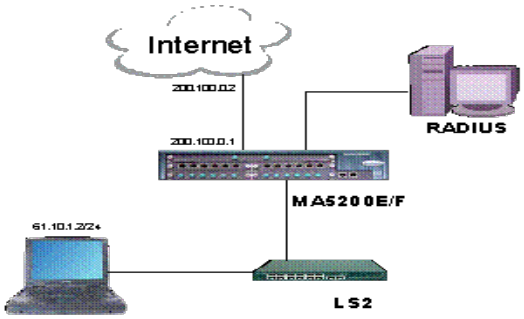
MA5200F实现vlan静态用户radius认证的案例

郭晓翔 2006-02-09 发表

在MA5200F上实现vlan静态用户radius认证

目前我们通过MA5200F与CAMS配合，在许多局点实现了用户集中认证，但是一部分绑定用户的认证用户希望也能够集中到CAMS上来认证，如果放到MA5200F本地当然也可以实现，但是对用户的技术水平要求要高很多，也不是特别方便。为使本例适用更多场合，本例中介绍vlan静态指定radius上认证，需要注意的是目前vlan静态用户在MA5200F上可以实现IP、MAC和用户帐号的捆绑，而且可以实现一个用户帐号绑定多个IP、MAC，而这一点在许多radius包括我们的CAMS暂时还无法实现，只能一个用户帐号绑定一个IP、MAC。整理一份实例实现供大家参考。

组网图



配置环境参数

计算机的IP地址：61.10.1.2

计算机的网关地址：61.10.1.1/24

MA5200F的上行口地址：200.100.0.1

MA5200F对端路由器地址：200.100.0.2

VLAN用户的接入流程

l 首先一个VLAN用户的报文在经过二层交换机的时候就带上了相应的VLAN ID；

l 用户的报文从5200的某一个端口进入的时候5200就会根据事先配置好的portvlan的数据来确定这样的一个用户是属于那个域的，以及采用什么样的接入方式（bind、web、pppoe）；

l 该用户在找到自己所属的域之后就会根据域下面配置的地址池分配一个ip地址，然后根据域下面设置好的认证和计费策略来进行认证和计费，认证通过之后该用户就能正常的上网了。

数据配置步骤

在了解了用户报文的基本接入流程之后我们就开始来配置数据，从上面的接入流程我们可以看出来，比较关键和重要的几个数据是：地址池、域、认证计费策略以及PORTVLAN的数据。

【配置地址池】

现在的版本对于静态用户也是需要配置地址池的，并且要将静态用户的地址包含进所配置的地址池中，同时还要执行禁用的命令，所以在做静态用户数据的第一步就是生成相应的地址池。

1. 创建一个名为huawei的地址池：

[MA5200F]ip pool huawei local

2. 配置地址池的网关以及掩码：

[MA5200F-ip-pool-huawei]gateway 61.10.1.1 255.255.255.0

3. 配置地址池的地址段：

[MA5200F-ip-pool-huawei]section 0 61.10.1.2 61.10.1.10

4. 在地址池里面将静态用户的地址去除：

MA5200F-ip-pool-huawei]excluded-ip-address 61.10.1.2

另外在实际开局中此处还要配置DNS服务器的IP，但由于是上机指导书，此处DNS的配置省略，具体配置可以参考开局指导书中的相关部分，下面的各配置中地址池的配置与此相同。

好了，现在我们已经给静态用户配置了一个地址池，接下来我们要为静态用户设置相应的认证和计费方案。

【配置认证方案】

这里我们配置一个采用radius认证的认证方案，在实际的应用当中认证方案可以是本地的也可以是radius的，如果是采用本地的认证方案，则需要在5200上面生成用户名和密码；如果是采用radius的认证方案，则需要在radius上面生成用户名和密码。

1. 进入AAA视图：
[MA5200F]aaa
2. 添加一个新的认证方案Auth1：
[MA5200F-aaa]authentication-scheme Auth1
这样接下来就进入了相应的认证方案视图。
3. 设置认证方案：
我们已经创建了一个新的认证方案Auth1，接下来我们将定义这个认证方案的具体内容。
[MA5200F-aaa-authen-auth1]authentication-mode radius
这里我们将Auth1这一个认证方案定义为了radius（远端）认证，也就是说采用这样的一个认证方案的用户的帐号是在远端的radius服务器上进行认证的。

【配置计费方案】
1. 进入AAA视图：
[MA5200F]aaa
2. 添加一个新的计费方案Acct1：
[MA5200F-aaa]accounting-scheme Acct1
3. 设置计费方案：
[MA5200F-aaa-accounting-acct1]accounting-mode radius
这里我们将Acct1这一个计费方案定义为了radius（远端）计费，也就是说采用这样的一个计费方案的用户是在远端计费服务器上进行计费的。

【配置radius服务器】
我们既然采用了radius的认证和计费方式，那么我们就需要在5200上面配置有关radius服务器的参数，这些参数包括了：服务器的地址、计费和认证端口、密钥等等。
1. 进入radius服务器配置视图：
[MA5200F]radius-server group radius1
其中的“radius1”是5200上面radius配置项的名字，长度不能超过32个字符。
2. 配置主备用radius服务地址和端口号：
配置主用radius服务器地址和端口号
[MA5200F-radius-radius1]radius-server authentication 202.10.1.2 1812
配置备用radius服务器地址和端口号（如果没有备用服务器这一步可以不配）
[MA5200F-radius-radius1]radius-server authentication 218.18.1.18 1812 secondary
3. 配置主备用计费服务地址和端口号：
配置主用计费服务器地址和端口号
[MA5200F-radius-radius1]radius-server accounting 202.10.1.2 1813
配置备用计费服务器地址和端口号（如果没有备用服务器这一步可以不配）
[MA5200F-radius-radius1]radius-server accounting 218.18.1.18 1813 secondary
4. 配置共享密钥：
共享密钥是5200和radius之间进行报文加密交互的重要参数，两端一定要设置的一致，因此在设置共享密钥之前需要和radius方面进行协商，这里我们假定共享密钥是huawei。
[MA5200F-radius-radius1]radius-server key Huawei

【配置域】
在5200上面每一个用户都是属于一个指定的（或者是默认的）域的，因此，在进行用户的配置之前我们首先要配置用户所属的域的一些参数。
1. 进入AAA视图：
[MA5200F]aaa
2. 新建一个名为isp的域：
[MA5200F-aaa]domain isp
接下来便进入了相应的域的配置视图。
3. 指定该域所使用的地址池：
[MA5200F-aaa-domain-isp]ip-pool first Huawei
4. 指定该域的认证方案和计费方案：
[MA5200F-aaa-domain-isp]authentication-scheme Auth1
[MA5200F-aaa-domain-isp]accounting-scheme Acct1
这里我们将该域的认证方案和计费方案设置为了先前定义好的两个方案Auth1和Acct1，分别是radius认证和radius计费。

【配置VLAN端口】
配置VLAN端口的目的是指定某个端口的某些指定的VLAN用户认证前后所使用的域，所采用的认证方法，以及静态用户的数据。
1. 进入端口VLAN的配置视图：
[MA5200F]portvlan ethernet 2 1 1
这里的含义是进入了2号以太网端口的从1开始总共1个VLAN ID的配置视图。

2. 设置该端口VLAN为二层普通用户接入类型：
[MA5200F-ethernet-2-vlan1-1]access-type layer2-subscriber
在access-type后面有多个选项，其中的layer-subscriber是指的普通的二层VLAN认证类型的端口，一般用于接入VLAN用户。
3. 配置用户所使用的域：
[MA5200F-ethernet-2-vlan1-1]default-domain authentication isp
4. 配置端口的认证方法：
[MA5200F-ethernet-2-vlan1-1]authentication-method bind
5. 添加静态用户：
[MA5200F-ethernet-2-vlan1-1]static-user 61.10.1.2 detect
这里的detect的含义是：静态用户不绑定MAC地址，设备主动探测。此应用主要是在静态用户是二层交换机等需管理设备。
此处配完后可以通过[MA5200F]display static-user

```
 Port-type  Port-ID  VLAN-ID   IP-address  Static-user-state
 ------------------------------------------------------------------
 Ethernet   1         1     61.10.1.2   Updated
 ------------------------------------------------------------------
 Total 4 item(s)
```

状态为UPDATED时表示这个静态用户目前处在预连结状态，如果为其它的状态的话请检查自己的数据配置情况。

【添加用户帐号】
1. 在以前vlan静态用户本地认证的配置中，在MA5200F上添加地地用户的过程如下面，现在我们想把它改成radius配置，实际上就是把类似于下面这个用户帐号添加到radius上面去。
2. 如在MA5200F上是这样来实现，进入本地认证管理配置视图：
[MA5200F]local-aaa-server
3. 在MA5200F本地会生成这样的用户帐号，本例中只是为了让大家知道radius帐号是什么样的，实际当中本地不需要再配置这个帐号：
[MA5200F-local-aaa-server]batch-user ethernet 2 1 1 domain isp
这之后便添加了一个用户名为：ma5200f-vlan-02-0001@isp的用户帐号。在这个帐号中用户名是关联上了sysname，所以请大家轻易不要改变sysname，否则会导致用户无法上网
4. 在radius上添加用户帐号
用户名：ma5200f-vlan-02-0001@isp
ma5200f-vlan-02*（这个数字代表端口）*-0001*（这个数字代表vlan ID）*@isp
密 码：vlan
所有的vlan用户静态帐号如果要在radius上配置密码都是vlan

【配置上行接口以及路由】
配置上行接口的目的是为了和上层的路由器或者交换机相连接，在配置上行接口的时候我们首先要将需要配置的接口指定为“非管理类型”。
1. 进入端口VLAN的配置视图：
[MA5200F]portvlan ethernet 24 0 1
2. 设置端口VLAN的接入类型为非管理类型：
[MA5200F-ethernet-24-vlan0-0]access-type interface
在access-type后面有多个选项，其中的interface是指的非管理类型的端口，用于连接上层交换机。
3. 创建VLAN子接口：
[MA5200F]interface Ethernet 24.0
这里需要说明一下，创建上行接口的步骤是先将一个端口上的某一个VLAN指定为“非管理类型”，然后再在这个端口上创建此VLAN的子接口。这里多了一个概念就是“VLAN子接口”。
这样，一个物理端口上就可以创建多个逻辑的VLAN子接口，每个子接口可以配置不同的ip地址。这样报文在上行的时候就可以根据需要走不同的ip上行，并且带上相应的VLAN ID，三层交换机（或者二层交换机）就可以根据这样的VLAN ID对用户的报文进行不同路径的转发了。增强了转发的灵活性。如果这里的VLAN子接口设置为0的话就是不带 VLAN ID上去。
4. 在 VLAN子接口下配置ip地址：
[MA5200F-Ethernet24.0]ip address 200.100.0.1 255.255.255.252
5. 配置默认路由：
对于一般条件的接入业务，5200上面只需要配置一条指向上行路由器端口的默认路由就可以了：
[MA5200F]ip route-static 0.0.0.0 0.0.0.0 200.100.0.2

测试验证
按照条件将计算机设置成相应的地址，此时应该可以ping通对端路由器的地址202.100.0.2（对端路由器需要做到MA5200F下面用户网段的回程路由）。
同时可用display access-user来查看用户是否上线。