

MACFF配置

目 录

第 1 章 MACFF 配置.....	1
1.1 MACFF 配置任务.....	1
1.1.1 开启/关闭 MACFF 功能.....	1
1.1.2 在 VLAN 上启动 MACFF.....	1
1.1.3 在 VLAN 上配置 MACFF 的默认 AR.....	2
1.1.4 在 VLAN 上配置 MACFF 的其他服务 AR.....	2
1.1.5 指定物理端口关闭 MACFF.....	2
1.1.6 打开 MACFF 调试开关.....	3
1.1.7 MACFF 配置示例.....	3

第 1 章 MACFF 配置

1.1 MACFF配置任务

MACFF 的任务就是隔离交换机上同一个 vlan 的下连端口之间的互访报文，使得这些报文必须通过 dhcp 服务器分配给客户端的默认网关，由默认网关转发至下连端口。通过截获下连端口之间的 ARP 报文，来阻止下连端口间的 ARP 学习，并且回复网关的 MAC 地址，从而达到所有下连端口之间的互访报文都经过网关处理的目的。

注：MACFF 需要 DHCP-snooping 的支持，在启用 MACFF 前请确保 DHCP-snooping 正常工作。默认网关需要关闭 ICMP 重定向。启用 MACFF 的交换机必须配置 vlan 管理地址。

- 开启/关闭 MACFF 功能
- 在 VLAN 上启动 MACFF
- 在 VLAN 上配置 MACFF 的默认 AR
- 在 VLAN 上配置 MACFF 的其他服务 AR
- 指定物理端口关闭 MACFF 功能

1.1.1 开启/关闭 MACFF 功能

在全局配置模式下进行下列配置：

命令	目的
macff enable	开启MACFF功能。
no macff enable	恢复缺省设置。

该命令是启动 MACFF 功能的全局控制命令。配置该命令，则交换机侦听所有 ARP 报文。

注意：在配置此命令之前，请确保已经打开 DHCP-snooping。如果客户端是在配置 DHCP-snooping 之前通过此交换机获取地址，则交换机不能添加相应的 DHCP 绑定关系。

1.1.2 在 VLAN 上启动 MACFF

在 VLAN 上启动 MACFF 功能，则对属于整个 VLAN 的所有 DHCP-snooping 非信任物理端口收到的 ARP 报文进行监听。响应 VLAN 内的非信任物理端口收到的 ARP 报文请求，如果请求目标 ip 地址为收到报文所在物理端口的任一 DHCP client 的 ip 地址，那么将此报文丢弃；如果是 ARP response，那么将此报文丢弃；如果是请求本端口的其他 DHCP client、默认网关或者其他服务地址那么会用相应 mac 地址回复 ARP 请求。

注意：启用 MACFF 的 vlan 必须配置 vlan 的管理地址，必须启用 DHCP-snooping。

在全局配置模式下进行下列配置：

命令	目的
----	----

macff vlan <i>vlan_id</i> enable	在VLAN上启动MACFF功能
no macff vlan <i>vlan_id</i> enable	在VLAN上关闭MACFF功能。

1.1.3 在 VLAN 上配置 MACFF 的默认 AR

在 *vlan* 上配置 MACFF 的默认 AR，此功能在客户端手动配置地址时（或者 DHCP server 没有配置默认路由 option3，但不建议这样使用 DHCP server），交换机会自动启用默认 AR 作为 MACFF 指定的默认网关（建议与客户端手动配置的默认网关一致），且默认 AR 只能有一个。

在全局配置模式下进行下列配置：

命令	目的
macff vlan <i>vlan_id</i> default-ar A.B.C.D	在VLAN上配置MACFF的默认AR。
no macff vlan <i>vlan_id</i> default-ar A.B.C.D	在VLAN上删除MACFF的默认AR。

注意：在配置此命令之前，可以通过 **ip source binding *xx:xx:xx:xx:xx:xx* A.B.C.D interface *name*** 来手动添加客户端在交换机上的绑定表，不这样做 MACFF 默认把手动配置的客户端作为非法客户端，MACFF 不会为其提供服务。

1.1.4 在 VLAN 上配置 MACFF 的其他服务 AR

在 *vlan* 上配置 MACFF 其他服务 AR，配置了其他服务 AR 以后，MACFF 允许 DHCP client 直接访问这些服务 AR，而无需将报文通过 DHCP server 分配的默认网关转发。

此功能可以在 *client* 的同网段下有某些服务器或者其他服务地址时使用。

在全局配置模式下进行下列配置：

命令	目的
macff vlan <i>vlan_id</i> other_ar A.B.C.D	在VLAN上配置MACFF的其他服务AR。
no macff vlan <i>vlan_id</i> other_ar A.B.C.D	在VLAN上删除MACFF的其他服务AR。

1.1.5 指定物理端口关闭 MACFF

指定物理端口关闭 MACFF，则该接口的报文不做隔离，且不对 ARP 报文监听。

在物理接口配置模式下进行下列配置：

命令	操作
macff disable	指定物理端口停用MACFF
no macff disable	指定物理端口启用MACFF（默认启用）。

缺省情况下接口允许启用 MACFF。

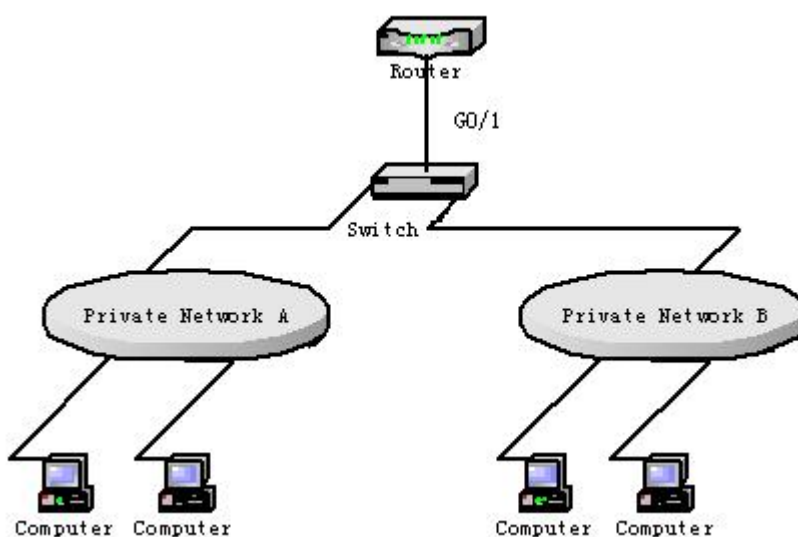
1.1.6 打开 MACFF 调试开关

在全局配置模式下进行下列配置：

命令	操作
debug macff	打开macff调试开关
no debug macff	关闭macff调试开关

1.1.7 MACFF 配置示例

示例网络连接如图 1：



配置 Switch：

- (1) 开启连接 Private Network A 的 VLAN 1 的 MACFF，.DHCP 服务器分配的默认网关为 192.168.2.1。


```
Switch_config#arp 192.168.2.1 00:e0:0f:17:92:ed vlan 1
Switch_config#ip dhcp-relay snooping
Switch_config#ip dhcp-relay snooping vlan 1
Switch_config#macff enable
Switch_config#macff vlan 1 enable
```
- (2) 开启连接 Private Network B 的 VLAN 2 的 MACFF，DHCP 服务器分配的默认网关为 192.168.2.2（如果需要，也可以是 192.168.2.1）。


```
Switch_config#arp 192.168.2.2 00:e0:0f:ea:74:ee vlan 2
Switch_config#ip dhcp-relay snooping vlan 2
Switch_config#macff vlan 2 enable
```
- (3) 配置 DHCP 服务器、默认网关连接端口和其他服务 AR 连接端口为信任端口。

```
Switch_config_g0/1#dhcp snooping trust
```

(4) 如果 vlan 1 下的下连主机 A 为手动配置的 ip 地址和默认网关，IP 地址为 192.168.2.102，MAC 地址为 6c:62:6d:59:18:b7，默认网关为 192.168.2.1 使得 MACFF 对其生效。（如果没有手动配置的客户端，跳过此步骤。）

```
Switch_config#arp 192.168.2.1 00:e0:0f:17:92:ed vlan 1
```

```
Switch_config#ip source binding 6c:62:6d:59:18:b7 192.168.2.102  
interface GigaEthernet0/1
```

```
Switch_config#macff vlan 1 default-ar 192.168.2.1
```

(5) 在启用 macff 的 vlan 下对指定物理端口关闭 macff。

```
Switch_config_g0/1#macff disable
```

(7) 配置与客户端主机同网段的其他服务 AR，MACFF 将允许客户端主机不通过默认网关而直接访问。（其他服务 AR 所在端口需要设置为信任端口）

```
Switch_config_g0/1#macff disable
```