【MVS】Cisco设备DHCP snooping的作用及举例

设备管理 **胡伟** 2024-01-09 发表

问题描述

【MVS】Cisco设备DHCP snooping的作用及举例

解决方法

由于没有附带具体的展示图，我只能提供一个基于典型场景的解释。

当在交换机上启用DHCP snooping后，交换机会区分未受信任的和受信任的端口。默认情况下，所有端口都被视为未受信任的端口。DHCP snooping特性会阻止未受信任端口上的DHCP服务器响应（比如OFFER、ACK、NAK等DHCP消息），因为它假定这些响应可能来自一个恶意的DHCP服务器。

如果DHCP服务器连接到一个被标记为未受信任的端口，那么来自该服务器的DHCP响应将会被交换机拦截，导致客户端无法获得DHCP配置。为了解决这个问题，需要将连接到DHCP服务器的交换机端口配置为受信任的，以允许DHCP响应通过。

要修复这个问题，你需要在连接到CPE路由器的交换机端口上执行以下命令，将其设置为受信任的端口：

```cisco
interface [接口号]
 ip dhcp snooping trust
```

请将 `[接口号]` 替换为实际连接到DHCP服务器的端口号。例如，如果DHCP服务器连接到交换机端口`GigabitEthernet1/0/1`，那么需要在该端口上执行如下命令：

```cisco
interface GigabitEthernet1/0/1
 ip dhcp snooping trust
```

这样设置后，来自该端口的DHCP消息将被视为合法的，并且能够到达连接到该交换机的DHCP客户端。在配置完成后，客户端应该能够正常地从DHCP服务器获取配置信息。