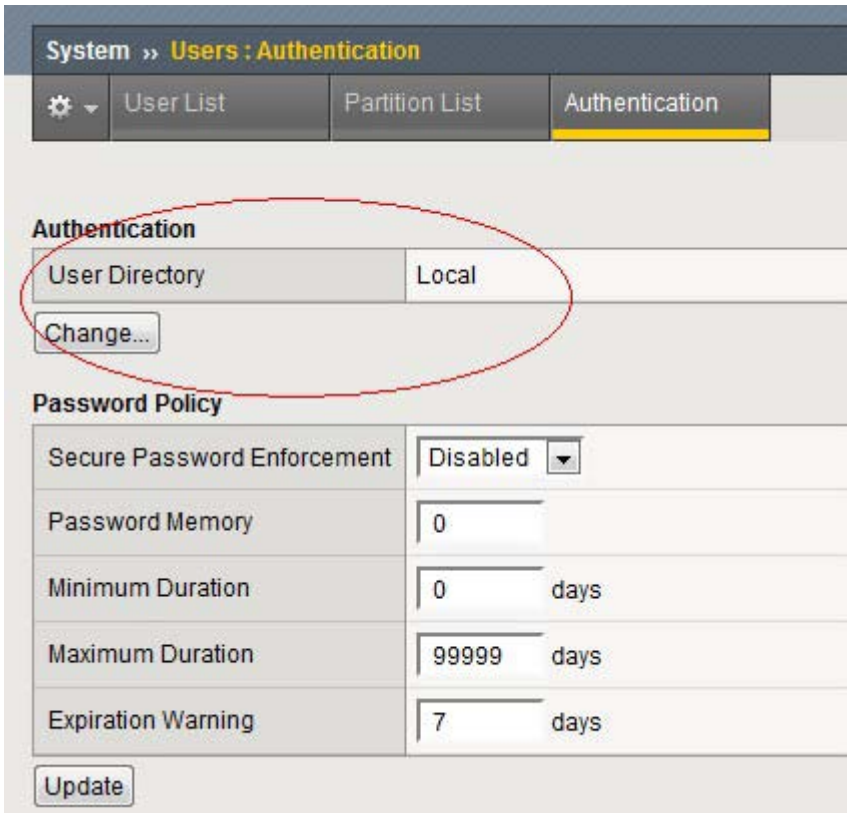
F5 设备管理帐号远程认证、授权之 TACAS+版

V10.1 在管理帐号的集中统一验证授权方面有了很大的提高，本文介绍如何实现基于 tacas+进行管理帐号认证及授权。

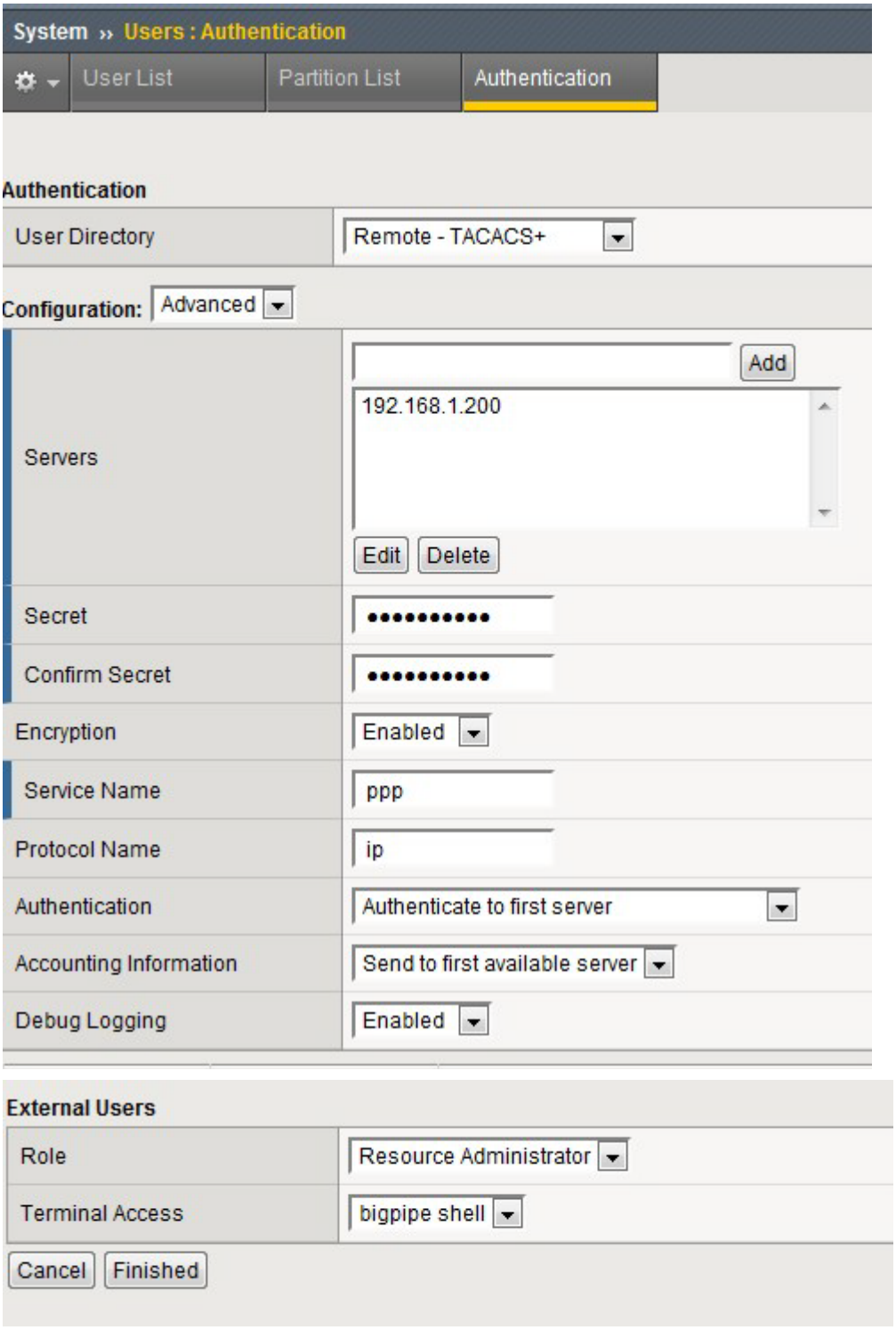
原理：
当用户登录时 F5 能够与 tacas+服务器进行通信，得到 tacas+对身份验证的结果（通过或不通过 失败等）。
如果身份验证失败，拒绝登陆，并在/var/log/secure,/var/log/aduit 日志文件中记录失败信息
如果身份验证通过，则利用 tacas+服务器返回的属性在本地查找对应匹配的 remoterole，根据 remoterole 中的定义赋予用户 console/user partition 以及对应的 role（即系统内置的 guest,operator,manager 等内置的 role 权限），同时记录相关日志
如果身份验证通过，但无法找到匹配的 remoterole，那么使用配置 tacas+时候所指定的“External Users”设置赋权---系统默认为 no access，即默认情况下即使验证通过也禁止访问。

设置方法：
一、F5 部分设置

1. 点击 system-users 菜单进入下图，并点击 change，将验证位置改为 remote-tacas+



2.随后将出现如下界面：



解释：

Server 处填写 tacacs+服务器服务 IP，如有多台则都填入，注意 F5 使用管理口 IP 与验证服务器通信

Secret 是通信加密 key，与 tacas+服务器端设置的 key 相同

Encryption 默认是启用的，如果选择禁用，那么上面的 key 则不起作用，需要注意这里设置要和服务器设置一致，即要么都加密要么都不加密。上截图显示启用，请注意下文为了观察 tacacs+的包，我其实关闭了加密功能。

Service name ，填写 TACAS+服务器端设置的服务名称，一般情况下都是默认的 ppp，因为

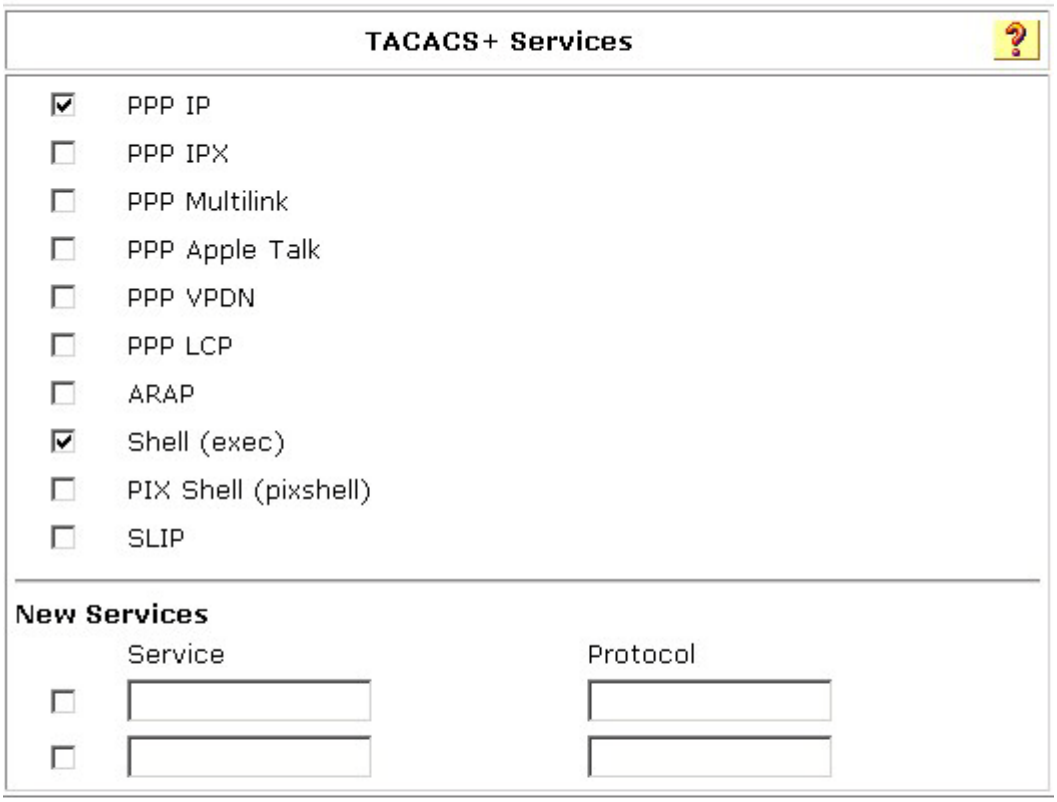
tacas 还可以为其他服务进行验证。对于 F5 这里填 ppp。
Protocol name ，填写对应上面服务所用的协议，大部分情况下是 ip，对于 F5 应该填 IP

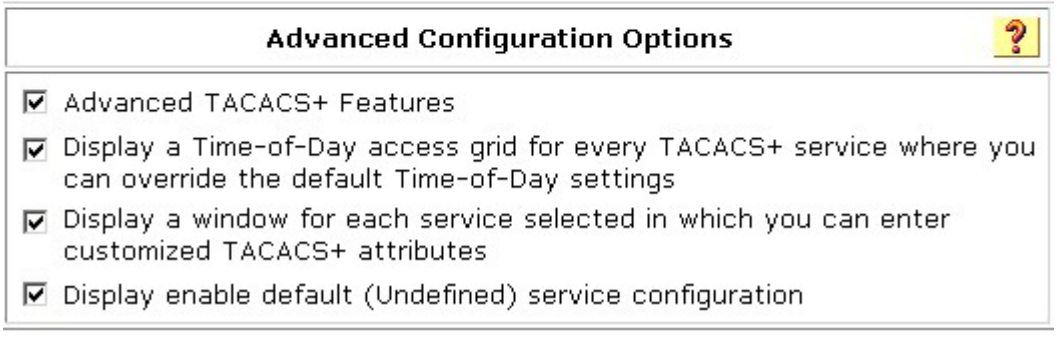
External users 部分配置缺省外部用户所用的 role 及 shell 的级别。注意不同版本的这部分关于 shell 的选项不同。10.0 的版本不支持配置 tmsh 在这里，10.1 即可。
3．至此，基本 F5 端配置完成，但是上述配置存在缺陷，即缺省所有外部用户都只能被赋予相同的 role，显然实际工作中肯定有很多不同 role 的用户，因此必须实现不同的用户或用户组能有不同的 role 权限，方法有两种：
A.在 F5 的 user 中添加所有外部用户的用户名，并逐一为其设置各自的 role。此方法的好处是 tacacs+服务器端不用考虑分组，tacas+服务器等于只负责验证，不负责授权，授权由本地来进行。
B.使用 b remoterole 命令在 F5 上配置不同的用户组管理不同的 role，F5 将在 tacas+服务器所返回的响应中查找是否存在匹配的 attribute，如果查到匹配则分配对应的 role

本文只讲述 B 方法。具体的 b remoterole 如何设置见下文。

二、TACAS+服务器设置
不同的软件设置方法不同，本文以 CISCO ACS 4.0 为例。
1. Cisco acs 安装方法略
2. 检查 service.msc 确保 tacas 服务已启动
3. 打开 acs 管理界面,点击左侧 interface configuration ，在出现的右侧界面点击 TACAS+(CISCO IOS)，勾选如下设置：

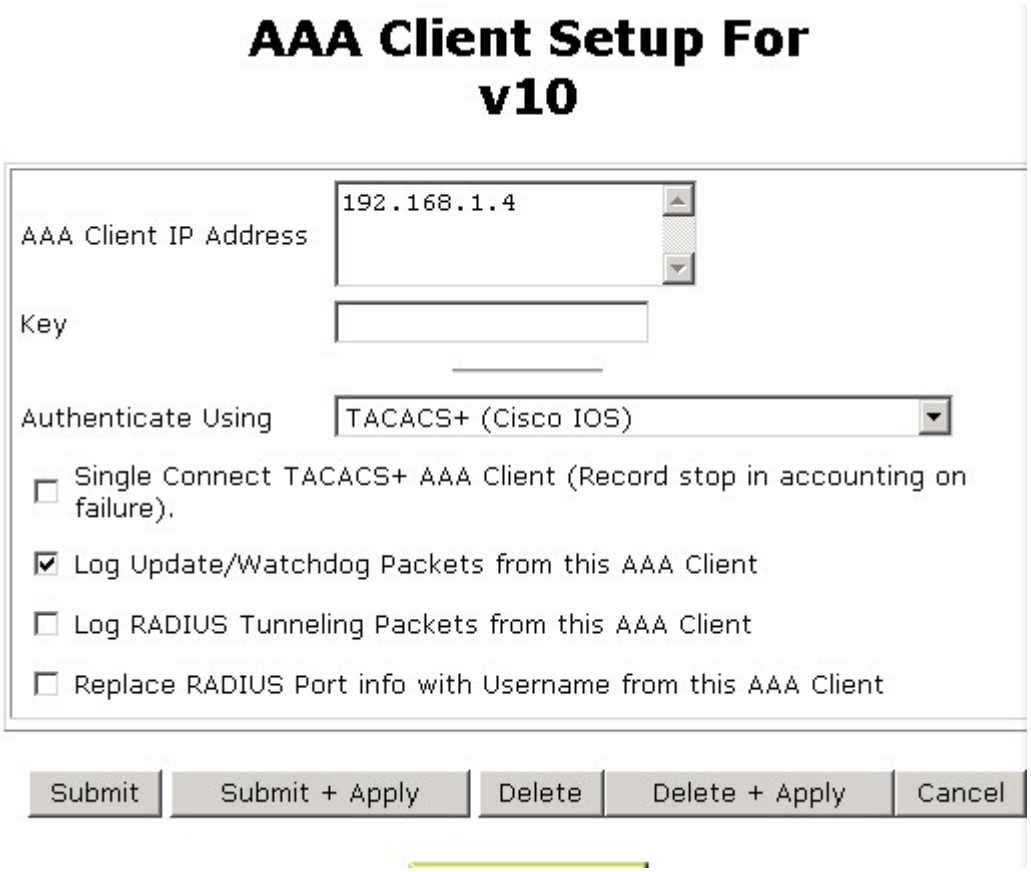
TACACS+ (Cisco)





4. 点击左侧 Network configuration

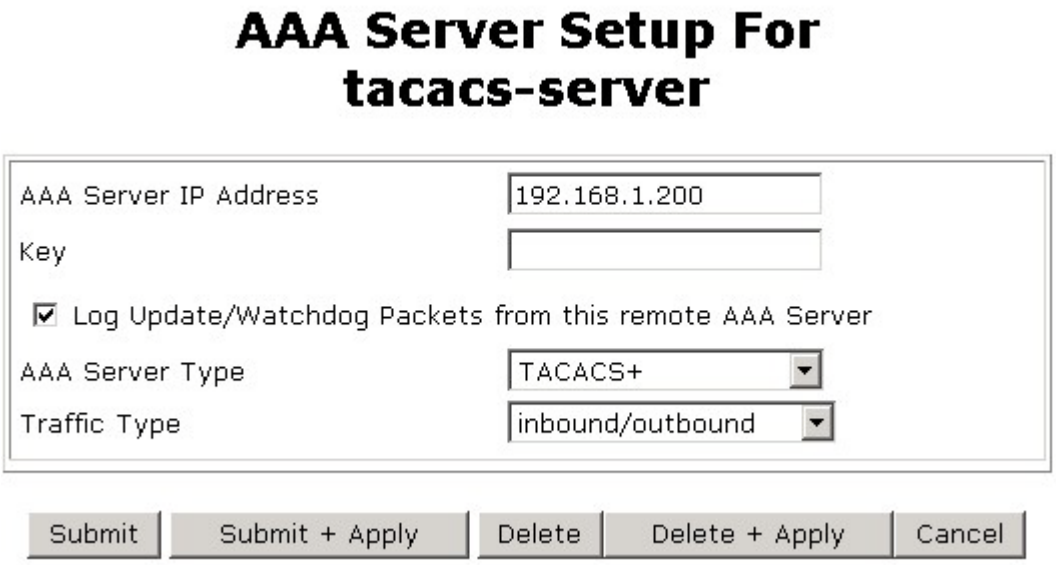
在 AAA clients 中添加 F5 ：



Client ip 填写 F5 管理口地址

请注意 key 部分，如果 F5 端是关闭加密的，则这里留空，否则填写与 F5 上一致的 key。

点击 submit+apply 提交后，会自动回到 network configuration 主界面，在 AAA servers 中添加一个 AAA server 定义:

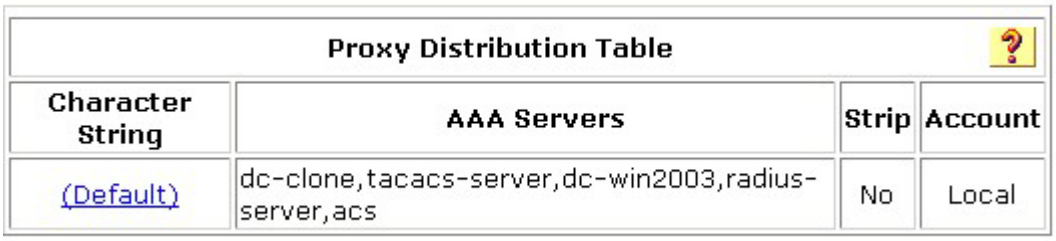


一样需要注意 KEY 部分，如不加密则留空，否则填写和 F5 端一致设置。

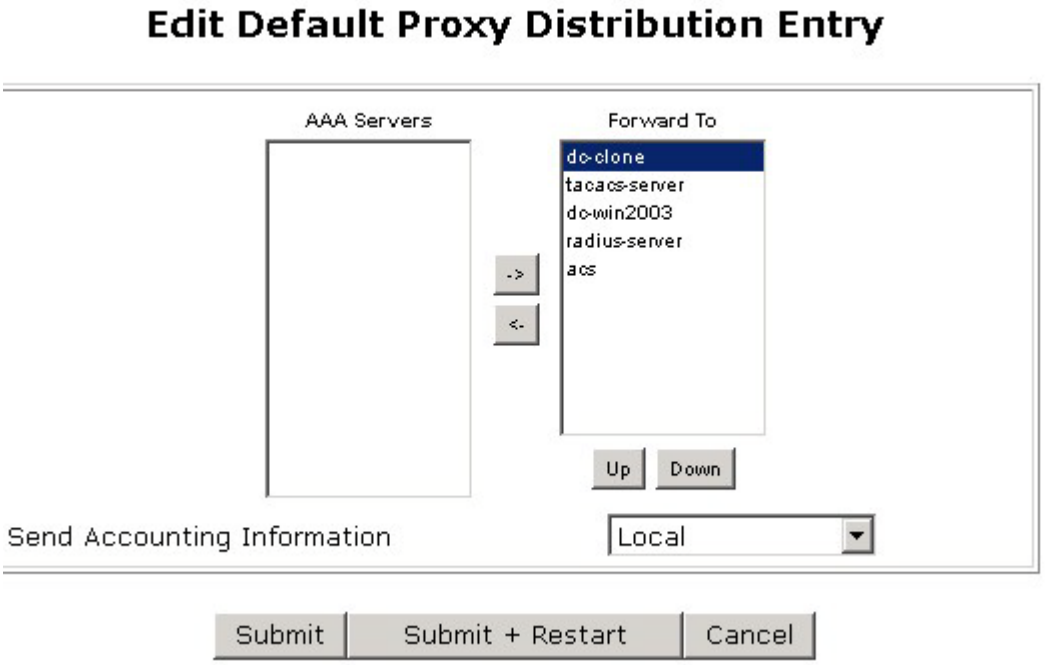
点击 submit+apply 提交。

另外，在 network configuration 中的 default proxy distribution tables 中，要把当前的所有 AAA

SERVER 都选择到 forwart to 一栏中

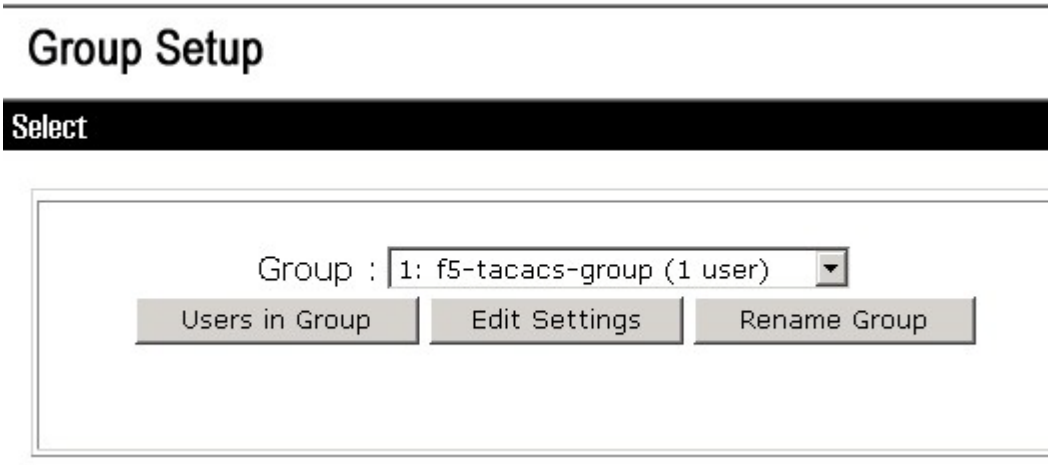


Proxy Distribution Table			
Character String	AAA Servers	Strip	Account
(Default)	dc-clone,tacacs-server,dc-win2003,radius-server,acs	No	Local



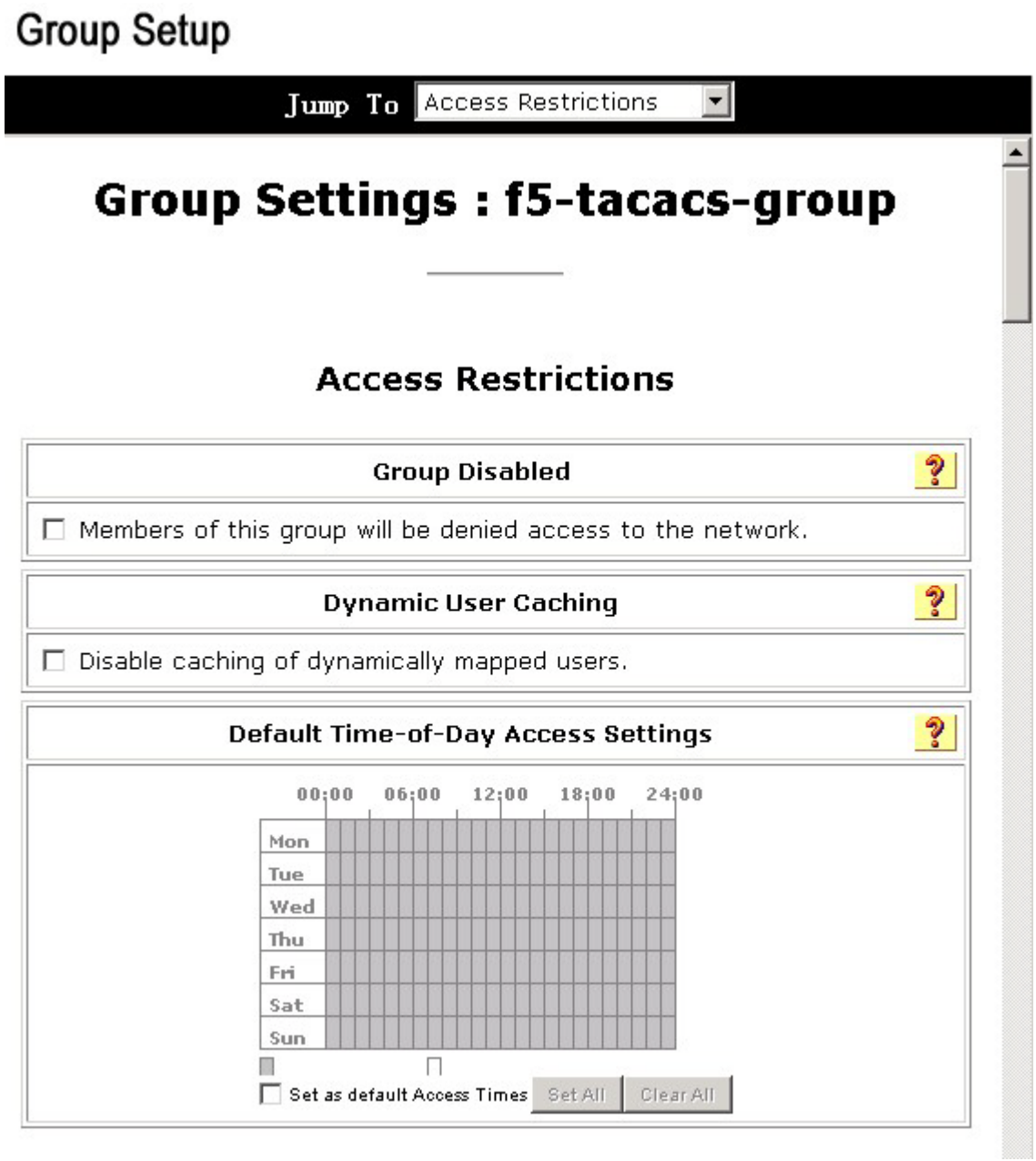
5. 设置用户组属性

点击左侧 Group setup，任意选择一个内置的组，

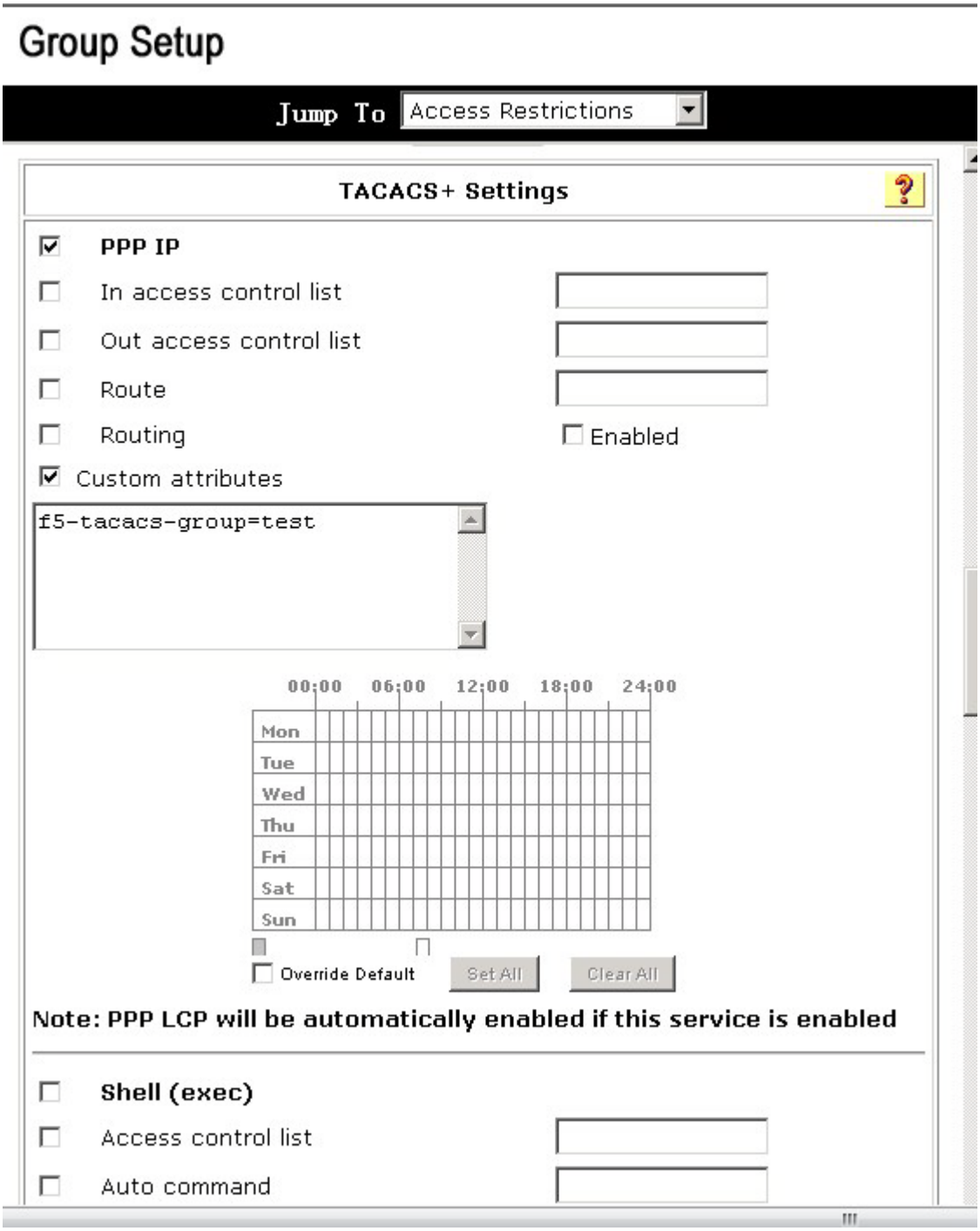


注意这里的组 1 的名字已被我自定义，你可以使用缺省名.选择一个组后点编辑设置，出现

下图：

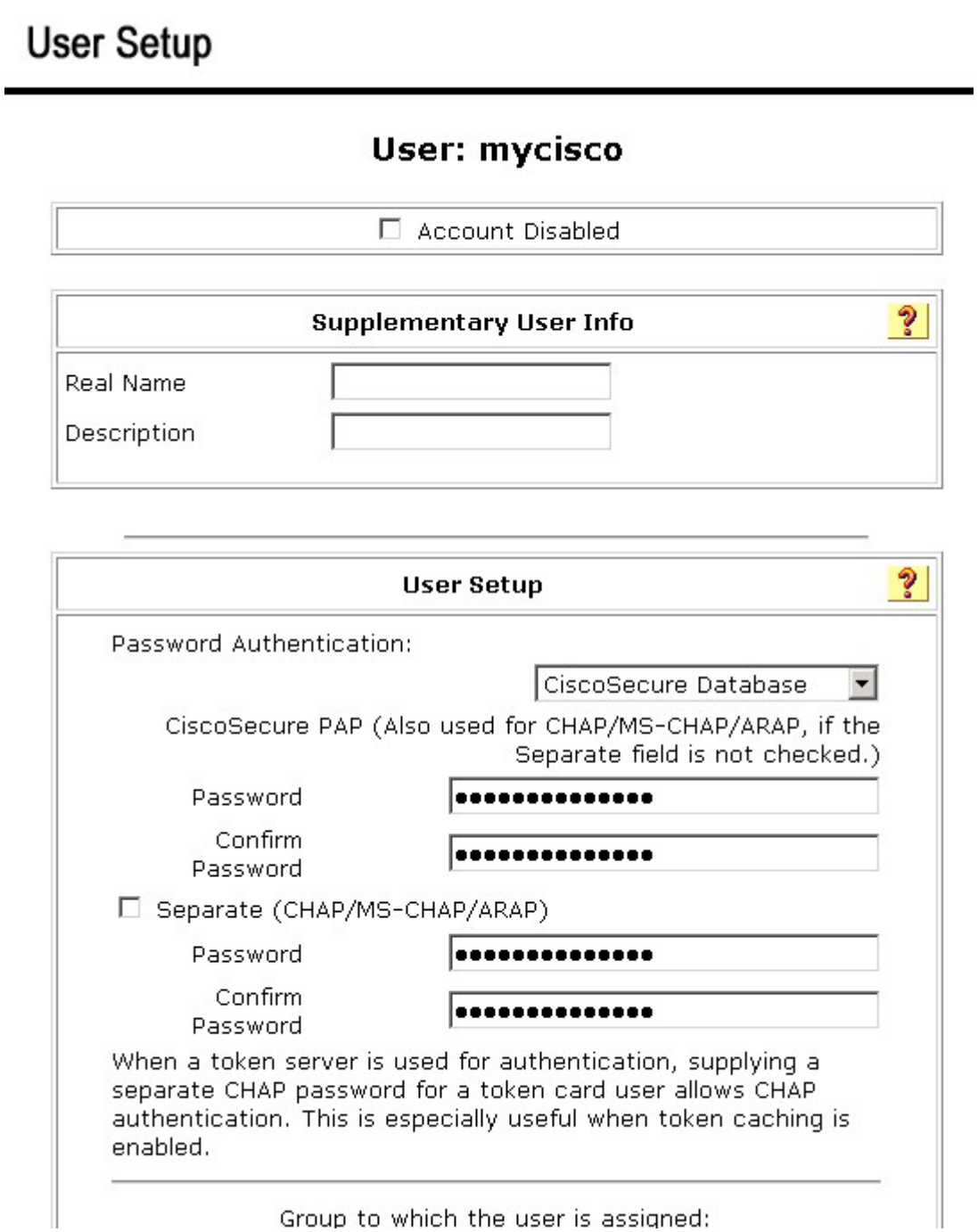


直接向下拉页面到 tacas setting 部分：



注意按上图设置，其中 custom attributes 部分按照类似格式任意定义，这里定义的就是为了让 F5 查找匹配一个 remoterole 的。
其他部分保持缺省，提交 group 设置。

6.添加用户
点击左侧 user setup ，输入一个用户名，点 add/edit:



注意不要勾选 account disabled，上图中所有密码处设置你要的密码，全部一样即可，剩余部分保持缺省，提交配置。

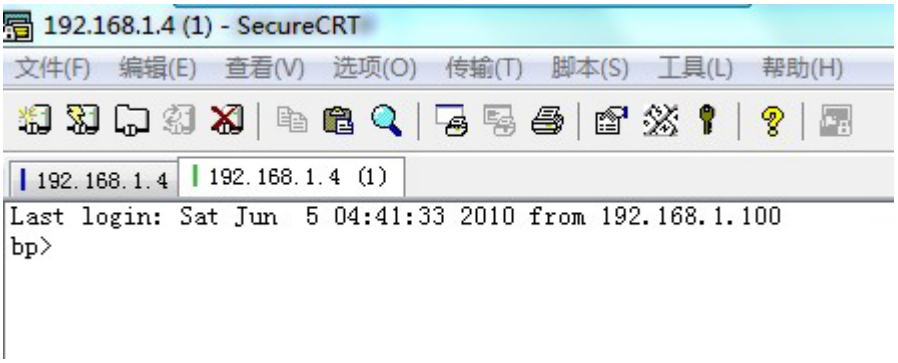
至此,ACS 部分配置完毕，开始调试。

小结：

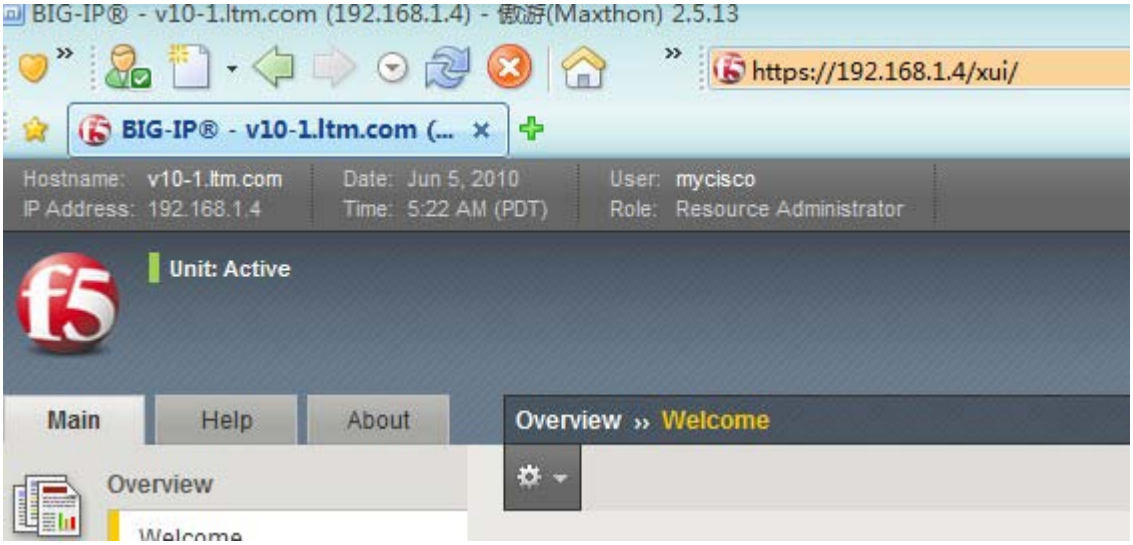
1. F5 启用了外部验证，不加密，设置了缺省的外部用户 role 及 sh 权限 （resource administrator/bigpiple shell），没有设置额外的 remoterole
2. ACS 设置不加密，配置了一个名为 mycisco 的用户，并设置了一个自定义属性

三、调试

1. 尝试使用 mycisco 帐号登录 ssh 和 web



Ssh 登录得到上述效果,符合要求，自动进入 b shell。



WEB 登录，显示 role 为 resource administrator ，符合要求。

两次登录的日志显示：

Jun 5 05:20:50 local/v10-1 warning sshd[10476]: _tac_crypt: using no TACACS+ encryption

Jun 5 05:20:51 local/v10-1 warning sshd[10476]: _tac_crypt: using no TACACS+ encryption

Jun 5 05:20:51 local/v10-1 warning sshd[10476]: _tac_crypt: using no TACACS+ encryption

Jun 5 05:20:51 local/v10-1 warning sshd[10476]: _tac_crypt: using no TACACS+ encryption

Jun 5 05:20:51 local/v10-1 info sshd(pam_audit)[10474]: user=mycisco(mycisco) partition=[All] level=Resource Administrator tty=ssh host=192.168.1.100 attempts=1 start="Sat Jun 5 05:20:51 2010".

Jun 5 05:20:51 local/v10-1 info sshd(pam_audit)[10474]: 01070417:6: AUDIT - user mycisco - RAW: sshd(pam_audit): user=mycisco(mycisco) partition=[All] level=Resource Administrator tty=ssh host=192.168.1.100 attempts=1 start="Sat Jun 5 05:20:51 2010".

Jun 5 05:22:41 local/v10-1 warning httpd[6205]: _tac_crypt: using no TACACS+ encryption

Jun 5 05:22:41 local/v10-1 warning httpd[6205]: _tac_crypt: using no TACACS+ encryption

Jun 5 05:22:41 local/v10-1 warning httpd[6205]: _tac_crypt: using no TACACS+ encryption

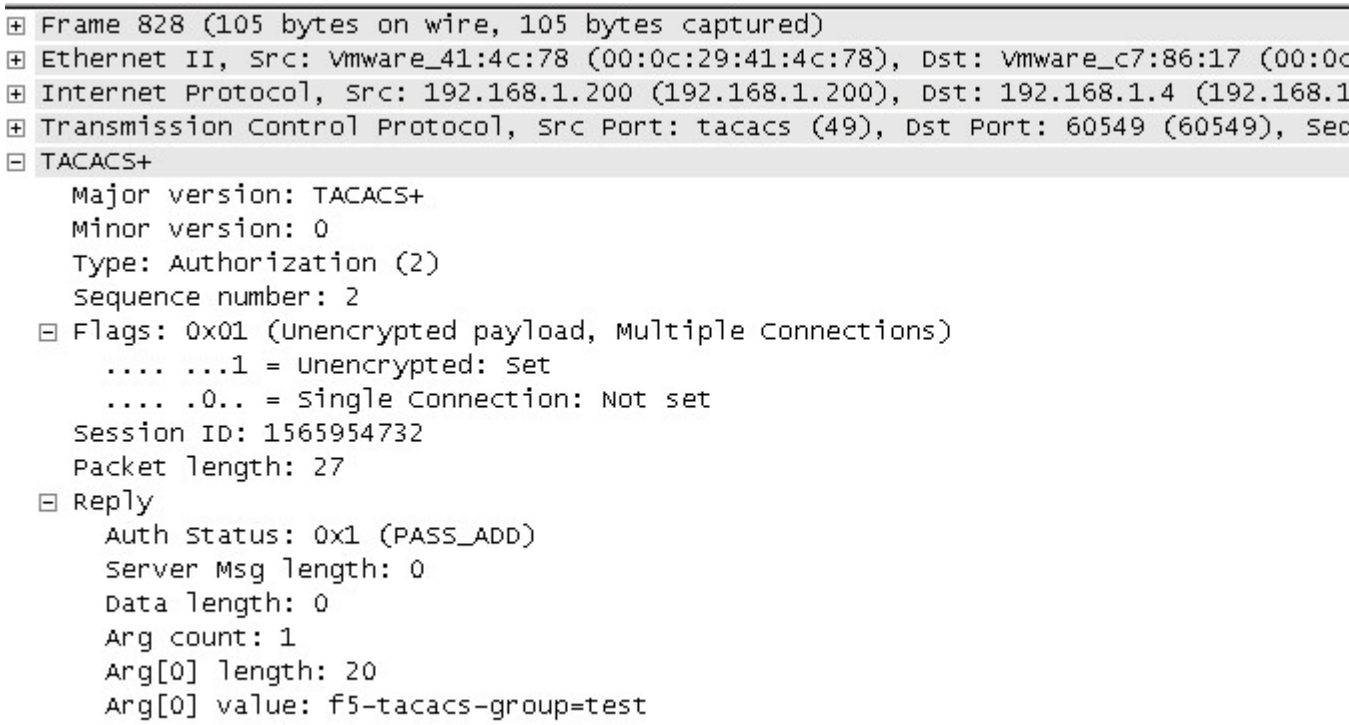
Jun 5 05:22:41 local/v10-1 warning httpd[6205]: _tac_crypt: using no TACACS+ encryption

Jun 5 05:22:41 local/v10-1 notice httpd[6205]: 01070417:0: AUDIT - user mycisco - RAW:

httpd(mod_auth_pam): user=mycisco(mycisco) partition=[All] level=Resource Administrator tty=/usr/bin/bpsh host=192.168.1.100 attempts=1 start="Sat Jun 5 05:22:41 2010".

抓包显示：

```
⊞ Transmission Control Protocol, Src Port: 60549 (60549), Dst Port: tacacs (49), Seq
⊞ [Reassembled TCP Segments (58 bytes): #825(12), #827(46)]
⊟ TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authorization (2)
    Sequence number: 1
  ⊟ Flags: 0x01 (Unencrypted payload, Multiple Connections)
      .... ...1 = Unencrypted: Set
      .... .0.. = Single Connection: Not set
    Session ID: 1565954732
    Packet length: 46
  ⊟ Request
      Auth Method: TACACSPLUS
      Privilege Level: 0
      Authentication type: PAP
      Service: PPP
      User len: 7
      User: mycisco
      Port len: 7
      Port: unknown
      Remaddr len: 0
      Arg count: 2
      Arg[0] length: 11
      Arg[0] value: service=ppp
      Arg[1] length: 11
      Arg[1] value: protocol=ip
```



2. 添加 remoterole 配置来 override 当前缺省的 role，在命令行中输入如下命令：

[root@v10-1:Active] log # b remoterole role info myrole {attribute "f5-tacacs-group=test" console "tmsh" line order 1 role administrator user partition all}

Myrole, 定义的 role 名字

F5-tacacs-group=test 这是在 TACACS 中设置的自定义 attribute

Console 部分指定 shell 级别 或禁用

Line order 用来排序配置在配置文件的顺序，F5 顺序检查，查到第一个匹配即认为成功

Uer partition 指定用户管理域

命令配置完毕后，可以用 b remoterole list 显示：

```
[root@v10-1:Active] log # b remoterole list
remoterole {
    role info myrole {
            attribute "f5-tacacs-group=test"
            console "tmsh"
            line order 1
            role "administrator"
            user partition "all"
        }
}
```

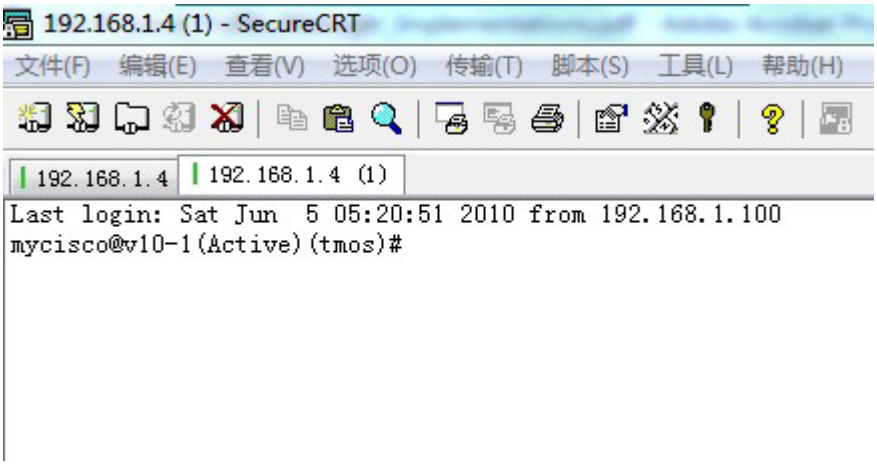
命令结构：

**bigpipe remoterole role info <user group> attribute (<string> | none) console **

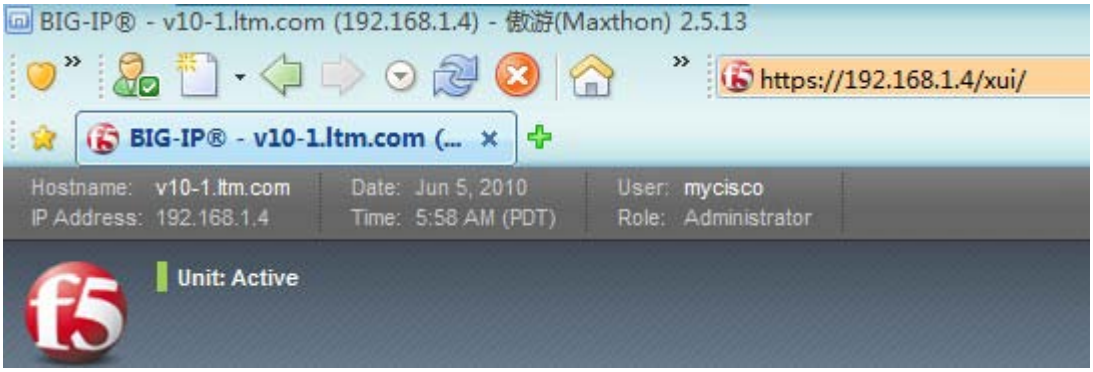
**(enable | disable) line order <number> role <user role> user partition **

(<string> | none)

3. 检查上述配置是否生效，仍然使用 mycisco 帐户登录，如果生效，此时应该拥有管理员权限及 tmsh 的权限



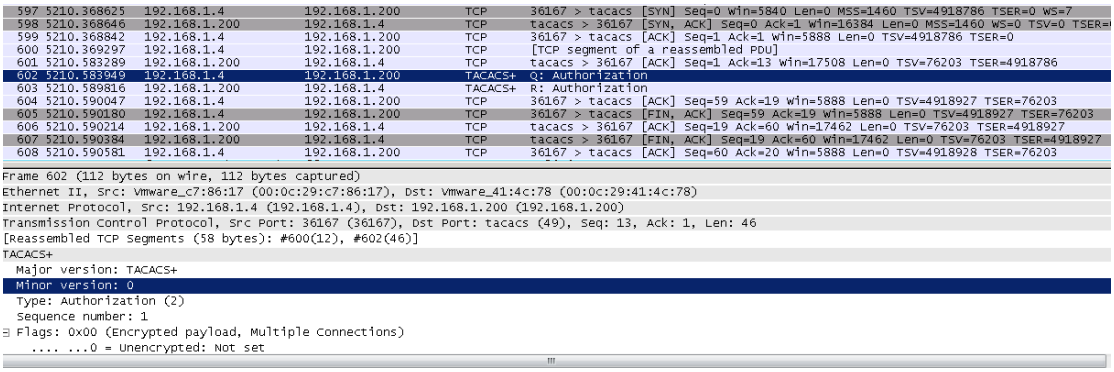
成功！



至此配置完成，测试成功。实际工作用应注意启用加密通讯，否则输入的密码都是明文传输。

附 1：

加密情形下的通讯抓包



附 2：

如果本地配置有一个相同用户名并指定一个 role 且该用户名又能命中 remoterole 的话，谁生效？

测试结果是本地指定的生效

附 3：

如果 TACACS+中的一个用户组配有多个自定义 attribute，而且这些 attribute 在 F5 里都有定义，那会如何匹配？
测试结果，ACS 只会发送第一行的自定义属性，其他定义的无效。