

安全配置命令

目 录

第 1 章 AAA认证配置命令	1
1.1 AAA认证配置命令	1
1.1.1 aaa authentication enable default	1
1.1.2 aaa authentication login	3
1.1.3 aaa authentication password-prompt	4
1.1.4 aaa authentication username-prompt	5
1.1.5 aaa group server	6
1.1.6 debug aaa authentication	7
1.1.7 enable password	8
1.1.8 server	10
1.1.9 service password-encryption	10
1.1.10 username	11
第 2 章 RADIUS配置命令	14
2.1 RADIUS配置命令	14
2.1.1 debug radius	14
2.1.2 ip radius source-interface	16
2.1.3 radius-server challenge-noecho	17
2.1.4 radius-server deadtime	17
2.1.5 radius-server host	18
2.1.6 radius-server optional-passwords	19
2.1.7 radius-server key	20
2.1.8 radius-server retransmit	21
2.1.9 radius-server timeout	22
2.1.10 radius-server vsa send	23
第 3 章 Web认证命令	25
3.1 web认证配置命令	25
3.1.1 web-auth enable	26
3.1.2 web-auth accounting	26
3.1.3 web-auth authentication	27
3.1.4 web-auth mode	28
3.1.5 web-auth keep-alive	29
3.1.6 web-auth holdtime	29
3.1.7 web-auth authtime	30
3.1.8 web-auth portal-server	31
3.1.9 web-auth vlan-password	32
3.1.10 web-auth kick-out	32
3.1.11 show web-auth	33
3.1.12 show web-auth interface	34
3.1.13 show web-auth user	35
3.1.14 debug web-auth event	35
3.1.15 debug web-auth error	36

3.1.16 debug web-auth verbose.....	37
3.1.17 debug web-auth http event.....	37
3.1.18 debug web-auth http request.....	38
3.1.19 debug web-auth http.....	39
3.1.20 debug web-auth.....	39

第1章 AAA认证配置命令

1.1 AAA认证配置命令

本章描述了用来配置 AAA 认证方法的命令。认证在用户被允许访问网络和网络服务之前对他们作出访问权利的鉴定。

如果想得到关于怎样用 AAA 的方法来配置认证的信息，请查阅“配置认证”。如果想查阅使用本章中命令进行配置的例子，阅读“配置认证”文档最后的示例部分。

AAA 认证配置命令有：

- `aaa authentication enable default`
- `aaa authentication login`
- `aaa authentication password-prompt`
- `aaa authentication username-prompt`
- `aaa group server`
- `debug aaa authentication`
- `enable password`
- `server`
- `service_password-encryption`
- `username`

1.1.1 aaa authentication enable default

要开放 AAA 认证，以确定某个用户是否可以访问特权级别的命令，使用本地配置命令 `aaa authentication enable default`。使用该命令的 `no` 形式关闭这种认证方法。

aaa authentication enable default *method1* [*method2*...]

no aaa authentication enable default *method1* [*method2*...]

参数

参数	参数说明
<i>method</i>	至少为表 1-1中所给出的关键字之一。

缺省

如果没有设置 **default**，则使用 **enable** 口令进行认证，与下面的命令具有相同的效果：

aaa authentication enable default enable

在配置表中，如果存在 **enable** 口令，则使用该口令。如果没有设置口令，则该过程总返回结果认为认证成功。

命令模式

全局配置态

使用说明

使用 **aaa authentication enable default** 命令创建一系列的认证方法，这些方法用来确定某个用户是否可以使用特权级别的命令。关键字 **method** 在表 1 中已经作了说明。只有在前面的认证方法返回错误时，才使用其它的认证方法，如果前面的认证方法返回结果通知认证失败，则不使用其它的认证方法。若希望即使所有的认证方法都返回失败，认证仍然成功，则可以把 **none** 指定为命令行的最后一个认证方法。

表 1-1 AAA 认证的有效缺省方法表

关键字	描述
group name	使用服务器组进行认证。
enable	使用enable口令进行认证。
line	使用线路口令进行认证。
none	认证无条件通过。
group radius	使用RADIUS进行认证。

示例

下面的示例创建一张认证列表，该列表首先尝试与 TACACS+服务器联系。如果没有发现 TACACS+服务器或服务器返回错误，AAA 尝试使用 **enable** 口令。如果这种尝试也返回错误（由于服务器上没有配置有效的口令），则允许用户不经认证就可以访问服务器。

aaa authentication enable default line enable none

相关命令

enable password

1.1.2 aaa authentication login

要设置在登录时进行 AAA 认证，使用全局配置命令 `aaa authentication login`。使用本命令的 `no` 形式关闭 AAA 认证。

aaa authentication login {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication login {**default** | *list-name*} *method1* [*method2*...]

参数

参数	参数说明
Default	使用跟随在该参数后面所列的认证方法作为用户注册时缺省的方法列表。
<i>list-name</i>	用来命名认证方法列表的字符串，用户登录时将激活认证方法列表中所列的方法。
method	至少为表 1-2 中描述的关键字之一。

缺省

如果没有设置 **default** 方式列表，则缺省不进行认证。此时，它与下面的命令具有同样的效果：

`aaa authentication login default none`

命令模式

全局配置态

使用说明

使用 `aaa authentication login` 命令创建的缺省列表或其他命名列表将由命令 `login authentication` 作用于某一具体线路。

只有前面的方法返回错误时，才使用其它的认证方法，如果前面的认证方法返回失败，则不使用其它的认证方法。要确保即使所有的方法都返回错误仍能认证成功，可将 **none** 指定为该命令行的最后方法。

如果没有给某条线路特别设置认证，缺省时不执行任何认证。

表 1-2 AAA 认证的注册方法

关键字	描述
enable	使用enable口令进行认证。
group	使用服务器组进行认证。
line	使用line密码进行认证。
local	使用本地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	不进行认证。
group radius	使用RADIUS进行认证。

示例

下面的示例创建一张名为“TEST”的 AAA 认证方法列表。这个认证首先尝试与 TACACS+ 服务器联系。如果没有发现服务器或 TACACS+ 返回错误，AAA 尝试使用 enable 口令。如果这种尝试也返回错误（由于交换机上没有配置 enable 口令），则允许该用户不经认证访问网络。

```
aaa authentication login TEST tacacs+ enable none
```

下面的示例创建同样的列表，但设置了缺省列表，如果没有指定其它列表，所有登录认证均使用这个列表：

```
aaa authentication login default tacacs+ enable none
```

相关命令

无

1.1.3 aaa authentication password-prompt

要改变向用户提示输入口令时的文本显示，使用全局配置命令 `aaa authentication password-prompt`。使用该命令的 `no` 形式重新使用缺省的口令提示文本。

```
aaa authentication password-prompt text-string
```

```
no aaa authentication password-prompt text-string
```

参数

参数	参数说明
test-string	向用户提示输入口令时将要显示的文本。

缺省

没有用户定义的 `text-string` 时，口令提示为 “Password:”。

命令模式

全局配置态

使用说明

使用 `aaa authentication password-prompt` 命令可改变向用户提示输入口令时显示的缺省文字信息。这条命令不但改变 `enable` 口令的口令提示，也改变登录口令的口令提示。该命令的 `no` 形式将口令提示改回到缺省值：

Password:

`aaa authentication password-prompt` 命令不改变由远程 TACACS+或 RADIUS 服务器提供的任何提示信息。

示例

下面的示例将口令提示修改为 “YourPassword:”：

`aaa authentication password-prompt YourPassword:`

相关命令

`aaa authentication username-prompt`

`enable password`

1.1.4 `aaa authentication username-prompt`

要改变向用户提示输入用户名时的文本显示，使用全局配置命令 `aaa authentication username-prompt`。使用该命令的 `no` 形式返回到缺省的用户名提示字符串。

`aaa authentication username-prompt text-string`

`no aaa authentication username-prompt text-string`

参数

参数	参数说明
<code>text-string</code>	向用户提示输入用户名时将要显示的文本

缺省

没有用户定义的 `text-string` 时，用户名提示字符串为 “Username”。

命令模式

全局配置态

使用说明

使用 `aaa authentication username-prompt` 命令改变向用户提示输入用户名时显示的提示字符串。该命令的 `no` 形式将用户名提示修改为缺省值：

Username:

某些协议（如 TACACS+）具备覆盖本地用户名提示信息的能力。在这种情况下，使用 `aaa authentication username-prompt` 命令将不改变用户名提示字符串。

注意：

`aaa authentication username-prompt` 命令不改变由远程 TACACS+服务器提供的任何提示信息。

示例

下面的示例将用户名提示修改为所示字符串：

`aaa authentication username-prompt YourUsername:`

相关命令

`aaa authentication password-prompt`

1.1.5 aaa group server

我们支持配置 AAA 服务器组，使用下面的命令进入服务器组配置层次。使用此命令的 `no` 形式删除已配置的服务器组。

aaa group server radius *group-name*

no aaa group server radius *group-name*

参数

参数	参数说明
<i>group-name</i>	服务器组的名称字符串。

缺省

无服务器组

命令模式

全局配置态

使用说明

使用此命令进入服务器组的配置层次，然后在其中添加相应的服务器。

示例

```
aaa group server radius radius-group
```

上面的命令将添加一个名字为“radius-group”的 radius 服务器组。

相关命令

server

1.1.6 debug aaa authentication

如果希望对用户的认证过程进行跟踪，可使用 debug aaa authentication 命令。使用此命令的 no 形式关掉 debug 信息。

debug aaa authentication

no debug aaa authentication

参数

无

缺省

关闭 debug 信息。

命令模式

管理态

使用说明

使用此命令可跟踪每个用户的认证过程，以发现认证失败的原因。

示例

下面的示例将打开认证的 debug 信息：

```
switch#debug aaa authentication
AAA: Authen start (0x1f74208), user=, authen_type=ASCII, priv=0, method-list=default
AAA: Use authen method LOCAL (0x1f74208).
AAA: Authen CONT, need username.
AAA: Authen CONT, need password.
AAA: Authen ERROR (0x1f74208)! Use next method.
AAA: Authen FAIL(0x1f74208)! Method-list polling finish.
```

输出信息	解释
Authen start (0x1f74208), user=, authen_type=ASCII, priv=0, method-list=default	认证开始，用户名未知，使用ASCII类型认证，用户要求进入的特权级别为0，使用default认证方式列表。UserID = 0x1f74208
Use authen method LOCAL (0x1f74208)	使用本地认证方式，UserID = 0x1f74208
Authen CONT, need username	询问用户名
Authen CONT, need password	询问密码
Authen ERROR (0x1f74208)! Use next method	本地无法完成此次认证，使用方式列表中的下一个认证方式。
Authen FAIL(0x1f74208)! Method-list polling finish	已经轮询了所有的认证方式，此处认证失败

相关命令

无

1.1.7 enable password

如果希望对进入特权级别的用户进行认证，可以通过 **enable password** 命令配置相应特权级别的认证密码。使用该命令的 **no** 形式取消此密码。

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

no enable password [*level number*]

参数

参数	参数说明
----	------

<i>password</i>	密码字符串明文。
encryption-type	密码加密的类型。
encrypted-password	和 encryption-type 限定的加密类型相对应的密码的密文。
level	特权级别参数。
number	特权级别具体取值（1—15）。

缺省

没有密码。

命令模式

全局配置态

使用说明

交换机配置的密码中不能包括空格，即在使用 **enable password** 命令时，如果需要直接输入密码明文时，不能输入空格。密码明文的长度不能超过 126 个字符。

当没有输入 **level** 参数时，缺省认为是第 15 级。特权级别越大拥有的权限越大。若某个特权级别没有配置密码，则当用户进入此级别时将不进行认证。

目前我们交换机系统中所支持的 **encryption-type** 只有两种，在命令中的参数分别为 0 和 7，0 代表 0 表示不加密，后面的 **encrypted-password** 直接输入密码的明文，这种方法和不加 **encryption-type** 而直接输入 **password** 参数的方法效果相同；7 表示使用一种本公司自定义的算法来进行加密，后面的 **encrypted-password** 需要输入加密后的密码密文，这个密文可以从其他交换机的配置文件中拷贝出来。

示例

下面的示例增加特权级别 10 的密码为 **clever**，采用的 **encryption-type** 为 0，即密码明文方式：

```
enable password 0 clever level 10
```

下面的示例增加了缺省特权级别（15 级）的密码为 **Oscar**，采用的 **encryption-type** 为 7，即加密方法，需要输入密码密文：

```
enable password 7 074A05190326
```

假设 **Oscar** 的密文为 074A05190326，该密文的值是从其他交换机上的配置文件中获得的。

相关命令

aaa authentication enable default

service password-encryption**1.1.8 server**

使用这条命令在一个 AAA 服务器组中添加一个服务器，使用次命令的 **no** 形式删除一个服务器。

server A.B.C.D

no server A.B.C.D

参数

参数	参数说明
A.B.C.D	服务器的IP地址。

缺省

无服务器

命令模式

服务器组配置态

使用说明

一个服务器组中最多添加 20 个不同的服务器。

示例

上面的命令将地址为 12.1.1.1 的服务器添加到服务器组中。

server 12.1.1.1

相关命令

aaa group server

1.1.9 service password-encryption

要对系统中相关的密码进行加密，可使用这条命令，使用该命令的 **no** 形式可以取消对新配置密码的加密。

service password-encryption

no service password-encryption

参数

无

缺省

不对系统中相关的密码进行加密。

命令模式

全局配置态

使用说明

目前我们交换机系统的实现中，此命令与 `username password`、`enable password` 和 `password` 这三条命令相关。如果没有配置此命令（即缺省状态），且在上述三条命令中采用密码明文存储方式，则在 `show running-config` 命令中可以显示出已配置的密码的明文；而一旦配置了这条命令后，上述三条命令中配置的密码将被加密，无法在 `show running-config` 命令中显示出已配置的密码的明文，使用 `no service password-encryption` 命令也无法恢复密码的明文显示，所以在使用这条命令加密前请确认已经配置的密码。`no service password-encryption` 命令仅对使用此命令后配置的密码有效，对使用此命令前配置的已被加密的密码无效。

示例

```
switch_config#service password-encryption
```

使用此命令对已经配置的明文密码进行加密，且对使用此命令后的明文密码也进行加密。

相关命令

```
username username password
enable password
password
```

1.1.10 username

要在本地用户数据库中增加用户，用于本地方式的认证和授权，可使用此条命令。使用该命令的 `no` 形式可删除相应的用户

```
username username [password { password | [encryption-type] encrypted-password }]
[user-maxlinks number] [autocommand command]
```

```
no username username
```

参数

参数	参数说明
Username	用户名字符串。
password	用户对应的密码。
password	密码字符串明文。
encryption-type	密码加密的类型。
encrypted-password	和encryption-type限定的加密类型相对应的密码的密文。
user-maxlinks	同一用户可同时与交换机建立的链接数（只统计通过本地认证的用户）。
number	同时建立的链接数。
autocommand	当用户登录交换机后自动执行指定的命令。 autocommand 命令必须使用在命令行的最后。
command	自动执行命令字符串。

缺省

没有用户

命令模式

全局配置态

使用说明

当没有 **password** 参数时，认为密码为空字符串。**trust-host** 将用户与特定的主机捆绑在了一起，此用户从其他主机登录交换机将无法通过认证。**user-maxlinks** 限制了同一个用户名同时可以与交换机建立的会话数，但是当此用户的某个会话不是由本地认证方式（**local**）认证时将不被计算在内。可通过 **show users** 命令查看每个在线用户是通过了那一种方式的认证。

我们交换机配置的密码中不能包括空格，即在使用 **enable password** 命令时，如果需要直接输入密码明文时，不能输入空格。

目前我们交换机系统中所支持的 **encryption-type** 只有两种，在命令中的参数分别为 **0** 和 **7**，**0** 代表 **0** 表示不加密，后面的 **encrypted-password** 直接输入密码的明文，这种方法和不加 **encryption-type** 而直接输入 **password** 参数的方法效果相同；**7** 表示使用一种本公司自定义的算法来进行加密，后面的 **encrypted-password** 需要输入加密后的密码密文，这个密文可以从其他交换机的配置文件中拷贝出来。

示例

下面的示例增加本地用户，用户名为 **someone**，密码为 **someother**：

```
username someone password someother
```

下面的示例增加了本地用户，用户名为 **Oscar**，密码为 **Joan**，采用的 **encryption-type** 为 **7**，即加密方法，需要输入密码密文：

```
enable password 7 1105718265
```

假设 **Joan** 的密文为 **1105718265**，该密文的值是从其他交换机上的配置文件中获得的。

相关命令

aaa authentication login

第2章 RADIUS配置命令

本章介绍 RADIUS 的配置命令。RADIUS 是能够拒绝非授权网络访问的分布式客户/服务器系统。RADIUS 客户机运行在交换机上，并向包含所有用户认证和网络服务访问信息的中央 RADIUS 服务器发出认证、授权或记录请求。

有关如何配置 RADIUS 的信息及配置示例，请参见“配置 RADIUS”。

2.1 RADIUS配置命令

RADIUS 配置命令有：

- debug radius
- ip radius source-interface
- radius-server challenge-noecho
- radius-server deadtime
- radius-server host
- radius-server optional-passwords
- radius-server key
- radius-server retransmit
- radius-server timeout
- radius-server vsa send

2.1.1 debug radius

为了跟踪 RADIUS 事件或报文，可执行 debug radius 命令。使用此命令的 no 形式关掉 debug 信息。

debug radius {event | packet}

no debug radius {event | packet}

参数

参数	参数说明
event	跟踪RADIUS事件。
packet	跟踪RADIUS报文。

缺省

无

命令模式

管理态

使用说明

此命令可用于网络系统调试，查找用户认证失败的原因。

Switch#debug radius event

RADIUS:return message to aaa, Give me your username

RADIUS:return message to aaa, Give me your password

RADIUS:inital transmit access-request [4] to 192.168.20.126 1812 <length=70>

RADIUS:retransmit access-request [4] to 192.168.20.126 1812 <length=70>

RADIUS:retransmit access-request [4] to 192.168.20.126 1812 <length=70>

RADIUS:192.168.20.126 is dead to response [4]

RADIUS:Have tried all servers, return error to aaa

输出信息	解释
return message to aaa, Give me your username	需要得到用户名。
return message to aaa, Give me your password	需要得到用户名对应的密码。
inital transmit access-request [4] to 192.168.20.126 1812 <length=70>	首次向RADIUS服务器发送认证请求，服务器地址为192.168.20.126，端口号为1812，报文长度为70。
retransmit access-request [4] to 192.168.20.126 1812 <length=70>	服务器对请求没有及时作出反应，重发此认证请求。
192.168.20.126 is dead to response [4]	重发多次后，服务器仍未回应，将此服务器标志为已死亡。
Have tried all servers, return error to aaa	RADIUS无法完成此次认证，返回error。

示例

下列示例打开 RADIUS 的事件跟踪：

debug radius event

2.1.2 ip radius source-interface

为了强制 RADIUS 对所有发送的 RADIUS 报文使用指定接口的 IP 地址，使用 **ip radius source-interface** 全局配置命令。使用该命令的 **no** 形式恢复为缺省值。

ip radius source-interface *interface-name*

no ip radius source-interface

参数

参数	参数说明
<i>interface-name</i>	RADIUS对所有发送的RADIUS报文使用该接口的IP地址。

缺省

本命令没有厂家指定的缺省值，即根据实际情况来决定源发 IP 地址。

命令模式

全局配置态

使用说明

使用本命令选择某一个接口的 IP 地址，作为所有流出 RADIUS 包的源地址。只要接口处于 **up** 状态，就一直使用这个地址。这样，对每个网络访问客户机来说，RADIUS 服务器只使用一个 IP 地址，而不用维护一个 IP 地址列表。当交换机有许多接口且打算确保来自某个特定交换机的全部 RADIUS 包具有相同的 IP 地址时，本命令就特别有用了。

指定的接口必须拥有与之相联系的 IP 地址。如果指定的接口不拥有 IP 地址，或者处于 **down** 状态，那么，RADIUS 就恢复到缺省值。为了避免出现这种情况，请向接口添加 IP 地址并且保证接口处于 **up** 状态。

示例

下列示例让 RADIUS 对所有发送的 RADIUS 包使用接口 **vlan 1** 的 IP 地址：

```
ip radius source-interface vlan 1
```

相关命令

ip tacacs source-interface

2.1.3 radius-server challenge-noecho

为了使在 Access-Challenge 方式下用户数据不显示，需使用 **radius-server challenge-noecho** 命令。

radius-server challenge-noecho

no radius-server challenge-noecho

参数

无

缺省

在 Access-Challenge 方式下用户数据都显示。

命令模式

全局配置态

使用说明

无

示例

```
radius-server challenge-noecho
```

2.1.4 radius-server deadtime

当某些服务器不可用时，为了改善 RADIUS 的响应时间，使用 **radius-server deadtime** 全局配置命令，该命令让系统立即跳过不可用的服务器。使用本命令的 **no** 形式将 **dead-time** 设置为 0，即认为所有的服务器一直可用。

radius-server deadtime minutes

no radius-server deadtime

参数

参数	参数说明
minutes	RADIUS服务器被视为不可用的持续时间长度，最多为1440分钟（24小时）。

缺省

不可用时间设置为 0，即始终认为该服务器可用

命令模式

全局配置态

使用说明

使用本命令，把那些对认证请求不作出响应的 RADIUS 服务器标记为“死机”，这样就避免了在使用下一个服务器之前等待回应的时间过长。标记为死机的 RADIUS 服务器，被 *minutes* 这段持续时间内的所以请求跳过，除非所以的服务器均被标记为死机。

示例

下列示例对那些不对请求作出响应的 RADIUS 服务器指定了 5 分钟的“死机”时间：

```
radius-server deadtime 5
```

相关命令

radius-server host

radius-server retransmit

radius-server timeout

2.1.5 radius-server host

要指定 RADIUS 服务器的 IP 地址，使用 **radius-server host** 全局配置命令。使用本命令的 **no** 形式则删除指定的 RADIUS 主机。

radius-server host *ip-address* [*auth-port port-number1*] [*acct-port port-number2*]

no radius-server host *ip-address*

参数

参数	参数说明
<i>ip-address</i>	RADIUS服务器主机的IP地址。
<i>auth-port</i>	(可选项)为认证请求指定UDP目的端口。
<i>port-number1</i>	(可选项)认证请求的端口编号；若设置为0，则主机不用于认证。
<i>acct-port</i>	(可选项)为记录请求指定UDP目的端口。

<i>port-number2</i>	(可选)记录请求的端口编号；若设置为0，则主机不用于记录。
---------------------	-------------------------------

缺省

未指定任何 RADIUS 主机。

命令模式

全局配置态

使用说明

可以多次使用 **radius-server host** 命令以指定多个服务器，必要时会按照配置顺序进行轮询。

示例

下述示例指定 IP 地址为 1.1.1.1 的 RADIUS 主机，记录和认证都使用缺省端口：

```
radius-server host 1.1.1.1
```

下述示例在 IP 地址为 1.2.1.2 的 RADIUS 主机上，指定端口 12 作为认证请求的目的端口，端口 16 作为记录请求的目的端口：

```
radius-server host 1.2.1.2 auth-port 12 acct-port 16
```

相关命令

aaa authentication

radius-server key

tacacs server

username

2.1.6 radius-server optional-passwords

为了指定向 RADIUS 服务器第一次发送 RADIUS 认证申请时只对用户名进行验证而不检查密码，使用 **radius-server optional-passwords** 全局配置命令。使用本命令的 **no** 形式则恢复缺省值。

radius-server optional-passwords

no radius-server optional-passwords

参数

本命令没有参数或关键字

缺省

不使用 optional-password 方式

命令模式

全局配置态

使用说明

当用户输入登录名时，认证请求将包括用户名和零长度的密码。如果被接受，那么登录认证过程完成。如果 RADIUS 服务器拒绝这一请求，那么服务器就提示输入口令，当用户提供了口令后，将再次尝试进行验证。RADIUS 服务器必须支持对无口令的用户进行认证，以利用这一特色。

示例

下述示例配置发送第一个认证请求时不包括用户密码：

```
radius-server optional-passwords
```

相关命令

radius-server host

2.1.7 radius-server key

为了对交换机和 RADIUS 服务器之间的所有 RADIUS 通信设置加密密钥，请使用 radius-server key 全局配置命令。使用本命令的 no 形式则使密钥失效。

radius-server key *string*

no radius-server key

参数

参数	参数说明
<i>string</i>	用于加密的密钥，本密钥必须与RADIUS服务器使用的密钥相匹配。

缺省

密钥为空字符串。

命令模式

全局配置态。

使用说明

输入的密钥必须与 RADIUS 服务器使用的密钥相匹配。所有的起始空格字符被忽略，密钥中不能包含空格字符。

示例

下述示例将加密密钥设置为“firsttime”：

```
radius-server key firsttime
```

相关命令

radius-server host

tacacs server

username

2.1.8 radius-server retransmit

要指定在放弃使用某一台服务器之前应进行尝试的次数，使用 **radius-server retransmit** 全局配置命令。使用本命令的 **no** 形式恢复缺省值。

radius-server retransmit *retries*

no radius-server retransmit

参数

参数	参数说明
<i>retries</i>	重复尝试的最大次数，缺省值是尝试3次。

缺省

尝试 3 次

命令模式

全局配置态

使用说明

此命令一般与 **radius-server timeout** 命令配合使用，指明等待多长时间后认为服务器回应超时及超时后重试的次数。

示例

下述示例指定重试计数器的值为 5 次：

```
radius-server retransmit 5
```

相关命令

radius-server timeout

2.1.9 radius-server timeout

要对交换机等待服务器应答的时间上限进行设置，请使用 **radius-server timeout** 全局配置命令。使用本命令的 **no** 形式则恢复缺省值。

radius-server timeout seconds

no radius-server timeout

参数

参数	参数说明
<i>seconds</i>	指定超时时间（以秒为单位），缺省值是5秒。

缺省

5 秒

命令模式

全局配置态

使用说明

本命令常与 **radius-server retransmit** 配合使用。

示例

下述示例把超时定时器设置为 10 秒：

```
radius-server timeout 10
```

相关命令

无

2.1.10 radius-server vsa send

要把交换机配置为可识别和使用厂商专用属性（VSA），使用 `radius-server vsa send` 全局配置命令。使用本命令的 `no` 形式恢复缺省值。

```
radius-server vsa send [authentication]
```

```
no radius-server vsa send [authentication]
```

参数

参数	参数说明
authentication	(可选项)识别的厂商专用属性集只限于认证属性。

缺省

不使用 vsa。

命令模式

全局配置态

使用说明

IETF 使用厂商专用属性（属性 26），为在交换机和 RADIUS 服务器之间交换厂商专用信息指定了方法。VSA 允许厂商支持它们自己的不适合于普遍用途的扩展属性。`radius-server vsa send` 命令使交换机能够识别和使用认证或记录的厂商专用属性。在 `radius-server vsa send` 命令中使用 `accounting` 关键字，把识别的厂商专用属性集仅限于记录属性。在 `radius-server vsa send` 命令中使用 `authentication` 关键字，把识别的厂商专用属性集仅限于认证属性。

示例

下述示例对交换机进行配置，使之识别和使用厂商专用记录属性：

```
radius-server vsa send accounting
```

相关命令

radius-server host

第3章 Web认证命令

3.1 web认证配置命令

web 认证配置命令有：

- web-auth enable
- web-auth accounting
- web-auth authentication
- web-auth mode
- web-auth keep-alive
- web-auth holdtime
- web-auth authtime
- web-auth portal-server
- web-auth vlan-password
- web-auth kick-out
- show web-auth
- show web-auth interface
- show web-auth user
- debug web-auth event
- debug web-auth error
- debug web-auth verbose
- debug web-auth http event
- debug web-auth http request
- debug web-auth http
- debug web-auth

3.1.1 web-auth enable

命令描述

web-auth enable

no web-auth enable

参数

无

缺省

未开启 web 认证

说明

在路由接口上开启 web 认证功能，如果不开启 web 认证功能，通过该路由接口的报文不受 web 认证的控制。

命令模式

接口配置模式

示例

下面的命令在 interface vlan 5 上开启 web 认证：

```
Switch_config_v5#web-auth enable
```

3.1.2 web-auth accounting

命令描述

web-auth accounting *method-name*

no web-auth accounting

参数

参数	参数说明
<i>method- name</i>	在AAA中配置的认证方法列表。

缺省

无认证方法

说明

系统在用户登录后后将使用配置的计费方法进行计费，如果计费操作不成功，则通知用户认证失败。如果未配置计费方法，则按“default”方法处理。

命令模式

接口配置模式

示例

下面的命令先配置一个名为 **weba-acct** 的计费方法列表，然后在 **interface vlan 5** 上使用该方法：

```
Switch_config# aaa accounting network weba-acct start-stop radius
```

```
Switch_config_v5# web-auth account weba-acct
```

3.1.3 web-auth authentication

命令描述

web-auth authentication *method-name*

no web-auth authentication

参数

参数	参数说明
<i>method-name</i>	在aaa中配置的计费方法列表。取值范围：N/A。

缺省

无认证方法

说明

系统在用户登录后后将使用配置的认证方法进行认证，如果认证操作不成功，则通知用户认证失败。如果未配置认证方法，则按“default”方法处理。

命令模式

接口配置模式

示例

下面的命令先配置一个名为 **weba-auth** 的认证方法列表，然后在 **interface vlan 5** 上使用该方法：

```
Switch_config# aaa authentication login weba local
Switch_config_v5# web-auth authentication weba
```

3.1.4 web-auth mode

命令描述

web-auth mode [*user* | *vlan-id*]

no web-auth mode

参数

参数	参数说明
user	通过用户名、口令的方式认证用户。取值范围：N/A。
<i>vlan-id</i>	通过物理接口所属的vlan id来认证用户。取值范围：N/A。

缺省

使用用户名、口令的方式认证用户。

说明

用于设置认证用户的方式，使用用户名、口令的方式时需要用户在 **web** 界面上填写用户名、口令信息，使用 **vlan id** 时用户只需要在 **web** 界面上点击相应的登录按钮即可。

命令模式

接口配置模式

示例

下面的命令将 **vlan interface 5** 的认证方式配置为 **VLAN ID** 方式：

```
Switch_config_v5#web-auth mode vlan-id
```

3.1.5 web-auth keep-alive

命令描述

web-auth keep-alive *keep-alive-time*

no web-auth keep-alive

参数

参数	参数说明
<i>keep-alive-time</i>	用户浏览器向交换机发送在线通知的周期，以秒为单位。取值范围：60-65535。

缺省

60 秒

说明

在重新配置 **keep alive** 之后，已经通过认证的用户的浏览器将在按原来的的周期发送一次在线通知报文后启用新的发送周期；在配置 **keep alive** 之后才通过认证的用户的浏览器将立即以配置后的周期发送在线通知报文。

命令模式

管理配置模式

示例

下面的命令将用户浏览器向交换机发送在线通知的周期设为 180 秒：

```
Switch_config#web-auth keep-alive 180
```

3.1.6 web-auth holdtime

命令描述

web-auth holdtime *holdtime*

no web-auth holdtime

参数

参数	参数说明
holdtime	交换机检测用户是否在线的定时器时长。取值范围：60-65535。

缺省

180 秒

说明

交换机通过用户浏览器发送的在线通知报文来检测用户是否在线，如果超过 **holdtime** 的时长没有收到在线通知报文，交换机将认为该用户非正常下线，强制该用户登出，并停止对该用户的计费。

命令模式

管理配置模式

示例

下面的命令将 **holdtime** 设置为 600 秒。

```
Switch_config#web-auth holdtime 600
```

3.1.7 web-auth authtime

命令描述

web-auth authtime *authtime*

no web-authtime

参数

参数	参数说明
<i>authtime</i>	从用户分配到DHCP地址开始到通过认证(包括计费)的最长时间。取值范围：60-65535。

缺省

180 秒

说明

在用户使用 **dhcp** 协议后交换机将为其分配一定的资源以便于认证，如果用户在 **authtime** 之内没有通过认证，交换机将释放为其分配的资源。如果用户需要再次发起认证，则需要重新利用 **dhcp** 触发交换机为其分配认证资源。

命令模式

管理配置模式

示例

下面的命令将 **authtime** 设置为 360 秒：

```
Switch_config#web-auth authtime 360
```

3.1.8 web-auth portal-server

命令描述

web-auth portal-server A.B.C.D

no web-auth portal-server

参数

参数	参数说明
<i>A.B.C.D</i>	用户在通过认证前，使用域名进行web访问时，实际访问到的目的地址。取值范围：交换机某三层接口的IP地址。

缺省

无

说明

用户在通过认证前，进行 DNS 解析时，其 DNS 应答报文中的 **answer** 段的 IP 地址被修改为 **portal server** 的地址，这样用户的 **http** 请求就被重定向到 **portal server**，交换机内置的 **portal server** 根据当前的配置给用户返回相应的 **web** 页面。

命令模式

管理配置模式

示例

下面的命令将 portal server 的地址设置为 192.168.20.41。

```
Switch_config#web-auth portal-server 192.168.20.41
```

3.1.9 web-auth vlan-password

命令描述

web-auth vlan-password *password*

no web-auth vlan-password

参数

参数	参数说明
<i>password</i>	使用VLAN ID进行认证时的用户口令。取值范围：N/A。

缺省

无

说明

当使用 vlan id 的认证方式时，交换以“vlan*n*”作为用户名其中“*n*”为相应 vlan 的编号，并以本命令配置的口令作为所有以 vlan id 进行认证的用户的口令。

命令模式

管理配置模式

示例

下面的命令将 vlan-password 设置为“abc”。

```
Switch_config#web-auth vlan-password abc
```

3.1.10 web-auth kick-out

命令描述

web-auth kick-out *A.B.C.D*

参数

参数	参数说明
A.B.C.D	用户的IP地址。取值范围：N/A。

缺省

无

说明

此命令将给定 IP 的用户从交换机中删除，如果删除之前已经开始对用户计费，删除时交换机会停止对该用户的计费。删除后用户如果要再次通过认证，需要使用 **dhcp** 分配地址来重新触发认证过程。

命令模式

管理配置模式

示例

下面的命令删除 IP 地址为 192.168.20.43 的用户：

```
Switch_config#web-auth kick-out 192.168.20.43
```

3.1.11 show web-auth

命令描述

show web-auth

参数

无

缺省

无

说明

该命令用来显示交换机中当前的 **web** 认证配置。

命令模式

特权模式

示例

下面的命令显示交换机中当前的 web 认证配置：

```
Switch_config#show web-auth
web authentication parameters
holdtime          3600
authtime          600
keep-alive        60
portal-server     192.168.20.41
```

3.1.12 show web-auth interface

命令描述

show web-auth interface [vlan | superVlan *intf-id*]

参数

参数	参数说明
<i>intf-id</i>	路由接口编号。取值范围：N/A。

缺省

无

说明

该命令用来显示交换机中指定接口的 web 认证配置。

命令模式

特权模式

示例

下面的命令显示 interface vlan 1 下面的 web 认证配置：

```
Switch_config#show web-auth interface Vlan 1
web authentication parameters
```

web-auth	enable
account-method	weba-acct
authen-method	weba
mode	user

3.1.13 show web-auth user

命令描述

show web-auth user

参数

无

缺省

无

说明

该命令用来显示交换机中当前的所有用户，包括已经通过认证的用户和尚未完成认证的用户。

命令模式

特权模式

示例

下面的命令显示当前的用户：

```
Switch#show web-auth user
IP             MAC-ADDR      state          remain-time(seconds)
192.168.20.42  0008.74b7.3de1 WEBA_USER_AUTHENTICATED 3572
-----
authenticated users: 1, authenticating users: 0
```

3.1.14 debug web-auth event

命令描述

debug web-auth event

参数

无

缺省

无

说明

该命令用来输出 **web** 认证过程中的事件信息，比如收到认证请求、认证失败、通过认证、用户登出等事件。

命令模式

特权模式

示例

```
Switch#debug web-auth event
```

3.1.15 debug web-auth error

命令描述

debug web-auth error

参数

无

缺省

无

说明

该命令用来输出一切错误信息，用于错误的定位。

命令模式

特权模式

示例

```
Switch#debug web-auth error
```

3.1.16 debug web-auth verbose

命令描述

debug web-auth verbose

参数

无

缺省

无

说明

该命令使 **debug web-auth event** 命令输出的信息更加详细，使其在可能的情况下输出和事件相关的用户的 MAC 地址。

命令模式

特权模式

示例

```
Switch#debug web-auth verbose
```

3.1.17 debug web-auth http event

命令描述

debug web-auth http event

参数

无

缺省

无

说明

该命令用来输出 web 认证中和 http 相关的事件信息，比如收到 socket 连接请求，socket 断开等。

命令模式

特权模式

示例

```
Switch#debug web-auth http event
```

3.1.18 debug web-auth http request

命令描述

debug web-auth request

参数

无

缺省

无

说明

该命令用来输出 http 请求的内容。

命令模式

特权模式

示例

```
Switch#debug web-auth http request
```

3.1.19 debug web-auth http

命令描述

debug web-auth http

参数

无

缺省

无

说明

该命令相当于同时执行了 `debug web-auth http event` 和 `debug web-auth request`。

命令模式

特权模式

示例

```
Switch#debug web-auth http
```

3.1.20 debug web-auth

命令描述

debug web-auth

参数

无

缺省

无

说明

该命令相当于同时打开 **web** 认证的所有调试开关。

命令模式

特权模式

示例

```
Switch#debug web-auth
```