配置指南-无线认证

本分册介绍无线认证配置指南相关内容，包括以下章节：

1. AAA
2. RADIUS
3. TACACS
4. 802.1x
5. 本地认证服务
6. Web 认证
7. ROLE-MGMT
8. APP 认证
9. SCC(安全控制中心)
10. GSN

1 AAA

1.1 概述

AAA 是 Authentication Authorization and Accounting（认证、授权和记账）的简称，它提供了对认证、授权和记账功能进行配置的一致性框架，设备支持使用 AAA。

AAA 以模块方式提供以下服务：

认证：验证用户是否可获得访问权，可选择使用 RADIUS 协议、TACACS+协议或 Local（本地）等。身份认证是在允许用户访问网络和网络服务之前对其身份进行识别的一种方法。

授权：授权用户可使用哪些服务。AAA 授权通过定义一系列的属性对来实现，这些属性对描述了用户被授权执行的操作。这些属性对可以存放在网络设备上，也可以远程存放在安全服务器上。

记账：记录用户使用网络资源的情况。当 AAA 记账被启用时，网络设备便开始以统计记录的方式向安全服务器发送用户使用网络资源的情况。每个记账记录都是以属性对的方式组成，并存放在安全服务器上，这些记录可以通过专门软件进行读取分析，从而实现对用户使用网络资源的情况进行记账、统计、跟踪。

尽管 AAA 是最主要的访问控制方法，设备同时也提供了在 AAA 范围之外的简单控制访问，如本地用户名身份认证、线路密码身份认证等。不同之处在于它们提供对网络保护程度不一样，AAA 提供更高级别的安全保护。

使用 AAA 有以下优点：

- 灵活性和可控制性强
- 可扩充性
- 标准化认证
- 多个备用系统

协议规范

- 暂无相应规范

1.2 典型应用

典型应用	场景描述
无域环境下的认证、授权、记账	所有用户处于同一个域，进行认证、授权、记账
多域环境下的认证、授权、记账	处于不同域的用户，采用不同的方法进行认证、授权、记账

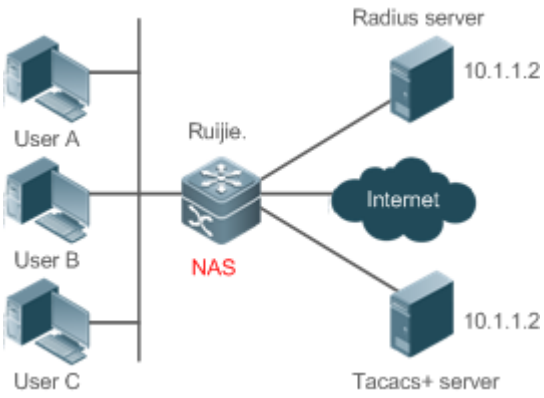
1.2.1 无域环境下的认证、授权、记账

应用场景

在图 1-1 所示的网络应用中，为了更好地对网络访问控制器设备（NAS，以下简称网络设备）进行安全管理，需要满足如下应用要求：

1. 不同的管理人员有各自的用户账号，其用户名和口令不能共享，便于帐号管理和防止泄漏。
2. 对网络设备的访问需经过认证，用户认证的实现方式可以分为本地认证和集中认证，应采用集中认证和本地认证相结合的方式，集中认证为主用、本地认证为备用。在集中认证过程中，要求先通过 RADIUS 服务器认证，若无响应再转本地认证。
3. 在认证时，不同的用户可以被限制只能访问特定的网络设备。
4. 对用户进行分权限管理：把网络管理用户分为超级用户和普通用户。其中，超级用户对网络设备拥有查看和配置的权限，普通用户对网络设备只拥有特定的查看权限。
5. 服务器端可将用户的认证信息、授权信息和网络行为记录在服务器中，以供日后查看和审计（本例采用 TACACS+进行记账）。

图 1-1



【注释】 UserA，UserB，UserC 直接或者通过网络和 NAS 相连接。
RADIUS 服务器可以是 Windows 2000/2003 Server（IAS）、UNIX 系统所带组件，也可以是厂商提供的专用服务器软件。
TACACS+服务器可以是厂商提供的专用的服务器软件。

功能部属

- 在 NAS 上启用 AAA
- 在 NAS 上配置安全服务器
- 在 NAS 上配置本地用户

- 在 NAS 上配置认证
- 在 NAS 上配置授权
- 在 NAS 上配置记账

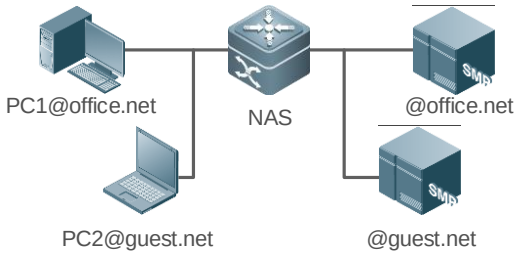
1.2.2 多域环境下的认证、授权、记账

应用场景

通过配置网络访问控制器设备实现基于域名的 AAA 服务，包括认证、授权、记账功能：

- 使用 802.1x 客户端进行登录认证，使用用户名为 PC1@office.net 或 PC2@guest.net，再输入正确的密码进行认证就可认证成功。
- 对用户进行分权限管理：把网络管理用户分为超级用户和普通用户。其中，超级用户对网络设备拥有查看和配置的权限，普通用户对网络设备只拥有特定的查看权限。
- 认证服务器端可将用户的认证信息、授权信息和网络行为记录在服务器中，以供日后查看和审计。

图 1-2



【注释】 PC1@office.net，PC2@guest.net 直接或者通过网络和 NAS 相连接。
NAS 通常为接入设备。
SAM 为锐捷公司提供的通用 RADIUS 服务器。

功能部属

- 在 NAS 上启用 AAA
- 在 NAS 上配置安全服务器
- 在 NAS 上配置本地用户
- 在 NAS 上定义 AAA 服务的方法列表
- 在 NAS 上打开基于域名的 AAA 服务开关
- 在 NAS 上创建域并配置域属性集

1.3 功能详解

基本概念

本地认证、远程服务器认证

对用户进行认证时，如果使用 NAS 上的用户数据库进行密码校验，就称为本地认证。

对用户进行认证时，如果使用远程服务器上的用户数据库进行密码校验，就称为远程服务器认证。目前，远程服务器认证主要是 RADIUS 服务器认证和 TACACA+服务器认证。

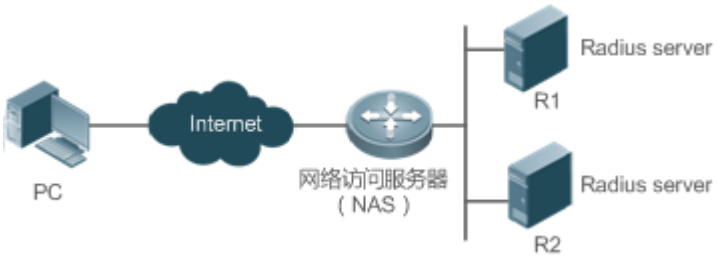
方法列表

由于对用户进行认证、授权和记账可以使用不同的安全方法，因此需要使用方法列表定义一个使用不同方法对用户进行认证、授权和记账的前后顺序。方法列表可以定义一个或多个安全协议，这样可以确保在第一个方法失败时，有备用系统可用。设备使用方法列表中列出的第一个方法时，如果该方法无应答，则选择方法列表中的下一个方法。该过程一直持续下去，直到与列出的某种安全方法成功地实现通信或用完方法列表。如果用完方法列表而还没有成功实现通信，则该安全功能宣告失败。

方法列表仅是定义将要被依次查询的、并用于认证用户身份的一系列安全方法。方法列表能够指定一个或多个用于身份认证的安全协议，这样确保在第一种方法失败的情况下，可以使用身份认证备份系统。设备使用第一种方法认证用户的身份，如果该方法无应答，将选择方法列表中的下一种方法。该过程一直持续下去，直到与列出的某种身份认证方法成功地实现通信或用完方法列表。如果用完方法列表而还没有成功实现通信，则身份认证宣告失败。

⚠ 只有在前一种方法没有应答的情况下，设备才会尝试下一种方法。例如在身份认证过程中，某种方法拒绝了用户访问，则身份认证过程结束，不再尝试其他的身份认证方法。

图 1-3



上图说明了一个典型的 AAA 网络配置，包含两台安全服务器：R1 和 R2 是 RADIUS 服务器。以及一台网络访问服务器（NAS），可以作为 RADIUS 客户端。

假设系统管理员已定义了一个方法列表，在该列表中，R1 首先被用来获取身份信息，之后是 R2，最后是访问服务器上的本地用户名数据库。如果一个远程 PC 用户试图拨号进入网络，网络访问服务器首先向 R1 查询身份认证信息，假如用户通过了 R1 的身份认证，R1 将向网络访问服务器发出一个 ACCEPT 应答，这样用户即获准访问网络。如果 R1 返回的是 REJECT 应答，则拒绝用户访问网络，断开连接。如果 R1 无应答，网络访问服务器就将它看作 TIMEOUT，并向 R2 查询身份认证信息。该过程会一直在余下的指定方法中持续下去，直到用户通过身份认证、被拒绝或对话被中止。如果所有的方法返回 TIMEOUT，则认证失败，连接将被断开。

REJECT 应答不同于 TIMEOUT 应答。REJECT 意味着用户不符合可用身份认证数据库中包含的标准，从而未能通过身份认证，访问请求被拒绝。TIMEOUT 则意味着安全服务器对身份认证查询未作应答，当检测到一个 TIMEOUT 时，AAA 选择身份认证方法列表中定义的下一个身份认证方法将继续进行身份认证过程。

在本文中，与 AAA 安全服务器相关的认证、授权和记账配置，均以 RADIUS 为例，而与 TACACS+有关的内容请另外参考“配置 TACACS+”。

AAA 服务器组

定义一个 AAA 服务器组，用于把一个或几个同一类型的服务器划分为同一组。配置方法列表时，引用该服务器组，则使用该方法列表进行认证、授权、记账操作时，首先向被引用服务器组中的服务器发起请求。

功能特性

功能特性	作用
AAA 认证	验证是否允许用户接入网络
AAA 授权	定义用户可以使用哪些服务或拥有哪些权限
AAA 记账	记录用户使用网络资源的情况
AAA 多域	针对不同域的用户，创建认证、授权和记账方案。

1.3.1 AAA 认证

在 AAA 中，认证、授权和计费是三个独立的业务过程。认证是用来验证用户是否可以获得访问权，其职责是完成各接入或服务请求的用户名、密码和用户信息的交互认证过程。在 AAA 中，可以只使用认证，而不使用授权或计费。

要配置 AAA 身份认证，首先得定义一个身份认证方法的命名列表，之后各个应用使用已定义列表进行认证。方法列表定义了身份认证的类型和执行顺序。对于已定义的身份认证方法，必须有特定的应用才会被执行。默认方法列表是唯一的例外。所有应用在未进行配置时使用默认方法列表。

AAA 认证方案：

- 不认证（none）

对用户高度信任，不对其进行合法性检查。一般情况下不采用这种方法。

- 本地认证（local）

认证过程在 NAS 设备上完成，用户信息（包括用户名、密码和各种属性）直接配置在接入设备上。当配置 local 参数使用本地数据库进行验证时，需要使用 username password/secret 命令预先在本地创建用户数据库。

- 远程服务器组认证（group）

认证过程在 NAS 和一个远程服务器组之间完成（一个服务器组可包含任意个相同类型的服务器），NAS 和远程服务器之间通过 RADIUS 或 TACACS+协议通信。用户信息集中在远程服务器上统一管理，可以实现大容量、高可靠性、支持多设备的集中式统一认证。为提防远程服务器组的服务器均无效时，可配置本地认证作为备选认证方式完成认证。

AAA 认证类型

设备目前支持以下认证类型：

- Login（登录）认证

针对 SSH、Telnet、FTP 等终端接入用户，在用户登录到 NAS 命令行界面时进行身份认证。

- Enable 认证

针对的是用户终端登录到 NAS 上的命令行界面以后，提升命令行界面执行权限时进行认证。即对 enable（进入特权模式）行为进行认证。

- PPP 认证

针对 PPP 拨号接入用户进行身份认证。

- DOT1X（IEEE802.1x）认证

针对 IEEE802.1x 接入用户进行身份认证。

- iportal（内置 portal）认证

针对使用一代 portal 服务器来进行身份认证。

- Web-auth（二代 portal）认证

针对使用二代 portal 服务器来进行身份认证。

- 通用认证方法

统一为 802.1x 认证、内置 portal 认证、二代 portal 认证指定认证方法。

相关配置

↘ 启动 AAA

缺省情况下，AAA 没有启动。

使用 **aaa new-model** 命令可以启动。

↘ 配置 AAA 认证方案

缺省情况下，没有配置任何 AAA 认证方案。

确定使用本地(Local)认证还是远程服务器认证。如果用户使用远程服务器认证，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 Local 认证，则需要在 NAS 上配置本地用户数据库信息。

↘ 配置 AAA 认证方法

缺省情况下，没有配置任何 AAA 认证方法。

确定要配置的接入方式，针对不同接入方式配置不同的认证方法。

1.3.2 AAA 授权

AAA 授权使管理员能够对用户可使用的服务或权限进行控制。启用 AAA 授权服务以后，网络设备通过本地或服务器中的用户配置文件信息对用户的会话进行配置。完成授权以后，该用户只能使用配置文件中允许的服务或只具备许可的权限。

↘ AAA 授权方案

- 直接授权（none）

对用户高度信任，直接授权用户的权限为接入设备允许用户所使用的默认权限。

- 本地授权（local）

授权过程在 NAS 设备上完成，根据 NAS 上为本地用户配置的相关属性进行授权。

- 远程服务器授权（group）

授权过程在 NAS 和远程服务器组之间完成。当远程服务器组的服务器均无效时，可以配置本地授权或直接授权作为备选授权方式完成授权。

↘ AAA 授权类型

- Exec 授权

针对的是用户终端登录到 NAS 上的 CLI 界面时，授予用户终端的权限级别（分为 0~15 级）。

- Config-commands 授权

对配置模式（包括全局配置模式及其子模式）下的命令进行授权。

- Console 授权

对通过控制台登录的用户所执行命令的授权。

- Command（命令）授权

用户终端登录到 NAS 上的 CLI 界面以后，针对具体命令的执行授权。

- Network（网络）授权

授予网络连接上的用户会话可用的服务。例如 PPP、SLIP 等网络连接接通过 Network 授权，可以获得诸如流量、带宽、超时等服务配置。

相关配置

↘ 启动 AAA

缺省情况下，AAA 没有启动。

使用 **aaa new-model** 命令可以启动。

↘ 配置 AAA 授权方案

缺省情况下，没有配置任何 AAA 授权方案。

确定使用本地（local）授权还是远程服务器授权。如果用户使用远程服务器授权，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 Local 授权，则需要在 NAS 上配置本地用户数据库信息。

↘ 配置 AAA 授权方法

缺省情况下，没有配置任何 AAA 授权方法。

确定要配置的接入方式，针对不同接入方式配置不同的认证方法。

1.3.3 AAA 记账

在 AAA 中，记账是一个和认证、授权同级别的独立流程，其职责为发送记账开始、更新和结束请求给所配置的记账服务器，由服务器记录用户使用网络资源的情况，实现对用户的活动进行计费、审计以及跟踪等功能。

在 AAA 配置中，记账方案不是必须配置的。

↘ AAA 记账方案

- 不记账（none）

不对用户记账。

- 本地记账（local）

记账过程在 NAS 上完成，实现了本地用户连接数的统计和限制，并没有实际的费用统计功能。

- 远程服务器组记账（group）

记账过程在接入设备和远程的服务器之间完成。当远程服务器组失效时，可配置本地记账作为备选记账方式完成记账。

↘ AAA 记账类型

- Exec 记账

针对的是用户终端登录到 NAS 上的 CLI 界面时，在登入和登出时分别进行记账。

- Command 记账

用户终端登录到 NAS 上的 CLI 界面以后，记录其具体执行的命令。

- Network 记账

记录与网络连接用户（如 802.1x、Web 认证等用户）会话有关的信息。

相关配置

↘ 启动 AAA

缺省情况下，AAA 没有启动。

使用 **aaa new-model** 命令可以启动。

↘ 配置 AAA 记账方案

缺省情况下，没有配置任何 AAA 记账方案。

确定使用本地(Local)记账还是远程服务器记账。如果用户使用远程服务器记账，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 Local 记账，则需要在 NAS 上配置本地用户数据库信息。

↘ 配置 AAA 记账方法

缺省情况下，没有配置任何 AAA 记账方案。

确定要配置的接入方式，针对不同接入方式配置不同的记账方法。

1.3.4 AAA 多域

在多域环境下，同一台网络访问服务器（NAS）设备可为不同域中的用户提供 AAA 服务，各域中用户的属性（例如用户名及密码、服务类型、权限等）有可能各不相同，因此有必要通过设置域的方法把它们区分开，并为每个域单独配置包括 AAA 服务方法列表（例如使用的 RADIUS）在内的属性集。

本产品支持以下几种的形式的用户名

6. userid@domain-name
7. domain-name\userid
8. userid.domain-name
9. userid

对于第 4 种不带 domain-name 的形式的用户名（即以上第 4 种：userid），认为其域名称为 default，即为默认的域名。

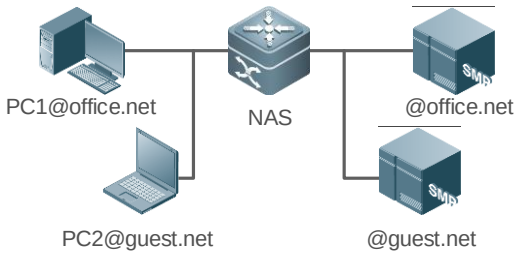
设备基于域名的 AAA 服务基本原理如下：

- 解析用户携带的域名称
- 根据域名称查找用户所配置的域
- 根据设备上域配置信息查找相应的 AAA 服务的方法列表名
- 根据方法列表名在系统中查找对应的方法列表
- 使用该方法列表提供 AAA 服务

上述任何一个步骤失败，用户将无法使用申请的 AAA 服务。

以下是典型的多个域环境拓扑图：

图 1-4



相关配置

↘ 启动 AAA

缺省情况下，AAA 没有启动。

使用 **aaa new-model** 命令可以启动。

↘ 定义 AAA 服务的方法列表

缺省情况下，没有配置任何 AAA 服务的方法列表。

配置方法列表请参照 5.2.1、5.2.2、5.2.3 章节

↘ 启用基于域名的 AAA 服务

缺省情况下，基于域名的 AAA 服务没有启动。

使用 **aaa domain enable** 命令可以启动基于域名的 AAA 服务。

↘ 创建域

缺省情况下，没有配置任何域。

使用 **aaa domain** *doman-name* 命令配置域名。

↘ 配置域属性集

缺省情况下，没有域属性集。

域属性集包括该域使用的认证、授权、记账方法列表；域的同时在线人数；是否去除用户名中的域名；域是否生效等。

↘ 查看域配置

使用 **show aaa domain** 查看域配置

系统最多支持配置 32 个域。

1.4 配置详解

配置项	配置建议&相关命令

配置 AAA 认证	如果要确认用户的身份，则必须配置。	
	aaa new-model	开启 AAA。
	aaa authentication login	定义 Login 认证的认证方法列表。
	aaa authentication enable	定义 enable 认证的方法类型和执行顺序。
	aaa authentication dot1x	定义 802.1x 认证的方法类型和执行顺序。
	aaa authentication ppp	定义 PPP 认证的方法类型和执行顺序。
	aaa authentication sslvpn	设置 sslvpn 认证的方法类型和执行顺序。
	aaa authentication web-auth	设置 Web 认证的方法类型和执行顺序。
	aaa authentication iportal	设置内置 Web 认证的方法类型和执行顺序。
	aaa authentication general	定义 802.1x 认证、Web 认证、内置 Web 认证的通用方法
	aaa local authentication attempts	设置 login 用户尝试登录次数的最大值。
	aaa local authentication lockout-time	设置 login 用户被锁定的时间长度。
配置 AAA 授权	如果要对不同用户赋予不同的权限，限制用户可以使用的服务，则必须配置。	
	aaa new-model	开启 AAA。
	aaa authorization exec	定义 exec 授权的方法类型和执行顺序。
	aaa authorization commands	定义 command 授权的方法类型和执行顺序。
	aaa authorization network	为接入用户配置授权方法列表。
	authorization exec	在特定终端线路上应用 exec 授权方法。
	authorization commands	在特定终端线路上应用 command 授权方法。
配置 AAA 记账	如果要实现对用户使用网络资源情况的记账、统计和跟踪，则必须配置。	
	aaa new-model	开启 AAA。
	aaa accounting exec	定义 exec 记账的方法类型及方法执行顺序。
	aaa accounting commands	定义 command 记账的方法类型及方法执行顺序。
	aaa accounting network	定义 network 记账的方法类型及方法执行顺序。
	accounting exec	在特定终端线路上应用 exec 记账方法。
	accounting commands	在特定终端线路上应用 command 记账方法。
	aaa accounting update	开启记账更新功能。
	aaa accounting update periodic	设置记账更新时间间隔。
配置 AAA 服务器组	如果有多台服务器且需要能灵活选择服务器进行认证、授权和记账的处理，则建议配置。	
	aaa group server	创建 AAA 自定义服务器组。
	server	添加 AAA 服务器组成员。
配置基于域名的 AAA 服务	如果需要通过域来对接入的 802.1x 用户进行 AAA 管理，则必须配置。	
	aaa new-model	开启 AAA。

	aaa domain enable	开启基于域名的 AAA 服务。
	aaa domain	创建域，并进入域配置模式。
	authentication dot1x	在域中，关联 802.1x 认证方法列表。
	authentication ppp	在域中，关联 PPP 认证方法列表。
	authentication web-auth	在域中，关联 Web 认证方法列表。
	accounting network	在域中，关联 Network 记账方法列表。
	authorization network	在域中，关联 Network 授权方法列表。
	state	设置域的状态。
	username-format	设置是否在用户名中携带域名信息。
	access-limit	设置当前域可容纳接入用户的数目限制。
配置用户计费开始失败策略	**aaa accounting start-fail**	指定用户计费开始失败的策略
配置 AAA 心跳检测	**[no] aaa heartbeat enable**	指定是否开启 AAA 心跳检测
配置 AAA 日志打印功能	**[no] aaa log enable**	指定是否开启 AAA 日志打印功能
	aaa log rate-limit *num*	配置 AAA 日志打印速率
	aaa user-diag log-num	调整每个 AAA 用户可记录的轨迹条数
	aaa user-diag user-num	调整所有 AAA 用户轨迹记录总数

1.4.1 配置 AAA 认证

配置效果

验证用户是否可以获得访问权。

注意事项

- 如果在一个认证方案中使用多种认证方法，则认证方法的执行顺序为配置的先后顺序。只有在当前认证方法没有响应的情况下，才会采用下一种认证方法；如果当前认证方法认证失败，则不会跳转到下一个认证方案进行认证。
- 由于 none 方法使得请求接入的任何用户在所有认证方法都没有应答情况下能通过身份认证，所以仅将它作为备用的身份认证方法。

一般情况下，不使用 none 身份认证。在特殊情况（如所有可能的申请接入用户都是可信任的，而且用户的工作不允许有由于系统故障造成的耽搁），可以在安全服务器无应答的情况下，将 none 作为最后一种可选的身份认证方法，建议在 none 认证方法前加上本地身份认证方法。

- AAA 认证开启的情况下，如果没有配置任何方法且不存在 default 认证方法时，对于控制台允许不认证直接登录；其他接入都要进行 local 认证。
- 如果进入 CLI 界面的时候经过了 Login 身份认证（none 方法除外），将记录当前使用的用户名。此时，进行 Enable 认证的时候，将不再提示输入用户名，直接使用与 Login 认证相同的用户名进行认证，注意输入的口令要与之匹配。

- 如果进入 CLI 界面的时候没有进行 Login 认证，或在 Login 认证的时候使用了 none 方法，将不会记录用户名信息。此时，如果进行 enable 认证，将会要求重新输入用户名。该用户名信息不会被记录，每次进行 Enable 认证都要重新输入。

配置方法

开启 AAA

- 必须配置。
- 使用 **aaa new-model** 开启 AAA。
- 缺省情况下，没有启动 AAA。

定义 Login 认证的方法类型和执行顺序。

- 使用命令 **aaa authentication login** 配置 Login 认证的方法类型和执行顺序。
- 如果为 Login 接入用户配置认证方法列表（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置 Login 认证方法列表。

定义 Enable 认证的方法类型和执行顺序。

- 使用命令 **aaa authentication enable** 配置 Enable 认证的方法类型和执行顺序。
- 如果为 Enable 过程配置认证方法列表（只能配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置 Enable 认证方法列表。

定义 802.1x 认证的方法类型和执行顺序。

- 使用命令 **aaa authentication dot1x** 配置 Login 认证的方法类型和执行顺序。
- 如果为 802.1x 接入用户配置认证方法列表（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置 dot1x 认证方法列表。

定义 PPP 认证的方法类型和执行顺序。

- 使用命令 **aaa authentication ppp** 配置 ppp 认证的方法类型和执行顺序。
- 如果为 PPP 拨号用户配置认证方法列表，则必须配置此命令。
- 缺省情况下，没有配置 ppp 认证方法列表。

定义 Web 认证的方法类型和执行顺序。

- 使用命令 **aaa authentication web-auth** 配置 Web 认证的方法类型和执行顺序。
- 如果为 Web 认证用户配置认证方法列表（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置 Web 认证方法列表。

定义内置 Web 认证的方法类型和执行顺序。

- 使用命令 **aaa authentication iportal** 配置内置 Web 认证的方法类型和执行顺序。
- 如果为内置 Web 认证用户配置认证方法列表（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置内置 Web 认证方法列表。

↘ 定义 802.1x 认证、Web 认证、内置 Web 认证的方法类型和执行顺序。

- 使用命令 **aaa authentication general 为** 802.1x 认证、Web 认证、内置 Web 认证配置通用方法类型和执行顺序。
- 如果同时配置有 aaa authentication dot1x（或者 web-auth、iportal），将以 aaa authentication dot1x（或者 web-auth、iportal）优先选择。
- 缺省情况下，没有配置 general 认证方法列表

↘ 定义 SSLVPN 认证的方法类型和执行顺序。

- 使用命令 **aaa authentication sslvpn** 配置 Web 认证的方法类型和执行顺序。
- 如果为 SSLVPN 认证用户配置认证方法列表（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置 SSLVPN 认证方法列表。

↘ 设置 login 用户尝试登录次数的最大值。

- 可选配置。
- 缺省情况下，允许 login 用户尝试密码的失败次数为 3 次。

↘ 设置 login 用户被锁定的时间长度。

- 可选配置。
- 缺省情况下，当 login 用户尝试登录的次数超过最大值，被锁定的时间为 15 分钟。

检验方法

- 使用 show aaa method-list 查看已配置的方法列表信息。
- 使用 show aaa lockout 查看用户尝试登录失败次数的最大值和用户锁定的时间长度的配置信息。
- 使用 show running-config 查看 Login 认证、dot1x 认证关联认证方法列表的信息。

相关命令

↘ 开启 AAA

【命令格式】 **aaa new-model**
【参数说明】 无
【命令模式】 全局模式
【使用指导】 该命令是 AAA 的开启命令，如果要使用 AAA 安全服务，就必须使用 **aaa new-model** 开启 AAA 安全服务。如果没有启用 AAA，则所有 AAA 命令将是不可配置的。

定义 Login 认证的方法类型和执行顺序。

【命令格式】 **aaa authentication login** { **default** | *list-name* } *method1* [*method2*...]

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 Login 认证的默认方法。

list-name：定义一个 Login 认证的方法列表，可以是任何字符串。

method：必须是“local、none、group”所列关键字之一，一个方法列表最多有 4 个方法。

local：使用本地用户名数据库进行身份认证。

none：不进行身份认证。

group：使用服务器组进行身份认证，目前支持 RADIUS 和 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】 如果设备启用 AAA 登录认证安全服务，用户就必须使用 AAA 进行 Login 认证协商。必须使用 **aaa authentication login** 命令配置默认的或可选的方法列表用于 Login 认证。

只有前面的方法没有响应，才能使用后面的方法进行身份认证。

设置了 Login 认证方法后，必须将其应用在需要进行 Login 认证的终端线路上，否则将不生效。

定义 Enable 认证的方法类型和执行顺序

【命令格式】 **aaa authentication enable default** *method1* [*method2*...]

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 Enable 认证的默认方法。

list-name：定义一个 Enable 认证的方法列表，可以是任何字符串。

method：必须是“enable、local、none、group”所列关键字之一，一个方法列表最多有 4 个方法。

enable：使用 enable 命令配置的密码进行认证。

local：使用本地用户名数据库进行身份认证。

none：不进行身份认证。

group：使用服务器组进行身份认证，目前支持 RADIUS 和 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】

- 如果设备启用 AAA 登录认证安全服务，用户就必须使用 AAA 进行 Enable 认证协商。必须使用 **aaa authentication enable** 命令配置默认的或可选的方法列表用于 Enable 认证。
- 只有前面的方法没有响应，才能使用后面的方法进行身份认证。
- Enable 认证方法列表配置以后，Enable 认证功能自动生效。
- aaa 开启 enable local 认证时，认证权限无法超过 username 账号的权限等级。

定义 802.1x 认证的方法类型和执行顺序。

【命令格式】 **aaa authentication dot1x** { **default** | *list-name* } *method1* [*method2*...]

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 dot1x 认证的默认方法。

list-name：定义一个 dot1x 认证的方法列表，可以是任何字符串。

method：必须是“local、none、group”所列关键字之一，一个方法列表最多有 4 个方法。

local：使用本地用户名数据库进行身份认证。

none：不进行身份认证。

group：使用服务器组进行身份认证，目前支持 RADIUS 服务器组。

【命令模式】 全局模式

【使用指导】 如果设备启用 AAA 802.1x 安全服务，用户就必须使用 AAA 进行 802.1x 用户认证协商。必须使用 **aaa authentication dot1x** 命令配置默认的或可选的方法列表用于 802.1x 用户认证。

只有前面的方法没有响应，才能使用后面的方法进行认证。

↘ 定义 PPP、Web 认证、内置 Web 认证和 SSLVPN 认证的方法类型和执行顺序。

【命令格式】 **aaa authentication** { **ppp** | **web-auth** | **iportal** | **sslvpn** } { **default** | *list-name* } *method1* [*method2*...]

【参数说明】 **ppp**：配置 PPP 拨号认证的方法列表。

web-auth：配置 Web 认证的方法列表。

iportal：配置内置 Web 认证的方法列表。

sslvpn：配置 SSLVPN 认证的方法列表。

default：使用该参数，则后面定义的方法列表作为 PPP 认证的默认方法。

list-name：定义一个 PPP 认证的方法列表，可以是任何字符串。

method：必须是“local、none、group”所列关键字之一，一个方法列表最多有 4 个方法。

local：使用本地用户名数据库进行身份认证。

none：不进行身份认证。

group：使用服务器组进行身份认证，目前支持 RADIUS 服务器组。

【命令模式】 全局模式

【使用指导】 如果设备启用 AAA PPP 安全服务，用户就必须使用 AAA 进行 PPP 用户认证协商。必须使用 **aaa authentication ppp** 命令配置默认的或可选的方法列表用于 PPP 用户认证。

只有前面的方法没有响应，才能使用后面的方法进行认证。

↘ 定义 802.1x 认证、Web 认证、内置 Web 认证的通用方法

【命令格式】 **aaa authentication general** { **default** | *list-name* } *method1* [*method2*...]

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为所有前端的默认方法。

list-name：定义一个通用的方法列表，可以是任何字符串。

method：必须是“local、none、group”所列关键字之一，一个方法列表最多有 4 个方法。

local：使用本地用户名数据库进行身份认证。

none：不进行身份认证。

group：使用服务器组进行身份认证，目前支持 RADIUS 服务器组。

【命令模式】 全局模式

【使用指导】 该配置的方法是通用的，目前只对 802.1x 认证、Web 认证、内置 Web 认证前端业务生效。

只有前面的方法没有响应，才能使用后面的方法进行认证。

↘ 设置 login 用户尝试登录次数的最大值。

【命令格式】 **aaa local authentication attempts** *max-attempts*

【参数说明】 *max-attempts*：最大尝试失败次数，取值范围 1~2147483647

【命令模式】 全局模式

【使用指导】 该命令配置 Login 登录用户尝试登录失败次数。

↘ 设置 login 用户被锁定的时间长度。

【命令格式】 **aaa local authentication lockout-time** *lockout-time*

【参数说明】 *lockout-time*：锁定时间（单位：分钟），取值范围 1~43200

【命令模式】 全局模式

【使用指导】 配置 Login 登录用户尝试超过配置登录失败次数后被锁定的时间长度。

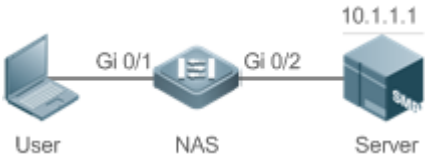
配置举例

以下配置举例，仅介绍与 AAA 认证相关的配置。

AAA Login 认证配置示例。对 Login 用户先用 RADIUS 服务器进行认证，在远程服务器没有响应的情况下转本地认证。

【网络环境】

图 1-5



【配置方法】 第一步：开启 AAA。

第二步：如果用户使用远程服务器认证，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 Local 认证，则需要在 NAS 上配置本地用户数据库信息。（本例需要配置 RADIUS 服务器和本地数据库信息）

第三步 :根据不同接入用户类型(本例为 Login 用户),配置 AAA 认证方法列表(本例的认证方法是先 RADIUS 认证，无响应后转 Local 认证)。

第四步：将方法应用于某个特定的接口或线路。如果使用的是 default 认证方法，则可以不必配置该步骤。

NAS

```
Hostname#configure terminal
Hostname(config)#username user password pass
Hostname(config)#aaa new-model
Hostname(config)#radius-server host 10.1.1.1
Hostname(config)#radius-server key Hostname
Hostname(config)#aaa authentication login list1 group radius local
Hostname(config)#line vty 0 20
Hostname(config-line)#login authentication list1
Hostname(config-line)#exit
```

【检验方法】 在 NAS 设备上，通过 **show aaa method-list** 命令查看配置效果。

NAS

```
Hostname#show aaa method-list

Authentication method-list:
aaa authentication login list1 group radius local

Accounting method-list:

Authorization method-list:
```

以 Telnet 用户为例，用户远程登录到 NAS 设备上，CLI 界面提示输入用户名/密码。

输入正确的用户名/密码，才能访问设备。

User

```
User Access Verification

Username:user
Password:pass
```

AAA enable 认证配置示例。对 enable 认证先使用 RADIUS 服务器进行认证，在远程服务器没有响应的情况下转本地认证，在本地认证用户名不存在的情况下转 enable 密码认证。

【网络环境】

图 1-6

【配置方法】 第一步：开启 AAA。

第二步：如果用户使用远程服务器认证，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 Local 认证，则需要在 NAS 上配置本地用户数据库信息。如果使用 enable 密码认证，则需要在 NAS 上配置 enable 认证密码。

第三步：根据不同接入用户类型，配置 AAA 认证方法列表。

Enable 认证方法列表全局只能定义一个，因此 Enable 认证不需要定义方法列表的名称，只要配置成默认的方法列表，配置以后，会自动被应用。

NAS

```
Hostname#configure terminal
Hostname(config)#username user privilege 15 password pass
Hostname(config)#enable secret w
Hostname(config)#aaa new-model
Hostname(config)#radius-server host 10.1.1.1
Hostname(config)#radius-server key Hostname
Hostname(config)#aaa authentication enable default group radius local enable
```

【检验方法】 在 NAS 设备上，通过 **show aaa method-list** 命令查看配置效果。

NAS

```
Hostname#show aaa method-list

Authentication method-list:
aaa authentication enable default group radius local enable

Accounting method-list:

Authorization method-list:
```

用户级别切换到 15 级，CLI 提示认证。输入正确的用户名/密码，才能访问设备。

NAS

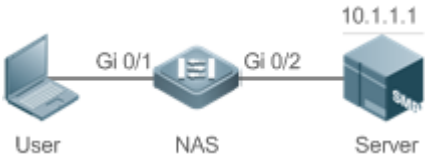
```
Hostname>enable
```

```
Username:user
Password:pass
Hostname#
```

↘ AAA 802.1x 认证配置示例。对 802.1x 接入用户先用 RADIUS 服务器进行认证，在远程服务器没有响应的情况下转本地认证。

【网络环境】

图 1-7



【配置方法】 第一步：开启 AAA。

第二步 :如果用户使用远程服务器认证 ,则需要先配置 RADIUS 服务器。如果使用 Local 认证 ,则需要在 NAS 上配置本地用户数据库信息。（本例需要配置 RADIUS 服务器和本地数据库信息）。目前，802.1x 认证不支持使用 TACACS+认证。

第三步：根据不同接入用户类型（本例为 802.1x 接入用户），配置 AAA 认证方法列表（本例的认证方法是先 RADIUS 认证，无响应后转 Local 认证）。

第四步：应用 AAA 认证方法。如果使用的是 default 认证方法，则可不必配置该步骤。

第五步：接口开启 802.1x 认证功能。

NAS

```
Hostname#configure terminal
Hostname(config)#username user1 password pass1
Hostname(config)#username user2 password pass2
Hostname(config)#aaa new-model
Hostname(config)#radius-server host 10.1.1.1
Hostname(config)#radius-server key Hostname
Hostname(config)#aaa authentication dot1x default group radius local
Hostname(config)#interface gigabitEthernet 0/1
Hostname(config-if-gigabitEthernet 0/1)#dot1 port-control auto
Hostname(config-if-gigabitEthernet 0/1)#exit
```

【检验方法】 在 NAS 设备上，通过 **show aaa method-list** 命令查看配置效果。

NAS

```
Hostname#show aaa method-list

Authentication method-list:
aaa authentication dot1x default group radius local

Accounting method-list:

Authorization method-list:
```

常见错误

- 没有配置 RADIUS 服务器或者 TACACS+服务器。
- 没有配置本地数据库用户名和密码。

1.4.2 配置 AAA 授权

配置效果

- 定义用户可以使用哪些服务或拥有哪些权限。

注意事项

- 关于 Exec 授权：Exec 授权通常结合 Login 认证一起使用，并可以在同一个线路上同时使用 Login 认证和 Exec 授权。但是要注意，由于授权和认证可以采用不同的方法和不同的服务器，因此对于相同的用户，认证和授权可能有不同的结果。用户登录时，如果 Exec 授权失败，即使已经通过了 Login 认证，也不能进入到 CLI 界面。
- 关于授权方法：如果在一个授权方案中使用多种授权模式，则授权模式的执行顺序为配置的先后顺序。只有在当前授权模式没有响应的情况下，才会采用下一种授权模式；如果当前授权模式失败，则不会采用下一种授权模式进行授权。
- 关于 Command 授权：Command 授权功能目前仅 TACACS+协议支持。
- 关于 Console 授权：设备支持区分通过控制台登录和其他终端登录的用户，可以设置控制台登录的用户，是否需要进行命令授权。如果关闭了控制台的命令授权功能，则已经应用到控制台线路的命令授权方法列表将不生效。

配置方法

开启 AAA

- 必须配置。
- 使用 **aaa new-model** 开启 AAA。
- 缺省情况下，没有启动 AAA。

定义 exec 授权的方法类型和执行顺序。

- 使用 **aaa authorization exec** 命令配置 exec 授权的方法类型和执行顺序。
- 如果要为 exec 用户配置授权方法列表（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置授权方法。

Exec 用户（控制台用户，可以通过 Console 口或者 Telnet 连接设备，每个连接称为一个 EXEC 用户，如 Telnet 用户、SSH 用户）的默认级别为最低权限的访问级别。

定义 command 授权的方法类型和执行顺序。

- 使用 **aaa authorization commands** 命令配置 command 授权的方法类型和执行顺序。
- 如果要为 command 授权配置授权方法列表（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置授权方法。

为接入用户配置授权方法列表。

- 使用 **aaa authorization network** 命令为接入用户配置认证方法列表。
- 如果要为 network 用户配置授权列表（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置授权方法。

在特定终端线路上应用 exec 授权方法。

- 使用 **authorization exec** (line 模式下)命令为特定终端线路上应用 exec 授权方法。
- 如果要在特定线路上应用指定的 exec 授权方法列表，则必须配置此命令。
- 缺省情况下，所有终端线路关联 default 授权方法列表。

在特定终端线路上应用 command 授权方法。

- 使用 **authorization commands** (line 模式下)命令为特定终端线路上应用 command 授权方法。
- 如果要在特定线路上应用指定的 command 授权方法列表，则必须配置此命令。
- 缺省情况下，所有终端线路关联 default 授权方法列表。

开启需要对配置模式下的命令进行授权。

- 使用 **aaa authorization config-commands** 命令开启需要对配置模式下的命令进行授权的功能。
- 缺省情况下，对配置模式下的命令不开启授权功能。

开启对控制台的用户执行的命令进行授权。

- 使用 **aaa authorization console** 命令开启对控制台的用户执行的命令进行授权的功能。
- 缺省情况下，不开启对控制台的用户执行的命令进行授权的功能。

检验方法

使用 **show running-config** 命令查看以上配置是否生效。

相关命令

开启 AAA。

【命令格式】 **aaa new-model**

【参数说明】 无

【命令模式】 全局模式

【使用指导】 该命令是 AAA 的开启命令，如果要使用 AAA 安全服务，就必须使用 **aaa new-model** 开启 AAA 安全服务。如果没有启用 AAA，则所有 AAA 命令将是不可配置的。

↘ 定义 exec 授权的方法类型和执行顺序。

【命令格式】 **aaa authorization exec** { **default** | *list-name* } *method1* [*method2*...]

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 exec 授权的默认方法。

list-name：定义一个 exec 授权的方法列表，可以是任何字符串。

method：必须是“local、none、group”所列关键字之一，一个方法列表最多有 4 个方法。

local：使用本地用户名数据库进行 exec 授权。

none：不进行 exec 授权。

group：使用服务器组进行 exec 授权，目前支持 RADIUS 和 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】 设备支持对登录到 NAS 的 CLI 界面的用户进行授权，赋予其 CLI 权限级别（0~15 级）。目前是对于通过了 Login 认证的用户，才进行 Exec 授权。如果 Exec 授权失败，则无法进入 CLI 界面。

配置了 Exec 授权方法后，必须将其应用在需要进行 Exec 授权的终端线路上，否则将不生效。

↘ 定义 command 授权的方法类型和执行顺序。

【命令格式】 **aaa authorization commands** *level* { **default** | *list-name* } *method1* [*method2*...]

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 command 授权的默认方法。

list-name：定义一个 command 授权的方法列表，可以是任何字符串。

method：必须是“none、group”所列关键字之一，一个方法列表最多有 4 个方法。

none：不进行 command 授权。

group：使用服务器组进行 command 授权，目前 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】 设备支持对用户可执行的命令进行授权，当用户输入并试图执行某条命令时，AAA 将该命令发送到安全服务器上，如果安全服务器允许执行该命令，则该命令被执行，否则该命令不执行，并会给出执行命令被拒绝的提示。

配置命令授权的时候需要指定命令的级别，该级别是命令的默认级别（例如，某命令对于 14 级以上用户可见，则该命令的默认级别就是 14 级的）。

配置了命令授权方法后，必须将其应用在需要进行命令授权的终端线路上，否则将不生效。

↘ 为接入用户配置授权方法列表。

【命令格式】 **aaa authorization network** { **default** | *list-name* } *method1* [*method2*...]

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 network 授权的默认方法。

list-name：定义一个 network 授权的方法列表，可以是任何字符串。

method：必须是“none、group”所列关键字之一，一个方法列表最多有 4 个方法。

none：不进行身份认证。

group：使用服务器组进行 network 授权，目前支持 RADIUS 和 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】 设备支持对所有网络有关的服务请求如 PPP、SLIP 等协议进行授权。如果配置了授权，则对所有的认证用户或接口自动进行授权。

可以指定三种不同的授权方法，与身份认证一样，只有当前的授权方法没有响应，才能继续使用后面的方法进行授权，如果当前授权方法失败，则不再使用其他后继的授权方法。

RADIUS 或 TACACS+服务器是通过返回一系列的属性对来完成对认证用户的授权。所以网络授权是建立在认证的基础上的，只有认证通过了才有可能获取网络授权。

↘ 开启对配置模式（包括全局配置模式及其子模式）下的命令进行授权的功能。

【命令格式】 **aaa authorization config-commands**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 如果只对非配置模式（如特权模式）下的命令进行授权，可以使用该命令的 **no** 模式关闭配置模式的授权功能，则配置模式及其子模式下的命令不需要进行命令授权即可执行。

↘ 开启对通过控制台登录的用户所执行的命令进行授权的功能。

【命令格式】 **aaa authorization console**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 设备支持区分通过控制台登录和其他终端登录的用户，可以设置控制台登录的用户，是否需要进行命令授权。如果关闭了控制台的命令授权功能，则已经应用到控制台线路的命令授权方法列表将不生效。

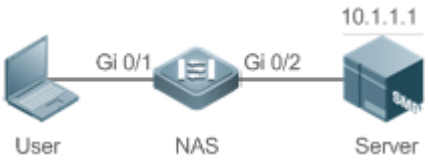
配置举例

以下配置举例，仅介绍与 AAA 授权相关的配置。

↘ 配置 AAA exec 授权。VTY 线路 0~4 上的用户登录时采用 Login 认证，并且进行 exec 授权。其中 Login 认证采用本地认证，exec 授权先采用 RADIUS，如果没有响应可以采用本地授权。

【网络环境】

图 1-8



【配置方法】 第一步：开启 AAA。

第二步：如果用户使用远程服务器授权，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 local 授权，则需要在 NAS 上配置本地用户数据库信息。

第三步：根据不同接入方式和服务类型，配置 AAA 授权方法列表。

第四步：将方法应用于某个特定的接口或线路。如果使用的是 default 认证方法，则可以不必配置该步骤。

Exec 授权通常结合 Login 认证一起使用，并可以在同一个线路上同时使用 Login 认证和 Exec 授权。

NAS

```
Hostname#configure terminal
Hostname(config)#username user password pass
```

```
Hostname(config)#username user privilege 6
Hostname(config)#aaa new-model
Hostname(config)#radius-server host 10.1.1.1
Hostname(config)#radius-server key test
Hostname(config)#aaa authentication login list1 group radius local
Hostname(config)#aaa authorization exec list2 group radius local
Hostname(config)#line vty 0 4
Hostname(config-line)#login authentication list1
Hostname(config-line)#authorization exec list2
Hostname(config-line)#exit
```

【检验方法】 在 NAS 设备上，通过 **show run、show aaa method-list** 命令查看配置效果。

NAS

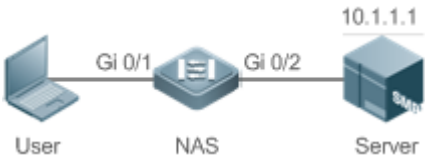
```
Hostname#show aaa method-list

Authentication method-list:
aaa authentication login list1 group radius local

Accounting method-list:

Authorization method-list:
aaa authorization exec list2 group radius local
```

```
Hostname# show running-config
aaa new-model
!
aaa authorization exec list2 group local
aaa authentication login list1 group radius local
!
username user password pass
username user privilege 6
!
radius-server host 10.1.1.1
radius-server key 7 093b100133
!
line con 0
line vty 0 4
 authorization exec list2
 login authentication list1
!
End
```

↘ 配置 Command 授权。为 Login 用户设置命令授权，应用 default 授权方法：对 15 级命令进行授权，先使用 tacacs+服务器授权，无响应后转 local 授权。授权同时应用于控制台登录用户和其他终端登录的用户。

【网络环境】

图 1-9



【配置方法】 第一步：开启 AAA。

第二步：如果用户使用远程服务器授权，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 local 授权，则需要在 NAS 上配置本地用户数据库信息。

第三步：根据不同接入方式和服务类型，配置 AAA 授权方法列表。

第四步：将方法应用于某个特定的接口或线路。如果使用的是 default 认证方法，则可以不必配置该步骤。

NAS

```
Hostname#configure terminal
Hostname(config)#username user1 password pass1
Hostname(config)#username user1 privilege 15
Hostname(config)#aaa new-model
Hostname(config)#tacacs-server host 192.168.217.10
Hostname(config)#tacacs-server key aaa
Hostname(config)#aaa authentication login default local
Hostname(config)#aaa authorization commands 15 default group tacacs+ local
Hostname(config)#aaa authorization console
```

【检验方法】 在 NAS 设备上，通过 **show run、show aaa method-list** 命令查看配置效果。

NAS

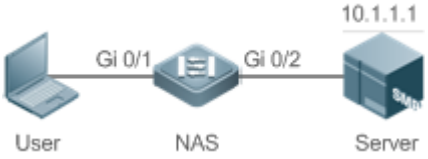
```
Hostname#show aaa method-list

Authentication method-list:
aaa authentication login default local

Accounting method-list:

Authorization method-list:
aaa authorization commands 15 default group tacacs+ local
```

```
Hostname#show run
!
aaa new-model
!
aaa authorization console
aaa authorization commands 15 default group tacacs+ local
aaa authentication login default local
!
!
```

```
nfpp
!
vlan 1
!
username user1 password 0 pass1
username user1 privilege 15
no service password-encryption
!
tacacs-server host 192.168.217.10
tacacs-server key aaa
!
line con 0
line vty 0 4
!
!
end
```

配置 Network 授权。

【网络环境】
图 1-10



【配置方法】 第一步：开启 AAA。
第二步：如果用户使用远程服务器授权，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 local 授权，则需要在 NAS 上配置本地用户数据库信息。
第三步：根据不同接入方式和服务类型，配置 AAA 授权方法列表。
第四步：将方法应用于某个特定的接口或线路。如果使用的是 default 认证方法，则可以不必配置该步骤。

NAS

```
Hostname#configure terminal
Hostname(config)#aaa new-model
Hostname(config)#radius-server host 10.1.1.1
Hostname(config)#radius-server key test
Hostname(config)#aaa authorization network default group radius none
Hostname(config)#end
```

【检验方法】 在 NAS 设备上，通过 **show aaa method-list** 命令查看配置效果。

NAS

```
Hostname#show aaa method-list

Authentication method-list:
```

```
Accounting method-list:

Authorization method-list:
aaa authorization network default group radius none
```

常见配置错误

无

1.4.3 配置 AAA 记账

配置效果

- 记录用户使用网络资源的情况。
- 记录用户进行设备管理时登入登出的过程、记录执行过的命令。

注意事项

关于记账方法：

- 如果在一个记账方案中使用多种记账模式，则记账模式的执行顺序为配置的先后顺序。只有在当前记账模式没有响应的情况下，才会采用下一种记账模式；如果当前记账模式失败，则不会采用下一种记账模式进行记账。
- 默认的记账方法（default 方法）列表一旦配置，将自动应用到所有终端上。在线路上应用非默认记账方法列表，将取代默认的方法列表。如果试图应用未定义的方法列表，则会给出一个警告提示信息，该线路上的记账将不会生效，直至定义了该记账方法列表才会生效。

关于 Exec 记账：

- 只有登录到 NAS 的用户终端通过了 Login 认证，才会进行 exec 记账。如果没有设置 Login 认证，或者认证时候采用了 none 方法，则不会进行 exec 记账。针对同一个用户终端的登录，登入时如果没有进行过 Start 记账，登出时也就不会进行 Stop 记账。

关于 Command 记账：

- Command 记账功能目前仅 TACACS+协议支持。

配置方法

↘ 开启 AAA。

- 必须配置。
- 使用 **aaa new-model** 开启 AAA。

- 缺省情况下，没有启动 AAA。

定义 exec 记账的方法类型及方法执行顺序。

- 使用命令 **aaa accounting exec** 配置 exec 记账的方法类型及方法执行顺序。
- 如果要为 exec 用户配置记账方法（包括配置 default 方法列表），则必须配置此命令。
- Exec 用户（控制台用户，可以通过 Console 口或者 Telnet 连接设备，每个连接称为一个 EXEC 用户，如 Telnet 用户、SSH 用户）的默认级别为最低权限的访问级别。
- 缺省情况下，没有配置记账方法。

定义 command 记账的方法类型及方法执行顺序。

- 使用命令 **aaa accounting commands** 配置 command 记账的方法类型及方法执行顺序。
- 如果要为 command 记账配置记账方法（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置记账方法。命令记账功能目前仅 TACACS+协议支持。

定义 network 记账的方法类型及方法执行顺序。

- 使用命令 **aaa accounting network** 配置 network 记账的方法类型及方法执行顺序。
- 如果要为 network 用户配置记账方法（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置记账方法。

在特定终端线路上应用 exec 记账方法。

- 使用命令 **accounting exec**(line 模式下)配置在特定终端线路上应用 exec 记账方法。
- 如果要在特定线路上应用指定的 exec 记账方法列表，则必须配置此命令。
- 如果应用的是 default 方法列表，则可不必配置此命令。
- 缺省情况下，所有终端线路关联 default 方法列表。

在特定终端线路上应用 command 记账方法。

- 使用命令 **accounting commands**(line 模式下)配置在特定终端线路上应用 command 记账方法。
- 如果要在特定线路上应用指定的 command 记账方法列表，则必须配置此命令。
- 如果应用的是 default 方法列表，则可不必配置此命令。
- 缺省情况下，所有终端线路关联 default 方法列表。

802.1x 应用 network 记账方法

- 使用命令 **dot1x accounting network** 命令配置 802.1x 的 network 记账方法。
- 如果要指定 802.1x 记账方法，则必须配置此命令。
- 如果应用的是 default 方法列表，则可不必配置此命令。
- 缺省情况下，关联 default 方法列表。

↘ 开启记账更新功能。

- 可选配置。
- 该功能有助于提高记账准确性，建议配置。
- 缺省情况下，记账更新功能关闭。

↘ 设置记账更新时间间隔。

- 可选配置。
- 除非有明确要求，否则不建议配置。

检验方法

使用 **show running-config** 命令查看配置是否生效。

相关命令

↘ 开启 AAA。

【命令格式】 **aaa new-model**

【参数说明】 无

【命令模式】 全局模式

【使用指导】 该命令是 AAA 的开启命令，如果要使用 AAA 安全服务，就必须使用 **aaa new-model** 开启 AAA 安全服务。如果没有启用 AAA，则所有 AAA 命令将是不可配置的。

↘ 定义 exec 记账的方法类型及方法执行顺序。

【命令格式】 **aaa accounting exec** { **default** | *list-name* } **start-stop** *method1* [*method2*...]

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 exec 记账的默认方法。

list-name：定义一个 exec 记账的方法列表，可以是任何字符串。

method：必须是“none、group”所列关键字之一，一个方法列表最多有 4 个方法。

none：不进行 exec 记账。

group：使用服务器组进行 exec 记账，目前支持 RADIUS 和 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】 设备只有在用户通过了登录认证后，才会启用 Exec 记账功能，如果用户登录时未进行认证或认证采用的方法为 none，则不会进行 Exec 记账。

启用记账功能后，在用户登录到 NAS 的 CLI 界面时候，发送记账开始（Start）信息给安全服务器，在用户退出登录的时候，发送记账结束（Stop）信息给安全服务器。如果一个用户在登录时没有发出 Start 信息，在退出登录时也不会发出 Stop 信息。

配置了 Exec 记账方法后，必须将其应用在需要进行命令记账的终端线路上，否则将不生效。

↘ 定义 command 记账的方法类型及方法执行顺序。

【命令格式】 **aaa accounting commands** *level* { **default** | *list-name* } **start-stop** *method1* [*method2*...]

【参数说明】 *level*：要进行记账的命令级别，范围 0~15，决定哪个级别的命令执行时，需要记录信息。

default：使用该参数，则后面定义的方法列表作为 command 记账的默认方法。

list-name：定义一个 command 记账的方法列表，可以是任何字符串。

method：必须是“none、group”所列关键字之一，一个方法列表最多有 4 个方法。

none：不进行 command 记账。

group：使用服务器组进行 command 记账，目前支持 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】 设备只有在用户通过了登录认证后，才会启用命令记账功能，如果用户登录时未进行认证或认证采用的方法为 none，则不会进行命令记账。启用记账功能后，在用户每次执行指定级别的命令后，将所执行的命令信息，发送给安全服务器。

配置了命令记账方法后，必须将其应用在需要进行命令记账的终端线路上，否则将不生效。

↘ 定义 network 记账的方法类型及方法执行顺序。

【命令格式】 **aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 network 记账的默认方法。

list-name：定义一个 command 记账的方法列表，可以是任何字符串。

start-stop：在用户访问活动开始和结束时均发送记账报文，开始记账报文无论是否成功启用记账，都允许用户开始进行网络访问。

method：必须是“none、group”所列关键字之一，一个方法列表最多有 4 个方法。

none：不进行 network 记账。

group：使用服务器组进行 network 记账，目前支持 RADIUS 和 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】 设备通过给安全服务器发送记录属性对来用户活动进行记账。使用关键字 **start-stop**，制定用户记账选项。

↘ 开启记账更新功能。

【命令格式】 **aaa accounting update**

【参数说明】 无

【命令模式】 全局模式

【使用指导】 如果没有启用 AAA 安全服务，则不能使用记账更新。如果已经启用 AAA 安全服务，则该命令用设置记账更新功能。

↘ 设置记账更新时间间隔。

【命令格式】 **aaa accounting update periodic** *interval*

【参数说明】 *interval*：记账更新间隔，以分钟为单位，取值范围为 1~525600。

【命令模式】 全局模式

【使用指导】 如果没有启用 AAA 安全服务，则不能使用记账更新。如果已经启用 AAA 安全服务，则该命令用设置记账更新间隔。

配置举例

以下配置举例，仅介绍与 AAA 记账相关的配置。

配置 AAA exec 记账。VTY 线路 0~4 上的用户登录时采用 Login 认证，并且进行 exec 记账。其中 Login 认证采用本地认证，exec 记账采用 RADIUS 记账。

【网络环境】

图 1-11

【配置方法】 第一步：开启 AAA。

第二步：如果用户使用远程服务器记账，则需要先配置 RADIUS 或 TACACS+服务器。

第三步：根据不同接入方式和服务类型，配置 AAA 记账方法列表。

第四步：将方法应用于某个特定的接口或线路。如果使用的是 default 认证方法，则可以不必配置该步骤。

NAS

```
Hostname#configure terminal
Hostname(config)#username user password pass
Hostname(config)#aaa new-model
Hostname(config)#radius-server host 10.1.1.1
Hostname(config)#radius-server key test
Hostname(config)#aaa authentication login list1 group radius local
Hostname(config)#aaa accounting exec list3 start-stop group radius
Hostname(config)#line vty 0 4
Hostname(config-line)#login authentication list1
Hostname(config-line)#accounting exec list3
Hostname(config-line)#exit
```

【检验方法】 在 NAS 设备上，通过 **show run**、**show aaa method-list** 命令查看配置效果。

NAS

```
Hostname#show aaa method-list

Authentication method-list:
aaa authentication login list1 group radius local

Accounting method-list:
aaa accounting exec list3 start-stop group radius
Authorization method-list:
```

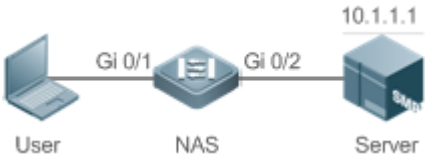
```
Hostname# show running-config
aaa new-model
!
aaa accounting execlist3 start-stop group radius
aaa authentication login list1 group local
!
```

```
username user password  pass
!
radius-server host 10.1.1.1
radius-server key 7 093b100133
!
line con 0
line vty 0 4
 accounting  exec list3
 login authentication list1
!
End
```

配置 command 记账。为 Login 用户设置命令记账 ,应用 default 记账方法。其中 Login 认证采用本地认证 ,使用 tacacs+ 服务器记账。

【网络环境】

图 1-12



【配置方法】 第一步：开启 AAA。

第二步：如果用户使用远程服务器记账，则需要先配置 RADIUS 或 TACACS+服务器。

第三步：根据不同接入方式和服务类型，配置 AAA 记账方法列表。

第四步：将方法应用于某个特定的接口或线路。如果使用的是 default 认证方法，则可以不必配置该步骤。

NAS

```
Hostname#configure terminal
Hostname(config)#username user1 password pass1
Hostname(config)#username user1 privilege 15
Hostname(config)#aaa new-model
Hostname(config)#tacacs-server host 192.168.217.10
Hostname(config)#tacacs-server key aaa
Hostname(config)#aaa authentication login default local
Hostname(config)#aaa accounting commands 15 default start-stop group tacacs+
```

【检验方法】 在 NAS 设备上，通过 show 命令查看配置效果。

NAS

```
Hostname#show aaa method-list

Authentication method-list:
aaa authentication login default local

Accounting method-list:
```

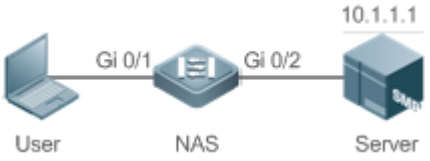
```
aaa accounting commands 15 default start-stop group tacacs+
Authorization method-list:
```

```
Hostname#show run
!
aaa new-model
!
aaa authorization config-commands
aaa accounting commands 15 default start-stop group tacacs+
aaa authentication login default local
!
!
nfpp
!
vlan 1
!
username user1 password 0 pass1
username user1 privilege 15
no service password-encryption
!
tacacs-server host 192.168.217.10
tacacs-server key aaa
!
line con 0
line vty 0 4
!
!
end
```

↘ 配置 network 记账。为 802.1x 用户配置记账方法列表，采用 RADIUS 远程服务器认证和记账。

【网络环境】

图 1-13



【配置方法】 第一步：开启 AAA。

第二步：如果用户使用远程服务器记账，则需要先配置 RADIUS 服务器。

第三步：根据不同接入方式和服务类型，配置 AAA 方法列表。

第四步：应用方法列表。如果使用的是 default 认证方法，则可以不必配置该步骤。

802.1x 用户在认证通过后才能进行记账。

NAS

```
Hostname#configure terminal
Hostname(config)#username user password pass
Hostname(config)#aaa new-model
Hostname(config)#radius-server host 10.1.1.1
Hostname(config)#radius-server key test
Hostname(config)#aaa authentication dot1x aut1x group radius local
Hostname(config)#aaa accounting network acc1x start-stop group radius
Hostname(config)#dot1x authentication aut1x
Hostname(config)#dot1x accounting acc1x
Hostname(config)#interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#dot1 port-control auto
Hostname(config-if-GigabitEthernet 0/1)#exit
```

【检验方法】 在 NAS 设备上，通过 show 命令查看配置效果。

NAS

```
Hostname#show aaa method-list

Authentication method-list:
aaa authentication dot1x aut1x group radius local
Accounting method-list:
aaa accounting network acc1x start-stop group radius
Authorization method-list:
```

常见配置错误

无

1.4.4 配置 AAA 服务器组

配置效果

- 创建自定义服务器组，每个服务器组可添加一台或多台服务器。
- 配置认证、授权、记账方法列表时，引用服务器组的组名作为认证、授权、记账方法，则表示在进行认证、授权、记账请求时使用该服务器组中的服务器。
- 使用自定义服务器组可以实现认证、授权、记账相分离。

注意事项

在自定义服务器组中，只能指定并应用默认服务器组中的服务器。

配置方法

↘ 创建 AAA 自定义服务器组。

- 必选配置
- 在创建自定义服务组名的时候，组名尽可能有明确的含义。不可以使用预定义的关键字”radius”和 “tacacs+”。

↘ 添加 AAA 服务器组成员。

- 必选配置
- 使用 sever 命令添加 AAA 服务器组的成员。
- 缺省情况下，自定义组中没有添加服务器。

检验方法

使用命令 **show aaa group** 查看配置的服务器组信息。

相关命令

↘ 创建 AAA 自定义服务器组。

【命令格式】 **aaa group server** { **radius** | **tacacs+** } *name*

【参数说明】 *name*：服务器组的取名，目前不能为关键字“radius” ，“tacacs+” ，因为这是 RADIUS 和 TACACS+默认的服务器组名称。

【命令模式】 全局模式

【使用指导】 该命令配置 AAA 服务器组，目前支持 RADIUS 和 TACACS+服务器组。

↘ 添加 AAA 服务器组成员。

【命令格式】 **server** *ip-addr* [**auth-port** *port1*] [**acct-port** *port2*]

【参数说明】 *ip-addr*：服务器 IP 地址

port1：服务器认证端口（仅 RADIUS 服务器组支持）

port2：服务器记账端口（仅 RADIUS 服务器组支持）

【命令模式】 服务器组配置模式

【使用指导】 往指定服务器中添加服务器，不指定端口时使用默认值。

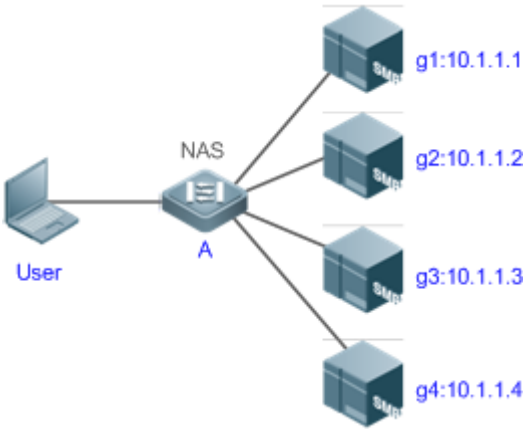
配置举例

以下配置举例，仅介绍与 AAA 服务器组相关的配置。

↘ 创建 AAA 自定义服务器组。RADIUS 服务器组 g1、g2，其中 g1 组的服务器的 IP 为 10.1.1.1 和 10.1.1.2，g2 组的服务器的 IP 为 10.1.1.3 和 10.1.1.4。

【网络环境】

图 1-14



【前置任务】 1，网络中已经完成了接口、IP 地址、Vlan 的配置，网络连通，NAS 设备到服务器的路由可达。

2，启用 AAA 服务。

【配置方法】 第一步：配置服务器（该服务器属于默认服务器组）

第二步：创建 AAA 自定义服务器组

第三步：在自定义服务器组中添加服务器组成员

NAS

```
Hostname#configure terminal
Hostname(config)#radius-server host 10.1.1.1
Hostname(config)#radius-server host 10.1.1.2
Hostname(config)#radius-server host 10.1.1.3
Hostname(config)#radius-server host 10.1.1.4
Hostname(config)#radius-server key secret
Hostname(config)#aaa group server radius g1
Hostname(config-gs-radius)#server 10.1.1.1
Hostname(config-gs-radius)#server 10.1.1.2
Hostname(config-gs-radius)#exit
Hostname(config)#aaa group server radius g2
Hostname(config-gs-radius)#server 10.1.1.3
Hostname(config-gs-radius)#server 10.1.1.4
Hostname(config-gs-radius)#exit
```

【检验方法】 在 NAS 设备上，通过 show aaa group、show run 命令查看配置效果。

NAS

```
Hostname#show aaa group
Type        Reference  Name
----------  ---------- ----------
radius      1          radius
tacacs+     1          tacacs+
```

```
radius     1          g1
radius     1          g2
```

```
Hostname#show run
!
radius-server host 10.1.1.1
radius-server host 10.1.1.2
radius-server host 10.1.1.3
radius-server host 10.1.1.4
radius-server key secret
!
aaa group server radius g1
 server 10.1.1.1
 server 10.1.1.2
!
aaa group server radius g2
 server 10.1.1.3
 server 10.1.1.4
!
!
```

常见配置错误

- 对于使用非默认认证、记账端口的 RADIUS 服务器，在使用命令 server 添加服务器时要同时指定认证端口或记账端口。

1.4.5 配置基于域名的 AAA 服务

配置效果

针对不同域的 802.1x 用户，创建认证、授权和记账方案，以及本地登录用户的认证方案。

注意事项

关于域中引用方法列表：

- 在域配置模式下，选择 AAA 服务方法列表时，这些方法列表是在进入域配置模式前已经定义；否则在域配置模式下，允许选择 AAA 方法列表名，但提示配置不存在。
- 域选择的 AAA 服务方法列表名称必须和 AAA 服务所定义的方法列表名称必须一致。若不一致，不能够为该域中的用户提供合适的 AAA 服务。

关于缺省域：

- 缺省域（default）：在基于域名的 AAA 服务开关打开情况下，如果用户没有携带域信息，则使用缺省域。如果用户携带的域在系统中没有配置，则判定为非法用户，不提供 AAA 服务。初始时没有配置 default 域，需要手工指定创建。
- 基于域名的 AAA 服务开关打开时，默认情况下没有配置缺省域，需要手动配置完成。缺省域的名称为“default”，若配置缺省域后，用户不携带域信息时，使用缺省域进行提供 AAA 服务。若缺省域没有配置，则未携带域信息的用户不能使用 AAA 服务。

关于域名：

- 用户所携带的域名称与设备上所配置的域名的匹配采用最准确匹配。例如：设备上配置了 domain.com 和 domain.com.cn 两个域，一个用户的请求信息携带为 aaa@domain.com。则设备认为会判定该用户所属于的域为 domain.com 而不是域 domain.com.cn。
- 如果认证用户携带有域信息，而域没有在设备上配置，不能为该用户提供 AAA 服务。

配置方法

开启 AAA。

- 必须配置。
- 使用 **aaa new-model** 开启 AAA。
- 缺省情况下，没有启动 AAA。

开启基于域名的 AAA 服务。

- 必选配置。
- 使用 **aaa domain enable** 开启基于域名的 AAA 服务。
- 缺省情况下，基于域名的 AAA 服务关闭。

创建域，并进入域配置模式。

- 必选配置。
- 使用 **aaa domain** 命令创建域或者进入已配置的域。
- 缺省情况下，没有配置任何域。

在域中，关联 802.1x 认证方法列表。

- 使用 **authentication dot1x** 命令关联 802.1x 认证方法列表。
- 如果要在域中应用指定的 802.1x 认证方法，则必须配置此命令。
- 目前基于域名的 AAA 服务，仅被应用于 802.1x 接入服务。

在域中，关联 PPP、Web 认证方法列表。

- 使用 **authentication ppp** 命令关联 PPP 认证方法列表。
- 使用 **authentication Web** 命令关联 Web 认证方法列表。

- 如果要在域中应用指定的 PPP 或 Web 认证方法，则必须配置此命令。
- 如果域中没有关联方法列表，则默认使用全局的 default 方法列表进行认证。

↘ 在域中，关联 Network 记账方法列表。

- 使用 **accounting network** 命令关联 network 记账方法列表。
- 如果要在域中应用指定的记账方法，则必须配置此命令。
- 如果域中没有关联方法列表，则默认使用全局的 default 方法列表进行记账。

↘ 在域中，关联 Network 授权方法列表。

- 使用 **authorization network** 命令关联 network 授权方法列表。
- 如果要在域中应用指定的授权方法，则必须配置此命令。
- 如果域中没有关联方法列表，则默认使用全局的 default 方法列表进行授权。

↘ 设置域的状态。

- 可选配置
- 当域的状态为 block 时，属于该域的用户不能登录。
- 缺省情况下，当域被创建以后，其状态为 active，即允许任何属于该域的用户请求网络服务。

↘ 设置是否在用户名中携带域名信息。

- 可选配置
- 缺省情况下，NAS 与服务器交互时用户名中携带域信息。

↘ 设置当前域可容纳接入用户的数目限制。

- 可选配置
- 缺省情况下，不对当前域可容纳的接入用户数作限制。

检验方法

使用命令 **show aaa domain** 查看配置的域信息是否生效。

相关命令

↘ 开启 AAA。

【命令格式】 **aaa new-model**
【参数说明】 无
【命令模式】 全局模式

【使用指导】 该命令是 AAA 的开启命令，如果要使用 AAA 安全服务，就必须使用 **aaa new-model** 开启 AAA 安全服务。如果没有启用 AAA，则所有 AAA 命令将是不可配置的。

↘ 开启基于域名的 AAA 服务。

【命令格式】 **aaa domain enable**

【参数说明】 无

【命令模式】 全局模式

【使用指导】 1、进行基于域名的 AAA 服务配置，需要打开该配置开关。

2、如果设备上已经有认证在线用户，开启或者关闭本功能可能导致用户记账异常。若出现用户记账异常，可通过以下方式恢复：

1）使用命令 **clear dot1x user all** 触发 802.1x 认证用户自动重认证。

2）使用命令 **clear web-auth user all** 命令将 Web 认证用户踢下线后，用户再通过手工认证上线。

↘ 创建域，并进入域配置模式。

【命令格式】 **aaa domain** { **default** | *domain-name* }

【参数说明】 **default**：使用该参数，进行缺省域的配置

domain-name：指定域的名称

【命令模式】 全局模式

【使用指导】 指定基于域名的 AAA 服务配置。default 为缺省域配置，也就是如果用户没有携带域信息，网络设备所使用的方法列表。*domain-name* 为指定域名配置，如果用户携带该域名，则指定使用该域所关联的方法列表。目前系统支持最多配置 32 个域。

↘ 在域中，关联 802.1x 认证方法列表。

【命令格式】 **authentication dot1x** { **default** | *list-name* }

【参数说明】 **default**：使用该参数，指定使用缺省配置方法列表

list-name：指定方法列表名称

【命令模式】 域配置模式

【使用指导】 为域指定一个 802.1x 认证方法列表。

↘ 在域中，关联 PPP 认证方法列表。

【命令格式】 **authentication ppp** { **default** | *list-name* }

【参数说明】 **default**：使用该参数，指定使用缺省配置方法列表

list-name：指定方法列表名称

【命令模式】 域配置模式

【使用指导】 为域指定一个 PPP 认证方法列表。

↘ 在域中，关联 Web 认证方法列表。

【命令格式】 **authentication web-auth** { **default** | *list-name* }

【参数说明】 **default**：使用该参数，指定使用缺省配置方法列表

list-name：指定方法列表名称

【命令模式】 域配置模式

【使用指导】 为域指定一个 webauth 认证方法列表。

在域中，关联 Network 记账方法列表。

【命令格式】 **accounting network** { **default** | *list-name* }
【参数说明】 **default**：使用该参数，指定使用缺省配置方法列表
list-name：指定方法列表名称
【命令模式】 域配置模式
【使用指导】 为域指定使用的 Network 记账方法列表。

在域中，关联 Network 授权方法列表。

【命令格式】 **authorization network** { **default** | *list-name* }
【参数说明】 **default**：使用该参数，指定使用缺省配置方法列表
list-name：指定方法列表名称
【命令模式】 域配置模式
【使用指导】

设置域的状态。

【命令格式】 **state** { **block** | **active** }
【参数说明】 **block**：配置的域无效
active：配置的域有效
【命令模式】 域配置模式
【使用指导】 指定配置的域是否有效。

设置是否在用户名中携带域名信息。

【命令格式】 **username-format** { **without-domain** | **with-domain** }
【参数说明】 **without-domain**：剥离域信息
with-domain：不剥离域信息
【命令模式】 域配置模式
【使用指导】 在域配置模式下，配置 NAS 针对指定域与服务器交互时，用户名中是否携带域信息。

设置当前域可容纳接入用户的数目。

【命令格式】 **access-limit** *num*
【参数说明】 *num*：域用户的数量限制，只限制 802.1x 用户
【命令模式】 域配置模式
【使用指导】 使用该命令对域的用户数量进行限制。

配置举例

以下配置举例，仅介绍与多域 AAA 相关的配置。

↘ 配置基于域的 AAA 认证记账服务。实现使用 RADIUS 服务器对通过 NAS 接入的 802.1x 域用户（用户名为 user@domain.com）进行认证和记账。NAS 向服务器发送的用户名不携带域名，不限制接入用户数。

【网络环境】

图 1-15

【配置方法】 本例使用 RADIUS 认证和记账，需要提前配置 RADIUS 服务器。

第一步：开启 AAA

第二步：定义 AAA 服务的方法列表

第三步：开启基于域名的 AAA 服务

第四步：创建域

第五步：在指定域中关联 AAA 方法列表

第六步：设置域属性

NAS

```
Hostname#configure terminal
Hostname(config)#aaa new-model
Hostname(config)#radius-server host 10.1.1.1
Hostname(config)#radius-server key test
Hostname(config)#aaa authentication dot1x default group radius
Hostname(config)#aaa accounting network list3 start-stop group radius
Hostname(config)# aaa domain enable
Hostname(config)# aaa domain domain.com
Hostname(config-aaa-domain)# authentication dot1x default
Hostname(config-aaa-domain)#accounting  networklist3
Hostname(config-aaa-domain)# username-format without-domain
```

【检验方法】 在 NAS 设备上，通过 **show run**、**show aaa domain** 命令查看配置效果。

NAS

```
Hostname#show aaa domain domain.com

=============Domain domain.com=============
State: Active
Username format: With-domain
Access limit: No limit
802.1X Access statistic: 0

Selected method list:
 authentication dot1x default
 accounting network list3
```

```
Hostname#show run
```

```
Building configuration...
Current configuration : 1449 bytes
version RGOS 10.4(3) Release(101069)(Wed Oct 20 09:12:40 CST 2010 -ngcf67)
co-operate enable
!
aaa new-model
aaa domain enable
!
aaa domain domain.com
 authentication dot1x default
 accounting network list3
!
aaa accounting network list3 start-stop group radius
aaa authentication dot1x default group radius
!
nfpp
!
no service password-encryption
!
radius-server host 10.1.1.1
radius-server key test
!
line con 0
line vty 0 4
!
end
```

常见配置错误

无

1.4.6 配置用户计费开始失败策略

配置效果

- 可以指定用户计费开始失败的策略。

注意事项

根据需要指定用户计费开始失败的策略。

配置方法

配置用户计费开始失败的策略。

- 可选配置。
- 缺省情况下，不指定用户计费开始失败的策略，即保持默认的计费开始失败策略。

检验方法

使用命令 **show run** 查看配置信息。

相关命令

配置用户计费开始失败的策略。

【命令格式】 **aaa accounting start-fail** { **online** | **offline** }

【参数说明】 **online**：计费开始失败策略为上线

offline：计费开始失败策略为下线

【命令模式】 全局模式

【使用指导】 该命令指定用户计费开始失败的策略。

配置举例

以下配置举例，仅介绍与指定用户计费开始失败策略相关的配置。

指定用户计费开始失败的策略。

【网络环境】

【配置方法】 第一步：指定用户计费开始失败的策略

NAS

```
Hostname#configure terminal
Hostname(config)#aaa accounting start-fail offline
```

【检验方法】 在 NAS 设备上，通过 **show run** 命令查看配置效果。

NAS

```
Hostname#sh run | inc aaa
aaa accounting start-fail offline
```

常见配置错误

无

1.4.7 配置 AAA 心跳检测

配置效果

- 可以指定是否开启 AAA 心跳检测。开启后，AAA 进程和 AAA 库间通过心跳信号检测对端是否可用。

注意事项

只有已知的 AAA 前端模块支持心跳（如 radius、dot1x 等）。

配置方法

↘ 配置 AAA 心跳检测。

- 可选配置。
- 缺省情况下，开启 AAA 心跳检测。

检验方法

使用命令 **show run** 查看配置信息。

相关命令

↘ 配置 AAA 心跳检测。

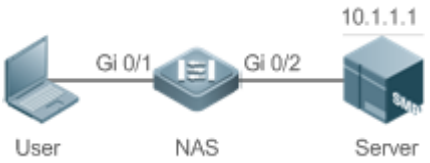
【命令格式】 [**no**] **aaa heartbeat enable**
【参数说明】 NA
【命令模式】 全局模式
【使用指导】 该命令开启或关闭 AAA 心跳检测功能。

配置举例

以下配置举例，仅介绍与 AAA 心跳检测相关的配置。

↘ 配置 AAA 心跳检测功能

【网络环境】



【配置方法】 关闭 AAA 心跳检测功能

NAS

```
Hostname#configure terminal
Hostname(config)#no aaa heartbeat enable
```

【检验方法】 在 NAS 设备上，通过 **show run** 命令查看配置效果。

NAS

```
Hostname#sh run | inc heart
no aaa heartbeat enable
```

常见配置错误

无

1.4.8 配置 AAA 日志打印功能

配置效果

- 通过配置本功能来关闭日志、限制日志打印速率或者调整 AAA 用户可记录的轨迹条数。

注意事项

无

配置方法

↘ 配置 AAA 日志打印功能

- 可选配置。
- 缺省情况下，开启日志打印功能。

↘ 配置 AAA 日志打印速率

- 可选配置。
- 缺省情况下，每秒打印 5 条日志。

调整每个 AAA 用户可记录的轨迹条数

- 可选配置。
- 缺省情况下，每个 AAA 用户可记录的轨迹条数为 20。

调整所有 AAA 用户轨迹记录总数

- 可选配置。
- 缺省情况下，所有 AAA 用户轨迹记录总数为 5000。

检验方法

使用命令 **show run** 查看配置信息。

相关命令

配置 AAA 日志打印功能

【命令格式】 [**no**] **aaa log enable**
【参数说明】 NA
【命令模式】 全局模式
【使用指导】 大量用户上线时打印 AAA 用户认证通过的 syslog，可能会造成刷屏或设备性能下降，因此可以通过配置本命令来关闭打印功能。

配置 AAA 日志打印速率

【命令格式】 **aaa log rate-limit** *num*
【参数说明】 *num*：表示打印日志的速率，取值范围为 0~65535,，缺省值为 5 个/秒。0 表示不限制打印的速率。
【命令模式】 全局模式
【使用指导】 大量用户上线时打印 AAA 用户认证通过的 syslog，可能会造成刷屏或设备性能下降。因此可以通过配置此命令来调整用户认证通过的 syslog 的打印速率。

调整每个 AAA 用户可记录的轨迹条数

【命令格式】 **aaa user-diag log-num** *num*
【参数说明】 *num*：每个 AAA 用户可记录的轨迹条数，范围为 1-100。
【命令模式】 全局配置模式
【使用指导】 大量用户上下线时，可能导致记录用户轨迹的进程占用的内存快速升高，因此可以通过配置此命令来调整每个用户轨迹记录条数来降低该进程的内存占用。

调整所有 AAA 用户轨迹记录总数

【命令格式】 **aaa user-diag user-num** *num*
【参数说明】 *num*：所有 AAA 用户轨迹记录总数，范围为 1-10000。
【命令模式】 全局配置模式

【使用指导】 大量用户上线时，可能导致记录用户轨迹的进程占用的内存快速升高，因此可以通过配置此命令来调整用户轨迹记录总数来降低该进程的内存占用。

配置举例

以下配置举例，仅介绍与 AAA 日志打印功能相关的配置。

配置 AAA 日志打印功能。

【网络环境】

【配置方法】 配置 AAA 日志每秒打印 10 条

NAS

```
Hostname# configure terminal
Hostname(config)# aaa log enable
Hostname(config)# aaa log rate-limit 10
```

【检验方法】 在 NAS 设备上，通过 **show run** 命令查看配置效果。

NAS

```
Hostname# show run | inc aaa log
 aaa log enable
 aaa log rate-limit 10
```

常见配置错误

无

1.5 监视与维护

清除各类信息

在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除被锁定的用户列表。	**clear aaa local user lockout** { **all** | **user-name** *username* }
清除所有 AAA 用户轨迹信息	**clear aaa user diag**

查看运行情况

作用	命令
显示记账更新相关的信息。	**show aaa accounting update**
显示当前所有配置域信息。	**show aaa domain**
显示当前 login 的锁定配置参数。	**show aaa lockout**
显示 AAA 配置的所有服务器组。	**show aaa group**
显示 AAA 所有的方法列表。	**show aaa method-list**
显示 AAA 用户相关信息。	**show aaa user**
显示 AAA 用户轨迹相关信息	**show aaa user diag** { **all** | **by-id** *session-id* | **by-mac** *mac-address* | **by-ip** *ip-address* }

查看调试信息

无

1 RADIUS

1.1 概述

RADIUS (Remote Authentication Dial-In User Service，远程认证拨号用户服务)是一种分布式的客户机/服务器系统。

RADIUS 与 AAA 配合对试图连接的用户进行身份认证，防止未经授权的访问。在系统实现中，RADIUS 客户端运行在设备或网络访问服务器（NAS）上，并向中央 RADIUS 服务器发出身份认证请求，中央服务器包含了所有的用户身份认证和网络服务信息。除了提供认证服务之外，RADIUS 服务器还提供接入用户的授权和记账的服务。

RADIUS 常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。由于 RADIUS 是一种完全开放的协议，很多系统如 UNIX、WINDOWS 2000、WINDOWS 2008 等均将 RADIUS 服务器作为一个组件安装，因此 RADIUS 是目前应用最广泛的安全服务器。

RADIUS 动态授权扩展协议（Dynamic Authorization Extensions to Remote Authentication Dial In User Service），在 IETF 的 RFC3576 中进行定义。该协议定义了一种针对用户下线管理方法。设备和 RADIUS 服务器之间通过 Disconnect-Messages（简称 DM)消息，将已认证通过的用户下线。该协议使得不同厂商间的设备和 RADIUS 服务器，在用户下线的处理上能够兼容。

DM 消息机制，由 RADIUS 服务器主动向设备发起用户下线请求，设备依据请求报文中携带的用户会话、用户名等信息来匹配用户并对其进行下线处理，再将处理结果以回应报文形式返回给 RADIUS 服务器，以实现服务器对用户的下线管理功能。

协议规范

- RFC2865：Remote Authentication Dial In User Service (RADIUS)
- RFC2866：RADIUS Accounting
- RFC2867：RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC2868：RADIUS Attributes for Tunnel Protocol Support
- RFC2869：RADIUS Extensions
- RFC3576：Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

1.2 典型应用

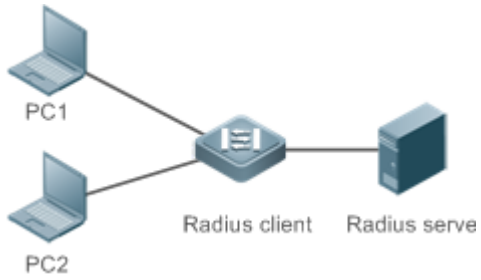
典型应用	场景描述
为接入用户提供认证、授权、记账服务	对网络中的接入用户进行认证、授权、记账，以防止未经授权的访问或操作。
已上线用户被服务器强制下线	对于已经认证的用户，服务器强制其下线

1.2.1 为接入用户提供认证、授权、记账服务

应用场景

RADIUS 的典型应用为对接入用户进行认证、授权、记账。网络设备作为 RADIUS 客户端，将用户信息发送给 RADIUS 服务器。RADIUS 服务器处理完成，给 RADIUS 客户端返回认证接受/认证拒绝/记账响应等信息。RADIUS 客户端根据 RADIUS 服务器的响应信息对接入用户进行相应处理。

图 1-1 典型的 RADIUS 网络配置



【注释】 PC1 和 PC2 作为接入用户通过有线或者无线方式和 RADIUS 客户端连接，并发起认证、记账请求。
RADIUS Client 通常为接入设备。
RADIUS Server 可以是 Windows 2000/2003 Server（IAS）、UNIX 系统所带组件，也可以是厂商提供的专用服务器软件。

功能部署

- 在 RADIUS Server 配置接入设备信息，包括接入设备 IP，共享密钥等。
- 在 RADIUS Client 配置 AAA 的认证、授权、记账方法列表。
- 在 RADIUS Client 配置 RADIUS server 信息，包括 IP，共享密钥等。
- 在 RADIUS Client 配置接入端口开启访问控制。
- 配置网络，使 RADIUS Client 和 RADIUS Server 之间通讯正常。

1.2.2 用户强制下线

应用场景

出于管理需要，RADIUS 服务器对于已经认证上线的用户，采取强制下线的措施。
网络配置请参考图 1-1

功能部署

在 1.2.1 的功能部署基础上加上以下部署：

- 在 RADIUS Client 开启 RADIUS 动态授权扩展功能

1.3 功能详解

基本概念

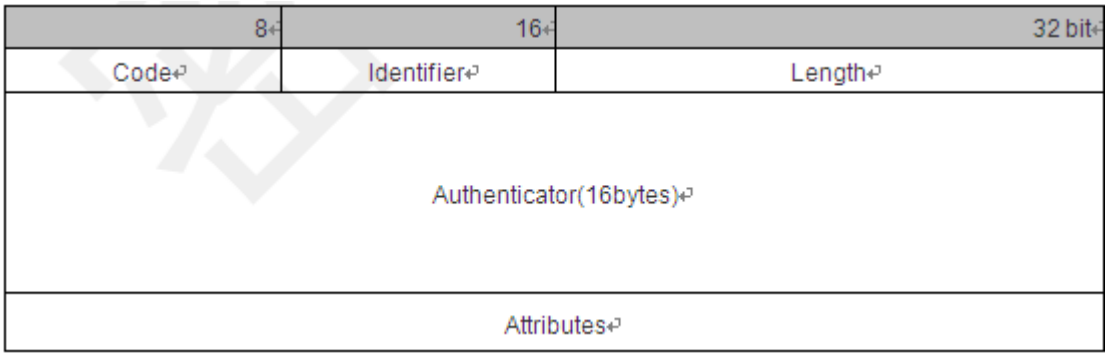
↘ 客户端/服务器模式

- 客户端：RADIUS 客户端作为 RADIUS 请求的发起端，通常运行在设备或者网络访问服务器(NAS)上，负责把用户信息发送给 RADIUS 服务器，并接受 RADIUS 服务器的返回信息，进行相应的处理。处理包括接受用户接入或者拒绝用户接入或者收集更多用户信息提供给服务器进行处理。

- 服务器：RADIUS 客户端和 RADIUS 服务器通常是多对一的关系。RADIUS 服务器维护所有的 RADIUS 客户端的 IP 和共享密钥信息，以及所有认证用户的信息。RADIUS 服务器接收 RADIUS 客户端的请求信息，并进行认证、授权、记账处理，再返回客户端需要的认证、授权、记账信息。

RADIUS 报文结构

RADIUS 的报文结构如下图所示：



- Code — Code 域长度为一个字节，用于标识 RADIUS 报文的类型，取值及含义参考下表。

Code	报文类型	Code	报文类型
1	Access-Request 认证请求报文	4	Accounting-Request 记账请求报文
2	Access-Accept 认证接受报文	5	Accounting-Response 记账相应报文
3	Access-Reject 认证拒绝报文	11	Access-Challenge 认证质询报文

- Identifier — Identifier 域占用 1 个字节，用于匹配请求和响应报文。同一类型的请求报文和响应报文的 Identifier 值相同。
- Length — Length 域占用 2 个字节，标识整个 RADIUS 报文的长度，包括 Code、Identifier、Length、Authenticator、Attributes 在内。超过 Length 域的字节将被忽略。如果接收到的报文的实际长度小于 Length 的值，则丢弃该报文。
- Authenticator — Authenticator 域占用 16 个字节。RADIUS 客户端使用该域来验证服务器的回应报文。Authenticator 域也用于用户密码的加密/解密。
- Attributes — Attributes 域的长度是不定的，用于携带认证、授权、记账信息。Attributes 域通常包含多个属性。每个属性采用 TLV(Type、Length、Value)三元组的结构表示。其中，Type 为 1 个字节，表示属性的类型，下表列出了 RADIUS 认证、授权、记账常用的属性；Length 为 1 个字节，表示该属性的长度，单位为字节；Value 为该属性的信息。

属性号	属性名	属性号	属性名
1	User-Name	43	Acct-Output-Octets
2	User-Password	44	Acct-Session-Id
3	CHAP-Password	45	Acct-Authentic
4	NAS-IP-Address	46	Acct-Session-Time
5	NAS-Port	47	Acct-Input-Packets
6	Service-Type	48	Acct-Output-Packets
7	Framed-Protocol	49	Acct-Terminate-Cause

8	Framed-IP-Address	50	Acct-Multi-Session-Id
9	Framed-IP-Netmask	51	Acct-Link-Count
10	Framed-Routing	52	Acct-Input-Gigawords
11	Filter-ID	53	Acct-Output-Gigawords
12	Framed-MTU	55	Event-Timestamp
13	Framed-Compression	60	CHAP-Challenge
14	Login-IP-Host	61	NAS-Port-Type
15	Login-Service	62	Port-Limit
16	Login-TCP-Port	63	Login-LAT-Port
18	Reply-Message	64	Tunnel-Type
19	Callback-Number	65	Tunnel-Medium-Type
20	Callback-ID	66	Tunnel-Client-Endpoint
22	Framed-Route	67	Tunnel-Server-Endpoint
23	Framed-IPX-Network	68	Acct-Tunnel-Connection
24	State	69	Tunnel-Password
25	Class	70	ARAP-Password
26	Vendor-Specific	71	ARAP-Features
27	Session-Timeout	72	ARAP-Zone-Access
28	Idle-Timeout	73	ARAP-Security
29	Termination-Action	74	ARAP-Security-Data
30	Called-Station-Id	75	Password-Retry
31	Calling-Station-Id	76	Prompt
32	NAS-Identifier	77	Connect-Info
33	Proxy-State	78	Configuration-Token
34	Login-LAT-Service	79	EAP-Message
35	Login-LAT-Node	80	Message-Authenticator
36	Login-LAT-Group	81	Tunnel-Private-Group-id
37	Framed-AppleTalk-Link	82	Tunnel-Assignment-id
38	Framed-AppleTalk-Network	83	Tunnel-Preference
39	Framed-AppleTalk-Zone	84	ARAP-Challenge-Response
40	Acct-Status-Type	85	Acct-Interim-Interval
41	Acct-Delay-Time	86	Acct-Tunnel-Packets-Lost
42	Acct-Input-Octets	87	NAS-Port-Id

↘ 共享密钥

RADIUS 客户端和 RADIUS 服务器进行通讯，相互之间通过共享密钥来确定对方的身份。共享密钥不能通过网络传输。此外，在传输过程中，为保证安全性，用户密码都是加密的。

↘ RADIUS 服务器组

RADIUS 安全协议，也称 RADIUS 方法，是以 RADIUS 服务器组为单位进行配置的。每一个 RADIUS 方法对应一个 RADIUS 服务器组，每一个 RADIUS 服务器组可配置一至多台 RADIUS 服务器（关于使用 RADIUS 方法的细节信息，请参见“AAA 配

置”章节）。如果在一个 RADIUS 服务器组中配置了多台 RADIUS 服务器，那么当设备同第一台 RADIUS 服务器通讯失败，或者第一台 RADIUS 服务器变成不可达的状态时，设备将自动尝试同第二台 RADIUS 服务器通讯，以此类推，直到成功或者全部失败为止。

↘ RADIUS 属性类型

- 标准属性

RFC 相关标准规定了 RADIUS 的属性号和属性的内容，但是对于某些属性类型，没有规定属性内容的格式。因此，为适应不同的 RADIUS 服务器要求，需要配置属性内容的格式。目前支持设置 RADIUS Calling-Station-ID 属性（属性号为 31）。

RADIUS Calling-Station-ID 属性用于网络设备向 RADIUS Server 发送请求报文时候，标识认证用户的身份。Calling-Station-ID 属性内容是字符串，可以有多种组成格式，由于要求必须能唯一标识一个用户，因此常选择使用用户的 MAC 地址作为其内容。例如在使用 IEEE 802.1x 认证时，选择使用安装 IEEE 802.1x 客户端所在设备的 MAC 地址。关于这 MAC 地址的格式，有以下几种：

格式	说明
ietf	IETF（RFC3580）规定的标准格式，使用 ‘-’ 作为分隔符。例如： 00-D0-F8-33-22-AC
normal	常用的表示 MAC 地址的格式（点分十六进制格式），使用 ‘.’ 作为分隔符。例如： 00d0.f833.22ac
unformatted	无格式，没有任何分隔符，默认使用该格式。例如： 00d0f83322ac

- 私有属性

RADIUS 协议是一个可扩展的协议。RFC2865 中定义了 26 号属性(Vendor-Specific)用于设备厂商对 RADIUS 协议进行扩展，以实现其私有的或者标准 RADIUS 没有定义的功能。锐捷公司支持的私有属性如表 1-3 所示。其中 TYPE 为锐捷产品私有属性类型的默认配置；扩展 TYPE 为扩展厂商类型的默认配置。

ID	功能	TYPE	扩展 TYPE
1	max-down-rate	1	76
2	port-priority	2	77
3	user-ip	3	3
4	VLAN-id	4	4
5	last-supplicant-version	5	5
6	net-ip	6	6
7	user-name	7	7
8	password	8	8
9	file-directory	9	9
10	file-count	10	10
11	file-name-0	11	11
12	file-name-1	12	12
13	file-name-2	13	13
14	file-name-3	14	14
15	file-name-4	15	15
16	max-up-rate	16	16

17	current-supplicant-version	17	17
18	flux-max-high32	18	18
19	flux-max-low32	19	19
20	proxy-avoid	20	20
21	dailup-avoid	21	21
22	ip-privilege	22	22
23	login-privilege	42	42
26	ipv6-multicast-address	79	79
27	ipv4-multicast-address	87	87
62	sdg-type	62	62
85	sdg-zone-name	85	85
103	sdg-group-name	103	103

功能特性

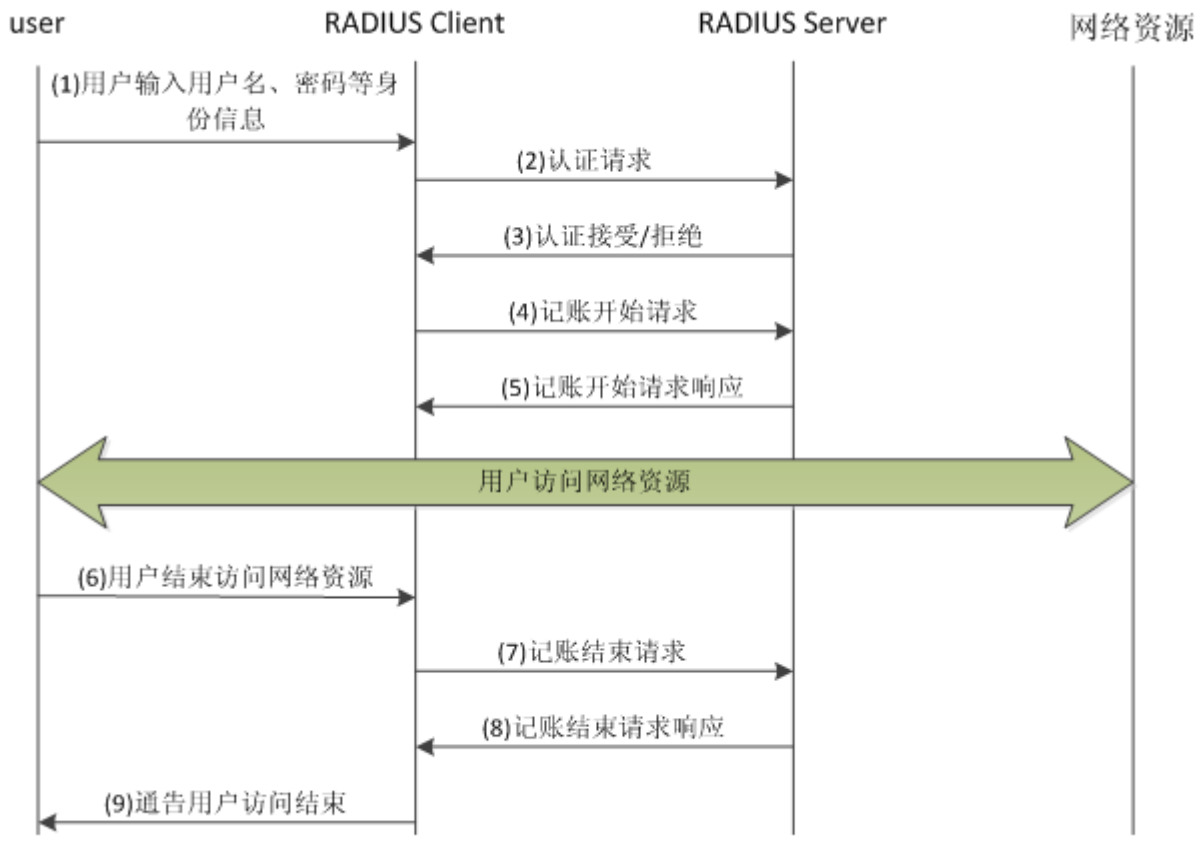
功能特性	作用
RADIUS 认证、授权	对访问用户进行身份认证、记账，保护网络安全以及便于网络管理员进行管理。
指定 RADIUS 报文源地址	指定 RADIUS 客户端向 RADIUS 服务器传送报文时的源 IP 地址。
RADIUS 超时重传	指定 RADIUS 服务器对 RADIUS 客户端传送的报文一定的时间内无响应时 RADIUS 客户端重传报文的参数。
RADIUS 服务器可达性检测	RADIUS 客户端主动探测 RADIUS 服务器是否可达，并维护各 RADIUS 服务器的可达性状态。进行业务处理时，总是优先选择状态为可达的服务器，以提高 RADIUS 业务的处理性能。
RADIUS 强制下线	对于已认证的用户，RADIUS 服务器主动要求其下线
配置 RADIUS 报文的 DSCP 优先级	DSCP 携带在 IP 报文的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。RADIUS 报文默认的 DSCP 优先级是 0。需要通过命令指定 RADIUS 报文的 DSCP 优先级，配置的 DSCP 优先级取值越大，RADIUS 报文的优先级越高。
配置发送给 RADIUS 服务器的数据流和数据包的单位	默认情况下，发送给 RADIUS 服务器的数据流的单位是字节，发送给 RASDIUS 服务器的数据包的单位是包。需要通过命令指定发送给 RADIUS 服务器的数据流和数据包的单位。
RADSEC 服务	RADSEC 将 TLS 与传输控制协议(TCP)结合使用。此传输配置文件提供比最初用于 RADIUS 传输的用户数据报协议（UDP）更强大的安全性。
配置 RADIUS 服务器组负载均衡	开启服务器组负载均衡，减小单个服务器资源开销。
配置 RADIUS 服务器支持热备功能	开启热备功能，备份服务器状态，使同一个 context 下的主备机的服务器状态保持一致。
配置记账报文复制功能	开启记账报文负责功能，服务器将复制记账报文，并发往指定服务器组下的服务器（仅发送给最先配置的 3 个服务器）。

1.3.1 RADIUS 认证、授权、记账

对访问用户进行身份认证、记账，保护网络安全以及便于网络管理员进行管理。

工作原理

图 1-2



RADIUS 的认证和授权流程为：

- 用户输入用户名、密码等身份信息，传送给 RADIUS 客户端。
- RADIUS 客户端获取用户的用户名、密码信息，向 RADIUS 传送认证请求报文。其中密码是加密的，加密方法请参照 RFC2865。
- RADIUS 服务器根据用户名、密码信息，决定接受或拒绝此次认证请求。如果接受，同时下发授权信息。不同类型的访问用户，其授权信息也不相同。

RADIUS 的记账流程为：

(4)如果步骤(3)中 RADIUS 服务器返回认证接受，则 RADIUS 客户端紧接着发送记账开始请求报文。

(5)RADIUS 服务器回应记账开始响应报文，开始记账。

(6)用户结束访问网络资源，请求 RADIUS 客户端断开连接。

(7)RADIUS 客户端发送记账结束请求报文。

(8)RADIUS 服务器返回记账结束响应报文，停止记账。

(9)用户断开连接，无法再访问网络资源

相关配置

↘ 配置 RADIUS 服务器参数

缺省情况下，没有配置任何 RADIUS 服务器。

使用 **radius-server host** 命令可以配置 RADIUS 服务器的相关信息。

必须至少配置一个 RADIUS 服务器，RADIUS 相关业务才能正常运转。

↘ 配置 AAA 认证方法列表

缺省情况下，没有配置任何 AAA 认证方法列表。

使用 **aaa authentication** 命令配置不同用户类型的方法列表，并且认证方法选择 group radius。

必须配置相应用户类型的 aaa 认证方法列表，才能进行 RADIUS 认证。

↘ 配置 AAA 授权方法列表

缺省情况下，没有配置任何 AAA 授权方法列表。

使用 **aaa authorization** 命令配置不同类型的授权方法列表，并且授权方法选择 group radius。

必须配置相应类型的 aaa 授权方法列表，才能进行 RADIUS 授权。

↘ 配置 AAA 记账方法列表

缺省情况下，没有配置任何 AAA 记账方法列表。

使用 **aaa accounting** 命令配置不同类型的记账方法列表，并且记账方法选择 group radius。

必须配置相应类型的 aaa 记账方法列表，才能进行 RADIUS 记账。

1.3.2 指定 RADIUS 报文源地址

指定 RADIUS 客户端向 RADIUS 服务器传送报文时的源 IP 地址。

工作原理

配置 RADIUS 时，通过指定 RADIUS 客户端向 RADIUS 服务器发送 RADIUS 报文的源 IP 地址，可以减少在 RADIUS 服务器上维护大量的 NAS 信息的工作量。

相关配置

缺省配置为使用全局路由寻路，确定发送 RADIUS 报文的源地址。

使用 **ip radius source-interface** 命令指定发送 RADIUS 报文的源接口，设备将把指定接口的第一个 ip 地址作为 RADIUS 报文的源地址。

1.3.3 RADIUS 超时重传

工作原理

RADIUS 客户端向 RADIUS 服务器传送报文后，启动定时器检测 RADIUS 服务器的响应，如果一定时间内 RADIUS 服务器没有响应，则 RADIUS 客户端重传报文。

相关配置

↘ 配置 RADIUS 服务器超时时间

缺省配置的超时时间为 5 秒。

使用命令 **radius-server timeout** 命令可以配置超时时间，时间范围为 1 到 1000 秒。

RADIUS 服务器的响应时间和其自身的性能、网络环境有关。需要根据实际情况配置合适的超时时间。

↘ 配置重传次数

缺省配置的重传次数为 3 次。

使用命令 **radius-server retransmit** 命令配置重传次数，范围 0 到 100 次。

↘ 配置记账更新是否重传

缺省配置为不会对计费更新报文进行重传。

使用命令 **radius-server account update retransmit** 命令配置认证用户的记账更新报文进行重传的功能。

1.3.4 RADIUS 服务器可达性检测

工作原理

RADIUS 客户端主动探测 RADIUS 服务器是否可达，并维护各 RADIUS 服务器的可达性状态。进行业务处理时，总是优先选择状态为可达的服务器，以提高 RADIUS 业务的处理性能。

相关配置

↘ 配置设备判定 RADIUS 安全服务器不可达的标准

缺省配置的判定 RADIUS 服务器不可达的标准为同时满足以下两个条件：一、设备在 60 秒内内没有收到来自 RADIUS 安全服务器的正确响应报文；二、设备向同一个 RADIUS 安全服务器发送的请求报文连续超时次数达到 10 次。

使用命令 **radius-server dead-criteria** 可以配置设备判定 RADIUS 安全服务器不可达的标准。

↘ 配置主动探测 RADIUS 安全服务器的测试用户名

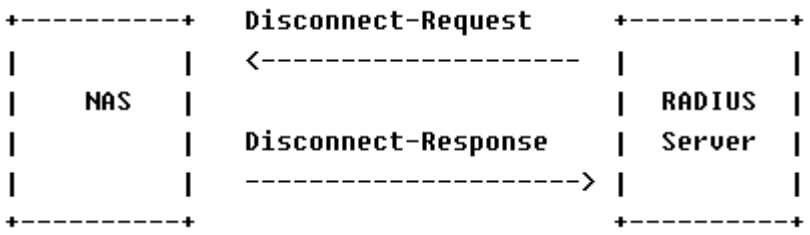
缺省配置时，不对 RADIUS 安全服务器指定主动探测的测试用户名。

使用命令 **radius-server host x.x.x.x testusername xxx** 来配置测试用户名。

1.3.5 RADIUS 强制下线

工作原理

图 3-3 RADIUS 动态授权扩展 DM 消息交互图



RADIUS 服务器和设备之间的 DM 消息交互图如上。RADIUS 服务器发送 Disconnect-Request 消息到设备的 3799 UDP 端口，设备处理结束之后，将处理结果通过 Disconnect-Response 消息返回给 RADIUS 服务器。

1.3.6 配置 RADIUS 报文的 DSCP 优先级

工作原理

DSCP 携带在 IP 报文的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。RADIUS 报文默认的 DSCP 优先级是 0。需要通过命令指定 RADIUS 报文的 DSCP 优先级，配置的 DSCP 优先级取值越大，RADIUS 报文的优先级越高。

相关配置

↘ 配置 RADIUS 报文的 DSCP 优先级

使用命令：radius dscp 来指定 RADIUS 报文的 DSCP 优先级，可配置的范围是 0 到 63。

1.3.7 配置发送给 RADIUS 服务器的数据流和数据包的单位

工作原理

默认情况下，发送给 RADIUS 服务器的数据流的单位是字节，发送给 RASDIUS 服务器的数据包的单位是包。需要通过命令指定发送给 RADIUS 服务器的数据流和数据包的单位。

相关配置

↘ 配置发送给 RADIUS 服务器的数据流和数据包的单位

使用命令：radius data-flow-format data {byte | kilo-byte | mega-byte | giga-byte} packet {one-packet | kilo-packet | mega-packet | giga-packet} 来指定发送给 RADIUS 服务器的数据流和数据包的。

1.3.8 RADSEC 服务

工作原理

TLS RADIUS 旨在使用传输安全层（TLS）协议为 RADIUS 请求提供安全通信。TLS 上的 RADIUS（也称为 RADSEC）将常规 RADIUS 流量重定向至通过 TLS 连接的远程 RADIUS 服务器。RADSEC 允许 RADIUS 身份验证、授权和计费数据在不受信任的网络上安全传递。

RADSEC 将 TLS 与传输控制协议（TCP）结合使用。此传输配置文件提供比最初用于 RADIUS 传输的用户数据报协议（UDP）更强大的安全性。基于 UDP 的 RADIUS 使用容易受到攻击的 MD5 算法对共享密钥密码进行加密。RADSEC 通过加密 TLS 隧道交换 RADIUS 数据包有效负载，可降低 MD5 遭受攻击的风险。

相关配置

↘ 配置

RADSEC 服务器由 RADSEC 目标对象表示。要配置 RADSEC，必须将 RADSEC 服务器定义为目标，并将 RADIUS 流量定向至该目标。RADSEC 目标由唯一的数字 ID 标识。可以配置多个 RADSEC 目标，其不同参数指向同一个 RADSEC 服务器。

要将流量从标准 RADIUS 服务器重定向至 RADSEC 服务器，请将 RADIUS 服务器与 RADSEC 目标相关联。例如，RADIUS 服务器 10.1.1.1 与 RADSEC 目标 10 相关联，则配置：radius-server host 10.1.1.1 radsec-destination 10

1.3.9 配置 RADIUS 服务器组负载均衡

工作原理

默认情况下，用户接入时是选择服务器组下的第一个服务器进行认证，只有在第一个服务器不可达时，才会选择下一个服务器进行认证。开启负载均衡后，采用轮询策略，第一个用户认证报文发往第一个服务器进行认证，第二用户认证报文发往第二个服务器进行认证，依此类推，在完成最后一个服务器分配用户认证之后，重新从第一个服务器开始分配用户认证。

相关配置

↘ 配置 RADIUS 服务器组的负载均衡

使用命令：**load-balance** 来开启 RADIUS 服务器组的负载均衡。

1.3.10 配置 RADIUS 服务器支持热备功能

工作原理

在配置 radius 服务器时，可选择开启热备功能，备份服务器状态，使同一个 context 下的主备机的服务器状态保持一致。

相关配置

↘ 配置 RADIUS 服务器支持热备

使用命令：**radius-server host** *ipv4-address* **context** *id hb_ipv4* **key** *text-string* 来配置 RADIUS 服务器支持热备。

1.3.11 配置记账报文复制功能

工作原理

RADIUS 的记账报文默认只发送给一个根据记账方法列表选择的服务器。开启此功能后，服务器将复制记账报文，并发往指定服务器组下的服务器（仅发送给最先配置的 3 个服务器）。

相关配置

↘ 配置记账报文复制功能

使用命令：**accounting-copy** *group_name* 在记账服务器组下配置，将记账报文复制给指定的服务器组内的服务器。

1.4 配置详解

配置项	配置建议 & 相关命令	
RADIUS 基本配置	⚠ 必须配置。用于 RADIUS 认证、授权、记账	
	radius-server host	配置远程 RADIUS 安全服务器的 IP 地址
	radius-server key	配置设备和 RADIUS 服务器进行通讯的共享密钥
	radius-server retransmit	配置设备在确认 RADIUS 无效以前发送请求的次数
	radius-server timeout	配置设备重传请求以前等待的时间
	radius-server account update retransmit	配置认证用户的记账更新报文进行重传的功能
	ip radius source-interface	配置 RADIUS 报文的源地址
配置 RADIUS 属性类型	⚠ 可选配置。用于定义设备封装和解析 RADIUS 报文时对属性的处理。	
	radius-server attribute 31	配置 RADIUS 的 31 号属性（Calling-Station-ID）的 MAC 地址格式。
	radius-server attribute class	配置 RADIUS 的 Class 属性的解析方式。
	radius-server attribute 30	配置 RADIUS 的 30 号属性（Called-Station-ID）的格式。
	radius set qos cos	配置设备处理服务器下发的私有属性 port-priority 为接口 cos 值。Cos 相关概念请参考 “配置 QoS”
	radius support cui	配置设备支持 cui 属性
	radius vendor-specific	配置设备解析私有属性的方式
	radius-server authentication attribute	配置 RADIUS 认证请求报文中是否携带指定属性
	radius-server account attribute	配置 RADIUS 记帐请求报文中是否携带指定属性
	radius-server authentication vendor	配置 RADIUS 认证请求报文是否携带其它产商的私有属性

	radius-server account vendor	配置 RADIUS 记帐请求报文是否携带其它产商的私有属性
配置 RADIUS 可达性检测	⚠ 可选配置。用于检测 RADIUS 服务器是否可达，以及维护 RADIUS 服务器的可达性状态。	
	radius-server dead-criteria	配置全局的 RADIUS 安全服务器不可达的判定标准
	radius-server deadtime	配置设备停止向不可达状态的 RADIUS 服务器发送请求报文的时长
	radius-server host	配置远程 RADIUS 安全服务器的 IP 地址 ,指定认证端口和记帐端口，指定主动探测的相关参数
配置 RADIUS 报文的 DSCP 优先级	**radius dscp**	配置 RADIUS 报文的 DSCP 优先级
配置发送给 RADIUS 服务器的数据流和数据包的单位	**radius data-flow-format data { byte | kilo-byte | mega-byte | giga-byte } packet {one-packet | kilo-packet | mega-packet | giga-packet }**	配置发送给 RADIUS 服务器的数据流和数据包的单位
配置 RADSEC 目标属性	⚠ 必需配置。用于 RADSEC 认证、授权、记账。	
	radsec destination	配置 RADSEC 属性
配置 RADIUS 服务器组负载均衡	**load-balacne**	配置开启 RADIUS 服务器组负载均衡策略
配置记账报文复制功能	⚠ 可选配置。用于配置记账报文复制功能。	
	accounting-copy	配置记账报文复制功能

1.4.1 RADIUS 基本配置

配置效果

- 完成 RADIUS 基本配置，即可进行 RADIUS 认证、授权、记账。

注意事项

- 在设备上配置 RADIUS 之前，应确保 RADIUS 服务器的网络通讯良好。
- 使用命令 **ip radius source-interface** 配置 RADIUS 报文的源地址时，应确保此源地址和 RADIUS 服务器通讯良好。
- 如果进行 RADIUS IPv6 认证，应确保 RADIUS 服务器也支持 RADIUS IPv6 认证。

配置方法

↘ 配置远程 RADIUS 安全服务器

- 必须配置。
- 配置 RADIUS 安全服务器的 IP 地址、认证端口、记账端口、共享密钥。

↘ 配置设备和 RADIUS 服务器进行通讯的共享密钥。

- 可选配置。
- 通过全局配置对所有未配置共享密钥选项的服务器配置一个共享密钥。

⚠ 设备上的共享密钥和 RADIUS 服务器上的共享密钥必须一致。

配置设备在确认 RADIUS 无效以前发送请求的次数

- 可选配置。
- 根据实际网络环境，配置设备确认 RADIUS 无效以前发送请求的次数。

配置设备重传请求以前等待的时间

- 可选配置。
- 根据实际网络环境，配置设备重传请求以前等待的时间。

⚠ 在使用 RADIUS 安全协议的 802.1x 认证环境中，如果网络设备作为 802.1x 认证者，并且采用锐捷 SU 作为 802.1x 客户端软件时，建议在网络设备上设置 **radius-server timeout** 值为 3 秒（默认为 5 秒），设置 **radius-server retransmit** 值为 2 次（默认为 3 次）

配置认证用户的记账更新报文进行重传的功能

- 可选配置。
- 根据实际实际需要，决定是否开启认证用户的记账更新报文重传功能。

配置 RADIUS 报文的源地址

- 可选配置。
- 根据实际网络环境，配置 RADIUS 报文的源地址。

检验方法

- 配置 AAA 方法列表使用 RADIUS 方法，用户进行认证、授权、记账。
- 设备与 RADIUS 服务器进行交互，通过抓包可以看到是通过 RADIUS 协议进行通信的。

相关命令

配置远程 RADIUS 安全服务器

【命令格式】 **radius-server host** { *ipv4-address* | *ipv6-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] [**context** *id hb_ipv4*] [**test username** *name* [**idle-time** *time*] [**ignore-auth-port**] [**ignore-acct-port**]] [**key** [**0** | **7**] *text-string*] [**radsec-destination** id-number]

【参数说明】 *ipv4-address*：RADIUS 安全服务器主机的 IPv4 地址。

ipv6-address：RADIUS 安全服务器主机的 IPv6 地址。

auth-port *port-number* ：RADIUS 身份认证的 UDP 端口，取值范围 0 - 65535，如果设置为 0，则该主机不进行身份认证。

acct-port *port-number*：RADIUS 记帐的 UDP 端口，取值范围 0 - 65535，如果设置为 0，则该主机不进行记帐。

context *id hb_ipv4*：RADIUS 开启热备功能，并指定热备 contex id 和对端 ip 地址，支持备份服务器状态，使同一个 context 下主备机的服务器保持状态一致。

test username *name*：开启对该 RADIUS 安全服务器的主动探测功能，并指定主动探测所使用的用户名。

idle-time *time*：配置设备向处于可达状态的 RADIUS 安全服务器发送测试报文的时间间隔。默认值为 60 分钟，可配置的范围为 1-1440 分钟（24 小时）。

ignore-auth-port：关闭对 RADIUS 安全服务器的认证端口的检测，默认开启。

ignore-acct-port：关闭对 RADIUS 安全服务器的记账端口的检测，默认开启。

key [**0** | **7**] *text-string*：配置用于该服务器的共享密钥，未配置则使用全局配置。配置的密钥可以指定加密类型，0 为无加密，7 简单加密，默认为 0。

radsec-destination id-number：将流量从 RADIUS 服务器重定向至 RADSEC 目标 id 号。

【命令模式】 全局模式。

【使用指导】 为了使用 RADIUS 实现 AAA 安全服务，必须定义 RADIUS 安全服务器。可以使用 **radius-server host** 命令定义一个或多个 RADIUS 安全服务器。

配置设备和 RADIUS 服务器进行通讯的共享密钥。

【命令格式】 **radius-server key** [**0** | **7**] *text-string*

【参数说明】 *text-string*：共享密钥的文本。

0 | **7**：口令的加密类型，0 无加密，7 简单加密，默认为 0。

【命令模式】 全局模式

【使用指导】 共享密钥是设备和 RADIUS 安全服务器进行正确通信的基础。为了使设备和 RADIUS 安全服务器能进行通信，必须在设备和 RADIUS 安全服务器上定义相同的共享密钥。

配置设备在确认 RADIUS 无效以前发送请求的次数

【命令格式】 **radius-server retransmit** *retries*

【参数说明】 *retries*：RADIUS 尝试重发次数，取值范围是 0-100

【命令模式】 全局模式

【使用指导】 AAA 在使用下一个方法对用户进行认证的前提是当前认证的安全服务器没有反应。设备判断安全服务器没有反应的标准是安全服务器在设备重发指定次数 RADIUS 报文期间均没有应答，每次重发之间有超时间隔。

配置设备重传请求以前等待的时间

【命令格式】 **radius-server timeout** *seconds*

【参数说明】 *seconds*：超时时间（单位为秒）。可设置的值范围为 1-1000 秒。

【命令模式】 全局模式

【使用指导】 使用该命令对重发报文的超时时间进行调整。

配置认证用户的记账更新报文进行重传的功能

【命令格式】 **radius-server account update retransmit**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 配置认证用户的记账更新报文进行重传的功能，默认重传。该配置不影响其他类型的用户。

配置 NAS 重启发送 accounting-on 报文功能

【命令格式】 **radius-server accounting-on enable**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 配置 NAS 重启发送 accounting-on 报文功能，默认发送，no 掉之后不发送。

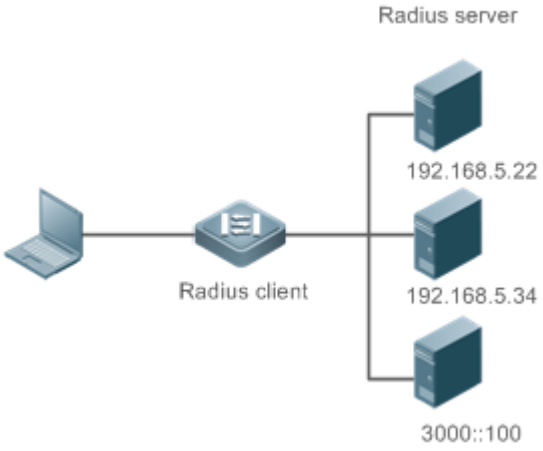
配置举例

以下配置举例，仅介绍与 RADIUS 相关的配置。

Login 用户使用 RADIUS 认证、授权、记账

【网络环境】

图 1-4



【配置方法】

- 配置启用 aaa。
- 配置 radius-server 信息。
- 配置使用 RADIUS 的认证方法、授权方法、记账方法。
- 在接口上应用配置认证方法。

RADIUS Client

```
Hostname# configure terminal
Hostname (config)# aaa new-model
Hostname (config)# radius-server host 192.168.5.22
Hostname (config)# radius-server host 3000::100
Hostname (config)# radius-server key aaa
Hostname (config)# aaa authentication login test group radius
Hostname (config)# aaa authorization exec test group radius
Hostname (config)# aaa accounting exec test start-stop group radius
Hostname (config)# line vty 0 4
Hostname (config-line)# login authentication test
Hostname (config-line)# authorization exec test
Hostname (config-line)# accounting exec test
```

【检验方法】

在 PC 上 Telnet 到设备上，要求输入用户名和密码。输入正确的用户名和密码，能够登录到设备上。并且被服务器授予一定的权限级别，仅运行执行该权限级别下的命令。在 RADIUS 服务器上可以查看到此用户的认证日志。用户对设备进行管理操作后退出登录，在 RADIUS 服务器上可以查看到此用户的记账信息。

```
Hostname#show running-config
!
radius-server host 192.168.5.22
radius-server host 3000::100
radius-server key aaa
aaa new-model
aaa accounting exec test start-stop group radius
aaa authorization exec test group radius
```

```
aaa authentication login test group radius
no service password-encryption
ip tcp not-send-rst
!
vlan 1
!
line con 0
line vty 0 4
 accounting exec test
 authorization exec test
 login authentication test
!
```

常见错误

- 设备配置的 key 与服务器配置的 key 不一致。
- 没有配置方法列表。

1.4.2 配置 RADIUS 属性类型

配置效果

- 定义设备封装和解析 RADIUS 报文时对属性的处理。

注意事项

- 设置 RADIUS 属性类型一节所涉及的私有属性均指锐捷公司的私有属性。

配置方法

↘ 配置 RADIUS 的 31 号属性（Calling-Station-ID）的 MAC 地址格式

- 可选配置
- 根据服务器类型，配置 Calling-Station-Id 的 MAC 地址格式为服务器支持的类型。

↘ 配置 RADIUS 的 Class 属性的解析方式

- 可选配置
- 根据服务器类型，配置对 Class 属性的解析方式。

↘ 配置 RADIUS 的 30 号属性（Called-Station-ID）的格式

- 可选配置
- 根据服务器类型，配置 Called-Station-ID 地址格式为服务器支持的类型。

↘ 配置 RADIUS 私有属性类型

- 可选配置
- 如果服务器为锐捷公司的应用服务器，则需要配置 RADIUS 私有属性类型来适应。

配置设备处理服务器下发的私有属性 port-priority 为接口的 cos 值

- 可选配置
- 根据需要，配置服务器下发的私有属性 port-priority 为接口的 cos 值。

配置设备支持 cui 属性

- 可选配置
- 根据需要，配置设备是否支持 RADIUS 的 CUI 属性。

配置设备解析私有属性的方式

- 可选配置
- 根据需要，配置设备解析锐捷私有属性时私有属性号的索引。

配置 RADIUS 认证请求报文中是否携带指定属性

- 可选配置
- 根据需要，配置 RADIUS 认证请求报文是否指定属性类型。

配置 RADIUS 记帐请求报文中是否携带指定属性

- 可选配置
- 根据需要，配置 RADIUS 记帐请求报文中是否指定属性类型。

配置 RADIUS 认证请求报文中是否携带指定产商的私有属性

- 可选配置
- 根据需要，配置 RADIUS 认证请求报文携带指定产商的私有属性。

配置 RADIUS 记帐请求报文中是否携带指定产商的私有属性

- 可选配置
- 根据需要，配置 RADIUS 记帐请求报文是否携带指定产商的私有属性。

配置 RADIUS 是否支持解析报文中思科、华为、微软的私有属性

- 可选配置
- 根据需要，配置 RADIUS 是否支持解析报文中思科、华为、微软的私有属性，缺省支持。

配置 RADIUS 报文 Nas-Port-Id 封装的格式

- 可选配置
- 根据是否 qinq 场景，配置 RADIUS 报文中 Nas-Port-Id 封装的格式。缺省是正常格式封装。

检验方法

- 配置 AAA 方法列表使用 RADIUS 方法，用户进行认证、授权、记账
- 设备与 RADIUS 服务器进行交互，通过抓包查看 Calling-Station-Id 的 MAC 地址格式。
- 设备与 RADIUS 服务器进行交互，通过设备 debug 信息查看锐捷公司的私有属性被设备正确的解析。
- 设备与 RADIUS 服务器进行交互，通过设备 debug 信息查看 CUI 属性被设备正确的解析。

相关命令

配置 RADIUS 的 31 号属性（Calling-Stationg-ID）的 MAC 地址格式

【命令格式】 **radius-server attribute 31 mac format** { **ietf | normal | unformatted | dot-split | colon-split | hyphen-split**} [**mode1** | **mode2**] [**lowercase** | **uppercase**]

【参数说明】 **ietf** ：指定 ETF（RFC3580）规定的标准格式，使用 '-' 作为分隔符。例如：00-D0-F8-33-22-AC。

normal：指定常用的表示 MAC 地址的格式(点分十六进制格式),使用 '.' 作为分隔符。例如 :00d0.f833.22ac。

unformatted：指定无格式，没有任何分隔符，默认使用该格式。例如：00d0f83322ac。

dot-split：指定 MAC 地址的格式，使用'.'作为分隔符，需要与 mode1 或 mode2 配合使用。

colon-split：指定 MAC 地址的格式，使用':'作为分隔符，需要与 mode1 或 mode2 配合使用。

hyphen-split：指定 MAC 地址的格式，使用'-'作为分隔符，需要与 mode1 或 mode2 配合使用。

mode1：指定 MAC 地址的格式，4 个字符一组，需要与 dot-split、colon-split、hyphen-split 配合使用。例如：00D0.F833.22AC、00D0:F833:22AC、00D0-F833-22AC。

mode2：指定 MAC 地址的格式，2 个字符一组，需要与 dot-split、colon-split、hyphen-split 配合使用。例如：00.D0.F8.33.22.AC、00:D0:F8:33:22:AC、00-D0-F8-33-22-AC。

lowercase：指定 MAC 地址的格式使用小写形式。

uppercase：指定 MAC 地址的格式使用大写形式。

【命令模式】 全局模式

【使用指导】 部分 RADIUS 安全服务器（主要用于 802.1x 认证）可能只识别 IETF 的格式，这种情况下需要将 Calling-Station-ID 属性设置为 IETF 格式类型。

配置 RADIUS 的 Class 属性的解析方式

【命令格式】 **radius-server attribute class user-flow-control { format-16bytes | format-32bytes }**

【参数说明】 **user-flow-control：**配置从 class 属性中解析限速配置。

format-16bytes：配置 class 属性中的限速值格式为 16 字节。

format-32bytes：配置 class 属性中的限速值格式为 32 字节。

【命令模式】 全局模式

【使用指导】 如果服务器通过 Class 属性下发限速值，则需要配置该命令。

配置 RADIUS 的 30 号属性（Called-Sation-ID）的格式

【命令格式】 **radius-server attribute 30 { ap-mac | ap-name }**

【参数说明】 **ap-mac：**指定 Called-Sation-ID 属性格式为 ap-mac:SSID，这种为默认的格式。

ap-name：指定 Called-Sation-ID 属性格式为 ap-name:SSID。

【命令模式】 全局模式

【使用指导】 根据服务器需要配置所需的格式，默认即是 ap-mac:SSID 的格式。

配置设备处理服务器下发的私有属性 port-priority 为接口的 cos 值

【命令格式】 **radius set qos cos**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 配置该命令，可以将传下的 QoS 值作为 cos 值，默认时作为 dscp 值。

配置设备支持 cui 属性

【命令格式】 **radius support cui**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 配置该命令，使 RADIUS 支持 cui 属性。

配置设备解析私有属性的方式

【命令格式】 **radius vendor-specific extend**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 使用该命令可对所有厂商 id 的属性按照配置是由类型识别。

配置 RADIUS 认证请求报文中是否携带指定属性

【命令格式】 **radius-server authentication attribute *type* package**

radius-server authentication attribute *type* unpackage

【参数说明】 ***type*,** RADIUS 属性类型。可设置范围为 1-255

【命令模式】 全局模式

【使用指导】 使用该命令可对认证请求报文中携带的属性进行指定。

配置 RADIUS 记帐请求报文中是否携带指定属性

【命令格式】 **radius-server account attribute *type* package**

radius-server account attribute *type* unpackage

【参数说明】 ***type*,** RADIUS 属性类型。可设置范围为 1-255

【命令模式】 全局模式

【使用指导】 使用该命令可对记帐请求报文中携带的属性进行指定。

配置 RADIUS 认证请求报文中是否携带指定产商的私有属性

【命令格式】 **radius-server authentication vendor *vendor_name* package**

【参数说明】 ***vendor_name*,** 产商的名称，可为 cmcc、microsoft、cisco、hw。

【命令模式】 全局模式

【使用指导】 使用该命令可配置认证请求报文中是否携带指定产商的私有属性。

配置 RADIUS 记帐请求报文中是否携带指定产商的私有属性

【命令格式】 **radius-server account vendor *vendor_name* package**

【参数说明】 ***vendor_name*,** 产商的名称，可为 cmcc、microsoft、cisco、hw。

【命令模式】 全局模式

【使用指导】 使用该命令可配置记帐请求报文中是否携带指定产商的私有属性。

配置 RADIUS 是否支持解析报文中思科、华为、微软的私有属性

【命令格式】 **radius vendor-specific attribute support *vendor_name***

【参数说明】 ***vendor_name*,** 产商的名称，可为 cisco、huawei、ms。

【命令模式】 全局模式

【使用指导】 使用该命令可以配置是否支持对报文中的思科、华为、微软的私有属性进行解析。

配置 RADIUS 报文 Nas-Port-Id 封装的格式

【命令格式】 **radius-server attribute nas-port-id format** { **qinq | normal | port-vid | mode1**}

【参数说明】 **qinq：**nas-port-id 封装的格式使用用户所在的接口名称以及内外层 vid 按既定的组合方式进行组合

port-vid：nas-port-id 封装格式使用用户所在的接口名称以及 vid 按既定的组合方式进行组合

normal：nas-port-id 封装的格式使用用户所在的接口名称

mode1：nas-port-id 封装的格式为：“slot = XX；subslot = XX；port = XXX；VLAN ID = XXXX”，其中，Slot 取值范围是 0～15，Subslot 取值范围是 0～15，Port 取值范围是 0～255，VLAN ID 取值范围是 1～4094。用户接口范围超过 255 的，不能用这种格式。

【命令模式】 全局模式

【使用指导】 使用该命令可以配置封装适合于 qinq 场景或非 qinq 场景的 nas-port-id 的格式。

配置举例

以下配置举例，仅介绍与 RADIUS 相关的配置。

配置 RADIUS 属性类型

【网络环境】 单设备

【配置方法】
- 配置 RADIUS 的 Calling-Station-Id 的 MAC 地址格式。
- 配置 RADIUS 传下的 QoS 值为接口 cos 值。
- 配置 RADIUS 支持 cui 属性。
- 扩展为不区别私有厂商 id。
- 认证请求不封装 NAS-PORT-ID 属性
- 记帐请求携带中移动要求的私有属性
- 配置对收到的 RADIUS 报文不支持解析思科的私有属性
- 配置 nas-port-id 的封装格式为 qinq 场景的格式

```
Hostname(config)# radius-server attribute 31 mac format ietf
Hostname(config)# radius set qos cos
Hostname(config)# radius support cui
Hostname(config)# radius vendor-specific extend
Hostname(config)# radius-server authentication attribute 87 unpackage
Hostname(config)# radius-server account vendor cmcc package
Hostname(config)# no radius vendor-specific attribute support cisco
Hostname(config)# radius-server attribute nas-port-id format qinq
```

【检验方法】 通过抓包或者设备 debug 信息查看 RADIUS 标准属性和私有属性的封装/解析是否正确。

1.4.3 配置 RADIUS 可达性检测

配置效果

设备维护所配置的每台 RADIUS 服务器的可达性状态：可达或者不可达。设备不会向处于不可达状态的 RADIUS 服务器发送接入用户的认证、授权和记账请求，除非，该 RADIUS 服务器所在的 RADIUS 服务器组的所有服务器均为不可达状态。

设备支持对指定的 RADIUS 服务器进行主动探测，默认关闭。如果为指定的 RADIUS 服务器开启主动探测功能，那么设备将会根据配置，定期向该 RADIUS 服务器发送探测请求（认证请求或者记账请求）。其时间间隔周期为：

- 处于可达状态的 RADIUS 服务器：该 RADIUS 服务器的可达状态的主动探测间隔时间（默认值为 60 分钟）。
- 处于不可达状态的 RADIUS 服务器：固定为 1 分钟。

注意事项

为指定的 RADIUS 服务器开启主动探测功能，需要满足如下所有条件：

- 在设备上配置了该 RADIUS 服务器的测试用户名。
- 在设备上至少配置了一个该 RADIUS 服务器的被测端口（认证端口或者记账端口）。

对于一台处于可达状态的 RADIUS 服务器，当以下两个条件均满足时，设备认为该 RADIUS 服务器进入不可达状态：

- 距离上次收到该 RADIUS 服务器的正确响应超过 radius-server dead-criteria time seconds 设定的时间。
- 在上次收到该 RADIUS 服务器的正确响应之后，设备发往该 RADIUS 服务器的请求而未收到正确响应的次数（包括重传），达到 radius-server dead-criteria tries number 设定的次数。

对于一台处于不可达状态的 RADIUS 服务器，当以下任一条件满足时，设备认为该 RADIUS 服务器进入可达状态：

- 设备收到来自该 RADIUS 服务器的正确响应。
- 该 RADIUS 服务器处于不可达状态超过 **radius-server deadtime** 设定的时间，并且该 RADIUS 服务器没有启用主动探测功能。
- 在设备上更新该 RADIUS 服务器的认证端口或者记账端口。

配置方法

配置全局的 RADIUS 安全服务器不可达的判定标准

- 必须配置
- 配置全局的 RADIUS 安全服务器不可达的判定标准是开启主动探测功能的必要条件。

配置远程 RADIUS 安全服务器的 IP 地址，指定认证端口和记帐端口，指定主动探测的相关参数

- 必须配置
- 指定 RADIUS 服务器主动探测的相关参数是开启主动探测功能的必要条件。

配置设备停止向不可达状态的 RADIUS 服务器发送请求报文的时长

- 可选配置
- RADIUS 服务器没有启用主动探测功能时，配置设备停止向不可达状态的 RADIUS 服务器发送请求报文的时长才会生效。

检验方法

- 通过 **show radius server** 命令可以查看各个 RADIUS 服务器的可达性信息。

相关命令

配置全局的 RADIUS 安全服务器不可达的判定标准

【命令格式】 **radius-server dead-criteria** { **time** *seconds* [**tries** *number*] | **tries** *number* }

【参数说明】 **time** *seconds*： 配置时间条件参数。设备在指定的时间内没有收到来自 RADIUS 安全服务器的正确响应报文，则认为该 RADIUS 安全服务器满足不可达的时长条件。可设置的值的范围为 1-120 秒。

tries *number* ：配置请求连续超时次数条件参数。当设备向同一个 RADIUS 安全服务器发送的请求报文连续超时次数达到所设定的次数，则认为该 RADIUS 安全服务器满足不可达的连续超时次数条件。可设置的值的范围为 1-100。

【命令模式】 全局模式

【使用指导】 如果一台 RADIUS 安全服务器同时满足时间条件和请求连续超时次数条件，则设备认为该 RADIUS 安全服务器不可达。使用该命令，用户可以对时间条件和请求连续超时次数条件的参数进行调整。

配置设备停止向不可达状态的 RADIUS 服务器发送请求报文的时长

【命令格式】 **radius-server deadtime** *minutes*

【参数说明】 *minutes*：配置设备停止向处于不可达状态的 RADIUS 安全服务器发送请求的时间，单位为分钟。可设置的值的范围为 1-1440 分钟（24 小时）。

【命令模式】 全局模式

【使用指导】 如果设备对一台 RADIUS 安全服务器启用了主动探测功能，那么 **radius-server deadtime** 的时间参数对该 RADIUS 安全服务器不起作用 ;否则 ,该 RADIUS 安全服务器 ,将在处于不可达状态的时间超过 **radius-server deadtime** 指定的时间时，被设备自动恢复为可达状态。

配置举例

以下配置举例，仅介绍与 RADIUS 相关的配置。

配置对 RADIUS 服务器进行不可达检测

【网络环境】

图 1-5

【配置方法】

- 配置全局的 RADIUS 安全服务器不可达的判定标准。
- 配置远程 RADIUS 安全服务器的 IP 地址，指定认证端口和记帐端口，指定主动探测的相关参数。

RADIUS Client

```
Hostname(config)# radius-server dead-criteria time 120 tries 5
Hostname(config)# radius-server host 192.168.5.22 test username test ignore-acct-port idle-time 90
```

【检验方法】 使设备与 192.168.5.22 服务器网络通讯断开。通过设备进行 RADIUS 认证。120 秒后 ,使用命令 **show radius server** 命令查看服务器状态为 dead。

```
Hostname#show running-config
...
radius-server host 192.168.5.22 test username test ignore-acct-port idle-time 90
radius-server dead-criteria time 120 tries 5
...
```

1.4.4 配置 RADIUS 报文的 DSCP 优先级

配置效果

- 可以指定 RADIUS 报文的 DSCP 优先级。

注意事项

- 配置的 DSCP 的值越大，RADIUS 报文的优先级越高。

配置方法

↘ **配置 RADIUS 报文的 DSCP 优先级**

- 可选配置。

检验方法

- 使用 show running-config 查看配置是否正确。

相关命令

↘ **配置 RADIUS 报文的 DSCP 优先级**

【命令格式】 **radius dscp** *dscp-value*

【参数说明】 *dscp-value*： DSCP 优先级的值。

【命令模式】 全局模式。

【使用指导】 可配置的范围是 0 到 63。

1.4.5 配置发送给 RADIUS 服务器的数据流和数据包的单位

配置效果

- 可以指定发送给 RADIUS 服务器的数据流和数据包的单位。

注意事项

无

配置方法

↘ **配置发送给 RADIUS 服务器的数据流和数据包的单位**

- 可选配置。

检验方法

- 使用 show running-config 查看配置是否正确。

相关命令

↘ 配置发送给 RADIUS 服务器的数据流和数据包的单位

【命令格式】 **radius data-flow-format data {byte | kilo-byte | mega-byte | giga-byte} packet {one-packet | kilo-packet | mega-packet | giga-packet}**

【参数说明】 **byte**：数据流单位为字节

kilo-byte：数据流单位为千字节

mega-byte：数据流单位为兆字节

giga-byte：数据流单位为吉字节

one-packet：数据包单位为包

kilo-packet：数据包单位为千包

mega-packet：数据包单位为兆包

giga-packet：数据包单位为吉包

【命令模式】 全局模式。

【使用指导】 根据需要指定数据流和数据包的单位。

1.4.6 配置 RADSEC 目标属性

配置效果

使用传输安全层（TLS）协议为 RADIUS 请求提供安全通信

注意事项

要使用 RADSEC，必须将 RADSEC 服务器定义为目标，并将 RADIUS 流量定向至该目标。

配置方法

↘ 配置 RADIUS 服务器与 RADSEC 目标相关联

- 必须配置
- 配置 RADSEC 服务器作为标准 RADIUS 服务器重定向流量目标。

↘ 配置 RADSEC 属性

- 必须配置
- 指定 RADSEC 服务器相关参数是开启 RADSEC 功能的必要条件。

检验方法

- 配置 RADIUS 流量重定向，用户进行认证、授权、记账。
- 设备与 RADSEC 服务器进行交互，通过抓包查看 TLS 报文信息。
- 设备与 RADIUS 服务器进行交互，通过设备 debug 信息查看 RADSEC 与服务器正常交互。

相关命令

配置 RADIUS 标准属性类型

【命令格式】 **radsec destination** *id-number* **host** *ipv4-address* [**port** *port-number*] [**tls-timeout** *seconds*]

【参数说明】 *id-number*：RADSEC 唯一 ID 标识

ipv4-address：RADSEC 目标服务器 IP 地址

port-number：*RADSEC 服务器的端口*

seconds：配置 TLS 连接超时，单位 s

【命令模式】 全局配置模式

【使用指导】 使用该命令可以根据需要配置 radsec 目标服务器属性。

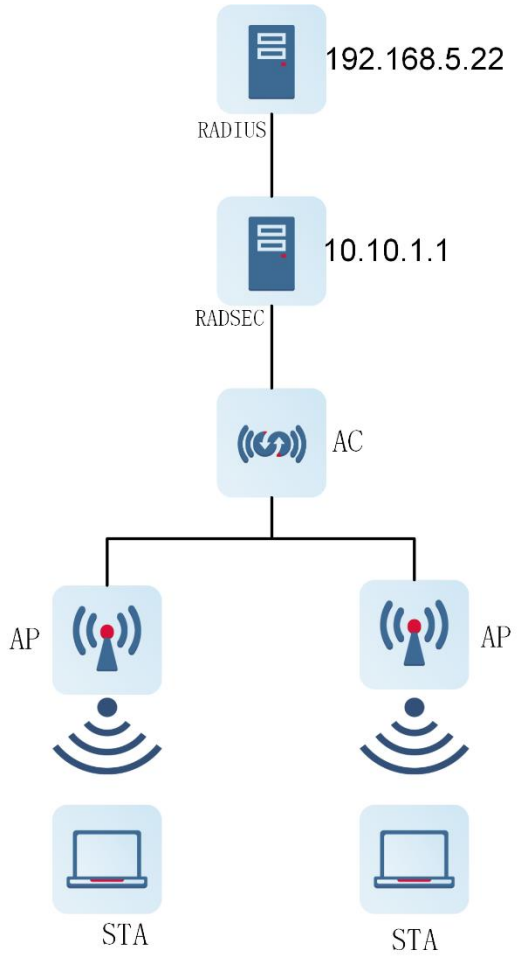
配置举例

以下配置举例，仅介绍与 RADSEC 相关的配置。

配置 RADSEC 目标属性

【网络环境】

图 1-4



【前置任务】 1，网络中已经完成了接口、IP 地址、Vlan 的配置，网络连通，NAS 设备到服务器的路由可达。
2，开启 PPSK 认证。

【配置方法】

- 配置 RADIUS 服务器与 RADSEC 目标相关联。
- 配置 RADSEC 目标唯一 ID 为 10、IP 地址为 10.10.1.1，服务器端口为 2022，连接超时时间为 10s。

```
Hostname(config)# radius-server host 192.168.5.22 radsec-destination 10

Hostname(config)# radsec destination 10 host 10.10.1.1 port 2022 tls-timeout 10
```

【检验方法】 1、 通过抓包或者设备 debug 信息查看 TLS 报文封装/解析是否正确。
2、 通过命令 **show radsec state** 查看

```
Hostname# show radsec state

Radsec server ip    : 10.10.1.1

Radsec id number    : 10
```

```
Radsec server port : 2022

Radsec server State: Active

tls-timeout        : 10 Seconds
```

1.4.7 配置 RADIUS 服务器组负载均衡

配置效果

- 用户认证报文会轮询选择服务器组下的不同服务器进行认证，同一个用户认证过程中的所有报文都发送至同一个服务器，下一个用户的认证报文才发往下一个服务器。

注意事项

- 服务器组下的服务器要有相同的配置，包括用户账号和密码、授权策略等。
- 服务器组下的一台服务器注册账号，要能自动同步到服务器组下的其他服务器，否则会影响认证效果。

配置方法

↘ 配置 RADIUS 服务器组负载均衡

- 可选配置。

【命令格式】 **load-balance**

【参数说明】 **-**

【命令模式】 服务器组配置模式。

【使用指导】 存在多个 radius 服务器组成服务器组，且服务器配置一样的情况，开启负载均衡策略，可以减少单个服务器的资源开销。

检验方法

- 使用 **show running-config** 查看配置是否正确。

1.4.8 配置记账报文复制功能

配置效果

- 用户记账报文会根据配置的服务器组，将记账报文复制并发送给指定服务器组内的服务器，目前仅发送给指定服务器组下最先配置的 3 个服务器。

注意事项

- 配置记账报文复制并发送的目标服务器组时，目标服务器组下配置的服务器应避免与当前服务器组下的服务器相同，避免影响记账准确性。

配置方法

配置记账报文复制功能

- 可选配置。

【命令格式】 **accounting-copy** *group_name*

【参数说明】 *group_name*：需要同步记账报文的目标服务器组名称，字符长度为 1~64

【命令模式】 服务器组配置模式

【使用指导】 1、配置记账报文复制并发送的目标服务器组时，目标服务器组下配置的服务器应避免与当前服务器组下的服务器相同，避免影响记账准确性。

2、默认当前记账报文复制后仅发送给目标服务器组下最先配置的 3 个服务器。若最先配置的 3 个服务器中包含了相同的发送和接收服务器，则发送时自动忽略该服务器，继续按服务器组配置顺序中的前三个服务器发送记账报文。

检验方法

- 使用 **show running-config** 命令查看已配置的记账同步目标服务器组；
- 使用 **show radius group** 命令查看记账同步目标服务器组的详细信息。

1.5 监视与维护

清除各类信息

⚠ 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除 RADIUS 用户轨迹	**clear radius user diag**
清除 RADIUS 消息轨迹	**clear radius event diag**

查看运行情况

作用	命令
显示 RADIUS 服务器全局参数。	**show radius parameter**
显示 RADIUS 服务器配置情况。	**show radius server**
显示 RADIUS 私有属性类型配置。	**show radius vendor-specific**
显示 RADIUS 认证相关统计信息	**show radius auth statistics**
显示 RADIUS 计费相关统计信息	**show radius acct statistics**
显示 RADIUS 服务器组的配置	**show radius group**
显示 RADIUS 标准属性	**show radius attribute**

显示 RADIUS 用户轨迹相关信息	**show radius user diag** { **all** | **by-id** *session-id* | **by-mac** *mac-address* | **by-ip** *ip-address* }
显示 RADIUS COA 消息轨迹相关信息	**show radius event diag coa** { **all** | **by-id** *msg-id* }
显示 RADIUS DM 消息轨迹相关信息	**show radius event diag dm** { **all** | **by-id** *msg-id* }
显示 RADSEC 目标的统计数据	**show radsec statistics**
显示 RADSEC 连接状态信息	**show radsec state**

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 RADIUS 事件的调试开关。	**debug radius event**
打开 RADIUS 报文打印的调试开关。	**debug radius detail**
打开 RADIUS 动态授权扩展功能的调试开关。	**debug radius extension event**
打开 RADIUS 动态授权扩展报文打印的调试开关。	**debug radius extension detail**

调整消息轨迹记录数

作用	命令
调整 RADIUS 消息轨迹记录总数。	**radius event-diag msg-num** *num*
调整每个 RADIUS 消息可记录的轨迹条数。	**radius event-diag log-num** *num*
调整 RADIUS 用户轨迹记录总数。	**radius user-diag user-num** *num*

1 TACACS

1.1 概述

TACACS+是在 TACACS（Terminal Access Controller Access Control System，终端访问控制器访问控制系统）基础上进行了功能增强的安全协议。用于实现多种用户的 AAA 功能，包括认证、授权、记账。

协议规范

- RFC 1492Terminal Access Controller Access Control System

1.2 典型应用

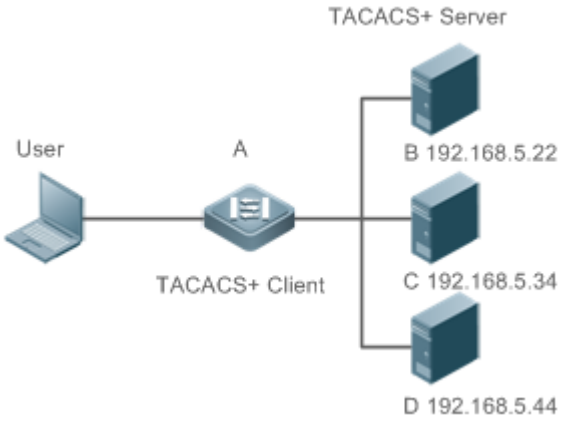
典型应用	场景描述
终端用户的登陆管理控制	对终端用户进行密码校验并进行授权。

1.2.1 终端用户的登陆管理控制

应用场景

TACACS+的典型应用为终端用户的登陆管理控制，网络设备作为 TACACS+的客户端，将用户名和密码发给 TACACS+服务器进行验证，验证通过并得到授权之后能够登录到网络设备上进行操作。下图所示：

图 1-1



【注释】 A 为发起 TACACS+请求的客户端。

B、C、D 为处理 TACACS+请求的服务器。

功能部署

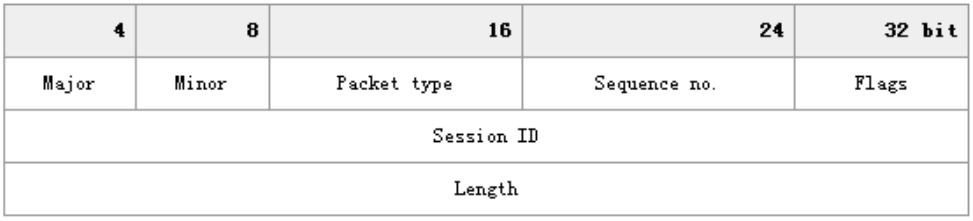
- 在服务器 B, C, D 上启动 TACACS+ Server，并且配置接入设备（设备 A）的信息，以便能够为设备提供基于 TACACS+协议的 AAA 功能。
- 。在设备 A 上开启 AAA 功能，为用户登录过程启用认证过程。
- 在设备 A 上启用 TACACS+ Client 功能，并且添加 TACACS+ Server（服务器 B, C, D）的 IP 地址和对应的共享密钥，以便设备 A 能和 TACACS+ Server 进行 TACACS+协议通信来实现 AAA 功能。

1.3 功能详解

基本概念

↘ TACACS+的报文格式

图 1-2



4	8	16	24	32 bit
Major	Minor	Packet type	Sequence no.	Flags
Session ID				
Length				

- Major Version — 主要 TACACS+ 版本号。
- Minor Version — 次要 TACACS+ 版本号。
- Packet Type — 可能值包括：
  TAC_PLUS_AUTHEN： = 0x01 （认证）;
  TAC_PLUS_AUTHOR：= 0x02 （授权）;
  TAC_PLUS_ACCT：= 0x03 （记账）。
- Sequence Number — 当前会话中的数据包序列号。会话中的第一个 TACACS+ 数据包序列号必须为 1，其后的每个数据包序列号逐次加 1。因此客户机只发送奇序列号数据包，而 TACACS+ Daemon 只发送偶序列号数据包。
- Flags — 该字段包括各种位图格式的标志（flag）。Flag 值表明数据包是否进行加密。
- Session ID — 该 TACACS+ 会话的 ID。
- Length — TACACS+ 数据包主体长度（不包括头部），报文全部以加密形式在网络上传输。

功能特性

功能特性	作用

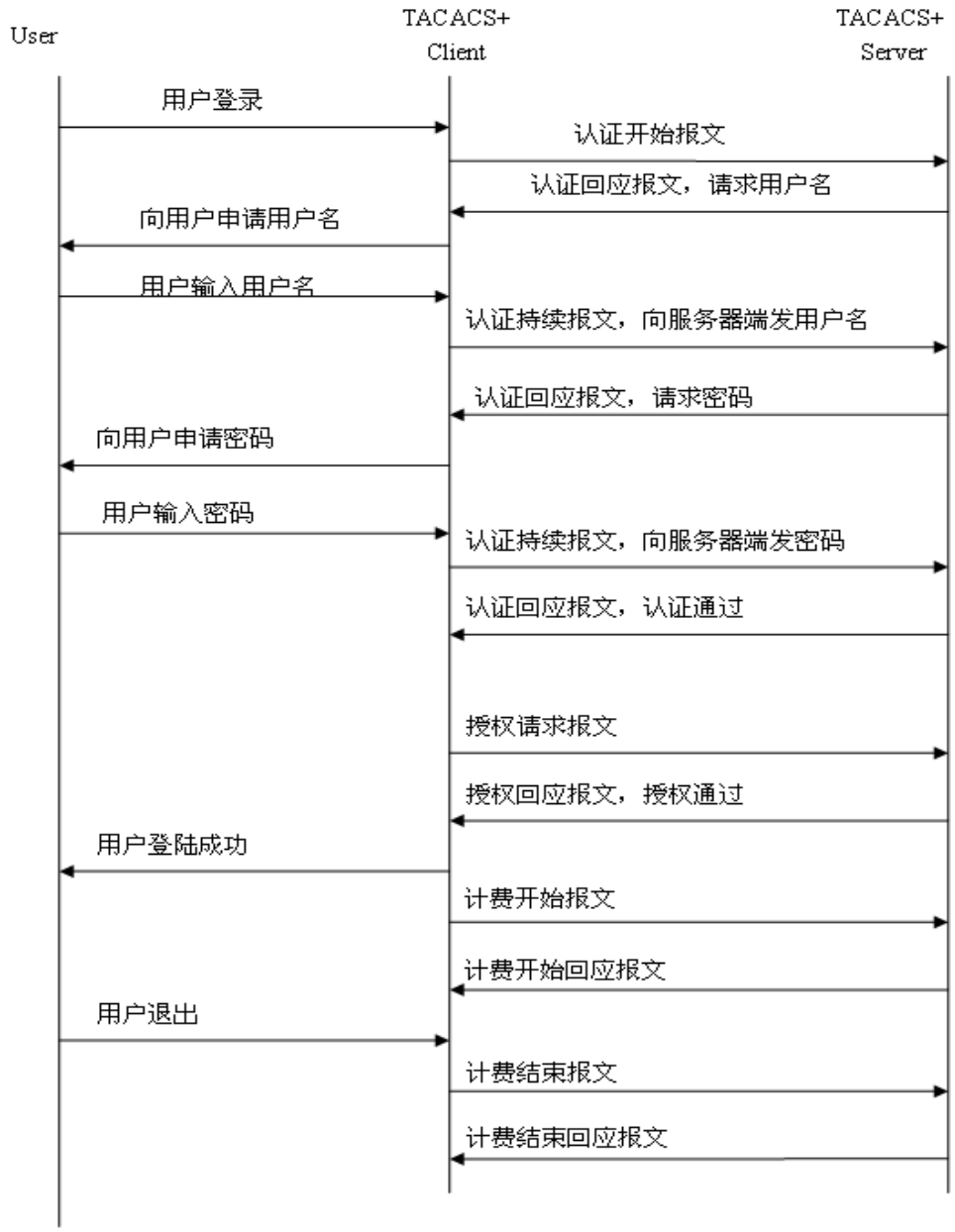
TACACS+认证、授权、记账	对终端用户进行认证、授权、记账

1.3.1 TACACS+认证、授权、记账

工作原理

下边以 Login 登录的基本认证、授权和记账说明 TACACS+运行中的数据报文的交互：

图 1-3



在整个过程中的基本消息交互流程可以分为三个部分：

1. 认证过程包含：

1) 用户请求登录网络设备。
2) TACACS+客户端收到请求之后，向 TACACS+服务器发送认证开始报文。
3) TACACS+服务器发送认证回应报文，请求用户名；
4) TACACS+客户端向用户询问用户名。
5) 用户输入登陆的用户名信息。
6) TACACS+客户端收到用户名后，向 TACACS+服务器发送认证持续报文，其中包括了用户名。
7) TACACS+服务器发送认证回应报文，请求登录密码；
8) TACACS+客户端收到向用户询问登录密码。
9) 用户输入登陆的密码信息。
10) TACACS+客户端收到登录密码后，向 TACACS+服务器发送认证持续报文，其中包括了登录密码。
11) TACACS+服务器发送认证回应报文，指示用户通过认证。

2. 认证通过后对用户进行授权：

1) TACACS+客户端向 TACACS+服务器发送授权请求报文。
2) TACACS+服务器发送授权回应报文，指示用户通过授权。
3) TACACS+客户端收到授权回应成功报文，向用户输出网络设备的配置界面。

3. 授权通过后，需要对登陆的用户进行记账，审计。

1) TACACS+客户端向 TACACS+服务器发送记账开始报文。
2) TACACS+服务器发送记账回应报文，指示记账开始报文已经收到。
3) 用户退出。
4) TACACS+客户端向 TACACS+服务器发送记账结束报文。
5) TACACS+务器发送记账回应报文，指示记账结束报文已经收到。

1.4 配置详解

配置项	配置建议&相关命令	
配置 TACACS+基本功能	⚠ 必须配置。用于开启 TACACS+安全服务。	
	tacacs-server host	配置 TACACS+服务器
	tacacs-server key	指定服务器与网络设备共享的密钥
	tacacs-server timeout	配置设备与 TACACS+服务器通信时，等待服务器的全局超时时间
	ip tacacs source-interface *interface-name*	指定 TACACS+报文的源地址。
配置 TACACS+的认证、授权、记账分离处理功能	⚠ 可选配置。用于分离处理认证、授权、记账请求。	
	aaa group server tacacs+	配置 TACACS+服务器组，将不同的 TACACS+服务器划分到不同的组
	server	添加 TACACS+服务器组的服务器

1.4.1 配置 TACACS+基本功能

配置效果

- 配置完成，TACACS+的基本功能准备就绪。配置 AAA 的方法列表时，指定使用 TACACS+方法，即可实现 TACACS+的认证、授权、记账。
- 进行认证、授权、记账操作时，TACACS+依据配置顺序向所配置的 TACACS+服务器发起认证、授权、记账请求。如果服务器响应超时，则依次遍历 TACACS+服务器列表。

注意事项

- TACACS+安全服务是 AAA 服务的一种，需要使用命令 **aaa new-model** 来开启安全服务。
- 配置了 TACACS+基本功能后 ,只是提供了一种安全服务 ,需要在配置 AAA 方法列表时指定使用 TACACS+服务 ,TACACS+的功能才会生效。

配置方法

↘ 启用 AAA

- 必须配置，启用 AAA 之后，才能配置 AAA 方法列表。TACACS+提供服务供是依赖于 AAA 方法列表的。

【命令格式】 **aaa new-model**
【参数说明】 -
【缺省配置】 AAA 功能没有打开。
【命令模式】 全局模式
【使用指导】 启用 AAA 之后，才能配置 AAA 方法列表。TACACS+提供服务供是依赖于 AAA 方法列表的。

↘ 配置 TACACS+服务器的 IP 地址

- 必须配置，否则设备无法和 TACACS+服务器通信来实现 AAA 功能。

【命令格式】 **tacacs-server host**{*ipv4-address* | *ipv6-address*} [**port***integer*] [**timeout** *integer*] [**key** [**0** | **7**] *text-string*]
【参数说明】 *ipv4-address*：TACACS+服务器的 IPv4 地址。
Ipv6-address：TACACS+服务器的 IPv6 地址。
port*integer*：TACACS+通信使用的 TCP 端口，默认为 TCP 端口 49。
timeout *integer*：与该 TACACS+服务器通信的超时时间，默认使用全局配置的超时时间。
key [**0** | **7**] *text-string*：配置用于该服务器的共享密钥，未配置则使用全局配置。配置的密钥可以指定加密类型，0 为无加密，7 简单加密，默认为 0。
【缺省配置】 没有配置任何 TACACS+服务器
【命令模式】 全局模式
【使用指导】 1. 可以在配置 IP 地址的同时指定该服务器的共享密钥，如果没有指定，则使用 **tacacs-server key** 命令配置的全局密钥作为该服务器的共享密钥。共享密钥必须与服务器上配置的完全相同。

2. 可以在配置 IP 地址的同时指定该服务器的通信端口。
3. 可以在配置 IP 地址的同时指定与该服务器通信的超时时间。
4. 可以指定与服务器的 TCP 连接方式。

配置 TACACS+服务器的共享密钥

- 可选配置。
- 如果没有通过该命令配置全局的通信协议，则在使用 **tacacs-server host** 命令添加服务器信息时，需要通过 **key** 关键字指定基于服务器的共享密钥，否则设备将无法和 TACACS+服务器进行通信。
- 如果在使用 **tacacs-server host** 命令添加服务器时没有通过 **key** 关键字指定共享密钥，则使用该全局密钥。

【命令格式】 **tacacs-server** [**key** [**0** | **7**] *text-string*]
【参数说明】 *text-string*：共享口令的文本
0 | 7：口令的加密类型，**0** 无加密，**7** 简单加密。
【缺省配置】 没有配置任何 TACACS+服务器的共享密钥。
【命令模式】 全局模式
【使用指导】 该命令配置全局使用的共享密钥服务器当需要为每个服务器指定不同的密钥时，使用 **tacacs-server host** 命令中的 **key** 选项实现。

配置 TACACS+服务器的超时时间

- 可选配置。
- 当设备和服务器之间的链路不稳定时，可以将超时时间改大。

【命令格式】 **tacacs-server timeout** *seconds*
【参数说明】 *seconds*：超时时间（单位为秒）。可设置的值范围为 1-1000 秒。
【缺省配置】 5 秒
【命令模式】 全局模式
【使用指导】 配置全局的服务器响应超时时间。当需要为每个服务器指定不同的超时时间时，使用 **tacacs-server host** 命令中的 **timeout** 选项实现。

配置 TACACS+报文的源地址

- 可选配置。
- 为了减少在 TACACS+服务器上维护大量的 nas 信息的工作量，可以通过该命令来设置 TACACS+报文的源地址。

【命令格式】 **ip tacacs source-interface** *interface-name*
【参数说明】 *interface-name*：TACACS+报文的源地址接口
【缺省配置】 缺省 TACACS+报文的源地址由网络层设置
【命令模式】 全局模式
【使用指导】 为了减少在 TACACS+服务器上维护大量的 nas 信息的工作量，可以通过该命令来设置 TACACS+报文的源地址。该命令将把指定接口的第一个 IP 地址作为 TACACS+报文的源地址。

检验方法

配置 AAA 方法列表使用 TACACS+方法，用户进行认证、授权、记账

- 设备与 TACACS+服务器进行交互，通过抓包可以查看设备与服务器间的 TACACS+协议的交互过程。
- 通过服务器的日志确认认证、授权、记账是否正常。

配置举例

↘ Login 认证使用 TACACS+

【网络环境】

图 1-4

【注释】 A 为发起 TACACS+请求的客户端。
B 为处理 TACACS+请求的服务器。

【配置方法】
- 配置启用 AAA。
- 配置 TACACS+ server 信息。
- 配置使用 TACACS+的认证方法。
- 在接口上应用配置认证方法。

A

```
Hostname#configure terminal
Hostname(config)#aaa new-model
Hostname(config)# tacacs-server host 192.168.5.22
Hostname(config)#tacacs-server key aaa
Hostname(config)#aaa authentication login test group tacacs+
Hostname(config)# line vty 0 4
Hostname(config-line)#login authentication test
```

【检验方法】 在 PC 上 telnet 到设备上 ,要求输入用户名和密码。输入正确的用户名和密码 ,能够登录到设备上。在 TACACS+服务器上可以查看到此用户的认证日志。

常见错误

- 没有开启 AAA 安全服务。
- 设备配置的 key 与服务器配置的 key 不一致。
- 没有配置方法列表。

1.4.2 配置 TACACS+的认证、授权、记账分离处理功能

配置效果

- 安全服务中的认证、授权、记账分别由不同的 TACACS+服务器处理。可以提高安全性，并实现一定负载均衡。

注意事项

- TACACS+安全服务是 AAA 服务的一种，需要使用命令 **aaa new-model** 来开启安全服务。
- 配置了 TACACS+基本功能后 ,只是提供了一种安全服务 ,需要在配置 AAA 方法列表时指定使用 TACACS+服务 ,TACACS+的功能才会生效。

配置方法

配置 TACACS+服务器组

- 必须配置。默认情况下，只有 tacacs+这一个服务器组，无法实现认证、授权、记账分离处理。
- 配置三个 TACACS+服务器组分别用于认证、授权、记账处理。

【命令格式】 **aaa group server tacacs+***group-name*

【参数说明】 *group-name*：组的名称，组名称不可为”radius”和”tacacs+”（不包括引号），这两个名字为内置组名字

【缺省配置】 没有配置 TACACS+服务器组

【命令模式】 全局模式

【使用指导】 通过对 TACACS+服务器进行分组，认证、授权、计帐可以使用不同的服务器组来完成。

配置 TACACS+服务器组引用服务器

- 必须配置。如果没有配置，则服务器组内没有服务器，设备无法与 TACACS+服务器通信。
- 在服务器组配置模式下，引用已经使用 **tacacs-server host** 命令配置好的服务器。

【命令格式】 **server {***ipv4-address* | *ipv6-address*}

【参数说明】 *ipv4-address*：TACACS+服务器的 IPv4 地址。

Ipv6-address：TACACS+服务器的 IPv6 地址。

【缺省配置】 无服务器配置。

【配置模式】 TACACS+服务器组配置模式

【使用指导】 配置此命令前，必须通过命令 **aaa group server tacacs+**进入 TACACS+组配置模式。

TACACS+服务器组中配置的服务器地址，必须在全局配置模式下，通过 **tacacs-server host** 命令配置此服务器。

如果一个服务器组内引用了多个服务器时，当一个服务器没有响应时，设备会继续向组内的下一个服务器发送 TACACS+请求。

检验方法

配置 AAA 方法列表使用 TACACS+方法，用户进行认证、授权、记账。

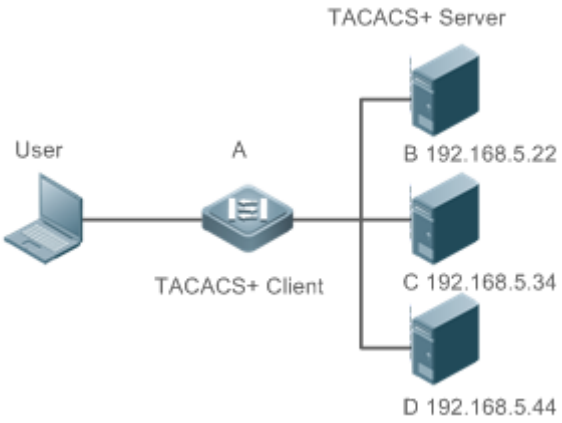
- 设备与 TACACS+服务器进行交互，通过抓包可以看到认证、授权、记账报文分别和不同的服务器交互，以及报文的源地址。

配置举例

↘ 配置认证、授权、记账使用不同 TACACS+服务器组。

【网络环境】

图 1-5



【注释】 A 为发起 TACACS+请求的客户端。
B 为处理 TACACS+认证请求的服务器。
C 为处理 TACACS+授权请求的服务器。
D 为处理 TACACS+记账请求的服务器。

【配置方法】
- 配置启用 AAA。
- 配置 TACACS+ server 信息。
- 配置 TACACS+服务器组。
- 向服务器组中添加服务器
- 配置使用 TACACS+的认证方法。
- 配置使用 TACACS+的授权方法。
- 配置使用 TACACS+的记账方法。
- 在接口上应用认证方法。
- 在接口上应用授权方法。
- 在接口上应用记账方法。

```
Hostname#configure terminal
Hostname(Hostname(config)#aaa new-model
Hostname(config)# tacacs-server host 192.168.5.22
Hostname(config)# tacacs-server host 192.168.5.34
Hostname(config)# tacacs-server host 192.168.5.44
Hostname(config)#tacacs-server key aaa
Hostname(config)#aaa group server tacacs+ tacgrp1
Hostname(config-gs-tacacs)# server 192.168.5.22
Hostname(config-gs-tacacs)# exit
Hostname(config)#aaa group server tacacs+ tacgrp2
Hostname(config-gs-tacacs)# server 192.168.5.34
Hostname(config-gs-tacacs)# exit
Hostname(config)#aaa group server tacacs+ tacgrp3
Hostname(config-gs-tacacs)# server 192.168.5.44
Hostname(config-gs-tacacs)# exit
Hostname(config-gs-tacacs)# tacacs-server single-connect-timeout 5
Hostname(config)#aaa authentication login test1 group tacacs+
Hostname(config)#aaa authentication enabledefault group tacgrp1
Hostname(config)#aaa authorization exec test2 group tacgrp2
Hostname(config)#aaa accounting commands 15 test3 start-stop group tacgrp3
Hostname(config)# line vty 0 4
Hostname(config-line)#login authentication test1
Hostname(config-line)#authorization exec test2
Hostname(config-line)# accounting commands 15 test3
```

【检验方法】 在 PC 上 telnet 到设备上 ,要求输入用户名和密码。输入正确的用户名和密码 ,能够登录到设备上。输入 **enable** 命令，输入正确的 **enable** 密码，发起 **enable** 认证，认证通过后，进入特权模式。对设备进行操作后，用户退出设备。

在服务器 192.168.5.22 上可以查看到此用户的认证日志。

在服务器 192.168.5.22 上可以查看到此用户的 **enable** 认证日志。

在服务器 192.168.5.34 上可以查看到此用户的 **exec** 授权日志。

在服务器 192.168.5.44 上可以查看到此用户的命令记账日志。

常见配置错误

- 没有开启 AAA 安全服务。
- 设备配置的 key 与服务器配置的 key 不一致。
- 服务器组引用为定义的服务器。
- 没有配置方法列表。

1.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
显示和各 TACACS+服务器的交互运行情况。	**show tacacs**

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 TACACS+的调试开关。	**debug tacacs+ detail**

1 802.1x

1.1 概述

IEEE802.1x（Port-Based Network Access Control）是一个基于端口的网络访问控制标准，为 LAN 提供安全接入服务。

IEEE 802 LAN 中，用户只要能接到网络设备上，不需要经过认证和授权即可直接访问网络资源。这种不受控行为会给网络带来安全隐。IEEE 802.1x 协议就是为了解决 802 LAN 安全问题提出来的。

802.1x 支持 Authentication，Authorization，Accounting 三种安全应用，简称 AAA。

- Authentication： 认证，用于判定用户是否可以获得访问权，限制非法用户；
- Authorization： 授权，授权用户可以使用哪些服务，控制合法用户的权限；
- Accounting： 计账，记录用户使用网络资源的情况，为收费提供依据。

802.1x 可以部署在对接入用户进行控制的网络中，以实现对接入用户身份验证、授权服务等

协议规范

- IEEE802.1x ：Port-Based Network Access Control

1.2 典型应用

典型应用	场景描述
无线 802.1x 认证	企业部署无线网络，在无线控制器上开启 802.1x 认证
EAP 终结	企业部署无线网络，在无线控制器上配置启用 dot1x 的 EAP 终结功能

1.2.1 无线 802.1x 认证

应用场景

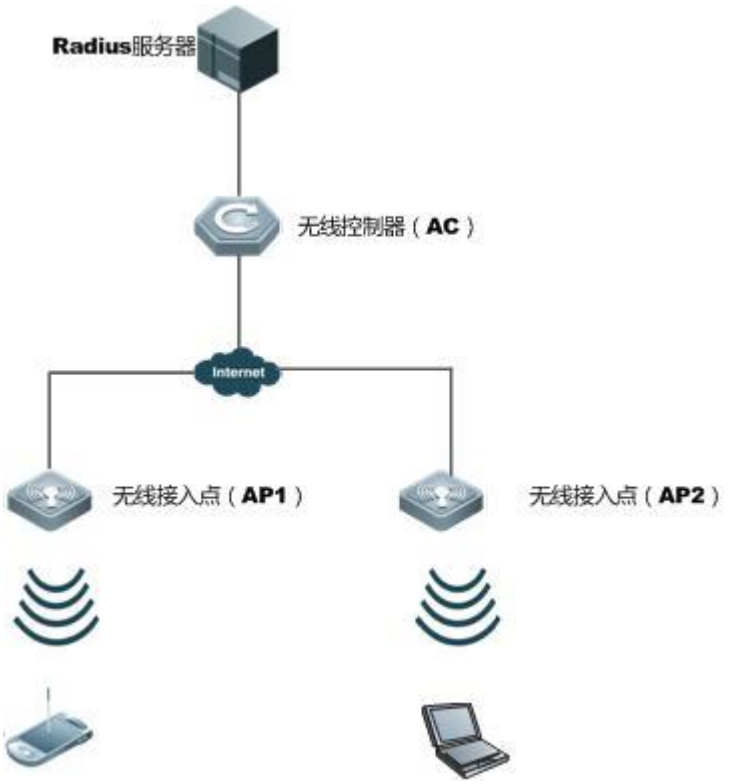
企业部署瘦 AP 的无线认证环境，包括瘦 AP，无线控制器（AC）等，部署 802.1x 做无线安全准入，STA 访问企业网时需要先通过 802.1x 认证。

以下图为例：

- 用户终端上要装有 802.1x 的客户端软件（操作系统自带，或者锐捷 supplicant， 或者其他符合 IEEE802.1x 标准的客户端软件）
- 无线控制器支持 IEEE 802.1x；

- 有一台（或多台）支持标准 RADIUS 的服务器作为认证服务器

图 1-1



【注释】 STA 支持 802.1x 认证，连接上 AP 之后，进行 802.1x 认证。无线控制器部署 802.1x 身份认证。RADIUS 服务器运行 RADIUS server 软件，执行身份校验。

功能部署

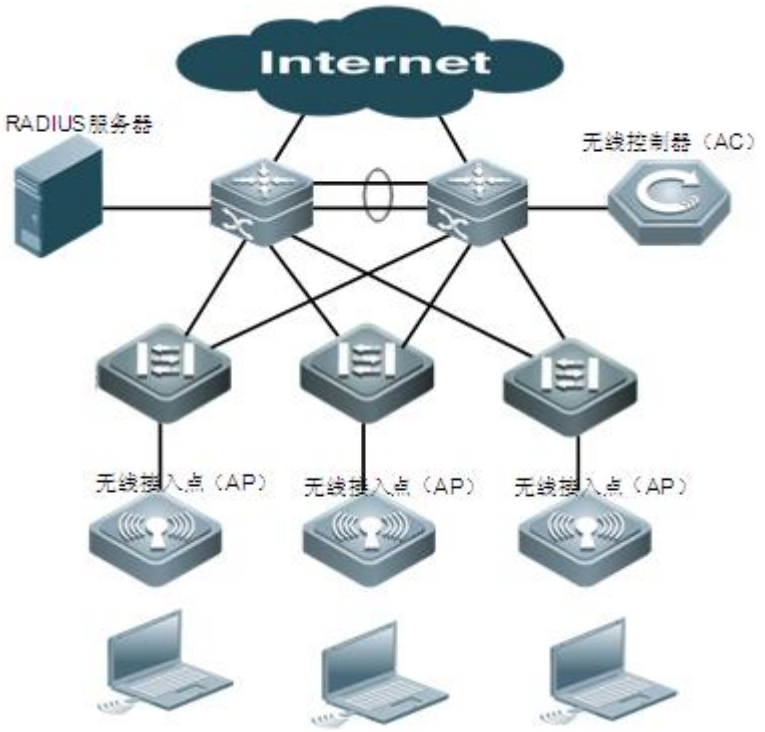
- 无线控制器通过 AP 广播的 WLAN 开启 802.1x 认证功能，实现关联的 STA 受控，只有认证通过的用户才能访问网络
- 配置 AAA 方法列表，使 802.1x 可以匹配正确的方法，使用正确的认证服务器
- 配置 RADIUS 参数,参考 RDS-SCG 的说明，确保设备可以和服务器正常通信
- 如果采用锐捷 RADIUS 服务器，还需要配置 snmp 参数，可以支持 RADIUS 服务器对设备进行查询设置等操作
- RADIUS 服务器创建帐号，注册接入设备的 IP 地址，并配置 RADIUS 相关参数，RADIUS 服务器才会对设备的请求作出响应

1.2.2 EAP 终结

应用场景

以下图为例，无线控制器和无线接入点组成无线网络，网络中部署 RADIUS 认证服务器。无线控制器上配置采用 802.1X 接入认证。由于 RADIUS 认证服务器不支持复杂的 EAP 认证协议，因此，需要在无线控制器上配置启用 dot1x 的 EAP 终结功能。

图 1-2



功能部属

- 配置 WLAN。
- 配置无线安全使用 802.1X 接入认证方式。
- 配置 AAA 的 802.1X 认证方法列表。
- 配置 RADIUS 服务器。
- 配置启用 802.1x 的 EAP 终结功能。

1.3 功能详解

基本概念

↘ 用户

在有线环境下，802.1x 协议是基于 LAN 的一个协议，对用户的识别不是基于账号，而是基于物理信息，在一个 LAN 里面，一个 MAC 地址+VID 的组合表示一个用户。除了上述信息是唯一外，其他信息都可以变，例如账号、IP 地址等。在无线环境下，WLAN 里面，一个 MAC 地址表示一个用户。

RADIUS

RADIUS（remote authentication dial-in user service）是一种远程认证协议，在 RFC2865 中定义，有着广泛的支持。利用该协议，可以实现服务器远程部署并实施认证。实际部署 802.1x 时，server 通常都是选择远程部署，设备和 server 间的 802.1x 认证信息通过 RADIUS 传输。

超时

认证过程中设备需要和终端、服务器通信，如果终端或服务器在协议指定的时间内没做出应答，则认为超时，超时会导致认证失败。实际部署时，需要注意 802.1x 协议的超时时间不同于 RADIUS 协议的超时时间，配合使用时必须保证 802.1x 的超时时间大于 RADIUS 的超时时间。

MAB

MAB 是指使用 MAC 地址作为用户名和密码进行认证，对于哑终端，例如网络打印机来说，无法安装 supplicant 软件，但是有需要做安全控制，此时可以通过 MAB 实现安全准入。

EAP

802.1x 协议使用 eap 协议承载认证信息，eap 协议在 rfc3748 中定义。eap 协议提供了一个通用的认证框架，在该框架内可以嵌套多种认证方法，例如 MD5 认证、CHAP 认证、PAP 认证、TLS 认证等。设备 802.1x 认证支持 MD5、CHAP、PAP、PEAP-MSCHAP、TLS 等认证方法。

授权

授权是指用户认证通过后给用户绑定一定的服务，例如绑定 IP 地址、绑定 vlan、绑定 ACL、绑定 QoS 等。

计费

计费功能可以实现用户网络审计，例如使用网络的时间、产生的流量，这有利于网络运维和管理。

有些 RADIUS 服务器，例如锐捷 SAM 和锐捷 SMP 软件，需要依靠计费报文来判断用户的上下线状态，因此选择这些服务器软件作为 RADIUS 服务器时，必须要配置计费功能。

RIPT

边缘智能感知技术，应用该技术可以在 AC 故障或者 AC 和 AP 断开连接时，AP 可以继续对外提供 WLAN 服务。802.1x 支持该技术，可以在这种情况 AP 上的 802.1x 对外继续提供认证服务。

功能特性

功能特性	作用
认证	提供用户的安全准入，通过认证的用户才可以访问网络。
授权	通过认证的用户具备的网络访问权限，例如 IP 绑定、acl 绑定等。
计费	提供上网记录审计，例如上网时长、流量等。
EAP 终结	设备能够将复杂的 EAP 认证协议终结在设备上 ,然后再代理转发 EAP 协议中包含的简单认证信息到外部服务器上的功能。

1.3.1 认证

认证的目的是为了确认用户身份是否合法，避免非法用户接入网络。用户为了获得访问网络的权限，需要先通过身份认证，服务器确认账号正确后，用户才可以访问网络。在用户通过认证之前，只有 EAPOL 报文(Extensible Authentication Protocol over LAN，802.1x 协议报文）可以在网络上通行（用于认证）。

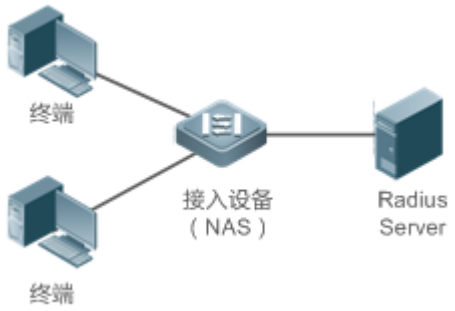
工作原理

802.1x 认证的原理比较简单，就是用户提交账号信息，设备将账号信息发给远程的 RADIUS 服务器进行身份验证，认证通过后允许用户访问网络。

↘ 认证过程的角色

IEEE802.1x 标准认证体系由恳请者(supplicant)、认证者(authenticator)、认证服务器(server)三个角色构成，在实际应用中，三者分别对应为：终端（Client）、接入设备(network access server，NAS)、认证服务器(最常见的是 RADIUS 服务器)。

图 1-3



- 恳请者

恳请者是最终用户所扮演的角色，一般是个人 PC。它请求对网络服务的访问，并对认证者的请求报文进行应答。恳请者必须运行符合 IEEE 802.1x 客户端标准的软件，目前最典型的就是操作系统自带的 IEEE802.1x 客户端支持，另外，锐捷也已推出符合该客户端标准的 RG Supplicant 软件。

- 认证者

认证者为无线访问热点等网络接入设备。该设备的职责是根据客户端当前的认证状态控制其与网络的连接状态。在客户端与服务器之间，该设备扮演着中介者的角色：从客户端要求用户名，核实从服务器端的认证信息，并且转发给客户端。因此，设备除了扮演 IEEE802.1x 的认证者的角色，还扮演 RADIUS Client 角色，因此把设备称作 network access server(NAS)，它要负责把从客户端收到的回应封装到 RADIUS 格式的报文并转发给 RADIUS Server，同时它要把从 RADIUS Server 收到的信息解释出来并转发给客户端。

扮演认证者角色的设备有两种类型的端口：受控端口（controlled Port）和非受控端口（uncontrolled Port）。连接在受控端口的用户只有通过认证才能访问网络资源；而连接在非受控端口的用户无须经过认证便可以直接访问网络资源。把用户连接在受控端口上，便可以实现对用户的控制；非受控端口主要是用来连接认证服务器，以便保证服务器与设备的正常通讯。

- 认证服务器

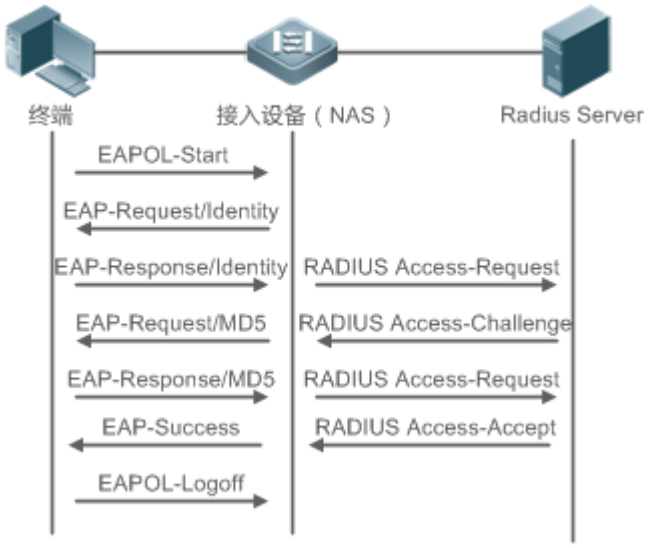
认证服务器通常为 RADIUS 服务器，认证过程中与认证者配合，为用户提供认证服务。认证服务器保存了用户名及密码，以及相应的授权信息，一台服务器可以对多台认证者提供认证服务，从而能够实现对用户的集中管理。认证服务器还负责管理从认证者发来的记帐数据。设备上的 802.1x 兼容标准的 RADIUS Server，如微软 IAS/NPS、Free RADIUS Server、思科 ACS 等。

认证过程及报文交互

恳请者和认证者之间通过 EAPOL 协议交换信息，而认证者和认证服务器通过 RADIUS 协议交换信息，通过这种转换完成认证过程。EAPOL 协议封装于 MAC 层之上，类型号为 0x888E。同时，标准为该协议申请了一个组播 MAC 地址 01-80-C2-00-00-03，用于初始认证过程中的报文传递。锐捷认证客户端还有可能将 01-D0-F8-00-00-03 用于认证开始的报文。

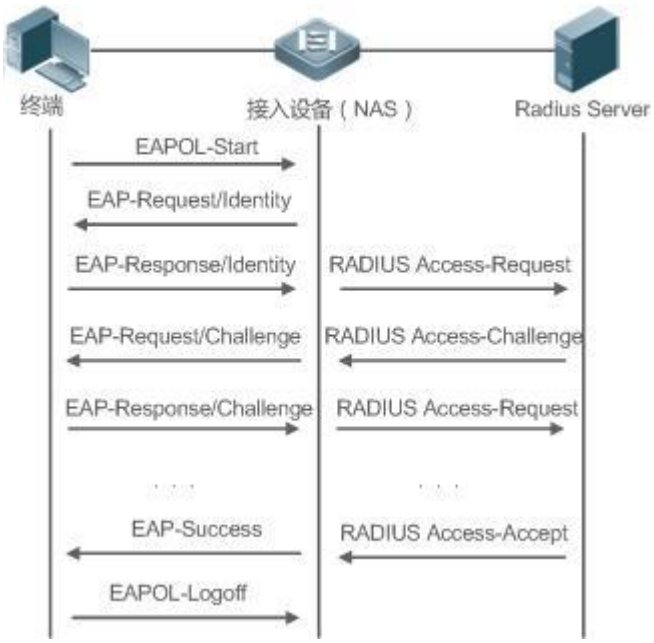
图 1-4 是有线设备一次典型的认证过程中，三个角色设备的报文交互过程：

图 1-4



该过程是一个典型的由用户发起的认证过程。在特殊的情形下，设备也可能主动发出认证请求，过程与该图一致，只是少了用户主动发出请求这一步。

图 1-5 是无线线设备一次典型的认证过程中，三个角色设备的报文交互过程



↘ 认证用户状态

802.1x 中根据端口的认证状态来决定该端口上的用户是否允许访问网络，设备扩展了 802.1X 协议， 默认是基于用户控制(一般以 MAC 标识一个用户)，所以，默认是根据一个端口下的用户的认证状态来决定该用户是否允许访问网络资源。设备上的 802.1x 也支持端口模式，详细可参考后续配置章节的描述。

一个非受控端口下的所有用户均可使用网络资源，而一个受控端口下的用户只有处于已认证状态（Authorized）才能访问网络资源。一个用户刚发起认证时，状态处于未认证状态（unauthorized），这时它不能访问网络，在认证通过后，该用户的状态会变为已认证状态（authorized），此时该用户便可以使用网络资源。

如果工作站不支持 802.1x，而该工作站连接在受控端口下，当设备请求该用户的用户名时，由于工作站不支持导致没对该请求做出响应。这就意味着该用户仍然处于未认证状态（unauthorized），不能访问网络资源。

相反地，如果工作站支持 802.1x，而所连的设备不支持 802.1x。用户发出的 EAPOL-START 帧无人响应，用户在发送一定数目的 EAPOL-START 帧仍未收到回应的情形下，将认为所连的端口是非受控端口，而直接使用网络资源。

在支持 802.1x 的设备下，所有端口的默认设置是非受控端口，可以把一个端口设置成受控端口，从而要求该端口下的所有用户都要进行认证。

当用户通过了认证（设备收到了从 RADIUS Server 服务器发来的成功报文），该用户便转变成已认证状态(authorized)，该用户可以自由使用网络资源。如果用户认证失败以至仍然处于未认证状态，可以重新发起认证。如果设备与 RADIUS server 之间的通讯有故障，那么该用户仍然处于未认证状态（unauthorized），网络对该用户来说仍然是不可使用的。

当用户发出 EAPOL-LOGOFF 报文后，该用户的状态由已认证(authorized)转向未认证状态(unauthorized)。

当设备的某个端口变为 LINK-DOWN 状态，该端口上的所有用户均变为未认证(unauthorized)状态。

当设备重新启动，该设备上的所有用户均变为未认证状态(unauthorized)。

如果要强制一个终端免认证，可以通过添加静态 MAC 地址或者配置 IP+MAC 绑定来实现。

↘ 搭建认证服务器

802.1x认证使用RADIUS server作为认证服务器，因此部署802.1x安全准入时，需要同时部署RADIUS server。常见的RADIUS server有微软的IAS/NPS、思科的ACS以及锐捷的SAM/SMP等。具体的部署步骤可参考对应软件的说明手册。

↘ 配置设备的认证参数

为了使用802.1x认证，需要在接入端口上开启802.1x认证功能，并配置aaa的方法列表以及RADIUS服务器参数。需要保证设备和RADIUS服务器是可达的，需要保证802.1x的服务器超时时间是大于RADIUS的服务器超时时间。

↘ supplicant

用户需要在终端上打开supplicant软件，输入账号并发起认证，如果使用的是操作系统自带的客户端，则操作系统在网络可用时会弹出对话框让用户输入账号。不同客户端软件的实现可能存在差异，界面的操作方式也可能存在差异，推荐使用锐捷supplicant软件作为认证客户端，如果使用其他软件，请参考相应的软件说明书。

↘ 下线

用户如果不想访问网络了，可以选择下线。下线有多种方式，包括：关机、断开端口网络连接、部分supplicant提供的下线功能。

1.3.2 授权

授权是指在用户通过认证之后，限定用户对网络使用的范围，例如MAC绑定IP、限制可上网时间或时段、可访问的vlan、可享受的带宽等。

工作原理

授权是指将权限和用户绑定，根据前面的描述，用户以MAC+VID标识，授权就是在MAC+VID的基础上再增加绑定信息，例如绑定IP、绑定vlan等。

↘ IP 授权

802.1x认证标准是不支持IP信息识别的，设备上的802.1x认证扩展了802.1x应用，支持MAC+IP绑定，称为IP授权。IP授权有四种模式，包括：

Supplicant授权：IP地址由supplicant提供，该模式需要锐捷supplicant配合才能支持；

RADIUS授权：IP地址由RADIUS服务器在认证通过后下发给设备；

Dhcp授权：用户终端认证通过后发起dhcp请求，获取到IP地址后将该IP和终端MAC绑定，适用于动态IP环境；

Mixed授权：认证用户按照Supplicant授权、RADIUS授权和Dhcp授权的顺序对用户进行MAC+IP的绑定。即supplicant提供了IP地址，则优先使用该IP地址，如果没有提供则使用RADIUS服务器提供的IP地址，如果RADIUS服务器没有提供，则最后使用dhcp提供的IP地址；

↘ ACL 授权

用户通过认证之后，服务器针对用户下发 acl 或者 ace，如果下发 acl，则需要事先在设备上配置好 acl，如果是下发 ace，则无需其他配置。ACL 授权基于 radius 的属性下发 ,支持标准属性、锐捷私有属性、思科私有属性 ,具体需要参考所使用的 RADIUS 服务器的软件说明。

↘ 踢线

设备上的 802.1x 和锐捷 SAM/SMP 配合使用时，支持服务器对在线用户实施踢线，踢线后用户将无法访问网络。该功能在上网时段控制、上网费用实时检查的环境中可以使用。

1.3.3 计费

计费功能允许网络运营方对接入用户实施上网审计或者费用审计，通常包括时间和流量的审计等。

工作原理

设备配置计费功能，RADIUS 服务器支持 rfc2869 定义的计费审计，用户上线时设备向服务器发送计费开始报文，服务器开始计费，用户下线时，设备向服务器发送计费结束报文，服务器完成一次审计，形成上网费用审计清单。关于计费，不同服务器可能会有不同实现，另外也不是所有服务器都支持计费功能，因此实际部署计费时需要参考服务器的使用说明。

↘ 计费开始

配置了计费功能情况下，用户通过认证后，设备会向服务器发送一个计费开始报文，报文携带用户的计费属性，例如用户名和计费 id 等，服务器收到报文后开始对用户计费。

↘ 计费更新

设备周期性的向服务器发送计费更新报文，计费更新报文可以使服务器的计费实时性特到提高。计费更新的间隔可以服务器下发，也可以设备上配置。

↘ 计费结束

用户下线后设备向服务器发送计费结束报文，携带用户的上网时长、上网消耗的流量等信息，服务器根据这些信息形成用户的上网记录。

1.3.4 EAP 终结

设备能够将复杂的 EAP 认证协议终结在设备上，然后再代理转发 EAP 协议中包含的简单认证信息到外部服务器上的功能。这一功能使得设备能够适配那些无法提供所需 EAP 方法的外部认证服务器，例如客户端认证要求使用 PEAPv1/GTC，而外部的认证服务器只能提供 PAP 认证方法。

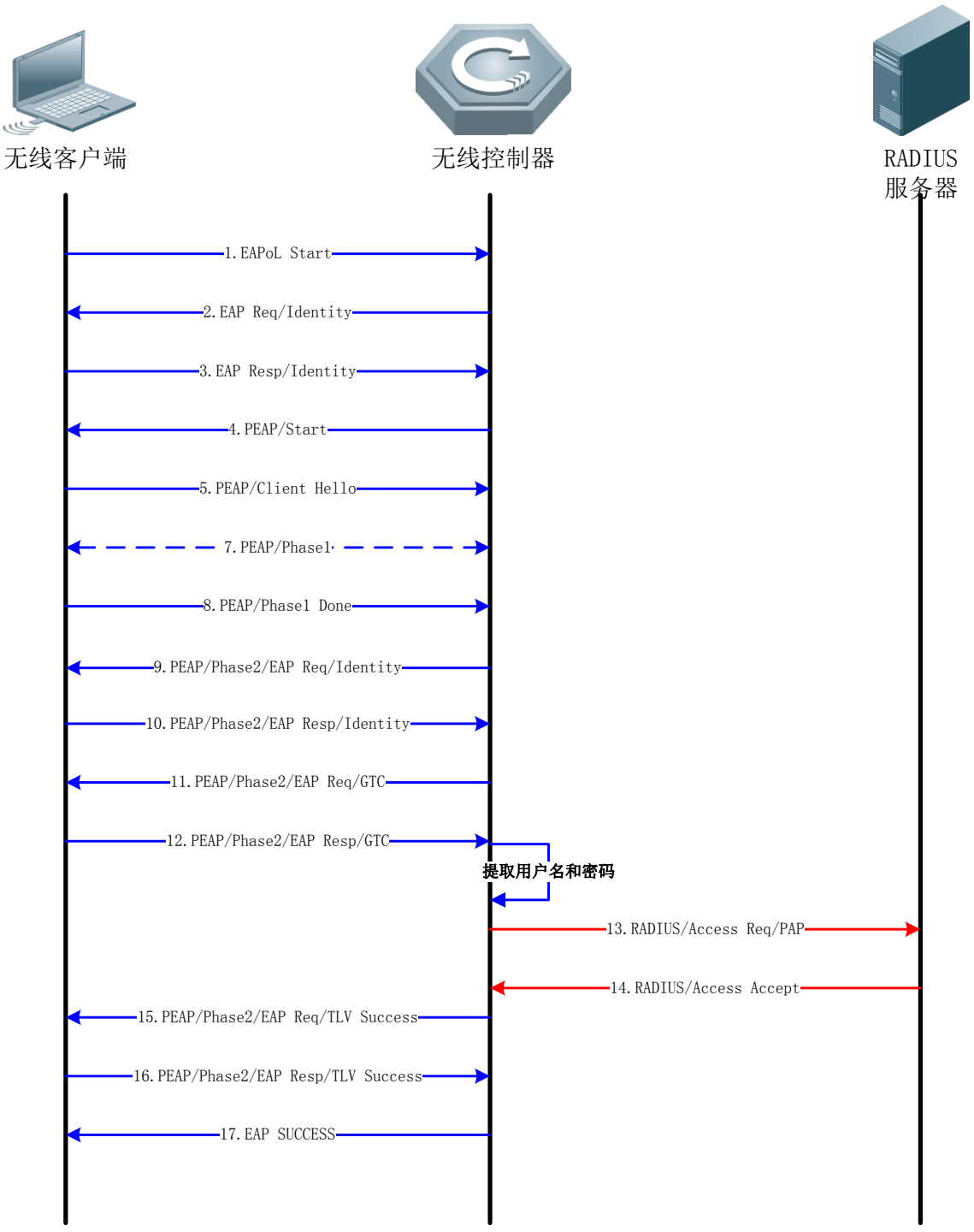
工作原理

现在以 EAP-GTC 终结为例来说明 EAP 终结的工作原理。下图是 EAP-GTC 终结的流程图 ,图中的 RADIUS 服务器仅支持 PAP 认证方式，而无线控制器和无线客户端之间执行 PEAPv1/GTC 认证方法。

- 步骤 1 到步骤 12：无线控制器和无线客户端之间进行 PEAPv1/GTC 认证方法所要求的交互流程，执行完步骤 12 后，无线控制器就获得了客户端的认证凭据（包括用户名和明文密码）。
- 步骤 13 到步骤 14：dot1x 模块使用获得的认证凭据向 RADIUS 服务器发起一次 PAP 认证过程，并且获得了认证通过的结果。
- 步骤 15 到步骤 17：dot1x 根据 RADIUS 服务器返回的结果继续执行 PEAPv1/GTC 认证过程。

从下图所示的流程可以看出，无线控制器进行 EAP-GTC 终结的时候，无线客户端是感知不到的，始终认为是在进行一次 PEAPv1/GTC 认证；而 RADIUS 服务器上则认为客户端是在进行一次 PAP 认证。当进行 PEAP 终结和 EAP-MSCHAPv2 终结时，流程也是类似的。

图 1-5



相关配置

↘ 配置 EAP 终结

缺省情况下，没有配置 EAP 终结。

使用 **dot1x eap-terminate peap inner-methods gtc** 配置启用 EAP-GTC 终结；使用 **dot1x eap-terminate peap inner-methods mschapv2** 配置启用 EAP-MSCHAPV2 终结。

1.4 配置详解

配置项	配置建议 & 相关命令	
配置 802.1x 基本功能	⚠ 必须配置，用于部署基本的安全认证和计费。	
	aaa new-model	开启 aaa
	aaa authentication dot1x	配置认证方法列表
	aaa accounting networks	配置计费方法列表
	radius-server host	配置 RADIUS 服务器
	radius-server key	配置设备和 RADIUS 服务器通信的密钥
	dot1x port-control auto	配置端口上的 802.1x 认证
配置 802.1x 协议参数	⚠ 可选配置。用于调整 802.1x 协议参数。 ⚠ 要确保 802.1x 的服务器超时时间大于 RADIUS 的服务器超时时间。 ⚠ 锐捷客户端在线检测功能仅适用于锐捷 supplicant	
	dot1x re-authentication	配置重认证功能
	dot1x timeout re-authperiod	配置重认证间隔
	dot1x timeout tx-period	配置 request/id 报文重传间隔
	dot1x reauth-max	配置 request/id 报文重传次数
	dot1x timeout supp-timeout	配置 request/challenge 报文重传间隔
	dot1x max-req	配置 request/challenge 报文重传次数
	dot1x timeout server-timeout	配置服务器超时时间
	dot1x timeout quiet-period	配置认证失败后的静默时间
	dot1x auth-mode	配置认证模式(eap/chap/pap)
	dot1x client-probe enable	配置锐捷客户端在线检测
	dot1x probe-timer interval	配置锐捷客户端检测周期
	dot1x probe-timer alive	配置锐捷客户端检测时长
配置授权	⚠ 可选配置。用于调整 802.1x 协议参数 ⚠ IP 授权模式中的 supplicant 授权需配合锐捷 supplicant	
	aaa authorization ip-auth-mode	配置 IP 授权模式
	dot1x private-supplicant-only	配置过滤非锐捷客户端功能
	dot1x redirect	配置二代 su 升级功能，通过浏览器重定向到指定的资源网站下载 supplicant 软件
	snmp	配置 SNMP 参数，锐捷 SAM/SMP 支持对将 802.1x 在线用户强制离线，通过 SNMP 协议实现，使用该功能需要配置 SNMP 参数

配置 MAB	⚠ 可选配置，用于支持 MAC 认证 ⚠ 802.1x 认证优先级高于 MAB 认证 ⚠ MAB 认证不支持 IP 授权 ⚠ 单 MAB 和多 MAB 互斥 ⚠ MAB 采用 PAP 认证模式，部署时需要注意服务器的配置	
	dot1x mac-auth-bypass	配置单 MAB 认证
	dot1x mac-auth-bypass multi-user	配置多 MAB 认证
	dot1x multi-mab quiet-period	配置多 MAB 认证失败后的静默时间
	dot1x mac-auth-bypass timeout-activity	配置 MAB 认证超时时间
	dot1x mac-auth-bypass violation	配置 MAB 违例
	dot1x mac-auth-bypass vlan	配置 MAB VLAN
配置 EAP 终结功能	⚠ 可选配置，用于置开启 EAP 终结功能。	
	dot1x eap-terminate peap inner-methods	配置开启 EAP 终结功能
配置 PKI 信息	⚠ 可选配置，用于配置重新生成或导入 PKI 信息。	
	dot1x pki-manage generate self-signed	配置重新生成自签名 PKI 信息
	dot1xpki-manage import pfx	配置导入 PKCS#12 格式的 PKI 信息
配置 EAP 终结功能 **配置效果** 配置后可将复杂的 EAP 认证协议终结在设备上，代理转发 EAP 协议中包含的简单认证信息到外部服务器上，使得设备能够适配那些无法提供所需 EAP 方法的外部认证服务器。 **配置**	⚠ 可选配置，用于配置端口主动请求 ⚠ 可选配置，配置可认证主机列表 ⚠ 可选配置，配置设备发送伪 mac ⚠ 可选配置，配置同 MAC 多帐号	
	dot1x auto-req	配置设备主动发起 802.1x 认证
	dot1x auto-req packet-num	配置设备主动发起认证请求报文的个数
	dot1x auto-req user-detect	配置主动认证检测是否有用户在认证
	dot1x auto-req req-interval	配置设备主动发起认证请求报文的间隔时间
	dot1x auth-address-table address	配置可认证主机列表
	dot1x pseudo source-mac	配置设备使用虚拟 MAC 作为设备发出的 802.1x 报文的源 MAC 地址
	dot1x multi-account enable	配置支持一个 MAC 使用多账号认证
	dot1x valid-ip-acct enable	配置获取 IP 后开始计费功能
	dot1x valid-ip-acct timeout	配置用户认证通过之后，允许等待该用户获取 IP 的时间，超过该时间用户未获取 IP 地址将被踢下线
	dot1x event server-invalid action bypass-wlan	配置 RADIUS 服务器逃生
	dot1x event server-invalid original-wlan action hide	配置 RADIUS 服务器逃生时的行为

方法 ↘ 配置开启 EAP 终结功能 ● 必选配置。 ● 当前仅支持这两种类型终结，可二者择其一，也可同时配置这两种类型	**dot1x encryption only**	配置 802.1x 和 WEB 认证共用
	dot1x logging rate-limit	配置认证用户上线和下线的日志速率限制
	dot1x offline-detect	配置基于 WLAN 的用户流量检查功能
	dot1x user-trap enable	配置 802.1x 认证用户上线下线的 Trap 消息通告
	dot1x mab-default-role	配置 MAB 认证成功后终端的默认角色
	dot1x dot1x-default-role	配置 802.1x 认证成功后终端的默认角色
	dot1x domain-name	配置 802.1x 认证域属性
	dot1x dbg-filter	配置过滤打印信息
	dot1x no-ip-before-mab	配置终端在 MAB 认证成功前终端不允许获取 IP

的终结。

相关命令

配置开启 EAP 终结功能

【命令格式】 **dot1x eap-terminate peap inner-methods** { **gtc** | **mschapv2** }

【参数说明】 **gtc :配置终结类型为 EAP-GTC 终结。mschapv2：配置终结类型为 EAP-MSCHAPv2 终结。**

【命令模式】 无线安全配置模式

【使用指导】

- 开启 GTC 终结时，设备认证方式从 EAP-GTC 转换为 PAP 认证，发送 PAP 认证请求给外部认证服务器。
- 开启 MSCHAPV2 终结时，设备从 PEAP-MSCHAPv2 协议中获取到 challenge 和 peer response 后，封装成一次 MSCHAPv2 认证报文后发送

1.4.2 配置 802.1x 基本功能

配置效果

- 提供基本的认证和计费服务。
- 有线环境下,使用接口模式下的配置端口 802.1x 命令可以启动或关闭接口上的 802.1x 认证功能.
- 无线环境下 ,WLAN 的安全模式为 WPA 或 WPA2 ,开启该 WLAN 的 802.1X 受控 ,连接该 WLAN 的 STA 必须通过 802.1x 认证才能通信.
- 通过 RADIUS 服务器命令配置服务器的 IP 和协议通信端口信息 ,配置设备和服务器间的 RADIUS 加密密钥 ,确保通信安全.
- 使用全局命令 **aaa accounting update** 命令开启计费更新，计费更新间隔可以在设备上通过 **aaa accounting uptate interval** 命令配置参数，也可以在服务器上配置，这取决于服务器是否支持该功能。如果服务器有下发，则优先使用服务器下发的参数，如果服务器没下发，则使用本机配置参数.

注意事项

- 注意 RADIUS 参数的配置准确性，确保基本的 RADIUS 协议通信正常。
- 802.1x 使用的认证方法列表和计费方法列表必须在 aaa 里面已经配置好了，否则会导致认证和计费出错。
- 如果端口 802.1x 开启并且认证的用户数大于端口安全的最大用户数，此时无法开启端口安全。
- 端口安全和 802.1x 同时开启时，如果安全地址老化，则 802.1x 对应的用户必须重新认证才可以继续通信。
- 静态地址或者符合 IP+MAC 绑定的用户无需认证即可访问网络。
- 802.1x 默认使用 default 方法类表，如果 aaa 配置的不是 default 方法列表，需要通过 dot1x authentication 和 dot1x accounting 命令重新制定 802.1x 使用的方法列表。
- 配合锐捷 SAM/SMP 软件使用时，必须配置计费功能，否则用户下线时服务器无法感知导致表项残留。

配置方法

↘ 开启 aaa

- 必须配置，开启 aaa 之后 802.1x 认证计费功能才会生效。
- 在使用 802.1x 对接入用户进行受控的设备开启

【命令格式】 **aaa new-model**
【参数说明】 **-**
【缺省配置】 关闭
【命令模式】 全局模式
【使用指导】 默认关闭，部署 802.1x 认证必须要配置该命令

配置 aaa 认证方法

- 必须配置。
- 需要和 801.x 使用的认证方法一致
- 在使用 802.1x 对接入用户进行受控的设备开启

【命令格式】 **aaa authentication dot1x** *list-name* **group radius**
【参数说明】 *list-name* ：aaa 的 dot1x 认证方法列表
【缺省配置】 关闭
【命令模式】 全局模式
【使用指导】 默认关闭
需要 802.1x 的认证方法一致

配置 RADIUS 服务器参数

- 必须配置，可以实现设备和 RADIUS 服务器的正常通信。
- 在使用 802.1x 对接入用户进行受控的设备开启

【命令格式】 **radius-server host** *ip-address* [**auth-port** *port1*] [**acct-port** *port2*]
【参数说明】 *ip-address*：指定服务器 IP 地址
port1 ：认证协议端口
port2 ：计费协议端口
【缺省配置】 默认无 RADIUS 服务器参数
【命令模式】 全局模式
【使用指导】 -

配置 RADIUS 服务器通信密钥

- 必须配置，可以实现设备和 RADIUS 服务器的正常通信。
- 在使用 802.1x 对接入用户进行受控的设备上开启

【命令格式】 **radius-server key** *string*
【参数说明】 *string*：RADIUS 通信密钥
【缺省配置】 默认无 RADIUS 通信密钥
【命令模式】 全局模式
【使用指导】 设备的 IP 地址必须和服务器上注册的设备地址一致
设备和服务器的通信的 key 也必须配置一致
如果服务器更改了默认的 RADIUS 通信端口，则配置时也需要指定协议端口

配置有线 802.1x

- 有线接口上必须配置。

【命令格式】 **dot1x port-control auto**
【参数说明】 -
【缺省配置】 关闭

【命令模式】 接口模式

【使用指导】 默认关闭，部署 802.1x 必须要配置该命令

默认使用 default 方法列表，如果 aaa 中的 802.1x 的方法列表不是 defautl，802.1x 的方法列表也需要匹配

配置无线 802.1x

- 必须配置。
- 在 AC 配置。
- WLAN 开启 802.1X 受控的时候，只允许 802.11 管理帧和 EAP 报文通过，其它报文全部被丢弃处理。
- 相关命令请见《RSNA》手册

检验方法

开启 supplicant 软件并发起认证，输入正确的账号并发起认证，通过 802.1x 的检查和 RADIUS 的检查确认配置是否准确。

通过 show dot1x summary 查看 802.1x 是否有创建认证表项

【命令格式】 **show dot1x summary**

【参数说明】 -

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 查看认证用户表项信息，通过该信息，可以知道认证终端当前处于什么阶段，例如正在认证、已经认证或者静默。

【命令展示】

```
Hostname#show dot1x summary
ID        Username   MAC            Interface VLAN Auth-State      Backend-state Port-Status
User-Type Time
--------- ---------- -------------- --------- ---- ---------------- ------------- -----------
--------- -----------------
16777302  ts-user    b048.7a7f.f9f3 wlan 1    1    Authenticated    Idle          Authed
static    0days 0h 0m12s
```

通过 show aaa user all 查看 aaa 是否有用户表项

【命令格式】 **show aaa user all**

【参数说明】 -

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 显示 AAA 用户相关信息。

【命令展示】

```
Hostname#show aaa user all
------------------------------

        Id ----- Name

 2345687901       wwxy

------------------------------
```

- 通过设备和服务器间的 RADIUS 报文检测服务器是否响应了认证，如果没有响应，则属于网络不通或者参数配置错误，如果服务器直接返回拒绝，则需要查看服务器的 log 文件，看是因为什么原因，例如服务器的认证方法配置错误等。

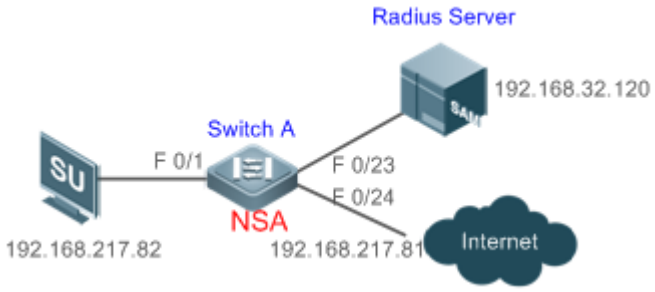
配置举例

以下配置举例，以锐捷 SAM 作为认证服务器。

配置有线 802.1x 认证

【网络环境】

图 1-6



【配置方法】

- 服务器上注册设备的 IP 信息，并配置设备和服务器的通信密钥
- 服务器上创建账号信息
- 设备开启 aaa
- 设备配置 RADIUS 参数
- 设备接口上开启 802.1x 认证

如下为设备上的相关配置，服务器端的配置请参考具体服务器的配置指导手册：

```
Hostname# configure terminal
Hostname (config)# aaa new-model
Hostname (config)# radius-server host 192.168.32.120
Hostname (config)# radius-server key Hostname
Hostname (config)# interface FastEthernet 0/1
Hostname (config-if)# dot1x port-control auto
```

【检验方法】

测试是否可以正常认证以及认证前后的网络访问行为是否变化。

- 服务器创建账号，例如 username:tests-user,password:test。
- 终端未认证前无法 ping 通 192.168.32.120。
- 终端打开 supplicant 后输入账号并点击认证，认证成功，可 ping 通 192.168.32.120。
- 可以显示认证通过的用户信息

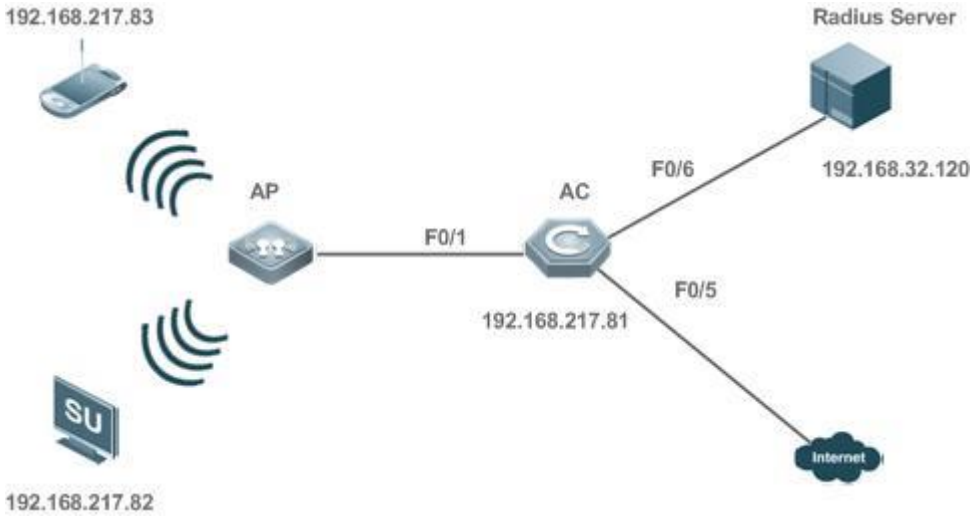
```
Hostname# show dot1x summary
ID        Username   MAC             Interface VLAN Auth-State      Backend-State
Port-Status User-Type Time
--------- ---------- --------------  --------- ---- --------------- -------------
----------- --------- ------------------
16778217  ts-user    0023.aeaa.4286  Fa0/1     2    Authenticated   Idle          Authed
```

```
static    0days 0h 0m 7s
```

配置无线 802.1x 认证

【网络环境】

图 1-7



【配置方法】

- 服务器上注册设备的 IP 信息，并配置设备和服务器的通信密钥
- 服务器上创建账号信息
- 设备开启 aaa
- 设备配置 RADIUS 参数
- 设备接口上开启 802.1x 认证

如下为设备上的相关配置，服务器端的配置请参考具体服务器的配置指导手册：

```
Hostname# configure terminal
Hostname (config)# aaa new-model
Hostname (config)# radius-server host 192.168.32.120
Hostname (config)# radius-server key Hostname
Hostname (config)# wlansec 1

Hostname(config-wlansec)# security rsn enable
Hostname(config-wlansec)# security rsn ciphers aes enable
Hostname(config-wlansec)# security rsn akm 802.1x enable
```

【检验方法】 测试是否可以正常认证以及认证前后的网络访问行为是否变化。

- 服务器创建账号，例如 username:tests-user,password:test。
- 终端未认证前无法 ping 通 192.168.32.120。
- 终端打开 supplicant 后输入账号并点击认证，认证成功，可 ping 通 192.168.32.120。
- 可以显示认证通过的用户信息

```
Hostname# show dot1x summary
ID        Username    MAC             Interface VLAN Auth-State      Backend-State
```

```
Port-Status User-Type Time
--------- ---------- --------------  --------- ---- --------------- -------------
----------- --------- ------------------
16778217  ts-user    0023.aeaa.4286  wlan 1     2    Authenticated   Idle          Authed
static    0days 0h 0m 7s
```

常见错误

- RADIUS 参数配置错误。
- 服务器有特殊的接入策略，例如要求 RADIUS 报文必须携带某些属性等。
- aaa 的方法列表和 802.1x 的方法类表不一致导致无法认证

1.4.3 配置 802.1x 协议参数

配置效果

- 根据网络实际情况调整协议的参数值，例如服务器性能较差的环境中，可以将服务器超时时间适当配大。

注意事项

- 802.1x 协议和 RADIUS 协议都有对应的服务器超时参数，默认情况下，802.1x 的超时参数是 5 秒，小于 RADIUS 的超时参数 15 秒。实际使用时，需要确保 802.1x 的服务器超时参数大于 RADIUS 的服务器超时参数。可使用 dot1x 服务器超时配置命令将 802.1x 的超时参数配置大, RADIUS 的超时规则请参考 RADIUS 配置手册.
- 锐捷客户端在线检测功能仅适用于锐捷 supplicant。

配置方法

↘ 开启重认证

- 可选配置，开启后即可定期对在线用户重认证。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x re-authentication**
【参数说明】 **-**
【缺省配置】 默认关闭
【命令模式】 全局模式
【使用指导】 在需要对认证用户定时重认证时可以配置此命令

↘ 配置重认证间隔

- 可选配置，配置用户的重认证周期。
- 在设备开启 802.1x 认证之后配置，开启重认证功能后生效

【命令格式】 **dot1x timeout re-authperiod** *period*
【参数说明】 *period*：重认证间隔，单位秒，默认 3600 秒
【缺省配置】 默认 3600 秒
【命令模式】 全局模式
【使用指导】 根据需要来调整认证用户的重认证间隔

配置 request/id 报文重传间隔

- 可选配置，设备重传报文的周期，周期越长则报文重传时间也越长。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x timeout tx-period** *period*
【参数说明】 *period*：报文重传间隔，单位秒，默认 4 秒
【缺省配置】 默认 4 秒
【命令模式】 全局模式
【使用指导】 使用默认值即可，根据认证客户端响应设备请求的时间长短来调整该数值

配置 request/id 报文重传次数

- 可选配置，设备重传报文的次数，数值越大，重传次数就越大。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x reauth-max** *num*
【参数说明】 *num*：报文重传次数，默认 6
【缺省配置】 默认 6 次
【命令模式】 全局模式
【使用指导】 使用默认值即可，容易丢包的环境增大该值可以提高客户端收到设备报文的概率

配置 request/challenge 报文重传间隔

- 可选配置，设备重传 request/challenge 报文的间隔，数值越大，重传间隔就越大。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x timeout supp-timeout** *time*
【参数说明】 *time*：报文重传间隔，单位秒，默认 3 秒
【缺省配置】 默认 3 秒
【命令模式】 全局模式
【使用指导】 使用默认值即可，容易丢包的环境中可以增大该数值

配置 request/challenge 报文重传次数

- 可选配置，设备重传 request/challenge 报文的次数，数值越大，重传次数就越大。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x max-req** *num*
【参数说明】 *num*：报文重传次数，单位秒，默认 3
【缺省配置】 默认 3 次
【命令模式】 全局模式
【使用指导】 可选配置
使用默认值即可，容易丢包的环境中可以增大该数值

配置服务器超时时间

- 可选配置，设备服务器超时时间，数值越大，等待服务器超时的时间就越长。
- 在设备开启 802.1x 认证之后配置
- RADIUS 和服务器之间的通信超时必须大于 802.1x 的服务器超时时间

【命令格式】 **dot1x timeout server-timeout** *time*
【参数说明】 *time*：服务器超时时间，单位秒，默认 5 秒
【缺省配置】 默认 5 秒
【命令模式】 全局模式
【使用指导】 使用默认值即可，设备和服务器通信不稳定的环境中可以增大该数值

配置认证失败后的静默时间

- 可选配置，用户认证失败后的时间，数值越大，静默用户的时间就越长。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x timeout quiet-period** *time*
【参数说明】 *time*：认证失败后的静默时间，单位秒，默认 10 秒
【缺省配置】 默认 10 秒
【命令模式】 全局模式
【使用指导】 使用默认值即可，增大该数值可以降低认证失败的用户频繁向服务器发起认证增加服务器的负担

配置认证模式

- 可选配置，配置 802.1x 认证方式。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x auth-mode** {**eap** | **chap** | **pap**}
【参数说明】 eap：采用 eap 方式认证
chap ：采用 chap 方式认证
pap ：采用 pap 方式认证
【缺省配置】 默认 eap
【命令模式】 全局模式
【使用指导】 认证模式的选择取决于 supplicant 和认证服务器的支持情况。

配置锐捷客户端在线检测

- 可选配置，配置锐捷在线客户端检测功能，开启该功能之后，可以及时发现客户端下线，避免对用户的错误计费。

- 客户端必须是锐捷 802.1x 认证客户端
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x client-probe enable**
【参数说明】 -
【缺省配置】 默认关闭
【命令模式】 全局模式
【使用指导】 使用锐捷 supplicant 时建议开启该功能。

配置锐捷客户端在线报文发送周期

- 可选配置，配置锐捷在线客户端报文发送周期，该数值越大，客户端发送检测报文的时间间隔就越长。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x probe-timer interval** *time*
【参数说明】 *time*：锐捷 supplicant 向设备发送心跳报文的时间间隔，单位秒，默认 20 秒
【缺省配置】 默认 20 秒
【命令模式】 全局模式
【使用指导】 建议使用默认值即可

配置锐捷客户端在线检测时长

- 可选配置，配置锐捷在线客户端检测时长，该数值越大，判断客户端下线的时间间隔就越长。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x probe-timer alive** *time*
【参数说明】 *time*：报文检测时长，单位秒，默认 250 秒
【缺省配置】 默认 250 秒
【命令模式】 全局模式
【使用指导】 可选配置
终端认证上线后，在检测时长内设备没收到终端的任何探测报文响应，则认为终端下线，建议使用默认值即可

检验方法

可以通过 show dot1x 查看参数配置是否生效。

配置举例

配置认证模式

【网络环境】 单机
【配置方法】 配置认证模式为 chap：

```
Hostname(config)#dot1x auth-mode chap
```

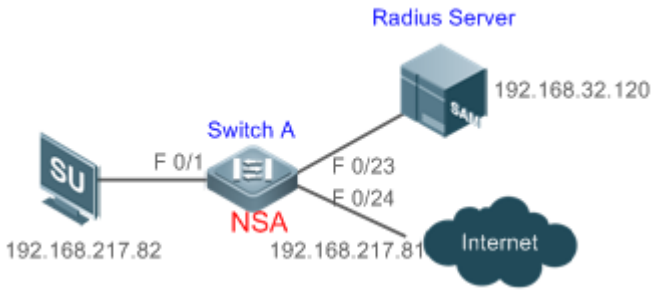
【检验方法】 显示配置结果。

```
Hostname(config)#show dot1x

802.1X basic information:
  802.1X Status ..................... enable
  Authentication Mode ................ chap
  Authorization mode ................. disable
  Total User Number .................. 0 (exclude dynamic user)
  Authenticated User Number .......... 0 (exclude dynamic user)
  Dynamic User Number ................ 0
  Re-authentication .................. disable
  Re-authentication Period ........... 3600 seconds
  Re-authentication max .............. 3 times
  Quiet Period ....................... 10 seconds
  Tx Period .......................... 30 seconds
  Supplicant Timeout ................. 3 seconds
  Server Timeout ..................... 5 seconds
  Maximum Request .................... 3 times
  Client Online Probe ................ disable
  Eapol Tag .......................... disable
  802.1x redirect .................... disable
  Private supplicant only ............ disable
```

配置锐捷客户端在线检测

【网络环境】

图 1-8



【配置方法】 开启锐捷客户端在线检测功能：

```
Hostname(config)#dot1x client-probe enable
```

- 由锐捷 supplicant 客户端有按时发送在线检测报文的才能持续在线

【检验方法】

- 显示配置结果。

```
Hostname(config)#show dot1x

802.1X basic information:
  802.1X Status ..................... enable
```

```
Authentication Mode ..................... chap
Authorization mode ...................... disable
Total User Number ....................... 0 (exclude dynamic user)
Authenticated User Number ............... 0 (exclude dynamic user)
Dynamic User Number ..................... 0
Re-authentication ....................... disable
Re-authentication Period ................ 3600 seconds
Re-authentication max ................... 3 times
Quiet Period ............................ 10 seconds
Tx Period ............................... 30 seconds
Supplicant Timeout ...................... 3 seconds
Server Timeout .......................... 5 seconds
Maximum Request ......................... 3 times
Client Online Probe ..................... enable
Eapol Tag ............................... disable
802.1x redirect ......................... disable
```

常见错误

- server-timeout 比 RADIUS 超时参数小。
- 认证软件不是锐捷 supplicant 却配置了客户端在线检测功能。

1.4.4 配置授权

配置效果

- 配置 IP 授权可限定认证用户必须使用指定的 IP 地址访问网络，可以防止 IP 盗用等问题。
- 配置过滤非锐捷客户端功能，可以限定终端必须使用锐捷 supplicant 软件认证，从而能够享受到锐捷 supplicant 提供的相关服务，例如防代理或者短消息等功能。
- 配置 redirect 功能 ,可以支持二代 su 部署。所谓的二代 su 部署是指终端先通过网页下载 supplicant 软件 ,再通过 supplicant 软件认证。二代 su 部署在用户量大的环境中有利于 su 的快速部署。

注意事项

- 如果使用锐捷 SAM/SMP 软件的实时踢线功能，需要配置正确的 snmp 参数，详细可参考 snmp 配置手册。
- 环境中有多种认证客户端软件时，不能开启过滤非锐捷客户端功能。
- 更改 IP 授权模式会导致已认证用户全部下线，需要重新认证才可以上网。

- 使用混合授权模式时，用户在认证上线过程中如果更高优先级的 IP 授权出现，则使用高优先级的 IP 授权，例如原来用户使用 RADIUS 授权，再一次认证时，如果 supplicant 提供了 IP 地址，则使用该 IP 地址进行授权。
- 二代 su 部署功能和 web 认证无法同时使用。
- 二代 su 部署需要配置重定向参数，具体请参考 web 认证配置手册。
- 锐捷 SAM/SMP 的踢线功能使用 snmp 协议，因此需要配置 snmp 参数，具体可参考 snmp 的配置说明

配置方法

配置 IP 授权模式

- supplicant 授权模式仅支持锐捷 supplicant
- RADIUS-server 授权模式需要服务器支持通过 framed-ip 属性下发 IP 地址
- dhcp-server 授权模式需要设备同时开启 dhcp snooping 或者开启 dhcp relay

配置 IP 授权模式

- 可选配置，配置对用户绑定 IP 和 MAC 的模式。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **aaa authorization ip-auth-mode** { **disable | supplicant | radius-server | dhcp-server | mixed** }

【参数说明】 **disable** ：关闭 IP 授权
supplicant ：supplicant 授权 IP
radius-server：RADIUS 服务器授权 IP
dhcp-server ：dhcp 服务器授权 IP
mixed ：混合授权 IP

【缺省配置】 **关闭**

【命令模式】 全局模式

【使用指导】 根据环境部署情况选择 IP 授权模式。

配置二代 su 部署

- 可选配置，配置第二代 su 部署，配置之后，受控口上的无 802.1x 认证客户端的用户可以通过 web 页面下载安装 802.1x 认证客户端。
- 在设备开启 802.1x 认证之后配置
- 必须配置重定向参数，具体请参考 web 认证配置手册。

【命令格式】 **dot1x redirect**

【参数说明】 -

【缺省配置】 关闭

【命令模式】 全局模式

【使用指导】 需要配置好重定向参数，具体参考 web 认证配置手册

配置过滤非锐捷客户端

- 可选配置，开启之后非锐捷客户端无法认证。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x private-supplicant-only**
【参数说明】 -
【缺省配置】 关闭
【命令模式】 全局模式
【使用指导】 要限制终端必须使用锐捷 supplicant 软件认证时才可以配置该功能

检验方法

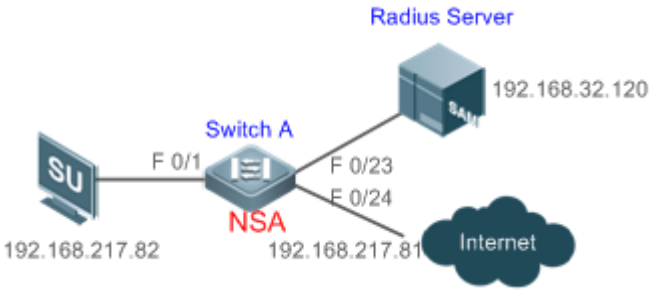
- 开启 IP 授权后，客户端先认证上线，之后更改客户端的 IP 地址，客户端无法访问网络
- 开启二代 su 部署，打开浏览器访问网址时，会自动重定向到下载页面并下载认证客户端，通过客户端认证通过后才可以访问网络。
- 用户认证上线后，在锐捷 SAM/SMP 上执行踢线功能，设备会将用户下线，此时用户就无法问网络

配置举例

配置 IP 授权模式

【网络环境】

图 1-9



【配置方法】
- 配置 aaa
- 配置 RADIUS
- 受控口开启 802.1x 功能
- 全局开启 supplicant 授权

```
Hostname(config)#aaa authorization ip-auth-mode supplicant
```

- 由锐捷 supplicant 客户端发起认证，认证成功
- 该认证客户端只能使用 192.168.217.82 地址进行通信

【检验方法】
- 显示配置结果。

```
Hostname(config)#show dot1x user name ts-user
Supplicant information:
  MAC address ..... b048.7a7f.f9f3
  Username ..... ts-user
```

```
User ID ............................. 16777303
Type ................................ static
VLAN ................................ 1
Port ................................ wlan 1
Online duration ..................... 0days 0h 0m21s
Up average bandwidth ................ 0 kBps
Down average bandwidth .............. 0 kBps
Authorized VLAN ..................... 1
Authorized session time ............. 20736000 seconds
Authorized flux ..................... unlimited
Accounting .......................... No
Proxy user .......................... Permit
Dial user ........................... Permit
IP privilege ........................ 0
Private supplicant .................. no
Max user number on this port ........ 0
Authorization ip address ............ 192.168.217.82
```

常见错误

- 网络中有多种认证客户端，但是开启了过滤非锐捷客户端功能，导致部分终端无法认证。
- 使用锐捷 SAM/SMP，但是设备没有配置 snmp 参数导致踢线功能失败。
- 未正确配置重定向参数导致二代 su 升级功能无法正常使用。

1.4.5 配置 MAB

配置效果

- 使用接入终端的 MAC 地址作为认证账号，终端无需安装认证客户端软件，适用于哑终端，例如网络打印机等。
- 单 MAB 适用于端口下只有一个哑终端的情况，或者只有一个终端需要认证，认证后其他终端都可以访问网络，例如端口下连了一个无线路由器，可以配置对无线路由器实时 MAB 认证，认证通过后，无线路由器下的用户均可以访问网络。
- 多 MAB 适用于端口下存在多种哑终端的情况，例如网络呼叫中心部署多台 voip 接入等。
- 多 MAB 支持和 802.1x 认证混合使用，适用于混合接入环境，例如 pc+voip 菊花链接入的方式。
- 无线环境下支持基于 WLAN 开启 MAB 认证，部署该功能之后，设备自动将关联相应 WLAN 的 STA 的 MAC 作为用户名和密码向服务器发起认证

注意事项

- 配置了 MAB 的端口，每隔 tx-period 发出一个认证请求报文，发送 reauth-max 次之后，如果没有客户端响应，则该端口进入 MAB 模式。进入 MAB 模式的端口可以学习 MAC 地址,并使用这些 MAC 地址为账号进行认证
- 服务器配置 MAC 账号的用户名和密码时，必须使用不带分隔符的格式，例如终端 MAC 地址为 00-d0-f8-00-01-02，服务器上添加帐号时需要配置为 00d0f8000102。
- 802.1x 优先级高于 MAB，因此一个终端先 MAB 认证通过后，如果再使用客户端软件做 802.1x 认证，MAB 的表项将被删除。
- MAB 仅支持 PAP 认证模式，服务器上的配置需要注意。
- MAB 功能主要主动发现终端是否可以做 802.1x 认证，通过主动认证来实现该目的，因此部署 MAB 的同时必须同时开启主动认证功能。
- 无线的 WLAN 开启 MAB 认证时，该 WLAN 的安全模式必须是 OPEN 模式。

配置方法

配置单 MAB

- 可选配置
- 适用于一个端口下只有一个终端需要认证的场景。
- 在设备的 802.1x 受控口配置

【命令格式】 **dot1x mac-auth-bypass**
【参数说明】 **-**
【缺省配置】 关闭
【命令模式】 接口模式
【使用指导】 如果要限制终端数量，可以配置违例处理。

配置 MAB 超时时间

- 可选配置
- MAB 模式下的 MAC 地址认证上线后，除非重认证失败、端口 down 或者因为管理策略原因下线，例如管理员强制下线等，否则设备将认为该 MAC 地址一直是可以在线的。用户可以配置许可这些认证地址的在线时间，默认是 0，表示允许一直在线。
- 在设备的 802.1x 受控口配置

【命令格式】 **dot1x mac-auth-bypass timeout-activity** *value*
【参数说明】 *value*：MAB 可在线时间，单位为秒，默认为 0，表示不限制时间
【缺省配置】 默认为 0，表示不限制时间
【命令模式】 接口模式
【使用指导】 对单 MAB 和对 MAB 均适用

配置 MAB 违例

- 可选配置
- 在设备的 802.1x 受控口配置
- 默认情况下，有一个 MAC 地址通过 MAB 认证后，该端口下的所有设备的数据都允许被转发。但是在某些安全应用下，管理员会要求一个 MAB 端口下只能有一个 MAC 地址存在，此时可以在该端口上配置 MAB 违例。配置了 MAB 违例后，一旦端口进入了 MAB 模式，如果发现该端口下有超过 1 个 MAC 地址，该端口将产生违例。

【命令格式】 **dot1x mac-auth-bypass violation**
【参数说明】 -
【缺省配置】 关闭
【命令模式】 接口模式
【使用指导】 要限制端口下只有一个哑终端时可以配置该命令，其它场景不能配置。

仅适用于单 MAB

配置多 MAB

- 可选配置
- 在设备的 802.1x 受控口配置

【命令格式】 **dot1x mac-auth-bypass multi-user**
【参数说明】 -
【缺省配置】 关闭
【命令模式】 接口模式
【使用指导】 端口下多哑终端需要做安全认证时配置该命令

配置多 MAB 认证失败的静默时间

- 可选配置
- 在设备的开启了多 mab 功能之后配置
- 开启多 MAB 认证功能时，为了防止接口下的非法用户对设备进行攻击，需要禁止非法用户频繁认证，以减少服务器的压力。在全局下配置多 MAB 用户的静默时间，默认为 30s，也就是说，如果一个 MAC 地址并认证失败后，该 MAC 地址需要等待 30s 才会重新发起认证。静默时间可以根据环境进行配置，如果配置为 0，表示一个用户认证失败后可以马上进行再认证。

【命令格式】 **dot1x multi-mab quiet-period** *value*
【参数说明】 *value*：认证失败后的静默时间
【缺省配置】 默认为 0s
【命令模式】 全局模式
【使用指导】 端口下认证的哑终端太多时间以配置该命令限制认证频率。

配置 MAB VLAN

- 可选配置
- 在设备的开启了多 mab 功能之后配置

- 为了仅允许接口上部分 VLAN 内的用户进行 MAB 认证，可以将这些 VLAN 配置成 MAB VLAN，不在 MAB VLAN 之内的用户不能进行 MAB 认证。

【命令格式】 **dot1x mac-auth-bypass vlan** *vlan-list*
【参数说明】 *vlan-list*：允许进行 MAB 认证的 VLAN
【缺省配置】 关闭
【命令模式】 接口模式
【使用指导】 端口下仅允许相应的 VLAN 内的用户进行 MAB 认证时可以使用此命令

配置无线 MAB

- 可选配置
- 在 WLAN 上配置

【命令格式】 **dot1x-mab**
【参数说明】 -
【缺省配置】 关闭
【命令模式】 wlansec 模式
【使用指导】 WLAN 下客户端需要使用其 MAC 需要做安全认证时配置该命令
仅无线平台可用

检验方法

通过哑终端接入网络是否可以访问网络验证 MAB 是否生效。

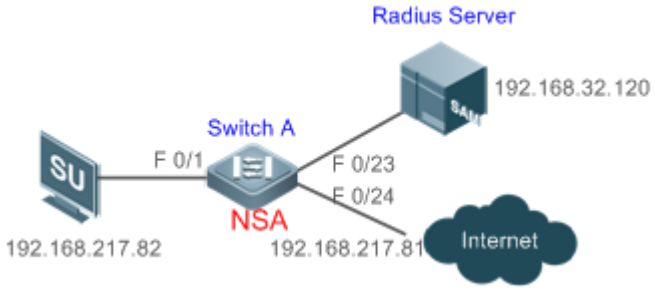
- 服务器和设备上先配置好 MAB 相关功能
- 不符合 MAC 地址账号的哑终端接入，无法访问网络
- 符合 MAC 地址账号的哑终端接入，可以访问网络

配置举例

配置有线的多 MAB 认证

【网络环境】

图 1-10



【配置方法】
- 服务器上注册设备的 IP 信息，并配置设备和服务器的通信密钥
- 服务器上创建账号信息

- 设备开启 aaa
- 设备配置 RADIUS 参数
- 设备接口上开启 802.1x 认证和多 MAB 认证功能

如下为设备上的相关配置，服务器端的配置请参考具体服务器的配置指导手册：

```
Hostname# configure terminal
Hostname (config)# aaa new-model
Hostname (config)# radius-server host 192.168.32.120
Hostname (config)# radius-server key Hostname
Hostname (config)# interface FastEthernet 0/1
Hostname (config-if)# dot1x port-control auto
Hostname (config-if)# dot1x mac-auth-bypass multi-user
```

【检验方法】 测试是否可以正常认证以及认证前后的网络访问行为是否变化。

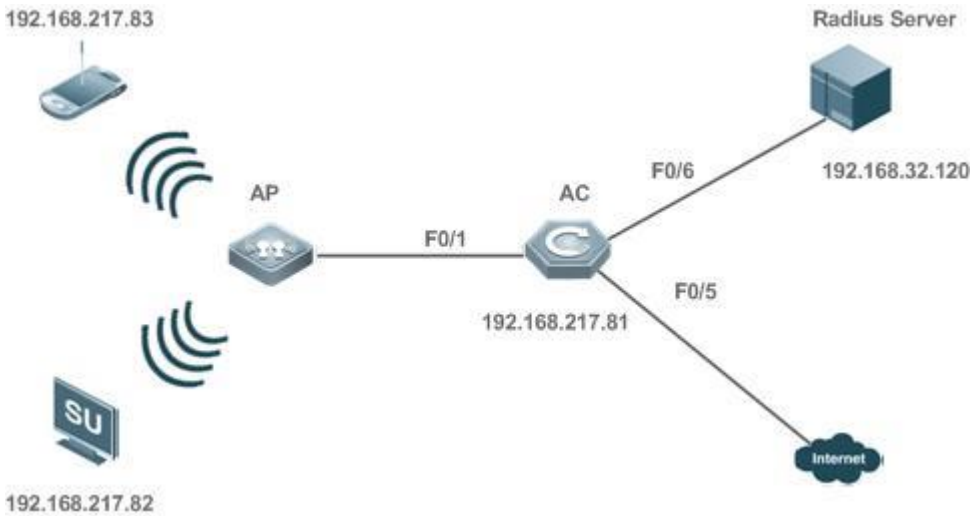
- 服务器创建账号，例如 username: 0023aeaa4286,password: 0023aeaa4286。
- 终端未认证前无法 ping 通 192.168.32.120。
- 终端连接上设备，认证成功，可 ping 通 192.168.32.120。
- 可以显示认证通过的用户信息

```
Hostname# show dot1x summary
ID        Username   MAC             Interface VLAN Auth-State      Backend-State
Port-Status User-Type Time
--------- ---------- --------------  --------- ---- ---------------- -------------
----------- --------- ------------------
16778217  0023aea...  0023.aeaa.4286  Fa0/1     2    Authenticated   Idle          Authed
static    0days 0h 5m 8s
```

配置无线 MAB 认证

【网络环境】

图 1-11



【配置方法】

- 服务器上注册设备的 IP 信息，并配置设备和服务器的通信密钥
- 服务器上创建账号信息
- 设备开启 aaa
- 设备配置 RADIUS 参数
- 设备 WLAN 上开启 MAB 认证功能

如下为设备上的相关配置，服务器端的配置请参考具体服务器的配置指导手册：

```
Hostname# configure terminal
Hostname (config)# aaa new-model
Hostname (config)# radius-server host 192.168.32.120
Hostname (config)# radius-server key Hostname
Hostname(config)#wlansec 1
Hostname(config-wlansec)#dot1x-mab
```

【检验方法】 测试是否可以正常认证以及认证前后的网络访问行为是否变化。

- 服务器创建账号，例如 username: 0023aeaa4286,password: 0023aeaa4286。
- 终端未认证前无法 ping 通 192.168.32.120。
- 终端连接上设备，认证成功，可 ping 通 192.168.32.120。
- 可以显示认证通过的用户信息

```
Hostname# show dot1x summary
ID        Username   MAC             Interface VLAN Auth-State      Backend-State
Port-Status User-Type Time
--------- ---------- --------------  --------- ---- ---------------- -------------
----------- --------- ------------------
16778217  0023aea...  0023.aeaa.4286  wlan 1    2    Authenticated   Idle          Authed
static    0days 0h 5m 8s
```

常见错误

- 服务器上的 MAC 账号格式不准确。

1.4.6 配置 EAP 终结功能

配置效果

配置后可将复杂的 EAP 认证协议终结在设备上，代理转发 EAP 协议中包含的简单认证信息到外部服务器上，使得设备能够适配那些无法提供所需 EAP 方法的外部认证服务器。

配置方法

配置开启 EAP 终结功能

- 必选配置。
- 当前仅支持这两种类型终结，可二者择其一，也可同时配置这两种类型的终结。

相关命令

配置开启 EAP 终结功能

【命令格式】 **dot1x eap-terminate peap inner-methods** { **gtc** | **mschapv2** }

【参数说明】 **gtc**：配置终结类型为 EAP-GTC 终结。

mschapv2：配置终结类型为 EAP-MSCHAPv2 终结。

【命令模式】 无线安全配置模式

【使用指导】
- 开启 GTC 终结时 ,设备认证方式从 EAP-GTC 转换为 PAP 认证 ,发送 PAP 认证请求给外部认证服务器。
- 开启 MSCHAPV2 终结时，设备从 PEAP-MSCHAPv2 协议中获取到 challenge 和 peer response 后，封装成一次 MSCHAPv2 认证报文后发送给外部认证服务器。
- dot1x 的 EAP 终结支持 VAC 场景。
- 同时开启 dot1x 的 EAP 终结和 local eap 终结功能，在 dot1x 终结完成后流量还会到 local eap 中进行处理，不过会判定为不需要终结。
- 当需要配置 EAP 终结时建议使用 dot1x 的 EAP 终结。

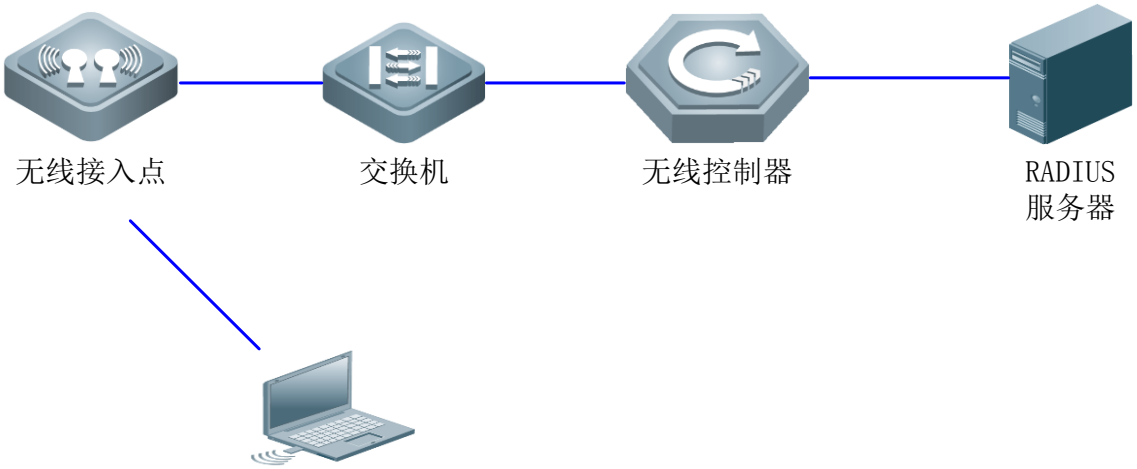
配置举例

以下配置举例，仅介绍与 EAP 终结密切相关的配置。

配置开启 EAP-GTC 终结功能。

【网络环境】

图 1-112



【配置方法】
- 配置 WLAN。
- 配置无线安全使用 802.1X 接入认证方式。

- 配置 AAA 的 802.1X 认证方法列表。
- 配置 RADIUS 服务器。
- 配置启用 dot1x 的 EAP 终结功能。

交换机

将交换机下联口划入 AP 所属 VLAN 100

```
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# poe enable
Hostname(config-if-GigabitEthernet 0/1)# switchport access vlan 100
```

将交换机上联口配置为 trunk 口

```
Hostname(config)# exit
Hostname(config)# interface GigabitEthernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# switchport mode trunk
```

无线控制器

将与交换机相连的 GigabitEthernet 0/1 口配置为 trunk 口

```
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode trunk
```

配置 Loopback 0 的 IP 地址，以便无线控制器和无线接入点之间建立 CAPWAP 隧道

```
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# interface Loopback 0
Hostname(config-if-Loopback 0)# ip address 10.1.1.1 255.255.255.255
```

配置 AP VLAN 100 及 STA VLAN 10，同时作为 VLAN 100 和 VLAN 10 的 DHCP 服务器

```
Hostname(config)#vlan 100
Hostname(config-vlan)#exit
Hostname(config)#interface vlan 100
Hostname(config-if-VLAN 100)# ip address 192.168.100.1 255.255.255.0
Hostname(config)#vlan 10
Hostname(config-vlan)#exit
Hostname(config)#interface vlan 10
Hostname(config-if-VLAN 100)# ip address 192.168.10.1 255.255.255.0
Hostname(config-if-VLAN 100)# exit
Hostname(config)# service dhcp
Hostname(config)# ip dhcp pool ap_vlan100
Hostname(dhcp-config)# option 138 ip 10.1.1.1    # 这个必须是 Loopback 0 口所配置的 IP 地址
Hostname(dhcp-config)# network 192.168.100.0 255.255.255.0 192.168.100.10 192.168.100.100
Hostname(dhcp-config)# default-router 192.168.100.1
Hostname(dhcp-config)# exit
Hostname(config)# ip dhcp pool sta_vlan10
Hostname(dhcp-config)# network 192.168.100.0 255.255.255.0 192.168.10.10 192.168.10.100
Hostname(dhcp-config)# default-router 192.168.10.1
Hostname(dhcp-config)# exit
```

```
# 配置 WLAN
Hostname(config)#wlan-config 1 miaosf_eap
Hostname(config-wlan)#exit
Hostname(config)#ap-group default
Hostname(config-ap-group)#interface-mapping 1 10
Hostname(config-ap-group)# exit
# 配置无线安全使用 802.1X 接入认证方式
Hostname(config)#wlansec 1
Hostname(config-wlansec)# security rsn enable
Hostname(config-wlansec)# security rsn ciphers aes enable
Hostname(config-wlansec)# security rsn akm 802.1x enable
Hostname(config-wlansec)# exit
# 配置 AAA 的 802.1X 认证方法列表及认证终结
Hostname(config)#wlansec 1
Hostname(config-wlansec)# dot1x authentication default
Hostname(config-wlansec)# dot1x eap-terminate peap inner-methods gtc
Hostname(config-wlansec)#dot1x eap-terminate peap inner-methods mschapv2
Hostname(config)# aaa new-model
Hostname(config)# aaa authentication login default none
Hostname(config)# aaa authentication dot1x default group radius
# 配置 RADIUS 服务器
Hostname(config)# radius-server host 192.168.197.79
Hostname(config)# radius-server key ruijie
```

【检验方法】 假设 radius 服务器上配置的用户名为 admin，密码为 admin，则只要在 STA（如：手机）上输入用户名 admin，密码 admin，即可正常地连接至 WLAN miaosf_eap。

常见错误

AAA 的 802.1X 认证方法列表配置错误。

1.4.7 配置 PKI 信息

配置效果

设备可自己生成的自签名 PKI 信息，或者是用户通过命令行导入的 PKCS#12 格式的 PKI 信息。

配置方法

↘ 配置重新生成自签名 PKI

- 可选配置。
- 当设备中不存在 PKI 信息时，设备会自动生成自签名的 PKI 信息，一般不需要用户通过命令行来生成。当出于某些原因，例如安全原因时，用户可以通过如下步骤重新生成自签名的 PKI 信息。

↘ 配置导入 PKCS#12 格式的 PKI

- 可选配置。
- 当设备生成的自签名 PKI 信息不满足用户需求时，用户可以通过 PKCS#12 格式的文件（一般后缀为.pfx 或者.p12）导入所需的 PKI 信息到设备中。
- 需要注意的是：导入证书会使正在认证的终端认证失败。

检验方法

- 通过 **show dot1x pki** [**self-signed | pfx** 查看 dot1x 中的 PKI 信息。

相关命令

↘ 配置重新生成自签名 PKI 信息

【命令格式】 **dot1x pki-manage generate self-signed**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】
- 当设备中不存在 PKI 信息时，设备会自动生成自签名的 PKI 信息，一般不需要用户通过命令行来生成。当出于某些原因，例如安全原因时，用户可以通过该命令重新生成自签名的 PKI 信息。
- 生成的 PKI 信息会被保存到 Flash 中，在系统启动的时候从 Flash 中载入。命令不会被保存在配置文件中。

↘ 配置导入 PKCS#12 格式的 PKI 信息

【命令格式】 **dot1x pki-manage import pfx** *filepath* [**password** *password*]

【参数说明】 *filepath：*PKCS#12 文件在设备 Flash 上的路径

*password：*可选的解密导入文件的密码，当文件没有加密时，不需要输入密码

【命令模式】 全局配置模式

【使用指导】
- 当设备生成的自签名 PKI 信息不满足用户需求时，用户可以通过 PKCS#12 格式的文件（一般后缀为.pfx 或者.p12）导入所需的 PKI 信息，导入的信息会被保存到 Flash 中，系统启动的时候从 Flash 中载入。该命令不会被保存在配置文件中。
- 用户导入的 PKI 信息的优先级比设备生成的优先级高，当设备生成的自签名 PKI 信息和用户导入的 PKI 信息都存在时，设备会使用用户导入的 PKI 信息。当设备启动的时候，发现以上两种 PKI 信息都不存在时，设备会自动生成一套自签名的 PKI 信息，并且投入使用。

配置举例

↘ 上传 PKCS#12 文件到设备上，配置 dot1x 导入 PKCS#12 格式的 PKI 信息。

【配置方法】

- 上传 PKCS#12 文件到设备上。
- 配置 dot1x 导入 PKCS#12 格式的 PKI 信息

上传 PKCS#12 文件到设备上

```
Hostname# copy tftp://192.168.1.1/pki.pfx flash:pki.pfx
```

配置 dot1x 导入 PKCS#12 格式的 PKI 信息

```
Hostname# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#dot1x pki-manage import pfx pki.pfx password filepassword
Import PKI from file [pki.pfx] successfully
```

【检验方法】

- 通过 **show dot1x pki** [**self-signed | pfx** 查看 dot1x 中的 PKI 信息。

```
Hostname#show dot1x pki summary
       TYPE       ACTIVATED
----------------------------
   Self-Signed      Yes
 * PFX-Imported     Yes
```

1.4.8 扩展功能配置

配置效果

- 部分终端采用操作系统自带认证客户端，这些客户端在终端接入网络后不一定会马上发起认证，影响用户使用网络，使用主动认证功能，可以促使这些终端接入网络后及时发起认证。
- 主动认证是指设备主动发出 request/id 报文，该报文可触发 supplicant 执行 802.1x 认证，因此可以利用该功能检测终端是否有使用 supplicant 软件，例如部署 MAB 时就需要使用此功能。
- 可认证主机列表可以限制接入端口下哪些终端可以认证，通过控制终端的接入物理位置来提高网络安全性。
- 多账号功能支持一个终端重认证时切换账号，对于特殊场景，例如 windows 的域认证，存在接入域时多次认证且认证时会变更账号，该功能适用这类场景。
- 默认情况下，设备使用设备本机的 MAC 地址作为 802.1x 认证时的 eap 报文源 MAC 地址。锐捷 supplicant 的部分版本，会根据 eap 报文的源 MAC 地址来判断接入设备是否为锐捷设备，并实施私有特性，和这些 supplicant 配合做 802.1x 认证时，如果要使用相关私有特性，可以开启虚拟源 MAC 地址功能。
- 802.1X 支持用户获取 IP 地址后再开始计费，从而可以满足服务器要求用户计费时必须携带 IP 地址的要求。用户先认证上线，可以从 supplicant 或者 dhcp snooping 等获用户的 IP，获取到 IP 地址后 802.1x 才会发起计费请求。为避免设备长时间没有获取到认证客户端的 IP 导致一直不发起计费，该功能配备了一个 IP 检测超时时间。如果在配置的时间内（默认 5min）没有获取到终端的 IP 地址，则将用户下线。

- 802.1X 功能支持 RADIUS 认证服务器不可用时 ,切换到预先配置的逃生 WLAN 功能。逃生 WLAN 一般是 OPEN 模式的，且服务默认不可用，当 802.1X 认证的 WLAN 服务不可用时打开该 WLAN 的服务，同时关闭 802.1x 认证的 WLAN 服务，用户切换到逃生 WLAN，可以正常访问网络。
- 802.1X 功能支持与 WEB 认证共用，当一个 WLAN 配置成与 WEB 认证共用时，进行 802.1X 认证的用户只起到加密作用，用户需要访问网络，还要进行 WEB 认证，用户的空口数据都是经过加密的，提高用户数据的安全性。
- 802.1X 功能支持对无线认证用户上线下线的打印 syslog 进行提示，可以根据认证环境中的用户认证速率调整用户上线下线的 syslog 的打印速率，避免大量用户上线下线而频繁打印 syslog 引起 CPU 利用率偏高。
- 在无线 802.1x 认证环境中，支持对认证用户上线和下线发送 SNMP Trap 消息给服务器，以通告认证用户上线和下线情况。
- 在无线 802.1x 认证环境中，支持基于 WLAN 开启流量监测功能，即通过认证的终端如果在指定时间内流量低于配置的阈值，将会被下线，使得服务器的计费可以及时处理。
- 802.1x 功能支持在获取了认证客户端的终端信息之后再向服务器发起计费，从而可以将认证客户端的终端信息传递到服务器。在有线设备上为避免长时间没有获取到认证客户端的终端信息，允许配置相应的超时时间，超过该时间设备如果还没有获取到终端信息，可以将终端踢下线。
- 在无线 802.1x 认证环境中，支持基于 WLAN 开启域认证功能，即通过在 WLAN 下配置域名，让不带域名的认证账户通过配置域名下的认证服务器进行认证。

注意事项

- 部署计费的环境中，不能开启多帐号功能，否则会影响计费准确性。
- MAB 认证需要使用到主动认证，因此部署 MAB 的环境必须开启主动认证功能
- 配置用户获取 IP 地址之后再开始计费时，需要注意：IPv4 环境且部署了锐捷 supplicant 客户端，由于 supplicant 具备上传终端 IPv4 地址的能力，因此该环境下无需开启此功能; 部署静态 IP 的环境中无法使用该功能
- 建议逃生 WLAN 的 SSID 不能跟 802.1x 认证的 WLAN SSID 相同，从而在使用逃生 WLAN 服务时能够有直观的体现，并且当服务器不可用，需要切换 WLAN 时，用户需要手工切换一次 SSID，由于终端通常具有 SSID 记忆功能，因此一次切换以后，后续再出问题能够自动切换。
- 802.1X 用户只做加密，因此对 802.1X 用户的授权将不生效，例如服务器下发 acl,下发限速都将不生效，但用户需要接入网络时还需进行 WEB 认证，可以对 WEB 认证用户进行授权。

配置方法

↘ 配置主动认证

- 可选配置，配置之后受控口发送主动请求，认证客户端收到主动请求之后就会发起 802.1x 认证。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x auto-req**
【参数说明】 **-**
【缺省配置】 开启

【命令模式】 全局模式

【使用指导】 主动认证报文的目的地址是组播报文；下联客户端有可能不会主动发起认证时，可以使用此命令让设备主动发起认证。受控口是 TRUNK 口时，开启此命令，可以基于 TRUNK 口的每一个 VLAN 发送主动请求

配置主动认证发送的报文数

- 可选配置，配置设备发送主动请求报文数量。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x auto-req packet-num** *num*

【参数说明】 *num*：主动认证报文数

【缺省配置】 不限报文数量

【命令模式】 全局模式

【使用指导】 在开启主动认证命令下，可以用来控制端口发出的主动认证报文数量，避免发送多余的报文。

配置主动认证用户检测

- 可选配置，配置受控口上有认证用户之后就不再发送主动请求。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x auto-req user-detect**

【参数说明】 -

【缺省配置】 开启

【命令模式】 全局模式

【使用指导】 配置该命令之后，ACCESS 的受控口上如果有认证用户则不再发出主动认证的报文；TRUNK 口上基于每一个 VLAN 来判断是有认证用户，有认证用户的则该 VLAN 内不再发出主动认证报文。

配置主动认证用发送报文的间隔

- 可选配置，配置设备发送主动请求报文时间间隔。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x auto-req req-interval** *time*

【参数说明】 *Time*：主动认证的报文间隔时间

【缺省配置】 30s

【命令模式】 全局模式

【使用指导】

配置可认证主机列表

- 可选配置，配置受控口上的可认证主机列表，只有在列表中的客户端才允许进行 801.1x 认证。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x auth-address-table address** *mac-addr* **interface** *interface*

【参数说明】 *mac-addr*：接入终端的 MAC 地址

interface ：接入终端所在的端口

【缺省配置】 用户均可以认证

【命令模式】 全局模式
【使用指导】 需要限制可以在受控口上认证的终端时可以使用此命令

配置使用虚拟 MAC 作为设备 802.1x 认证的源 MAC

- 可选配置，设备的 MAC 无法被锐捷 su 识别为锐捷设备时配置此命令。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x pseudo source-mac**
【参数说明】 -
【缺省配置】 关闭
【命令模式】 全局模式
【使用指导】 部分锐捷 supplicant 无法通过设备发出的 eapol 报文源 MAC 认出该设备是锐捷设备，无法在认证过程中实施私有属性，此时可以开启此命令，则设备发出的 eapol 报文使用 00-1A-A9-17-FF-FF 作为源 MAC，确保前述客户端可以将设备认出为锐捷设备。

配置多帐号认证

- 可选配置，允许同一个 MAC 被多个帐号使用时可以配置此命令。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x multi-account enable**
【参数说明】 -
【缺省配置】 关闭
【命令模式】 全局模式
【使用指导】 DOT1X 认证中，某些环境中存在切换帐号认证的需求，例如部署 windows 的域认证，需要配置该功能，从而认证客户端可以在前一个帐号还没有下线的情况下，直接使用新的帐号发起认证。默认禁止切换帐号认证。

配置接口下的认证用户数限制

- 可选配置，可以限制受控口上线的用户数量，包括静态用户和动态用户。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x default-user-limit** *num*
【参数说明】 *num*:用户数限制
【缺省配置】 不限制端口用户
【命令模式】 接口模式
【使用指导】 默认不限制端口可以认证的用户数量，需要限制端口下可认证用户数时可配置此命令

配置获取 IP 后开始计费功能

- 可选配置，设备获取到客户端的 IP 地址之后，才会想服务器发出记账。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x valid-ip-acct enable**
【参数说明】
【缺省配置】 关闭

【命令模式】 全局模式

【使用指导】 开启此命令后，在开启记账的情况下，只有获取到了认证客户端的 IP 之后，设备才会发起记账，超时没有获取到 IP 则将此用户强制下线；没有开启记账时开启此命令，设备获取到 IP 之后不会发起记账，而超时没有获取到 IP 则同样会将此用户强制下线。

配置用户认证通过之后，允许等待该用户获取 IP 的时间

- 可选配置，开启获取 IP 开始计费功能，允许等待获取该用户 IP 的时间。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x valid-ip-acct timeout** *time*

【参数说明】 *time*：超时时间，单位为分钟，默认为 5 分钟

【缺省配置】 默认为 5 分钟

【命令模式】 全局模式

【使用指导】 使用默认值即可，需要改变用户认证通过后等待获取 IP 的时间，可以使用此命令

配置 RADIUS 服务器逃生功能

- 可选配置。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x event server-invalid action bypass-wlan** *wlan_id*

【参数说明】 *wlan_id*：逃生的 WLAN

【缺省配置】 关闭

【命令模式】 全局模式和 wlan 安全配置模式

【使用指导】 使用默认值即可，需要在服务器不可达时提供相应的 WLAN，可以使用此命令

配置 RADIUS 服务器逃生时的行为

- 可选配置。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x event server-invalid original-wlan action hide**

【参数说明】 -

【缺省配置】 缺省 RADIUS 服务器故障逃生时，关闭 wlan 信号

【命令模式】 全局模式

【使用指导】 1、在 RADIUS 服务器不可达时，想要隐藏 wlan 信号，可通过配置此命令实现。

2、需先为 wlan 配置开启 RADIUS 服务器故障逃生功能，此命令方可生效。

配置 802.1x 和 WEB 认证共用

- 可选配置，802.1x 和 WEB 认证共用时 802.1x 仅作加密功能时。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x encryption only**

【参数说明】 -

【缺省配置】 关闭

【命令模式】 WLAN 安全配置模式
【使用指导】 使用默认值即可。

配置 802.1x 认证用户上下线的 syslog 速率

- 可选配置，可以用来控制 802.1x 用户上线时打印 log 的速率。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x logging rate-limit** *value*
【参数说明】 *value*：每一秒打印用户上下线 syslog 的速率，默认是 5 条/s，0 表示不限速率
【缺省配置】 默认是 5 条/s
【命令模式】 全局模式
【使用指导】 一般使用默认值即可，如果有大量的认证用户频繁的上线下线，需要调低该速率

配置 802.1x 认证用户上下线的 SNMP Trap 通告

- 可选配置，可以用来开关 802.1x 用户上线时是否发送 trap 给 snmp 服务器。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x user-trap enable**
【参数说明】
【缺省配置】 关闭
【命令模式】 全局模式
【使用指导】 无线 802.1x 认证设备上支持
需要向 SNMP 服务器发送认证用户上线和下线 Trap 消息时开启此命令，需要配置 SNMP 服务器并允许发送 Trap 消息，具体见 SNMP 配置

配置流量检查功能

- 可选配置，开启之后 802.1x 认证用户在检测时间周期内低于流量阀值则被踢下线，避免错误计费。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x offline-detect {[interval** *val***] | [flow** *num***]}**
【参数说明】 *val*：检测时间，默认为 15 分钟
num：流量阈值，则默认是 0KB
【缺省配置】 AC 上默认开启，AP 上默认关闭
【命令模式】 Wlan 安全模式
【使用指导】 无线 802.1x 认证设备上支持
为避免 STA 下线了，但设备还没完全探测到而继续对用户计费可以配置此命令

配置 MAB 认证成功后终端的默认角色

- 可选配置，配置 MAB 认证成功后终端的默认角色。

【命令格式】 **dot1x mab-default-role** *role-name*
【参数说明】 role-name：认证成功之后为终端分配的默认角色名称
【缺省配置】 无默认角色

【命令模式】 WLAN 安全模式

【使用指导】 仅在单独 MAB 认证场景中该配置才能生效。

配置 802.1x 认证成功后终端的默认角色

- 可选配置，配置 802.1x 认证成功后终端的默认角色。

【命令格式】 **dot1x dot1x-default-role** *role-name*

【参数说明】 *role-name*：认证成功之后为终端分配的默认角色名称

【缺省配置】 无默认角色

【命令模式】 WLAN 安全模式

【使用指导】 在 MAB+802.1x 认证场景中，最终为终端分配的是 802.1x 认证成功后的默认角色。

配置 802.1x 认证域属性

- 可选配置，可以为 WLAN 指定认证域。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x domain-name** *domain-name*

【参数说明】 *domain-name：指定域名*

【缺省配置】 没有配置任何域

【命令模式】 WLAN 安全模式

【使用指导】 当 WLAN 安全模式下配置了此域名，如果用户名中未携带域名进行认证时，将会在此用户名后添加“@”和配置上的域名进行认证操作；如果用户名中已经携带域名进行认证，则不在用户名后添加“@”和此域名进行认证。

配置过滤打印信息

- 可选配置。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x dbg-filter** *H.H.H*

【参数说明】 *H.H.H*：需要输出调试信息的用户的 MAC 地址

【缺省配置】 所有认证用户的调试信息均打印

【命令模式】 全局模式

【使用指导】 网络中有大量用户且需要在当前网络中定位故障时，可以通过该命令对个别用户打印调试信息，避免设备打印过多调试信息。

配置终端在 MAB 认证成功前终端不允许获取 IP

- 可选配置，控制终端进行 MAB 用户认证前是否允许获取 IP 地址。
- 在设备开启 MAB 认证之后配置

【命令格式】 **dot1x no-ip-before-mab**

【参数说明】

【缺省配置】 关闭

【命令模式】 wlan 安全配置模式

【使用指导】 配置终端在 MAB 用户认证成功前不允许获取 IP 地址

配置 MAB 用户认证成功后需要进行 web 认证

- 可选配置，控制终端在 MAB 用户认证成功后是否需要进行 web 认证。
- 设备需同时开启 MAB+WEB 认证模式，部分终端无法自动弹窗，需要手动打开网页访问。

【命令格式】 **dot1x mab-pass-to-web**
【参数说明】
【缺省配置】 关闭
【命令模式】 wlan 安全配置模式
【使用指导】 配置终端在 MAB 用户认证成功后需要进行 web 认证

检验方法

无。

配置举例

无。

1.5 监视与维护

清除各类信息

⚠ 关闭 802.1x 认证功能后，认证用户信息可以被清除。

作用	命令
清除 802.1x 认证用户信息。	**no do1x port-control auto**
清除 802.1x 认证用户信息	**clear dot1x user**
恢复 802.1x 的默认配置	**dot1x default**

查看运行情况

作用	命令
查看 RADIUS 服务器参数和状态	**show radius server**
查看 802.1x 功能状态和协议参数	**show dot1x**
查看可认证主机列表	**show dot1x auth-address-table**
查看主动认证状态	**show dot1x auto-req**
查看接口受控情况	**show dot1x port-control**
查看客户端探测功能状态和参数	**show dot1x probe-timer**

查看认证用户表项信息	**show dot1x summary**
查看 equest/challenge 报文重传次数	**show dot1x max-req**
查看受控口信息	**show dot1x port-control**
查看过滤非锐捷客户端开关的状态	**show dot1x private-supplicant-only**
查看重认证开关的状态	**show dot1x re-authentication**
查看 request/id 报文重传次数	**show dot1x reauth-max**
查看认证失败之后的静默时间	**show dot1x timeout quiet-period**
查看重认证周期	**show dot1x timeout re-authperiod**
查看服务器超时时间	**show dot1x timeout server-timeou**t
查看客户端超时时间	**show dot1x timeout supptimeout**
查看 request/id 报文重传间隔	**show dot1x timeout tx-period**
根据用户 MAC 来查看用户信息	**show dot1x user mac**
根据用户名来查看用户信息	**show dot1x user name**

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
AAA 调试信息（详见 AAA 配置手册）	**debug aaa**
RADIUS 调试信息（详见 RADIUS 配置手册）	**debug radius**
打开 dot1x 事件相关的调试开关	**debug dot1x event**
打开 dot1x 报文处理相关的调试开关	**debug dot1x packet**
打开 dot1x 认证状态机相关的调试开关	**debug dot1x stm**
打开 dot1x 内部通信相关的调试开关	**debug dot1x com**
打开 dot1x 错误相关的调试开关	**debug dot1x error**

1 本地认证服务

1.1 概述

Local EAP 是设备提供的一种本地认证服务，该服务允许设备直接对使用 EAP 认证协议的客户端进行本地认证，而不需要部署外部的认证服务器。例如，可以在设备上对使用 802.1X 接入认证方式的无线客户端进行认证。具有 local EAP 功能的设备，相当于一台 EAP 服务器，既可以作为首选的认证服务器直接提供认证服务；也能够作为外部服务器的备份，在外部服务器不可用的时候，继续提供认证服务功能。当前，Local EAP 支持 PEAPv0/MSCHAPv2 和 PEAPv1/GTC 认证方法。

此外，local EAP 还提供 EAP 终结功能。这一功能是指设备能够将复杂的 EAP 认证协议终结在设备上，之后再代理转发 EAP 协议中包含的简单认证信息到外部服务器上的功能。这一功能使得设备能够适配那些无法提供所需 EAP 方法的外部认证服务器，例如客户端认证要求使用 PEAPv1/GTC，而外部的认证服务器只能提供 PAP 认证方法。

协议规范

- RFC 3748：Extensible Authentication Protocol (EAP)
- RFC 4137：State Machines for Extensible Authentication Protocol (EAP)
- RFC 5216：The EAP-TLS Authentication Protocol
- RFC 5246：The Transport Layer Security (TLS) Protocol Version 1.2
- RFC 5280：Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

1.2 典型应用

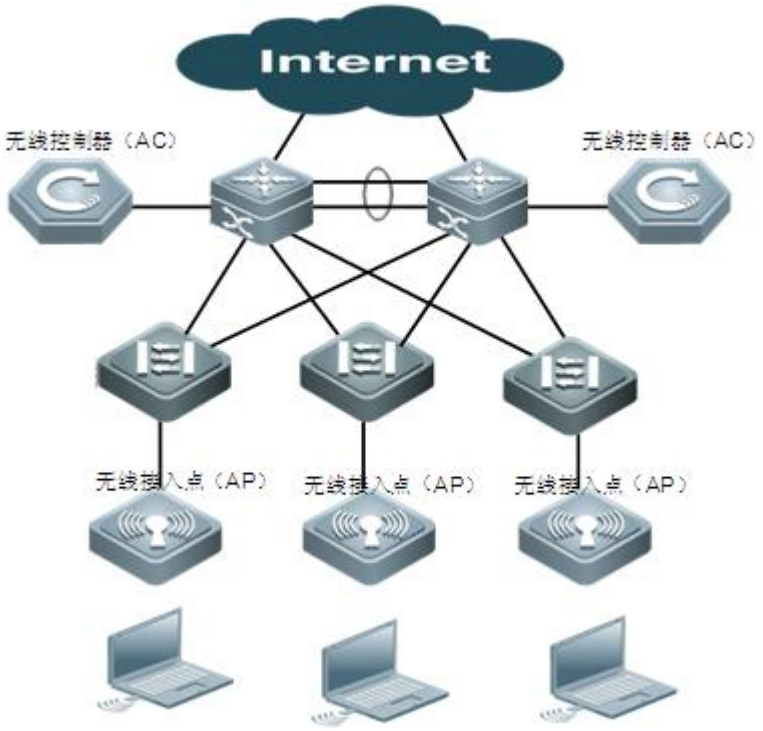
典型应用	场景描述
本地认证	设备直接对使用 EAP 认证协议的客户端进行本地认证，而不需要部署外部的认证服务器。
EAP 终结	将复杂的 EAP 认证协议终结在设备上，之后再代理转发 EAP 协议中包含的简单认证信息到外部服务器上，使得设备能够适配那些无法提供所需 EAP 方法的外部认证服务器。

1.2.1 本地认证

应用场景

以下图为例，无线控制器和无线接入点组成无线网络，无线控制器上配置采用 802.1X 接入认证和配置启用 Local EAP 的本地认证功能（充当认证服务器，不需要再部署外部的认证服务器）。

图 1-1



功能部署

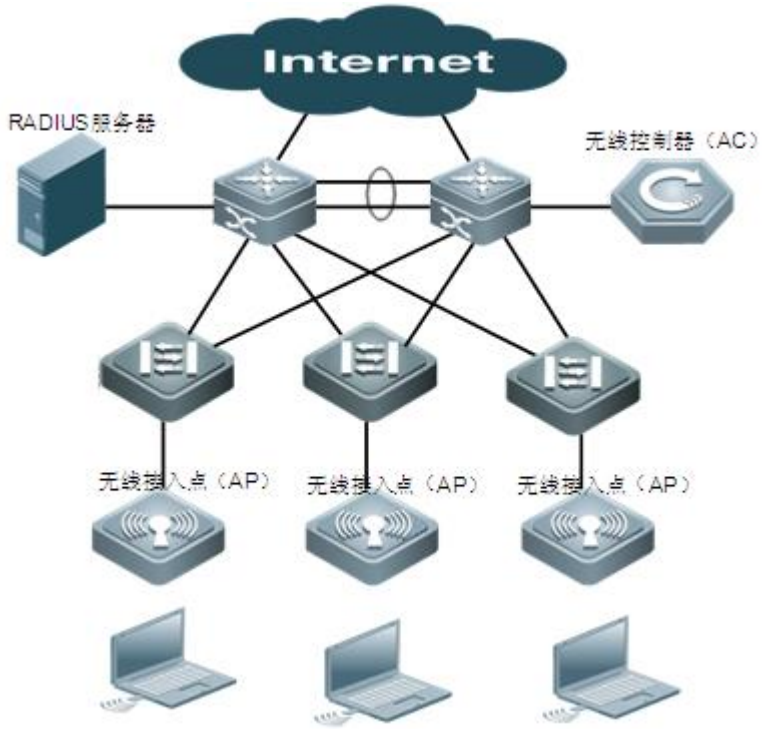
- 配置 WLAN。
- 配置无线安全使用 802.1X 接入认证方式。
- 配置 AAA 的 802.1X 认证方法列表。
- 配置 Local EAP 作为本地认证服务器的认证用户名和密码。

1.2.2 EAP 终结

应用场景

以下图为例，无线控制器和无线接入点组成无线网络，网络中部署 RADIUS 认证服务器。无线控制器上配置采用 802.1X 接入认证。由于 RADIUS 认证服务器不支持复杂的 EAP 认证协议，因此，在无线控制器上还配置启用 Local EAP 的 EAP 终结功能。

图 1-2



功能部署

- 配置 WLAN。
- 配置无线安全使用 802.1X 接入认证方式。
- 配置 AAA 的 802.1X 认证方法列表。
- 配置 RADIUS 服务器。
- 配置启用 Local EAP 的 EAP 终结功能。

1.3 功能详解

基本概念

↘ EAP 协议

EAP 协议的全称是 Extensible Authentication Protocol（可扩展认证协议）。EAP 是一种认证框架，它定义了认证的基本流程和消息格式，但是没有定义具体的认证方法。基于 EAP 框架的每个具体的认证协议，都需要定义所需的数据交互流程和封装格式。目前常用 EAP 认证协议有：EAP-MD5、EAP-GTC、EAP-TLS、EAP-MSCHAPv2、PEAPv0/MSCHAPv2 和 PEAPv1/GTC 等，其中无线网络中常用的是：EAP-TLS、EAP-MSCHAPv2、PEAPv0/MSCHAPv2 和 PEAPv1/GTC。

- PEAPv0/MSCHAPv2 协议

  PEAPv0/MSCHAPv2 协议是目前无线网络中最常用的认证协议，几乎所有的系统都支持。该协议的外层为 PEAP 协议，目的

是建立一条 TLS 隧道用来保护真实的认证信息；内层为 EAP-MSCHAPv2 协议，用来对用户的身份进行验证。

- PEAPv1/GTC 协议

  PEAPv1/GTC 协议和 PEAPv0/MSCHAPv2 协议类似，目前的绝大部分移动设备都支持该认证协议，不过 Windows 系统默认不支持该协议。该协议的外层也是 PEAP 协议，内层则运行 EAP-GTC 协议来对用户的身份进行验证。

EAP 终结

EAP 终结功能是指：local EAP 和认证客户端之间运行一种 EAP 认证协议，而 local EAP 和外部认证服务器之间运行另一种认证协议（不一定是 EAP 协议），local EAP 作为代理，在客户端和外部认证服务器之间转换和转发认证消息或认证结果。local EAP 能够将复杂的 EAP 认证协议终结在设备上，提取必要的认证信息后再转发到外部服务器上；外部服务器返回的认证结果或者需要传递给客户端的认证信息，会由 local EAP 封装成指定的 EAP 协议后再发送给认证客户端。这一功能主要用于对接某些不支持指定 EAP 认证方法的认证服务器。目前，无线控制器设备支持以下两种类型的 EAP 终结：EAP-GTC 终结和 EAP-MSCHAPv2 终结。

- EAP-GTC 终结

  EAP-GTC 终结是指 local EAP 和客户端之间运行 EAP-GTC 协议，local EAP 从 EAP-GTC 协议中获取到了客户端所提交的用户名和密码后，使用此用户名和密码发送一个 PAP 认证请求给外部认证服务器，由外部认证服务器来决定认证结果。

- EAP-MSCHAPv2 终结

  EAP-MSCHAPv2 终结是指 local EAP 和客户端之间运行 EAP-MSCHAPv2 协议，local EAP 从 EAP-MSCHAPv2 协议中获取到 challenge 和 peer response 后，封装成一次 MSCHAPv2 认证后发送给外部认证服务器，由外部认证服务器来决定认证结果。

PKI

Local EAP 支持的某些 EAP 方法，例如 PEAP 方法，需要采用非对称加密算法和客户端建立起一条可信加密隧道，如 TLS 隧道。这就需要依赖于 PKI（Public-Key Infrastructure，公钥基础设施），由于 PKI 涉及的范围太广，此处只做个简要的介绍。

PKI 基于非对称密码体制的一种身份识别和通信加密体制，PKI 的基础是非对称密码体制和证书。在 PKI 中，通信的双方通过一个可信第三方来确认通信对方的身份是否和它所声明的身份是一致的。该可信的第三方称为 Certificate Authority(CA)。目前，PKI 中的身份是通过 X509 证书来标识的。证书中主要包含有三方面的内容：持有者的身份信息、持有者的公钥以及可信第三方对这些信息的签名。另外，证书一般可以分为两个类别，自签名证书和 CA 签发的证书。

- 自签名证书是 CA 的证书。CA 使用私钥对身份信息和公钥进行签名得到一张 CA 证书，这张证书就是该 CA 的身份标识。由于 CA 的证书中包含有 CA 的公钥，因此可以使用此公钥来验证由该 CA 签发的证书（这些证书是使用 CA 的私钥进行签名的，所以可以用 CA 的公钥进行验证）。当信赖一个 CA 时，可以使用该 CA 的证书来验证通信对端的证书，确保是在和正确的个体进行通信。
- CA 签发的证书是指由 CA 的私钥对证书请求进行签名得到的证书。一个个体可以通过提交一份证书签发请求给 CA，此请求中包含了该个体的身份信息和公钥，CA 使用自身的私钥对此请求进行签名后，就得到了该个体所需的证书。此后，该个体能够使用证书来标识自身的身份，只要对端信赖同一个 CA，那么对端就能够验证该个体的身份。

上面的描述简述了证书以及公私钥对的关系和作用。公私钥对除了上面的验证身份的作用外，还具备有非对称加解密的作用。通信的双方使用各自的私钥和对方的公钥能够建立起一条加密的通信隧道，这条隧道理论上来说是其他人不可解密的，因此在这条隧道中传输数据是安全和可信的。

EAP 协议中的 EAP-TLS 和 PEAP 两种协议都是依赖于 PKI 的协议，这两种协议会在认证客户端和认证服务器之间建立起一条 TLS 隧道，之后在这条隧道的保护下进行用户身份认证。对于 PEAP 协议，建立这条隧道需要使用到服务器端的证书和公私钥，以及可选的 CA 证书（如果客户端选择不验证服务器的证书，则不需要 CA 证书）；对于 EAP-TLS 协议，建立这条隧道需要使用到服务器

和客户端的证书和公私钥，以及 CA 证书。

功能特性

功能特性	作用
本地认证	设备直接对使用 EAP 认证协议的客户端进行本地认证，而不需要部署外部的认证服务器。既可以作为首选的认证服务器直接提供认证服务；也能够作为外部服务器的备份，在外部服务器不可用的时候，继续提供认证服务功能。
EAP 终结	设备能够将复杂的 EAP 认证协议终结在设备上，之后再代理转发 EAP 协议中包含的简单认证信息到外部服务器上的功能。这一功能使得设备能够适配那些无法提供所需 EAP 方法的外部认证服务器，例如客户端认证要求使用 PEAPv1/GTC，而外部的认证服务器只能提供 PAP 认证方法。

1.3.1 本地认证

设备直接对使用 EAP 认证协议的客户端进行本地认证，而不需要部署外部的认证服务器。既可以作为首选的认证服务器直接提供认证服务；也能够作为外部服务器的备份，在外部服务器不可用的时候，继续提供认证服务功能。

工作原理

在进行本地认证时，Local EAP 的工作原理和 RADIUS 服务器比较相似，可以作为一种认证服务器来看待。不同的是，使用外部 RADIUS 认证服务器时，认证客户端的 EAP 认证请求需要封装成 RADIUS 协议后才能发送给 RADIUS 服务器；而使用 local EAP 作为认证服务器，认证客户端的 EAP 认证请求在设备内部直接由 local EAP 处理了。

由于 Local EAP 支持多种 EAP 方法，对于 PEAP 方法则支持多种内部方法，因此 local EAP 会根据配置指定的顺序来选择要使用哪个方法与客户端进行认证。在 EAP 认证过程中，使用哪种 EAP 方法是由服务端决定的。

相关配置

↘ 配置 802.1X 的认证方法列表

若 802.1X 需要使用 local EAP 作为认证服务器，则需要在 802.1X 的认证方法列表中指定采用 local 方法。

使用 **aaa authentication dot1x** {**default** | *list-name*} *method1* [*method2*...]命令可指定 802.1X 的认证方法列表，如：**aaa authentication dot1x default local**。

必须在 802.1X 的认证方法列表中指定采用 local 方法，用户的认证请求报文才会被发给 local EAP，以便进行本地认证。

↘ 配置采用哪些方法和客户端进行身份认证

允许配置 local EAP 采用哪些方法和客户端进行身份认证。缺省情况下，支持的 EAP 方法只有 PEAP，支持的 PEAP 内部方法及顺序为 EAP-MSCHAPv2, EAP-GTC。

当前，支持的 EAP 方法只有 PEAP，不能修改。 当前，支持的 PEAP 内部方法及顺序可以通过命令 **peap inner-methods** { **eap-mschapv2** [**eap-gtc**] | **eap-gtc** [**eap-mschapv2**] } 进行修改（注：所谓“顺序“是指先配置的先使用）。

1.3.2 EAP 终结

设备能够将复杂的 EAP 认证协议终结在设备上，之后再代理转发 EAP 协议中包含的简单认证信息到外部服务器上的功能。这一功能使得设备能够适配那些无法提供所需 EAP 方法的外部认证服务器，例如客户端认证要求使用 PEAPv1/GTC，而外部的认证服务器只能提供 PAP 认证方法。

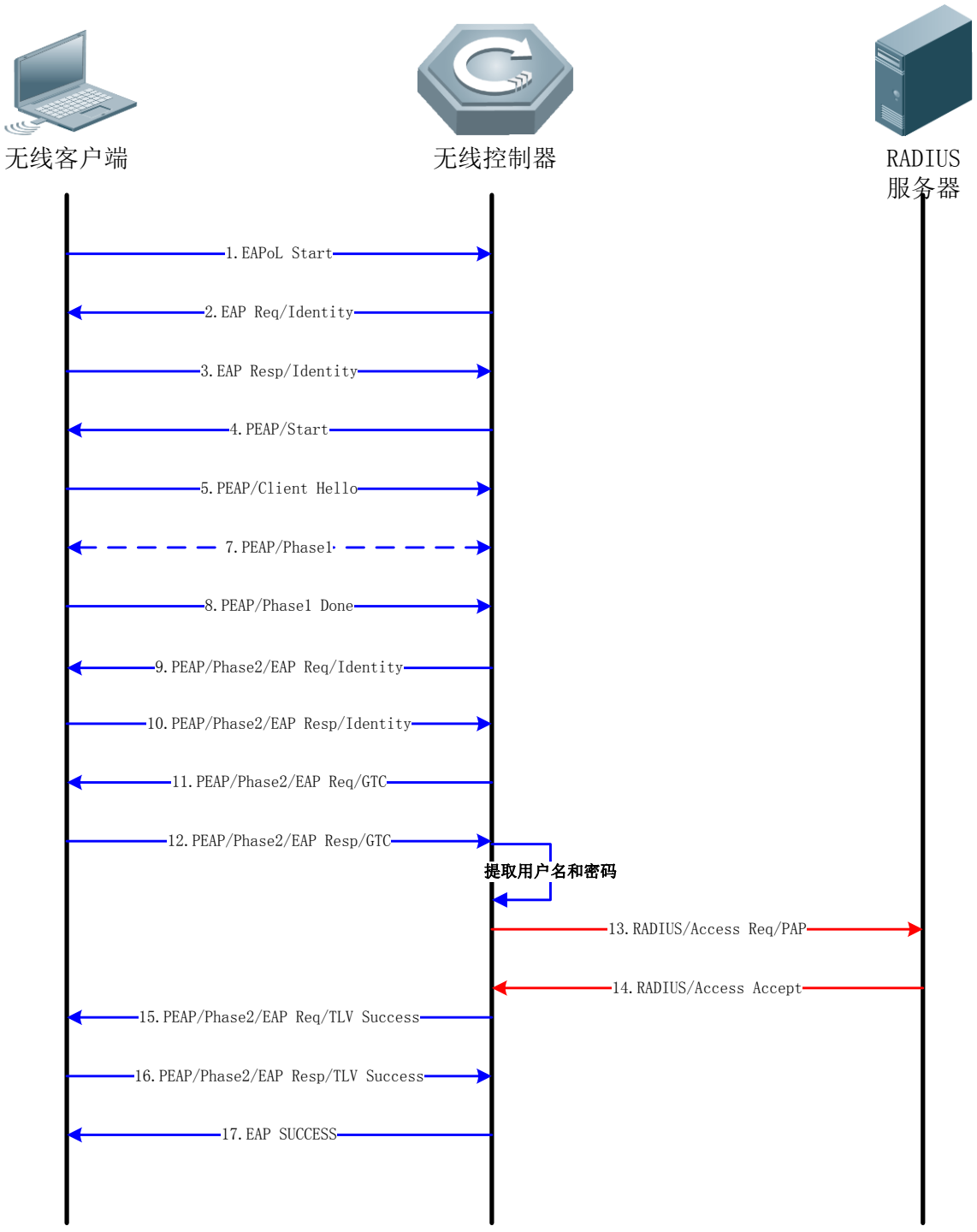
工作原理

现在以 EAP-GTC 终结为例来说明 EAP 终结的工作原理。下图是 EAP-GTC 终结的流程图，图中的 RADIUS 服务器仅支持 PAP 认证方式，而无线控制器和无线客户端之间执行 PEAPv1/GTC 认证方法。

- 步骤 1 到步骤 12：无线控制器和无线客户端之间进行 PEAPv1/GTC 认证方法所要求的交互流程，执行完步骤 12 后，无线控制器就获得了客户端的认证凭据（包括用户名和明文密码）。
- 步骤 13 到步骤 14：local EAP 模块使用获得的认证凭据向 RADIUS 服务器发起一次 PAP 认证过程，并且获得了认证通过的结果。
- 步骤 15 到步骤 17：local EAP 根据 RADIUS 服务器返回的结果继续执行 PEAPv1/GTC 认证过程。

从下图所示的流程可以看出，无线控制器进行 EAP-GTC 终结的时候，无线客户端是感知不到的，始终认为是在进行一次 PEAPv1/GTC 认证；而 RADIUS 服务器上则认为客户端是在进行一次 PAP 认证。当进行 PEAP 终结和 EAP-MSCHAPv2 终结时，流程也是类似的。

图 1-3



相关配置

↘ 配置 AAA 方法列表和 RADIUS 认证服务器

在使用 EAP 终结功能时，local EAP 相当于一个代理，它需要把一些信息转发到外部服务器上。因此，需要配置相关的外部服务器。

可以通过命令 **radius-server host** { *ipv4-address* | *ipv6-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] 指明外部服务器；通过命令 **aaa authentication localeap default group** { **radius** | *group-name* } 指明将终结后的认证请求发送到哪些外部服务器上进行认证。

配置 EAP 终结

缺省情况下，没有配置 EAP 终结。

可使用 **eap-gtc terminate** 配置启用 EAP-GTC 终结； 使用 **eap-mschapv2 terminate** 配置启用 EAP-MSCHAPV2 终结。

1.4 配置详解

配置项	配置建议 & 相关命令	
配置本地认证	⚠ 可选配置。用于配置使设备可当认证服务器，不再需要部署外部的认证服务器，或者让设备充当外部认证服务器的备份。	
	eap-methods { **peap** }	用于配置 local EAP 使用哪些 EAP 方法和客户端进行身份认证。当前只支持 PEAP 方法
	peap inner-methods { **eap-mschapv2** [**eap-gtc**] | **eap-gtc** [**eap-mschapv2**] }	用于配置 local EAP 在 PEAP 内部使用哪些方法和客户端进行身份认证。先配置的先使用，至少要选择一个方法
配置 EAP 终结	⚠ 可选配置。配置将复杂的 EAP 认证协议终结在设备上，之后再代理转发 EAP 协议中包含的简单认证信息到外部服务器上，使得设备能够适配那些无法提供所需 EAP 方法的外部认证服务器。	
	eap-gtc terminate	配置 EAP-GTC 终结
	eap-mschapv2 terminate	配置 EAP-MSCHAPV2 终结
配置 PKI	⚠ 可选配置。Local EAP 支持使用设备自身生成的自签名 PKI 信息，或者是用户通过命令行导入的 PKCS#12 格式的 PKI 信息。缺省情况下，采用设备自身生成的自签名 PKI 信息。	
	pki-manage generate self-signed default	当设备中不存在 PKI 信息时，设备会自动生成自签名的 PKI 信息，一般不需要用户通过命令行来生成。当出于某些原因，例如安全原因时，用户可以通过该命令重新生成自签名的 PKI 信息。
	pki-manage import pfx *filepath* [**password** *password*]	当设备生成的自签名 PKI 信息不满足用户需求时 ,用户可以通过 PKCS#12 格式的文件(一般后缀为.pfx 或者.p12) 导入所需的 PKI 信息到设备中
	server restart	当更新了 Local EAP 服务所使用的 PKI 信息后 ,需要重启 Local EAP 服务 ,才能使新的 PKI 信息生效。

1.4.1 配置本地认证

配置效果

- 可选配置。
- 对使用 EAP 认证协议的客户端进行本地认证，而不需要部署外部的认证服务器。既可以作为首选的认证服务器直接提供认证服务；也能够作为外部服务器的备份，在外部服务器不可用的时候，继续提供认证服务功能。

配置方法

↘ 配置 EAP 方法序列

- 可选配置。
- 当前，仅支持 PEAP 方法，且默认的 EAP 方法就是 PEAP，因此，无需配置。

↘ 配置 PEAP 内部方法序列

- 可选配置。
- 缺省情况下，支持的 PEAP 内部方法及顺序为 EAP-MSCHAPv2, EAP-GTC，若无特殊需求，通常无需配置。

检验方法

- show localeap methods 确认认证方法的配置。

相关命令

↘ 配置 EAP 方法序列

【命令格式】 **eap-methods** { **peap** }
【参数说明】 -。
【命令模式】 localeap 模式
【使用指导】 用于配置 local EAP 使用哪些 EAP 方法和客户端进行身份认证。当前只支持 PEAP 方法。

↘ 配置 PEAP 内部方法序列

【命令格式】 **peap inner-methods** { **eap-mschapv2** [**eap-gtc**] | **eap-gtc** [**eap-mschapv2**] }
【参数说明】 -
【命令模式】 localeap 模式
【使用指导】 用于配置 local EAP 在 PEAP 内部使用哪些方法和客户端进行身份认证。先配置的先使用，至少要选择一个方法。

配置举例

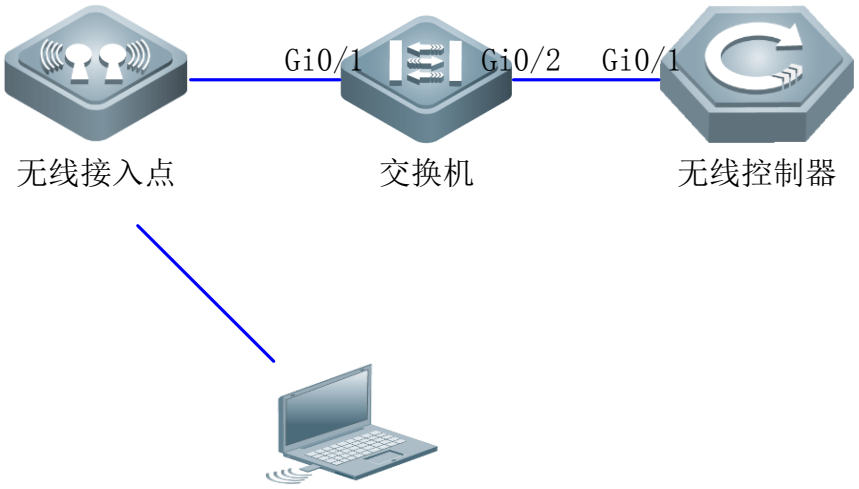
以下配置举例，仅介绍与 Local EAP 本地认证密切相关的配置。

启用 Local EAP 的本地认证功能

以下图为例，无线控制器和无线接入点组成无线网络，无线控制器上配置采用 802.1X 接入认证和配置启用 Local EAP 的本地认证功能（充当认证服务器，不需要再部署外部的认证服务器）。

【网络环境】

图 1-4



【配置方法】

- 配置 WLAN。
- 配置无线安全使用 802.1X 接入认证方式。
- 配置 AAA 的 802.1X 认证方法列表。
- 配置 Local EAP 作为本地认证服务器的认证用户名和密码

交换机

```
# 将设备的下联口划入 AP 所属 VLAN 100
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# poe enable
Hostname(config-if-GigabitEthernet 0/1)# switchport access vlan 100
# 将设备的上联口配置为 trunk 口
Hostname(config)# exit
Hostname(config)# interface GigabitEthernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# switchport mode trunk
```

无线控制器

```
# 将与设备相连的 GigabitEthernet 0/1 口配置为 trunk 口
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode trunk
# 配置 Loopback 0 的 IP 地址，以便无线控制器和无线接入点之间建立 CAPWAP 隧道
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# interface Loopback 0
Hostname(config-if-Loopback 0)# ip address 10.1.1.1 255.255.255.255
# 配置 AP VLAN 100 及 STA VLAN 10，同时作为 VLAN 100 和 VLAN 10 的 DHCP 服务器
Hostname(config)#vlan 100
Hostname(config-vlan)#exit
```

```
Hostname(config)#interface vlan 100
Hostname(config-if-VLAN 100)# ip address 192.168.100.1 255.255.255.0
Hostname(config)#vlan 10
Hostname(config-vlan)#exit
Hostname(config)#interface vlan 10
Hostname(config-if-VLAN 100)# ip address 192.168.10.1 255.255.255.0
Hostname(config-if-VLAN 100)# exit
Hostname(config)# service dhcp
Hostname(config)# ip dhcp pool ap_vlan100
Hostname(dhcp-config)# option 138 ip 10.1.1.1    # 此处必须是 Loopback 0 口所配置的 IP 地址
Hostname(dhcp-config)# network 192.168.100.0 255.255.255.0 192.168.100.10 192.168.100.100
Hostname(dhcp-config)# default-router 192.168.100.1
Hostname(dhcp-config)# exit
Hostname(config)# ip dhcp pool sta_vlan10
Hostname(dhcp-config)# network 192.168.100.0 255.255.255.0 192.168.10.10 192.168.10.100
Hostname(dhcp-config)# default-router 192.168.10.1
Hostname(dhcp-config)# exit
# 配置 WLAN
Hostname(config)#wlan-config 1 miaosf_eap
Hostname(config-wlan)#exit
Hostname(config)#ap-group default
Hostname(config-ap-group)#interface-mapping 1 10
Hostname(config-ap-group)# exit
# 配置无线安全使用 802.1X 接入认证方式
Hostname(config)#wlansec 1
Hostname(config-wlansec)# security rsn enable
Hostname(config-wlansec)# security rsn ciphers aes enable
Hostname(config-wlansec)# security rsn akm 802.1x enable
Hostname(config-wlansec)# exit
# 配置 AAA 的 802.1X 认证方法列表
Hostname(config)# dot1x authentication default
Hostname(config)# aaa new-model
Hostname(config)# aaa authentication login default none
Hostname(config)# aaa authentication dot1x default local
Hostname(config)# aaa authentication enable default none
# 配置 Local EAP 作为本地认证服务器的认证用户名和密码
Hostname(config)# username admin password admin
```

【检验方法】 只要在 STA（如：手机）上输入用户名 admin，密码 admin，即可正常地连接至 WLAN miaosf_eap。

常见错误

- AAA 的 802.1X 认证方法列表配置错误。

1.4.2 配置 EAP 终结

配置效果

- 可选配置。
- 配置将复杂的 EAP 认证协议终结在设备上，之后再代理转发 EAP 协议中包含的简单认证信息到外部服务器上，使得设备能够适配那些无法提供所需 EAP 方法的外部认证服务器。

配置方法

↘ 配置 AAA 和 RADIUS

- 必选配置。
- 在使用 EAP 终结功能时，local EAP 相当于一个代理，它需要把一些信息转发到外部服务器上。因此，需要配置相关的外部服务器。

↘ 配置 EAP-GTC 终结和 EAP-MSCHAPv2 终结

- 必选配置。
- 当前仅支持这两种类型终结，可二者择其一，也可同时配置这两种类型的终结。

检验方法

- show localeap methods 确认 EAP 终结的配置。

相关命令

↘ 配置 AAA 和 RADIUS

【命令格式】 **radius-server host** { *ipv4-address* | *ipv6-address*} [**auth-port** *port-number*] [**acct-port** *port-number*]
aaa authentication localeap default group { **radius** | *group-name* }

【参数说明】 *group-name*：配置 local EAP 使用指定的服务器组内的服务器作为外部服务器。

【命令模式】 全局配置模式

【使用指导】 上述的第一条命令由 radius 模块提供，第二条命令由 AAA 模块提供，关于这两条命令的更详细描述，可参见对应的用户手册。

↘ 配置 EAP-GTC 终结和 EAP-MSCHAPv2 终结

【命令格式】 **eap-gtc terminate**
eap-mschapv2 terminate

【参数说明】 -

【命令模式】 localeap 模式

【使用指导】 用于开启 EAP-GTC 终结和 EAP-MSCHAPv2 终结。

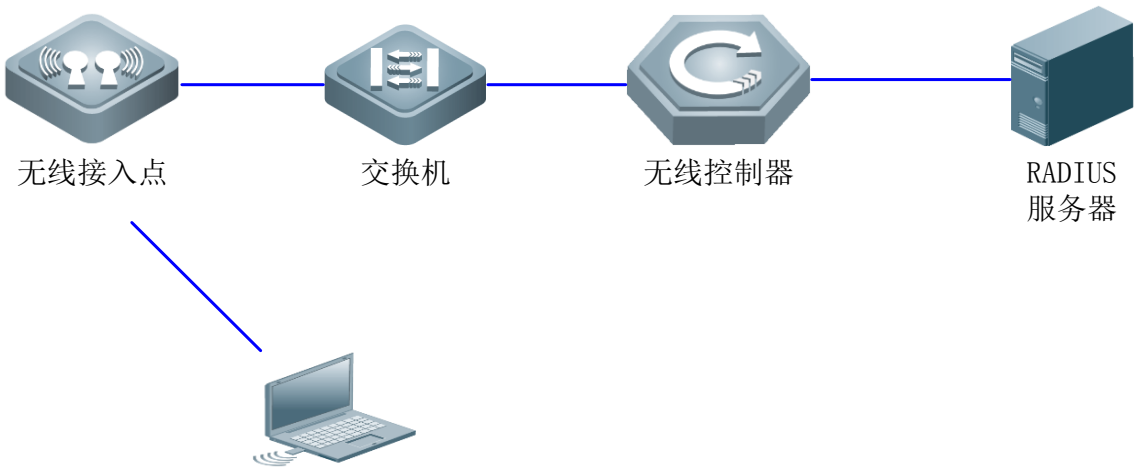
配置举例

以下配置举例，仅介绍与 EAP 终结密切相关的配置。

以下图为例，无线控制器和无线接入点组成无线网络，无线控制器连接到一个 RADIUS 认证服务器。无线控制器上配置采用 802.1X 接入认证。无线客户端采用 PEAPv1/GTC 认证方法。由于 RADIUS 认证服务器不支持 PEAPv1/GTC 终结，因此，在无线控制器上需配置 EAP-GTC 终结。

【网络环境】

图 1-5



【配置方法】

- 配置 WLAN。
- 配置无线安全使用 802.1X 接入认证方式。
- 配置 AAA 的 802.1X 认证方法列表。
- 配置 RADIUS 服务器。
- 配置启用 Local EAP 的 EAP 终结功能。

交换机

```
# 将交换机下联口划入 AP 所属 VLAN 100
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# poe enable
Hostname(config-if-GigabitEthernet 0/1)# switchport access vlan 100
# 将交换机上联口配置为 trunk 口
Hostname(config)# exit
Hostname(config)# interface GigabitEthernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# switchport mode trunk
```

无线控制器

```
# 将与交换机相连的 GigabitEthernet 0/1 口配置为 trunk 口
```

```
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode trunk
# 配置 Loopback 0 的 IP 地址，以便无线控制器和无线接入点之间建立 CAPWAP 隧道
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# interface Loopback 0
Hostname(config-if-Loopback 0)# ip address 10.1.1.1 255.255.255.255
# 配置 AP VLAN 100 及 STA VLAN 10，同时作为 VLAN 100 和 VLAN 10 的 DHCP 服务器
Hostname(config)#vlan 100
Hostname(config-vlan)#exit
Hostname(config)#interface vlan 100
Hostname(config-if-VLAN 100)# ip address 192.168.100.1 255.255.255.0
Hostname(config)#vlan 10
Hostname(config-vlan)#exit
Hostname(config)#interface vlan 10
Hostname(config-if-VLAN 100)# ip address 192.168.10.1 255.255.255.0
Hostname(config-if-VLAN 100)# exit
Hostname(config)# service dhcp
Hostname(config)# ip dhcp pool ap_vlan100
Hostname(dhcp-config)# option 138 ip 10.1.1.1    # 此处必须是 Loopback 0 口所配置的 IP 地址
Hostname(dhcp-config)# network 192.168.100.0 255.255.255.0 192.168.100.10 192.168.100.100
Hostname(dhcp-config)# default-router 192.168.100.1
Hostname(dhcp-config)# exit
Hostname(config)# ip dhcp pool sta_vlan10
Hostname(dhcp-config)# network 192.168.100.0 255.255.255.0 192.168.10.10 192.168.10.100
Hostname(dhcp-config)# default-router 192.168.10.1
Hostname(dhcp-config)# exit
# 配置 WLAN
Hostname(config)#wlan-config 1 miaosf_eap
Hostname(config-wlan)#exit
Hostname(config)#ap-group default
Hostname(config-ap-group)#interface-mapping 1 10
Hostname(config-ap-group)# exit
# 配置无线安全使用 802.1X 接入认证方式
Hostname(config)#wlansec 1
Hostname(config-wlansec)# security rsn enable
Hostname(config-wlansec)# security rsn ciphers aes enable
Hostname(config-wlansec)# security rsn akm 802.1x enable
Hostname(config-wlansec)# exit
# 配置 AAA 的 802.1X 认证方法列表
Hostname(config)# dot1x authentication default
```

```
Hostname(config)# aaa new-model
Hostname(config)# aaa authentication login default none
Hostname(config)# aaa authentication dot1x default local
Hostname(config)# aaa authentication enable default none
Hostname(config)# aaa authentication localeap default group radius
# 配置 RADIUS 服务器
Hostname(config)# radius-server host 192.168.197.79
Hostname(config)# radius-server key Hostname
```

【检验方法】 假设 radius 服务器上配置的用户名为 admin，密码为 admin，则只要在 STA（如：手机）上输入用户名 admin，密码 admin，即可正常地连接至 WLAN miaosf_eap。

常见错误

- AAA 的 802.1X 认证方法列表配置错误。

1.4.3 配置 PKI

配置效果

- 可选配置。
- Local EAP 支持使用设备自身生成的自签名 PKI 信息，或者是用户通过命令行导入的 PKCS#12 格式的 PKI 信息。缺省情况下，采用设备自身生成的自签名 PKI 信息。
- 用户导入的 PKI 信息的优先级比设备生成的优先级高，当设备生成的自签名 PKI 信息和用户导入的 PKI 信息都存在时，设备会使用用户导入的 PKI 信息。当设备启动的时候，发现以上两种 PKI 信息都不存在时，设备会自动生成一套自签名的 PKI 信息，并且投入使用。

配置方法

↘ 配置重新生成自签名 PKI

- 可选配置。
- 当设备中不存在 PKI 信息时，设备会自动生成自签名的 PKI 信息，一般不需要用户通过命令行来生成。当出于某些原因，例如安全原因时，用户可以通过本功能重新生成自签名的 PKI 信息。

↘ 配置导入 PKCS#12 格式的 PKI

- 可选配置。
- 当设备生成的自签名 PKI 信息不满足用户需求时，用户可以通过 PKCS#12 格式的文件（一般后缀为.pfx 或者.p12）导入所需的 PKI 信息到设备中。

↘ 重启 Local EAP 服务，使新的 PKI 信息生效

- 可选配置。
- 当更新了 Local EAP 服务所使用的 PKI 信息后，需要重启 Local EAP 服务，才能使新的 PKI 信息生效，具体的情况有如下几种：
    - 正在使用自签名的 PKI 信息，但重新生成了自签名的 PKI 信息，或者从外部导入了 PKI 信息。
    - 正在使用从外部导入的 PKI 信息，但是将外部导入的 PKI 信息删除掉或者重新导入了新的 PKI 信息。
- 需要注意的是： 重启 Local EAP 服务会使得所有通过 Local EAP 服务认证上线的用户掉线。

检验方法

- 通过 **show localeap pki** [**self-signed | pfx** 查看 local EAP 中的 PKI 信息。

相关命令

配置重新生成自签名 PKI

【命令格式】 **pki-manage generate self-signed default**

【参数说明】 -

【命令模式】 localeap 配置模式

【使用指导】 当设备中不存在 PKI 信息时，设备会自动生成自签名的 PKI 信息，一般不需要用户通过命令行来生成。当出于某些原因，例如安全原因时，用户可以通过本命令重新生成自签名的 PKI 信息。
重新生成自签名的 PKI 信息后，需要重启 Local EAP 服务才能生效。

配置导入 PKCS#12 格式的 PKI

【命令格式】 **pki-manage import pfx** *filepath* [**password** *password*]

【参数说明】 *filepath*：PKCS#12 文件在设备 Flash 上的路径
password：可选的解密导入文件的密码，当文件没有加密时，不需要输入密码

【命令模式】 localeap 模式

【使用指导】 当设备生成的自签名 PKI 信息不满足用户需求时，用户可以通过 PKCS#12 格式的文件（一般后缀为.pfx 或者.p12）导入所需的 PKI 信息到设备中。
导入 PKI 信息或者删除已经导入的 PKI 信息后，需要重启 Local EAP 服务后才能生效。

重启 Local EAP 服务，使新的 PKI 信息生效

【命令格式】 **service restart**

【参数说明】 -

【命令模式】 localeap 模式

【使用指导】 当更新了 Local EAP 服务所使用的 PKI 信息后，需要重启 Local EAP 服务，才能使新的 PKI 信息生效，具体的情况有如下几种：

- 正在使用自签名的 PKI 信息，但重新生成了自签名的 PKI 信息，或者从外部导入了 PKI 信息。
- 正在使用从外部导入的 PKI 信息，但是将外部导入的 PKI 信息删除掉或者重新导入了新的 PKI 信息。

重启 Local EAP 服务会使得所有通过 Local EAP 服务认证上线的用户掉线。

配置举例

↘ 上传 PKCS#12 文件到设备上，配置 local EAP 导入 PKCS#12 格式的 PKI 信息。

【配置方法】

- 上传 PKCS#12 文件到设备上。
- 配置 local EAP 导入 PKCS#12 格式的 PKI 信息

```
# 上传 PKCS#12 文件到设备上
Hostname# copy tftp://192.168.1.1/pki.pfx flash:pki.pfx
# 配置 local EAP 导入 PKCS#12 格式的 PKI 信息
Hostname# config
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#localeap
Hostname(config-localeap)#pki-manage import pfx pki.pfx password filepassword
Apr 29 23:03:27: %LOCALEAP-6-PKIMANAGE: Import PKI from file [pki.pfx] successfully
```

【检验方法】

- 通过 **show localeap pki** [**self-signed | pfx** 查看 local EAP 中的 PKI 信息。

【配置方法】

- 上传 PKCS#12 文件到设备上。
- 配置 local EAP 导入 PKCS#12 格式的 PKI 信息

```
# 上传 PKCS#12 文件到设备上
Hostname# copy tftp://192.168.1.1/pki.pfx flash:pki.pfx
# 配置 local EAP 导入 PKCS#12 格式的 PKI 信息
Hostname# config
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#localeap
Hostname(config-localeap)#pki-manage import pfx pki.pfx password filepassword
Apr 29 23:03:27: %LOCALEAP-6-PKIMANAGE: Import PKI from file [pki.pfx] successfully
```

【检验方法】

- 通过 **show localeap pki** [**self-signed | pfx** 查看 local EAP 中的 PKI 信息。

```
Hostname#show localeap pki
       TYPE       ACTIVATED
----------------------------
   Self-Signed      Yes
 * PFX-Imported     Yes
```

1.5 监视与维护

查看运行情况

作用	命令
查看 EAP 方法相关的信息	**show localeap methods**
查看 PKI 摘要信息	**show localeap pki [self-signed | pfx]**

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 Local EAP PKI 的调试开关。	**debug localeap pki**
打开 Local EAP 用户认证的调试开关	**debug localeap user {verbose | error | add mac** *mac-address* **| delete mac** *mac-address***}**

1 Web 认证

1.1 概述

1.1.1 Web 认证概述

Web 认证是一种对用户访问网络的权限进行控制的身份认证方法，这种认证方法不需要用户安装专用的客户端认证软件，使用普通的浏览器软件即可进行身份认证。

未认证用户使用浏览器上网时，网络设备会强制浏览器访问特定站点，即 Web 认证服务器，通常称为 Portal 服务器。用户无需认证即可访问 Portal 服务器上的服务，比如下载安全补丁、阅读公告信息等。当用户需要访问认证服务器以外的其它网络资源时，就必须通过浏览器在 Portal 服务器上进行身份认证，只有认证通过后才可以使用网络资源。

除了认证上的便利性之外，由于 Portal 服务器和用户的浏览器有页面交互，可以利用此特性在 Portal 服务器页面放置一些广告、通知、业务链接等个性化的服务。

Web 认证概述

Web 认证有 3 个版本，不同版本的 Web 认证流程不同，分别称为一代 Web 认证、二代 Web 认证、内置 Portal Web 认证。

⚠ 由于三个版本的 Web 认证存在较大差异，配置参数也差别很大，因此在配置 Web 认证相关功能前必须仔细阅读对应章节内容，避免配置错误。

⚠ 二代 Web 认证和内置 Portal Web 认证均支持设备的本地帐号认证，但是由于 RADIUS 认证在实际网络部署中更为常见，因此应用举例中使用了 RADIUS 认证。

⚠ 不同产品端口的概念不一样，无线可能是一个 WLAN，本文统一采用术语端口。

⚠ Web 认证支持低流量检测用户下线，具体参考 Layer23 组件和 SCC 组件的配置手册。

⚠ Web 认证支持域认证，即帐号采用"用户名@域名"的形式，该功能需要 AAA 开启域认证功能，详细参考 AAA 的配置手册。

ℹ 下文仅介绍 Web 认证的相关内容。

协议规范

- HTTP：RFC1945、RFC2068
- HTTPS：RFC2818
- SNMP：RFC1157、RFC2578
- RADIUS：RFC2865、RFC2866、RFC3576

- 与 MAC 短信认证相关的规范参照《中国移动无线局域网(WLAN)设备接口规范 V3.1.0_20130901(MAC 认证扩展)doc》，《浙江移动 WLAN 快速认证方案-接口规范 V1.1-2011.3.22.doc》，《基于 MAC+短信的 WLAN 快速认证方案 V1.1-2011.3.21.doc》

1.2 典型应用

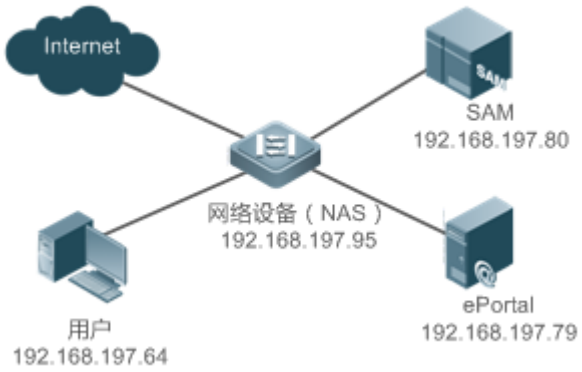
典型应用	场景描述
Web 认证基本场景	常见的二、三层基本认证场景，设备、Portal 服务器、RADIUS 服务器组成认证体系，用户通过二、三层网络连接设备

1.2.1 Web 认证基本场景

应用场景

- 在网络设备上部署 Web 认证方案
- 下联用户需要通过 Web 认证才能访问 internet

图 1-1 Web 认证方案网络拓扑图



【注释】 Web 认证方案可以用于二三层网络。相比于二层网络，三层网络的特点是报文经过了路由后 mac 地址和 vid 信息变了，此时对终端的唯一性识别只有 ip，因此在三层设备上，Web 认证的绑定策略只能用仅 ip 模式。此处以二层接入设备为例。
RADIUS 服务器安装了锐捷 SAM 服务器软件，Portal 服务器安装了锐捷 ePortal 服务器软件。

功能部署

- 在 NAS 上用户所在端口或者全局开启 Web 认证受控。
- 在 NAS 上配置 Web 认证服务器信息和通信加密密钥(仅一代认证和二代认证)。
- 在 NAS 上配置 Web 认证服务器 SNMP 通信参数(仅一代认证和二代认证)。

- 在 Portal 服务器和 SAM 服务器上配置两个服务器间相匹配的通信参数(仅一代 Web 认证)。
- 在 SAM 服务器上配置开通用户账户。
- 在 NAS 上配置 AAA 功能和方法列表(仅二代认证和内置认证)。
- 在 NAS 上配置 RADIUS 服务器地址(仅二代认证和内置认证)。
- 在 NAS 上配置 Web 认证方法列表名(仅二代认证和内置认证)。

1.3 功能详解

基本概念

↘ 一代 Web 认证方案

一代 Web 认证方案需要锐捷专有 ePortal 服务器软件的配合，用户通过 ePortal 软件提供的认证页面提交认证信息，ePortal 服务器直接向相应的 RADIUS 服务器请求认证，认证通过后将用户信息通过 SNMP 协议通告设备，由设备完成用户的准入控制。一代 Web 认证通过私有 SNMP 节点进行认证通信，认证记账功能由 ePortal 服务器承载，减轻了设备的业务压力。

↘ 二代 Web 认证方案

二代 Web 认证方案兼容中国移动 Portal 协议规范。Portal 服务器单纯负责用户页面交互部分，较为简单；而 RADIUS 服务器认证交互部分由设备来实现；Portal 服务器和设备间的交互遵循《中国移动 Portal 协议规范》。用户通过 Portal 服务器提供的认证页面提交认证信息，Portal 服务器将用户信息通过 Portal 协议告知网络设备，网络设备利用该身份信息完成 RADIUS 服务器认证，对合法用户进行准入，同时将结果信息回应给 Portal 服务器。

二代 Web 认证方案由于主要流程都是在设备上完成，对设备的要求比较高，处理能力压力大；但是 Portal 服务器得到了简化，同时使用业界支持度较高的中国移动 Portal 规范进行交互，使得各设备厂商和服务器厂商能够开发出兼容的产品。

↘ 内置 Portal Web 认证

内置 Portal Web 认证由设备集成页面交互功能，以及 RADIUS 服务器认证交互部分的功能。设备默认预置了页面包，用户也可按照配置手册中介绍的页面包定制规范，定制化页面包并下载到设备的存储介质上生效。

↘ 不同 Web 认证方式的对比

对比维度 1	对比维度 2	一代 Web 认证	一代 Web 认证	内置 Portal Web 认证
认证角色	客户端	功能相同	功能相同	功能相同
	网络设备	设备负责重定向，以及与 Portal 服务器交互的用户的上下网通知	设备负责重定向、用户的认证、通告 Portal 服务器认证是否成功	设备集成重定向、页面交互、以及用户的认证等功能
	Portal 服务器	Portal 服务器负责和客户端的页面交互、用户的认证、通告网络设备用户认证是否可上	Portal 服务器负责和客户端的页面交互、通告网络设备用户的认证信息、接收网络	Portal 服务器由设备内置实现，功能较为简单，主要负责页面交互过程

对比维度 1	对比维度 2	一代 Web 认证	一代 Web 认证	内置 Portal Web 认证
		网	设备通告的用户是否认证成功	
	RADIUS 服务器	功能相同	功能相同	功能相同
认证流程		认证记账主要由 Portal 服务器和 RADIUS 服务器共同完成	将认证记账从 Portal 服务器迁移到网络设备。 由于认证在网络设备上，因此无需等待来自 Portal 服务器发送的用户是否可上网的通告	将一二代中 Portal 服务器功能简化，并移到设备上进行支持
下线流程		下线动作可能来自 Portal 服务器的通告或者本机的流量检测、端口状态检测。 计费结束报文由 Portal 服务器发起	下线动作可能来自 Portal 服务器的通告、RADIUS 服务器的踢下线通告、或者本机的流量检测、端口状态检测。 计费结束报文由设备发起	下线动作可能来自用户主动点击页面的下线按钮、RADIUS 服务器的踢下线通告、或者本机的流量检测、端口状态检测。 计费结束报文由设备发起

由上表可知，实际网络中部署 Web 认证类型，取决于所使用的 Portal 服务器的类型。

各类 Web 认证中有部分参数可以共用，请仔细阅读，避免参数配置不当导致 Web 认证使用异常。

功能特性

功能特性	作用
一代 Web 认证	网络中部署了 Portal 服务器且 Portal 服务器仅支持一代 Web 认证
二代 Web 认证	网络中的部署了 Portal 服务器且 Portal 服务器兼容中国移动 Portal 规范
内置 Portal Web 认证	网络中没有部署 Portal 服务器，需要设备支持页面交互功能
MAC 短信认证	未认证用户关联到 WLAN 后，允许使用网络，但用户在指定周期内使用了指定阈值的流量时，认证设备向绑定 Portal 服务器发起 MAC 绑定查询
RIPT	在 AC 故障或者 AC 和 AP 断开连接时，可以使得 AP 上的 Web 认证模块继续对外提供认证服务
WiFiDog	未认证用户能够被重定向到认证页面并完成认证
微信认证	未认证手机终端用户关联到 WLAN 后，使用浏览器可以重定向到微信连 WiFi 一键上网页面，通过页面上的链接可以直接唤醒微信客户端进行微信连 WiFi 认证

功能特性	作用
Clearpass 认证	未认证用户能够被重定向到认证页面并完成认证

1.3.1 一代 Web 认证

HTTP 拦截

HTTP 拦截指网络设备将原本需要转发的 HTTP 报文拦截下来，不进行转发。这些 HTTP 报文是连接在网络设备下的用户的浏览器所发出的，但目的并不是网络设备本身。例如，某用户通过浏览器访问 www.google.com，网络设备本应该将这些 HTTP 请求报文转发到网关的，但如果启动 HTTP 拦截，这些报文将不被转发。

HTTP 拦截之后，网络设备需要将用户的 HTTP 连接请求转向自身，于是网络设备和用户之间将建立起连接会话。网络设备将利用 HTTP 重定向功能，将重定向页面推送给用户，用户的浏览器上将弹出一个页面，此页面可以是认证页面，也可以是下载软件的链接等等。

在 Web 认证功能中，哪些用户所发出的到哪个目的端口的 HTTP 报文需要进行拦截，哪些不需要，都是可以设置的。一般地，未经过认证的用户发出的 HTTP 请求报文会被拦截，已通过认证的用户将不被拦截。HTTP 拦截是 Web 认证功能的基础，一旦浏览器发出的 HTTP 报文被拦截，就会自动触发 Web 认证的过程。

HTTP 重定向

根据 HTTP 协议规定，正常情况下，用户的浏览器发出 HTTP GET 或 HEAD 请求报文后，如果服务器能够提供资源，则以 200 状态码为报文进行响应，表示请求成功；如果服务器上的资源被临时移动到新地址，且服务器希望客户端使用新的地址访问该资源，则以 302 状态码为报文进行响应，表示临时重定向，且在 302 响应报文中，提供了一个新的站点路径，用户收到响应后，可以向该新的站点重新发出 HTTP GET 或 HEAD 报文请求资源，即重定向。

HTTP 重定向是 Web 认证的重要环节，是发生在 HTTP 拦截之后的，利用的就是 HTTP 协议中的 302 报文的特性。HTTP 拦截过程将使得网络设备和用户之间建立起连接会话，随后用户将（本应发给其他站点的）HTTP GET 或 HEAD 报文发给网络设备，网络设备收到后，回应以 302 报文，并且在 302 报文中加入重定向页面的站点路径，这样用户将向该站点路径重新发出请求，就会获取到重定向的页面。

由于越来越多的应用程序基于 HTTP 协议运行，采用 302 重定向报文有可能会将大量的非浏览器发出的 HTTP 流引向 Portal 服务器，影响网络认证，因此设备的重定向技术采用的是通过 js 脚本代替 302 报文，此技术称为降噪。

工作原理

组网拓扑图如 图 1-1 Web 认证方案网络拓扑图。

Web 认证的角色：

- 认证客户端：通常为浏览器，该浏览器运行 HTTP 协议，用户通过浏览器上网时浏览器将发出 HTTP 请求。
- 网络设备：在网络拓扑中一般为接入层设备（例如在无线网络中可以是无线 AP），并与用户终端设备直接相连，在设备上需要启动 Web 认证功能。

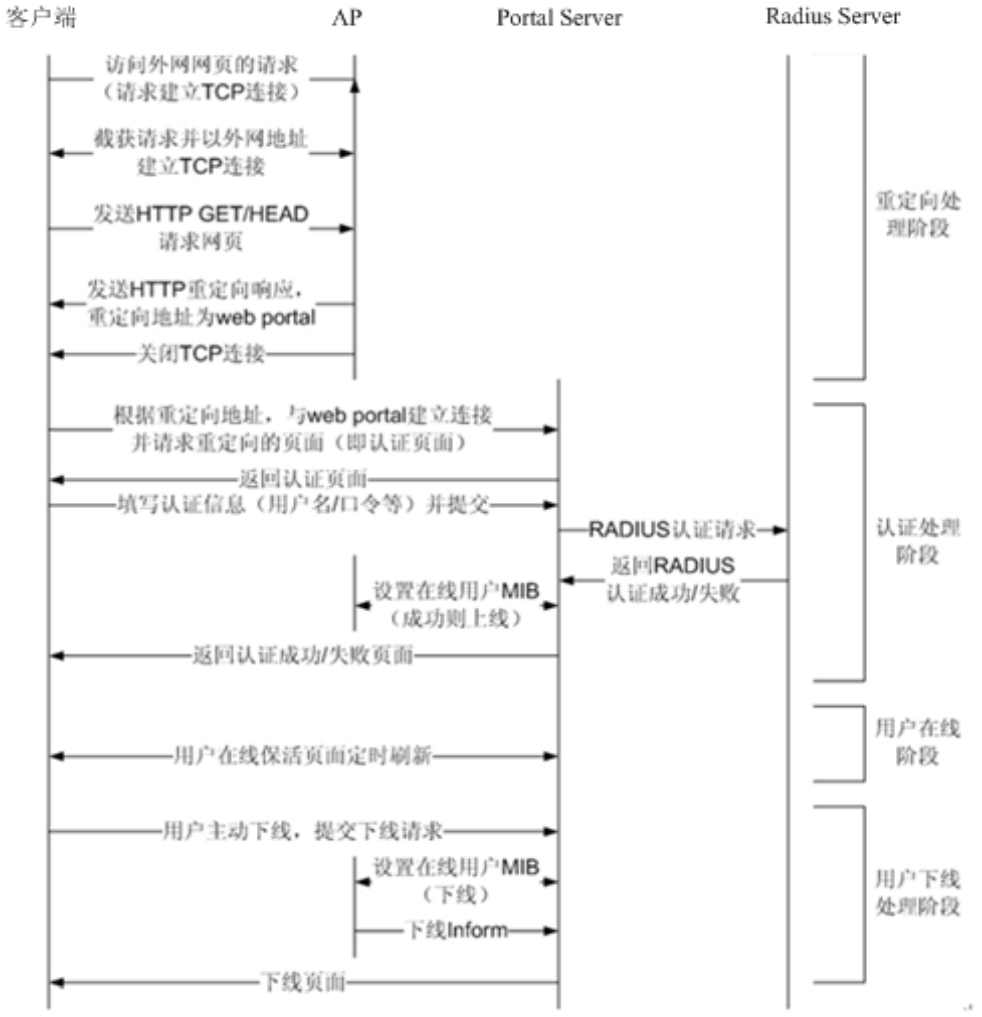
- Portal 服务器：提供 Web 认证的认证界面和相关操作。Portal 服务器接受认证客户端发出的基于 HTTP 的认证请求，提取其中的账号信息，将此信息发送到认证服务器进行认证，之后通告用户和网络设备认证结果。图中为锐捷 ePortal 服务器。
- RADIUS 服务器：提供基于 RADIUS 协议的远程用户认证，Portal 服务器从 HTTP 中获取用户的认证账号信息，之后通过 RADIUS 协议向 RADIUS 服务器请求认证。RADIUS 服务器通过 RADIUS 协议向 Portal 服务器反馈认证结果。图中为锐捷 SAM 服务器。

Web 认证的流程：

1. 请求拦截与重定向：在用户尝试访问网络资源之前，网络设备（如接入点 AP 等）会拦截所有来自未认证用户的 HTTP 请求，并将请求重定向至 Portal 服务器。此步骤确保了用户的浏览器会首先显示认证页面，要求用户进行身份验证。
2. 用户身份认证：在认证页面上，用户输入必要的认证信息，如用户名、口令、校验码等，并提交给 Portal 服务器进行处理，验证用户输入的信息是否有效且符合安全策略。
3. 认证成功与访问授权：Portal 服务器确认用户身份认证成功，会立即通知网络设备该用户已通过认证。收到此通知后，网络设备会更新其访问控制策略，允许该用户访问互联网资源。

详细的原理图如下图所示：(图中以 AP 设备为例)

图 1-2 一代 Web 认证流程图



用户下线流程分如下两种类型：

- 设备端触发的用户下线流程

1. 检测与判定：设备端持续监控用户的在线状态，包括在线时长、使用的流量量以及网络连接状态。当用户的在线时长达到预设的阈值、使用的流量达到限额，或者由于链路断开等原因导致用户实际离线时，设备端会判定用户需要下线。
2. 通知 Portal 服务器：一旦确定用户需要下线，设备端会立即向 Portal 服务器发送用户下线的通知。该通知应包含用户标识、下线原因等必要信息，以便 Portal 服务器进行相应的处理。
3. SNMP 协议应用：Portal 服务器在接收到设备端的下线通知后，通过 SNMP 协议向设备发送指令，要求设备删除该用户的会话信息，确保用户资源得到及时释放。
4. 用户反馈：Portal 服务器在完成上述操作后，通过 Web 重定向或其他方式向用户展示下线页面，明确告知用户他们已被下线，可能的原因以及后续操作建议。

- Portal 服务器端触发的用户下线流程

1. 用户主动申请或超时判定：Portal 服务器监控用户行为，包括用户是否通过下线页面主动发起下线申请，或者保活页面是否因超时而失效。当检测到这些情况时，Portal 服务器会判定用户需要下线。
2. 通知设备端：Portal 服务器通过 SNMP 协议向设备端发送用户下线的指令，要求设备端删除用户会话信息，并同步更新网络状态。
3. 设备响应：设备端在接收到 Portal 服务器的下线指令后，执行相应的操作，如删除用户会话、释放网络资源等，并确认操作完成。
4. 用户反馈：Portal 服务器在确认设备端已完成下线操作后，再次通过 Web 重定向或其他方式向用户展示下线页面，确保用户明确了解他们的会话已结束。

以上两种情况，Portal 服务器都会向 RADIUS 服务器发起计费结束请求，通告 RADIUS 服务器用户下线。

相关配置

↘ 创建配置模板

缺省情况下无配置。

在全局配置模式下，使用 **web-auth template eportalv1** 命令创建模板。

可以使用该配置模板进行 Web 认证功能。

↘ 配置服务器 IP 地址

缺省情况下无配置。

在模板配置模式下，使用 **ip** *ip-address* 配置服务器 IP 地址。

访问服务器的请求被设备放行，并且支持对发往服务器的请求进行限速保护。

↘ 配置服务器认证 URL

缺省情况下无配置。

在模板配置模式下，使用 **url** *url-string* 进行配置。

用户重定向到的 URL 地址，通常使用 Portal 认证页面地址。

配置绑定模式

缺省情况下为仅 ip 绑定。

在模板配置模式下，使用 **bindmode** 进行配置。

对于跨三层网络认证的环境，由于经过路由后 mac 地址已经变了，需要配置为仅 ip 绑定模式。

配置通信加密密钥

缺省情况下无配置。

在全局配置模式下，使用 **web-auth portal key** [**0** | **1** | **7**] *key-string* 配置通信加密密钥。

用作 URL 参数加密，避免信息泄漏。

开启 Web 认证

缺省情况下该功能关闭。

在无线安全配置模式下，使用 **webauth** 命令开启认证。

配置 Web 认证 SNMP 协议服务器

缺省情况下无配置。

在全局配置模式下 ,使用 **snmp-server host** *ip-address* **inform version 2c** *community-string* **web-auth** 配置 Web 认证 SNMP 协议服务器。

设备可以通过 inform/trap 报文通告用户下线消息给配置的服务器。

配置服务器 SNMP 通信团体字

缺省情况下无配置。

在全局配置模式下，使用 **snmp-server community** *community-string* **rw** 配置服务器 SNMP 通信团体字。

服务器通过该团体字来读写设备的用户表项信息。

启用 SNMP TRAP/INFORM 通告功能

缺省情况下无配置。

在全局配置模式下，使用 **snmp-server enable traps web-auth** 配置启用 SNMP TRAP/INFORM 通告功能。

开始通告功能，用于设备向服务器通告用户下线消息。

1.3.2 二代 Web 认证

HTTP 拦截

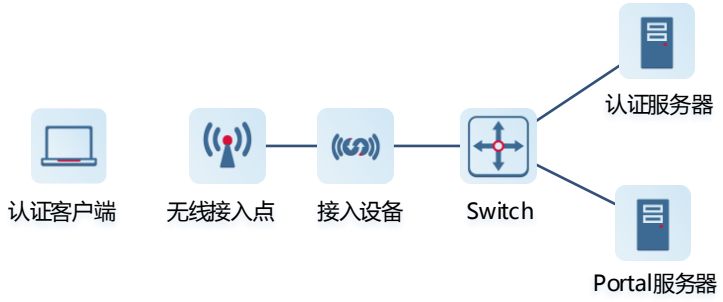
同一代 Web 认证的 HTTP 拦截技术。

HTTP 重定向

同一代 Web 认证的 HTTP 重定向技术。

工作原理

图 1-3 无线外置 Portal Web 认证系统



Web 认证的角色：

- 认证客户端：通常为浏览器，该浏览器运行 HTTP 协议，用户通过浏览器上网时浏览器将发出 HTTP 请求。
- 接入设备（AC 或 AP）：在网络拓扑中一般为接入层设备（例如在无线网络中可以是无线 AP），并与用户终端设备直接相连，在设备上需要启动 Web 认证功能。接入设备主要有以下几个方面的作用：

（1）负责拦截认证客户端的网络访问请求。
（2）利用 HTTP 重定向功能将重定向页面推送给认证客户端。
（3）接收 Portal 服务器发过来的客户端认证信息，向认证服务器发起认证请求。
（4）根据认证结果设置客户端是否可以上网，同时向 Portal 服务器反馈认证结果。

- Portal 服务器：提供 Web 认证的认证界面和相关操作。Portal 服务器接受认证客户端发出的基于 HTTP 的认证请求，提取其中的账号信息，将此信息发送到网络设备，同时根据网络设备反馈的认证结果，通过页面反馈给用户。该 Portal 服务器可以是锐捷自研的 Portal 服务器，也可以是第三方 Portal 服务器。
- 认证服务器：提供基于 RADIUS 协议的远程用户认证。

Web 认证主要流程：

1、 拦截与重定向：在用户尝试访问网络资源之前，网络设备（如接入点 AP 等）会拦截所有来自未认证用户的 HTTP 请求，并将请求重定向至 Portal 服务器。此步骤确保了用户的浏览器会首先显示认证页面，要求用户进行身份验证。

2、 用户认证交互：在认证页面上，用户输入必要的认证信息，如用户名、口令、校验码等，并提交给 Portal 服务器进行处理。

3、 认证信息转发：Portal 服务器将收集到的用户认证信息转发给设备，设备作为认证流程的发起者，需要此信息进一步验证用户的身份。

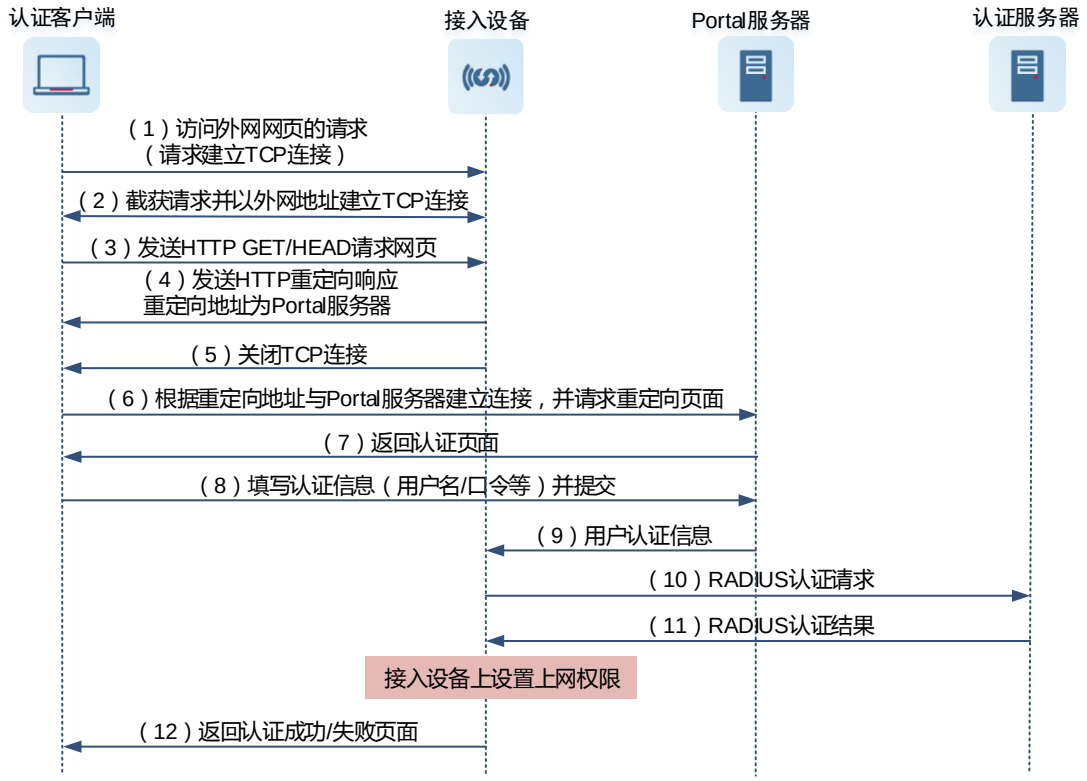
4、 设备向 RADIUS 服务器认证：设备接收到认证信息后，会向 RADIUS 服务器发起认证请求。在请求中，设备会携带一系列关键参数，包括但不限于：用户 IP（wlanuserip）、接入控制器名称（wlanacname）、服务集标识符（SSID）、网络

接入服务器 IP（nasip）、用户 MAC 地址（mac）以及用户最初尝试访问的 URL（url）。这些参数有助于 RADIUS 服务器进行准确的身份验证和授权决策。

5、 认证结果反馈：RADIUS 服务器处理完认证请求后，会将认证结果（成功或失败）返回给设备。设备接收到认证结果后，会立即将此信息反馈给 Portal 服务器。

6、 认证结果通知用户：Portal 服务器根据从设备接收到的认证结果，向用户展示相应的页面。如果认证成功，用户将被允许访问网络资源；如果认证失败，用户将收到错误提示，并可能需要重新尝试认证或联系管理员。

图 1-4 二代 Web 认证流程



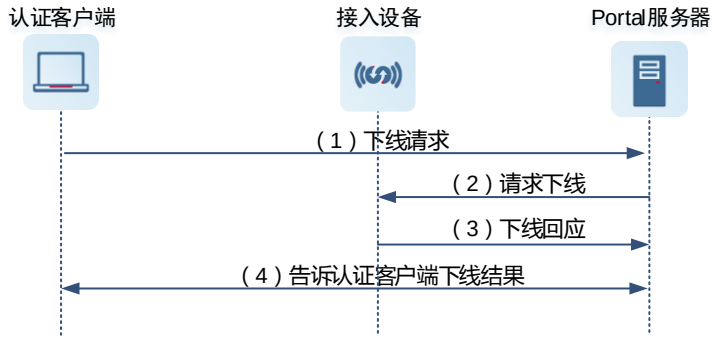
用户下线流程：

- 设备端触发的用户下线：设备持续监控用户的网络活动，当检测到用户的流量使用降至预设的低流量阈值以下，或者由于链路断开等原因导致用户实际离线，并持续一段时间（具体依配置参数而定）时，设备会自动判定用户处于非活跃状态，从而触发用户下线流程。设备会通知 Portal 服务器，Portal 服务器记录此事件，但通常不会主动向用户推送下线页面，因为用户可能已自行关闭浏览器或设备。
- Portal 服务器端触发的用户下线

  用户主动下线：用户在使用网络服务过程中，可通过点击页面上提供的“下线”按钮主动申请下线。此操作会触发 Portal 服务器接收到用户下线的请求。Portal 服务器随后会向设备发送指令，要求设备将该用户从活跃用户列表中移除，并确认用户下线状态。用户下线后，Portal 服务器可能向用户显示一个确认页面，告知用户已成功下线。

  RADIUS 策略下线 :RADIUS 服务器可能因为安全策略、资源限制或其他管理需求 ,主动将用户从网络中踢出。当 RADIUS 服务器执行此操作时，会向设备发送一个包含用户下线指令的消息。设备在接收到此指令后，会立即执行用户下线操作，并通知 Portal 服务器。Portal 服务器随后会根据需要向用户推送一个下线页面，明确告知用户他们的会话已被终止。

图 1-5 二代 Web 认证下线流程



相关配置

创建配置模板

缺省情况下无配置。

在全局配置模式下，使用 **web-auth template { eportalv2 |** *template-name* **v2 }**命令创建二代认证模板。

可以使用该配置模板进行 Web 认证功能。

配置服务器 IP 地址

缺省情况下无配置。

在模板配置模式下，使用 **ip** *ip-address* 配置服务器 IP 地址。

访问服务器的请求被设备放行，并且支持对发往服务器的请求进行限速保护。

配置服务器认证 URL

缺省情况下无配置。

在模板配置模式下，使用 **url** *url-string* 进行配置。

用户重定向到的 URL 地址，通常使用 Portal 认证页面地址。

配置绑定模式

缺省情况下为仅 ip 绑定。

在模板配置模式下，使用 **bindmode** 进行配置。

对于跨三层网络认证的环境，由于经过路由后 mac 地址已经变了，需要配置为仅 ip 绑定模式。

配置通信加密密钥

缺省情况下无配置。

在全局配置模式下，使用 **web-auth portal key** [**0** | **1** | **7**] *key-string* 配置通信加密密钥。

用作 URL 参数加密，避免信息泄漏。

开启 Web 认证

缺省情况下该功能关闭。

在无线安全配置模式下，使用 **webauth** 命令开启认证。

配置启用 AAA 认证

缺省情况下关闭 AAA 认证。

在全局配置模式下，使用 **aaa new-model** 命令来开启 AAA 认证功能。

二代 Web 认证功能需要依赖于 AAA 认证功能，使用时需要开启 AAA 功能。

配置 RADIUS 服务器和通信密钥

缺省情况下无配置。

在全局配置模式下，使用 **radius-server host** 命令配置 RADIUS 服务器和通信密钥。

对应于 Web 认证中的 RADIUS 服务器。用于为 Web 认证用户进行身份校验。

配置 AAA 模块 Web 认证的方法列表

缺省情况下无配置。

在全局配置模式下，使用 **aaa authentication web-auth** 命令配置二代 Web 认证的认证方法。

Web 认证功能可以配置使用该方法列表来进行认证交互。

配置 AAA 模块网络记账方法列表

缺省情况下无配置。

在全局配置模式下，使用 **aaa accounting network** 命令配置网络记账方法。

Web 认证功能可以配置使用该方法列表来进行记账交互。

配置 Web 认证使用的 AAA 认证方法列表名

缺省情况下使用 default 方法。

在模板配置模式下，使用 **authentication** 命令进行配置。

Web 认证功能通过该方法列表名字向 AAA 功能发起认证请求。

配置 Web 认证使用的 AAA 认证记账列表名

缺省情况下使用 default 方法。

在模板配置模式下，使用 **accounting** 命令进行配置。

Web 认证功能通过该方法列表名字向 AAA 功能发起记账请求。

配置 Portal 服务器的通信 UDP 端口号

缺省情况下使用 50100 端口号。

在模板配置模式下，使用 **port** 命令进行配置。

设备通过发送报文到该端口来同 Portal 服务器进行交互。

1.3.3 内置 Portal Web 认证

HTTP 拦截

同一代 Web 认证的 HTTP 拦截技术。

HTTP 重定向

同一代 Web 认证的 HTTP 重定向技术。

工作原理

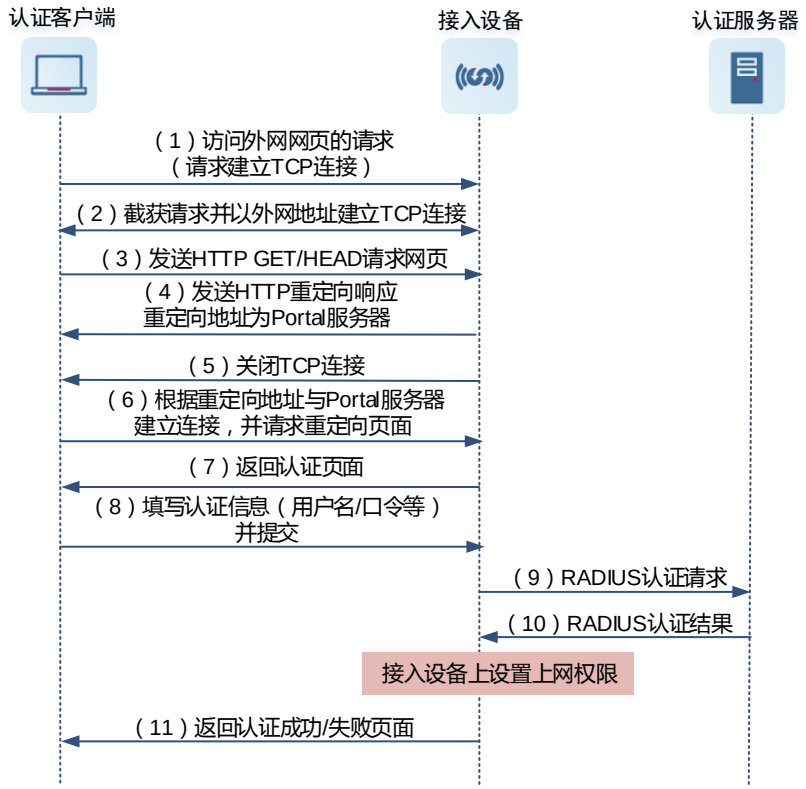
图 1-6 无线内置 Portal Web 认证系统

Web 认证的角色：

- 认证客户端：通常为浏览器，该浏览器运行 HTTP 协议，用户通过浏览器上网时浏览器将发出 HTTP 请求。
- 网络设备 :在网络拓扑中一般为接入层设备 ,并与用户终端设备直接相连接(有线或者无线) ,在设备上需要启动内置 Portal Web 认证功能。由设备解析用户在页面中输入的帐号并向 RADIUS 服务器发起认证请求，根据认证结果设置用户是否可以上网，同时向终端浏览器推送认证结果。
- RADIUS 服务器：提供基于 RADIUS 协议的远程用户认证。图中为锐捷 SAM 服务器。

Web 认证主要流程：

图 1-7 无线内置 Portal Web 认证流程



1、 拦截与重定向：在用户尝试访问网络资源之前，网络设备（如接入点 AP 等）会拦截所有来自未认证用户的 HTTP 请求，并将请求重定向至本机内置的 Portal 服务器。此步骤确保了用户的浏览器会首先显示认证页面，要求用户进行身份验证。

2、 用户认证交互：在认证页面上，用户输入必要的认证信息，如用户名、口令、校验码等，并提交给内置的 Portal 服务器进行处理。

3、 设备向 RADIUS 服务器认证：设备接收到内置的 Portal 服务器给出的认证信息后，会向 RADIUS 服务器发起认证请求。在请求中，设备会携带一系列关键参数，包括但不限于：用户 IP（wlanuserip）、接入控制器名称（wlanacname）、服务集标识符（SSID）、网络接入服务器 IP（nasip）、用户 MAC 地址（mac）以及用户最初尝试访问的 URL（url）。这些参数有助于 RADIUS 服务器进行准确的身份验证和授权决策。

4、 认证结果反馈：RADIUS 服务器处理完认证请求后，会将认证结果（成功或失败）返回给设备。设备接收到认证结果后，会立即将此信息反馈给内置的 Portal 服务器。

5、 认证结果通知用户：内置的 Portal 服务器根据从设备接收到的认证结果，向用户展示相应的页面。如果认证成功，用户将被允许访问网络资源；如果认证失败，用户将收到错误提示，并可能需要重新尝试认证或联系管理员。

用户下线流程：

- 用户主动下线：用户在使用网络服务过程中，可通过点击页面上提供的“下线”按钮主动申请下线。设备实时监测到这一页面交互动作后，会立即触发下线流程，将用户从活跃会话中移除，实现用户下线。
- 设备端触发的用户下线：设备持续监控用户的网络活动，当检测到用户的流量使用降至预设的低流量阈值以下，或者由于链路断开等原因导致用户实际离线，并持续一段时间（具体依配置参数而定）时，设备会自动判定用户处于非活跃状态，从而触发用户下线流程。下线过程中，设备可能会记录相关日志，以便后续审计或分析。

- RADIUS 策略下线 :RADIUS 服务器可能因为安全策略、资源限制或其他管理需求 ,主动将用户从网络中踢出。当 RADIUS 服务器执行此操作时，向设备发送一个包含用户下线指令的消息。设备在接收到此指令后，会立即执行用户下线操作，并通知内置 Portal 服务器。内置 Portal 服务器随后会根据需要向用户推送一个下线页面，明确告知用户他们的会话已被终止。

相关配置

创建配置模板

缺省情况下无配置。

在全局配置模式下，使用 **web-auth template iportal** 命令创建模板。

可以使用该配置模板配置内置 Portal Web 认证相关参数。

配置页面包

缺省情况下使用设备出厂自带的页面包。

在模板配置模式下，使用 **page-suite** 配置使用指定的页面包。

指定页面包之前需要先将页面包下载到 FLASH 中。

配置广告推送方式和地址

缺省情况认证后推送。

在模板配置模式下，使用 **login-popup** *url-string* 配置认证前推送的广告地址；使用 **online-popup** *url-string* 配置认证后推送的广告地址。

配置绑定模式

缺省情况下为仅 ip 绑定。

在模板配置模式下，使用 **bindmode** 进行配置。

对于跨三层网络认证的环境，由于经过路由后 mac 地址已经变了，需要配置为仅 ip 绑定模式。

开启 Web 认证

缺省情况下该功能关闭。

在无线安全配置模式下，使用 **webauth** 命令开启认证。

配置启用 AAA 认证

缺省情况下关闭 AAA 认证。

在全局配置模式下，使用 **aaa new-model** 命令来开启 AAA 认证功能。

二代 Web 认证功能需要依赖于 AAA 认证功能，使用时需要开启 AAA 功能。

配置 RADIUS 服务器和通信密钥

缺省情况下无配置。

在全局配置模式下，使用 **radius-server host** 命令配置 RADIUS 服务器和通信密钥。

对应于 Web 认证中的 RADIUS 服务器，用于为 Web 认证用户进行身份校验。

↘ 配置 AAA 模块 Web 认证的方法列表

缺省情况下无配置。

在全局配置模式下，使用 **aaa authentication iportal** 命令配置二代 Web 认证的认证方法。

Web 认证功能可以配置使用该方法列表来进行认证交互。

↘ 配置 AAA 模块网络记账方法列表

缺省情况下无配置。

在全局配置模式下，使用 **aaa accounting network** 命令配置网络记账方法。

Web 认证功能可以配置使用该方法列表来进行记账交互

↘ 配置 Web 认证使用的 AAA 认证方法列表名

缺省情况下使用 default 方法。

在模板配置模式下，使用 **authentication** 命令进行配置。

Web 认证功能通过该方法列表名字向 AAA 功能发起认证请求。

↘ 配置 Web 认证使用的 AAA 认证记账列表名

缺省情况下使用 default 方法。

在模板配置模式下，使用 **accounting** 命令进行配置。

Web 认证功能通过该方法列表名字向 AAA 功能发起记账请求。

1.3.4 MAC 短信认证

工作原理

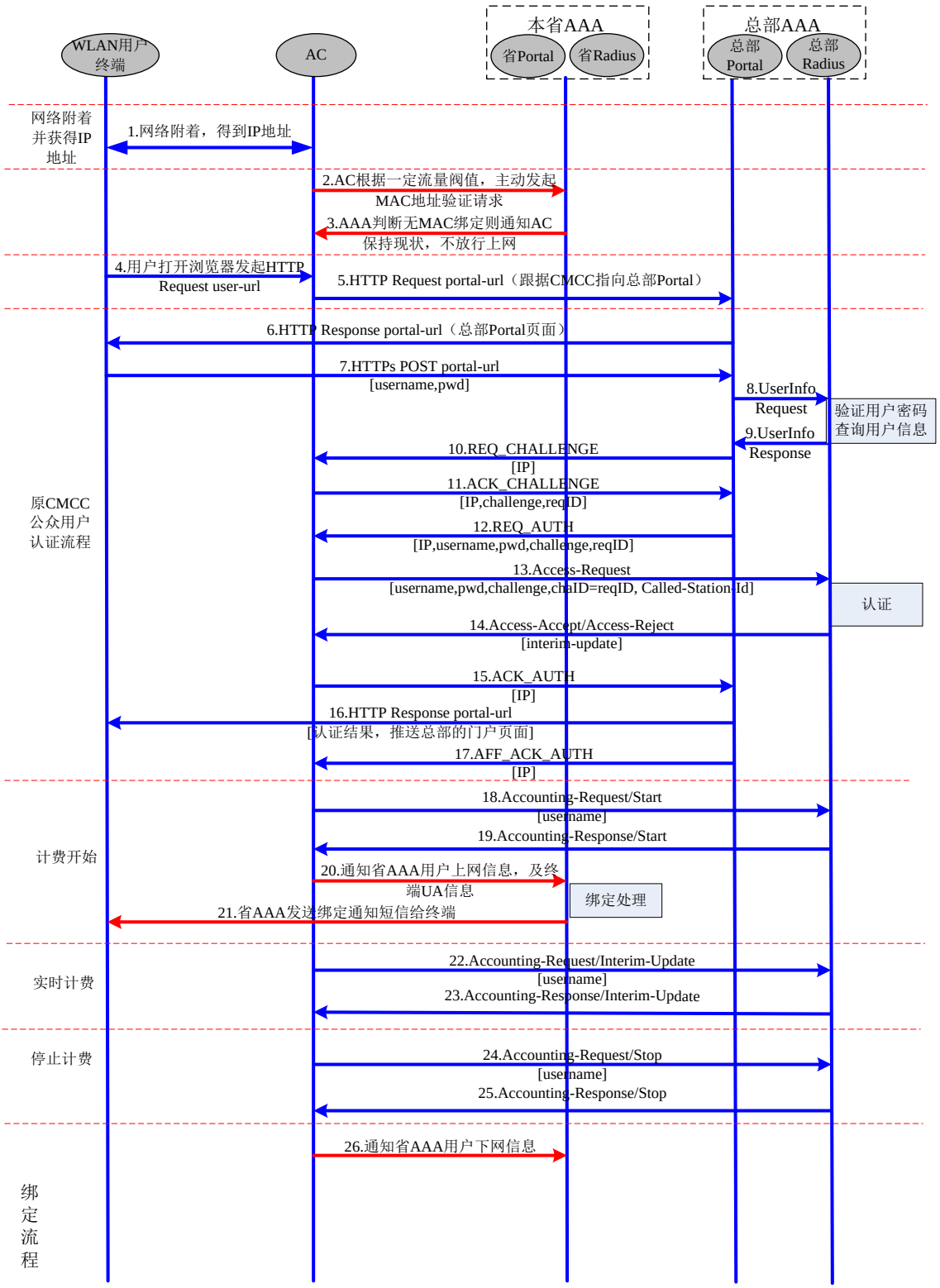
终端用户关联到一个已开启 MAC 短信认证功能的 SSID，并通过 DHCP 获取 IP 地址后，被允许使用网络。在使用网络过程中，如果流量使用达到设定的阈值时，系统将触发 MAC 绑定查询流程。即 AC 向 Portal 服务器发起用户 MAC 地址绑定状态查询请求，如果用户 MAC 地址为已绑定状态，则 Portal 服务器直接向终端用户发起认证请求，用户通过预设的认证方式（如短信验证码）进行认证；如果用户 MAC 地址为未绑定状态，Portal 服务器将引导终端用户重定向至认证页面，用户完成 Portal 认证流程后方可接入网络。

↘ 未绑定用户上网流程

未绑定用户首次接入已开启 MAC 短信认证的 SSID 网络时，系统会自动触发重定向机制，将用户浏览器重定向到 Portal 认证页面。在认证前，系统会自动进行 MAC 地址绑定状态的查询。如果识别到用户为首次接入或未绑定 MAC 地址，则在用户到达认证页面后，除了常规的账号登录或短信验证信息填写外，还可根据需求选择是否勾选“绑定”复选框，并完成相应的认证

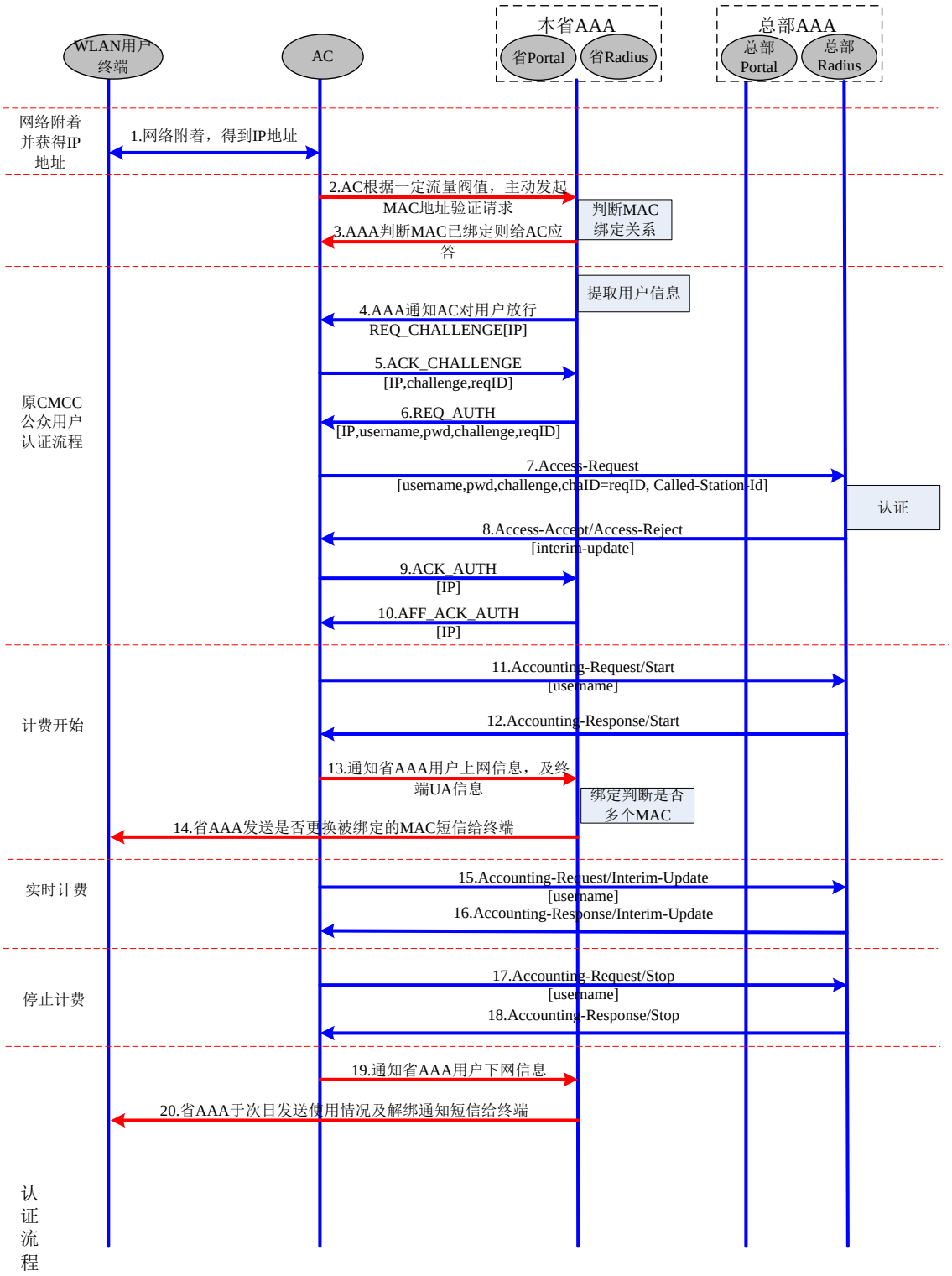
操作。若用户选择绑定，认证成功后，系统会将用户的 MAC 地址与认证账号进行绑定，并将此信息同步至 Portal 服务器。一旦完成绑定，用户在未来的网络接入中将直接根据已绑定用户的便捷流程进行上网，无需再次进行繁琐的认证操作，提升了用户体验。

除此之外，用户在线期间及下线时，系统会自动向 Portal 服务器发送通告，确保服务器实时掌握用户连接状态，便于后续管理和维护。



↘ 已绑定用户的上网流程

已绑定用户上网时，无需要通过打开浏览器进行认证上网，关联网络后自动完成网络接入，极大地方便了用户使用无线网络。



1.3.5 RIPT

Web 认证支持 RIPT（Remote Intelligent Perceptive Technology，边缘智能感知技术，又称智能 AP）功能，在 AC 故障或者 AC 和 AP 断开连接时，可以使得 AP 上的 Web 认证模块继续对外提供认证服务。

工作原理

通过 AC 上配置 RIPT AP 组，开启 RIPT 功能（RIPT 的详细配置见《边缘智能感知配置手册》）。在 RIPT 的 AP 认证模式下，AC 上的 Web 认证相关的配置下发到 RIPT 的 AP 上，AP 即可作为接入设备单独对外提供完整的 Web 认证服务（终端用户不必在 AC 上进行 Web 认证）。AP 上认证通过的用户信息同步到 AC 上，AC 上可查看认证用户状况。

↘ 下发配置

RIPT 的 AP 认证模式下，AC 上配置 AAA，RADIUS 以及 rsna 开启 Web 认证受控口，可以下发到支持 RIPT 的对应 AP 上。下发到 AP 的配置完备之后，AP 即可对外提供 WLAN 服务，包括 Web 认证服务。

↘ 同步 AP 的用户信息到 AC

终端用户连接上对外提供 Web 认证服务的 RIPT AP，进行认证。AP 上认证通过的 WEB 用户信息可以同步到 AC 上，方便 AC 上查看认证用户状况。

1.3.6 WiFiDog

HTTP 拦截

同一代 Web 认证的 HTTP 拦截技术。

HTTP 重定向

同一代 Web 认证的 HTTP 重定向技术。

工作原理

组网拓扑图同 图 1-1 Web 认证方案网络拓扑图。

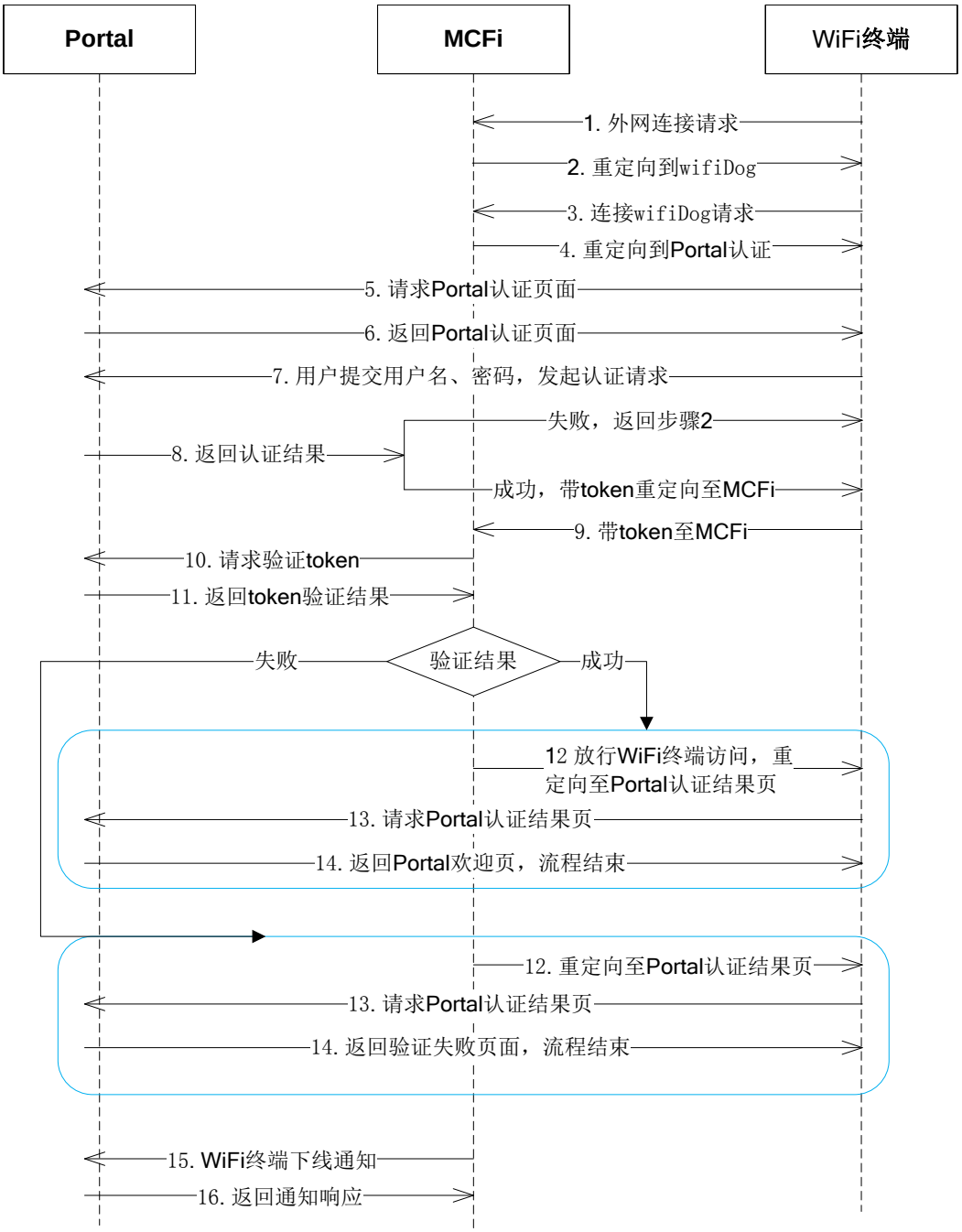
Web 认证的角色：

- 认证客户端：通常为浏览器，该浏览器运行 HTTP 协议，用户通过浏览器上网时浏览器将发出 HTTP 请求。
- 网络设备：在网络拓扑中一般为接入层设备（例如在无线网络中可以是无线 AP），并与用户终端设备直接相连，在设备上需要启动 Web 认证功能。设备控制用户的上网权限，接收认证客户端发来的 token 校验请求或放行网络的请求，同时还负责向 Portal 服务器校验 token 信息。
- Portal 服务器：提供 Web 认证的认证界面和相关操作。Portal 服务器接受认证客户端发出的基于 HTTP 的认证请求，提取其中的账号信息，后台认证后，此认证结果经认证客户端中转给网络设备，网络设备校验完成后再要求认证客户端重定向端 Portal 服务器的相关页面。
- 认证服务器：提供用户认证服务，具体协议由 Portal 服务器和认证服务器协商决定（例如 RADIUS 协议）。

WiFiDog 认证的流程：

1. 请求拦截与重定向：在用户尝试访问网络资源之前，网络设备（如接入点 AP 等）会拦截所有来自未认证用户的 HTTP 请求，并将请求重定向至 WiFiDog 服务，与 WiFiDog 服务连接成功后，会将用户重定向到 Portal 服务器。此步骤确保了用户的浏览器会首先显示认证页面，要求用户进行身份验证。
2. 用户身份认证：在认证页面上，用户输入必要的认证信息，如用户名、口令、校验码等，并提交给 Portal 服务器进行处理，验证用户输入的信息是否有效且符合安全策略。
3. 认证成功与访问授权：Portal 服务器确认用户身份认证成功，会立即通知网络设备该用户已通过认证。收到此通知后，网络设备会更新其访问控制策略，允许该用户访问互联网资源。

图 1-8 WiFiDog 认证流程



用户下线流程：

- 用户主动下线：用户在使用网络服务过程中，可通过点击页面上提供的“下线”按钮主动申请下线。设备实时监测到这一页面交互动作后，会立即触发下线流程，将用户从活跃会话中移除，实现用户下线。
- 设备端触发的用户下线：设备持续监控用户的网络活动，当检测到用户的流量使用降至预设的低流量阈值以下，或者由于链路断开等原因导致用户实际离线，并持续一段时间（具体依配置参数而定）时，设备会自动判定用户处于非活跃状态，从而触发用户下线流程。下线过程中，设备可能会记录相关日志，以便后续审计或分析。

相关配置

↘ 创建配置模板

缺省情况下无配置。

在全局配置模式下，使用 **web-auth template** { **wifidog** | *template-name* **wifidog** }命令创建 WiFiDog 模板。

可以使用该配置模板进行 Web 认证功能。

↘ 配置服务器 IP 地址

缺省情况下无配置。

在模板配置模式下，使用 **ip** *ip-address* 配置服务器 IP 地址。

访问服务器的请求被设备放行，并且支持对发往服务器的请求进行限速保护。

↘ 配置服务器认证 URL

缺省情况下无配置。

在模板配置模式下，使用 **url** *url-string* 进行配置。

用户重定向到的 URL 地址，通常使用 Portal 认证页面地址。

↘ 配置设备 IP

缺省情况下无配置。

在模板配置模式下，使用 **nas-ip** *ip-address* 进行配置。

设置 WiFiDog 的设备接入服务 ip，用于服务器向此 ip 发起通讯。

配置的设备接入服务 ip 不能够被设置成直通地址。

配置接入服务 ip 为设备 IP 时会导致此认证模板下的终端访问此 ip 时被设备拦截并转发给服务器，从而不能访问设备的 Web 管理界面。

如有此认证模板下的终端直接访问此 ip 对此设备进行管理的需求，可将此接入服务 ip 设置为一个未使用的虚拟服务 ip，如 1.1.1.1，2.2.2.2 等。

一般情况下使用设备的真实 ip 直接登录管理设备无法保证安全性，需要把管理设备的 ip 映射成外网 ip，使用外网 ip 进行管理。由于外网和服务器之间有防火墙等安全设备防护，以保证安全性。而直接通过内网访问则无任何防护，如设备的真实 ip 对用户可见容易使设备直面攻击，因此建议配置为虚拟 ip。

配置 Gateway ID

缺省情况下配置为设备的序列号，在热备和 VAC 下必须配置，可以配置为其中一台设备的 MAC 地址。

在模板配置模式下，使用 **gateway-id** *string* 进行配置。

该参数为 WiFiDog 协议交互报文中需要携带的参数，开放命令给对接第三方 Portal 使用.

开启 Web 认证

缺省情况下该功能关闭。

在无线安全配置模式下，使用 **webauth** 命令开启认证。

1.3.7 微信认证

微信是一个为接入终端（iPhone、iPad、Android、PC）提供跨平台即时通讯的应用程序，微信公众平台通过公众号方式建立起商户与终端用户直接的互通平台。微信认证是快速连接 WiFi 的一种接入认证方式，通过引导移动终端关注微信公众号，商户通过公众号满足自身的特定需求，实现线上线下互通从而增加用户黏性。微信认证也是一种特殊的 Portal 认证，商户启用该认证后，移动终端无需输入繁琐的密码，仅需通过微信扫描公众号二维，重定向到 Portal 服务器提供的认证引导页完成实名认证接入，保障用户安全入网

HTTP 拦截

同一代 Web 认证的 HTTP 拦截技术。

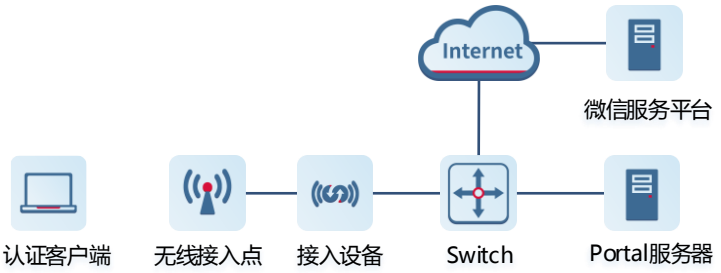
HTTP 重定向

同一代 Web 认证的 HTTP 重定向技术。

工作原理

微信认证系统

图 1-9 微信认证系统



- 认证客户端（STA）

认证客户端可以是 PC、iPhone、iPad、Android 等，是安装有微信的终端，也是微信认证的发起者，通常是商场内固定客户及进入线下场所的流动客户。

- 接入设备（AC 或 AP）

在网络规划中一般是接入层设备（在无线网络中可以是无线控制器 AC 或无线接入点 AP），在接入设备上需要启用微信认证模式的 Web 认证功能。在微信认证系统中，接入设备主要有以下几方面的作用：
在未认证通过之前，接入设备拦截认证客户端的外网访问 HTTP 请求重定向到 Portal 服务器。
在认证过程中，认证客户端、接入设备、Portal 服务器通过 HTTP 协议交互完成对认证客户端的身份合法性校验。
在认证结束之后，根据认证结果设置客户端是否可以上网，并返回认证结果页面给认证客户端。

- Portal 服务器

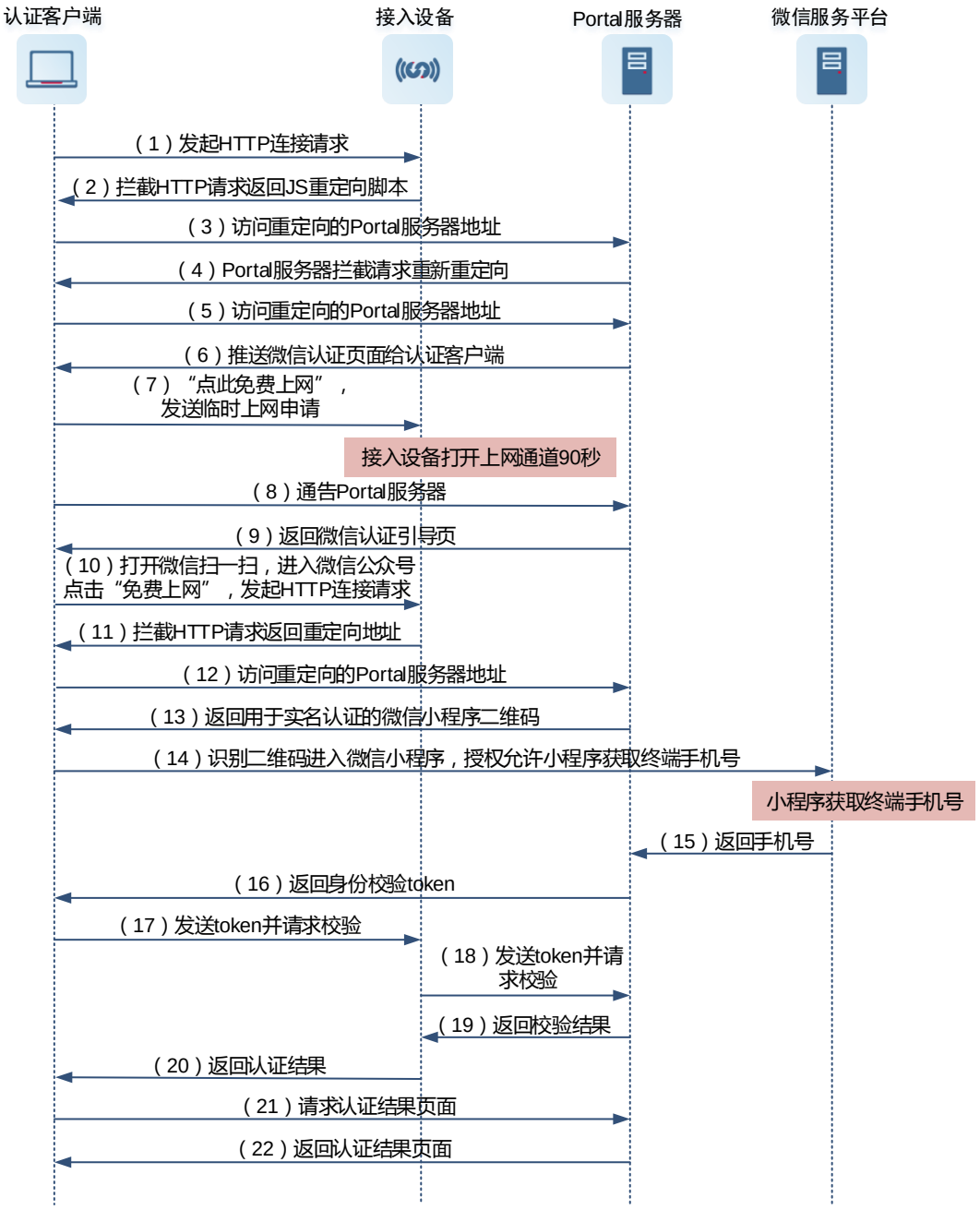
Portal 服务器负责接收认证客户端发出的认证请求，提供微信认证界面，并和接入设备完成认证信息交互。当微信认证应用在无线网接入认证时，Portal 服务器通常是锐捷网络自研的 RG-MCP 或者 RG-MACC 服务器。

- 微信服务平台

微信服务平台在微信认证过程中提供多种服务，如微信公众号服务、微信小程序服务、微信扫一扫服务。在微信认证过程中，认证客户端通过微信扫一扫识别商家二维码进入微信公众号，通过锐捷网络自研的用于实名认证的微信小程序向小程序服务器统一获取客户端手机号从而完成客户端实名认证。

↘ 微信认证流程

图 1-10 微信认证流程图



如图所示的微信认证流程中，可看出其认证流程大致如下：

1. 认证客户端连接已应用有微信认证的无线信号，在打开浏览器访问外网时发起 HTTP 连接请求。
2. 接入设备拦截认证客户端的 HTTP 请求并重定向到 Portal 服务器。
3. 认证客户端访问重定向地址，Portal 服务器推送微信认证页面给认证客户端。
4. 认证客户端在微信认证页面上通过点击“点我免费上网”，触发打开上网通道 90 秒请求，同时通告给 Portal 服务器。
5. 接入设备接收到认证客户端的请求后打开上网通道 90 秒。

6. Portal 服务器接收认证客户端的通告后，发送微信认证引导页给认证客户端用于完成后续的微信认证过程。
7. 认证客户端通过微信认证引导页进入微信客户端首页，打开扫一扫，扫描微信公众号。
8. 点击“点此免费上网”按钮（公众号里面），认证客户端发起 HTTP 连接请求。
9. 接入设备再次拦截重定向到 Portal 服务器。Portal 服务器将返回用于实名制认证的微信小程序二维码。
10. 认证客户端通过识别二维码进入微信小程序，并授权允许微信小程序获取认证客户端获取手机号。
11. 微信小程序获取该认证客户端的手机号，并返回手机号给 Portal 服务器。
12. Portal 服务器获取到认证客户端的基本信息，返回身份校验 token 给认证客户端。
13. 认证客户端发送身份校验 token 给接入设备。
14. 接入设备发送身份校验 token 给 Portal 服务器。
15. Portal 服务器接收到接入设备的身份校验信息判断认证客户端的合法性后返回 token 校验结果给接入设备。
16. 接入设备根据认证结果设置上网通道，返回认证结果给认证客户端。
17. 认证客户端向 Portal 服务器请求认证结果页面。
18. Portal 服务器返回认证结果页面认证客户端。

相关配置

创建配置模板

缺省情况下无配置。

在全局配置模式下，使用 **web-auth template** { **wechat** | *template-name* **wechat** }命令创建微信连 WiFi 认证模板。

可以使用该配置模板进行 Web 认证功能。

配置服务器 IP 地址

缺省情况下无配置。

在模板配置模式下，使用 **ip** *ip-address* 配置服务器 IP 地址。

访问服务器的请求被设备放行，并且支持对发往服务器的请求进行限速保护。

配置服务器 URL

缺省情况下无配置。

在模板配置模式下，使用 **service-url** *url-string* 进行配置。

设备和服务器通讯使用的 url 地址，当前只支持配置 ip 和端口。

支持配置服务器域名，方便与 MACC 的服务器对接，并要求服务器域名只能解析出一个 IP。配置域名时，url 中的协议名称部分将自动被去除，当前只支持 http 协议 url 的域名解析。

service_url 配置域名后，模版下的服务器 IP 地址将会被域名解析出的 IP 覆盖。

配置 Portal 服务器认证页面地址

缺省情况下配置为当前与服务器使用微信与短信共存认证时的短信认证重定向地址。

在模板配置模式下，使用 **url** *url-string* 进行配置。

该地址为使用微信与短信共存认证时的短信认证重定向地址。

↘ 配置设备 IP

缺省情况下无配置。

在模板配置模式下，使用 **nas-ip** *ip-address* 进行配置。

设置微信连 WiFi 认证的设备接入服务 ip，用于服务器向此 ip 发起通讯。

配置的设备接入服务 ip 不能够被设置成直通地址。

配置接入服务 ip 为设备 IP 时会导致此认证模板下的终端访问此 ip 时被设备拦截并转发给服务器，从而不能访问设备的 Web 管理界面。

如有此认证模板下的终端直接访问此 ip 对此设备进行管理的需求，可将此接入服务 ip 设置为一个未使用的虚拟服务 ip，如 1.1.1.1，2.2.2.2 等。

一般情况下使用设备的真实 ip 直接登录管理设备无法保证安全性，需要把管理设备的 ip 映射成外网 ip，使用外网 ip 进行管理。由于外网和服务器之间有防火墙等安全设备防护，以保证安全性。而直接通过内网访问则无任何防护，如设备的真实 ip 对用户可见容易使设备直面攻击，因此建议配置为虚拟 ip。

↘ 配置与服务器通讯使用的加密秘钥

缺省情况下无配置。

在模板配置模式下，使用 **key** {*key-string* }进行配置。

该秘钥是用来加密用户认证的信息，需要和服务器上配置的秘钥一致。

↘ 配置 nas-id

缺省情况下配置为设备 MAC，在热备和 VAC 场景下必须配置。

在 AC 配置模式下，使用 **nas-id** { *nas-id-str* }进行配置。

↘ 开启 Web 认证

缺省情况下该功能关闭。

在无线安全配置模式下，使用 **web-auth portal { eportalv1 | eportalv2 | iportal | wifidog | wechat | cpweb |** *name* **}**和 **webauth** 命令开启用户所在端口 Web 认证。

开启认证后端口下未认证手机终端用户会被重定向到服务器一键上网页面，未认证的 PC 用户会被重定向到二维码页面。

↘ 配置逃生功能

缺省情况下该功能关闭。

在全局配置模式或无线安全配置模式下，使用 **web-auth wechat-escape interval** *minutes* 进行配置。
无线安全配置模式下配置优先生效，若无线安全配置模式下该模式下未配置则使用全局模式配置。

配置后，当满足逃生条件时（服务器不通或者服务器希望用户逃生），后续接入的用户都可以逃生免认证。逃生用户的上网时长由 **interval** *minutes* 指定。

如果要取消逃生状态，可以在全局配置模式使用 **web-auth wechat-escape recover**。

↘ 配置服务器检测功能

缺省情况下该功能关闭。

在全局配置模式使用 **web-auth wechat-check interval** *minutes* 进行配置。

配置后，设备开始对服务器进行检测，如果一定间隔内（由 **interval** *minutes* 指定）检测到服务器没有应答或者回应不可用，同时设备配置了集体逃生功能，后面接入的所有用户都直接逃生免认证。

如果要取消服务器检测，可以在全局配置模式使用 **no web-auth wechat-check** 取消服务器检测功能。

1.3.8 Clearpass 认证

HTTP 拦截

同一代 Web 认证的 HTTP 拦截技术。

HTTP 重定向

同一代 Web 认证的 HTTP 重定向技术。

工作原理

组网拓扑图同 图 1-1 Web 认证方案网络拓扑图。

Web 认证的角色：

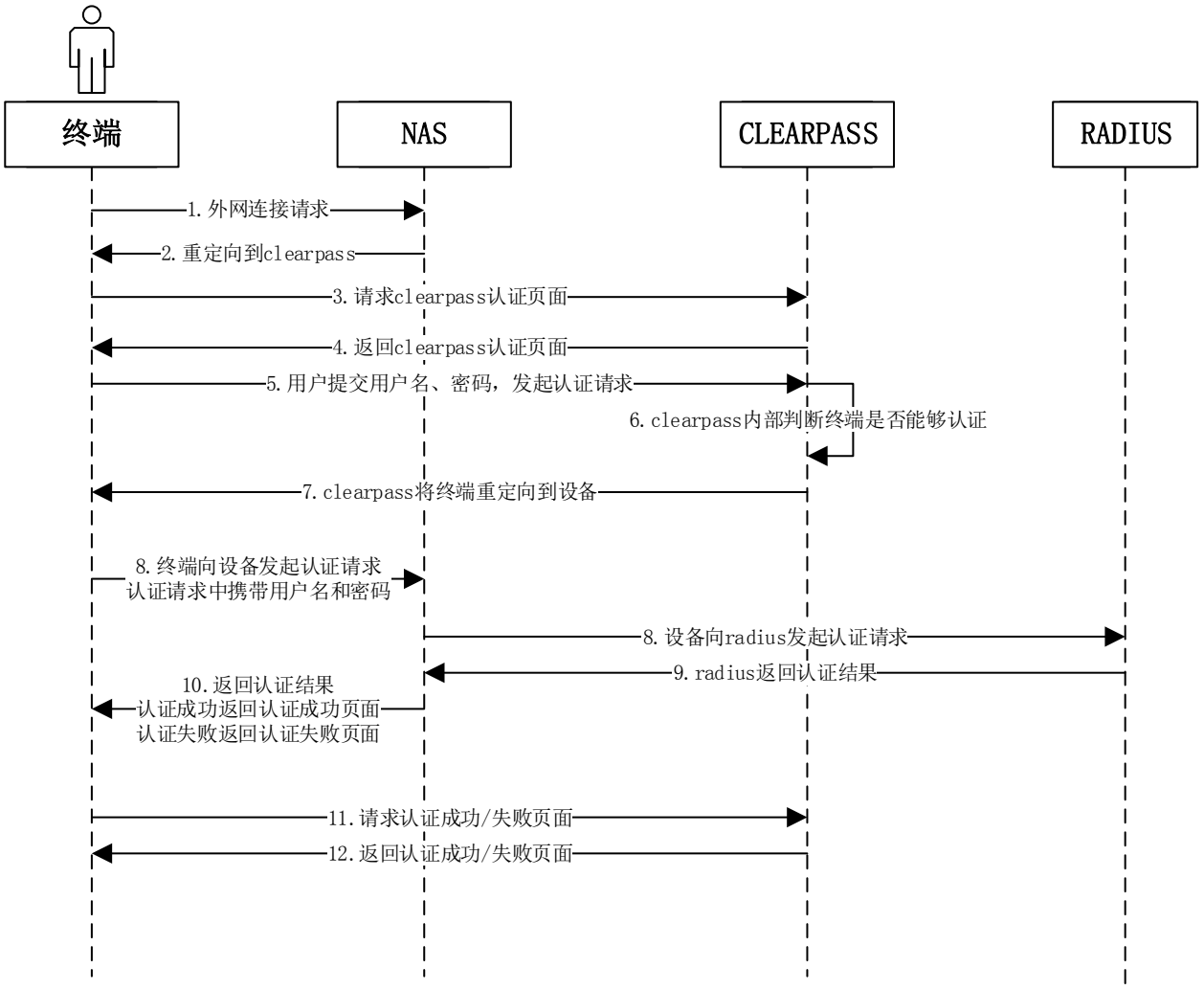
- 认证客户端：通常为浏览器，该浏览器运行 HTTP 协议，用户通过浏览器上网时浏览器将发出 HTTP 请求。
- 网络设备：在网络拓扑中一般为接入层设备（例如在无线网络中可以是无线 AP），并与用户终端设备直接相连，在设备上需要启动 Web 认证功能。设备控制用户的上网权限，接收认证客户端发来的 token 校验请求或放行网络的请求，同时还负责向 Portal 服务器校验 token 信息。
- Portal 服务器：提供 Web 认证的认证界面和相关操作。Portal 服务器接受认证客户端发出的基于 HTTP 的认证请求，提取其中的账号信息，后台认证后，此认证结果经认证客户端中转给网络设备，网络设备校验完成后再要求认证客户端重定向端 Portal 服务器的相关页面。
- 认证服务器：提供用户认证服务，具体协议由 Portal 服务器和认证服务器协商决定（例如 RADIUS 协议）。

Clearpass 认证主要流程：

1. 拦截与重定向：在用户尝试访问网络资源之前，网络设备（如接入点 AP 等）会拦截所有来自未认证用户的 HTTP 请求，并将请求重定向至 Clearpass 服务器。此步骤确保了用户的浏览器会首先显示认证页面，要求用户进行身份验证。

2. 用户认证交互：在认证页面上，用户输入必要的认证信息，如用户名、口令、校验码等，并提交给 Clearpass 服务器进行处理，判断认证信息是否有效。
3. 认证信息转发：Clearpass 服务器将收集到的用户认证信息转发给设备，设备作为认证流程的发起者，需要此信息进一步验证用户的身份。
4. 设备向 RADIUS 服务器认证：设备接收到认证信息后，会向 RADIUS 服务器发起认证请求，进行身份验证和授权决策。
5. 认证结果反馈：RADIUS 服务器处理完认证请求后，会将认证结果（成功或失败）返回给设备。设备接收到认证结果后，会向终端请求显示认证成功或失败的页面。

- 图 1-11 Clearpass 认证流程



用户下线流程：

- 用户主动下线：用户在使用网络服务过程中，可通过点击页面上提供的“下线”按钮主动申请下线。设备实时监测到这一页面交互动作后，会立即触发下线流程，将用户从活跃会话中移除，实现用户下线。

- 设备端触发的用户下线：设备持续监控用户的网络活动，当检测到用户的流量使用降至预设的低流量阈值以下，或者由于链路断开等原因导致用户实际离线，并持续一段时间（具体依配置参数而定）时，设备会自动判定用户处于非活跃状态，从而触发用户下线流程。下线过程中，设备可能会记录相关日志，以便后续审计或分析。

相关配置

创建配置模板

缺省情况下无配置。

在全局配置模式下，使用 **web-auth template** { **cpweb** | *template-name* **cpweb** }命令创建 Clearpass 模板。

可以使用该配置模板进行 Web 认证功能。

配置服务器 IP 地址

缺省情况下无配置。

在模板配置模式下，使用 **ip** *ip-address* 配置服务器 IP 地址。

访问服务器的请求被设备放行，并且支持对发往服务器的请求进行限速保护。

配置服务器认证 URL

缺省情况下无配置。

在模板配置模式下，使用 **url** *url-string* 进行配置。

用户重定向到的 URL 地址，通常使用 Portal 认证页面地址。

配置认证成功后的响应方式

缺省的响应方式为返回包含成功消息的页面（即 msg 方式）。

在模板配置模式下，使用 **login-success response** { **redirect-init-url** [**default-url** *def-string*] | **msg** *msg-string* | **redirect-url** *url-string* }进行配置。

三种响应方式：

redirect-init-url：重定向回用户最初访问的页面，依赖服务器下发该地址。可以指定默认 url，在服务器不下发 url 时使用。

msg：认证成功后返回包含指定消息的页面。

redirect-url：认证成功后将用户重定向到指定页面。

配置认证失败后的响应方式

缺省的响应方式为重定向到登录页面。

在模板配置模式下，使用 **login-fail response** { **redirect-login-url** | **redirect-url** *url-string* [**errmsg-key** *key-string*] | **msg** *msg-string* }进行配置。

三种响应方式：

redirect-login-url：认证失败后重定向回登录页面。

redirect-url：认证失败后重定向到指定 url，并支持配置错误消息的参数名称。

msg：认证失败后返回包含指定消息的页面。

配置设备解析认证请求的方式

缺省的认证信息参数名称为 username、password、url。

缺省情况下密码未明文，未加密。

在模板配置模式下，使用 **http-method** { **post** | **get** } [**init-url-key** *init-string* **| username-key** *username-string* **| password-key** *password-string* **| password-encrypt** { **none | uam** }]

uam：采用 ascii 方式加密密码。

配置认证成功后是否弹窗主动下线页面

缺省情况下不弹出。

在模板配置模式下，使用 **logout-popup-window** 进行配置。

配置设备 IP

缺省情况下无配置。

在全局配置模式使用 **web-auth auth-server ip** *ip-address* 进行配置。

设置 clearpass 的设备接入服务 ip，用于服务器向此 ip 发起通讯。

配置的设备接入服务 ip 不能够被设置成直通地址。

配置接入服务 ip 为设备 IP 时会导致此认证模板下的终端访问此 ip 时被设备拦截并转发给服务器，从而不能访问设备的 Web 管理界面。

如有此认证模板下的终端直接访问此 ip 对此设备进行管理的需求，可将此接入服务 ip 设置为一个未使用的虚拟服务 ip，如 1.1.1.1，2.2.2.2 等。

一般情况下使用设备的真实 ip 直接登录管理设备无法保证安全性，需要把管理设备的 ip 映射成外网 ip，使用外网 ip 进行管理。由于外网和服务器之间有防火墙等安全设备防护，以保证安全性。而直接通过内网访问则无任何防护，如设备的真实 ip 对用户可见容易使设备直面攻击，因此建议配置为虚拟 ip。

配置设备端口

缺省情况下无配置。

在全局配置模式下，使用 **web-auth auth-server http** [**port** *port-number*]进行配置。

该参数为 clearpass 监听的端口，在认证的时候终端会向此端口发起 http 请求。

配置后设备将开启该端口的监听。

配置终端发起认证的 url

缺省情况下的 url 为 http://ip:port/login。

在全局配置模式下，使用 **web-auth auth-server submit-url** *url-string* 进行配置。

该参数为 clearpass 用户发起认证的 url，必须已 http://开头，不能包含?，具体配置要和 clearpass 上配置的一致。

提交认证信息到该 url 将触发认证请求。

配置启用 AAA 认证

缺省情况下关闭 AAA 认证。

在全局配置模式下，使用 **aaa new-model** 命令来开启 AAA 认证功能。

clearpass 认证功能需要依赖于 AAA 认证功能，使用时需要开启 AAA 功能。

配置 RADIUS 服务器和通信密钥

缺省情况下无配置。

在全局配置模式下，使用 **radius-server host** 命令配置 RADIUS 服务器和通信密钥。

对应于 Web 认证中的 RADIUS 服务器。用于为 Web 认证用户进行身份校验。

配置 AAA 模块 Web 认证的方法列表

缺省情况下无配置。

在全局配置模式下，使用 **aaa authentication cpweb** 命令配置二代 Web 认证的认证方法。

Web 认证功能可以配置使用该方法列表来进行认证交互。

配置 AAA 模块网络记账方法列表

缺省情况下无配置。

在全局配置模式下，使用 **aaa accounting network** 命令配置网络记账方法。

Web 认证功能可以配置使用该方法列表来进行记账交互。

配置 Web 认证使用的 AAA 认证方法列表名

缺省情况下使用 default 方法。

在全局或者无线安全配置模式下，使用 **web-auth authentication cpweb** 命令进行配置。

Web 认证功能通过该方法列表名字向 AAA 功能发起认证请求。

配置 Web 认证使用的 AAA 认证记账列表名

缺省情况下使用 default 方法。

在全局或者无线安全配置模式下，使用 **web-auth accounting cpweb** 命令进行配置。

Web 认证功能通过该方法列表名字向 AAA 功能发起记账请求。

开启 Web 认证

缺省情况下该功能关闭。

在接口模式下，使用 **webauth** 命令开启用户所在端口 Web 认证。

开启认证后端口下未认证用户会被重定向到认证页面。

1.4 配置详解

配置项	配置建议 & 相关命令	
配置一代 Web 认证功能	⚠ 必须配置。用于配置一代 Web 认证功能基本参数	
	web-auth template eportalv1	创建一代 eportalv1 模板
	ip *ip-address*	配置服务器的 IP 地址
	context *ctx-id peer-ip-address*	配置热备服务器 ctx id 和 IP 地址
	url *url-string*	配置服务器的主页地址
	fmt { **ace** | **default** | **custom** }	配置 Portal 服务器 URL 格式
	bindmode { **ip-mac-mode** | **ip-only-mode** }	配置用户绑定模式
	redirect { **http** | **js** }	配置重定向方式
	web-auth portal key [**0** | **1** | **7**] *key-string*	配置服务器通信密钥
	snmp-server community *community-string* **rw**	配置 SNMP 通信团体字
	snmp-server host *ip-address* **inform version 2c** *community-string* **web-auth**	配置 SNMP 通信服务器
	snmp-server enable traps web-auth	开启 Web 认证 trap/inform 通告
	webauth	开启 Web 认证
配置二代 Web 认证功能	⚠ 必须配置。用于配置二代 Web 认证功能基本参数	
	aaa new-model	开启 AAA 功能
	radius-server host *ip-address* [**auth-port** *port-number1*] [**acct-port** *port-number2*] **key** *string*	配置 RADIUS 服务器和密钥
	aaa authentication web-auth { **default** | *list-name* } *method1* [*method2*...]	配置 Web 认证方法列表(使用 RADIUS 认证)
	aaa accounting network { **default** | *list-name* } **start-stop** *method1* [*method2*...]	配置网络记账方法列表(使用 RADIUS 记账)
	web-auth template { **eportalv2** | *portal-name* **v2** }	创建二代认证模板
	ip *ip-address*	配置服务器的 IP 地址
	context *ctx-id peer-ip-address*	配置热备服务器 ctx id 和 IP 地址
	url *url-string*	配置服务器的主页地址
	fmt { **cmcc-ext1** | **cmcc-ext2** | **cmcc-mtx** | **cmcc-normal** | **cmcc-ext3** | **ct-jc** | **cucc** | **default** | **custom** }	配置 Portal 服务器 URL 格式
	bindmode { **ip-mac-mode** | **ip-only-mode** }	配置用户绑定模式
	redirect { **http** | **js** }	配置重定向方式
	web-auth portal key [**0** | **1** | **7**] *key-string*	配置服务器通信密钥

	webauth	开启 Web 认证
配置内置 Portal Web 认证	⚠ 必须配置。用于配置内置 Portal Web 认证功能基本参数	
	aaa new-model	开启 AAA 功能
	radius-server host *ip-address* [**auth-port** *port-number1*] [**acct-port** *port-number2*] **key** *string*	配置 RADIUS 服务器和密钥
	aaa authentication iportal { **default** | *list-name* } *method1* [*method2*...]	配置 Web 认证方法列表(使用 RADIUS 认证)
	aaa accounting network { **default** | *list-name* } **start-stop** *method1* [*method2*...]	配置网络记账方法列表(使用 RADIUS 记账)
	web-auth template iportal	创建内置 Portal Web 认证模板
	login-popup *url-string*	配置用户认证前广告推送 URL
	online-popup *url-string*	配置用户认证成功后广告推送 URL
	page-suit *file-name*	配置定制页面包
	time-interval *hour*	配置内置广告弹出周期
	webauth	开启 Web 认证
配置 MAC 短信认证功能	⚠ 必须配置。用于配置内置 Portal Web 认证功能基本参数	
	aaa new-model	开启 AAA 功能
	radius-server host *ip-address* [**auth-port** *port-number1*] [**acct-port** *port-number2*] **key** *string*	配置 RADIUS 服务器和密钥
	aaa authentication web-auth { **default** | *list-name* } *method1* [*method2*...]	配置 AAA 中 Web 认证方法列表
	aaa accounting network { **default** | *list-name* } **start-stop** *method1* [*method2*...]	配置网络记账方法列表
	web-auth template { **eportalv2** | *portal-name* **v2** }	创建 Portal Web 认证模板
	ip *ip-address*	配置服务器 IP
	url *url-string*	配置服务器 URL
	fmt { **cmcc-ext1** | **cmcc-normal** | **default** }	配置 Portal 服务器 URL 格式
	web-auth portal key [**0** | **1** | **7**] *key-string*	配置服务器加密密钥
	web-auth sms-flow interval *interval* **threshold** *flows*	配置 mac 短信查询周期与阈值
	web-auth bind-portal *string* **type** { **group-spec** | **local-spec** }	配置 MAC 短信认证绑定的服务器
	web-auth winterface *string*	配置重定向 URL 中 winterface 字段参数
	web-auth wlan-ac-ip *ipv4*	配置重定向 URL 中 ACIP 字段参数

配置 WiFiDog 认证功能	必须配置。用于配置 WIFIDOG 认证功能基本参数	
	web-auth template wifidog	创建 Portal Web 认证模板
	ip *ip-address*	配置服务器的 ip 地址
	url *url-string*	配置服务器的 url 链接
	nas-ip *ip-address*	配置接入服务 ip 地址
	web-auth sta-perception enable	配置 WiFiDog 无感知认证功能
	gateway-id *string*	配置 Gateway ID
	web-auth portal wifidog	使用 WiFiDog 模板
	webauth	开启 Web 认证
配置微信连 WiFi 认证功能	必须配置。用于配置微信连 WiFi 认证功能基本参数	
	web-auth template { **wechat** | (*portal-name* **wechat**) }	创建微信连 WiFi 认证模板
	ip *ip-address*	配置服务器的 ip 地址
	service-url *url-string*	配置服务器的 url 链接
	url *url-string*	配置 Portal 服务器的认证页面地址
	key *key-string*	配置服务器的加密密钥
	nas-ip *ip-address*	配置设备 IP
	web-auth sta-perception enable	配置微信连 WiFi 无感知认证功能
	web-auth wechat-escape interval *minutes*	配置开启逃生功能
	web-auth wechat-check interval *minutes*	配置服务器检测功能
	web-auth valid-ip-acct [**timeout** *seconds*]	配置无感知的 ip 校验功能
	web-auth portal wechat	使用 webchat 模板
	webauth	开启 Web 认证
配置 Clearpass 认证功能	必须配置。用于配置微信连 WiFi 认证功能基本参数	
	aaa new-model	开启 AAA 功能
	radius-server host *ip-address* [**auth-port** *port-number1*] [**acct-port** *port-number2*] **key** *string*	配置 RADIUS 服务器和密钥
	aaa authentication cpweb { **default** | *list-name* } *method1* [*method2*...]	配置 Web 认证方法列表(使用 RADIUS 认证)
	aaa accounting network { **default** | *list-name* } **start-stop** *method1* [*method2*...]	配置网络记账方法列表(使用 RADIUS 记账)
	web-auth template cpweb	创建 clearpass 认证模板
	ip *ip-address*	配置服务器的 ip 地址
	context *ctx-id peer-ip-address*	配置热备服务器的 ctx id 和 IP 地址
	url *url-string*	配置服务器的 url 链接

	login-success response { **redirect-init-url** [**default-url** *url-string*] | **msg** *msg-string* | **redirect-url** *url-string* }	配置认证成功后的响应方式
	login-fail response { **redirect-login-url** | **redirect-url** *url-string* [**errmsg-key** *key-string*] | **msg** *msg-string* }	配置认证失败后的响应方式
	http-method { **post** | **get** } [**init-url-key** *init-string* **| username-key** *username-string* **| password-key** *password-string* **| password-encrypt** { **none | uam** }]	配置设备解析认证请求的方式
	logout-popup-window	配置认证成功后是否弹窗主动下线页面
	web-auth auth-server ip *ip-address*	配置设备 IP
	web-auth auth-server http [**port** *port-number*]	配置设备端口
	web-auth auth-server submit-url *url-string*	配置终端发起认证使用的 url
	webauth	启用 Web 认证
配置认证方法列表名	⚠ 可选配置。在 template 模板下指定认证方法列表名，和 AAA 模块的方法列表配置保持一致	
	authentication *method-list*	配置认证方法列表名(仅二代和内置)
配置记账方法列表名	⚠ 可选配置。在 template 模板下指定记账方法列表名，和 AAA 模块的方法列表配置保持一致	
	accounting *method-list*	配置记账方法列表名(仅二代和内置)
配置 Portal 服务器通信端口	⚠ 可选配置。在 template 模板下指定 Portal 服务器通信端口，需要和服务器端的通信端口一致	
	port *port-num*	配置 Portal 服务器通信端口
配置绑定模式	⚠ 可选配置。在 template 模板下指定用户表项绑定模式	
	bindmode { **ip-mac-mode** | **ip-only-mode** }	配置模板表项绑定模式
配置定制页面包	⚠ 选配置。在 template 模板下指定内置 Portal Web 认证使用特定的页面包。	
	page-suite *file-name*	指定内置 Portal 使用特定的页面包
配置广告推送方式	⚠ 可选配置。在 template 模板下配置广告推送方式。	
	login-popup *url-string*	认证前弹出，也是登录的时候弹出的地址
	online-popup *url-string*	认证成功后前弹出的地址
配置定制化 URL 格式	⚠ 可选配置。在 template 模板下配置重定向 URL 格式。	

	fmt custom [**encrypt** { **md5** | **des** | **des_ecb** | **des_ecb3** | **none** }] [**user-ip** *userip-str*] [**user-mac** *usermac-str* **mac-format** [**dot** | **line** | **none** | **5colon**]] [**user-vid** *uservid-str*] [**user-id** *userid-str*] [**nas-ip** *nasip-str*] [**nas-id** *nasid-str*] [**nas-id2** *nasid2-str*] [**ac-name** *acname-str*] [**ap-mac** *apmac-str* **mac-format** [**dot** | **line** | **none]**] [**url** *url-str*] [**ssid** *ssid-str*] [**port** *port-str*] [**ac-serialno** *ac-sno-str*] [**ap-serialno** *ap-sno-str*] [**additional** *extern-str*]	配置重定向 URL 的格式
设置重定向的 HTTP 端口	可选配置。用于指定重定向 TCP 拦截端口，补充拦截环境中的特定端口报文进行重定向	
	http redirect port *port-num*	配置重定向 TCP 拦截端口
设置 Web 认证模块 SYSLOG 功能	可选配置。用于配置 Web 认证 SYSLOG 功能	
	web-auth logging enable	配置 Web 认证 SYSLOG 输出速率
设置未认证用户的最大 HTTP 会话数	可选配置。用于调整 HTTP 会话数限制，对于后台会话数较多的场景需要放宽限制	
	http redirect session-limit *session-num* [**port** *port-session-num*]	配置用户的 HTTP 会话限制数
设置维持重定向连接的超时时间	可选配置。用于修改重定向连接超时时间，在网络环境较差时调大参数有利于完成重定向	
	http redirect timeout *seconds*	用于设置重定向连接超时时间
设置免认证网络资源范围	**http redirect direct-site** { *ipv6-address* | *ipv4-address* [*mask* | **arp** | *port-number*... }	设置免认证网络资源范围
设置直通 ARP 资源范围	可选配置。用于放行指定地址的 ARP，开启 ARP CHECK 时需要放行网关 ARP	
	http redirect direct-arp *ip-address* [*ip-mask*]	用于配置直通 ARP 资源范围
设置无需认证用户范围	可选配置。用于配置特殊用户不用认证就能上网	
	web-auth direct-host { *ipv4-address* [*ip-mask*] [**arp**] [**port** *interface-name*] | *ipv6-address* | *mac-address* | **range** *starip-address endip-address* } [**description** *description-str*] [**group** *group-name*] [**permit-ipv6**]	用于配置免认证用户
设置在线用户信息的更新时间间隔	可选配置。用于配置用户信息的更新周期	
	web-auth update-interval *seconds*	用于配置用户信息更新周期
配置 Portal 检测	可选配置。用于检测 Portal 服务器是否可用，如果不可用，则进行切换，该功能要结合主备 Portal 使用。	

	web-auth portal-check [**interval** *intsec* [**timeout** *tosec*] [**retransmit** retries]	配置 Portal 检测的周期、超时时间、超时重传次数
	web-auth ping [**interval** *minutes*] [**retry** *times*]	配置 ping 检测的周期和超时重传次数
配置 Portal 逃生	⚠ 可选配置。配置当 Portal 服务器不可用时，新接入用户免认证。	
	web-auth portal-escape [**nokick**]	配置 Portal 不可用时新接入用户免认证。
配置 DHCP 地址核查	⚠ 可选配置。用于检测认证用户的 ip 地址是否是 DHCP 服务器分配的，如果不是则拒绝认证请求。	
	web-auth dhcp-check	检测终端的 ip 地址是否是 DHCP 服务器分配
配置关闭链路检测	⚠ 可选配置。用于防抖，用户断开链路时，可以保证 Web 认证表项不删除，当用户再次接入时则无需认证即可继续上网。	
	no web-auth sta-leave detection	配置关闭链路检测
配置关闭 Portal 协议扩展	⚠ 可选配置。对接锐捷 Portal 服务器软件时需要开启扩展，对接标准中国移动 Portal 服务器，需要关闭扩展。	
	no web-auth portal extension	配置关闭 Portal 协议扩展
配置黑白名单	⚠ 可选配置。配置黑名单表示某些网络资源认证通过也不可访问，配置白名单表示某些资源不用认证也可以访问。	
	web-auth acl { **black-ip** *ip* | **black-port** *port* | **black-url** *name* | **white-url** *name* }	配置黑白名单
配置防抖动计费	⚠ 可选配置。配置防抖时间是否算入在线时长，提高计费精度。具体的防抖时间则需要参考具体产品的防抖功能的设置情况。	
	web-auth accounting jitter-off	配置防抖时间是否算入在线时长
配置 Portal 通信端口	⚠ 可选配置。配置后设备与 Portal 服务器通信的源端口为所配置端口。	
	ip portal source-interface *interface-type interface-num*	指定设备与 Portal 服务器的通信接口
配置宁盾系统兼容 URL	⚠ 可选配置。配置 Web 重定向 URL 支持宁盾系统。	
	web-auth dkey-compatible url-parameter *string*	配置 URL 兼容宁盾系统。
配置多 Portal 映射	⚠ 可选配置。配置不同网段用户使用不同 Portal 进行认证。	
	web-auth portal { **eportalv1** | **eportalv2** | **iportal** | **wifidog** | **wechat** | **cpweb** | *name* } **ip-mapping** *ipv4 mask*	配置不同网段用户使用不同 Portal 进行认证
配置内置 Web 认证 NAT 功能	⚠ 可选配置。配置内置 Web 认证支持 NAT。	

	iportal nat enable	支持内置 Web 认证 NAT
配置内置 Web 认证重传次数	可选配置。配置内置 Web 认证 http 连接重传次数。	
	iportal retransmit *count*	配置内置 Web 认证 http 连接重传次数
配置内置 Web 认证服务选择	可选配置。配置内置 Web 认证使用的服务类型。	
	iportal service [**internet** *internet-name*] [**local** *local-name*]	配置内置 Web 认证使用的服务类型
配置内置 Web 认证用户 UA 字段	可选配置。配置用户的 UA 字段对应的终端名称。	
	iportal user-agent *ua-name* **type mobile** *ua-string*	配置用户的 UA 字段对应的终端名称
配置内置 Web 认证导入页面包	**web-auth import-page-suite tftp:***path*	配置内置 Web 认证导入页面包
配置 Web 记账方法列表	可选配置。在全局配置模式下，配置 Web 认证的记账方法。	
	web-auth accounting { **v2** | **intra** | **cpweb** } { **default** | *name* }	在全局配置模式下，配置 Web 认证的记账方法
配置 Web 认证方法列表	可选配置。在全局配置模式下，配置 Web 认证方法。	
	web-auth authentication { **v2** | **intra** | **cpweb** } { **default** | *name* }	在全局配置模式下，配置 Web 认证方法
配置 RADIUS 逃生功能开关	可选配置。	
	web-auth radius-escape	配置 RADIUS 服务器逃生开关
配置内置 logo 替换功能	**web customized-logo enable**	配置开启内置 Portal 的 logo 替换功能
配置无线 Web 认证降噪功能	**web-auth noise** [**aging** *agmin*] [**hit** *times*]	配置无线 Web 认证降噪策略
配置微信认证 IOS 自动弹框控制命令	**http redirect adapter ios**	配置微信认证 IOS 自动弹框控制命令
配置微信认证无感知命令	**web-auth sta-perception enable**	开启微信认证无感知功能
配置 ipfix 上传流量开关	**web-auth acct-mtehod ipfix**	配置 ipfix 上传流量开关
配置 Portal 协议 0x05 号属性透传功能	可选配置。用于配置 Portal 协议 0x05 号属性透传功能	
	web-auth portal-attribute [**5** | **textinfo**]	用于配置 Portal 协议 0x05 号属性透传功能
配置 Portal 认证账号唯一性检查功能	可选配置。用于配置 Portal 认证账号唯一性检查功能	
	web-auth portal-valid unique-name	用于配置 Portal 证账号唯一性检查功能
配置无线 WiFiDog 一键配置	可选配置。用于无线 WiFiDog 一键配置	

	web-auth wifidog-template wlan-range portal-ip nas-ip url [**perception**]	无线 WiFiDog 一键配置
配置无线微信连 WiFi 一键配置	⚠ 可选配置。用于无线 wechat 一键配置	
	web-auth wechat-template wlan-range portal-ip nas-ip [**ios-adapter** | **perception**]	无线微信连 WiFi 一键配置
配置 AP 的 NAS-PORT-ID	**nas-port-id** *string*	配置 AP 的 NAS-PORT-ID
配置认证用户名自动添加域信息功能	**domain** *domain-string*	配置认证用户名自动添加域信息
配置 app 认证模板	**web-auth template** { **app |** *portal-name* **app** }	创建 APP 认证模板
	web-auth portal { **app** | *name* }	应用 APP 认证模板
配置 ISE 认证功能	⚠ 必需配置。用于 ISE 认证的参数配置	
	aaa new-model	开启 AAA 功能
	aaa authentication cpweb { **default** | *list-name* } *method1* [*method2*...]	配置 AAA 中 Web 认证方法列表（使用 Clearpass 认证）
	web-auth template cpweb	创建模板（使用 Clearpass 认证）
	ip *ip-address*	配置 ISE 服务器 IP
	url *url-string*	配置 ISE 服务器 URL
	web-auth auth-server ip *ip-address*	设置 ISE 认证的设备接入服务 ip
	web-auth auth-server http [**port** *port-number*]	配置 ISE 认证终端发起认证时使用的 tcp 端口
	web-auth auth-server submit-url *url-string*	配置 ISE 认证终端发起认证时使用的 url 地址
	webauth	配置接口上启用 Web 认证
配置角色重定向模板	**web-auth template** *template-name* **rdweb**	创建模板
	ip *ip-address*	配置服务器 IP
	url *url-string*	配置服务器 URL
配置认证成功默认角色	**web-auth default-role**	配置 Web 认证成功后终端默认角色
配置二代认证支持直接访问	⚠ 可选配置。配置二代认证支持直接访问认证页面进行用户认证	

认证页面进行认证	**web-auth portal direct-auth**	配置二代认证支持直接访问认证页面进行用户认证
配置 SSL 证书导入和使能	**web-auth import-ssl** [**auth-server**] { **cert ftp:***path* | **cert tftp:***path* } { **key ftp:***path* | **key tftp:***path* }	配置 SSL 证书导入
	web-auth ssl-policy { **https-redirect** | **auth-server** }	启用 SSL 证书
配置用户轨迹数量	**web-auth user-diag** { **user-num** *user-num* | **log-num** *log-num* }	配置可记录的用户及轨迹数量

1.4.1 配置一代 Web 认证功能

配置效果

未认证用户能够被重定向到认证页面并完成认证。

注意事项

无

配置方法

配置 Portal 服务器

- 必须配置，要成功应用 Web 认证功能，必须设置并应用 Portal 服务器。
- 当接入/汇聚设备发现未认证用户试图通过 HTTP 访问网络资源时，设备将用户的访问请求重定向到指定的 Portal 认证页面，通过认证页面，引导用户向认证服务器发起认证。Portal 服务器地址将被设置为一个特殊的免认证的网络资源，未认证用户才可以直接与该地址进行 HTTP 通讯。

配置设备与认证服务器之间的通信密钥

- 必须配置，要成功应用 Web 认证功能，必须设置接入/汇聚设备与认证服务器进行通信的密钥。
- 当设备发现未认证用户在访问网络资源时，设备将通过重定向功能，向用户弹出认证页面，通过认证页面，引导用户向认证服务器发起认证。在认证过程中，设备与认证服务器间通过密钥对部分数据进行加密，以加强安全性。

设置设备与认证服务器之间的 SNMP 网管参数

- 必须配置，要成功应用 Web 认证功能，必须设置设备与认证服务器之间的 SNMP 网管通信参数。

- 接入/汇聚设备和认证服务器之间通过 SNMP/MIB 对认证用户进行管理，在设备上，使用 MIB 来管理认证用户表，认证服务器通过访问该 MIB，可以获取用户相关的统计信息，以及进行控制用户的上线、下线的操作。当用户下线时，设备将发送 SNMP-Inform 消息给认证服务器。

在端口上开启 Web 认证功能

- 必须配置。
- 当 Web 认证功能基于端口开启时，默认情况下，端口未开启 Web 认证功能，此时该端口下所连接的用户不进行 Web 认证。

检验方法

- 未认证用户被要求认证
- 已认证用户可以正常使用网络

相关命令

创建模板

【命令格式】 **web-auth template eportalv1**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 eportalv1 为默认的一代 Web 认证模板

配置服务器 IP

【命令格式】 **ip** *ip-address*
【参数说明】 *ip-address*：Portal 服务器的地址
【命令模式】 Web 认证模板配置模式
【使用指导】 -

配置热备服务器 ctx id 和 IP 地址

【命令格式】 **context** *ctx-id peer-ip-address*
【参数说明】 *ctx-id*：配置热备服务器对应的 context id
peer-id-address：热备（备机）的 IP 地址
【命令模式】 Web 认证模板配置模式
【使用指导】 -

配置服务器 URL

【命令格式】 **url** *url-string*
【参数说明】 *url-string*：Portal 服务器的认证页面地址
【命令模式】 Web 认证模板配置模式
【使用指导】 以 http://或 https://开头

配置 Portal 服务器 URL 格式

【命令格式】 **fmt** { **ace** | **default** | **custom** }
【参数说明】 Portal 服务器的 url 格式
【命令模式】 Web 认证模板配置模式
【使用指导】 fmt 参数为 ace 时，支持 ACE 联动。

配置用户绑定模式

【命令格式】 **bindmode** { **ip-mac-mode | ip-only-mode** }
【参数说明】 用户的绑定模式
【命令模式】 Web 认证模板配置模式
【使用指导】 -

配置重定向方式

【命令格式】 **redirect** { **http** | **js** }
【参数说明】 重定向报文的封装格式
【命令模式】 Web 认证模板配置模式
【使用指导】 某些 app 无法执行 javascript 脚本动作时，需要配置成 http 封装格式触发重定向

配置服务器加密密钥

【命令格式】 **web-auth portal key** [**0** | **1** | **7**] *key-string*
【参数说明】 **0**：配置服务器密钥加密类型为不加密，即以明文输入，以明文保存与显示
1：配置服务器密钥加密类型为密文保存，即以明文输入，以密文保存与显示
7：配置服务器密钥加密类型为完全密文，即以密文输入，以密文保存与显示
key-string：Portal 服务器的加密密钥，配置设备与认证服务器进行通信的密钥；密钥最大长度为 255 个字符。
【命令模式】 全局配置模式
【使用指导】 -

配置服务器 SNMP 通信团体字

【命令格式】 **snmp-server community** *community-string* **rw**
【参数说明】 *community-string*：Community 字符串
rw：由于需要对 MIB 进行 Set 操作，因此需要设置成 RW，支持读写操作
【命令模式】 全局配置模式
【使用指导】 设置 SNMP Community，认证服务器可以使用该 Community 管理接入/汇聚设备上的在线用户。

配置服务器 SNMP 通信服务器

【命令格式】 **snmp-server host** *ip-address* **inform version 2c** *community-string* **web-auth**
【参数说明】 *ip-address*：目的主机地址，即认证服务器的地址
community-string：通信团体字，发送 SNMP-Inform 消息使用的 Community 字符串
【命令模式】 全局配置模式
【使用指导】 设置发送 Web 认证消息的目的主机，类型、版本、Community 等参数。
inform：设置发送 SNMP-Inform 类型的消息。用于接入/汇聚设备在用户下线的时候向认证服务器发送消息，

为了防止消息丢失，所以采用 SNMP-Inform 而不是 SNMP-Trap。

version 2c：SNMPv2 以后的版本才支持 SNMP-Inform 类型，因此此处不能设置为 SNMPv1。

web-auth：指明发送 Web 认证消息采用上述的参数。

SNMP 的配置命令和其他具体内容参见“SNMP 配置指南”中的相关章节。

此处列出的 SNMP 通信参数是以 SNMPv2 的设置为例的，如果要求设备和认证服务器之间的 SNMP 网管通信有更高的安全性，可以考虑采用 SNMPv3。这样，SNMP Community 的设置需要改为 SNMP User，并且 SNMP-Inform 的版本也需要改为 SNMPv3 版本的，另外还需要设置和 SNMPv3 相关的安全参数，具体参见“SNMP 配置”中相关的章节，此处不再进行详细介绍。

配置开启 Web 认证 trap/inform 通告

【命令格式】 **snmp-server enable traps web-auth**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 设置接入/汇聚设备允许向外发送 Web 认证的消息，消息类型包括 Trap 和 Inform。

web-auth：即 Web 认证的消息。

启用 Web 认证

【命令格式】 **webauth**

【参数说明】 -

【命令模式】 无线安全配置模式

【使用指导】 -

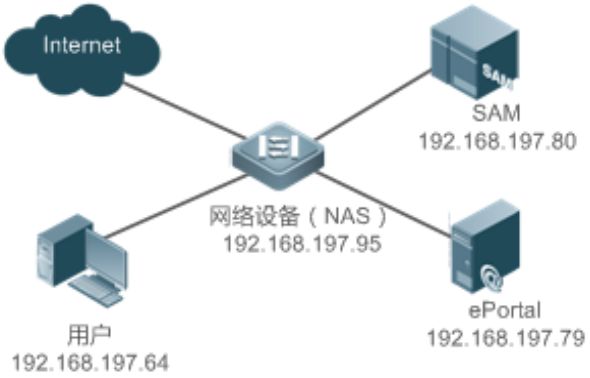
配置举例

以下配置举例，仅介绍与 Web 认证相关的配置。

一代 Web 认证

【网络环境】

图 1-12



【配置方法】

- 在网络设备上设置认证服务器的 IP 地址及与认证服务器进行通信的密钥(webkey)

- 在网络设备上设置认证页面的主页地址
- 设置网络设备与认证服务器之间的 SNMP 网管参数(团体字 public)
- 在 WLAN 上开启 Web 认证功能

```
Hostname# config
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)# web-auth template eportalv1
Hostname(config.tmplt.eportalv1)# ip 192.168.197.79
Hostname(config.tmplt.eportalv1)# exit
Hostname(config)# web-auth portal key webkey
```

```
Hostname(config)# web-auth template eportalv1
Hostname(config.tmplt.eportalv1)# url http://192.168.197.79:8080/eportal/index.jsp
Hostname(config.tmplt.eportalv1)# exit
```

```
Hostname(config)# snmp-server community public rw
Hostname(config)# snmp-server enable traps web-auth
Hostname(config)# snmp-server host 192.168.197.79 inform version 2c public web-auth
Hostname(config)# exit
```

```
Hostname(config)# wlansec 1
Hostname(config-wlansec)# web-auth portal eportalv1
Hostname(config-wlansec)# webauth
```

【检验方法】

- Web 认证配置是否成功

```
Hostname(config)# show running-config
…
snmp-server host 192.168.197.79 inform version 2c public web-auth
snmp-server enable traps web-auth
snmp-server community public rw
…
web-auth template eportalv1
 ip 192.168.197.79
 url http://192.168.197.79:8080/eportal/index.jsp
!
web-auth portal key webkey
…
wlansec 1
 web-auth portal eportalv1
 webauth
```

常见错误

- Portal 服务器和设备间的 SNMP 参数配置不正确导致用户无法认证上线。
- 跨三层部署 Web 认证，模板中的绑定模式需要选择 ip-only-mode。
- 和 vrrp 一起使用的时候，需要通过 snmp-server trap-source ip 命令指定 vrrp 地址，否则 Portal 服务器无法正确处理 trap 报文。

1.4.2 配置二代 Web 认证功能

配置效果

未认证用户能够被重定向到认证页面并完成认证。

注意事项

- 二代 Web 认证支持中国移动 Portal 规范，同时做了扩展以支持锐捷 Portal 服务器，实际部署时需要根据服务器情做相关兼容性配置，具体参考后续章节的说明。
- 在配置二代 Web 认证的 Portal 服务器的 URL 时，如果 URL 中带有 IPv6 地址，需要将 ipv6 地址用中括号包含起来。例如：配置 IPv6 地址为 2001::1 时，实际配置应该为 url http://[2001::1]/index.jsp。同时 ipv6 的模板下不支持 fmt 配置。
- fmt 参数为 cmcc-normal 和 cmcc-ext1 时，其中 IP 仅支持 IPv4 形式。

配置方法

配置开启 AAA 认证

- 必须配置，要使用二代 Web 认证功能，必须开启 AAA 认证。
- 二代 Web 认证向服务器发起认证的功能由设备完成，在设备 AAA 功能实现。

配置 RADIUS 服务器和密钥

- 必须配置，要成功应用二代 Web 认证功能，必须设置 RADIUS 服务器。
- 用户账户信息保存在 RADIUS 服务器上，设备需要连接 RADIUS 服务器来确认用户身份合法性。

配置 AAA 中 Web 认证方法

- 必须配置，要成功应用二代 Web 认证功能，必须设置 AAA 认证方法。
- 认证方法列表将 Web 认证的请求和 RADIUS 服务器关联起来，设备依据认证方法列表来选择认证方式和对应的服务器。

配置 AAA 网络记账方法

- 必须配置，要成功应用二代 Web 认证功能，必须设置 AAA 网络记账方法。
- 记账方法用于关联对应的记账方式和服务器，Web 认证需要记账功能记录用户信息或费用。

配置 Portal 服务器

- 必须配置，要成功应用二代 Web 认证功能，必须设置并应用 Portal 服务器。
- 当接入/汇聚设备发现未认证用户试图通过 HTTP 访问网络资源时，设备将用户的访问请求重定向到指定的 Portal 认证页面，通过认证页面，引导用户向认证服务器发起认证。Portal 服务器地址将被设置为一个特殊的免认证的网络资源，未认证用户才可以直接与该地址进行 HTTP 通讯。

配置设备与认证服务器之间的通信密钥

- 必须配置，要成功应用二代 Web 认证功能，必须设置接入/汇聚设备与认证服务器进行通信的密钥。
- 当设备发现未认证用户在访问网络资源时，设备将通过重定向功能，向用户弹出认证页面，通过认证页面，引导用户向认证服务器发起认证。在认证过程中，设备与认证服务器间通过密钥对部分数据进行加密，以加强安全性。

设置全局/接口上使用的 Portal 服务器

- 二代认证必须配置，要成功应用二代 Web 认证功能，必须在全局/接口上指定使用二代 portal。
- 设备会优先选择所在接口配置的 Portal 服务器，如果所在接口不存在 Portal 服务器配置，设备会选择全局配置的 Portal 服务器，全局不存在配置时默认使用 eportalv1。设备将用户重定向到所选择的 Portal 服务器。

在端口上开启 Web 认证功能

- 必须配置。
- 当 Web 认证功能基于端口开启时，默认情况下，端口未开启 Web 认证功能，此时该端口下所连接的用户不进行 Web 认证。

检验方法

- 未认证用户被要求认证
- 已认证用户可以正常使用网络

相关命令

开启 AAA 功能

【命令格式】 **aaa new-model**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 AAA 的方法列表等命令需要在功能开启后才能输入

配置 RADIUS 服务器和密钥

【命令格式】 **radius-server host** *ip-address* [**auth-port** *port-number1*] [**acct-port** *port-number 2*] **key** *string*
【参数说明】 *ip-address*：服务器 IP 地址
port-number1：认证端口号
port-number2：记账端口号
string：密钥字符串

【命令模式】 全局配置模式

【使用指导】 认证端口默认 1812，记账端口默认 1813

配置 AAA 中 Web 认证方法列表

【命令格式】 **aaa authentication web-auth** { **default** | *list-name* } *method1* [*method2*...]

【参数说明】 *list-name*：方法列表名

method1：方法 1

method2：方法 2

【命令模式】 全局配置模式

【使用指导】 二代 Web 认证通常使用 RADIUS 认证方法

配置网络记账方法列表

【命令格式】 **aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]

【参数说明】 *list-name*：方法列表名

method1：方法 1

method2：方法 2

【命令模式】 全局配置模式

【使用指导】 二代 Web 认证通常使用 RADIUS 记账方法

创建模板

【命令格式】 **web-auth template** { **eportalv2** | *portal-name* **v2** }

【参数说明】 *portal-name*：自定义的 Portal 服务器名

【命令模式】 全局配置模式

【使用指导】 eportalv2 为默认的二代 Web 认证模板

配置服务器 IP

【命令格式】 **ip** { *ip-address* | *ipv6-address* }

【参数说明】 *ip-address/ ipv6-address*：Portal 服务器的地址

【命令模式】 Web 认证模板配置模式

【使用指导】 -

配置热备服务器 ctx id 和 IP 地址

【命令格式】 **context** *ctx-id peer-ip-address*

【参数说明】 *ctx-id*：配置热备服务器对应的 context id

peer-id-address：热备（备机）的 IP 地址

【命令模式】 Web 认证模板配置模式

【使用指导】 -

配置服务器 URL

【命令格式】 **url** *url-string*

【参数说明】 *url-string*：Portal 服务器的认证页面地址

【命令模式】 Web 认证模板配置模式
【使用指导】 以 http://或 https://开头

配置 Portal 服务器 URL 格式

【命令格式】 **fmt** { **cmcc-ext1** | **cmcc-ext2** | **cmcc-mtx** | **cmcc-normal** | **cmcc-ext3** | **ct-jc** | **cucc** | **default** | **custom** }
【参数说明】 Portal 服务器的 url 格式
【命令模式】 Web 认证模板配置模式
【使用指导】 fmt 参数为 cmcc-normal 和 cmcc-ext1 时，其中 IP 仅支持 IPv4 形式。
fmt 默认为 default 格式。
fmt 参数为 custom 时，定制化格式。
fmt 参数为 cmcc-ext2，支持辽宁移动 portal 格式。
fmt 参数为 cmcc- ext3 时，支持宁波/嘉兴移动 AC 厂商 URL 格式。
fmt 参数为 cmcc-mtx 时，支持移动 AC 厂商 URL 格式。
fmt 参数为 ct-jc 时，支持电信集采 URL 格式。
fmt 参数为 cucc 时，支持山东联通 portal 格式。

配置用户绑定模式

【命令格式】 **bindmode** { **ip-mac-mode** | **ip-only-mode** }
【参数说明】 用户的绑定模式
【命令模式】 Web 认证模板配置模式
【使用指导】 -

配置重定向方式

【命令格式】 **redirect** { **http** | **js** }
【参数说明】 重定向报文的封装格式
【命令模式】 Web 认证模板配置模式
【使用指导】 某些 app 无法执行 javascript 脚本动作时，需要配置成 http 封装格式触发重定向

配置服务器加密密钥

【命令格式】 **web-auth portal key** [**0** | **1** | **7**] *key-string*
【参数说明】 **0**：配置服务器密钥加密类型为不加密，即以明文输入，以明文保存与显示
1：配置服务器密钥加密类型为密文保存，即以明文输入，以密文保存与显示
7：配置服务器密钥加密类型为完全密文，即以密文输入，以密文保存与显示
key-string：Portal 服务器的加密密钥。配置设备与认证服务器进行通信的密钥；密钥最大长度为 255 个字符。
【命令模式】 全局配置模式
【使用指导】 -

配置启用 Web 认证

【命令格式】 **webauth**
【参数说明】 无
【命令模式】 WLAN 安全配置模式

【使用指导】 -

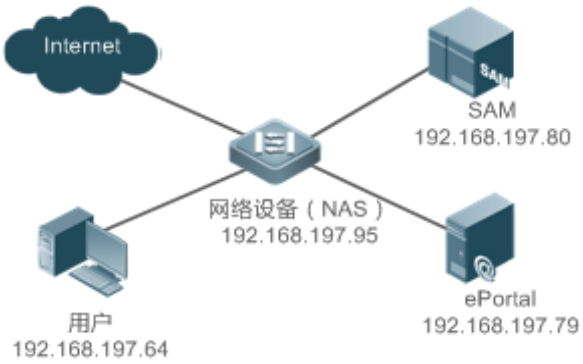
配置举例

以下配置举例，仅介绍与 Web 认证相关的配置。

二代 Web 认证

【网络环境】

图 1-13



【配置方法】

- 在网络设备上开启 AAA
- 在网络设备配置 RADIUS 服务器和密钥
- 在网络设备配置 AAA 的 Web 认证默认方法列表和默认网络记账方法列表
- 在网络入设备上设置认证服务器的 IP 地址及与认证服务器进行通信的密钥(webkey)
- 在网络设备上设置认证页面的主页地址
- 在网络设备上配置全局使用二代 portal 进行认证
- 在 WLAN 上开启 Web 认证功能

```
Hostname# configureterminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)# aaa new-model
```

```
Hostname(config)# radius-server host 192.168.197.79 key webkey
```

```
Hostname(config)# aaa authentication web-auth default group radius
Hostname(config)# aaa accounting network default start-stop group radius
```

```
Hostname(config)# web-auth template eportalv2
Hostname(config.tmplt.eportalv2)# ip 192.168.197.79
Hostname(config.tmplt.eportalv2)# exit
Hostname(config)# web-auth portal key webkey
```

```
Hostname(config)# web-auth template eportalv2
Hostname(config.tmplt.eportalv2)# url http://192.168.197.79:8080/eportal/index.jsp
Hostname(config.tmplt.eportalv2)# exit
```

```
Hostname(config)# wlansec 1
Hostname(config-wlansec)# web-auth portal eportalv2
Hostname(config-wlansec)# webauth
Hostname(config-wlansec)# exit
```

【检验方法】

- Web 认证配置是否成功

```
Hostname(config)# show running-config
…
aaa new-model
aaa authentication web-auth default group radius
aaa accounting network default start-stop group radius
…
radius-server host 192.168.197.79 key webkey
…
web-auth template eportalv2
 ip 192.168.197.79
 url http://192.168.197.79:8080/eportal/index.jsp
!
web-auth portal key webkey
!
wlansec 1
 web-auth portal eportalv2
 webauth
```

```
Hostname# show web-auth control
 Port                      Control  Server Name           Online User Count
 ------------------------- -------- --------------------- -----------------
 wlansec 1                 On       eportalv2             0
```

```
Hostname#show web-auth template
Webauth Template Settings:
-------------------------------------------------------------
  Name:           eportalv2
  BindMode:       ip-mac-mode
  Type:           v2
  Port:           50100
  Ip:             192.168.197.79
  Url:            http://192.168.197.79:8080/eportal/index.jsp
  Wechat enable:   0
  Temporary permit:0
```

常见错误

- Portal 服务器和设备间的 key 配置错误或者有一方配置了加密，一方未配置导致认证异常
- RADIUS 服务器和设备间参数配置不正确导致认证异常
- Portal 服务器不支持中国移动 Portal 协议规范导致无法对接

1.4.3 配置内置 Portal Web 认证

配置效果

未认证用户能够被重定向到认证页面并完成认证，无需外置 Portal 服务器。

注意事项

- 部分设备，比如 AP110 并没有内置页面包，使用前需要先导入页面包，具体产品对页面包的支持情况，请参考具体产品的说明。
- 如果要使用自定义页面包，必须严格按照定制规范章节给出的说明实现。

配置方法

↘ 配置开启 AAA 认证

- 必须配置，要使用二代 Web 认证功能，必须开启 AAA 认证。
- 内置 Portal Web 认证向服务器发起认证的功能由设备完成，在设备 AAA 功能实现。

↘ 配置 RADIUS 服务器和密钥

- 必须配置，要成功内置 Portal Web 认证功能，必须设置 RADIUS 服务器。
- 用户账户信息保存在 RADIUS 服务器上，设备需要连接 RADIUS 服务器来确认用户身份合法性。

↘ 配置 AAA 中 Web 认证方法

- 必须配置，要成功应用内置 Portal Web 认证功能，必须设置 AAA 认证方法。
- 认证方法列表将 Web 认证的请求和 RADIUS 服务器关联起来，设备依据认证方法列表来选择认证方式和对应的服务器。

↘ 配置 AAA 网络记账方法

- 可选配置，部分服务器要求认证和记账必须同时开启，因此是否配置记账要根据服务器特性决定。
- 记账方法用于关联对应的记账方式和服务器，Web 认证需要记账功能记录用户信息或费用。

↘ 配置内置 iportal 模板

- 必须创建 iportal 模板。
- 如果之前创建的认证、计费方法不是 default，则需要在模板中配置对应名字，否则默认使用 default。

在全局或者端口上开启 Web 认证功能

- 必须配置。

检验方法

- 未认证用户被要求认证，弹出页面为内置页面包中的对应页面文件。
- 已认证用户可以正常使用网络。

相关命令

开启 AAA 功能

【命令格式】 **aaa new-model**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 AAA 的方法列表等命令需要在功能开启后才能输入

配置 RADIUS 服务器和密钥

【命令格式】 **radius-server host** *ip-address* [**auth-port** *port-number1*] [**acct-port** *port-number 2*] **key** *string*
【参数说明】 *ip-address*：服务器 IP 地址
port-number1：认证端口号
port-number2：记账端口号
string：密钥字符串
【命令模式】 全局配置模式
【使用指导】 认证端口默认 1812，记账端口默认 1813

配置 AAA 中 Web 认证方法列表

【命令格式】 **aaa authentication iportal** { **default** | *list-name* } *method1* [*method2*...]
【参数说明】 *list-name*：方法列表名
method1：方法 1
method2：方法 2
【命令模式】 全局配置模式
【使用指导】 方法名需要和 AAA 的配置一致

配置网络记账方法列表

【命令格式】 **aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
【参数说明】 *list-name*：方法列表名
method1：方法 1

method2：方法 2

【命令模式】 全局配置模式

【使用指导】 方法名需要和 AAA 的配置一致

创建模板

【命令格式】 **web-auth template iportal**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 -

配置用户认证前广告推送 URL

【命令格式】 **login-popup** *url-string*

【参数说明】 推送广告的地址

【命令模式】 Web 认证模板配置模式

【使用指导】 以 http://或 https://开头

配置用户认证成功后广告推送 URL

【命令格式】 **online-popup** url-string

【参数说明】 推送广告的地址

【命令模式】 Web 认证模板配置模式

【使用指导】 以 http://或 https://开头

配置定制页面包

【命令格式】 **page-suit** *file-name*

【参数说明】 指定页面包的文件名

【命令模式】 Web 认证模板配置模式

【使用指导】 -

配置内置广告弹出周期

【命令格式】 **time-interval** *hour*

【参数说明】 广告弹出周期

【命令模式】 Web 认证模板配置模式

【使用指导】 -

启用 Web 认证

【命令格式】 **webauth**

【参数说明】

【命令模式】 全居配置模式

【使用指导】 -

配置举例

以下配置举例，仅介绍与 Web 认证相关的配置。

内置 Portal Web 认证

【配置方法】

- 在网络设备上开启 AAA
- 在网络设备配置 RADIUS 服务器和密钥
- 在网络设备配置 AAA 的 Web 认证默认方法列表和默认网络记账方法列表
- 在网络设备上配置全局使用内置 Portal 进行认证
- 在 WLAN 上开启 Web 认证功能

```
Hostname# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)# aaa new-model
Hostname(config)# radius-server host 192.168.197.79 key Hostname
Hostname(config)# aaa authentication iportal default group radius
Hostname(config)# aaa accounting network default start-stop group radius
Hostname(config)# web-auth template iportal
Hostname(config.tmplt.iportal)# exit
Hostname(config.tmplt.iportal)# accounting default
Hostname(config.tmplt.iportal)# authentication default
Hostname(config.tmplt.iportal)# page-suite default
Hostname(config.tmplt.iportal)# exit
Hostname(config)# wlansec 1
Hostname(config-wlansec)# web-auth portal iportal
Hostnameconfig-wlansec)# webauth
```

【检验方法】

- Web 认证配置是否成功

```
Hostname(config)# show running-config
…
aaa new-model
aaa authentication web-auth default group radius
aaa accounting network default start-stop group radius
…
radius-server host 192.168.197.79 key Hostname
…
web-auth template iportal
page-suite default
 authentication default
 accounting default
!
…
wlansec 1
```

```
web-auth portal iportal

webauth
```

```
Hostname# show web-auth control
 Port                       Control  Server Name           Online User Count
 -------------------------- -------- --------------------- -----------------
wlansec 1                  On       iportal               0...
```

```
Hostname#show web-auth template
Webauth Template Settings:
-------------------------------------------------------------

 Name:           iportal

 BindMode:       ip-mac-mode

 Type:           intra

 Port:           8081

 time_interval:  1

 Login_popup:    (null)

 Online_popup:   (null)

 Suitename:      default

 Authentication: default

 Accounting:     default
```

常见错误

- 定制新页面包时未按定制规范制作
- 指定了定制页面包但是页面包未下载到 FLASH 或者未下载到指定目录

1.4.4 配置 MAC 短信认证功能

配置效果

未认证用户关联到 WLAN 后，允许使用网络，但用户在指定周期内使用了指定阈值的流量时，认证设备向绑定 Portal 服务器发起 MAC 绑定查询。如果用户为已绑定状态，绑定 Portal 发起认证请求，用户进行认证；如果用户为未绑定状态，用户需要通过 Portal 认证来接入网络。

注意事项

- 创建的 Portal 服务器 URL 必须是 cmcc-ext1 格式。

配置方法

开启 AAA 功能

- 必须配置，要使用二代 Web 认证功能，必须开启 AAA 认证。
- 二代 Web 认证向服务器发起认证的功能由设备完成，在设备 AAA 功能实现。

【命令格式】 **aaa new-model**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 AAA 的方法列表等命令需要在功能开启后才能输入

配置 RADIUS 服务器和密钥

- 必须配置，要成功应用二代 Web 认证功能，必须设置 RADIUS 服务器。
- 用户账户信息保存在 RADIUS 服务器上，设备需要连接 RADIUS 服务器来确认用户身份合法性。

【命令格式】 **radius-server host** *ip-address* [**auth-port** *port-number1*] [**acct-port** *port-number 2*] **key** *string*
【参数说明】 *ip-address*：服务器 IP 地址
port-number1：认证端口号
port-number2：记账端口号
string：密钥字符串
【命令模式】 全局配置模式
【使用指导】 认证端口默认 1812，记账端口默认 1813

配置 AAA 中 Web 认证方法列表

- 必须配置，要成功应用二代 Web 认证功能，必须设置 AAA 认证方法。
- 认证方法列表将 Web 认证的请求和 RADIUS 服务器关联起来，设备依据认证方法列表来选择认证方式和对应的服务器。

【命令格式】 **aaa authentication web-auth** { **default** | *list-name* } *method1* [*method2*...]
【参数说明】 *list-name*：方法列表名
method1：方法 1
method2：方法 2
【命令模式】 全局配置模式
【使用指导】 二代 Web 认证通常使用 RADIUS 认证方法

配置网络记账方法列表

- 必须配置，要成功应用二代 Web 认证功能，必须设置 AAA 网络记账方法。
- 记账方法用于关联对应的记账方式和服务器，Web 认证需要记账功能记录用户信息或费用。

【命令格式】 **aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
【参数说明】 *list-name*：方法列表名
method1：方法 1
method2：方法 2

【命令模式】 全局配置模式

【使用指导】 二代 Web 认证通常使用 RADIUS 记账方法

创建模板

- 必须配置，要成功应用二代 Web 认证功能，必须设置并应用 Portal 服务器。
- 当接入/汇聚设备发现未认证用户试图通过 HTTP 访问网络资源时，设备将用户的访问请求重定向到指定的 Portal 认证页面，通过认证页面，引导用户向认证服务器发起认证。Portal 服务器地址将被设置为一个特殊的免认证的网络资源，未认证用户才可以直接与该地址进行 HTTP 通讯。

【命令格式】 **web-auth template** { **eportalv2** | *portal-name* **v2** }

【参数说明】 自定义的 Portal 服务器名

【命令模式】 全局配置模式

【使用指导】 eportalv2 为默认的二代 Web 认证模板

配置服务器 IP

【命令格式】 **ip** { *ip-address* | *ipv6-address* }

【参数说明】 Portal 服务器的地址

【命令模式】 Web 认证模板配置模式

【使用指导】 -

配置服务器 URL

【命令格式】 **url** *url-string*

【参数说明】 Portal 服务器的认证页面地址

【命令模式】 Web 认证模板配置模式

【使用指导】 以 http://或 https://开头

配置 Portal 服务器 URL 格式

【命令格式】 **fmt** { **cmcc-ext1** | **cmcc-normal** | **default** }

【参数说明】 Portal 服务器的 url 格式

【命令模式】 Web 认证模板配置模式

【使用指导】 fmt 参数为必须配置为 cmcc-ext1。

配置服务器加密密钥

- 必须配置，要成功应用二代 Web 认证功能，必须设置接入/汇聚设备与认证服务器进行通信的密钥。
- 当设备发现未认证用户在访问网络资源时，设备将通过重定向功能，向用户弹出认证页面，通过认证页面，引导用户向认证服务器发起认证。在认证过程中，设备与认证服务器间通过密钥对部分数据进行加密，以加强安全性。

【命令格式】 **web-auth portal key** [**0** | **1** | **7**] *key-string*

【参数说明】 **0**：配置服务器密钥加密类型为不加密，即以明文输入，以明文保存与显示

1：配置服务器密钥加密类型为密文保存，即以明文输入，以密文保存与显示

7：配置服务器密钥加密类型为完全密文，即以密文输入，以密文保存与显示

key-string：Portal 服务器的加密密钥，配置设备与认证服务器进行通信的密钥；密钥最大长度为 255 个字符

【命令模式】 全局配置模式
【使用指导】 -

配置触发 MAC 绑定状态查询的周期和阈值

- 终端关联上打开 MAC 短信认证的 WLAN 后，可以在配置周期内使用免费流量，超过阈值后，触发 MAC 绑定查询。

【命令格式】 **web-auth sms-flow interval** *interval* **threshold** *flows*
【参数说明】 interval 为检测周期单位分钟，flows 为检测流量，单位 KB
【命令模式】 全局配置模式
【使用指导】 -

配置绑定 Portal 服务器

- 必须配置。

【命令格式】 **web-auth bind-portal** *string* **type** { **local-spec** | **group-spec** }
【参数说明】 string 为自定义模板名
【命令模式】 无线安全配置模式
【使用指导】 -

配置 winterface 参数

- 集团 MAC 认证规范要求重定向 URL 中携带 winterface 字段，字段的具体值要能够配置，winterface 基于 wlan 配置。

【命令格式】 **web-auth winterface** *string*
【参数说明】 winterface 参数字段
【命令模式】 无线安全配置模式
【使用指导】 -

配置 AC IP ADDRESS

- 集团 MAC 认证规范要求重定向 URL 中携带 AC IP 字段，因为 AC 可能有多个 IP，所以提供配置命令，在指定 wlan 下面配置 IPv4 地址作为 URL 中的 AC IP 参数。

【命令格式】 **web-auth wlan-ac-ip** *ipv4*
【参数说明】 acip 参数字段
【命令模式】 无线安全配置模式
【使用指导】 -

检验方法

- 未认证用户流量未达到阈值可以访问网络。
- 流量超过配置阈值后，触发认证。

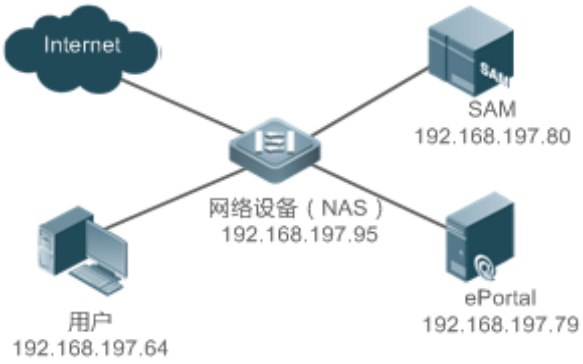
配置举例

以下配置举例，仅介绍与 Web 认证相关的配置。

MAC 短信认证

【网络环境】

图 1-14



【配置方法】

- 在网络设备上开启 AAA
- 在网络设备配置 RADIUS 服务器和密钥
- 在网络设备配置 AAA 的 Web 认证默认方法列表和默认网络记账方法列表
- 在网络入设备上设置认证服务器的 IP 地址及与认证服务器进行通信的密钥(webkey)
- 在网络设备上设置认证页面的主页地址
- 在网络设备上 MAC 短信认证检测周期和阈值，指定 winterface 参数和 acip 参数
- 在网络设备上对 WLANSEC1 开启 MAC 短信认证功能

```
Hostname# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)# aaa new-model
Hostname(config)# radius-server host 192.168.197.79 key webkey
Hostname(config)# aaa authentication web-auth default group radius
Hostname(config)# aaa accounting network default start-stop group radius
Hostname(config)# web-auth template eportalv2
Hostname(config.tmplt.eportalv2)# ip 192.168.197.79
Hostname(config.tmplt.eportalv2)# exit
Hostname(config)# web-auth portal key webkey
Hostname(config)# web-auth template eportalv2
Hostname(config.tmplt.eportalv2)# url http://192.168.197.79:8080/eportal/index.jsp
Hostname(config.tmplt.eportalv2)# fmt cmcc-ext1
Hostname(config.tmplt.eportalv2)# exit
Hostname(config)# web-auth sms-flow interval 5 threshold 10
Hostname(config)# wlansec 1
Hostname(config-wlansec)# web-auth bind-portal eportalv2 type group-spec
Hostname(config-wlansec)# web-auth accounting v2 default
Hostname(config-wlansec)# web-auth authentication v2 default
Hostname(config-wlansec)# webauth
Hostname(config-wlansec # exit
```

【检验方法】

- Web 认证配置是否成功

```
Hostname(config)# show running-config
…
aaa new-model
aaa authentication web-auth default group radius
aaa accounting network default start-stop group radius
…
radius-server host 192.168.197.79 key webkey
…
web-auth template eportalv2
 ip 192.168.197.79
 url http://192.168.197.79:8080/eportal/index.jsp
 fmt cmcc-ext1
!
web-auth portal key webkey
web-auth sms-flow interval 5 threshold 10
…
wlansec 1
 web-auth bind-portal eportalv2 type group-spec
 web-auth accounting v2 default
 web-auth authentication v2 default
webauth
```

常见错误

- Portal 服务器和设备间的 key 配置错误或者有一方配置了加密，一方未配置导致认证异常
- RADIUS 服务器和设备间参数配置不正确导致认证异常
- Portal 服务器不支持中国移动 Portal 协议规范导致无法对接

1.4.5 配置 WiFiDog 认证功能

配置效果

未认证用户能够被重定向到认证页面并完成认证

注意事项

无

配置方法

配置 Portal 服务器

- 必须配置，要成功应用 Web 认证功能，必须设置并应用 Portal 服务器。
- 当设备发现未认证用户试图通过 HTTP 访问网络资源时，设备将用户的访问请求重定向到指定的 Portal 认证页面，通过认证页面，引导用户向认证服务器发起认证。Portal 服务器地址将被设置为一个特殊的免认证的网络资源，未认证用户可以直接与该地址进行 HTTP 通讯。

配置设备 IP

- 必须配置，缺省情况下无配置。
- 该 IP 是给用户访问的，因此应该配置一个用户能访问到设备 IP。

在端口上开启 Web 认证功能

- 必须配置。
- 当 Web 认证功能基于端口开启时，默认情况下，端口未开启 Web 认证功能，此时该端口下所连接的用户不进行 Web 认证。

检验方法

- 未认证用户被要求认证
- 已认证用户可以正常使用网络

相关命令

创建模板

【命令格式】 **web-auth template wifidog**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 wifidog 为默认的 WiFiDog 认证模板

配置服务器 IP

【命令格式】 **ip** *ip-address*
【参数说明】 Portal 服务器的地址
【命令模式】 Web 认证模板配置模式
【使用指导】 -

配置服务器 URL

【命令格式】 **url** *url-string*
【参数说明】 Portal 服务器的认证页面地址
【命令模式】 Web 认证模板配置模式
【使用指导】 以 http://开头

配置设备 IP

【命令格式】 **nas-ip** *ip-address*
【参数说明】 设置 wifidog 的设备接入服务 ip，用于服务器向此 ip 发起通讯
【命令模式】 Web 认证模板配置模式
【使用指导】 配置的设备接入服务 ip 不能够被设置成直通地址。
配置接入服务 ip 为设备 IP 时会导致此认证模板下的终端访问此 ip 时被设备拦截并转发给服务器，从而不能访问设备的 Web 管理界面。
如有此认证模板下的终端直接访问此 ip 对此设备进行管理的需求，可将此接入服务 ip 设置为一个未使用的虚拟服务 ip，如 1.1.1.1，2.2.2.2 等。

配置 WiFiDog 无感知认证功能

- 可选配置。

【命令格式】 **web-auth sta-perception enable**
【参数说明】 无
【命令模式】 全局配置模式
【使用指导】 根据客户需求配置，开启之后同时要开启 ip dhcp snooping 功能才能实现无感知功能。

配置 Gateway ID

【命令格式】 **gateway-id** *string*
【参数说明】 WiFiDog 协议使用的 **gateway-id** 值，默认情况下为本设备的序列号
【命令模式】 Web 认证模板配置模式
【使用指导】 该参数为 WiFiDog 协议交互报文中需要携带的参数，开放命令给对接第三方 Portal 使用，在热备和 VAC 场景下必须配置。

使用 WiFiDog 模板

【命令格式】 **web-auth portal wifidog**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 wifidog 为默认的 WiFiDog 认证模板

启用 Web 认证

【命令格式】 **webauth**
【参数说明】 -
【命令模式】 无线安全配置模式
【使用指导】 -

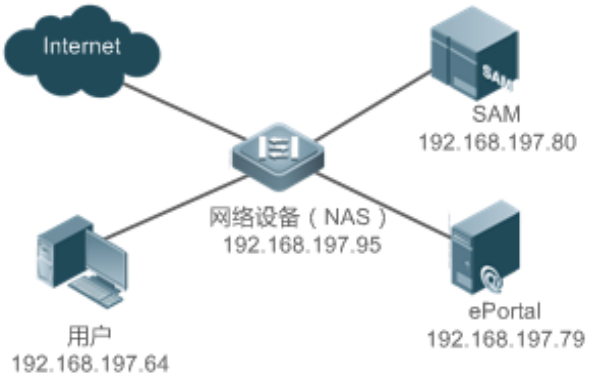
配置举例

以下配置举例，仅介绍与 Web 认证相关的配置。

WiFiDog 认证

【网络环境】

图 1-15



【配置方法】

- 在网络设备上设置认证服务器的 IP 地址
- 在网络设备上设置认证页面的主页地址
- 在网络设备上设置设备 IP 地址
- 在网络设备上对 wlan 10 开启 Web 认证功能

```
Hostname# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)# web-auth template wifidog
Hostname(config.tmplt.wifidog)# ip 192.168.197.79
Hostname(config.tmplt.wifidog)# url http://192.168.197.79/auth/wifidogAuth
Hostname(config.tmplt.wifidog)# nas-ip 1.1.1.1
Hostname(config.tmplt.wifidog)# exit
Hostname(config)# wlansec 10
Hostname(config-wlansec)# web-auth portal wifidog
Hostname(config-if-range)# webauth
Hostname(config-if-range)# exit
```

【检验方法】

- Web 认证配置是否成功

```
Hostname(config)# show running-config
...
web-auth template wifidog
 ip 192.168.197.79
 nas-ip 1.1.1.1
 url http://192.168.197.79/auth/wifidogAuth
```

```
...
wlansec 10
 web-auth portal wifidog
 webauth
```

```
Hostname#show web-auth control
Port                        Control  Server Name           Online User Count
 -------------------------- -------- --------------------- -----------------
 wlansec 10                  On       wifidog               0                 ...
```

```
Hostname# show web-auth template
Webauth Template Settings:
-------------------------------------------------------------
  Name:           wifidog
  Type:           wifidog
  Ip:             192.168.197.79
  Url:            http://192.168.197.79/auth/wifidogAuth
  NasIp:          1.1.1.1
......
```

常见错误

- 没配置设备 IP 导致无法重定向。

1.4.6 配置微信连 WiFi 认证功能

配置效果

1、 未认证手机终端用户关联到 WLAN 后，使用浏览器可以重定向到微信连 WiFi 一键上网页面，通过页面上的链接可以直接唤醒微信客户端进行微信连 WiFi 认证。
2、 未认证的手机终端用户扫描微信连 WiFi 的二维码之后，可以进行微信连 WiFi 认证
3、 未认证的 PC 用户关联到 WLAN 后，使用浏览器可以重定向到微信连 WiFi 的二维码页面，通过关联同一个 WLAN 的手机终端用户扫描该二维码，可以让 PC 用户直接认证通过上网。

注意事项

- 无

配置方法

↘ 创建微信连 WiFi 模板

- 必须配置，要使用微信连 WiFi 认证，必须配置微信连 WiFi 模板。

【命令格式】 **web-auth template** { **wechat** | (*portal-name* **wechat**) }
【参数说明】 自定义的微信连 WiFi 模板名
【命令模式】 全局配置模式
【使用指导】 wechat 为默认的微信连 WiFi 认证模板

配置服务器 IP

- 必须配置，要使用微信连 WiFi 认证，必须配置服务器地址。

【命令格式】 **ip** *ip-address*
【参数说明】 配置 ip 地址
【命令模式】 Web 认证模板配置模式
【使用指导】 -

配置服务器 URL

- 必须配置，要使用微信连 WiFi 认证，必须配置服务器的 url 地址。

【命令格式】 **service-url** *url-string*
【参数说明】 服务器的 url 地址，当前支持者配置 IP 和端口
支持域名配置，要求域名对应的 IP 只有一个。当前只支持 http 协议的 url 解析，url 中的协议名称部分将被自动去除
【命令模式】 Web 认证模板配置模式
【使用指导】 只要配置域名，不允许以 http://或者 https://开头

配置 Portal 服务器的认证页面地址

- 11.1(5)B9 的版本必须配置，要使用微信连 WiFi 认证，必须配置 Portal 服务器认证页面地址。

【命令格式】 **url** *url-string*
【参数说明】 该地址为使用微信与短信共存认证时的短信认证重定向地址
【命令模式】 Web 认证模板配置模式
【使用指导】 以 http://或 https://开头

配置与服务器通讯的加密密钥 KEY

- 必须配置，要使用微信连 WiFi 认证，必须配置服务器的加密密钥。

【命令格式】 **key** *key-string*
【参数说明】 服务器的加密密钥。配置设备与认证服务器进行通信的密钥；密钥最大长度为 255 个字符
【命令模式】 Web 认证模板配置模式
【使用指导】 加密密钥必须和服务器上配置的一致，否则会出现对接不成功的问题。

配置设备 IP

【命令格式】 **nas-ip** *ip-address*

【参数说明】 设置微信连 WiFi 认证设备接入服务 ip，用于服务器向此 ip 发起通讯

【命令模式】 Web 认证模板配置模式

【使用指导】 配置的设备接入服务 ip 不能够被设置成直通地址。

配置接入服务 ip 为设备 IP 时会导致此认证模板下的终端访问此 ip 时被设备拦截并转发给服务器，从而不能访问设备的 Web 管理界面。

如有此认证模板下的终端直接访问此 ip 对此设备进行管理的需求，可将此接入服务 ip 设置为一个未使用的虚拟服务 ip，如 1.1.1.1，2.2.2.2 等。

配置微信连 WiFi 无感知认证功能

- 可选配置。

【命令格式】 **web-auth sta-perception enable**

【参数说明】 无

【命令模式】 全局配置模式

【使用指导】 根据客户需求配置，开启之后同时要开启 ip dhcp snooping 功能才能实现无感知功能。

配置开启逃生功能

- 配置后，当满足逃生条件时（服务器不通或者服务器希望用户逃生），后续接入的用户都可以逃生免认证。逃生用户的上网时长由 **interval** *minutes* 指定。
- 无线安全模式下的配置优先生效，若该模式下未配置则使用全局下的配置。
- 如果要取消逃生状态，可以在全局配置模式使用 web-auth wechat-escape recover。

【命令格式】 **web-auth wechat-escape interval** *minutes*

【参数说明】 *minutes*：逃生定时器超时时间，单位：分钟，默认值为 60 分钟

【命令模式】 全局配置模式和无线安全配置模式

【使用指导】 -

配置服务器检测功能

- 可选配置，配置后，设备开始对服务器进行检测，如果一定间隔内（由 **interval** *minutes* 指定）检测到服务器没有应答或者回应不可用，同时设备配置了集体逃生功能，后面接入的所有用户都直接逃生免认证。
- 如果要取消服务器检测，可以在全局配置模式使用 **no web-auth wechat-check** 取消服务器检测功能。

【命令格式】 **web-auth wechat-check interval** *minutes*

【参数说明】 *minutes*：服务器检测定时器间隔，单位：分钟，无默认值

【命令模式】 全局配置模式

【使用指导】 -

配置无感知的 ip 校验功能

- 可选配置，配置后，超过时间用户还未获取 IP 地址，就将被踢下线。

【命令格式】 **web-auth valid-ip-acct** [**timeout** *seconds*]

【参数说明】 *seconds*： 允许等待用户获取 IP 的时间，单位：秒钟，默认值为 30s

【命令模式】 全局配置模式

【使用指导】 -

使用 webchat 模板

【命令格式】 **web-auth portal wechat**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 webchat 为默认的微信连 WiFi 认证模板

启用 Web 认证

【命令格式】 **webauth**
【参数说明】 -
【命令模式】 无线安全配置模式
【使用指导】 -

检验方法

- 未认证用户被要求认证
- 已认证用户可以正常使用网络

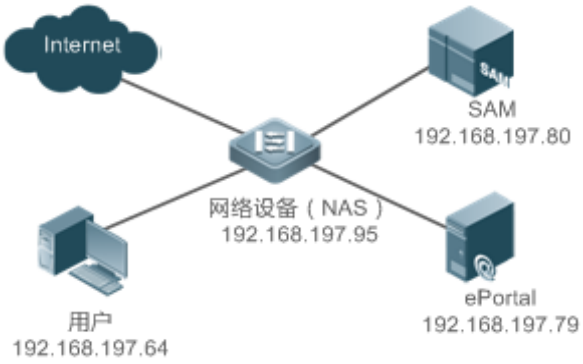
配置举例

以下配置举例，仅介绍与 Web 认证相关的配置。

微信连 WiFi 认证

【网络环境】

图 1-10



【配置方法】
- 在网络设备上配置域名服务器地址 192.168.58.110
- 在网络设备上配置微信连 WiFi 认证模板
- 在网络设备上配置服务器的 ip 和 service-url 地址
- 在网络设备上配置与服务器进行通信的加密密钥(webkey)
- 在网络设备上配置设备的 ip 地址
- 在网络设备上对 WLANSEC1 应用模板并开启微信连 WiFi 认证功能

```
Hostname# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)# ip name-server 192.168.58.110
Hostname(config)# web-auth template wechat
Hostname(config.tmplt.wechat)# ip 192.168.197.79
Hostname(config.tmplt.wechat)# service-url wmc.Hostname.com.cn
Hostname(config.tmplt.wechat)# key webkey
Hostname(config.tmplt.wechat)# nas-ip 1.1.1.1
Hostname(config.tmplt.wechat)# exit
Hostname(config)# wlansec 1
Hostname(config-wlansec)# web-auth portal wechat
Hostname(config-wlansec)# webauth
```

【检验方法】

- Web 认证配置是否成功

```
Hostname(config)# show running-config
...
ip name-server 192.168.58.110
...
web-auth template wechat
 ip 192.168.197.79
 service-url wmc.Hostname.com.cn http://192.168.197.79:8080/eportal/index.jsp
 key webkey
 nas-ip 1.1.1.1
!...
wlansec 1
 web-auth portal wechat
 webauth
!
```

常见错误

- 服务器和设备间的 key 配置错误或者有一方配置了加密，一方未配置导致认证异常
- 设备 IP 地址配置成直通，Web 认证无法收到认证报文，导致认证失败
- 域名服务器地址没有配置导致白名单解析失败，微信服务器地址没有放行
- 开启无感知认证时没有配置 **ip dhcp snooping**、**ip dhcp snooping trust** 和 **web-auth sta-perception enable** 命令，导致二次认证无感知失效

1.4.7 配置 Clearpass 认证功能

配置效果

未认证用户能够被重定向到认证页面并完成认证

注意事项

无

配置方法

配置 Portal 服务器

- 必须配置，要成功应用 Web 认证功能，必须设置并应用 Portal 服务器。
- 当设备发现未认证用户试图通过 HTTP 访问网络资源时，设备将用户的访问请求重定向到指定的 Portal 认证页面，通过认证页面，引导用户向认证服务器发起认证。Portal 服务器地址将被设置为一个特殊的免认证的网络资源，未认证用户可以直接与该地址进行 HTTP 通讯。

配置认证成功后的响应方式

- 可选配置。
- 根据用户需求进行配置。

配置认证失败后的响应方式

- 可选配置
- 根据用户需求进行配置。

配置设备解析认证请求的方式

- 可选配置。
- 根据对接的服务器要求进行配置。

配置认证成功后是否弹窗主动下线页面

- 可选配置。
- 根据用户需求进行配置。

配置设备 IP

- 必须配置，缺省情况下无配置。
- 该 IP 是给用户访问的，因此应该配置一个用户能访问到设备 IP.

配置设备端口

- 必须配置，缺省情况下无配置。
- 该端口是给用户访问的，不能与内置、Web 网管配置的端口冲突.

配置终端发起认证使用的 url

- 可选配置，缺省情况下为 http://ip:port/login，其中 ip 和 port 分别为设备 IP 和设备端口。
- 该 url 是给用户访问的，需要配置成和 clearpass 上配置的地址一致。

在端口上开启 Web 认证功能

- 必须配置。
- 当 Web 认证功能基于端口开启时，默认情况下，端口未开启 Web 认证功能，此时该端口下所连接的用户不进行 Web 认证。

检验方法

- 未认证用户被要求认证
- 已认证用户可以正常使用网络

相关命令

开启 AAA 功能

【命令格式】 **aaa new-model**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 AAA 的方法列表等命令需要在功能开启后才能输入

配置 RADIUS 服务器和密钥

【命令格式】 **radius-server host** *ip-address* [**auth-port** *port-number1*] [**acct-port** *port-number 2*] **key** *string*
【参数说明】 *ip-address*：服务器 IP 地址
port-number1：认证端口号
port-number2：记账端口号
string：密钥字符串
【命令模式】 全局配置模式
【使用指导】 认证端口默认 1812，记账端口默认 1813

配置 AAA 中 Web 认证方法列表

【命令格式】 **aaa authentication cpweb** { **default** | *list-name* } *method1* [*method2*...]
【参数说明】 *list-name*：方法列表名
method1：方法 1

method2：方法 2

【命令模式】 全局配置模式

【使用指导】 clearpass 认证通常使用 RADIUS 认证方法

配置网络记账方法列表

【命令格式】 **aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]

【参数说明】 *list-name*：方法列表名

method1：方法 1

method2：方法 2

【命令模式】 全局配置模式

【使用指导】 clearpass 认证通常使用 RADIUS 记账方法

创建模板

【命令格式】 **web-auth template cpweb**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 cpweb 为默认的 Clearpass 认证模板

配置服务器 IP

【命令格式】 **ip** *ip-address*

【参数说明】 Portal 服务器的地址

【命令模式】 Web 认证模板配置模式

【使用指导】 -

配置热备服务器 ctx id 和 IP 地址

【命令格式】 **context** *ctx-id peer-ip-address*

【参数说明】 *ctx-id*：配置热备服务器对应的 context id

peer-id-address：热备（备机）的 IP 地址

【命令模式】 Web 认证模板配置模式

【使用指导】 -

配置服务器 URL

【命令格式】 **url** *url-string*

【参数说明】 Portal 服务器的认证页面地址

【命令模式】 Web 认证模板配置模式

【使用指导】 以 http://开头

配置认证成功后的响应方式

【命令格式】 **login-success response** { **redirect-init-url** [**default-url** *def-string*] | **msg** *msg-string* | **redirect-url** *url-string* }

【参数说明】 *def-string*：默认 url，在服务器未下发 url 时使用

msg-string：认证成功后显示的消息文本

url-string：认证成功后跳转的 url

【命令模式】 Web 认证模板配置模式

【使用指导】 可选配置

配置认证失败后的响应方式

【命令格式】 配置 clearpass 认证失败后显示的提示信息

login-fail response msg *msg-string*

配置 clearpass 认证失败后的重定向至登陆页面地址。

login-fail response redirect-login-url

配置 clearpass 认证失败后跳转的 url 地址

login-fail response redirect-url *url-string* [**err-msg** *msg-key*]

配置 clearpass 认证失败后跳转的 url 地址，格式为 http://xxx/xx?ap_mac=6c:8b:d3:37:e2:60&wlan=Guest&statusCode=5，其中 wlan 字段为 ssid 的名字

login-fail response redirect-url *url-string* [**fmt ntes** [**errmsg-key** *key-string*]]

配置 clearpass 认证失败后跳转的 url 地址，支持 url 定制

login-fail response redirect-url *url-string* [**fmt custom encry** { **md5 | des** | **des_ecb** | **des_ecb3 | none** } { **additional** *extern-str* | **ap-mac** *ap-mac-str* **mac-format** { **dot** | **line** | **5colon** | **none** } | **ssid** *ssid-str* | **errmsg-key** *key-string* }]

【参数说明】 *msg-string*：认证失败后消失的消息文本

redirect-login-url：认证失败之后重定向到登陆页面地址

url-string：认证失败后跳转的 url

ntes：定制的 url 格式

key-string：url 中错误消息的参数名称

custom：进行认证失败后重定向的 url 定制

encry：配置加密方式，可选加密方式有：md5、des、des_ecb、des_ecb3、none

extern-str：定制的额外信息字符串

ap-mac-str：apmac 参数的参数名字

mac-format：配置 mac 地址的格式，可选格式有：dot、line、5colon、none

ssid-str：ssid 参数的参数名字

【命令模式】 Web 认证模板配置模式

【使用指导】 可选配置

配置设备解析认证请求的方式

【命令格式】 **http-method** { **post** | **get** } [**init-url-key** *init-string* **| username-key** *username-string* **| password-key** *password-string* **| password-encrypt** { **none | uam** }]

【参数说明】 *username-string*：认证请求中用户名参数名称

password-string：认证请求中密码参数名称

init-string：认证请求中 url 参数名称

【命令模式】 Web 认证模板配置模式

【使用指导】 可选配置，根据服务器要求进行配置

配置认证成功后是否弹窗主动下线页面

【命令格式】 **logout-popup-window**

【参数说明】 -

【命令模式】 Web 认证模板配置模式

【使用指导】 可选配置，需要主动下线功能时开启，但是主动弹窗有可能会被终端浏览器拦截

配置设备 IP

【命令格式】 **web-auth auth-server ip** *ip-address*

【参数说明】 设置 clearpass 的设备接入服务 ip，用于服务器向此 ip 发起通讯

【命令模式】 全局配置模式

【使用指导】 配置的设备接入服务 ip 不能够被设置成直通地址。

配置接入服务 ip 为设备 IP 时会导致此认证模板下的终端访问此 ip 时被设备拦截并转发给服务器，从而不能访问设备的 Web 管理界面。

如有此认证模板下的终端直接访问此 ip 对此设备进行管理的需求，可将此接入服务 ip 设置为一个未使用的虚拟服务 ip，如 1.1.1.1，2.2.2.2 等。

配置设备端口

【命令格式】 **web-auth auth-server http** [**port** *port-number*]

【参数说明】 *port-number*：Clearpass 终端发起认证时使用的 tcp 端口

【命令模式】 全局配置模式

【使用指导】 该参数为终端发起认证使用的 tcp 端口，不能和内置、Web 网管使用的端口冲突。

配置终端发起认证使用的 url

【命令格式】 **web-auth auth-server submit-url** *url-string*

【参数说明】 *url-string*：Clearpass 终端发起认证时使用的 url 地址

【命令模式】 全局配置模式

【使用指导】 该参数为终端发起认证使用的 url 地址，必须以 http://开头。

启用 Web 认证

【命令格式】 **webauth**

【参数说明】 -

【命令模式】 无线安全配置模式

【使用指导】 -

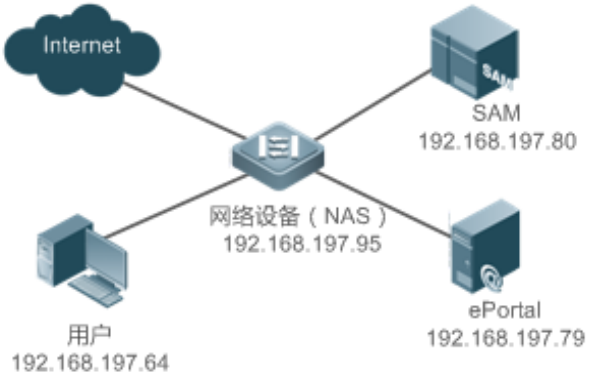
配置举例

以下配置举例，仅介绍与 Web 认证相关的配置。

clearpass 认证

【网络环境】

图 1-16



【配置方法】

- 在网络设备上设置认证服务器的 IP 地址
- 在网络设备上设置认证页面的主页地址
- 在网络设备上设置设备 IP 地址
- 在网络设备上设置设备的端口
- 在网络设备上设置终端认证的 url
- 在网络设备上对 wlan 10 开启 Web 认证功能

```
Hostname# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)# web-auth auth-server http port 8082
Hostname(config)# web-auth auth-server ip 1.1.1.1
Hostname(config)# web-auth auth-server submit-url http://1.1.1.1:8082/login
Hostname(config)# web-auth template cpweb
Hostname(config.tmplt.cpweb)# ip 192.168.197.79
Hostname(config.tmplt.cpweb)# url http://192.168.197.79/web_login.php
Hostname(config.tmplt.cpweb)# exit
Hostname(config)# wlansec 10
Hostname(config-wlansec)# web-auth portal cpweb
Hostname(config-if-range)# webauth
Hostname(config-if-range)# exit
```

【检验方法】

- Web 认证配置是否成功

```
Hostname(config)# show running-config
...
web-auth auth-server ip 1.1.1.1
web-auth auth-server http
web-auth auth-server submit-url http://1.1.1.1:8082/login
```

```
web-auth template cpweb
 ip 192.168.197.79
 url http://192.168.197.79/web_login.php
...
wlansec 10
 web-auth portal cpweb
 webauth
```

```
Hostname# show web-auth control
Port                        Control  Server Name           Online User Count
 ------------------------- -------- --------------------- -----------------
 wlansec 10                  On       cpweb                0                  ...
```

```
Hostname#show web-auth template
Webauth Template Settings:
-------------------------------------------------------------
  Name:           cpweb
  Type:           cpweb
  Ip:             192.168.197.79
  Url:            http://192.168.197.79/web_login.php
```

常见错误

- 没配置设备 IP 导致无法重定向。

1.4.8 配置认证方法列表名

配置效果

- 当用户提交认证信息时，Portal 服务器会向设备发起认证请求，设备依据配置的认证方法列表名解析认证服务器等信息，发起认证过程。
- 配置认证方法列表名后，设备可以通过指定的方法列表名选择认证服务器进行认证。

注意事项

- 配置认证方法列表名前 ,必须保证在 AAA 中已经定义了该方法。对应定义命令为 **aaa authentication web-auth** { **default** | *list-name* } *method1* [*method2*...]。
- 无法分别给 IPv4 和 ipv6 认证指定不同的认证方法。

配置方法

- 可选配置
- 默认使用 default 方法，在 AAA 修改方法列表名或存在多个方法列表名时，使用本命令进行配置。

检验方法

- 在 AAA 中配置两个方法列表，方法列表 1 使用服务器 1，方法列表 2 使用服务器 2
- 在服务器 1 创建用户 a 和密码；服务器 2 创建用户 b
- 配置使用方法列表 1
- 用户使用账号 b 进行认证，认证失败
- 用户使用账户 a 进行认证，认证成功

相关命令

配置认证方法列表名

【命令格式】 **authentication** *method-list*
【参数说明】 方法列表名
【命令模式】 Web 认证模板配置模式
【使用指导】 应与 AAA 中 Web 认证方法列表名一致

配置举例

配置认证方法列表名

【配置方法】
- 配置认证方法列表名为 mlist1

```
Hostname(config.tmplt.iportal)# authentication mlist1
```

【检验方法】
- 查看配置是否成功

```
Hostname# show web-auth template
Webauth Template Settings:
-----------------------------------------------------------
  Name:       eportalv2
  Url:        http://17.17.1.21:8080/eportal/index.jsp
  Ip:         17.17.1.21
  BindMode:   ip-only-mode
  Type:       v2
  Port:       50100
  State:      Active
  Acctmlist: default
  Authmlist: mlist1
```

1.4.9 配置记账方法列表名

配置效果

- 用户认证通过后，设备会自动发起记账请求，请求的对象依赖于记账方法列表的配置，通常为认证所在服务器。
- 配置记账方法列表名后，设备可以通过指定的方法列表名选择记账服务器进行记账。

注意事项

- 配置记账方法列表名前，必须保证在 AAA 中已经定义了该方法。对应定义命令为 **aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]。
- 无法分别给 IPv4 和 ipv6 认证指定不同的记账方法。

配置方法

- 可选配置
- 默认使用 default 方法，在 AAA 修改方法列表名或存在多个方法列表名时，使用本命令进行配置。

检验方法

- 在 AAA 中配置两个记账方法列表，方法列表 1 使用服务器 1，方法列表 2 使用服务器 2
- 配置使用方法列表 1
- 用户使用合法账号进行认证上线
- 在服务器 1 和服务器 2 上分别查看用户记账信息；只有服务器 1 存在

相关命令

↘ 配置记账方法列表名

【命令格式】 **accounting** *method-list*
【参数说明】 方法列表名
【命令模式】 Web 认证模板配置模式
【使用指导】 应与 AAA 中网络记账方法列表名一致

配置举例

↘ 配置记账方法列表名

【配置方法】
- 配置记账方法列表名为 mlist1

```
Hostname(config.tmplt.eportalv2)# accounting mlist1
```

【检验方法】

- 查看配置是否成功

```
Hostname# show web-auth template
Webauth Template Settings:
------------------------------------------------------------
 Name:       eportalv2
 Url:        http://17.17.1.21:8080/eportal/index.jsp
 Ip:         17.17.1.21
 BindMode:   ip-mac-mode
 Type:       v2
 Port:       50100
 State:      Active
 Acctmlist: mlist1
 Authmlist: mlist1
```

1.4.10 配置 Portal 服务器通信端口

配置效果

- 设备检测到用户下线等情况时，需要同时通告 Portal 服务器用户下线；设备和 Portal 服务器使用 Portal 协议进行交互，协议使用约定的端口号进行报文侦听和收发。
- 当 Portal 服务器侦听端口改变时，设备需要修改 Portal 服务器通信端口才能进行交互。
- 如果是内置 Portal Web 认证，此功能用于配置本机监听的 http 端口，默认是 8081.

注意事项

- 端口号配置需要和服务器实际使用端口相一致。
- 适用于二代 Web 认证和内置 Portal Web 认证 ,且两种认证的默认端口号不一致。二代 Web 认证端口号用于设备和 Portal 服务器交互 Portal 协议，内置 Portal Web 认证的端口号用于本机报文监听。

配置方法

- 可选配置
- 服务器不使用默认端口号或者本机监听端口有冲突需要调整时，使用本命令配置来保持一致。

检验方法

- 配置二代 Web 认证

- 改变服务器侦听端口为 10000
- 通过本命令配置端口号为 10000
- 用户 Web 认证上线
- 在设备端踢用户下线，刷新在线页面，提示用户下线

相关命令

配置 Portal 服务器通信端口

【命令格式】 **port** *port-num*
【参数说明】 *port-num*：端口号
【命令模式】 Web 认证模板配置模式
【使用指导】 -

配置举例

配置 Portal 服务器通信端口

【配置方法】
- 配置服务器通信端口为 10000

```
Hostname(config.tmplt.eportalv2)# port 10000
```

【检验方法】
- 查看配置是否成功

```
Hostname# show web-auth template
Webauth Template Settings:
-------------------------------------------------------------
  Name:       eportalv2
  Url:        http://17.17.1.21:8080/eportal/index.jsp
  Ip:         17.17.1.21
  BindMode:   ip-only-mode
  Type:       v2
  Port:       10000
  Acctmlist:
  Authmlist:
```

1.4.11 配置绑定模式

配置效果

- 用户成功上线时，需要将用户表项写到转发规则中，指定不同的绑定模式，可以改变转发规则的匹配方式，影响用户的上网规则。比如仅 IP 绑定时，只要符合该 IP 的报文都被放行，用户都能上网；而 IP+MAC 绑定时，只有同时符合该 IP 和 MAC 的用户能访问网络。

注意事项

- 在三层认证场景中，设备看到的 MAC 地址都是用户网关地址，MAC 地址都不准确，此时应该采用仅 IP 绑定模式。

配置方法

- 可选配置，缺省默认：IP+MAC 绑定。
- 依据设备能获得的用户准确信息决定选择哪种绑定模式 ,当用户 IP、MAC 均准确时 ,比如二层网络部署 ,优先选择 IP+MAC 绑定；否则优先选择仅 IP 绑定模式。

检验方法

- 改变绑定模式为仅 IP 模式
- 用户认证上线
- 修改用户 MAC，或者使用另一台同 IP，不同 MAC 的客户端访问网络
- 用户上网正常

相关命令

↘ 配置绑定模式

【命令格式】 **bindmode** { **ip-mac-mode** | **ip-only-mode** }

【参数说明】 **ip-mac-mode**：IP+MAC 同时绑定

ip-only-mode：仅 IP 绑定

【命令模式】 Web 认证模板配置模式

【使用指导】 -

配置举例

↘ 配置绑定模式

【配置方法】

- 配置绑定模式为仅 IP 模式

```
Hostname(config.tmplt.eportalv2)# bindmode ip-only-mode
```

【检验方法】

- 查看配置是否成功

```
Hostname# show web-auth template
Webauth Template Settings:
```

【配置方法】 ● 配置绑定模式为仅 IP 模式

```
Hostname(config.tmplt.eportalv2)# bindmode ip-only-mode
```

【检验方法】 ● 查看配置是否成功

```
------------------------------------------------------------
  Name:       eportalv2
  Url:        http://17.17.1.21:8080/eportal/index.jsp
  Ip:         17.17.1.21
  BindMode:   ip-only-mode
  Type:       v2
  Port:       10000
  Acctmlist:
  Authmlist:
```

1.4.12 配置定制页面包

配置效果

- 用户可以指定内置 Portal 使用特定页面包，之后在这些页面包上嵌入特色内容或者信息，比如特有的 LOGO 或者公告信息等。

注意事项

- 页面包需要手工下载到设备的 FLASH 中，并且固定存放在./portal 目录下，如果未事先存放页面包或者存放目录错误，会导致无法推送页面，进而导致 Web 认证时效。如果对页面包没特殊要求，可以使用设备默认页面包。
- 页面包的定制规范请参考”页面包定制规范”。

配置方法

- 可选配置，缺省使用设备自带的页面包。

检验方法

- 配置内置 Portal Web 认证。
- 下载新的页面包。
- 指定使用该页面包。
- 用户上网，登录页面为定制页面。

相关命令

↘ 配置定制页面包

【命令格式】 **page-suit** *file-name*

【参数说明】 *file-name*：定制页面包的文件名

【命令模式】 Web 认证模板配置模式

【使用指导】 新的页面包需要提前下载到 FLASH 的./porta/zipl 目录。

配置举例

↘ 配置定制页面包

【配置方法】

- 配置定制页面包

```
Hostname(config.tmplt.iportal)# page-suit Hostnamepage
```

【检验方法】

- 查看配置是否成功

```
Advertising mode: online-popup
Type:      Intral Portal
Acctmlist:default
Authmlist:default
```

1.4.13 配置广告推送方式

配置效果

- 可选则认证前弹出广告、认证后弹出广告。

注意事项

- 需要先配置好广告 url。
- 默认是认证成功后弹广告。
- 如果要实现用户不认证，只弹广告的效果，请选择 Advertising 功能，具体参考 Advertising 的配置手册。

配置方法

- 可选配置，缺省认证成功后弹广告。

检验方法

- 配置内置 Portal Web 认证
- 配置一个可访问互联网 url 地址
- 用户上网，认证成功后浏览器弹出一个新窗口并显示指定 url 的页面信息

相关命令

配置用户认证前广告推送 URL

【命令格式】 **login-popup** *url-string*
【参数说明】 *url-string* ：认证前弹出，也是登录的时候弹出的地址
【命令模式】 Web 认证模板配置模式
【使用指导】 无

配置用户认证成功后广告推送 URL

【命令格式】 **online-popup** *url-string*
【参数说明】 *url-string*：认证成功后前弹出的地址
【命令模式】 Web 认证模板配置模式
【使用指导】 无

配置举例

配置广告推送模式

【配置方法】
- 配置广告推送模式为认证前弹广告

```
Hostname(config.tmplt.iportal)# login-popup http://www.Hostname.com.cn/
```

【检验方法】
- 查看配置是否成功

```
Hostname# show web-auth template
Webauth Template Settings:
-------------------------------------------------------------
  Name:           iportal
  BindMode:       ip-mac-mode
  Type:           intra
  Port:           8081
  time_interval:  1
  Login_popup:    http://www.Hostname.com.cn/
  Online_popup:   (null)
  Suitename:      default
  Authentication:
  Accounting:
```

1.4.14 配置定制化 URL 格式

配置效果

- 用户配置了定制化 URL 后，重定向到 portal 的 URL 会根据定制化的参数进行设置。

注意事项

- 定制化配置后的参数顺序与实际 url 的参数顺序不一定一致。

配置方法

- 可选配置

检验方法

- 配置定制化 URL
- 未认证 PC，使用浏览器访问该端口的外网网络
- 用户访问请求被重定向，重定向 URL 参数与配置的定制化 URL 一致

相关命令

↘ 配置定制化 URL 格式

【命令格式】 **fmt custom** [**encrypt** { **md5** | **des** | **des_ecb** | **des_ecb3** | **none** }] [**user-ip** *userip-str*] [**user-mac** *usermac-str* **mac-format** [**dot** | **line** | **none** | **5colon**]] [**user-vid** *uservid-str*] [**user-id** *userid-str*] [**nas-ip** *nasip-str*] [**nas-id** *nasid-str*] [**nas-id2** *nasid2-str*] [**ac-name** *acname-str*] [**ap-mac** *apmac-str* **mac-format** [**dot** | **line** | **none]**] [**url** *url-str*] [**ssid** *ssid-str*] [**port** *port-str*] [**ac-serialno** *ac-sno-str*] [**ap-serialno** *ap-sno-str*] [**additional** *extern-str*]

【参数说明】 *userip-str*：用户 ip 对应的参数名称
usermac-str：用户 mac 对应的参数名称
uservid-str：用户 vid 对应的参数名称
userid-str：用户 id 对应的参数名称
nasip-str：设备 IP 对应的参数名称
nasid-str：NAS 设备 ID 对应的参数名称
nasid2-str：NAS 设备 ID 对应的参数名称(支持定制两个 nasid 参数)
ac-name：设备名称对应的参数名称
apmac-str：关联 AP 的 MAC 地址对应的参数名称
url-str：用户原始访问 url 对应的参数名称
ssid-str：SSID 对应的参数名称

port-str：用户认证端口对应的参数名称
ac-sno-str：ac 设备序列号对应的参数名称
ap-sno-str：ap 设备序列号对应的参数名称
extern-str：固定字符串，某些 portal 需要特定字符串标识
md5：所配置参数采用 md5 加密
des：所配置参数采用 des 加密
des_ecb：所配置参数采用 des_ecb 加密
des_ecb3：所配置参数采用 des_ecb3 加密
none：所配置参数不加密，明文传输

【命令模式】 模板配置模式

【使用指导】 支持添加或删除单个参数。

配置举例

↘ 配置定制化 URL 格式

【配置方法】
- 配置明文用户 ip，用户 mac，nasip，ssid，url 等参数作为重定向 URL 参数

```
Hostname(config.tmplt.eportalv2)# fmt custom encry none user-ip userip user-mac usermac mac-format none nas-ip nasip ssid ssid url firsturl
```

【检验方法】
- 查看配置是否成功

```
Hostname(config)# show running-config
...
fmt custom encry none user-ip userip user-mac usermac mac-format none nas-ip nasip ssid ssid url firsturl
```

1.4.15 设置重定向的 HTTP 端口

配置效果

- 当用户访问网络资源时（例如使用浏览器上网），此时用户会发出 HTTP 报文，接入/汇聚设备通过拦截来自用户的 HTTP 报文，来判断用户是否在访问网络资源。当设备检测到未认证的用户在访问网络资源时，将阻止用户访问网络资源，并向用户弹出认证页面。缺省情况下，网络设备通过拦截用户发出的端口号为 80 的 HTTP 报文，来检测用户是否在访问网络资源。
- 设置重定向的 HTTP 端口后，可以对用户发出的特定目的端口号的 HTTP 请求进行重定向。

注意事项

- 接入/汇聚设备上常用的管理协议端口（例如 22、23、53）以及系统内部保留的端口，不允许被设置为重定向端口。实际上，除了 80 端口外，HTTP 协议很少会使用小于 1000 的端口号。为了避免与知名 TCP 协议端口冲突，除非必要，尽量避免设置较小端口号的端口作为重定向端口。

配置方法

- 可选配置
- 在配置自动获取客户端时，如果要新增网络设备拦截用户发出的特定端口号的 HTTP 报文，可以进行该配置。

检验方法

- 配置拦截端口
- 未认证 PC，使用浏览器访问该端口的外网网络
- 用户访问请求被重定向到认证页面

相关命令

↘ 设置重定向的 HTTP 端口

【命令格式】 **http redirect port** *port-num*

【参数说明】 *port-num*：端口号

【命令模式】 全局配置模式

【使用指导】 最大允许配置 10 个不同的目的端口号，默认端口号(80，443)不含在该总数量范围内。

配置举例

↘ 设置重定向的 HTTP 端口

【配置方法】

- 配置 8080 端口为重定向的 HTTP 端口

```
Hostname(config)# http redirect port 8080
```

【检验方法】

- 查看配置是否成功

```
Hostname(config)# show web-auth rdport
Rd-Port:
80 443 8080
```

1.4.16 设置 Web 认证模块 SYSLOG 功能

配置效果

- 当用户上下线时，Web 认证模块会通过 SYSLOG 将上下线的用户信息和事件呈现给管理员。缺省情况下，该 SYSLOG 信息被屏蔽。
- 设置 SYSLOG 限速功能后，可以按照一定的速率将该信息呈现出来。

注意事项

- 当认证上下线速率很高时，频繁的 SYSLOG 输出会影响设备性能，同时导致输出信息刷屏。

配置方法

- 可选配置
- 需要查看基本上下线 SYSLOG 信息时，可以配置 SYSLOG 限速功能。

检验方法

- 配置 SYSLOG 限速
- 用户按照一定速率上下线
- SYSLOG 按照限制要求打印输出

相关命令

↘ 设置 SYSLOG 限速

【命令格式】 **web-auth logging enable** *num*

【参数说明】 *num*：SYSLOG 输出速率（条/秒）

【命令模式】 全局配置模式

【使用指导】 0 为不限制速率；不输出受限的 SYSLOG。受限的 SYSLOG 不包括严重级 SYSLOG，及异常错误输出的 SYSLOG。

配置举例

↘ 设置 SYSLOG 限速

【配置方法】
- 配置不限制 SYSLOG 输出

```
Hostname(config)# web-auth logging enable 0
```

【检验方法】
- 查看配置是否成功

```
Hostname(config)# show running-config
...
web-auth logging enable 0
...
```

1.4.17 设置未认证用户的最大 HTTP 会话数

配置效果

- 未认证的用户在访问网络资源时，用户 PC 会发出 HTTP 会话连接请求，HTTP 报文会被接入/汇聚设备拦截，并通过重定向要求用户进行 Web 认证。为了防止同一个未认证用户发起过多的 HTTP 连接请求，以节约网络设备的资源，需要在设备上限制未认证用户的最大 HTTP 会话数。
- 由于用户在认证时，会占用一个 HTTP 会话，而用户的其他应用程序也可能占用着 HTTP 会话，因而不建议设置未认证用户的最大 HTTP 会话数为 1。缺省情况下，全局每个未认证用户的最大 HTTP 会话数为 255，而每个端口下的未认证用户的 HTTP 会话总数最大为 300。

注意事项

- 如果一个用户在进行 Web 认证时，出现经常无法弹出认证页面的情况，则很可能是受到最大 HTTP 会话数的限制了。此时，应该建议用户暂时关闭可能会占用 HTTP 会话的应用程序，之后再进行 Web 认证。

配置方法

- 可选配置
- 要更改每个未认证用户的最大 HTTP 会话数及每个端口下的未认证用户的 HTTP 会话总数时，可进行该配置。
- 在配置自动获取 SU 客户端功能时， 需要进行该配置。

检验方法

- 修改未认证用户最大会话数
- 未认证用户构造相同会话不间断对设备进行连接
- 未认证用户通过浏览器访问外网，访问请求不被重定向，设备提示用户会话数超过限制

相关命令

↘ 设置每个未认证用户的最大 HTTP 会话数

【命令格式】 **http redirect session-limit** *session-num* [**port** *port-session-num*]

【参数说明】 *session-num*：最大会话数。取值范围 1-255，默认为 255。

port-session-num：端口最大会话数。取值范围 1-65535，默认为 300。

【命令模式】 全局配置模式

【使用指导】 无

配置举例

↘ 设置每个未认证用户的最大 HTTP 会话数

【配置方法】
- 设置每个未认证用户的最大 HTTP 会话数为 3

```
Hostname(config)# http redirect session-limit 3
```

【检验方法】
- 查看配置是否成功

```
Hostname(config)# show web-auth parameter
HTTP redirection setting:
  session-limit: 3
  timeout:       3
Hostname(config)#
```

1.4.18 设置维持重定向连接的超时时间

配置效果

- 设置维持重定向连接的超时时间。因为未认证的用户通过 HTTP 访问网络资源时，其 TCP 连接请求将被拦截，实际上是与接入/汇聚设备建立起 TCP 连接。在连接建立后，设备需要等待用户发出的 HTTP 的 GET/HEAD 报文，再回复 HTTP 重定向报文后才能关闭连接。设置此限制可以防止用户不发 GET/HEAD 报文，而又长时间占用 TCP 连接。缺省情况下，维持重定向连接的超时时间为 3 秒。

注意事项

- 无

配置方法

- 可选配置
- 要更改维持重定向连接的超时时间时，可进行该配置。

检验方法

- 修改超时时间配置
- 使用网络发包工具构造建立 tcp 连接
- 查看设备上该 tcp 连接状态，超过超时时间后连接被关闭

相关命令

↘ 设置维持重定向连接的超时时间

【命令格式】 **http redirect timeout** *seconds*

【参数说明】 *seconds*：重定向连接超时时间，单位为秒。取值范围 1-10。默认为 3 秒。

【命令模式】 全局配置模式

【使用指导】 无

配置举例

↘ 设置维持重定向连接的超时时间

【配置方法】

- 设置维持重定向连接的超时时间 5

```
Hostname(config)# http redirect timeout 5
```

【检验方法】

- 查看配置是否成功

```
Hostname(config)# show web-auth parameter
HTTP redirection setting:
  session-limit: 255
  timeout:       5
```

1.4.19 设置免认证网络资源范围

配置效果

- 在端口上启动 Web 认证或者 802.1x 认证后，未认证用户需先通过 Web 认证或者 802.1x 认证，才能访问网络资源。
- 使用此命令设置免认证的网络资源，可以允许未认证用户，也可以访问一些免认证的网络资源。
- 设置了免认证的网络资源，如果某网站属于免认证的网络资源，那么所有用户（包括未认证用户）都可以访问该网站。缺省情况下，没有设置免认证的网络资源，未认证用户不能访问网络资源。
- 支持 IPv6。

注意事项

- 设置免认证的网络资源和设置无需认证用户共享资源，这两者各自都不能超过 1000 个。此外，实际可用数量也会受其它安全功能占用表项的影响而减少。因此，如果需要设置的地址较多，请尽量使用网段的方式进行设置。
- **http redirect direct-site** 是配置免认证访问地址，**http redirect** 是配置 Web 认证的服务器地址。从效果上看，用这两条命令配置的地址都是可以不用认证就直接访问的，但是实际用途是不一样的，因此实际使用时建议避免用 **http redirect direct-site** 配置 Web 认证服务器地址，否则会引起误解。
- IPv6 场景下，需要配置放行本地链路地址，否则会导致设备无法学习到终端的 mac 地址。

配置方法

- 可选配置
- 如果需要让未认证用户能够访问网络中的资源，使用本命令实现。

检验方法

- 配置免认证网络资源
- 未认证用户 PC 直接访问该资源，访问成功

相关命令

设置免认证网络资源范围

【命令格式】 **http redirect direct-site** { *ipv6-address* | *ipv4-address* [*mask* | **arp** | *port-number*... }

【参数说明】 *Ipv6-address*：免认证网络 IPv6 地址

Ipv4-address：免认证网络 IPv4 地址

mask：免认证网络 IPv4 地址掩码

port-number：免认证四层端口，该参数最多允许输入 8 次。取值范围为 1~65535。免认证网络的描述信息

【命令模式】 全局配置模式

【使用指导】 ARP 放行请优先采用直通 ARP 命令

配置举例

设置免认证网络资源范围

【配置方法】

- 设置免认证的网络资源范围 192.168.0.0/16

```
Hostname(config)# http redirect direct-site 192.168.0.0 255.255.0.0
```

- 设置连续免认证的范围为 10.0.0.1 到 12.0.0.1

```
Hostname (config)# http redirect direct-site range 10.0.0.1 12.0.0.1
```

【检验方法】

- 查看配置是否成功

```
Hostname(config)# show web-auth direct-site
Direct sites:
  Address         Mask            ARP Binding Group       Description
  --------------- --------------- ----------- ----------- -------------
  192.168.0.0     255.255.0.0     Off         N/A         N/A
Hostname(config)#
Hostname(config)#show web-auth direct-site range
Direct site Ranges: 1
  Start Address   End Address     Group          Description
  --------------- --------------- -------------- -------------
10.0.0.1         12.0.0.1        N/A            N/A
Hostname(config)#
```

1.4.20 设置直通 ARP 资源范围

配置效果

- 开启 ARP CHECK 或类似功能时，用户的 ARP 学习受控，导致用户无法学到网关及其他设备的 ARP，影响用户使用。此时可以通过设置直通 ARP 资源来对指定地址的 ARP 学习报文进行放行

注意事项

- 对于开启 ARP Check 情况，需要将二层接入设备下联 PC 的网关设置为直通 ARP 资源。需要注意以下问题：
  对同一地址/网段同时设置直通网站和直通 ARP 时，命令会自动进行合并；如果直通网站的配置没有指定 ARP 选项，合并后该选项会自动增加。
- 对于开启 ARP Check 情况，若下联 PC 的出口地址不是网关地址，也需要将出口地址设置为直通 ARP 资源。若存在多个出口地址，这些出口地址也需要设置为直通 ARP 资源。

配置方法

- 可选配置
- 如果设备启用了 ARP CHECK 功能，那么需要对免认证的网络资源范围和网关配置 ARP 直通。

检验方法

- 配置直通 ARP 资源
- 未认证用户 PC 上清空 ARP 缓存(Windows 执行命令 arp -d)
- 未认证用户 PC 执行 ping 直通 ARP 资源
- 未认证用户 PC 查看 ARP 缓存(Windows 执行命令 arp -a)，学习到直通 ARP 资源的 ARP 地址

相关命令

↘ 设置直通 ARP 资源范围

【命令格式】 **http redirect direct-arp** *ip-address* [*ip-mask*]

【参数说明】 *ip-address*：免认证网络 ip 地址

ip-mask：免认证网络掩码

【命令模式】 全局配置模式

【使用指导】 -

配置举例

↘ 设置直通 ARP 资源范围

【配置方法】
- 设置直通 ARP 资源范围 192.168.0.0/16

```
Hostname(config)# http redirect direct-arp 192.168.0.0 255.255.0.0
```

【检验方法】
- 查看配置是否成功

```
Hostname(config)# show web-auth direct-arp
Direct arps:
  Address         Mask
  --------------- ---------------
  192.168.0.0     255.255.0.0
Hostname(config)#
```

1.4.21 设置无需认证用户范围

配置效果

- 如果用户属于无需认证用户范围，那么该用户不需要通过 Web 认证，也能访问所有可达的网络资源。缺省时，没有设置无需认证用户，所有用户都必须先通过 Web 认证，才能访问网络资源。
- 支持 IP 地址和 MAC 地址设置。

注意事项

无

配置方法

- 可选配置
- 要设置无需认证用户时，可进行该配置。

检验方法

- 配置用户为无需认证用户
- 用户直接访问网络，访问成功

相关命令

↘ 设置无需认证用户 IP 范围

【命令格式】 **web-auth direct-host** { *ipv4-address* [*ip-mask*] [**arp**] [**port** *interface-name*] | *ipv6-address* | *mac-address* | **range** *starip-address endip-address* } [**description** *description-str*] [**group** *group-name*] [**permit-ipv6**]

【参数说明】 *ipv4-address*：免认证用户 IPv4 地址
ipv6-address：免认证用户 IPv6 地址
ip-*mask*：免认证用户 IPv4 地址掩码
interface-name：接口名
mac-address：免认证用户 mac 地址
startip-address: 连续免认证用户的起始 ip
endip-address: 连续免认证用户的结束 ip
group-name: 免认证用户的所属的组
description-str: 免认证用户的描述信息

【命令模式】 全局配置模式

【使用指导】 arp 字段用来设置放行 arp 报文，当开启 ARP-CHECK 功能时需要配置
配置 port 字段后，用户仅在所配置接口下时免认证功能生效，在其余接口上不生效

配置举例

↘ 设置无需认证用户 IP 范围

【配置方法】
- 设置无需认证用户 IP 范围

```
Hostname(config)# web-auth direct-host 192.168.197.64
```

- 设置连续免认证用户的范围为 10.0.0.1 到 12.0.0.1

```
Hostname(config)# web-auth direct-host range 10.0.0.1 12.0.0.1
```

【检验方法】
- 查看配置是否成功

```
Hostname(config)# show web-auth direct-host
Direct hosts:
  Address         Mask            Port           ARP Binding   Group      Description
  --------------- --------------- -------------- ------------- ---------- ------------
  192.168.197.64  255.255.255.255                Off           N/A        N/A
Hostname(config)#
Hostname# show web-auth direct-host range
Direct host Ranges: 1
  Start Address    End Address      Port       Group        Description
  ---------------- ---------------- ---------- ------------ -----------
  10.0.0 . 1       12.0.0.1         Gi0/2      N/A          N/A
```

1.4.22 设置在线用户信息的更新时间间隔

配置效果

- 接入/汇聚设备维护着在线用户信息，设备需要定时地更新在线用户信息，包括在线时间等，以监控在线用户使用网络资源的情况，比如：用户的在线时间大于或等于在线时限，该用户会被停止使用网络。

注意事项

- 用户更新时间必须配置为 60 的倍数，否则实际配置自动向上取最近的 60 倍数来生效。

配置方法

- 可选配置
- 要设置无需认证用户时，可进行该配置。

检验方法

- 配置用户信息更新时间
- 超过更新时间间隔后，查看在线用户信息

相关命令

↘ 设置在线用户信息更新时间间隔

【命令格式】 **web-auth update-interval** *seconds*

【参数说明】 *seconds*：信息更新时间间隔，单位为秒。取值范围 30-3600。默认为 180 秒

【命令模式】 全局配置模式

【使用指导】 如果要恢复更新时间间隔为默认值，在全局配置模式下，使用 **no web-auth update-interval**

配置举例

↘ 设置已认证用户信息的更新时间间隔为 60 秒

【配置方法】
- 设置已认证用户信息的更新时间间隔为 60 秒

```
Hostname (config)# web-auth update-interval 60
```

【检验方法】
- 查看配置是否成功

```
Hostname(config)# show run | include web-auth update-interval
web-auth update-interval 60
```

1.4.23 配置 Portal 检测

配置效果

- 定时检测 Portal 服务器是否可用，如果不可用，切换到备用 Portal 服务器。

- 对于二代认证有两种检测方法，第一种方法，是设备构造 Portal 协议报文发给 Portal 服务器，并通过检测 Portal 服务器是否响应来确定服务器是否可用。第二种方法，是设备向服务器发 ping 报文，通过是否响应 ping 报文来检测。由于部分服务器或者中间网络会过滤 ping 报文，因此大部分情况下是选择方法一作为检测方法，只有在极个别环境，比如有特殊规范要求的，才选择 ping 检测。而一代认证和 Clearpass 认证，采用 connect 服务器端口是否可达的方式来判断服务是否可用。
- 针对二代认证的第一种检测方法，检测算法为每隔 **interval** 时间进行一次检测，每次检测最多发 **retransmit** 个报文，如果些报文服务器都不响应，则判断服务器不可用，否则可用。每个报文的超时时间由参数 **timeout** 决定。一代认证同样支持此配置。
- 该功能对一代 Web 认证、Clearpass 认证、二代 Web 认证都有效。
- 如果配置了多个个 Portal 服务器，则称为主备 Portal。

注意事项

- 需要配置多个 Portal 服务器，这样检测到错误时才能实现切换。
- 为避免检测算法冲突，两种检测方法只能选一个，同时配置会引起检测冲突或者检测结果不准确。
- 配置时如果使用一代认证，系统会自动选择一代检测方式，二代认证同样会自动选择二代认证的检测方式

配置方法

- 可选配置。
- 配置多个一，二代 Web 认证的 Portal 模板。

检验方法

- 配置两个二代或一代 Portal 服务器模板，第一个模板指向的服务器不可用，第二个模板指向的服务器可用。
- 控制台出现 Portal 不可用的 log 时，用户打开浏览器登录认证，被重定向到第二个 Portal 服务器。

相关命令

↘ 设置 Portal 检测

【命令格式】 **web-auth portal-check** [**interval** *intsec* [**timeout** *tosec*] [**retransmit** retries]

【参数说明】 *intsec*：检测周期，默认 10 秒

tosec：报文超时时间，默认 5 秒

intsec：超时重传次数，默认 3 次

【命令模式】 全局配置模式

【使用指导】 大部分网络环境中只有一台服务器，无需配置此功能，如果有多台，参数不宜配置太小，否则会出现短时间内设备发出太多报文，影响设备性能。

本命令不能与 **fmt** 命令同时使用。如果要使用 **fmt** 命令配置 URL 格式，请使用 **web-auth ping** 命令进行 Portal

服务器检测。

↘ 配置 ping 检测的周期和超时重传次数

【命令格式】 **web-auth ping** [**interval** *minutes*] [**retry** *times*]

【参数说明】 *minutes*：检测周期，默认 1 分钟

times：超时重传次数，默认 3 次

【命令模式】 全局配置模式

【使用指导】 大部分网络环境中只有一台服务器，无需配置此功能，如果有多台，参数不宜配置太小，否则会出现短时间内设备发出太多报文，影响设备性能。

本命令需要结合 **fmt** 命令使用。使用前必须先通过 **fmt** 命令配置报文的 URL 格式，否则本命令功能不生效。

配置举例

↘ 设置 Portal 检测

【配置方法】

- 配置 Portal 检测

```
Hostname(config)# web-auth portal-check interval 20 timeout 2 retransmit 2
```

【检验方法】

- 查看配置是否成功

```
Hostname(config)# show running-config
...
web-auth portal-check interval 20 timeout 2 retransmit 2
...
```

1.4.24 配置 Portal 逃生

配置效果

- 当配置的 Portal 服务器都不可用时，新接入网络的用户免认证。

注意事项

- 需要同时配置 Portal 检测功能。
- 如果配置了多个 Portal 服务器，则需要所有 Portal 服务器均不可用时逃生功能才会生效。
- 此功能仅针对 Portal 服务器，不针对 RADIUS 服务器。

配置方法

- 可选配置。
- 配置 Portal 检测功能。
- 配置 Portal 逃生功能。
- 可配置 nokick 属性。

检验方法

- 配置一个 Portal 服务器，服务器不可用。
- 配置 Portal 检测功能和逃生功能。
- 设备检测出 Portal 不可用后，用户接入网络，无需认证即可访问网络。

相关命令

↘ 设置 Portal 逃生

【命令格式】 **web-auth portal-escape** [**nokick**]

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 如果网络中有一些关键业务不允许中断，可以配置此功能，这样当 Portal 服务器出现异常时，可以保证业务不受影响。配置此功能要同时配置 Portal 检测功能。

配置 nokick 属性后，逃生生效时，对已在线用户不做下线处理。删除该属性，会下线在线用户。

配置举例

↘ 设置 Portal 逃生

【配置方法】
- 配置 Portal 逃生

```
Hostname(config)# web-auth portal-escape
```

【检验方法】
- 查看配置是否成功

```
Hostname(config)# show running-config
...
web-auth portal-escape
...
```

1.4.25 配置 DHCP 地址核查

配置效果

- 只有通过 DHCP 分配地址的终端才允许进行认证。

注意事项

- 需要配置 DHCP SNOOPING 功能。
- 仅支持 IPv4。
- 仅支持二代 Web 认证和内置 Portal Web 认证。
- 网络部署时明确用户使用 DHCP 获得 IP 地址，不存在静态 IP 地址混用的情况，否则会影响静态 IP 地址的用户。
- 如果有少数用户需要用静态 IP 地址，可以通过配置直通地址放行，对这些用户不认证。
- 如果部分接口或者接口下部分 vlan 才需要进行 dhcp 地址核查，需要关闭全局 dhcp 地址核查，再在各个接口下分别配置需要生效的 vlan 范围。

配置方法

- 可选配置。
- 配置 DHCP SNOOPING。
- 配置地址核查。

检验方法

- 配置 DHCP 地址核查功能。
- 终端配置静态地址，该地址未经 DHCP 服务器分配。
- 终端连接到网络，无法认证。

相关命令

↘ 基于全局设置 DHCP 地址核查

【命令格式】 **web-auth dhcp-check**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 网络部署时指定用户需要使用 DHCP 获取 IP 地址上网，配置此功能有助于屏蔽一些私设 IP 地址的用户认证上网。

↘ 基于接口设置 DHCP 地址核查

【命令格式】 **web-auth dhcp-check** { **vlan** [*vlan-list*] }
【参数说明】 *vlan-list*：接口下需要 dhcp 地址核查功能的 vlan 范围
【命令模式】 接口配置模式

【使用指导】 如果部分接口或者接口下部分 vlan 才需要进行 dhcp 地址核查，需要关闭全局 dhcp 地址核查，再在各个接口下分别配置需要生效的 vlan 范围。

配置举例

↘ 设置 DHCP 地址核查

【配置方法】 ● 基于全局配置 DHCP 地址核查

```
Hostname(config)# web-auth dhcp-check
```

【配置方法】 ● 基于接口配置 DHCP 地址核查

```
Hostname(config-if-TenGigabitEthernet 3/1)# web-auth dhcp-check vlan 1,3-4
```

【检验方法】 ● 查看配置是否成功

```
Hostname(config)# show running-config
...
web-auth dhcp-check
...
interface TenGigabitEthernet 3/1
web-auth dhcp-check vlan 1,3-4
...
```

1.4.26 配置关闭链路检测

配置效果

- 终端通过 Web 认证后，断开链路，认证表项不会被删除，终端再次连接到网络时，只要 IP 地址不变，即可继续上网。
- 该功能适用于有经常性移动办公的场所，或者部署了无线的 Web 认证但是所在场所无线信号不好。

注意事项

- 如果终端是通过 DHCP 获取 IP 地址，且 DHCP 地址池小于网络用户数，则不适合开该功能，因为当一个终端离开时，其 IP 地址有可能会被其它人获取，这会导致用户信息错误。
- 如果关闭链路检测，则用户下线只能通过点击页面主动下线、服务器踢下线、设备配置低流量检测下线。因此配置此功能时，建议要同时开启低流量检测功能，具体参考 SCC 的配置手册。
- 对于无线环境，建议关闭链路检测功能，同时开启低流量检测，主要是因为无线连接受信号干扰导致掉线比较突出，关闭链路检测有助于提高无线体验。

配置方法

- 可选配置。
- 配置 Web 认证。
- 关闭链路检测功能。

检验方法

- 配置二代 Web 认证并关闭链路检测功能。
- 终端连接到网络，认证通过，断开网络，再再连接到网络，在 IP 地址不变的情况下，无需认证即可访问网络。

相关命令

↘ 关闭链路检测功能

【命令格式】 **no web-auth sta-leave detection**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 无线环境或者有经常需要移动办公的有线环境可以关闭链路检测，同时需要开启低流量检测功能。

配置举例

↘ 关闭链路检测功能

【配置方法】

- 关闭链路检测功能

```
Hostname(config)# no web-auth sta-leave detection
```

【检验方法】

- 查看配置是否成功

```
Hostname(config)# show running-config
...
no web-auth sta-leave detection
...
```

1.4.27 配置关闭 Portal 协议扩展

配置效果

- 通过开关此功能来支持锐捷 Portal 服务器和标准中国移动规范的 Portal 服务器。
- 对接标准中国移动 Portal 规范服务器时，可选择多种重定向 URL 格式，用于兼容不同服务器。

注意事项

- 仅支持二代 Web 认证。
- 二代 Web 认证扩展了中国移动 Portal 协议，实际使用时需要根据服务器情况选择是否运行在扩展模式。
- 如果 Portal 服务器为锐捷产品，则使用默认值，即扩展模式，如果 Portal 服务器为标准中国移动 Portal 服务器，则需要关闭扩展。
- 如果 Portal 服务器为标准中国移动 Portal 服务器产品，由于中国移动 Portal 规范存在多种 url 重定向格式，需要依据实际的 Portal 服务器支持情况选择格式。

配置方法

- 可选配置。
- 根据服务器类型选择是否关闭扩展。
- 如果关闭扩展，根据服务器的支持情况选择合适的重定向 url 格式。

检验方法

- 分别选择锐捷 Portal 服务器和中国移动标准 Portal 服务器作为二代 Web 认证的服务器。
- 终端连接到网络，均可正常认证并访问网络。

相关命令

↘ 关闭 Portal 协议扩展

【命令格式】 **no web-auth portal extension**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 环境中使用的是中国移动标准 Portal 服务器，如果是锐捷 Portal 服务器，则需要开启扩展。

配置举例

↘ 关闭 Portal 协议扩展

【配置方法】
- 关闭 Portal 协议扩展

```
Hostname(config)# no web-auth web-auth portal extension
Hostname(config)# http redirect url-fmt ext1
```

【检验方法】
- 查看配置是否成功

```
Hostname(config)# show running-config
```

【配置方法】
- 关闭 Portal 协议扩展

```
Hostname(config)# no web-auth web-auth portal extension
Hostname(config)# http redirect url-fmt ext1
```

【检验方法】
- 查看配置是否成功

```
...
no web-auth web-auth portal extension
http redirect url-fmt ext1
...
```

1.4.28 配置黑白名单

配置效果

- 白名单可以使用户在认证前可以访问部分网络资源，黑名单可以使用户在认证后无法访问部分网络资源。
- 黑白名单支持端口、url、ip 等信息过滤的过滤。

注意事项

- 黑白名单只支持配置最多 1000 条。
- 如果以域名形式配置，需要配置设备的 DNS 功能，使得设备可以正确解析 IP 地址。
- 部分域名有多 IP，仅支持一个域名最多 8 个 IP 地址。

配置方法

- 可选配置。
- 配置 DNS 域名解析。
- 配置黑白名单。

检验方法

- 配置一条白名单和一条黑名单。
- 终端认证前可以访问白名单地址。
- 终端认证后无法访问黑名单地址。

相关命令

↘ 配置黑白名单

【命令格式】 **web-auth acl** { **black-ip** *ip* | **black-port** *port* | **black-url** *name* | **white-url** *name* }

【参数说明】 *ip*：黑名单 ip 地址

port：黑名单端口

name：黑白名单的 url

【命令模式】 全局模式配置模式，无线上黑名单还支持无线安全模式

【使用指导】 允许认证前访问采用白名单，禁止认证后访问采用黑名单。

配置举例

配置认证模式

【配置方法】

- 配置黑白名单

```
Hostname(config)# web-auth acl black-ip 192.168.1.2
Hostname(config)# web-auth acl white-url www.Hostname.com.cn
```

【检验方法】

- 查看配置是否成功

```
Hostname(config)# show running-config
...
web-auth acl black-ip 192.168.1.2
web-auth acl white-url www.Hostname.com.cn
...
```

1.4.29 配置防抖动计费

配置效果

- 如果设备配置了防抖功能或者低流量下线 ,通过此功能决定是否将防抖时间或者低流量检测时间计算入计费报文中的在线时长。此功能用于减小计费误差，如果环境中的计费策略允许不扣除这些检测时间，可以配置该功能。如果配置了防抖或者低流量检测，则默认情况防抖时间或者低流量检测时间不计如在线时长。

注意事项

- 设备需支持防抖功能或者低流量检测功能。
- 终端的下线动作是由链路长时间断开或者低流量检测导致。
- 由于防抖功能和流量检测功能可以同时开启，防抖计费只对其中先触发下线的生效，比如配置防抖时间 5 分钟，配置流量检测 10 分钟，如果终端离开网络，则防抖功能优先出发了 Web 认证将用户下线，因此计费报文中的在线时长只扣除 5 分钟。

配置方法

- 可选配置。
- 配置计费功能。
- 配置防抖功能或者低流量检测功能。
- 配置防抖计费功能。

检验方法

- 终端认证上线，再通过低流量下线。
- 捕获设备发出的计费结束报文，确认其中的在线时间没有扣除流量检测时长。

相关命令

↘ 配置防抖动计费

【命令格式】 **web-auth accounting jitter-off**

【参数说明】 -

【命令模式】 全局模式配置模式

【使用指导】 根据服务器计费策略选择是将防抖时长或者低流量检测时长计算入计费结束报文的在线时长中，默认是不计入。

配置举例

↘ 配置防抖计费

【配置方法】
- 配置防抖计费

```
Hostname(config)# web-auth accounting jitter-off
```

【检验方法】
- 查看配置是否成功

```
Hostname(config)# show running-config
...
web-auth accounting jitter-off
...
```

1.4.30 配置 Portal 通信端口

配置效果

- 配置后设备与 Portal 服务器通信的源端口为所配置端口。

注意事项

- 端口只能配置一个。

配置方法

- 配置指定端口为 portal 通信口。

检验方法

- 开启 web 受控后，认证时服务器上抓包，认证报文源 IP 为指定端口的 IP。

相关命令

↘ 配置通信端口

【命令格式】 **ip portal source-interface** *interface-type interface-num*

【参数说明】 *interface-type*：端口类型

interface-num：端口号

【命令模式】 全局模式配置模式。

【使用指导】 无

配置举例

↘ 配置 portal 通信端口

【配置方法】

- 使用聚合口当作 portal 通信口地址。

```
Hostname(config)# ip portal source-interface Aggregateport 1
```

【检验方法】

- 查看配置是否成功

```
Hostname(config)# show running-config
ip portal source-interface Aggregateport 1
```

1.4.31 配置宁盾系统兼容 URL

配置效果

- 配置 web 重定向 URL 支持宁盾系统。

注意事项

- 无。

配置方法

↘ 配置宁盾系统兼容 URL 参数

- 全局模式下配置 post 参数。

【命令格式】 **web-auth dkey-compatible url-parameter** *string*
【参数说明】 *string*：post 参数内容
【命令模式】 全局配置模式
【使用指导】 无。

检验方法

- 配置后执行重定向，重定向 URL 中会加入 post 参数。

配置举例

↘ 配置宁盾系统兼容 URL 参数

【配置方法】
- 配置兼容参数。

```
Hostname(config)# web-auth dkey-compatible url-parameter login
```

【检验方法】
- 查看配置是否成功

```
Hostname(config)# show running-config
...
web-auth dkey-compatible url-parameter login
```

1.4.32 配置多 Portal 映射

配置效果

- 配置不同网段用户使用不同 Portal 进行认证。

注意事项

- 可配置多个映射，用户不在映射范围内，会使用默认 Portal 进行认证。

- 不同的映射范围不可相互覆盖。

配置方法

配置多 Portal 映射

- 全局模式下配置映射参数。

【命令格式】 **web-auth portal** { **eportalv1** | **eportalv2** | **iportal** | **wifidog** | **wechat** | **cpweb** | *name* } **ip-mapping** *ipv4 mask*

【参数说明】 *name*：使用的模板名称

ipv4：使用该模板的 ip 网段

mask：使用该模板的 ip 掩码

【命令模式】 全局配置模式

【使用指导】 无。

检验方法

- 配置后使用不同网段进行认证，用户可以使用不同的 Portal 进行认证。

配置举例

配置多 Portal 映射

【配置方法】

- 配置映射网段。

```
Hostname(config)# web-auth portal eportalv2 ip-mapping 192.168.1.0 255.255.255.0
Hostname(config)# web-auth portal eportalv1 ip-mapping 192.168.2.0 255.255.255.0
Hostname(config)# web-auth portal eportalv2
```

【检验方法】

- 查看配置是否成功

```
Hostname(config)# show running-config
...
web-auth portal eportalv2
web-auth portal eportalv2 ip-mapping 192.168.1.0 255.255.255.0
web-auth portal eportalv1 ip-mapping 192.168.2.0 255.255.255.0
```

1.4.33 配置内置 Web 认证 NAT 功能

配置效果

- 配置内置 Web 认证支持 NAT。

注意事项

- 只对内置 Web 认证有效。

配置方法

↘ 配置 NAT 支持功能

- 全局模式下开启功能。

【命令格式】 **iportal nat enable**
【参数说明】 无
【命令模式】 全局配置模式
【使用指导】 无。

检验方法

- 配置后 NAT 场景可以使用内置 Web 认证。

配置举例

↘ 配置 NAT 功能支持

【配置方法】
- 配置 NAT 功能支持。

```
Hostname(config)# iportal nat enable
```

【检验方法】
- 查看配置是否成功

```
Hostname(config)# show running-config
...
iportal nat enable
```

1.4.34 配置内置 Web 认证重传次数

配置效果

- 配置内置 Web 认证 http 连接重传次数。

注意事项

- 重传次数只对内置页面推送的 http 连接有效。

配置方法

↘ 配置内置 Web 认证 http 重传次数

- 全局模式下配置参数。

【命令格式】 **iportal retransmit** *count*
【参数说明】 *count*：重传次数
【命令模式】 全局配置模式
【使用指导】 无。

检验方法

- 配置后发送内置 Web 认证请求后，断开连接，设备可以发出重传。

配置举例

↘ 配置重传次数

【配置方法】
- 配置重传次数。

```
Hostname(config)# iportal retransmit 5
```

【检验方法】
- 查看配置是否成功

```
Hostname(config)# show running-config
...
iportal retransmit 5
```

1.4.35 配置内置 Web 认证服务选择

配置效果

- 配置内置 Web 认证使用的服务类型。

注意事项

无。

配置方法

↘ 配置内置 Web 认证服务类型

- 全局模式下配置服务类型。

【命令格式】 **iportal service** [**internet** *internet-name*] [**local** *local-name*]
【参数说明】 *internet-name*：使用的外部服务名称
local-name：使用的内部服务名称
【命令模式】 全局配置模式
【使用指导】 无

检验方法

无。

配置举例

配置服务类型

【配置方法】
- 配置服务类型。

```
Hostname(config)# iportal service local local-srv
```

【检验方法】
- 查看配置是否成功

```
Hostname# show running-config
...
iportal service local local-srv
```

1.4.36 配置内置 Web 认证用户 UA 字段

配置效果

- 配置用户的 UA 字段对应的终端名称。

注意事项

- 用终端识别功能代替该功能，命令已经无效。

配置方法

配置内置 Web 认证用户 UA 字段

- 全局模式下配置 UA 字段。

【命令格式】 **iportal user-agent** *ua-name* **type mobile** *ua-string*

【参数说明】 *ua-name*：UA 字段对应的名称
ua-string：UA 字符串内容
【命令模式】 全局配置模式
【使用指导】 无。

检验方法

无。

配置举例

无。

1.4.37 配置内置 Web 认证导入页面包

配置效果

- 配置内置 Web 认证能导入页面包

注意事项

- 无

配置方法

↘ 配置内置 Web 认证导入页面包

【命令格式】 **web-auth import-page-suite tftp:***path*
【参数说明】 *path*：文件路径
【缺省配置】 无
【命令模式】 特权模式
【使用指导】 先打开 tftp 服务器，服务器上放置需要导入的文件。

检验方法

- 导入页面包后，在模板模式下执行 page-suite 命令查看是否成功

配置举例

↘ 配置导入页面包

【配置方法】
- 配置导入页面包。

```
Hostname# web-auth import-page-suite tftp://10.104.8.66/custom.zip
```

【检验方法】
- 查看配置是否成功

```
Hostname#show running-config
```

1.4.38 配置 Web 记账方法列表

配置效果

- 在全局配置模式下，指定 Web 认证的记账方法。

注意事项

- 不配置会使用默认记账方法进行记账。

配置方法

↘ 配置记账方法

- 全局配置模式下配置记账方法。

【命令格式】 **web-auth accounting** { **v2** | **intra** | **cpweb** } { **default** | *name* }
【参数说明】 *name*：使用的记账列表名称
【命令模式】 全局配置模式
【使用指导】 无。

检验方法

- 配置查看记账报文目的地址。

配置举例

↘ 配置记账方法

【配置方法】
- 配置记账方法。

```
Hostname(config)# web-auth accounting v2 test
Hostname(config)# web-auth accounting intra test
Hostname(config)# web-auth accounting cpweb test
```

【检验方法】

- 查看配置是否成功

```
Hostname# show running-config
...
web-auth accounting v2 test
web-auth accounting intra test
web-auth accounting cpweb test
```

1.4.39 配置 Web 认证方法列表

配置效果

- 在全局配置模式下，指定 Web 认证方法。

注意事项

- 不配置会使用默认认证方法进行认证。

配置方法

↘ 配置认证方法

- 全局配置模式下配置认证方法。

【命令格式】 **web-auth authentication** { **v2** | **intra** | **cpweb** } { **default** | *name* }
【参数说明】 *name*：使用的认证方法列表名称,最大长度为 63 个字符
【命令模式】 全局配置模式
【使用指导】 无。

检验方法

- 配置查看认证报文目的地址。

配置举例

↘ 配置认证方法

【配置方法】

- 配置认证方法。

```
Hostname(config)# web-auth authentication v2 test
Hostname(config)# web-auth authentication intra test
Hostname(config)# web-auth authentication cpweb test
```

【检验方法】

- 查看配置是否成功

```
Hostname# show running-config
...
web-auth authentication v2 test
web-auth authentication intra test
web-auth authentication cpweb test
```

1.4.40 页面包定制规范

配置效果

- 使用内置 Porttal Web 认证时，允许定制自有 Web 页面，比如显示特定 LOGO 或者显示广告等。
- 单个也面包支持两套页面，以适配终端屏幕大小，比如小屏幕的移动终端。

注意事项

- 必须严格按照规范制作页面，避免新也面包无法使用。
- 页面包的文件数量不得超过 50 个（含 PC 版页面文件和移动终端版页面文件），每个页面文件名不得长于 32 字节
- 新也面包必须下载到./portal 目录下，新也面包名字不能默认页面包重叠，否则会覆盖默认页面包。
- 部分设备没有默认也面包，使用内置 Portal Web 认证时必须根据规范制定也面包并导入 FLASH。

配置方法

无

检验方法

- 用户连接到网络，打开浏览器认证，弹出定制页面。

相关命令

↘ 页面文件命名规范

页面文件名（含扩展名）	用途
login.htm	登录页面
online.htm	在线页面（用户登录成功之后的页面）
offline.htm	下线页面
login_mobile.htm	移动终端登录页面
online_mobile.htm	移动终端在线页面（用户登录成功之后的页面）
offline_mobile.htm	移动终端下线页面

↘ 登录页面制作规范

根据页面命名规范，PC 版的登录页面名称为 login.htm，移动终端版的登录页面名称为 login_mobile.htm。登录页面的内容规范说明如下：

- 表单元素

登录页面必须包含一个表单，提交方式固定为 POST。下面以 PC 版登录页面为例（移动终端版的类似），假设 PC 版的登录页面存放在/portal 目录下，相应的表单 html 编码大致如下：

```
<form method="post" action="/portal/login.htm">
...
</form>
```

一般来说，表单中需要包括以下页面元素：

1. 用户名文本框，用于给用户输入用户名，ID 为 username。(必选)
2. 密码文本框，用于给用户输入密码信息(不明文显示密码)，ID 为 password。(必选)
3. 登录按钮，用于 POST 方法提交表单。(必选)。
4. 显示认证失败原因的页面标签，ID 为 errormsg。(可选)，如果用户不关心登录失败的原因，那么登录页面中可以不包含该 errormsg 标签；如果想把认证失败的原因呈现给认证用户，那么就必须包括有这么一个可显示认证失败原因的区域，并且在页面加载的时候以 GET 的方式发送请求，请求内容为 errormessage，请求的结果将在 errormsg 标签中呈现。向服务器请求 errormsg 内容的脚本大致如下（以下只是一个例子，不代表是唯一写法）：

```
< script language=”javascript”>
//向服务器请求 errormessage 内容
function requestErrorMsg() {
    var _errormsg=document.getElementById(“errormsg”);
      var script=document.createElement(“script”);
script.src=”errormessage”+location.search;
_errormsg.appendChild(script);
}
```

```
//页面加载时需要调用 init 函数
function init() {
……
requestErrorMsg();
}
……
</script>
```

- 表单提交：

表单提交时，提交格式为 username=[AAAA]&password=[BBBB]&lang=[CCCC]，各个填充字段的含义如下：

[AAAA]：为用户在用户名文本框中填写的用户名。(必选)

[BBBB]：为用户在密码文本框中填写的密码。(必选)

[CCCC]：为用户当前的语言环境（可选），值 1 表示简体中文环境，2 表示英文环境，其他暂未定义，默认为简体中文，当语言环境是英文时，提交表单时需要将语言环境信息一并提交，否则象认证失败原因信息返回的是中文，与用户的实际语言环境就不一致了。

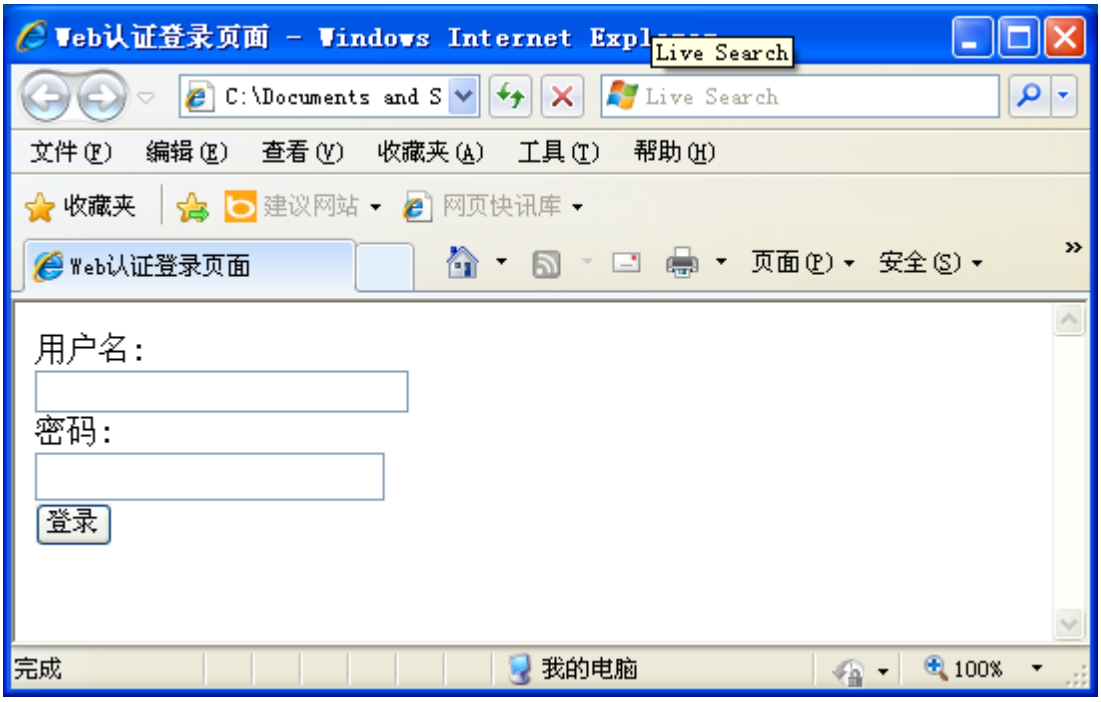
因此，登录页面的表单中至少要有 username 和 password 以及登录按钮这三个输入域（ 即 input 标签），如果登录页面有中英文环境，表单中还可能会有一个 lang 输入域，该域一般是不可见的。

综上所述，可以得到登录页面最基本的 HTML 源码大致如下：

```
<html>
  <head>
  <title>Web 认证登录页面</title>
  </head>
  <script language=”javascript”>
   // 请求认证错误信息，如果认证成功或登录页面首次加载错误信息为空，不显示
   function requestErrorMsg() {
   var _errormsg=document.getElementById(“errormsg”);
     var script=document.createElement(“script”);
script.src=”errormessage”+location.search;
_errormsg.appendChild(script);
   }

function init() {
……
```

```
requestErrorMsg();
}

// 用户点登录按钮时执行的脚本。
function login() {
   document.getElementById('loginForm').action = "./login.htm"+location.search;
       document.getElementById('loginForm').submit();
       window.onbeforeunload = null;
       window.onunload = null;
}
……

</script>
   <body onload="init()">
      <form method="post" id=”loginForm”>
      用户名:<br>
      <input type="text" name="username" accesskey="u" size="25" value="" id="usrename">
      <br>
      密码:<br>
      <input type="password" name="password" accesskey="p" size="25"
            value="" id="password">
      <br>
<input type="button" onclick=”login()” value="登录" id=”loginButton”>
<input type="hidden" name="lang" value="" id="lan">
       <p name=”errormsg” id="errormsg"></p>
      </form>
   </body>
</html>
```

根据上述的定制，内置 Portal 服务器向用户推送的登录页面样式大致如下：



通过上述的定制过程，登录页面已经具备了所有必要的元素，但这样的页面没有什么美观可言。用户可以在此基础之上进行美化，以及添加一些其他功能。比如添加背景、设置各种页面元素的样式等。

在线页面制作规范

在线页面的作用是告诉用户已经通过认证，可以正常使用网络。PC 版的在线页面名称为 online.htm，移动终端版的登录页面名称为 online_mobile.htm。

- 表单元素

在线页面必须包含一个表单，该表单的作用是来提交下线请求的，因此，表单中也需要有一个下线按钮，表单的提交方式固定为 POST。下面以 PC 版的在线页面为例（移动终端版的类似），假设 PC 版的在线页面存放在/portal 目录下，相应的表单 html 编码大致如下：

```
<form method="post" action="/portal/online.htm">
...
</form>
```

在线页面的表单中需要包括以下页面元素：

1. ID 为 username 的页面标签，用于呈现用户的用户名信息。(可选)
2. ID 为 userip 的页面标签，用于呈现用户的 IP 地址。(可选)
3. ID 为 usermac 的页面标签，用于呈现用户的 MAC 地址。(可选)
4. ID 为 ssid 的页面标签，用于呈现用户所在的 SSID。(可选)
5. ID 为 availtime 的页面标签，用于呈现用户可用时长。(可选)

6. 下线按钮，用户想下线时可以点击该按钮，用于请求下线页面。(必选)

在线页面加载时需要通过 GET 方法向服务器请求用户信息，包括用户名、用户 IP 地址、用户 MAC 地址、关联的 SSID 以及可用时长，URI 为 getonlineinfo，为此需要实现 html 中 body 的 onload 方法。大致如下（只是举一个例子，不是唯一实现）：

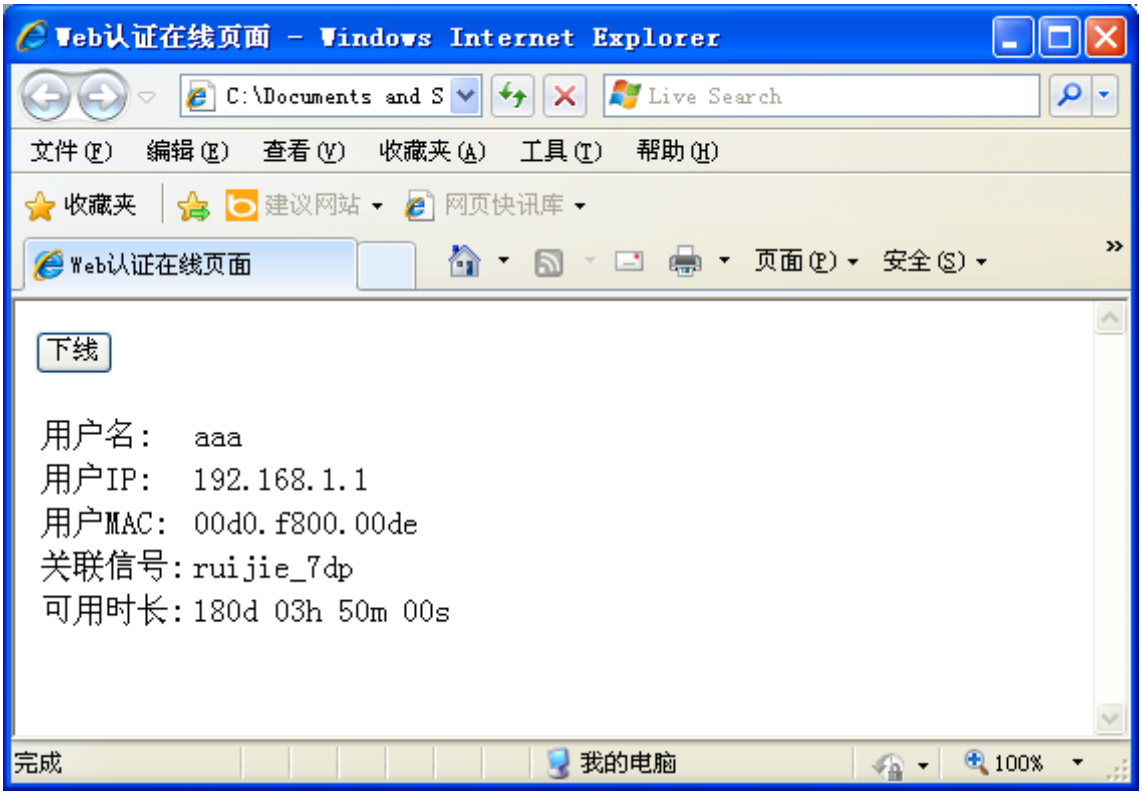
```
<script language="javascript">
    // 获取在线用户信息,包括用户名、IP、MAC、关联信号、可用时长
    function requestOnlineInfo() {
        var _availTime=document.getElementById("availtime");
        var script=document.createElement(“script”);
        script.src="getonlineinfo"+location.search;
        _availTime.appendChild(script);
    }

    function init() {
        requestOnlineInfo();
    }
  </script>
<body onload="init()">
……
</body>
```

综上所述，可以得到在线页面最基本的 HTML 源码大致如下：

```
<html>
  <head>
  <title>Web 认证在线页面</title>
  </head>
  <script language="javascript">
    // 获取在线用户信息,包括用户名、IP、MAC、关联信号、可用时长
    function requestOnlineInfo() {
        var _availTime=document.getElementById("availtime");
        var script=document.createElement(“script”);
```

```
            script.src="getonlineinfo"+location.search;
            _availTime.appendChild(script);
        }

        function init() {
            requestOnlineInfo ();
        }
        // 用户点下线按钮时执行的脚本，请求的 URI 为 offline.htm。
        function logout() {
            document.logoutform.action = "./offline.htm"+location.search;
            document.logoutform.submit();
            window.onbeforeunload = null;
            window.onunload = null;
        }

    </script>

    <body onload="init()">
        <form method="post" action="/portal/offline.htm" id="logoutform">
        <input type="button" onclick="logout()" value="下线" id="logoutButton">
        </form>
        <table>
        <tr><td>用户名:</td><td id="username"></td></tr>
        <tr><td>用户 IP:</td><td id="userip"></td></tr>
        <tr><td>用户 MAC:</td><td id="usermac"></td></tr>
        <tr><td>关联信号:</td><td id="ssid"></td></tr>
        <tr><td>可用时长:</td><td id="availtime"></td></tr>
        </table>
    </body>
</html>
```

根据上述的定制，内置 Portal 服务器向用户推送的登录页面样式大致如下：



上述的在线页面就已具备了所有必要的元素。用户可以在此基础之上进行美化，以及添加一些其他功能。比如添加背景、设置各种页面元素的样式等。

下线页面制作规范

当用户在在线页面上点击下线按钮后就会引出下线页面，其作用是告诉用户已经下线成功，如果要使用网络，需要重新进行认证。PC 版的在线页面名称为 offline.htm，移动终端版的登录页面名称为 offline_mobile.htm。

页面元素：

1. ID 为 timeused 的页面标签，用于呈现用户已用时长的信息。(可选)

在下线页面的加载过程中，需要向服务器发送 GET 请求获取已经用时长信息，请求的 URI 为 getofflineinfo。为此需要实现 html 中 body 的 onload 方法。获取已用时长信息时，可以动态创建 script，比如要发送的字段信息包含在 script 的 src 中，script.src="getofflineinfo"。大致如下（只是举一个例子，不是唯一实现）：

```
<script language="javascript">
    // 获取已用时长信息
    function requestOfflineInfo() {
    var _timeused =document.getElementById("timeused");
    var script=document.createElement("script");
    script.src="getofflineinfo"+location.search;
```

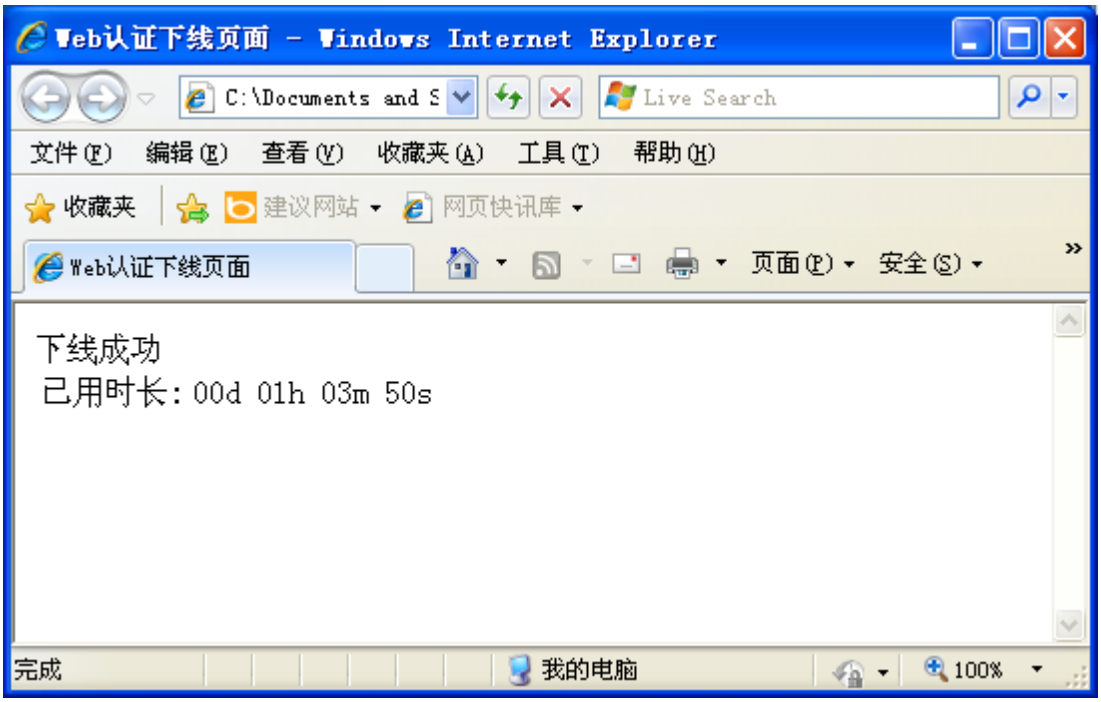
```
        _timeused.appendChild(script);
 }

 function init() {
        requestUserInfo();
 }
</script>
<body onload="init()">
……
</body>
```

下线页面整体最基本的 HTML 源码大致如下：

```
<html>
   <head>
   <title>Web 认证下线页面</title>
   </head>
   <script language="javascript">
      // 获取已用时长信息
      function requestOfflineInfo() {
        var _timeused=document.getElementById("timeused");
        var script=document.createElement("script");
        script.src="getofflineinfo"+location.search;
        _timeused.appendChild(script);
 }

 function init() {
        requestOfflineInfo();
 }
   </script>
```

```
<body onload="init()">
    下线成功<br>
<table>
<tr><td>已用时长:</td><td id="timeused"></td></tr>
</table>
</body>
</html>
```

根据上述的定制，内置 Portal 服务器向用户推送的下线页面样式大致如下

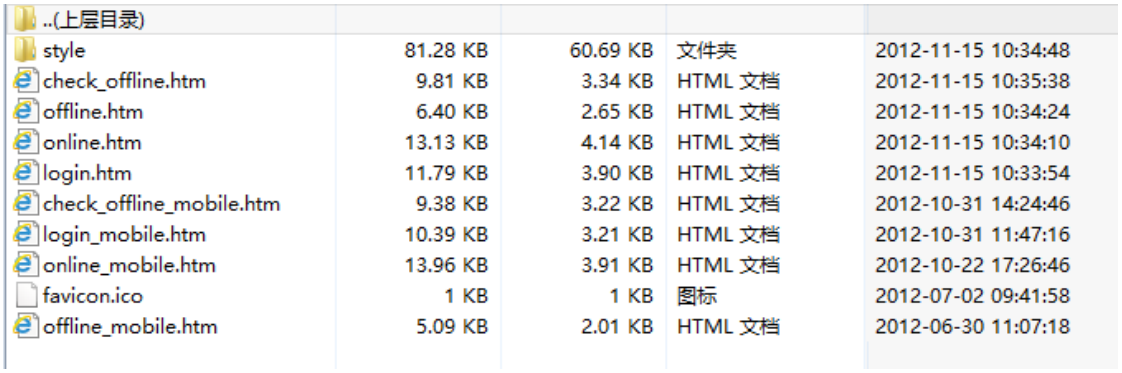


上述的下线页面就已具备了所有必要的元素。用户可以在此基础之上进行美化，以及添加一些其他功能。比如添加背景、设置各种页面元素的样式等

↘ 页面打包规范

按照本规范定制好页面后，需要将所有页面和页面元素文件打包，上传到设备，再使用该页面包。有关压打包的相关规范如下：

1. 按照本规范定制好页面后，需要将所有页面和页面元素文件（如图片文件、样式表文件等）打包成 ZIP 格式的压缩包，比如 portal1_page.zip。
2. 页面包中可以包含目录。如下图所示，portal1_page.zip 中就包含有 style 目录。目录里包含了页面的 css 文件及其他图片资源文件。



..(上层目录)				
style	81.28 KB	60.69 KB	文件夹	2012-11-15 10:34:48
check_offline.htm	9.81 KB	3.34 KB	HTML 文档	2012-11-15 10:35:38
offline.htm	6.40 KB	2.65 KB	HTML 文档	2012-11-15 10:34:24
online.htm	13.13 KB	4.14 KB	HTML 文档	2012-11-15 10:34:10
login.htm	11.79 KB	3.90 KB	HTML 文档	2012-11-15 10:33:54
check_offline_mobile.htm	9.38 KB	3.22 KB	HTML 文档	2012-10-31 14:24:46
login_mobile.htm	10.39 KB	3.21 KB	HTML 文档	2012-10-31 11:47:16
online_mobile.htm	13.96 KB	3.91 KB	HTML 文档	2012-10-22 17:26:46
favicon.ico	1 KB	1 KB	图标	2012-07-02 09:41:58
offline_mobile.htm	5.09 KB	2.01 KB	HTML 文档	2012-06-30 11:07:18

页面包打包之后，再通过 TFTP 等工具上传到设备的 flash:/portal/zip/目录下。此后要为 Portal 服务器指定使用该页面包（也就是将 Portal 服务器与页面包关联），为 Portal 服务器指定页面包的具体过程，请参考 Web 认证相关的配置指南。为 Portal 服务器指定页面包之后，可以看到 flash:/portal/ext_zip/目录下会生成一个与压缩包同名的目录，比如，压缩包名称为 portal1_page.zip，就会生成 flash:/portal/ext_zip/protal1_page/此目录，压缩包中的内容会自动解压到该目录下。之后，Portal 服务器可以实现为用户推送用户指定的 Web 认证页面。

配置举例

↘ 配置定制也面包

【配置方法】

- 配置定制也面包

```
Hostname(config.tmplt.iportal)#page-suit Hostnamepage
```

【检验方法】

- 查看配置是否成功

```
Hostname#show web-auth template
Webauth Template Settings:
-----------------------------------------------------------
  Name:      iportal
  Page-suit:    Hostnamepage
  Advertising url:  default
  Advertising mode: online-popup
  Type:      Intral Portal
  Acctmlist:default
  Authmlist:default
```

1.4.41 升级兼容性说明

配置效果

- 部分配置命令在 11.X 系列软件上做了优化，格式上有所变化，具体参考后面的说明。
- 10.X 系列软件可以实现平滑升级，不会出现功能丢失的情况，但是升级后部分旧命令的显示会转化为新命令。
- 在 11.X 系列软件上对这部分旧命令执行 no 操作会提示不支持，需要用新的格式执行 no 操作。

注意事项

无

配置方法

- 部分格式变化的命令建议使用新格式配置。

检验方法

- 10.X 软件版本升级到 11.X 软件版本不会出现功能丢失，同时显示以及保存的格式采用新命令。
- 新格式命令的功能效果和旧命令一致。

相关命令

↘ 配置一代 Web 认证的 Portal 服务器 ip 地址

【命令格式】 **http redirect** *ip-address*

【参数说明】 *ip-addressl*：一代 Web 认证的 ePortal 服务器 ip 地址

【命令模式】 全局配置模式

【使用指导】 11.X 版本首先会将该命令转化为一个 eportalv1 模板 ,再用模板模式下的 ip 命令配置和显示服务器的 ip 地址。

↘ 配置一代 Web 认证的 Portal 服务器资源地址

【命令格式】 **http redirect homepge** *url*

【参数说明】 *url*：一代 Web 认证的 ePortal 服务器资源地址

【命令模式】 全局配置模式

【使用指导】 11.X 版本首先会将该命令转化为一个 eportalv1 模板，再用模板模式下的 url 命令配置和显示服务器地址。

↘ 配置 portal-server

【命令格式】 **portal-server** [**eportal1** | **eportalv2**]

【参数说明】 **eportav1**：一代 Web 认证的 portal 信息

eportav2：二代 Web 认证的 portal 信息

【命令模式】 全局配置模式

【使用指导】 11.X 版本首先会将该命令转化为一个 eportalv1 或者 eportalv2 模板，再用对应的信息填充，portal-server 主要参数包括服务器 ip 地址和 url 地址，会被模板中的 ip 命令和 url 命令替代。

↘ 配置接口 Web 认证受控

【命令格式】 **web-auth port-control**
【参数说明】 无
【命令模式】 接口配置模式
【使用指导】 11.X 版本会将该命令转化 web-auth enable <type>此处的 type 是指一代或者二代，默认是一代。

配置仅 ip 绑定模式

【命令格式】 **web-auth port-control ip-only-mode**
【参数说明】 无
【命令模式】 接口配置模式
【使用指导】 11.X 版本首先会将该命令转化为一个 eportalv1 模板或者 eportalv2 模板，取决于实际配置。再用模板模式下的 bindmode 命令配置和显示服务器绑定模式。

配置基于 vlan 的 Web 认证功能

【命令格式】 **web-auth allow-vlan** *list*
【参数说明】 *list*：设置支持基于 VLAN 的 Web 认证的 VLAN 列表为 list
【命令模式】 全局配置模式
【使用指导】 11.X 版本会将该命令转化为一个 scc 免认证 vlan 命令。

显示一代 Web 认证配置信息

【命令格式】 **show http redirect**
【参数说明】 无
【命令模式】 特权模式
【使用指导】 11.X 版本该旧命令不可用，改为 show web-auth template。

显示端口受控信息

【命令格式】 **show web-auth port-control**
【参数说明】 无
【命令模式】 特权模式
【使用指导】 11.X 版本该旧命令不可用，改为 show web-auth control。

配置举例

配置一代 Web 认证

【配置方法】
- 产品运行 10.X 版本并且已经配置了一代 Web 认证服务器 ip

```
Hostname(config)# http redirect 192.168.197.64
```

- 产品升级到 11.X 版本

【检验方法】
- 升级后 **show running-config**，配置已更新为新命令格式

```
Hostname# show running-config
web-auth template eportalv1
  Ip 192.168.197.64
!
```

1.4.42 配置 RADIUS 逃生功能开关

配置效果

- 配置 RADIUS 逃生功能开关，打开时，当 RADIUS 服务器挂掉，Web 认证用户依然可以认证通过上网。

注意事项

- 该功能需要和 RADIUS 检测命令配合使用。

配置方法

↘ 配置 RADIUS 逃生功能开关

【命令格式】 **web-auth radius-escape**
【参数说明】 无
【命令模式】 全局配置模式
【使用指导】 无

检验方法

- 在配置了 RADIUS 检查命令后，配置好 Web 认证 RADIUS 服务器，在 RADIUS 服务器挂掉后，用一个错误的用户名和密码认证通过。

配置举例

↘ 配置 RADIUS 逃生开关命令

【配置方法】
- 打开 RADIUS 逃生开关功能。

```
Hostname(config)# web-auth radius-escape
```

【检验方法】
- 查看配置是否成功

```
Hostname# show running-config
```

1.4.43 配置内置 logo 替换功能

配置效果

- 配置内置 logo 替换功能，可以替换内置 portal 所有页面的 logo

注意事项

- Logo 上传目录为/data/portal/logo，名字固定为 free_login_logo.jpg

配置方法

配置内置 logo 替换功能

【命令格式】 **web customized-logo enable**
【参数说明】 无
【命令模式】 全局模式
【使用指导】 无

检验方法

- 配置开启此功能后，上传图片，查看内置 portal 的页面的 logo 是否有被替换掉。

配置举例

配置 logo 替换开关命令

【配置方法】
- 打开 logo 替换功能开关功能。
- 非必须配置，在有需要替换内置认证页面的 logo 时开启

```
Hostname(config)# web customized-logo enable
```

【检验方法】
- 查看配置是否成功

```
Hostname# show running-config
```

1.4.44 配置无线 Web 认证降噪功能

配置效果

- 用户重定向过程访问某个目的 ip 的次数等于配置的次数，就把用户后续访问该目的 ip 的报文都丢弃不处理，达到降噪目的。

注意事项

- 需根据网络环境和实际需求配置降噪策略的两个参数(老化时间和命中次数),以免用户的正常报文被当作噪声报文丢弃，无法重定向。

配置方法

↘ 配置无线 Web 认证降噪功能

【命令格式】 **web-auth noise** [**aging** *agmin*] [**hit** *times*]

【参数说明】 *agmin*：噪声表项老化时间，默认 1 分钟

times：噪声判定规则：访问某个目的 ip 达到 *times* 次，就认为是噪声，默认 3 次

【命令模式】 全局配置模式

【使用指导】 无

检验方法

- 配置开启此功能后，重定向过程，用户访问某个目的 ip 次数到达配置的次数后，再次访问该目的 ip 就不会被重定向。等到噪声表项老化时间到期后，再访问该目的 ip 又可以被重定向。

配置举例

↘ 配置无线 Web 认证降噪功能

【配置方法】

- 配置无线 Web 认证降噪功能参数。

```
Hostname(config)# web-auth noise aging 1 hit 3
```

【检验方法】

- 查看配置是否成功

```
Hostname# show running-config
```

1.4.45 配置微信认证 IOS 自动弹框控制命令

配置效果

- 微信认证 (微信关注认证，微信连 WiFi 等) 场景下，IOS 终端能够自动弹窗并且显示 WiFi 信号 (结合微信流量放行功能，IOS 终端未上线前可以使用微信 App ）。

注意事项

- 需配合微信流量放行（ web-ctrl free-auth weixin ）功能使用。
- 该功能开启，会降低重定向性能。

- 如果有放行苹果网站的相关配置，该功能开启无效。例如：下例任何一个配置都会导致该功能无效，

  web-ctrl free-auth iphone

  web-auth acl white-url http://www.apple.com.cn

  web-auth acl white-url http://captive.apple.com

配置方法

↘ 配置微信认证 IOS 自动弹框控制命令

【命令格式】 **http redirect adapter ios**
【参数说明】 无
【命令模式】 全局配置模式
【使用指导】 无

检验方法

- 配置开启此功能后，微信认证（微信关注认证，微信连 WiFi 等）场景下，IOS 终端能够自动弹窗并且显示 WiFi 信号（结合微信流量放行功能，IOS 终端未上线前可以使用微信 App）。

配置举例

↘ 配置微信认证 IOS 自动弹框控制命令

【配置方法】
- 打开 IOS 自动弹框控制开关功能。
- 非必须配置，在微信认证场景（有配置 web-ctrl free-auth weixin）下配置有效。

```
Hostname(config)# http redirect adapter ios
```

【检验方法】
- 查看配置是否成功

```
Hostname# show running-config
```

1.4.46 配置微信认证无感知命令

配置效果

- 微信认证（微信关注认证，微信连 WiFi 等）场景下，用户第二次关联 SSID，无需经过认证流程，服务器直接设置上线。

注意事项

- 要开启 ip dhcp snooping 功能，该功能才生效。

配置方法

↘ 配置微信认证无感知命令

【命令格式】 **web-auth sta-perception enable**
【参数说明】 无
【命令模式】 全局模式或者无线安全配置模式
【使用指导】 无

检验方法

- 配置开启此功能后，微信认证（微信关注认证，微信连 WiFi 等）场景下，用户第二次关联 SSID，无需经过认证流程，服务器直接设置上线。

配置举例

↘ 配置微信认证无感知命令

【配置方法】
- 打开微信认证二次无感知开关功能。
- 非必须配置，在微信认证场景下配置有效。

```
Hostname(config)# web-auth sta-perception enable
```

【检验方法】
- 查看配置是否成功

```
Hostname# show running-config
```

1.4.47 配置 ipfix 上传流量开关

配置效果

- 配置 ipfix 上传流量开关，打开时，使用 ipfix 封装流量报文上传到服务器。

注意事项

- 该功能需要和 ipfix 功能配合使用。

配置方法

↘ 配置 ipfix 上传流量开关

【命令格式】 **web-auth acct-mtehod ipfix**
【参数说明】 无
【命令模式】 全局模式
【使用指导】 无

检验方法

- 配置后认证上线，此时流量通过 ipfix 报文封装发送到服务器。

配置举例

↘ 配置 ipfix 开关命令

【配置方法】
- 打开 ipfix 开关功能。

```
Hostname(config)# web-auth acct-method ipfix
```

【检验方法】
- 查看配置是否成功

```
Hostname# show running-config
```

1.4.48 配置 Portal 协议 0x05 号属性透传功能

配置效果

- 配置 Portal 协议 0x05 号属性透传功能，开启后 Web 认证支持下面两个场景的属性透传功能：
- 与中国移动 Portal 协议对接时，Web 认证会把错误标识封装到 0x05 号属性（ErrID）中并透传到 Portal Server。
- 与华为 Portal 2.0 协议对接时，Web 认证会把 RADIUS 等第三方鉴权设备的提示信息封装到 0x05 号属性（TextInfo）中并透传到 Portal Server。

注意事项

- 该功能默认是关闭的。

配置方法

- 可选配置
- 需要中国移动 Portal 协议规定的 ErrID（0x05）属性时配置。
- 需要华为 Portal 2.0 协议规定的 TextInfo（0x05）属性时配置。

相关命令

配置 Portal 协议 0x05 号属性透传功能

【命令格式】 **web-auth portal-attribute 5**
【参数说明】 无
【命令模式】 全局模式
【使用指导】 一般在特定 Portal Server 需要设备上传错误标识（ErrID）时开启。

【命令格式】 **web-auth portal-attribute textinfo**
【参数说明】 无
【命令模式】 全局模式
【使用指导】 一般在特定 Portal Server（使用华为 Portal 2.0 协议规范）需要设备上传 RADIUS 等第三方鉴权设备的提示信息（TextInfo）时开启。

检验方法

- 开启此命令后，在回应 Portal 的 ack 报文中会带上 0x05 号属性。

配置举例

配置 Portal 协议 0x05 号属性透传功能

【配置方法】
- 配置 0x05 号属性透传功能。

```
Hostname(config)# web-auth portal-attribute 5
```

或者：

```
Hostname(config)# web-auth portal-attribute textinfo
```

【检验方法】
- 查看配置是否成功

```
Hostname(config)#show running-config
```

1.4.49 配置 Portal 认证账号唯一性检查功能

配置效果

- 配置 Portal 认证账号唯一性检查功能，开启后 Web 认证会检查用户认证请求的账号信息，如果发现该账号已经有其他用户在线，则直接应答 ACK_AUTH 带 ErrCode 2 给 Portal Server。有些 Portal Server 收到该种应答后，就会给用户推送“终端抢占”提示信息。

注意事项

- 该功能默认是关闭的。

配置方法

- 可选配置
- Portal Server 需要给用户推送“终端抢占”提示信息时配置。

相关命令

↘ 配置 Portal 认证账号唯一性检查功能

【命令格式】 **web-auth portal-valid unique-name**
【参数说明】 无
【命令模式】 全局配置模式
【使用指导】 一般在特定 Portal Server 需要给用户推送“终端抢占”提示信息时开启。

检验方法

- 开启此命令后，如果发现相同账号已经有其他用户在线，则直接应答 ACK_AUTH 带 ErrCode 2 给 Portal Server。

配置举例

↘ 配置 Portal 认证账号唯一性检查功能

【配置方法】
- 配置认证账号唯一性检查功能。

```
Hostname(config)# web-auth portal-valid unique-name
```

【检验方法】
- 查看配置是否成功

```
Hostname# show running-config
```

1.4.50 配置无线 WiFiDog 一键配置

配置效果

- WiFiDog 的模板信息，端口受控，ios 弹窗，无感知配置可以集中一条命令配置生效。

注意事项

- 一键配置的 no 操作只能删除模板信息和受控端口，不对全局配置生效。

配置方法

配置无线 WiFiDog 一键配置

- 可选配置

【命令格式】 **web-auth wifidog-template** *template-name* **wlan-range** *wlanid-start wlanid-end* **portal-ip** *portal-ip-address* **nas-ip** *nas-ip-address* **url** *url-string* [**gateway-id** *gwid-string*] [**perception**]

【参数说明】 *template-name*：模板名称

wlanid-start：开启受控的 wlan 范围开始

wlanid-end：开启受控的 wlan 范围结束

portal-ip-address：Portal 服务器的地址

nas-ip-address：设置 WiFiDog 的设备接入服务 ip，用于服务器向此 ip 发起通讯

url-string：Portal 服务器的认证页面地址

gwid-string：只适用于热备和 VAC 场景，一般配置成主 AC 的设备序列号。单机场景不需要配置

perception：配置无感知功能

【命令模式】 全局配置模式

【使用指导】 在开始一键配置之前，必须先创建 wlansec，否则无法受控配置成功。

检验方法

- 使用 show running-config 查看配置是否正常。

配置举例

配置无线 WiFiDog 一键配置

【配置方法】

- 无线 WiFiDog 一键配置

```
Hostname(config)# web-auth wifidog-template aaa wlan-range 1 32 portal-ip 172.21.6.78 nas-ip 192.168.197.227 url http://172.21.6.78/auth/wifidogAuth
```

【检验方法】

- 使用 **show running-config** 命令，可以查看是否配置成功。

1.4.51 配置无线微信连 WiFi 一键配置

配置效果

- 微信连 WiFi 的模板信息，端口受控， ios 弹窗，无感知配置可以集中一条命令配置生效。

注意事项

- 一键配置的 no 操作只能删除模板信息和受控端口，不对全局配置生效。

配置方法

↘ 配置无线微信连 WiFi 一键配置

- 可选配置

【命令格式】 **web-auth wechat-template** *template-name* **wlan-range** *wlanid-start wlanid-end* **portal-ip** *portal-ip-address* **nas-ip** *nas-ip-address* [**nas-id** *nas-id-str*] [**perception** | **ios-adapter**]

【参数说明】 *template-name*：模板名称

wlanid-start：开启受控的 wlan 范围开始

wlanid-end：开启受控的 wlan 范围结束

portal-ip-addr：Portal 服务器的地址
nas-ip-addr：设置微信连 WiFi 的设备接入服务 ip，用于服务器向此 ip 发起通讯
nas-id-str：只适用于热备和 VAC 场景，一般配置成主 AC 的设备序列号。单机场景不需要配置
perception：配置无感知功能
ios-adapter：配置自动弹窗功能

【命令模式】 全局配置模式

【使用指导】 在开始一键配置之前，必须先创建 wlansec，否则无法受控配置成功。

检验方法

- 使用 show running-config 查看配置是否正常。

配置举例

↘ 配置无线微信连 WiFi 一键配置

【配置方法】
- 无线微信连 WiFi 一键配置

```
Hostname(config)# web-auth wechat-template aaa wlan-range 1 32 portal-ip 172.21.6.78 nas-ip 192.168.197.227
```

【检验方法】
- 使用 **show running-config** 命令，可以查看是否配置成功。

1.4.52 配置 AP 的 NAS-PORT-ID

配置效果

- 广东移动要求配置每个 AP 的 NAS-PORT-ID，配置之后在 Portal 报文和 RADIUS 报文中会携带给 Portal 和 RADIUS 服务器

注意事项

- 只能基于单个 AP 配置。

配置方法

↘ 配置 AP 的 NAS-PORT-ID

- 可选配置

【命令格式】 **nas-port-id** *string*
【参数说明】 *string*：给 ap 分配的 nas-port-id 名字
【命令模式】 AP 配置模式
【使用指导】 只能基于单个 AP 配置，用 no nas-port-id 取消配置。

检验方法

- 使用 show ap-config running 查看配置是否正常。

配置举例

↘ 配置 AP 的 NAS-PORT-ID

【配置方法】
- NAS-PORT-ID 的配置

```
Hostname(config)# ap-config ap740
Hostname(config-ap)# nas-port-id guangdongyidong
```

【检验方法】
- 使用 **show ap-config running** 命令，可以查看是否配置成功。

1.4.53 配置认证用户名自动添加域信息功能

配置效果

- 二代和内置 Portal 认证如果在模板中配置了域信息，则会自动在原始用户名之后添加上配置的域信息，并发给 AAA 服务器。

注意事项

- 域信息最多支持 63 字节，当前处理会直接将 Portal 传来的用户名之后补齐配置的域信息，如果用户名+域信息的长度超过 253 的话，会将域信息截断。

配置方法

- 可选配置。
- Portal 服务器不支持自动添加域名但是 RADIUS 服务器要求携带域信息时，需要配置自动添加域信息的功能。

检验方法

- show running-config 显示配置命令正常

相关命令

↘ 配置欠费页面地址

【命令格式】 **domain** *domain-string*

【参数说明】 *domain-string*：需要添加的域信息字符串

【命令模式】 Web 认证模板配置模式

【使用指导】 自动添加域信息之后，若 Portal 服务器传递的用户名为 host，配置的域信息为@wifi，则最终发给服务器的用户名为 host@wifi。

配置举例

↘ 配置欠费页面地址

【配置方法】

- 指定 eportalv2 模板自动添加域信息为@wifi” 。

```
Hostname(config.tmplt.eportalv2)# domain @wifi
```

【检验方法】

- 查看配置是否成功

```
Hostname(config)# show running-config
web-auth template eportalv2
 domain @wifi
Hostname(config)#
```

1.4.54 配置 app 认证模板

配置效果

- 配置该模板后，可以实现微信、企业微信和钉钉认证。

注意事项

- 进入模板配置模式后，配置命令和微信认证命令相同。

配置方法

- 可选配置。
- 要配置微信、企业微信和钉钉认证时，可进行该配置。

检验方法

- 通过 show running-config 查看配置是否正常
- 进行微信、企业微信和钉钉认证时，能正常认证

相关命令

↘ 创建 app 认证模板

【命令格式】 **web-auth template** { **app** | *portal-name* **app** }

【参数说明】 自定义的 Portal 服务器名

【命令模式】 全局配置模式

【使用指导】 app 为默认的 app 认证模板

↘ 应用 app 认证模板

【命令格式】 **web-auth portal** { **app** | *name* }

【参数说明】 自定义的模板名

【命令模式】 全局配置模式或者无线安全配置模式

【使用指导】 app 为默认的 app 认证模板

配置举例

↘ 配置 app 认证

【配置方法】

- 在网络设备上配置 app 认证模板
- 在网络设备上配置服务器的 ip 和 service-url 地址
- 在网络设备上配置与服务器进行通信的加密密钥(ruijie)
- 在网络设备上配置设备的 ip 地址
- 在网络设备上对 WLANSEC1 应用模板并开启 app 认证功能

```
Hostname# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)# web-auth template app
Hostname(config.tmplt.app)# ip 192.168.197.79
Hostname(config.tmplt.app)# service-url wmc.ruijie.com.cn
Hostname(config.tmplt.app)# key ruijie
Hostname(config.tmplt.app)# nas-ip 1.1.1.1
Hostname(config.tmplt.app)# exit
Hostname(config)# wlansec 1
Hostname(config-wlansec)# web-auth portal app
Hostname(config-wlansec)# webauth
```

【检验方法】

- Web 认证配置是否成功

```
Hostname# show running-config
web-auth template app
 ip 192.168.197.79
 service-url wmc.ruijie.com.cn http://192.168.197.79:8080/eportal/index.jsp
 key ruijie
 nas-ip 1.1.1.1
!...
wlansec 1
 web-auth portal app
 webauth
!
```

1.4.55 配置 ISE 认证功能

配置效果

未认证用户能够被重定向到认证页面并完成认证

注意事项

无

配置方法

配置 Portal 服务器

- 必须配置，要成功应用 Web 认证功能，必须设置并应用 Portal 服务器。
- 当设备发现未认证用户试图通过 HTTP 访问网络资源时，设备将用户的访问请求重定向到指定的 Portal 认证页面，通过认证页面，引导用户向认证服务器发起认证。Portal 服务器地址将被设置为一个特殊的免认证的网络资源，未认证用户可以直接与这个地址进行 HTTP 通讯。

配置认证成功后的响应方式

- 可选配置。
- 根据用户需求进行配置。

配置认证失败后的响应方式

- 可选配置
- 根据用户需求进行配置。

配置设备解析认证请求的方式

- 可选配置。
- 根据对接的服务器要求进行配置。

配置认证成功后是否弹窗主动下线页面

- 可选配置。
- 根据用户需求进行配置。

配置设备 IP

- 必须配置，缺省情况下无配置。
- 该 IP 是给用户访问的，因此应该配置一个用户能访问到设备 IP.

配置设备端口

- 必须配置，缺省情况下无配置。
- 该端口是给用户访问的，不能与内置、Web 网管配置的端口冲突.

配置终端发起认证使用的 url

- 必须配置，缺省情况下为 http://ip:port/login，其中 ip 和 port 分别为设备 IP 和设备端口。

在端口上开启 Web 认证功能

- 必须配置。
- 当 Web 认证功能基于端口开启时，默认情况下，端口未开启 Web 认证功能，此时这个端口下所连接的用户不进行 Web 认证。

检验方法

- 未认证用户被要求认证
- 已认证用户可以正常使用网络

相关命令

开启 AAA 功能

【命令格式】 **aaa new-model**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 AAA 的方法列表等命令需要在功能开启后才能输入

配置 AAA 中 Web 认证方法列表

【命令格式】 **aaa authentication cpweb** { **default** | *list-name* } *method1* [*method2*...]
【参数说明】 *list-name*：方法列表名
method1：方法 1
method2：方法 2
【命令模式】 全局配置模式
【使用指导】 ISE 认证复用 clearpass 认证方法，使用方式同 clearpass 认证

创建模板

【命令格式】 **web-auth template cpweb**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 ISE 认证复用 clearpass 的认证模板，使用方式同 clearpass 认证

配置服务器 IP

【命令格式】 **ip** *ip-address*
【参数说明】 *ip-address*：Portal 服务器的地址
【命令模式】 Web 认证模板配置模式
【使用指导】 -

配置服务器 URL

【命令格式】 **url** *url-string*

【参数说明】 *url-string*：Portal 服务器的认证页面地址

【命令模式】 Web 认证模板配置模式

【使用指导】 登录 ISE 服务器，在 portal 页面中点击“Portal test URL”，获取 portal 页面的 url，其格式如：https://192.168.197.79:8443/portal/PortalSetup.action?portal=401e25d0-2e02-11e8-ba71-0050568 72c7f，将 url 中的符号”?”替换成”#”。另外在该页面的 Authentication Success Settings 选项下配置 URL 为任意有效页面，默认配置为 http://www.cisco.com，防止出现设备未认证成功，跳出登录成功页面。

配置设备 IP

【命令格式】 **web-auth auth-server ip** *ip-address*

【参数说明】 *ip-address*：设置 ISE 认证的设备接入服务 ip，用于服务器向此 ip 发起通讯

【命令模式】 全局配置模式

【使用指导】 配置的设备接入服务 ip 不能够被设置成直通地址。

配置接入服务 ip 为设备 IP 时会导致此认证模板下的终端访问此 ip 时被设备拦截并转发给服务器，从而不能访问设备的 Web 管理界面。

如有此认证模板下的终端直接访问此 ip 对此设备进行管理的需求，可将此接入服务 ip 设置为一个未使用的虚拟服务 ip，如 1.1.1.1，2.2.2.2 等。

配置设备端口

【命令格式】 **web-auth auth-server http** [**port** *port-number*]

【参数说明】 *port-number*：ISE 认证终端发起认证时使用的 tcp 端口

【命令模式】 全局配置模式

【使用指导】 该参数为终端发起认证使用的 tcp 端口，不能和内置、Web 网管使用的端口冲突。

配置终端发起认证使用的 url

【命令格式】 **web-auth auth-server submit-url** *url-string*

【参数说明】 *url-string*：ISE 认证终端发起认证时使用的 url 地址

【命令模式】 全局配置模式

【使用指导】 该参数为终端发起认证使用的 url 地址，必须以 http://开头。

配置接口上启用 Web 认证

【命令格式】 **webauth**

【参数说明】 -

【命令模式】 接口配置模式

【使用指导】 -

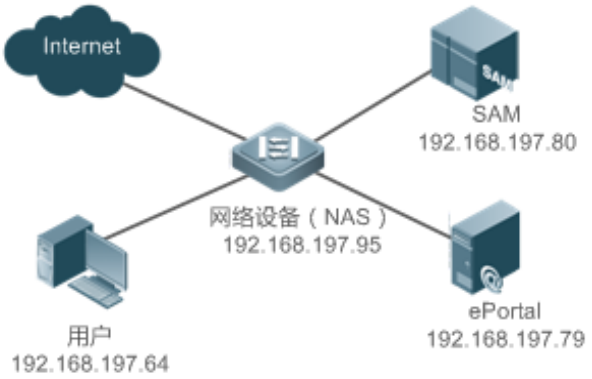
配置举例

以下配置举例，仅介绍与 Web 认证相关的配置。

ISE 认证

【网络环境】

图 1-17



【配置方法】

- 在网络设备上设置认证服务器的 IP 地址
- 在网络设备上设置认证页面的主页地址
- 在网络设备上设置设备 IP 地址
- 在网络设备上设置设备的端口
- 在网络设备上设置终端认证的 url
- 在网络设备上对 wlan 10 开启 Web 认证功能

```
Hostname# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)# web-auth auth-server http port 8082
Hostname(config)# web-auth auth-server ip 1.1.1.1
Hostname(config)# web-auth auth-server submit-url http://1.1.1.1:8082/login
Hostname(config)# web-auth template cpweb
Hostname(config.tmplt.cpweb)# ip 192.168.197.79
Hostname(config.tmplt.cpweb)# url
https://192.168.197.79:8443/portal/PortalSetup.action#portal=401e25d0-2e02-11e8-ba71-005056872c
7f
Hostname(config.tmplt.cpweb)# exit
Hostname(config)# wlansec 10
Hostname(config-wlansec)# web-auth portal cpweb
Hostname(config-if-range)# webauth
Hostname(config-if-range)# exit
```

【检验方法】

Web 认证配置是否成功

```
Hostname# show running-config
...
web-auth auth-server ip 1.1.1.1
```

```
web-auth auth-server http
web-auth auth-server submit-url http://1.1.1.1:8082/login
web-auth template cpweb
 ip 192.168.197.79
 url
https://192.168.197.79:8443/portal/PortalSetup.action#portal=401e25d0-2e02-11e8-ba71-005056872c
7f
...
wlansec 10
 web-auth portal cpweb
 webauth
```

```
Hostname# show web-auth control
Port                        Control  Server Name           Online User Count
 -------------------------- -------- --------------------- -----------------
 wlansec 10                  On       cpweb                 0                   ...
```

```
Hostname# show web-auth template
Webauth Template Settings:
-------------------------------------------------------------
  Name:           cpweb
  Type:           cpweb
  Ip:             192.168.197.79
  Url:
https://192.168.197.79:8443/portal/PortalSetup.action#portal=401e25d0-2e02-11e8-ba71-005056872c
7f
```

常见错误

没配置设备 IP 导致无法重定向。

1.4.56 配置角色重定向模板

配置效果

角色绑定重定向模板，则属于该角色的终端访问网络将被重定向。

注意事项

无

配置方法

配置重定向 Portal 模板

- 必须配置，要为角色绑定重定向 Portal 模板，需要先配置一个可用的重定向 Portal 模板。
- 当设备发现网络访问受限角色下的用户试图通过 HTTP 访问网络资源时，设备将用户的访问请求重定向到指定的 Portal 页面。Portal 服务器地址将被设置为一个特殊的免认证的网络资源，访问受限角色下的用户可以直接与该地址进行 HTTP 通讯。

为角色绑定重定向 Portal 模板

- 必须配置。
- 角色与重定向模板绑定，相应角色访问网络才会被重定向。

检验方法

- 受限角色的用户访问网络被重定向
- 不受限角色的用户可以正常使用网络

相关命令

创建模板

【命令格式】 **web-auth template** *template-name* **rdweb**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 无

配置服务器 IP

【命令格式】 **ip** *ip-address*
【参数说明】 *ip-address*：Portal 服务器的地址
【命令模式】 Portal 模板配置模式
【使用指导】 -

配置服务器 URL

【命令格式】 **url** *url-string*
【参数说明】 *url-string*：Portal 服务器的重定向页面地址
【命令模式】 Portal 模板配置模式
【使用指导】 -

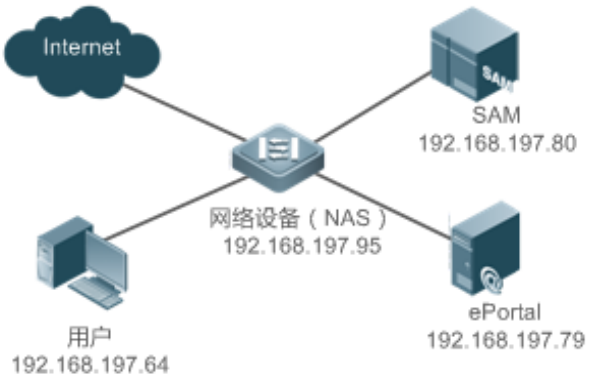
配置举例

以下配置举例，仅介绍与角色相关的配置。

配置角色绑定重定向模板

【网络环境】

图 1-18



【配置方法】

- 在网络设备上设置重定向模板 rdweb 的重定向服务器的 IP 地址
- 在网络设备上设置重定向模板的 Portal 页面主页地址
- 配置角色 limit 绑定重定向模板 rdweb

```
Hostname# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)# web-auth template rdweb
Hostname(config.tmplt.rdweb)# ip 192.168.197.79
Hostname(config.tmplt.rdweb)# url http://192.168.197.79:8443/portal/login
Hostname(config.tmplt.rdweb)# exit
Hostname(config)# user-role limit
Hostname(config.user-role)# captive-portal rdweb
Hostname(config-if-range)# exit
```

【检验方法】

通过 **show running-config** 命令查看 Web 认证配置是否成功

```
Hostname(config)# show running-config
...
web-auth template rdweb
 ip 192.168.197.79
 url http://192.168.197.79:8443/portal/login
...
user-role limit
 captive-portal rdweb
Hostname# show web-auth template
Webauth Template Settings:
-------------------------------------------------------------
  Name:           rdweb
```

```
Type:           rdweb
Ip:             192.168.197.79
Url:            http://192.168.197.79:8443/portal/login
```

常见错误

无

1.4.57 配置认证成功默认角色

配置效果

- Web 认证成功后，分配默认角色

注意事项

- 先创建需要的角色，再进行默认角色配置

配置方法

↘ 配置 Web 认证成功后终端默认角色

【命令格式】 **web-auth default-role** *name*
【参数说明】 *name*：角色名称
【缺省配置】 无默认角色
【命令模式】 WLAN 安全配置模式
【使用指导】 先创建需要的角色，再进行默认角色配置。

检验方法

- 用户认证成功后，查看终端角色是否为分配的默认角色

配置举例

↘ 配置默认角色

【配置方法】
- 配置默认角色。

```
Hostname(config)# wlansec 1
Hostname(config-wlansec)# web-auth default-role teacher
```

【检验方法】

- 查看配置是否成功

```
Hostname(config)# show running-config
```

1.4.58 配置二代认证支持直接访问认证页面进行认证

配置效果

终端接入网络后无需主动发起 http 请求触发重定向，允许直接访问 Portal 页面进行认证。

注意事项

- 本命令仅适用于二代认证，即配置该命令后，仅在使用二代认证的情况下允许用户直接访问认证页面进行认证。
- VAC 环境中开启该功能后，对于关联在非主 AC 的终端，若终端接入网络后用户信息丢失（如通过 **clear web-auth user** 命令等方式删除用户信息、用户表项信息超时等），将无法直接通过访问认证页面进行用户认证，需终端重新通过 http 请求触发重定向后进行用户认证。

配置方法

↘ 配置二代认证支持直接访问认证页面进行认证

【命令格式】 **web-auth portal direct-auth**

【参数说明】 无

【缺省配置】 缺省不支持二代认证直接访问认证页面进行用户认证

【命令模式】 全局配置模式

【使用指导】 1、 VAC 场景中，关联在非主 AC 上的终端，终端接入网络后，若未在用户表项超时导致的用户信息被删除前进行认证，则需终端重新通过 http 请求触发重定向后进行用户认证，否则将认证失败。

2、 仅在使用二代认证的情况下该命令生效。

检验方法

在不存在指定终端用户的情况下（即通过 **show web-auth user all** 看不到对应用户），在终端接入网络后，直接访问认证页面发起用户认证，可以成功完成认证。

配置举例

↘ 配置二代认证支持直接访问认证页面进行认证

【配置方法】 配置二代认证支持直接访问认证页面进行用户认证。

```
Hostname(config)# web-auth portal direct-auth
```

【检验方法】 查看配置是否成功。

```
Hostname(config)#show running-config
...
web-auth portal direct-auth
...
!
end
```

1.4.59 配置 SSL 证书导入和使能

配置效果

- 配置后 Web 认证重定向时或者对接 clearpass 服务器使用 https 时，浏览器不会提示告警。

注意事项

- 无。

配置方法

↘ 配置 SSL 证书导入

【命令格式】 **web-auth import-ssl** [**auth-server**] { **cert ftp:***path* | **cert tftp:***path* } { **key ftp:***path* | **key tftp:***path* }
【参数说明】 *path*：证书和密钥的路径
【命令模式】 特权模式
【使用指导】 无

↘ 启用 SSL 证书

【命令格式】 **web-auth ssl-policy** { **https-redirect** | **auth-server** }
【参数说明】 **https-redirect**：启用 https 重定向证书
auth-server：启用 Clearpass 认证证书
【命令模式】 全局配置模式
【使用指导】 无

检验方法

- 访问 https 的页面进行 Web 认证重定向时，浏览器不会提示告警；对接 clearpass 服务器，提交用户名密码发起认证后，浏览器也不会提示告警。

配置举例

↘ 配置 SSL 证书导入和使能

【配置方法】

- 导入证书密钥。
- 启用证书

```
Hostname# web-auth import-ssl auth-server cert tftp://10.104.8.66/cpwebsrv.pem key
tftp://10.104.8.66/cpwebkey.pem
Hostname(config)# web-auth ssl-policy auth-server
```

【检验方法】

- 查看配置是否成功

```
Hostname(config)#show running-config
web-auth ssl-policy auth-server
```

1.4.60 配置用户轨迹数量

配置效果

- 配置后将设备上可记录轨迹的用户数和轨迹数量限制为用户设定的值，当用户或轨迹数量超过设定值时，丢弃最早的用户轨迹。

注意事项

- AC 上轨迹最多可记录 10000 个用户，每个用户 20 条轨迹。
- 轨迹即用户行为记录，例如用户认证、用户上线等记录。

配置方法

↘ 配置可记录的用户及轨迹数量

【命令格式】 **web-auth user-diag** { **user-num** *user-num* | **log-num** *log-num* }

【参数说明】 *user-num*：配置可记录的用户数量

log-num：配置每个用户可记录的轨迹数量

【命令模式】 全局配置模式

【使用指导】 无

检验方法

- 使用 **show web-auth user diag** { **all** | **ip** *ip-addr* | **mac** *mac-addr* } 查看用户轨迹，用户数量和每个用户可记录的轨迹数均不超过设定的值。

配置举例

配置可记录的用户及轨迹数量

【配置方法】

- 配置最多可记录 100 个用户，每个用户 10 条轨迹

```
Hostname(config)# web-auth user-diag user-num 100 log-num 10
```

【检验方法】

- 查看配置是否成功

```
Hostname(config)#show running-config
web-auth user-diag user-num 100 log-num 10
```

1.5 监视与维护

清除各类信息

作用	命令
强制用户下线	**clear web-auth user** { **all** | **ip** *ip-address* | **mac** *mac-address* | **name** *name-string* | **id** *id-num* }
删除全部免认证网络资源	**clear web-auth direct-site**
删除全部免认证用户	**clear web-auth direct-host**
删除 Web 黑白名单配置	**clear web-auth acl [white-url]**
删除全部免计费 IP 配置	**clear web-auth free-acct ip**
删除全部免计费 URL 配置	**clear web-auth free-acct url**
删除全部免认证 arp 资源	**clear web-auth direct-arp**
删除所有用户轨迹	**clear web-auth user diag**

查看运行情况

作用	命令
查看 Web 认证黑白名单。	**show web-auth acl**
查看 Web 认证基本参数配置。	**show web-auth parameter**
查看 Web 认证模板配置信息	**show web-auth template**
查看免 Web 认证的用户范围。	**show web-auth direct-host [range]**

查看直通地址范围。	**show web-auth direct-site [range]**
查看直通 ARP 范围。	**show web-auth direct-arp**
查看 TCP 拦截端口。	**show web-auth rdport**
接口上的认证配置信息。	**show web-auth control**
查看所有用户或是指定用户的在线信息。	**show web-auth user**{ **all | ip** *ip-address* | *ipv6-address* | **mac** *mac-address* **| name** *name-string* | **by-ap** *ap-name* | **by-ap-group** *ap-group-name* }
显示 Web 认证 CGI 配置	**show web-auth cgi**
查看全局 Web 认证基本信息	**show web-auth global**
查看全局 Web 认证方法	**show web-auth global authentication**
查看全局 Web 认证定制页面包	**show web-auth global customized-pages**
查看内置认证服务器信息	**show web-auth global local-portal**
查看全局 Web 认证模板信息	**show web-auth global template**
查看全局 Web 认证类型	**show web-auth global webauth-type**
查看 Web 认证配置信息	**show web-auth info**
查看内置 Web 认证信息	**show web-auth local-portal**
查看 Web 认证映射信息	**show web-auth ip-mapping**
查看 Web 认证的 portal- check 信息	**show web-auth portal-check**
查看 Web 认证降噪功能配置信息	**show web-auth noise**
查看用户的上下线记录	**show web-auth syslog ip** *ip-address*
查看认证体验数据	**show web-auth authmng** [statistic | abnormal]
显示本地 http server 的基本信息	**show web-auth auth-server**
显示全部或指定用户的轨迹信息	**show web-auth user diag** { **all** | **ip** *ip-address* | **mac** *mac-address* }

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
Web 认证 debug	**debug web-auth all**
显示内存占用统计	**debug web-auth dump memory**
显示处理重定向及认证请求的速率	**debug web-auth dump msg-rate**

1 ROLE-MGMT

1.1 概述

ROLE-MGMT(用户角色管理)是 AC/AP 上用户角色管理的组件，负责在设备上创建角色，当无线终端接入网络被分配角色后，由该组件维护终端的角色表项，并可以与具体策略绑定。

1. 角色创建。
2. 角色分配。
3. 角色与策略绑定（在对应的策略组件配置文档中说明）。

协议规范

暂无相应规范。

1.2 典型应用

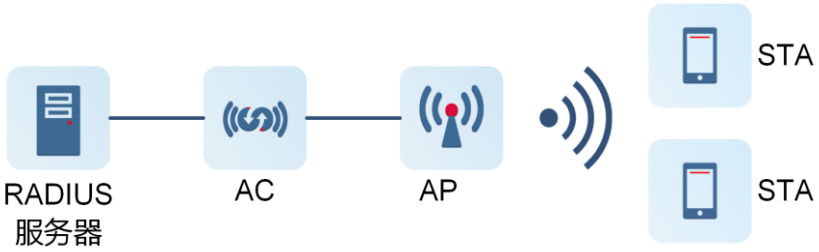
典型应用	场景描述
基于角色的 Portal 重定向	用角色来控制终端的网络访问权限
基于角色的关键业务保障	配置角色作为关键业务保障功能的关键用户
基于角色的上行 DSCP 优先级策略控制	配置角色下的终端上行报文到达 AP 后打上 DSCP 标记
基于角色的 ACL 策略	在角色下应用 ACL 过滤报文
基于角色的用户优先接入网络策略	在角色下配置基于角色的用户优先接入网络策略
基于角色的无线应用识别 QoS 策略控制	在角色下配置基于角色的无线应用 QoS 策略
基于角色的 vlan 跳转	在无线网络中，不同终端接入网络，在认证成功后为终端分配不同的角色，802.1x 认证成功（账号和密码正确）后，服务器下发角色信息，通过角色中配置的 vlan 信息进行指定 vlan 跳转

1.2.1 基于角色的 Portal 重定向

应用场景

在无线网络中，不同终端接入网络，在认证成功后为终端分配不同的角色，如果终端所属的角色网络访问受限，则根据绑定的重定向 Portal 跳转至指定页面。例如无线终端接入网络，802.1x 认证成功（账号和密码正确），但账号超过数量限制，则禁止其上网，将 HTTP 请求重定向到指定页面，并在页面中给出提示。

典型拓扑如下：



功能部署

- 配置重定向 Portal 模板（包括配置 url 和 ip 地址）
- 在 AC 上创建 Portal 重定向的角色，并在角色下绑定重定向 Portal 模板
- 终端接入无线网络，认证成功，服务器下发角色（角色名为设备上配置的重定向 Portal 模板绑定的角色）

1.2.2 基于角色的关键业务保障

应用场景

在无线网络中，存在多用户同时抢占空口资源造成空口拥塞的情况，可以启用动态限速功能对终端流量进行一定的限制。通过在角色下配置关键业务保障，这部分角色的用户将获得更高的保障带宽。

典型拓扑如下：

功能部署

- 配置启用 WQoS 动态限速功能
- 在角色下配置基于角色的关键业务保障
- 在无线网络空口拥塞的情况下，关键用户将获得更高的保障带宽

1.2.3 基于角色的上行 DSCP 优先级策略控制

应用场景

终端的上行流量经 WLAN 到达 AP，后续经过有线网络进行转发。当终端的上行流量由 WLAN 经过 AP，被打上特定的 DSCP 标记后，到达有线网络核心层出口，终端的上行流量可以按照 DSCP 优先级队列进行调度，从而保证关键用户的上行有线网络体验、抑制非关键用户的上行有线转发。

典型拓扑如下：

功能部署

- 在角色下配置基于角色的 DSCP 优先级策略控制
- 该角色的终端上行报文到达 AP 后打上特定的 DSCP 标记

1.2.4 基于角色的 ACL 策略

应用场景

终端接入网络后，如果绑定的角色下应用了 ACL 策略，则对终端的报文进行过滤，过滤的结果为放行或者丢弃。通过 ACL 可以实现终端网络访问控制：如限制终端访问指定服务（如只需要访问 WWW 和电子邮件服务，其他服务如 TELNET 则禁止），或者仅允许在指定的时间段内访问，或只允许特定终端访问网络等。

典型拓扑如下：

功能部署

- 配置用于过滤报文的 ACL 策略。
- 在角色下应用已创建的 ACL 策略。
- 终端接入无线网络，获得角色的 ACL 策略，只允许访问 ACL 放行的网络资源。

1.2.5 基于角色的用户优先接入网络策略

应用场景

终端接入网络时，若接入 Radio、AP、WLAN、AC 的在线终端达到任意一个配置的接入数上限，则仅在终端所绑定的角色上配置了用户优先接入网络策略的情况下，允许该终端成功接入。同时，由于终端接入数已达上限，系统将在通信质量不佳的非 VIP-FIRST 用户或未配置高优先接入策略的角色用户中，按 MAC 地址顺序，对第一个用户强制下线。

典型拓扑如下：

功能部署

- 在角色下配置基于角色的用户优先接入网络策略；
- 当拥有高优先接入网络权限的角色用户接入已达终端接入数上限的 Radio、AP、WLAN、AC 时，终端将被允许成功接入网络，系统将选择一个通信质量不佳的非 VIP-FIRST 用户或未配置高优先接入网络策略的角色用户进行强制下线。

1.2.6 基于角色的无线应用识别 QoS 策略控制

应用场景

AC 上的应用识别组件可以根据数据流的特征，来识别出相应的应用。针对角色用户的不同应用，可以设置下行 DSCP 值，报文到达 AP 时，AP 上的 WMM 功能会将报文的 DSCP 值转换为相应的 802.11e 优先级，再根据不同的优先级进行调度，从而实现不同的应用的优先级控制。针对角色用户的特定应用，可以配置丢弃报文，达到阻断角色非法应用流量的目的。针对角色用户不同的应用，可以设置不同的限速值，比如对下载类应用流量进行限速，避免其占用过多带宽。

典型拓扑如下：

功能部署

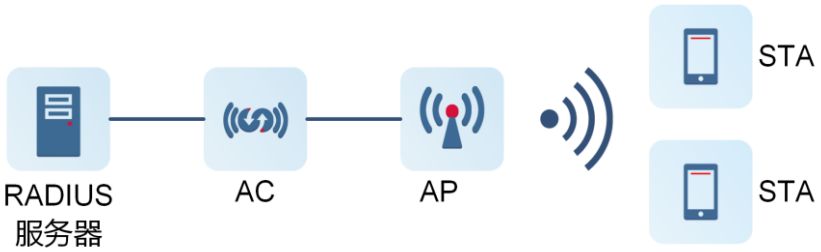
- 配置角色的无线应用 QoS 策略控制。
- 对该角色的终端进行特定应用的无线下行 DSCP 优先级控制、应用流量阻断、应用流量限速。

1.2.7 基于角色的 vlan 跳转

应用场景

在无线网络中，不同终端接入网络，在认证成功后为终端分配不同的角色，802.1x 认证成功（账号和密码正确）后，服务器下发角色信息，通过角色中配置的 vlan 信息进行指定 vlan 跳转。

典型拓扑如下：



功能部署

- 在 AC 上创建角色，并在角色下绑定需要进行跳转的 vlan
- 终端接入无线网络，802.1x 认证成功，服务器下发角色（角色名为设备上配置绑定的角色）

1.3 功能详解

基本概念

↘ 用户角色

设备上创建角色，通过角色进行终端权限控制，最多可以创建 256 个角色。

功能特性

功能特性	作用
角色管理	在设备上创建角色，并在角色下绑定策略

1.3.1 角色管理

在设备上创建角色，并维护终端的角色表项。

工作原理

管理员在 AC 设备上创建角色，并在角色下绑定策略（比如 Portal 模板）。当终端接入无线网络时，给终端分配角色后，则终端网络访问会受到该角色下的策略控制。

相关配置

↘ 配置用户角色

使用 **user-role** *name* 命令来创建角色。

使用 **captive-portal** { *portal-name* }命令来绑定 Portal 模板。

使用 **critical-business guarantee enable** 命令来配置角色的关键业务保障。

使用 **user-upstream-dscp** *dscp-value* 命令来配置角色的上行 DSCP 优先级策略。

使用 **access-group** { *acl-id* | *acl-name* } [**priority** *value*]命令来配置基于角色的 ACL 策略。

使用 **user-priority-assoc high** 来为该角色配置用户优先接入策略。

使用 **app-profile** *profile-name* 为该角色配置无线应用识别 QoS 策略模板。

使用 vlan-id vlan-id 来配置基于角色跳转的 vlan。

1.4 配置详解

配置项	配置建议 & 相关命令	
角色管理	⚠ 必须配置。用于创建角色。	
	user-role	创建角色
	captive-portal	绑定 Portal 模板
	critical-business guarantee enable	使能关键业务保障
	user-upstream-dscp	配置角色的上行 DSCP 优先级策略
	access-group	配置基于角色的 ACL 策略

	user-priority-assoc high	配置基于角色的用户优先接入策略
	app-profile	配置基于角色的无线应用识别 QoS 策略模板
	vlan-id	配置基于角色跳转的 VLAN 功能

1.4.1 角色管理

配置效果

创建角色后，才可以为接入无线的终端分配角色。

注意事项

分配的角色名必须是设备上已创建的。

配置方法

↘ 创建用户角色

必须配置。

【命令格式】 **user-role** *name*
【参数说明】 *name*：角色名称
【缺省配置】 默认无自定义角色
【命令模式】 全局配置模式
【使用指导】 需要先在 AC 上创建角色，认证服务器才能成功下发角色信息。

↘ 配置角色绑定 Portal 模板

必须配置。

【命令格式】 **captive-portal** { *portal-name* }
【参数说明】 *portal-name*：Portal 模板名称
【缺省配置】 默认未绑定模板。
【命令模式】 用户角色配置模式
【使用指导】 需要先创建 Portal 模板再进行绑定。

↘ 配置角色关键业务保障

必须配置。

【命令格式】 **critical-business guarantee enable**
【参数说明】 -
【缺省配置】 默认未开启关键业务保障。
【命令模式】 用户角色配置模式

【使用指导】 1、配置关键业务保障前，需要先启用 WQoS 动态限速功能。
2、开启关键业务保障后，该角色下的用户将获得更高的保障带宽。

配置角色的上行 DSCP 优先级策略

必须配置。

【命令格式】 **user-upstream-dscp** *dscp-value*
【参数说明】 *dscp-value*：为角色配置的上行 DSCP 值
【缺省配置】 默认未配置角色的上行 DSCP 值
【命令模式】 用户角色配置模式
【使用指导】 配置用户角色上行 DSCP 策略，该角色的终端上行报文到达 AP 后会被打上特定的 DSCP 值，通过 DSCP 策略控制保障关键用户的业务。

配置基于角色的 ACL 策略

必须配置。

【命令格式】 **access-group** { *acl-id* | *acl-name* } [**priority** *value*]
【参数说明】 *acl-id*：ACL 的编号
acl-name：ACL 的名称
value：ACL 的优先级，取值范围 1~16。1 表示最高优先级，16 表示最低优先级，优先级参数为可选配置，未指定优先级时默认优先级为 16。
【缺省配置】 默认未应用任何 ACL
【命令模式】 用户角色配置模式
【使用指导】 1、单个角色下最多支持配置 16 条不同的 ACL 策略，可以通过 **priority** 参数来指定 ACL 的优先级，priority 值只用于指定插入顺序，不会作为配置的一部分保存。
2、报文将按照 ACL 策略的优先级从高到低进行过滤，命中任意规则后即停止。
3、应用任意 ACL 后，在角色 ACL 策略末尾将隐含一条丢弃所有报文的 ACL，如果报文和任何规则都不匹配，将被丢弃。

配置角色用户优先接入策略

必须配置。

【命令格式】 **user-priority-assoc high**
【参数说明】 -
【缺省配置】 默认未开启角色用户的高优先接入网络策略。
【命令模式】 用户角色配置模式
【使用指导】 1、角色用户的高优先接入网络权限与 VIP-FIRST 的 VIP 用户接入网络权限的优先级相同。
2、由于用户角色是在终端认证成功之后才能获取，所以在 AC 整机已达终端接入数上限时仍允许最多 500 个终端用户与 AC 进行关联。若新接入用户未开启高优先接入网络配置，且非 VIP 用户，则在在线终端已达接入数上限的情况下，新终端将无法成功接入网络。

配置角色的无线应用识别 QoS 策略控制

必须配置。

【命令格式】 **app-profile** *profile-name*

【参数说明】 *profile-name*：配置角色关联的应用识别策略名称

【缺省配置】 缺省未关联任何应用识别策略

【命令模式】 用户角色配置模式

【使用指导】 1、用户角色与无线应用识别策略建立关联后，该角色下的终端报文流量将归属于角色关联策略下的应用组，受应用组策略的约束。

2、角色与 WLAN 关联不同的无线应用识别策略，若终端的角色和 WLAN 均满足这两个策略，则优先采用角色关联的应用识别策略。

3、为角色关联应用识别策略前，应先创建对应的应用识别策略。

↘ 配置基于角色跳转的 VLAN 功能

- 可选配置，认证用户在服务器认证成功下发角色信息时，根据角色配置的跳转 VLAN 进行跳转。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **vlan-id** *vlan-id*

【参数说明】 *vlan-id*：属于此角色要跳转的 VLAN

【缺省配置】 未配置角色跳转 VLAN，角色认证成功后不进行 VLAN 跳转

【命令模式】 角色配置模式

【使用指导】 1、配置本功能后，802.1x 用户认证通过，服务器下发角色信息，根据角色查找到绑定的 vlan-id，这个 vlan-id 需要事先配置在 WLAN 关联的 vlan-group 中，否则无法完成跳转。

2、角色下绑定的 VLAN 优先级**低于**通过 Radius 属性下发的 VLAN 优先级。

3、COA 下发角色进行 VLAN 跳转后，由于终端无法变更 ip，会导致网络不通。

检验方法

通过 **show running-config** 查看配置。

配置举例

↘ 用户角色绑定 Portal 模板

【配置方法】 配置重定向 portal 模板。

```
Hostname(config)# web-auth template rdweb
Hostname(config.tmplt.rdweb)# ip 10.10.10.10
Hostname(config.tmplt.rdweb)# url http://10.10.10.10/warning
```

创建用户角色，并在角色下应用 portal 模板

```
Hostname(config)# user-role limit
Hostname(config.user-role)# captive-portal rdweb
```

↘ 用户角色配置关键业务保障

【配置方法】 配置启用动态限速功能。

```
Hostname(config)# ap-config all
Hostname (config-ap)# smart-rate-control enable
```

创建用户角色，并在角色下配置关键业务保障

```
Hostname(config)# user-role teacher
Hostname(config.user-role)# critical-business guarantee enable
```

用户角色配置上行 DSCP 优先级策略

【配置方法】 创建用户角色，并在角色下配置上行 DSCP 优先级为 56

```
Hostname(config)# user-role teacher
Hostname(config.user-role)# user-upstream-dscp 56
```

用户角色配置基于角色的 ACL 策略

【配置方法】 配置 ACL。

```
Hostname(config)# ip access-list standard 1
Hostname (config-std-nacl)# permit host 1.1.1.1
Hostname(config-std-nacl)# exit
Hostname(config)# ip access-list standard 2
Hostname (config-std-nacl)# permit host 1.1.1.1
```

创建用户角色，并在角色下应用 ACL

```
Hostname(config)# user-role test
Hostname(config.user-role)# access-group 1
Hostname(config.user-role)# access-group 2 priority 1
```

查看应用的 ACL

```
Hostname(config.user-role)# show this
Building configuration...
!
 access-group 2
 access-group 1
!
end
```

用户角色配置优先接入策略

【配置方法】 创建用户角色，并在角色下配置高优先级接入策略

```
Hostname(config)# user-role teacher
Hostname(config.user-role)# user-priority-assoc high
```

用户角色的无线应用识别 QoS 策略控制

【配置方法】 设置角色 teacher 关联应用识别策略 P-Tencent

```
Hostname(config)#user-role teacher
Hostname(config.user-role)#app-profile P-Tencent
```

↘ 配置基于角色跳转的 VLAN 功能

【配置方法】 ● 创建用户角色，并在角色下配置基于角色跳转的 vlan id

```
Hostname(config)#user-role teacher
Hostname(config.user-role)# vlan-id 2
```

1.5 监视与维护

清除各类信息

无。

查看运行情况

作用	命令
显示终端的角色信息	**show user-role**
显示设备配置的角色信息	**show role**
显示角色下的 ACL 策略信息	**show access-group** [**role** *role-name*]
显示角色下的优先接入权限	**show role priority-assoc**

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开事件的调试开关。	**debug rlmgt rlmgtd info**
打开严重错误的调试开关	**debug rlmgt rlmgtd error**

1 APP 认证

1.1 概述

APP 认证是一种对用户访问网络的权限进行控制的身份认证方法，它提供了一种基于应用(组)进行认证的方式。APP 认证不需要用户提供用户名、密码进行认证，用户只需要在终端上产生指定应用的数据流，或者在终端上访问预设的 URL 时即认证通过。

APP 认证可用于应用软件的推广，如指定用户安装微信应用，进行微信关注操作时才能认证通过。

协议规范

- 无。

1.2 典型应用

典型应用	场景描述
微信关注认证应用场景	AC 与 MCP 服务器进行联动，使用微信关注认证完成对下联终端认证前网络访问权限的控制及认证。

1.2.1 微信关注认证应用场景

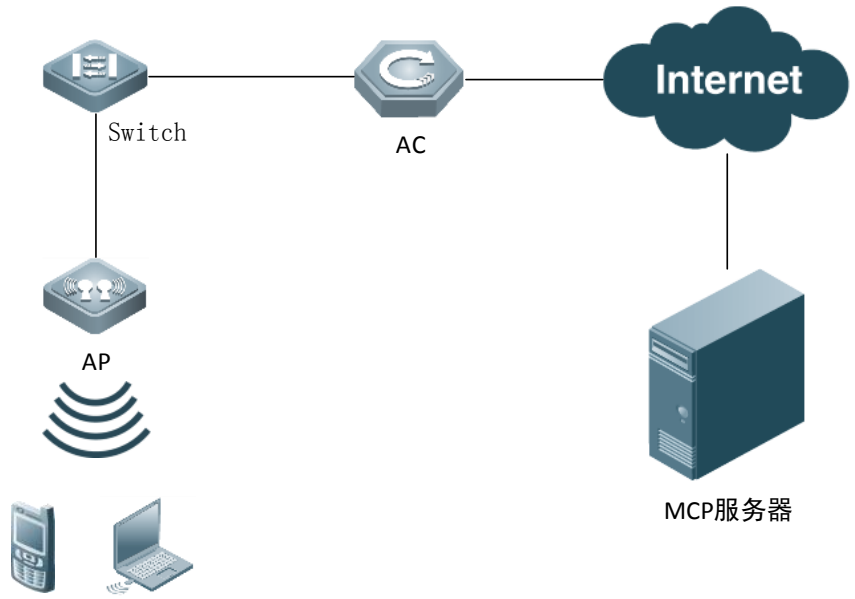
应用场景

如下图所示，AC 与 MCP 服务器进行联动，使用微信关注认证完成对下联终端认证前网络访问权限的控制及认证。

认证前，终端仅能访问微信内容，通过关注微信公众号可通过认证。

认证后，终端的网络访问权限不受限制。

图 1-1



【注释】 Switch：交换机。
AC：无线控制器。
AP：无线接入点。
MCP：云服务器。

功能部署

- 在 AC 上开启微信关注认证功能，与 MCP 服务器进行联动。

1.3 功能详解

基本概念

↘ 免认证 APP

用户通过认证前就具有网络访问权限的应用，可以是微信软件，也可以是新浪微博等其它 APP。

↘ 微信关注认证

当设备检测到用户发生微信关注公众号行为时，用户即通过认证。

↘ CWMP 协议

CWMP（CPE WAN Management Protocol，CPE 广域网管理协议）是由 DSL（Digital Subscriber's Line，数字用户线路）论坛发起开发的技术规范之一，编号为 TR-069，所以又被称为 TR-069 协议。它提供了对下一代网络中家庭网络设备进行管理配置的通用框架、消息规范、管理方法和数据模型。

TR-069 协议实现十分复杂，对 APP 认证来说，TR-069 提供了设备与 MCP 服务器进行通信的网络通道。

功能特性

功能特性	作用
免认证 APP 功能	AC 开启 web 认证功能，未认证用户无法正常访问网络内容。通过配置免认证 APP，可以放行用户特定 APP 的流量。
微信关注认证功能	AC 开启 web 认证功能，未认证用户使用微信关注公众号即可通过认证。

1.3.1 免认证 APP 功能

AC 上配置免认证 APP，可以对未认证用户放行指定 APP 流量。免认证 APP 功能开启后在某些外部情况下（如 APP 服务器增加、均衡策略变化等）会显著影响设备的转发性能，其中特别是苹果服务器的数量多更为明显。

工作原理

AC 上开启 web 认证功能，未认证用户无法正常访问网络内容。配置免认证 APP 后，AC 检测到未认证用户的流量符合 APP 特征，会放行这部分流量，用户不通过认证便可以使用特定 APP。

1.3.2 微信关注认证功能

AC 开启 web 认证时，未认证用户使用微信关注公众号即可通过认证。

工作原理

用户通过 web 认证之前，终端发出的数据流默认被设备丢弃(免认证应用的数据流除外)。

微信关注认证功能需要与免认证 APP 功能配合使用，首先将微信加入免认证 APP，这样用户可以正常访问微信内容。当用户关注公众账号时，设备会将用户信息上报给 MCP 服务器，若 MCP 服务器返回用户认证成功，AC 上该用户会成为 web 认证用户，该用户的所有数据流会被放行，否则仍然阻断该用户除了微信之外的数据流。

1.4 配置详解

配置项	配置建议 & 相关命令	
配置免认证 APP	⚠ 必须配置。基于全局配置免认证 APP。	
	web-ctrl free-auth	配置免认证 APP，目前支持微信、新浪 APP 和 iphone 特定 APP。
配置微信关注认证功能	⚠ 必须配置。基于 WLAN 配置微信关注认证功能。	
	app-auth weixin-follow	打开微信关注认证功能。

1.4.1 配置免认证 APP

配置效果

- 配置免认证 APP，可以对未认证用户放行指定 APP 流量。

注意事项

- 开启 web 认证的前提下，配置免认证 APP 才有实际效果。

配置方法

↘ 配置免认证 APP

- 必须配置。
- 在 AC 上配置免认证 APP。

【命令格式】 **web-ctrl free-auth** { **weixin | sina | iphone** }

【参数说明】 **weixin**：微信

sina：新浪 APP

iphone：iphone 特定 APP

【缺省配置】 缺省无配置

【命令模式】 全局配置模式

【使用指导】 免认证 APP 可以同时开启多个

有配置并引发性能降低的需要手动配置关闭。

Iphone 特定 APP 免认证不推荐配置。

检验方法

- 通过 **show web-ctrl** 查看配置结果。
- AC 上开启 web 认证时，在未认证的终端上检查是否可以正常使用免认证 APP。

配置举例

↘ 在 AC 上配置微信为免认证 APP

【配置方法】
- 进入全局配置模式。
- 配置微信为免认证 APP。

AC

```
Hostname#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#web-ctrl free-auth weixin
```

```
Hostname(config)#exit
```

【检验方法】 通过 **show web-ctrl** 命令查看免认证 APP 信息。

AC

```
Hostname#show web-ctrl
************web_ctrl_struct***********
===== WEIXIN domain name table =======
[0]:  short.weixin.qq.com
[1]:  long.weixin.qq.com
[2]:  dns.weixin.qq.com
[3]:  szshort.weixin.qq.com
[4]:  *.qpic.cn
[5]:  *.weixin.qq.com
-----------------------------------
========== WEIXIN IP table ===========
[0]: 101.227.131.102
[1]: 101.226.76.175
[2]: 101.226.129.199
[3]: 101.227.131.105
[4]: 101.226.76.145
[5]: 183.60.15.188
[6]: 123.151.10.172
[7]: 115.236.148.177
```

常见错误

- 无。

1.4.2 配置微信关注认证功能

配置效果

- 在 web 认证开启的情况下，默认情况下用户是无法访问网络内容。如果打开微信关注认证功能，用户使用微信关注公众号即可通过认证。
- 用户微信关注认证成功后，在设备上成为 web 认证用户。

注意事项

- 需要先开启 web 认证，对用户的网络访问权限进行控制。

配置方法

配置微信关注认证功能

- 必须配置。
- 在 AC 上基于 WLAN 配置微信关注认证功能。

【命令格式】 **app-auth weixin-follow**
【参数说明】 -
【缺省配置】 缺省不配置微信关注认证
【命令模式】 无线安全配置模式
【使用指导】 需要先开启 web 认证，否则无意义

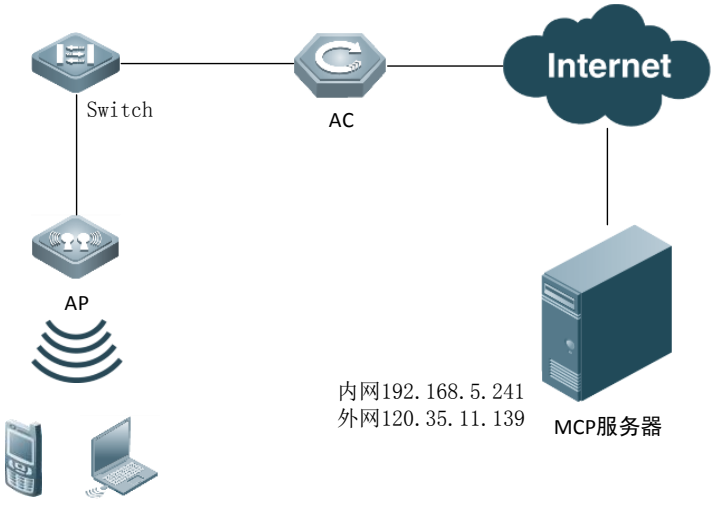
检验方法

- 开启一代 web 认证，再配置微信关注认证功能，并将微信配置为免认证 APP。
- 用户未通过认证前，仅能访问微信内容。
- 用户通过认证后，网络访问不受限制。

配置举例

配置微信关注认证功能

【网络环境】
图 1-2



【配置方法】
- MCP 服务器内网地址为 192.168.5.241，外网地址为 120.35.11.139。
- 在 AC 上配置 TR069 协议(MCP 服务器通过 TR069 协议在 AC 上打开用户的上网通道)。
- AC 上配置一代 web 认证。
- AC 上配置微信为免认证 APP。

- AC 上开启 web 认证，配置微信关注认证。

AC

```
Hostname#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#acs url http://192.168.5.241/mcp/tr069Servlet
Hostname(config-cwmp)#acs username Hostname
Hostname(config-cwmp)#acs password Hostname
Hostname(config-cwmp)#cpe username Hostname
Hostname(config-cwmp)#cpe password Hostname
Hostname(config-cwmp)#cpe inform interval 30
Hostname(config-cwmp)#exit
```

AC

```
Hostname(config)#web-auth template eportalv1
Hostname(config.tmplt.eportalv1)#ip 192.168.5.241
Hostname(config.tmplt.eportalv1)#url http://192.168.5.241/auth/servlet/authServlet
Hostname(config.tmplt.eportalv1)#exit
Hostname(config)#web-auth portal key Hostname
Hostname(config)#web-auth acl white-url http://120.35.11.139:70
Hostname(config)#web-auth acl white-url http://mcp.Hostname.com.cn
```

AC

```
Hostname(config)#web-ctrl free-auth weixin
Hostname(config)#wlansec 1
Hostname(wlansec)#web-auth portal eportalv1
Hostname(wlansec)#webauth
Hostname(wlansec)#app-auth weixin-follow
Hostname(wlansec)#exit
```

【检验方法】 在 AC 上查看配置是否成功。

AC

```
Hostname#show run
...
web-auth acl white-url http://120.35.11.139:70
web-auth acl white-url http://mcp.Hostname.com.cn
!
web-auth template eportalv1
 ip 192.168.5.241
 url http://192.168.5.241/auth/servlet/authServlet
!
web-auth portal key Hostname
!
cwmp
 acs url http://192.168.5.241/mcp/tr069Servlet
 acs username Hostname
 acs password Hostname
```

```
 cpe username Hostname
 cpe password Hostname
 cpe inform interval 30
!
...
!
wlansec 1
 web-auth portal eportalv1
 webauth
 app-auth weixin-follow
!
...
```

常见错误

- 与 MCP 服务器的 TR069 协议不通。
- 没有开启 web 认证。
- 没有配置微信为免认证 APP。

1.5 监视与维护

清除各类信息

无。

查看运行情况

作用	命令
show web-ctrl	查看免认证 APP 情况

查看调试信息

无。

1 SCC

1.1 概述

SCC (Security Control Center，安全控制中心)为各种接入控制和网络安全业务提供了公共的配置方法和策略整合服务，从而使得各种接入控制业务以及网络安全业务能够在一台设备上共存，实现多元化的接入安全控制需求，以满足不同的接入场景需要。

典型的接入控制业务如 dot1x、web 认证、arp check、ip source guard 等；网络安全业务如 ACL、NFPP、防网关 ARP 欺骗等。当设备上同时开启两个或两个以上的上述接入控制业务或网络安全业务时 ,或者同时开启接入控制业务和网络安全业务时，SCC 通过相关的策略整合负责协调共存关系。

有关接入控制和网络安全业务相关的说明请参考相应的配置指南，下文仅介绍 SCC 的相关内容。

协议规范

无

1.2 典型应用

典型应用	场景描述
高校大二层校园网访问控制应用	在高校校园网中学生可通过 dot1x 客户端认证上网或通过 web 认证来上网，同时要防止相互间 ARP 欺骗。另外，允许某些部门（比如校长办公室）的终端设备无需认证就能上网。

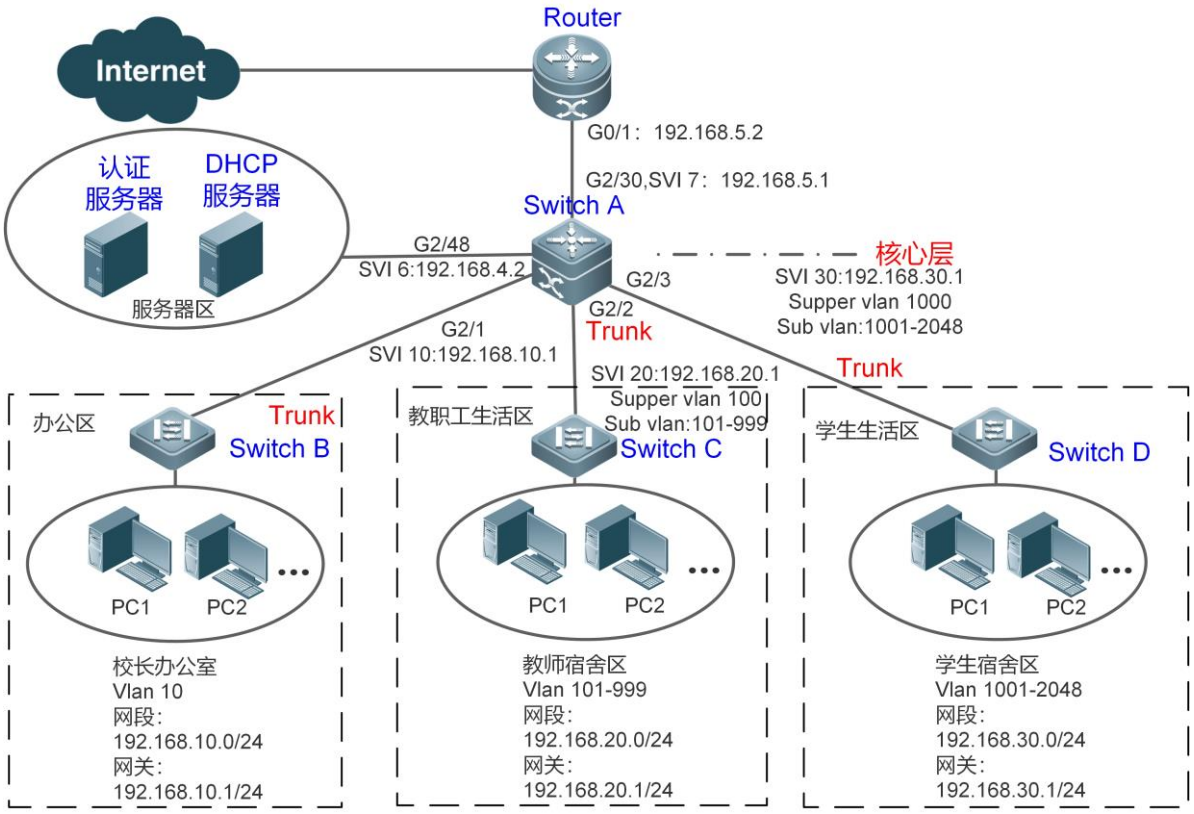
1.2.1 高校大二层校园网访问控制应用

应用场景

在高校校园网中，学生上网前一般都需要前进行 1x 认证或 web 认证，从而方便计费，以保障高校的利益：

- 学生可以通过 dot1x 客户端认证上网，也可以通过 web 认证上网。
- 防止学生相互间进行 ARP 欺骗，以保证网络的稳定性。
- 允许某些部门（如校长办公室）的终端无需认证就能上网。

图 1-1



【注释】 传统的高校校园网网络是分层设计的，有接入层、汇聚层和核心层，用户接入控制在接入层上完成；而在高校大二层校园网中，用户的接入控制是由核心设备来承担的，核心设备以下都是二层设备，中间不再有汇聚。核心设备与用户接入交换设备（如上图的 switch B、switch C 以及 switch D）之间都是 TRUNK 口。

接入层设备 B、C、D：连接各部门的 PC，各个接入端口配置成 Access 口，VLAN 与核设备对应下联端口上配置的 SUB VLAN 相对应，这样每个接入用户处于不同的 VLAN 中，防止相互间进行 arp 欺骗。

核心层设备 A 连接各种服务器 如认证服务器、DHCP 服务器等。并在下联端口上配置 Supper VLAN 和 Sub VLAN。一个 Super VLAN 对应多个 Sub vlan，每个 Sub VLAN 代表一个接入用户。

功能部署

- 核心设备上通过 vlan + 端口号来区分不同的接入用户，每个接入用户（当然也可以是一组用户）一个 vlan。接入层设备下联用户的端口配置成 Access 口，并按规划为每个用户配置一个用户 vlan，核心设备上不转发 ARP 请求报文，只有被请求用户已认证才作应答 ,以此来达到防止用户间的 ARP 欺骗问题。核心设备 switch A 上面将用户 VLAN 作为 Sub VLAN，并配置 Super VLAN 以及将 Super VLAN 对应的 SVI 配置成用户网关。
- 通过在核心设备（本例为设备 A）下联教职工生活区和学生生活区的端口上同时开启 dot1x 认证和 web 认证功能来达到由用户自由选择使用哪种认证方式的目的。
- 对于特殊部门（本例为校长办公室）可以划到单独特定的一个 VLAN 中，通过配置该 VLAN 为免认证 VLAN 的方式来达到不需要通过认证即可上网的目的。

1.3 功能详解

基本概念

IPv4 用户容量

为了保护已上线用户的上网稳定性，同时也为了让设备能够更加稳定地运行，可以对 IPv4 接入用户数量进行限制。

默认情况下不会对 IPv4 接入用户数量进行限制，可以让大量用户认证上线，直到上线用户数达到设备的硬件最大容量。

IPv4 接入用户包括 dot1x 认证产生的 IP 用户(比如 IP 授权用户)、WEB 认证用户、用户手工绑定的 IP 用户(包括 IP source guard、arp check 等)。

用户在线检测

对于计费用户来说，用户认证上线之后就会开始计费，用户离开时需要主动下线才能真正结束计费过程，但有可能用户上网结束离开时未主动下线或者因终端原因无法主动下线等原因，继续产生上网费用从而导致用户的经济损失。为了更加精确地判断用户是否真的在上网，可以预设在一个时间段内用户流量低于某个值或者在一个时间段内用户无流量时就认为用户没有使用网络，直接将该用户进行下线操作。

功能特性

功能特性	作用
IPv4 用户容量	可以对指定接口上的 IPv4 用户容量进行限制以保证容量内的用户上网稳定。
用户在线检测	可以指定是否对在线用户进行流量检测，在一段时间内流量低于某个值时设备主动将用户下线。
用户策略规则	对控制策略名称进行解析，并转化成功对应的策略规则，进行安装生效。

1.3.1 IPv4 用户容量

为了让设备能够更加稳定地运行，避免非法用户的暴力冲击，可以对设备某个接口上的 IPv4 可接入用户总数进行限制。

工作原理

如果对 IPv4 的可接入用户数进行了限制，超过限制的新用户将无法接入网络，也就无法正常上网。

默认情况下，设备不对 IPv4 接入用户数进行限制，可接入用户数取决于设备的硬件容量。

此处的 IPv4 接入用户包括 dot1x 产生的 IPv4 授权用户、WEB 认证产生的 IPv4 用户，以及各种绑定功能产生的 IPv4 用户表项。由于 IPv4 可接入用户数限制是在接口下配置的，限制的范围包括在本接口上生成的 IPv4 用户，同时也包括全局生成的 IPv4 用户。比如，配置接口 Gi 0/1 的 IPv4 接入用户最大数量为 2，使用命令在接口上绑定一个 IPv4 用户，再使用命令绑定一个全局的 IPv4 用户，实际上该接口上的接入用户数已经达到最大 2，此时再想在该接口上绑定一个 IPv4 用户或者再想绑定一个全局的 IPv4 用户将会失败。

1.3.2 用户在线检测

用户在上好网之后，有可能会忘了点下线或者由于终端缘故无法主动下线，这个时候会造成持续计费而招致经济损失。在这种情况下，为了保障上网用户的利益，设备提供了判断用户是否在线即用户在线检测功能，由设备来判断用户是否真的在线，如果设备认为用户不在线，主动将该用户进行下线。

工作原理

在设备上预设一个指定的检测周期，在这个周期内如果用户流量低于某个值时就认为此时用户没有使用网络，从而直接将该用户进行下线操作。

- 用户在线检测功能仅针对通过 dot1x 认证或 web 认证上线的用户。

1.3.3 用户策略规则

用户认证成功后，服务器有可能会下发该用户的控制策略名称，此时，需要 scc 对控制策略名称进行解析，并转化成功对应的策略规则，进行安装生效。

工作原理

在设备上先配置相关的策略名称，策略下可配置具体限速策略和过滤策略，用户认证通过后，同时设置这个策略名称时，相应的限速策略和过略策略生效。

同时，过滤策略也可以应用到用户组中，实现对用户组策略的控制。

- 过滤策略只能关联一条对应的 acl
- 过滤策略被用户组应用后内容将不能被修改，策略也不能被删除
- 策略配置仅针对通过 dot1x 认证或 web 认证上线的用户。

1.4 配置详解

配置项	配置建议 & 相关命令	
配置 IPv4 用户容量	可选配置。用于限制某个接口上可接入的用户数	
	[no] nac-author-user maximum	配置接口下可接入的 IPv4 用户数
配置用户在线检测	可选配置。用于指定是否开启用户在线检测功能	
	offline-detect interval thredshold	配置用户在线检测参数

	no offline-detect	关闭用户在线检测功能
	default offline-detect	恢复成缺省的用户在线检测方式
配置用户策略规则	⚠ 可选配置。用于指定用户策略使用的具体规则	
	[no] rate-policy	进入限速策略配置模式。
	upstream average-rate burst-rate	配置上行限速流量平均值和突发值。
	no upstream	删除上行限速流量配置
	downstream average-rate burst-rate	配置下行限速流量平均值和突发值。
	no downstream	删除下行限速流量配置
	[no] filter-policy	进入过滤策略配置模式。
	filter_acl	配置过滤策略关联的安全 acl
	no filter_acl	删除过滤策略关联的安全 acl
	[no] service-policy	进入用户策略配置模式。
	rate-policy apply	配置使用的限速策略。
	no rate-policy	删除使用的限速策略
	filter-policy apply	配置使用的过滤策略
	no filter-policy	删除使用的过滤策略

1.4.1 配置 IPv4 用户容量

配置效果

通过配置 IPv4 用户容量，可以限制一个接入端口上的可接入用户数。

注意事项

无

配置方法

↘ 配置 IPv4 用户容量

- 可选配置。如果要限制一个接入端口上的最大可接入用户数，就必须配置 IPv4 的用户容量。默认没限制。如果指定接口上配置了用户容量限制，则当该接口上认证用户数量达到上限时，新用户无法认证上线，必须等到有用户下线后才可以认证上线。
- 需要配置在接入设备上。

【命令格式】 **nac-author-user maximum** *max-user-num*

no nac-author-user maximum

【参数说明】 **no**： 该选项若被配置，表示取消端口下的 IPv4 接入用户容量限制。

max-user-num：表示所配置端口下 IPv4 接入用户容量限制值，取值范围[1, 1024]。

【缺省配置】 不对 IPv4 接入用户数量进行限制
【命令模式】 接口模式
【使用指导】 此命令可以用来限制指定接入端口的 IPv4 接入用户数。

检验方法

可以通过以下方法检验端口上的 IPv4 用户容量的配置效果：

- 如果是 dot1x 认证，可以在该端口上下联的 1x 客户端认证上线达到指定的用户容量，这时再想认证上线一个用户，不能上线成功。
- 如果是 web 认证，可以在该端口上下联的客户端通过 web 认证上线达到指定的用户容量，这时再想认证上线一个用户，不能上线成功。
- 使用 **show nac-author-user** [**interface** *interface-name*]命令检查设备上的 IPv4 用户容量配置。

【命令格式】 **show nac-author-user** [**interface** *interface-name*]
【参数说明】 *interface-name*：接口名称
【命令模式】 特权模式、全局模式、接口模式
【使用指导】 全局模式
【使用展示】

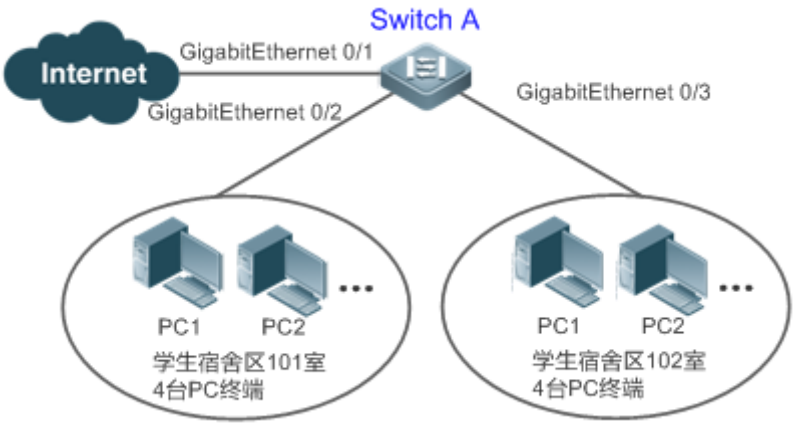
```
Hostname#show nac-author-user interface GigabitEthernet 0/1
 Port      Cur_num  Max_num
 --------  -------  -------
 Gi0/1     0         4
```

配置举例

以下配置举例，仅介绍与 SCC 相关的配置。

通过限制端口上的 IPv4 用户数，防止过多的上网终端设备冲击网络。

【网络环境】
图 1-2



【配置方法】
- 此处假设接入设备 Swtich A 的 dot1x 认证环境都已经配置好了，dot1x 受控在 Gi 0/2 端口上开启。
- 配置 Gi 0/2 端口下的 IPv4 接入用户最大容量为 4。

Switch A

```
SwitchA(config)#int GigabitEthernet 0/2
SwitchA(config-if-GigabitEthernet 0/2)#nac-author-user maximum 4
```

【检验方法】
- 将宿舍内的 4 台 PC 全部进行 dot1x 认证上线。再额外拿一台终端接入网络，企图进行 dot1x 认证，确定无法成功认证上线。
- 使用 show nac-author-user 命令可以查看配置是否生效

Switch A

```
SwitchA(config)#show nac-author-user
 Port      Cur_num  Max_num
 --------  -------  -------
 Gi0/1     0         4
```

1.4.2 配置用户在线检测

配置效果

当配置了认证用户在线检测功能后，在指定的周期内如果流量低于一定的门限，设备会自动将用户下线，以免造成持续计费而导致用户的经济损失。

注意事项

配置如果配置无流量下线，需要注意的是，终端一般来说都会默认运行 360 安全卫士等软件，这些软件会时不时地往外发送报文，此时，只有终端关机的情况下设备才会将用户下线、

配置方法

配置用户在线检测

- 可选配置。默认为 8 小时内无流量就将用户下线。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。只对被配置的设备上有效，不会影响网络中的其他设备。

流量门限参数 thredshold 如果配置成 0，则表示进行无流量检测。

【命令格式】 **offline-detect interval** *interval* **thredshold** *thredshold*

no offline-detect

default offline-detect

【参数说明】 *interval*：下线检测周期，取值范围为 1-65535min。默认 8 小时，即 480min。

thredshold：流量门限，取值范围为 0-4294967294Bytes。默认为 0，表示无流量检测下线。

no offline-detect：关闭用户在线检测功能。

default offline-detect：恢复成默认值，即 8 小时无流量就将已在线认证用户下线。

【缺省配置】 8 小时

【命令模式】 全局模式

【使用指导】 此命令可以用来配置用户在线检测，指定在一定的时间段内在线认证用户的流量低于指定的门限时将用户下线。使用 **no offline-detect** 命令关闭用户在线检测功能，使用 **default offline-detect** 恢复成缺省的检测方式。

检验方法

可以通过以下方法检验认证用户在线检测的配置效果：

- 配置了在线用户检测功能后，用户上线后，将指定的已认证终端关机，再等待指定的周期，在设备上使用 dot1x 或 web 认证提供的在线用户查询命令确认指定的用户已经下线。

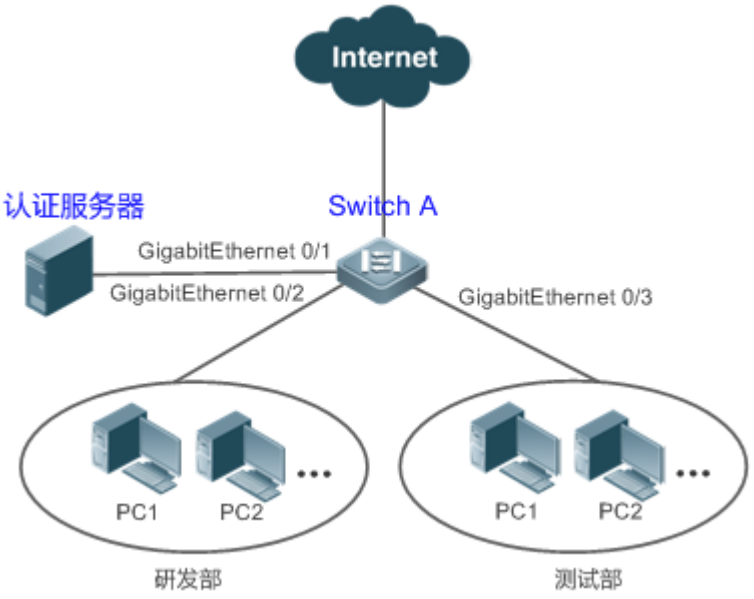
配置举例

以下配置举例，仅介绍与 SCC 相关的配置。

通过用户在线检测功能，指定 5min 内无流量就将用户下线。

【网络环境】

图 1-3



【配置方法】

- 在接入端口 Gi 0/2 上开启 dot1x 受控，并配置认证所需参数，基于 MAC 认证
- 配置用户在线检测功能，指定 5min 内无流量就将用户下线。

Switch A

```
sw1(config)# offline-detect interval 5 threshold 0
```

【检验方法】

- 在研发部中的一台电脑上通过 dot1x SU 客户端认证上线，再将电脑直接关机，等待 6min 后，在 switch1 设备上使用 dot1x 提供的在线用户查询命令确认该用户已经下线。

Switch A	sw1(config)#show running-config | include offline-detect offline-detect interval 5

1.4.3 配置用户策略规则

配置效果

当配置了策略规则后，认证通过的用户，指定了对应策略名称后，可以根据策略配置的规则，对该用户进行限速设置。

注意事项

需要认证服务器支持对应的策略属性下发。

- 过滤策略只能关联一条安全 ACL。

配置方法

配置用户策略规则

- 可选配置。
- 先配置限速策略和过滤策略，再在用户策略规则中指定使用的限速策略名称。

上下行限速参数突发值不小于平均值。

【命令格式】 **rate-policy** *name*
{downstream | upstream } average-rate *avg-threshold* **burst-rate** *burst-threshold*

【参数说明】 *name*：限速策略名称
avg-threshold：流量限速平均值，取值范围为 8-261120，单位为 KBps。
burst-threshold：流量限速突发值,取值范围为 8-261120,单位为 KBps,突发值不小于平均值。

【缺省配置】 无

【命令模式】 全局模式

【使用指导】 需要先配置限速策略规则。

【命令格式】 **filter-policy** *name*
filter-acl { *acl-name* | *acl-id* }

【参数说明】 *name*：过滤策略名称
acl-name：过滤策略关联的安全 acl 的 acl-name。
acl-id：过滤策略关联的安全 acl 的 acl-id。

【缺省配置】 无

【命令模式】 全局模式

【使用指导】 需要先配置过滤策略规则。

【命令格式】 **service-policy** *service-name*
rate-policy *rate-name* **apply**
filter-policy *filter-name* **apply**
【参数说明】 *service-name*：用户策略名称。
rate-name：使用的限速策略名称。
filter-name：使用的过滤策略名称。
【缺省配置】 无
【命令模式】 全局模式
【使用指导】 配置限速策略和过滤策略规则后，才能在用户策略规则中使用。

检验方法

可以通过以下方法检验策略规则配置效果：

- 配置了限速策略规则后，用户认证上线，查看 wqos 对应的限速策略表项。
- 配置了过滤策略规则后，用户认证上线，查看 aclk 对应的用户 acl 应用表项。
- 通过 **show running** 确认用户策略相关配置。

配置举例

以下配置举例，仅介绍与 SCC 相关的配置。

通过用户策略规则功能，指定认证用户的限速策略。

【配置方法】
- 在 WLAN 1 上开启 WEB 受控，并在服务器配置对应的用户策略名称。
- 配置用户策略规则，指定限速策略。

AC1

```
AC(config)# rate-policy user-rate
AC(config-rate-policy)#upstream average-rate 10 burst-rate 10
AC(config-rate-policy)#downstream average-rate 10 burst-rate 10
AC(config)# ip access-list extended user_2000
AC(config)# filter-policy user-filter
AC(config-filter-policy)#filter-acl user_2000
AC(config)# service-policy user-policy
AC(config-service-policy)# rate-policy user-rate apply
AC(config-service-policy)# filter-policy user-filter apply
```

【检验方法】
- 认证通过后，查看用户的报文上下行速率。

1.5 监视与维护

清除各类信息

作用	命令
清除 SCC 记录的 AP 事件轨迹信息	**clear scc event diag** [**ap-mac** *mac-address*]

查看运行情况

作用	命令
显示指定接口上 IPv4 用户表项信息。	**show nac-author-user** [**interface** *interface-name*]

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
监视 SCC 运行过程信息	**debug scc event**
调试查看当前 SCC 的相关用户表项	**debug scc user** [**mac** | **author** | **mac**]
调试查看当前 SCC 中保存的所有业务下发的相关 ACL 摘要信息	**debug scc acl-show summary**
调试查看当前 SCC 中保存的所有 ACL 信息	**debug scc acl-show all**
显示 SCC 记录的事件轨迹信息	**debug scc event diag** [**ap-mac** *mac-address*] [**type** *type-id*]
显示 SCC 接收消息速率的信息	**debug scc dump msg-rate** [**type** *type-id*]
显示 SCC 内存统计的信息	**debug scc jemalloc**

配置日志和消息记录数

作用	命令
配置 SCC 支持记录的日志和消息最大条目数	**scc event diag** { **log-num** *log-num-count* | **msg-num** *msg-num-count* }

1 GSN

1.1 概述

GSN（Global Security Network，全局安全网络）是一个安全策略平台，包括接入控制和网络安全等一系列安全策略管理。GSN 平台包括设备端和服务器端两个部分。锐捷 SMP（RG Security policy Management Platform，锐捷安全策略管理平台）安全策略服务器提供 GSN 服务器端的功能。

在系统中，GSN 接受 SMP 服务器下发的策略，并在设备上安装，来决定是否允许或者禁止某种条件范围内的数据报文通过安全设备进行传输。这些安全策略包括绑定、隔离和阻断。其中绑定就是在设备上，将用户（通常是在服务器上已认证的用户）的 IP+MAC 进行绑定。而隔离和阻断则是通过设置 ACL 允许或者禁止特定数据的传输。

GSN 配合 SMP 服务器、802.1x 认证、web 认证使用。

下文仅介绍 GSN 设备端的相关内容。

1.2 典型应用

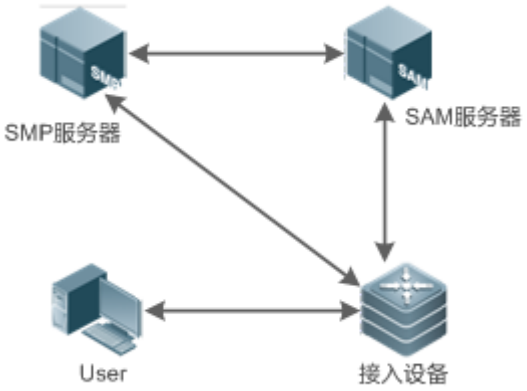
典型应用	场景描述
认证用户 GSN 安全防护	用户通过 802.1x 认证后，SMP 服务器下发安全策略（如 ARP 防攻击、主机完整性等），维护用户的网络安全。

1.2.1 认证用户 GSN 安全防护

应用场景

用户通过 802.1x 认证后，SMP 服务器通过 SAM 服务器学习已通过认证的合法用户的 IP-MAC 对应关系，SMP 下发安全策略到接入设备。

图 1-1



【注释】 流程介绍:

1. 用户先通过 802.1x 认证；
2. SAM 服务器将用户信息反馈给 SMP 服务器；
3. 认证成功后接入设备根据配置决定是否安装用户的地址绑定策略；
4. 之后接入用户端和 SMP 服务器实时交互报文，接入设备负责报文的格式转换和转发工作；
5. SMP 服务器根据接入用户端反馈的信息向接入设备下发安全策略；
6. 此外，SMP 服务器会定时或手工地和设备进行策略同步，如果发现双方维护的策略不一致，则会删除接入设备上的所有策略，之后将 SMP 服务器上维护的策略全部重新向接入设备安装一次；
7. 对于 3、5 和 6 的操作，接入设备根据 GSN 的策略规则执行策略的整理和安装。

功能部署

- 在接入设备上开启 802.1x 认证及部署 SAM 服务器。
- 部署 SMP 服务器，加入接入设备，使得能够下发安全策略。
- 接入设备开启 GSN 及地址绑定功能。

1.3 功能详解

基本概念

↘ 锐捷安全方案组成

锐捷安全解决方案由以下四个元素组成：

- 锐捷安全策略管理平台（RG Security policy Management Platform）
- 锐捷安全客户端（RG Security Agent）
- 锐捷安全修复系统（RG Restore System）

- 锐捷安全设备（RG Security Switch）

锐捷安全策略管理平台（RG Security policy Management Platform）

锐捷安全策略管理平台通过配置策略，来决定是否允许或者禁止某种条件范围内的数据报文通过安全设备进行传输。安装策略就是将策略设置到设备上，卸载策略就是将策略从设备上移除。

锐捷安全客户端

锐捷安全客户端是运行在企业网络中的每一台接入网络的主机上的一个软件，它负责收集客户端信息、认知用户的网络行为、监控客户机的网络通讯和安全状态并将收集到的信息发送到安全策略管理平台以便管理员针对性地制定相应的安全策略。同时安全客户端也将自动地从安全策略管理平台中下载新的安全策略并在本地执行指定的安全策略。

锐捷安全修复系统

安全修复系统对异常行为做如下操作：

对于不符合企业安全策略的用户，管理员在安全策略管理平台上预先配置相应的策略，这些策略可屏蔽这些“非法用户”的绝大部分的网络访问权限，只留下一条绿色的安全通道。该安全通道连接到的主机只能是企业安全策略升级服务器。包括：Windows 补丁升级服务器、防病毒软件的病毒升级库服务器，或是企业的其他升级服务器。

当安全客户端在检测到自身的安全策略不符合管理平台制定的安全等级之后，安全代理会立即将自身的安全日志上传至安全策略管理平台，安全策略管理平台根据接收到安全客户端传来的报警日志从预先配置好的策略集中选择相应的一条，将此条策略下发到所有的安全设备，安全设备接受最新的策略配置后立即应用配置，使该报警的用户只能根据策略服务器规定的恢复动作访问指定的升级服务器，自动安装这些补丁程序。

当用户已经完成了策略服务器规定的一切恢复动作之后，安全客户端会再次对客户端操作平台进行安全检测，如果此时客户端满足所有的安全策略集，安全客户端会通知安全策略管理平台解除对此客户端的访问列表限制，将客户端设置成正常的用户。

锐捷安全设备

做为锐捷安全解决方案的一部分，锐捷安全设备负责从锐捷安全策略管理平台上接收策略，并且实现策略的安装，并根据安装的策略对用户进行控制。

1.4 配置详解

配置项	配置建议 & 相关命令	
配置 GSN 基础功能	⚠ 必须配置。用于开启 GSN 安全方案及同 SMP 服务器的通讯。	
	security gsn enable	打开 GSN 全局配置开关，缺省关闭。
	security { [**v1** | **v2**] **community** *community* | **v3 user** *username* }	配置和 SMP 服务器通信的安全名。
	smp-server host *ip-address*	配置 SMP 服务器地址。
	⚠ 可选配置。用于配置安全事件传输最小时间间隔。	

	security event interval *interval*	配置安全事件传输最小时间间隔配置，interval 的取值范围为 1-65535 秒，缺省情况下该时间间隔为 5 秒。
配置 WLAN 支持地址绑定	可选配置。用于控制是否在 WLAN 上产生地址绑定策略。	
	gsn address-bind	配置 WLAN 上启用地址绑定策略，缺省关闭。

1.4.1 配置 GSN 基础功能

配置效果

- 使设备全局开启 GSN 安全方案。
- 使设备能够同 SMP 服务器通讯。

注意事项

- 配置和 SMP 服务器通讯的安全认证名时，支持 SNMP v1、v2、v3。
- security v1 community 和 security community 效果一样,都是配置 v1，只是为了方便用户配置。如果选择了 v3，则必须在 snmp-server 命令下配置相应的 v3 用户，相关配置命令请参看《SNMP 配置》章节。
- 需要注意 GSN 支持的表项数目。

配置方法

开启 GSN 安全方案全局开关

- 必须配置。
- 若无特殊要求，应在每台需要支持安全方案的设备上启动该功能。

配置与 SMP 服务器通讯

- 必须配置。
- 若无特殊要求，应在每台需要支持安全方案的设备上启动该功能，以实现设备与 SMP 服务器的通讯。

配置 SMP 服务器 IP 地址

- 必须配置。
- 若无特殊要求，应在每台需要支持安全方案的设备上启动该功能，以实现设备与 SMP 服务器的通讯。

配置安全事件传输最小时间间隔

- 为了避免非法用户通过伪造安全事件，频繁地发送安全事件信息对安全设备和 SMP 服务器进行攻击，用户可以通过配置安全事件传输最小时间间隔来限制用户通告安全事件的最小时间间隔。

- 如果需要改变默认的安全事件传输的最小时间间隔，则需要执行该配置项，默认该时间间隔为 5 秒。

相关命令

开启 GSN 安全方案全局开关

【命令格式】 **security gsn enable**
【参数说明】 **-**
【命令模式】 全局模式
【使用指导】 -

配置与 SMP 服务器通讯

【命令格式】 **security** { [**v1** | **v2**] **community** *community* | **v3 user** *username* }
【参数说明】 **community** *community*：指定和 SMP 服务器通讯的安全名。
user *username*：SNMP v3 用户名。

【配置模式】 全局模式
【使用指导】 security v1 community 和 security community 效果一样 ,都是配置 v1 ,只是为了方便用户配置.如果选择了 v3，则需要在 snmp-server 命令下配置相应的 v3 用户，相关配置命令请参看《SNMP 配置》章节。

配置 SMP 服务器 IP 地址

【命令格式】 **smp-server host** *ip-address*
【参数说明】 *ip-address*：指定 SMP 服务器的 IP 地址。
【配置模式】 全局模式
【使用指导】 -

配置安全事件传输最小时间间隔

【命令格式】 **security event interval** *interval*
【参数说明】 **interval** *interval*：指定安全事件传输最小时间间隔，取值范围为 1-65535 秒，缺省情况下该时间间隔为 5 秒。
【配置模式】 全局模式
【使用指导】 -

配置举例

以下配置举例，仅介绍设备开启 GSN 安全方案及与 SMP 服务器通讯相关的配置。

设备开启 GSN 安全方案及与 SMP 服务器通讯

【配置方法】
- 在设备上开启 GSN 安全方案全局开关。
- 配置设备同 SMP 服务器通讯的安全名。
- 配置 SMP 服务器的 IP 地址。

```
Hostname# configure terminal
```

```
Hostname(config)# security gsn enable
Hostname(config)# security v1 community test-name
Hostname(config)# smp-server host 192.168.30.9
Hostname(config)# exit
```

【检验方法】 Show 配置。

- 通过 show smp-server 显示 SMP 服务器的 IP 地址。
- 通过 show security event interval 显示安全事件转输最小时间间隔。

```
Hostname# show smp-server
   SMP-Server IP:192.168.30.9
Hostname# show security event interval
   Event sending interval(Seconds):5
```

常见错误

- SMP 服务器路由不可达

1.4.2 配置 WLAN 支持地址绑定

配置效果

- 用户可以通过该配置来控制是否在 WLAN 产生地址绑定策略。

注意事项

只有全局 GSN 支持功能打开并且配置 WLAN 的安全模式是 WPA 或 WPA2 时，该功能才能起作用。

由于 GSN 应用的特性，当使用该功能时，需要关闭 802.1x 的 IP 授权功能，两者不能共用，否则会影响安全策略的实际运行效果。

配置方法

↘ WLAN 开启支持地址绑定

- 如果需要基于 WLAN 开启地址绑定，则应该执行此配置项。

相关命令

↘ 配置 WLAN 开启地址绑定策略

【命令格式】 **gsn address-bind**

【参数说明】 -

【命令模式】 WLAN 安全配置模式

【使用指导】 -

配置举例

开启 WLAN 支持地址绑定。

【配置方法】

- 创建 WLAN。
- 进入 WLAN 安全配置模式。
- 配置 WLAN 支持地址绑定。

```
Hostname# configure terminal
Hostname(config)# wlansec 100
Hostname(config-wlansec)# gsn address-bind
Hostname(config)# exit
```

1.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看 SMP 服务器 IP 地址	**show smp-server**
查看安全事件传输最小时间间隔	**show security event interval**

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 GSN 各类调试开关	**debug gsn** { **all** | **error** | **event** | **packet** | **server** | **detail** }