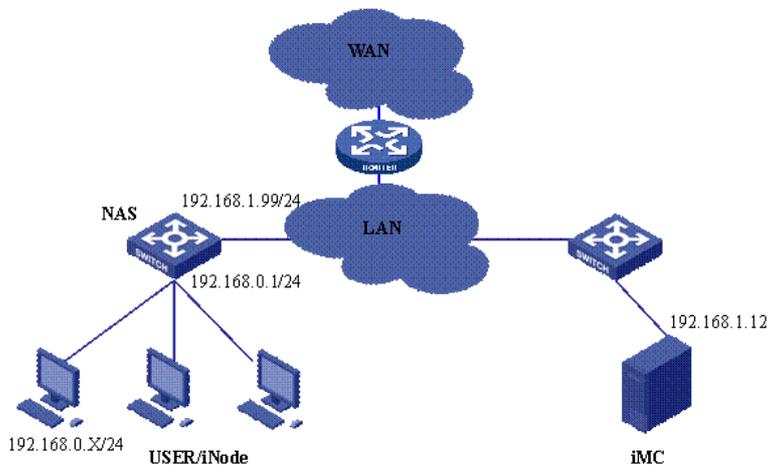


知 V7 iMC与我司交换机配合做802.1x认证的典型配置

802.1X iNode 马光彬 2015-09-08 发表

支持802.1x特性的交换机；iMC服务器；iNode客户端。



设备说明:

NAS: S3652

iMC: 7.0E0102或更高版本。其IP地址为192.168.1.12

iNode: V2.4-F0335或更高版本。

前提是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-isp-h3c] authentication lan-access radius-scheme test
```

```
[H3C-isp-h3c] authorization lan-access radius-scheme test
```

```
[H3C-isp-h3c] accounting lan-access radius-scheme test
```

```
[H3C]domain default enable test
```

//将交换机上的缺省domain设置为定义的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] dot 1x 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。

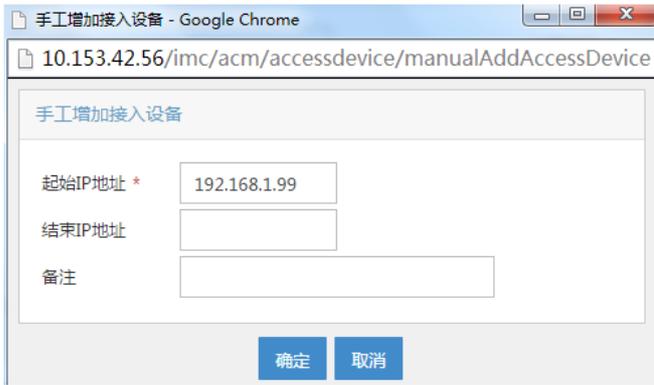
注：这里只是列出了802.1X的所有必须的配置，还有一些高级选项可以自行配置，如version check、accounting on等。具体的配置命令参考设备的配置手册。

2. 配置iMC

1). 配置接入设备参数：用户>>接入策略管理>>接入设备管理>>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。





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。



若是要修改，请在修改完成后点击手工生效按钮。



2) 增加接入策略：用户>>接入策略管理>>接入策略管理>>增加接入策略

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略

基本信息

接入策略名 * 1x

业务分组 * 未分组

描述

授权信息

接入时段 无 分配IP地址 * 否

下行速率(Kbps)

上行速率(Kbps)

优先级

证书认证 不使用 EAP证书认证 WAPI证书认证 启用RSA认证

3). 配置IMC服务: 用户>>接入策略管理>>接入服务管理>>增加接入服务

服务名可根据需求取名。接入策略选择前面创建的1x。其他选项如无要求可不填。然后确定即可。

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

基本信息

服务名 * service1

业务分组 * 未分组

缺省安全策略 * 不使用

缺省私有属性下发策略 * 不使用

计费策略 * 不计费

缺省单帐号最大绑定终端数 * 0

服务描述

可申诉

缺省单帐号 * 1x

缺省内网外连策略 * 不使用

缺省移动办公策略 * 不使用

缺省单帐号在线数量限制 * 0

Portal无感知认证

4). 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

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

增加用户完成, 您可继续选择如下操作:

增加接入用户 增加接入用户帐号。

增加EoC用户 增加EoC用户

返回用户列表 返回用户列表。

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。

用户 > 接入用户 > 增加接入用户

接入用户

接入信息

用户姓名 * 张三 选择 增加用户

帐号名 * zhngsan

预开户用户 缺省BYOD用户 MAC地址认证用户 主机名用户 快速认证用户

密码 * 密码确认 *

允许用户修改密码 启用用户密码控制策略 下次登录须修改密码

生效时间 失效时间

最大闲置时长(分钟) 在线数量限制 1

帐号类型 预付费 预付款额(元) * 0

当帐号“zhngsan”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。



3) 然后填入帐号名和密码。图中的“用户名”是指iMC系统中的帐号名（例如“zhangsan”），而非用户名（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(N): 我的802.1X连接

用户名(U): zhangsan

密码(P): ***

保存用户密码(S)

域(D):

启用高级认证(E)

MAC认证(M)

智能卡认证(K)

证书认证(C) 证书设置(S)...

<上一步(B) 下一步(N)> 完成(F) 取消

四、配置关键点

- 1、iMC和NAS设备路由可达；
- 2、iMC与NAS设备之间的UDP 1812,1813端口放行；
- 3、确保radius scheme test配置的共享密钥和iMC添加接入设备时配置的共享密钥一致。