BESS Workgroup
Internet-Draft
Intended status: Standards Track
Expires: July 20, 2019

Yuan Gao
Haibo Wang
Huawei Technologies
January 16, 2019

EVPN blackhole community extention for Blackholing
draft-gao-bess-evpn-blackhole-01

Abstract

Ethernet Virtual Private Networks (EVPN) is becoming the de-facto standard-based control plane solution for Data Center and layer-2 Service Provider applications.The risk of hacking and DDos attacks within the EVPN network is general common concern.Blackhole mac is a method used to block hacking or DDos attacks, The network device discard the packets where destionation match the blackhole mac.Normally blackhole mac is mannually configured on the networkdevic,Configure blackhole mac is complex and error-prone task for network operators.This document introduces a blackhole community extension for evpn mac route to distribute the blackhole mac in the EVPN networks.The evpn mac route with blackhole community allows the bgp speaker to notify the recipients the specific mac is a blackhole mac.

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 .

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 https://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 July 20, 2019.

Table of Contents

1. Introduction

Hacking attacks are a serious threat to the network infrastructure.In order to prevent a hacker from using a MAC address to attack a user device or network, the MAC address of an untrusted user is configured as blackhole mac on the network device.

DDoS attacks targeting a certain mac may cause congestion of links,In order to block DDoS attacks, the mac being attacked could be congfigured as blackhole mac on the network device, The network device directly discards the received packets where the destination MAC address is the blackhole MAC address.

Normally blackhole mac address entrys are manually configured on the device. After blackhole mac entrys are configured, the device discards packets destined for the blackhole mac address. Configure blackhole mac is complex and error-prone task for network operators. Therefore a well-known BGP community for blackholing based on evpn route is defined for operational ease.

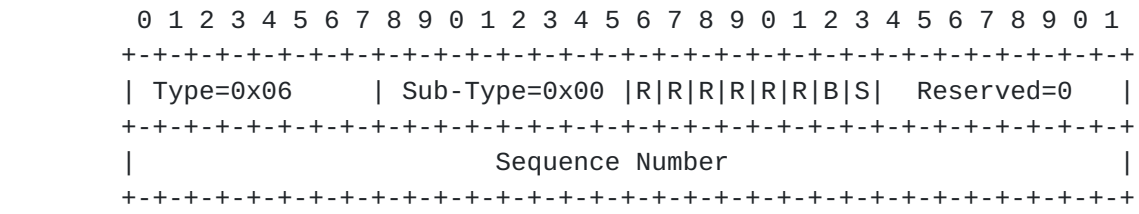
This document introduces a blackhole community extension for evpn mac route, The BGP speaker advertise evpn mac route with this community indicate that the specific mac is a blackhole mac, the recipients install the mac address as blackhole mac address entry and discard the packet corresponds to the blackhole mac address.

2. Blackhole Extended Community Attribute

MAC Mobility Extended Community can be used to carry the blackhole mac attribute. MAC Mobility Extended Community may be advertised along with MAC/IP Advertisement routes. The thirdly octet of the first word is Flags octect. The Flag bit 7(B Bit) of the flags octect is defined as the "blackhole" bit . A value of 1 means that the MAC address is blackhole mac . The semantics of this attribute is to allow a network to interpret the presence of this community as an advisory qualification to drop any traffic being sent towards or from this mac.

When the Mac Mobility Extended Community's B bit is set to 1, the sequence number is meaningless and should be set to zero.

The MAC Mobility extended community is encoded as an 8-octet value, as follows:



3. Control Plane Processing

When a network device is under DDos attack, it may announce the victim's mac address as blackhole mac address for the purpose of signaling to neighboring networks any traffic destinated to the mac address should be discard. In such a scenarior, the victim's mac route should attach Blackhole Extended Community. The network device will install the victim's mac address as blackhole mac entry. Then the network device advertise the victim's mac address in evpn mac route with MAC Mobility Extended Community, the MAC Mobility Extended Community set the "blackhole" flag . The recipients install the mac address as blackhole mac address entry.

4. Data Packets Processing

When the network device received packets where the destination MAC address match the blackhole MAC address. The network device discards the packet directly.

5. IANA Considerations

TBD.

6. Security Considerations

Unauthorized addition of the BLACKHOLE BGP community to a mac route by the forwarding agent may cause a unexpected packet discard. BGP have to support the mechanism to prevent the unauthorized modification of information by the forwarding agent.Recipients of routing information have the ability to to detect the unauthorized modification. Howto prevent the unauthorized modification is out of the scope of this document.

7. Acknowledgements

The authors of this document would like to thank zhuangshunwan for his comments and review of this document.

8. References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7432] Sajassi, A., Ed., Aggarwal, R., Bitar, N., Isaac, A., Uttaro, J., Drake, J., and W. Henderickx, "BGP MPLS-Based Ethernet VPN", RFC 7432, DOI 10.17487/RFC7432, February 2015, <https://www.rfc-editor.org/info/rfc7432>.

Authors' Addresses

Yuan Gao
Huawei Technologies
101 Software Avenue, Yuhua District
Nanjing 210012
P.R. China

Email: sean.gao@huawei.com

Haibo Wang
Huawei Technologies
Huawei Bld., No.156 Beiqing Rd.
Beijing 100095
P.R. China

Email: rainsword.wang@huawei.com