目 录

1 MAC地址认证

1.1 MAC地址认证简介

1.1.1 MAC地址认证概述

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。设备在启动了 MAC 地址认证的端口上首次检测到用户的 MAC 地址以后，即启动对该用户的认证操作。认证过程中，不需要用户手动输入用户名或者密码。若该用户认证成功，则允许其通过端口访问网络资源，否则该用户的 MAC 地址就被设置为静默 MAC。在静默时间内（可通过静默定时器配置），来自此 MAC 地址的用户报文到达时，设备直接做丢弃处理，以防止非法 MAC 短时间内的重复认证。

说明

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 MAC 地址认证失败后的 MAC 静默功能将会失效。

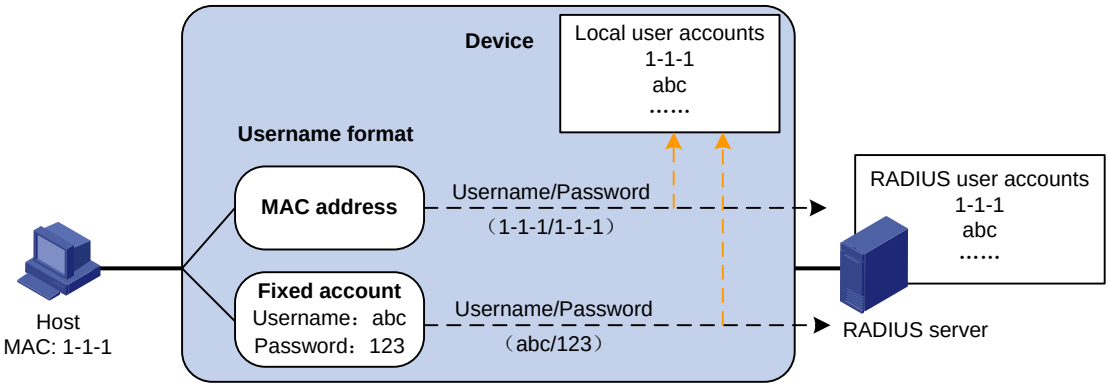
1.1.2 使用不同用户名格式的MAC地址认证

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）服务器进行远程认证和在接入设备上进行本地认证。有关远程 RADIUS 认证和本地认证的详细介绍请参见“安全配置指导”中的“AAA”。

根据设备最终用于验证用户身份的用户名格式和内容的不同，可以将 MAC 地址认证使用的用户帐户格式分为两种类型：

- MAC 地址用户名格式：使用用户的 MAC 地址作为认证时的用户名和密码。
- 固定用户名格式：不论用户的 MAC 地址为何值，所有用户均使用设备上指定的一个固定用户名和密码替代用户的 MAC 地址作为身份信息进行认证。由于同一个端口下可以有多个用户进行认证，因此这种情况下端口上的所有 MAC 地址认证用户均使用同一个固定用户名进行认证，服务器端仅需要配置一个用户帐户即可满足所有认证用户的认证需求，适用于接入客户端比较可信的网络环境。

图1-1 不同用户名格式下的 MAC 地址认证示意图



1. 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：

- 若采用 MAC 地址用户名格式，则设备将检测到的用户 MAC 地址作为用户名和密码发送给 RADIUS 服务器进行验证。
- 若采用固定用户名格式，则设备将一个已经在本地指定的 MAC 地址认证用户使用的固定用户名和对应的密码作为待认证用户的用户名和密码，发送给 RADIUS 服务器进行验证。

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。

2. 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：

- 若采用 MAC 地址用户名格式，则设备将检测到的用户 MAC 地址作为待认证用户的用户名和密码与配置的本地用户名和密码进行匹配。
- 若采用固定用户名，则设备将一个已经在本地指定的 MAC 地址认证用户使用的固定用户名和对应的密码作为待认证用户的用户名和密码与配置的本地用户名和密码进行匹配。

用户名和密码匹配成功后，用户可以访问网络。

1.2 MAC地址认证支持VLAN下发

1.2.1 授权VLAN

为了将受限的网络资源与未认证用户隔离，通常将受限的网络资源和未认证的用户划分到不同的 VLAN。MAC 地址认证支持远程 AAA 服务器/接入设备下发授权 VLAN，即当用户通过 MAC 地址认证后，远程 AAA 服务器/接入设备将指定的受限网络资源所在的 VLAN 作为授权 VLAN 下发到用户进行认证的端口。该端口被加入到授权 VLAN 中后，用户便可以访问这些受限的网络资源。

1. 远程AAA授权

该方式下，需要在 AAA 服务器上指定下发给用户的授权 VLAN 信息，下发的授权 VLAN 信息可以有多种形式，包括数字型 VLAN 和字符型 VLAN，字符型 VLAN 又可分为 VLAN 名称、携带后缀的 VLAN ID（后缀只能为字母 u 或 t，用于标识是否携带 Tag）。

设备收到服务器的授权 VLAN 信息后，首先对其进行解析，只要解析成功，即以对应的方法下发授权 VLAN；如果解析不成功，则用户授权失败。

- 若认证服务器下发的授权 VLAN 信息为一个 VLAN ID 或一个 VLAN 名称，则仅当对应的 VLAN 不为动态学习到的 VLAN、保留 VLAN 和 Super VLAN 时，该 VLAN 才是有效的授权 VLAN。
- 若认证服务器下发的授权 VLAN 信息为一个包含若干个“VLAN ID+后缀”形式的字符串，则只有第一个不携带后缀或者携带 untagged 后缀的 VLAN 将被解析为唯一的 untagged 的授权 VLAN，其余 VLAN 都被解析为 tagged 的授权 VLAN。例如服务器下发字符串“1u 2t 3”，其中的 u 和 t 均为后缀，分别表示 untagged 和 tagged。该字符串被解析之后，VLAN 1 为 untagged 的授权 VLAN，VLAN 2 和 VLAN 3 为 tagged 的授权 VLAN。该方式下发的授权 VLAN 仅对端口链路类型为 Hybrid 或 Trunk 的端口有效。
  - 端口的缺省 VLAN 将被修改为 untagged 的授权 VLAN。若不存在 untagged 的授权 VLAN，则不修改端口的缺省 VLAN。
  - 端口将允许所有解析成功的授权 VLAN 通过。

2. 本地AAA授权

该方式下，可以通过配置本地用户的授权属性指定下发给用户的授权 VLAN 信息，且只能指定一个授权 VLAN。设备将此 VLAN 作为该本地用户的授权 VLAN。关于本地用户的相关配置，请参见“安全配置指导”中的“AAA”。

3. 不同类型的端口加入授权VLAN

设备根据用户接入的端口链路类型和授权的 VLAN 是否携带 Tag，按如下情况将端口加入到下发的授权 VLAN 中。需要注意的是，仅远程 AAA 服务器支持授权携带 Tag 的 VLAN。

授权 VLAN 未携带 Tag 的情况下：

- 若用户从 Access 类型的端口接入，则端口离开当前 VLAN 并加入第一个通过认证的用户的授权 VLAN 中。
- 若用户从 Trunk 类型的端口接入，则设备允许下发的授权 VLAN 通过该端口，并且修改该端口的缺省 VLAN 为第一个通过认证的用户的授权 VLAN。
- 若用户从 Hybrid 类型的端口接入，则设备允许授权下发的授权 VLAN 以不携带 Tag 的方式通过该端口，并且修改该端口的缺省 VLAN 为第一个通过认证的用户的授权 VLAN。需要注意的是，若该端口上使能了 MAC VLAN 功能，则设备将根据认证服务器/接入设备下发的授权 VLAN 动态地创建基于用户 MAC 地址的 VLAN，而端口的缺省 VLAN 并不改变。

授权 VLAN 携带 Tag 的情况下：

- 若用户从 Access 类型的端口接入，则不支持下发带 Tag 的 VLAN。
- 若用户从 Trunk 类型的端口接入，则设备允许授权下发的 VLAN 以携带 Tag 的方式通过该端口，但是不会修改该端口的缺省 VLAN。
- 若用户从 Hybrid 类型的端口接入，则设备允许授权下发的 VLAN 以携带 Tag 的方式通过该端口，但是不会修改该端口的缺省 VLAN。

说明

- 在授权 VLAN 未携带 Tag 的情况下，只有开启了 MAC VLAN 功能的端口上才允许给不同的用户 MAC 授权不同的 VLAN。如果没有开启 MAC VLAN 功能，授权给所有用户的 VLAN 必须相同，否则仅第一个通过认证的用户可以成功上线。
- 在授权 VLAN 携带 Tag 的情况下，无论是否开启了 MAC VLAN 功能，设备都会给不同的用户授权不同的 VLAN。

1.2.2 MAC地址认证Guest VLAN

MAC 地址认证的 Guest VLAN 功能允许用户在认证失败的情况下访问某一特定 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。需要注意的是，这里的认证失败是认证服务器因某种原因明确拒绝用户认证通过，比如用户密码错误，而不是认证超时或网络连接等原因造成的认证失败。

如果接入用户的端口上配置了 Guest VLAN，则该端口上认证失败的用户会被加入 Guest VLAN，且设备允许 Guest VLAN 以不携带 Tag 的方式通过该端口，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 AAA 服务器/接入设备是否下发授权 VLAN 决定是否将用户加入到下发的授权 VLAN 中，在 AAA 服务器/接入设备未下发授权 VLAN 的情况下，用户回到缺省 VLAN 中。

1.2.3 MAC地址认证Critical VLAN

MAC 地址认证 Critical VLAN 功能允许用户在所有认证服务器都不可达的情况下访问某一特定 VLAN 中的资源，这个 VLAN 称之为 Critical VLAN。在端口上配置 Critical VLAN 后，若该端口上有用户认证时，所有认证服务器都不可达，则端口将允许 Critical VLAN 通过，用户将被授权访问 Critical VLAN 里的资源。已经加入 Critical VLAN 的端口上有用户发起认证时，如果所有认证服务器不可达，则端口仍然在 Critical VLAN 内；如果服务器可达且认证失败，且端口配置了 Guest VLAN，则该端口将会加入 Guest VLAN，否则回到缺省 VLAN 中；如果服务器可达且认证成功，则会根据 AAA 服务器是否下发授权 VLAN 决定是否将用户加入到下发的授权 VLAN 中，在 AAA 服务器未下发授权 VLAN 的情况下，用户回到缺省 VLAN 中。

1.2.4 MAC地址认证Critical Voice Vlan

MAC 地址认证的 Critical Voice VLAN 功能允许语音用户进行 MAC 地址认证时，若采用的 ISP 域中的所有认证服务器都不可达，则访问端口上已配置的 Voice VLAN 中的资源，这个 VLAN 也被称为 MAC 地址认证的 Critical Voice VLAN。已经加入 Critical Voice VLAN 的端口上有用户发起认证时，如果所有认证服务器不可达，则端口仍然在 Critical Voice VLAN 内；如果服务器可达且认证失败，且端口配置了 Guest VLAN，则该端口将会加入 Guest VLAN，否则回到缺省 VLAN 中；如果服务器可达且认证成功，则会根据 AAA 服务器是否下发授权 VLAN 决定是否将用户加入到下发的授权 VLAN 中，在 AAA 服务器未下发授权 VLAN 的情况下，用户回到缺省 VLAN 中。

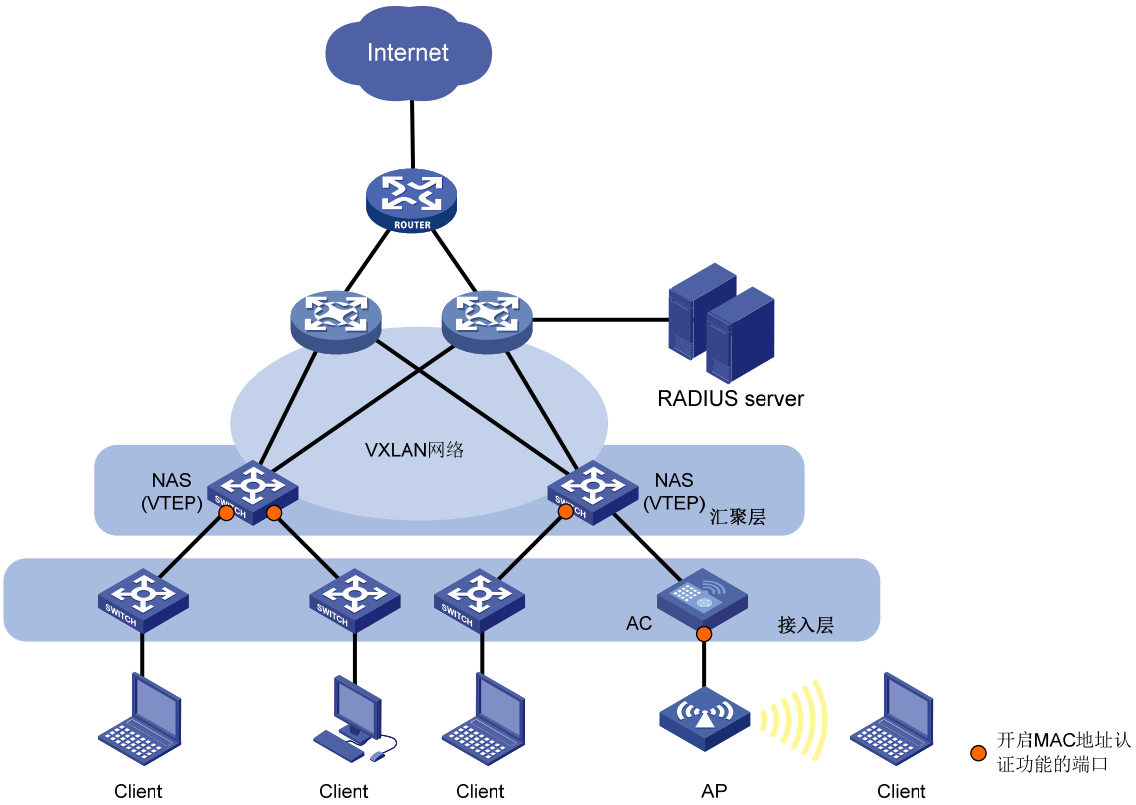
1.3 MAC地址认证支持VSI下发

1.3.1 MAC地址认证支持VXLAN

如 图 1-2 所示，在VXLAN网络中，VTEP设备作为用户的接入认证设备时，用户所在VLAN往往不能标识其业务信息，此时需要在服务器上配置为MAC地址认证成功用户下发授权VSI。NAS会根据用户的MAC地址、所属VLAN和接入端口把用户流量映射到对应的VXLAN中，实现不同的MAC地址认证用户可以访问不同的网络资源。

有关 VSI 和 VXLAN 的详细介绍请参见“VXLAN 配置指导”中的“VXLAN 简介”。

图1-2 MAC 地址认证支持 VXLAN 组网示意图



1.3.2 授权VSI

为了将受限的网络资源与未认证用户隔离，通常将受限的网络资源放置在未认证的用户不可访问的 VXLAN 中，该 VXLAN 所在的 VSI 称为授权 VSI。MAC 地址认证支持远程 AAA 服务器下发授权 VSI，即当通过 MAC 地址认证后，若服务器为用户配置了授权 VSI，则设备根据用户的接入端口、所在 VLAN 以及 MAC 地址动态创建 AC，并将该 AC 与服务器授权的 VSI 相关联。此后通过该端口接入的，指定 VLAN 和 MAC 地址的用户便可以访问这些受限的网络资源；若服务器未为用户配置授权 VSI，则用户不能访问任何 VXLAN 中的资源。有关动态创建 AC 的详细介绍，请参见“VXLAN 配置指导”中的“配置 VXLAN”。

1.3.3 MAC地址认证Guest VSI

MAC 地址认证的 Guest VSI 功能允许用户在认证失败的情况下访问某一特定 VXLAN 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 VXLAN 所在的 VSI 称之为 Guest VSI。需要注意的是，这里的认证失败是认证服务器因某种原因明确拒绝用户认证通过，比如用户密码错误，而不是认证超时或网络连接等原因造成的认证失败。

如果接入用户的端口上配置了 Guest VSI，则该端口上认证失败的用户会被加入 Guest VSI。若 Guest VSI 中的用户再次发起认证未成功，则该用户将仍然处于 Guest VSI 内；若认证成功，则用户会离开 Guest VSI，根据 AAA 服务器是否下发授权 VSI 决定是否将用户加入到下发的授权 VSI 中。

1.3.4 MAC地址认证Critical VSI

MAC 地址认证 Critical VSI 功能允许用户在所有认证服务器都不可达的情况下访问某一特定 VXLAN 中的资源，这个 VXLAN 所在的 VSI 称之为 Critical VSI。在端口上配置 Critical VSI 后，若该端口上有用户认证时，所有认证服务器都不可达，则用户会被加入 Critical VSI 中。Critical VSI 中的用户再次发起认证时，如果所有认证服务器仍不可达，则用户仍然在 Critical VSI 内；如果服务器可达且认证失败，且端口配置了 Guest VSI，则该用户将会加入 Guest VSI；如果服务器可达且认证成功，则用户离开 Critical VSI，根据 AAA 服务器是否下发授权 VSI 决定是否将用户加入到下发的授权 VSI 中。

1.4 MAC地址认证支持ACL下发

由远程 AAA 服务器/接入设备下发给用户的 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。当用户通过 MAC 地址认证后，如果远程 AAA 服务器/接入设备上为用户指定了授权 ACL，则设备会根据下发的授权 ACL 对用户所在端口的数据流进行控制，仅禁止 ACL 规则中 deny 的数据流通过该端口。为使下发的授权 ACL 生效，需要提前在设备上配置相应的 ACL 规则。而且在用户访问网络的过程中，可以通过改变远程 AAA 服务器/设备本地的授权 ACL 设置来改变用户的访问权限。需要注意的是，MAC 地址认证可成功授权的 ACL 类型为基本 ACL（ACL 编号为 2000～2999）和高级 ACL（ACL 编号为 3000～3999）。

1.5 MAC地址认证支持下发User Profile

从认证服务器（远程或本地）下发的 User Profile 被称为授权 User Profile，它为用户访问网络提供了良好的过滤条件设置功能。MAC 地址认证支持认证服务器授权下发 User Profile 功能，即当用户通过 MAC 地址认证后，如果认证服务器上配置了授权 User Profile，则设备会根据服务器下发的授权 User Profile 对用户所在端口的数据流进行控制。为使下发的授权 User Profile 生效，需要提前在设备上配置相应的 User Profile。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 User Profile 名称或者设备对应的 User Profile 配置来改变用户的访问权限。

1.6 MAC地址认证支持URL重定向功能

当用户进行 MAC 地址认证时，可以根据 RADIUS 服务器下发的重定向 URL 属性到指定的 Web 认证界面进行认证。Web 认证通过后，RADIUS 服务器记录用户的 MAC 地址信息，并通过 DM 报文

强制 Web 用户下线。此后该用户再次进行 MAC 地址认证，由于 RADIUS 服务器上已记录该用户和其 MAC 地址的对应信息，用户可以成功上线。

1.7 MAC地址认证配置限制和指导

- 如果服务器同时下发了授权 VSI 和授权 VLAN，设备以授权 VLAN 为准。
- 端口上配置 MAC 地址认证的 Guest VLAN、Critical VLAN 与配置 MAC 地址认证的 Guest VSI、Critical VSI 互斥。
- 为使 MAC 地址认证支持 VLAN 下发或 VSI 下发功能的正常应用，请保证设备和服务器配置的一致性：若设备上配置了 Guest VLAN 或 Critical VLAN，则需要在服务器上配置为 MAC 地址认证用户授权 VLAN；若设备上配置了 Guest VSI 或 Critical VSI，则需要在服务器配置为 MAC 地址认证用户授权 VSI。
- 支持配置 MAC 地址认证功能的端口为二层以太网接口。
- 在二层以太网接口视图下开启 MAC 地址认证之前，请保证接口未加入二层聚合组。

1.8 MAC地址认证配置任务简介

表1-1 MAC 地址认证配置任务简介

配置任务	说明	详细配置
开启MAC地址认证	必选	1.9
配置MAC地址认证用户使用的认证域	可选	1.10
配置MAC地址认证用户名格式	可选	1.11
配置MAC地址认证定时器	可选	1.12
配置端口上最多允许同时接入的MAC地址认证用户数	可选	1.13
配置端口工作在MAC地址认证的多VLAN模式	可选	1.14
配置MAC地址认证延迟功能	可选	1.15
配置端口MAC地址认证和802.1X认证并行处理功能	可选	1.16
配置MAC地址认证的Guest VLAN	可选	1.17
配置MAC地址认证的Critical VLAN	可选	1.18
配置MAC地址认证的Critical Voice VLAN	可选	1.19
配置MAC地址认证Guest VSI	可选	1.20
配置MAC地址认证Critical VSI	可选	1.21
配置MAC地址认证的重认证	可选	1.22
配置MAC地址认证请求中携带用户IP地址	可选	1.23
配置MAC地址认证Guest VLAN中的用户进行重新认证的时间间隔	可选	1.24
配置MAC地址认证Guest VSI中的用户进行重新认证的时间间隔	可选	1.25
开启端口的MAC地址认证下线检测功能	可选	1.26

1.9 开启MAC地址认证

1. 配置准备

(1) 缺省情况下，对端口上接入的用户进行MAC地址认证时，使用系统缺省的认证域（由命令**domain default enable**指定）。若需要使用非缺省的认证域进行MAC地址认证，则需指定MAC地址认证用户使用的认证域（参见“1.10 指定MAC地址认证用户使用的认证域”），并配置该认证域。认证域的具体配置请参见“安全配置指导”中的“AAA”。

- 若采用本地认证方式，还需创建本地用户并设置其密码，且本地用户的服务类型应设置为**lan-access**。
- 若采用远程 RADIUS 认证方式，需要确保设备与 RADIUS 服务器之间的路由可达，并添加 MAC 地址认证用户帐号。

(2) 保证端口安全功能关闭。具体配置请参见“安全配置指导”中的“端口安全”。

2. 配置步骤

只有全局和端口的 MAC 地址认证均开启后，MAC 地址认证配置才能在端口上生效。

表1-2 开启 MAC 地址认证

操作	命令	说明
进入系统视图	**system-view**	-
开启全局MAC地址认证	**mac-authentication**	缺省情况下，全局的MAC地址认证处于关闭状态
进入接口视图	**interface** *interface-type interface-number*	-
开启端口MAC地址认证	**mac-authentication**	缺省情况下，端口的MAC地址认证处于关闭状态

1.10 指定MAC地址认证用户使用的认证域

为了便于接入设备的管理员更为灵活地部署用户的接入策略，设备支持指定 MAC 地址认证用户使用的认证域，可以通过以下两种配置实现：

- 在系统视图下指定一个认证域，该认证域对所有开启了 MAC 地址认证的端口生效。
- 在接口视图下指定该端口的认证域，不同的端口可以指定不同的认证域。

端口上接入的 MAC 地址认证用户将按照如下顺序选择认证域：端口上指定的认证域 > 系统视图下指定的认证域 > 系统缺省的认证域。关于认证域的相关介绍请参见“安全配置指导”中的“AAA”。

表1-3 指定 MAC 地址认证用户使用的认证域

配置步骤	命令	说明
进入系统视图	**system-view**	-
指定MAC地址认证用户使用	**mac-authentication domain** *domain-name*	二者至少选其一

配置步骤	命令	说明
的认证域	**interface** *interface-type interface-number* **mac-authentication domain** *domain-name*	缺省情况下，未指定MAC地址认证用户使用的认证域，使用系统缺省的认证域

1.11 配置MAC地址认证用户名格式

表1-4 配置 MAC 地址认证用户名格式

操作		命令	说明
进入系统视图		**system-view**	-
配置MAC地址认证用户的用户名格式	MAC地址格式	**mac-authentication user-name-format mac-address** [{ **with-hyphen** | **without-hyphen** } [**lowercase** | **uppercase**]]	二者选其一 缺省情况下，使用用户的MAC地址作为用户名与密码，其中字母为小写，且不带连字符“-”
	固定用户名格式	**mac-authentication user-name-format fixed** [**account** *name*] [**password** { **cipher** | **simple** } *string*]	

1.12 配置MAC地址认证定时器

可配置的 MAC 地址认证定时器包括以下几种：

- 下线检测定时器（**offline-detect**）：用来设置用户空闲超时的时间间隔。若设备在一个下线检测定时器间隔之内，没有收到某在线用户的报文，将切断该用户的连接，同时通知 RADIUS 服务器停止对其计费。配置 **offline-detect** 时，需要将 MAC 地址老化时间配成相同时间，否则会导致用户异常下线。
- 静默定时器（**quiet**）：用来设置用户认证失败以后，设备停止对其提供认证服务的时间间隔。在静默期间，设备不对来自认证失败用户的报文进行认证处理，直接丢弃。静默期后，如果设备再次收到该用户的报文，则依然可以对其进行认证处理。
- 服务器超时定时器（**server-timeout**）：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，如果到服务器超时定时器超时时设备一直没有收到 RADIUS 服务器的应答，则设备将在相应的端口上禁止此用户访问网络。

表1-5 配置 MAC 地址认证定时器

操作	命令	说明
进入系统视图	**system-view**	-
配置MAC地址认证定时器	**mac-authentication timer** { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **server-timeout** *server-timeout-value* }	缺省情况下，下线检测定时器为300秒，静默定时器为60秒，服务器超时定时器取值为100秒

1.13 配置端口上最多允许同时接入的MAC地址认证用户数

由于系统资源有限，如果当前端口下接入的用户过多，接入用户之间会发生资源的争用，因此适当地配置该值可以使端口上已经接入的用户获得可靠的性能保障。

表1-6 配置端口上最多允许同时接入的 MAC 地址认证用户数

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置端口上最多允许同时接入的MAC地址认证用户数	**mac-authentication max-user** *max-number*	缺省情况下，端口上最多允许同时接入的MAC地址认证用户数为4294967295

1.14 配置端口工作在MAC地址认证的多VLAN模式

端口工作在单 VLAN 模式下时，在用户已上线，且没有被下发授权 VLAN 情况下，如果此用户在属于不同 VLAN 的相同端口再次接入，则，设备将让原用户下线，使得该用户能够在新的 VLAN 内重新开始认证。如果已上线用户被下发了授权 VLAN，则此用户在属于不同 VLAN 的相同端口再次接入时不会被强制下线。

端口工作在多 VLAN 模式下时，如果相同 MAC 地址的用户在属于不同 VLAN 的相同端口再次接入，设备将能够允许用户的流量在新的 VLAN 内通过，且允许该用户的报文无需重新认证而在多个 VLAN 中转发。

对于接入 IP 电话类用户的端口，指定端口工作在 MAC 地址认证的多 VLAN 模式或为 IP 电话类用户授权 VLAN，可避免 IP 电话终端的报文所携带的 VLAN tag 发生变化后，因用户流量需要重新认证带来语音报文传输质量受干扰的问题。

表1-7 配置端口工作在 MAC 地址认证的多 VLAN 模式

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置端口工作在MAC地址认证的多VLAN模式	**mac-authentication host-mode multi-vlan**	缺省情况下，端口工作在MAC地址认证的单VLAN模式

1.15 配置MAC地址认证延迟功能

端口同时开启了 MAC 地址认证和 802.1X 认证的情况下，某些组网环境中希望设备对用户报文先进行 802.1X 认证。例如，有些客户端在发送 802.1X 认证请求报文之前，就已经向设备发送了其它报文，比如 DHCP 报文，因而触发了并不期望的 MAC 地址认证。这种情况下，就可以开启端口的 MAC 地址认证延时功能。

开启端口的 MAC 地址认证延时功能之后，端口就不会在收到用户报文时立即触发 MAC 地址认证，而是会等待一定的延迟时间，若在此期间该用户一直未进行 802.1X 认证或未成功通过 802.1X 认证，则延迟时间超时后端口会对之前收到的用户报文进行 MAC 地址认证。

需要注意的是，开启了 MAC 地址认证延迟功能的端口上不建议同时配置端口安全的模式为 **mac-else-userlogin-secure** 或 **mac-else-userlogin-secure-ext**，否则 MAC 地址认证延迟功能不生效。端口安全模式的具体配置请参见“安全配置指导”中的“端口安全”。

表1-8 配置 MAC 地址认证延迟功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
开启MAC地址认证延迟功能，并指定延迟时间	**mac-authentication timer auth-delay** *time*	缺省情况下，MAC地址认证延迟功能处于关闭状态

1.16 配置端口MAC地址认证和802.1X认证并行处理功能

端口采用802.1X和MAC地址组合认证，且端口所连接的用户有不能主动发送EAP报文触发802.1X认证的情况下，如果端口配置了 802.1X 单播触发功能，则端口收到源 MAC 地址未知的报文，会先进行 802.1X 认证处理，完成后再进行 MAC 地址认证处理。

配置端口的 MAC 地址认证和 802.1X 认证并行处理功能后，在上述情况下，端口收到源 MAC 地址未知的报文，会向该 MAC 地址单播发送 EAP-Request 帧来触发 802.1X 认证，但不等待 802.1X 认证处理完成，就同时进行 MAC 地址认证的处理。

在某些组网环境下，例如用户不希望端口先被加入 802.1X 的 Guest VLAN 中，接收到源 MAC 地址未知的报文后，先触发 MAC 地址认证，认证成功后端口直接加入 MAC 地址认证的授权 VLAN 中，那么需要配置 MAC 地址认证和 802.1X 认证并行处理功能和端口延迟加入 802.1X Guest VLAN 功能。关于端口延迟加入802.1X Guest VLAN 功能的详细介绍，请参见“安全配置指导”中的“802.1X”。

端口采用 802.1X 和 MAC 地址组合认证功能适用于如下情况：

- 端口上同时开启了 802.1X 和 MAC 地址认证功能，并配置了 802.1X 认证的端口的接入控制方式为 macbased。
- 开启了端口安全功能，并配置了端口安全模式为 userlogin-secure-or-mac 或 userlogin-secure-or-mac-ext。端口安全模式的具体配置请参见“安全命令参考”中的“端口安全”。

为保证 MAC 地址认证和 802.1X 认证并行处理功能的正常使用，不建议配置端口的 MAC 地址认证延迟功能，否则端口触发 802.1X 认证后，仍会等待一定的延迟后再进行 MAC 地址认证。

表1-9 配置端口的 MAC 地址认证和 802.1X 认证并行处理功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-

配置步骤	命令	说明
配置端口的MAC地址认证和802.1X认证并行处理功能	**mac-authentication parallel-with-dot1x**	缺省情况下，端口在收到源MAC地址未知的报文触发认证时，按照802.1X完成后再进行MAC地址认证的顺序进行处理

1.17 配置MAC地址认证的Guest VLAN

提示

- 端口上生成的 MAC 地址认证 Guest VLAN 表项会覆盖已生成的阻塞 MAC 表项。开启了端口安全入侵检测的端口关闭功能时，若端口因检测到非法报文被关闭，则 MAC 地址认证的 Guest VLAN 功能不生效。关于阻塞 MAC 表项和端口的入侵检测功能的具体介绍请参见“安全配置指导”中的“端口安全”。
- 如果某个 VLAN 被指定为 Super VLAN，则该 VLAN 不能被指定为某个端口的 MAC 地址认证的 Guest VLAN；同样，如果某个 VLAN 被指定为某个端口的 MAC 地址认证的 Guest VLAN，则该 VLAN 不能被指定为 Super VLAN。关于 Super VLAN 的详细内容请参见“二层技术-以太网交换配置指导”中的“Super VLAN”。

配置 MAC 地址认证的 Guest VLAN 之前，需要进行以下配置准备：

- 保证端口类型为 Hybrid，端口上的 MAC VLAN 功能处于使能状态，且不建议将指定的 Guest VLAN 修改为携带 Tag 的方式。
- 创建需要配置为 Guest VLAN 的 VLAN。

需要注意的是，MAC 地址认证 Guest VLAN 功能的优先级高于 MAC 地址认证的静默 MAC 功能，即认证失败的用户可访问指定的 Guest VLAN 中的资源，且该用户的 MAC 地址不会被加入静默 MAC。

表1-10 配置 MAC 地址认证的 Guest VLAN

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置端口的MAC地址认证Guest VLAN	**mac-authentication guest-vlan** *guest-vlan-id*	缺省情况下，未配置MAC地址认证的Guest VLAN 不同的端口可以指定不同的MAC地址认证 Guest VLAN，一个端口最多只能指定一个MAC地址认证 Guest VLAN

1.18 配置MAC地址认证的Critical VLAN

提示

- 端口上生成的 MAC 地址认证 Critical VLAN 表项会覆盖已生成的阻塞 MAC 表项。开启了端口安全入侵检测的端口关闭功能时，MAC 地址认证的 Critical VLAN 功能不生效。关于阻塞 MAC 表项和端口的入侵检测功能的具体介绍请参见“安全配置指导”中的“端口安全”。
- 如果某个 VLAN 被指定为 Super VLAN，则该 VLAN 不能被指定为某个端口的 MAC 地址认证的 Critical VLAN；同样，如果某个 VLAN 被指定为某个端口的 MAC 地址认证的 Critical VLAN，则该 VLAN 不能被指定为 Super VLAN。关于 Super VLAN 的详细内容请参见“二层技术-以太网交换配置指导”中的“Super VLAN”。

配置 MAC 地址认证的 Critical VLAN 之前，需要进行以下配置准备：

- 保证端口类型为Hybrid，端口上的MAC VLAN功能处于使能状态，且不建议将指定的Critical VLAN 修改为携带 Tag 的方式。
- 创建需要配置为 Critical VLAN 的 VLAN。

需要注意的是，当端口上的用户加入指定的 Critical VLAN 后，该用户的 MAC 地址不会被加入静默 MAC。

表1-11 配置 Critical VLAN

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置端口的Critical VLAN	**mac-authentication critical vlan** *critical-vlan-id*	缺省情况下，未配置MAC认证的Critical VLAN 不同的端口可以指定不同的MAC地址认证 Critical VLAN，一个端口最多只能指定一个MAC地址认证Critical VLAN

1.19 配置MAC地址认证的Critical Voice VLAN

1.19.1 配置准备

配置 MAC 地址认证 Critical Voice VLAN 之前，需要进行以下配置准备：

- 全局和端口的 LLDP（Link Layer Discovery Protocol，链路层发现协议）已经开启，设备通过 LLDP 来判断用户是否为语音用户。有关 LLDP 功能的详细介绍请参见“二层技术-以太网交换配置指导”中的“LLDP”。
- 端口的语音 VLAN 功能已经开启。有关语音 VLAN 的详细介绍请参见“二层技术-以太网交换配置指导”中的“VLAN”。

1.19.2 配置步骤

表1-12 配置 MAC 地址认证的 Critical Voice VLAN

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置端口的Critical Voice VLAN	**mac-authentication critical-voice-vlan**	缺省情况下，端口下MAC地址认证的Critical Voice VLAN功能处于关闭状态

1.20 配置MAC地址认证Guest VSI

1.20.1 配置限制和指导

- MAC 地址认证 Guest VSI 功能的优先级高于 MAC 地址认证的静默 MAC 功能，即 MAC 地址认证用户加入指定的 Guest VSI 后，该用户的 MAC 地址不会被加入静默 MAC。
- 不同的端口可以指定不同的 MAC 地址认证 Guest VSI，一个端口最多只能指定一个 MAC 地址认证 Guest VSI。

1.20.2 配置准备

配置 MAC 地址认证的 Guest VSI 之前，需要进行以下配置：

- 开启 L2VPN 功能。
- 创建配置为 Guest VSI 的 VSI，并在该 VSI 下创建 VXLAN。
- 端口下动态创建 AC 匹配 MAC 地址功能处于开启状态。

上述配置的详细介绍，请参见“VXLAN 配置指导”中的“配置 VXLAN”。

1.20.3 配置步骤

表1-13 配置 MAC 地址认证的 Guest VSI

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置MAC地址认证的Guest VSI	**mac-authentication guest-vsi** *guest-vsi-name*	缺省情况下，未配置MAC地址认证的Guest VSI

1.21 配置MAC地址认证Critical VSI

1.21.1 配置限制和指导

- MAC 地址认证 Critical VSI 功能的优先级高于 MAC 地址认证的静默 MAC 功能，即 MAC 地址认证用户加入指定的 Critical VSI 后，该用户的 MAC 地址不会被加入静默 MAC。
- 不同的端口可以指定不同的 MAC 地址认证 Critical VSI，一个端口最多只能指定一个 MAC 地址认证 Critical VSI。

1.21.2 配置准备

配置 MAC 地址认证的 Critical VSI 之前，需要进行以下配置：

- 开启 L2VPN 功能。
- 创建配置为 Critical VSI 的 VSI，并在该 VSI 下创建 VXLAN。
- 端口下动态创建 AC 匹配 MAC 地址功能处于开启状态。

上述配置的详细介绍，请参见“VXLAN 配置指导”中的“配置 VXLAN”。

1.21.3 配置步骤

表1-14 配置 MAC 地址认证的 Critical VSI

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置MAC地址认证的Critical VSI	**mac-authentication critical vsi** *critical-vsi-name*	缺省情况下，未配置MAC地址认证的Critical VSI

1.22 配置MAC地址认证的重认证

1.22.1 功能简介

MAC 地址重认证是指设备周期性对端口上在线的 MAC 地址认证用户发起重认证，以检测用户连接状态的变化，确保用户的正常在线，并及时更新服务器下发的授权属性（例如 ACL、VLAN 等）。

对 MAC 地址认证用户进行重认证时，设备将按照如下由高到低的顺序为其选择重认证时间间隔：服务器下发的重认证时间间隔、接口视图下配置的周期性重认证定时器的值、系统视图下配置的周期性重认证定时器的值、设备缺省的周期性重认证定时器的值。

认证服务器可以通过下发 RADIUS 属性（session-timeout、Termination-Action）来指定用户会话超时时长以及会话中止的动作类型。认证服务器上如何下发以上 RADIUS 属性的具体配置以及是否可以下发重认证周期的情况与服务器类型有关，请参考具体的认证服务器实现。

设备作为 RADIUS DAE 服务器，认证服务器作为 RADIUS DAE 客户端时，后者可以通过 COA（Change of Authorization）Messages 向用户下发重认证属性，这种情况下，无论设备上是否开

启了周期性重认证功能，端口都会立即对该用户发起重认证。关于 RADIUS DAE 服务器的详细内容，请参见“安全配置指导”中的“AAA”。

1.22.2 配置限制

MAC 地址认证用户认证通过后，端口对用户的重认证功能具体实现如下：

- 当认证服务器下发了用户会话超时时长，且指定的会话中止的动作类型为要求用户进行重认证时，则无论设备上是否开启周期性重认证功能，端口均会在用户会话超时时长到达后对该用户进行重认证；
- 当认证服务器下发了用户会话超时时长，且指定的会话中止的动作类型为要求用户下线时：
  - 若设备上开启了周期性重认证功能，且设备上配置的重认证定时器值小于用户会话超时时长，则端口会以重认证定时器的值为周期向该端口在线 MAC 地址认证用户发起重认证；若设备上配置的重认证定时器值大于等于用户会话超时时长，则端口会在用户会话超时时长到达后强制该用户下线；
  - 若设备上未开启周期性重认证功能，则端口会在用户会话超时时长到达后强制该用户下线。
- 当认证服务器未下发用户会话超时时长时，是否对用户进行重认证，由设备上配置的重认证功能决定。
- 对于已在线的 MAC 地址认证用户，要等当前重认证周期结束并且认证通过后才会按新配置的周期进行后续的重认证。
- 端口对用户进行重认证过程中，重认证服务器不可达时端口上的 MAC 地址认证用户状态由端口上的配置决定。在网络连通状况短时间内不良的情况下，合法用户是否会因为服务器不可达而被强制下线，需要结合实际的网络状态来调整。若配置为保持用户在线，当服务器在短时间内恢复可达，则可以避免用户频繁上下线；若配置为强制下线，当服务器可达性在短时间内不可恢复，则可避免用户在线状态长时间与实际不符。
- 在用户名不改变的情况下，端口允许重认证前后服务器向该用户下发不同的 VLAN。

1.22.3 配置步骤

表1-15 配置重认证服务器不可达时保持用户在线状态

配置步骤	命令	说明
进入系统视图	**system-view**	-
（可选）配置全局周期性重认证定时器	**mac-authentication timer reauth-period** *reauth-period-value*	缺省情况下，全局周期性重认证定时器的值为3600秒
进入接口视图	**interface** *interface-type interface-number*	-
开启周期性重认证功能	**mac-authentication re-authenticate**	缺省情况下，周期性重认证功能关闭
（可选）配置端口周期性重认证定时器	**mac-authentication timer reauth-period** *reauth-period-value*	缺省情况下，端口上未配置MAC地址周期性重认证定时器，端口使用系统视图下配置的MAC地址周期性重认证定时器的取值

配置步骤	命令	说明
（可选）配置重认证服务器不可达时端口上的MAC地址认证用户保持在线状态	**mac-authentication re-authenticate server-unreachable keep-online**	缺省情况下，端口上的MAC地址在线用户重认证时，若认证服务器不可达，则用户会被强制下线

1.23 配置MAC地址认证请求中携带用户IP地址

在终端用户采用静态 IP 地址方式接入的组网环境中，如果终端用户擅自修改自己的 IP 地址，则整个网络环境中可能会出现 IP 地址冲突等问题。

为了解决以上问题，管理员可以在端口上开启 MAC 地址认证请求中携带用户 IP 地址的功能，用户在进行 MAC 地址认证时，设备会把用户的 IP 地址上传到 iMC 服务器。然后 iMC 服务器会把认证用户的IP地址和MAC地址与服务器上已经存在的IP与MAC的绑定表项进行匹配，如果匹配成功，则该用户 MAC 地址认证成功；否则，MAC 地址认证失败。

H3C 的 iMC 服务器上 IP 与 MAC 地址信息绑定表项的生成方式如下：

- 如果在 iMC 服务器上创建用户时手工指定了用户的 IP 地址和 MAC 地址信息，则服务器使用手工指定的 IP 和 MAC 信息生成该用户的 IP 与 MAC 地址的绑定表项。
- 如果在 iMC 服务器上创建用户时未手工指定用户的 IP 地址和 MAC 地址信息，则服务器使用用户初次进行 MAC 地址认证时使用的 IP 地址和 MAC 地址生成该用户的 IP 与 MAC 地址的绑定表项。

此功能仅对采用静态 IP 地址方式接入的认证用户才有效。在采用 DHCP 方式获取 IP 地址的情况下，因为用户 MAC 地址认证成功之后才可以进行 IP 地址获取，所以用户在进行 MAC 地址认证时，设备无法上传用户的 IP 地址。

在开启了 MAC 地址认证的端口上，不建议同时配置 **mac-authentication carry user-ip** 和 **mac-authentication guest-vlan** 命令；因为当同时配置了以上两条命令之后，加入 Guest VLAN 的用户无法再次发起 MAC 地址认证，用户会一直停留在 Guest VLAN 中。

表1-16 开启 MAC 地址认证请求中携带用户 IP 地址功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置MAC地址认证请求中携带用户IP地址	**mac-authentication carry user-ip**	缺省情况下，MAC地址认证请求中不携带用户IP地址

1.24 配置MAC地址认证Guest VLAN中的用户进行重新认证的时间间隔

在 MAC 地址认证中，如果接入用户的端口上配置了 Guest VLAN，则该端口上认证失败的用户会被加入此 Guest VLAN。用户被加入 Guest VLAN 之后，设备将以指定的时间间隔对该用户发起重新认证，直到该用户认证成功。

表1-17 配置 MAC 地址认证中设备对 Guest VLAN 中的用户进行重新认证的时间间隔

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置MAC地址认证中设备对Guest VLAN中的用户进行重新认证的时间间隔	**mac-authentication guest-vlan auth-period** *period-value*	缺省情况下，设备对Guest VLAN中的用户进行重新认证的时间间隔为30秒

1.25 配置MAC地址认证Guest VSI中的用户进行重新认证的时间间隔

在 MAC 地址认证中，如果接入用户的端口上配置了 Guest VSI，则该端口上认证失败的用户会被加入此 Guest VSI。用户被加入 Guest VSI 之后，设备将以指定的时间间隔对该用户发起重新认证，直到该用户认证成功。

表1-18 配置 MAC 地址认证中设备对 Guest VSI 中的用户进行重新认证的时间间隔

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置MAC地址认证中设备对Guest VSI中的用户进行重新认证的时间间隔	**mac-authentication guest-vsi auth-period** *period-value*	缺省情况下，设备对Guest VSI中的用户进行重新认证的时间间隔为30秒

1.26 配置端口的MAC地址认证下线检测功能

开启端口的 MAC 地址认证下线检测功能后，若设备在一个下线检测定时器间隔之内，未收到此端口下某在线用户的报文，则将切断该用户的连接，同时通知 RADIUS 服务器停止对此用户进行计费。关闭端口的 MAC 地址认证下线检测功能后，设备将不会对在线用户的状态进行检测。

表1-19 开启端口的 MAC 地址认证下线检测功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
开启端口的MAC地址认证下线检测功能	**mac-authentication offline-detect enable**	缺省情况下，端口的MAC地址认证下线检测功能处于开启状态

1.27 MAC地址认证的显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 MAC 地址认证的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可以清除相关统计信息。

表1-20 MAC 地址认证的显示和维护

操作	命令
显示MAC地址认证的相关信息	**display mac-authentication** [**interface** *interface-type interface-number*]
显示MAC地址认证连接信息	**display mac-authentication connection** [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-addr* | **user-name** *user-name*]
清除MAC地址认证的统计信息	**reset mac-authentication statistics** [**interface** *interface-type interface-number*]
清除Critical VLAN内MAC地址认证用户	**reset mac-authentication critical vlan interface** *interface-type interface-number* [**mac-address** *mac-address*]
清除Critical Voice VLAN内MAC地址认证用户	**reset mac-authentication critical-voice-vlan interface** *interface-type interface-number* [**mac-address** *mac-address*]
清除Guest VLAN内MAC地址认证用户	**reset mac-authentication guest-vlan interface** *interface-type interface-number* [**mac-address** *mac-address*]
清除Critical VSI内MAC地址认证用户	**reset mac-authentication critical vsi interface** *interface-type interface-number* [**mac-address** *mac-address*]
清除Guest VSI内MAC地址认证用户	**reset mac-authentication guest-vsi interface** *interface-type interface-number* [**mac-address** *mac-address*]

1.28 MAC地址认证典型配置举例

1.28.1 本地MAC地址认证

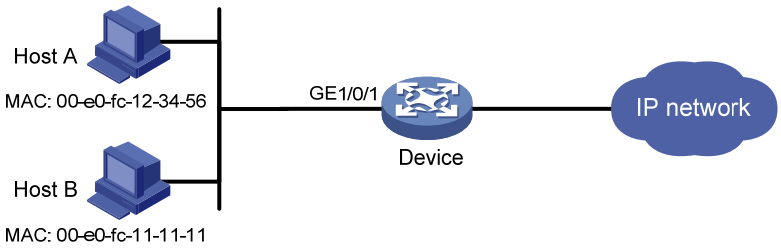
1. 组网需求

如 图 1-3 所示，某子网的用户主机与设备的端口GigabitEthernet1/0/1 相连接。

- 设备的管理者希望在端口 GigabitEthernet1/0/1 上对用户接入进行 MAC 地址认证，以控制它们对 Internet 的访问。
- 要求设备每隔 180 秒就对用户是否下线进行检测；并且当用户认证失败时，需等待 180 秒后才能对用户再次发起认证。
- 所有用户都属于 ISP 域 bbb，认证时使用本地认证的方式。
- 使用用户的 MAC 地址作用户名和密码，其中 MAC 地址带连字符、字母小写。

2. 组网图

图1-3 启动 MAC 地址认证对接入用户进行本地认证



3. 配置步骤

添加网络接入类本地接入用户。本例中添加 Host A 的本地用户，用户名和密码均为 Host A 的 MAC 地址 00-e0-fc-12-34-56，服务类型为 **lan-access**。

```
<Device> system-view
[Device] local-user 00-e0-fc-12-34-56 class network
[Device-luser-network-00-e0-fc-12-34-56] password simple 00-e0-fc-12-34-56
[Device-luser-network-00-e0-fc-12-34-56] service-type lan-access
[Device-luser-network-00-e0-fc-12-34-56] quit
```

配置 ISP 域，使用本地认证方法。

```
[Device] domain bbb
[Device-isp-bbb] authentication lan-access local
[Device-isp-bbb] quit
```

开启端口 GigabitEthernet1/0/1 的 MAC 地址认证。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-authentication
[Device-GigabitEthernet1/0/1] quit
```

配置 MAC 地址认证用户所使用的 ISP 域。

```
[Device] mac-authentication domain bbb
```

配置 MAC 地址认证的定时器。

```
[Device] mac-authentication timer offline-detect 180
[Device] mac-authentication timer quiet 180
```

配置 MAC 地址认证用户名格式：使用带连字符的 MAC 地址作为用户名与密码，其中字母小写。

```
[Device] mac-authentication user-name-format mac-address with-hyphen lowercase
```

开启全局 MAC 地址认证。

```
[Device] mac-authentication
```

4. 验证配置

当用户接入端口 GigabitEthernet1/0/1 之后，可以通过如下显示信息看到 Host A 成功通过认证，处于上线状态，Host B 没有通过认证，它的 MAC 地址被加入静默 MAC 列表。

```
<Device> display mac-authentication
Global MAC authentication parameters:
   MAC authentication     : Enabled
   User name format       : MAC address in lowercase(xx-xx-xx-xx-xx-xx)
           Username       : mac
           Password       : Not configured
```

```
  Offline detect period  : 180 s
  Quiet period           : 180 s
  Server timeout         : 100 s
  Reauth period          : 3600 s
  Authentication domain  : bbb
Online MAC-auth users    : 1

Silent MAC users:
         MAC address       VLAN ID  From port               Port index
         00e0-fc11-1111    8        GE1/0/1                1
GigabitEthernet1/0/1 is link-up
  MAC authentication         : Enabled
  Carry User-IP              : Disabled
  Authentication domain      : Not configured
  Auth-delay timer           : Disabled
  Periodic reauth            : Disabled
  Re-auth server-unreachable : Logoff
  Guest VLAN                 : Not configured
  Guest VLAN auth-period     : 30 s
  Critical VLAN              : Not configured
  Critical voice VLAN        : Disabled
  Host mode                  : Single VLAN
  Offline detection          : Enabled
  Authentication order       : Default
  Guest VSI                  : Not configured
  Guest VSI auth-period      : 30 s
  Critical VSI               : Not configured
  Max online users           : 4294967295
  Auto-tag feature           : Disabled
  VLAN tag configuration ignoring : Disabled
   Authentication attempts    : successful 1, failed 0
  Current online users       : 1
         MAC address       Auth state
         00e0-fc12-3456    Authenticated
```

1.28.2 使用RADIUS服务器进行MAC地址认证

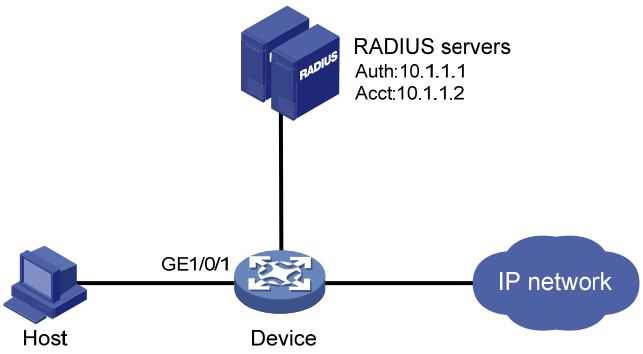
1. 组网需求

如 图 1-4 所示，用户主机Host通过端口GigabitEthernet1/0/1 连接到设备上，设备通过RADIUS服务器对用户进行认证、授权和计费。

- 设备的管理者希望在端口 GigabitEthernet1/0/1 上对用户接入进行 MAC 地址认证，以控制其对 Internet 的访问。
- 要求设备每隔 180 秒就对用户是否下线进行检测；并且当用户认证失败时，需等待 180 秒后才能对用户再次发起认证。
- 所有用户都属于域 bbb，认证时采用固定用户名格式，用户名为 aaa，密码为 123456。

2. 组网图

图1-4 启动 MAC 地址认证对接入用户进行 RADIUS 认证



3. 配置步骤

说明

确保 RADIUS 服务器与设备路由可达，并成功添加了接入用户帐户：用户名为 aaa，密码为 123456。

配置 RADIUS 方案。

```
<Device> system-view
[Device] radius scheme 2000
[Device-radius-2000] primary authentication 10.1.1.1 1812
[Device-radius-2000] primary accounting 10.1.1.2 1813
[Device-radius-2000] key authentication simple abc
[Device-radius-2000] key accounting simple abc
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

配置 ISP 域的 AAA 方法。

```
[Device] domain bbb
[Device-isp-bbb] authentication default radius-scheme 2000
[Device-isp-bbb] authorization default radius-scheme 2000
[Device-isp-bbb] accounting default radius-scheme 2000
[Device-isp-bbb] quit
```

开启端口 GigabitEthernet1/0/1 的 MAC 地址认证。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-authentication
[Device-GigabitEthernet1/0/1] quit
```

配置 MAC 地址认证用户所使用的 ISP 域。

```
[Device] mac-authentication domain bbb
```

配置 MAC 地址认证的定时器。

```
[Device] mac-authentication timer offline-detect 180
[Device] mac-authentication timer quiet 180
```

配置 MAC 地址认证使用固定用户名格式：用户名为 aaa，密码为明文 123456。

```
[Device] mac-authentication user-name-format fixed account aaa password simple 123456
```

开启全局 MAC 地址认证。

```
[Device] mac-authentication
```

4. 验证配置

显示 MAC 地址认证配置信息。

```
<Device> display mac-authentication
Global MAC authentication parameters:
   MAC authentication     : Enabled
   Username format        : Fixed account
           Username       : aaa
           Password       : ******
   Offline detect period  : 180 s
   Quiet period           : 180 s
   Server timeout         : 100 s
   Reauth period          : 3600 s
   Authentication domain  : bbb
 Online MAC-auth users    : 1

 Silent MAC users:
          MAC address       VLAN ID  From port               Port index

 GigabitEthernet1/0/1  is link-up
   MAC authentication         : Enabled
   Carry User-IP              : Disabled
   Authentication domain      : Not configured
   Auth-delay timer           : Disabled
   Periodic reauth            : Disabled
   Re-auth server-unreachable : Logoff
   Guest VLAN                 : Not configured
   Guest VLAN auth-period     : 30 s
   Critical VLAN              : Not configured
   Critical voice VLAN        : Disabled
   Host mode                  : Single VLAN
   Offline detection          : Enabled
   Authentication order       : Default
   Guest VSI                  : Not configured
   Guest VSI auth-period      : 30 s
   Critical VSI               : Not configured
   Max online users           : 4294967295
   Auto-tag feature           : Disabled
   VLAN tag configuration ignoring : Disabled
    Authentication attempts    : successful 1, failed 0
   Current online users       : 1
          MAC address       Auth state
          00e0-fc12-3456    Authenticated
```

1.28.3 下发ACL典型配置举例

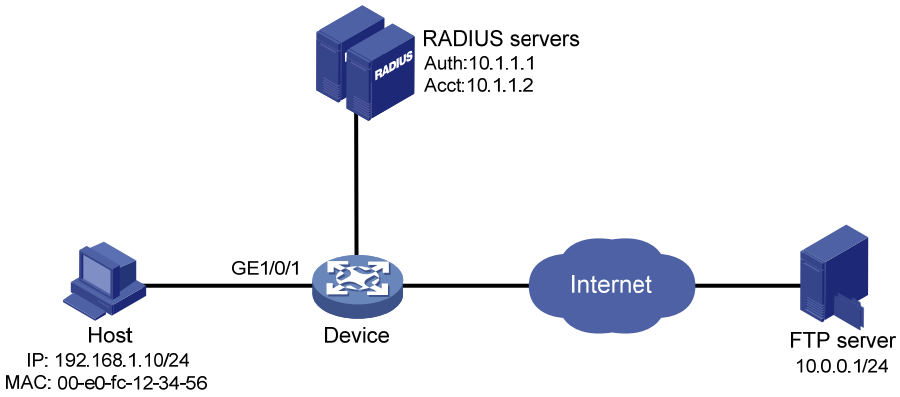
1. 组网需求

如 图 1-5 所示，用户主机Host通过端口GigabitEthernet1/0/1 连接到设备上，设备通过RADIUS服务器对用户进行认证、授权和计费，Internet网络中有一台FTP服务器，IP地址为 10.0.0.1。现有如下组网需求：

- 在端口 GigabitEthernet1/0/1 上对用户接入进行 MAC 地址认证，以控制其对 Internet 的访问。认证时使用用户的源 MAC 地址做用户名和密码，其中 MAC 地址带连字符、字母小写。
- 当用户认证成功上线后，允许用户访问除 FTP 服务器之外的 Internet 资源。

2. 组网图

图1-5 下发 ACL 典型配置组网图



3. 配置步骤

说明

- 确保 RADIUS 服务器与设备路由可达。
- 由于该例中使用了 MAC 地址认证的缺省用户名和密码，即使用用户的源 MAC 地址做用户名与密码，因此还要保证 RADIUS 服务器上正确添加了接入用户帐户：用户名为 00-e0-fc-12-34-56，密码为 00-e0-fc-12-34-56。
- 指定 RADIUS 服务器上的授权 ACL 为设备上配置的 ACL 3000。

(1) 配置授权 ACL

配置 ACL 3000，拒绝目的 IP 地址为 10.0.0.1 的报文通过。

```
<Device> system-view
[Device] acl advanced 3000
[Device-acl-ipv4-adv-3000] rule 0 deny ip destination 10.0.0.1 0
[Device-acl-ipv4-adv-3000] quit
```

(2) 配置使用 RADIUS 服务器进行 MAC 地址认证

配置 RADIUS 方案。

```
[Device] radius scheme 2000
```

```
[Device-radius-2000] primary authentication 10.1.1.1 1812
[Device-radius-2000] primary accounting 10.1.1.2 1813
[Device-radius-2000] key authentication simple abc
[Device-radius-2000] key accounting simple abc
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

配置 ISP 域的 AAA 方法。

```
[Device] domain bbb
[Device-isp-bbb] authentication default radius-scheme 2000
[Device-isp-bbb] authorization default radius-scheme 2000
[Device-isp-bbb] accounting default radius-scheme 2000
[Device-isp-bbb] quit
```

配置 MAC 地址认证用户所使用的 ISP 域。

```
[Device] mac-authentication domain bbb
```

配置 MAC 地址认证用户名格式：使用带连字符的 MAC 地址做用户名与密码，其中字母小写。

```
[Device] mac-authentication user-name-format mac-address with-hyphen lowercase
```

开启端口 GigabitEthernet1/0/1 上的 MAC 地址认证。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-authentication
[Device-GigabitEthernet1/0/1] quit
```

开启全局 MAC 地址认证。

```
[Device] mac-authentication
```

4. 验证配置

显示 MAC 地址认证配置信息。

```
<Device> display mac-authentication
Global MAC authentication parameters:
   MAC authentication     : Enable
   Username format        : MAC address in lowercase(xx-xx-xx-xx-xx-xx)
           Username       : mac
           Password       : Not configured
   Offline detect period  : 300 s
   Quiet period           : 60 s
   Server timeout         : 100 s
   Reauth period          : 3600 s
   Authentication domain  : bbb
 Online MAC-auth users    : 1

 Silent MAC users:
         MAC address       VLAN ID  From port               Port index

 GigabitEthernet1/0/1  is link-up
   MAC authentication         : Enabled
   Carry User-IP              : Disabled
   Authentication domain      : Not configured
   Auth-delay timer           : Disabled
   Periodic reauth            : Disabled
```

```
   Re-auth server-unreachable : Logoff
   Guest VLAN                 : Not configured
   Guest VLAN auth-period     : 30 s
   Critical VLAN              : Not configured
   Critical voice VLAN        : Disabled
   Host mode                  : Single VLAN
   Offline detection          : Enabled
   Authentication order       : Default
   Guest VSI                  : Not configured
   Guest VSI auth-period      : 30 s
   Critical VSI               : Not configured
   Max online users           : 4294967295
   Auto-tag feature           : Disabled
   VLAN tag configuration ignoring : Disabled
    Authentication attempts    : successful 1, failed 0
   Current online users       : 1
          MAC address       Auth state
          00e0-fc12-3456    Authenticated
```

用户认证上线后，Ping FTP 服务器，发现服务器不可达，说明认证服务器下发的 ACL 3000 已生效。

```
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.1:
   Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

1.28.4 MAC地址认证授权VSI配置举例

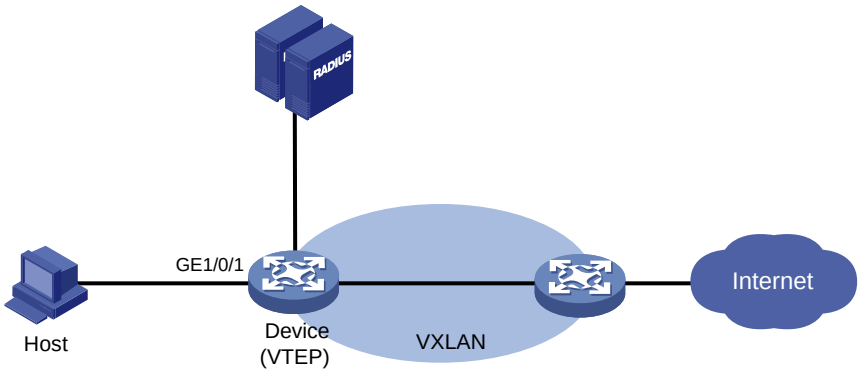
1. 组网需求

如 图 1-6 所示，一台主机通过Device（作为VETP设备）接入VXLAN网络，认证服务器为RADIUS服务器。现有如下组网需求：

- 设备的管理者希望在端口 GigabitEthernet1/0/1 上对用户接入进行 MAC 地址认证，以控制其对 Internet 的访问。
- 用户认证成功上线后，认证服务器下发 VSI bbb，此时 Host 的流量被映射到 VSI bbb 对应的 VXLAN 5 内，Host 可以访问对应的资源。
- 所有用户都属于域 2000，认证时采用 MAC 地址用户名格式，用户名和密码为用户的 MAC 地址（本例为 d485-64be-c63e）。

2. 组网图

图1-6 MAC 地址认证支持授权 VSI 下发



3. 配置步骤

说明

- 完成 RADIUS 服务器的配置，添加用户帐户（用户名为 d485-64be-c63e，密码为 d485-64be-c63e），指定要授权下发的 VSI，并保证用户的认证/授权/计费功能正常运行。
- 确保 RADIUS 服务器与设备路由可达。
- 若实际组网中认证/授权服务器采用的是 H3C ADCAM 服务器，有关 MAC 地址认证支持下发 VSI 的相关配置需要在 H3C ADCAM 服务器端完成，再自动下发到设备上。因此，Device 上不需要做认证相关配置。

配置 RADIUS 方案。

```
<Device> system-view
[Device] radius scheme bbb
[Device-radius-bbb] primary authentication 10.1.1.1
[Device-radius-bbb] primary accounting 10.1.1.2
[Device-radius-bbb] key authentication simple bbb
[Device-radius-bbb] key accounting simple bbb
[Device-radius-bbb] user-name-format without-domain
[Device-radius-bbb] quit
```

配置 ISP 域的 2000 方法。

```
[Device] domain 2000
[Device-isp-2000] authentication lan-access radius-scheme bbb
[Device-isp-2000] authorization lan-access radius-scheme bbb
[Device-isp-2000] accounting lan-access radius-scheme bbb
[Device-isp-2000] quit
```

开启端口 GigabitEthernet1/0/1 的 MAC 地址认证。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-authentication
```

在端口 GigabitEthernet1/0/1 开启动态创建的以太网服务实例匹配 MAC 地址功能。

```
[Device-GigabitEthernet1/0/1] mac-based ac
```

```
[Device-GigabitEthernet1/0/1] quit
```

开启 L2VPN 功能。

```
[Device] l2vpn enable
```

配置授权 VSI 下的 VXLAN。

```
[Device] vsi bbb
[Device-vsi-bbb] vxlan 5
[Device-vsi-bbb-vxlan-5] quit
```

配置 MAC 地址认证用户所使用的 ISP 域。

```
[Device] mac-authentication domain 2000
```

配置 MAC 地址认证使用 MAC 地址用户名格式，且携带连字符，字母小写。

```
[Device] mac-authentication user-name-format mac-address with-hyphen lowercase
```

开启全局 MAC 地址认证。

```
[Device] mac-authentication
```

4. 验证配置

在用户认证成功之后，通过命令 **display mac-authtication connection** 可以看到服务器已下发授权 VSI bbb。

```
[Device] display mac-authentication connection
Slot ID: 1
User MAC address: d485-64be-c63e
Access interface: GigabitEthernet1/0/1
Username: d485-64be-c63e
Authentication domain: 2000
Initial VLAN: 1
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization VSI name: bbb
Authorization ACL ID: N/A
Authorization user profile: N/A
Authorization URL:  N/A
Termination action: N/A
Session timeout period: N/A
Online from: 2016/06/13 09:06:37
Online duration: 0h 0m 35s

Total connections: 1
```

通过命令 **display l2vpn forwording ac verbose** 可以看到成功创建动态 AC。

```
[Device] display l2vpn forwarding ac verbose
VSI Name: bbb
  Interface: GE1/0/1  Service Instance: 1
    Link ID      : 0
    Access Mode  : VLAN
    Encapsulation: untagged
    Type         : Dynamic (MAC-based)
    MAC address  : d485-64be-c63e
```