

安全配置

目 录

第 1 章 AAA配置.....	1
1.1 AAA概述.....	1
1.1.1 AAA安全服务.....	1
1.1.2 使用AAA的优点.....	2
1.1.3 AAA基本原理.....	2
1.1.4 AAA方法列表.....	2
1.2 AAA配置过程.....	3
1.2.1 AAA配置过程概览.....	3
1.3 AAA认证配置任务列表.....	4
1.4 AAA认证配置任务.....	4
1.4.1 使用AAA配置登录认证.....	4
1.4.2 在进入特权级别时开启口令保护.....	6
1.4.3 为AAA认证配置消息标语.....	7
1.4.4 改变提示输入用户名时的字符串.....	7
1.4.5 改变提示输入口令时的字符串.....	8
1.4.6 建立本地用户名认证数据库.....	8
1.4.7 建立本地特权级别认证数据库.....	8
1.5 AAA认证配置示例.....	9
1.6 AAA授权配置任务列表.....	9
1.7 AAA授权配置任务.....	9
1.7.1 使用AAA配置exec授权.....	10
1.8 AAA授权示例.....	10
1.9 AAA记帐配置任务列表.....	11
1.10 AAA记帐配置任务.....	11
1.10.1 使用AAA配置connection记帐.....	12
1.10.2 使用AAA配置network记帐.....	12
1.10.3 使用AAA配置记帐更新.....	13
1.10.4 抑制无用户名的用户记帐.....	13
第 2 章 配置RADIUS.....	14
2.1 概述.....	14
2.1.1 RADIUS概述.....	14
2.1.2 RADIUS协议操作.....	15
2.2 RADIUS配置步骤.....	15
2.3 RADIUS配置任务列表.....	15
2.4 RADIUS配置任务.....	16
2.4.1 配置交换机与RADIUS服务器的通信.....	16
2.4.2 使用厂商专用的RADIUS属性配置交换机.....	16

2.4.3 配置RADIUS认证	17
2.4.4 配置RADIUS授权	17
2.4.5 配置RADIUS记录	17
2.5 RADIUS配置示例	17
2.5.1 RADIUS认证和授权示例	17
2.5.2 AAA中应用RADIUS示例	17
第3章 Web认证配置	19
3.1 概述	19
3.1.1 理解Web认证	19
3.1.2 规划web认证	21
3.2 配置web认证	22
3.2.1 全局配置	22
3.2.2 接口配置	23
3.2.3 使能web认证	24
3.3 监控和维护web认证	24
3.3.1 查看全局配置	24
3.3.2 查看接口配置	25
3.3.3 查看用户状态	25
3.3.4 强行踢出用户	25
3.4 web认证配置示例	25

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 AAA 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”。

- 记帐（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帐单、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。

记帐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、客户帐单或审计分析。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 进行记帐配置的材料，请参见“记帐配置”。

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、授权及记帐类型。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。

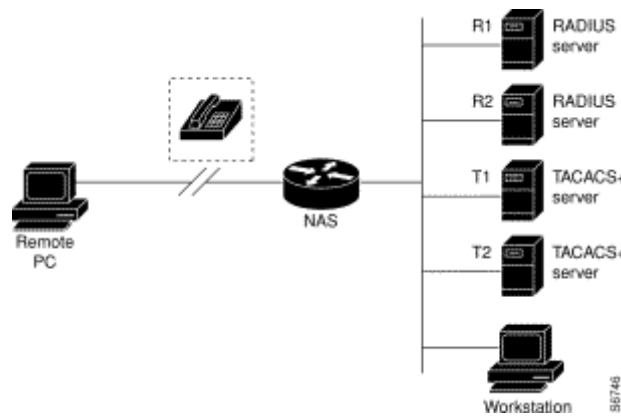


图 1-1 AAA 网络配置示意图

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。

1.2 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。

1.2.1 AAA配置过程概览

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）。

1.3 AAA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

1.4 AAA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。

1.4.1 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
<code>aaa authentication login {default list-name} method1 [method2...]</code>	创建全局认证列表。
<code>line [console vty] line-number [ending-line-number]</code>	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。
line	使用线路密码进行认证。
local	使用本地数据库进行认证。
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 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”。

1.4.2 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
<code>aaa authentication enable default method1 [method2...]</code>	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
<code>enable</code>	使用enable口令认证。
<code>group group-name</code>	使用命名的服务器组进行认证。
<code>group radius</code>	使用RADIUS进行认证。
<code>line</code>	使用线路口令认证。
<code>none</code>	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。

1.4.3 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 <i>text-string delimiter</i>	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 <i>text-string delimiter</i>	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。

1.4.4 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 <i>text-string</i>	在提示用户输入用户名时改变缺省的显示文本。

1.4.5 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 <i>text-string</i>	在提示用户输入口令时改变缺省的显示文本。

1.4.6 建立本地用户名认证数据库

创建基于本地认证的用户和密码，主要用于不支持 AAA 服务器（如 RADIUS）时，对用户提认证方法，以及提供专门情况下的注册：例如，访问列表验证、无口令验证、在注册时自动执行以及“无转义码”情况。

要建立本地用户名认证，可以在全局配置模式下，使用下面命令进行配置，删除用户名，利用该命令的 `no` 形式：

username *name* {**nopassword** | **password** *password* | **password** **encryption-type** *encrypted-password*}

username *name* [**autocommand** *command*]

username *name* [**callback-dialstring** *telephone-number*]

username *name* [**callback-rotary** *rotary-group-number*]

username *name* [**callback-line** [**tty** | **aux**] *line-number* [*ending-line-number*]]

username *name* [**noescape**] [**nohangup**]

username *name* [**privilege** *level*]

username *name* [**user-maxlinks** *number*]

no username *name*

1.4.7 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]

1.5 AAA认证配置示例

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 radius local
aaa authorization network radius-network radius
line vty
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 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 authentication ppp radius-ppp radius** 将交换机配置为：在用户尚未登录时，采用 chap 或是 pap 的 ppp 认证方法。如果 EXEC 已经对用户进行了认证，则不再执行认证。
- 命令 **aaa authorization network radius-network 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。

1.6 AAA授权配置任务列表

- 使用 AAA 配置 EXEC 授权

1.7 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。

1.7.1 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，或者授予用户在进入 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
<code>group WORD</code>	使用命名的服务器组进行授权。
<code>group radius</code>	使用 RADIUS 授权。
<code>local</code>	使用本地数据库进行授权。
<code>if-authenticated</code>	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。
<code>none</code>	授权无条件通过。

1.8 AAA授权示例

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
!
username exec1 password 0 abc privilege 15
username exec2 password 0 abc privilege 10
username exec3 nopassword
username exec4 password 0 abc user-maxlinks 10
username exec5 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
- 用户 `exec1`，登陆密码为 `abc`，EXEC 特权级别为 15（最高级别），即只要用户 `exec1` 登陆 EXEC shell，其特权级别即为 15，可以查看和执行所有命令。
- 用户 `exec2`，登陆密码为 `abc`，EXEC 特权级别为 10，即只要用户 `exec2` 登陆 EXEC shell，其特权级别即为 10，只可以查看和执行特权级别不大于 10 的命令。
- 用户 `exec3`，无需登陆密码。
- 用户 `exec4`，登陆密码为 `abc`，该用户限制回话最多为 10 条。
- 用户 `exec5`，登陆密码为 `abc`，该用户登陆到 exec shell 上以后，马上执行命令 `telnet 172.16.20.1`

1.9 AAA记帐配置任务列表

- 使用 AAA 配置 connection 记帐
- 使用 AAA 配置 network 记帐

1.10 AAA记帐配置任务

AAA 记帐的一般配置过程

要配置 AAA 记帐，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` 命令定义记帐方法列表。缺省情况下，不提供记帐服务。

- (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。

1.10.1 使用AAA配置connection记帐

使用 `aaa accounting` 命令开启 AAA 记帐。在 `aaa accounting connection` 命令中，创建一张或是多条记帐方法的列表，开启 `connection` 记帐，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 none} group groupname	创建全局记帐列表。

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` 指定记帐过程所采用的实际方法。

下表列出了目前支持的 `connection` 记帐方式：

关键字	说明
group WORD	使用命名的服务器组进行记帐。
group radius	使用 RADIUS 记帐。
none	关闭记帐服务。
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帐通知。
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帐通告，在该事件结束时发出终止通告。

1.10.2 使用AAA配置network记帐

使用 `aaa accounting` 命令开启 AAA 记帐。在 `aaa accounting network` 命令中，创建一张或是多条记帐方法的列表，开启 `network` 记帐，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 none} group groupname	创建全局记帐列表。

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` 指定记帐过程所采用的实际方法。

下表列出了目前支持的 `network` 记帐方式：

关键字	说明
group WORD	使用命名的服务器组进行记帐。

group radius	使用 RADIUS 记帐。
none	关闭记帐服务。
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帐通知。
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帐通告，在该事件结束时发出终止通告。

1.10.3 使用AAA配置记帐更新

使用 `aaa accounting` 命令激活 AAA 记帐更新功能，以便 AAA 为系统中的所有用户发送临时记帐记录。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记帐更新

如果使用关键字 `newinfo`，则每当有新的记帐信息要报告时，向记帐服务器发送临时记帐记录。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，临时记帐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帐记录，该周期由数字参数定义。临时记帐记录包含了到记帐记录发送时为止的该用户的所有记帐信息。

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 `aaaaccounting update newinfo`，则当前注册的所有用户仍将产生周期性的临时记帐记录。所有新用户将基于 `newinfo` 算法产生记帐记录。

1.10.4 抑制无用户名的用户记帐

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

- **aaa accounting suppress null-username**

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** 认证发式的方法列表。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 <i>ip-address</i> [auth-port <i>port-number</i>][acct-port <i>portnumber</i>]	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 <i>string</i>	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 <i>retries</i>	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 <i>seconds</i>	指定交换机在重新传输RADIUS请求之前，对响应等待的秒数。
radius-server deadtime <i>minutes</i>	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用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 [<i>authentication</i>]	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认证和授权示例

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 radius local
```

在这个示例中,各行命令的意义为:

`aaa authentication login use-radius 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 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 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 Web认证配置

本章中的配置任务介绍了交换机 web 认证的概念，以及如何配置和使用 web 认证。

3.1 概述

3.1.1 理解Web认证

交换机的 Web 认证是和 PPPoE、802.1x 并列的接入控制方式。用户在使用 Web 认证的时候，通过浏览器与交换机内置的 portal server 进行交互，完成登录和登出操作，不需要安装其他客户端软件。

1. 设备角色

使用Web认证时网络中设备角色如图 3-1：

- **client:** 需要通过交换机访问网络的用户计算机，用户计算机要求配备有网络浏览器、具有作为 DHCP client 的能力，能发起 DNS 查询。
- **DHCP server:** 负责为用户分配 IP 地址。
- **AAA server:** AAA server 保存用户的权限信息，并可对用户的网络访问进行记账。
- **switch:** 配备 web 认证功能的交换机，交换机控制用户的访问权限，并充当用户和 AAA server 之间的代理。

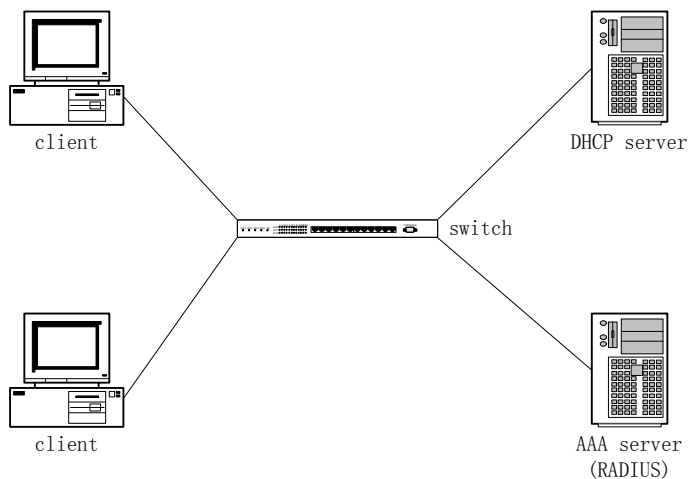


图 3-1 Web 认证网络

2. 认证流程

根据不同的配置策略，本交换机的web认证流程可能会和dhcp、dns等协议相关，其典型流程见图 3-2，概括起来，有以下几个步骤：

- (1) **DHCP server** 通过交换机向用户发送 **DHCP** 确认报文（当然，这之前，需要由用户发起 **DHCP** 地址分配过程），交换机识别并记录该用户；
- (2) 用户使用浏览器访问任意的 **web** 站点（浏览器中的 **url** 栏的主机部分填写域名而不是 **IP** 地址），这个过程会触发用户计算机的 **DNS** 请求；
- (3) **DNS server** 向用户发查询应答，交换机俘获该查询应答报文，并将解析出的地址更改为交换机内置的 **portal server** 的地址；
- (4) 用户浏览器在获得 **DNS** 解析后继续请求过程，交换机收到请求后，根据不同的认证方式返回相应的认证页面；
- (5) 用户提交自己的认证请求；交换机获得用户提交的信息后通过 **AAA server** 认证用户，如果认证通过，视配置需要通知 **AAA server** 开始记账；交换机放开用户的网络访问权限，并向用户返回包含认证成功信息的页面，同时交换机还返回一个 **keep alive** 页面，该页面周期性地向交换机发送用户在线通知报文；
- (6) 用户通过浏览器发出登出请求，交换机通知 **AAA server** 停止记账，并取消用户的网络访问权限；
- (7) 在用户通过认证之后和登出之前，交换机会周期性地检测来自用户的在线通知报文，如果在预定的时间之内收不到该报文，则认为用户已经非正常离线，于是交换机通知 **AAA server** 停止记账，并取消用户的网络访问权限；

以上步骤，随配置策略和用户的操作的不同会略有差异。比如，如果用户在通过认证之前直接访问交换机的 **portal server**，那么和 **DNS** 相关的过程是不会出现的。

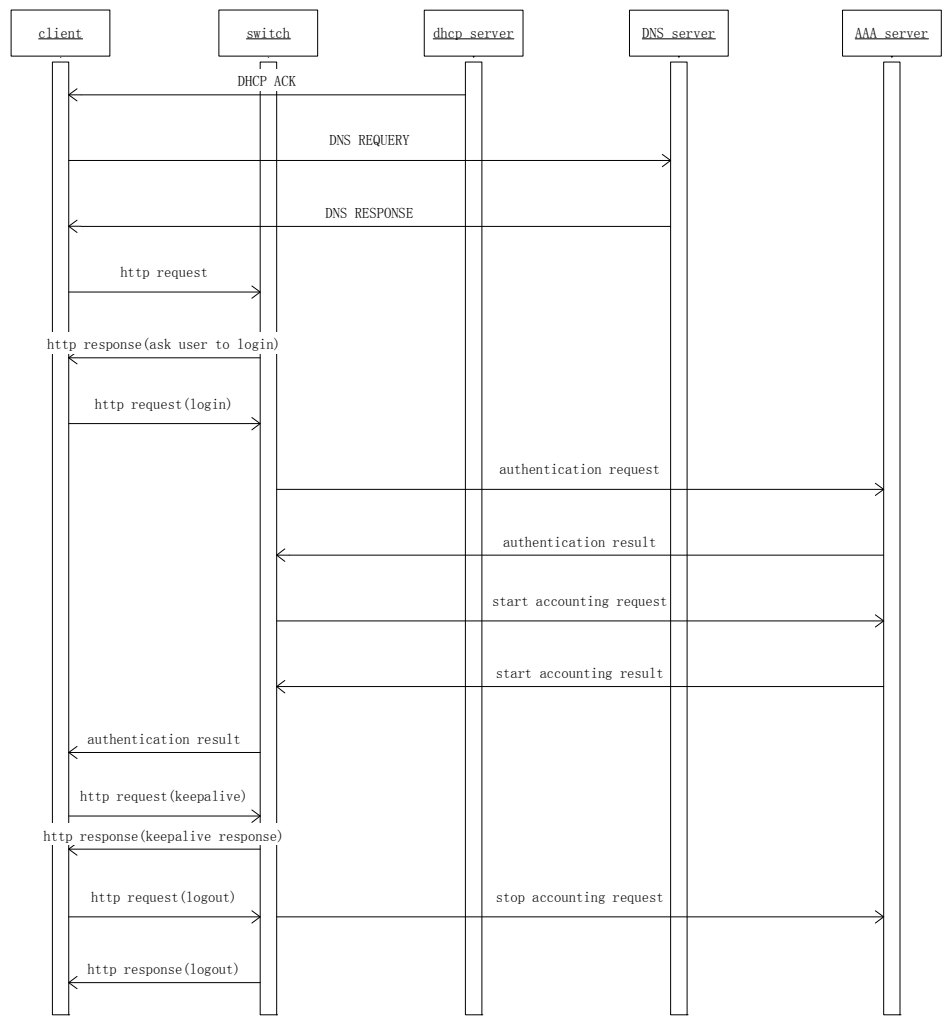


图 3-2 web 认证流程

3.1.2 规划web认证

1. 规划认证模式

我们提供两种认证模式来控制用户的接入：

第一种是用户名/口令的认证模式，在这种模式下，交换机根据用户名和口令来鉴别用户身份并根据用户名进行记账，用户在认证时需要通过浏览器输入用户名和口令；

第二种是 VLAN ID 认证模式，在这种模式下，交换机根据用户所属的 VLAN ID 来鉴别用户身份并根据 VLAN ID 来记账，这种模式下，用户在认证时不需要填写用户名和口令等信息，只需要在 Web 界面上进行确认操作即可完成网络接入。

这两种认证模式分别针对不同的运营策略，同时不同的认证模式可支持的最大同时接入用户数量也是不同的，采用第一种认证模式，交换机可同时接入和其性能匹配的用户数，采用第二种认证方式，可同时接入的最大用户数量等于交换机支持的 VLAN 数量。

2. 规划网络拓扑

交换机以路由接口作为设置认证属性的单位，凡是激活了web认证功能的路由接口，通过该接口接入的跨接口的网络访问皆受web认证的控制。DHCP server、DNS server、AAA server应该通过未激活web认证功能的接口和交换机连接，和外部网络连接的接口也不应该激活web认证功能，视配置需要，可以把DHCP server、DNS server、AAA server和外部网络通过同一个未激活web认证功能的接口和交换机连接。典型的网络拓扑见图 3-3：

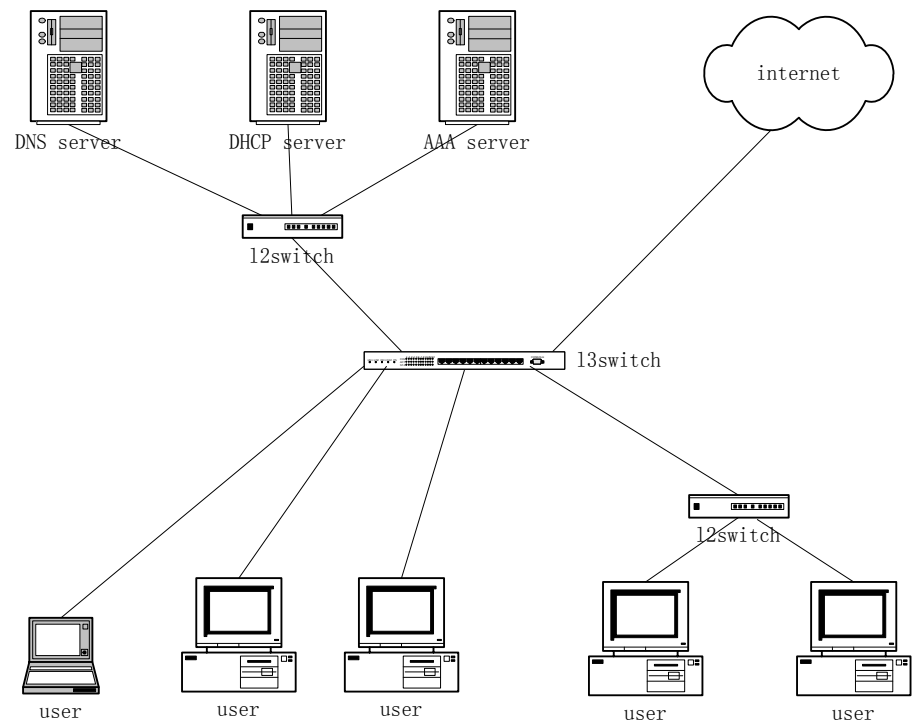


图 3-3 典型的网络拓扑

3.2 配置web认证

3.2.1 全局配置

1. 配置portal server 地址

在交换机的全局配置态下运行下面的命令配置 portal server 的 IP 地址：

命令	说明
web-auth portal-server A.B.C.D	配置portal server IP地址。

2. 配置认证持续时间

authtime 决定用户的认证过程可以持续的最长时间，如果超过这个时间还未通过认证，交换机将终止认证过程。

在交换机的全局配置态下运行下面的命令配置以秒为单位的认证持续时间：

命令	说明
web-auth authtime <60-65535>	配置认证持续时间。

3. 配置用户发送在线通知报文的周期

交换机通过用户浏览器周期性发送的在线通知报文来检测用户是否在线。

在交换机的全局配置态下运行下面的命令配置以秒为单位的发送周期：

命令	说明
web-auth keep-alive <60-65535>	配置在线通知报文发送周期。

4. 配置检测用户非正常下线的时长

当在设定的时长之内没有收到用户浏览器发送的在线通知报文，交换机将认为该用户非正常下线。

在交换机的全局配置态下运行下面的命令配置以秒为单位的检测时长：

命令	说明
web-auth holdtime <60-65535>	配置检测用户非正常下线的时长。

5. 配置使用VLAN ID进行认证时的口令

当接口的认证模式设置为 VLAN ID 时，交换机以 “vlan *n*” 作为用户名 “*n*” 表示相应的 VLAN 编号，所有的用户名都使用相同的口令。

在交换机的全局配置态下运行下面的命令配置以 VLAN ID 进行认证的用户的口令：

命令	说明
web-auth vlan-password <WORD>	配置以VLAN ID进行认证的用户的口令。

3.2.2 接口配置

1. 配置认证模式

交换机提供按用户名/口令和 VLAN ID 两种认证模式。

在交换机的接口配置态下运行下面的命令配置认证模式：

命令	说明
web-auth mode user vlan-id	配置接口的认证模式。

2. 配置认证方法列表

每个接口可以使用不同的认证方法列表，缺省情况下，使用名为“default”的认证方法列表。

在交换机的接口配置态下运行下面的命令配置认证方法列表：

命令	说明
web-auth authentication WORD	配置接口的认证方法列表。

3. 配置记账方法列表

每个接口可以使用不同的记账方法列表，缺省情况下，使用名为“default”的记账方法列表。

在交换机的接口配置态下运行下面的命令配置记账方法列表：

命令	说明
web-auth accounting WORD	配置接口的记账方法列表。

3.2.3 使能web认证

确认全局配置和接口配置符合需求后可以在指定的路由接口上使能 web 认证。

在交换机的接口配置态下运行下面的命令使能 web 认证：

命令	说明
web-auth enable	使能web认证。

3.3 监控和维护web认证

3.3.1 查看全局配置

为了查看 web 认证的全局配置参数可以在交换机的特权模式下运行下面的命令：

命令	说明
show web-auth	查看全局配置。

3.3.2 查看接口配置

为了查看指定接口的 web 认证配置参数可以在交换机的接口配置模式下运行下面的命令：

命令	说明
show web-auth interface [vlan SuperVlan]	查看接口配置。

3.3.3 查看用户状态

为了查看当前正在认证或者通过交换机接入网络的用户状态，可以在交换机的特权模式下运行下面的命令：

命令	说明
show web-auth user	查看用户状态

3.3.4 强行踢出用户

为了强行终止某个用户的认证过程或者中断已经通过认证的用户网络访问，可以在交换机的全局配置态下运行下面的命令：

命令	说明
web-auth kick-out user-IP	强行踢出用户。

3.4 web认证配置示例

网络拓扑

见图 3-4:

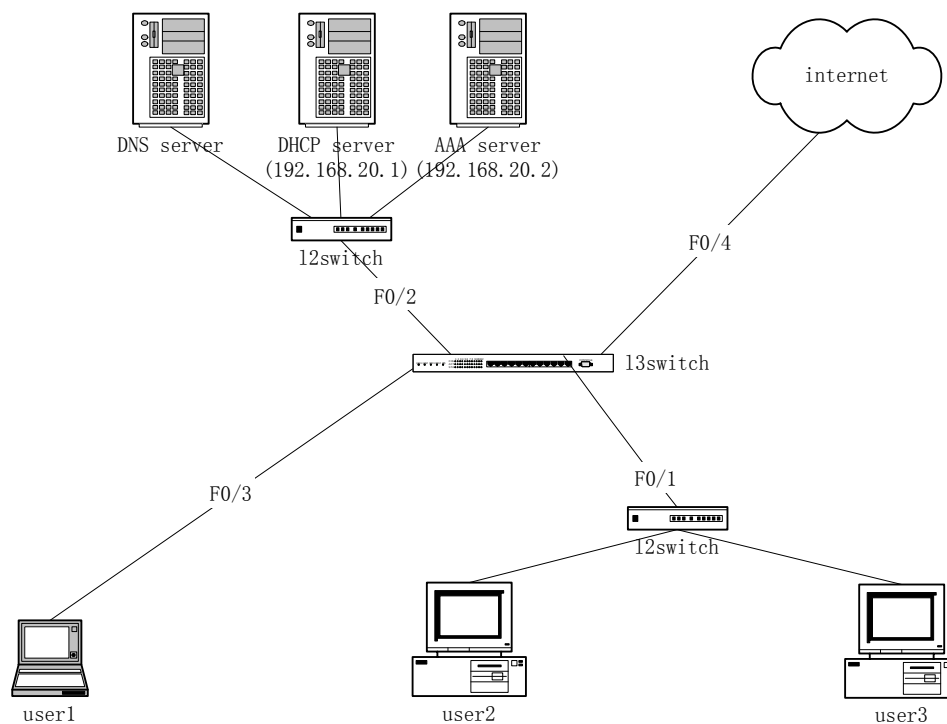


图 3-4 网络拓扑图

全局的配置

```

aaa authentication login auth-weba radius
aaa accounting network acct-weba start-stop radius
!
radius-server host 192.168.20.2 auth-port 1812 acct-port 1813
radius-server key 405.10
!
ip dhcpd enable
ip http server
!
vlan 1-4
!
web-auth portal-server 192.168.20.41
web-auth holdtime 3600
web-auth authtime 600
web-auth keep-alive 180

```

二层接口的配置

```

interface FastEthernet0/1
 switchport pvid 1
!
interface FastEthernet0/2
 switchport pvid 2

```

```
!  
interface FastEthernet0/3  
    switchport pvid 3  
!  
interface FastEthernet0/4  
    switchport pvid 4
```

路由接口的配置

```
interface VLAN1  
    no ip directed-broadcast  
    ip helper-address 192.168.20.1  
    web-auth accounting acct-weba  
    web-auth authentication auth-weba  
    web-auth mode vlan-id  
    web-auth enable  
!  
interface VLAN2  
    ip address 192.168.20.41 255.255.255.0  
    no ip directed-broadcast  
!  
interface VLAN3  
    no ip directed-broadcast  
    ip helper-address 192.168.20.1  
    web-auth accounting acct-weba  
    web-auth authentication auth-weba  
    web-auth mode user  
    web-auth enable  
!  
interface VLAN4  
    no ip directed-broadcast  
!
```