802.1X典型配置案例

iMC 802.1X Radius 王波 2020-04-27 发表

组网及说明

1 配置需求或说明

本案例是通用802.1X认证，不包含任何接入控制和安全检查，仅进行身份验证。

1.1 适用场合

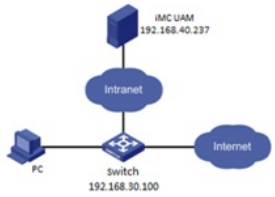
适用于不要求进行接入控制和安全检查的企业网或校园网。

1.2 配置前提

接入设备需支持802.1X协议。

1.3 组网需求

某公司计划启用802.1X认证，用户接入网络时需要进行身份验证。具体的组网如图1所示。UAM服务器IP地址为192.168.40.237，接入设备IP地址为192.168.30.100。PC安装了Windows操作系统，并准备安装iNode客户端。



配置步骤

2.1 iMC 侧配置

1. 增加接入设备

增加接入设备是为了建立iMC服务器和接入设备之间的联动关系。

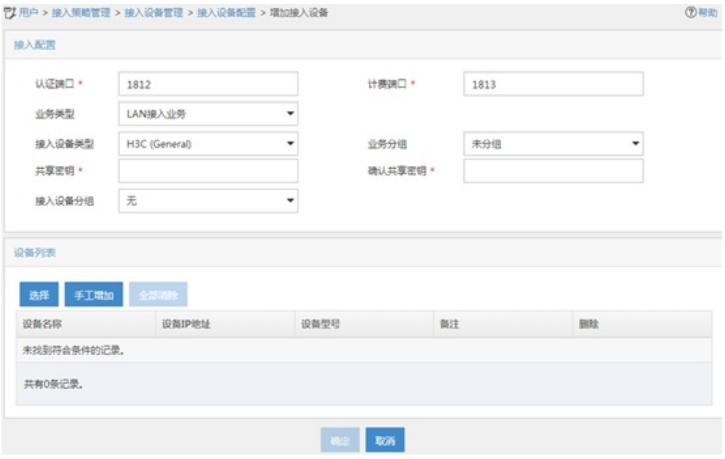
增加接入设备的方法如下：

(1) 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，进入接入设备配置页面，如图2所示。

图2 进入接入设备列表

(2) 单击<增加>按钮，进入增加接入设备页面，如图3所示。

图3 增加接入设备页面



(3) 配置接入设备。

配置接入设备有两种方法：

·在设备列表中单击<选择>按钮从iMC平台中选择设备

·在设备列表中单击<手工增加>按钮，手工配置接入设备。

无论采用哪种方式接入设备的IP地址都必须满意以下要求：

·如果在接入设备上配置radius scheme时配置了nas ip命令，则UAM中接入设备的IP地址必须与nas ip的配置保持一致。

·如果未配置nas ip命令，则UAM中接入设备的IP地址必须是设备连接UAM服务器的接口IP地址（或接口所在VLAN的虚接口IP地址）。

从iMC平台中选择设备时，设备的IP地址无法修改。因此如果设备加入iMC平台时使用的IP地址不满足上述要求，则可以采用手工增加的方式增加接入设备。本例采用手工增加的方式进行说明。

单击设备列表中的<手工增加>按钮，弹出手工增加接入设备窗口，如图4所示。输入接入设备的IP地址，单击<确定>按钮，返回增加接入设备页面。

图4 手工输入接入设备的IP地址

(4)　配置公共参数。

公共参数的配置要求如下：

·认证端口：UAM监听RADIUS认证报文的端口。此处的配置必须与接入设备命令行配置的认证端口保持一致。UAM和接入设备一般都会采用默认端口1812。

·计费端口：UAM监听RADIUS计费报文的端口。此处的配置必须与接入设备命令行配置的计费端口保持一致。UAM和接入设备一般都会采用默认端口1813。

目前仅支持将UAM同时作为认证和计费服务器，即不支持将UAM作为认证服务器，而其他服务器作为计费服务器的场景。

·业务类型：在下拉框中选择该设备承载的业务，包括LAN接入业务和设备管理业务。前者用于用户接入和使用网络，后者用于设备管理员登录和管理设备。

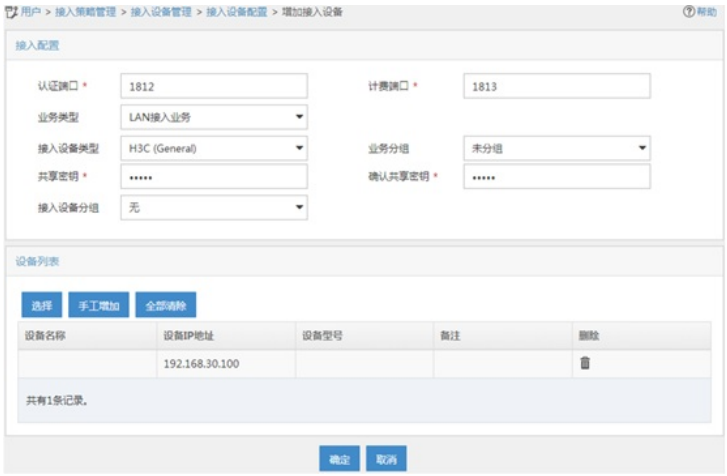
·接入设备类型：在下拉框中选择接入设备的厂商和类型。下拉框中包含了Standard、UAM系统预定义和管理员自定义的厂商和类型。支持标准RADIUS协议的设备都可以选择Standard。系统预定义的厂商和类型有以下几种，包括H3C(General)、3COM(General)、HUAWEI(General)、CISCO(General)、RG(General)、HP(MSM)、HP(Comware)、MICROSOFT(General)、JUNIPER(General)和HP(Pro Curve)。

·业务分组：在下拉框中选择接入设备所属的业务分组。将接入设备加入不同的业务分组以便进行分权管理。

·共享密钥/确认共享密钥：输入两次相同的共享密钥。接入设备与UAM配合进行认证时，使用该密钥互相验证对方的合法性。此处的配置必须与接入设备命令行配置的共享密钥保持一致。如果系统参数中的“密钥显示方式”设置为明文时，只需输入一次共享密钥即可。

·接入设备分组：在下拉框中选择接入设备需要加入的接入设备分组。可选项包括UAM中已经存在的接入设备分组和“无”。接入设备分组是区分终端用户的接入条件之一。

图5 公共参数配置



(5)　单击<确定>按钮，增加接入设备完毕，进入结果显示页面。点击“返回接入设备列表”链接，返回接入设备配置页面，可在接入设备列表中查看新增的接入设备，如图6所示。

图6 查看新增的接入设备

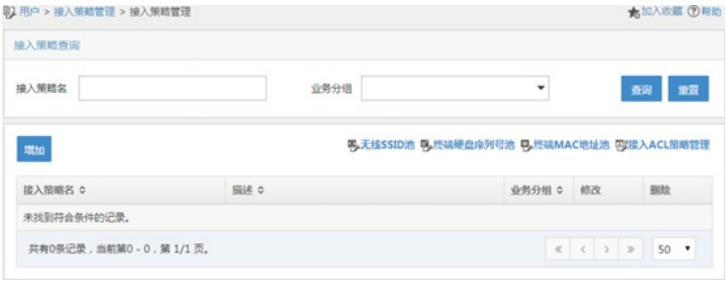
2. 增加接入策略

配置一个不进行任何接入控制的接入策略。

增加接入策略的方法如下：

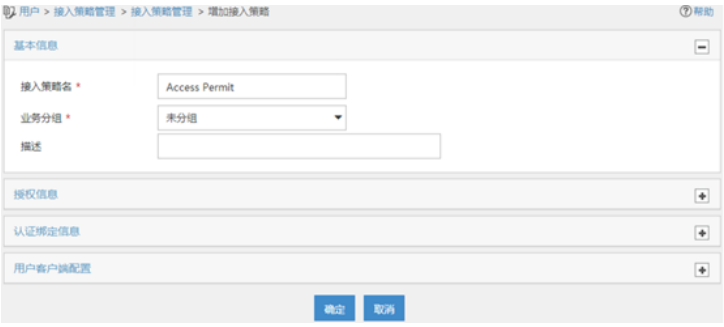
(1)　选择“用户”页签，单击导航树中的“接入策略管理 > 接入策略管理”菜单项，进入接入策略管理页面，如图7所示。

图7 进入接入策略列表



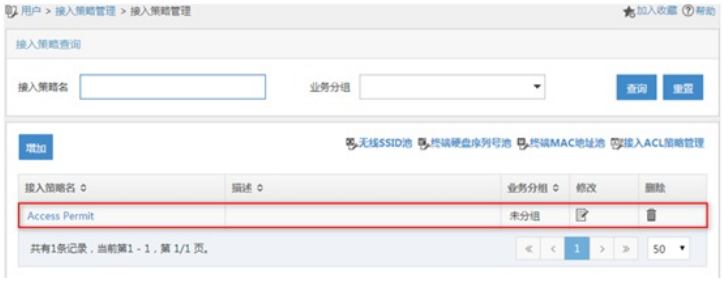
(2)　单击<增加>按钮，进入增加接入策略页面，如图8所示。由于不进行任何接入控制，因此只需输入接入策略名，其他参数均保持为空即可。

图8 增加接入策略页面



(3)　单击<确定>按钮，接入策略增加完毕。返回接入策略管理页面，可在接入策略列表中查看新增的接入策略，如图9所示。

图9 查看增加的接入策略



3. 增加接入服务

接入服务是对用户进行认证授权的各种策略的集合。本例不对用户进行任何接入控制，因此只需增加一个简单的接入服务即可。

增加接入服务的方法如下：

(1)　选择“用户”页签，单击导航树中的“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，如图10所示。

图10 进入接入服务列表

(2)　单击<增加>按钮，进入增加接入服务页面，如图11所示。

图11 增加接入服务页面

配置服务的各个参数：

·服务名：输入服务名称，在UAM中必须唯一。

·服务后缀：服务后缀、认证连接的用户名、设备的Domain和设备Radius scheme中的命令这四个要素密切相关，具体的搭配关系请参见表1。

·缺省接入策略：选择之前新增的接入策略。

·其他参数：保持缺省值。

表1 iMC中服务后缀的选择

认证连接用户名	设备用于认证的Domain	设备Radius scheme中的命令	iMC中服务的后缀
X@Y	Y	user-name-format with-domain	Y
		user-name-format without-domain	无后缀
X	[Default Domain]设备上指定的缺省域	user-name-format with-domain	[Default Domain]
		user-name-format without-domain	无后缀

(3)　单击<确定>按钮，接入服务增加完毕。返回接入服务管理页面，可在接入服务列表中查看新增的接入服务，如图12所示。

图12 查看增加的接入服务

4. 增加接入用户

接入用户是用户接入网络时使用的身份证，包含帐号名、密码和使用的服务等信息。

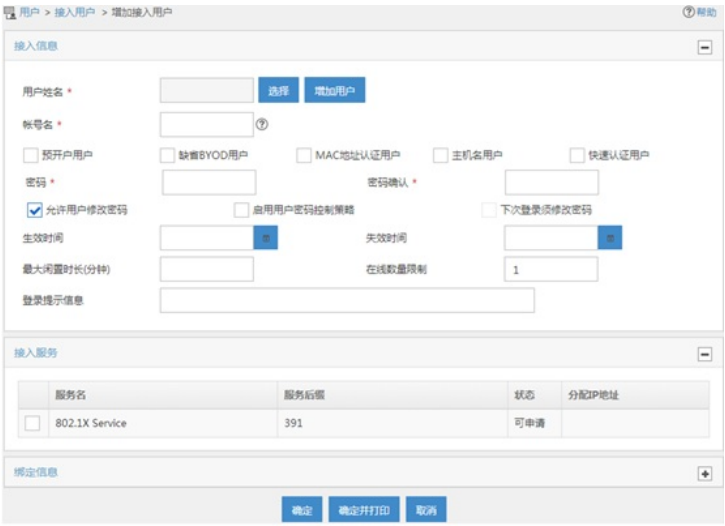
增加接入用户的方法如下：

(1)　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，如图13所示。

图13 接入用户页面

(2)　单击<增加>按钮，进入增加接入用户页面，如图14所示。

图14 增加接入用户页面



配置接入信息和接入服务：

·用户姓名：接入用户所关联的iMC平台用户。有两种方式关联平台用户：

¡ 单击<选择>按钮，弹出选择用户窗口，单击<查询>按钮，可以查询出所有已存在的平台用户，如图15所示，选择一个用户后单击<确定>按钮。

¡ 单击<增加用户>按钮，弹出增加用户窗口，如图16所示，输入用户名、证件号码以及其他参数后单击<确定>按钮。

图15 选择平台用户

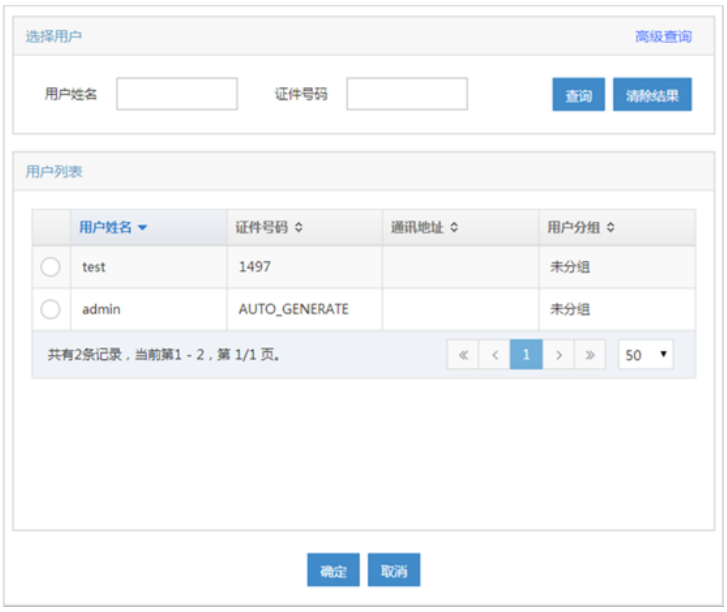


图16 新增平台用户

·帐号名：输入用于认证的帐号名，在UAM中必须唯一。

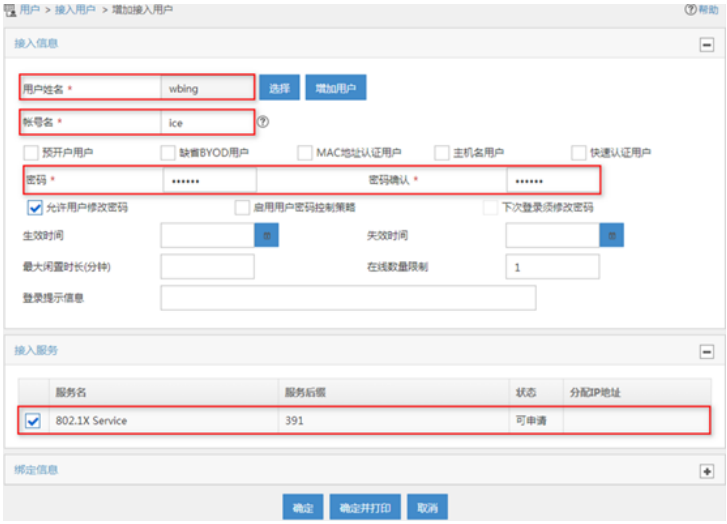
·密码/确认密码：输入两次相同的密码。

·接入服务：选择之前增加的接入服务。

·其他参数：保持缺省值。

参数设置完成后的效果图如图17所示。

图17 接入用户



(3)　单击<确定>按钮，接入用户增加完毕。返回接入用户页面，可在接入用户列表中查看新增的接入用户，如图18所示。

图18 查看新增的接入用户

2.2 设备配置

接入设备用于控制用户的接入。通过认证的用户可以接入网络，未通过认证的用户无法接入网络。

以下使用Windows的CLI窗口telnet到接入设备并进行配置，具体的命令及其说明如下：

<H3C>system-view

System View: return to User View with Ctrl+Z.

#创建RADIUS方案1xallpermit

[H3C]radius scheme 1xallpermit

New Radius scheme

#认证、计费服务器都指向UAM，认证、计费端口与UAM中增加接入设备时的配置保持一致。

[H3C-radius-1xallpermit]primary authentication 192.168.40.237 1812

[H3C-radius-1xallpermit]primary accounting 192.168.40.237 1813

#认证、计费共享密钥与UAM中增加接入设备时的配置保持一致。

[H3C-radius-1xallpermit]key authentication movie

[H3C-radius-1xallpermit]key accounting movie

#本地采用携带Domain的认证方式。UAM、设备中配置的搭配关系请参见3. (2)图11表1。

[H3C-radius-1xallpermit]user-name-format with-domain

[H3C-radius-1xallpermit]quit

#创建域391，根据3. (2)图11表1中的搭配，domain的名称必须与UAM中服务的后缀保持一致。

[H3C]domain 391

New Domain added.

#认证、授权、计费都采用之前配置的Radius scheme 1xallpermit。

[H3C-isp-391]authentication lan-access radius-scheme 1xallpermit

[H3C-isp-391]authorization lan-access radius-scheme 1xallpermit

[H3C-isp-391]accounting lan-access radius-scheme 1xallpermit

[H3C-isp-391]quit

#只有在全局和接口上都启用802.1X认证，802.1X认证才生效。

[H3C]dot1x

802.1X is enabled globally.

[H3C]dot1x interface Ethernet 1/0/1

802.1X is enabled on port Ethernet1/0/1.

#802.1X的认证方式包括PAP、CHAP和EAP。如果进行证书认证，则必须设置为EAP。

[H3C]dot1x authentication-method chap

2.3 使用iNode PC客户端完成802.1X接入验证

用户使用iNode PC客户端和配置的帐号名、密码进行802.1X认证，最终用户通过认证，完成802.1X接

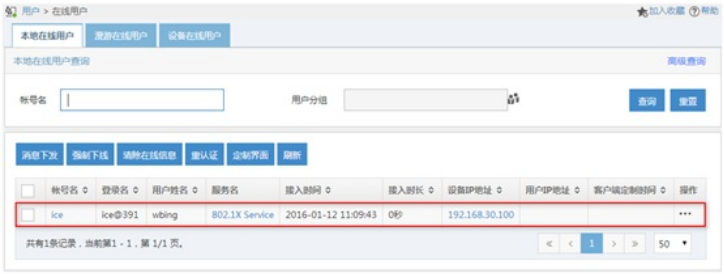
入。
验证步骤如下：
1.安装具有802.1X功能的iNode PC客户端
注意，iNode客户端版本必须与iMC UAM配套，具体的配套关系请参见UAM版本说明书。
2. 进行802.1X认证连接
(1)　在iNode PC客户端主页面，选择“802.1X连接”，展开802.1X连接区域，如图19所示。
图19 iNode客户端主界面

(2)　输入用户名和密码后，单击<连接>按钮，如图20所示，开始认证。
图20 认证界面

认证成功的界面如图21所示，验证了本案例的配置正确。
图21 认证成功

3. 在UAM中查看在线用户
在UAM配置页面中，选择“用户”页签，单击导航树中的“接入用户管理 > 在线用户”菜单项，默认进入本地在线用户页签页面，可查看在线用户，如图22所示。

图22 在线用户



配置关键点