安全配置

目 录

第 1 章 AAA 配置 1
1.1 AAA 概述 1
1.1.1 AAA 安全服务 1
1.1.2 使用 AAA 的优点 2
1.1.3 AAA 基本原理 2
1.1.4 AAA 方法列表 2
1.2 AAA 配置过程 4
1.2.1 AAA 配置过程概览 4
1.3 AAA 认证配置任务列表 4
1.4 AAA 认证配置任务 4
1.4.1 使用 AAA 配置登录认证 5
1.4.2 使用 AAA 进行 PPP 认证 6
1.4.3 在进入特权级别时开启口令保护 8
1.4.4 为 AAA 认证配置消息标语 9
1.4.5 改变提示输入用户名时的字符串 9
1.4.6 改变提示输入口令时的字符串 10
1.4.7 建立本地用户名认证数据库 10
1.4.8 建立本地特权级别认证数据库 11
1.5 AAA 认证配置示例 11
1.6 AAA 授权配置任务列表 12
1.7 AAA 授权配置任务 12
1.7.1 使用 AAA 配置 exec 授权 13
1.8 AAA 授权示例 14
1.9 AAA 记帐配置任务列表 14
1.10 AAA 记帐配置任务 14
1.10.1 使用 AAA 配置 connection 记帐 15
1.10.2 使用 AAA 配置 network 记帐 15
1.10.3 使用 AAA 配置记帐更新 16
1.10.4 抑制无用户名的用户记帐 16
第 2 章 RADIUS 配置 17
2.1 概述 17
2.1.1 RADIUS 概述 17
2.1.2 RADIUS 协议操作 18
2.2 RADIUS 配置步骤 18
2.3 RADIUS 配置任务列表 18
2.4 RADIUS 配置任务 19
2.4.1 配置路由器与 RADIUS 服务器的通信 19

2.4.2 使用厂商专用的 RADIUS 属性配置路由器 19
2.4.3 配置 RADIUS 认证 20
2.4.4 配置 RADIUS 授权 20
2.4.5 配置 RADIUS 记录 20
2.5 RADIUS 配置示例 20
2.5.1 RADIUS 认证和授权示例 20
2.5.2 AAA 中应用 RADIUS 示例 20
第 3 章 TACACS+配置 22
3.1 TACACS+概述 22
3.1.1 TACACS+的协议操作 22
3.2 TACACS+配置流程 23
3.3 TACACS+配置任务列表 23
3.4 TACACS+配置任务 24
3.4.1 指定 TACACS+服务器 24
3.4.2 设置 TACACS+加密密钥 24
3.4.3 指定使用 TACACS+进行认证 25
3.4.4 指定使用 TACACS+进行授权 25
3.4.5 指定使用 TACACS+进行记录 25
3.5 TACACS+配置示例 25
3.5.1 TACACS+认证示例 25
3.5.2 TACACS+授权示例 26
3.5.3 TACACS+记录示例 26
第 4 章 IPSec 配置 28
4.1 IPSec 概述 28
4.1.1 支持的标准 28
4.1.2 术语 29
4.1.3 限制 29
4.1.4 IPSec 工作过程概述 29
4.1.5 IPSec 嵌套 30
4.2 IPSec 配置任务列表 31
4.3 IPSec 配置任务 31
4.3.1 确保访问列表和 IPSec 相兼容 31
4.3.2 创建 id 身份验证配置 31
4.3.3 创建加密访问列表 32
4.3.4 加密访问列表技巧 32
4.3.5 在加密访问列表中使用 any 关键字 33
4.3.6 定义变换集合 33
4.3.7 创建加密映射表 34
4.3.8 应该建立多少个加密映射表 35
4.3.9 创建手工方式的加密映射表 35
4.3.10 创建使用 IKE 的加密映射表 36

4.3.11 将加密映射表集合应用于接口 37
4.4 IPSec 配置示例 37
第 5 章 配置 Internet 密钥交换安全协议 39
5.1 概述 39
5.1.1 IKE 概要 39
5.1.2 支持的标准 39
5.1.3 术语 40
5.2 IKE 配置任务列表 40
5.3 IKE 配置任务 40
5.3.1 确保访问列表与 IKE 兼容 40
5.3.2 创建 IKE 策略 40
5.3.3 配置预共享密钥 43
5.3.4 配置 RSA (暂时不支持) 43
5.3.5 配置证书(部分版本支持) 44
5.3.6 配置 DPD(dead peer detection)(可选) 44
5.3.7 配置 EZVPN 服务器(暂时不支持) 44
5.3.8 配置 EZVPN 客户端(可选) 45
5.3.9 清除 IKE 连接（可选） 46
5.3.10 IKE 诊断（可选） 46
5.4 IKE 配置示例 46

第1章 AAA 配置

1.1 AAA概述

访问控制是用来控制接入路由器或网络访问服务器（NAS）的用户，并限制他们可使用的服务种类。提供认证、授权和记录（Authentication，Authorization，Accounting）功能，以提高网络安全性能。

1.1.1 AAA 安全服务

AAA 是使用相同方式配置三种独立的安全功能的一种体系结构。它提供了完成下列服务的模块化方法：

- 认证（Authentication）——提供一种识别用户的方法，包括用户名和口令的询问，以及根据所选择的安全协议进行加密。

  认证是接受用户访问请求和提供网络服务之前识别他们身份的方法。通过定义一张命名的认证方法列表来对 AAA 认证进行配置，然后应用该列表于各种接口。方法列表定义了所执行的认证的类型和它们执行的次序；任何定义的认证方法执行之前都必须应用在具体的接口上。唯一的例外是缺省方法列表（其名称为 default）。如果没有定义其它方法列表，缺省方法列表自动应用于所有接口。定义任何方法列表将覆盖缺省方法列表。有关所有认证的配置方法的详细资料，请参见“认证配置”。

- 授权（Authorization）——提供一种远程访问控制的方法，用于限制用户的服务权限。

  AAA 授权通过相对于该用户的一组属性来发挥作用，这些属性描述了用户被授予哪些权限。将这些属性与包括在数据库中某个特定用户的信息相比较，结果返回给 AAA，以确定该用户的实际权限。这个数据库可以位于所访问的本地服务器或路由器，或者位于远程 RADIUS 或 TACACS+安全服务器。像 RADIUS 和 TACACS+这样的远程安全服务器，通过与用户相联系的属性值（AV）对（Attribute-Value Pairs）来完成对用户的授权，属性值（AV）对定义了允许授予的权限。所有的授权方法必须通过 AAA 定义。与认证一样，首先要定义一个授权方法列表，然后在各种接口中应用该列表。有关使用 AAA 进行授权配置的详细情况，请参见“授权配置”。

- 记帐（Accounting）——提供一种收集用户服务信息，并发送给安全服务器的方法，这些信息可用于开列帐单、审计和形成报表，如用户标识、开始时间和停止时间、执行的命令、数据包的数量以及字节数。

  记帐功能不仅可以跟踪用户访问的服务，同时还可以跟踪他们消耗的网络资源数量。当激活 AAA 记录功能时，网络访问服务器以记录的形式向 TACACS+或 RADIUS 安全服务器报告用户的活动。每条记录包括记录属性值（AV）对，存储在安全服务器上。这些数据可用于网络管理、客户帐单或审计分析。与认证和授权一样，要先定义一个记录方法列表，然后在不同的接口中使用这张表。有关使用 AAA 进行记帐配置的详细材料，请参见“记帐配置”。

1.1.2 使用 AAA 的优点

AAA 提供了如下优点：

- 灵活性和易于控制
- 方便升级
- 标准化的认证方法，如 RADIUS、TACACS+
- 多重备用系统

1.1.3 AAA 基本原理

AAA 用来动态配置基于每条线路（每个用户）或者每项服务（例如，IP、IPX 或 VPDN）的认证、授权及记帐类型。通过创建方法列表定义认证和授权的类型，然后把这些方法列表应用到具体服务或接口上。

1.1.4 AAA 方法列表

要对 AAA 进行配置，首先定义一个命名的方法列表，然后将这张列表应用到具体的服务或者接口上。该方法列表定义了所要执行的 AAA 类型，以及他们将被执行的次序；所定义的任何方法列表在被执行之前，必须应用于某一个具体的接口或者服务。唯一例外的是缺省方法列表（default）。缺省方法列表自动的应用于所有的接口或者服务。除非该接口明确引用了其他方法列表，这时此方法列表将替代缺省方法列表。

方法列表是用户在请求 AAA 服务时需要顺序查询的 AAA 方法的表格。在方法列表中可以指派一个或多个安全协议。因此确保了万一最初的方法失败后有一个备用的认证系统。本公司路由器软件使用方法列表中的第一个方法鉴别用户；如果该方法没有反应，则会选择方法列表中的下一个方法。这一个过程一直进行下去，直至所列的某个方法成功的进行 AAA 服务，或者所有的方法用完为止。

注意到这一点是很重要的，即本公司路由器软件仅仅在前面的方法没有反应时，才尝试使用列在后面的 AAA 方法进行 AAA 服务。如果 AAA 服务在这个过程中的任何一点上失败了，即安全服务器或是本地用户数据库的反应是拒绝用户访问，则 AAA 服务过程停止，并且不再尝试其他的认证方法。

下图显示了一个很有代表性的 AAA 网络配置，包含四个安全服务器，R1 和 R2 是 RADIUS 服务器，T1 和 T2 是 TACACS＋服务器。我们以认证为例来讲述 AAA 服务与 AAA 方法列表的关系。

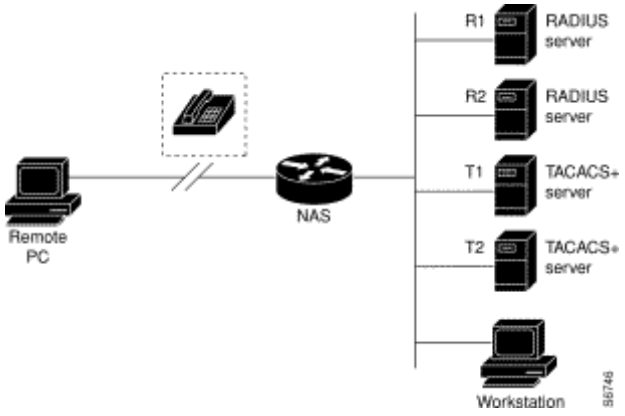

图 **错误！未找到引用源。**-1 AAA 网络配置示意图

假设系统管理员决定，在其安全方案中所有的接口使用同样的认证方法来认证基于 PPP 协议的连接：首先接通了 R1 来了解有关认证信息，如果 R1 没有反应，接通 R2，如果 R2 仍没有反应，接通 T1，如果 T1 也没有反应，接通 T2，如果所有指派的服务器都没有反应，认证工作就落在访问服务器本身的本地用户名数据库上。要实现这一点，系统管理员应该输入下面的命令，创建一张缺省的方法列表：aaa authentication ppp default groupradius local。

本例中，default 是方法列表的名称，包括在方法列表中的协议以及他们将被查询的次序列在方法列表名称后面。缺省列表自动的应用于所有的接口。

当远程用户试图通过拨号进入网络时，网络访问服务器首先在 R1 上查询有关的认证信息，如果鉴别该用户合法，他就发一条 PASS 应答给网络访问服务器，从而允许用户访问服务器。如果 R1 返回一条 FAIL 应答，则该用户被拒绝访问，本次对话结束。如果 R1 没有反应，网络访问服务器将其当成一次错误，并且在 R2 上查阅有关的认证信息。这种模式在剩下的方法中一直进行下去，直到该用户被接受或者被拒绝、或者本次对话结束为止。

记住这一条是很重要的，即 FAIL 应答与 ERROR 应答是截然不同的两个东西，FAIL 意味着用户没有满足包含在认证数据库中要认证成功所需的标准。认证以 FAIL 应答结束。ERROR 意味着该安全服务器对认证查询没有应答。仅仅当 AAA 检测到 ERROR 应答时，他才选择定义在认证方法链表中的下一个认证方法。

假设系统管理员想将方法列表仅仅应用于某个或某种特定的端口。在这种情况下，系统管理员应当创建一个非缺省的方法列表，然后把这个命名的列表应用到适当的端口上。下面的实例演示了系统管理员如何实现某个认证方法只应用异步端口的过程：

```
aaa authentication ppp default group radius local
aaa authentication ppp async0 group radius group tacacs+ local none
interface async 0/0
ppp authentication chap async0
```

在这个例子中，async0 是方法列表的名称，包括在这个方法列表中的认证协议依次列在他的后面，他们将有可能被依次使用。创建好方法列表后，将列表应用到合适的端口上。

注意：aaa authentication 命令中的方法名称必须与 ppp authentication 命令中的方法列表名称相匹配。

1.2 AAA配置过程

首先，必须决定想要实现何种类型的安全方案。用户需要评估自己网络中的安全风险，并且确定合适的方法来阻止未经授权的登录和攻击。

1.2.1 AAA 配置过程概览

在明白了配置所涉及的基本过程后，配置 AAA 就相对简单了。在本公司路由器或访问服务器上使用 AAA 进行安全配置，遵循如下步骤：

- 如果决定使用安全服务器，则先配置安全协议参数，如 RADIUS，TACACS+。
- 使用命令 aaa authentication 定义用于认证的方法列表。
- 如果需要的话，把该方法列表应用到某个具体的接口或线路上
- 使用命令 aaa authorization 进行授权配置（可选）。
- 使用命令 aaa accounting 进行记录配置（可选）。

1.3 AAA认证配置任务列表

- 使用 AAA 配置登录认证
- 使用 AAA 进行 PPP 认证
- 在进入特权级别时开启口令保护
- 为 AAA 认证配置消息标语
- 改变提示输入用户名时的字符串
- 改变提示输入口令时的字符串
- 建立本地用户名认证数据库
- 建立本地特权级别认证数据库

1.4 AAA认证配置任务

AAA 认证的一般配置过程：

要配置 AAA 认证，需要完成下列配置过程：

(1) 如果使用的是安全服务器，配置安全协议参数，如 RADIUS、TACACS＋。具体配置方法参见相应章节。

(2) 使用 aaa authentication 命令定义认证方法列表。

(3) 如果需要的话，把方法列表应用到特定的端口或是线路上。

1.4.1 使用 AAA 配置登录认证

AAA 安全服务使得使用各种认证方法变得更容易了，不论决定使用哪种登录方法，都使用 aaa authentication 命令开启 AAA 认证。在 aaa authentication login 命令中，创建一张或是多张认证方法的列表，这些列表在登录时使用。使用线路配置命令 login authentication 来应用这些列表。配置时，从全局配置模式开始，使用如下命令：

命令	目的
aaa authentication login {**default** | *list-name*}*method1* [*method2...*]	创建全局认证列表。
line [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]	进入某个线路的配置状态。
login authentication {**default** | *list-name*}	应用该认证列表于某条或是某几个线路上。

关键字 list-name 是用来命名所创建的列表的任何字符串。关键字 method 指定认证过程所采用的实际方法。仅当前面所用的方法返回认证错误时，才会使用其他的认证方法，如果前面的方法指明认证失败了，则不再使用其他的认证方法。如果要指定即使所有的方法都返回认证错误仍能成功登录，只要在命令行中指定 none 作为最后一个认证方法。例如：即使 TACACS+服务返回错误仍能认证成功，可用下面的命令行：

aaa authentication login default group tacacs+ none

使用 default 参数可建立一个缺省的列表，缺省列表自动的应用于所有的接口。例如：指定 RADIUS 作为用户登录时的缺省认证方式，使用下面的命令：

aaa authentication login default group radius

注意：

由于关键字 none 使得登录的任何用户都可成功的通过认证，所以应当将该关键字作为备用的认证方法。

登陆时，如果找不到认证方法列表的话，除 console 口登陆以外，其它任何形式的登陆将以认证失败结束。

下表列出了目前支持的登录认证方式：

关键字	说明
enable	使用enable口令进行认证。
group *name*	使用命名的服务器组进行认证。
group radius	使用 RADIUS 认证。
group tacacs+	使用TACACS+ 认证。
line	使用线路密码进行认证。
local	使用本地数据库进行认证。
local-case	使用本地用户名数据库进行认证(用户名区分大小写)。
none	认证无条件通过。

(1) 使用 enable 口令进行登录认证

在 aaa authentication login 命令中使用 enable 方法关键字指定 enable 口令作为登录认证方法，例如：在没有定义其他方法时，指定 enable 口令作为登录时用户认证的方法，使用下面的命令：

aaa authentication login default enable

(2) 使用线路口令进行登录认证

在使用 aaa authentication login 命令时，用 line 方法关键字指定线路口令作为登录时的认证方法。例如，在用户登录时指定线路口令为用户认证方法，并且不定义任何其他方法，可以输入下面的命令行：

aaa authentication login default line

在能够使用线路口令进行注册认证之前，需要定义一条线路口令。

(3) 使用本地口令进行登录认证

在使用 aaa authentication login 命令时，用 local 方法关键字指定使用本地用户名数据库作为登录认证方法。例如，在用户注册时指定本地用户名数据库作为用户认证方法，并且不定义任何其他方法，可以输入下面的命令行：

aaa authentication login default local

有关增加用户到本地用户名数据库中的详细资料，参见“建立本地认证数据库”。

(4) 使用 RADIUS 进行登录认证

在使用 aaa authentication login 命令时，用 radius 方法关键字指定 RADIUS 作为登录认证方法。例如在用户登录时指定 RADIUS 为用户认证方法，并且不定义任何其他方法，可以输入下面的命令：

aaa authentication login default group radius

在能使用 RADIUS 作为注册认证方法之前，需要首先配置 RADIUS 服务，有关的更多信息参见“配置 RADIUS”。

(5) 使用 TACACS+进行登录认证

在使用 aaa authentication login 命令时，使用 TACACS＋方法关键字指定 TACACS＋作为认证方法。例如，在用户登录时指定 TACACS＋认证方法，并且不定义任何其他方法，可以输入下面的命令：

aaa authentication login default group tacacs+

在能够使用 TACACS+进行认证方法之前，需要首先配置 TACACS+服务，有关详细信息，参见“配置 TACACS+”。

1.4.2 使用 AAA 进行 PPP 认证

许多用户通过异步或是 ISDN 拨号访问网络中心服务器。AAA 安全服务使得在串口上大量运行 PPP 时的认证方法变得容易了。不管决定使用所支持的何种 PPP 认证方法，均可以使用 aaa authentication ppp 开启 AAA 认证。配置时，在全局配置模式下使用下面的命令：

命令	目的
aaa authentication ppp {**default** | *list-name*} *method1* [*method2...*]	创建本地认证列表。

interface *interface-type number*	进入端口配置模式，认证列表将应用于该端口上。
ppp authentication {**chap** | **pap** | **chap pap** | **pap chap**} {**default** | *list-name*}	将认证列表应用于某条或是某几条线路上。

使用 aaa authentication 命令，可以创建一张或是几张认证方法列表，在用户开始运行 PPP 时使用这些列表。使用 ppp authentication 配置命令来应用这些列表。要创建一张缺省列表，使用 defalut 参数，在其后紧跟缺省情况下想要使用的方法。例如，指定本地用户名数据库作为认证的缺省方法，输入下面的命令行：

aaa authentication ppp default local

关键字 list-name 是用来命名所建立的列表的任何字符串。关键字 method 指定认证过程所采用的实际方法。仅当前面的方法返回认证错误时，才会使用其他的认证方法。如果前面使用的方法返回认证失败，则不再使用其他的认证方法。如果指定即使所有的方法都返回错误仍能成功认证，只需在命令行中指定 none 作为最后一个认证方法。例如，下面例子中即使 TACACS＋服务器返回错误，仍要保证认证成功，可以输入下面的命令行：

aaa authentication ppp default　group tacacs+ none

注意：

由于关键字 none 使得登录的任何用户都能成功的被认证，所以应当将该关键字作为备用的认证方法。

认证时，如果找不到方法列表，将以认证失败而结束。

下表列出了 PPP 可使用的认证方式：

关键字	说明
group *group-name*	使用命名的服务器组进行认证。
group radius	使用RADIUS 认证 。
group tacacs+	使用TACACS+ 认证。
local	使用本地用户名数据库认证。
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	认证无条件通过。

(1) PPP 认证使用本地口令

在 aaa authentication ppp 命令中，用 local 关键字指定使用本地用户名数据库进行认证。例如，在运行 PPP 的线路上要指定本地用户名数据库为认证方法，并且不需要其他任何方法，可以输入下面的命令行：

aaa authentication ppp default local

有关更多的增加用户到本地用户名数据库的更多信息，参见“建立本地认证数据库”。

(2) PPP 认证使用 RADIUS

在 aaa authentication ppp 命令中，用 RADIUS 关键字指定 RADIUS 作为运行 PPP 时的认证方法。例如，要指定 RADIUS 为用户认证的方法，并且不需要定义其他方法，可以输入下面的命令行：

aaa authentication ppp default　group radius

在使用 RADIUS 作为注册认证方法时，需要配置 RADIUS 服务，有关详细信息参见“配置 RADIUS”。

(3) PPP 认证使用 TACACS+

在 aaa authentication ppp 命令中，用 TACACS+关键字指定 TACACS+作为运行 PPP 的端口的认证方法。例如，要指定 TACACS+为用户认证的方法，并且不需要定义其他方法，可以输入下面的命令行：

aaa authentication ppp default group tacacs+

在能够使用TACACS+作为PPP认证方法之前，需要首先配置TACACS+服务，有关详细信息参见“配置TACACS+”。

1.4.3 在进入特权级别时开启口令保护

使用 aaa authentication enable default 命令创建一个认证方法列表，这些方法决定了某个用户是否可以执行特权级别的 EXEC 命令。可以至多指定四种认证方法。仅当前面所用的方法返回认证错误时，才会使用其他的认证方法。如果前面使用的方法返回认证失败，则不再使用其他的认证方法，如果指定即使所有的方法都返回错误仍能成功认证，只需在命令中指定 none 作为最后一个认证方法。配置时，在全局配置模式下使用下面的命令：

命令	目的
aaa authentication enable default *method1* [*method2...*]	在用户进入特权级别时开启口令认证。

关键字 method 指定认证过程使用的实际方法，在认证时依输入的次序使用。

下表列出了所支持的口令保护认证方法：

关键字	说明
enable	使用enable口令认证。
group *group-name*	使用命名的服务器组进行认证。
group radius	使用RADIUS进行认证。
group tacacs+	使用TACACS+ 认证。
line	使用线路口令认证。
none	认证无条件通过。

当配置了 enable 认证方法为远端认证时（即配置了 group，group-restrict，radius 或 tacacs+关键字时），使用 RADIUS 进行认证和使用 TACACS+认证的用户名不同，下面分别介绍：

(1) 使用 RADIUS 进行 enable 认证：

认证的用户名为$ENABLE*level*$，其中 level 是指用户要进入的特权级别，即 enable 命令后的特权级别的数字，举例来说，如果某用户要进入级别为 7 的特权级别，需要输入命令 enable 7，如果此时配置了使用 RADIUS 进行认证，则提交给 Radius Server 的用户名为$ENABLE7$，缺省条件下 enable 进入的特权级别均为 15，即在使用 RADIUS 进行认证时，提交给 Radius Server 的用户名为$ENABLE15$。这就需要预先在 Radius Server 上配置相应的用户名和密码，特别要指出的是：在

Radius Server 的用户数据库中，要指明用于特权认证的用户的服务类型（Service-Type）为 6，即 Admin-User。

(2) 使用 TACACS+进行 enable 认证：

进行 enable 认证时使用的用户名为该用户登录路由器时使用的用户名，举例来说，如果某用户登录进路由器时输入的用户名为 chen，则进行 enable 认证时使用的用户名也是 chen，如果用户登录路由器时没有被要求认证或者认证时没有被要求输入用户名，则登录成功后该用户的用户名为 DEFAULT，需要在 TACACS+ Server 的用户数据库中进行相应设置。

1.4.4 为 AAA 认证配置消息标语

支持使用可配置的、个性化的登陆及登陆失败标语。即在用户登陆进入系统将用 AAA 认证时，以及无论什么原因认证失败时，将显示所配置的消息标语。

配置注册标语

全局配置模式下，使用下述命令：

命令	目的
aaa authentication banner *delimiter text-string delimiter*	配置一个个性化的登陆注册标语

配置登陆失败标语

全局配置模式下，使用下述命令：

命令	目的
aaa authentication fail-message *delimiter text-string delimiter*	配置一个个性化的登陆失败的标语

使用说明

创建标语时，需要配置一个定界符号”，然后再配置文本字符串本身，该定界符号的作用是通知系统下面的文本字符串将被作为标语显示。定界字符在文本字符串的尾部重复出现，表示标语结束。

1.4.5 改变提示输入用户名时的字符串

使用 aaa authentication username-prompt 命令可以改变提示用户输入用户名时所显示的缺省文本。该命令的 no 形式恢复口令提示为如下形式的缺省值：

username：

命令 aaa authentication username-prompt 不改变远程 TACACS＋或是 RADIUS 服务器所提供的任何提示信息。配置时，在全局模式下使用下面的命令：

命令	目的
aaa authentication username-prompt *text-string*	在提示用户输入用户名时改变缺省的显示文本。

1.4.6 改变提示输入口令时的字符串

使用 aaa authentication password-prompt 命令可以改变提示用户输入口令时所显示的缺省文本。这条命令不仅改变 enable 口令的口令提示，也同时改变远端登录时的口令提示。该命令的 no 形式恢复口令提示为如下形式的缺省值：

password：

命令 aaa authentication password-prompt 不改变远程 TACACS＋或是 RADIUS 服务器所提供的任何提示信息。配置时，在全局模式下使用下面的命令：

命令	目的
aaa authentication password-prompt *text-string*	在提示用户输入口令时改变缺省的显示文本。

1.4.7 建立本地用户名认证数据库

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

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

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

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

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

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

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

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

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

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

no username *name*

1.4.8 建立本地特权级别认证数据库

创建基于本地的密码数据库，用于控制用户获取各种特权级别，要建立本地各种特权级别的 enable 密码数据库，可以在全局配置模式下，使用下面命令进行配置，删除时，利用该命令的 no 形式：

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

no enable password [**level** *level*]

1.5 AAA认证配置示例

1. RADIUS 认证示例

本节提供了一个使用 RADIUS 进行认证的配置示例，展示了如何配置路由器，以便使用 RADIUS 进行认证和授权的过程：

```
aaa authentication login radius-login group radius local
aaa authentication ppp radius-ppp group radius
aaa authorization network radius-network   group radius
line tty/vty
login authentication radius-login
interface serial 1/0
```

在这个示例中，各命令行的意义为：

- 命令 aaa authentication login radius-login group radius local 配置路由器在认证登录用户时使用 RADIUS 作为认证方法。如果 RADIUS 返回认证错误（ERROR），则使用本地数据库对用户进行认证。
- 命令 aaa authentication ppp radius-ppp group radius 将路由器配置为：在用户尚未登录时，采用 chap 或是 pap 的 ppp 认证方法。如果 EXEC 已经对用户进行了认证，则不再执行认证。
- 命令 aaa authorization network radius-network group radius 向 radius 请求 NETWORK 服务的授权，如：地址分配以及其他访问控制项目。
- 命令 login authentication radius-login 在线路上开启 radius-login 方法列表

2. TACACS＋认证示例

下面的示例将 TACACS＋配置为 PPP 认证时使用的安全协议：

```
aaa authentication ppp test group tacacs+ local
interface serial1\0
ppp authentication chap pap test
tacacs server 1.2.3.4
tacacs key testkey
```

在这个 TACACS＋认证配置中，各命令行的意义为：

- 命令 aaa authentication ppp test tacacs+ local 定义方法列表 test，该方法列表用于运行 ppp 的串行接口。关键字 tacacs+意味着认证将通过 TACACS＋进行。如果在认证期间，TACACS＋返回认证错误（ERROR），关键字 local 指示使用网络访问服务器上的本地数据库来尝试认证。
- 令 interface 选择端口。
- 命令 ppp authentication 将方法列表应用于该端口上。
- 命令 tacacs server 标识 TACACS＋服务器的 IP 地址为 1.2.3.4。
- 命令 tacacs key 定义共享的加密密钥 testkey

下面的示例为 PPP 配置 AAA 认证：

```
aaa authentication ppp default group tacacs+ local
```

在这个例子中，关键字 default 表示缺省的 ppp 认证方法列表。关键字 tacacs＋的意义是使用 TACACS＋服务器进行认证。如果 TACACS＋返回认证错误（ERROR），关键字 local 指示使用路由器上的本地数据库进行认证。

下面的示例为 PAP 创建了同样的认证过程，与上面不同的是，本示例调用了方法列表 test-list，而不是缺省方法列表 default：

```
aaa authentication ppp test-list group tacacs+ local
interface serial1/0
ppp authentication pap test-list
```

在本例中，由于方法列表未应用于任何端口，管理员必须使用 interface 命令选择端口，以便该认证方法能够应用到这个端口上。然后，管理员必须使用 ppp authentication 将方法列表应用于具体端口上。

1.6 AAA授权配置任务列表

- 使用 AAA 配置 EXEC 授权

1.7 AAA授权配置任务

AAA 授权的一般配置过程

要配置 AAA 授权，需要完成下列配置过程：

(1) 如果使用的是安全服务器，配置安全协议参数，如 RADIUS、TACACS＋。具体配置方法参见相应章节。

(2) 使用 aaa authorization 命令定义授权方法列表。缺省情况下，不提供授权服务。

(3) 如果需要的话，把方法列表应用到特定的端口或是线路上。

注意：目前仅仅支持 exec 授权。

1.7.1 使用 AAA 配置 exec 授权

使用 aaa authorization 命令开启 AAA 授权。在 aaa authorization exec 命令中，创建一张或是多张授权方法的列表，开启 EXEC 授权，以决定是否允许用户运行 EXEC 外壳程序，或者授于用户在进入 EXEC 外壳程序时的特权级别。使用线路配置命令 login authorization 来应用这些列表。配置时，从全局配置模式开始，使用如下命令：

命令	目的
aaa authorization exec {**default** | *list-name*}*method1* [*method2...*]	创建全局授权列表。
line [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]	进入某个线路的配置状态。
login authorization {**default** | *list-name*}	应用该授权列表表于某条或是某几个线路上。

关键字 list-name 是用来命名所创建的列表的任何字符串。关键字 method 指定授权过程所采用的实际方法。仅当前面所用的方法返回授权错误时，才会使用其他的授权方法，如果前面的方法指明授权失败了，则不再使用其他的授权方法。如果要指定即使所有的方法都返回授权错误仍能进入 EXEC shell，只要在命令行中指定 none 作为最后一个授权方法。例如：即使 TACACS+服务返回错误仍能授权成功，可用下面的命令行：

aaa authorization exec default group tacacs+ none

使用 default 参数可建立一个缺省的列表，缺省列表自动的应用于所有的接口。例如：指定 RADIUS 作为 exec 的缺省授权方式，使用下面的命令：

aaa authorization exec default group radius

注意：

授权时，如果找不到授权方法列表的话，将不再进行授权服务，并允许授权通过。

下表列出了目前支持的 EXEC 授权方式：

关键字	说明
group *WORD*	使用命名的服务器组进行授权。
group radius	使用 RADIUS 授权。
group tacacs+	使用TACACS+ 授权。
local	使用本地数据库进行授权。
if-authenticated	如果选择了该方法， 则所要求的所有功能都自动的授予已经认证的用户。
none	授权无条件通过。

1.8 AAA授权示例

1. EXEC 本地授权示例

本节提供了一个使用本地进行授权的配置示例，展示了如何配置路由器，以便使用 LOCAL 进行认证和授权的过程：

```
aaa authentication login default local
aaa authorization exec default local
!
username exec1 password 0 bdcom priviledge 15
username exec2 password 0 bdcom priviledge 10
username exec3 nopassword
username exec4 password 0 bdcom user-maxlinks 10
username exec5 password 0 bdcom autocommand telnet 172.16.20.1
!
```

此配置中，各命令行的意义为：

- 命令 aaa authentication login default local 定义 login 认证的默认方法列表，该方法列表自动运用于所有登陆认证服务
- 命令 aaa authorization exec default local 定义了 exec 授权的默认方法列表，该方法列表自动运用于所有需要进入 EXEC shell 的用户
- 用户 exec1，登陆密码为 bdcom，EXEC 特权级别为 15（最高级别），即只要用户 exec1 登陆 EXEC shell，其特权级别即为 15，可以查看和执行所有命令。
- 用户 exec2，登陆密码为 bdcom，EXEC 特权级别为 10，即只要用户 exec2 登陆 EXEC shell，其特权级别即为 10，只可以查看和执行特权级别不大于 10 的命令。
- 用户 exec3，无需登陆密码。
- 用户 exec4，登陆密码为 bdcom，该用户限制回话最多为 10 条。
- 用户 exec5，登陆密码为 bdcom，该用户登陆到 exec shell 上以后，马上执行命令 telnet 172.16.20.1

1.9 AAA记帐配置任务列表

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

1.10 AAA记帐配置任务

AAA 记帐的一般配置过程：

要配置 AAA 记帐，需要完成下列配置过程：

(1) 如果使用的是安全服务器，配置安全协议参数，如 RADIUS、TACACS＋。具体配置方法参见相应章节。

(2) 使用 aaa accounting 命令定义记帐方法列表。缺省情况下，不提供记帐服务。

(3) 如果需要的话，把方法列表应用到特定的端口或是线路上。

1.10.1 使用 AAA 配置 connection 记帐

使用 aaa accounting 命令开启 AAA 记帐。在 aaa accounting connection 命令中，创建一张或是多条记帐方法的列表，开启 connection 记帐，以提供所有从路由器产生的出站连接的信息，这些出站连接包括 Telnet、包重装/拆分（PAD）、H323 和 rlogin 等，暂时只支持 H323。配置时，从全局配置模式开始，使用如下命令：

命令	目的
aaa accounting connection {**start-stop** | **stop-only** | **none**} {**default** | *list-name*} **group** *groupname*	创建全局记帐列表。

关键字 list-name 是用来命名所创建的列表的任何字符串。关键字 method 指定记帐过程所采用的实际方法。

下表列出了目前支持的 connection 记帐方式：

关键字	说明
group *WORD*	使用命名的服务器组进行记帐。
group radius	使用 RADIUS 记帐。
group tacacs+	使用TACACS+ 记帐。
none	关闭记帐服务。
stop-only	该关键字指示所指定的方法只在所请求的用户过程结束时发送一条停止记录记帐通知。
start-stop	该关键字指示所指定的方法在所要求的事件开始时发出开始记帐通告，在该事件结束时发出终止通告。

1.10.2 使用 AAA 配置 network 记帐

使用 aaa accounting 命令开启 AAA 记帐。在 aaa accounting network 命令中，创建一张或是多条记帐方法的列表，开启 network 记帐，以给所有 PPP 或 SLIP 会话提供信息，包括包、字节及时间计数等。配置时，从全局配置模式开始，使用如下命令：

命令	目的
aaa accounting network {**start-stop** | **stop-only** | **none**} {**default** | *list-name*} **group** *groupname*	创建全局记帐列表。

关键字 list-name 是用来命名所创建的列表的任何字符串。关键字 method 指定记帐过程所采用的实际方法。

下表列出了目前支持的 network 记帐方式：

关键字	说明
group *WORD*	使用命名的服务器组进行记帐。
group radius	使用 RADIUS 记帐。
group tacacs+	使用TACACS+ 记帐。
none	关闭记帐服务。
stop-only	该关键字指示所指定的方法在所请求的用户过程结束时发送一条停止记录记帐通知。
start-stop	该关键字指示所指定的方法在所要求的事件开始时发出开始记帐通告，在该事件结束时发出终止通告。

1.10.3 使用 AAA 配置记帐更新

使用 aaa accounting 命令激活 AAA 记帐更新功能，以便 AAA 为系统中的所有用户发送临时记帐记录。配置时，从全局配置模式开始，使用如下命令：

命令	目的
aaa accounting update [**newinfo**] [**periodic** *number*]	激活AAA记帐更新

如果使用关键字 newinfo，则每当有新的记帐信息要报告时，向记帐服务器发送临时记帐记录。比如，当 IPCP 完成与远程终端的 IP 地址协商时就是发生这种情况的一个示例，临时记帐记录将包括远程终端使用的协商 IP 地址。

当使用关键字 periodic 时，则周期性地发送临时记帐记录，该周期由数字参数定义。临时记帐记录包含了到记帐记录发送时为止的该用户的所有记帐信息。

这两个关键字是相互排斥的，即无论后配置的是哪个关键字，都将取代前面的配置。例如，如果配置了 aaa accounting update periodic，然后配置了 aaaaccounting update newinfo，则当前注册的所有用户仍将产生周期性的临时记帐记录。所有新用户将基于 newinfo 算法产生记帐记录。

1.10.4 抑制无用户名的用户记帐

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

aaa accounting suppress null-username

第2章 RADIUS 配置

本章介绍 RADIUS（Remote Authentication Dial-In User Service）安全系统。定义其操作，说明适宜使用 RADIUS 技术和不适宜使用 RADIUS 技术的网络环境。“RADIUS 配置步骤”一节介绍如何使用认证、授权和记录（AAA）命令集配置 RADIUS。本章最后一节“RADIUS 配置示例”提供了两个实例。

2.1 概述

2.1.1 RADIUS 概述

RADIUS 是分布式客户机/服务器系统，它保护网络不受未经授权的访问的干扰。RADIUS 客户机运行于路由器上，并向中央 RADIUS 服务器发出认证请求，这里的中央服务器包含了所有的用户认证和网络访问服务信息。在路由器上我们利用 AAA 安全模式支持 RADIUS ，RADIUS 已经在既要求高级别安全性、又要求维持远程用户访问的各种网络环境中得以应用。

可以在具有下述访问安全要求的网络环境中使用 RADIUS：

- 拥有多厂商访问服务器的网络环境，并且每个服务器都支持 RADIUS。例如，几家厂商提供的访问服务器可以使用单一的基于服务器的 RADIUS 安全数据库。在使用多厂商提供的访问服务器的基于 IP 的网络中，拨号用户通过 RADIUS 服务器进行认证。

- 在用户必须只访问单一服务的网络中。使用 RADIUS，能够控制用户访问单一主机、单一实用程序（如 Telnet）或单一协议（如点对点协议 PPP）。例如，当用户登录时，RADIUS 规定并限制这个用户使用 IP 地址 10.2.3.4 来运行 PPP，并启动定义的访问列表。

- 要求资源记录的网络。可以使用与 RADIUS 认证或授权无关的 RADIUS 记录。RADIUS 记录允许在服务的开始和结束发送数据，以指示会话期间使用的资源数量（如时间、字节等等）。

RADIUS 不适合应用于下述网络安全情况中：

- RADIUS 不支持下述协议：

  AppleTalk 远程访问（ARA，AppleTalk Remote Access）协议

  NetBIOS 帧控制协议（NBFCP，NetBIOS Frame Control Protocol）

- NetWare 异步服务接口（NASI，NetWare Asynchronous ServicesInterface）

- X.25 PAD 连接。

- 路由器到路由器的情况。RADIUS 不提供双向认证。在路由器上运行 RADIUS，只能完成呼入认证，对于呼出认证（即本地路由器要登录到远端路由器时需要通过远端路由器的认证）是无法完成的。
- 使用多种服务的网络。RADIUS 通常把用户捆绑到一个服务模型上。

2.1.2 RADIUS 协议操作

当用户使用 RADIUS 进行登录认证时，发生下述步骤：

- 提示用户输入用户名和口令。
- 用户名和加密的口令通过网络发送到 RADIUS 服务器。
- 用户从 RADIUS 服务器收到下述响应之一：

  ACCEPT：用户通过认证。

  REJECT：用户没有通过认证，提示用户重新输入用户名和口令，否则访问被拒绝。

  CHALLENGE：服务器发出 Challenge 请求。该请求从用户那里收集附加数据。

  ACCEPT 和 REJECT 响应与附加授权信息一起返回，用于 EXEC 或 NETWORK 授权。在使用 RADIUS 授权之前，必须首先完成 RADIUS 认证。ACCEPT 和 REJECT 包中包括的附加数据由下述内容组成：

- 用户能够访问的服务，包括 Telnet、rlogin、PPP、SLIP 或 EXEC 服务。
- 连接参数，包括主机或客户机的 IP 地址、访问列表和用户超时设定等。

2.2 RADIUS配置步骤

为了在路由器或访问服务器上配置 RADIUS ，必须执行下述任务：

(1) 使用 aaa authentication 全局配置命令定义使用 RADIUS 认证方式的方法列表。有关使用 aaa authentication 命令的更多信息，请参见“认证配置”。

(2) 使用line和interface命令来引用已定义的方法列表。要了解更多的信息，请参见“认证配置”。

下述配置任务可根据需要进行选择：

- 如有必要，使用 aaa authorization 全局命令对用户的服务请求进行授权。有关使用 aaa authorization 命令的更多信息，请参见“授权配置”。
- 如有必要，使用 aaa accounting 全局命令对用户的服务过程进行记录。有关使用 aaa accounting 命令的更多信息，请参见“记录配置”。

2.3 RADIUS配置任务列表

- 配置路由器与 RADIUS 服务器的通信

- 使用厂商专有的 RADIUS 属性配置路由器
- 配置 RADIUS 认证
- 配置 RADIUS 授权
- 配置 RADIUS 记录

2.4 RADIUS配置任务

2.4.1 配置路由器与 RADIUS 服务器的通信

RADIUS 服务器通常是运行由 Livingston、Merit、 Microsoft 或另外的软件提供商提供的 RADIUS 服务器软件的多用户系统，RADIUS 服务器和路由器使用共享的密钥来加密口令并交换响应。使用 **radius-server host** 命令来指定 RADIUS 服务器，使用 **radius-server key** 命令来指定共享密钥。配置时，在全局配置模式下使用下述命令：

命令	目的
radius-server host *ip-address* [**auth-port** *port-number*][**acct-port** *portnumber*]	指定远程RADIUS服务器的IP地址，指定认证和记录的目的端口号。
radius-server key *string*	指定路由器和RADIUS服务器之间使用的共享密钥。

另外为了定制路由器和 RADIUS 服务器之间的通信，请使用下述可选的 RADIUS 全局配置命令：

命令	目的
radius-server retransmit *retries*	指定路由器在放弃重试之前向服务器传输每个RADIUS请求的次数（缺省值为2）。
radius-server timeout *seconds*	指定路由器在重新传输RADIUS请求之前，对应答应等待的秒数。
radius-server deadtime *minutes*	当RADIUS服务器不对认证请求作出反应时，需要将此台服务器标志为“死亡”的持续时间。

2.4.2 使用厂商专用的 RADIUS 属性配置路由器

Internet 工程任务组（IETF）草案标准通过使用厂商专用属性（Attribute26），为在网络访问服务器和 RADIUS 服务器之间交互基于厂商的专用扩展属性提供了一种方法。厂商专用属性（VSA）允许厂商支持属于它们自己的不适合于普遍用途的扩展属性。有关厂商 ID 和厂商专用属性的更多信息，请参见 RFC 2138：远程认证拨号用户服务（RADIUS）。要把网络服务器配置为能够识别和使用厂商专用属性的方式，请在全局配置模式下使用下述命令：

命令	目的
radius-server vsa send [**authentication**]	使网络访问服务器能够如同RADIUS IETF属性26所定义的那样去识别和使用厂商专用属

	性。

2.4.3 配置 RADIUS 认证

在标识了 RADIUS 服务器并定义了 RADIUS 认证密钥之后，就需要为 RADIUS 认证定义方法列表。由于 RADIUS 认证是通过 AAA 来进行的，所以需要输入 aaa authentication 命令，指定 RADIUS 作为认证方法。要了解与此相关的更多信息，请参见 “认证配置”。

2.4.4 配置 RADIUS 授权

利用 AAA 授权可以设置参数、限制用户的网络访问。使用 RADIUS 的授权提供了一种远程访问控制的方法，包括一次性授权或对每个服务的授权。因为 RADIUS 授权是通过 AAA 进行的，所以需要使用 aaa authorization 命令，指定 RADIUS 作为授权方法。要了解与此相关的更多信息，请参见“授权配置”。

2.4.5 配置 RADIUS 记录

AAA 记录特性让我们能够追踪用户正在访问的服务及他们占用的网络资源数量。由于 RADIUS 记录特性是通过 AAA 提供的，所以需要使用 aaa accounting 命令，指定 RADIUS 作为记录方法。要了解与此相关的更多信息，请参见“记录配置”。

2.5 RADIUS配置示例

2.5.1 RADIUS 认证和授权示例

下述示例说明了怎样对路由器进行配置以使用 RADIUS 进行认证和授权：

```
aaa authentication login use-radius   group radius local
aaa authorization exec default group radius
aaa authorization network default group radius
```

在这个示例中，各行命令的意义为：

- aaa authentication login use-radius radius local 命令配置路由器在登录过程中使用 RADIUS 进行认证。如果 RADIUS 服务器返回认证错误（ERROR），再使用本地数据库进行认证。在这个示例中，use-radius 是方法列表的名称，group radius local 是认证方法，它指定首先进行 RADIUS 认证，然后再进行本地认证。
- aaa authorization exec default group radius 命令设置了进行 EXEC 服务的授权。
- aaa authorization network default group radius 命令设置了进行 NETWORK（PPP、SLIP）服务的授权。

2.5.2 AAA 中应用 RADIUS 示例

下面是一个使用 AAA 命令集定义通用配置的示例：

```
radius-server host 1.2.3.4
radius-server key myRaDiUSpassWoRd
username root password AlongPassword
aaa authentication ppp dialins   group radius local
aaa authentication login admins local
line vty 1 16
login authentication admins
interface async0/0
encap ppp
ppp authentication pap dialins
```

在这个示例中，各命令行的意义为：

- radius-server host 命令定义 RADIUS 服务器的 IP 地址；
- radius-server key 命令定义网络访问服务器和 RADIUS 服务器主机之间的共享密钥；
- aaa authentication ppp dialins group radius local 命令定义了认证方法列表 dialins，它指定首先通过 RADIUS 进行认证，然后（若 RADIUS 服务器不响应）使用本地认证；
- ppp authentication pap dialins 命令对指定的线路运用 dialins 认证方法列表；
- aaa authentication login admins local 命令为登录认证定义另外一个方法列表 admins；
- login authentication admins 命令指定在登录认证中运用 admins 方法列表；

第3章 TACACS+配置

3.1 TACACS+概述

TACACS+是一种访问安全控制协议，它为用户获得对路由器或网络访问服务器的访问权提供集中化的验证。由于网络访问服务器和 TACACS+服务程序之间的信息交换采用加密形式，所以它可以保证通信的安全性。

在网络访问服务器上配置的 TACACS+特性使用之前，必须能够访问并配置 TACACS+服务器。TACACS+提供了独立的模块化认证、授权和记录能力。

认证——支持多种认证方式（ASCII、PAP、CHAP 等），同时提供处理与用户进行任意对话的能力（比如，提供登录用户名和口令后，向用户提出一些询问性问题，诸如家庭住址、服务类型和身份证号码等）。另外，TACACS+认证服务支持向用户屏幕发送信息，例如，发送信息通知用户，由于公司的口令老化政策，他们的口令必须更换。

授权——对提供服务期间用户的服务权限进行细致的控制，包括设置自动命令、访问控制、会话持续时间等。还可以对用户可能执行的命令强制加以限制。

记录——收集和发送用于生成收费单据、进行审计或网络资源使用状况统计的信息。网络管理员可以使用记录能力，为安全审计追踪用户的活动，或者为用户账单提供信息。记录功能记录了包括用户标识、起止时间、执行的命令、包的数量以及字节的数量等。

3.1.1 TACACS+的协议操作

1. ASCII 形式的认证

当用户登录到使用 TACACS+的网络访问服务器，并要求进行简单的 ASCII 形式的认证时，典型情况下会出现下述过程：

连接建立后，网络访问服务器与 TACACS+服务程序联系以获得用户名提示符，然后显示给用户。用户输入用户名，网络访问服务器与 TACACS+服务程序再次进行联系，得到口令提示符，把口令提示符显示给用户，用户输入口令，然后口令被发送给 TACACS+服务程序。

注意：

TACACS+允许在服务器程序和用户之间进行任意的会话，直到收集到足够的信息对用户进行认证为止。这通常是通过提示用户名和口令的组合而完成的，但是还可以包括其它的项目，诸如证件号码等，一切都是在 TACACS+服务器程序的控制之下进行的。

网络访问服务器最终从 TACACS+服务器收到下述反应之一：

ACCEPT	用户通过了认证，服务可以开始了。如果网络访问服务器被配置为要求服务授权，那么此时开始进行授权。

REJECT	用户未通过认证。用户可能被拒绝进行进一步的访问，或者提示重新进入登录过程，这取决于TACACS+服务器的处理方式。
ERROR	在认证期间发生了错误，原因可能发生在服务器，也可能是发生在服务器与网络访问服务器之间的网络连接中。如果收到ERROR回应，一般情况下，网络访问服务器会试着使用另一种方法对用户进行认证。
CONTINUE	提示用户输入附加的认证信息。

2. PAP 和 CHAP 形式的认证

PAP 登录与 ASCII 登录相类似，只不过到达网络访问服务器的用户名和口令是在 PAP 报文中，而不是由用户输入，所以不用提示用户输入相关信息。CHAP 登录在主要的内容上也是类似的。认证之后，如果网络访问服务器要求对用户进行授权，那么用户就需要进入授权阶段，但在处理 TACACS+授权之前，必须首先成功地完成 TACACS+认证。

如果要求进行 TACACS+授权，则再次与 TACACS+服务器程序联系并返回 ACCEPT 或 REJECT 授权反应。如果返回了 ACCEPT 反应，则可能包含 AV（attribute-value）对数据，用于规范该用户的 EXEC 或 NETWORK 会话，确定用户能够访问的服务。

3.2 TACACS+配置流程

为了把路由器配置为支持 TACACS+的方式，必须执行下述任务：

使用 tacacs-server 命令，指定一个或多个 TACACS+服务器 IP 地址。使用 tacacs key 命令，为网络访问服务器和 TACACS+服务器之间的所有信息交换指定加密密钥。同一密钥也必须在 TACACS+服务器程序中进行配置。

使用 aaa authentication 全局配置命令对使用 TACACS+进行认证的方法列表进行定义。有关 aaa authentication 命令的更多信息，请参见“认证配置”。

使用 line 和 interface 命令，对端口或线路运用所定义的方法列表。与此相关的更多信息，请参见“认证配置”。

3.3 TACACS+配置任务列表

- 指定 TACACS+服务器
- 设置 TACACS+加密密钥
- 指定使用 TACACS+进行认证
- 指定使用 TACACS+进行授权
- 指定使用 TACACS+进行记录

3.4 TACACS+配置任务

3.4.1 指定 TACACS+服务器

Tacacs-server 命令使你能够指定 TACACS+服务器的 IP 地址。由于 TACACS+软件按照配置的顺序搜索主机，这一特色对于设置不同的服务器优先级是有用的。为了指定 TACACS+主机，以全局配置模式使用下述命令：

命令	目的
tacacs server *ip-address* [**single-connection**| **multi-connection**] [**port** *integer*] [**timeout** *integer*] [**key** *string*]	指定TACACS+服务器IP地址及相应属性。

使用 tacacs-server 命令，还可以配置下述选项：

- 使用 single-connection 关键字指定采用单一连接, 这样做允许服务器程序处理更多的 TACACS＋操作，可能更有效。multi-connection 则是指示采用多条 TCP 连接。
- 使用 port 参数，指定 TACACS+服务器程序使用的 TCP 端口号。缺省的端口号是 49。
- 使用 timeout 参数，指定路由器等待服务器回应的时间上限（以秒为单位）。
- 使用 key 参数指定对报文进行加密和解密的密钥。

注意：

使用 tacacs-server 后接 host，再接 timeout 等命令指定的超时值将覆盖 tacacs-server timeout 命令设置的全局超时值； 使用 tacacs-server 指定的加密密钥将覆盖使用全局配置命令 tacacs-server key 设置的缺省密钥。所以可以使用本命令配置唯一的 TACACS+连接来加强网络的安全性。

3.4.2 设置 TACACS+加密密钥

为了设置 TACACS+报文加密密钥，在全局配置模式使用下述命令：

命令	目的
tacacs-server key *keystring*	设置与TACACS+服务器所使用密钥相匹配的加密密钥。

注意 ：

为了成功地进行加密，必须对 TACACS+服务器程序配置相同的密钥。

3.4.3 指定使用 TACACS+进行认证

在标识了 TACACS+服务器并定义了与之相联系的加密密钥后，就需要为 TACACS+认证定义方法列表。由于 TACACS+认证通过 AAA 进行操作，所以需要设置 aaa authentication 命令指定 TACACS+作为其认证方法。与此相关的更多信息，请参见“认证配置”。

3.4.4 指定使用 TACACS+进行授权

AAA 授权使得能够设置参数限制用户的网络访问权限。TACACS+授权，可以应用于命令、网络连接和 EXEC 会话等服务。由于 TACACS+授权是通过 AAA 提供的，所以需要配置 aaa authorization 命令指定 TACACS+作为授权方法。与此相关的更多信息，请参见“授权配置”。

3.4.5 指定使用 TACACS+进行记录

AAA 记录使得能够跟踪用户正在使用的服务以及他们消耗的网络资源的数量。由于 TACACS+记录是通过 AAA 提供的，所以需要配置 aaa accounting 命令指定 TACACS+作为记录方法。与此相关的更多信息，请参见“记录配置”。

3.5 TACACS+配置示例

本节包括了下述 TACACS+配置示例：

3.5.1 TACACS+认证示例

下述示例配置 PPP 认证由 TACACS+完成：

```
aaa authentication ppp test group tacacs+ local
tacacs -server host 1.2.3.4
tacacs-server key testkey
interface serial 1/1
ppp authentication chap pap test
```

在这个示例中：

aaa authentication 命令定义了运行 PPP 的串口上使用的认证方法列表 test。关键字 tacacs+意味着认证通过 TACACS+进行，如果 TACACS+在认证期间返回某种类型的 ERROR，则关键字 local 指示使用网络访问服务器上的本地数据库进行认证。

tacacs serverhost 命令标识 TACACS+服务器的 IP 地址为 1.2.3.4。tacacs-server key 命令定义共享的加密密钥为 testkey。

interface 命令选择端口，ppp authectication 命令在该端口应用方法列表 test。

下述示例将 TACACS+配置为 PPP 认证时使用的安全协议，但是不再使用方法列表 test，而是使用方法列表 default：

```
aaa authentication ppp default if-needed group tacacs+ local
```

```
tacacs-server host 1.2.3.4
tacacs-server key goaway
interface serial 1/1
ppp authentication default
```

在这个示例中：

aaa authentication 命令定义运行 PPP 的串口上使用认证方法列表 default。关键字 if-needed 意味着如果用户已经通过了登录过程进行的认证，那么 PPP 认证就不再必要；如果需要认证，那么关键字 tacacs+意味着认证通过 TACACS+进行，如果 TACACS+在认证期间返回某种类型的 ERROR，则关键字 local 指示使用网络访问服务器上的本地数据库进行认证。

tacacs serverhost 命令标识 TACACS+服务器程序的 IP 地址为 1.2.3.4。tacacs-server key 命令定义共享的加密密钥为 goaway。

interface 命令选择端口，ppp authectication 命令在该端口应用缺省的 PPP 认证方法列表。

3.5.2 TACACS+授权示例

```
aaa authentication ppp default if-needed group tacacs+ local
aaa authorization network default group tacacs+
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 1/1
ppp authentication default
ppp authorization default
```

在这个示例中：

aaa authentication 命令定义运行 PPP 的串口上使用的认证方法列表 default。关键字 if-needed 意味着如果用户已经通过登录过程进行了认证，那么 PPP 认证就不再必要；如果需要认证，那么关键字 tacacs+意味着认证通过 TACACS+进行，如果 TACACS+在认证期间返回某种类型的 ERROR，则关键字 local 指示使用网络访问服务器上的本地数据库进行认证。

aaa authorization 命令配置通过 TACACS+进行网络服务授权。

tacacs serverhost 命令标识 TACACS+服务器 IP 地址为 10.1.2.3。tacacs-server key 命令定义共享的加密密钥为 goaway。

interface 命令选择端口，ppp authectication 和 ppp authorization 命令对该端口应用缺省的认证或授权方法列表。

3.5.3 TACACS+记录示例

下述示例配置 PPP 认证的方法列表使用 TACACS+作为方法之一，并配置通过 TACACS+进行记录：

```
aaa authentication ppp default if-needed group tacacs+ local
aaa accounting network default stop-only group tacacs+
```

```
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 1/1
ppp authentication default
ppp accounting default
```

在这个示例中：

aaa authentication 命令定义 PPP 协议使用的认证方法列表 default。关键字 if-needed 意味着如果用户已经通过登录过程进行了认证，那么 PPP 认证就不再必要；如果需要认证，那么关键字 tacacs+意味着认证通过 TACACS+进行，如果 TACACS+在认证期间返回某种类型的 ERROR，则关键字 local 指示使用网络访问服务器上的本地数据库进行认证。

aaa accounting 命令配置通过 TACACS+进行网络服务的记录。在这个示例中，只记录服务结束时的相应信息，在网络连接结束时被发送到 TACACS+服务器。

tacacs serverhost 命令标识 TACACS+服务器的 IP 地址为 10.1.2.3。tacacs-server key 命令定义共享的加密密钥为 goaway。

- interface 命令选择端口， ppp authectication 命令在该端口应用缺省的认证方法列表；ppp accounting 命令在该端口应用缺省的记录方法列表。

第4章　IPSec 配置

本章阐述了如何配置 IPSec。IPSec 是由 IETF 开发的开放标准框架。IPSec 为无保护网络（例如 Internet）上传输敏感数据提供了安全性。IPSec 在网络层起作用，对参与 IPSec 的设备（例如本公司路由器）之间传输的 IP 包进行保护和验证。

IPSec 提供了下列网络安全性服务。这些服务是可选的。通常，本地安全策略将规定使用下列这些服务的一种或多种：

- 数据机密性——IPSec 发送方在通过网络传输报文前对报文进行加密。
- 数据完整性——IPSec 接收方对发送方发送来的报文进行验证，以确保数据在传输过程中没有被篡改。
- 数据来源验证——IPSec 接收方对 IPSec 报文的源地址进行验证。这项服务基于数据完整性服务。
- 抗重播——IPSec 接收方可以检测和拒绝被重播的报文。

有了 IPSec，数据在通过公共网络传输时，就不用担心被监视、篡改和伪造。

要得到本章所用到的 IPSec 命令的完整阐述，请参阅“IPSec 配置命令”。

4.1　IPSec概述

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。

4.1.1　支持的标准

本公司路由器 IPSec 实现了如下标准：

- IPSec——IP 安全性协议。IPSec 是在参与通信的两端之间提供数据机密性、数据完整性、数据验证的一种开放标准框架。IPSec 在 IP 层提供这些安全性服务；它使用 IKE 来协商基于本地策略的协议和算法，并产生加密和验证密钥供 IPSec 使用。IPSec 可为一对主机、一对安全网关或一台主机和一台安全网关之间的一条或多条数据流提供保护。
- Internet 密钥交换（IKE）——一种在 ISAKMP 网络中实现 Oakley 和 SKEME 密钥交换的混合协议。尽管 IKE 可以和其他协议一起使用，它最初是和 IPSec 协议一起使用的。IKE 提供对 IPSec 对端的验证，协商 IPSec 安全联盟，生成 IPSec 密钥。要进一步了解 IKE，请参阅“配置 Internet 密钥交换安全性协议”。

4.1.2 术语

- DES——数据加密标准（DES）用于对包数据进行加密，属于对称加密算法，本公司路由器使用 IV 为 56 位 DES-CBC。CBC 需要一个初始化向量（IV）来进行加密。
- 3DES——3DES 用于对包数据进行加密，属于对称加密算法。本公司路由器使用 IV 为 168 位 DES-CBC。3DES 比 DES 更为安全。
- AES——AES 代表高级加密标准（AES），是一种密码块，由 NIST 开发作为加密标准。AES 意在执行一种未分类的、公开于众的对称加密算法。AES 使用更长的密钥，比 DES 更加安全。AES 密码块大小固定为 128 位，密钥大小为 128、192 或 256 位。
- MD5（HMAC 变量）——MD5 是一种散列算法。HMAC 是一个用于对数据进行验证的加密散列变量。
- SHA（HMAC 变量）——SHA 是一种散列算法。HMAC 是一个用于对数据进行验证的加密散列变量。

本公司路由器软件的 IPSec 还支持下列这些标准：

- AH——是一种安全协议，用于为 IP 提供数据完整性、数据原始身份验证和一些可选的抗重播服务。AH 可用来保护一个上层协议（传输模式）或一个完整的 IP 数据包（隧道模式）。AH 可单独使用，也可与 ESP 一起使用。定义在 RFC2402 中。
- ESP——是一种安全协议，用于为 IP 提供机密性、数据源验证、抗重播以及数据完整性等安全服务。ESP 可用来保护一个上层协议（传输模式）或一个完整的 IP 数据包（隧道模式）。定义在 RFC2406 中。

4.1.3 限制

现阶段，IPSec 只能用于单点传送 IP 数据报。因为 IPSec 工作组还没有从事组密钥分布的工作，IPSec 目前不支持多点传送或广播 IP 数据报。如果使用网络地址翻译技术（NAT），那么应该配置静态 NAT 翻译来使 IPSec 正常工作。总而言之，NAT 翻译必须在路由器进行 IPSec 封装之前进行；换句话说，IPSec 应该使用全局地址。

4.1.4 IPSec 工作过程概述

IPSec 可以为两个路由器之间提供安全隧道。自己定义哪些报文由这些安全隧道传送。并且，通过指定这些隧道的参数来定义用于保护这些敏感报文的参数。然后，当 IPSec 得到这样的一个报文时，它将建立起相应的安全隧道，通过这条隧道将数据报文传送给对端。

更精确的说，隧道是 IPSec 两端建立的安全联盟的集合。这些安全联盟定义了哪些协议和算法将被应用于敏感报文，同时指定了 IPSec 两端将使用到的密钥。安全联盟是单向的，每个安全性协议（AH 或 ESP）都分别建立。

在 IPSec 中，通过配置访问列表，将访问列表配置在加密映射表中，再将加密映射表应用到接口上，可以使特定通信将受到保护。因此，可以基于源和目标地址、任意的第四

层协议或端口对通信进行过滤(用于 IPSec 的访问列表只用于定义哪些通信将受到 IPSec 的保护，而不是定义哪些通信允许通过或禁止通过某个接口。一个加密映射表集合可包含多个加密映射表，每个都对应一个不同的访问列表。

当报文匹配某个特定访问列表中的第一条 permit 规则时，并且相应的加密映射表类型为 ipsec-isakmp，将由 IPSec 来处理。如果没有保护报文的安全联盟存在，IPSec 使用 IKE 来和对端协商建立安全联盟。

如果加密映射表类型为 ipsec-manual，将由 IPSec 来处理。如果没有保护报文的安全联盟存在，报文将被丢弃。在这种情况下，安全联盟通过手工配置，而无需 IKE。如果安全联盟不存在，那么一定没有配置所有必须的参数。

安全联盟集合一旦被建立，就被应用于处理报文，以及随后的适用报文。适用报文是指那些满足相同访问列表条件的报文。

如果使用 IKE 来建立安全联盟，那么这些安全联盟将具有生命周期，它们将阶段性地超时，需要重新协商（这提供了一层附加的安全性）。

IPSec 两端可以存在多条 IPSec 隧道来对不同数据流进行加密，每条隧道对应一个独立的安全联盟集合。例如，一些数据流可能只需要被验证，同时另一些数据流既需要被加密又需要被验证。IPSec 加密映射表所设置的访问列表指定了需要对哪些通信进行 IPSec 保护。进入报文依据加密映射表进行处理——如果一个未加密报文匹配了和一个 IPSec 加密映射表设置的特定访问列表中的 permit，这个报文将被丢弃，因为它不是作为一个受 IPSec 保护的报文被传送的。加密映射表同时包括了变换集合。一个变换集合是安全性协议、算法以及将用于受 IPSec 保护的通信的其它设置的组合。在 IPSec 安全联盟协商期间，一致使用一个特定的变换集合来保护一个数据报文。

4.1.5 IPSec 嵌套

你可以在一系列的 IPSec 路由器上进行 IPSec 通信的嵌套。例如，为了使通信横穿多个防火墙（这些防火墙都有相应的策略，不允许自己不能验证的通信通过），路由器需要按次序和每个防火墙建立 IPSec 隧道。

在下图所示的例子中，路由器 A 使用 IPSec 对去往路由器 C 的通信进行封装（路由器 C 是 IPSec 对端）。但是，在路由器 A 能够传送通信之前，它必须使用 IPSec 对这个通信进行预封装，其目的是为了将报文传送给路由器 B。

图 4-1 IPSec 路由器嵌套示例图

外部 IPSec 两端之间可能拥有同一种保护（例如数据验证），内部 IPSec 两端之间也可能拥有不同的保护（例如既有数据验证，又有加密）。

4.2 IPSec配置任务列表

在完成 IKE 配置以后，进行 IPSec 配置。要配置 IPSec，就要在每台参与通信的 IPSec 路由器上完成下列各节的操作。

- 确保访问列表和 IPSec 相兼容
- 创建加密访问列表
- 加密访问列表技巧
- 在加密访问列表中使用 any 关键字
- 定义变换集合
- 创建加密映射表
- 应该建立多少个加密映射表
- 创建手工方式的加密映射表
- 创建使用 IKE 的加密映射表
- 将加密映射表集合应用于接口

4.3 IPSec配置任务

4.3.1 确保访问列表和 IPSec 相兼容

IKE 使用 UDP 端口 500。IPSec ESP 和 AH 协议使用 IP 协议号 50、51。确信在配置访问列表时，IPSec 使用的接口上协议 50、51 以及 UDP 端口 500 的通信没有被禁止

4.3.2 创建 id 身份验证配置

主模式中协商中验证对端是否正确的协商对象使用 id，id 通常情况下使用 ip 地址作为验证内容。部分情况下允许使用 ip 地址以外的方式验证，包括 fqdn,dn 等。

通过创建一个 id 验证，用户可以指定 id 验证中使用的 id 类型和 id 内容。

在全局配置态下使用下列命令来定义一个 id 配置：

先需要在全局状态下定义 id 的类型:

Crypto isakmp identity address/dn/hostname (默认是 address, dn 还不支持)

然后定义本地的 id 内容：

Crypto isakmp client-id [ID name]

4.3.3 创建加密访问列表

加密访问列表用于定义哪些 IP 通信要被加密保护，哪些不要被加密保护（这些访问列表和一般的访问列表不同，一般的访问列表用于决定一个接口上的哪些通信可以通过，哪些要被禁止）。

IPSec 加密映射表指定的加密访问列表有四个主要功能：

- 判断由 IPSec 进行保护的出报文（permit 为保护）。
- 当开始协商 IPSec 安全联盟时，指示数据流将由新安全联盟进行保护（由一条单独的 permit 指出）。
- 处理入报文，其目的是过滤和丢弃那些本应受到 IPSec 保护而没有受到保护的通信。
- 在处理 IPSec 对端发起的 IKE 协商时，决定是否接受其 IPSec 安全联盟申请。
- 如果想让某种报文使用一种 IPSec 保护的组合（例如，只是验证），另一种报文使用另一种不同的 IPSec 保护的组合（例如，既要验证又要加密），那么就需要创建两个不同的加密访问列表来定义这两种不同类型的通信。这两个不同的访问列表用在不同的加密映射表中，这些加密映射表设定了不同的 IPSec 策略。

以后应用加密映射表集合到接口的时候，就把这些加密访问列表和这些接口联系起来了。在全局配置态下使用下列命令来创建加密访问列表：

命令	目的
ip access-list extended *name*	进入的IP访问扩展列表配置模式。
permit	允许命令设置访问规则。
deny	禁止命令设置访问规则。
protocol source *source-mask* **destination** *destination-mask*	定义哪些IP通信要被加密保护。

4.3.4 加密访问列表技巧

使用 permit 关键字将使得满足条件的所有 IP 通信都受到相应加密映射表中所描述策略的加密保护。使用 deny 关键字可以防止通信受到特定加密映射表的加密保护（换句话说，它不允许此加密映射表中指定的策略被应用到这个通信上）。如果某通信被接口上的所有加密映射表拒绝，那么该通信将不被加密保护。

在定义了相应的加密映射表，并且将加密映射表集合应用到接口上以后，所指定的加密访问列表将被应用到这个接口上。入和出报文将被相同的 IPSec 访问列表进行判定。因此，访问列表既对出报文正向使用，又对入报文反向使用。所以只需在访问列表中定义一条规则，IPSec 在使用这个规则时会匹配具有正好相反的源和目标地址的数据报文。

如果为一个给定的加密访问列表配置了多条规则，那么起作用的只是第一条规则。

4.3.5 在加密访问列表中使用 any 关键字

在创建加密访问列表的时候，使用 any 关键字可能会带来问题。所以不提倡用 any 关键字来指定源或目标地址。

当需要通过 IPSec 接口传输多点传送的通信时，不提倡在 permit 语句中使用 any 关键字；any 关键字将导致多点传送失败。permit any any 语句尤其不宜使用，因为这将导致所有的出报文受到保护（并且所有的受保护报文都被发送到在相应的加密映射表中指定的对端），并且将要求所有的入报文都要受到保护。

4.3.6 定义变换集合

变换集合是特定安全协议和算法的组合。在 IPSec 安全联盟协商期间，两端协商使用一个特定的变换集合来保护特定的数据流。

可以定义多个变换集合，然后在一个加密映射表中设置这些变换集合中的一个或多个。

在 IKE 协商安全联盟时，两端会查找双方一致的变换集合，当找到这样的变换集合后，安全联盟使用这变换集合保护保护特定的数据流。

对于手工建立的安全联盟，两端之间不存在协商过程，所以双方必须指定相同的变换集合。

如果对变换集合的定义进行改变，那么改变将只被应用于设置了这个变换集合的加密映射表中。改变将不被应用于现存的安全联盟，但它将被应用于随后建立新安全联盟的协商中。如果想让这些新的设置马上生效，可以通过使用 clear crypto sa 命令将安全联盟数据库部分或全部清除。

在全局配置态下使用下列命令来定义一个软件加密变换集合：

命令	目的
crypto ipsec transform-set *transform-set-name algorithm1 algorithm2 …*	定义一个变换集合执行此命令将进入加密变换配置态。
mode [**tunnel** | **transport**]	（可选）改变变换集合的模式。模式设置只对那些源和目标地址都是IPSec两端地址的通信有用；对于所有其他通信无效（所有其他通信都只在隧道模式下进行），默认是tunnel。
exit	退出加密变换配置态。

下表为可行的变换组合：

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）	esp-des	采用DES的	esp-md5-hmac	带 MD5

	的AH验证算法		ESP加密算法		（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
		esp-aes128	采用AES的ESP加密算法（128位）		
		esp-aes192	采用AES的ESP加密算法（192位）		
		esp-aes256	采用AES的ESP加密算法（256位）		

4.3.7 创建加密映射表

关于加密映射表

为 IPSec 创建的加密映射表包括以下部分：

- 哪些通信应该受到 IPSec 保护（加密访问列表）
- 将受到一个安全联盟集合保护的数据流间隔
- 用于 IPSec 通信的对端地址
- 用于 IPSec 通信的本端地址
- 对这些通信应用哪些 IPSec 安全策略（从一个或多个变换集合中选择）
- 安全联盟是手工建立还是通过 IKE 建立
- 其他可能用于定义 IPSec 安全联盟的参数

具有相同加密映射表名（但映射序列号不同）的加密映射表组成一个加密映射表集合。然后将加密映射表集合应用到接口上；这样，所有通过这接口的 IP 报文都将被应用在接口上的加密映射表集合进行判断。如果一个加密映射表匹配到应该受到保护的出报文，并且加密映射表指定了使用 IKE，将根据该加密映射表中所包含的参数与对端进行安全联盟协商。如果加密映射表使用手工建立的安全联盟，那么安全联盟在进行配置时就必须已经被建立好了。如果是本地发起协商，那么将使用加密映射表中指定的策略来创建发送给 IPSec 对端。如果是 IPSec 对端发起协商，那么本地路由器将在加密映射表检查对端所提供的策略，再决定是接受还是拒绝对端的申请。

为了使 IPSec 两端之间的 IPSec 通信能够顺利进行，两端的加密映射表必须包含相兼容的配置语句。

当两端尝试建立安全联盟时，双方都必须至少有一条加密映射表和对端的一条加密映射表相兼容。两条加密映射表相兼容必须至少满足以下条件：

- 加密映射表必须包含兼容的加密访问列表。
- 双方的加密映射表都必须确定对端地址。
- 加密映射表必须至少有一个相同的变换集合。

4.3.8 应该建立多少个加密映射表

对于单个接口可以只应用一个加密映射表集合。加密映射表集合中包含了 IPSec/ipsec-isakmp，或 IPSec/ipsec-manual 的组合。如果想要将相同的策略应用到多个接口上，也可以让多个接口共享同一加密映射表集合。

如果为给定的接口创建多个加密映射表，那么就要使用映射的 seq-num 参数将这些映射排序；seq-num 值越小，优先级越高。在配有这个加密映射表集合的接口上，首先用高优先级的映射对通信进行判断。如果存在下面几种情况中的一种，就必须为一个接口创建多个加密映射表：

- 如果不同的数据报文将由不同的 IPSec 对端进行处理。
- 如果想要对不同类型的数据报文应用不同的 IPSec 安全策略；例如，想让一组子网间的通信使用验证，而另一组子网间的通信既使用验证又使用加密。在这种情况下，不同类型的通信应该在两个不同的访问列表中被定义，并且必须为每个加密访问列表创建一个单独的加密映射表。
- 如果使用手工方式建立安全联盟，并且想要指定多个访问列表，那么必须创建不同的访问列表（每一个包含一条 permit），并且为每一个访问列表指定一个单独的加密映射表集合。

4.3.9 创建手工方式的加密映射表

手工安全联盟的使用是本地路由器和 IPSec 对端管理员之间预先安排的结果。双方可能想在开始的时候使用手工安全联盟，然后再使用基于 IKE 的安全联盟上来，或者远端系统可能不支持 IKE。如果不用 IKE 来建立安全联盟，那么就不存在安全联盟的协商过程，所以为了 IPSec 顺利处理报文，两端的配置必须完全一样。

路由器可以同时支持手工建立安全联盟，又支持 IKE 建立安全联盟。

要创建创建手工方式的加密映射表，在全局配置态下使用下列命令：

命令	目的
crypto map *map-name seq-num* **ipsec-manual**	创建或修改的加密映射表，执行此命令将进入加密映射表配置态。
match address *access-list-name*	设置IPSec访问列表。这个访问列表决定哪些

	报文受到IPSec的保护，哪些报文不受到此加密映射表中定义的IPSec安全性的保护。
set peer *ip-address*	设置IPSec对端地址。受到IPSec保护的报文将被发往这个地址。
set transform-set *transform-set-name*	设置变换集合（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）。
set security-association inbound ah *spi hex-key-data* 和 **set security-association outbound ah** *spi hex-key-data*	如果指定的变换集合包括了AH协议，则要使用这条命令来为出和入的报文设置AH安全参数索引（SPIs）和密钥。这条命令手工指定了AH安全联盟将用于保护报文。
set security-association inbound esp *spi* [**cipher** *hex-key-data*][**authenticator** *hex-key-data*]和**set security-association outbound esp** *spi* [cipher *hex-key-data*] [**authenticator** *hex-key-data*]	如果指定的变换集合包括了ESP协议，那么就要使用这条命令来为出和入报文设置ESP安全参数索引和密钥。如果变换集合包括了ESP加密算法，必须给出加密密钥。如果变换集合包括了ESP验证算法，必须给出验证密钥。这条命令手工指定了ESP安全联盟将用于保护通信。
exit	退出加密映射表配置态，并返回全局配置态。

重复这些步骤来建立其他加密映射表。

4.3.10 创建使用 IKE 的加密映射表

要创建使用 IKE 来建立安全联盟的加密映射表，在全局配置态下使用下列命令：

命令	目的
crypto map *map-name seq-num* **ipsec-isakmp**	创建或修改的加密映射表，执行此命令将进入加密映射表配置态。
match address *access-list-name*	设置IPSec访问列表。这个访问列表决定哪些报文受到IPSec的保护，哪些报文不受到此加密映射表中定义的IPSec安全性的保护。
set peer *ip-address*	设置IPSec对端地址。受到IPSec保护的报文将被发往这个地址。
set transform-set *transform-set-name1* [*transform-set-name2...transform-set-name6*]	设置变换集合，可以指定不多于六个加密映射表集合（第一个具有最高优先级）。
set security-association lifetime seconds *seconds*或**set security-association lifetime kilobytes** *kilobytes*	（可选）设置加密映射表进行协商的安全联盟的生命周期。
set pfs [**group1 | group2**]	（可选）指定IPSec使用此加密映射表申请新安全联盟时，同时申请理想转发安全机制，还要求从IPSec对端发回的申请中必须有PFS要求。
exit	退出加密映射表配置态，并且返回全局配置态。

重复这些步骤来建立其他加密映射表。

4.3.11 将加密映射表集合应用于接口

要使配置的加密映射表开始工作，要将加密映射表集合应用于接口。路由器使用该加密映射表集合来判断通过此接口的所有报文，并在安全联盟协商过程中，对不同的受保护的报文使用特定的策略。

要将加密映射表集合应用于接口，在接口配置态下使用下面的命令。

命令	目的
crypto map *map-name*	将加密映射表集合应用于接口。

可以将同一加密映射表集合应用于多个接口。

4.4 IPSec配置示例

下面是使用 IKE 协商安全联盟的 IPSec 配置的例子。

关于 IKE，请参考“配置 IKE”文档。

1. 定义加密访问列表

```
ip access-list extended aaa
permit ip 130.130.0.0 255.255.0.0 131.131.0.0 255.255.0.0
```

2. 定义 id 配置

```
Crypto isakmp identity hostname
Crypto isakmp client-id abc
```

3. 定义变换集合

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

4. 加密映射表设置 IPSec 访问列表和变换集合，并指定加密报文发往何处（IPSec 对端）：

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

5. 将加密映射表作用于接口

```
interface Serial1/1
ip address 192.2.2.2
crypto map toShanghai
```

6. 将加密映射属性作用于 tunnel 接口 (部分版本不支持)

```
crypto ipsec transform-set tset esp-des
crypto ipsec profile ipsec_profile
    set transfomr-set tset
int tunnel 1
    tunnel protection ipsec profile ipsec_profile
```

tunnel 上经过的报文都会被 ipsec_profile 保护

第5章　配置 Internet 密钥交换安全协议

5.1　概述

本章讨论如何配置 Internet 密钥交换（IKE）协议。IKE 是一种密钥管理协议标准，与 IPSec 标准一起使用。IPSec 可以不使用 IKE，但 IKE 通过提供额外功能、灵活性及使 IPSec 更易于配置，增强了 IPSec 的功能。IKE 是一种混合协议，该协议在因特网安全联盟及密钥管理协议（ISAKMP）框架内实现了 Oakley 密钥交换和 Skeme 密钥交换（ISAKMP、Oakley 和 Skeme 是 IKE 实现的安全协议）。

5.1.1　IKE 概要

IKE 自动地处理 IPSec 安全联盟（SA），无需预先手工配置而进行 IPSec 安全通信。IKE 提供了下列好处：

- IKE 避免了在通信两端的加密映射表中用手工设置所有的 IPSec 安全参数。
- IKE 允许指定 IPSec 安全联盟的生命周期。
- IKE 允许在 IPSec 会话期间更换加密密钥。
- IKE 允许 IPSec 提供抗重播服务。
- IKE 允许在端与端之间动态验证。

5.1.2　支持的标准

路由器实现了下列标准：

IPSec——IPSec 是一种开放标准体制，在端与端之间提供数据加密、数据完整性以及数据验证服务。IPSec 在 IP 层提供这些安全服务，使用 IKE 来协商协议及算法，并生成 IPSec 所用的加密和验证密钥。IPSec 可以用来保护一对主机之间、一对安全网关之间或者一个安全网关与一台主机之间的一个或多个数据流。

IKE——该混合协议在 ISAKMP 框架内实现了 Oakley 和 Skeme 密钥交换协议，可以与其它协议一起使用，而其最初实现的目的是与 IPSec 协议一起使用。IKE 提供了 IPSec 两端的验证，协商 IPSec 密钥以及协商 IPSec 安全联盟。

ISAKMP——该协议框架定义了有效负荷的格式，实现密钥交换协议的机制以及安全协会的协商。

Oakley——一种密钥交换协议，定义如何得到验证的密钥材料。

Skeme——一种密钥交换协议，定义如何得到验证的密钥材料，并可进行快速密钥更新。

5.1.3 术语

DES——数据加密标准（DES）。

3DES——3DES 用于对包数据进行加密。

AES——高级加密标准(AES)

Diffie-Hellman——一种公钥加密协议，允许两个组在非保密的通信信道上建立共享的秘密。Diffie-Hellman 与 IKE 一起使用建立会话密钥。支持 768 比特和 1024 比特 Diffie-Hellman 组。

MD5（HMAC 变量）——MD5 是一种散列算法。HMAC 是一个用于对数据进行验证的加密散列变量。

SHA（HMAC 变量）——SHA 是一种散列算法。HMAC 是一个用于对数据进行验证的加密散列变量。

5.2 IKE配置任务列表

要配置 IKE，执行下面各节的任务。开头三节的任务是必需的；其余的是可选的，这取决于所配置的参数。

- 确保访问列表与 IKE 兼容
- 创建 IKE 策略
- 配置预共享密钥
- 清除 IKE 连接（可选）
- IKE 诊断（可选）

5.3 IKE配置任务

5.3.1 确保访问列表与 IKE 兼容

IKE 协商使用端口 500 的 UDP。确保 UDP 端口 500 的通信在 IKE 和 IPSec 使用的接口上不被禁止。在有些情况下需要在访问列表中增加一条规则来明确地允许 UDP 端口 500 的报文。

5.3.2 创建 IKE 策略

必须在 IPSec 两端创建 IKE 策略。IKE 策略定义了在 IKE 协商期间使用的安全参数组合。

要创建 IKE 策略，注意以下问题：

- 创建策略的原因
- 策略中定义的参数
- IKE 如何达成匹配的策略
- 确定策略参数值
- 创建策略
- IKE 策略所需要的额外配置

1. 创建策略的原因

IKE 协商必须被保护起来，因此每个 IKE 协商从达成公共的 IKE 策略开始。这个策略描述了使用哪些安全参数来保护后续的 IKE 协商。

在两端达成公共的一个 IKE 策略后，该策略的安全参数由每端建立的 ISAKMP 安全联盟标识，在协商期间这些安全联盟将应用于所有的后续 IKE 通信。

必须在每端创建多个具有不同优先级的策略，以确保至少有一个策略能够匹配远端的策略。

2. 策略中定义的参数

在每个 IKE 策略中定义五个参数：

参数	接受的值	关键字	缺省值
加密算法	56位 DES-CBC	des	56位 DES-CBC
	168位3DES-CBC	3des	
	128位AES-CBC	aes128	
	192位AES-CBC	aes192	
	256位AES-CBC	aes256	
哈希算法	SHA-1 MD5	sha md5	SHA-1
验证方法	预共享密钥 RSA签名 RSA 实时加密	pre-share rsa-sig rsa-encr	预共享密钥
Diffie-Hellman组标识	768比特 Diffie-Hellman 1024比特Diffie-Hellman	1 2	768比特Diffie-Hellman
安全联盟的生命周期	可以指定60到86400秒之间任意数目的秒数	–	86400 秒 (一天)

3. IKE 如何达成匹配的策略

当 IKE 协商开始时，IKE 寻找一个在两端都一样 IKE 策略。发起协商端将其所有的策略发给远端，而远端会试着寻找一个匹配的策略。远端通过将其最高优先级的策略与所接收到的策略相比较来寻找匹配项。远端按优先级的次序（最高优先级优先）检查其每一种策略直到发现一个匹配的策略。

当来自两端的策略均包括相同的加密、哈希、验证及 Diffie-Hellman 参数值，并且当远端的策略所指定的生命周期小于或等于所比较的策略生命周期时作出匹配选择。

如果没有发现可接受的匹配策略，IKE 拒绝协商，从而不会建立 IPSec。

如果找到一种匹配的策略，IKE 将完成协商，并且创建 IPSec 安全联盟。

注意：

根据策略中指定的验证方法的不同，需要对参数进行额外的配置。

4. 确定策略参数值

加密算法有两个选择：56 位 DES-CBC 和 168 位 3DES-CBC。3DES-CBC 更安全。

哈希算法有两个选项：SHA-1 和 MD5。MD5 的摘要信息较少，要比 SHA-1 快一些。针对 MD5 的攻击有一种被证明是成功的（但极其困难）；然而，由 IKE 使用的 HMAC 变体能阻止这种攻击。

验证方法有三种选择：目前只支持预共享密钥。

Diffie-Hellman 组有两种选择：768 比特或 1024 比特 Diffie-Hellman。1024 比特 Diffie-Hellman 较难于攻克，但要求更多的 CPU 时间来执行。

安全联盟的生命周期可以设置为 60 到 86400 秒之间任意值。生命周期越短，IKE 协商将越安全，但 CPU 开销也超大。对于较长的生命期，后面 IPSec 安全联盟可以更快地建立起来。关于该参数的更多信息以及如何使用该参数，参见 lifetime（IKE 策略）命令的命令描述。

5. 创建策略

可以创建多重 IKE 策略，每条策略对应不同的参数值组合。对所创建的每一条策略，须分配唯一的优先权（1 到 10000，1 是最高优先级）。

可以在每台终端上配置多重策略——然而至少这些策略中的某条策略必须包含与远程终端上某个策略完全一样的加密、哈希、验证及 Diffie-Hellman 参数值。

如果不配置任何策略，则路由器使用缺省的策略，该策略总是设为最低优先级，并包含每个参数的缺省值。

要配置一条策略，在全局配置模式下使用下面的命令：

命令	目的
crypto isakmp policy *priority*	创建IKE策略（每条策略唯一地由优先级标识）

	（该命令使你进入ISAKMP策略配置态）。
encryption {**des**|**3des**|**aes128**|**aes192**|**aes256**}	指定加密算法。
hash {**sha | md5**}	指定哈希算法。
authentication { **pre-share**|**rsa-sig**|**rsa-encr**}	指定验证方法。
group {**1 | 2**}	指定Diffie-Hellman组。
lifetime *seconds*	指定IKE安全联盟的生命周期。
exit	退出ISAKMP策略配置态。

如果不给参数指定数值，则使用缺省值。

注意：

在发出 show running 命令时，缺省策略和所配置的策略的缺省值并不在配置中显示出来。要查看缺省策略和所配置的策略内的缺省值，使用 show crypto isakmp policy 命令。

6. IKE 策略所需要的额外配置

预共享密钥验证方法：如果在策略中指定预共享密钥作为验证方法，则必须配置预共享密钥。

5.3.3 配置预共享密钥

在 IPSec 两端指定共享密钥。注意所给的预共享密钥是在两端共享的。在两端上应当指定相同的密钥。

要在配置预共享密钥，在全局配置态下使用下面的命令：

命令	目的
crypto isakmp key 0 keystring address *peer-address*	在本端：指定与远端一起使用的共享密钥。
crypto isakmp key 0 keystring address *peer-address*	在远端：指定与本端一起使用的共享密钥。

5.3.4 配置 RSA (暂时不支持)

在 IPSec 两端指定对端公共的公钥。注意所给的预共享密钥是在两端非共享的。在两端上应当指定对应的公钥。

要在配置预共享密钥，在全局配置态下使用下面的命令：

命令	目的
crypto key generate	生成RSA 密钥对

crypto key pubkey-chain rsa **address-key** *peer-address* **key-string** *HEX-data*	配置对端的公钥

5.3.5 配置证书(部分版本支持)

使用证书认证。

要在配置预共享密钥，在全局配置态下使用下面的命令：

命令	目的
crypto pki trustpoint *name* **subject-name** *subject*	配置信任点以及参数
crypto pki authenticate *name*	导入根证书
crypto pki enrollment *name*	生成本地证书请求
crypto pki import *name* **certificate**	导入本地证书

5.3.6 配置 DPD(dead peer detection)(可选)

在 IPSec 一端配置 DPD 功能。注意必须对端也支持 DPD。

要 IPSec DPD，在全局配置态下使用下面的命令：

命令	目的
crypto isakmp keepalive *seconds on-demand*	On demand 是真正意义上的dpd,在一段时间没有收到对端报文，并且本地需要发送报文时，才会触发 isakmp information 报文。 On demand 模式没有重传的设定。一次探测失败即认为失败
crypto isakmp keepalive *seconds retry-number period*	这个是周期性的keepalive发送，是传统的检测方式，可设定发送周期，和失败时的重传次数

5.3.7 配置 EZVPN 服务器(暂时不支持)

在 IPSec 一端配置 EZVPN 服务器功能。注意必须对端配置为 EZVPN 客户端。

要配置 IPSec EZVPN 服务器，在全局配置态下使用下面的命令：

命令	目的

aaa authentication login *authenlist* **local**	配置认证列表
aaa authorization network *authorlist* **local**	配置授权列表
username *admin* **password** *admin*	配置用户名密码
crypto map *bdcom* **client authentication list** *authenlist*	配置map相关认证列表
crypto map *bdcom* **isakmp authorization list** *authorlist*	配置map相关授权列表
crypto isakmp client configuration group *groupname*	创建group
key *pre-key*	配置预共享密钥
dns *dns-server1 dns-server2*	配置dns服务器地址（可选）
domain *domain-string*	配置域名（可选）
pool *pool-name start-address end-address*	配置地址池
acl *acl-name*	配置acl(可选)
save-password	配置密码保存（可选）
pfs	配置开启pfs（可选）

5.3.8 配置 EZVPN 客户端(可选)

在 IPSec 一端配置 EZVPN 客户端功能。注意必须对端配置为 EZVPN 服务器。

要配置 IPSec EZVPN 客户端，在全局配置态下使用下面的命令：

命令	目的
crypto ipsec client ezvpn *vpn-name*	创建ezvpn tunnel
group *group-name* **key** *pre-key*	配置group、预共享密钥
peer *peer-address*	配置服务器地址
mode *[client | network-extension | network-plus]*	配置tunnel模式
connect *[auto | manual | acl]*	配置连接方式
Acl *acl-name*	配置acl（可选）
username *admin* **password** *admin*	配置用户名密码（可选）
xuaht userid mode interactive	配置认证方式
crypto ipsec client ezvpn *vpn-name* **inside**	配置入端口（端口下配置）
crypto ipsec client ezvon *vpn-name* **outside**	配置出端口（端口下配置）

5.3.9 清除 IKE 连接（可选）

如果需要，可以清除已经存在的 IKE 连接。要清除 IKE 连接，在管理态使用下面的命令：

命令	目的
show crypto isakmp sa	显示存在的isakmp SA 。
clear crypto isakmp [**map** *map-name* | **peer** *ip-address*]	清除isakmp连接。

5.3.10 IKE 诊断（可选）

要在 IKE 诊断中获取帮助，在管理态使用下面的命令：

命令	目的
show crypto isakmp policy	浏览IKE策略的参数。
show crypto sa isakmp	浏览所有当前IKE安全联盟。
debug crypto isakmp	显示关于IKE事件的debug消息。

在完成 IKE 配置后，可以配置 IPSec。参见“配置 IPSEC”

5.4 IKE配置示例

本例创建了两个 IKE 策略，其中策略 10 为最高优先级，策略 20 为下一个优先级，已知的缺省优先级为最低的优先级。该策略同时创建一条预共享密钥，与 IP 地址为 192.168.1.3 的远端策略一起使用。

```
crypto isakmp policy 10
encryption des
hash md5
authentication pre-share
group 2
lifetime 5000
crypto isakmp policy 20
authentication pre-share
lifetime 10000
crypto isakmp key 0 1234567890 address 192.168.1.3
```

在上面示例中，策略 10 的 encryption des 在书面配置中将不会出现，因为这是加密算法参数的缺省值。