H3C S9500交换机TACACS功能的配置

楼依帆 2006-09-10 发表

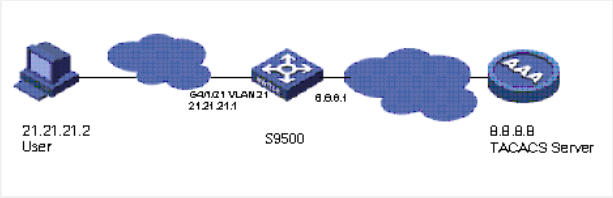
H3C S9500交换机TACACS功能的配置

一、组网需求:

如下组网所示，需要通过对交换机的配置实现TACACS服务器对登录交换机的Telnet用户的远端认证。

一台TACACS服务器（其担当认证、授权、计费服务器的职责）与交换机相连，服务器IP地址为8.8.8.8，设置交换机与认证、授权、计费TACACS服务器交互报文时的共享密钥均为“expert”，设置交换机除去用户名中的域名后再将之传给TACACS服务器；在TACACS服务器上设置与交换机交互报文时的共享密钥为“expert”。

二、组网图



三、配置步骤:

软件版本：S9500交换机全系列软件版本

硬件版本：S9500交换机全系列硬件版本

1）配置Telnet用户采用远端认证方式，即Scheme方式

[S9500]user-interface vty 0 4

[S9500-ui-vty0-4]authentication-mode scheme

2）配置Domain

[S9500] domain hwtacacs

3）配置HWTACACS认证、授权、计费服务器IP地址

[S9500] hwtacacs scheme tacacs

[S9500-hwtacacs-tacacs] primary authentication 8.8.8.8

[S9500-hwtacacs-tacacs] primary authorization 8.8.8.8

[S9500-hwtacacs-tacacs] primary accounting 8.8.8.8

4）配置认证、授权、计费的加密key

[S9500-hwtacacs-tacacs] key authentication expert

[S9500-hwtacacs-tacacs] key authorization expert

[S9500-hwtacacs-tacacs] key accounting expert

5）指示系统从用户名中去除用户域名后再将之传给TACACS服务器

[S9500-hwtacacs-tacacs] user-name-format without-domain

6）配置Domain和HWTACACS的关联

[S9500] domain hwtacacs

[S9500-isp-hwtacacs] scheme hwtacacs-scheme tacacs

四、配置关键点:

1）设置本地Radius时需要指定认证和计费端口1645、1646，不能默认；

2）本地的认证和计费密钥必须和远程服务器上的配置一致；

3）只有在远程Radius无响应时才会转到本地认证。