先后在交换机上开启802.1X、MA5200F上开启三层WEB认证控制不同用户组接入的案例

郭晓翔 2006-03-08 发表

先后在交换机上开启802.1X、MA5200F上开启三层WEB认证控制不同用户组接入的案例

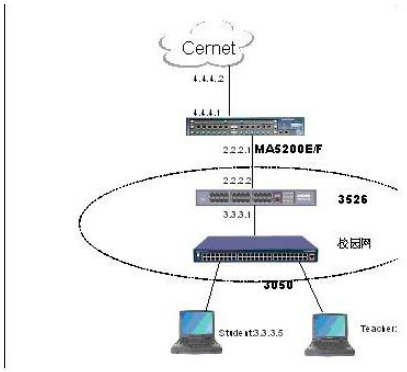
某校园网如下：MA5200F挂三层交换机或者路由器，进行三层WEB认证；三层设备下面接入二层交换机，让所有的用户在接入到三层设备之前进行802.1X认证。

实际需求：

教师登录局域网需要在3050上经过802.1X认证，登录Cernet不需要认证；

学生登录局域网需要在3050上经过802.1X认证，登录Cernet需要进行三层WEB认证。

组网图



配置环境参数

学生的计算机IP地址段为：3.3.3.2-3.3.3.10/8

教师的计算机IP地址段为：3.3.3.11-3.3.3.20/8

MA5200F的上行口地址：4.4.4.1/8

MA5200F对端路由器地址：4.4.4.2/8

MA5200F上接下端三层交换机的端口的地址为：2.2.2.1/8

MA5200F下连的三层交换机的三层接口地址为：2.2.2.2/8

三层交换机上的教师和学生网段的网关都为3.3.3.1/8

本例中PC地址采用静态IP地址，学生PC地址3.3.3.5/8，教师PC地址3.3.3.15/8

采用M5200F内置portal页面进行认证，请首先加载内置WEB页面，方法请参见《升级指导书》

数据配置步骤

【3050相关配置】

使用3050上的缺省域配置认证，计费等属性，下面提供本地认证用户的最简配置，如果需要进行radius认证计费需要配置相关参数，此处不再赘述；

系统视图下开启802.1X

```
[Quidway]dot1x
```

接入用户的端口开启802.1X

```
[Quidway]interface Ethernet 0/1
[Quidway-Ethernet0/1]dot1x
```

配置本地用户

```
[Quidway]local-user 1
[Quidway-luser-1]password simple 1
[Quidway-luser-1]service-type lan-access
```

【3526相关配置】

3526在这里只作三层路由转发，不作详细配置介绍，最简配置如下：

```
vlan 2
#
vlan 3
#
interface Vlan-interface2
 ip address 2.2.2.2 255.0.0.0
#
interface Vlan-interface3
 ip address 3.3.3.1 255.0.0.0
#
```

interface Ethernet0/1
 port access vlan 3
interface Ethernet0/2
 port access vlan 2
ip route-static 0.0.0.0 0.0.0.0 2.2.2.1

【5200F相关配置】
【配置认证方案】
由于在进行强制WEB认证的时候需要配置两个域，所以这里需要分别设置这两个域里面的认证和计费策略。但是由于第一个域仅仅是用来使用户能够获取IP地址，所以在这个域里面所指定的认证和计费方法可以尽量的简单，可以采用不认证不计费的方式，认证的时候用户将会属于另外一个域（通过用户名里面所带的域名或者5200上设置的默认域名来确定用户认证的时候属于哪个域），这样在第二个域里面可以采用合适的认证方法（本地或者radius）来对用户进行认证。
如果用户想用动态获取IP地址，请根据实际组网来进行具体配置，或者在下挂路由器、三层交换机（需要三层交换机支持该功能）开启dhcp-server功能，直接为用户分配IP地址；如果dhcp-server是放在5200F以上，需要在三层交换机上开启dhcp-relay功能。
进入AAA视图：
[MA5200F]aaa
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。
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 local

【配置计费方案】
进入AAA视图：
[MA5200F]aaa
添加一个新的计费方案Acct1：
[MA5200F-aaa]accounting-scheme Acct1
设置计费方案：
[MA5200F-aaa-accounting-acct1]accounting-mode local

【内置WEB服务器的配置】
在配置内置WEB服务器之前首先要加载内置WEB的页面文件，详细请参见《升级指导书》
进入WEB SEVER的配置视图
[MA5200F]web-server
指定WEB文件的路径
[MA5200F-web-server]directory flash:/webfile/eng
指定默认页面
[MA5200F-web-server]default-page /index.html

【配置认证前的域】
对于该域的认证和计费策略这里不用配置，采用默认的设置（不认证不计费）就可以了。
配置域下面用户所属的UCL组：
[MA5200F-aaa-domain-default0]ucl-group 1
配置强制WEB认证的WEB服务器地址：
[MA5200F-aaa-domain-default0]web-authentication-server 127.0.0.1

【配置认证时的域】
这里配置的是进行WEB认证的时候所使用的域，用户在接入的时候使用的是default0的默认域。
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。
进入AAA视图：
[MA5200F]aaa
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。
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LOCAL认证和LOCAL计费。

【添加本地用户帐号】
[MA5200F-local-aaa-server]user 1@isp password 1

【配置一个free域】
这里配置的是采用不认认证不计费的用户或者网段所使用的域，
进入AAA视图：
[MA5200F]aaa
新建一个名为isp的域：
[MA5200F-aaa]domain free
接下来便进入了相应的域的配置视图。
指定该域的认证方案和计费方案：
[MA5200F-aaa-domain-free]authentication-scheme default0
[MA5200F-aaa-domain-free]accounting-scheme default0
这里我们在该域直接引用系统缺省的认证方案default0和计费方案default0，分别是不认证和不计费。
这个域将在下面设置三层用户认证的网段时引用。

【配置系统的ACL策略】
这里所配置的ACL策略主要是针对认证前和认证后的用户来说的，上面我们以及在认证前和认证时的域里面指定了用户分别在认证前后属于不同的UCL组，现在我们就要针对这些不同的UCL组来进行ACL的控制，使得进行WEB认证前的用户不能访问其它资源，而WEB认证后的用户能够访问所有的资源。
进入增强型ACL配置视图，采用默认匹配模式：
[MA5200F]acl number 101 match-order auto
提示：
100到199是增强型ACL组，采用五元组进行控制。1到99是普通型的ACL组，采用三元组进行控制。
配置对于WEB认证前的用户只能访问WEB服务器和DNS服务器：
[MA5200F-acl-adv-101] rule user-net deny ip source 1 destination any bidirectional
最后面的参数表示双向，使用该参数就无需手动添加两条命令
以上的配置限制了UCL group 1的用户不能访问其它资源。
将101的ACL引用到全局：
[MA5200F]access-group 101

【配置与下挂路由器相连的接口地址】
[MA5200F]interface Ethernet 2.0
[MA5200F-Ethernet2.0]ip address 2.2.2.1 255.0.0.0
这里需要说明一下，如果MA5200F下挂的路由器或者交换机是带了vlan上来的话，那么这里就要配置相应的VLAN子接口，否则这里的子接口设置为0（也就是没有vlan）即可。

【配置到用户网段的路由】
三层认证由于是下挂的三层交换机，一次需要配置到用户网段的静态路由，下一跳是下挂路由器的接口地址。同时，通过配置到用户网段的静态路由来限制专线用户的接入网段。
[MA5200F]ip route-static 3.3.3.0 255.0.0.0 2.2.2.2

【配置三层认证用户所对应的网段和预连接的域】
[MA5200F]layer3-subscriber 3.3.3.2 3.3.3.10 domain-name default0

【配置不认证用户或者网段使用的域】
[MA5200F]layer3-subscriber 3.3.3.11 3.3.3.20 domain-name free
实际上在这个网段认证时，不存在认证前的概念，只有一个认证域，它的认证方式是不认证，计费方式为不计费。而且这个域没有受到ACL的控制。

【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。
进入端口VLAN的配置视图：
[MA5200F]portvlan ethernet 2 vlan 0 1
设置该端口VLAN为三层认证用户接入类型：
[MA5200F-ethernet-2-vlan0-1]access-type layer3-subscriber
[MA5200F-ethernet-2-vlan0-1]default-domain authentication isp

【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”。
进入端口VLAN的配置视图：

[MA5200F]portvlan ethernet 24 vlan 0 1
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。
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。
在 VLAN子接口下配置ip地址：
[MA5200F-Ethernet24.0]ip address 4.4.4.1 255.0.0.0
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 4.4.4.2

测试验证

PC地址是3.3.3.5，经过802.1X认证，再经过WEB认证之后可以ping通4.4.4.2
PC地址是3.3.3.15，经过802.1X认证之后就可以PING通4.4.4.2，因为在本例中802.1X认证和WEB认证都采取的是本地认证，如果使用CAMS认证的话，可以给一个用户申请两个服务，一个服务使用的dot1x的，另外一个使用portal的，这样可以划分出不同地址的访问时长，而且对于计费来说也比较清晰！
计算机3.3.3.0/8能够直接ping通对端路由器的地址4.4.4.2（对端路由器需要做到MA5200F下面用户网段的回程路由）。