MAC VLAN 技术白皮书

目 录

1 概述

1.1 产生背景

VLAN 最常用的划分方式是基于端口划分，该方式按照设备端口来划分 VLAN 成员，将指定端口加入到指定 VLAN 中之后，该端口就可以转发该 VLAN 的报文。该方式配置简单，适用于终端设备物理位置比较固定的组网环境。随着移动办公和无线接入的普及，终端设备不再通过固定端口接入设备，它可能本次使用端口 A 接入网络，下次使用端口 B 接入网络。如果端口 A 和端口 B 的 VLAN 置不同，则终端设备第二次接入后就会被划分到另一 VLAN，导致无法使用原 VLAN 内的资源；如果端口 A 和端口 B 的 VLAN 配置相同，当端口 B 被分配给别的终端设备时，又会引入安全问题。如何在这样灵活多变的网络环境中部署 VLAN 呢？MAC VLAN 应运而生。

MAC VLAN 是基于 MAC 划分 VLAN，它根据报文的源 MAC 地址来划分 VLAN，决定为报文添加某个 VLAN 的标签。该功能通常和安全技术（比如 802.1X）联合使用，以实现终端的安全、灵活接入。

1.2 技术优点

MAC VLAN 具有以下优点：

- MAC VLAN 能够实现精确的接入控制，它能精确定义某个终端和 VLAN 的绑定关系，从而实现将指定终端的报文在指定 VLAN 中转发。
- MAC VLAN 能够实现灵活的接入控制，同一终端通过不同端口接入设备时，设备会给终端分配相同的 VLAN，不需要重新配置 VLAN；而不同终端通过同一端口接入设备时，设备可以给不同终端分配不同的 VLAN。

2 技术实现

2.1 运行机制

设备是如何根据 MAC 地址来划分 VLAN 的呢？当端口收到一个 untagged 报文后，以报文的源 MAC 地址为匹配关键字，通过查找 MAC VLAN 表项来获知该终端绑定的 VLAN，从而实现将指定终端的报文在指定 VLAN 中转发。

MAC VLAN 表项有两种生成方式：静态配置和动态配置。

2.1.1 静态 MAC VLAN

1. 手动配置静态 MAC VLAN

手动配置静态 MAC VLAN 常用于 VLAN 中用户相对较少的网络环境。在该方式下，用户需要手动配置 MAC VLAN 表项，开启基于 MAC 地址的 VLAN 功能，并将端口加入 MAC VLAN。其原理为：

- 当端口收到的报文为 Untagged 报文时，根据报文的源 MAC 地址匹配 MAC VLAN 表项。

a. 首先进行模糊匹配，即查询 MAC VLAN 表中掩码不是全 F 的表项。将源 MAC 地址和掩码相与运算后与 MAC VLAN 表项中的 MAC 地址匹配。如果完全相同，则模糊匹配成功，为报文添加表项中对应的 VLAN Tag 并转发该报文。

b. 如果模糊匹配失败，则进行精确匹配，即查询表中掩码为全 F 的表项。如果报文中的源 MAC 地址与某 MAC VLAN 表项中的 MAC 地址完全相同，则精确匹配成功，为报文添加表项中对应的 VLAN Tag 并转发该报文。

c. 如果没有找到匹配的 MAC VLAN 表项，则继续按照其他原则（基于 IP 子网的 VLAN、基于协议的 VLAN、基于端口的 VLAN）确定报文所属的 VLAN，为报文添加对应的 VLAN Tag 并转发该报文。

- 当端口收到的报文为 Tagged 报文时，如果报文的 VLAN ID 在该端口允许通过的 VLAN ID 列表里，则转发该报文；否则丢弃该报文。

该方式实现简单，只涉及接入设备，但该方式下需要在终端可能接入的端口手工配置允许终端的 MAC VLAN 通过，配置量大。

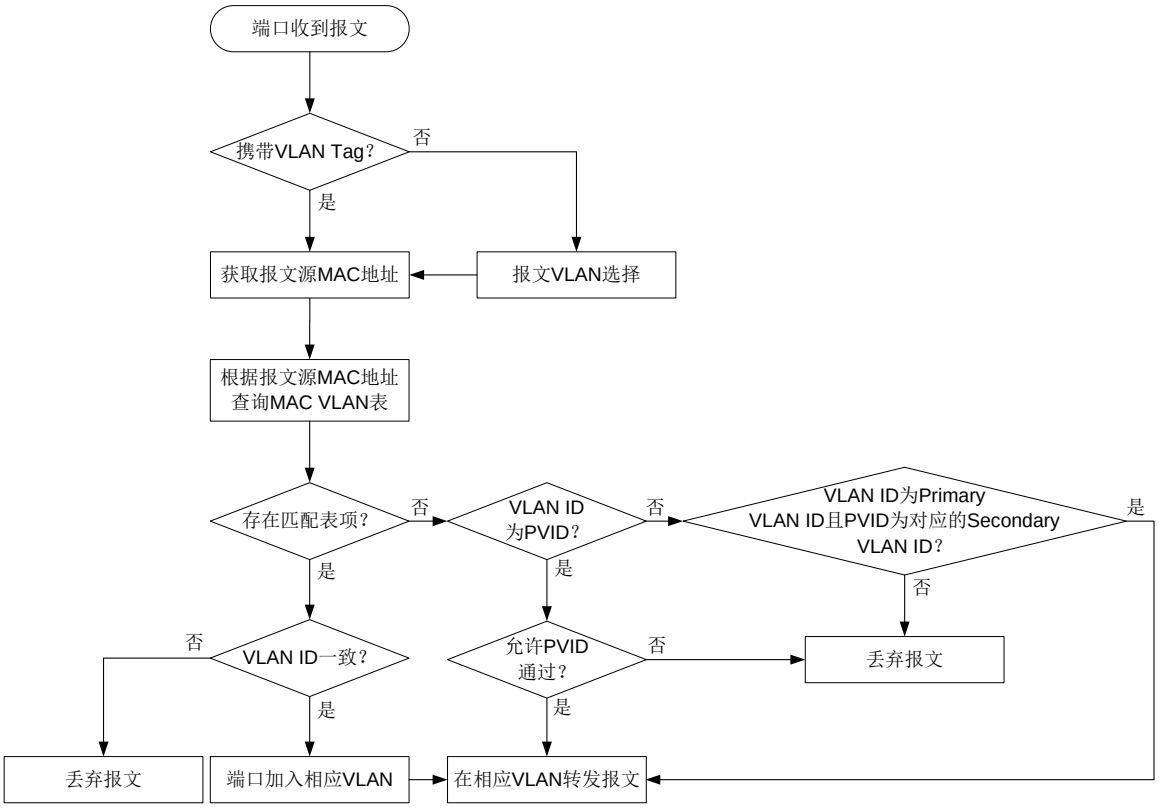
2. 动态触发端口加入静态 MAC VLAN

手动配置静态 MAC VLAN 时，如果不能确定从哪些端口收到指定 VLAN 的报文，就不能把相应端口加入到 MAC VLAN。采用动态触发方式可以将端口自动加入静态 MAC VLAN。在该方式下，配置 MAC VLAN 表项后，需要在端口上开启基于 MAC 的 VLAN 功能和 MAC VLAN 的动态触发功能，不需要手动把端口加入 MAC VLAN。

配置动态触发端口加入静态 MAC VLAN 后，端口在收到报文时，首先判断报文是否携带 VLAN Tag，若带 VLAN Tag，则直接获取报文源 MAC 地址；若不带 VLAN Tag，则先进行报文 VLAN 选择（按照基于 MAC 的 VLAN->基于 IP 子网的 VLAN->基于协议的 VLAN->基于端口的 VLAN 的优先次序为该 Untagged 报文添加对应的 VLAN Tag，并获取该 VLAN Tag），再获取报文源 MAC 地址，然后根据报文的源 MAC 地址和 VLAN 查询静态 MAC VLAN 表项：

- 如果报文源 MAC 地址与 MAC VLAN 表项中的 MAC 地址精确匹配，再检查报文的 VLAN ID 是否与对应表项中的 VLAN ID 一致。若一致，通过该报文动态触发端口加入相应 VLAN，同时转发该报文；否则丢弃该报文。
- 如果报文源 MAC 地址与 MAC VLAN 表项的 MAC 地址不精确匹配，当报文 VLAN ID 为 PVID（Port VLAN ID，端口缺省 VLAN），判断端口是否允许报文在 PVID 内转发。若允许，则在 PVID 中转发该报文，否则丢弃该报文。当报文 VLAN ID 不为 PVID，判断是否报文 VLAN ID 为 Primary VLAN ID 且 PVID 为对应的 Secondary VLAN ID。若是，则转发该报文；否则丢弃该报文。处理流程如图 1 所示：

图1 动态触发端口加入静态 MAC VLAN 的处理流程



2.1.2 动态 MAC VLAN

动态 MAC VLAN 是由接入认证过程来动态决定接入用户报文所属的 VLAN。该方式下，需要在设备上同时配置 MAC VLAN 和基于 MAC 的接入认证方式（比如 MAC 地址认证或者基于 MAC 的 802.1X 认证）。如果用户发起认证请求，认证服务器会对认证用户名和密码进行验证，如果通过，则会下发 VLAN 信息。此时设备就可根据认证请求报文的源 MAC 地址和下发的 VLAN 信息生成 MAC VLAN 表项，并自动将 MAC VLAN 添加到端口允许通过的 untagged VLAN 列表中。用户下线后，设备又自动删除 MAC VLAN 表项，并将 MAC VLAN 从端口允许通过的 VLAN 列表中删除。该方式的优点是灵活、安全：

- 它能够自动识别 MAC 地址、能够自动创建 MAC VLAN 表项、能够自动允许 MAC VLAN 通过接入端口。因此该方式应用于大型网络时能够大大简化配置，使用灵活。
- 只有用户接入认证成功，才能通过指定的 VLAN 接入网络，因此提高了网络的安全性。

2.2 应用限制

- MAC VLAN 只对 Hybrid 端口配置有效，所以在开启 MAC VLAN 前，请将端口的链路类型配置为 Hybrid。

- MAC VLAN 有静态配置和动态配置两种方式，但是同一 MAC 地址只能绑定一个 VLAN。因此，如果已进行了静态配置，而动态下发的绑定关系与静态配置不一致，则动态下发失败，用户不能通过认证；反之，如果动态下发已生效，而静态配置与动态下发的不一致，则静态配置失败。
- 采用动态方式配置 MAC VLAN 时需要基于 MAC 地址的 AAA 远程认证的配合，网络中需要部署 AAA 认证服务器，服务器必须能够下发 VLAN。
- MAC VLAN 的配置会影响聚合成员端口的选中状态。所以，建议不要在聚合成员端口上配置 MAC VLAN 功能。
- Super VLAN 不能作为 MAC VLAN 表项中的 VLAN。

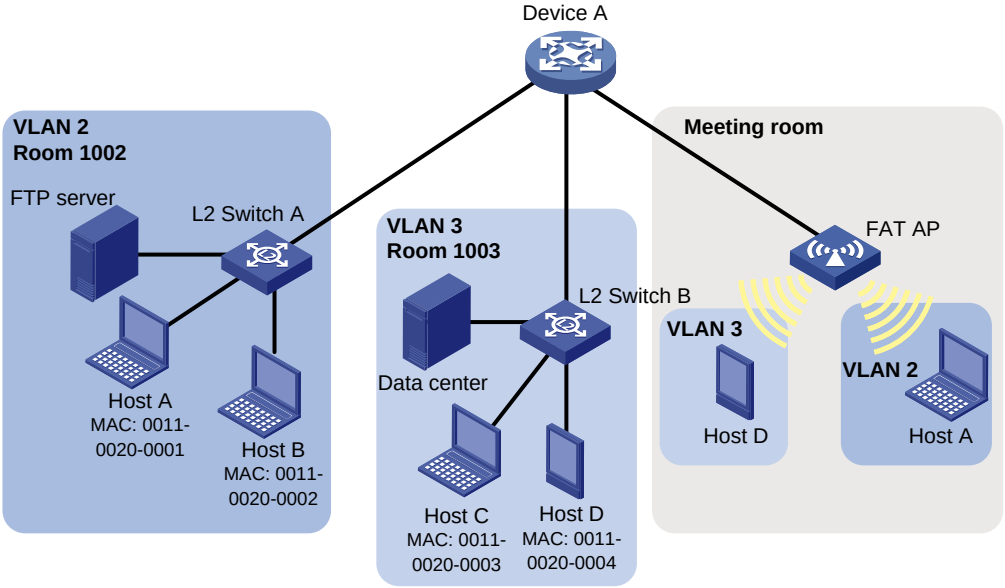
3 典型组网应用

3.1 静态配置MAC VLAN

某公司为了实现通信安全以及隔离广播报文，给不同的部门指定了不同的 VLAN。销售部的办公区在 1002 房间，部门所有资产属于 VLAN 2；技术支持部门的办公区在 1003 房间，部门所有资产属于 VLAN 3。因为人员的流动性很大，公司在 Meeting room 里提供了临时办公场所，职员可以通过无线接入公司网络，但要求接入后只能划分到自己部门所在的 VLAN，比如 Host A 到 Meeting room 办公后必须归属于 VLAN 2，Host D 到 Meeting room 办公后必须归属于 VLAN 3。

基于以上需求，在 1002 房间和 1003 房间因为人员和工位比较稳定，可以采用基于端口的方式划分 VLAN。但是在 Meeting room 里，因为人员流动性比较大，人员接入网络的端口不确定，所以可以通过 MAC VLAN，将 MAC 地址和员工所在部门的 VLAN 绑定。从而不管员工从哪个接口接入，不需要修改配置，就能被划分到部门所在的 VLAN。

图2 静态配置 MAC VLAN 组网图



3.2 动态配置MAC VLAN

用户通过无线接入点 AP 1 和 AP n 接入网络，在 AP 1 和 AP n 上同时使能 MAC VLAN 和基于 MAC 的 802.1X 方式认证，就能很简便地实现：

- 用户接入前需先通过认证，从而防止非法用户占用网络资源；
- 用户通过任意 AP 的任意端口接入网络，仍能属于原来的 VLAN。

图3 动态配置 MAC VLAN 组网图