Abstract

A principal feature of EVPN is the ability to support multihoming from a customer equipment (CE) to multiple provider edge equipment (PE) with all-active links. This draft specifies a mechanism of default mac to reduce amounts of advertising mac route and enhance EVPN network reliability.

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 9, 2020.

Copyright Notice

Copyright (c) 2019 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 (https://trustee.ietf.org/license-info) in effect on the date of
Table of Contents

1. Introduction ................................................. 2
   1.1. Situation Anyalisis ................................... 2
   1.2. Alternative Solutions ................................. 3
   1.3. Design Requirement .................................. 3
   1.4. Terminology .......................................... 4
2. Solution Overview ............................................ 4
3. Default MAC Capability negotiation ......................... 5
4. Default MAC Actions .......................................... 6
   4.1. Mac Route Extension ................................ 6
   4.2. Default MAC Flow Transmission ....................... 6
5. Application Senario ........................................... 7
   5.1. Remote Interaction ................................... 7
   5.2. Local Interaction .................................... 8
6. Security Considerations ..................................... 8
7. Acknowledgements ............................................ 8
8. Contributors ............................................... 8
9. References ................................................ 9
Authors’ Addresses .............................................. 9

1. Introduction

A principal feature of EVPN is the ability to support multihoming from a customer equipment (CE) to multiple provider edge equipment (PE) with links used in the all-active redundancy mode. That mode is where a device is multihomed to a group of two or more PEs and where all PEs in such a redundancy group can forward traffic to/from the multihomed device or network for a given VLAN (RFC7209). This draft specifies a mechanism of default mac to reduce amounts of advertising mac route and enhance EVPN network reliability.

1.1. Situation Anyalisis

One of the biggest features of EVPN is to transfer the VPLS network side MAC address learning and publishing process from the data plane to the control plane. But it also brings obvious drawbacks. Firstly, compared with the route aggregation in the EVPN L3VPN scenario, the MAC address of the control plane cannot be aggregated, which results in a large overhead for large-scale user MAC advertisements. Secondly, different from routing, the local MAC address will age
periodically, causing intermittent MAC revoke routing in all EVPN network. This kind of route revocation is directed to the EVPN network, which has a great impact on the performance of the network. At last, EVPN advertises all user MACs to all reachable neighbors. For a single device, the MAC capacity is equal to the sum of MACs sent by all neighbors. However, the mac capacity of a single device is limited. The risk of insufficient MAC is widespread. MAC Once exceeded, the EVPN network data traffic will be flooded.

1.2. Alternative Solutions

The MAC routing in 1.1 is based on the risk that the flooding of the EVPN neighbors on the control plane may cause flooding of the network traffic. Without modifying the basic principles of protocol interaction and traffic forwarding, there are two main solutions for mitigating risks:

1) Statically limit the number of local MAC learning on the AC side of the routing source device. This limitation can be either interface-based or broadcast domain-based. This solution has a certain protection effect on the large-size MAC traffic injection on the access side.

2) For the routing initiator device to limit the number of PEER-level MAC routes to be advertised, the solution is especially applicable to scenarios where the user MAC traffic is not large but the number of EVPN neighbors is large. A scene with a large number of user MAC addresses and a large number of EVPN neighbors needs to be combined with 1) for protection.

1.3. Design Requirement

Although the user local MAC restriction and the neighbor-based MAC restriction mentioned in 1.2 have an inhibitory effect on the size of the entire network MAC route, the disadvantages are obvious:

1) The number of access users and the number of neighbors in each device in the network are different, and the order of magnitude may vary greatly. Therefore, the network administrator must be aware of the dynamic changes of users and neighbors, and adjust the MAC limit value in real time. The cost of maintenance is very high.

2) When the network environment is unstable, there may be a large number of illegal user MAC attacks. The device cannot identify the illegal MAC address and the legal MAC address. The illegal MAC address causes the global MAC address to reach the upper limit. The data traffic destined for the legitimate user MAC on the network side continues to be flooded.
In order to avoid the problem that the number of network MAC routes increases exponentially with the number of users and neighbors, the solution of default MAC route generation and release is proposed by referring to the default route scheme of the L3VPN scenario.

Draft ietf-bess-dci-evpn-overlay-10#section-3.5.1 only mentions the concept of all-zero MAC routing, but does not describe the application scenarios and implementation principles of all-zero MAC. The purpose of this draft is to describe the default MAC capability negotiation, default MAC routing sending and receiving, default MAC application scenario, default MAC mobility and so on completely based on all-zero MAC.

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.

"LOCAL PE": The local PE refers to the CSG PE. The local PE needs to be configured with the default MAC route receiving enable.

"REMOTE PE": The remote PE refers to the RSG PE. The remote PE needs to be configured with the default MAC route sending enable.

"default mac": Similar to the default route, it is used to guide the forwarding behavior when the unicast traffic misses the detailed MAC entry.

2. Solution Overview

The program includes the following points:

1) The default MAC advertisement is not the default behavior of the device. You need to manually configure the default MAC route sending enable (for the route sender) and the receive enable (for the route receiver). The EVPN neighbors use the MAC route to implement the default MAC capability negotiation.

2) default mac routing sending and receiving needs to be supported. Unicast traffic additionally matches the default mac in case of detailed MAC mismatching.

3) After the default MAC capability negotiation is successful, AC interworking (including the same PE and cross-PE) needs to be supported.
3. Default MAC Capability negotiation

Although the default MAC belongs to the device global capability, considering the simplicity of the protocol extension, the MAC-IP route carries the Layer 2 Attributes extended community to support the default mac negotiation between the route sender and receiver. The extention of the "Reserved" field is needed. The Layer 2 Attributes extended community defined here is defined as follows:

```
+-------------------------------------------+
|  Type (0x06) / Sub-type (0x04) (2 octets) |
+-------------------------------------------+
|  Control Flags  (2 octets)               |
+-------------------------------------------+
|  L2 MTU (2 octets)                       |
+-------------------------------------------+
|  Reserved (2 octets)                     |
+-------------------------------------------+
```

Figure 1: EVPN Layer 2 Attributes Extended Community

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7
+-------------------------------------------+
|  D |                                          |
+-------------------------------------------+
```

Figure 2. The extention of the "Reserved" field

The first bit in the "Reserved" field is used to indicate whether the default MAC route is enabled on the route sender.

Name Meaning

Name Meaning

D If set to 1, this flag indicates that default mac advertising capability is enabled by the advertising PE.

If the default mac advertising capability is not enabled, then the bit must be set to 0.

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

4. Default MAC Actions

4.1. Mac Route Extension

Based on the D bit in the Layer 2 attributes extended community defined in Section 3, the default MAC route is released by the special 0 mac and Layer 2 attributes extended community. The extended MAC routing format is as follows:

```
+---------------------------------------+     
|  RD (8 octets)                       +     
|Ethernet Segment Identifier (10 octets)|     
|---------------------------------------+     
|  Ethernet Tag ID (4 octets)           |     
|---------------------------------------+     
|  MAC Address Length (=48)             |     
|---------------------------------------+     
|  MAC Address (=0)                     |     
|---------------------------------------+     
|  IP Address Length (1 octet)          |     
|---------------------------------------+     
|  IP Address (0, 4, or 16 octets)      |     
|---------------------------------------+     
|  MPLS Label1 (3 octets)               |     
|---------------------------------------+     
|  MPLS Label2 (0 or 3 octets)          |     
```

Figure 3. Extended Mac Route Format

The Ethernet Tag ID, MAC Address Length, MAC Address, IP Address Length, and IP Address fields are still considered to be part of the prefix in the NLRI. At the same time, the MAC address field must be filled in all zero.

4.2. Default MAC Flow Transmission

For the data traffic from the network side to the access side, the BUM traffic still goes through the broadcast process, and unicast traffic preferentially matches the detailed MAC, and the broadcast process goes on for mismatching. For data traffic from the access side to the network side, broadcast and multicast traffic still go through the broadcast process. The priority control of unicast traffic is as follows:
1) Query the detailed MAC entry, if it matches, the traffic is forwarded according to the detailed MAC entry, otherwise go to 2);

2) Query the default MAC entry, if it matches, forward the traffic according to the default MAC entry, otherwise go to 3);

3) Neither hit the detailed MAC entry nor hit the default MAC entry, indicating that the device does not enable the MAC route receiving capability and is unknown to unicast, and can only go through the broadcast process.

5. Application Scenario

5.1. Remote Interaction

The remote-side interaction refers to the interworking between the users of different PEs. For the unicast traffic from the local PE to the remote PE, the local PE hits the default MAC address and goes to the remote PE. The unicast traffic of the local PE takes precedence over the detailed MAC address. If the detailed MAC is missed, the broadcast is performed.

For the case where the local PE is dual-homed to two remote PEs, there exists two scenarios:

1) In the dual-active scenario, the 0 MAC routes or the 0 MAC route/EVI-AD routes sent by the remote PE1 and the remote PE2 form a load-sharing relationship on the local PE.

2) For the single-live scenario, the 0 MAC routes or the 0 MAC route/EVI-AD routes sent by the remote PE1 and the remote PE2 form a master/slave relationship on the local PE.

Based on the implementation of 1) and 2), the local PE can be instructed to go to the remote PE for unicast traffic with ms-level fault fast switch.

For the case where the remote PE is dual-homed to two local PEs, the existing dual-homing technology is completely inherited, and no additional scenario expansion is required.

For ARP/ND pickup, the local ARP/ND learning extension is required to generate a 0 MAC ARP/ND pickup entry. After the remote PE receives the ARP/ND route, the extension supports the generation of a 0 MAC ARP/ND pickup entry.

For the E-Tree function, the flag corresponding to the Root and Leaf roles is carried in the MAC route as the E-Tree extended community
attribute content, and the default MAC route advertisement and reception processing is not additionally processed.

5.2. Local Interaction

Local interaction refers to the interworking of user traffic on the same PE. To prevent local traffic from hitting the default MAC address, set the MAC aging time to be greater than the ARP aging time on the local PE. For example, the default ARP aging time is 20 minutes, then the MAC aging time can be configured to 30 minutes. As a result, MAC address entries for local interworking are always present. You do not need to consider the impact of matching the default MAC address.

When the MAC address aging time is less than 20 minutes, once the destination MAC address is aged out, the local PE will match the default MAC address. The solution may be: The access side is flooded, and the default MAC address is taken on the network side. Therefore, once the destination user goes online, the flooding on the access side will disappear. However, the MAC address of the remote interworking will continue to flood, and the impact on the network may only be reduced by configuring BUM suppression.

6. Security Considerations

By default, the MAC route is an abnormal route. The route receiving router may not support the forwarding process based on the default MAC route. Forcibly receiving the 0 MAC route may cause the forwarding exception. Therefore, if the MAC route receiving capacity is not configured, 0 MAC routes must be discarded.

7. Acknowledgements

The author of this document would like to thank Yuan Gao, Yang Huang, Tong Zhu for their comments and review of this document.

8. Contributors

The following individuals gave significant contributions to this document:

Haibo Wang
Huawei Technologies
rainsword.wang@huawei.com
9. References


Authors’ Addresses

GuoLiang
Huawei Technologies
101 software Avenue, Yuhua District
Nanjing 210012
China

Email: liuguoliang@huawei.com

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

Email: rainsword.wang@huawei.com