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stan dard,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18 12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、a ccounting 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。

播IP地址从	1			至				
備名称				接入设备类型			•	重词 11
tia <b>2</b> 899 49	ix • Free	REMOND	4平台设备同步 <b>期</b>	Ħ.		3 <b>4</b> 4	AATXMR	S.ASITX
设备名称	设备IP地址	设备型号	下发配置类型	養注	下发结果	城口配置同步结果	irmag	1 操作
	10.153.42.82				未下发	元衛同步	II,	
	10.153.42.83				未下发	无需同步	illa,	
	彩展1-2.第1/	1 TT.					1 >	» 50 •
10日 > 接入策制 10日 > 接入策制 10日間	8管理 > 接入省	→→→	没备配置 > 增加接入设	ă			_	-
10日 - 1000000000000000000000000000000000	8管理 > 接入3 181	2 2	设新配置 > 增加接入设	Ť	计费调口。	1813		_
H中 2 投入領 用户 > 投入領 礼 正 祖 の方式	8管理 > 接入3 181 不細	2 2 四混合祖网	设备和图 > 增加200人设	Ξ.	计表演口 * 业务类型	1813 LAN境入业务		-
H市 2000家, 目 用户 > 接入領護 认证満日 * 祖网方式 接入设备典型	部管理 > 接入る 181 不用 130	2 2 2(General)	Q新配置 > 項加速入设 	9	计题词曰 * <u> </u>	1813 LAN接入业务 未分组		•
用户 > 接入領 規 入配置 认证調口 * 祖の方式 換入设备类型 共享定明 *	8管理 > 接入3 181 不能 H30 h3c	2 2 2周混合组网 C(General)	2番和型 > 現加線入设 	<u>8</u>	计整通口。 业务类型 业务外组	1813 LAN陳入业勞 未分语		•
用户 > 接入策額 入配置 认证第日 * 组网方式 接入设备供型 关系空衔 * 接入设备分组	諸管理 > 絶入道 181 不細 H30 h3c	各管理 > 接入的 2 2周混合组网 C(General)	Q用在田 > 和20余入Q ● ● ●	8	计意调口。 业务类型 业务分组	1813 LAN線入业务 未分组		•
用户 > 扱入領 用户 > 扱入領 入配置 以证通口 * 坦阿方式 使入设备供型 共享定明 * 接入设备分词 接入设备分词	<ul> <li>181</li> <li>181</li> <li>不量</li> <li>193</li> <li>193</li></ul>	留管理 > 接入に 2 明現会世界 (General)	Q # 4032 > %2039 \ 12 ▼ ▼	ž	计推测口。 业务类型 业务分组	1813 LAN除入业务 未分语		•

手工增加接入设备。	Google Chrome
10.153.42.56/	mc/acm/accessdevice/manualAddAccessDevice
手工增加接入设备	
起始IP地址 *	192.168.1.99
结束IP地址	
备注	
	确定取消

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。

1812		计费调口*	1813	
不启用混合组网	-	业务类型	LAN接入业务	
H3C(General)	-	业务分组	未分组	
h3c				
无	-			
23-00				
	1812 不应用意会组网 H3C(General) h3c 无	1812       不由用意会组网       H3C(General)       市3c       无	1812     計書第回・       不应用意点也问 ・     业労労型       H3C(General) ・     山労労道       h3c     ・       天     ・	1812     計画第二*     1813       不屈用意会组网     ・     北労典型     LAN接入业务       H3C(General)     ・     北労力组     赤分祖       元     ・     ・     ・

若是要修改,请在修改完成后点击手工生效按钮。

接入策略管理	~				
1 快速入门					
2 接入服务管理	- 1				
1 12 接入策略管理	>				
▶ 接入条件管理	- 1				
▶ 接入设备管理	- 1				
▶ LDAP业务管理	- 1				
▶ Portal服务管理	- 1				
▼ 业务参数配置	- 1				
😂 系统配置					
🔁 证书配置	- 1				
😂 客户端升级	- 1				
音 智能终端客户端升级	- 1				
📮 单点登录配置	- 1				
20 系统配置手 <u>工生</u> 效					
用户 > 按入策略管理 > 业务参数配置 > 系统配置手工	主效				
✓ 系統配置手工生	动成功,正在进行后	台处理,请勿再次	在由"系统配置手工生	效",否则系统将无	法正确明应该操作。

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 > 増加接入策略		
基本信息			
接入策略名*	1x		
业务分组。	*718		
描述			
接权信息			
接入时段	无 👻	分配P地址*	否 •
下行連率(Kbps)		上行速率(Kbps)	
优先级		应用RSA认证	
证书认证	●不启用 ◯ EAP证书认证 ◯ WAPI证书认证		

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。

[牛信息					
服务名"	service		服务后缀		
业劳分组 *	未分组	•	缺直接入策略。	lx	
快需安全策略"	不使用	•	缺窗内网外连策略*	不使用	
2首私有属住下发策略。	不使用	• 🕐	缺直移动力公策瞄*	不使用	-
+應領路 •	不计费	*			
Aga单帐号最大绑定终调数。	0		缺重单标号在远数量限制。	0	
<b>股劳描述</b>					
✔ 可申请⑦			Portal无感知认证 ⑦		

## 4). 开户: 创建帐号。

创建帐号时,首先增加用户姓名。例如"张三"。

€0 用户 > 増加用户				
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		1
电子邮件		⑦ 用户分组*	未分组	ůů,

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。

增加用户字成、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详细信息
继续增加用户	继续增加新的用户。

<del>夏</del> 入用户					
接入信息					
用户姓名	张三	选择 增加用户			
秋号名 *	khangsan				
预开户用户	□ 缺省BYOD用户	MAC地址认证用户	主机名用	ŧP (	快速认证用
127ZI +		密码机	BL ·		
TT by					
✓ 允许用户排放密码		启用用户密码控制策略		下次豐景质修改密研	
✓ 允许用户修改密码 生效时间		] 启用用户密码控制策略	1 <b>0</b>	下次登录须修改密码	m
<ul> <li>✓ 允许用户排放宽码</li> <li>生双时间</li> <li>最大闲置时长(分钟)</li> </ul>		] 自用用户密码控制策略	加	下次豐豪汤修改密研 1	<b>m</b>

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		
<b>选择认证协议</b> iNode智能客户端	为多种协议提供了统一的认证平台	*
<ul> <li>802.1X协议 802.1X是一种</li> <li>Portal协议 Portal是一种書</li> </ul>	(2) 网络访问控制协议。 (2) 责于门户的宽带认证上网方式。	
	                   	(取消)
建连接向导 选择连接类型		采
协议当前所支持由 ● <b>普通连接(C)</b>		
您将需要一个) ○快速认证连接 使用特定的用。	用尸名和密码来创建新的连接。 【 <b>①】</b> 户名和密码来创建新的连接。	
○ <b>域统一认证连</b> 在登录Window 成功,登录域)	接 (2) s城之前首先使用域登录口令进行身份认证,如果 后您就可以直接访问网络了。	眼域统一认证
		Tinak

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)。

: <b>户信息</b> 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( <u>c</u> ):	我的802.1X连接	
用户名( <u>U</u> ):	zhangsan	
密码(P):	***	
	✔ 保存用户密码(D)	
域( <u>D</u> ):		*
□ 启用高级认证	Ē(E)	
() MACILIE(	1)	
一智能卡认证	Æ(K)	
○证书认证(	D	证书设置(5)

- 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端口放通;
- 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。