安全配置命令

目 录

第 1 章　AAA 配置命令

本章描述了 AAA 的配置命令。AAA 配置命令分为认证、授权、记账、本地账号策略配置命令。下面各节加以阐述。

1.1　认证配置命令

本节描述了用来配置认证方法的命令。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来配置认证的信息，请查阅“配置认证”。如果想查阅使用本节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。

认证配置命令有：

- aaa authentication banner
- aaa authentication fail-message
- aaa authentication username-prompt
- aaa authentication password-prompt
- aaa authentication dot1x
- aaa authentication enable default
- aaa authentication login
- aaa group server
- server
- debug aaa authentication
- enable password
- enable(enter)
- service password-encryption

1.1.1　aaa authentication banner

要配置在用户登陆时显示的个性化风格的标语，可以使用全局配置命令 aaa authentication banner。使用该命令的 no 形式删除标语。

aaa authentication banner *delimiter string delimiter*

no aaa authentication banner

参数

参数	参数说明
delimiter string delimiter	在将要用户登陆时显示的文本*string*，*delimiter*为定界符，定界符采用双引号

缺省

没有用户定义的登陆标语时，默认标语为：

User Access Verification

命令模式

全局配置态

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。

示例

下面的示例将登陆时标语提示修改为所示字符串：

aaa authentication banner “Welcome to system!”

相关命令

aaa authentication fail-message

1.1.2 aaa authentication fail-message

要配置在用户登陆失败时显示的个性化风格的标语，可以使用全局配置命令 aaa authentication fail-message。使用该命令的 no 形式删除登陆失败标语。

aaa authentication fail-message *delimiter string delimiter*

no aaa authentication fail-message

参数

参数	参数说明
delimiter string delimiter	向用户登陆失败时将要显示的文本*string*，*delimiter*为定界符，

	定界符采用双引号

缺省

没有用户定义的登陆失败标语时，默认的标语为：

Authentication failed!

命令模式

全局配置态

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。

示例

下面的示例将用户名提示修改为所示字符串：

aaa authentication fail-message “See you later”

相关命令

aaa authentication banner

1.1.3 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

参数

参数	参数说明
text-string	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+或 RADIUS 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 “YourUsernam:”

相关命令

aaa authentication password-prompt

1.1.4 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

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

1.1.5 aaa authentication dot1x

dot1x 接入认证，设置 dot1x 接入认证使用全局配置命令 aaa authentication dot1x。使用本命令的 no 形式关闭 dot1x 认证。

aaa authentication dot1x {**default** | *list-name*} *method1* [*method2...*]

no aaa authentication dot1x {**default** | *list-name*}

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接入认证时缺省的方法列表。
list-name	用来命名认证方法列表的字符串，用户接入认证时将激活认证方法列表中所列的方法。
method	至少为“dot1x认证方法”描述的关键字之一。

缺省

没有设置认证方法，则进行认证时返回失败。

命令模式

全局配置态

使用说明

使用 aaa authentication dot1x 命令创建的缺省列表或其他命名列表将由 dot1x 应用来引用， 用来对接入的 dot1x 用户进行认证。

只有前面的方法不能准确的获得成功或者失败的结果时，才使用下一个认证方法，如果前面的认证方法返回失败，则不使用其它的认证方法。

dot1x 认证方法

关键字	描述
group name	使用服务器组进行认证。
group radius	使用RADIUS进行认证。
group tacacs+	使用TACACS+进行认证。
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。

示例

下面的示例创建一张名为“TEST”的认证方法列表。这个认证首先尝试与 TACACS+服务器联系。如果不能从 TACACS+服务器组准确的获得成功或者失败的结果（没有发现 TACACS+服务器或服务器返回 dead 错误），则尝试下一个方法 local，当 local 方法也不能准确的获得成功或者失败的结果，则允许用户不经认证就可以访问网络。（目前我们设备的 aaa 系统 enable(line)、local 类型的认证方法都能准确的获得一个成功或者失败的结果。所以下列命令不会进行到 none 方法）

aaa authentication dot1x TEST group tacacs+ local 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 dot1x 认证均使用这个列表：

aaa authentication dot1x default group tacacs+ local none

相关命令

无

1.1.6 aaa authentication enable default

enable 特权认证，以确定某个用户是否可以访问特权级别的命令，使用全局配置命令 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

参数

参数	参数说明
method	至少为“enable认证方法”中所给出的关键字之一。

缺省

没设置认证方法，如果是 console 口用户则该认证过程返回成功，否则为失败。

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不能准确的得到成功或失败的结果时，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。

enable 认证方法

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

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。如果不能从 TACACS+服务器组准确的获得成功或者失败的结果（没有发现 TACACS+服务器或服务器返回 dead 错误），则尝试下一个方法 eanble，当 enable 方法也不能准确的获得成功或者失败的结果，则允许用户不经认证就可以访问服务器。（目前我们设备的 aaa 系统 enable(line)、local 类型的认证方法都能准确的获得一个成功或者失败的结果。所以下列命令不会进行到 none 方法）。

aaa authentication enable default group tacacs+ enable none

相关命令

enable password

1.1.7 aaa authentication login

登录认证，使用全局配置命令 aaa authentication login。使用本命令的 no 形式关闭认证。

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

no aaa authentication login {**default** | *list-name*}

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登陆认证时缺省的方法列表。
list-name	用来命名认证方法列表的字符串，用户登陆认证时将激活认证方法列表中所列的方法。
method	至少为“login认证方法”中描述的关键字之一。

缺省

没有设置认证方法，如果是 console 口用户则该认证过程返回成功，否则为失败。

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相关应用（如 vty）的相关命令作用于某一具体线路。

只有在前面的认证方法不能准确的得到成功或失败的结果时，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不能准确的得到成功或失败的结果时，可将 none 指定为该命令行的最后方法。

login 认证方法

关键字	描述
enable	使用enable口令进行认证。
group name	使用服务器组进行认证。
group radius	使用RADIUS进行认证。
group tacacs+	使用TACACS+进行认证。
line	使用line密码进行认证。
local	使用本地用户名数据库进行认证。
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	不进行认证。

示例

下面的示例创建一张名为“TEST”的认证方法列表。这个认证首先尝试与 TACACS+服务器联系。如果不能从 TACACS+服务器组准确的获得成功或者失败的结果（没有发现 TACACS+服务器或服务器返回 dead 错误），则尝试下一个方法 radius，当 radius 方法也不能准确的获得成功或者失败的结果，则允许用户不经认证就可以登陆。

aaa authentication login TEST group tacacs+ group radius 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 group tacacs+ group radius none

相关命令

无

1.1.8 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 | tacacs+} *group-name*

no aaa group server {radius | tacacs+} *group-name*

参数

参数	参数说明
group-name	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。最大可设 63 个服务器组。

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

1.1.9 server

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

在一个 radius 服务器组中添加一个服务器：

server {A.B.C.D | X:X:X:X::X} [**key** {*password* | {*encryption-type encrypted-password*}}] [**auth-port** *num*] [**acct-port** *num*] [**retransmit** *value*] [**timeout** *value*] [**privilege** *pri*]

在一个 tacacs+服务器组中添加一个服务器：

server {A.B.C.D | X:X:X:X::X} [**key** {*password* | {*encryption-type encrypted-password*}}]

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。
X:X:X:X::X	服务器的IPv6地址
key	密钥

password	密钥字符串
encryption-type	加密类型， 0表示不加密，7表示加密
encrypted-password	加密类型对应的密钥字符串
auth-port	认证目的端口
acct-port	记账目的端口
num	端口号
retransmit *value*	重传次数，默认2次
timeout *value*	超时重传的超时时间， 默认3秒
privilege *pri*	服务器优先级， 默认0

缺省

无服务器

命令模式

服务器组配置态

使用说明

最大可设63个服务器组，外加radius和tacacs+服务器链表各一个，所有radius服务器组及服务器链表中的服务器相加的总数最大值为64，所有tacacs+服务器组及服务器链表中的服务器相加的总数最大值也为64。

示例

下面的命令将地址为 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

1.1.10 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

无

相关命令

无

1.1.11 enable password

如果希望使用 enable 方法进行认证，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
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。
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

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 127 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 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

1.1.12 enable(enter)

在用户登录进入系统以后，要想进入特权方式（即管理态#），可使用命令 enable(enter)。

enable(enter) <*1-15*>

参数

参数	参数说明
<1-15>	想要获得的特权优先级

缺省

不进入特权方式

命令模式

用户态

使用说明

无

示例

>enable(默认下用户为 15 级)

Password: (输入密码进行认证)

#

#exi

>enable 1(想要获得特权优先级为 1)

Password:(输入密码进行认证)

#

相关命令

aaa authentication enable default

enable password

1.1.13 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 aaa 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（vty 下的配置命令，可用于 line 认证）

1.2 授权配置命令

本节描述了用来配置授权方法的命令。授权可以限制对某个用户的有效服务，当授权有效时，系统使用从用户属性文档（profile）中检索出的信息配置该用户的会话，用户的属性文档位于本地用户数据库或者位于安全服务器上。完成这件工作后，就允许该用户访问所要求的服务，只要包含在用户属性文档中的信息允许提供这项服务。

如果想得到关于怎样配置授权的信息，请查阅“配置授权”。如果想查阅使用本章中命令进行配置的例子，阅读“配置授权”文档最后的示例部分。

授权配置命令有：

- aaa authorization
- debug aaa authorization

1.2.1 aaa authorization

使用全局配置命令 aaa authorization 设置参数来限制用户的网络访问权限。使用该命令的 no 形式关闭某个功能的授权。

aaa authorization {{commands *<0-15>***} | network** | **exec}** {**default** | *list-name*} *method1* [*method2...*]

no aaa authorization {{commands *<0-15>***} | network** | **exec }** {**default** | *list-name*}

参数

参数	参数说明
commands	EXEC（shell）命令授权
<0-15>	要授权的命令的优先级
network	网络类型服务的授权，如：PPP、SLIP
exec	适用于与用户EXEC终端对话相关的属性，决定用户注册时是否允许启动EXEC外壳程序，或者授予用户进入EXEC shell时的特权级别。
default	缺省授权方法列表。
list-name	用来命名授权方法列表的字符串。
method	至少为“授权方法”中描述的关键字之一。

缺省

用户要求进行授权，但没有在相应的线路或接口上指定要求使用的授权方法列表，则会使用缺省方法列表。如果没有定义缺省方法列表，则不发生授权行为。

命令模式

全局配置态

使用说明

使用 aaa authorization 命令开启授权，创建授权方法列表，定义在用户访问指定功能时可使用的授权方法。授权方法列表定义了授权执行的方式以及执行这些授权方法的次序。方法列表只是一张简单的命名列表，它描述要顺序查询的授权方法（如 RADIUS 或 TACACS+）。方法列表可以指定一个或多个用来授权的安全协议，因此，它能够确保万一前面所列的授权方法不能用时有一个备用的方法。 一般情况下，先使用所列的第一个方法试图授予用户访问指定网络服务的权限；如果该方法没有响应，再选择方法列表中

所列的下一个方法。这个过程继续进行下去，直到使用的某个授权方法成功地返回授权结果，或者用完了所定义的所有方法。

授权方法

关键字	描述
group name	使用服务器组进行授权。
group radius	使用RADIUS进行授权。
group tacacs+	使用TACACS+进行授权。
if-authenticated	如果认证通过则授权成功。
local	使用本地用户名数据库进行授权。
none	不进行授权。

一旦定义了授权方法列表后，在所定义的方法被执行之前，该方法列表必须应用到指定的线路或接口上。作为授权过程的一部分，授权命令向 RADIUS 或 TACACS＋服务器程序发送包括一系列 AV 对的请求包。服务器可能执行下述动作之一：

- 完全接受请求。
- 接受请求，并增加属性限制用户服务权限。
- 拒绝请求，授权失败。

示例

下述示例定义名为 have_a_try 的 exec 授权方法列表，该方法列表指定在 vty 线路上使用 RADIUS 授权方法。如果 RADIUS 服务器没有响应，则执行本地授权。

aaa authorization exec have_a_try radius local

相关命令

aaa authentication

aaa accounting

1.2.2 debug aaa authorization

如果希望对用户的授权过程进行跟踪，可使用 debug aaa authorization 命令。使用此命令的 no 形式关掉 debug 信息。

debug aaa authorization

no debug aaa authorization

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授权过程，以发现授权失败的原因。

示例

无

相关命令

无

1.3 记账配置命令

本节描述了用来配置记账方法的命令。记账功能可以跟踪用户访问的服务，同时可以跟踪他们消耗的网络资源数量。当激活记账功能时，系统以记账记录的形式向 TACACS+ 或 RADIUS 安全服务器（依赖于所实现的安全方法）报告用户的活动。每条记账记录包括记账属性值（AV）对，并存储在访问控制服务器上。然后这些数据可用于网络管理、客户账单和/或审计等分析。

授权配置命令有：

- aaa accounting
- aaa accounting update
- aaa accounting suppress null-username
- debug aaa accounting

1.3.1 aaa accounting

当使用 RADIUS 或 TACACS+时，基于记账或安全的目的要对所要求的服务开放 AAA 记账，可以使用全局配置命令 aaa accounting。使用该命令的 no 形式关闭记账：

aaa accounting {{**commands** *<0-15>*} **| network** | **exec** | **connection**} {**default** | *list-name*} {{{**start-stop** | **stop-only**} **group** {*groupname* | **radius | tacacs+**}} | **none** }

no aaa accounting { **network** | **exec** | **connection**} {**default** | *list-name*}

参数

参数	参数说明
commands	给某一优先级的命令提供记账。
<0-15>	命令的优先级别。
network	给所有PPP会话提供记账记录信息，包括包、字节及时间计数。
exec	提供有关用户EXEC终端会话的信息。
connection	提供发出的所有出站连接的信息，目前只支持H323会话信息。
default	缺省记账方法列表。
list-name	用来命名记账方法列表的字符串。
start-stop	开始和结束时记账
stop-only	结束时记账
none	不记账
group *groupname*	使用服务器组进行记账
group radius	使用RADIUS进行记账
group tacacs+	使用TACACS+进行记账

缺省

用户要求进行记账，但没有在相应的线路或接口上指定要求使用的记账方法列表，则会使用缺省方法列表。如果没有定义缺省方法列表，则不发生记账行为。

命令模式

全局配置态

使用说明

使用 aaa accounting 命令开启记账，创建记账方法列表，定义在用户发送记账记录时可使用的记账方法。记账方法列表定义了记账执行的方式以及执行这些记账方法的次序。方法列表只是一张简单的命名列表，它描述要顺序查询的记账方法（RADIUS 或

TACACS+）。方法列表可以指定一个或多个用来记账的安全协议，因此，它能够确保万一前面所列的记账方法失败后有一个备用的方法。

相关命令

aaa authentication

aaa accounting

1.3.2 aaa accounting update

如果需要向记账服务器周期性的发送临时的记账记录，可以使用全局配置命令 aaa accounting update。使用该命令的 no 形式关闭临时记账记录：

aaa accounting update { **newinfo** | **periodic** *number*}

no aaa accounting update { **newinfo** | **periodic**}

参数

参数	参数说明
update	激活发送临时记账记录（需要端用户支持，目前不支持）
newinfo	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
periodic	周期性地发送临时记账记录，该周期由数字参数定义
number	发送临时记账记录的周期数字参数

缺省

不发生临时记账行为。

命令模式

全局配置态

使用说明

该功能需要应用端的支持，目前不支持。

相关命令

aaa accounting

1.3.3 aaa accounting suppress null-username

如果需要阻止为没有用户名的会话产生记账记录，可以使用全局配置命令如下。使用该命令的 no 形式关闭：

aaa accounting suppress null-username

no aaa accounting suppress null-username

参数

无

缺省

不阻止为没有用户名的会话产生记账记录。

命令模式

全局配置态

使用说明

无。

相关命令

aaa accounting

1.3.4 debug aaa accounting

如果希望对用户的记账过程进行跟踪，可使用 debug aaa accounting 命令。使用此命令的 no 形式关掉 debug 信息。

debug aaa accounting

no debug aaa accounting

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记账过程，以发现记账失败的原因。

示例

无

相关命令

无

1.4 本地账号策略配置命令

本节介绍本地账号策略的配置命令。本地账号策略用来进行本地认证和本地授权。

如果想得到关于怎样来配置本地账号策略的信息，请查阅“配置本地账号策略”。如果想查阅使用本节中命令进行配置的例子，阅读“配置本地账号策略”文档最后的示例部分。

本地账号策略配置的命令有：

- localauthen
- localauthor
- localpass
- localgroup
- local authen-group
- local author-group
- local pass-group
- local user
- username

1.4.1 localauthen

要配置本地认证策略，使用全局配置命令 localauthen 。使用该命令的 no 形式删除：

localauthen *WORD*

no localauthen *WORD*

参数

参数	参数说明
WORD	本地认证策略名称

缺省

没配置

命令模式

全局配置态

使用说明

使用 localauthen WORD 进入本地认证策略的配置层次，此配置层次下使用以下命令配置本地认证策略：

- 一定时间内的最大登陆尝试次数

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

参数	参数说明
max-tries	最大登陆尝试次数
<1-9>	最大登陆尝试次数范围为1-9次
try-duration	持续时间
1d2h3m4s	表示天、小时、分、秒的时间格式

相关命令

login max-tries

localgroup

local authen-group

username

1.4.2 localauthor

要配置本地授权策略，使用全局配置命令 localauthor 。使用该命令的 no 形式删除：

localauthor *WORD*

no localauthor *WORD*

参数

参数	参数说明
WORD	本地授权策略名称

缺省

没配置

命令模式

全局配置态

使用说明

使用 localauthor WORD 进入本地授权策略的配置层次，此配置层次下使用以下命令配置本地授权策略：

- 对登录进来的用户进行优先级授权

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

参数	参数说明
default	默认优先级（当没对具体的登陆方式设置时，采用该优先级进行授权）
console	Console口登陆用户的授权优先级
ssh	ssh登陆用户的授权优先级
telnet	telnet登陆用户的授权优先级
<1-15>	优先级

相关命令

exec privilege

localgroup

local author-group

username

1.4.3 localpass

要配置本地密码策略，使用全局配置命令 localpass 。使用该命令的 no 形式删除：

localpass *WORD*

no localpass *WORD*

参数

参数	参数说明
WORD	本地密码策略名称

缺省

没配置

命令模式

全局配置态

使用说明

使用 localpass WORD 进入本地密码策略的配置层次，此配置层次下使用以下命令配置本地密码策略：

- 密码和用户名不同

  non-user

- 历史口令检查（和历史口令不同，当修改用户口令时）

  non-history

- 指定口令组成成分

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

参数	参数说明
number	必须包含数字
lower-letter	必须包含小写字母
upper-letter	必须包含大写字母

special-character	必须包含特殊字符

- 口令最小长度

  min-length *<1-127>*

参数	参数说明
<1-127>	最小长度（范围为1-127）

- 口令有效期

  validity *1d2h3m4s*

参数	参数说明
1d2h3m4s	表示天、小时、分、秒的时间格式

相关命令

non-use

non-history

element

min-length

validity

localgroup

local pass-group

username

1.4.4 localgroup

要配置本地策略组，使用全局配置命令 localgroup ，全局配置态下为默认本地策略组。使用该命令的 no 形式删除：

localgroup *WORD*

no localgroup *WORD*

参数

参数	参数说明
WORD	本地策略组名称

缺省

没配置

命令模式

全局配置态

使用说明

使用 localgroup WORD 进入本地策略组的配置层次，此配置层次下使用以下命令配置本地策略组：

- 本地认证配置

  local authen-group

- 本地授权配置

  local author-group

- 本地密码配置

  local pass-group

- 本地账号配置

  local user

- 配置账号

  username

相关命令

local authen-group

local author-group

local pass-group

local user

username

localgroup

local author-group

1.4.5 local authen-group

在本地策略组下应用已配置的本地认证策略，使用命令 local authen-group ，全局配置态下被认为是默认本地策略组。使用该命令的 no 形式删除：

local authen-group *WORD*

no local authen-group

参数

参数	参数说明
WORD	本地认证策略名称

缺省

没配置

命令模式

全局配置状态、本地策略组配置态

使用说明

无

相关命令

localauthen

localgroup

local authen-group

1.4.6 local author-group

在本地策略组下应用已配置的本地授权策略，使用命令 local author-group ，全局配置态下被认为是默认本地策略组。使用该命令的 no 形式删除：

local author-group *WORD*

no local author-group

参数

参数	参数说明
WORD	本地授权策略名称

缺省

没配置

命令模式

全局配置状态、本地策略组配置态

使用说明

无

相关命令

localauthor

localgroup

local author-group

1.4.7 local pass-group

在本地策略组下应用已配置的本地密码策略，使用命令 local pass-group ，全局配置态下被认为是默认本地策略组。使用该命令的 no 形式删除：

local pass-group *WORD*

no local pass-group

参数

参数	参数说明
WORD	本地密码策略名称

缺省

没配置

命令模式

全局配置状态、本地策略组配置态

使用说明

无

相关命令

localpass

localgroup

local pass-group

1.4.8 local user

在本地策略组下配置的账号的最大连接数和冻结用户，使用命令 local user ，全局配置态下被认为是默认本地策略组。使用该命令的 no 形式删除配置或者取消配置：

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

no local user {maxlinks | { **freeze** *WORD* }**}**

参数

参数	参数说明
maxlinks	限制使用同一用户名同时登录的用户个数
<1-255>	个数（范围为1-255）
freeze	冻结用户
WORD	用户名

缺省

没配置

命令模式

全局配置状态、本地策略组配置态

使用说明

无

相关命令

localgroup

1.4.9 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。该命令用在本地策略组配置态下，全局配置态被认为是默认本地策略组。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*}] [**maxlinks** *number*] [**authen-group** *WORD*] [**author-group** *WORD*] [**pass-group** *WORD*] [**autocommand** *command*] [**bind-ip** *A.B.C.D*] [**bind-mac** *H:H:H:H:H:H*] [**bind-pool** *WORD*] [**bind-port** *port*][**callback-dialstring** *string*] [**callback-line** *line*] [**callback-rotary** *rotary*] [**nocallback-verify**] [**nohangup**] [**noescape**]

no username *username*

参数

参数	参数说明
username	用户名字符串；
password	用户密码
password	密码字符串明文；
encryption-type	密码加密的类型；
encrypted-password	限定的加密类型相对应的密码的密文
maxlinks	该账号可建立的链接数（使用此用户名可同时登录的用户个数）。
number	链接数
authen-group	*指定本地认证策略*
WORD	本地认证策略名
author-group	*指定本地授权策略*
WORD	本地授权策略名
pass-group	*指定本地密码策略*
WORD	本地密码策略名
autocommand	当用户登录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。
以下选项交换机不支持	
bind-ip	*绑定用户ip地址(不支持)*
A.B.C.D	IP地址
bind-mac	*绑定用户mac地址(不支持)*
H:H:H:H:H:H	*ARP记录的48比特硬件地址*
bind-pool	*绑定用户地址池(不支持)*
WORD	地址池名
bind-port	*绑定用户端口(不支持)*
port	端口
callback-dialstring	回拨电话号码(不支持)；
string	电话号码字符串；
callback-line	回拨时使用的线路（不支持）；
line	线路号
callback-rotary	回拨rotary配置（不支持）；
rotary	rotary号码；
nocallback-verify：	回拨不认证（不支持）
nohangup	用户登陆并执行自动命令完后不断开连接（不支持）。
noescape	禁止用户登陆后使用转义字符（不支持）。

缺省

没有用户。

命令模式

全局配置态、本地策略组配置态

使用说明

当没有 password 参数时，认为密码为空字符串。

user-maxlinks 限制了同一个账号同时可以建立的会话数，但是当此账号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 aaa users 命令查看每个在线用户的基本信息。

我们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 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，这个密文可以从本公司的设备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路由器上的配置文件中获得的。

相关命令

aaa authentication login

1.4.10 show local-users

要显示所有本地 AAA 账号的概要信息，可使用 show local-users 命令。

show local-users

参数

无

缺省

无

命令模式

管理态

使用说明

使用此命令可显示所有的 AAA 账号，包括以下信息：所属策略组（Local group default:）、使用连接数（links）、 密码存在时间（pw_present）、密码匹配失败次数（login_tries）、密码匹配失败已过时间（login_try_time）、冻结原因（freezing_cause）。

示例

#show local-users

Local group default:

username	links	pw_present	login_tries	login_try_time	freezing_cause
admin	1	0s	0	0s	
aaa	0	0s	0	0s	

域	解释
Local group default:	账号所属的本地策略组
links	该账号正在使用的连接数（即多少个用户正在使用）
pw_present	密码存在时间（配置了密码有效期）
login_tries	密码匹配失败次数（设置了最大登录尝试次数，0表示没设）
login_try_time	密码匹配失败已过时间（设置了最大登录尝试次数，0表示没设）
freezing_cause	账号被冻结的原因

相关命令

username

1.4.11 show aaa users

要显示所有在线 AAA 用户的概要信息，可使用 show aaa users 命令。

show aaa users

参数

无

缺省

无

命令模式

管理态

使用说明

使用此命令可显示所有的在线用户，包括以下信息：接口（port）、用户名(username)、服务类型(service)、在线持续时间(time)以及 IP 地址(peer_address)。

示例

#show aaa users

Port	User	Service	Duration	Peer Address
console 0	zjl	exec	04:14:03	unknown
vty 0	aaa	exec	00:12:24	172.16.20.120

域	解释
Port	用户所处的接口ID或Vty的索引号。
User	用户名字符串。
Service	用户请求的服务。
Duration	用户在线的持续统计时间。
Peer Address	用户所处的远端主机IP地址。

相关命令

username

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 key
- radius-server optional-passwords
- 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。

示例

下列示例打开 RADIUS 的事件跟踪：

```
debug radius event
```

2.1.2 ip radius source-interface

对所有发送的 RADIUS 报文指定发送端口，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
interface-name	RADIUS报文发送端口。

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发送端口。

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，作为所有流出 RADIUS 包的源端口。只要接口处于 up 状态，就一直使用这个端口。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 attribute

在 radius 认证和计费过程中，是否指定传输某些属性使用全局配置命令 radius-server attribute。使用本命令的 no 形式关闭 AAA 认证。

radius-server attribute {**4 | 32 | 95**}

no radius-server attribute {**4 | 32 | 95**}

参数

参数	参数说明
4	将跟随在该参数后面的地址作为属性4（NAS ip address）的值在radius处理过程中传输
32	根据跟随在该参数后面的指令指定在radius认证或记费请求中传输属性attribute32（NAS identifier）
95	将跟随在该参数后面的地址作为属性95（NAS ipv6 address）的值在radius处理过程中传输。

缺省

无

命令模式

全局配置态

使用说明

使用 radius-server attribute 命令配置并指定在 radius 处理过程中传输某种特定的属性。

radius-server attribute 4 配置 radius 属性 4（NAS 的 IP 地址）并指定在 RADIUS 报文中传输。

radius-server attribute 32 指定在 RADIUS 认证或计费请求报文中传输 radius 属性 32（NAS 的 ID）或配置该属性。

radius-server attribute 95 配置 radius 属性 95（NAS 的 IPV6 地址）并指定在 RADIUS 报文中传输。

示例

radius-server attribute 4 X.X.X.X 在 RADIUS 报文中传输 radius 属性 4，并用 X.X.X.X 作为属性值

radius-server attribute 32 in-access-req 在认证请求中传输 NAS identifier

radius-server attribute 32 in-account-req 在计费请求中传输 NAS identifier

radius-server attribute 32 *identifier* 配置 NAS identifier

radius-server attribute 95 X:X:X:X::X 在 RADIUS 报文中传输 radius 属性 95，并用 X:X:X:X::X 作为属性值

相关命令

无

2.1.4 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

2.1.5 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有请求跳过，除非所有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

2.1.6 radius-server directed-resquest

允许用户以'@server'格式来指定 RADIUS 服务器，使用 radius-server directed-resquest 全局配置命令，使用本命令的 no 形式来关闭该配置。

radius-server directed-resquest [restricted]

no radius-server directed-resquest [restricted]

参数

参数	参数说明
restricted	表示只限定用户使用以'@server'格式来指定RADIUS服务器

缺省

不支持使用'@server'格式来指定 RADIUS 服务器

命令模式

全局配置态

使用说明

无

示例

radius-server directed-resquest

相关命令

无

2.1.7 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*|*ipv6-address* [*auth-port port-number1*] [acct-port *port-number2*]

no radius-server host ip-address|*ipv6-address*

参数

参数	参数说明
ip-address	RADIUS服务器主机的IP地址。
ipv6-address	RADIUS服务器主机的IPv6地址。
auth-port	(可选项)为认证请求指定UDP目的端口。
port-number1	(可选项)认证请求的端口编号。
acct-port	(可选项)为记录请求指定UDP目的端口。
port-number2	(可选项)记录请求的端口编号。

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

2.1.8 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* | {encryption-type encrypted-password}

no radius-server key

参数

参数	参数说明
string	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。
encryption-type	密钥加密类型，0表示不加密，7表示加密
encrypted-password	encryption-type类型对应的加密密钥字符串

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“firstime”：

```
radius-server key firstime
```

相关命令

radius-server host

tacacs server

username

2.1.9 radius-server optional-passwords

为了指定向 RADIUS 服务器第一次发送 RADIUS 认证请求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

2.1.10 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
retries	重复尝试的最大次数，缺省值是尝试2次。

缺省

尝试 2 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

下述示例指定重试记数器的值为 5 次：

radius-server retransmit 5

相关命令

radius-server timeout

2.1.11 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
seconds	指定超时时间（以秒为单位），缺省值是3秒。

缺省

3 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

2.1.12 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 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认证属性：

radius-server vsa send authentication

相关命令

radius-server host

第 3 章　TACACS+配置命令

本章介绍 TACACS+的配置命令。TACACS+可以完成对用户身份的认证；对用户服务权限的授权以及对用户服务执行过程的记录。

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

3.1　TACACS+配置命令

TACACS+配置命令有：

- debug tacacs
- ip tacacs source-interface
- tacacs-server host
- tacacs-server key
- tacacs-server timeout
- server

3.1.1　debug tacacs

当希望跟踪 TACACS+协议事件或查看收发的报文时，可使用 debug tacacs 命令。使用此命令的 no 形式取消跟踪。

debug tacacs {**event** | **packet**}

no debug tacacs {**event** | **packet**}

参数

参数	参数说明
event	跟踪TACACS+事件。
packet	跟踪TACACS+报文。

缺省

关闭 debug 信息。

命令模式

管理态

使用说明

此命令一般只在网络调试时使用，用于查找用户 AAA 服务失败的原因。

示例

下述示例将打开 TACACS+的事件跟踪：

debug tacacs event

相关命令

无

3.1.2 ip tacacs source-interface

要对所有 TACACS＋报文使用指定接口，使用全局配置命令 ip tacacs source-interface。使用本命令的 no 形式取消对此源接口的使用。

ip tacacs source-interface *subinterface-name*

no ip tacacs source-interface

参数

参数	参数说明
subinterface-name	所有TACACS＋报文的源接口名称。

缺省

本命令没有指定的缺省值。

命令模式

全局配置态

使用说明

使用本命令可以为所有的 TACACS＋报文指定源接口，只要该接口处于 up 状态，所有的 TACACS+报文将使用这个接口的 IP 地址作为源发地址。这样，将保证每一台设备的 TACACS+报文具有相同的源发 IP 地址，TACACS＋服务器就不再需要维护包含所有 IP

地址的地址列表。也就是说，当设备有许多接口，但为了确保来自于特定设备的所有TACACS＋报文具有相同的源 IP 地址时，本命令将发挥作用。

指定的接口必须有与之相联系的 IP 地址。如果指定的接口没有 IP 地址或处于 down 状态，就会回到缺省值，也就是根据实际情况来确定源 IP 地址。为了避免发生这样的情况，一定要为该接口添加 IP 地址并保证该接口处于 up 状态。

示例

下述示例将使用接口 vlan1 的 IP 地址作为所有 TACACS+报文的源发 IP 地址：

```
ip tacacs source-interface vlan1
```

相关命令

ip radius source-interface

3.1.3 tacacs-server host

为了指定 TACACS＋服务器，使用全局配置命令 tacacs-server host。使用本命令的 no 形式则删除指定的服务器。

tacacs-server host *ip-address* [**single-connection**|**multi-connection**] [**port** *integer1*] [**timeout** *integer2*] [**key** *string*]

no tacacs-serve *ip-address*

参数

参数	参数说明
ip-address	服务器的IP地址。
single-connection	（可选）指定为来自AAA/TACACS+服务器的确认维持着单一开放的TCP连接。
multi-connection	（可选）指定为来自AAA/TACACS+服务器的不同确认维持不同的TCP连接。
port	（可选）指定服务器端口号。本选项覆盖缺省的端口号49。
integer1	（可选）服务器的端口号，有效端口号的范围是1至65536。
timeout	（可选）指定等待服务器回应超时值。它将覆盖使用tacacs timeout命令为本服务器设置的全局超时值。
integer2	（可选）设定超时记时器值，按秒计算。
key	（可选）指定认证和加密密钥。这个密钥必须与TACACS+服务器程序使用的密钥相匹配。指定这个。密钥将覆盖使用全局命令tacacs key为本服务器设置的密钥。
string	（可选）指定加密密钥字符串。

缺省

没有 TACACS＋服务器被指定。

命令模式

全局配置态

使用说明

可以使用多个 tacacs-server 命令可以通过后接 host 指定多个主机，并按照指定的顺序搜索主机。由于 tacacs-server host 命令的一些参数将覆盖由 tacacs-server timeout 和 tacacs-server key 命令在全局配置态所做的设置，所以利用本命令，可唯一地配置每台 TACACS+服务器的通信属性，以增强网络的安全性。

示例

下述示例指定路由器与 IP 地址为 1.1.1.1 的 TACACS+服务器进行协商，以进行 AAA 认证。并指定服务器的 TCP 服务端口号为 51，设定超时值是三秒，加密密钥为 a_secret。

tacacs -server host 1.1.1.1 single-connection port 51 timeout 3 key a_secret

3.1.4 tacacs-server key

为了设置路由器与 TACACS+服务器之间所有通信过程使用的加密密钥，请使用 tacacs-server key 全局配置命令。使用本命令的 no 形式则关闭该密钥。

tacacs-server key

no tacacs-server key

参数

参数	参数说明
key	用于设置加密密钥。这一密钥必须与TACACS+服务器程序使用的密钥相匹配。

命令模式

全局配置态

使用说明

在开始运行 TACACS+协议之前必须使用 tacacs-server key 命令设置加密密钥。输入的密钥必须与 TACACS+服务程序使用的密钥相匹配。所有的打头空格都被忽略，密钥中间不能有空格。

示例

下述示例设置加密密钥为 testkey:

tacacs-server key testkey

3.1.5 tacacs-server timeout

要设置 TACACS+等待某服务器作出应答的超时时间长度，请使用 tacacs-server timeout 全局配置命令。使用本命令的 no 形式则恢复缺省值。

tacacs-server timeout *seconds*

no tacacs-server timeout

参数

参数	参数说明
seconds	以秒计算的超时值（在1和600之间）。缺省为5秒。

缺省

5 秒

命令模式

全局配置态

使用说明

若针对某台服务器通过 tacacs-server 命令中的 timeout 参数设置了自己的等待超时值，将覆盖此命令设置的全局超时值。

示例

下述示例将超时定时器的值修改为 10 秒：

tacacs-server timeout 10