

目 录

MAC地址认证 ..... 1

    MAC地址认证简介 ..... 1

        RADIUS服务器认证方式进行MAC地址认证 ..... 1

        本地认证方式进行MAC地址认证 ..... 1

    相关概念..... 2

        MAC地址认证定时器 ..... 2

        静默MAC ..... 2

        下发VLAN..... 2

        下发ACL ..... 2

        MAC地址认证的Guest VLAN ..... 3

# MAC 地址认证

## MAC 地址认证简介

MAC 地址认证是一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法，它不需要用户安装任何客户端软件。设备在首次检测到用户的 MAC 地址以后，即启动对该用户的认证操作。认证过程中，也不需要用户手动输入用户名或者密码。

目前设备支持两种方式的 MAC 地址认证：

- 通过 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器认证。
- 本地认证。

认证方式确定后，可根据需求选择 MAC 认证用户名的类型，包括以下两种方式：

- MAC 地址用户名：使用用户的 MAC 地址作为认证时的用户名和密码；
- 固定用户名：不论用户的 MAC 地址为何值，所有用户均使用在设备上预先配置的本地用户名和密码进行认证。

## RADIUS 服务器认证方式进行 MAC 地址认证

当选用 RADIUS 服务器认证方式进行 MAC 地址认证时，设备作为 RADIUS 客户端，与 RADIUS 服务器配合完成 MAC 地址认证操作：

- 采用 MAC 地址用户名时，设备将检测到的用户 MAC 地址作为用户名和密码发送给 RADIUS 服务器。
- 采用固定用户名时，设备将已经在本地配置的用户名和密码作为待认证用户的用户名和密码，发送给 RADIUS 服务器。

RADIUS 服务器完成对该用户的认证后，认证通过的用户可以访问网络。

## 本地认证方式进行 MAC 地址认证

当选用本地认证方式进行 MAC 地址认证时，直接在设备上完成对用户的认证。需要在设备上配置本地用户名和密码：

- 采用 MAC 地址用户名时，需要配置的本地用户名为各接入用户的 MAC 地址。
- 采用固定用户名时，需要配置的本地用户名为自定义的，所有用户对应的用户名和密码与自定义的一致。

## 相关概念

### MAC 地址认证定时器

MAC 地址认证过程受以下定时器的控制：

- 下线检测定时器：用来设置设备用户空闲超时的时间间隔。如果在两个时间间隔之内，没有来自用户的流量通过，设备将切断用户的连接，同时通知 RADIUS 服务器，停止对该用户的计费。
- 静默定时器：用来设置用户认证失败以后，设备需要等待的时间间隔。在静默期间，设备不处理该用户的认证功能，静默之后设备再重新对用户发起认证。
- 服务器超时定时器：用来设置设备同 RADIUS 服务器的连接超时时间。在用户的认证过程中，如果服务器超时定时器超时，设备将在相应的端口上禁止此用户访问网络。

### 静默 MAC

当一个 MAC 地址认证失败后，此 MAC 就被添加为静默 MAC，在静默时间内，来自此 MAC 地址的数据报文到达时，设备直接做丢弃处理。静默 MAC 的功能主要是防止非法 MAC 短时间内的重复认证。



注意：

若配置的静态 MAC 或者当前认证通过的 MAC 地址与静默 MAC 相同，则此 MAC 地址的静默功能失效。

### 下发 VLAN

为了将受限的网络资源与用户隔离，通常将受限的网络资源和用户划分到不同的 VLAN。当用户通过身份认证后，受限的网络资源所在的 VLAN 会作为授权 VLAN 从授权服务器上下发。同时用户所在的端口被加入到此授权 VLAN 中，用户可以访问这些受限的网络资源。

### 下发 ACL

从授权服务器下发的 ACL 被称为授权 ACL，它为用户访问网络提供了良好的过滤条件设置功能。当用户上线时，如果 RADIUS 服务器上配置了授权 ACL，则设备会根据服务器下发的授权 ACL 对用户所在端口的数据流进行控制。而且在用户访问网络的过程中，可以通过改变服务器的授权 ACL 设置来改变用户的访问权限。

## MAC 地址认证的 Guest VLAN

**Guest VLAN** 功能允许用户在未认证或者认证失败的情况下，可以访问某一特定 VLAN 中的资源，比如获取客户端软件，升级客户端或执行其他一些用户升级程序。这个 VLAN 称之为 **Guest VLAN**。

MAC 地址认证支持基于 MAC 的 **Guest VLAN**（**MAC-based Guest VLAN**），简称 **MGV**。如果接入用户的端口上配置了 **MGV**，则该端口上认证失败的用户会被加入 **Guest VLAN**，即该用户被授权访问 **Guest VLAN** 里的资源。

若 **Guest VLAN** 中的用户再次发起认证未成功，则该用户将仍然处于 **Guest VLAN** 内；若认证成功，则会根据认证服务器是否下发 **VLAN** 将用户加入到下发的 **VLAN** 中，或回到加入 **Guest VLAN** 之前端口所在的 **VLAN**。