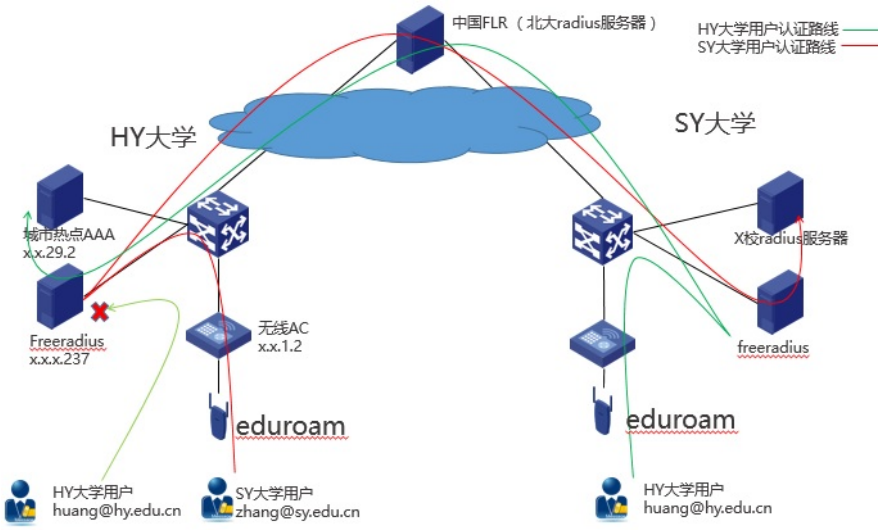
AC配合freeradius与第三方AAA实现eduroam功能的配置案例

AAA wlan接入 潘永鹏 2017-07-25 发表

部分高校及科研院所会加入无线全球漫游联盟eduroam，无线名称eduroam。成员单位需要提供eduroam的无线服务，成员单位的账号在其它成员单位也可以连接无线网络。本案例附加要求：本校账号不能在本校登录，本校的账号由城市热点提供，需要freeradius做本地账号的radius代理服务器，本案例描述AC配置，freeradius配置，城市热点配置由城市热点完成（将freeradius添加为radius client）。



AC+FITAP结构提供WPA2-企业的无线认证SSID：eduroam。无线AC做为NAS认证设备，AC上配置指定freeradius为radius服务器，freeradius做为radius代理将radius报文根据域名如果是hy.edu.cn将转发给本地城市热点做认证，如果是其它域名转发给北大radius代理服务器FLR进行转发到相应的代理服务器，最终到达用户母校的radius服务器做验证。

AC配置（本案例使用的无线AC为V5产品，V7产品请参考 V7配置手册）：

配置基本的WPA2-RSN的认证：

```
wlan service-template 7 crypto
 ssid eduroam
 bind WLAN-ESS 6
 cipher-suite tkip
 cipher-suite ccmp
 security-ie rsn
 security-ie wpa
 service-template enable

interface WLAN-ESS6
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2012 untagged
 port hybrid pvid vlan 2012
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type 11key
 undo dot1x handshake
 dot1x mandatory-domain freeradius
 undo dot1x multicast-trigger
#指定freeradius为radius服务器
radius scheme freeradius
 primary authentication x.x.x.237
 primary accounting x.x.x.237
 key authentication cipher $c$3$RoOhZruVGJkGl1jFMu6jTKYwV5
 key accounting cipher $c$3$W53uDOB2+YjLvZqE7vAweKwha
```

```
 user-name-format without-domain
 nas-ip x.x.x.2
#
domain freeradius
 authentication lan-access radius-scheme freeradius
 authorization lan-access radius-scheme freeradius
 accounting lan-access radius-scheme freeradius
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
```

freeradius配置（文件的相对路径为安装目录）：

修改client.conf文件:

配置AC为radius的client

```
client AC_6108_M1 {                //给AC起个名字
        ipaddr          = x.x.1.2      //AC的IP地址
        proto           = *
        secret          = h3c                   //radius对接密码与AC侧要一致
        shortname       = AC6108M1              //给这个AC起个别名，后面要用
        require_message_authenticator = no
}
client AC_6108_S1 {
        ipaddr          = x.x.2.2
        proto           = *
        secret          = h3c
        shortname       = AC6108S1
        require_message_authenticator = no
}
client AC_6108_M2 {
        ipaddr          = x.x.3.2
        proto           = *
        secret          = h3c
        shortname       = AC6108M2
        require_message_authenticator = no
}
client AC_6108_S2 {
        ipaddr          = x.x.4.2
        proto           = *
        secret          = h3c
        shortname       = AC6108S2
        require_message_authenticator = no
}
```

配置北大radius服务器FLR也做为client，本部分为固定配置由联盟管理员提供。

```
client flr.edu.cn {
        ipaddr          = xxx.xxx.129.2
        proto           = *
        secret          = xxxxxxxxxxxxx
        require_message_authenticator = no
}
client backup.flr.edu.cn {
        ipaddr          = xxx.xxx.129.5
        proto           = *
        secret          = xxxxxxxxxxx
        require_message_authenticator = no
}
```

修改proxy.conf文件:

配置北大radius服务器为freeradius的radius服务器， 这部分也由联盟管理员提供。

```
home_server flr.edu.cn {
        type = auth
        ipaddr = xxx.xxx.129.2
        port = 1812
        secret = xxxxxxxxxx
```

```
        response_window = 20
        zombie_period = 40
        status_check = status-server
        check_interval = 120
        num_answers_to_alive = 3
        max_outstanding = 65536
}

home_server backup.flr.edu.cn {                         //备机
        type = auth
        ipaddr = xxx.xxx.129.5
        port = 1812
        secret = xxxxxxxxxxxx
        response_window = 20
        zombie_period = 40
        status_check = status-server
        check_interval = 120
        num_answers_to_alive = 3
        max_outstanding = 65536
}
home_server_pool edu.cn-Failover {              //将主备要做个服务器池
        type = fail-over
        home_server = flr.edu.cn
        home_server = backup.flr.edu.cn
}
配置城市热点为本校的radius服务器用来最终验证账号
home_server dr.hy.edu.cn {                      //给服务器取个名字
        type = auth
        ipaddr = "x.x.29.2"                     //城市热点radius服务器
        port = 1812
        secret = xxxxxxxxx                      //对接密码
}

home_server_pool hy.edu.cn-Failover {       //做个服务器池，添加创建的服务器，这只有一台
        type = fail-over
        home_server = dr.hy.edu.cn
}
配置不同的域名转不同的服务器处理
realm hy.edu.cn {                   //配置域名调用的服务器池，必须与报给联盟的域名一致
        auth_pool = hy.edu.cn-Failover     //调用本地服务器池
                nostrip                     //转发radius报文里带域名
}

realm DEFAULT {                     //默认域名转发到FLR
        auth_pool = edu.cn-Failover
        nostrip
}

(可选)城市热点可能要求配置NAS-IP-ADDRESS字段为freeradius的IP
修改文件sites-available/default
pre-proxy {                         //修改代理服务器替换某些字段
        files                       //将files前的#去掉，在FILES中定义要替换的内容
#       attr_filter.pre-proxy
#       pre_proxy_log
}
修改文件preproxy_users
#DEFAULT Realm == "extisp"
#       NAS-IP-Address := 10.1.2.3
//增加两行配置针域名hy.edu.cn修改代理radius报文中的NASIP为本机IP
DEFAULT Realm == "hy.edu.cn"
        NAS-IP-Address := x.x.x.237

满足附加条件：本校账号不能访问本校的eduroam.
修改文件sites-available/default
```

在authorize中增加下面红色条件语句
authorize {

if(Realm == "NULL" || (Realm == "hy.edu.cn" && "%{clint:shortname}" == "AC6108M1") || (Real
m == "hy.edu.cn" && "%{client:shortname}" == "AC6108S1") || (Realm == "hy.edu.cn" && "%
{client:shortname}" == "AC6108M2") || (Realm == "hy.edu.cn" && "%{client:shortname}" == "AC6108
S2")) {
reject
}
}
//条件语句的意思解释为：如果满足if的条件拒绝登录，条件是域名为空,或者域名为hy.edu.cn时认证设备的别名为AC6108M1/ AC6108S1/ AC6108M2/ AC6108S2(即本校的AC)。

Freeradius的安装可以在线安装比较简单，这里不讲解。
启动freeradius: radiusd –X
如果忘记安装目录在启动时会提示
[root@localhost radius]# radiusd -X
radiusd: FreeRADIUS Version 2.2.6, for host x86_64-redhat-linux-gnu, built on Sep 22 2015 at 15:27:
25
Copyright (C) 1999-2013 The FreeRADIUS server project and contributors.
There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE.
You may redistribute copies of FreeRADIUS under the terms of the
GNU General Public License.
For more information about these matters, see the file named COPYRIGHT.
Starting - reading configuration files ...
including configuration file /etc/raddb/radiusd.conf //红色为安装目录
including configuration file /etc/raddb/proxy.conf
including configuration file /etc/raddb/clients.conf

城市热点AAA需要支持802.1X PEAP MS-CHAPv2的认证，部分版本不支持的话需要升级热点系统内核。