered in both local and public contexts. On this basis, it is suggested that both private network address blocks and documentation prefixes described in [RFC5737] are inappropriate for the purpose of RTBH configurations.
While it could be argued that there are other addresses and address prefixes which could be used for this purpose (e.g. ::/128), or that an operator could assign an address block from their own address space for this purposes, there is currently no operational clarity on what address block would be appropriate or inappropriate to use for this purpose. By creating an assigned discard prefix for IPv6, the IETF will

introduce operational clarity and good practice for implementation of IPv6 RTBH configurations.

1.1. Notational 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 [RFC2119].

2. A Discard Prefix for IPv6

For the purposes of implementing an IPv6 remote triggered black hole configuration, a unicast address block is required. There are currently no IPv6 unicast address blocks which are specifically nominated for the purposes of implementing such RTBH systems.
As [RFC3882] and [RFC5635] describe situations where more than one discard address may be used for implementing multiple remote triggered black hole scenarios, a single assigned prefix is not sufficient to cover all likely RTBH situations. Consequently, an address block is required in preference to a single address.

3. Operational Implications

This assignment MAY be carried in a dynamic routing protocol within an autonomous system. The assignment SHOULD NOT be announced to third party autonomous systems and IPv6 traffic with an destination address within this prefix SHOULD NOT be forwarded to third party autonomous systems.
On networks which implement IPv6 remote triggered black holes, some or all of this network block MAY be configured with a destination of a discard or null interface on any or all IPv6 routers within the autonomous system.

4. IANA Considerations

This document directs IANA to record the allocation of the IPv6 address prefix xxxx/64 as a discard-only prefix in the IPv6 Address Space registry. No end party is to be assigned this prefix. The prefix should be allocated from ::/3.

5. Security Considerations

As the prefix specified in this document should not normally be transmitted or accepted over inter-domain BGP sessions, it is usually appropriate to include this prefix in inter-domain BGP prefix filters [RFC3704].

6. References

6.1. Normative References

[RFC3882]	Turk, D., "Configuring BGP to Block Denial-of-Service Attacks", RFC 3882, September 2004.
[RFC5635]	Kumari, W. and D. McPherson, "Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)", RFC 5635, August 2009.

6.2. Informative References

[RFC1918]	Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G. and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.
[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[RFC3704]	Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, March 2004.
[RFC3849]	Huston, G., Lord, A. and P. Smith, "IPv6 Address Prefix Reserved for Documentation", RFC 3849, July 2004.
[RFC5226]	Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.
[RFC5737]	Arkko, J., Cotton, M. and L. Vegoda, "IPv4 Address Blocks Reserved for Documentation", RFC 5737, January 2010.

Author's Address

Nick Hilliard Hilliard INEX 4027 Kingswood Road Dublin, 24 IE EMail: nick@inex.ie