Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 13, 2022

G. Liu
H. Wang
T. Zhu
Huawei Technologies

July 12, 2021

EVPN LOOP PREVENTION BASED ON TRUSTED MAC
draft-glendon-bess-evpn-trusted-mac-02

Abstract

A principal feature of EVPN is the ability to support MAC duplication detection based on MAC Mobility Extended Community. This draft specifies a mechanism of valid loop prevention based on trusted MAC to avoid servce interruption of the specifed source or destination MAC address due to "black-holing".

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].

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 January 13, 2022.

Table of Contents

1. Introduction

A principal feature of EVPN is the ability to support MAC duplication dection based on MAC Mobility extended Community. The MAC duplication detection is proposed in EVPN [RFC7432]. The draft [draft-snr-bess-evpn-loop-protect] re-uses and enhances the MAC duplication solution specified in EVPN [RFC7432]. This draft is a further enhancement for [RFC7432] and [draft-snr-bess-evpn-loop-protect]. Trusted MAC is proposed to avoid servce interruption of the specifed source or destination MAC address due to "black-holing".

1.1. Situation Anyalisis

Based on [RFC7432], when the MAC duplication threshold is met(MAC moving for 5 times in 180 minutes in default), the PE MUST alert the operator and stop sending and processing any MAC/IP advertisement routes for that MAC address, but the other PEs in the EVI will forward the traffic for the duplicated MAC address to one of the PEs

that have advertised it. In order to prevent loop and not just detect loop, it is necessary to introduce a new mechanism, [draft-snr-bess-evpn-loop-protect] proposes the idea of "black-holing". "Black-holing" is a good means of service isolation, however, the user's real intention is that the system has the ability to recognize the real AC port or peer neighbour of the MAC after detecting MAC duplication successfully.

1.2. Alternative Solutions

Sticky MAC address is proposed in section 15.2 [RFC7432]. There are scenarios in which it is desired to configure static MAC addresses so that they are not subjected to MAC moves. In such scenarios, these MAC addresses are advertised with the MAC mobility extended community where the flags field is set to 1 and the sequence number is set to zero. Static MAC can be used to prevent loop without service interruption, but the following problems come:

1) In most scenarios, the user MAC is unpredictable, and it is impossible to predict the AC port or the peer neighbour for the user accessing to the specific PE.

2) Even if we can predict on the AC port or the peer neighbor that the user accesses, what should I do if the static MAC that is learned locally and the sticky MAC route that is received from the peer neighbour coexist at the same time? Customers are hard to understand, regardless of whether to choose local MAC or remote MAC.

1.3. Design Requirement

This draft proposes a new method to prevent loop based on trusted MAC. The generation of trusted MAC belongs to the local behavior of the PE. After the generation of trusted MAC, it is delivered to the EVPN neighbour through the EVPN route, and the MAC duplication detection mechanism based on the MAC mobility extended community is extended to finally generate a truly reliable MAC outbound interface or EVPN neighbour. Loop prevention comes true finally.

1.4. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

"PE": Provider edge device. It is a unique access point for users to access the carrier network.

"AC": A physical or logical link. It is used to connect a user edge device and a PE device.

"trusted MAC": The MAC entry to the AC port or EVPN neighbour. It is generated based on the user's trusted traffic.

2. Solution Overview

The draft includes the following technical points:

1) Trusted MAC sending and receiving is not the default behavior of the device. It is needed to manually configure the trusted MAC route sending enable (for the route sender) and the receiving enable (for the route receiver). The EVPN neighbours use the MAC route to implement trusted MAC capability negotiation.

2) Trusted MAC needs to be generated based on certain rules, then MAC mobility extended community is extended to add T bit for supporting trusted MAC delivery.

3) After trusted MAC negotiation and delivery, the MAC duplication detection mechanism between trusted MAC and static MAC needs to be supported. MAC duplication between trusted MAC and dynamic MAC is also a consideration.

3. Trusted MAC Capability negotiation

Although trusted MAC belongs to the device-level global capability, considering the simplicity of the protocol extension, the UMR (Unknown MAC Route, [RFC7543]) carries the MAC mobility extended community to support trusted MAC negotiation between the route sender and the receiver. The extension of the "Flags" field is needed. The MAC mobility extended community defined here is defined as follows:

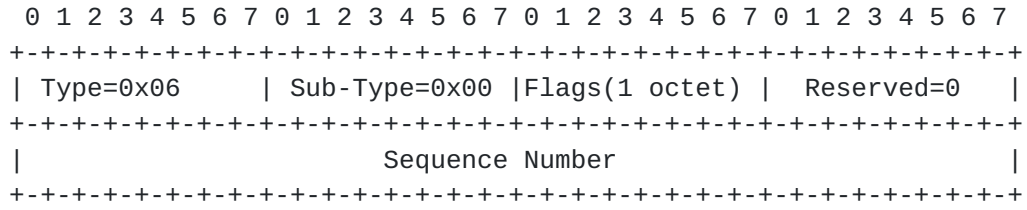

Figure 1: MAC Mobility Extended Community

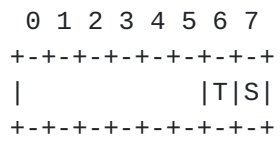

Figure 2. The extension of the "Flags" field

The bit 6 in the "Flags" field is marked as T bit and is used to indicate whether the trusted MAC route is enabled on the route sender.

Name Meaning

T If set to 1, this flag indicates that trusted MAC advertising capabilicy is enabled by the advertising PE.

If the trusted MAC advertising capability is not enabled, then the T bit must be set to 0.

For the receiving PE, it is necessary to determine whether to allow crossover based on the trusted MAC receiving enable configuration. If only the T bit is set and the trusted MAC route receiving for the receiving PE is enabled, the received route can finally crossed successfully. From the perspective of route optimization, if the trusted MAC route sending enable is not configured on the sender, the trusted MAC negotiation route may not be sent.

4. Trusted MAC Actions

4.1. Flag Extension

In order to distinguish between dynamic MAC, static MAC and trusted MAC, the flags field in MAC mobility extended community shown as section 3 figure 1 needs to extend new value.

Name Meaning

If Flag T-bit is set to 1 and S-bit is set to 1, it indicates that trusted sticky MAC is advertised to the remote PE.

If only flag T-bit is set to 1, it indicates that trusted dynamic MAC is advertised to the remote PE.

4.2. Trusted MAC Generation and Delivery

The generation of trusted MAC belongs to the local behavior of the PE. Generally speaking, the stable MAC out port or EVPN neighbor in the specified period of the first time learned locally is defined as trusted MAC. The specified period can be assigned to a default value, such as 60 seconds. The value of the period may be modified to other values, for example, 1 minutes, 5 minutes or else. Once the local trusted MAC is generated, it will not be overwritten by the other dynamic MAC, but it can be overwritten by static MAC. Since trusted MAC is still in the category of dynamic MAC, trusted MAC aging needs to support.

There exists several limitations for trusted MAC generation and delivery:

1) In a very poor network environment, the specified MAC may have a persistent mobility after the MAC entry is generated for the first time. In this case, trusted MAC may not be generated. Static MAC may only be used to restrict the forwarding behavior of the user's traffic.

2) After trusted MAC is generated, if the generation cycle of the trusted MAC is dynamically modified, the generated trusted MAC will not be deleted automatically in order to reduce the impact on the existing MAC duplication detection mechanism based on trusted MAC. If only trusted MAC is manually deleted or aged, the system will generate a new trusted MAC based on the modified period.

3) After trusted MAC is generated, if the specified MAC is reconfigured as a static MAC, the MAC route carrying the MAC mobility extended community with flags=1 will be re-advertised, so the result of the MAC duplication detection may be changed.

4) After trusted MAC is generated, if the specified MAC is reconfigured as a black-holing MAC, the previously advertised trusted MAC route needs to be withdrew to prevent invalid network traffic caused by the black-holing MAC.

5. Application Senario

5.1. Trusted MAC and Sticky MAC

The sticky MAC may be configured on the PE or be received from the other PEs, when trusted MAC and sticky MAC coexist in the same PE, There exist two sub-scenarios:

1) Only one sticky MAC exists beyond trusted MAC. The only sticky MAC guides the user's traffic and will survive forever until sticky MAC is manually deleted.

2) Several sticky MACs exist beyond trusted MAC. When there exists a local static MAC, since the local static MAC is unique, the user's traffic is preferentially guided according to the local MAC. When there exists no local static MAC, the same PE may receive the same sticky MAC from different EVPN neighbours. Therefore, the PE selects the sticky MAC route from the neighbour with th smallest original ip address to guide the final user's traffic.

In the above two sub-scenarios, the coexistence between trusted MAC and sticky MAC triggers the MAC duplication alarm, and all trusted MACs are eventually ignored.

5.2. Trusted MAC and Dynamic MAC

The coexistence of trusted MAC and dynamic MAC occurs when there is no sticky MAC in the system, There exist two sub-scenarios:

1) Only one trusted MAC (local or remote) exists beyond dynamic MAC. The only trusted MAC guides the user's traffic and will age when the user's traffic based on the trusted MAC (source MAC or desination MAC) disappears.

2) Several trust MACs exist beyond dynamic MAC. The locally learned trusted MAC or the trusted MAC route received from the remote PE have higher priority than the normal dynamic MAC. After detecting the MAC duplication, the locally learned trust MAC or the trusted MAC route with the larger serial number is used to guide the final user's traffic.

Note: If the local PE receives the trusted MAC route with the same serial number from different neighbours, the route received from the neighbour with the smallest original ip is selected to participate in the MAC duplication detection.

5.3. Limitations

the default MAC route received from the other PE cannot participate in the MAC duplication detection. In this case, the traffic-based MAC duplication detection mechanism can only be used on the access side. Similarly, the priority of sticky MAC is higher than trusted MAC, the priority of trusted MAC is higher than dynamic MAC.

6. Security Considerations

When multiple network elements in the same network detect the MAC duplication at the same time, trusted MAC may cause the traffic between the network elements to loop. The probability of this situation is relatively small. Perhaps the user's traffic can only be isolated by black holing in order to reduce the whole network security risk.

7. IANA Considerations

NA

8. Contributors

NA

9. References

[I-D.snr-bess-evpn-loop-protect]
Rabadan, J., Sathappan, S., Nagaraj, K., Bueno, J., and J. M. Crespo, "Loop Protection in EVPN networks", draft-snr-bess-evpn-loop-protect-04 (work in progress), August 2019.

[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>.

[RFC7543] Jeng, H., Jalil, L., Bonica, R., Patel, K., and L. Yong, "Covering Prefixes Outbound Route Filter for BGP-4", RFC 7543, DOI 10.17487/RFC7543, May 2015, <https://www.rfc-editor.org/info/rfc7543>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

Authors' Addresses

GuoLiang Liu
Huawei Technologies
No.101 Software Avenue, Yuhuatai District
Nanjing 210012
China

Email: liuguoliang@huawei.com

Haibo Wang
Huawei Technologies
Huawei Bld., No.156 Beiqing Rd.
Beijing 10095
China

Email: rainsword.wang@huawei.com

Tong Zhu
Huawei Technologies
No.101 Software Avenue, Yuhuatai District
Nanjing 210012
China

Email: zhu.tong@huawei.com