802.1X 闫宁 2020-09-04 发表

组网及说明

1 配置需求或说明

1.1 适用产品系列

本案例适用于如SS5500-20TP-SI、S5500-52C-EI、S5500-52C-PWR-EI、S5500-34C-HI、S5800-32 C-EI、5800-32F、S5800-60C-PWR、S5830-106S等S5500、S5800、S5830系列的交换机。

1.2 配置需求及实现的效果

电脑通过交换机的2口连入网络,设备对该端口接入的用户进行802.1X认证以控制其访问Internet,RADIUS服务器与交换机相连,其地址是10.1.1.2/24,RADIUS服务器作为认证计费服务器。认证时首先进行RADIUS认证,如果RADIUS服务器没有响应则进行本地认证。

2 组网图



配置步骤 3 配置步骤

3.1 交换机VLAN及虚接口基本配置 #进入交换机系统视图 <H3C>system-view System View: return to User View with Ctrl+Z. #创建vlan 1-2 [H3C]vlan 1 to 2 #配置vlan 1, vlan 2虚接口IP地址 [H3C]interface Vlan-interface 1 [H3C-Vlan-interface1] ip address 192.168.1.1 255.255.255.0 [H3C-Vlan-interface1]quit [H3C]interface Vlan-interface 2 [H3C-Vlan-interface2] ip address 10.1.1.1 255.255.255.0 [H3C-Vlan-interface2]quit #将端口分别划分到所属vlan,端口2默认属于vlan 1,端口10属于vlan 2 [H3C] int Ethernet 1/0/10 [H3C-Ethernet1/0/10] port access vlan 2 [H3C-Ethernet1/0/10]quit #配置到服务器的缺省路由 [H3C] ip route-static 0.0.0.0 0 10.1.1.2 3.2 配置RADIUS方案 #配置radius认证,配置radius服务器的IP地址、秘钥 [H3C]radius scheme radius1 New Radius scheme #配置RADIUS方案的主认证和主计费服务器及其通信密钥。 [H3C-radius-radius1]primary authentication 10.1.1.2 1812 key simple key [H3C-radius-radius1]primary accounting 10.1.1.2 1813 key simple key #配置发送给RADIUS服务器的用户名不携带ISP域名 [H3C-radius-radius1]user-name-format without-domain [H3C-radius-radius1]qu 3.3 配置认证域 #创建名为a的ISP域并进入其视图 [H3C]domain a #为dot1x用户配置AAA认证方法为RADIUS并采用local作为备选方案 [H3C-isp-a]authentication lan-access radius-scheme radius1 local #为dot1x用户配置AAA授权方法为RADIUS并采用local作为备选方案

[H3C-isp-a]authorization lan-access radius-scheme radius1 local #为dot1x用户配置AAA计费方法为RADIUS并采用local作为备选方案 [H3C-isp-a] accounting lan-access radius-scheme radius1 local [H3C-isp-a]qu 3.4 配置802.1X认证 #全局开启802.1X认证 [H3C]dot1x 802.1X is already enabled globally. # Ethernet 1/0/2接口下开启802.1X认证 [H3C]int Ethernet 1/0/2 [H3C-Ethernet1/0/2]dot1x 802.1X is enabled on port Ethernet1/0/2 already. #在以太网端口Ethernet1/0/2上配置802.1X用户使用强制认证域a [H3C-Ethernet1/0/2]dot1x mandatory-domain a [H3C-Ethernet1/0/2]qu 3.5 配置本地账户和密码(服务器无响应可用本地用户认证) #创建本地用户h3c,密码为h3c,服务类型为lan-access [H3C]local-user h3c New local user added. [H3C-luser-dot1x]password simple h3c [H3C-luser-dot1x]service-type lan-access [H3C-luser-dot1x]qu #保存配置

[H3C]save force

3.6 Radius服务器设置

#下面以装有WinRadius软件的电脑(10.1.1.2/24)为例

1、设置-数据库-自动配置ODBC-重启软件

ODBC 设置	3			
请在 '控制面板/ ODBC' 中设置 RADIUS 数据库。 缺省数据库是 'WinRadius.mdb'。您也可以通过点 击下面按钮把该数据库添加到您的 ODBC 系统 中。				
自动配置 ODBC				
ODBC名: WinRadius				
注意:如果需要 username/password, 请输入 'YourOdbcName;Uid=yourUsername; Pwd=yourPassword''。				
用户账号表名: tbUsers				
计费记录表名: tbLogs				
VoIP记录表名: tbVoIP				
每隔 0 分钟刷新一次用户信息				
该数据库支持 <mark>dynaset ▼</mark>				
确定 取消				

2、设置-系统,配置NAS密钥和交换机RADIUS方案的密钥一致,重启软件

系统设置			X
	NAS 密钥:	key	
	认证端口:	1812	
	计费端口:	1813	
□ 在系:	统启动时自动	加载	
□ 启动	时最小化窗口		
(确定		取消

3、高级-创建RADIUS表,重启软件

4、操作-添加用户和账号

添加账号			X
	用户名:	ceshi	
	密码:	ceshi	
	组名:		
纠	驼龙地址:		
请填写MAC 白表示不绑	:地址或主[]定,O表示	叫号码来3 R绑定到首	实现用户绑定。空 款使用的地址。
预	问什金额:		0 分钱
	到期日:		
注意: ууу 次接入开始	//mm/dd 表 的有效天	示到期日 数; 空白:	,数字表示从第一 表示永不过期。
	其它:		
○ 预付	费用户	◉ 后付到	费用户
ੀ	费方法:	按时间;	+费 ▼
	确定		取消

备注:

可以利用软件Radius Test测试RADIUS服务器设置是否正确,在软件输入服务器地址,密钥,用户名和密码,点击发送,如下图所示提示用户 (ceshi) 认证通过。

Radius - 无标题		
日志 海泉 設置 査着 帮助		
2 2 × + - 9 1 8 1		
and ison		
2020年8月29日20时20日 LOAD D8: #20日期間第名称开目#180	御い変い程序	
2020年8月29日20时20分_ 清使用"设置/板据库_"为约约 RADIUS	Billing School .	
2020年8月29日20时20份 加数用户数据失效。		
2020年8月29日20时20分		
2020/08/01/29/02/09/20/9		
2020年8月29日20世33分用户(ceshi)以证書过		
	(The factor	
	(D) Radiustent	Charles and Charle
	Redius IP: 10.1.1.2 Redius	Port 1813
	AR. Santa	
	Millin (Access Request	key
	用户名: ceahi 密码:	orahi
		1
	東波 性紀所以	40
	Gred Access_Region1	
	交理 1 で没理範囲 1 堂村 From IP=10.1.1.2. Port=1013. Size=44.	
	Received 02 02 00 20 8b 6e c6 1a de b8 13 29 e0 1	fa 10 eT fa GI fa 84
	10 00 00 10 10 11 00 12 00 17 10 00 00 00	es po 18 po 22 81 00
	Send Access Faquest 任權1 个词或重要 5 使的	
	From IP=10.1.1.2, Fort=1813, Size=44.	6 B 4 6 6 6 6 M
	15 06 00 98 96 7f 50 12 44 17 Tc 50 bc	e4 95 1a 90 22 al d6
	49 10 07 db	
	C	

3.7 配置客户端

#在客户端电脑上配置有线网卡的IPV4地址192.168.1.2/24,网关为192.168.1.1,安全INODE客户端软件,定制802.1X连接,输入用户名和密码是ceshi/ceshi

₩ iNode智能客户端	En 📽 — 🗙
802.1X连接	
用户名 ceshi	
密码 •••••	
■ 保存用户名 ■ 保存密码	
	5 按 ▼
👪 L2TP IPsec VPN连接	× .
₽ Portal还接	1
SSL VPN连接	1
	·我的场景》
0	≣ %

3.8 实验结果验证

将装有INODE客户端软件的电脑接入交换机的Ethernet 1/0/2,选择802.1X连接,输入正确的用户名和 密码后点击连接,如下图802.1X认证通过



此时未进行802.1X认证的电脑可以ping通自己的网关

C:\Users\ASUS>ping 192.168.1.1



当交换机与服务器的接口断开连接,客户端向服务器认证无响应时可以用h3c/h3c的用户名和密码进行本地802.1X认证

Wode智能客户 端	En ¥ — 🗙
802.1X连接	
用户名 h3c	
密 码 •••	
🔲 保存用户名 📃 保存密码	
<u>نة</u>	换 ▼
L2TP IPsec VPN连接	
Portal连接	~
😭 SSL VPN连接	~
	我的场景 »
0	i≣ %