安全配置

目 录

第 1 章　AAA 配置

1.1　AAA概述

访问控制是用来控制接入交换机或网络访问服务器（NAS）的用户，并限制他们可使用的服务种类。提供认证、授权和记录（Authentication，Authorization，Accounting）功能，以提高网络安全性能。

1.1.1　AAA 安全服务

AAA 是使用相同方式配置三种独立的安全功能的一种体系结构。它提供了完成下列服务的模块化方法：

- 认证（Authentication）——提供一种识别用户的方法，包括用户名和口令的询问，以及根据所选择的安全协议进行加密。

  认证是接受用户访问请求和提供网络服务之前识别他们身份的方法。通过定义一张命名的认证方法列表来对认证进行配置，然后应用该列表于各种接口。方法列表定义了所执行的认证的类型和它们执行的次序；任何定义的认证方法执行之前都必须应用在具体的接口上。唯一的例外是缺省方法列表（其名称为 default）。如果没有定义其它方法列表，缺省方法列表自动应用于所有接口。定义任何方法列表将覆盖缺省方法列表。有关所有认证的配置方法的详细资料，请参见“认证配置”。

- 授权（Authorization）——提供一种远程访问控制的方法，用于限制用户的服务权限。

  AAA 授权通过相对于该用户的一组属性来发挥作用，这些属性描述了用户被授予哪些权限。将这些属性与包括在数据库中某个特定用户的信息相比较，结果返回给 AAA，以确定该用户的实际权限。这个数据库可以位于所访问的本地服务器或交换机，或者位于远程 RADIUS 或 TACACS+安全服务器。像 RADIUS 和 TACACS+这样的远程安全服务器，通过与用户相联系的属性值（AV）对（Attribute-Value Pairs）来完成对用户的授权，属性值（AV）对定义了允许授予的权限。所有的授权方法必须通过 AAA 定义。与认证一样，首先要定义一个授权方法列表，然后在各种接口中应用该列表。有关使用 AAA 进行授权配置的详细情况，请参见“授权配置”。

- 记账（Accounting）——提供一种收集用户服务信息，并发送给安全服务器的方法，这些信息可用于开列账单、审计和形成报表，如用户标识、开始时间和停止时间、执行的命令、数据包的数量以及字节数。

  记账功能不仅可以跟踪用户访问的服务，同时还可以跟踪他们消耗的网络资源数量。当激活 AAA 记录功能时，网络访问服务器以记录的形式向 TACACS+或 RADIUS 安全服务器报告用户的活动。每条记录包括记录属性值（AV）对，存储在安全服务器上。这些数据可用于网络管理、客户账单或审计分析。与认证和授权一样，要先定义一个记录方法列表，然后在不同的接口中使用这张表。有关使用 AAA 进行记账配置的详细材料，请参见“记账配置”。

1.1.2 使用 AAA 的优点

AAA 提供了如下优点：

- 灵活性和易于控制
- 方便升级
- 标准化的认证方法，如 RADIUS、TACACS+
- 多重备用系统

1.1.3 AAA 基本原理

AAA 用来动态配置基于每条线路（每个用户）或者每项服务（例如，IP、IPX 或 VPDN）的认证、授权及记账类型。通过创建方法列表定义认证和授权的类型，然后把这些方法列表应用到具体服务或接口上。

1.1.4 AAA 方法列表

要对 AAA 进行配置，首先定义一个命名的方法列表，然后将这张列表应用到具体的服务或者接口上。该方法列表定义了所要执行的 AAA 类型，以及他们将被执行的次序；所定义的任何方法列表在被执行之前，必须应用于某一个具体的接口或者服务。唯一例外的是缺省方法列表（default）。缺省方法列表自动的应用于所有的接口或者服务。除非该接口明确引用了其他方法列表，这时此方法列表将替代缺省方法列表。

方法列表是用户在请求 AAA 服务时需要顺序查询的 AAA 方法的表格。在方法列表中可以指派一个或多个安全协议。因此确保了万一最初的方法失败后有一个备用的认证系统。本公司交换机软件使用方法列表中的第一个方法鉴别用户；如果该方法没有反应，则会选择方法列表中的下一个方法。这一个过程一直进行下去，直至所列的某个方法成功的进行 AAA 服务，或者所有的方法用完为止。

注意到这一点是很重要的，即本公司交换机软件仅仅在前面的方法没有反应时，才尝试使用列在后面的 AAA 方法进行 AAA 服务。如果 AAA 服务在这个过程中的任何一点上失败了，即安全服务器或是本地用户数据库的反应是拒绝用户访问，则 AAA 服务过程停止，并且不再尝试其他的认证方法。

下图显示了一个很有代表性的 AAA 网络配置，包含四个安全服务器，R1 和 R2 是 RADIUS 服务器，T1 和 T2 是 TACACS＋服务器。我们以认证为例来讲述 AAA 服务与 AAA 方法列表的关系。

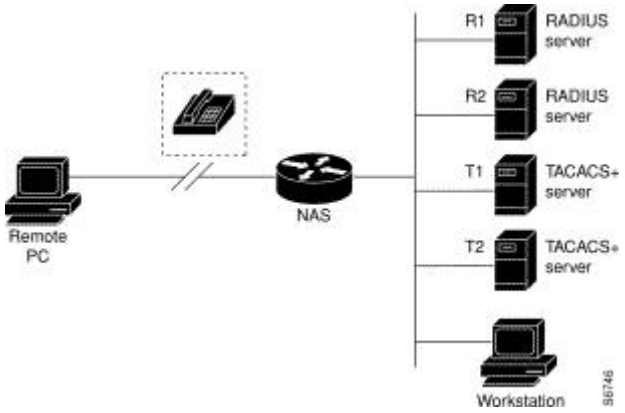

图 1-1 AAA 网络配置示意图

本例中，default 是方法列表的名称，包括在方法列表中的协议以及他们将被查询的次序列在方法列表名称后面。缺省列表自动的应用于所有的接口。

当远程用户试图通过拨号进入网络时，网络访问服务器首先在 R1 上查询有关的认证信息，如果鉴别该用户合法，他就发一条 PASS 应答给网络访问服务器，从而允许用户访问服务器。如果 R1 返回一条 FAIL 应答，则该用户被拒绝访问，本次对话结束。如果 R1 没有反应，网络访问服务器将其当成一次错误，并且在 R2 上查阅有关的认证信息。这种模式在剩下的方法中一直进行下去，直到该用户被接受或者被拒绝、或者本次对话结束为止。

记住这一条是很重要的，即 FAIL 应答与 ERROR 应答是截然不同的两个东西，FAIL 意味着用户没有满足包含在认证数据库中要认证成功所需的标准。认证以 FAIL 应答结束。ERROR 意味着该安全服务器对认证查询没有应答。仅仅当 AAA 检测到 ERROR 应答时，他才选择定义在认证方法链表中的下一个认证方法。

假设系统管理员想将方法列表仅仅应用于某个或某种特定的端口。在这种情况下，系统管理员应当创建一个非缺省的方法列表，然后把这个命名的列表应用到适当的端口上。

1.1.5 AAA 配置过程

首先，必须决定想要实现何种类型的安全方案。用户需要评估自己网络中的安全风险，并且确定合适的方法来阻止未经授权的登录和攻击。在明白了配置所涉及的基本过程后，配置 AAA 就相对简单了。在本公司交换机或访问服务器上使用 AAA 进行安全配置，遵循如下步骤：

- 如果决定使用安全服务器，则先配置安全协议参数，如 RADIUS，TACACS+。
- 使用命令 aaa authentication 定义用于认证的方法列表。
- 如果需要的话，把该方法列表应用到某个具体的接口或线路上
- 使用命令 aaa authorization 进行授权配置（可选）。
- 使用命令 aaa accounting 进行记录配置（可选）。

1.2 认证配置

1.2.1 认证配置任务列表

- 使用 AAA 配置登录认证
- 使用 AAA 进行 PPP 认证
- 在进入特权级别时开启口令保护
- 为 AAA 认证配置消息标语
- 改变提示输入用户名时的字符串
- 改变提示输入口令时的字符串
- 建立本地用户名认证数据库
- 建立本地特权级别认证数据库

1.2.2 认证配置任务

AAA 认证的一般配置过程

要配置 AAA 认证，需要完成下列配置过程：

(1) 如果使用的是安全服务器，配置安全协议参数，如 RADIUS、TACACS＋。具体配置方法参见相应章节。

(2) 使用 aaa authentication 命令定义认证方法列表。

(3) 如果需要的话，把方法列表应用到特定的端口或是线路上。

1.2.2.1 使用 AAA 配置登录认证

AAA 安全服务使得使用各种认证方法变得更容易了，不论决定使用哪种登录方法，都使用 aaa authentication 命令开启 AAA 认证。在 aaa authentication login 命令中，创建一张或是多张认证方法的列表，这些列表在登录时使用。使用线路配置命令 login authentication 来应用这些列表。配置时，从全局配置模式开始，使用如下命令：

命令	目的
aaa authentication login {**default** | *list-name*}*method1* [*method2...*]	创建全局认证列表。
line [**console** | **vty**] *line-number* [*ending-line-number*]	进入某个线路的配置状态。
login authentication {**default** | *list-name*}	应用该认证列表于某条或是某几个线路上。(在线路模式下)

关键字 list-name 是用来命名所创建的列表的任何字符串。关键字 method 指定认证过程所采用的实际方法。仅当前面所用的方法返回认证错误时，才会使用其他的认证方法，如果前面的方法指明认证失败了，则不再使用其他的认证方法。如果要指定即使所有的方法都返回认证错误仍能成功登录，只要在命令行中指定 none 作为最后一个认证方法。

使用 default 参数可建立一个缺省的列表，缺省列表自动的应用于所有的接口。例如：指定 RADIUS 作为用户登录时的缺省认证方式，使用下面的命令：

aaa authentication login default group radius

注意：

由于关键字 none 使得登录的任何用户都可成功的通过认证，所以应当将该关键字作为备用的认证方法。

登陆时，如果找不到认证方法列表的话，除 console 口登陆以外，其它任何形式的登陆将以认证失败结束。

下表列出了目前支持的登录认证方式：

关键字	说明
enable	使用enable口令进行认证。
group *name*	使用命名的服务器组进行认证。
group radius	使用 RADIUS 认证。
group tacacs+	使用TACACS+进行认证。
line	使用线路密码进行认证。
local	使用本地数据库进行认证。
localgroup	使用本地策略组用户名数据库进行认证。
local-case	使用本地用户名数据库进行认证(用户名区分大小写)。
none	认证无条件通过。

(1) 使用 enable 口令进行登录认证

在 aaa authentication login 命令中使用 enable 方法关键字指定 enable 口令作为登录认证方法，例如：在没有定义其他方法时，指定 enable 口令作为登录时用户认证的方法，使用下面的命令：

aaa authentication login default enable

(2) 使用线路口令进行登录认证

在使用 aaa authentication login 命令时，用 line 方法关键字指定线路口令作为登录时的认证方法。例如，在用户登录时指定线路口令为用户认证方法，并且不定义任何其他方法，可以输入下面的命令行：

aaa authentication login default line

在能够使用线路口令进行注册认证之前，需要定义一条线路口令。

(3) 使用本地口令进行登录认证

在使用 aaa authentication login 命令时，用 local 方法关键字指定使用本地用户名数据库作为登录认证方法。例如，在用户注册时指定本地用户名数据库作为用户认证方法，并且不定义任何其他方法，可以输入下面的命令行：

aaa authentication login default local

有关增加用户到本地用户名数据库中的详细资料，参见“建立本地认证数据库”。

(4) 使用 RADIUS 进行登录认证

在使用 aaa authentication login 命令时，用 radius 方法关键字指定 RADIUS 作为登录认证方法。例如在用户登录时指定 RADIUS 为用户认证方法，并且不定义任何其他方法，可以输入下面的命令：

aaa authentication login default group radius

在能使用 RADIUS 作为注册认证方法之前，需要首先配置 RADIUS 服务，有关的更多信息参见“配置 RADIUS”。

1.2.2.2 在进入特权级别时开启口令保护

使用 aaa authentication enable default 命令创建一个认证方法列表，这些方法决定了某个用户是否可以执行特权级别的 EXEC 命令。可以至多指定四种认证方法。仅当前面所用的方法返回认证错误时，才会使用其他的认证方法。如果前面使用的方法返回认证失败，则不再使用其他的认证方法，如果指定即使所有的方法都返回错误仍能成功认证，只需在命令中指定 none 作为最后一个认证方法。配置时，在全局配置模式下使用下面的命令：

命令	目的
aaa authentication enable default *method1* [*method2...*]	在用户进入特权级别时开启口令认证。

关键字 method 指定认证过程使用的实际方法，在认证时依输入的次序使用。

下表列出了所支持的口令保护认证方法：

关键字	说明
enable	使用enable口令认证。
group *group-name*	使用命名的服务器组进行认证。
group radius	使用RADIUS进行认证。
group tacacs+	使用tacacs+进行认证。
line	使用线路口令认证。
none	认证无条件通过。

当配置了 enable 认证方法为远端认证时，使用 RADIUS 进行认证，如下面介绍：

(1) 使用 RADIUS 进行 enable 认证：

认证的用户名为$ENABLE*level*$，其中 level 是指用户要进入的特权级别，即 enable 命令后的特权级别的数字，举例来说，如果某用户要进入级别为 7 的特权级别，需要输入命令 enable 7，如果此时配置了使用 RADIUS 进行认证，则提交给 Radius-server host 的用户名为$ENABLE7$，缺省条件下 enable 进入的特权级别

均为 15，即在使用 RADIUS 进行认证时，提交给 Radius-server host 的用户名为 $ENABLE15$。这就需要预先在 Radius-server host 上配置相应的用户名和密码，特别要指出的是：在 Radius-server host 的用户数据库中，要指明用于特权认证的用户的服务类型（Service-Type）为 6，即 Admin-User。

1.2.2.3 为 AAA 认证配置消息标语

支持使用可配置的、个性化的登陆及登陆失败标语。即在用户登陆进入系统将用 AAA 认证时，以及无论什么原因认证失败时，将显示所配置的消息标语。

配置注册标语

全局配置模式下，使用下述命令：

命令	目的
aaa authentication banner *delimiter text-string delimiter*	配置一个个性化的登陆注册标语

配置登陆失败标语

全局配置模式下，使用下述命令：

命令	目的
aaa authentication fail-message *delimiter text-string delimiter*	配置一个个性化的登陆失败的标语

使用说明

创建标语时，需要配置一个定界符号”，然后再配置文本字符串本身，该定界符号的作用是通知系统下面的文本字符串将被作为标语显示。定界字符在文本字符串的尾部重复出现，表示标语结束。

1.2.2.4 改变提示输入用户名时的字符串

使用 aaa authentication username-prompt 命令可以改变提示用户输入用户名时所显示的缺省文本。该命令的 no 形式恢复口令提示为如下形式的缺省值：

username：

命令 aaa authentication username-prompt 不改变远程 TACACS＋或是 RADIUS 服务器所提供的任何提示信息。配置时，在全局模式下使用下面的命令：

命令	目的
aaa authentication username-prompt *text-string*	在提示用户输入用户名时改变缺省的显示文本。

1.2.2.5 改变提示输入口令时的字符串

使用 aaa authentication password-prompt 命令可以改变提示用户输入口令时所显示的缺省文本。这条命令不仅改变 enable 口令的口令提示，也同时改变远端登录时的口令提示。该命令的 no 形式恢复口令提示为如下形式的缺省值：

password：

命令 aaa authentication password-prompt 不改变远程 TACACS＋或是 RADIUS 服务器所提供的任何提示信息。配置时，在全局模式下使用下面的命令：

命令	目的
aaa authentication password-prompt *text-string*	在提示用户输入口令时改变缺省的显示文本。

1.2.2.6 建立本地特权级别认证数据库

创建基于本地的密码数据库，用于控制用户获取各种特权级别，要建立本地各种特权级别的 enable 密码数据库，可以在全局配置模式下，使用下面命令进行配置，删除时，利用该命令的 no 形式：

enable password { [***encryption-type***] *encrypted-password*} [**level** *level*]

no enable password [**level** *level*]

1.2.3 认证配置示例

1.2.3.1 RADIUS 认证示例

本节提供了一个使用 RADIUS 进行认证的配置示例，展示了如何配置交换机，以便使用 RADIUS 进行认证和授权的过程：

```
aaa authentication login radius-login group radius local
aaa authorization network radius-network group radius
line vty 3
login authentication radius-login
```

在这个示例中，各命令行的意义为：

- 命令 aaa authentication login radius-login group radius local 配置交换机在认证登录用户时使用 RADIUS 作为认证方法。如果 RADIUS 返回认证错误，则使用本地数据库对用户进行认证。
- 命令 aaa authorization network radius-network group radius 向 radius 请求 NETWORK 服务的授权，如：地址分配以及其他访问控制项目。
- 命令 login authentication radius-login 在线路 3 上开启 radius-login 方法列表。

1.3 授权配置

1.3.1 AAA 授权配置任务列表

- 使用 AAA 配置 EXEC 授权

1.3.2 AAA 授权配置任务

AAA 授权的一般配置过程

要配置 AAA 授权，需要完成下列配置过程：

(1) 如果使用的是安全服务器，配置安全协议参数，如 RADIUS、TACACS＋。具体配置方法参见相应章节。

(2) 使用 aaa authorization 命令定义授权方法列表。缺省情况下，不提供授权服务。

(3) 如果需要的话，把方法列表应用到特定的端口或是线路上。

1.3.2.1 使用 AAA 配置 exec 授权

使用 aaa authorization 命令开启 AAA 授权。在 aaa authorization exec 命令中，创建一张或是多张授权方法的列表，开启 EXEC 授权，以决定是否允许用户运行 EXEC 外壳程序，或者授于用户在进入 EXEC 外壳程序时的特权级别。使用线路配置命令 login authorization 来应用这些列表。配置时，从全局配置模式开始，使用如下命令：

命令	目的
aaa authorization exec {**default** | *list-name*}*method1* [*method2...*]	创建全局授权列表。
line [**console** | **vty**] *line-number* [*ending-line-number*]	进入某个线路的配置状态。
login authorization {**default** | *list-name*}	应用该授权列表于某条或是某几个线路上。(在线路模式下)

关键字 list-name 是用来命名所创建的列表的任何字符串。关键字 method 指定授权过程所采用的实际方法。仅当前面所用的方法返回授权错误时，才会使用其他的授权方法，如果前面的方法指明授权失败了，则不再使用其他的授权方法。如果要指定即使所有的方法都返回授权错误仍能进入 EXEC shell，只要在命令行中指定 none 作为最后一个授权方法。

使用 default 参数可建立一个缺省的列表，缺省列表自动的应用于所有的接口。例如：指定 RADIUS 作为 exec 的缺省授权方式，使用下面的命令：

aaa authorization exec default group radius

注意：

授权时，如果找不到授权方法列表的话，将不再进行授权服务，并允许授权通过。

下表列出了目前支持的 EXEC 授权方式：

关键字	说明
group *WORD*	使用命名的服务器组进行授权。
group radius	使用 RADIUS 授权。
group tacacs+	使用TACACS+进行授权。
local	使用本地数据库进行授权。
if-authenticated	如果选择了该方法， 则所要求的所有功能都自动的授予已经认证的用户。
none	授权无条件通过。

1.3.3 AAA 授权示例

1.3.3.1 EXEC 本地授权示例

本节提供了一个使用本地进行授权的配置示例，展示了如何配置交换机，以便使用 LOCAL 进行认证和授权的过程：

```
aaa authentication login default local
aaa authorization exec default local
!
localauthor a1
 exec privilege default 15
!
local author-group a1
username exec1 password 0 abc
username exec2 password 0 abc author-group a1
username exec3 password 0 abc maxlinks 10
username exec4 password 0 abc autocommand telnet 172.16.20.1
!
```

此配置中，各命令行的意义为：

- 命令 aaa authentication login default local 定义 login 认证的默认方法列表，该方法列表自动运用于所有登陆认证服务
- 命令 aaa authorization exec default local 定义了 exec 授权的默认方法列表，该方法列表自动运用于所有需要进入 EXEC shell 的用户
- 命令 localauthor a1 定义了一个名为 a1 的本地授权策略。exec privilege default 15 表示默认授予 exec 登陆用户优先级为 15。
- 命令 local author-group a1 表示把本地授权策略 a1 用于全局配置（即默认本地策略组）下。

- 命令 username exec1 password 0 abc 定义了一个全局配置下的账号 exec1，密码为 abc。
- 命令 username exec2 password 0 abc author-group a1 定义了一个全局配置下的账号 exec2，密码为 abc，该账号使用本地授权策略 a1。
- 命令 username exec3 password 0 abc maxlinks 10 定义了一个全局配置下的账号 exec3，密码为 abc，该账号最多允许同时 10 个用户使用。
- 命令 username exec4 password 0 abc autocommand telnet 172.16.20.1 了一个全局配置下的账号 exec4，密码为 abc，用户使用该账号登陆后自动执行 telnet 172.16.20.1。

1.4 记账配置

1.4.1 AAA 记账配置任务列表

- 使用 AAA 配置 connection 记账
- 使用 AAA 配置 network 记账

1.4.2 AAA 记账配置任务

AAA 记账的一般配置过程

要配置 AAA 记账，需要完成下列配置过程：

(1) 如果使用的是安全服务器，配置安全协议参数，如 RADIUS、TACACS＋。具体配置方法参见相应章节。

(2) 使用 aaa accounting 命令定义记账方法列表。缺省情况下，不提供记账服务。

(3) 如果需要的话，把方法列表应用到特定的端口或是线路上。

1.4.2.1 使用 AAA 配置 connection 记账

使用 aaa accounting 命令开启 AAA 记账。在 aaa accounting connection 命令中，创建一张或是多条记账方法的列表，开启 connection 记账，以提供所有从交换机产生的出站连接的信息，这些出站连接包括 Telnet、包重装/拆分（PAD）、H323 和 rlogin 等，暂时只支持 H323。配置时，从全局配置模式开始，使用如下命令：

命令	目的
aaa accounting connection {default | *list-name*} {{{start-stop | stop-only} group	创建全局记账列表。

groupname} | **none}**	

关键字 list-name 是用来命名所创建的列表的任何字符串。关键字 method 指定记账过程所采用的实际方法。

下表列出了目前支持的 connection 记账方式：

关键字	说明
group *WORD*	使用命名的服务器组进行记账。
group radius	使用 RADIUS 记账。
group tacacs+	使用 TACACS+ 记账。
none	关闭记账服务。
stop-only	该关键字指示所指定的方法只在所请求的用户过程结束时发送一条停止记录记账通知。
start-stop	该关键字指示所指定的方法在所要求的事件开始时发出开始记账通告，在该事件结束时发出终止通告。

1.4.2.2 使用 AAA 配置 network 记账

使用 aaa accounting 命令开启 AAA 记账。在 aaa accounting network 命令中，创建一张或是多条记账方法的列表，开启 network 记账，以给所有 PPP 或 SLIP 会话提供信息，包括包、字节及时间计数等。配置时，从全局配置模式开始，使用如下命令：

命令	目的
aaa accounting network {**default** | *list-name*} {{{**start-stop** | **stop-only**} **group** *groupname}* | **none**}	创建全局记账列表。

关键字 list-name 是用来命名所创建的列表的任何字符串。关键字 method 指定记账过程所采用的实际方法。

下表列出了目前支持的 network 记账方式：

关键字	说明
group *WORD*	使用命名的服务器组进行记账。
group radius	使用 RADIUS 记账。
group tacacs+	使用 TACACS+ 记账。
none	关闭记账服务。
stop-only	该关键字指示所指定的方法在所请求的用户过程结束时发送一条停止记录记账通知。
start-stop	该关键字指示所指定的方法在所要求的事件开始时发出开始记账通告，在该事件结束时发出终止通告。

1.4.2.3 使用 AAA 配置记账更新

使用 aaa accounting 命令激活 AAA 记账更新功能，以便 AAA 为系统中的所有用户发送临时记账记录。配置时，从全局配置模式开始，使用如下命令：

命令	目的
aaa accounting update [**newinfo**] [**periodic** *number*]	激活AAA记账更新

如果使用关键字 newinfo，则每当有新的记账信息要报告时，向记账服务器发送临时记账记录。比如，当 IPCP 完成与远程终端的 IP 地址协商时就是发生这种情况的一个示例，临时记账记录将包括远程终端使用的协商 IP 地址。

当使用关键字 periodic 时，则周期性地发送临时记账记录，该周期由数字参数定义。临时记账记录包含了到记账记录发送时为止的该用户的所有记账信息。

这两个关键字是相互排斥的，即无论后配置的是哪个关键字，都将取代前面的配置。例如，如果配置了 aaa accounting update periodic，然后配置了 aaa accounting update newinfo，则当前注册的所有用户仍将产生周期性的临时记账记录。所有新用户将基于 newinfo 算法产生记账记录。

1.4.2.4 抑制无用户名的用户记账

要阻止 AAA 系统给用户名字符串为空的用户发送记账记录，从全局配置模式开始，使用如下命令：

- **aaa accounting suppress null-username**

1.5 本地账号策略配置

1.5.1 本地账号策略配置任务列表

- 本地认证策略配置
- 本地授权策略配置
- 本地密码策略配置
- 本地策略组配置

1.5.2 本地账号策略配置任务

1.5.2.1 本地认证策略配置

全局配置态下，使用命令 localauthen *WORD* 进入本地认证策略配置态，在该配置态下下使用以下命令配置本地认证策略：

（1）一定时间内的最大登陆尝试次数

login max-tries *<1-9>* **try-duration** *1d2h3m4s*

配置好的本地认证策略可以应用在某个本地策略组或者直接应用在某个本地账号上，直接应用在某个本地账号上的优先使用。

1.5.2.2 本地授权策略配置

全局配置态下，使用命令 localauthor *WORD* 进入本地授权策略配置态，在该配置态下下使用以下命令配置本地授权策略：

（1）对登录进来的用户进行优先级授权

exec privilege {default | console | ssh | telnet} *<1-15>*

配置好的本地授权策略可以应用在某个本地策略组或者直接应用在某个本地账号上，直接应用在某个本地账号上的优先使用。

1.5.2.3 本地密码策略配置

全局配置态下，使用命令 localpass *WORD* 进入本地密码策略配置态，在该配置态下下使用以下命令配置本地密码策略：

（1）密码和用户名不同（配置账号或者修改密码时，密码和用户名不能相同）

non-user

（2）历史口令检查（修改密码时，密码和历史密码不能相同，记录历史口令 20 项）

non-history

（3）指定口令组成成分（配置账号或者修改密码时，增加密码的复杂度）

element *[number] [lower-letter] [upper-letter] [special-character]*

（4）口令最小长度（配置账号或者修改密码时，增加密码的复杂度）

min-length *<1-127>*

（5）口令有效期（配置账号或者修改密码后，密码的使用时间）

validity 1d2h3m4s

配置好的本地密码策略可以应用在某个本地策略组或者直接应用在某个本地账号上，直接应用在某个本地账号上的优先使用。

1.5.2.4 本地策略组配置

全局配置态下，使用命令 localgroup *WORD* 进入本地策略组配置态（全局配置态被认为是默认本地策略组配置态），在该配置态下下使用以下命令配置本地策略组：

（1）本地认证配置,把配置好的某个本地认证策略应用到该策略组下

local authen-group *WORD*

（2）本地授权配置,把配置好的某个本地授权策略应用到该策略组下

local author-group *WORD*

（3）本地密码配置,把配置好的某个本地密码策略应用到该策略组下

local pass-group *WORD*

（4）本地账号配置，对该策略组下的账号设置最大连接数、冻结

local user {{maxlinks *<1-255>***} | { freeze** *WORD* **}}**

（5）配置账号，在该策略组下配置账号，建立本地数据库

username *username* [**password** *password* | {**encryption-type** *encrypted-password*}] [**maxlinks** *number*] [**authen-group** *WORD*] [**author-group** *WORD*] [**pass-group** *WORD*] [**autocommand** *command*]

配置好的本地策略组可以应用于本地认证和授权。local 方法使用的是默认本地策略组，

localgroup word 使用的是配置的某个本地策略组。

1.5.3 本地账号策略配置示例

本节提供了一个本地账号策略的配置示例，展示了如何配置交换机，以便使用本地认证和授权的过程：

```
aaa authentication login default local
aaa authorization exec default local
!
localpass a3
 non-user
 non-history
 element number lower-letter upper-letter special-character
 min-length 10
 validity 2d
!
localauthen a1
 login max-tries 4 try-duration 2m
!
localauthor a2
```

```
 exec privilege default 15
!
local pass-group a3
local authen-group a1
local author-group a2
!
```

在这个示例中，各命令行的意义为：

- 命令 aaa authentication login default local 定义 login 认证的默认方法列表，该方法列表自动运用于所有登陆认证服务
- 命令 aaa authorization exec default local 定义了 exec 授权的默认方法列表，该方法列表自动运用于所有需要进入 EXEC shell 的用户
- 命令 localpass a3 定义了名为 a3 的密码策略。
- 命令 localauthen a1 定义了名为 a1 的认证策略。
- 命令 localauthor a2 定义了名为 a2 的授权策略。
- 命令 local pass-group a3 把名为 a3 的密码策略应用于默认策略组下。
- 命令 localauthen a1 把名为 a1 的认证策略应用于默认策略组下。
- 命令 localauthor a2 把名为 a2 的授权策略应用于默认策略组下。

第 2 章　配置 RADIUS

本章介绍 RADIUS（Remote Authentication Dial-In User Service）安全系统。定义其操作，说明适宜使用 RADIUS 技术和不适宜使用 RADIUS 技术的网络环境。“RADIUS 配置步骤”一节介绍如何使用认证、授权和记录（AAA）命令集配置 RADIUS。本章最后一节“RADIUS 配置示例”提供了两个实例。有关本章使用的 RADIUS 命令的完整描述，请参见“RADIUS 配置命令”。

2.1　概述

2.1.1　RADIUS 概述

RADIUS 是分布式客户机/服务器系统，它保护网络不受未经授权的访问的干扰。RADIUS 客户机运行于交换机上，并向中央 RADIUS 服务器发出认证请求，这里的中央服务器包含了所有的用户认证和网络访问服务信息。在交换机上我们利用 AAA 安全模式支持 RADIUS ，RADIUS 已经在既要求高级别安全性、又要求维持远程用户访问的各种网络环境中得以应用。

可以在具有下述访问安全要求的网络环境中使用 RADIUS：

- 拥有多厂商访问服务器的网络环境，并且每个服务器都支持 RADIUS。例如，几家厂商提供的访问服务器可以使用单一的基于服务器的 RADIUS 安全数据库。在使用多厂商提供的访问服务器的基于 IP 的网络中，拨号用户通过 RADIUS 服务器进行认证。

- 在用户必须只访问单一服务的网络中。使用 RADIUS，能够控制用户访问单一主机、单一实用程序（如 Telnet）或单一协议（如点对点协议 PPP）。例如，当用户登录时，RADIUS 规定并限制这个用户使用 IP 地址 10.2.3.4 来运行 PPP，并启动定义的访问列表。

- 要求资源记录的网络。可以使用与 RADIUS 认证或授权无关的 RADIUS 记录。RADIUS 记录允许在服务的开始和结束发送数据，以指示会话期间使用的资源数量（如时间、字节等等）。

RADIUS 不适合应用于下述网络安全情况中：

- RADIUS 不支持下述协议：

  AppleTalk 远程访问（ARA，AppleTalk Remote Access）协议

  NetBIOS 帧控制协议（NBFCP，NetBIOS Frame Control Protocol）

- NetWare 异步服务接口（NASI，NetWare Asynchronous ServicesInterface）

- X.25 PAD 连接

- 交换机到交换机的情况。RADIUS 不提供双向认证。在交换机上运行 RADIUS，只能完成呼入认证，对于呼出认证（即本地交换机要登录到远端交换机时需要通过远端交换机的认证）是无法完成的。
- 使用多种服务的网络。RADIUS 通常把用户捆绑到一个服务模型上。

2.1.2 RADIUS 协议操作

当用户使用 RADIUS 进行登录认证时，发生下述步骤：

(1) 提示用户输入用户名和口令。

(2) 用户名和加密的口令通过网络发送到 RADIUS 服务器。

(3) 用户从 RADIUS 服务器收到下述响应之一：

ACCEPT：用户通过认证。

REJECT：用户没有通过认证，提示用户重新输入用户名和口令，否则访问被拒绝。

CHALLENGE：服务器发出 Challenge 请求。该请求从用户那里收集附加数据。

ACCEPT 和 REJECT 响应与附加授权信息一起返回，用于 EXEC 或 NETWORK 授权。在使用 RADIUS 授权之前，必须首先完成 RADIUS 认证。ACCEPT 和 REJECT 包中包括的附加数据由下述内容组成：

a. 用户能够访问的服务，包括 Telnet、rlogin 等服务。

b. 连接参数，包括主机或客户机的 IP 地址、访问列表和用户超时设定等。

2.2 RADIUS配置步骤

为了在交换机或访问服务器上配置 RADIUS ，必须执行下述任务：

- 使用 aaa authentication 全局配置命令定义使用 RADIUS 认证方式的方法列表。有关使用 aaa authentication 命令的更多信息，请参见“认证配置”。
- 使用 line 和 interface 命令来引用已定义的方法列表。要了解更多的信息，请参见“认证配置”。

下述配置任务可根据需要进行选择：

- 如有必要，使用 aaa authorization 全局命令对用户的服务请求进行授权。有关使用 aaa authorization 命令的更多信息，请参见“授权配置”。
- 如有必要，使用 aaa accounting 全局命令对用户的服务过程进行记录。有关使用 aaa accounting 命令的更多信息，请参见“记录配置”。

2.3 RADIUS配置任务列表

- 配置交换机与 RADIUS 服务器的通信
- 使用厂商专用的 RADIUS 属性配置交换机

- 配置 RADIUS 认证
- 配置 RADIUS 授权
- 配置 RADIUS 记录

2.4 RADIUS配置任务

2.4.1 配置交换机与 RADIUS 服务器的通信

RADIUS 服务器通常是运行由 Livingston、Merit、 Microsoft 或另外的软件提供商提供的 RADIUS 服务器软件的多用户系统，RADIUS 服务器和交换机使用共享的密钥来加密口令并交换响应。使用 radius-server host 命令来指定 RADIUS 服务器，使用 radius-server key 命令来指定共享密钥。配置时，在全局配置模式下使用下述命令：

命令	目的
radius-server host *ip-address* [**auth-port** *port-number*][**acct-port** *portnumber*]	指定远程RADIUS服务器的IP地址，指定认证和记录的目的端口号。
radius-server key *string*	指定交换机和RADIUS服务器之间使用的共享密钥。

另外为了定制交换机和 RADIUS 服务器之间的通信，请使用下述可选的 radius 全局配置命令：

命令	目的
radius-server retransmit *retries*	指定交换机在放弃重试之前向服务器传输每个RADIUS请求的次数（缺省值为2）。
radius-server timeout *seconds*	指定交换机在重新传输RADIUS请求之前，对应答应等待的秒数。
radius-server deadtime *minutes*	当RADIUS服务器不对认证请求作出反应时，需要将此台服务器标志为“死亡”的持续时间。

2.4.2 使用厂商专用的 RADIUS 属性配置交换机

Internet 工程任务组（IETF）草案标准通过使用厂商专用属性（Attribute26），为在网络访问服务器和 RADIUS 服务器之间交互基于厂商的专用扩展属性提供了一种方法。厂商专用属性（VSA）允许厂商支持属于它们自己的不适合于普遍用途的扩展属性。有关厂商 ID 和厂商专用属性的更多信息，请参见 RFC 2138：远程认证拨号用户服务（RADIUS）。要把网络服务器配置为能够识别和使用厂商专用属性的方式，请在全局配置模式下使用下述命令：

命令	目的
radius-server vsa send [authentication]	使网络访问服务器能够如同RADIUS IETF属性26所定义的那样去识别和使用厂商专用属性。

2.4.3 配置 RADIUS 认证

在标识了 RADIUS 服务器并定义了 RADIUS 认证密钥之后，就需要为 RADIUS 认证定义方法列表。由于 RADIUS 认证是通过 AAA 来进行的，所以需要输入 aaa authentication 命令，指定 RADIUS 作为认证方法。要了解与此相关的更多信息，请参见 “认证配置”。

2.4.4 配置 RADIUS 授权

利用 AAA 授权可以设置参数、限制用户的网络访问。使用 RADIUS 的授权提供了一种远程访问控制的方法，包括一次性授权或对每个服务的授权。因为 RADIUS 授权是通过 AAA 进行的，所以需要使用 aaa authorization 命令，指定 RADIUS 作为授权方法。要了解与此相关的更多信息，请参见“授权配置”。

2.4.5 配置 RADIUS 记录

AAA 记录特性让我们能够追踪用户正在访问的服务及他们占用的网络资源数量。由于 RADIUS 记录特性是通过 AAA 提供的，所以需要使用 aaa accounting 命令，指定 RADIUS 作为记录方法。要了解与此相关的更多信息，请参见 “记录配置”。

2.5 RADIUS配置示例

2.5.1 RADIUS 认证示例

下述示例说明了怎样对交换机进行配置以使用 RADIUS 进行认证：

```
aaa authentication login use-radius group radius local
```

在这个示例中，各行命令的意义为：

aaa authentication login use-radius group radius local 命令配置交换机在登录过程中使用 RADIUS 进行认证。如果 RADIUS 服务器返回认证错误（ERROR），再使用本地数据库进行认证。在这个示例中，use-radius 是方法列表的名称，它指定首先进行 RADIUS 认证，然后再进行本地认证。

2.5.2 AAA 中应用 RADIUS 示例

下面是一个使用 AAA 命令集定义通用配置的示例：

```
radius-server host 1.2.3.4
radius-server key myRaDiUSpassWoRd
username root password AlongPassword
aaa authentication login admins group radius local
line vty 1 16
login authentication admins
```

在这个示例中，各命令行的意义为：

radius-server host 命令定义 RADIUS 服务器的 IP 地址；

radius-server key 命令定义网络访问服务器和 RADIUS 服务器主机之间的共享密钥；

aaa authentication login admins group radius local 命令定义了认证方法列表 admins，它指定首先通过 RADIUS 进行认证，然后（若 RADIUS 服务器不响应）使用本地认证；

login authentication admins 命令指定在登录认证中运用 admins 方法列表；

第 3 章　TACACS+配置

3.1　TACACS+概述

TACACS+是一种访问安全控制协议，它为用户获得对网络访问服务器的访问权提供集中化的验证。由于网络访问服务器和 TACACS+服务程序之间的信息交换采用加密形式，所以它可以保证通信的安全性。

在网络访问服务器上配置的 TACACS+特性使用之前，必须能够访问并配置 TACACS+服务器。TACACS+提供了独立的模块化认证、授权和记录能力。

认证——支持多种认证方式（ASCII、PAP、CHAP 等），同时提供处理与用户进行任意对话的能力（比如，提供登录用户名和口令后，向用户提出一些询问性问题，诸如家庭住址、服务类型和身份证号码等）。另外，TACACS+认证服务支持向用户屏幕发送信息，例如，发送信息通知用户，由于公司的口令老化政策，他们的口令必须更换。

授权——对提供服务期间用户的服务权限进行细致的控制，包括设置自动命令、访问控制、会话持续时间等。还可以对用户可能执行的命令强制加以限制。

记录——收集和发送用于生成收费单据、进行审计或网络资源使用状况统计的信息。网络管理员可以使用记录能力，为安全审计追踪用户的活动，或者为用户账单提供信息。记录功能记录了包括用户标识、起止时间、执行的命令、包的数量以及字节的数量等。

3.1.1　TACACS+的协议操作

3.1.1.1 ASCII 形式的认证

当用户登录到使用 TACACS+的网络访问服务器，并要求进行简单的 ASCII 形式的认证时，典型情况下会出现下述过程：

连接建立后，网络访问服务器与 TACACS+服务程序联系以获得用户名提示符，然后显示给用户。用户输入用户名，网络访问服务器与 TACACS+服务程序再次进行联系，得到口令提示符，把口令提示符显示给用户，用户输入口令，然后口令被发送给 TACACS+服务程序。

注意：

TACACS+允许在服务器程序和用户之间进行任意的会话，直到收集到足够的信息对用户进行认证为止。这通常是通过提示用户名和口令的组合而完成的，但是还可以包括其它的项目，诸如证件号码等，一切都是在 TACACS+服务器程序的控制之下进行的。

网络访问服务器最终从 TACACS+服务器收到下述反应之一：

ACCEPT	用户通过了认证，服务可以开始了。如果网络访问服务器被配置为要求服务授权，那么此时开始进行授权。

REJECT	用户未通过认证。用户可能被拒绝进行进一步的访问，或者提示重新进入登录过程，这取决于TACACS+服务器的处理方式。
ERROR	在认证期间发生了错误，原因可能发生在服务器，也可能是发生在服务器与网络访问服务器之间的网络连接中。如果收到ERROR回应，一般情况下，网络访问服务器会试着使用另一种方法对用户进行认证。
CONTINUE	提示用户输入附加的认证信息。

3.1.1.2 PAP 和 CHAP 形式的认证

PAP 登录与 ASCII 登录相类似，只不过到达网络访问服务器的用户名和口令是在 PAP 报文中，而不是由用户输入，所以不用提示用户输入相关信息。CHAP 登录在主要的内容上也是类似的。认证之后，如果网络访问服务器要求对用户进行授权，那么用户就需要进入授权阶段，但在处理 TACACS+授权之前，必须首先成功地完成 TACACS+认证。

如果要求进行 TACACS+授权，则再次与 TACACS+服务器程序联系并返回 ACCEPT 或 REJECT 授权反应。如果返回了 ACCEPT 反应，则可能包含 AV（attribute-value）对数据，用于规范该用户的 EXEC 或 NETWORK 会话，确定用户能够访问的服务。

3.2 TACACS+配置流程

为了配置为支持 TACACS+的方式，必须执行下述任务：

使用 tacacs-server 命令，指定一个或多个 TACACS+服务器 IP 地址。使用 tacacs key 命令，为网络访问服务器和 TACACS+服务器之间的所有信息交换指定加密密钥。同一密钥也必须在 TACACS+服务器程序中进行配置。

使用 aaa authentication 全局配置命令对使用 TACACS+进行认证的方法列表进行定义。有关 aaa authentication 命令的更多信息，请参见“认证配置”。

使用 line 和 interface 命令，对端口或线路运用所定义的方法列表。与此相关的更多信息，请参见“认证配置”。

3.3 TACACS+配置任务列表

- 指定 TACACS+服务器
- 设置 TACACS+加密密钥
- 指定使用 TACACS+进行认证
- 指定使用 TACACS+进行授权
- 指定使用 TACACS+进行记录

3.4 TACACS+配置任务

3.4.1 指定 TACACS+服务器

Tacacs-server 命令使你能够指定 TACACS+服务器的 IP 地址。由于 TACACS+软件按照配置的顺序搜索主机，这一特色对于设置不同的服务器优先级是有用的。为了指定 TACACS+主机，以全局配置模式使用下述命令：

命令	目的
tacacs-server host *ip-address* [**single-connection**| **multi-connection**] [**port** *integer*] [**timeout** *integer*] [**key** *string*]	指定TACACS+服务器IP地址及相应属性。

使用 tacacs-server 命令，还可以配置下述选项：

- 使用 single-connection 关键字指定采用单一连接, 这样做允许服务器程序处理更多的 TACACS＋操作，可能更有效。multi-connection 则是指示采用多条 TCP 连接。
- 使用 port 参数，指定 TACACS+服务器程序使用的 TCP 端口号。缺省的端口号是 49。
- 使用 timeout 参数，指定路由器等待服务器回应的时间上限（以秒为单位）。
- 使用 key 参数指定对报文进行加密和解密的密钥。

注意：

使用 tacacs-server 后接 host，再接 timeout 等命令指定的超时值将覆盖 tacacs-server timeout 命令设置的全局超时值； 使用 tacacs-server 指定的加密密钥将覆盖使用全局配置命令 tacacs-server key 设置的缺省密钥。所以可以使用本命令配置唯一的 TACACS+连接来加强网络的安全性。

3.4.2 设置 TACACS+加密密钥

为了设置 TACACS+报文加密密钥，在全局配置模式使用下述命令：

命令	目的
tacacs-server key *keystring*	设置与TACACS+服务器所使用密钥相匹配的加密密钥。

注意 ：

为了成功地进行加密，必须对 TACACS+服务器程序配置相同的密钥。

3.4.3 指定使用 TACACS+进行认证

在标识了 TACACS+服务器并定义了与之相联系的加密密钥后，就需要为 TACACS+认证定义方法列表。由于 TACACS+认证通过 AAA 进行操作，所以需要设置 aaa authentication 命令指定 TACACS+作为其认证方法。与此相关的更多信息，请参见“认证配置”。

3.4.4 指定使用 TACACS+进行授权

AAA 授权使得能够设置参数限制用户的网络访问权限。TACACS+授权，可以应用于命令、网络连接和 EXEC 会话等服务。由于 TACACS+授权是通过 AAA 提供的，所以需要配置 aaa authorization 命令指定 TACACS+作为授权方法。与此相关的更多信息，请参见“授权配置”。

3.4.5 指定使用 TACACS+进行记录

AAA 记录使得能够跟踪用户正在使用的服务以及他们消耗的网络资源的数量。由于 TACACS+记录是通过 AAA 提供的，所以需要配置 aaa accounting 命令指定 TACACS+作为记录方法。与此相关的更多信息，请参见“记录配置”。

3.5 TACACS+配置示例

本节包括了下述 TACACS+配置示例：

3.5.1 TACACS+认证示例

下述示例配置 login 认证由 TACACS+完成：

```
aaa authentication login test group tacacs+ local
tacacs -server host 1.2.3.4
tacacs-server key testkey
line vty 0
login authentication test
```

在这个示例中：

aaa authentication 命令定义了运行在 vty0 上使用的认证方法列表 test。关键字 tacacs+意味着认证通过 TACACS+进行，如果 TACACS+在认证期间不响应，则关键字 local 指示使用网络访问服务器上的本地数据库进行认证。

tacacs-server host 命令标识 TACACS+服务器的 IP 地址为 1.2.3.4。tacacs-server key 命令定义共享的加密密钥为 testkey。

下述示例将 TACACS+配置为 login 认证时使用的安全协议，但是不再使用方法列表 test，而是使用方法列表 default：

```
aaa authentication login default group tacacs+ local
tacacs-server host 1.2.3.4
tacacs-server key goaway
```

在这个示例中：

aaa authentication 命令定义 login 认证时使用的默认认证方法列表 default。如果需要认证，那么关键字 tacacs+意味着认证通过 TACACS+进行，如果 TACACS+在认证期间不响应，则关键字 local 指示使用网络访问服务器上的本地数据库进行认证。

tacacs-server host 命令标识 TACACS+服务器程序的 IP 地址为 1.2.3.4。tacacs-server key 命令定义共享的加密密钥为 goaway。

3.5.2 TACACS+授权示例

```
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+
tacacs-server host 10.1.2.3
tacacs-server key goaway
```

在这个示例中：

aaa authentication 命令定义 login 认证时使用的默认认证方法列表 default。如果需要认证，那么关键字 tacacs+意味着认证通过 TACACS+进行，如果 TACACS+在认证期间不响应，则关键字 local 指示使用网络访问服务器上的本地数据库进行认证。

aaa authorization 命令配置通过 TACACS+进行网络服务授权。

tacacs-server host 命令标识 TACACS+服务器 IP 地址为 10.1.2.3。tacacs-server key 命令定义共享的加密密钥为 goaway。

3.5.3 TACACS+记录示例

下述示例配置 login 认证的方法列表使用 TACACS+作为方法之一，并配置通过 TACACS+进行记录：

```
aaa authentication login default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
tacacs-server host 10.1.2.3
tacacs-server key goaway
```

在这个示例中：

aaa authentication 命令定义 login 认证时使用的默认认证方法列表 default。如果需要认证，那么关键字 tacacs+意味着认证通过 TACACS+进行，如果 TACACS+在认证期间不响应，则关键字 local 指示使用网络访问服务器上的本地数据库进行认证。

aaa accounting 命令配置通过 TACACS+进行网络服务的记录。在这个示例中，记录服务开始和结束时的相应信息，发送到 TACACS+服务器。

tacacs-server host 命令标识 TACACS+服务器的 IP 地址为 10.1.2.3。tacacs-server key 命令定义共享的加密密钥为 goaway