

安全配置命令

目 录

第 1 章 AAA配置命令	1
1.1 AAA安全配置命令（授权+认证）	1
1.1.1 aaa authentication enable default	1
1.1.2 aaa authentication login	2
1.1.3 aaa authentication password-prompt	4
1.1.4 aaa authentication ppp	5
1.1.5 aaa authentication username-prompt	6
1.1.6 aaa default-username	7
1.1.7 aaa directed-request	8
1.1.8 aaa group server	9
1.1.9 debug aaa authentication	10
1.1.10 enable password	11
1.1.11 ppp authentication	12
1.1.12 ppp chap hostname	14
1.1.13 ppp chap password	15
1.1.14 ppp chap refuse	16
1.1.15 ppp pap sent-username	17
1.1.16 server	18
1.1.17 show users	19
1.1.18 service password-encryption	20
1.1.19 username	21
1.1.20 aaa authorization	23
第 2 章 IPsec配置命令	26
2.1 IPsec配置命令	26
2.1.1 clear crypto sa	26
2.1.2 crypto dynamic-map	27
2.1.3 crypto ipsec secure	28
2.1.4 crypto ipsec transform-set	29
2.1.5 crypto map (global configuration)	30
2.1.6 crypto map (interface configuration)	33
2.1.7 crypto map local-address	34
2.1.8 debug crypto packet	34
2.1.9 match address	35
2.1.10 mode	37
2.1.11 set peer	38
2.1.12 set pfs	40
2.1.13 set security-association lifetime	41
2.1.14 set security-association {inbound outbound}	43
2.1.15 set transform-set	46
2.1.16 show crypto ipsec sa	47
2.1.17 show crypto ipsec transform-set	49

2.1.18 show crypto map	50
2.1.19 transform-type	51
第 3 章 Internet 密钥交换安全协议命令	54
3.1 IKE 配置命令	54
3.1.1 authentication(IKE policy)	54
3.1.2 clear crypto isakmp	55
3.1.3 crypto isakmp key	56
3.1.4 crypto isakmp policy	57
3.1.5 debug crypto isakmp	59
3.1.6 encryption(IKE policy)	60
3.1.7 group(IKE policy)	61
3.1.8 hash(IKE policy)	62
3.1.9 lifetime(IKE policy)	63
3.1.10 show crypto isakmp policy	65
3.1.11 show crypto isakmp sa	66

第1章 AAA配置命令

1.1 AAA安全配置命令（授权+认证）

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。

1.1.1 aaa authentication enable default

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

aaa authentication enable default method1 [method2...]

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

参数

参数	参数说明
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**，则使用 **enable** 口令进行认证，与下面的命令具有相同的效果：

aaa authentication enable default enable

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

命令模式

全局配置态

使用说明

使用 **aaa authentication enable default** 命令创建一系列的认证方法，这些方法用来确定某个用户是否可以使用特权级别的命令。关键字 **method** 在表 1 中已经作了说明。只有在前面的认证方法返回错误时，才使用其它的认证方法，如果前面的认证方法返回结果通

知认证失败，则不使用其它的认证方法。若希望即使所有的认证方法都返回失败，认证仍然成功，则可以把 **none** 指定为命令行的最后一个认证方法。

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	使用服务器组进行认证。
group-restrict	使用服务器组进行认证，但当用户指定使用某台服务器后，此服务器组失效。
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。
tacacs+	使用TACACS+进行认证。
radius	使用RADIUS进行认证。

示例

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

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

相关命令

enable password

1.1.2 aaa authentication login

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

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

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

参数

参数	参数说明
default	使用跟随在该参数后面所列的认证方法作为用户注册时缺省的方法列表

<i>list-name</i>	用来命名认证方法列表的字符串，用户登录时将激活认证方法列表中所列的方法
method	至少为表2中描述的关键字之一。

缺省

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

```
aaa authentication login default none
```

命令模式

全局配置态

使用说明

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

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

如果没有给某条线路特别设置认证，缺省时不执行任何认证。

表 2：AAA 认证的注册方法

关键字	描述
enable	使用enable口令进行认证。
group	使用服务器组进行认证。
group-restrict	使用服务器组进行认证，但当用户指定使用某台服务器后，此服务器组失效。
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	使用本地用户组数据库认证
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。
radius	使用RADIUS进行认证。
tacacs+	使用TACACS+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

无

1.1.3 aaa authentication password-prompt

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

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

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

参数

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

缺省

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

命令模式

全局配置态

使用说明

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

```
Password:
```

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

示例

下面的示例将口令提示修改为 “YourPassword:”:

```
aaa authentication password-prompt YourPassword:
```

相关命令

aaa authentication username-prompt

enable password

1.1.4 aaa authentication 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} method1 [method2...]

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；
<i>list-name</i>	用来命名认证方法列表的字符串；
method1 [method2...]	至少为表3中描述的方法之一。

缺省

如果没有设置 default，则检查本地用户数据库进行认证，它与下面的命令具有相同的效果：

```
aaa authentication ppp default local
```

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。

只有在前面的方法返回错误时，才使用其它的认证方法，如果前面的方法返回的结果是认证失败，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	使用服务器组进行认证
group-restrict	使用服务器组进行认证，但当用户指定使用某台服务器后，此服务器组失效。
local	使用本地用户名数据库进行认证。
localgroup	使用本地用户组数据库认证
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。
radius	使用RADIUS进行认证。
tacacs+	使用TACACS+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

1.1.5 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 *text-string*

参数

参数	参数说明
<i>text-string</i>	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

1.1.6 aaa default-username

当用户没有进行认证时，我们将为这样的用户设置一个缺省的用户名。如果想改变缺省用户名使用的字符串，可以使用下面的命令。使用此命令的 **no** 形式恢复其缺省值。

aaa default-username *username*

no aaa default-username

参数

参数	参数说明
<i>username</i>	缺省用户名字符串。

缺省

缺省情况下缺省用户名为：DEFAULT

命令模式

全局配置态

使用说明

当用户没有进行认证，使用缺省用户名时，如果进行授权操作，他只能得到此缺省用户名对应的服务权限。

示例

下面的示例将缺省用户名改为:default-user

```
aaa default-username default-user
```

相关命令

无

1.1.7 aaa directed-request

如果允许用户通过 `username@host-ip-address` 的形式指定希望首先使用的 AAA 服务器，可以使用此条命令。使用此命令的 `no` 形式禁止这种方式

aaa directed-request [`no-truncate`]

no aaa directed-request

参数

参数	参数说明
<code>no-truncate</code>	不将 <code>@host-ip-address</code> 从用户名中剥离出来，将其也作为用户名的一部分。

缺省

不允许使用这种方式指定希望首先使用的服务器。

命令模式

全局配置态

示例

下面的示例允许使用 `@host-ip-address` 的形式指定希望首先使用的 AAA 服务器，但是 `@host-ip-address` 不作为用户名的一部分：

```
aaa directed-request
```

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 group-name
```

```
no aaa group server radius group-name
```

参数

参数	参数说明
<i>group-name</i>	服务器组的名称字符串。

缺省

无服务器组

命令模式

全局配置态

使用说明

使用此命令进入服务器组的配置层次，然后在其中添加相应的服务器。

示例

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

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

相关命令

server

1.1.9 debug aaa authentication

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

debug aaa authentication

no debug aaa authentication

参数

无

缺省

关闭 **debug** 信息。

命令模式

管理态

使用说明

使用此命令可跟踪每个用户的认证过程，以发现认证失败的原因。

示例

下面的示例将打开认证的 **debug** 信息：

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

输出信息	解释
Authen start (0x1f74208), user=, authen_type=ASCII, method-list=default priv=0,	认证开始，用户名未知，使用ASCII类型认证，用户要求进入的特权级别为0，使用default认证方式列表。 UserID = 0x1f74208

Use authen method LOCAL (0x1f74208)	使用本地认证方式，UserID = 0x1f74208。
Authen CONT, need username	询问用户名。
Authen CONT, need password	询问密码。
Authen ERROR (0x1f74208)! Use next method	本地无法完成此次认证，使用方式列表中的下一个认证方式。
Authen FAIL(0x1f74208)! Method-list polling finish	已经轮询了所有的认证方式，此处认证失败。

相关命令

无

1.1.10 enable password

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

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

no enable password [level number]

参数

参数	参数说明
<i>password</i>	密码字符串明文；
encryption-type	密码加密的类型；
encrypted-password 和 encryption-type	限定的加密类型相对应的密码的密文；
<i>level</i>	特权级别参数；
<i>number</i>	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不进行认证。

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

1.1.11 ppp authentication

要使用 CHAP 或 PAP（或者同时使用这两种协议），并且指定该接口选择 CHAP 和 PAP 认证的次序，可使用配置命令 `ppp authentication`。使用该命令的 `no` 形式关闭这种认证。

ppp authentication {chap | chap pap | pap chap | pap | ms-chap} [*list-name* | default] [*callin*]

no ppp authentication

参数

参数	参数说明
chap	在串行接口上激活CHAP。

pap	在串行接口上激活PAP。
chap pap	同时激活CHAP和PAP，在执行PAP认证之前，先执行CHAP认证。
pap chap	同时激活CHAP和PAP，在执行CHAP认证之前，先执行PAP认证。
ms-chap	在串行接口上激活CHAP的微软版本（MS-CHAP）。
list-name	与AAA一起使用。指定要使用的认证方法列表的名称。如果没有指定列表名称，则系统使用缺省列表。该列表是由aaaa uthentication ppp命令创建的。（可选）
default	由aaa authentication ppp命令创建的方法列表的名称。（可选）
callin	指定只对拨入呼叫进行认证。（可选）

警告：

如果使用了未经 aaa authentication ppp 命令配置的方法列表，在该接口上将无法运行 PPP。

缺省

不激活 PPP 认证

命令模式

接口配置态

使用说明

在激活 CHAP 或 PAP 认证（或同时激活这两种认证）时，本地路由器要求远程设备在允许数据传输之前证明其身份。PAP 认证要求远程设备发送名称和口令，将名称和口令与本地用户名数据库或远程安全服务器数据库中匹配的项进行对照。CHAP 认证向远程设备发送一条询问信息。该远程设备对询问信息使用共享密钥加密，在应答消息中返回加密后的值和其名称给本地路由器。本地路由器使用存储在本地用户名数据库或远程安全服务器数据库中与该远程设备的名称相关的秘密信息进行匹配；它使用存储的密钥加密原始的询问信息，验证加密的值是否匹配。

可以任意次序激活 PAP 或 CHAP（或二者）。如果同时激活了这两种方法，则在链接会话期间要求的是所指定的第一种方法。如果终端建议使用第二种方法，或者拒绝了第一种方法，则尝试使用第二种方法。有些远程设备只支持 CHAP，而另一些远程设备只支持 PAP。基于远程设备与合适的方法之间正确地会话的能力和所要求的数据线路安全级别来指定所用方法的次序。PAP 的用户名称和口令是作为明文字符串发送的，这样可能被中途截获并重新使用。CHAP 消灭了大部分已知的安全漏洞。

激活或关闭 PPP 认证不影响本地路由器向远程设备认证自身的能力。

如果在 TTY 线路上使用自动选择，可以使用 ppp authentication 命令为对应的接口打开 PPP 认证。

MS-CHAP 是 CHAP 的微软版本。与 CHAP 的标准版一样，MS-CHAP 用于 PPP 认证；在这种情况下，在一台使用 Microsoft Windows NT 或 Microsoft Windows 95 的 PC 机与本公司路由器或用作网络访问服务器的访问服务器之间进行认证。

激活或关闭 PPP 认证不影响本地路由器是否自动向远程设备认证自身。

如果在 TTY 线路上使用自动选择，则可能会希望使用 `ppp authentication` 命令为对应的接口激活 PPP 认证。

示例

下面的示例在异步接口 4 上激活 CHAP，使用认证列表 MIS-access:

```
interface async 4
encapsulation ppp
ppp authentication chap MIS-access
```

相关命令

aaa authentication ppp

username

1.1.12 ppp chap hostname

要创建一个在 CHAP 认证时以同一主机形式出现的拨号路由器组，使用接口配置命令 `ppp chap hostname`。要关闭这个功能，使用该命令的 `no` 形式。

ppp chap hostname *hostname*

no ppp chap hostname *hostname*

参数

参数	参数说明
<i>hostname</i>	在 CHAP 询问中发送的名字。

缺省

无效。路由器的名字在任何 CHAP 询问中发送。

命令模式

接口配置态

使用说明

当前，拨号到一组访问路由器的路由器要求这组路由器中每个可能的路由器都有一个用户名项，原因在于每个路由器都使用其用户名进行询问。如果在拨号路由器组中增加一台路由器，则所有连接的路由器都必须进行更新。命令 **ppp chap hostname** 允许给路由器组中所有路由器指定一个公共的别名，这样在拨号路由器中只须配置一个用户名也就可以了。该命令通常与本地 **CHAP** 认证一起使用（这时路由器对终端进行认证），然而该命令也可以用于远程 **CHAP** 认证中。

示例

下面示例中的命令把拨号接口 0 指定为拨号路由器组的首项，并且指定 **ppp** 为由所有成员接口使用的封装方法。该示例演示了在接收呼叫中使用 **CHAP** 认证的方法，而用户名 **ISPCorp** 将在所有 **CHAP** 询问和回应中发送：

```
interface dialer 0/0
encapsulation ppp
ppp authentication chap callin
ppp chap hostname ISPCorp
```

相关命令

aaa authentication ppp

ppp authentication

ppp chap password

ppp chap refuse

1.1.13 ppp chap password

要在呼叫不支持该命令的路由器组的路由器上激活配置公共的 **CHAP** 秘密口令，并在响应未知终端的询问时使用该口令，使用接口配置命令 **ppp chap password**。使用该命令的 **no** 形式关闭 **PPP CHAP** 口令。

ppp chap password secret

no ppp chap password secret

参数

参数	参数说明
<i>secret</i>	用来计算未知终端发出的 CHAP 询问的回应值的秘密口令。

缺省

无效

命令模式

接口配置态

使用说明

该命令允许在任何拨号接口或异步组接口上使用该命令的单一拷贝来替代几个用户名和口令配置。

该命令只在远程 CHAP 认证中使用（这时路由器对终端认证），并且不影响本地 CHAP 认证。

示例

下面示例中的命令指定 ISDN BRI 编号为 0。该接口上封装的方法为 PPP。如果从终端上接收到 CHAP 询问，该终端的名称没有在全局用户名列表中找到，则加密的密钥 7 1234567891 被解密，并用来创建一个 CHAP 回应值。

```
interface bri 0/0
encapsulation ppp
ppp chap password 1234567891
```

相关命令

aaa authentication ppp

ppp authentication

ppp chap hostname

ppp chap refuse

1.1.14 ppp chap refuse

要拒绝要求 CHAP 认证的终端的请求，使用接口配置命令 **ppp chap refuse**。使用该命令的 **no** 形式允许 CHAP 认证。

ppp chap refuse [callin]

no ppp chap refuse [callin]

参数

参数	参数说明
callin	（可选）这个关键字指示路由器拒绝回答来自终端的CHAP认证询问，但仍要求终端回答路由器发出的任何CHAP询问。

缺省

无效

命令模式

接口配置态

使用说明

该命令指示对所有的呼叫关闭 CHAP 认证，它意味着所有试图强制用户使用 CHAP 进行认证的终端将被拒绝。如果使用关键字 **callin**，则对来自终端的呼叫关闭 CHAP 认证，而对传向终端的呼叫仍执行 CHAP 认证。

如果激活了出站 PAP（使用 **ppp pap sent-username** 命令），则将在拒绝包中建议使用 PAP 作为认证方法。

示例

下面示例中的命令指定 ISDN BRI 编号为 0。该接口封装的方法为 PPP。该示例关闭那些呼叫请求 CHAP 认证的终端的 CHAP 认证请求：

```
interface bri 0/0
encapsulation ppp
ppp chap refuse
```

相关命令

aaa authentication ppp

ppp authentication

ppp chap hostname

1.1.15 ppp pap sent-username

要重新激活对某接口的远程 PAP 支持，并在发送给终端的 PAP 认证请求包中使用 sent-username 和 password，可使用接口配置命令 **ppp pap sent-username**。使用该命令的 **no** 形式关闭远程 PAP 支持。

ppp pap sent-username *username* **password** *password*

no ppp pap sent-username

参数

参数	参数说明
----	------

<i>username</i>	在PAP认证请求中发送的用户名。
<i>Password</i>	必须包括1到25个大写字母、小写字母或数字字符。

缺省

关闭远程 PAP 支持。

命令模式

接口配置态

使用说明

使用该命令重新激活远程 PAP 支持（例如，对终端要求使用 PAP 认证的请求给予应答），并指定在发送 PAP 认证请求时所使用的参数。这是个单接口命令。必须为每一个接口配置该命令。

示例

下述示例中的命令将拨号接口 0 标识为循环拨号组的开始，并指定 PPP 为该接口使用的封装方法。只在接收到呼叫时使用 CHAP 或 PAP 进行认证。如果终端要求路由器使用 PAP 进行认证，ISPCorp 作为用户名发送给终端。

```
interface dialer 0/0
encapsulation ppp
ppp authentication chap pap callin
ppp chap hostname ISPCorp
ppp pap sent username ISPCorp fjhfue
```

相关命令

aaa authentication ppp

ppp authentication

ppp chap hostname

ppp chap refuse

ppp chap password

1.1.16 server

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

server A.B.C.D

no server A.B.C.D

参数

参数	参数说明
A.B.C.D	服务器的IP地址。

缺省

无服务器

命令模式

服务器组配置态

使用说明

一个服务器组中最多添加 20 个不同的服务器。

示例

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

1.1.17 show users

要显示所以在线用户的概要信息，可使用 show users 命令。

show 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)、认证方式(Auth_Meth)、在线时间(time)以及 IP 地址(peer_address)。

示例

```
#show users
```

```
Port User Service Auth_Meth Time Peer-address
```

```
=====
```

```
0 someone exec unknown 2d06h01m(m) unknown
```

```
2 admin ppp local 2d01h10m(m) 192.168.30.87
```

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。
Auth_Meth	用户通过何种方式获得的认证。
Time	用户在线的统计时间。
Peer-address	用户所处的远端主机IP地址。

相关命令

username

1.1.18 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

```
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

username username password

enable password

password

1.1.19 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 }] [trust-host ip_address] [user-maxlinks number]
[callback-dialstring string] [callback-line line] [callback-rotary rotary]
[nocallback-verify] [autocommand command]
```

no username username

参数

参数	参数说明
----	------

<i>username</i>	用户名字符串；
password	用户对应的密码；
<i>password</i>	密码字符串明文；
encryption-type	密码加密的类型；
encrypted-password encryption-type	限定的加密类型相对应的密码的密文
trust-host	用户对应的信任主机；
<i>ip_address</i>	信任主机IP地址，用户只有从此台主机登录路由器才能通过认证；
user-maxlinks	同一用户可同时与路由器建立的链接数（只统计通过本地认证的用户）。
<i>number</i>	同时建立的链接数
<i>callback-dialstring</i>	回拨电话号码；
<i>string</i>	电话号码字符串；
callback-line	回拨时使用的线路；
<i>line</i>	线路号
callback-rotary	回拨rotary配置；
<i>rotary</i>	rotary号码；
nocallback-verify:	回拨不认证
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。
<i>command</i>	自动执行命令字符串。
Bind-ip	指定分配给用户的 I P 地址
<i>ip</i>	I P 地址
Freeze	冻结用户，使其不能登录

缺省

没有用户。

命令模式

全局配置态

使用说明

当没有 **password** 参数时，认为密码为空字符串。**trust-host** 将用户与特定的主机捆绑在了一起，此用户从其他主机登录路由器将无法通过认证。**user-maxlinks** 限制了同一个用

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 users** 命令查看每个在线用户是通过了那一种方式的认证。

我们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。

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 pp

1.1.20 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 {default | list-name} [method1 [method2...]]

no aaa authorization network

参数

参数	参数说明
network	网络类型服务的授权，如：PPP、SLIP
default	缺省授权方法列表。
<i>list-name</i>	用来命名授权方法列表的字符串。
<i>method1</i>	下表中所列的关键字之一。

[method2...]	
--------------	--

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。

AAA 授权关键字：

关键字	描述
group	使用服务器组获得授权信息。
group-restrict	使用服务器组获得授权信息。但是，当用户已指定要求使用的服务器时，此服务器组失效。
tacacs+	使用TACACS+获得授权信息。
if-authenticated	如果用户通过认证，则允许用户访问所要求的功能。
none	授权无条件通过。
local	使用本地数据库进行授权。
radius	使用RADIUS获得授权信息。

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

第2章 IPsec配置命令

2.1 IPsec配置命令

本章描述了 IPsec 配置命令。IPsec 提供了在公共网络上——如 Internet——上传输敏感信息的安全性。IPsec 提供的安全性解决方案非常健壮，并且是基于标准的。作为对数据机密性的补充，IPsec 还提供了数据验证和抗重播服务。

要了解配置信息，可以参阅“配置 IPsec”。

2.1.1 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

clear crypto sa peer *ip-address*

clear crypto sa map *map-name*

参数

参数	参数说明
<i>ip-address</i>	指定对端的IP地址。
<i>map-name</i>	指定加密映射表集合的名字。

缺省

如果未使用 peer、map 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 **peer**、**map** 等关键字，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 **map** 关键字将删除由加密映射表集合所创建的全部 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。注意这条命令只清除 IPsec 安全联盟；要清除 IKE 状态，请使用 **clear crypto isakmp** 命令。

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

clear crypto isakmp

2.1.2 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或集合。

crypto dynamic-map *map-name*

no crypto dynamic-map *map-name*

参数

参数	参数说明
<i>map-name</i>	动态加密映射表集合的名字。

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。

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

2.1.3 crypto ipsec secure

指定本地路由器是否接收非 IPSec 报文或不正确的 IPSec 报文。

crypto ipsec secure

no crypto ipsec secure

参数

无

缺省

允许通过非 IPSec 报文或不正确的 IPSec 报文。

命令模式

全局配置态。

使用说明

当有报文通过路由器且匹配了用户所设定的规则时，若该报文不是 IPSec 报文或者是不正确的 IPSec 报文，如果此时未设置该选项，那么路由器仍会照常处理该报文，如果此时设置了该选项，那么路由器就会丢弃该报文。

示例

以下例子设置了路由器的该选项。

```
crypto ipsec secure
```

相关命令

crypto map

2.1.4 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*

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

参数

参数	参数说明
<i>transform-set-name</i>	指定要创建（或修改）的变换集合的名称。

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。

可使用 **transform-type** 命令来具体配置变换类型。

示例

以下例子定义了一个变换集合。

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

相关命令

mode

transform-type

set transform-set

show crypto ipsec transform-set

2.1.5 crypto map (global configuration)

要创建或修改一个加密映射表，进入加密映射表配置态，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或集合。

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

```
no crypto map map-name seq-num
```

参数

参数	参数说明
<i>map-name</i>	加密映射表集合的名字。
<i>seq-num</i>	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。
<i>dynamic-map-name</i>	该加密映射表用来作模板的动态加密映射表名字。

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

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 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 abcdefabcdefabcd
```

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

2.1.6 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 **mymap** 集合中的所有加密映射表对它进行判断。当出站报文匹配 **mymap** 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

2.1.7 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
<i>map-name</i>	加密映射表集合的名称。
<i>interface-id</i>	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)

2.1.8 debug crypto packet

在 IPSec 的处理过程中，查看 IPSec 对于上层数据处理的出错信息。

参数

无

缺省

缺省情况下不显示相关信息。

命令模式

管理态

使用说明

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 padding.	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

show crypto ipsec sa

debug crypto isakmp

2.1.9 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

2.1.10 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。

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
router_config_crypto_trans# transform-type 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

2.1.11 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

2.1.12 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]

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。

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

2.1.13 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 <i>seconds</i>	指定一个安全联盟在超时终止前所能存活的秒数。
kilobytes <i>kilobytes</i>	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 3600 秒 (1 小时)，缺省超时通信量为 4,608,000 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** 处理时间就越多。

在手工方式建立安全联盟时，生命周期值将被忽略（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時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

2.1.14 set security-association {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 security-association {inbound|outbound} ah spi hex-key-string

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

set security-association {inbound|outbound} ah

set security-association {inbound|outbound} esp

参数

参数	参数说明
<i>inbound</i>	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）。
<i>outbound</i>	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）。
<i>ah</i>	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。

<i>esp</i>	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。
<i>spi</i>	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。
<i>hex-key-string</i>	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。
<i>cipher</i>	指示此密钥字符串是ESP加密变换的密钥。
<i>authenticator</i>	（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。

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 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 map aaa 100 ipsec-manual
match address aaa
set transform-set one
set peer 192.2.2.1
set association inbound ah 300 9876543210987654321098765432109876543210
set security-association outbound ah 300 fedcbafedcbafedcbafedcbafedcbafedcbafedc
fedc
set security-association inbound esp 300 cipher 0123456789012345
authenticator 0000111122223333444455556666777788889999
set security-association outbound esp 300 cipher abcdefabcdefabcd
authenticator 9999888877776666555544443333222211110000
```

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

2.1.15 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
<i>transform-set-name</i>	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 two
transform-type ah-sha-hmac 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

2.1.16 show crypto ipsec sa

要查看当前安全联盟所使用的设置，可以使用 **show crypto ipsec sa** 命令。

show crypto ipsec sa [map map-name [interface interface-id] [detail]

参数

参数	参数说明
----	------

map <i>map-name</i>	（可选）显示名为map-name的加密映射表所创建的现存的安全联盟。
interface <i>interface-id</i>	（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。
detail	（可选）同时显示安全联盟的统计信息。

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 ipsec sa 命令的一个输出示例。

```
router#show crypto ipsec sa detail
Interface: Ethernet0/0
Crypto map name:aaa
local ident (addr/mask/prot/port): (191.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (197.7.7.0/255.255.255.0/0/0)
local crypto endpt.: 192.2.2.87, remote crypto endpt.: 192.2.2.86
inbound esp sas:
  spi:0x190(400)
    transform: esp-des esp-sha-hmac
    in use settings ={ Tunnel }
    no sa timing
    #pkts decaps: 0, #pkts decrypt: 0, #pkts auth: 0
    #pkts decaps err: 0, #pkts decrypt err: 0, #pkts auth err: 0
    #pkts replay failed: 0
inbound ah sas:
  spi:0x12c(300)
    transform: ah-md5-hmac
    in use settings ={ Tunnel }
    no sa timing
    #pkts decaps: 0, #pkts decrypt: 0, #pkts auth: 0
    #pkts decaps err: 0, #pkts decrypt err: 0, #pkts auth err: 0
    #pkts replay failed: 0
outbound esp sas:
  spi:0x191(401)
```

```

transform: esp-des esp-sha-hmac
in use settings ={ Tunnel }
no sa timing
#pkts encaps: 0, #pkts encrypt: 0, #pkts auth: 0
#pkts encaps err: 0, #pkts encrypt err: 0, #pkts auth err: 0
#pkts replay failed: 0
outbound ah sas:
spi:0x12d(301)
transform: ah-md5-hmac
in use settings ={ Tunnel }
no sa timing
#pkts encaps: 0, #pkts encrypt: 0, #pkts auth: 0
#pkts encaps err: 0, #pkts encrypt err: 0, #pkts auth err: 0
#pkts replay failed: 0

```

相关命令

无

2.1.17 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

2.1.18 show crypto map

要查看加密映射表配置，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）只显示用map-name指定的加密映射表。

缺省

如果没有指定关键字，则显示路由器上所有的加密映射表配置。

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_config#show crypto map
Crypto Map aaa 100 ipsec-manual
    Extended IP access list aaa
    permit ip 192.2.2.0 255.255.255.0 193.3.3.0 255.255.255.0
```

```

peer = 192.2.2.1
Inbound esp spi: 300 ,
  cipher key: 1234567812345678 ,
  auth key  ,
Inbound ah spi: 301 ,
  key: 000102030405060708090a0b0c0d0e0f ,
Outbound esp spi: 300 ,
  cipher key: 1234567812345678 ,
  auth key  ,
Outbound ah spi: 301 ,
  key: 000102030405060708090a0b0c0d0e0f
Transform sets={ 1}
Crypto Map aaa 101 ipsec-isakmp
Extended IP access list bbb
  permit ip 191.1.1.0 255.255.255.0 197.7.7.0 255.255.255.0
peer = 192.2.2.19
PFS (Y/N): N
Security association lifetime: 2560 kilobytes/3600 seconds
Transform sets={ 1, 2,}

```

相关命令

无

2.1.19 transform-type

加密变换配置态下，要设置变换类型，使用 **transform-type** 命令。

transform-type transform1 [transform2[transform3]]

参数

参数	参数说明
transform1/ transform2/ transform3	可以指定3个以下的变换。这些变换定义了IPSec安全协议和算法。可接受的变换值在“使用说明”中详细阐述。

缺省

缺省的变换类型为 **ESP-DES**（ESP 采用 DES 加密算法）。

命令模式

加密变换配置态

使用说明

变换集合可以指定一个或两个 IPsec 安全协议（或 ESP，或 AH，或两者都有），并且指定和选定的安全协议一起使用哪种算法。ESP 和 AH IPsec 安全协议在“IPsec 协议：封装安全协议和校验头”一节中做了详细阐述。

变换集合的定义可以指定一到三个变换——每个变换代表一个 IPsec 安全协议（ESP 或 AH）和想要使用的算法的组合。当 IPsec 安全联盟协商时使用了某一变换集合，整个变换集合（协议、算法和其它设置的组合）必须和对端的一个变换集合相匹配。

在一个变换集合中，可以指定 AH 协议、ESP 或两者都指定。如果在变换集合中指定了一个 ESP，那么可以只定义 ESP 加密变换，也可以 ESP 加密变换和 ESP 验证变换两者都定义。

下表中显示了可行的变换组合。

为变换集合选择变换：可行的变换组合					
AH 变换中选择一种		ESP 加密变换中选择一种		ESP 验证变换中选择一种，	
变换	描述	变换	描述	变换	描述
ah-md5-hmac	带 MD5（HMAC 变量）的 AH 验证算法	esp-des	采用 DES 的 ESP 加密算法	esp-md5-hmac	带 MD5（HMAC 变量）的 ESP 验证算法
ah-sha-hmac	带 SHA（HMAC 变量）的 AH 验证算法	esp-3des	采用 3DES 的 ESP 加密算法	esp-sha-hmac	带 SHA（HMAC 变量）的 ESP 验证算法

IPsec 协议：ESP 和 AH

ESP 和 AH 协议都为 IPsec 提供了安全服务。

ESP 提供了分组加密，以及可选的数据验证和抗重播服务。

AH 提供了数据验证和抗重播服务。

ESP 使用一个 ESP 头和一个 ESP 尾对受保护数据——或是一个完整的 IP 自寻址数据包（或仅是有效负载）——进行封装。AH 是嵌入在受保护数据中的；它将一个 AH 头直接插入在外部 IP 头后、内部 IP 数据包或有效负载前。隧道模式中要对整个 IP 数据报文进行封装和保护，而传送模式中只对 IP 数据报文中的有效负载进行封装/保护。要进一步了解这两种模式，请参阅 mode 命令的描述。

选择适当的变换

IPsec 变换比较复杂。下面的提示能够帮助你选择适合自己情况的变换：

- 如果想要提供数据机密性，那么可以使用 ESP 加密变换。

- 如果想要提供对外部 IP 报头以及数据的数据验证，那么可以使用 AH 变换。
- 如果使用一个 ESP 加密变换，那么可以考虑使用 ESP 验证变换或 AH 变换来提供变换集合的验证服务。
- 如果想要数据验证功能（或使用 ESP 或使用 AH），可以选择 MD5 或 SHA 验证算法。SHA 算法比 MD5 要健壮，但速度更慢。

加密变换配置态

在执行了 `crypto ipsec transform-set` 命令以后，就将进入加密变换配置态。在这种状态下，可以将模式改变到隧道模式或传输模式（这是可选的改变）。在做完这些改变以后，键入 `exit` 来返回到全局配置态下。要深入了解这些可选改变的信息，请参看 `mode` 命令的详细阐述。

改变现存的变换

如果在 `transform-type` 命令中为一个变换集合指定一个或多个变换，那么指定的这些变换将会替换掉变换集合中现存的变换。如果改变了 `transform-type`，改变将只被运用到引用了此变换集合的加密映射表上。但改变将不会被运用到现存的安全联盟上，会被用于新建立的安全联盟。如果想让新的设置立即生效，可以使用 `clear crypto sa` 命令来清除安全联盟数据库的部分或全部。

示例

以下例子定义了一个变换集合。

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

相关命令

crypto ipsec transform-set

mode

set transform-set

show crypto ipsec transform-set

第3章 Internet密钥交换安全协议命令

3.1 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。

IPSec 可以不使用用 IKE，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）。

3.1.1 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)

show crypto isakmp policy

3.1.2 clear crypto isakmp

要清除正在运行的 IKE 连接，使用全局配置命令 clear crypto isakmp。

clear crypto isakmp [**map** *map-name* | **peer** *ip-address*]

参数

参数	参数说明
map <i>map-name</i>	（可选）清除名为map-name的加密映射表的IKE连接。
peer <i>ip-address</i>	（可选）清除对端地址为ip-addressIKE连接。

缺省

如果没有使用 map，peer 参数，则在发出该命令时清除所有存在的 IKE 连接。

命令模式

管理态

使用说明

使用该命令清除活动的 IKE 连接。

示例

本例清除 isakmp 连接。

```
Router# show crypto isakmp sa
      dst          src          state          state-id          conn
192.2.2.19      192.2.2.199    <I>M_SA_SETUP          1          aaa 100
Router# clear crypto isakmp
Router# exit
Router# show crypto isakmp sa
Router#
```

相关命令

show crypto isakmp sa

3.1.3 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* *peer-address*

no crypto isakmp key *keystring* *peer-address*

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。
peer-address	指定远端的IP地址。

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)

3.1.4 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
<i>priority</i>	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，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
```

上面的配置结果为下面的策略：

Router# show crypto isakmp policy

Protection suite of priority 10

```
encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
hash algorithm:        Message Digest 5
authentication method:  Pre-Shared Key
Diffie-Hellman group:   #1 (768 bit)
lifetime:               5000 seconds
```

Protection suite of priority 20

```
encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
hash algorithm:        Secure Hash Standard
authentication method:  Pre-Shared Key
Diffie-Hellman group:   #1 (768 bit)
lifetime:               10000 seconds
```

Default protection suite

encryption algorithm:	DES - Data Encryption Standard (56 bit keys).
hash algorithm:	Secure Hash Standard
authentication method:	Pre-Shared Key
Diffie-Hellman group:	#1 (768 bit)
lifetime:	86400 seconds

相关命令

authentication(IKE policy)

encryption(IKE policy)

group(IKE policy)

hash(IKE policy)

lifetime(IKE policy)

show crypto isakmp policy

3.1.5 debug crypto isakmp

在 IKE 的协商过程中，查看相关的报文交互处理信息。

参数

无

缺省

缺省情况下不显示相关信息。

命令模式

管理态

使用说明

显示和 IKE 协商相关的一些重要信息，下表列举了几种常见的信息。

显示信息	信息含义
ISAKMP(xxx): no acceptable Oakley Transform	双方配置的ISAKMP策略不匹配。（对端发起协商）
ISAKMP(xxx) : negotiate error NO_PROPOSAL_CHOSEN	

ISAKMP(xxx): no acceptable Proposal in IPsec SA ISAKMP(xxx) : negotiate error NO_PROPOSAL_CHOSEN	双方配置的IPSec策略不匹配。(对端发起协商)
ISAKMP(xxx): ISAKMP: not found matchable policy	双方配置的IPSec规则不匹配。
ISAKMP(xxx): dealing with Notify Payload ISAKMP: Notify-Message: NO_PROPOSAL_CHOSEN	双方配置的ISAKMP策略不匹配。(本端发起协商, 第一阶段中)
ISAKMP(xxx): dealing with Notify Payload ISAKMP: Notify-Message: NO_PROPOSAL_CHOSEN	双方配置的IPSec策略不匹配, 或配置的规则(access-list)不匹配。(本端发起协商, 第二阶段中)
ISAKMP(xxx): negotiate error ATTRIBUTES-NOT-SUPPORTED	本端不支持对端建议的属性。(对端发起协商)
ISAKMP(xxx): dealing with Notify Payload ISAKMP:Notify-Message: ATTRIBUTES-NOT-SUPPORTED	对端不支持本端建议的属性。(本端发起协商)

相关命令

show crypto ipsec sa

show crypto isakmp sa

debug crypto packet

3.1.6 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)

show crypto isakmp policy

3.1.7 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

authentication(IKE policy)

crypto isakmp policyen

crypton(IKE policy)

hash(IKE policy)

lifetime(IKE policy)

show crypto isakmp policy

3.1.8 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

authentication(IKE policy)

crypto isakmp policy encryption(IKE policy)

group(IKE policy)

lifetime(IKE policy)

show crypto isakmp policy

3.1.9 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

86400 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

authentication(IKE policy)

crypto isakmp policy

encryption(IKE policy)**group(IKE policy)****hash(IKE policy)****show crypto isakmp policy**

3.1.10 show crypto isakmp policy

要浏览每个 IKE 策略的参数，使用 show crypto isakmp policy。

show crypto isakmp policy

参数

该命令没有参数。

命令模式

管理态

示例

下面是配置了两个 IKE 策略（分别为优先级 10 和 20）后 show crypto isakmp policy 命令的输出：

```
router# show crypto isakmp policy
```

Protection suite of priority 10

encryption algorithm:	DES - Data Encryption Standard (56 bit keys).
hash algorithm:	Message Digest 5
authentication method:	Pre-Shared Key
Diffie-Hellman group:	#1 (768 bit)
lifetime:	5000 seconds

Protection suite of priority 20

encryption algorithm:	3DES - Triple Data Encryption Standard.
hash algorithm:	Secure Hash Standard
authentication method:	Pre-Shared Key
Diffie-Hellman group:	#2 (1024 bit)
lifetime:	10000 seconds

Default protection suite

encryption algorithm:	DES - Data Encryption Standard (56 bit keys).
hash algorithm:	Secure Hash Standard
authentication method:	Pre-Shared Key
Diffie-Hellman group:	#1 (768 bit)
lifetime:	86400 seconds

相关命令

authentication(IKE policy)

crypto isakmp policy

encryption(IKE policy)

group(IKE policy)

hash(IKE policy)

lifetime(IKE policy)

3.1.11 show crypto isakmp sa

要显示所有当前 IKE SA，使用 show crypto isakmp sa。

show crypto isakmp sa

参数

该命令没有参数。

命令模式

管理态

使用说明

示例下面是在两台终端之间成功地完成 IKE 协商之后，show crypto isakmp sa 命令的输出范例：

MyPeerRouter# show crypto isakmp sa

dst	src	state	state-id	conn
192.2.2.19	192.2.2.199	<I>Q_SA_SETUP	2	aaa 100
192.2.2.19	192.2.2.199	<I>M_SA_SETUP	1	aaa 100

下面表格显示在 show crypto isakmp sa 命令的输出中可能显示的各种不同的状态。当存在 ISAKMP SA 时，则它大多数时候为静止状态（Q_SA_SETUP）。

主模式交换中的状态：

状态	解释
M_NO_STATE	该阶段为“初期”阶段，没有状态。

M_SA_EXCH	终端已经形成ISAKMP SA的参数。
M_KEY_EXCH	终端已经交换Diffie-Hellman公共密钥，并且产生了共享的秘密。ISAKMP SA还未认证。
M_SA_SETUP	ISAKMP SA已经认证。开始快速模式交换。

快速模式交换中的状态：

状态	解释
Q_IDLE_1	快速模式状态1。
Q_IDLE_2	快速模式状态2。
Q_SA_SETUP	IPSec SA协商成功。

相关命令

crypto isakmp policy

lifetime(IKE policy)