安全配置命令

目 录

第 1 章 AAA 配置命令 1
1.1 用户命令 1
1.1.1 username 1
1.1.2 local user maxlinks 3
1.1.3 local user freeze 4
1.1.4 local pass-group 4
1.1.5 local authen-group 5
1.1.6 local author-group 6
1.1.7 localgroup 7
1.1.8 show aaa users 8
#show aaa users 8
1.1.9 show local-users 9
#show aaa users 9
1.2 密码命令 10
1.2.1 service password-encryption 10
1.2.2 localpass 11
1.2.3 element 12
1.2.4 min-length 12
1.2.5 validity 13
1.3 认证命令 14
1.3.1 aaa authentication enable default 14
1.3.2 aaa authentication login 15
1.3.3 aaa authentication ppp 17
1.3.4 aaa authentication password-prompt 18
1.3.5 aaa authentication username-prompt 19
1.3.6 aaa authentication banner 20
User Access Verification 20
1.3.7 aaa authentication fail-message 20
1.3.8 aaa group server 21
1.3.9 server 22
1.3.10 enable 23
1.3.11 enable password 23
1.3.12 localauthen 25
1.3.13 login max-tries 25
1.3.14 debug aaa authentication 26
1.4 授权命令 27
1.4.1 aaa authorization 27
1.4.2 localauthor 28
1.4.3 exec privilege 29
1.5 记帐命令 30
1.5.1 aaa accounting 30

1.5.2 aaa accounting update 31
1.5.3 aaa accounting suppress null-username 31
第 2 章 RADIUS 配置命令 33
2.1 RADIUS 配置命令 33
2.1.1 debug radius 33
Router#debug radius event 33
RADIUS:return message to aaa, Give me your password 33
RADIUS:retransmit access-request [4] to 192.168.20.126 1812 <length=70> 33
2.1.2 ip radius source-interface 34
2.1.3 radius-server attribute 35
2.1.4 radius-server challenge-noecho 36
2.1.5 radius-server dead-time 36
2.1.6 radius-server host 37
2.1.7 radius-server optional-passwords 38
2.1.8 radius-server key 39
2.1.9 radius-server retransmit 40
2.1.10 radius-server timeout 40
2.1.11 radius-server vsa send 41
第 3 章 TACACS+配置命令 43
3.1 TACACS+配置命令 43
3.1.1 debug tacacs 43
3.1.2 ip tacacs source-interface 43
3.1.3 tacacs server 44
3.1.4 tacacs key 45
3.1.5 tacacs timeout 46
第 4 章 IPSec 配置命令 48
4.1 Crypto map 配置命令 48
4.1.1 crypto map (global configuration) 48
4.1.2 crypto map (interface configuration) 50
4.1.3 crypto map local-address 51
4.1.4 crypto map isakmp authorization 52
4.1.5 crypto map isakmp-profile 52
4.1.6 match address 52
4.1.7 set peer 53
4.1.8 set pfs 54
4.1.9 set security-association lifetime 55
4.1.10 set security-association idle-time 57
4.1.11 set security-association level per-host 58
4.1.12 set security-association replay 59
4.1.13 set transform-set 60
4.1.14 set session-key {inbound|outbound} 62
4.1.15 crypto dynamic-map 64
4.2 Crypto ipsec 配置命令 65
4.2.1 crypto ipsec df-bit 65

4.2.2 crypto ipsec fragmentation (暂时不支持)..... 66
4.2.3 crypto ipsec security-association idle-time..... 67
4.2.4 crypto ipsec security-association lifetime..... 68
4.2.5 crypto ipsec security-association replay 69
4.2.6 crypto ipsec nat-transparency 70
4.2.7 crypto ipsec transform-set..... 72
4.2.8 mode 73
4.2.9 crypto ipsec ipsec6-enable..... 74
4.3 ipsec 相关的 show, clear, debug 命令 75
4.3.1 show crypto ipsec transform-set 75
4.3.2 show crypto map 75
4.3.3 show crypto dynamic-map 76
4.3.4 show crypto sa isakmp..... 77
4.3.5 show crypto sa ipsec..... 78
4.3.6 clear crypto sa..... 81
4.3.7 debug crypto..... 82
第 5 章 Internet 密钥交换安全协议命令 84
5.1 IKE 配置命令 84
5.1.1 crypto isakmp enable 84
5.1.2 crypto isakmp identity..... 84
5.1.3 crypto isakmp invalid-spi-recovery..... 86
5.1.4 crypto isakmp keepalive..... 86
5.1.5 crypto isakmp key 87
5.1.6 crypto isakmp nat keepalive..... 88
5.1.7 crypto isakmp peer..... 89
5.1.8 crypto isakmp policy..... 90

第1章　AAA 配置命令

1.1　用户命令

本章描述配置本地用户命令以及本地用户组命令，本地用户组用来分组管理本地用户。

1.1.1　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* }] [**maxlinks** *number*] [**callback-dialstring** *string*] [**callback-line** *line*] [**callback-rotary** *rotary*] [**nocallback-verify**] [**autocommand** *command*] [**nohangup**] [**noescape**] [**bind-ip** *A.B.C.D*] [**bind-mac** *H:H:H:H:H:H*] [**bind-pool** *WORD*] [**bind-port** *INTERFACE*] [**authen-group** *WORD*] [**author-group** *WORD*] [**pass-group** *WORD*]

no username *username*

参数

参数	参数说明
username	用户名字符串；
password	设置用户密码。
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	同一用户可同时与路由器建立的连接数（只统计通过本地认证的用户）。
number	同时建立的连接数
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）
autocommand	当用户登录路由器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。

nohangup	阻止用户登陆并执行自动命令完后断开连接（不支持）。
noescape	阻止用户登陆后使用转义字符（不支持）。
bind-ip	设置用户绑定的IP地址。
A.B.C.D	绑定IPv4地址。
bind-mac	设置用户绑定的MAC地址。
H:H:H:H:H:H	绑定MAC地址。
bind-pool	设置用户绑定的地址池，远端用户认证后从该地址池分配地址。
WORD	绑定地址池名称。
bind-port	设置用户认证绑定端口。
INTERFACE	绑定端口名称。用户从别的端口认证则失败。
authen-group	设置用户本地认证策略组。
WORD	本地用户策略组名称。
author-group	设置用户本地授权策略组。
WORD	本地用户授权策略组名称。
pass-group	设置用户本地密码管理策略组。
WORD	本地密码管理策略组名称。

缺省

没有用户。

命令模式

全局配置态或本地用户组配置态

使用说明

当没有 password 参数时，认为密码为空字符串。

maxlinks 限制了同一个用户名同时可以与路由器建立的会话数，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 aaa users 命令查看每个在线用户是通过了那一种方式的认证。

目前我们路由器系统中所支持的 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路由器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

aaa authentication ppp

1.1.2 local user maxlinks

配置本地用户默认最大连接数。

local user maxlinks *number*

no local user maxlinks

参数

参数	参数说明
number	本地用户默认同时建立的最大连接数

缺省

没有最大连接数限制。

命令模式

全局配置态或本地用户组配置态

使用说明

该命令在全局配置态下配置时，作用于全局配置态下的用户；在本地用户组配置态下配置时，作用于该组内用户。

当用户认证通过后算一条有效链接，达到最大连接数后不再接受其他认证请求。除非 username 命令里特别指定了最大连接数，否则以该条命令配置的为准。

示例

下面的示例设置本地默认最大连接数为 10。

local user maxlinks 10

相关命令

username

localgroup

local pass-group

local authen-group

local author-group

1.1.3 local user freeze

手动冻结本地用户。

local user freeze *username*

no local user freeze *username*

参数

参数	参数说明
username	被手动冻结的本地用户名。

缺省

不冻结任何用户。

命令模式

全局配置态或本地用户组配置态

使用说明

该命令在全局配置态下配置时，作用于全局配置态下的用户；在本地用户组配置态下配置时，作用于该组内用户。

当某用户被手动冻结时，不接受 AAA 请求，只有当手动解冻后，才能接受 AAA 请求。

示例

下面的示例设置冻结本地用户 guest。

local user freeze guest

相关命令

username

localgroup

local pass-group

local authen-group

local author-group

1.1.4 local pass-group

配置本地用户默认采用的密码策略组。

local pass-group *WORD*

no local pass-group

参数

参数	参数说明
WORD	本地用户默认采用的密码策略组名。

缺省

用户没有默认密码策略组。

命令模式

全局配置态或本地用户组配置态

使用说明

该命令在全局配置态下配置时，作用于全局配置态下的用户；在本地用户组配置态下配置时，作用于该组内用户。

当配置该命令后，用户如果没有在 username 命令里特别指定密码策略组，则使用该条命令指定的密码策略组。

示例

下面的示例设置本地用户默认密码策略组为 A。

local pass-group A

相关命令

username

localgroup

local user

local authen-group

local author-group

1.1.5 local authen-group

配置本地用户默认采用的认证策略组。

local authen-group *WORD*

no local authen-group

参数

参数	参数说明
WORD	本地用户默认采用的认证策略组名。

缺省

用户没有默认认证策略组。

命令模式

全局配置态或本地用户组配置态

使用说明

该命令在全局配置态下配置时，作用于全局配置态下的用户；在本地用户组配置态下配置时，作用于该组内用户。

当配置该命令后，用户如果没有在 username 命令里特别指定认证策略组，则使用该条命令指定的认证策略组。

示例

下面的示例设置本地用户默认认证策略组为 B。

local authen-group B

相关命令

username

localgroup

local user

local pass-group

local author-group

1.1.6 local author-group

配置本地用户默认采用的授权策略组。

local author-group *WORD*

no local author-group

参数

参数	参数说明
WORD	本地用户默认采用的授权策略组名。

缺省

用户没有默认授权策略组。

命令模式

全局配置态或本地用户组配置态

使用说明

该命令在全局配置态下配置时，作用于全局配置态下的用户；在本地用户组配置态下配置时，作用于该组内用户。

当配置该命令后，用户如果没有在 username 命令里特别指定授权策略组，则使用该条命令指定的授权策略组。

示例

下面的示例设置本地用户默认授权策略组为 C。

local author-group C

相关命令

username

localgroup

local user

local pass-group

local authen-group

1.1.7 localgroup

本地用户组命令。

localgroup *WORD*

no localgroup *WORD*

参数

参数	参数说明
WORD	本地用户组名。

缺省

无本地用户组。

命令模式

全局配置态

使用说明

本地用户组用来分组管理本地用户，并可在组内使用特定的管理策略。

所有本地用户组和全局下的用户名不能出现同名。

示例

下面的示例增加一个本地用户组 team，在组内增加两个用户名 user1 和 user2，并冻结用户 user2。

```
localgroup team
  username user1 password 123
  username user2 password abc
  local user freeze user2
```

相关命令

username

local user

local authen-group

local author-group

local pass-group

1.1.8 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以的在线用户，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         wl            exec          00:12:24        172.16.20.120
serial2/1     admin               ppp(chap)      01:43:09        192.168.20.87
```

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

1.1.9 show local-users

要显示所有本地用户的概要信息，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以的在线用户，包括以下信息：用户名(username)、当前连接数(links)、密码存在时间(pw_present)、登录尝试次数(login_tries)、登录尝试时间(login_try_time)以及用户冻结缘由(freezing_cause)。

示例

```
#show aaa users
Local group default:
username        links   pw_present   login_tries   login_try_time   freezing_cause
a               1       20d3h5m30s   1             0s
b               0       35d          0             0s               command
```

域	解释
username	本地用户名。
links	当前连接数。
pw_present	密码存在时间。
login_tries	登录尝试次数。

login_try_time	登录尝试时间。
freezing_cause	用户冻结缘由。

相关命令

username

1.2 密码命令

本章描述了密码管理命令。

1.2.1 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显示。

命令模式

全局配置态

使用说明

目前我们路由器系统的实现中，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显示方式，即在 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。另外，除 AAA 相关命令外，其他命令涉及密码则在配置该命令时显示密文，去掉该命令时显示明文。

示例

router_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

无

1.2.2 localpass

本地密码策略组命令。

localpass *WORD*

no localpass *WORD*

参数

参数	参数说明
WORD	本地密码策略组名。

缺省

无本地密码策略组。

命令模式

全局配置态

使用说明

本地密码策略组用来配置密码配置和管理策略，可指定密码的组成、有效时间、最小长度等。

凡是采用了密码策略组，并且不满足该组策略的密码都视为无效密码，用户被冻结，认证时不予通过，在登录时会提示更新密码。

示例

下面的示例增加一个本地密码策略组 A，配置密码组成必须包含大小写字母和数字，最小长度为 10，有效期为 30 天。

```
localpass A
 element number lower-letter upper-letter
 min-length 10
 validity  20d
```

相关命令

element

min-length

validity

1.2.3 element

配置密码组成必须包含的元素。

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

no element

参数

参数	参数说明
number	密码必须包含数字。
lower-letter	密码必须包含小写字母。
upper-letter	密码必须包含大写字母。
Special-character	密码必须包含特殊字符。

缺省

密码可以为任何形式，包括空密码。

命令模式

密码策略组配置态

使用说明

配置该命令后，密码复杂度必须大于该命令配置要求，否则被视为无效密码。

示例

下面的示例在本地密码策略组 A 内，配置密码组成必须包含小写字母和数字。

localpass A

element number lower-letter

相关命令

localpass

min-length

validity

1.2.4 min-length

配置密码最小长度。

min-length *number*

no min-length

参数

参数	参数说明
number	最小密码长度值。

缺省

密码可以为任何长度，包括空密码。

命令模式

密码策略组配置态

使用说明

配置该命令后，密码长度必须大于等于该命令配置要求，否则被视为无效密码。

示例

下面的示例在本地密码策略组 A 内，配置密码最小长度为 5。

```
localpass A
 min-length 5
```

相关命令

localpass

element

validity

1.2.5 validity

配置密码有效期。

validity *1d2h3m4s*

no validity

参数

参数	参数说明
1d2h3m4s	密码有效期时长。

缺省

密码无有效期限制。

命令模式

密码策略组配置态

使用说明

配置该命令后，密码从配置时开始算起，超过有效期后将被视为无效密码。

示例

下面的示例在本地密码策略组 A 内，配置密码有效期为 2 天 10 小时 5 分 6 秒。

```
localpass A
 validity 2d10h5m6s
```

相关命令

localpass

min-length

element

1.3 认证命令

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。

1.3.1 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

参数

参数	参数说明
method	至少为表1中所给出的关键字之一

缺省

如果没有设置 default，除 console 能登陆成功外，其它皆返回认证失败结果。

如果设置了 default 表，如果不存在相应特权级别的 enable 口令，则进入该特权级别的认证过程的返回结果总是认证失败。

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。

另外，如果使用 RADIUS 或 TACACS+方式进行 enable 认证，使用的用户名不同，使用 RADIUS 认证时，用户名为$ENABLElevel$，其中 level 是指用户要进入的特权级别；使用 TACACS+认证时，用户名为该用户登录路由器时使用的用户名，相关的具体配置请参照“AAA 认证配置”文档中相关章节。

表 1：AAA 认证的有效缺省方法。

关键字	描述
group *WORD*	使用命名的服务器组进行认证。
group tacacs+	使用TACACS+进行认证。
group radius	使用RADIUS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。

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 tacacs+ enable none

相关命令

enable password

1.3.2 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*}

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。
list-name	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2中描述的关键字之一。

缺省

如果用户在请求 login 服务时，搜索不到指定或者默认的方法列表，则除 console 以外，一律返回认证失败结果。

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。

表 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 *WORD*	使用命名的服务器组进行认证。
group tacacs+	使用TACACS+进行认证。
group radius	使用RADIUS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 。

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（由于路由器上没有配置 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

username

enable password

1.3.3 aaa authentication ppp

要指定一种或者多种用于运行 PPP 的串行接口的 AAA 认证方法，可以使用全局配置命令 aaa authentication ppp。使用该命令的 no 形式关闭认证。

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

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

参数

参数	参数说明
default	将跟随在该参数后面所列的认证方法作为用户注册时使用的缺省认证方法；
list-name	用来命名认证方法列表的字符串；
mehod1 [method2...]	至少为表3中描述的方法之一。

缺省

如果用户在请求 login 服务时，搜索不到指定或者默认的方法列表，则一律返回认证失败结果。

命令模式

全局配置态

使用说明

使用 aaa authentication ppp 命令创建的缺省列表和命名列表在 ppp authentication 命令中引用。这些列表至多能够包含四种认证方法，用户连接到该串行接口时使用这些认证方法。

通过输入 aaa authentication ppp list-name method 命令来创建列表，其中 list-name 是用来命名该列表的任何字符串。参数 method 指定具体认证方法，认证过程按配置次序使用这些方法。可以至多输入四种方法。方法关键字在表 3 中描述。

认证失败，则不再使用其它的认证方法。在命令行中指定 none 作为最后的方法，则即使所有的方法均返回错误，仍能认证成功。

表 3：AAA 认证的 PPP 方法 。

关键字	描述
group *WORD*	使用命名的服务器组进行认证。
group tacacs+	使用TACACS+进行认证。

group radius	使用RADIUS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

下面的示例为使用 PPP 的串行线路创建一个名为“TEST”的 AAA 认证列表。这种认证首次尝试与 TACACS+服务器联系。如果返回错误，则允许用户不经认证访问网络。

aaa authentication ppp TEST tacacs+ none

相关命令

ppp authentication

1.3.4 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

1.3.5 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+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

1.3.6 aaa authentication banner

要配置个性化风格的标语(该标语在用户登陆时显示)，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	向用户登陆时将要显示的文本*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 AAA Router”

相关命令

aaa authentication fail-message

1.3.7 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

1.3.8 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。

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

1.3.9 server

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

server *ADDR* key *WORD*

no server *ADDR*

参数

参数	参数说明
ADDR	服务器的IP地址(v4或v6)。
WORD	服务器所需的key值。

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

server 12.1.1.1

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。

相关命令

aaa group server

1.3.10 enable

进入管理态或改变当前权限级别。

enable [*number***]**

参数

参数	参数说明
number	指定权限级别。

缺省

采用当前用户的授权级别。

命令模式

管理态或全局配置态

使用说明

如果指定权限级别比用户授权级别高，则需要输入高级别 enable 密码，认证通过才能进入；否则进入指定权限级别。未指定权限级别，则默认为用户授权级别。

示例

下面的示例中，假定当前权限级别为 10，用户授权级别为 15，则可进入 15 权限级别。

Router#enable

Router# <190>Sep 22 12:56:04 Router - 036EE9D0 [Core 0]: User admin enter privilege mode from console 0, level = 15

相关命令

enable password

enter

1.3.11 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
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；
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

我们路由器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返回认证失败。

目前我们路由器系统中所支持的 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路由器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路由器上的配置文件中获得的。

相关命令

aaa authentication enable default

service password-encryption

1.3.12 localauthen

本地认证策略组命令。

localauthen *WORD*

no localauthen *WORD*

参数

参数	参数说明
WORD	本地认证策略组名。

缺省

无本地认证策略组。

命令模式

全局配置态

使用说明

本地认证策略组用来配置认证的限制条件，如最大尝试次数和最大尝试时间。

如果用户采用了认证策略组，则在认证时超过认证策略组的限制将被冻结，限制条件有效期结束后将被解冻。

示例

下面的示例增加一个本地认证策略组 B，配置 1 天内最大认证尝试失败次数为 5 次。

```
localauthen B
 login max-tries 5 try-duration 1d
```

相关命令

login max-tries

1.3.13 login max-tries

配置登录最大尝试失败次数。

login max-tries *number* **try-duration** *1d2h3m4s*

no login max-tries

参数

参数	参数说明
number	最大登录尝试失败次数。
try-duration	在指定时间内限制最大登录尝试失败次数。

1d2h3m4s	指定时间时长。

缺省

无任何尝试次数限制。

命令模式

认证策略组配置态

使用说明

配置该命令后，在指定时间内超过最大登录尝试失败次数，用户将被冻结，等指定时间过后才可解冻继续尝试。

示例

下面的示例在本地认证策略组 B 内，配置 12 小时内最大认证尝试失败次数为 3 次。

localauthen B

login max-tries 3 try-duration 12h

相关命令

localauthen

1.3.14 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。

相关命令

debug aaa authorization

debug aaa accounting

1.4 授权命令

本章描述了用来配置 AAA 授权方法的命令。AAA 授权可以限制对某个用户的有效服务，当 AAA 授权有效时，路由器使用从用户开工文档（profile）中检索出的信息配置该用户的会话，用户的开工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，只要包含在用户开工文档中的信息允许提供这项服务。

如果想得到关于怎样用 AAA 的方法来配置授权的信息，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。

1.4.1 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 { **network** | **exec** } {**default** | *list-name*} [*method1* [*method2...*]]

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

参数

参数	参数说明
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。
method1 [method2...]	授权方法，参见“授权配置”文档

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失败后有一个备用的方法。 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。

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 的网络授权方法列表，该方法列表指定在使用 PPP 的串行线路上使用 RADIUS 授权方法。如果 RADIUS 服务器没有响应，则执行本地网络授权。

aaa authorization network have_a_try radius local

相关命令

aaa authentication

aaa accounting

priviledge

1.4.2 localauthor

本地授权策略组命令。

localauthor *WORD*

no localauthor *WORD*

参数

参数	参数说明
WORD	本地授权策略组名。

缺省

无本地授权策略组。

命令模式

全局配置态

使用说明

本地认证策略组用来配置认证的限制条件，如最大尝试次数和最大尝试时间。

如果用户采用了认证策略组，则在认证时超过认证策略组的限制将被冻结，限制条件有效期结束后将被解冻。

示例

下面的示例增加一个本地认证策略组 C，配置 telnet 登录方式授权级别为 15，ssh 登录方式授权级别为 12。

localauthor C

exec privilege telnet 15

exec privilege ssh 12

相关命令

exec privilege

1.4.3 exec privilege

配置密码组成必须包含的元素。

exec privilege {default | aux | console | ssh | telnet | rtelnet} *number*

no exec privilege {default | aux | console | ssh | telnet | rtelnet}

参数

参数	参数说明
default	默认exec授权级别。
aux	通过aux口登录的授权级别。
console	通过console口登录的授权级别。
ssh	通过ssh方式登录的授权级别。
telnet	通过telnet方式登录的授权界别。
rtelnet	通过反向telnet方式登录的授权界别。
number	授权级别数。

缺省

无授权级别指定。

命令模式

授权策略组配置态

使用说明

配置该命令后，用指定的方式登录会用对应的授权级别给用户，如果没有对应的配置，则用 default 的，default 没有配置，则默认为 15。

示例

下面的示例在本地授权策略组 C 内，配置 telnet 登录方式授权级别为 14。

localauthor C

exec privilege telnet 14

相关命令

localauthor

1.5 记帐命令

本章描述了用来配置 AAA 认证方法的命令。记帐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 AAA 记帐功能时，路由器以记帐记录的形式向 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。每条记帐记录包括记帐属性值（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、客户帐单和/或审计等分析。

1.5.1 aaa accounting

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

aaa accounting { **network** | **exec** | **connection**} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} **group** *groupname*

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

参数

参数	参数说明
network	给所有PPP会话提供记帐记录信息，包括包、字节及时间计数。
exec	提供有关路由器的用户EXEC终端会话的信息（目前不支持）。
connection	提供有关路由器发出的所有出站连接的信息，目前只支持H323会话信息。
default	缺省记帐方法列表。
list-name	用来命名记帐方法列表的字符串。
method1 [method2...]	记帐方法，参见“记帐配置”文档

缺省

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

命令模式

全局配置态

使用说明

使用 aaa accounting 命令开启记帐，创建记帐方法列表，定义在用户发送记帐记录时可使用的记帐方法。记帐方法列表定义了记帐执行的方式以及执行这些记帐方法的次序。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帐方法（RADIUS 或 TACACS+）。方法列表可以指定一个或多个用来记帐的安全协议，因此，它能够确保万一前面所列的记帐方法失败后有一个备用的方法。

相关命令

aaa authentication

aaa accounting

1.5.2 aaa accounting update

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

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

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

参数

参数	参数说明
update	激活路由器发送临时记帐记录（需要端用户支持）
newinfo	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
periodic	周期性地发送临时记帐记录，该周期由数字参数定义
number	发送临时记帐记录的周期数字参数

缺省

不发生临时记帐行为。

命令模式

全局配置态

使用说明

参见“记帐配置”文档。

相关命令

aaa accounting

1.5.3 aaa accounting suppress null-username

如果需要阻止为没有用户名的会话产生记帐记录，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帐记录。

命令模式

全局配置态

使用说明

参见“记帐配置”文档。

相关命令

aaa accounting

第2章 RADIUS 配置命令

2.1 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 客户机运行在路由器上，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”。

2.1.1 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。

Router#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	需要得到用户名。

username	
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
interface-name	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。当路由器有许多接口且打算确保来自某个特定路由器的全部 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 s1/2 的 IP 地址：

ip radius source-interface s1/2

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认证或请求中传输属性attribute32（NAS identifier）
95	根据跟随在该参数后面的指令指定在radius认证或请求中传输属性attribute32（NAS IPv6 address attribute）

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）。

radius-server attribute 95 指定在 RADIUS 认证或计费请求报文中传输 radius 属性 95（NAS IPv6 地址）。

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

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 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 dead-time

当某些服务器不可用时，为了改善 RADIUS 的响应时间，使用 radius dead-time 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，即认为所以的服务器一直可用。

radius-server dead-time *minutes*

no radius-server dead-time

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 dead-time 5

相关命令

host

radius-server retransmit

radius-server timeout

2.1.6 radius-server host

要指定 RADIUS 服务器的 IP 地址，使用 **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]

radius-server host *ip-address*

参数

参数	参数说明
ip-address	RADIUS服务器主机的IP地址（v4或v6）。
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；若设置为0，则主机不用于认证。
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；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 IPv4 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

下述示例指定 IPv6 地址为 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

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

username

2.1.7 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

host

2.1.8 radius-server key

为了对路由器和 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
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。

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

host

username

2.1.9 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

下述示例指定重试记数器的值为 5 次：

radius-server retransmit 5

相关命令

radius-server timeout

2.1.10 radius-server timeout

要对路由器等待服务器应答的时间上限进行设置，请使用 radius 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

2.1.11 radius-server vsa send

要把路由器配置为可识别和使用厂商专用属性（VSA），使用 radius 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 [**accounting** | **authentication**]

no radius-server vsa send [**accounting** | **authentication**]

参数

参数	参数说明
accounting	(可选项)识别的厂商专用属性集只限于记录属性。
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），为在路由器和 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 命令使路由器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

下述示例对路由器进行配置，使之识别和使用厂商专用记录属性：

radius-server vsa send accounting

相关命令

host

第3章 TACACS+配置命令

3.1 TACACS+配置命令

这里我们将介绍 TACACS+安全协议的配置命令。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。

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＋报文使用指定接口的 IP 地址，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 IP 地址的使用。

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IP地址对应的接口名称。

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

使用本命令可以通过指定源接口来为所有的 TACACS＋报文设置源 IP 地址，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，将保证每一台路由器的 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，当路由器有许多接口，但为了确保来自于特定路由器的所有 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 s1/0 的 IP 地址作为所有 TACACS+报文的源发 IP 地址：

ip tacacs source-interface s1/0

相关命令

ip radius source-interface

3.1.3 tacacs server

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

t**acacs server** *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(v4或v6)。
single-connection	（可选）指定路由器为来自AAA/TACACS+服务器的确认维持着单一开放的TCP连接。
multi-connection	（可选）指定路由器为来自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 命令以指定多个主机，并按照指定的顺序搜索主机。由于 tacacs server 命令的一些参数将覆盖由 tacacs timeout 和 tacacs key 命令所作的全局设置，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 1.1.1.1 single-connection port 51 timeout 3 key a_secret
```

相关命令

tacacs key

tacacs timeout

3.1.4 tacacs 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 key 全局配置命令。使用本命令的 no 形式则关闭该密钥。

tacacs key key

no tacacs 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 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 key testkey

相关命令

tacacs server

3.1.5 tacacs 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 timeout 全局配置命令。使用本命令的 no 形式则恢复缺省值。

tacacs timeout *seconds*

no tacacs 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 timeout 10

相关命令

tacacs server

第4章 IPSec 配置命令

4.1 Crypto map配置命令

4.1.1 crypto map (global configuration)

要创建或修改一个加密映射表，进入加密映射表表配置态，可以使用 crypto map 全局配置命令。使用此命令的 no 格式来删除一个加密映射表表或集合。

crypto map *map-name seq-num* [**ipsec-manual**| **ipsec-isakmp** [**dynamic** *dynamic-map-name*[discovery]]]

no crypto map *map-name seq-num*

参数

参数	参数说明
map-name	加密映射表集合的名字。
seq-num	加密映射表的序号。参看“使用说明”一节中对于使用此参数的详细解释。
ipsec-manual	表示对于此加密映射表所指定的通信，将采用手工方式来建立IPSec安全联盟对其进行保护。
ipsec-isakmp	表示对于此加密映射表所指定的通信，将使用IKE来建立IPSec安全联盟对其进行保护。
dynamic-map-name	该加密映射表用来作模板的动态加密映射表名字。
discovery	启动tunnel endpoint discovery

缺省

不存在加密映射表。

命令模式

全局配置态。当无 dynamic 及其参数时，使用此命令将进入加密映射表配置态。

使用说明

使用此命令可以创建一个新的加密映射表，或修改一个现存的加密映射表。

在创建了一个加密映射表以后，不能对全局配置态下指定的参数进行改变，因为这些参数决定了在加密映射表配置态中可以使用哪些配置命令。例如，一个映射表一旦作为 ipsec-isakmp 创建，就不能将它改变成 ipsec-manual；必须将它删除并重新进入加密映射表配置态才能这样做。在定义了加密映射表以后，可以使用 crypto map（interface configuration）命令将此加密映射表集合运用到接口上。

- 加密映射表的功能

加密映射表提供了两个功能：对要保护的通信进行过滤和分类，以及定义通信的策略。IPSec 加密映射表将下面这些定义联系在一起：

- 哪些通信应该受到保护

  受保护数据可以到达哪个 IPSec 对端——这个对端能够和本地路由器建立起一个安全联盟。

  对于受保护通信，可用的变换集合是哪些。

  如何对密钥和安全联盟进行管理和使用（或者在不使用 IKE 时，密钥是什么）。

  具有相同 map-name（加密映射表名称）的多个加密映射表组成了一个加密映射表集合。

  加密映射表集合是由加密映射表组成的集合，其中每条都有不同的 seq-num 和相同的 map-name。因此，对于给定接口，你可以对发往一个 IPSec 对端通信采取某种安全策略，而对于发往同一或不同 IPSec 对端的其它通信采用不同的安全策略。要达到这一目的，你应该创建两个加密映射表，每个都有相同的 map-name，但有不同的 seq-num。

- seq-num 参数

  seq-num 参数的数值不能随便定。此数字是用来对一个加密映射表集合中的多个加密映射表进行排序的。在一个加密映射表集合中，seq-num 参数小的加密映射表在 seq-num 参数大的加密映射表之前进行判断；也就是说，序号越小的映射优先级越高。

  例如，假设加密映射表集合包含了三个加密映射表：aaa 10，aaa 20 以及 aaa 30。名为 aaa 的加密映射表集合被运用在接口 Serial 0 上。当通信通过接口 Serial 0 时，首先用 aaa 10 对它进行判断。如果通信匹配 aaa 10 指定的扩展访问列表中的一条 permit，那么将使用 aaa 10 中定义的策略对通信进行处理（包括必要的时候建立 IPSec 安全联盟）。如果通信不匹配 aaa 10 访问列表，将用 aaa 20，然后是 aaa 30 对通信进行判断，直到通信匹配一个映射中的 permit 语句（如果不匹配任何加密映射表中的 permit 语句，那么此通信将不受任何 IPSec 的保护直接发送）。

示例

下面的例子显示了使用 IKE 来建立安全联盟时，所需的最小加密映射表配置：

```
crypto map aaa 10 ipsec-isakmp
match address aaa
set transform-set one
set peer 192.2.2.1
```

下面的例子显示了使用动态加密映射表来建立安全联盟时，所需的最小加密映射表配置：

```
crypto dynamic-map aaa 22
match address aaa
set transform-set one
crypto map bbb 10 ipsec-isakmp dynamic-map aaa
```

如果配置如果使用的 dynamic map 并不存在，那么命令设定将失败

下面的例子显示了手工建立安全联盟时，所需的最小加密映射表配置：

```
crypto transform-set one
 transform-type ah-md5-hmac esp-des
crypto transform-set one ah-md5-hmac esp-des

crypto map aaa 10 ipsec-manual
match address aaa
set transform-set one
```

```
set peer 192.2.2.1
set security-association inbound ah 300 98765432109876543210987654
set security-association outbound ah 300 fedcbafedcbafedcfedcbafedcbafedc
set security-association inbound esp 300 cipher 0123456789012345
set security-association outbound esp 300 cipher abcedfabcdefabcd
```

相关命令

crypto map (interface configuration)

crypto map local-address

match address

set peer

set pfs

set security-association lifetime

set transform-set

show crypto map

4.1.2 crypto map (interface configuration)

要将预先定义好的加密映射表集合运用到接口上，可以使用 crypto map 接口配置命令。

使用此命令的 no 格式可以从一个接口上移除加密映射表集合。

crypto map *map-name*

no crypto map

参数

参数	参数说明
map-name	加密映射表集合的名称。

缺省

接口上没有设置加密映射表。

命令模式

接口配置态

使用说明

使用此命令可以将加密映射表集合运用到接口。在接口可以提供 IPSec 服务之前，必须在接口上配置一个加密映射表集合。对于一个接口，只能设置一个加密映射表集合。如果多个加密映射表具有相同的 map-name 和不同的 seq-num，那么它们位于同一集合，并被运用到同一接口上。Seq-num 越小的加密映射表具有越高的优先级，并且先进行判断。一个加密映射表集合中可能包含 ipsec-isakmp、ipsec-manual 加密映射表的组合。

示例

下面的例子将加密映射表集合 aaa 赋给接口 S0。当报文经过接口 S0 时，将使用 aaa 集合中的所有加密映射表对它进行判断。当出站报文匹配 aaa 加密映射表中某一条所对应的访问列表时，一条基于加密映射表配置的安全联盟（若是 IPSec）连接将被建立（如果没有现存的安全联盟的话）。

interface s0

crypto map aaa

相关命令

crypto map (global configuration）

crypto map *local-address*

show crypto map

4.1.3 crypto map local-address

指定一个接口标识，并在加密映射表中指定它用于 IPSec 通信，可以使用 crypto map local-address 全局配置命令。使用此命令的 no 格式可以从配置中删除这条命令。

crypto map *map-name local-address interface-id*

no crypto map *map-name local-address*

参数

参数	参数说明
map-name	加密映射表集合的名称。
interface-id	指定加密映射表集合使用的接口标识。

缺省

无

命令模式

全局配置态

使用说明

如果设置了此命令，加密映射表集合中的加密映射表的 IPSec 本端地址使用指定接口的 IP 地址。

示例

无

相关命令

crypto map (interface configuration)

4.1.4 crypto map isakmp authorization

(xauth 命令)

4.1.5 crypto map isakmp-profile

进入 crypto map 特殊模式后的命令

4.1.6 match address

要为一个加密映射表指定一个扩展访问列表，可以使用 match address 加密映射表配置命令。使用此命令的 no 格式可以从一条加密映射表中取消设置的扩展访问列表。

match address *access-list-name*

no match address *access-list-name*

参数

参数	参数说明
access-list-name	加密访问列表。此名字必须和配置的访问列表的name相匹配。

缺省

加密映射表不配置任何访问列表。

命令模式

加密映射表配置态

使用说明

此命令对于所有加密映射表来说都是必须的。

使用此命令将扩展访问列表赋给一条加密映射表。需要使用 ip access-list extended 命令来定义此访问列表。

用此命令指定的扩展访问列表将被 IPSec 用于判断哪些通信应被加密保护，而哪些通信不被加密保护（此访问列表所允许的通信都将受到保护。被此访问列表拒绝的通信在相应加密映射表中将不受保护）。

注意加密访问列表不是用来决定是否允许通信通过某个接口，这项工作由直接作用于接口上的访问列表来完成。

此命令指定的加密访问列表既用于判断入通信，也用于判断出通信。接口加密映射表所对应的加密访问列表将对出通信进行判断，决定它是否应该受到加密保护，并且如果是（通信匹配一条 permit），那么应该应用什么加密策略。在通过了接口上普通访问列表的检查以后，入通信将被接口的加密映射表集合所指定的加密访问列表进行判断，判定它是否应该受到加密保护，如果是，应该受到哪种加密策略的保护（在使用 IPSec 的情况下，未受保护的通信将被丢弃，因为它本应受到 IPSec 的保护）。

示例

下面的例子是使用 IKE 来建立安全联盟时所需的最小加密映射表配置。

```
crypto map aaa 100 ipsec-isakmp
match address aaa
set transform-set one
set peer 192.2.2.1
```

相关命令

crypto map(global configuration)

crypto map(interface configuration)

crypto map local-address

ip access-list extended

set peer

set pfs

set security-association lifetime

set transform-set

show crypto map

4.1.7 set peer

要在加密映射表中指定 IPSec 对端，可以使用 set peer 加密映射表配置命令。使用此命令的 no 格式，可以从加密映射表中删除 IPSec 对端。

set peer *ip-address*

no set peer *ip-address*

参数

参数	参数说明
ip-address	用IP地址指定的IPSec对端。

缺省

缺省情况下不指定 IPSec 对端。

命令模式

加密映射表配置态

使用说明

使用此命令可为加密映射表指定一个 IPSec 对端。对于所有加密映射表，这条命令都是必须的。一个加密映射表只能指定一个 IPSec 对端。如果想要改变对端，指定新的对端即可，会覆盖原先设置。

示例

下面的例子展示了当使用 IKE 来建立安全联盟时的一个加密映射表配置。

```
crypto map aaa 100 ipsec-isakmp
match address aaa
set transform-set one
set peer 192.2.2.1
```

相关命令

crypto map(global configuration)

crypto map(interface configuration)

crypto map local-address

match address

set pfs

set security-association lifetime

set transform-set

show crypto map

4.1.8 set pfs

当为加密映射表申请新的安全联盟时，要指定 IPSec 将同时申请理想转发安全机制（PFS），或当收到建立新安全联盟的申请时，IPSec 将要求 PFS，可以使用 set pfs 加密映射表配置命令。要确定 IPSec 不会进行 PFS 申请，可以使用这条命令的 no 格式。

set pfs [**group1**|**group2**|**group5**]

no set pfs

参数

参数	参数说明
group1	当组织新的Diffle-Hellman交换时，指定IPSec将使用768位的Diffle-Hellman组。
group2	当组织新的Diffle-Hellman交换时，指定IPSec将使用1024位的Diffle-Hellman组。
Group5	当组织新的Diffle-Hellman交换时，指定IPSec将使用1536位的Diffle-Hellman组

缺省

在缺省情况下，不要求 PFS。

命令模式

加密映射表配置态

使用说明

此命令只对 ipsec-isakmp 加密映射表可用。

在协商期间，此命令将使得 IPSec 在为这条加密映射表申请新安全联盟时，同时也申请 PFS。如果本端发起协商，且本地配置指定了使用 PFS，对端必须组织 PFS 交换，否则协商将失败。如果本地配置没有指定组，那么本地路由器将提议使用缺省值 group1，而对方无论提供 group1 或 group2 都会被接受。如果本地配置指定了 group2，那么对端必须提供此组，否则协商将会失败。如果本地配置没有指定 PFS，那么本地路由器也会接受对端所提供的 PFS。

PFS 增加了另一种级别的安全性，因为如果一个密钥曾被攻击者解开过，那么只有那些用此密钥进行传送的数据受到威胁。如果没有 PFS，用其它密钥传送的数据也可能受到威胁。

在使用 PFS 的情况下，每次协商新安全联盟的时候都会引发一次新 Diffle-Helman 交换（这种交换需要额外的处理时间）。

1024 比特的 Diffle-Hellman 组，即 group2，比 group1 提供了更多的安全性，但比 group1 需要更多的处理时间。

示例

下面的例子指定了无论什么时候加密映射表 aaa 100 协商新安全联盟时都要使用 PFS：

```
crypto map aaa 100 ipsec-isakmp
set pfs group2
```

相关命令

crypto map (global configuration)

crypto map (interface configuration)

crypto map local-address

match address

set peer

set security-association lifetime

set transform-set

show crypto map

4.1.9 set security-association lifetime

要为某个加密映射表设置生命周期值（此值用于 IPSec 安全联盟的协商），可以使用 Set security-association lifetime 加密映射表配置命令。要将一个加密映射表的生命周期值恢复成缺省值，可以使用此命令的 no 格式。

set security-association lifetime [**seconds** *seconds* | **kilobytes** *kilobytes*]

no set security-association lifetime [*seconds* | *kilobytes*]

参数

参数	参数说明
seconds *seconds*	指定一个安全联盟在超时终止前所能存活的秒数。
kilobytes *kilobytes*	在一个安全联盟超时以前，使用此安全联盟所能传输的通信量（以千字节计）。

缺省

加密映射表的安全联盟根据缺省生命周期值进行协商。

缺省超时秒数为 28800 秒 (1 小时) ，缺省超时通信量为 2560000 千字节。

命令模式

加密映射表配置态

使用说明

此命令只对 ipsec-isakmp 加密映射表可用。

IPSec 安全联盟使用共享密钥。这些密钥和它们对应的安全联盟同时超时。假设在安全联盟协商过程中，路由器申请新的安全联盟时，给定的加密映射表已经配置了新生命周期值，那么它将在向对端发起的申请中使用自己的加密映射表生命周期值；它将使用此值作为新的安全联盟的生命周期值。当路由器收到从对端发来的协商申请时，它将取对端提议的和本地路由器配置的生命周期值中较小者作为新安全联盟的生命周期。

生命周期有两种：一个时间生命周期、一个通信量生命周期。这两个生命周期中无论哪个先到期，安全联盟都将超时。

要改变时间生命周期，可以使用命令的 set security-association lifetime seconds 格式。时间生命周期指定了安全联盟和密钥在经过了一定的秒数后超时。

要改变通信量生命周期，可以使用命令的 set security-association lifetimekilobytes 格式。通信量生命周期指定了安全联盟和密钥在使用安全联盟密钥进行加密的通信量（以 KB 计）达到了一定数量以后超时。

生命周期值越短，密钥破解攻击越难成功，因为攻击者用于分析的用同一密钥加密的数据越少。但是，生命周期越短，用于建立新安全联盟的 CPU 开销就越多。

在手工方式建立安全联盟时，生命周期值将被忽略，其生命周期是永久的，除非手动改变（使用 ipsec-manual 加密映射表来建立安全联盟）。

生命周期是如何工作的

假设给定的加密映射表没有配置新的生命周期值，那么当路由器申请新的安全联盟时，它在向对端发起的申请中使用缺省生命周期值；它将使用此值作为新安全联盟的生命周期。当路由器收到从对端发来的协商申请时，它使用对端提议的和本地配置的生命周期值中较小者作为新安全联盟的生命周期值。

经过了一定的时间（由 seconds 关键字指定）后，已传递了一定字节的通信量（由 kilobytes 关键字指定），这两件事情无论哪件先发生，安全联盟（以及相应的密钥）都将超时。

新的 SA 在原有安全联盟的生命周期极限值到达以前就开始进行协商，以确保当原有安全联盟超时的时候，已经有一个新的安全联盟备用了。新安全联盟在 seconds 生命周期超时前 30 秒，或经由这条隧道的通信量距 kilobytes 生命周期还有 256KB 时开始进行协商（根据哪个先发生）。

如果在一个安全联盟的整个生命周期中都没有通信经过这条隧道，那么当此安全联盟超时的时候不会进行新安全联盟的协商。相应地，新的安全联盟只有当 IPSec 得到应该受到保护的一个分组时才开始进行协商。

示例

此例子加密映射表设置较短的生命周期值，因为属于此加密映射表的安全联盟的密钥可能被窃取。通信量生命周期值未被改变，因为分享这些安全联盟的通信量不是很大。时间生命周期值缩短到 1800 秒（30 分钟）。

```
crypto map aaa 100 ipsec-isakmp
set security-association lifetime seconds 1800
```

相关命令

crypto map (global configuration)

crypto map (interface configuration)

crypto map local-address

match address

set peer

set pfs

set transform-set

show crypto map

4.1.10 set security-association idle-time

要设定在没有收到任何报文的情况下，sa 多久超时失效，可以使用 Set security-association idle-time 加密映射表配置命令。要将一个加密映射表的 idle 生命周期值恢复成缺省值，可以使用此命令的 no 格式。

set security-association idle-time [**seconds** *seconds*]

no set security-association idle-time [*seconds*]

参数

参数	参数说明
seconds *seconds*	指定一个安全联盟在没有收到报文多久后超时终止存活的秒数。

缺省

关闭此超时功能

命令模式

加密映射表配置态

使用说明

当一段时间没有收到关于某个 sa 的报文后，认为这个 sa 对应的 peer 出现问题，从而删除这个 sa，如果 set peer 有设定 default peer，则之后的报文传输会使用这个 peer 进行协商和通讯

示例

```
crypto map tohub 1 ipsec-isakmp
 set peer 10.1.1.1 default
 set peer 10.2.2.2
 set security-association idle-time 120 default
```

相关命令

set peer

4.1.11 set security-association level per-host

要根据符合 sp acl 中的主机地址对来建立 security association，可以使用 Set security-association leve per-host 加密映射表配置命令。要恢复成每条 acl 建立一个 sa，可以使用此命令的 no 格式。

set security-association level per-host

no set security-association level per-host

参数

缺省

关闭此功能

命令模式

加密映射表配置态

使用说明

该命令仅支持 ipsec-isakmp map 不支持 dynamic map.

默认情况下,sa 的建立是与每个 access list 对应，如果一个报文属于这个 acl 触发了 ike 协商,并建立了 sa，那么下一个报文,即使源目的地址不同,但仍然属于同一个 acl，则会使用刚才的 sa 来保护报文,不会重新开始协商.

但是当这个命令配置后，只要符合 acl，任何不同的主机地址对之间都会建立一个独立的 sa.

在使用这条命令时,需要考虑由于 sa 数量的增大,和协商次数的增多,会给系统带来不小的负担

示例

With an access list entry of **permit ip 1.1.1.0 255.255.255.0 2.2.2.0 255.255.255.0** and a per-host level:

- A packet from 1.1.1.1 to 2.2.2.1 will initiate a security association request which would look like it originated via **permit ip host 1.1.1.1 host 2.2.2.1**.

- A packet from 1.1.1.1 to 2.2.2.2 will initiate a security association request which would look like it originated via **permit ip host 1.1.1.1 host 2.2.2.2**.

- A packet from 1.1.1.2 to 2.2.2.1 will initiate a security association request which would look like it originated via **permit ip host 1.1.1.2 host 2.2.2.1.**

Without the per-host level, any of the above packets will initiate a single security association request originated via **permit ip 1.1.1.0 255.255.255.0 2.2.2.0 255.255.255.0**

相关命令

crypto dynamic-map
crypto map (global configuration) (IPSec)
crypto map (interface configuration) (IPSec)
crypto map local-address
match address (IPSec)
set peer (IPSec)
set pfs
set security-association lifetime
set transform-set
show crypto map (IPSec)

4.1.12 set security-association replay

要关闭 SA 的抗重播检查,或者设定抗重播窗口大小，可以使用 Set security-association replay 加密映射表配置命令。要将一个加密映射表的抗重播窗口大小恢复成缺省值，可以使用此命令的 no 格式。

set security-association replay [**window-size** [1024/128/256/64] / **disable**]

no set security-association replay [**window-size** [1024/128/256/64] / **disable**]

参数

参数	参数说明
disable	取消抗重播功能
Window-size 1024/128/256/64	指定抗重播窗口的大小

缺省

开启抗重播功能，窗口大小为 64

命令模式

加密映射表配置态

使用说明

抗重播的作用在于,抵御攻击者不断的使用相同的报文进行发送,从而迫使网关不停的进行解密等相关处理,从而消耗网关的系统资源.

Anti replay 的使用规则如小:

如果没有启动replay windows,包总是可以接受.

开启replay window之后,

收到的包seq 比之前收到的seq大，包可以接受。

如果收到的包seq 比之前收到的seq小，且差距大于窗口大小，则丢弃

如果收到的包seq比之前收到的包seq 小，差距小于窗口大小，但bitmap表示该包已经收到过，则丢弃。

否则包可以接受

一定要开启认证，才能使用replay window,

因为认证的范围包括esp/ ah 的头部，如果没有认证，而replay window check 和update是在加密前完成． 攻击者可以不断的发一些包,占有bitmap 里的一些seq,导致正常的包无法通过replay window check.

或者攻击通过发送一个seq很大的包，根据原理将replay window 右移很大一块，那之后的所有小于这个seq，可能都会被拒绝

所有进入replay window检查的包，首先要经过认证检查，除非即没有使用AH，又没有使用esp的auth功能

示例

```
router# configure
router(config)# crypto ipsec security-association replay window-size 128
```

相关命令

4.1.13 set transform-set

要指定加密映射表将使用哪些变换集合，可以使用 set transform-set 加密映射表配置命令。要从一个加密映射表中移除所有变换集合，可以使用此命令的 no 格式。

set transform-set *transform-set-name1* [*transform-set-name2*...*transform-set-name6*]

no set transform-set

参数

参数	参数说明
transform-set-name	变换集合的名字。对于ipsec-manual加密映射表，只能指定一个变换集合。 对于ipsec-isakmp，可以指定不多于六个加密映射表集合。

缺省

缺省情况下不包括任何变换集合。

命令模式

加密映射表配置态

使用说明

此命令对于所有的加密映射表都是必须的。

使用此命令可以指定一条加密映射表中将包含哪些变换集合。

对于 ipsec-isakmp 加密映射表，可以使用此命令列出多个变换集合。首先列出的是最高优先级的变换集合。

如果是本地路由器发起协商，那么将按照在加密映射表中指定的顺序将变换集合提供给对端。如果是对端发起协商，那么本地路由器接受第一个相匹配的变换集合。

在两端找到的第一个相匹配的变换集合将用于建立安全联盟。如果没有找到匹配项，那么 IPSec 不会建立安全联盟。报文将被丢弃，因为没有安全联盟保护这些通信。

对于 ipsec-manual 加密映射表，只能指定唯一的变换集合。如果此变换集合不能匹配对端的加密映射表的变换集合，则 IPSec 两端不能正常通信，因为它们使用不同的规则来保护通信。

如果想要改变变换集合的内容，重新设置变换集合的内容来覆盖旧的内容。此改变不会影响现存的安全联盟，但将用于建立新的安全联盟。如果想让改变尽快生效，可以使用 clear crypto sa 命令来清除全部或部分安全联盟数据库的内容。

包含在一个加密映射表中的任何变换集合都必须事先用 crypto ipsec transform-set 命令进行定义。

示例

下面的例子定义了两个变换集合，并且指定它们可用于同一个加密映射表（只有当使用 IKE 来建立安全联盟时，此例子才能使用。对于手工建立的安全联盟所使用的加密映射表，给定的一条加密映射表中只能包含一个变换集合）。

```
crypto ipsec transform-set one
transform-type esp-des esp-sha-hmac
crypto ipsec transform-set one esp-des esp-sha-hmac

crypto ipsec transform-set two
transform-type ah-sha-hmac esp-des esp-sha-hmac
crypto ipsec transform-set two esp-des esp-sha-hmac

crypto map aaa 100 ipsec-isakmp
```

match address aaa
set transform-set one two
set peer 192..2.2.1

在此例中，当通信匹配了访问列表 aaa 时，安全联盟既可以使用变换集合 one（第一优先级），也可以使用 two（第二优先级），这取决于哪个变换集合和对端上的变换集合相匹配。

相关命令

crypto map (global configuration)

crypto map (interface configuration)

crypto map local-address

match address

set peer

set pfs

set security-association lifetime

set security-association inbound

set security-association outbound

show crypto map

4.1.14 set session-key {inbound|outbound}

要在加密映射表中手工指定 IPSec 密钥，可以使用 set 加密映射表配置命令。要从加密映射表中删除 IPSec 密钥，可以使用此命令的 no 格式。此命令只对 ipsec-manual 加密映射表可用。

set session-key {*inbound*|*outbound*} *ah spi hex-key-string*

set session-key {*inbound*|*outbound*} *esp spi* [**cipher** *hex-key-string*] [**authenticator** *hex-key-string*]

参数

参数	参数说明
inbound	设置入报文IPSec密钥（必须对入报文和出报文密钥都进行设置）。
outbound	设置出报文IPSec密钥（必须对入报文和出报文密钥都进行设置）。
ah	为AH协议设置IPSec密钥。只有当此加密映射表的变换集合包括AH变换时才起作用。
esp	为ESP协议设置IPSec密钥。只有当此加密映射表的变换集合包括ESP变换时才起作用。
spi	安全参数索引值（SPI），此索引用来唯一标识一个安全联盟。SPI是在256到4,294,967,295（FFFFFFFF）之间任意给定的一个数字。对于两种方向（出、入）和两种协议（AH、ESP）的安全联盟，可以赋给同一SPI。对于一个给

	定目的地址/协议的组合，必须使用唯一的SPI值。如果是入站的情况，那么目的地址就是本路由器地址。如果是出站，那么目的地址就是对端的地址。
hex-key-string	密钥；按十六进制的格式输入。这是一个长度为8、16、20或24字节的任意十六进制字符串。如果加密映射表的变换集合包括了DES算法，那么每个密钥至少需要8字节。如果加密映射表的变换集合包括了3DES算法，那么每个密钥至少需要24字节。如果加密映射表的变换集合包括了MD5算法，那么每个密钥至少需要16字节。如果加密映射表的变换集合包括了SHA算法，那么每个密钥至少需要20字节。超过上述长度的密钥将简单地被截断。
cipher	指示此密钥字符串是ESP加密变换的密钥。
authenticator	（可选）指示此密钥字符串是ESP验证变换的密钥。此参数仅当这个加密映射表的变换集合包括了ESP验证算法时才需要。

缺省

缺省情况下不定义任何 IPSec 密钥。

命令模式

加密映射表配置态

使用说明

使用此命令可以为那些经过 ipsec-manual 加密映射表建立起来的安全联盟指定 IPSec 密钥(对于 ipsec-isakmp 加密映射表,安全联盟以及相应密钥是通过 IKE 协商自动建立的)。

如果加密映射表的变换集合包括了 AH 协议，那么必须为 AH 的出和入通信都定义 IPSec 密钥。如果加密映射表的变换集合包括了 ESP 加密协议，那么必须为 ESP 加密的出和入通信都定义 IPSec 密钥。如果加密映射表的变换集合包括了 ESP 验证协议，那么必须为 ESP 验证的出和入通信都定义 IPSec 密钥。

在为一个加密映射表定义多个 IPSec 密钥的时候，可以将相同的 SPI 数字赋给所有的密钥。SPI 用于标识此加密映射表所对应的安全联盟。但是，不是所有的 SPI 赋值上都有相同的随意性，应确保对于相同的目的地址/协议的组合，相同的 SPI 赋值不超过一次。

通过这条命令建立起来的安全联盟不会超时（不同于通过 IKE 建立起来的安全联盟）。

本端的密钥必须和对端密钥相匹配。如果改变一个密钥，那么使用此密钥的安全联盟将被删除和重新增加。

ipsec-manual map 没有 security-association 以及 set pfs 的配置

示例

下面的例子经过手工建立安全联盟的加密映射表。变换集合 one 只包含了一个 AH 协议。

```
crypto ipsec transform-set one
transform-set ah-md5-hmac
crypto ipsec transform-set one ah-md5-hmac

crypto map aaa 100 ipsec-manual
match address aaa
set transform-set one
```

```
set peer 192.2.2.1
set security-association inbound ah 300 11111111111111111111111111111111
set security-association outbound ah 300 22222222222222222222222222222222
```

下面的例子是一个手工建立安全联盟的加密映射表。变换集合 one 包含了一个 AH 协议和一个 ESP 协议。这样，对 AH 和 ESP 的出和入通信都要配置密钥。此变换集合包括了 ESP 的加密和验证变换，所以需要使用 cipher 和 authenticator 关键字对两种变换都创建密钥。

```
crypto ipsec transform-set one
transform-type ah-sha-hmac esp-des esp-sha-hmac
crypto ipsec transform-set one ah-sha-hmac esp-des esp-sha-hmac

crypto map aaa 100 ipsec-manual
match address aaa
set transform-set one
set peer 192.2.2.1
set association inbound ah 300 98765432109876543210987654321098765432 10
set security-association outbound ah 300 fedcbafedcbafedcbafedcbafedcbafedcbafedcba
fedc
set security-association inbound esp 300 cipher 0123456789012345
authenticator 00001111222233334444555566667777888899999
set security-association outbound esp 300 cipher abcdefabcdefabcd
authenticator 99998888777766665555444433332222111100000
```

相关命令

crypto map(global configuration)

crypto map(interface configuration)

crypto map local-address

match address

set peer

set transform-set

show crypto map

4.1.15 crypto dynamic-map

要创建或修改一个动态加密映射表，进入动态加密映射表表配置态，可以使用 crypto dynamic-map 全局配置命令。使用此命令的 no 格式来删除一个动态加密映射表表或集合。

crypto dynamic-map *map-name seq-num*

no crypto dynamic-map *map-name seq-num*

参数

参数	参数说明
map-name	动态加密映射表集合的名字。

Seq-num	动态加密映射表集合的序列号

缺省

不存在动态加密映射表。

命令模式

全局配置态。使用此命令将进入动态加密映射表配置态。

使用说明

使用此命令可以创建一个新的动态加密映射表，或修改一个现存的动态加密映射表。

动态加密映射表的功能和普通的加密映射表（crypto map)是类似的。主要区别在于：

动态加密映射表中可以不用设置对端的 IP 地址（set peer），允许任何地址的 IPSec 设备来协商，这一功能可以用来支持和移动用户的连接。而普通的加密映射表则必须指定对端的 IP 地址，且只允许该地址的 IPSec 设备来协商。当然动态加密映射表中也可以设置 IP 地址，这种情况下，基本等同于普通的加密映射表。

dynamic map 的配置和 ipsec-isakmp 一样，不过完整性约束很低

示例

下面的例子显示了使用 IKE 来建立安全联盟时，所需的最小加密映射表配置：

```
crypto dynamic-map aaa
match address aaa
set transform-set one
```

相关命令

crypto map (global configuration)

match address

set peer

set pfs

set security-association lifetime

set transform-set

show crypto map

4.2 Crypto ipsec配置命令

4.2.1 crypto ipsec df-bit

要规定如何在 ipsec tunnel mode 外层 ip header 里设定 df bit，可以使用 crypto ipsec df-bit 全局配置命令。使用此命令的 no 格式来恢复默认设定。

crypto ipsec df-bit {clear / set / copy}

no crypto ipsec df-bit

参数

参数	参数说明
clear	无论内层报文如何设定，外层报头不设定df bit
Set	如果在tunnel 增加报头之后，确实超过了pmtu，则必须在外层报头里设定df bit
copy	如果内层报文头设定了df bit，那么外层报文头也要设定

缺省

df-bit copy

命令模式

全局配置态。

使用说明

该命令的使用主要取决于用户是否希望发送大于 Pmtu 的报文,如果希望,就要设定成 clear,但是必须考虑到由此带来的分片和组包操作,会影响系统的性能.

示例

```
router# configure
router(config)# crypto ipsec df-bit clear
```

相关命令

crypto ipsec transform-set

mode tunnel

4.2.2 crypto ipsec fragmentation (暂时不支持)

要规定在需要对报文做分片时，是在加密前分片,还是加密后分片，可以使用 crypto ipsec fragmentation 全局配置命令。使用此命令的 no 格式来恢复默认设定。

crypto ipsec fragment {after-encryption / before-encryption}

no crypto ipsec fragment

参数

参数	参数说明
before-encryption	在encap之前，对报文进行分片，然后做encap 和encrypt. 判断报文是否需要分片，需要估计报文在完成encap以及encrypt之后的长度

After-encryption	在完成encap和所有sa 保护后，再对报文做分片

缺省

crypto ipsec fragment After-encryption

命令模式

全局配置态。

使用说明

开启预分片功能,可以使网关只是专注于解密，解封装和转发，而将组包的工作交给 host, 或上层应用，对系统的效率是有一定帮助的.

示例

```
router# configure
router(config)# crypto ipsec fragmentation before-fragmentation
```

相关命令

crypto ipsec transform-set

mode tunnel

4.2.3 crypto ipsec security-association idle-time

配置全局 security-association idle-time 属性，可以使用 crypto ipsec security-association idle-time 全局配置命令。使用此命令的 no 格式来恢复默认设定。

crypto ipsec security-association idle-time <60-86400>

no crypto ipsec fragment security-association idle-time

参数

参数	参数说明
seconds *seconds*	指定所有安全联盟在没有收到报文多久后超时终止存活的秒数。

缺省

没有 idle time 配置

命令模式

全局配置态。

使用说明

全局配置 sa 的 idle timeout 时间，如果加密映射表没有设定 sa idle time，那么就使用全局的设定．否则,使用加密映射表自己配置的 sa idle time

工作原理见 set security-association idle-time

示例

```
router# configure
router(config)# crypto ipsec security-association idle-time 600
```

相关命令

clear crypto ipsec sa

clear crypto sa ipsec

crypto ipsec security-association lifetime

set security-association idle-time

4.2.4 crypto ipsec security-association lifetime

配置全局 security-association lifetime 属性，可以使用 crypto ipsec security-association lifetime 全局配置命令。使用此命令的 no 格式来恢复默认设定。

crypto ipsec security-association lifetime [**seconds** *seconds* | **kilobytes** *kilobytes*]

no crypto ipsec security-association lifetime [**seconds** | **kilobytes**]

参数

参数	参数说明
seconds *seconds*	指定一个安全联盟在超时终止前所能存活的秒数。
kilobytes *kilobytes*	在一个安全联盟超时以前，使用此安全联盟所能传输的通信量（以千字节计）。

缺省

缺省超时秒数为 28800 秒（1 小时），缺省超时通信量为 2560000 千字节。

命令模式

全局配置态。

使用说明

全局配置sa 的lifetime 时间，如果加密映射表没有设定litetime，那么就使用全局的设定.否则,使用加密映射表自己配置的sa lifetime

工作原理见set security-association lifetime

示例

```
router# configure
router(config)# crypto ipsec security-association lifetime seconds 2700
router(config)# crypto ipsec security-association lifetime kilobytes 2304000
```

相关命令

clear crypto ipsec sa

clear crypto sa ipsec

crypto ipsec security-association idle-time

set security-association lifetime

4.2.5 crypto ipsec security-association replay

配置全局security-association replay属性，可以使用crypto ipsec security-association replay全局配置命令。使用此命令的no格式来恢复默认设定。

crypto ipsec security-association replay [disable| window-size [1024/128/256/64]**]**

no crypto ipsec security-association replay [disable| window-size]

参数

参数	参数说明
disable	取消抗重播功能
Window-size 1024/128/256/64	指定抗重播窗口的大小

缺省

开启抗重播功能，窗口大小为64

命令模式

全局配置态。

使用说明

全局配置 sa 的 replay 配置，如果加密映射表没有设定 replay，那么就使用全局的设定. 否则，使用加密映射表自己配置的 sa replay

工作原理见 set security-association replay

示例

```
router# configure
router(config)# cry ipsec security-association replay disable
router(config)# cry ipsec security-association replay window-size 512
```

相关命令

clear crypto ipsec sa

clear crypto sa ipsec

cry ipsec security-association replay

4.2.6 crypto ipsec nat-transparency

配置全局 nat 穿越属性，可以使用 crypto ipsec nat-transparency 全局配置命令。使用此命令的 no 格式来恢复默认设定。

crypto ipsec nat-transparency [spi-matching| udp-encapsulation]

no crypto ipsec nat-transparency [spi-matching| udp-encapsulation]

参数

参数	参数说明
udp-encapsulation	通过外层封装udp包头的方式实现nat 穿越
spi-matching	通过spi 标识区分来实现nat 穿越，还未实现

缺省

udp-encapsulation

命令模式

全局配置态。

使用说明

如果建立 ipsec vpn 的两端，有一端或两端在 nat 设备之后，那么由于经过 nat 时会改变报文头部信息，导致接受端的认证检查失败．失败的原因有以下几种

1. AH 报文对整体报文做了完整性检查, nat 对报文的任何改动都会造成接收端检查失败
2. esp transport mode 时，如果 tcp 报文，那么 nat 会修改 tcp checksum，从而破坏 esp 的加密数据，导致接收端解密失败
3. esp tunnel mode 时，虽然可以通过仅有 Ip address translation 的 nat，但如果是 port translation，就一样会造成 esp 加密数据被修改.

Udp-encapsulation 的解决方法就是无论 transport mode 还是 tunnel mode 都会在报文最外层的 ip 头之后附加一个 udp 头，使得 port translation 也可以让 esp 报文加密部分不经修改的通过．而接收端也会做相应的 udp decap 工作．至于转换成什么端口，会在 ike 协商阶段确定下来. (协商 nat 的过程，可以参考 ipsec 白皮书).

对于 ah，目前没有任何方法帮助它穿越 nat

在使用 nat-transparency 时，注意同时要配置 crypto isakmp nat keepalive 命令，因为如果 nat 上的 cache 如果超时，那么从外网主动发起的报文就无法通过 nat 设备

示例

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key 1234 address 56.0.0.1
crypto isakmp nat keepalive 20
!
!
crypto ipsec transform-set t2 esp-des esp-sha-hmac
!
crypto map test2 10 ipsec-isakmp
 set peer 56.0.0.1
 set transform-set t2
match address 101
```

nat-transparency udp-encapsulation 默认情况下是启用的， 所以请不要配置这句话

相关命令

crypto isakmp nat keepalive

4.2.7 crypto ipsec transform-set

要定义一个 ipsec 变换集合——安全协议和算法的一个可行组合，使用 crypto ipsec transform-set 全局配置命令。要删除一个变换集合，可以使用这条命令的 no 格式。

crypto ipsec transform-set *transform-set-name*[[ah-md5-hmac| ah-sha-hmac][esp-3des| esp-aes| esp-des| esp-null| esp-seal][esp-md5-hmac| esp-sha-hmac][comp-lzs]]

no crypto ipsec transform-set *transform-set-name*

参数

参数	参数说明
transform-set-name	指定要创建（或修改）的变换集合的名称。
ah-md5-hmac| ah-sha-hmac	设定ah 使用的认证算法
esp-3des| esp-aes| esp-des| esp-null| esp-seal	设定esp使用的加密算法
esp-md5-hmac| esp-sha-hmac	设定esp使用的认证算法
comp-lzs	设定压缩算法

缺省

无

命令模式

全局配置态。执行此命令将进入加密变换配置态。

使用说明

变换集合是安全协议、算法以及将用于受 IPSec 保护的通信的其它设置的组合。

可以配置多个变换集合，然后在加密映射表中指定这些变换集合中的一个或多个。在加密映射表中定义的变换集合用于协商 IPSec 安全联盟，以保护匹配加密映射表设定的访问列表的那些报文。在协商过程中，双方寻找一个在双方都有的相同变换集合。当找到了一个这样的变换集合时，此集合将被选中，并作为双方 IPSec 安全联盟的一部分被运用到受保护的通信上。

如果不是使用 IKE 来建立安全联盟，那么必须指定唯一一个变换集合。此集合无须进行协商。

只有使用此命令对变换集合进行了定义后，此变换集合才能被设置在加密映射表中。

示例

以下例子定义了一个变换集合。

```
crypto ipsec transform-set one esp-des esp-sha-hmac
```

mode transport

相关命令

mode

set transform-set

show crypto ipsec transform-set

4.2.8 mode

要改变一个变换集合的模式，可以使用 mode 加密变换配置命令。要将模式恢复成缺省值隧道模式，可以使用这条命令的 no 格式。

mode {tunnel | transport}

no mode

参数

参数	参数说明
tunnel| transport	指定一个变换集合的模式：隧道模式或传输模式。如果既没有指定tunnel，也没有指定transport，那么将使用缺省值（隧道模式）。

缺省

隧道模式

命令模式

加密变换配置态

使用说明

使用此命令来改变变换的模式。只有当要被保护的报文和 IPSec 两端有相同的 IP 地址值时（这样的通信既可在隧道模式下又可在传输模式下进行封装），此设置才有效。对于所有其它通信（所有其它的通信都在隧道模式下进行封装），此设置都无效。

如果要被保护的通信具有和 IPSec 两端有相同的 IP 地址，并且指定了传输模式，那么在协商期间，路由器将申请传输模式，但既可接受传输模式又可接受隧道模式。如果指定了隧道模式，那么路由器将申请隧道模式，并且只接受隧道模式。

如果要被保护的通信和 IPSec 两端有不相同的 IP 地址，并且指定了传输模式，那么在协商期间，路由器将申请隧道模式。

在定义了变换集合以后，将进入加密变换配置态。在此配置状态下，可以将模式改变为隧道方式或传输方式。

如果开始在定义变换集合的时候没有设置模式，以后想要改变此变换集合的模式，那么必须重新进入此变换集合（指定变换的名字），并且改变它的模式。

如果使用此命令来改变模式，那么改变将只影响那些指定了此变换集合的加密映射表的后续 IPSec 安全联盟的生成。如果想尽快使变换集合的配置生效，那么可以清除安全联盟数据库的部分或全部。可以参看 clear crypto sa 命令来获得更多的细节。

- 隧道模式

  在隧道模式下，整个原始的 IP 报文都受到保护（加密、验证或两者都有），并且由 IPSec 进行封装（ESP、AH 或两者都有）。然后，新的 IP 头被在增加到报文中，此 IP 头指定了 IPSec 源和目的地址。

  任何 IP 通信都可使用隧道模式进行传送。如果 IPSec 是对接在 IPSec 两端后面的主机的通信进行保护，那么必须使用隧道模式。

- 传输模式

  在传输模式下，只有 IP 分组的有效负载（数据）才受到保护（加密、验证或两者都有）。并且由 IPSec 封装（ESP、AH 或两者都有）。原始的 IP 报头保持原样，不受 IPSec 的保护。

  只有当要保护的 IP 分组的源和目的地址都是 IPSec 两端时，才能使用传输模式。例如，可以使用传输模式来保护路由器管理通信。在申请中指定传输模式，可以使得路由器能够和远端协商决定是使用传输模式还是隧道模式。

示例

下面的例子定义了一个变换集合，并将模式改变为传输模式。

```
router_config# crypto ipsec transform-set one esp-des esp-sha-hmac
router_config_crypto_trans # mode transport
router_config_crypto_trans # exit
router_config#
```

相关命令

crypto ipsec transform-set

4.2.9 crypto ipsec ipsec6-enable

crypto ipsec ipsec6-enable

在ipv6 上使能ipsec功能。使用此命令的no格式来取消ipv6 的ipsec功能。

crypto ipsec ipsec6-enable

no crypto ipsec ipsec6-enable

参数

无

缺省

不开启ipv6 的ipsec功能

命令模式

全局配置态。

使用说明

该命令的使用是在ipv6 上开启ipsec功能，提供ipsec加密保护

示例

```
router# configure
```

```
router(config)# crypto ipsec ipsec6-enable
```

相关命令

4.3 ipsec 相关的show, clear, debug命令

4.3.1 show crypto ipsec transform-set

要查看所配置的变换集合，可以使用 show crypto ipsec transform-set 命令。

show crypto ipsec transform-set [*transform-set-name*]

参数

参数	参数说明
transform-set-name	(可选)只显示具有所指定的transform-set-name的变换集合。

缺省

如果不使用关键字，那么将显示路由器上所有的变换集合。

命令模式

管理态

使用说明

无

示例

下面是 show crypto ipsec transform-set 命令的一个输出示例。

```
router# show crypto ipsec transform-set
Transform set aaa: { esp-des }
will negotiate ={ Tunnel }
Transform set bbb: { ah-md5-hmac esp-3des }
will negotiate ={ Tunnel }
```

相关命令

无

4.3.2 show crypto map

要查看所配置的加密映射表，可以使用 show crypto map 命令。

show crypto map [*map name*]

参数

参数	参数说明
map-name	(可选)只显示具有所指定的map-name的加密映射表。

缺省

如果不使用关键字，那么将显示路由器上所有的加密映射表。

命令模式

管理态

使用说明

无

示例

下面是 show crypto map 命令的一个输出示例。

```
router# show crypto map-name
Crypto Map m 1 ipsec-isakmp
acl name :101,       exist : 0
  peer = 172.16.20.101
    no PFS
    Security association ---    idle_time : 0, level_per_host enable:0, lifetime in
kilobyte : 2560000, lifetime in seconds : 28800, replay window size :64,sa repla
y enable :1
        Transform sets={ t1,    }

sub map incompleted
```

相关命令

无

4.3.3 show crypto dynamic-map

要查看所配置的动态加密映射表，可以使用 show crypto dynamic-map 命令。

show crypto dynamic-map [*map name*]

参数

参数	参数说明
map-name	(可选)只显示具有所指定的map-name的动态加密映射表。

缺省

如果不使用关键字，那么将显示路由器上所有的动态加密映射表。

命令模式

管理态

使用说明

无

示例

下面是 show crypto dynamic-map 命令的一个输出示例。

```
Router_config#show crypto dynamic-map
dynamic map dyn
Crypto Map dyn 10 ipsec-isakmp
acl name :101,       exist : 0
   no PFS
   Security association ---   idle_time : 0, level_per_host enable:0, lifetime in
kilobyte : 2560000, lifetime in seconds : 5000, replay window size :64,sa replay
  enable :1
        Transform sets={}
```

相关命令

无

4.3.4 show crypto sa isakmp

要查看当前第一阶段安全联盟所使用的设置，可以使用 show crypto sa isakmp 命令。

show crypto sa isakmp

参数

缺省

如果没有指定任何关键字，那么所有的安全联盟都将被显示出来。

命令模式

管理态

使用说明

无

示例

相关命令

无

4.3.5 show crypto sa ipsec

要查看当前第二阶段安全联盟所使用的设置，可以使用 show crypto sa ipsec 命令。

show crypto sa ipsec

参数

参数	参数说明
interface *interface-id*	（可选）显示标识接口上加密映射表所创建的现存的安全联盟。

缺省

如果没有指定任何关键字，那么所有的安全联盟都将被显示出来。

命令模式

管理态

使用说明

无

示例

下面是 show crypto sa ipsec 命令的一个输出示例。

```
Router_config#show crypto sa ipsec
sa bundle property
sa type : negotiation
diID : 4
local addr : 172.16.20.102
peer addr : 172.16.20.101
mode :1
nat use :0
```

```
port :500
refcnt : 0
sa status using
life left : 3491d
kilobytes life left : 4607872d

sa property
protocol id : 51
inbound spi : d0ef8dff
inbound auth id : 1
inbound crypto id : 0
outbound spi : 8696e777
outbound auth id : 1
outbound crypto id : 0
sa recv success bytes 0
sa send success bytes 128
sa recv err bytes 0
sa send err bytes 0

sa bundle property
sa type : negotiation
diID : 4
local addr : 172.16.20.102
peer addr : 172.16.20.101
mode :1
nat use :0
port :500
refcnt : 0
sa status using
life left : 3329d
kilobytes life left : 4608000d

sa property
protocol id : 51
inbound spi : db31bbcf
```

```
inbound auth id : 1
inbound crypto id : 0
outbound spi : 93d5f2bc
outbound auth id : 1
outbound crypto id : 0
sa recv success bytes 0
sa send success bytes 0
sa recv err bytes 0
sa send err bytes 0

sa bundle property
sa type : negotiation
diID : 4
local addr : 172.16.20.102
peer addr : 172.16.20.101
mode :1
nat use :0
port :500
refcnt : 0
sa status using
life left : 28411d
kilobytes life left : 2559756d

sa property
protocol id : 51
inbound spi : eb95a3a7
inbound auth id : 1
inbound crypto id : 0
outbound spi : 5e78e6b9
outbound auth id : 1
outbound crypto id : 0
sa recv success bytes 100
sa send success bytes 144
sa recv err bytes 0
sa send err bytes 0
```

相关命令

无

4.3.6 clear crypto sa

要删除相关的 IPSec 安全联盟数据库，使用 clear crypto sa 命令。

clear crypto sa [isakmp[ip-address] | ipsec[interface | ip-address]]

clear crypto sa [isakmp｜ipsec]

参数

参数	参数说明
isakmp	删除所有第一阶段sa
Ipsec	删除所有第二阶段sa
ip-address	指定对端的IP地址。(暂时不支持)
interfacee	指定建立sa的端口。(暂时不支持)

缺省

如果未使用 isakmp, ipsec 等关键字，所有的 IPSec 安全联盟都将被删除。

命令模式

管理态

使用说明

这条命令用于清除（删除）IPSec 安全联盟。如果安全联盟是通过 IKE 建立的，那么它们将被删除，以后的 IPSec 通信需要重新协商新的安全联盟（使用 IKE 时，IPSec 安全联盟只有在需要的时候才被建立）。

如果安全联盟是通过手工建立的，那么安全联盟将被删除并且被重新建立。

如果没有使用关键字，所有的 IPSec 安全联盟都将被删除。使用 peer 关键字将删除指定对端地址的全部 IPSec 安全联盟。使用 interface 关键字将删除在这个端口上所创建的全部 IPSec 安全联盟。通过使用 clear crypto sa 命令可以重新建立所有的安全联盟，这样这些联盟就可以使用最新的配置设置了。在手工建立安全联盟的情况下，如果修改其用到变换集合，在生效之前必须使用 clear crypto sa 命令。

如果路由器正在处理 IPSec 通信，那么最好只清除安全联盟数据库中会被影响到的那部分内容。这样可以避免当前正在进行的 IPSec 通信突然中断。

注意 clear crypto sa isakmp 在清除第一阶段安全联盟之前,还会清除掉对应的 IKE 协商状态.

示例

下面的示例清除路由器上所有的 IPsec 安全联盟：

clear crypto sa

相关命令

4.3.7 debug crypto

在 IPSec 的处理过程中，查看 IPSec 的调试信息。

debug crypto control
debug crypto isakmp
debug crypto packet
debug crypto sadb

参数

无

缺省

缺省情况下不显示调试信息。

命令模式

管理态

使用说明

debug crypto control 会显示配置中的错误

debug crypto isakmp 会显示 IKE 协商过程中的流程以及错误

debug crypto packet 显示 esp/ah 报文收发以及加解密阶段的流程以及错误信息

debug crypto sadb 显示 sadb 建立，查找，删除时的流程以及错误信息.

显示和 IPSec 处理相关的一些重要错误信息，下表列举了几种常见的出错信息。

显示信息	信息含义
rec'd IPSEC packet from IPADDR has invalid spi.	对端的outbound的spi值与本端的inbound不同或配置的配置策略不同（esp、ah）。
packet missing policy.	对端的outbound的配置策略和本地不同（esp、ah）。
rec'd IPSEC packet from IPADDR has bad pading.	对端的outbound的加密密钥与本端的inbound的不同。

rec'd IPSEC packet mac verify failed.	对端的outbound的ESP或AH验证密钥与本端的inbound的不同。
rec'd IPSEC packet from IPADDR to IPADDR does not agree with policy.	IPSEC处理完成的包与相应的access-list不同，子MAP的访问列表配置有问题。

相关命令

第5章 Internet 密钥交换安全协议命令

5.1 IKE配置命令

本章讨论 Internet 密钥交换安全协议（IKE）的命令。

IKE 是一种密钥管理协议标准，与 IPSec 协议结合使用。

通过 crypto isakmp enable 命令，IPSec 可以选择使用或者不使用 IKE 协商建立 SA，但是 IKE 通过提供额外的功能、灵活性以及对 IPSec 标准配置的简化，增强了 IPSec 的功能。

IKE 是一种混合协议，在因特网安全协会及密钥管理协议（ISAKMP）框架内实现了 Oakley 密钥交换和 Skeme 密钥交换（ISAKMP，Oakley 和 Skeme 是由 IKE 实现的安全协议）。

5.1.1 crypto isakmp enable

要选择启用 IKE 协商生成 SA，使用全局配置命令 crypto isakmp enable。要选择禁用 IKE 协商，在这个全局配置命令前加 no 前缀。

(no) crypto isakmp enable

参数

无

缺省

默认情况下，允许 IKE 进行协商，即 enable IKE。

命令模式

全局配置态

使用说明

使用该命令启用或禁用 IKE。

示例

无

相关命令

无

5.1.2 crypto isakmp identity

要定义参与 IKE 协商时使用的设备身份标识类型，使用全局配置态下的 crypto isakmp identity 命令。当你指定预共享密钥时，用以指定 ISAKMP 的身份标识。要将 ISAKMP 身份标识重置成默认值（IP 地址），在这个全局配置命令前加 no 前缀。

crypto isakmp identity {address|hostname}

no crypto isakmp identity

参数

参数	参数说明
address	设置在IKE协商过程中使用设备接口的IP地址作为ISAKMP的身份标识。
hostname	设置在IKE协商过程中使用设备的主机名或域名作为ISAKMP的身份标识。

缺省

默认使用 IP 地址作为设备的 ISAKMP 身份标识。

命令模式

全局配置态

使用说明

address 关键字通常用于设备只有一个接口会用于 IKE 协商，且这个接口的 IP 地址已知的情况下。

hostname 关键字通常用于设备可能有多个接口用于 IKE 协商，或者这些接口的 IP 地址未知的情况下（如接口的 IP 地址是动态分配的）。

作为一个通用的规则，你通常应当将参与 IKE 协商的所有设备身份标识设置为相同的类型。

示例

下面的示例在两端设备上配置了预共享密钥并使用 IP 地址作为 ISAKMP 的身份标识：

本地端（10.0.0.1）

```
crypto isakmp identity address
crypto isakmp key sharedkeystring address 192.168.1.33
```

远端（192.168.1.33）

```
crypto isakmp identity address
crypto isakmp key sharedkeystring address 10.0.0.1
```

下面的示例在两端设备上配置了预共享密钥并使用主机名作为 ISAKMP 的身份标识：

本地端（10.0.0.1）

```
crypto isakmp identity hostname
crypto isakmp key sharedkeystring hostname remote.aacom.com
ip host name remote.aacom.com 192.168.1.33 192.168.1.34
```

本地端（192.168.1.33 192.168.1.34）

```
crypto isakmp identity hostname
crypto isakmp key sharedkeystring hostname local.aacom.com
ip host name local.aacom.com 10.0.0.1
```

相关命令

crypto isakmp identity

crypto isakmp key

ip host name

5.1.3 crypto isakmp invalid-spi-recovery

要配置设备通过 IKE SA 通知对端 IPSec 设备存在一个“非法 SPI”的错误，使用全局配置命令 crypto isakmp invalid-spi-recovery 命令。要禁止对这种情况产生通知，在这个全局配置命令前面加 no 前缀。

crypto isakmp invalid-spi-recovery

no crypto isakmp invalid-spi-recovery

参数

无

缺省

默认禁止产生这个通知。

命令模式

全局配置态

使用说明

IPsec 处理报文过程中，会出现"非法 SPI"的状况。Invalid SPI Recovery 要求 IKE 重新建立 SA，保证 IPsec 能够正常处理报文。重新建立 SA 前，IKE 会向引起"非法 SPI"的 IPsec 终端发送一个错误号是"Invalid SPI"的通知，终端收到这样的错误号后会删除本地的 SA（SA 已经失效），随后 IPsec 两端通过 IKE 重新协商一个新的 SA。一旦两端设备的 SADB 重新同步了，数据包也就能正常地通信不再被丢弃了。

示例

无

相关命令

无

5.1.4 crypto isakmp keepalive

要配置 IPSec DPD（dead peer detection）功能，使用全局配置命令 crypto isakmp keepalive。该命令用于当对端节点不可达时及时发现并清除本地存储的关于该节点的相关信息。使用该命令的 no 形式取消 IPSec DPD 配置。

crypto isakmp keepalive *seconds types*

no crypto isakmp keepalive

参数

参数	参数说明
Seconds	指定两次发送DPD消息的时间间隔。范围<10-3600>,单位:秒。
types	指定在什么情况下发送DPD消息，默认为on-demand。 <2-69> DPD探测失败时重试的次数； On-demand 仅在发送报文失败时发送DPD消息； periodic 在线路空闲时定期发送DPD消息

缺省

Seconds 的缺省值为 10.

Types 的缺省值为 on-demand.

DPD 探测失败时默认的重试次数为 5.

命令模式

全局配置态

使用说明

开启此功能时需要对端也支持 DPD（dead peer detection）。

示例

指定时间间隔为 10，失败重传次数为 5，类型为 on-demand 的 DPD 功能：

crypto isakmp keepalive 10 5

指定时间间隔为 10，失败重传次数为 5，类型为 periodic 的 DPD 功能：

crypto isakmp keepalive 10 5 periodic

取消 DPD 配置：

no crypto isakmp keepalive

相关命令

无

5.1.5 crypto isakmp key

要配置预共享认证密钥，使用全局配置命令 crypto isakmp key。无论何时只要在 IKE 策略中指定预共享密钥，都必须配置该密钥。使用该命令的 no 形式删除预共享认证密钥。

crypto isakmp key *keystring* {**address** *peer-address [mask]*|**hostname** *hostname*}

no crypto isakmp key *keystring* {**address** *peer-address [mask]*|**hostname** *hostname*}

参数

参数	参数说明
keystring	指定预共享密钥。使用最多128字节的字母数字字符的任意组合。该预共享密钥必须在两端上完全一样。
address	使用IP地址作为远端设备的ISAKMP身份标识。
peer-address	指定远端设备的IP地址。
mask	（可选）指定远端设备的子网掩码，只有当远端设备的ISAKMP身份标识设置为IP地址时才能配置子网掩码。
hostname *hostname*	指定远端设备的FQDN。

缺省

没有缺省的预共享认证密钥。

命令模式

全局配置态

使用说明

如果 IKE 策略中包括预共享密钥作为认证方法，这些预共享密钥必须在两端上配置；否则，该策略不能使用（IKE 过程将不会提交该策略用于匹配）。

示例

指定预共享密钥，并用 IP 地址指定远程终端：

crypto isakmp key abcdefghijkl 192.2.2.1

相关命令

authentication (IKE policy)

5.1.6 crypto isakmp nat keepalive

要允许设备发送 NAT keepalive 报文，使用全局配置命令 crypto isakmp nat keepalive。要禁止设备发送 NAT keepalive 报文，在这个全局配置命令前加 no 前缀。

crypto isakmp nat keepalive *seconds*

no crypto isakmp nat keepalive

参数

参数	参数说明
seconds	发送nat keepalive报文的时间间隔，单位为秒，取值范围5-3600。

缺省

Nat keepalive 关闭。

命令模式

全局配置态

使用说明

crypto isakmp nat keepalive 命令允许用户在两个 IPSec 对端设备通信期间保持动态 NAT 映射有效。当 IPSec 在一个指定的时间间隔没有发送或接收到数据包时就会发送 NAT keepalive 报文。

如果配置了这条命令，用户应当保证空闲时间的值小于 NAT 映射的有效时间。

示例

下面的示例指定每隔 20 秒发送 NAT keepalive 报文：

crypto isakmp keepalive 20

相关命令

无

5.1.7 crypto isakmp peer

要定义 IKE 策略，使用全局配置命令 crypto isakmp policy。IKE 策略定义一套参数在 IKE 协商期间使用。使用该命令的 no 形式来删除 IKE 策略。

crypto isakmp peer {**ip-address** *ip-address*|**fqdn** *fqdn*}

no crypto isakmp peer {**ip-address** *ip-address*|**fqdn** *fqdn*}

参数

参数	参数说明
ip-address *ip-address*	对端设备的IP地址。
fqdn *fqdn*	对端设备的FQDN

缺省

无

命令模式

全局配置态

使用说明

使用该命令配置 ISAKMP 协商过程中对端 IPSec 设备的 RADIUS 隧道属性。

使用此命令进入 ISAKMP 对端属性配置态(用 IKE peer 表示)，在 ISAKMP 对端属性配置态中，下面的命令在指定策略中的参数值是有效的：

set aggressive-mode client-endpoint(IKE peer);

set aggressive-mode password(IKE peer);

示例

下面的示例说明如何使用 RADIUS 隧道属性发起 aggressive mode 协商：

```
crypto isakmp peer address 1.1.1.1
set aggressive-mode client-endpoint user-fqdn user@test.com
set aggressive-mode password hello
```

相关命令

无

5.1.8 crypto isakmp policy

要定义 IKE 策略，使用全局配置命令 crypto isakmp policy。IKE 策略定义一套参数在 IKE 协商期间使用。使用该命令的 no 形式来删除 IKE 策略。

crypto isakmp policy *priority*

no crypto isakmp policy *priority*

参数

参数	参数说明
priority	标识IKE策略的优先级。使用1到10000的整数，1是最高优先级而10000是最低优先级。

缺省

存在一条缺省的策略，该策略总是最低优先级。这条缺省的策略中加密、哈希、认证，Diffie-Hellman 组和生命期参数均为缺省值。

在创建一条 IKE 策略时，如果不给特定参数指定值，则该参数使用缺省值。

命令模式

全局配置态

使用说明

使用该命令指定在 IKE 协商期间要使用的参数（这些参数用来创建 IKE SA）。

使用此命令进入 ISAKMP 策略配置态(用 IKE policy 表示)，在 ISAKMP 策略配置态中，下面的命令在指定策略中的参数值是有效的：

encryption(IKE policy);缺省值=56 比特 DES-CBC

hash(IKE policy); 缺省值=SHA-1

authentication(IKE policy); 缺省值=Pre-Shared Key

group(IKE policy); 缺省值=768 比特 Diffie-Hellman

lifetime(IKE policy); 缺省值=86400 秒

如果不给策略指定这些命令中的某一个，则将使用该参数的缺省值。

可以给参与 IPSec 的两端配置多个 IKE 策略。在 IKE 协商开始时，将试图找到在两端配置的公共策略，从对端上所指定的最高优先级的策略开始。

示例

下面的示例配置两条 ISAKMP 策略：

```
crypto isakmp policy 10
hash md5
authentication pre-share
group 2
lifetime 5000
crypto isakmp policy 20
authentication pre-share
lifetime 10000
```

相关命令

authentication(IKE policy)

encryption(IKE policy)

group(IKE policy)

hash(IKE policy)

lifetime(IKE policy)

show crypto isakmp policy

1. authentication(IKE policy)

要在 IKE 策略中指定认证方法，使用 ISAKMP 策略配置命令 authentication(IKE policy)。IKE 策略定义一组在 IKE 协商期间使用的参数。使用该命令的 no 形式来恢复认证方法的缺省值。

authentication { **pre-share**|**rsa-sig**|**rsa-encr**}

no authentication { **pre-share**|**rsa-sig**|**rsa-encr**}

参数

参数	参数说明
pre-share	指定预共享密钥作为认证方法。
rsa-sig	指定RSA签名作为认证方法。
rsa-encr	指定RSA实时加密作为认证方法。

缺省

预共享密钥认证方法

命令模式

ISAKMP 策略配置态

使用说明

使用该命令指定用在 IKE 策略中的认证方法。

指定预共享密钥，则必须同时分别配置这些预共享密钥（crypto isakmp key 命令）。

示例

本例配置 IKE 策略，使用预共享密钥作为其认证方法（所有其它参数为缺省值）：

```
router_config#crypto isakmp policy 10
router_config_isakmp# authentication pre-share
router_config_isakmp# exit
router_config #
```

相关命令

crypto isakmp key

crypto isakmp policy

encryption(IKE policy)

group(IKE policy)

hash(IKE policy)

lifetime(IKE policy)

2. encryption(IKE policy)

要在 IKE 策略内指定加密算法，使用 ISAKMP 策略配置命令 encryption(IKE policy)。IKE 策略定义一套参数，在 IKE 协商期间使用这些参数。使用该命令的 no 形式恢复加密算法为缺省值。

encryption {**des**|**3des**}

no encryption {**des**|**3des**}

参数

参数	参数说明
des	指定DES作为加密算法。
3des	指定3DES作为加密算法。

缺省

DES 加密算法。

命令模式

ISAKMP 策略配置态

使用说明

使用该命令指定在 IKE 策略中使用的加密算法。

示例

本示例配置 IKE 策略中加密算法为 DES 加密算法（所有其它参数设置为缺省值）：

```
router_config# crypto isakmp policy 10
router_config_isakmp# encryption des
router_config_isakmp# exit
router_config#
```

相关命令

authentication(IKE policy)

crypto isakmp policy

group(IKE policy)

hash(IKE policy)

lifetime(IKE policy)

3. group(IKE policy)

要在 IKE 策略内指定 Diffie-Hellman 组，使用 ISAKMP 策略配置命令 group(IKE policy)。IKE 策略定义一套参数，在 IKE 协商期间使用这些参数。使用该命令的 no 形式恢复 Diffie-Hellman 组为缺省值。

group {**1**|**2**}

no group {**1**|**2**}

参数

参数	参数说明
1	指定768比特Diffie-Hellman组。
2	指定1024比特Diffie-Hellman组。

缺省

768 比特 Diffie-Hellman 组（group 1）。

命令模式

ISAKMP 策略配置态

使用说明

使用该命令指定 IKE 策略中使用的 Diffie-Hellman 组。

示例

本示例配置 IKE 策略为 1024 比特 Diffie-Hellman 组（所有其它参数设置为缺省值）：

```
router_config# crypto isakmp policy 10
router_config _isakmp# group 2
router_config _isakmp# exit
router_config#
```

相关命令

crypto isakmp policy

authentication(IKE policy)

encryption(IKE policy)

hash(IKE policy)

lifetime(IKE policy)

4. hash(IKE policy)

要在 IKE 策略内指定哈氏算法，使用 ISAKMP 策略配置命令 hash(IKEpolicy)。IKE 策略定义一套参数，在 IKE 协商期间使用这些参数。使用该命令的 no 形式恢复哈希算法为缺省的 SHA-1 哈希算法。

hash {**sha**|**md5**}

no hash {**sha**|**md5**}

参数

参数	参数说明
sha	指定SHA-1(HMAC变体)作为哈希算法。
md5	指定MD5(HMAC变体)作为哈希算法。

缺省

SHA-1 哈希算法

命令模式

ISAKMP 策略配置态

使用说明

使用该命令指定 IKE 策略中使用的哈希算法。

示例

本示例配置 IKE 策略为使用 MD5 哈希算法（所有其它参数设置为缺省值）：

```
router_config # crypto isakmp policy 10
router_config _isakmp# hash md5
router_config _isakmp# exit
router_config#
```

相关命令

crypto isakmp policy

authentication(IKE policy)

encryption(IKE policy)

group(IKE policy)

lifetime(IKE policy)

5. lifetime(IKE policy)

要描述 IKE SA 的生命期，使用 ISAKMP 策略配置命令 lifetime(IKE policy)。使用该命令的 no 形式恢复 SA 生命期为缺省值。

lifetime *seconds*

no lifetime *seconds*

参数

参数	参数说明
seconds	指定每个IKE SA在失效之前存在的秒数。使用60到86400秒之间的整数。

缺省

28800 秒

命令模式

ISAKMP 策略配置态

使用说明

使用该命令指定 IKE SA 在失效之前存在多长时间。

当 IKE 开始协商时，首先为其对话在安全参数上达成一致。这些一致的参数由 SA 引用。IKE SA 一直保留，直到其生命期失效。在 IKE SA 失效之前，它可以被后续的 IKE 协商重新使用，这在设置新的 IPSec SA 时可以节省时间。新的 IKE SA 在当前 IKE SA 失效之前协商。

因此，要节省设置 IPSec 的时间，应配置较长的 IKE SA 生命期。配置的生命期越短，IKE 协商可能会越安全。

注意:

当本端发起与对端之间的 IKE 协商时，只有对端策略的生命期比本端的策略的生命期短或者相等，才可以选择该策略。

如果生命期不相等，选择较短的生命期。

示例

本示例配置 IKE 策略的安全协会生命期为 600 秒（所有其它参数设置为缺省值）：

```
router_config# crypto isakmp policy 10
router_config_isakmp# lifetime 600
router_config_isakmp# exit
router_config#
```

相关命令

crypto isakmp policy

authentication(IKE policy)

encryption(IKE policy)

group(IKE policy)

hash(IKE policy)