**AAA是一种后台服务，是一种对网络用户进行控制的安全措施。**

**Authentication 认证 (你是谁)**

**认证强度跟元素有关,用于认证的元素越多越安全，元素包括密码，指纹，证书，视网膜等等**

**Authorization 授权（确定你能做什么）**

**授权用户能够使用的命令**

**授权用户能够访问的资源**

**授权用户能够获得的信息**

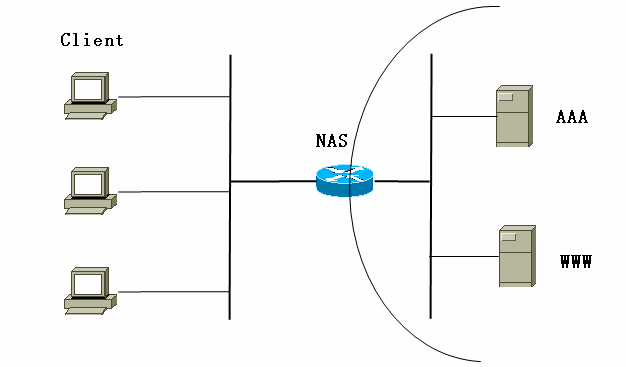
**Accounting 审计(确定你做了什么)**

**两类审计：**

**1、时间审计**

**2、命令审计**

**AAA的基本拓扑：**

****

**NAS--网络访问服务器，或者叫网络接入服务器。其实就是你网络的边缘网关，外部节点需要通过这台路由器来访问你的网络。需要在这台路由器上对接入的用户进行控制。**

**AAA--通过在服务器上装上CISCO的ACS软件，就能构建出一台AAA服务器。**

**NAS是AAA服务器的client端**

**为什么要用AAA：**

**通过AAA技术，我们能对接入网络的用户进行控制，可以控制哪些用户能接入网络，能得到什么样的权限，还能记录用户上来之后做了啥事。**

**1、跟网络设备数量有关，也就是跟NAS的数量有关**

**2、跟用户数量有关**

**3、由于用户的频繁变动**

**三大类的需要认证的流量类型client-----NAS(网络访问服务器)**

**也就是三种到达NAS的流量**

**1、登入nas telnet/ssh/http/https(也叫网管流量)**

**2、拔入nas pptp/l2tp/pppoe/ipsec vpn.....**

**3、穿越nas auth-proxy(ios)认证代理/cut-through(pix)**

**AAA安全服务器的选择：**

**1、本地安全数据库**

**2、远程安全服务器，也就是AAA服务器**

**本地安全数据库：**

**本地安全数据库运行在NAS上为一小部分用户提供服务，实现起来容易，但是功能不够强大。**

**特点：**

**1、在小型网络中使用**

**2、在CISCO的路由器上存储用户名和密码**

**3、通过CISCO路由器上的本地安全数据库进行用户验证**

**4、不需要外部的数据库服务器**

**AAAprotocols:RADIUS和TACACS+**

**通常在网络中实现AAA，都是通过部署一台单独的AAA服务器来实现，而AAA服务器是需要跟NAS通信的，它们之间通信的协议有两种：RADIUS和TACACS+**

**TACACS+ 基于TCP cisco标准 端口号49 信息是加密后传送的**

**RADIUS 基于UDP 国际标准 新端口号1812(authen/author) 1813(account)**

**旧端口号1645(authen/author) 1646(account)**

**RADIUS的信息是明文传送的，只有密码是加密传送的。**

**注意：RADIUS各厂家是不一样的，有不同的av pair**

**RADIUS:**

**有四种消息类型：**

**access-request 访问请求，客户发给server**

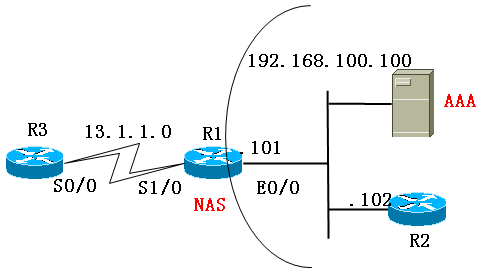
**access-challenge 挑战信息，查询AAA服务器上的配置**

**access-accept　　允许访问，查到有这个配置才会允许**

**access-reject　　拒绝访问**

**ACS---CISCO的访问控制服务器，也就是AAA服务器。只需要在一台服务器上装上CISCO的ACS软件，就得到了一台AAA服务器。这台服务器可以配置为使用tacacs+和NAS通信，也可以配置为使用radius协议与NAS通信。**

**以下是在路由器上配置AAA的步骤：**

****

**先做准备工作：**

**1、启用AAA**

**aaa new-model 注意：启用AAA后，路由器上不符合AAA的命令会被去掉**

**2、client指server的地址**

**NAS（config）#tacacs-server host 150.100.1.100 key cisco 密码后面千万不要打上空格,敏感的**

**还要在AAA服务器上增加一个client，并指明client的地址,最好起个环回口让服务器指，在服务器的CMD下加一个路由指向这个环回口。如果server指的是环回口，在client上还要指定一下更新源。**

**ip tacacs source-interface lo0**

**3、测试**

**test aaa group tacacs+ testR5(用户名) cisco（口令） new-code 本命令纯属测试，没别的作用，只是看AAA服务器起没起作用,new-code是在新的IOS中才要用到的。**

**如果出现user successfully authenticated表示没问题**

**4、做保护**

**为了防止启用AAA后，导致自已进不了路由器，建议在console接口下做个保护设置，让console口即使不用密码也能登录。**

**aaa authentication login NOACS none 保护-不认证**

**aaa authorization exec NOACS none 保护-不授权**

**line console 0 本地线路的保护**

**login authentication NOACS 设定对CON口不进行认证，保留最后一个进入的方法,以防万一**

**authorization exec NOACS 建议配置，但最好配置上**

**line aux 0 AUX的保护**

**login authentication NOACS**

**authorization exec NOACS**

**一、认证：**

**1、开启对login的认证**

**aaa authentication login FOR\_VTY none 不进行认证直接进入**

**aaa authentication login FOR\_VTY line 注意line意思是用line下的密码进行认证**

**aaa authentication login FOR\_VTY local 启用本地数据库,要自定义username和password**

**aaa authentication login FOR\_VTY local-case 用户名大小写敏感**

**aaa authentication login FOR\_VTY enable 使用enable密码进行验证**

**aaa authentication login FOR\_VTY group tacacs+ 使用AAA服务器进行验证**

**aaa authentication login FOR\_VTY local line none 如果第一种方法没有的话，就用第二种进行认证，如果第二种也没有，就不进行认证直接进入了,因为设了none**

**需要在线程下调用：**

**line vty 0 4**

**login authenticate FOR\_VTY**

**login authenticate default**

**2、开启对enable的认证**

**aaa authentication enable default group tacacs+ 在用户进入enable模式的时候进行认证，本命令不需要再单独调用，默认就启用了。**

**二、授权：**

**基本知识：**

**在IOS中，对用户分为16个级别，0-15，默认用户登录时级别为1**

**在IOS中，对于命令也为分16个级别库，分别对应于16个用户级别。高级别的用户可以使用低级别的命令。默认情况下，只有0级、1级、15级这三个级别库中有命令。**

**分为本地命令授权和AAA服务器授权**

**1、本地授权**

**NAS(config)#username ccnp privilege 15 password cisco**

**NAS(config)#aaa authorization exec VTY group local(name)**

**line vty 0 4**

**authorization exec VTY**

**2、AAA授权**

**注意：在AAA服务器上的授权分为用户级别的授权和命令的授权**

**用户级别的授权：确定你是几级的用户**

**NAS(config)#aaa authorization exec VTY group tacacs+**

**line vty 0 4**

**authorization exec VTY**

**命令的授权：**

**NAS(config)#aaa authorization commands 0 FOR\_VTY group tacacs+**

**NAS(config)#aaa authorization commands 1 FOR\_VTY group tacacs+**

**NAS(config)#aaa authorization commands 15 FOR\_VTY group tacacs+ 对15级的命令进行授权，在你使用15级的命令时，会先去查询否已有授权，然后才能使用。注意，最好从高级别的向低级别的授权**

**调用：**

**line vty 0 4**

**authorization commands 0 FOR\_VTY**

**authorization commands 1 FOR\_VTY**

**authorization commands 15 FOR\_VTY**

**这样，你所输入的各种命令都会发向AAA服务器去检查是否得到授权，得到授权的才能使用。**

**注意：在cisco的路由器上有16个用户级别（0-15），其中0、1、15级是有命令的，其他的级别默认没有定义任何命令，高级别的用户可以使用低级别的命令。**

**在本地路由器上改动命令的级别：**

**R1(config)#privilege exec level 0 conf terminal 将一条15级命令放入0级(特指在特权模式下的命令)**

**R1(config)#privilege configure level 0 interface 将一条全局命令放入0级**

**R1(config)#privilege configure all level 0 router 将router命令及其下的所有命令放入0级**

**当一条命令被放入0级后，它就不属于原来的级别了，因为被剪切过去了。但是因为高级别的授权能使用低级别的命令。所以在高级别用户还是可用的。**

**show privilege 查看用户级别**

**aaa authorization config-commands 开启对全局命令的授权，如果不打上这条命令，在AAA服务器上对conf terminal 命令做了授权后，所有的全局命令都可以使用了。打上后，就仅仅只能使用授权的命令。**

**aaa authorization console 新的IOS中AAA默认不影响console口的授权，需要打上这条命令才能影响。**

**三、审计：**

**分为命令审计和时间审计**

**aaa accounting commands 0 VTY start-stop group tacacs+ 基于命令的审计，会记录所有0级命令的操作**

**aaa accounting commands 1 VTY start-stop group tacacs+**

**aaa accounting commands 15 VTY start-stop group tacacs+**

**aaa accounting exec VTY start-group group tacacs+ 基于时间的审计，会记录所有登录用户的进出时间**

**line vty 0 4**

**accounting commands 0 vty**

**accounting commands 1 vty**

**accounting commands 15 vty**

**accounting exec vty**

**----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------**

**举例：**

**aaa authentication login VTY group tacacs+**

**line vty 0 4**

**login auth VTY**

**aaa authentication login VTY group tacacs+ local 服务器down后转到本地认证**

**aaa auth exec VTY group tacacs+**

**line vty 0 4**

**login auth exec VTY**

**aaa accounting login VTY start-stop group tacacs+ 审计**

**aaa accounting commands 0 VTY start-stop group tacacs+**

**注意，路由器的0-15级中，只有0、1、15级是有命令的，2-14级没有命令**

**NAR网络访问限制：**

**在AAA上配置，可以用来限制只有哪些IP地址能够来访问网络，还可以限制端口号。**

**AUX ,VTY 口 默认是Login ，Console 口 默认是没有Login**

**1，不存盘**

**2，远距离，用一个telnet session 在里边耗着，一个退出去，看看没问题，里边的Session 去存盘**

**在NAS Client上 测试：**

**server#test aaa group tacacs+ cisco cisco new-code**

**Trying to authenticate with Servergroup tacacs+**

**Sending password**

**User successfully authenticated 如果认证失败，一般是由于ACS 的网卡的IP 地址 经常变。**

**========================================================================================================================**

**2010.3.26 晚**

**Show Privilege**

**0 -----> exit;**

**1-------->show version;**

**15---------> show run ;**

**2 - 14 级留给用户自定义。将某条命令放到哪个级别。**

**1，配置 认证LIST + 策略；**

**称为LIST 因为 可以有多个认证策略，一个策略出现问题,方法失败，不是认证失败，则可以跳到下个认证方式。**

**2，调用**

**tacacs+ accounting 状态审计**

**tacacs+ administration 命令审计**