Catalyst 9500X/9600X系列交换机上EVPN中的DHCP丢包故障排除

目录

简介

本文档介绍Cisco Catalyst 9500X/9600X系列交换机上EVPN中DHCP丢包的故障排除步骤和解决方案。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本了解DHCP及其在网络中的运行。
- 熟悉Cisco IOS命令和故障排除技术。
- 知识：LAN交换和路由协议。
- 了解EVPN常见配置方案。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 硬件：Cisco Catalyst 9500X-28C8D、9500X-60L4D或9600X-SUP-2
- 软件版本：17.12.x

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题

观察到的问题是，当DHCP客户端和服务器连接到同一VTEP/枝叶节点，但位于两个不同的VRF中时，充当中继代理的交换机将丢弃从DHCP服务器返回的DHCP数据包(DHCP OFFER)。

在本示例中，客户端位于VLAN 10中的VRF绿色，而服务器位于VLAN 20中的VRF红色。

- 此问题可以通过以下命令输出确定：

<#root>

```
device#

show run interface vlan 10

interface Vlan10
 description CLIENT
 mac-address cafe.cafe.cafe


vrf forwarding GREEN

 ip dhcp relay source-interface Loopback10
 ip address 172.30.208.1 255.255.255.128

 ip helper-address vrf RED 192.168.1.10 <-- Leaking from GREEN to RED



device#

show run interface vlan 20

interface Vlan20
 description SERVER
 mac-address abcd.abcd.abcd

 vrf forwarding RED                  <--- Server is in VRF RED (Same VTEP)

 ip address 192.168.1.1 255.255.255.0


device#

show plat soft fed switch active punt asic-cause br

ASIC Cause Statistics Brief

+--------------------------------------------------------------------------------+
| Source |         Cause        |           Rx            |

Drop

          |
|        |                      |     cur    |    delta   |     cur    |    delta   |
+--------------------------------------------------------------------------------+

    LPTS

DHCPv4 S to S

           577087870         9219

30905
```

```
7  <-- Drops in this counter

    LPTS    DHCPv4 C to S               56467            0        56467            0
```

解决方案

该解决方案涉及升级软件版本以解决此问题。这些步骤概括了整个过程：

选项1：应用解决方法

- 将DHCP服务器移动到不依赖该服务器的DHCP客户端的其他VTEP
- 部署多个DHCP服务器
- 将服务器移出交换矩阵。

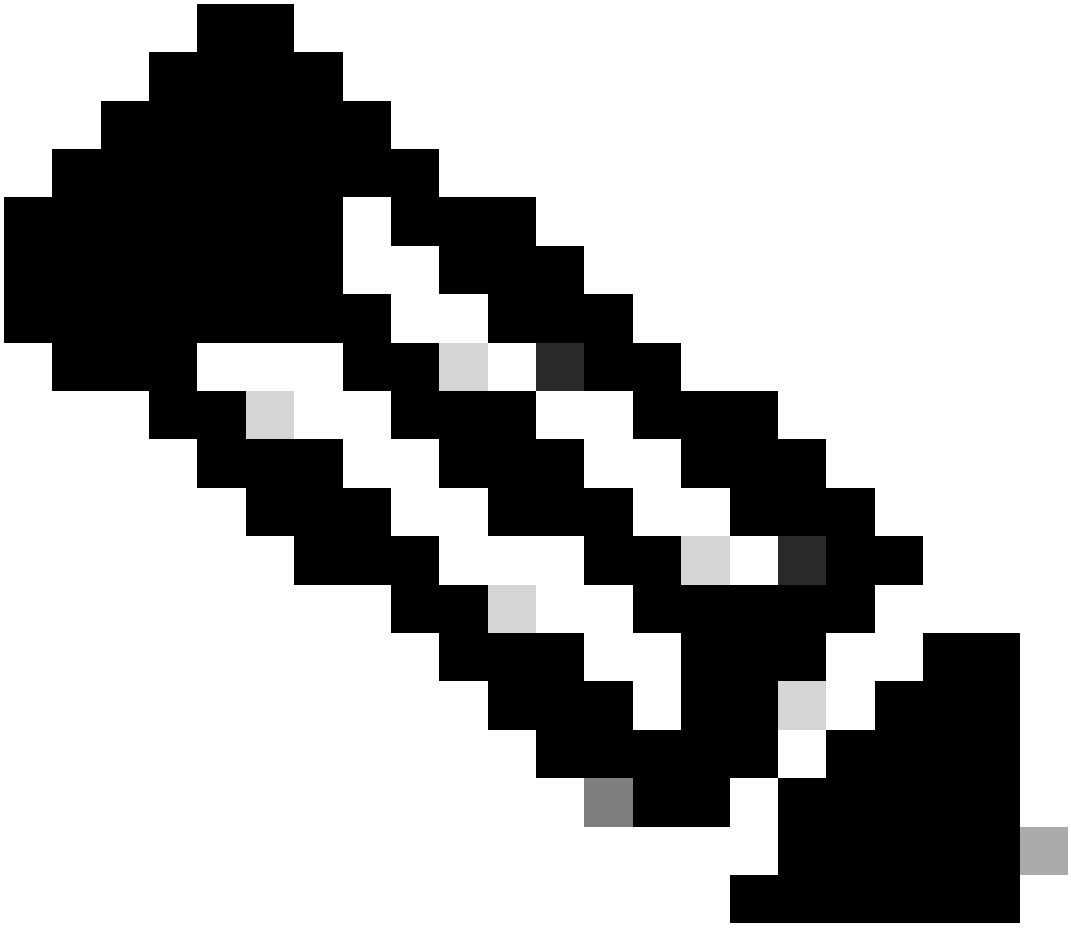
选项2：升级软件

将交换机升级到可修复Cisco Bug ID CSCwm44805的代码版本

- 版本17.15.1及更高版本。

升级过程不在本文档的讨论范围之内。 有关如何升级交换机的详细信息，请参阅：

- 9500安装和升级指南
- 9600安装和升级指南
- Catalyst 9000 交换机升级指南
- Catalyst 9200/9300/9400/9500/9600 平台的推荐版本



注意： 在17.15.1之前的版本系列中，没有修复此问题的计划

相关信息

- 思科技术支持和下载
- 思科漏洞ID CSCwm44805

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。