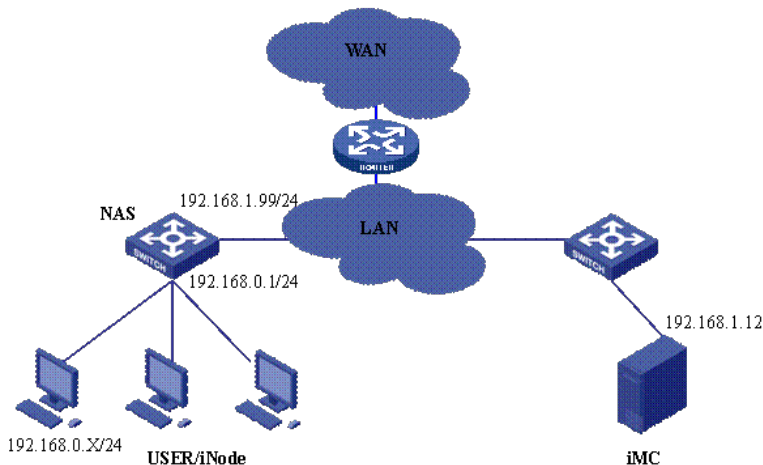


iMC与我司交换机配合做802.1x认证的典型配置

一、组网需求:

支持802.1x特性的交换机; iMC服务器; iNode客户端。

二、组网图:



设备说明:

NAS: S3652

iMC: V3.2 E0401P05或更高版本。其IP地址为192.168.1.12

iNode: V2.4-F0335或更高版本。

三、配置步骤:

前提条件是iMC、NAS、User均路由可达。

1. 配置NAS

配置Radius服务器

[H3C]radius scheme test

//radius策略取名只要符合字符要求即可, 此例中取名为test

[H3C -radius-h3c]server-type extended

//服务类型选择为extended, 表示启用的是扩展类型。可以配合iMC使用更多扩展特性。若选择为standard, 则仅仅只能做简单的身份认证。

[H3C -radius-h3c]primary authentication 192.168.1.12 1812

[H3C -radius-h3c]primary accounting 192.168.1.12 1813

//配置radius服务器的IP地址, 本例中radius服务器的IP地址为192.168.1.12, 认证和计费端口分别为1812和1813

[H3C -radius-h3c]key authentication h3c

[H3C -radius-h3c]key accounting h3c

//认证和计费的共享密钥必须一致。此例中密钥设置为h3c。当然也可根据情况设置为其符合要求的字符。

[H3C -radius-h3c]user-name-format without-domain

配置认证域domain

[H3C]domain h3c

//域名的取名只要是符合要求的字符均可。本例中名称取为h3c。

[H3C -domain-h3c]radius-scheme test

//将预先定义的radius策略引用到新建的domain中。

[H3C]domain default enable test

//将交换机上的缺省domain设置为定义的test

以上的关于domain部分的配置是针对ComwareV3平台的设备而言。若是使用ComwareV5平台的设备做NAS设备, 其domain部分的配置有些区别, 需加上AAA认证中的authorization。802.1x的对应的类型是lan-access。具体的配置命令可参考设备的配置手册。

```
#
domain h3c
authentication lan-access radius-scheme test
authorization lan-access radius-scheme test
```

```
# 配置VLAN
[H3C]Vlan 2
[H3C-vlan2]Port interface GigabitEthernet1/1/1 to GigabitEthernet1/1/4
[H3C]Interface vlan 2 //管理Vlan
[H3C -Interface-vlan-2]ip add 192.168.1.99 255.255.255.0
[H3C]Interface vlan 1 //用户Vlan
[H3C -Interface-vlan-1]ip add 192.168.0.1 255.255.255.0

# 启动802.1X认证
[H3C] dot1x //全局启动802.1x
[H3C]interface Ethernet 1/0/1 //准备对接口启用802.1x
[H3C-Ethernet1/0/1]dot1x
//表示对下行口Ethernet 1/0/1 接口 (连接客户端PC的接口) 启动802.1x认证, 当然如果配置[H3C] dot1x interface Ethernet 1/0/1 to Ethernet 1/0/48则表示Ethernet 1/0/1 到 Ethernet 1/0/48所有下行口都启用dot1x认证。但不能对连接认证服务器的上行口启动dot1x。
```

注：这里只是列出了802.1X的所有必须的配置，还有一些高级选项可以自行配置，如 version check、accounting on等。具体的配置命令参考设备的配置手册。

2. 配置iMC

1). 配置接入设备参数：业务>>接入业务>>接入设备配置

这里必须将NAS的上行端口（靠近iMC的端口）地址添加到起始地址和结束地址之间。共享密钥和端口必须与设备的配置一致。

The screenshot displays the iMC management interface for configuring access devices. It is divided into three main sections:

- 接入设备查询 (Access Device Search):** A search form with fields for '设备IP地址 从' (Device IP Address From), '到' (To), '设备名称' (Device Name), and '接入设备类型' (Access Device Type). A '查询' (Search) button is present.
- 接入设备列表 (Access Device List):** A table showing one device:

设备名称	设备IP地址	设备型号	接入设备类型	接入配置信息
AR28-11	3.3.3.3	Huawei AR28-11	H3C	
- 接入配置 (Access Configuration):** A form for configuring the selected device. Fields include:
 - 共享密钥 (Shared Key): h3c
 - 认证端口 (Authentication Port): 1812
 - 计费端口 (Billing Port): 1813
 - 业务类型 (Service Type): LAN接入业务
 - 接入设备类型 (Access Device Type): H3C
- 手工增加接入设备 (Manually Add Access Device):** A dialog box with the following fields:
 - * 起始IP地址 (Start IP Address): 192.168.1.99
 - 结束IP地址 (End IP Address): (empty)

如果接入认证设备为iMC网管中已有的被管理设备，在增加接入设备时可选择上述图中的【选择】，然后查询出网管中现有的设备作为接入认证的设备。

业务 >> 接入业务 >> 接入设备配置 >> 增加接入设备

接入配置

* 共享密钥: h3c
 * 认证端口: 1812
 * 业务类型: LAN接入业务
 * 计费端口: 1813
 * 接入设备类型: H3C

设备列表

选择 手工增加 全部清除

共有0条记录。

设备名称	设备IP地址	设备型号	删除
------	--------	------	----

若是要修改，请在修改完成后点击手工生效按钮。

接入业务

- 服务配置管理
- 接入区域策略管理
- 接入时段策略管理
- 接入设备配置
- 接入业务拓扑视图
- Portal服务管理
- 业务参数配置
 - 系统参数配置
 - 证书配置
 - 客户端升级配置
 - 系统配置手工生效

业务 >> 接入业务 >> 系统配置手工生效

系统配置手工生效成功。

2). 配置iMC服务: 业务>>接入业务>>服务配置管理>>增加服务配置
 服务名可根据需求取名。其他选项如无要求可不填。然后确定即可。

业务 >> 接入业务 >> 服务配置管理 >> 增加服务配置

增加服务配置

基本信息

* 服务名: service
 * 业务分组: 未分组
 * 安全策略: 不使用安全策略
 服务描述:
 LDAP优先级:
 可申请

授权信息

* 接入时段: 无
 * 不绑定接入区域: 无
 下行速率: kbps
 上行速率: kbps
 优先级:
 证书认证: 不启用 EAP证书认证 WAP证书认证

3). 开户: 创建帐号。
 创建帐号时，首先增加用户姓名。例如“张三”。

用户 >> 增加用户

增加用户

基本信息

* 用户姓名: 张三
 * 证件号码: 123
 通讯地址:
 电话:
 电子邮件:
 * 用户分组: 未分组

确定 取消

增加用户名称之后，继续选择“增加用户帐号”，此过程是创建帐号、密码及选择绑定服务的过程。

用户 >> 增加用户结果

增加用户“张三”成功。

增加用户完成，您可继续选择如下操作：

增加用户帐号	增加接入用户帐号。
返回用户列表	返回所有用户的列表。
查看用户详细信息	查看刚刚增加的用户的信息。
继续增加用户	继续增加新的用户。



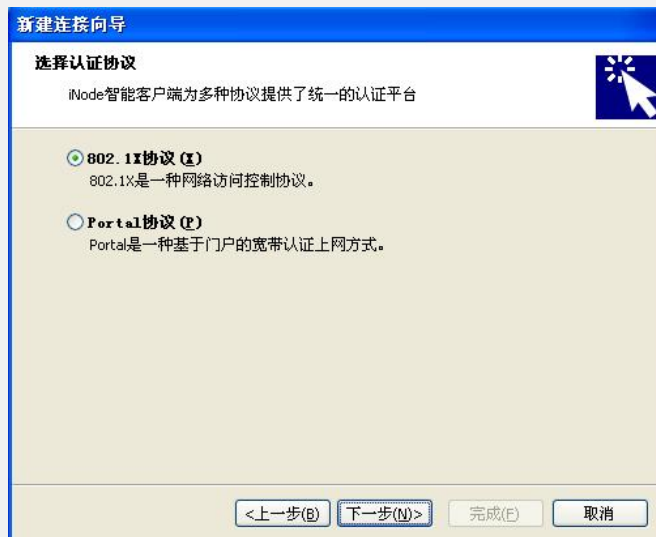
当帐号“zhangsan”创建好后，所有的基本配置结束。也可在此基础上做其他功能的配置。

3. 配置客户端

1) 在iNode客户端中点击<创建一个新的连接>创建802.1x认证连接



2) 选择基本的认证方式，本例中为802.1X认证，所以选择<802.1x协议>，然后选择<普通连接>即可。



新建连接向导

选择连接类型

协议当前所支持的连接类型

- 普通连接 (C)**
您将需要一个用户名和密码来创建新的连接。
- 快速认证连接 (Q)**
使用特定的用户名和密码来创建新的连接。
- 域统一认证连接 (U)**
在登录Windows域之前首先使用域登录口令进行身份认证，如果域统一认证成功，登录域后您就可以直接访问网络了。

<上一步(B) 下一步(N)> 完成(F) 取消

3)然后填入帐号名和密码。图中的“用户名”是指iMC系统中的帐户名（例如“zhangsan”），而非用户姓名（张三）。

新建连接向导

帐户信息

您需要用户名和密码来访问网络，使用证书认证将增强通信的安全性。

连接名(C):

用户名(U):

密码(P):

保存用户密码(D)

域(D):

启用高级认证(E)

- MAC认证(M)
- 智能卡认证(K)
- 证书认证(I)

证书设置(S)...

<上一步(B) 下一步(N)> 完成(F) 取消