目 录

1 User Profile

说明

仅 WX2500H-WiNet 系列不支持 slot 参数。

1.1 User Profile简介

User Profile（用户配置文件）提供一个配置模板，用于保存预设配置（一系列配置的集合）。用户可以根据不同的应用场景在这个配置模板中定义不同的内容。

用户访问设备时，需要先进行上线用户身份认证（User Profile 目前支持 802.1X 和 Portal 等接入认证方式）。用户通过身份认证后，认证服务器会将与用户帐户绑定的 User Profile 名称下发给设备，设备会根据指定 User Profile 里配置的内容对上线用户进行限制。

基于 User Profile 的用户身份认证需要与认证服务器配合使用。

- 若用户采用远程认证，则需要在远程认证服务器上指定与该用户帐户相关联的 User Profile。
- 若用户采用本地认证，则需要在设备对应的本地用户视图中指定该用户的授权 User Profile。关于本地用户的相关配置，请参见“安全配置指导”中的“AAA”。

当用户通过认证上线后，其访问行为将受到 User Profile 的限制。当用户下线时，系统会自动取消相应的限制。因此，User Profile 适用于限制上线用户的访问行为，没有用户上线（例如没有用户接入、用户没有通过认证或者用户下线）时，对应的 User Profile 配置并不生效。

使用 User Profile 之后，可以：

- 更精确地利用系统资源。比如基于接口进行流量监管，此时限制的是一群用户（从指定接口接入的用户）。使用 User Profile 之后，可以基于用户进行流量监管，此时限制的是单个用户。
- 更灵活地限制用户访问系统资源。比如只对当前接口的所有流进行流量监管，当用户的物理位置移动时（比如从另一个接口接入），则需要先取消旧的接入接口下的流量监管功能，再在新的接入接口下配置流量监管功能。使用 User Profile 之后，可以基于用户进行流量监管，只要用户上线，认证服务器会自动下发相应的 User Profile，当用户下线，对应的配置亦会失效，不需要再进行手工调整。

1.2 User Profile配置任务简介

表1-1 User Profile 配置任务简介

配置任务	说明	详细配置
配置User Profile	必选	1.3

1.3 配置User Profile

User Profile 特性支持 802.1X 和 Portal 等接入认证方式，User Profile 是和认证配合使用的，用户需要保证相应的认证配置。同时，需要在本地或服务器上配置指定下发给用户的 User Profile。还可以为会话指定进入的队列，从而由队列的不同决定其不同优先级的调度方式。

表1-2 创建 User Profile

操作	命令	说明
进入系统视图	**system-view**	-
创建User Profile并进入相应的User Profile视图	**user-profile** *profile-name*	如果指定的User Profile已经存在，则直接进入相应的User Profile视图，不需要再创建

User Profile 创建之后，需要在 User Profile 视图下配置具体的内容才能对上线用户进行限制。

1.4 User Profile显示和维护

在任意视图下执行 **display** 命令可以显示 User Profile 的配置信息和在线用户信息，通过查看显示信息验证配置的效果。

表1-3 显示 User Profile

操作	命令
显示user profile的配置信息和在线用户信息	**display user-profile** [**name** *profile-name*] [**slot** *slot-number*]

1.5 User Profile典型配置举例

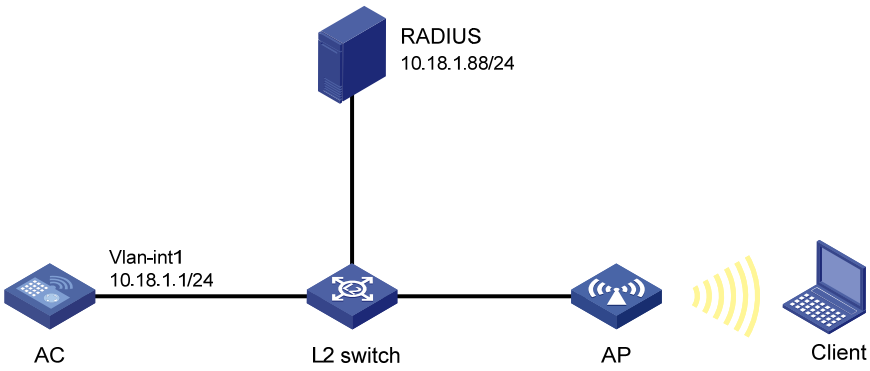
1.5.1 使用RADIUS服务器进行MAC地址认证的User Profile典型配置举例

1. 组网需求

- AC 和 RADIUS 服务器通过交换机建立连接。AC 的 IP 地址为 10.18.1.1，与 AC 相连的 RADIUS 服务器的 IP 地址为 10.18.1.88。
- 要求使用 MAC 认证方式进行用户身份认证。
- 要求 MAC 地址认证用户在指定的 AP 上接入无线网络。

2. 组网图

图1-1 使用 RADIUS 服务器进行 MAC 地址认证典型配置组网图



3. 配置步骤

说明

确保 RADIUS 服务器与设备路由可达，完成服务器的配置，并成功添加了接入用户账户，用户名为 123，密码为 aaa_maca。

(1) 配置 RADIUS 方案

配置 Radius 方案，名称为 imcc，认证服务器的 IP 地址为 10.18.1.88，端口号为 1812，配置计费服务器的 IP 地址为 10.18.1.88，端口号为 1813，认证密钥为明文 12345678，计费密钥为明文 12345678，用户名格式为 without-domain。

```
<AC> system-view
[AC] radius scheme imcc
[AC-radius-imcc] primary authentication 10.18.1.88  1812
[AC-radius-imcc] primary accounting 10.18.1.88  1813
[AC-radius-imcc] key authentication simple 12345678
[AC-radius-imcc] key accounting simple 12345678
[AC-radius-imcc] user-name-format without-domain
[AC-radius-imcc] quit
```

(2) 配置 ISP 域的 AAA 方法

配置名称为 imc 的 ISP 域，并将认证、授权和计费的方式配置为使用 Radius 方案 imcc。

```
[AC] domain imc
[AC-isp-imc] authentication lan-access radius-scheme imcc
[AC-isp-imc] authorization lan-access radius-scheme imcc
[AC-isp-imc] accounting lan-access radius-scheme imcc
[AC-isp-imc] quit
```

(3) 配置 MAC 地址认证

配置 MAC 地址认证用户名格式为固定用户名格式，用户名为 123，密码为明文 aaa_maca（若配置成大写、不带连字符的 mac 地址格式，服务器需要配置与之对应的用户名格式；若配置成固定用户名格式，服务器也需要配置与其对应的用户名格式）。

```
[AC] mac-authentication user-name-format fixed account 123 password simple aaa_maca
```

配置无线服务模板 maca_imc 的 SSID 为 maca_imc，并设置用户认证方式为 MAC 地址认证，ISP 域为 imc。

```
[AC] wlan service-template maca_imc
[AC-wlan-st-maca_imc] ssid maca_imc
[AC-wlan-st-maca_imc] client-security authentication-mode mac
[AC-wlan-st-maca_imc] mac-authentication domain imc
```

无线服务模板使能。

```
[AC-wlan-st-maca_imc] service-template enable
[AC-wlan-st-maca_imc] quit
```

(4) 配置手工 AP 并将无线服务模板绑定到 radio 上

创建 ap1。

```
[AC] wlan ap ap1 model WA5320E-WiNet
[AC-wlan-ap-ap1] serial-id 219801A1FF8171E00361
```

配置信道为 149，并使能射频。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] channel 149
[AC-wlan-ap-ap1-radio-1] radio enable
```

绑定无线服务模板。

```
[AC-wlan-ap-ap1-radio-1] service-template maca_imc
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

(5) 配置 User Profile

配置名称为 macauth1 的 AP 组，在 AP 组内添加允许接入的 AP 列表

```
[AC]wlan ap-group macauth1
[AC-wlan-ap-group-macauth1] ap ap1
[AC-wlan-ap-group-macauth1] quit
```

配置基于 MAC 地址认证用户的 user-profile，名称为 mac1。添加允许接入的 AP 组为 macauth1，让用户只能够在指定 AP 组 macauth1 的 AP1 上接入，控制用户在无线网络中接入位置。

```
[AC] user-profile mac1
[AC-user-profile-mac1] wlan permit-ap-group macauth1
[AC-user-profile-mac1] quit
```

(6) 配置 RADIUS server（iMC V7）

说明

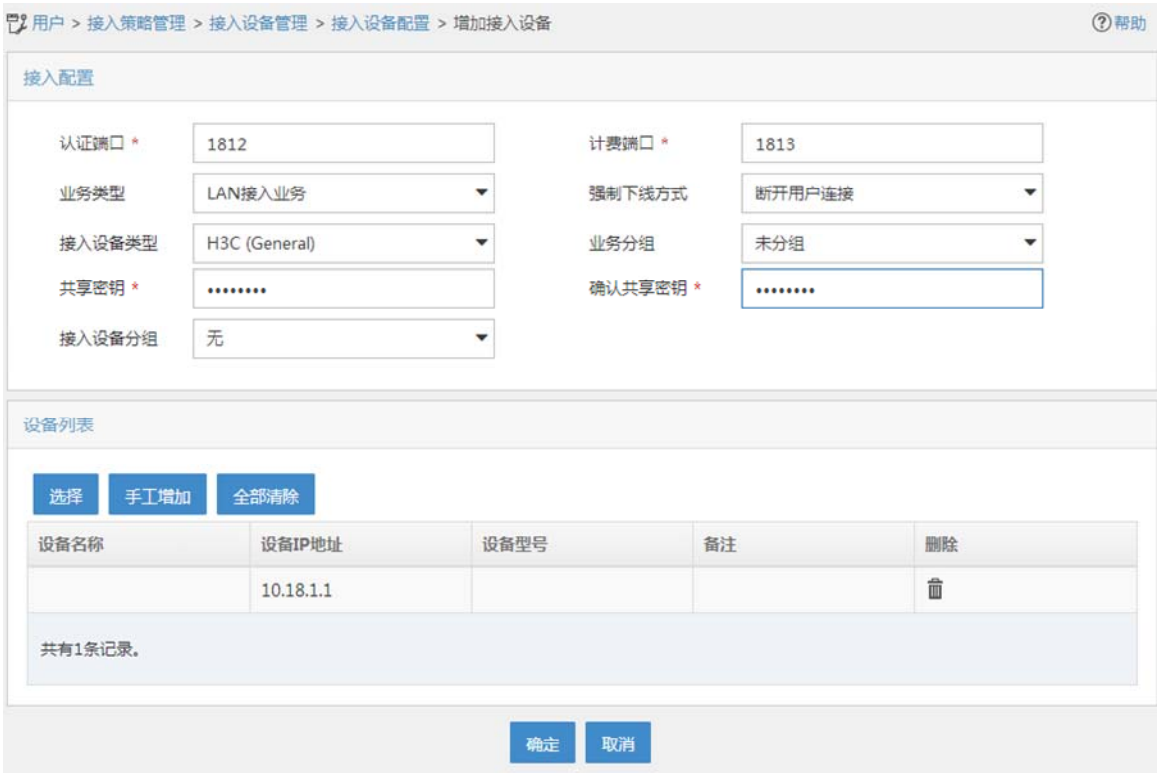
下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 7.2、iMC EIA 7.2），说明 RADIUS server 的基本配置。

增加接入设备。

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备管理页面，点击页面中的进入接入设备配置按钮，进入接入设备配置页面，在该页面中单击“增加”按钮，进入增加接入设备页面。

- 设置认证、计费共享密钥为 12345678，其它保持缺省配置；
- 选择或手工增加接入设备，添加 IP 地址为 10.18.1.1 的接入设备。

图1-2 增加接入设备页面

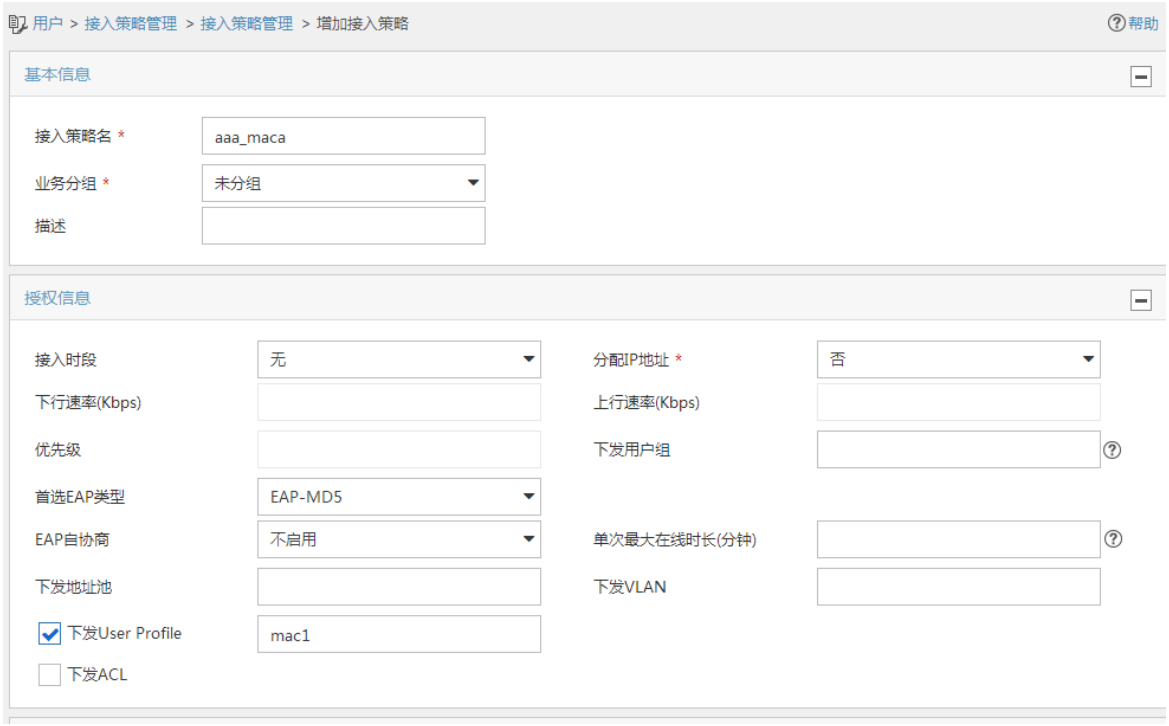


增加服务策略。

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，进入接入策略管理页面，在该页面中单击“增加”按钮，进入增加接入策略页面。

设置接入策略名为 aaa_maca，其它保持缺省配置。

图1-3 增加服务策略页面

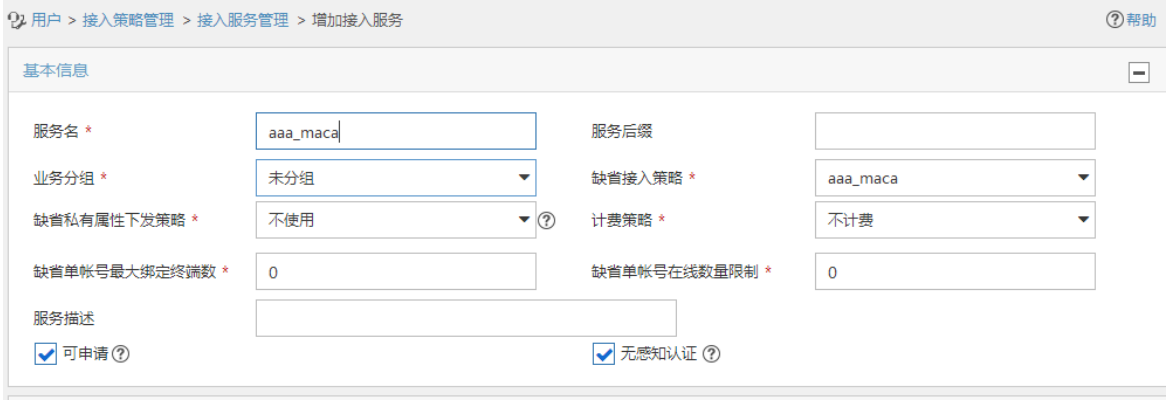


增加接入服务。

选择“用户”页签，单击导航栏中的[接入策略管理/接入服务管理]菜单项，进入接入服务管理页面，在该页面中单击<增加>按钮，进入增加接入服务页面。

- 设置服务名为 aaa_maca；
- 设置缺省接入策略为已经创建的 aaa_maca。

图1-4 增加接入服务页面



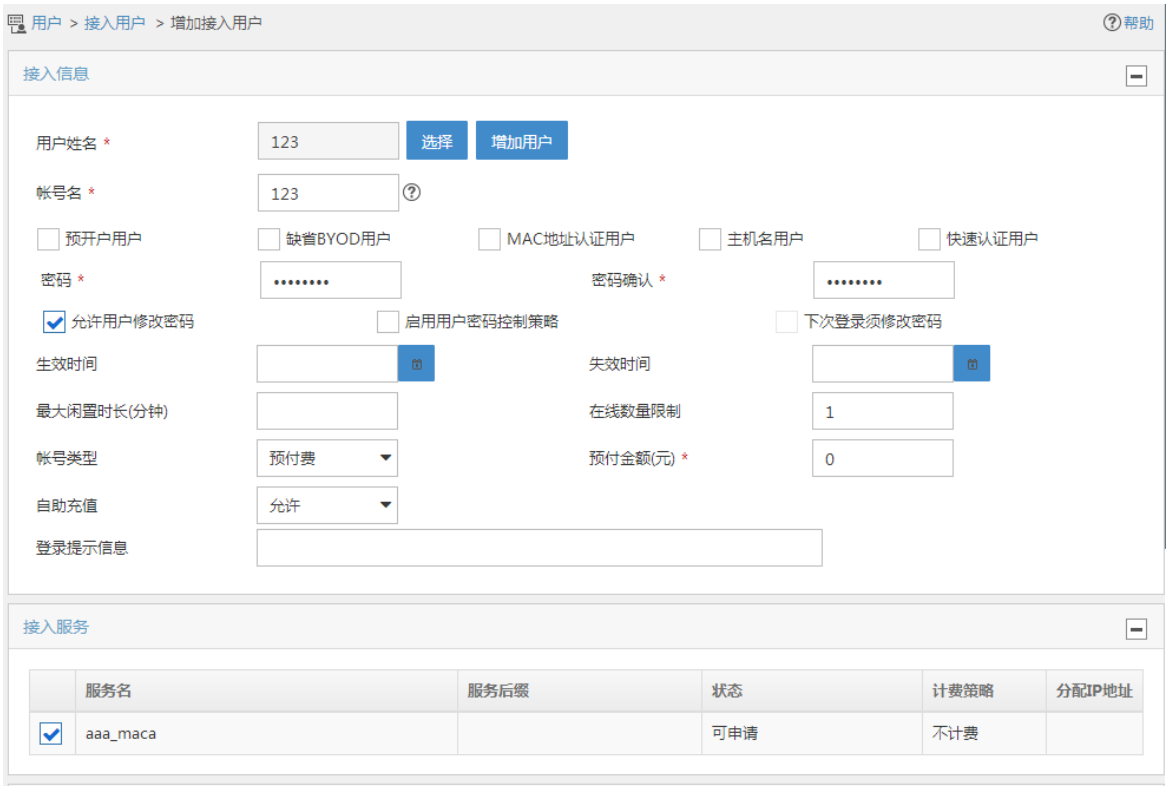
增加接入用户。

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，进入接入用户页面，在该页面中单击<增加>按钮，进入增加接入用户页面。

- 添加用户 123；

- 添加帐号名为 123，密码为 aaa_maca；
- 选中之前配置的服务 aaa_maca。

图1-5 增加接入用户页面



4. 验证结果

客户端通过 MAC 认证成功关联 AP，并且可以访问无线网络。

通过 **display mac-authentication connection** 命令显示 MAC 用户连接信息。

```
[AC] display mac-authentication connection
Total connections: 1

User MAC address              : 0452-f33a-02fa
AP name                       : ap1
Radio ID                      : 1
SSID                          : maca_imc
BSSID                         : 741f-4a35-7b40
Username                      : 123
Authentication domain         : imc
Initial VLAN                  : 1
Authorization VLAN            : N/A
Authorization ACL number      : N/A
Authorization user profile    : mac1
Termination action            : Default
Session timeout period        : 86400 s
Online from                   : 2016/06/23 20:42:00
```

```
Online duration                : 0h 0m 21s
```

通过 **display wlan client** 显示命令查看无线客户端在线情况查看 MAC 地址认证用户上线信息，可看到 MAC 地址认证用户成功上线。

```
[AC] display wlan client
Total number of clients: 1

MAC address     Username   AP name      RID   IP address      IPv6 address   VLAN
0452-f33a-02fa  123        ap1          1     10.18.1.100     N/A            1
```