目 录

第1章 网络安全配置

1.1 VRP 提供的网络安全特性简介

路由器必须防范来自公网上的恶意攻击。另外，有时用户无意识但有破坏性的访问也会导致设备的性能下降，甚至无法正常工作。因此，其安全特性有特别重要的地位。

VRP 提供的网络安全特性：

- 基于 RADIUS（Remote Authentication Dial-In User Service）的 AAA（Authentication, Authorization, Accounting）服务：与 RADIUS 服务器配合实施的 AAA 服务，可以提供对接入用户的验证、授权和计费安全服务，防止非法访问。
- 验证协议：在 PPP 线路上支持 CHAP 和 PAP 验证。
- 包过滤（Packet Filter）：用访问控制列表实现，允许指定可以通过（或禁止通过）路由器的报文类型。
- 应用层报文过滤 ASPF（Application Specific Packet Filter）：也称为状态防火墙，是一种高级通信过滤，它检查应用层协议信息并且监控基于连接的应用层协议状态，维护每一个连接的状态信息，并动态地决定数据包是否被允许通过防火墙或者被丢弃。
- 网络层安全（IP Security，IPSec）：特定的通信方之间在 IP 层通过加密与数据源验证，来保证数据包在 Internet 上传输时的私有性、完整性和真实性。
- 事件日志：记录系统安全方面事件，实时跟踪非法侵入。
- 地址转换：NAT 网关将公共网络和企业内部网分隔离开来，在公共网络中隐藏企业内部设备的 IP 地址，阻止来自公共网络上的攻击。
- 相邻路由器验证：确保所交换路由信息的可靠性。
- 视图分级保护：将用户分成 4 级，每级用户赋予不同的配置权限，级别低的用户不能进入更高级的视图。

本章中将详细介绍 AAA 及 RADIUS 配置、用户口令配置、防火墙和包过滤配置等，IPSec 配置，IKE 配置。PPP 验证协议配置请参见链路层协议中的 PPP 配置，日志的配置请参见系统管理中日志配置，地址转换请参见网络协议中的 NAT 配置部分内容，相邻路由器验证请参见路由协议中各路由协议的配置。

1.2 命令行分级保护

系统命令行采用分级保护方式，命令行划分为参观级、监控级、配置级、管理级 4 个级别，只有提供了正确的登录口令，才能使用相应的命令。

1.3 基于 RADIUS 的 AAA

AAA 是验证（Authentication）、授权（Authorization）、计费（Accounting）的缩写，用来实现访问用户管理功能。AAA 可以用多种协议来实现，这里 AAA 是基于 RADIUS 协议来实现的。

AAA 提供如下功能：

- 用户的分级管理：用户可以对系统的配置数据进行管理维护，对设备进行监控和维护等操作，而这些操作对系统的正常运行至关重要。因此要对用户进行严格分级管理，不同级别的用户有不同的权限；低级别的用户只能进行一些查看操作，只有高级用户才能进行一些如修改数据、维护设备，以及其它比较敏感的操作。所有用户都必须进行口令验证，否则无法进入系统。
- PPP 用户的验证：建立 PPP 连接时，对用户名进行验证。
- PPP 用户的地址管理和分配：建立 PPP 连接时，可以为 PPP 用户分配事先指定的 IP 地址。

第二章将详细介绍 RADIUS 协议及其配置、用户口令配置、PPP 用户地址配置。PPP 验证协议请参见链路层协议配置模块中的 PPP 配置。

1.4 包过滤和防火墙

1.4.1 防火墙的概念

防火墙一方面阻止来自因特网的对受保护网络的未授权或未验证的访问，另一方面允许内部网络的用户对因特网进行 Web 访问或收发 E-mail 等。防火墙也可以作为一个访问因特网的权限控制关口，如允许组织内的特定的人可以访问因特网。

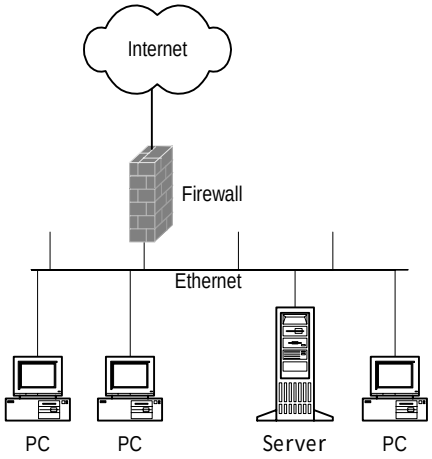

图1-1 防火墙使内部网络和因特网隔离

防火墙不单应用于和外部因特网的连接，也可以用于保护组织内部网络的大型机和重要资源（如数据）。对受保护数据的访问都必须经过防火墙的过滤，即使该访问是来自组织内部。

当外部网络的用户访问网内资源时，要经过防火墙；而内部网络的用户访问网外资源时，也会经过防火墙。这样，防火墙就起到了一个“ 警卫 ”的作用，可以将需要禁止的数据包在这里给丢掉。

1.4.2 防火墙的分类

一般把防火墙分为两类：网络层防火墙、应用层防火墙。网络层的防火墙主要获取数据包的包头信息，如协议号、源地址、目的地址和目的端口等，或者直接获取包头的一段数据；而应用层的防火墙则对整个信息流进行分析。

常见的防火墙有以下几种：

- 应用网关（Application Gateway）：检验通过此网关的所有数据包中的应用层的数据。如 FTP 应用网关，对于连接的 Client 端来说是一个 FTP Server，对于 Server 端来说是一个 FTP Client。连接中传输的所有 FTP 数据包都必须经过此 FTP 应用网关。
- 电路级网关（Circuit-Level Gateway）：此电路指虚电路。在 TCP 或 UDP 发起（Open）一个连接或电路之前，验证该会话的可靠性。只有在握手被验证为合法且握手完成之后，才允许数据包的传输。一个会话建立后，此会话的信息被写入防火墙维护的有效连接表中。数据包只有在它所含的会话信息符合该有效连接表中的某一条目（Entry）时，才被允许通过。会话结束时，该会话在表中的条目被删掉。电路级网关只对连接在会话层进行验证。一旦验证通过，在该连接上可以运行任何一个应用程序。以 FTP 为例，电路层网关只在一个

FTP 会话开始时，在 TCP 层对此会话进行验证。如果验证通过，则所有的数据都可以通过此连接进行传输，直至会话结束。

- 包过滤（Packet Filter）：对每个数据包按照用户所定义的项目进行过滤，如比较数据包的源地址、目的地址等是否符合规则。包过滤不管会话的状态，也不分析数据。如用户规定允许端口是 21 或者大于等于 1024 的数据包通过，则只要端口符合该条件，数据包便可以通过此防火墙。如果配置的规则比较符合实际应用的话，在这一层能够过滤掉很多有安全隐患的数据包。
- 地址转换（NAT）：地址转换又称地址代理，它实现了私有网络访问外部网络的功能。地址转换的机制就是将私有网络内主机的 IP 地址和端口替换为路由器的外部网络地址和端口，以及从路由器的端口转换为私有网络主机的 IP 地址和端口，即<私有地址+端口>与<公有地址+端口>之间的转换。私有地址是指内部网络或主机地址，公有地址是指在因特网上全球唯一的 IP 地址。因特网地址分配组织规定将下列的 IP 地址被保留用作私有地址：

10.0.0.0～10.255.255.255

172.16.0.0～172.31.255.255

192.168.0.0～192.168.255.255

也就是说这三个范围内的地址不会在因特网上被分配，可在一个单位或公司内部使用。各企业根据在预见未来内部主机和网络的数量后，选择合适的内部网络地址，不同企业的内部网络地址可以相同。如果一个公司选择上述三个范围之外的其它网段作为内部网络地址，则有可能会造成混乱。地址转换在允许内部网络的主机访问网外资源的同时，为内部主机提供“ 隐私 ”（Privacy）保护。

1.4.3 包过滤

1. 包过滤的功能

包过滤一般是指对 IP 数据包的过滤。对路由器需要转发的数据包，先获取包头信息，包括 IP 层所承载的上层协议的协议号、数据包的源地址、目的地址、源端口和目的端口等，然后和设定的规则进行比较，根据比较的结果对数据包进行转发或者丢弃。

包过滤（对 IP 数据包）所选取用来判断的元素如图 1-2 所示（图中 IP 所承载的上层协议为 TCP/UDP）。

图1-2 包过滤元素示意图

大多数包过滤系统在数据本身上不做任何事，不做基于内容的筛选。

2. 访问控制列表

为了过滤数据包，需要配置一些规则，规定什么样的数据包可以通过，什么样的数据包不能通过。这些规则就是通过访问控制列表（Access Control List）体现的。

用户需要根据自己的安全策略来确定访问控制列表，并将其应用到整机或指定接口上，路由器就会根据访问控制列表来检查所有接口或指定接口上的所有数据包，对于符合规则的报文作正常转发或丢弃处理，从而起到防火墙的作用。

作为包过滤的访问控制列表和用于 QoS 的复杂流分类规则一同处理，二者在原理和操作上几乎相同，只是匹配后的动作有区别。

1.5 交换路由信息时的安全认证

对于骨干路由器而言，维护正确的路由转发表是路由器正常工作的基础，而路由转发表的维护是通过相邻路由器动态交换路由信息来实现的。

1. 交换路由信息时进行安全认证的必要性

在网络上，相邻的路由器需要交换大量的路由信息，不可靠的路由器可能会发送攻击网络设备的信息。如果具有路由信息认证的功能，路由器会对收到的相邻路由器的交换路由更新报文进行认证处理，从而保证路由器只接收可靠的路由信息。

2. 认证的实现

相互交换路由信息的路由器都共享一个口令字，口令字与路由信息报文一起发送，收到路由信息的路由器对报文进行认证，检查报文中的口令字，如果与共享口令字相同，则接受报文，否则丢弃。

认证的实现有两种方式：明文认证和 MD5 认证。明文认证以明文形式发送口令字，安全性较低。而 MD5 认证是发送加密后的口令字，MD5 认证方式安全性较高。

第2章 AAA 及 RADIUS/HWTACACS 协议配置

2.1 简介

2.1.1 AAA 概述

AAA 是 Authentication，Authorization and Accounting（认证、授权和计费）的简称，它提供了一个用来对认证、授权和计费这三种安全功能进行配置的一致性框架，实际上是对网络安全的一种管理。

这里的网络安全主要是指访问控制，包括：

- 哪些用户可以访问网络服务器？
- 具有访问权的用户可以得到哪些服务？
- 如何对正在使用网络资源的用户进行计费？

针对以上问题，AAA 必须提供下列服务：

1. 认证功能

AAA 支持以下认证方式：

- 不认证：对用户非常信任，不对其进行合法检查，一般情况下不采用这种方式。
- 本地认证：将用户信息（包括本地用户的用户名、密码和各种属性）配置在宽带接入服务器上。本地认证的优点是速度快，可以为运营降低成本；缺点是存储信息量受设备硬件条件限制。
- 远端认证：支持通过 RADIUS 协议或 HWTACACS 协议进行远端认证，由宽带接入服务器做为 Client 端，与 RADIUS 服务器或 TACACS 服务器通信。对于 RADIUS 协议，可以采用标准 RADIUS 协议或华为 3COM 公司的扩展 RADIUS 协议，与 iTELLIN/CAMS 等设备配合完成认证。

2. 授权功能

AAA 支持以下授权方式：

- 直接授权：对用户非常信任，直接授权通过。
- 本地授权：根据宽带接入服务器上为本地用户帐号配置的相关属性进行授权。
- HWTACACS 授权：由 TACACS 服务器对用户进行授权。
- if-authenticated 授权：如果用户通过了验证，并且使用的验证方法不是 none，则对用户授权通过。

- RADIUS 认证成功后授权：RADIUS 协议的认证和授权是绑定在一起的，不能单独使用 RADIUS 进行授权。

3. 计费功能

AAA 支持以下计费方式：

- 不计费：不对用户计费。
- 远端计费：支持通过 RADIUS 服务器或 TACACS 服务器进行远端计费。

AAA 一般采用客户/服务器结构：客户端运行于被管理的资源侧，服务器上集中存放用户信息。因此，AAA 框架具有良好的可扩展性，并且容易实现用户信息的集中管理。AAA 是一种管理框架，因此，它可以用多种协议来实现，VRP 中 AAA 是基于 RADIUS 协议或 HWTACACS 协议来实现的。

2.1.2 RADIUS 协议概述

1. 什么是 RADIUS

RADIUS 是 Remote Authentication Dial-In User Service（远程认证拨号用户服务）的简称，它是一种分布式的、客户机/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常被应用在既要求较高安全性、又要求维持远程用户访问的各种网络环境中（例如，它常被应用来管理使用串口和调制解调器的大量分散拨号用户）。RADIUS 系统是 NAS（Network Access Server）系统的重要辅助部分。

RADIUS 服务包括三个组成部分：

- 协议：RFC2865、2866 协议基于 UDP/IP 层定义了 RADIUS 帧格式及消息传输机制，并定义了 1812 作为认证端口，1813 作为计费端口。
- 服务器：RADIUS 服务器运行在中心计算机或工作站上，包含了相关的用户认证和网络服务访问信息。
- 客户端：位于拨号访问服务器 NAS（Network Access Server）侧，可以遍布整个网络。

RADIUS 基于客户/服务器模型，NAS（如路由器）作为 RADIUS 客户端，负责传输用户信息到指定的 RADIUS 服务器，然后根据从服务器返回的信息进行相应处理（如接入/挂断用户）。RADIUS 服务器负责接收用户连接请求，认证用户，然后给 NAS 返回所有需要的信息。

RADIUS 服务器通常要维护三个数据库：第一个数据库“ Users ”用于存储用户信息（如用户名、口令以及使用的协议、IP 地址等配置），第二个数据库“ Clients ”用于存储 RADIUS 客户端的信息（如共享密钥），第三个数据库“ Dictionary ”存储的信息用于解释 RADIUS 协议中的属性和属性值的含义。如下图所示：

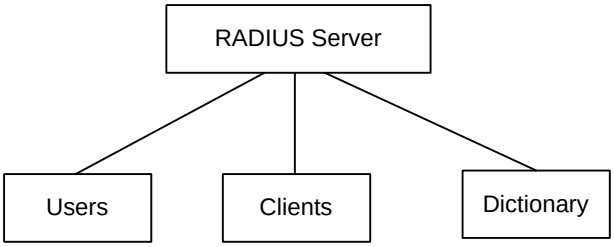

图2-1 RADIUS 服务器的组成

另外，RADIUS 服务器还能够作为其他 AAA 服务器的客户端进行代理认证或计费。RADIUS 服务器支持多种方法来认证用户，如基于 PPP 的 PAP、CHAP 认证、基于 UNIX 的 Login 等。

2. RADIUS 的基本消息交互流程

RADIUS 服务器对用户的认证过程通常需要利用 NAS 等设备的代理认证功能，RADIUS 客户端和 RADIUS 服务器之间通过共享密钥认证相互间交互的消息，用户密码采用密文方式在网络上传输，增强了安全性。RADIUS 协议合并了认证和授权过程，即响应报文中携带了授权信息。操作流程图和步骤如下所示：

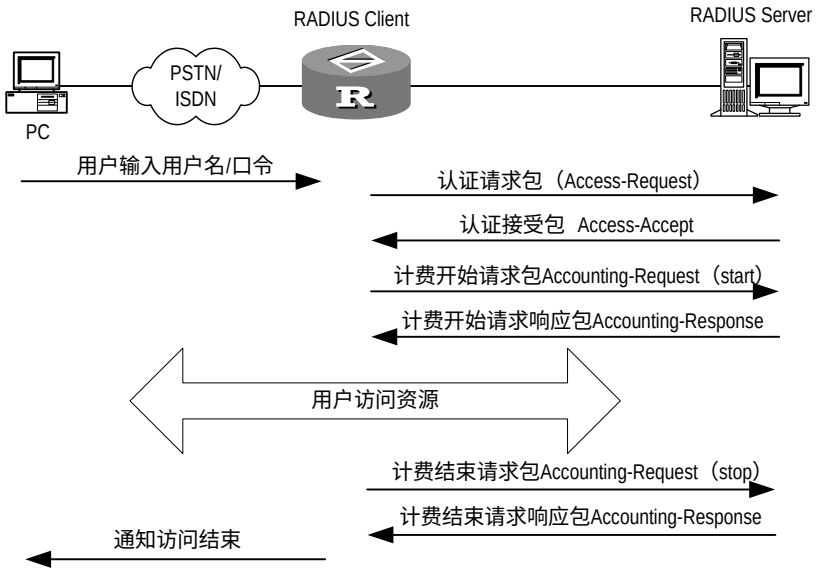

图2-2 RADIUS 的基本消息交互流程

基本交互步骤如下：

(1) 用户输入用户名和口令；

(2) RADIUS 客户端根据获取的用户名和口令，向 RADIUS 服务器发送认证请求包（Access-Request）。

(3) RADIUS 服务器将该用户信息与 Users 数据库信息进行对比分析，如果认证成功，则将用户的权限信息以认证响应包（Access-Accept）发送给 RADIUS 客户端；如果认证失败，则返回 Access-Reject 响应包。

(4) RADIUS 客户端根据接收到的认证结果接入/拒绝用户。如果可以接入用户，则 RADIUS 客户端向 RADIUS 服务器发送计费开始请求包（Accounting-Request），Status-Type 取值为 start；

(5) RADIUS 服务器返回计费开始响应包（Accounting-Response）；

(6) RADIUS 客户端向 RADIUS 服务器发送计费停止请求包（Accounting-Request），Status-Type 取值为 stop；

(7) RADIUS 服务器返回计费结束响应包（Accounting-Response）。

3. RADIUS 协议的报文结构

RADIUS 采用 UDP 传输消息，通过定时器管理机制、重传机制、备用服务器机制，确保 RADIUS 服务器和客户端之间交互消息正确收发。RADIUS 报文结构如下：

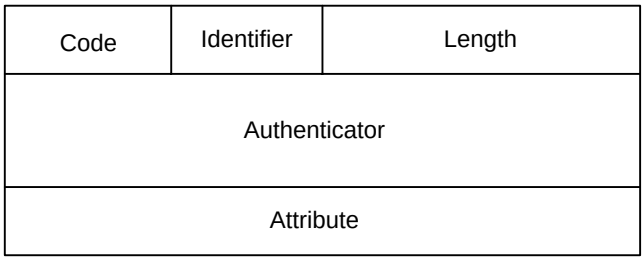

图2-3 RADIUS 报文结构

其中 Identifier 域用于匹配请求包和响应包，随着 Attribute 域改变、接收到有效响应包而不断变化，而在重传时保持不变化。Authenticator 域（16 字节）用于验证 RADIUS 服务器传输回来的请求，同时用于密码隐藏算法上，分为 Request Authenticator 和 Response Authenticator。

- Request Authenticator 采用 16 字节的随机码。
- Response Authenticator 以对 Code、Identifier、Request Authenticator 、Length、Attribute 和共享密钥进行 MD5 算法后的结果。

(1) 由 Code 域决定 RADIUS 报文的类型，主要包括：

表2-1 Code 域主要取值的说明

Code	报文类型	报文说明
1	Access-Request 认证请求包	方向 Client->Server，Client 将用户信息传输到 Server 以判断是否接入该用户。该报文中必须包含 User-Name 属性，可选包含 NAS-IP-Address、User-Password、NAS-Port 等属性。
2	Access-Accept 认证接受包	方向 Server->Client，如果 Access-Request 报文中所有 Attribute 值都是可以接受（即认证通过），则传输该类型报文。

Code	报文类型	报文说明
3	Access-Reject 认证拒绝包	方向 Server->Client，如果 Access-Request 报文中存在任何 Attribute 值无法被接受（即认证失败），则传输该类型报文。
4	Accounting-Request 计费请求包	方向 Client->Server，Client 将用户信息传输到 Server，请求 Server 开始计费，由该报文中的 Acct-Status-Type 属性区分计费开始请求和计费结束请求。该报文包含属性和 Access-Request 报文大致相同。
5	Accounting-Response 认证响应包	方向 Server->Client，Server 通知 Client 侧已经收到 Accounting-Request 报文并且已经正确记录计费信息。该报文包含端口上输入/输出字节数、输入/输出包数、会话时长等信息。

(2) Attribute 域携带专门的认证、授权和计费信息，提供请求和响应报文的配置细节，该域采用（Type、Length、Value）三元组的形式提供，RFC 中定义的标准 Attribute 域大致包括：

表2-2 Attribute 域主要取值的说明

Type	属性类型	Type	属性类型
1	User-Name	23	Framed-IPX-Network
2	User-Password	24	State
3	CHAP-Password	25	Class
4	NAS-IP-Address	26	Vendor-Specific
5	NAS-Port	27	Session-Timeout
6	Service-Type	28	Idle-Timeout
7	Framed-Protocol	29	Termination-Action
8	Framed-IP-Address	30	Called-Station-Id
9	Framed-IP-Netmask	31	Calling-Station-Id
10	Framed-Routing	32	NAS-Identifier
11	Filter-ID	33	Proxy-State
12	Framed-MTU	34	Login-LAT-Service
13	Framed-Compression	35	Login-LAT-Node
14	Login-IP-Host	36	Login-LAT-Group
15	Login-Service	37	Framed-AppleTalk-Link
16	Login-TCP-Port	38	Framed-AppleTalk-Network
17	(unassigned)	39	Framed-AppleTalk-Zone
18	Reply_Message	40-59	(reserved for accounting)
19	Callback-Number	60	CHAP-Challenge
20	Callback-ID	61	NAS-Port-Type

Type	属性类型	Type	属性类型
21	(unassigned)	62	Port-Limit
22	Framed-Route	63	Login-LAT-Port

RADIUS 协议具有良好的可扩展性，协议中定义的 26 号属性（Vender-Specific）可以被方便地扩展以支持用户自己定义的扩展属性，报文结构如下图所示：

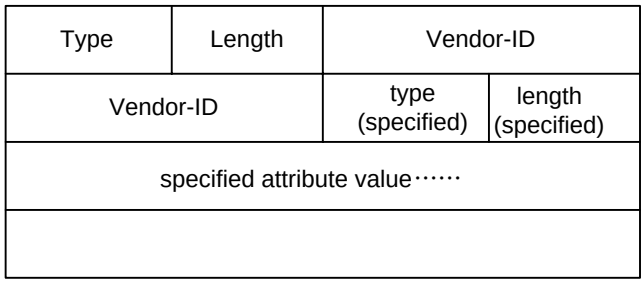

图2-4 包括扩展属性的 RADIUS 报文片断

2.1.3 HWTACACS 协议概述

1. HWTACACS 特性

HWTACACS 安全协议是在 TACACS（RFC1492）基础上进行了功能增强的一种安全协议。该协议与 RADIUS 协议类似，主要是通过 Server-Client 模式与 TACACS 服务器通信来实现多种用户的 AAA 功能，可用于 PPP 和 VPDN 接入用户及 login 用户的认证、授权和计费。

与 RADIUS 相比，HWTACACS 具有更加可靠的传输和加密特性，更加适合于安全控制。HWTACACS 协议与 RADIUS 协议的主要区别如下表：

表2-3 HWTACACS 协议和 RADIUS 协议区别

HWTACACS 协议	RADIUS 协议
使用 TCP，网络传输更可靠。	使用 UDP。
除了标准的 HWTACACS 报文头，对报文主体全部进行加密。	只是对验证报文中的密码字段进行加密。
认证和授权分离，例如，可以用一个 TACACS 服务器进行认证，另外一个 TACACS 服务器进行授权。	认证和授权一起处理。
适于进行安全控制。	适于进行计费。
支持对路由器上的配置命令进行授权使用。	不支持。

HWTACACS 的典型应用是拨号用户或终端用户需要登录到路由器上进行操作，路由器作为 HWTACACS 的客户端，将用户名和密码发给 TACACS 服务器进行验证，验证通过并得到授权之后可以登录到路由器上进行操作。如下图所示：

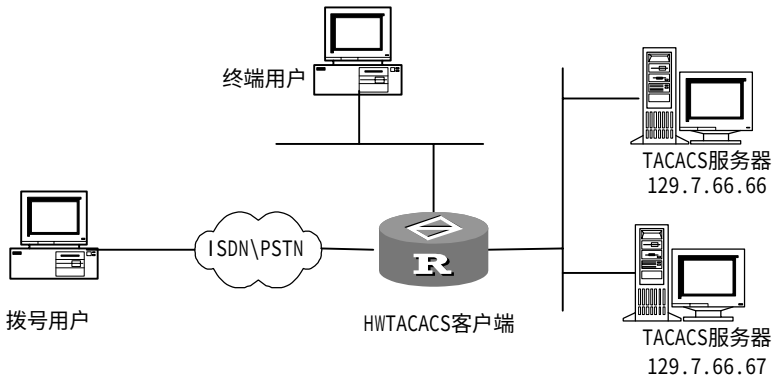

图2-5 HWTACACS 的典型应用组网图

2. HWTACACS 的基本消息交互流程

以 Telnet 用为例，使用 HWTACACS 对用户进行认证、授权和计费。在整个过程中的基本消息交互流程如下：

(1) 用户请求登录路由器，TACACS 客户端收到请求之后，向 TACACS 服务器发送开始认证报文；

(2) TACACS 服务器发送认证回应报文，请求用户名；TACACS 客户端收到回应报文后，向用户询问用户名；

(3) TACACS 客户端收到用户名后，向 TACACS 服务器发送认证持续报文，其中包括了用户名；

(4) TACACS 服务器发送认证回应报文，请求登录密码；TACACS 客户端收到回应报文，向用户询问登录密码；

(5) TACACS 客户端收到登录密码后，向 TACACS 服务器发送认证持续报文，其中包括了登录密码；

(6) TACACS 服务器 发送认证回应报文，指示用户通过认证；

(7) TACACS 客户端 向 TACACS 服务器发送用户授权报文；

(8) TACACS 服务器 发送授权回应报文，指示用户通过授权；

(9) TACACS 客户端 收到授权回应成功报文，向用户输出路由器的配置界面；

(10) TACACS 客户端 向 TACACS 服务器发送计费开始报文；

(11) TACACS 服务器 发送计费回应报文，指示计费开始报文已经收到；

(12) 用户退出，TACACS 客户端 向 TACACS 服务器发送计费结束报文；

(13) TACACS 服务器 发送计费结束报文，指示计费结束报文已经收到。

基本消息交互流程图如下：

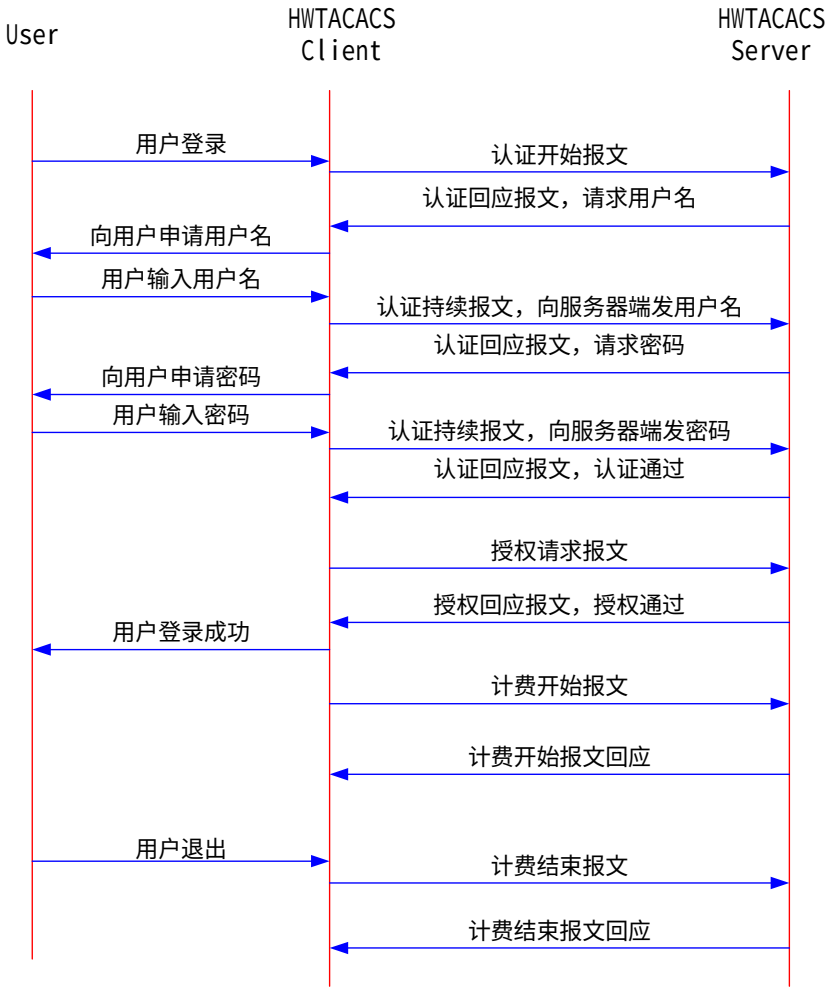

图2-6 Telnet 用户认证、授权和计费流程图

📖 说明：

在配置路由器的过程中，用户可能会发现超级终端上看到的个别命令及参数在本手册中没有描述，这主要是因为 VRP3.4 软件兼容了 LAN Switch 的配置，实际上路由器是不支持这些命令的。

2.2 AAA 配置

AAA 的配置包括：

(1) 创建 ISP 域并配置相关属性

- 创建 ISP 域
- 配置用户使用的 AAA 方案
- 配置 ISP 域的状态

- 配置可接入用户数量的最大值
- 配置计费可选开关
- 定义本地地址池并为 PPP 用户分配 IP 地址

(2) 创建本地用户并配置相关属性（仅用于本地认证）

2.2.1 创建 ISP 域并配置相关属性

1. 创建 ISP 域

什么是 ISP（Internet Service Provider）域？简单点说，ISP 域即 ISP 用户群，一个 ISP 域即是由同属于一个 ISP 的用户构成的用户群。一般说来，在“ userid@isp-name ”形式（例如 gw20010608@huawei163.net）的用户名中，“ @ ”后的“ isp-name ”（如例中的“ huawei163.net ”）即为 ISP 域的域名。在路由器对用户进行接入控制时，对于用户名为“ userid@isp-name ”形式的 ISP 用户，系统就将把“ userid ”作为用于身份认证的用户名，把“ isp-name ”作为域名。

引入 ISP 域的设置是为了支持多 ISP 的应用环境：在这种环境中，同一个接入设备接入的有可能是不同 ISP 的用户。由于各 ISP 用户的用户属性（例如用户名及密码构成、服务类型/权限等）有可能各不相同，因此有必要通过设置 ISP 域的方法把它们区别开。在 ISP 域视图下，可以为每个 ISP 域配置包括使用的 AAA 方案在内的一整套单独的 ISP 域属性。

对于 Quidway 系列路由器来说，每个接入用户都属于一个 ISP 域。系统中最多可以配置 16 个 ISP 域。如果某个用户在登录时没有上报 ISP 域名，则系统将把它归于缺省的 ISP 域。

请在系统视图下进行下列配置。

表2-4 创建/删除 ISP 域

操作	命令
创建 ISP 域或进入指定 ISP 域视图	**domain** [*isp-name* | **default** { **disable** | **enable** *isp-name* }]
删除指定的 ISP 域	**undo domain** *isp-name*

缺省情况下，系统中使用的域为“ system ”。

2. 配置用户使用的 AAA 方案

用户可以通过引用配置好的 *radius-scheme-name* 来实现认证、授权、计费，也可以通过引用配置好的 *hwtacacs-scheme-name* 来实现认证、授权、计费；而采用本地方案时只能进行认证、授权，无法实现计费。

如果配置了 **radius-scheme** *radius-scheme-name* **local** 或 **hwtacacs-scheme** *hwtacacs-scheme-name* **local**，则 **local** 为 **radius server** 或 **tacacs server** 没有

正常响应后的备选认证方案。即当 radius server 或 tacacs server 有效时，不使用本地认证；当 radius server 或 tacacs server 无效时，使用本地认证。

如果 **local** 作为第一方案，那么只能采用本地认证，不能再同时采用 RADIUS 或 HWTACACS 方案。如果 none 作为第一方案，那么不能同时采用 RADIUS 或 HWTACACS 方案。

请在 ISP 域视图下进行下列配置。

表2-5 配置 ISP 域的相关属性

操作	命令
配置域使用的 AAA 方案	**scheme** { **radius-scheme** *radius-scheme-name* [**local**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** }
恢复域使用的缺省的 AAA 方案	**undo scheme** { **radius-scheme** | **hwtacacs-scheme** | **none** }

系统缺省使用的 AAA 方案为 **local**。

3. 配置 ISP 域的状态

每个 ISP 域有两种状态：active 或 block。当指示某个 ISP 域处于 active 状态时，允许该域下的用户请求网络服务；当指示某个 ISP 域处于 block 状态时，不允许该域下的用户请求网络服务，但是不影响已经在线的用户。一个 ISP 域在刚被创建时是处于 active 状态的，即在这个时候，允许任何属于该域的用户请求网络服务。

请在 ISP 域视图下进行下列配置。

表2-6 配置 ISP 域的状态

操作	命令
设置 ISP 域的状态	**state** { **active** | **block** }

缺省情况下，当一个 ISP 域被创建以后，其状态为 **active**。

4. 配置可接入用户数量的最大值

可容纳接入用户数的最大值用来指定该 ISP 域最多可容纳多少个接入用户。缺省情况下，对任何一个 ISP 域，没有任何可容纳接入用户数的限制。

请在 ISP 域视图下进行下列配置。

表2-7 配置可接入用户数量的最大值

操作	命令
指定可容纳接入用户数的最大值	**access-limit** { **disable** | **enable max-user-number** }
恢复可容纳接入用户数到缺省设置	**undo access-limit**

缺省情况下，当一个 ISP 域被创建以后，其可容纳的接入用户没有数量限制。

5. 配置计费可选开关

在对用户实施计费时，当发现没有可用的计费服务器或与计费服务器通信失败时，只要用户配置了 **accounting optional**，即使无法实施计费，也不会挂断用户。

accounting optional 命令与 **scheme** 命令中的 **none** 方案的区别在于，使用此命令时，系统仍然向计费服务器发送计费信息，但不管计费服务器是否响应，能否实施计费，系统都不会挂断用户。而使用 **none** 方案时，系统就不会向计费服务器发送计费信息，当然，也不会挂断用户。如果 **scheme** 命令中指定了采用 RADIUS 或 HWTACACS 方案，但没有配置此命令，系统就会向计费服务器发送计费信息，如果计费服务器没有响应，不能实施计费，那么系统就会挂断用户。

请在 ISP 域视图下进行下列配置。

表2-8 配置计费可选开关

操作	命令
打开计费可选开关	**accounting optional**
关闭计费可选开关	**undo accounting optional**

缺省情况下，当一个 ISP 域被创建以后，计费可选开关关闭。

6. 定义地址池并为 PPP 域用户分配 IP 地址

采用 PPP 方式接入的用户，可以利用 PPP 地址协商功能获得 IP 地址。有三种方法可以为 PPP 用户分配 IP 地址：

- 不配置地址池，在接口上直接给对方配置 IP 地址。
- 在系统视图下定义 IP 地址池，然后在接口视图下指定该接口给对端分配地址时使用的 IP 地址池（只能指定一个）。
- 在域视图下定义 PPP 域用户的 IP 地址池（可以定义多个），依次使用这些地址池直接给用户分配 IP 地址。

前两种地址分配方式适用于不对 PPP 用户进行认证的情况，配置方法请参见《VRP3.4 操作手册》链路层协议的 PPP 部分；第三种分配方式适用于对 PPP 用户进行认证的情况，配置方法如下。

请在 ISP 域视图下进行下列配置。

表2-9 定义 PPP 域用户的 IP 地址池

操作	命令
定义为 PPP 用户分配 IP 地址的地址池	**ip pool** *pool-number low-ip-address* [*high-ip-address*]
删除指定的地址池	**undo ip pool** *pool-number*

缺省情况下，没有配置 IP 地址池。

下面介绍 AAA 对 PPP 用户的地址分配原则：

(1) 对于域的用户（包括 *userid* 和 *userid@isp-name* 两种用户）分配地址的优先级如下：

- 如果采用 Radius 或 Tacacs 认证和授权，并且服务器给用户下发了地址，则采用服务器下发的地址。
- 如果服务器没有下发地址，而是下发地址池，则在域视图下相应的地址池中查找地址给用户。
- 如果上述两种方式没有分配到地址或是采用本地认证，则依次查找域视图下的地址池，并分配给用户。

(2) 对于不认证用户，采用接口下指定的地址池（即在系统视图下定义的地址池）给用户分配地址。

2.2.2 创建本地用户并配置相关属性

当 AAA 方案选择了本地认证方案（**local**）时，应在路由器上创建本地用户并配置相关属性。

📖 说明：

当用户配置了 **radius-scheme** 或 **hwtacacs-scheme** 认证方法时，应在 radius 或 tacacs 服务器端进行类似的配置（是否能配置及如何配置取决于采用服务器），此时本地配置将不起作用。

---

1. 创建本地用户

所谓本地用户，是指在 NAS（即路由器）上设置的一组用户的集合。该集合以用户名为用户的唯一标识。为使某个请求网络服务的用户可以通过本地认证，需要在 NAS 的本地用户数据库中添加相应的表项。

请在系统视图下进行下列配置。

表2-10 创建/删除本地用户

操作	命令
添加本地用户	**local-user** *user-name*
删除指定类型的本地用户	**undo local-user** { *user-name* | **all** }

缺省情况下，系统中没有任何本地用户。

2. 设置本地用户的属性

本地用户的属性包括：用户密码显示方式、用户密码、用户状态以及授权用户可以使用业务类型等。

请在系统视图下进行下列设置。

表2-11 设置本地用户密码显示方式

操作	命令
设置所有本地用户密码的显示方式	**local-user password-display-mode** { **cipher-force** | **auto** }
取消已设置的本地用户密码的显示方式	**undo local-user password-display-mode**

其中，**auto** 表示按照用户配置的密码显示方式（参考下面表格中 **password** 命令）显示，**cipher-force** 表示所有接入用户的密码显示必须采用密文方式。

请在本地用户视图下进行下列配置。

表2-12 设置/取消指定用户的相关属性

操作	命令
设置指定用户的密码	**password** { **simple** | **cipher** } *password*
取消指定用户的密码设置	**undo password**
设置指定用户的状态	**state** { **active** | **block** }
取消指定用户的状态	**undo state** { **active** | **block** }
设置用户可以使用的服务类型	**service-type** { **telnet** | **ssh** | **terminal** | **pad** }
取消用户可以使用的服务	**undo service-type** { **telnet** | **ssh** | **terminal** | **pad** }
设置用户的优先级	**level** *level*
恢复缺省的优先级	**undo level**
授权 FTP 用户可以访问的目录	**service-type ftp** [**ftp-directory** *directory*]
恢复对 FTP 用户授权的缺省目录	**undo service-type ftp** [**ftp-directory**]

操作	命令
设置 PPP 用户的回呼及主叫号码属性	**service-type ppp** [**callback-nocheck** | **callback-number** *callback-number* | **call-number** *call-number* [: *subcall-number*]]
恢复 PPP 用户回呼及主叫号码属性的缺省设置	**undo service-type ppp** [**callback-nocheck** | **callback-number** | **call-number**]

系统缺省不对用户授权任何服务。用户缺省优先级为 0。

📖 说明：

如果配置的认证方式需要用户名和口令（包括本地认证、radius 认证及 hwtacacs 认证），则用户登录系统后所能访问的命令级别由用户的优先级确定。如果配置的认证方式为不认证或采用 password 认证，则用户登录到系统后所能访问的命令级别由用户界面的优先级确定。

2.3 RADIUS 协议配置

RADIUS 协议配置是以 RADIUS 方案为单位进行的，一个 RADIUS 方案在实际组网环境中既可以是一台独立的 RADIUS 服务器，也可以是两台配置相同、但 IP 地址不同的主、从 RADIUS 服务器。由于存在上述情况，因此每个 RADIUS 方案的属性包括：主服务器的 IP 地址、从服务器的 IP 地址、共享密钥以及 RADIUS 服务器类型等。

实际上，RADIUS 协议配置仅仅定义了 NAS 和 RADIUS Server 之间进行信息交互所必须的一些参数。为了使这些参数能够生效，还必须在某个 ISP 域视图下指定该域引用配置有上述参数的 RADIUS 方案。具体配置命令的细节，请参见前述的“ AAA 配置 ”一节。

RADIUS 协议的配置包括：

- 创建 RADIUS 方案
- 设置 RADIUS 认证/授权服务器
- 设置 RADIUS 计费服务器及相关属性
- 设置 RADIUS 报文的共享密钥
- 设置 RADIUS 请求报文的最大传送次数
- 设置支持的 RADIUS 服务器的类型
- 设置 RADIUS 服务器的状态
- 设置发送给 RADIUS 服务器的用户名格式
- 设置发送给 RADIUS 服务器的数据流的单位

- 配置 NAS 发送 RADIUS 报文使用的源地址
- 配置 RADIUS 服务器的定时器

在以上的配置任务中，创建 RADIUS 方案、配置 RADIUS 认证/授权服务器是必需的；其余任务则是可选的，用户可以根据各自的具体需求决定是否进行这些配置。

2.3.1 创建 RADIUS 方案

如前所述，RADIUS 协议的配置是以 RADIUS 方案为单位进行的。因此，在进行其它 RADIUS 协议配置之前，必须先创建 RADIUS 方案并进入其视图。

可以使用下面命令创建/删除 RADIUS 方案。

请在系统视图下进行下列配置。

表2-13 创建/删除 RADIUS 方案

操作	命令
创建 RADIUS 方案并进入其视图	**radius scheme** *radius-scheme-name*
删除 RADIUS 方案	**undo radius scheme** *radius-scheme-name*

一个 RADIUS 方案可以同时被多个 ISP 域引用。

缺省情况下，系统中已创建了一个名为 “ system ” 的 RADIUS 方案，其各项属性均为缺省值。

⚠ 注意：

FTP、Terminal、SSH 不是 RADIUS 协议的标准属性取值，需要修改 RADIUS 服务器的属性，在属性 login-service（标准属性 15）中增加两个取值的定义：
login-service(50) = SSH
login-service（51）＝FTP
login-service(52) = Terminal
修改后再启动 RADIUS 服务器方可。

2.3.2 配置 RADIUS 认证/授权服务器

可以使用下面命令设置 RADIUS 认证/授权服务器的 IP 地址和端口号。

请在 RADIUS 视图下进行下列配置。

表2-14 设置 RADIUS 认证/授权服务器的 IP 地址和端口号

操作	命令
设置主 RADIUS 认证/授权服务器的 IP 地址和端口号	**primary authenticaiton** *ip-address* [*port-number*]

操作	命令
将主 RADIUS 认证/授权服务器的 IP 地址和端口号恢复为缺省值	**undo primary authentication**
设置从 RADIUS 认证/授权服务器的 IP 地址和端口号	**secondary authentication** *ip-address* [*port-number*]
将从 RADIUS 认证/授权服务器的 IP 地址和端口号恢复为缺省值	**undo secondary authentication**

RADIUS 服务器的授权信息是随认证应答报文发给 RADIUS 客户端的，故不需要指定单独的授权服务器。

在实际组网环境中，可以指定 2 台 RADIUS 服务器分别作为主、备认证/授权服务器；也可以指定一台服务器既作为主认证/授权服务器，又作为备份认证/授权服务器。

2.3.3 配置 RADIUS 计费服务器及相关属性

1. 配置 RADIUS 计费服务器

可以使用下面命令设置 RADIUS 计费服务器的 IP 地址和端口号。

请在 RADIUS 视图下进行下列配置。

表2-15 设置 RADIUS 计费服务器的 IP 地址和端口号

操作	命令
设置主 RADIUS 计费服务器的 IP 地址和端口号	**primary accountig** *ip-address* [*port-number*]
将主 RADIUS 计费服务器的 IP 地址和端口号恢复为缺省值	**undo primary accounting**
设置从 RADIUS 计费服务器的 IP 地址和端口号	**secondary accounting** *ip-address* [*port-number*]
将从 RADIUS 计费服务器的 IP 地址和端口号恢复为缺省值	**undo secondary accounting**

在实际组网环境中，可以指定 2 台 RADIUS 服务器分别作为主、备计费服务器；也可以指定一台服务器既作为主计费服务器，又作为从计费服务器。

为了保证 NAS 与 RADIUS 服务器能够正常交互，在设置 RADIUS 服务器的 IP 地址和 UDP 端口之前，必须确保 RADIUS 服务器与 NAS 的路由连接正常。此外，由于 RADIUS 协议采用不同的 UDP 端口来收发认证/授权和计费报文，因此必须将认证/授权端口号和计费端口号设置得不同。RFC2138/2139 中建议的认证/授权端口号为 1812、计费端口号为 1813，但是也可以不选用 RFC 建议值（尤其是比较早期的 RADIUS Server，普遍采用 1645 作为认证/授权端口号、1646 作为计费端口号）。在使用中，请保证 Quidway 系列路由器上的 RADIUS 服务端口设置与 RADIUS 服务器上的端口设置保持一致。

缺省情况下，主、备计费服务器的 IP 地址为 0.0.0.0，计费服务的 UDP 端口号为 1813。

2. 使能停止计费报文缓存及重传功能

由于停止计费请求报文涉及到话单结算、并最终影响收费多少，对用户和 ISP 都有比较重要的影响，因此 NAS 应该尽最大努力把它发送给 RADIUS 计费服务器。所以，如果 RADIUS 计费服务器对 Quidway 系列路由器发出的停止计费请求报文没有响应，路由器应将其缓存在本机上，然后重新发送直到 RADIUS 计费服务器产生响应，或者在重新发送的次数达到指定的次数限制后将其丢弃。可以使用下面的命令来设置路由器允许停止计费报文缓存功能。

请在 RADIUS 视图下进行下列配置。

表2-16 设置使能停止计费报文缓存及重传功能

操作	命令
使能停止计费报文缓存功能	**stop-accounting-buffer enable**
关闭停止计费报文缓存功能	**undo stop-accounting-buffer enable**
使能停止计费报文重传功能，并配置停止计费报文可以传送的最大次数	**retry stop-accounting** *retry-times*
恢复停止计费报文最大传送次数为缺省值	**undo retry stop-accounting**

缺省情况下，使能停止计费报文缓存功能，最多可以将缓存的停止计费请求报文重发 500 次。

3. 设置允许实时计费请求无响应的最大次数

RADIUS 服务器通常通过连接超时定时器来判断用户是否在线。如果 RADIUS 服务器长时间收不到 NAS 传来的实时计费报文，它会认为线路或设备故障并停止对用户计费。为了配合 RADIUS 服务器的这种特性，有必要在不可预见的故障条件下在 NAS 端尽量与 RADIUS 服务器同步切断用户连接。Quidway 系列路由器提供对连续实时计费请求无响应次数限制的设置——在 NAS 向 RADIUS 服务器发出的实时计费请求没有得到响应的次数超过所设定的限度时，NAS 将切断用户连接。

可以使用下面的命令设置允许实时计费请求无响应的最大次数。

请在 RADIUS 视图下进行下列配置。

表2-17 设置允许实时计费请求无响应的最大次数

操作	命令
设置允许实时计费请求无响应的最大次数	**retry realtime-accounting** *retry-times*
恢复允许实时计费请求无响应的最大次数为缺省值	**undo retry realtime-accounting**

考虑一下该值如何计算：假设 RADIUS 服务器的连接超时时长为 T，NAS 的实时计费间隔为 t，则 NAS 的 *count* 应取为 T 除以 t 后取整的数值。因此，在实际应用中，应尽量将 T 设置为一个能被 t 整除的数。

缺省情况下，最多允许 5 次实时计费请求无响应。

2.3.4 设置 RADIUS 报文的共享密钥

RADIUS 客户端（即路由器）与 RADIUS 服务器使用 MD5 算法来加密 RADIUS 报文，双方通过设置共享密钥来验证报文的合法性。只有在密钥一致的情况下，双方才能彼此接收对方发来的报文并作出响应。

可以使用下面命令设置 RADIUS 报文的共享密钥。

请在 RADIUS 视图下进行下列配置。

表2-18 设置 RADIUS 报文的共享密钥

操作	命令
设置 RADIUS 认证/授权报文的共享密钥	**key authentication** *string*
恢复 RADIUS 认证/授权报文共享密钥为缺省	**undo key authentication**
设置 RADIUS 计费报文的共享密钥	**key accounting** *string*
恢复 RADIUS 计费报文共享密钥为缺省	**undo key accounting**

缺省情况下，RADIUS 认证/授权报文和 RADIUS 计费报文的共享密钥均为“huawei”。

2.3.5 设置 RADIUS 请求报文的最大传送次数

由于 RADIUS 协议采用 UDP 报文来承载数据，因此其通信过程是不可靠的。如果 RADIUS 服务器在响应超时定时器规定的时长内没有响应 NAS，则 NAS 有必要向 RADIUS 服务器重传 RADIUS 请求报文。如果累计的传送次数超过最大传送次数而 RADIUS 服务器仍旧没有响应，则 NAS 将认为其与当前 RADIUS 服务器的通信已经中断，并将转而向其它的 RADIUS 服务器发送请求报文。

可以使用下面命令设置 RADIUS 请求报文的最大传送次数。

请在 RADIUS 视图下进行下列配置。

表2-19 设置 RADIUS 请求报文的最大传送次数

操作	命令
设置 RADIUS 请求报文的最大传送次数	**retry** *retry-times*
将 RADIUS 请求报文的最大传送次数恢复为缺省值	**undo retry**

缺省情况下，RADIUS 请求报文的最大传送次数为 3 次。

2.3.6 设置支持的 RADIUS 服务器的类型

可以使用下面的命令来选择支持何种 RADIUS 服务器类型。

请在 RADIUS 视图下进行下列配置。

表2-20 设置支持何种类型的 RADIUS 服务器

操作	命令
设置支持何种类型的 RADIUS 服务器	**server-type** { **huawei** | **standard** }
恢复 RADIUS 服务器类型为缺省设置	**undo server-type**

缺省情况下，RADIUS 服务器的类型为 **standard**。

2.3.7 设置 RADIUS 服务器的状态

对于某个 RADIUS 方案中的主、备服务器（无论是认证/授权服务器还是计费服务器），当主服务器因故障与 NAS 的通信中断时，NAS 会主动地转而与从服务器交互报文。当主服务器恢复正常后，NAS 却不会立即恢复与其通信，而是继续与从服务器通信；直到从服务器也出现故障后，NAS 才能再转而恢复与主服务器交互报文。为了使 NAS 在主服务器故障排除后迅速恢复与其通信，需要通过下面的命令手工将主服务器的状态设为 **active**。

当主服务器与从服务器的状态都为 **active** 或都为 **block** 时，NAS 将只把报文发送到主服务器上。

请在 RADIUS 视图下进行下列配置。

表2-21 设置 RADIUS 服务器的状态

操作	命令
设置主 RADIUS 认证/授权服务器的状态	**state primary authentication** { **block** | **active** }
设置主 RADIUS 计费服务器的状态	**state primary accounting** { **block** | **active** }
设置从 RADIUS 认证/授权服务器的状态	**state secondary authentication** { **block** | **active** }
设置从 RADIUS 计费服务器的状态	**state secondary accounting** { **block** | **active** }

缺省情况下，RADIUS 方案中各 RADIUS 服务器的状态均为 **active**。

2.3.8 设置发送给 RADIUS 服务器的用户名格式

如前所述，接入用户通常以“ userid@isp-name ”的格式命名，“ @ ”后面的部分为 ISP 域名，Quidway 系列路由器就是通过该域名来决定将用户归于哪个 ISP 域的。

但是，有些较早期的 RADIUS 服务器不能接受携带有 ISP 域名的用户名，在这种情况下，有必要将用户名中携带的域名去除后再传送给 RADIUS 服务器。因此，Quidway 系列路由器提供下面的命令以指定发送给 RADIUS 服务器的用户名是否携带有 ISP 域名。

表2-22 设置发送给 RADIUS 服务器的用户名格式

操作	命令
设置发送给 RADIUS 服务器的用户名格式	**user-name-format** { **with-domain** | **without-domain** }

📖 说明：

如果指定某个 RADIUS 方案不允许用户名中携带有 ISP 域名，那么请不要在两个乃至两个以上的 ISP 域中同时设置使用该 RADIUS 方案，否则，会出现虽然实际用户不同（在不同的 ISP 域中）、但 RADIUS 服务器认为用户相同（因为传送到它的用户名相同）的错误。

缺省情况下，NAS 发送给 RADIUS 服务器的用户名携带有 ISP 域名。

2.3.9 设置发送给 RADIUS 服务器的数据流的单位

Quidway 系列路由器提供下面的命令以指定发送给 RADIUS 服务器的数据流的单位。

表2-23 设置发送给 RADIUS 服务器的数据流的单位

操作	命令
设置发送给 RADIUS 服务器的数据流的单位	**data-flow-format data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** }
恢复发送到 RADIUS 服务器的数据流的单位为缺省设置	**undo data-flow-format**

缺省情况下，RADIUS 方案默认的发送数据单位为 byte，数据包的单位为 one packet。

2.3.10 配置 NAS 发送 RADIUS 报文使用的源地址

请进行下列配置。

表2-24 配置 NAS 发送 RADIUS 报文使用的源地址

操作	命令
配置 NAS 发送 RADIUS 报文使用的源地址(RADIUS 视图)	**nas-ip** *ip-address*
取消 NAS 发送 RADIUS 报文使用的源地址(RADIUS 视图)	**undo nas-ip**
配置 NAS 发送 RADIUS 报文使用的源地址(系统视图)	**radius nas-ip** *ip-address*
取消 NAS 发送 RADIUS 报文使用的源地址(系统视图)	**undo radius nas-ip**

这两条命令的作用相同。缺省情况下，不指定源地址，即以发送报文的接口地址作为源地址。

2.3.11 配置 RADIUS 服务器的定时器

1. 设置 RADIUS 服务器应答超时定时器

如果在 RADIUS 请求报文（认证/授权请求或计费请求）传送出去一段时间后，NAS 还没有得到 RADIUS 服务器的响应，则有必要重传 RADIUS 请求报文，以保证用户确实能够得到 RADIUS 服务。

可以使用下面命令设置 RADIUS 服务器应答超时定时器。

请在 RADIUS 视图下进行下列配置。

表2-25 设置 RADIUS 服务器应答超时定时器

操作	命令
设置 RADIUS 服务器应答超时定时器	**timer response-timeout** *seconds*
将 RADIUS 服务器应答超时定时器恢复为缺省值	**undo timer response-timeout**

缺省情况下，RADIUS 服务器应答超时定时器为 3 秒。

2. 配置 RADIUS 服务器的主服务器恢复激活状态时间

请在 RADIUS 视图下进行下列配置。

表2-26 配置 RADIUS 服务器的主服务器恢复激活状态时间

操作	命令
配置恢复激活时间	**timer quiet** *minutes*
恢复缺省配置	**undo timer quiet**

缺省情况下，主服务器恢复激活状态前需要等待 5 分钟。

3. 设置实时计费时间间隔

为了对用户实施实时计费，有必要设置实时计费的时间间隔。在设置了该属性以后，每隔设定的时间，NAS 会向 RADIUS 服务器发送一次在线用户的计费信息。

可以使用下面命令设置实时计费间隔。

请在 RADIUS 视图下进行下列配置。

表2-27 设置实时计费间隔

操作	命令
设置实时计费间隔	**timer realtime-accounting** *minutes*
将实时计费间隔恢复为缺省值	**undo timer realtime-accounting**

其中，*minutes* 为实时计费间隔时间，单位为分钟，其取值必须为 3 的整数倍。

实时计费间隔的取值对 NAS 和 RADIUS 服务器的性能有一定的相关性要求——取值越小，对 NAS 和 RADIUS 服务器的性能要求越高。建议当用户量比较大（≥1000）时，尽量把该间隔的值设置得大一些。以下是实时计费间隔与用户量之间的推荐比例关系：

表2-28 实时计费间隔与用户量之间的推荐比例关系

用户数	实时计费间隔（分钟）
1~99	3
100~499	6
500~999	12
≥1000	≥15

缺省情况下，实时计费间隔为 12 分钟。

2.4 HWTACACS 协议配置

HWTACACS 的配置包括：

- 创建 HWTACACS 方案
- 配置 TACACS 认证服务器
- 配置 TACACS 授权服务器
- 配置 TACACS 计费功能
- 配置 TACACS 服务器的密钥
- 配置 TACACS 服务器的用户名格式
- 配置 TACACS 服务器的流量单位

- 配置 NAS 发送 HWTACACS 报文使用的源地址
- 配置 TACACS 服务器的定时器

📖 说明：

与 RADIUS 的配置相比，配置 TACACS 服务器时需要注意以下几点：

- 除删除方案外，HWTACACS 的大部分属性在改变配置时都不检查当前是否有用户在使用此方案。
- HWTACAS 服务器缺省没有密钥。

在以上的配置任务中，创建 HWTACACS 方案、配置 TACACS 认证/授权服务器是必需的；其余任务则是可选的，用户可以根据各自的具体需求决定是否进行这些配置。

2.4.1 创建 HWTACACS 方案

如前所述，HWTACACS 协议的配置是以 HWTACACS 方案为单位进行的。因此，在进行其它 HWTACACS 协议配置之前，必须先创建 HWTACACS 方案并进入其视图。

请在系统视图下进行下列配置。

表2-29 创建 HWTACACS 方案

操作	命令
创建 HWTACACS 方案，并进入 HWTACACS 视图	**hwtacacs scheme** *hwtacacs-scheme-name*
删除 HWTACACS 方案	**undo hwtacacs scheme** *hwtacacs-scheme-name*

如果指定的 HWTACACS 方案名不存在，将创建一个新的 HWTACACS 方案并进入 HWTACACS 视图。

在 HWTACACS 视图下，可以对此 HWTACACS 方案进行具体配置。

系统最多支持配置 128 个 HWTACACS 方案。只有当方案没有用户使用时，才能删除该方案。

缺省情况下，没有定义 hwtacacs 方案。

2.4.2 配置 HWTACACS 认证服务器

请在 HWTACACS 视图下进行下列配置。

表2-30 配置 TACACS 认证服务器

操作	命令
配置 TACACS 主认证服务器	**primary authentication** *ip-address* [*port*]
删除 TACACS 主认证服务器	**undo primary authentication**
配置 TACACS 从认证服务器	**secondary authentication** *ip-address* [*port*]
删除 TACACS 从认证服务器	**undo secondary authentication**

主认证服务器和备用认证服务器的 IP 地址不能相同，否则将提示配置不成功。端口号缺省使用 49。

如果多次执行此命令，新的配置将覆盖原来的配置。

只有当没有活跃的用于发送认证报文的 TCP 连接使用该认证服务器时，才允许删除该服务器。删除服务器只对之后的报文有效。

2.4.3 配置 HWTACACS 授权服务器

请在 HWTACACS 视图下进行下列配置。

表2-31 配置 TACACS 授权服务器

操作	命令
配置 TACACS 主授权服务器	**primary authorization** *ip-address* [*port*]
删除 TACACS 主授权服务器	**undo primary authorization**
配置 TACACS 从授权服务器	**secondary authorization** *ip-address* [*port*]
删除 TACACS 从授权服务器	**undo secondary authorization**

📖 说明：

对于所有类型的用户，如果配置了 TACACS 认证，但没有配置 TACACS 授权服务器，则用户无法登录。

主授权服务器和备用授权服务器的 IP 地址不能相同，否则将提示配置不成功。端口号缺省使用 49。

如果多次执行此命令，新的配置将覆盖原来的配置。

只有当没有活跃的用于发送授权报文的 TCP 连接使用该授权服务器，才允许删除该服务器。

2.4.4 配置 TACACS 计费服务器及相关属性

1. 配置 TACACS 计费服务器

请在 HWTACACS 视图下进行下列配置。

表2-32 配置 HWTACACS 计费服务器

操作	命令
配置 TACACS 主计费服务器	**primary accounting** *ip-address* [*port*]
删除配置的 TACACS 主计费服务器	**undo primary accounting**
配置 TACACS 从计费服务器	**secondary accounting** *ip-address* [*port*]
删除配置的 TACACS 从计费服务器	**undo secondary accounting**

主计费服务器和备用计费服务器的 IP 地址不能相同，否则将提示配置不成功。端口号缺省使用 49。

缺省情况下，HWTACACS 计费服务器的 IP 地址为全零。

如果多次执行此命令，新的配置将覆盖原来的配置。

只有当没有活跃、用于发送计费报文的 TCP 连接使用该计费服务器时，才允许删除该服务器。

2. 使能停止计费报文重传功能

请在 HWTACACS 视图下进行下列配置。

表2-33 配置停止计费报文重传功能

操作	命令
使能停止计费报文重传，并配置传送的最大次数	**retry stop-accounting** *retry-times*
关闭停止计费报文重传功能	**undo retry stop-accounting**

缺省情况下，使能停止计费报文重传功能，且允许停止计费报文传送 100 次。

2.4.5 配置 NAS 发送 HWTACACS 报文使用的源地址

请进行下列配置。

表2-34 配置 NAS 发送 HWTACACS 报文使用的源地址

操作	命令
配置 NAS 发送 HWTACACS 报文使用的源地址 (HWTACACS 视图)	**nas-ip** *ip-address*
取消 NAS 发送 HWTACACS 报文使用的源地址 HWTACACS 视图)	**undo nas-ip**

操作	命令
配置 NAS 发送 HWTACACS 报文使用的源地址(系统视图)	**hwtacacs nas-ip** *ip-address*
取消 NAS 发送 HWTACACS 报文使用的源地址(系统视图)	**undo hwtacacs nas-ip**

缺省情况下，不指定源地址，即以发送报文的接口地址作为源地址。

2.4.6 配置 TACACS 服务器的密钥

使用 TACACS 服务器作为 AAA 服务器时，可设置密钥以提高路由器与 TACACS 服务器通信的安全性。

请在 HWTACACS 视图下进行下列配置。

表2-35 配置 TACACS 服务器的密钥

操作	命令
配置 TACACS 计费、授权及认证服务器的密钥	**key** { **accounting** | **authorization** | **authentication** } *string*
删除配置	**undo key** { **accounting** | **authorization** | **authentication** }

缺省情况下，没有密钥。

2.4.7 配置 TACACS 服务器的用户名格式

用户名通常采用“ userid@isp-name ”格式，“ @ ”后面的部分为域名。

如果 TACACS 服务器不接受带域名的用户名时，可以配置将用户名的域名去除后再传送给 TACACS 服务器。

请在 HWTACACS 视图下进行下列配置。

表2-36 配置 TACACS 服务器的用户名格式

操作	命令
配置用户名带域名	**user-name-format with-domain**
配置用户名不带域名	**user-name-format without-domain**

缺省情况下，发往 TACACS 服务器的用户名带域名。

2.4.8 配置 TACACS 服务器的流量单位

请在 HWTACACS 视图下进行下列配置。

表2-37 配置 TACACS 服务器的流量单位

操作	命令
配置 TACACS 服务器的流量单位	**data-flow-format data** [**byte** | **giga-byte** | **kilo-byte** | **mega-byte**] **data-flow-format packet** [**giga-packet** | **kilo-packet** | **mega-packet** | **one-packet**]
恢复发送到 TACACS 服务器的数据流的单位为缺省设置	**undo data-flow-format** [**data** | **packet**]

缺省情况下，使用字节做为流量的单位（**byte**）。

2.4.9 配置 TACACS 服务器的定时器

1. 配置 TACACS 服务器的应答超时时间

由于 HWTACACS 是基于 TCP 实现的，因此，服务器应答超时或 TCP 超时都可能导致与 TACACS 服务器的连接断开。

请在 HWTACACS 视图下进行下列配置。

表2-38 配置 TACACS 服务器应答超时时间

操作	命令
配置应答超时时间	**timer response-timeout** *seconds*
恢复缺省配置	**undo timer response-timeout**

缺省情况下，应答超时时间为 5 秒。

2. 配置 TACACS 服务器的主服务器恢复激活状态时间

请在 HWTACACS 视图下进行下列配置。

表2-39 配置 TACACS 服务器的主服务器恢复激活状态时间

操作	命令
配置恢复激活时间	**timer quiet** *minutes*
恢复缺省配置	**undo timer quiet**

缺省情况下，主服务器恢复激活状态前需要等待 5 分钟。

3. 设置实时计费时间间隔

为了对用户实施实时计费，有必要设置实时计费的时间间隔。在设置了该属性以后，每隔设定的时间，NAS 会向 TACACS 服务器发送一次在线用户的计费信息。

可以使用下面命令设置实时计费间隔。

请在 HWTACACS 视图下进行下列配置。

表2-40 设置实时计费间隔

操作	命令
设置实时计费间隔	**timer realtime-accounting** *minutes*
将实时计费间隔恢复为缺省值	**undo timer realtime-accounting**

其中，*minutes* 为实时计费间隔时间，单位为分钟，其取值必须为 3 的整数倍。

实时计费间隔的取值对 NAS 和 TACACS 服务器的性能有一定的相关性要求——取值越小，对 NAS 和 TACACS 服务器的性能要求越高。建议当用户量比较大（≥1000）时，尽量把该间隔的值设置得大一些。以下是实时计费间隔与用户量之间的推荐比例关系：

表2-41 实时计费间隔与用户量之间的推荐比例关系

用户数	实时计费间隔（分钟）
1~99	3
100~499	6
500~999	12
≥1000	≥15

缺省情况下，实时计费间隔为 12 分钟。

2.5 AAA 及 RADIUS/HWTACACS 协议的显示和调试

完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 AAA、RADIUS/HWTACACS 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可清除相关配置。

在用户视图下，执行 **debugging** 命令可进行调试。

表2-42 AAA 协议的显示和调试

操作	命令
显示所有或指定 ISP 域的配置信息	**display domain** [*isp-name*]
显示用户连接的相关信息	**display connection** [**domain** *isp-name* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **ucibindex** *ucib-index* | **user-name** *user-name*]
显示本地用户的相关信息	**display local-user** [**domain** *isp-name* | **service-type** { **pad** | **telnet** | **ssh** | **terminal** | **ftp** | **ppp** } | **state** { **active** | **block** } | **user-name** *user-name*]

表2-43 RADIUS 协议的显示和调试

操作	命令
显示所有或指定RADIUS方案的配置信息或统计信息	**display radius** [*radius-server-name* | **statistics**]
显示 RADIUS 报文的统计信息	**display radius statistics**
显示缓存的没有得到响应的停止计费请求报文	**display stop-accounting-buffer** { **radius-scheme** *radius-server-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }
打开 RADIUS 报文调试开关	**debugging radius packet**
关闭 RADIUS 报文调试开关	**undo debugging radius packet**
删除那些缓存的、没有得到响应的停止计费请求报文	**reset stop-accounting-buffer** { **radius-scheme** *radius-server-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }
清除 RADIUS 服务器的统计信息	**reset radius statistics**

表2-44 HWTACACS 协议的显示和调试

操作	命令
显示所有或指定HWTACACS方案的配置信息	**display hwtacacs** [*hwtacacs-server-name* [**statistics**]]
显示缓存的没有得到响应的停止计费请求报文	**display stop-accounting-buffer hwtacacs-scheme** *hwtacacs-scheme-name*
打开 HWTACACS 协议调试开关	**debugging hwtacacs** { **all** | **error** | **event** | **message** | **receive-packet** | **send-packet** }
关闭 HWTACACS 协议调试开关	**undo debugging hwtacacs** { **all** | **error** | **event** | **message** | **receive-packet** | **send-packet** }
删除那些在路由器上缓存的、没有得到响应的停止计费请求报文	**reset stop-accounting-buffer** { **hwtacacs-scheme** *hwtacacs-scheme-name* }
清除 TACACS 服务器的统计信息	**reset hwtacacs statistics** {**accounting** | **authentication** | **authorization** | **all** }

2.6 AAA 及 RADIUS/HWTACACS 协议典型配置举例

2.6.1 Telnet/SSH 用户通过 RADIUS 服务器认证、计费的应用

> 说明：
>
> SSH/Telnet 用户通过 RADIUS 服务器认证、计费的配置方法类似，下面的描述以 Telnet 用户的远端认证为例。
> 目前 RADIUS 及 TACACS+协议均不支持对 FTP 用户进行计费。

1. 组网需求

如下图所示的环境中，现需要通过配置路由器实现 RADIUS 服务器对登录路由器的 Telnet 用户进行认证、计费。

一台 RADIUS 服务器（其担当认证 RADIUS 服务器和计费 RADIUS 服务器的职责）与路由器相连，服务器 IP 地址为 10.110.91.146，设置路由器与认证 RADIUS 服务器交互报文时的共享密钥为“ expert ”、与计费 RADIUS 服务器交互报文时的共享密钥“ expert ”。

RADIUS 服务器可使用华为 3COM 的 CAMS 服务器。使用第三方 RADIUS 服务器时，RADIUS 方案中的 server-type 可以选择 standard 类型或 huawei 类型；使用华为 3COM 的 CAMS 服务器时，RADIUS 方案中的 server-type 应选择 huawei 类型。在 RADIUS 服务器上设置与路由器交互报文时的共享密钥为“ expert ”；设置验证及计费的端口号；添加 Telnet 用户名及登录密码。如果 RADIUS 方案中设置路由器不从用户名中去除用户域名而是一起传给 RADIUS 服务器，RADIUS 服务器上添加的 Telnet 用户名应为“ *userid@isp-name* ”形式。

2. 组网图

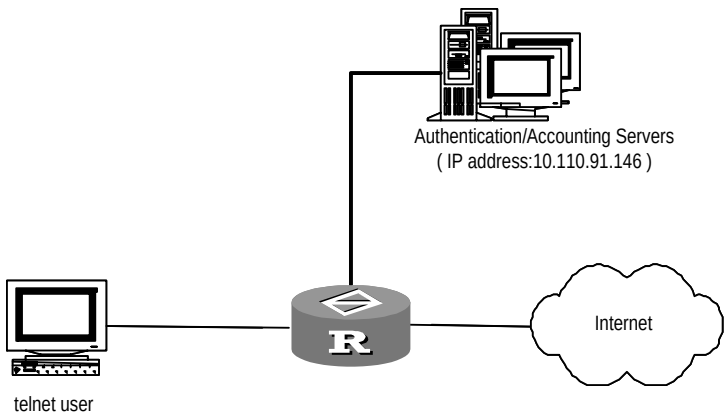

图2-7 配置 Telnet 用户的远端 RADIUS 认证

3. 配置步骤

配置 Telnet 用户采用 AAA 认证方式。

```
[Quidway-ui-vty0-4] authentication-mode scheme
```

配置 domain。

```
[Quidway] domain cams
[Quidway-isp-cams] access-limit enable 10
[Quidway-isp-cams] accounting optional
[Quidway-isp-cams] quit
```

配置 RADIUS 方案。

```
[Quidway] radius scheme cams
[Quidway-radius-cams] primary authentication 10.110.91.146 1812
[Quidway-radius-cams] primary accounting 10.110.91.146 1813
[Quidway-radius-cams] key authentication expert
[Quidway-radius-cams] key accounting expert
[Quidway-radius-cams] server-type Huawei
[Quidway-radius-cams] user-name-format with-domain
[Quidway-radius-cams] quit
```

配置 domain 和 RADIUS 的关联。

```
[Quidway] domain cams
[Quidway-isp-cams] scheme radius-scheme cams
```

Telnet 用户登录时输入用户名 *userid* @cams，以使用 cams 域进行认证。

2.6.2 FTP/Telnet 用户本地认证配置

📖 说明：

FTP 用户与 Telnet 用户通过本地认证的配置方法类似，下面描述仅以 Telnet 用户为例。

1. 组网需求

如下图所示的环境中，现需要通过配置路由器实现对登录路由器的 Telnet 用户进行本地认证。

2. 组网图

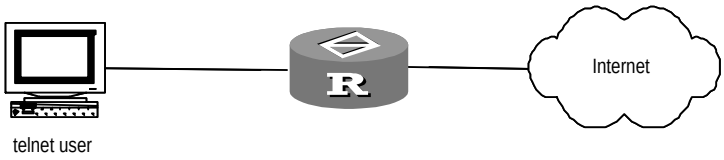

图2-8 配置 Telnet 用户的本地认证

3. 配置步骤

配置 Telnet 用户采用 AAA 认证方式。

```
[Quidway-ui-vty0-4] authentication-mode scheme
```

创建本地用户 telnet。

```
[Quidway] local-user telnet
[Quidway-luser-telnet] service-type telnet
[Quidway-luser-telnet] password simple huawei
[Quidway] domain system
[Quidway-isp-system] scheme local
```

使用 Telnet 登陆时输入用户名为 *userid* @system，以使用 system 域进行认证。

2.6.3 PPP 用户通过 TACACS 服务器认证、授权、计费的应用

1. 组网需求

如下图所示的环境中，现需要通过配置路由器实现 TACACS 服务器对登录路由器的 PPP 用户分配 IP 地址，并进行认证、授权、计费。

一台 TACACS 服务器（其担当认证、授权、计费服务器的职责）与路由器相连，服务器 IP 地址为 10.110.91.146，设置路由器与认证、授权、计费 TACACS 服务器交互报文时的共享密钥均为“ expert ”，设置路由器除去用户名中的域名后再将之传给 TACACS 服务器。

在 TACACS 服务器上设置与路由器交互报文时的共享密钥为“ expert ”；添加 PPP 用户名及密码。

2. 组网图

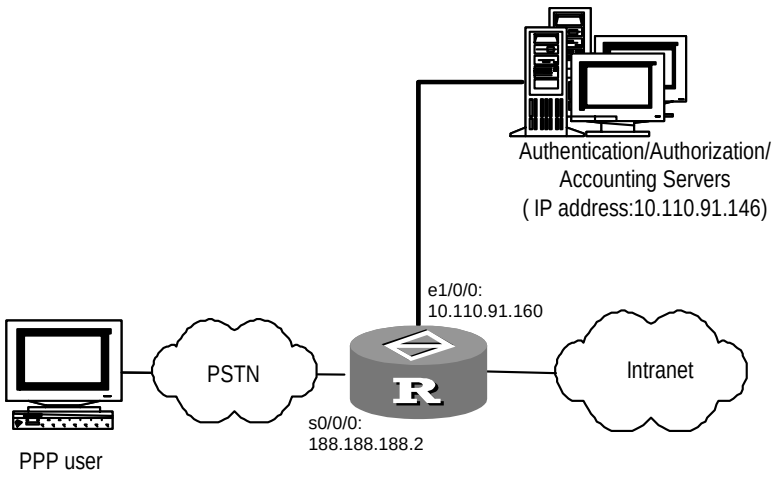

图2-9 配置 PPP 用户的远端 HWTACACS 认证

3. 配置步骤

配置 HWTACACS 方案。

```
[Quidway] hwtacacs scheme hwtac
[Quidway-hwtacacs-hwtac] primary authentication 10.110.91.146 1812
[Quidway-hwtacacs-hwtac] primary authorization 10.110.91.146 1813
[Quidway-hwtacacs-hwtac] primary accounting 10.110.91.146 1814
[Quidway-hwtacacs-hwtac] key authentication expert
[Quidway-hwtacacs-hwtac] key authorization expert
[Quidway-hwtacacs-hwtac] key accounting expert
[Quidway-hwtacacs-hwtac] user-name-format with-domain
[Quidway-hwtacacs -hwtac] quit
```

配置 domain 和 hwtacacs 的关联。

```
[Quidway] domain hwtacacs
[Quidway-isp-hwtacacs] scheme hwtacacs-scheme hwtac
[Quidway-isp-hwtacacs] ip pool 1 200.1.1.1 200.1.1.99
[Quidway-isp-hwtacacs] quit
```

配置串口。

```
[Quidway] interface serial 0/0/0
[Quidway-Serial0/0/0] link-protocol ppp
[Quidway-Serial0/0/0] ppp authentication-mode pap domain hwtacacs
[Quidway-Serial0/0/0] ip address 188.188.188.2 255.255.255.0
[Quidway-Serial0/0/0] remote address pool 1
```

配置以太网口。

```
[Quidway-Serial0/0/0] interface ethernet 1/0/0
[Quidway-ethernet 1/0/0] ip address 10.110.91.160 255.255.255.0
```

2.6.4 Telnet 用户通过 TACACS+服务器认证（一次性认证）、计费的应用

1. 组网需求

如下图所示的环境中，现需要通过配置路由器实现 TACACS+服务器对登录路由器的 Telnet 用户进行一次性认证、计费。

一台 TACACS+服务器（其担当认证 TACACS+服务器和计费 TACACS+服务器的职责）与路由器相连，服务器 IP 地址为 10.110.91.146，设置路由器与认证 TACACS+服务器交互报文时的共享密钥为“ expert ”、与计费 TACACS+服务器交互报文时的共享密钥“ expert ”。TACACS+服务器提供一次性口令认证功能，路由器不从用户名中去除用户域名而是一起传给 TACACS+服务器，故 TACACS+服务器上添加的 Telnet 用户名应为“ test@ tacacs ”。

2. 组网图

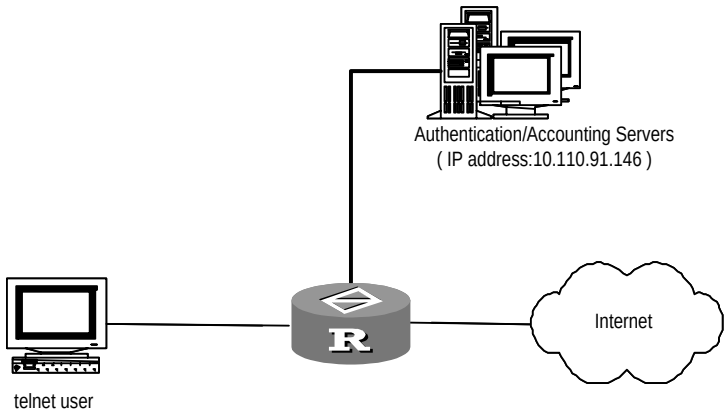

图2-10 配置 Telnet 用户的远端 TACACS+认证

3. 配置步骤

(1) 配置路由器

配置 Telnet 用户采用 AAA 认证方式。

```
[Quidway] user-interface vty0 4
[Quidway-ui-vty0-4] authentication-mode scheme
```

配置 domain。

```
[Quidway] domain tacacs
[Quidway-isp-tacacs] access-limit enable 10
[Quidway-isp-tacacs] accounting optional
[Quidway-isp-tacacs] quit
```

配置 TACACS 方案。

```
[Quidway] hwtacacs scheme system
[Quidway-hwtacacs-system] primary authentication 10.110.91.146
```

```
[Quidway-hwtacacs-system] primary accounting 10.110.91.146
[Quidway-hwtacacs-system] key authentication expert
[Quidway-hwtacacs-system] key accounting expert
[Quidway-hwtacacs-system] user-name-format with-domain
[Quidway-hwtacacs-system] quit
```

配置 domain 和 TACACS 方案的关联。

```
[Quidway] domain tacacs
[Quidway-isp-tacacs] scheme hwtacacs-scheme system
```

(2) 配置 tacacs+服务器

- 配置 IP 地址
- 配置共享密钥
- 添加 Telnet 用户名 test@ tacacs
- 启动一次性认证

(3) 登录过程

Telnet 一次性认证用户登录过程如下。

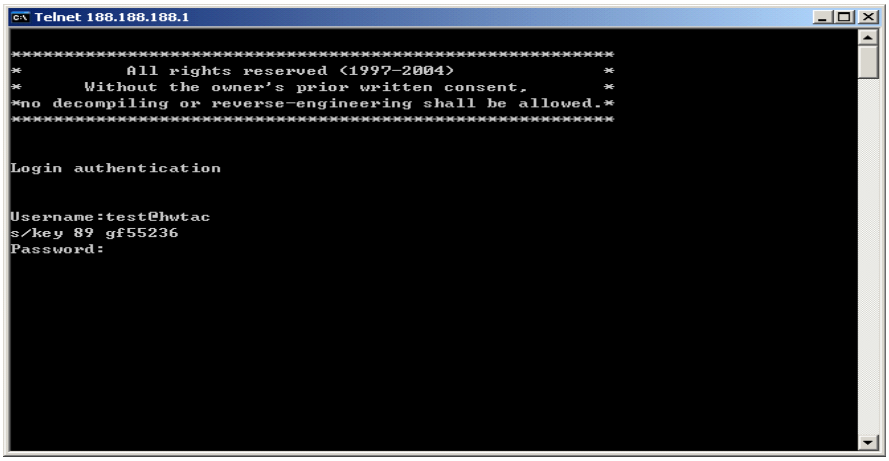

图2-11 Telnet 用户登录界面

第一步：输入用户名 test@ tacacs；

第二步：根据登录界面上的提示信息“ s/key 89 gf55236 ”，利用 winkey.exe 计算器计算登录密码；

图2-12 计算登录密码

图中：

Challenge：框输入服务器返回的提示信息“ 89 gf55236 ”；

Password：输入用户的私有密码，例如“ test ”；

Response：输出的计算结果，也就是要在登录界面上输入的密码。

第三步：在登录界面上输入计算得到的密码，即可通过认证。

2.7 AAA 及 RADIUS/HWTACACS 协议故障的诊断与排除

2.7.1 RADIUS 协议故障诊断与排除

RADIUS 协议在 TCP/IP 协议族中处于应用层，它主要规定 NAS 与 ISP 的 RADIUS 服务器间如何交互用户信息，因此它失效的可能性比较大。

- 故障之一：用户认证/授权总是失败

故障排除：

(1) 用户名不是“ userid@isp-name ”的形式，或 NAS 没有指定缺省的 ISP 域——请使用正确形式的用户名或在 NAS 中设定缺省的 ISP 域。

(2) RADIUS 服务器的数据库中没有配置该用户——检查 RADIUS 服务器的数据库以保证该用户的配置信息确实存在。

(3) 用户侧输入的密码不正确——请保证接入用户输入正确的密码。

(4) RADIUS 服务器和 NAS 的报文共享密钥不同——请仔细比较两端的共享密钥，确保它们相同。

(5) NAS 与 RADIUS 服务器之间存在通信故障（可以通过在 NAS 上 ping RADIUS 服务器来检查）——请保证 NAS 与 RADIUS 服务器之间能够正常通信。

- 故障之二：RADIUS 报文无法传送到 RADIUS 服务器

故障排除：

(1) NAS 与 RADIUS 服务器之间的通信线路不通（物理层/链路层）——请保证线路通畅。

(2) NAS 上没有设置相应的 RADIUS 服务器 IP 地址——请保证正确设置 RADIUS 服务器的 IP 地址。

(3) 认证/授权和计费服务的 UDP 端口设置得不正确——请保证与 RADIUS 服务器提供的端口号一致。

- 故障之三：用户认证通过并获得授权，但是不能向 RADIUS 服务器传送计费话单。

故障排除：

(1) 计费端口号设置得不正确——请正确设置 RADIUS 计费端口号。

(2) 计费服务器和认证/授权服务器不是同一台机器，NAS 却要求认证/授权和计费在同一个服务器（IP 地址相同）——请保证 NAS 的认证/授权和计费服务器的设置与实际情况相同。

2.7.2 HWTACACS 协议故障诊断与排除

HWTACACS 的故障现象与 RADIUS 基本相似，可以参考上面内容。

第3章 访问控制列表配置

3.1 访问控制列表简介

3.1.1 访问控制列表概述

路由器为了过滤数据包，需要配置一系列的规则，以决定什么样的数据包能够通过，这些规则就是通过访问控制列表 ACL（Access Control List）定义的。访问控制列表是由 **permit | deny** 语句组成的一系列有顺序的规则，这些规则根据数据包的源地址、目的地址、端口号等来描述。ACL 通过这些规则对数据包进行分类，这些规则应用到路由器接口上，路由器根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。

3.1.2 访问控制列表的分类

按照访问控制列表的用途，可以分为四类：

- 基本的访问控制列表（basic acl）
- 高级的访问控制列表（advanced acl）
- 基于接口的访问控制列表（interface-based acl）
- 基于 MAC 的访问控制列表（mac-based acl）

访问控制列表的使用用途是依靠数字的范围来指定的，1000～1999 是基于接口的访问控制列表，2000～2999 范围的数字型访问控制列表是基本的访问控制列表，3000～3999 范围的数字型访问控制列表是高级的访问控制列表，4000～4999 范围的数字型访问控制列表是基于 MAC 地址访问控制列表。

3.1.3 访问控制列表的匹配顺序

一个访问控制列表可以由多条“ **permit | deny** ”语句组成，每一条语句描述的规则是不相同，这些规则可能存在重复或矛盾的地方，在将一个数据包和访问控制列表的规则进行匹配的时候，到底采用哪些规则呢？就需要确定规则的匹配顺序。

有两种匹配顺序：

- 配置顺序
- 自动排序

配置顺序，是指按照用户配置 ACL 的规则的先后进行匹配。

自动排序使用“ 深度优先 ”的原则。

“ 深度优先 ”规则是把指定数据包范围最小的语句排在最前面。这一点可以通过比较地址的通配符来实现，通配符越小，则指定的主机的范围就越小。比如 129.102.1.1 0.0.0.0 指定了一台主机：129.102.1.1，而 129.102.1.1 0.0.255.255 则指定了一个网段：129.102.1.1～129.102.255.255，显然前者在访问控制规则中排在前面。具体标准为：对于基本访问控制规则的语句，直接比较源地址通配符，通配符相同的则按配置顺序；对于基于接口的访问控制规则，配置了 “ **any** ”的规则排在后面，其它按配置顺序；对于高级访问控制规则，首先比较源地址通配符，相同的再比较目的地址通配符，仍相同的则比较端口号的范围，范围小的排在前面，如果端口号范围也相同则按配置顺序。

使用 **display acl** 命令就可以看出是哪条规则首先生效。显示时，列在前面的规则首先生效。

3.1.4 访问控制列表的创建

一个访问控制列表是由 **permit** | **deny** 语句组成的一系列的规则列表，若干个规则列表构成一个访问控制列表。在配置访问控制列表的规则之前，首先需要创建一个访问控制列表。

可以使用如下命令创建一个访问控制列表：

acl number *acl-number* [**match-order** { **config** | **auto** }]

使用如下的命令删除一个或所有的访问控制列表：

undo acl { **number** *acl-number* | **all** }

参数说明：

- **number** *acl-number*：定义一个数字型的 ACL。
- *acl-number*：访问控制规则序号。1000～1999 是基于接口的访问控制列表，2000～2999 范围的数字型访问控制列表是基本的访问控制列表，3000～3999 范围的数字型访问控制列表是高级的访问控制列表，4000～4999 是基于 MAC 地址的访问控制列表。
- **match-order config**：指定匹配该规则时按用户的配置顺序。
- **match-order auto**：指定匹配该规则时系统自动排序，即按 “ 深度优先 ”的顺序。
- **all**：删除所有配置的 ACL。

缺省情况下匹配顺序为按用户的配置排序，即 “ **config** ”。用户一旦指定某一条访问控制列表的匹配顺序，就不能再更改该顺序，除非把该 ACL 的内容全部删除，再重新指定其匹配顺序。

创建了一个访问控制列表之后，将进入 ACL 视图，ACL 视图是按照访问控制列表的用途来分类的，例如创建了一个数字编号为 3000 的数字型 ACL，将进入高级 ACL 视图，路由器的提示符如下所示：

```
[Quidway-acl-adv-3000]
```

进入了 ACL 视图之后，就可以配置 ACL 的规则了。对于不同的 ACL，其规则是不一样的，具体的各种 ACL 的规则的配置方法将在后面小节分别介绍。

3.1.5 基本访问控制列表

基本访问控制列表只能使用源地址信息，做为定义访问控制列表的规则的元素。通过上面小节介绍的 acl 命令，可以创建一个基本的访问控制列表，同时进入基本访问控制列表视图，在基本访问控制列表视图下，可以创建基本访问控制列表的规则。

可以使用如下的命令定义一个基本访问控制列表的规则：

rule [*rule-id*] { **permit** | **deny** } [**source** *sour-addr sour-wildcard* | **any**] [**time-range** *time-name*] [**logging**] [**fragment**] [**vpn-instance** *vpn-instance-name*]

参数说明：

- *rule-id*：可选参数，ACL 规则编号，范围为 0～65534。当指定了编号，如果与编号对应的 ACL 规则已经存在，则会使用新定义的规则覆盖旧的定义，相当于编辑一个已经存在的 ACL 的规则。如果与编号对应的 ACL 规则不存在，则使用指定的编号创建一个新的规则。如果不指定编号，表示增加一个新规则，系统自动会为这个 ACL 规则分配一个编号，并增加新规则。
- **permit**：通过符合条件的数据包。
- **deny**：丢弃符合条件的数据包。
- **source**：可选参数，指定 ACL 规则的源地址信息。如果不指定，表示报文的任何源地址都匹配。
- *sour-addr*：数据包的源地址，点分十进制表示；或用“ **any** ”代表源地址 0.0.0.0，通配符 255.255.255.255。
- *sour-wildcard*：源地址通配符，点分十进制表示。
- **time-range**：可选参数，指定访问控制列表的生效时间。
- *time-name*：访问控制列表生效的时间段名字。
- **logging**：可选参数，是否对符合条件的数据包做日志。日志内容包括访问控制规则的序号，数据包通过或被丢弃，数据包的数目。
- **fragment**：可选参数，指定该规则是否仅对非首片分片报文有效。当包含此参数时表示该规则仅对非首片分片报文有效。
- **vpn-instance**：可选参数，指定报文是属于哪个 VPN 实例的。如果没有指定，该规则对所有 VPN 实例中的报文都有效；如果指定了，则表示该规则仅仅对指定的 VPN 实例中的报文有效。

对已经存在的 ACL 规则，如果采用指定 ACL 规则编号的方式进行编辑，没有配置的部分是不受影响的。例如：

先配置了一个 ACL 规则：

```
rule 1 deny source 1.1.1.1 0
```

然后再对这个 ACL 规则进行编辑：

```
rule 1 deny logging
```

这个时候，ACL 的规则则变成：

```
rule 1 deny source 1.1.1.1 0 logging
```

可以使用如下命令删除一个基本访问控制列表的规则：

undo rule *rule-id* [**source**] [**time-range**] [**logging**] [**fragment**] [**vpn-instance** *vpn-instance-name*]

参数说明：

- *rule-id*：ACL 规则编号，必须是一个已经存在的 ACL 规则编号。如果后面不指定参数，则将这个 ACL 规则完全删除。否则只是删除对应 ACL 规则的部分信息。
- **source**：可选参数，仅仅删除编号对应的 ACL 规则的源地址部分的信息设置。
- **time-range**：可选参数，仅仅删除编号对应的 ACL 规则在规定时间生效的设置。
- **logging**：可选参数，仅仅删除编号对应的 ACL 规则对符合条件的数据包做日志的设置。
- **fragment**：可选参数，仅仅删除编号对应的 ACL 规则仅对非首片分片报文有效的设置。
- **vpn-instance**：可选参数，仅仅删除编号对应的 ACL 规则中关于 VPN 实例的设置。

3.1.6 高级访问控制列表

高级访问控制列表可以使用数据包的源地址信息、目的地址信息、IP 承载的协议类型、针对协议的特性，例如 TCP 的源端口、目的端口，ICMP 协议的类型、代码等内容定义规则。可以利用高级访问控制列表定义比基本访问控制列表更准确、更丰富、更灵活的规则。

通过前面小节介绍的 acl 命令，可以创建一个高级的访问控制列表，同时进入高级访问控制列表视图，在高级访问控制列表视图下，可以创建高级访问控制列表的规则。

可以使用如下的命令定义一个高级访问控制列表规则：

rule [*rule-id*] { **permit** | **deny** } *protocol* [**source** *sour-addr sour-wildcard* | **any**] [**destination** *dest-addr dest-mask* | **any**] [**soucre-port** *operator port1* [*port2*]] [**destination-port** *operator port1* [*port2*]] [**icmp-type** { *icmp-message* |*icmp-type icmp-code*}] [**dscp** *dscp*] [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-name*] [**logging**] [**fragment**] [**vpn-instance**]

参数说明：

- *rule-id*：可选参数，ACL 规则编号，范围为 0～65534。当指定了编号，如果与编号对应的 ACL 规则已经存在，则会使用新定义的规则覆盖旧的定义，相当于编辑一个已经存在的 ACL 的规则。如果与编号对应的 ACL 规则不存在，则使用指定的编号创建一个新的规则。如果不指定编号，表示增加一个新规则，系统自动会为这个 ACL 规则分配一个编号。
- **deny**：拒绝符合条件的数据包。
- **permit**：允许符合条件的数据包。
- *protocol*：用名字或数字表示的 IP 承载的协议类型。数字范围为 1～255；名字取值范围为：gre、icmp、igmp、ip、ipinip、ospf、tcp、udp。
- **source**：可选参数，指定 ACL 规则的源地址信息。如果不配置，表示报文的任何源地址都匹配。
- *sour-addr*：数据包的源地址，点分十进制表示；或用“ **any** ”代表源地址 0.0.0.0，通配符 255.255.255.255。
- *sour-wildcard*：源地址通配符，点分十进制表示。
- **destination**：可选参数，指定 ACL 规则的目的地址信息。如果不配置，表示报文的任何目的地址都匹配。
- *dest-addr*：数据包的目的地址，点分十进制表示；或用 “ **any** ” 代表目的地址 0.0.0.0 ，通配符 255.255.255.255。
- *dest-wildcard*：目的地址通配符，点分十进制表示；或用 “ **any** ” 代表目的地址 0.0.0.0，通配符 255.255.255.255。
- **icmp-type**：可选参数，指定 ICMP 报文的类型和消息码信息，仅仅在报文协议是 ICMP 的情况下有效。如果不配置，表示任何 ICMP 类型的报文都匹配。
- *icmp-type*：ICMP 包可以依据 ICMP 的消息类型进行过滤。取值为 0～255 的数字。
- *icmp-code*：依据 ICMP 的消息类型进行过滤的 ICMP 包也可以依据消息码进行过滤。取值为 0～255 的数字。
- *icmp-message*：ICMP 包可以依据 ICMP 消息类型名字或 ICMP 消息类型和码的名字进行过滤。

- **source-port**：可选参数，指定 UDP 或者 TCP 报文的源端口信息，仅仅在规则指定的协议号是 TCP 或者 UDP 有效。如果不指定，表示 TCP/UDP 报文的任何源端口信息都匹配。
- **destination-port**：可选参数，指定 UDP 或者 TCP 报文的目的端口信息，仅仅在规则指定的协议号是 TCP 或者 UDP 有效。如果不指定，表示 TCP/UDP 报文的任何目的端口信息都匹配。
- *operator*：可选参数。比较源或者目的地址的端口号的操作符，名字及意义如下：lt（小于），gt（大于），eq（等于），neq（不等于），range（在范围内）。只有 range 需要两个端口号做操作数，其他的只需要一个端口号做操作数。
- *port1，port2*：可选参数。TCP 或 UDP 的端口号，用名字或数字表示，数字的取值范围为 0～65535。
- **dscp** *dscp*：指定 DSCP 字段（IP 报文中的 DS 字节）。
- **precedence**：可选参数，数据包可以依据优先级字段进行过滤。取值为 0～7 的数字，或名字。
- **tos** *tos*：可选参数，数据包可以依据服务类型字段进行过滤。取值为 0～15 的数字，或名字。
- **logging**：可选参数，是否对符合条件的数据包做日志。日志内容包括访问控制列表规则的序号，数据包通过或被丢弃，IP 承载的上层协议类型，源/目的地址，源/目的端口号，数据包的数目。
- **time-range** *time-name*：配置这条访问控制规则生效的时间段。
- **fragment**：指定该规则是否仅对非首片分片报文有效。当包含此参数时表示该规则仅对非首片分片报文有效。
- **vpn-instance**：可选参数，指定报文是属于哪个 VPN 实例的。如果没有指定，该规则对所有 VPN 实例中的报文都有效；如果指定了，则表示该规则仅仅对指定的 VPN 实例中的报文有效。

对已经存在的 ACL 规则，如果采用指定 ACL 规则编号的方式进行编辑，没有配置的部分是不受影响的。例如：

先配置了一个 ACL 规则：

```
rule 1 deny ip source 1.1.1.1 0
```

然后再对这个 ACL 规则进行编辑：

```
rule 1 deny ip destination 2.2.2.1 0
```

这个时候，ACL 的规则则变成：

```
rule 1 deny ip source 1.1.1.1 0 destination 2.2.2.1 0
```

可以使用如下命令删除一个高级访问控制列表的规则：

undo rule *rule-id* [**source**] [**destination**] [**source-port**] [**destination-port**] [**icmp-type**] [**dscp**] [**precedence**] [**tos**] [**time-range**] [**logging**] [**fragment**] [**vpn-instance** *vpn-instance-name*]

参数说明：

- *rule-id*：ACL 规则编号，必须是一个已经存在的 ACL 规则编号。如果后面不指定参数，则将这个 ACL 规则完全删除。否则只是删除对应 ACL 规则的部分信息。
- **source**：可选参数，仅仅删除编号对应的 ACL 规则的源地址部分的信息设置。
- **destination**：可选参数，仅仅删除编号对应的 ACL 规则的目的地址部分的信息设置。
- **source-port**：可选参数，仅仅删除编号对应的 ACL 规则的源端口部分的信息设置，仅仅在规则的协议号是 TCP 或者 UDP 的情况下有效。
- **destination-port**：可选参数，仅仅删除编号对应的 ACL 规则的目的端口部分的信息设置，仅仅在规则的协议号是 TCP 或者 UDP 的情况下有效。
- **icmp-type**：可选参数，仅仅删除编号对应的 ACL 规则 ICMP 类型和消息码部分的信息设置，仅仅在规则的协议号是 ICMP 的情况下有效。
- **precedence**：可选参数，仅仅删除编号对应的 ACL 规则的 precedence 的相关设置。
- **tos**：可选参数，仅仅删除编号对应的 ACL 规则的 tos 的相关设置。
- **time-range**：可选参数，仅仅删除编号对应的 ACL 规则在规定时间生效的设置。
- **logging**：可选参数，仅仅删除编号对应的 ACL 规则对符合条件的数据包做日志的设置。
- **fragment**：可选参数，仅仅删除编号对应的 ACL 规则仅对非首片分片报文有效的设置。
- **vpn-instance**：可选参数，仅仅删除编号对应的 ACL 规则中关于 VPN 实例的设置。

只有 TCP 和 UDP 协议需要指定端口范围。支持的操作符及其语法如下表。

表3-1 高级访问控制列表的操作符意义

操作符及语法	意义
eq portnumber	等于端口号 portnumber
gt portnumber	大于端口号 portnumber
lt portnumber	小于端口号 portnumber

操作符及语法	意义
neq portnumber	不等于端口号 portnumber
range portnumber1 portnumber2	介于端口号 portnumber1 和 portnumber2 之间

在指定 *portnumber* 时，对于部分常见的端口号，可以用相应的助记符来代替其实际数字，支持的助记符如下表。

表3-2 端口号助记符

协议	助记符	意义及实际值
TCP	Bgp	Border Gateway Protocol (179)
	Chargen	Character generator (19)
	Cmd	Remote commands (rcmd, 514)
	Daytime	Daytime (13)
	Discard	Discard (9)
	Domain	Domain Name Service (53)
	Echo	Echo (7)
	Exec	Exec (rsh, 512)
	Finger	Finger (79)
	Ftp	File Transfer Protocol (21)
	Ftp-data	FTP data connections (20)
	Gopher	Gopher (70)
	Hostname	NIC hostname server (101)
	Irc	Internet Relay Chat (194)
	Klogin	Kerberos login (543)
	Kshell	Kerberos shell (544)
	Login	Login (rlogin, 513)
	Lpd	Printer service (515)
	Nntp	Network News Transport Protocol (119)
	Pop2	Post Office Protocol v2 (109)
	Pop3	Post Office Protocol v3 (110)
	Smtp	Simple Mail Transport Protocol (25)
	Sunrpc	Sun Remote Procedure Call (111)
	Syslog	Syslog (514)
	Tacacs	TAC Access Control System (49)
	Talk	Talk (517)
	Telnet	Telnet (23)
	Time	Time (37)
	Uucp	Unix-to-Unix Copy Program (540)
	Whois	Nicname (43)
	Www	World Wide Web (HTTP, 80)

协议	助记符	意义及实际值
UDP	biff	Mail notify (512)
	bootpc	Bootstrap Protocol Client (68)
	bootps	Bootstrap Protocol Server (67)
	discard	Discard (9)
	dns	Domain Name Service (53)
	dnsix	DNSIX Securit Attribute Token Map (90)
	echo	Echo (7)
	mobilip-ag	MobileIP-Agent (434)
	mobilip-mn	MobilIP-MN (435)
	nameserver	Host Name Server (42)
	netbios-dgm	NETBIOS Datagram Service (138)
	netbios-ns	NETBIOS Name Service (137)
	netbios-ssn	NETBIOS Session Service (139)
	ntp	Network Time Protocol (123)
	rip	Routing Information Protocol (520)
	snmp	SNMP (161)
	snmptrap	SNMPTRAP (162)
	sunrpc	SUN Remote Procedure Call (111)
	syslog	Syslog (514)
	tacacs-ds	TACACS-Database Service (65)
	talk	Talk (517)
	tftp	Trivial File Transfer (69)
	time	Time (37)
	who	Who(513)
	Xdmcp	X Display Manager Control Protocol (177)

- 对于 ICMP 协议可以指定 ICMP 报文类型，缺省为全部 ICMP 报文。指定 ICMP 报文类型时，可以用数字（0～255），也可以用助记符。

表3-3 ICMP 报文类型助记符

助记符	意义
echo	Type=8, Code=0
echo-reply	Type=0, Code=0
fragmentneed-DFset	Type=3, Code=4
host-redirect	Type=5, Code=1
host-tos-redirect	Type=5, Code=3
host-unreachable	Type=3, Code=1
information-reply	Type=16,Code=0
information-request	Type=15,Code=0
net-redirect	Type=5, Code=0
net-tos-redirect	Type=5, Code=2
net-unreachable	Type=3, Code=0
parameter-problem	Type=12,Code=0
port-unreachable	Type=3, Code=3
protocol-unreachable	Type=3, Code=2
reassembly-timeout	Type=11,Code=1
source-quench	Type=4, Code=0
source-route-failed	Type=3, Code=5
timestamp-reply	Type=14,Code=0
timestamp-request	Type=13,Code=0
ttl-exceeded	Type=11,Code=0

配置举例请参考命令手册。

这样，用户通过配置防火墙，添加适当的访问规则，就可以利用包过滤来对通过路由器的 IP 包进行检查，从而过滤掉用户不希望通过路由器的包，起到保护网络安全的作用。

3.1.7 基于接口的访问控制列表

基于接口的访问控制列表，是一种特殊的访问控制列表，可以根据接收报文的接口指定规则。

通过前面小节介绍的 acl 命令，可以创建一个基于接口的访问控制列表，同时进入基于接口的访问控制列表视图，在基于接口的访问控制列表视图下，可以创建基于接口的访问控制列表规则。

可以使用如下的命令定义一个基于接口的访问控制列表规则：

rule [*rule-id*] { **permit** | **deny** } **interface** { *interface-type interface-number* | **any** } [**time-range** *time-name*] [**logging**]

参数说明：

- *rule-id*：可选参数，ACL 规则编号，范围为 0～65534。当指定了编号，如果与编号对应的 ACL 规则已经存在，则会使用新定义的规则覆盖旧的定义，相

当于编辑一个已经存在的 ACL 的规则。如果与编号对应的 ACL 规则不存在，则使用指定的编号创建一个新的规则。如果不指定编号，表示增加一个新规则，系统自动会为这个 ACL 规则分配一个编号，并增加新规则。

- **deny**：丢弃符合条件的数据包。
- **permit**：通过符合条件的数据包。
- **interface** *interface-type interface-number*：指定数据包的接口信息。如果不指定，表示所有的接口都匹配。**any** 代表所有的接口。
- **logging**：可选参数，是否对符合条件的数据包做日志。日志内容包括访问控制列表规则的序号，数据包通过或被丢弃，数据包的数目。
- **time-range** *time-name*：配置这条访问控制规则生效的时间段。

可以使用如下的命令删除一个基于接口的访问控制列表的规则：

undo rule *rule-id* [**logging** | **time-range**]*

参数说明：

- *rule-id*：ACL 规则编号，必须是一个已经存在的 ACL 规则编号。
- **logging**：可选参数，是否对符合条件的数据包做日志。日志内容包括访问控制列表规则的序号，数据包通过或被丢弃，数据包的数目。
- **time-range**：可选参数，指定规则在一定时间段内有效。

3.1.8 基于 MAC 地址的访问控制列表

基于以太网的 MAC 地址的访问控制列表的 *acl-number* 取值范围是 4000～4999。

可以使用如下的命令定义一个基于 MAC 地址的访问控制列表规则：

rule [*rule-id*] { **deny** | **permit** } [**type** *type-code type-mask* | **lsap** *lsap-code lsap-mask*]] [**source-mac** *sour-addr sour-mask*] [**dest-mac** *dest-addr dest-mask*]

参数说明如下：

- rule-id 为规则号。
- *type-code* 为一个十六进制数，格式为 xxxx，用来匹配传输报文的协议类型。type-mask 为协议类型的通配符（掩码）。关于 *type-code* 值，请参考本手册“链路层协议配置”部分的“网桥配置”中的附表。
- *lsap-code* 为一个十六进制数，格式为 xxxx，用来匹配接口上桥接报文的封装格式，*lsap-mask* 为协议类型的通配符（掩码）.
- *sour-addr* 为数据帧的源 MAC 地址，格式为 xxxx-xxxx-xxxx，用来匹配一个数据帧的源地址。*sour-mask* 为源 MAC 地址的通配符（掩码）。

- *dest-addr* 为报文的目的 MAC 地址，格式为 xxxx-xxxx-xxxx，用来匹配一个数据帧的目的地址。*dest- mask* 为目的 MAC 地址的通配符（掩码）。

可以使用如下的命令删除一个基于 MAC 地址的访问控制列表的规则：

undo rule *rule-id*

参数说明：

- *rule-id*：ACL 规则编号，必须是一个已经存在的 ACL 规则编号。

3.1.9 ACL 对分片报文的支持

传统的包过滤并不处理所有 IP 报文分片，而是只对第一个（首片）分片报文进行匹配处理，后续分片一律放行。这样，网络攻击者可能构造后续的分片报文进行流量攻击，就带来了安全隐患。

VRP 平台的包过滤提供了对分片报文过滤的功能，包括：对所有的分片报文进行三层（IP 层）的匹配过滤；同时，对于包含扩展信息的 ACL 规则项（例如包含 TCP/UDP 端口号，ICMP 类型），提供标准匹配和精确匹配两种匹配方式。标准匹配即三层信息的匹配，匹配将忽略三层以外的信息；精确匹配则对所有的 ACL 项条件进行匹配，这就要求防火墙必须记录首片分片报文的状态以获得完整的后续分片的匹配信息。缺省的功能方式为标准匹配方式。

在 ACL 的规则配置项中，通过关键字 **fragment** 来标识该 ACL 规则仅对非首片分片报文有效，而对非分片报文和首片分片报文则忽略此规则。而不包含此关键字的配置规则项对所有报文均有效。

例如：

```
[Quidway-basic-2000] rule deny source 202.101.1.0 0.0.0.255 fragment
[Quidway-basic-2000] rule permit source 202.101.2.0 0.0.0.255
[Quidway-adv-3001] rule permit ip destination 171.16.23.1 0 fragment
[Quidway-adv-3001] rule deny ip destination 171.16.23.2 0
```

上述规则项中，所有项对非首片分片报文均有效；第一，三项对非分片和首片分片报文是被忽略的，仅仅对非首片分片报文有效。

3.2 访问控制列表配置

访问控制列表的配置包括：

- 配置基本访问控制列表
- 配置高级访问控制列表
- 配置基于接口的访问控制列表
- 配置基于 MAC 地址的访问控制列表

- 删除访问控制列表

3.2.1 配置基本访问控制列表

请进行下列配置。

表3-4 配置基本访问控制列表

操作	命令
在系统视图下，创建一个基本访问控制列表。	**acl number** *acl-number* [**match-order** { **config** | **auto** }]
在基本访问控制列表视图下，配置 ACL 规则	**rule** [*rule-id*] { **permit** | **deny** } [**source** *sour-addr sour-wildcard* | **any**] [**time-range** *time-name*] [**logging**] [**fragment**] [**vpn-instance** *vpn-instance-name*] **undo rule** *rule-id* [**source**] [**time-range**] [**logging**] [**vpn-instance** *vpn-instance-name*] [**fragment**]

3.2.2 配置高级访问控制列表

请进行下列配置。

表3-5 配置高级访问控制列表

操作	命令
在系统视图下，创建一个高级访问控制列表。	**acl number** *acl-number* [**match-order** { **config** | **auto** }]
在高级访问控制列表视图下，配置 ACL 规则	**rule** [*rule-id*] { **permit** | **deny** } *protocol* [**source** *sour-addr sour-wildcard* | **any**] [**destination** *dest-addr dest-mask* | **any**] [**source-port** *operator port1* [*port2*]] [**destination-port** *operator port1* [*port2*]] [**icmp-type** {*icmp-type icmp-code*| *icmp-message}*] [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-name*] [**logging**] [**fragment**] [**vpn-instance** *vpn-instance-name*] **undo rule** *rule-id* [**source**] [**destination**] [**source-port**] [**destination-port**] [**icmp-type**] [**precedence**] [**tos**] [**time-range**] [**logging**] [**fragment**] [**vpn-instance** *vpn-instance-name*]

3.2.3 配置基于接口的访问控制列表

请进行下列配置。

表3-6 配置基于接口的访问控制列表

操作	命令
在系统视图下，创建一个基于接口的访问控制列表。	**acl number** *acl-number* [**match-order** { **config** | **auto** }]
在基于接口的访问控制列表视图下，配置 ACL 规则。	**rule** { **permit** | **deny** } [**interface** *type number*] [**time-range** *time-name*] [**logging**] **undo rule** *rule-id* [**time-range** | **logging**]*

其中， **interface** *type number* 指定接口名，**any** 表示所有接口。

3.2.4 配置基于 MAC 地址的访问控制列表

请进行下列配置。

表3-7 配置基于 MAC 地址的访问控制列表

操作	命令
在系统视图下，创建一个基于 MAC 地址的访问控制列表	**acl number** *acl-number* [**match-order** { **config** | **auto** }]
在基于 MAC 地址的访问控制列表视图下，配置 ACL 规则。	**rule** [*rule-id*] { **deny** | **permit** } [**type** *type-code type-wildcard* | **lsap** *lsap-code lsap-wildcard*]] [**source-mac** *sour-addr sour-wildcard*] [**dest-mac** *dest-addr dest-mask*] **undo rule** *rule-id*

3.2.5 删除访问控制列表

请在系统视图下进行下列配置。

表3-8 删除访问控制列表

操作	命令
删除访问控制列表	**undo acl** { **number** *acl-number* | **all**}

3.3 时间段配置

时间段的配置包括：

- 创建一个时间段

3.3.1 创建/删除一个时间段

在同一个名字下可以配置多个时间段，这些时间段是“ 或 ”关系。

请在系统视图下进行下列配置。

表3-9 配置时间段

操作	命令
创建一个时间段	**time-range** *time-name* [*start-time* **to** *end-time*] [*days*] [**from** *time1 date1*] [**to** *time2 date2*]
删除一个时间段	**undo time-range** *time-name* [*start-time* **to** *end-time*] [*days*] [**from** *time1 date1*] [**to** *time2 date2*]

3.4 访问控制列表的显示与调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 ACL 和时间段的运行情况，通过查看显示信息确认配置的效果。在用户视图下执行 **reset** 命令可以清除访问规则计数器。

表3-10 访问控制列表的显示与调试

操作	命令
显示配置的访问控制列表规则	**display acl** { **all** | *acl-number* }
显示时间段	**display time-range** { **all** | *time-name* }
清除访问规则计数器	**reset acl counter** { **all** | *acl-number* }

3.5 访问控制列表典型配置案例

请参见包过滤防火墙部分典型配置案例。

第4章 防火墙配置

4.1 防火墙简介

在大厦构造中，防火墙被设计用来防止火从大厦的一部分传播到另一部分。网络的防火墙服务于类似目的：防止因特网的危险传播到您的内部网络。

防火墙一方面阻止来自因特网的对受保护网络的未授权或未认证的访问，另一方面允许内部网络的用户对因特网进行 Web 访问或收发 E-mail 等。防火墙也可以作为一个访问因特网的权限控制关口，如允许组织内的特定的人可以访问因特网。现在的许多防火墙同时还具有一些其他特点，如进行身份鉴别，对信息进行安全（加密）处理等等。

防火墙不单用于对因特网的连接，也可以用来在组织网络内部保护大型机和重要的资源（如数据）。对受保护数据的访问都必须经过防火墙的过滤，即使网络内部用户要访问受保护的数据，也要经过防火墙。

当外部网络的用户访问网内资源时，要经过防火墙；而内部网络的用户访问网外资源时，也会经过防火墙。这样，防火墙就起到了一个“ 警卫 ”的作用，可以将需要禁止的数据包在这里给丢掉。

VRP 中的防火墙主要是指基于访问控制列表（ACL）的包过滤（以下简称 ACL/包过滤）、基于应用层的包过滤（以下简称状态防火墙 ASPF）和地址转换。有关地址转换请参见网络协议的内容，本章以下部分将重点介绍 ACL/包过滤防火墙和状态防火墙。

4.1.1 ACL/包过滤防火墙简介

1. ACL/包过滤概述

ACL/包过滤应用在路由器中，就为路由器增加了对数据包的过滤功能。ACL/包过滤实现对 IP 数据包的过滤，对路由器需要转发的数据包，先获取数据包的包头信息，包括 IP 层所承载的上层协议的协议号，数据包的源地址、目的地址、源端口和目的端口等，然后和设定的 ACL 规则进行比较，根据比较的结果决定对数据包进行转发或者丢弃。

2. 包过滤对分片报文过滤的支持

VRP 平台 ACL/包过滤提供了对分片报文检测过滤的支持。包过滤防火墙将检测报文类型（非分片报文、首片分片报文、非首片分片报文）；获得报文的三层（IP 层）信息（基本 ACL 规则和不含三层以外信息的高级 ACL 规则）及三层以外的信息（包含三层以外信息的高级 ACL 规则）用于匹配，并获得配置的 ACL 规则。

对于配置了精确匹配过滤方式的高级 ACL 规则，包过滤防火墙需要记录每一个首片分片的三层以外的信息，当后续分片到达时，使用这些保存的信息对 ACL 规则的每一个匹配条件进行精确匹配。

应用精确匹配过滤后，包过滤防火墙的执行效率会略微降低，配置的匹配项目越多，效率降低越多，可以配置门限值来限制防火墙最大处理的数目。

有关标准匹配及精确匹配的概念参见访问控制列表配置。

4.1.2 ASPF 简介

ACL/包过滤防火墙为静态防火墙，目前存在如下问题：

- 对于多通道的应用层协议（如 FTP，H.323 等），部分安全策略配置无法预知。
- 无法检测某些来自于应用层的攻击行为（如 TCP SYN，Java applet 等）。

故提出了状态防火墙——ASPF 的概念。ASPF（Application Specific Packet Filter）是针对应用层及传输层的包过滤，即基于状态的报文过滤。ASPF 能够实现的应用层协议检测包括：FTP、HTTP、SMTP、RTSP、H.323（Q.931，H.245，RTP/RTCP）检测；能够实现的传输层协议检测包括：通用 TCP/UDP 检测。

ASPF 的主要功能如下：

- 能够检查应用层协议信息，如报文的协议类型和端口号等信息，并且监控基于连接的应用层协议状态。对于所有连接，每一个连接状态信息都将被 ASPF 维护并用于动态地决定数据包是否被允许通过防火墙进入内部网络，以便阻止恶意的入侵。
- 能够检测传输层协议信息（即通用 TCP 和 UDP 协议检测），能够根据源、目的地址及端口号决定 TCP 或 UDP 报文是否可以通过防火墙进入内部网络。

ASPF 的其它功能：

- ASPF 不仅能够根据连接的状态对报文进行过滤还能够对应用层报文的内容加以检测，提供对不可信站点的 Java Blocking（Java 阻断）功能，用于保护网络不受有害的 Java Applets 的破坏。
- 增强的会话日志功能。可以对所有的连接进行记录，包括：记录连接的时间、源地址、目的地址、使用的端口和传输的字节数。
- 支持应用协议端口映射 PAM（Port to Application Map），允许用户自定义应用层协议使用非通用端口。

在网络边界，ASPF 和普通的静态防火墙协同工作，能够为企业内部网络提供更全面的、更符合实际需求的安全策略。

1. 基本概念

- Java Blocking

Java Blocking 是对通过 HTTP 协议传输的 Java applet 小程序进行阻断。当配置了 Java Blocking 时，用户为试图在 web 页面中获取包含 Java applet 的程序而发送的请求指令将会被 ASPF 阻断过滤。

- 端口映射

应用层协议使用通用的端口号进行通信。端口映射允许用户对不同的应用定义一组新的端口号。端口映射提供了一些机制来维护和使用用户定义的端口配置信息。

PAM 支持两类映射机制：通用端口映射和基于基本访问控制列表（ACL）的主机端口映射。通用端口映射是将用户自定义端口号和应用层协议建立映射关系，例如：将 8080 端口映射为 HTTP 协议，这样所有目标端口是 8080 的 TCP 报文被认为是 HTTP 报文。主机端口映射是对去往/来自某些特定主机的报文建立自定义端口号和应用协议的映射，例如：将目的地址为 10.110.0.0 网段的使用 8080 端口的 TCP 报文映射为 HTTP 报文。主机的范围可由基本的 ACL 指定。

- 单通道协议/多通道协议

单通道协议：从会话建立到删除的全过程中，只有一个通道参与数据交互，例如 SMTP，HTTP。

多通道协议：包含一个控制通道和若干其它控制或数据通道，即控制信息的交互和数据的传送是在不同的通道上完成的，例如 FTP，RTSP。

- 内部接口和外部接口

如果路由器连接了内部网和 Internet，并且路由器要通过部署 ASPF 来保护内部网的服务器，则路由器上与内部网连接的接口就是内部接口，与 Internet 相连的接口就是外部接口。

当 ASPF 应用于路由器外部接口的出方向时，可以在防火墙上为内部网用户访问 Internet 的返回报文打开一个临时通道。

2. 应用层协议检测的基本原理

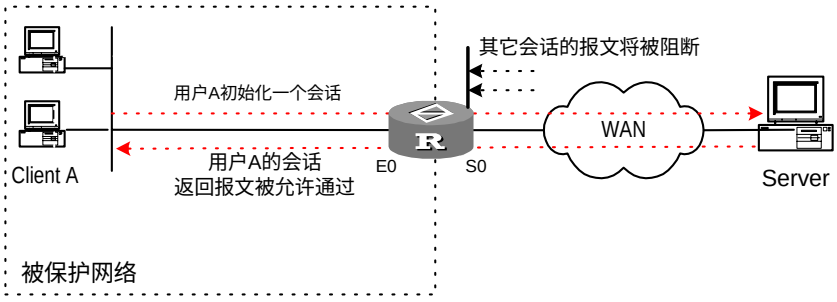

图4-1 应用层协议检测的基本原理

如上图所示，为了保护内部网络，一般情况下需要在路由器上配置静态访问控制列表，以便允许内部网的主机的访问外部网络，同时拒绝外部网络的主机访问内部网络。但静态访问控制列表会将用户发起连接后返回的报文过滤掉，导致连接无法正常建立。当在路由器上配置了应用层协议检测后，ASPF 可以检测每一个应用层的会话，并创建一个状态表和一个临时访问控制表（TACL）。状态表在检测到第一个外发报文时创建，用于维护了一次会话中某一时刻会话所处的状态，并检测会话状态的转换是否正确。临时访问控制列表的表项在创建状态表项的时候同时创建，会话结束后删除，它相当于一个扩展 ACL 的 permit 项。TACL 主要用于匹配一个会话中的所有返回的报文，可以为某一应用返回的报文在防火墙的外部接口上建立了一个临时的返回通道。

下面以 FTP 检测为例说明多通道应用层协议检测的过程。

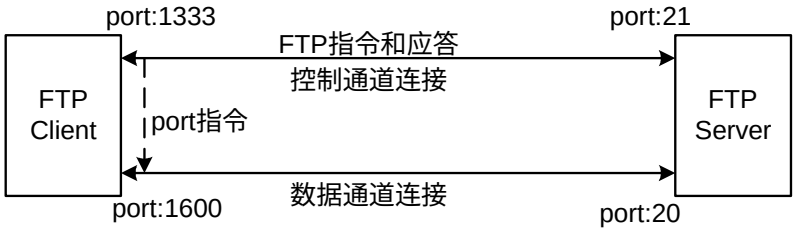

图4-2 FTP 检测过程示意图

FTP 连接的建立过程如下：

假设 FTP Client 以 1333 端口向 FTP Server 的 21 端口发起 FTP 控制通道的连接，通过协商决定由 Server 端的 20 端口向 Client 端的 1600 端口发起数据通道的连接，数据传输超时或结束后连接删除。

FTP 检测在 FTP 连接建立到拆除过程中的处理如下：

(1) 检查从出接口上向外发送的 IP 报文，确认为基于 TCP 的 FTP 报文。

(2) 检查端口号确认连接为控制连接，建立返回报文的 TACL 和状态表。

(3) 检查 FTP 控制连接报文，解析 FTP 指令，根据指令更新状态表，如果包含数据通道建立指令，则创建数据连接的 TACL；对于数据连接，不进行状态检测。

(4) 对于返回报文，根据协议类型做相应匹配检查，检查将根据相应协议的状态表和 TACL 决定报文是否允许通过。

(5) FTP 连接删除时，状态表及 TACL 随之删除。

单通道应用层协议（例如 SMTP，HTTP）的检测过程比较简单，当发起连接时建立 TACL，连接删除时随之删除 TACL 即可。

3. 传输层协议检测基本原理

这里的传输层协议检测是指通用 TCP/UDP 检测。通用 TCP 和 UDP 检测与应用层协议检测不同，是对报文的传输层信息进行的检测，如源、目的地址及端口号等。

通用 TCP/UDP 检测要求返回到 ASPF 外部接口的报文要与前面从 ASPF 外部接口发出去的报文完全匹配，即源、目的地址及端口号恰好对应，否则返回的报文将被阻塞。因此对于 FTP，H.323 这样的多通道应用层协议，在不配置应用层检测而直接配置 TCP 检测的情况下会导致连接无法建立。

4.2 包过滤防火墙配置

包过滤防火墙的配置包括：

- 允许或禁止防火墙
- 设置防火墙缺省过滤方式
- 设置包过滤防火墙分片报文检测开关
- 配置分片报文检测的上、下门限值
- 在接口上应用访问控制列表

4.2.1 允许或禁止防火墙

请在系统视图下进行下列配置。

表4-1 允许或禁止防火墙

操作	命令
允许防火墙	**firewall enable**
禁止防火墙	**undo firewall enable**

系统缺省情况下禁止防火墙。

4.2.2 设置防火墙缺省过滤方式

设置防火墙的缺省过滤方式，即在没有一个合适的规则去判定用户数据包是否可以通过的时候，防火墙采取的策略是允许还是禁止该数据包通过。

请在系统视图下进行下列配置。

表4-2 设置防火墙缺省过滤方式

操作	命令
设置缺省过滤方式为允许通过	**firewall default permit**
设置缺省过滤方式为禁止通过	**firewall default deny**

在防火墙开启时，系统缺省为允许。

4.2.3 设置包过滤防火墙分片报文检测开关

请在系统视图下进行下列配置。

表4-3 设置分片报文检测开关

操作	命令
打开分片报文检测开关	**firewall fragments-inspect**
关闭分片报文检测开关	**undo firewall fragments-inspect**

⚠ 注意：

只有打开了分片报文检测开关，精确匹配模式才能真正有效。

4.2.4 配置分片报文检测的上、下门限值

请在系统视图下进行下列配置。

表4-4 配置分片报文检测的上、下门限值

操作	命令
指定上、下限分片状态记录数目	**firewall fragments-inspect** { **high** | **low** } { **default** | *number* }
恢复上限分片状态记录数目为缺省值	**undo firewall fragments-inspect** { **high** | **low** }

缺省的上限（**high**）分片状态记录数目为 2000；下限（**low**）分片状态记录数目为 1500。

4.2.5 在接口上应用访问控制列表

将访问规则应用到接口时，同时会遵循时间段过滤原则，另外可以对接口的收发报文分别指定访问规则。

请在接口视图下进行下列配置。

表4-5 在接口上应用访问控制列表

操作	命令
指定接口上过滤接收报文的规则	**firewall packet-filter** *acl-number* { **inbound** | **outbound** } [**match-fragments** { **normally** | **exactly** }]
取消接口上过滤接收报文的规则	**undo firewall packet-filter** *acl-number* { **inbound** | **outbound** }

基于接口的访问控制列表（即序号为 1000 到 1999 的 ACL）只能用参数 **outbound**。

高级访问控制列表提供标准匹配和精确匹配两种匹配方式。标准匹配即三层信息的匹配，匹配将忽略三层以外的信息；精确匹配则对所有的高级 ACL 的过滤规则进行匹配，这就要求防火墙必须记录首片分片报文的状态以获得完整的后续分片的匹配信息。缺省的模式为标准匹配方式。

match-fragments 参数仅能应用于高级访问控制列表。

4.2.6 包过滤防火墙显示与调试

在完成上述配置后，在所有视图下执行如下 **display** 命令可以显示包过滤防火墙的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **debugging** 命令可以对包过滤防火墙进行调试。

表4-6 防火墙显示与调试

操作	命令
显示接口的有关防火墙的统计信息	**display firewall-statistics** { **all** | **interface** *type number* | **fragments-inspect** }
打开防火墙包过滤调试信息开关	**debugging firewall** { **all** | **eff** | **icmp** | **tcp** | **udp** | **fragments-inspect** | **others** } [**interface** *type number*]
关闭防火墙包过滤调试信息开关	**undo debugging firewall** { **all** | **eff** | **icmp** | **tcp** | **udp** | **fragments-inspect** | **others** } [**interface** *type number*]

4.2.7 包过滤防火墙典型配置举例

1. 组网需求

以下通过一个公司配置防火墙的实例来说明防火墙的配置。

该公司通过一台 Quidway 路由器的接口 Serial1/0/0 访问 Internet，路由器与内部网通过以太网接口 Ethernet0/0/0 连接。公司内部对外提供 WWW、FTP 和 Telnet 服务，公司内部子网为 129.38.1.0，其中，内部 FTP 服务器地址为 129.38.1.1，内部 Telnet 服务器地址为 129.38.1.2，内部 WWW 服务器地址为 129.38.1.3，公司对外地址为 202.38.160.1。在路由器上配置了地址转换，这样内部 PC 机可以访问 Internet，外部 PC 可以访问内部服务器。通过配置防火墙，希望实现以下要求：

- 外部网络只有特定用户可以访问内部服务器。
- 内部网络只有特定主机可以访问外部网络。

假定外部特定用户的 IP 地址为 202.39.2.3。

2. 组网图

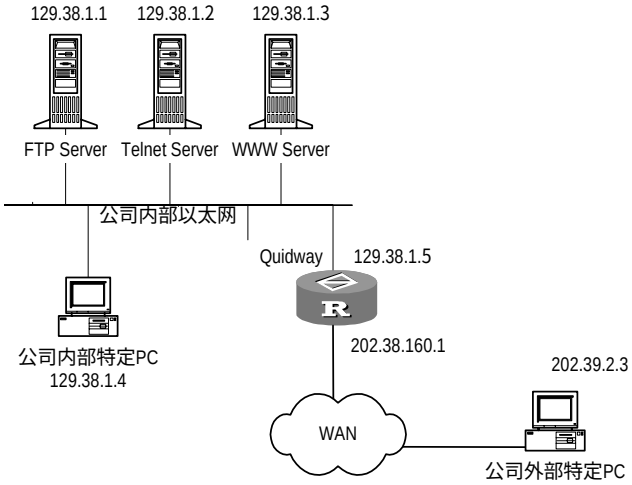

图4-3 包过滤防火墙配置案例组网图

3. 配置步骤

在路由器 Quidway 上允许防火墙。

```
[Quidway] firewall enable
```

设置防火墙缺省过滤方式为允许包通过。

```
[Quidway] firewall default permit
```

创建访问控制列表 3001。

```
[Quidway] acl number 3001
```

配置规则禁止所有 IP 包通过。

```
[Quidway-acl-adv-3001] rule deny ip
```

配置规则允许特定主机访问外部网，允许内部服务器访问外部网。

```
[Quidway-acl-adv-3001] rule permit ip source 129.38.1.4 0
[Quidway-acl-adv-3001] rule permit ip source 129.38.1.1 0
[Quidway-acl-adv-3001] rule permit ip source 129.38.1.2 0
[Quidway-acl-adv-3001] rule permit ip source 129.38.1.3 0
```

创建访问控制列表 3002

```
[Quidway] acl number 3002
```

配置规则允许特定用户从外部网访问内部服务器。

```
[Quidway-acl-adv-3002] rule permit tcp source 202.39.2.3 0 destination
202.38.160.1 0
```

配置规则允许特定用户从外部网取得数据（只允许端口大于 1024 的包）。

```
[Quidway-acl-adv-3002] rule permit tcp destination 202.38.160.1 0
destination-port gt 1024
```

将规则 3001 作用于从接口 Ethernet0/0/0 进入的包。

```
[Quidway-Ethernet0/0/0] firewall packet-filter 3001 inbound
```

将规则 3002 作用于从接口 Serial1/0/0 进入的包。

```
[Quidway-Serial1/0/0] firewall packet-filter 3002 inbound
```

4.3 ASPF 配置

ASPF 主要配置包括：

- 允许防火墙
- 配置访问控制列表
- 定义一个 ASPF 策略
- 在选定的接口上应用 ASPF 策略

4.3.1 允许防火墙

此配置与包过滤防火墙配置相同，请参见上一节的内容。

4.3.2 配置访问控制列表

为了保护内部网络，需要在路由器上配置访问控制列表，允许内部网的主机的访问外部网络，同时拒绝外部网络的主机访问内部网络，并将访问控制列表应用到外部接口上。

表4-7 配置访问控制列表

操作	命令
配置访问控制列表（在 ACL 视图下）	**rule deny**
将 ACL 应用到出接口上（在接口视图下）	**firewall packet-filter** *acl-num* **inbound**

4.3.3 定义 ASPF 策略

请按以下步骤定义一个 ASPF 策略：

- 创建一个 ASPF 策略；
- 配置空闲超时值；
- 配置应用层协议检测；
- 配置通用 TCP 和 UDP 检测。

1. 创建一个 ASPF 策略

请在系统视图下进行下列配置

表4-8 创建一个 ASPF 策略

操作	命令
创建一个 ASPF 策略	**aspf-policy** *aspf-policy-number*
删除创建一个 ASPF 策略	**undo aspf-policy** *aspf-policy-numbe*

aspf-policy-number 为 ASPF 策略号，范围为 1～99。

2. 配置空闲超时值

请在 ASPF 策略视图下进行下列配置。

表4-9 配置空闲超时值

操作	命令
配置空闲超时值	**aging-time** { **syn** | **fin** | **tcp** | **udp** } *seconds*
恢复默认的空闲超时值	**undo aging-time** { **syn** | **fin** | **tcp** | **udp** }

该任务用来配置 TCP 的 SYN 状态等待超时值、FIN 状态等待超时值，TCP 和 UDP 会话表项空闲状态超时值。缺省情况 syn、fin、tcp、udp 的超时时间分别为 30s、5s、3600s 和 30s。

3. 配置应用层协议检测

请在 ASPF 策略视图下进行下列配置。

表4-10 配置应用层协议检测

操作	命令
为应用层协议配置 ASPF 检测	**detect** *protocol* [**aging-time** *seconds*]
删除配置的应用协议检测	**undo detect** *protocol*

应用层协议包括：ftp、http、h323、smtp、rtsp；传输层协议包括：tcp、udp。应用层协议的超时时间缺省值为 3600 秒。基于 TCP 协议的超时时间缺省值为 3600 秒；基于 UDP 协议的 **timeout** 超时时间缺省值为 30 秒。

在 *protocol* 选择 http 时，可以配置 Java 阻断，如下。

表4-11 配置 Java 阻断检测

操作	命令
配置 Java 阻断检测	**detect http** [**java-blocking** *acl-number*] [**aging-time** *seconds*]
取消对 HTTP 的检测规则	**undo detect http**

4. 配置通用 TCP 和 UDP 协议检测

请在 ASPF 策略视图下进行下列配置。

表4-12 配置通用 TCP 和 UDP 协议检测

操作	命令
配置通用 TCP 协议检测	**detect tcp** [**aging-time** *seconds*]
配置通用 UDP 协议检测	**detect udp** [**aging-time** *seconds*]
删除通用 TCP 协议检测	**undo detect tcp**
删除通用 UDP 协议检测	**undo detect udp**

基于 TCP 协议的超时时间缺省值为 3600 秒；基于 UDP 协议的超时时间缺省值为 30 秒。

在不配置应用层检测，直接配置 TCP 或 UDP 检测的情况下，可能会产生部分报文无法返回的情况，故建议应用层检测和 TCP/UDP 检测配合使用。

📖 说明：

对于 Telnet 应用，直接配置通用 TCP 检测即可实现 ASPF 功能。

4.3.4 在接口上应用 ASPF 策略

将定义好 ASPF 策略应用到外部接口上，才能对通过接口的流量进行检测。

请在接口视图下进行下列配置。

表4-13 在接口上应用 ASPF 策略

操作	命令
在接口上应用 ASPF 策略	**firewall aspf** *aspf-policy-number* { **inbound** | **outbound** }
删除该接口上应用的 ASPF 策略	**undo firewall aspf** *aspf-policy-number* { **inbound** | **outbound** }

由于 ASPF 对于应用层协议状态的保存和维护都是基于接口的，因此，在实际应用中，必须保证报文入口的一致性，即必须保证连接发起报文和返回报文基于同一接口。

4.3.5 端口映射配置

1. 配置端口映射项

请在系统视图下进行下列配置。

表4-14 配置端口映射

操作	命令
配置通用端口映射功能	**port-mapping** *application-name* **port** *port-number*
删除用户配置的通用端口映射	**undo port-mapping** *application-name* **port** *port-number*
配置主机端口映射功能	**port-mapping** *application-name* **port** *port-number* **acl** *acl-number*
删除用户配置的主机端口映射	**undo port-mapping** *application-name* **port** *port-number* **acl** *acl-number*

主机端口映射中特定主机的范围应由基本的 ACL 指定。

4.3.6 ASPF 显示与调试

在完成上述配置后，在所有视图下执行如下 **display** 命令可以显示 ASPF 的运行情况，通过查看显示信息验证配置的效果。在用户视图下执行 **debugging** 命令查看 ASPF 调试信息。

表4-15 ASPF 显示与调试

操作	命令
显示所有 ASPF 配置情况	**display aspf all**
显示应用 ASPF 策略和访问列表的接口配置	**display aspf interface**
显示一个特定 ASPF 策略的配置	**display aspf policy** *aspf-policy-number*
显示 ASPF 当前会话状态	**display aspf session** [**verbose**]
显示端口映射信息	**display port-mapping** [*application-name* | **port** *port-number*]
打开 ASPF 调试开关	**debugging aspf** { **all** | **verbose** | **events** | **ftp** | **h323** | **http** | **rtsp** | **session** | **smtp** | **tcp** | **timers** | **udp** }
关闭 ASPF 调试开关	**undo debugging aspf** { **all** | **verbose** | **events** | **ftp** | **h323** | **http** | **rtsp** | **session** | **smtp** | **tcp** | **timers** | **udp** }

4.3.7 ASPF 典型配置案例

1. 组网需求

在防火墙上配置一个 ASPF 策略，检测通过防火墙的 FTP 和 HTTP 流量。要求：如果该报文是内部网络用户发起的 FTP 和 HTTP 连接的返回报文，则允许其通过防火墙进入内部网络，其他报文被禁止；并且，此 ASPF 策略能够过滤掉来自服务器 2.2.2.11 的 HTTP 报文中的 Java Applets。本例可以应用在本地用户需要访问远程网络服务的情况下。

2. 组网图

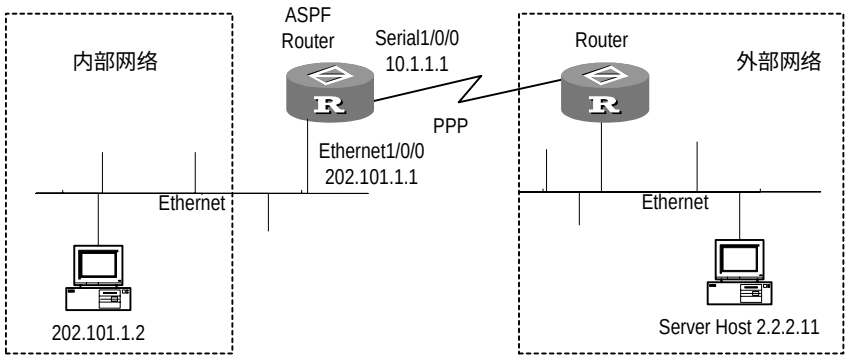

图4-4 ASPF 配置案例组网图

3. 配置步骤

在 ASPF 路由器上配置允许防火墙。

```
[Quidway] firewall enable
```

配置访问控制列表 3111，以拒绝所有 TCP 和 UDP 流量进入内部网络，ASPF 会为允许通过的流量创建临时的访问控制列表。

```
[Quidway] acl number 3111
[Quidway-acl-adv-3111] rule deny ip
```

创建 ASPF 策略，策略号为 1，该策略检测应用层的两个协议：FTP 和 HTTP 协议，并定义没有任何行为的情况下，这两个协议的超时时间为 3000 秒。

```
[Quidway] aspf-policy 1
[Quidway-aspf-policy-1] detect ftp aging-time 3000
[Quidway-aspf-policy-1] detect http aging-time 3000
[Quidway-aspf-policy-1] detect http java-blocking 2001
```

配置访问控制列表 2001，以过滤来自站点 2.2.2.11 的 Java Applets。

```
[Quidway] acl number 2001
[Quidway-acl-basic-2001] rule deny source 2.2.2.11 0
[Quidway-acl-basic-2001] rule permit
```

在接口上应用 ASPF 策略

```
[Quidway-Serial1/0/0] firewall aspf 1 outbound
```

在接口上应用访问控制列表 3111

```
[Quidway-Serial1/0/0] firewall packet-filter 3111 inbound
```

第5章 IPSec 配置

5.1 IPSec 概述

5.1.1 IPSec 协议简介

IPSec（IP Security）协议族是 IETF 制定的一系列协议，它为 IP 数据报提供了高质量的、可互操作的、基于密码学的安全性。特定的通信方之间在 IP 层通过加密与数据源验证等方式，来保证数据报在网络上传输时的私有性、完整性、真实性和防重放。

📖 说明：

私有性（Confidentiality）指对用户数据进行加密保护，用密文的形式传送。
完整性（Data integrity）指对接收的数据进行验证，以判定报文是否被篡改。
真实性（Data authentication）指验证数据源，以保证数据来自真实的发送者。
防重放（Anti-replay）指防止恶意用户通过重复发送捕获到的数据包所进行的攻击，即接收方会拒绝旧的或重复的数据包。

IPSec 通过 AH（Authentication Header，认证头）和 ESP（Encapsulating Security Payload，封装安全载荷）这两个安全协议来实现上述目标。并且还可以通过 IKE（Internet Key Exchange，因特网密钥交换协议）为 IPSec 提供了自动协商交换密钥、建立和维护安全联盟的服务，以简化 IPSec 的使用和管理。

- AH（Authentication Header）是报文头验证协议，主要提供的功能有数据源验证、数据完整性校验和防报文重放功能；然而，AH 并不加密所保护的数据报。
- ESP（Encapsulating Security Payload）是封装安全载荷协议，它除提供 AH 协议的所有功能之外（数据完整性校验不包括 IP 头），还可提供对 IP 报文的加密功能。

📖 说明：

AH 和 ESP 可以单独使用，也可以同时使用。对于 AH 和 ESP，都有两种操作模式：传输模式和隧道模式。工作模式将在后文介绍。

- IKE 用于协商 AH 和 ESP 所使用的密码算法，并将算法所需的必备密钥放到恰当位置。

📖 说明：

IKE 协商并不是必须的，IPSec 所使用的策略和算法等也可以手工协商。关于两种协商方式的比较，将在后文介绍。

5.1.2 IPSec 基本概念

1. 安全联盟

IPSec 在两个端点之间提供安全通信，端点被称为 IPSec 对等体。

IPSec 能够允许系统、网络的用户或管理员控制对等体间安全服务的粒度。例如，某个组织的安全策略可能规定来自特定子网的数据流应同时使用 AH 和 ESP 进行保护，并使用 3DES（Triple Data Encryption Standard，三重数据加密标准）进行加密；另一方面，策略可能规定来自另一个站点的数据流只使用 ESP 保护，并仅使用 DES 加密。通过 SA（Security Association，安全联盟），IPSec 能够对不同的数据流提供不同级别的安全保护。

安全联盟是 IPSec 的基础，也是 IPSec 的本质。SA 是通信对等体间对某些要素的约定，例如，使用哪种协议（AH、ESP 还是两者结合使用）、协议的操作模式（传输模式和隧道模式）、密码算法（DES 和 3DES）、特定流中保护数据的共享密钥以及密钥的生存周期等。

安全联盟是单向的，在两个对等体之间的双向通信，最少需要两个安全联盟来分别对两个方向的数据流进行安全保护。同时，如果希望同时使用 AH 和 ESP 来保护对等体间的数据流，则分别需要两个 SA，一个用于 AH，另一个用于 ESP。

安全联盟由一个三元组来唯一标识，这个三元组包括 SPI（Security Parameter Index，安全参数索引）、目的 IP 地址、安全协议号（AH 或 ESP）。SPI 是为唯一标识 SA 而生成的一个 32 比特的数值，它在 AH 和 ESP 头中传输。

安全联盟具有生存周期。生存周期的计算包括两种方式：

- 以时间为限制，每隔指定长度的时间就进行更新；
- 以流量为限制，每传输指定的数据量（字节）就进行更新。

2. IPSec 协议的操作模式

IPSec 协议有两种操作模式：传输模式和隧道模式。SA 中指定了协议的操作模式。

在传输模式下，AH 或 ESP 被插入到 IP 头之后但在所有传输层协议之前，或所有其他 IPSec 协议之前。在隧道模式下，AH 或 ESP 插在原始 IP 头之前，另外生成一个新头放到 AH 或 ESP 之前。不同安全协议在传输模式和隧道模式下的数据封装形式（传输协议以 TCP 为例）如下图所示：

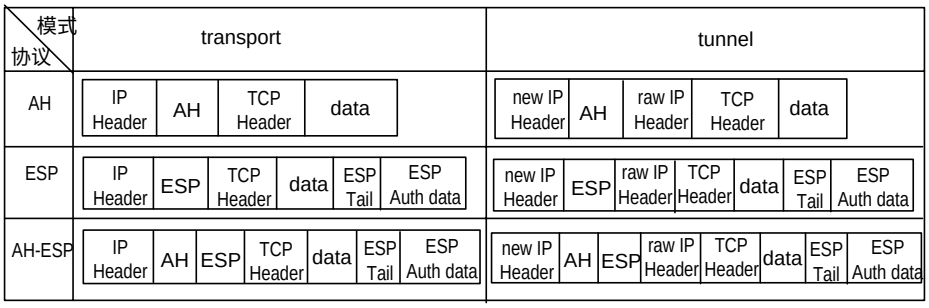

图5-1 安全协议数据封装格式

从安全性来讲，隧道模式优于传输模式。它可以完全地对原始 IP 数据报进行验证和加密；此外，可以使用 IPSec 对等体的 IP 地址来隐藏客户机的 IP 地址。从性能来讲，隧道模式比传输模式占用更多带宽，因为它有一个额外的 IP 头。因此，到底使用哪种模式需要在安全性和性能间进行权衡。

3. 验证算法与加密算法

(1) 验证算法

AH 和 ESP 都能够对 IP 报文的完整性进行验证，以判别报文在传输过程中是否被篡改。验证算法的实现主要是通过杂凑函数，杂凑函数是一种能够接受任意长的消息输入，并产生固定长度输出的算法，该输出称为消息摘要。IPSec 对等体计算摘要，如果两个摘要是相同的，则表示报文是完整未经篡改的。一般来说 IPSec 使用两种验证算法：

- MD5：MD5 通过输入任意长度的消息，产生 128bit 的消息摘要。
- SHA-1：SHA-1 通过输入长度小于 2 的 64 次方比特的消息，产生 160bit 的消息摘要。

SHA-1 的摘要长于 MD5，因而是更安全的。

(2) 加密算法

ESP 能够对 IP 报文内容进行加密保护，防止报文内容在传输过程中被窥探。加密算法实现主要通过对称密钥系统，它使用相同的密钥对数据进行加密和解密。VRP 中 IPSec 实现三种加密算法：

- DES（Data Encryption Standard）：使用 56bit 的密钥对一个 64bit 的明文块进行加密。
- 3DES（Triple DES）：使用三个 56bit 的 DES 密钥（共 168bit 密钥）对明文进行加密。
- AES（Advanced Encryption Standard）：VRP 实现了 128bit 密钥长度的 AES 算法，这也是 IETF 标准要求实现的。

4. 协商方式

有两种协商方式建立安全联盟，一种是手工方式（**manual**），一种是 IKE 自动协商（**isakmp**）方式。前者配置比较复杂，创建安全联盟所需的全部信息都必须手工配置，而且 IPSec 的一些高级特性（例如定时更新密钥）不被支持，但优点是可以不依赖 IKE 而单独实现 IPSec 功能。而后者则相对比较简单，只需要配置好 IKE 协商安全策略的信息，由 IKE 自动协商来创建和维护安全联盟。

当与之进行通信的对等体设备数量较少时，或是在小型静态环境中，手工配置安全联盟是可行的。对于中、大型的动态网络环境中，推荐使用 IKE 协商建立安全联盟。

5.1.3 加密卡简介

在实际应用中，IPSec 对报文的处理包括 ESP 协议处理和 AH 协议处理。为了确保信息的安全，加密/解密、认证的算法一般比较复杂，路由器 IPSec 软件进行加密/解密算法将占用大量的 CPU 资源，从而影响了路由器整体的处理效率。因此，对于模块化的路由器，可以使用加密卡（模块化硬件插卡），以硬件方式完成数据的 IPSec 运算，消除了 VRP 主体软件处理 IPSec 对整体性能的影响，提高了路由器的工作效率，同时也提高了 IPSec 的处理效率。

(1) 加密卡进行加/解密处理的过程是：路由器将需要加/解密处理的数据发给加密卡，加密卡对数据进行加/解密运算并给数据添加/删除加密帧头，然后加密卡将处理后的数据发送回路由器，再由路由器进行转发处理。

(2) 加密卡处理数据流：模块化路由器支持最多四块加密卡同时处理数据；主机软件将不同安全需求的数据分发给加密卡安全提议中指定的加密卡进行数据处理，同一块加密卡可以处理不同安全策略定义的数据流，但同一种数据流不能分发给多块加密卡来轮循处理。

(3) 在使用加密卡进行 IPSec 处理的过程中，若处理某特定数据流的加密卡状态异常时，加密卡将无法进行 IPSec 的处理。此时，若已经打开主机备份处理开关，并且 VRP 主体软件 IPSec 模块支持该加密卡使用的加密/认证算法，则 VRP 主体软件 IPSec 模块将代替加密卡对数据进行 IPSec 处理，从而实现了对加密卡的备份功能。但加密卡之间无法互做备份。

📖 说明：

加密卡与 VRP 主体软件 IPSec 模块对数据的处理机制完全相同，区别仅仅在于 VRP 主体软件是通过软件实现 IPSec 处理的，而加密卡是通过硬件实现 IPSec 处理的。

5.1.4 IPSec 在 VRP 上的实现

VRP 实现了上述所介绍的 IPSec 的全部内容。

其实现方式是基于下列思路：通过 IPSec，对等体之间（此处是指 VRP 所在路由器及其对端）能够对不同的数据流实施不同的安全保护（验证、加密或两者同时使用）。其中数据流的区分通过配置 ACL 来进行；安全保护所用到的安全协议、验证算法和加密算法、操作模式等通过配置安全提议来进行；数据流和安全提议的关联（即定义对何种数据流实施何种保护）、SA 的协商方式、对等体 IP 地址的设置（即保护路径的起/终点）、所需要的密钥和 SA 的生存周期等通过配置安全策略来进行；最后在路由器接口上实施安全策略即完成了 IPSec 的配置。

具体介绍如下：

(1) 定义被保护的数据流

数据流是一组流量（traffic）的集合，由源地址/掩码、目的地址/掩码、IP 报文承载的协议号、源端口号、目的端口号等来规定。一个数据流用一个 ACL 来定义，所有匹配一个访问控制列表规则的流量，在逻辑上作为一个数据流。一个数据流可以小到是两台主机之间单一的 TCP 连接，也可以大到是两个子网之间所有的流量。IPSec 能够对不同的数据流施加不同的安全保护，因此 IPSec 配置的第一步就是定义数据流。

(2) 定义安全提议

安全提议规定了对要保护的数据流所采用的安全协议、验证或加密算法、操作模式（即报文的封装方式）等。

VRP 支持的 AH 和 ESP 安全协议，两者既可单独使用，也可联合使用。其中，AH 支持 MD5 和 SHA-1 验证算法；ESP 协议支持 MD5、SHA-1 验证算法和 DES、3DES 加密算法。VRP 支持的操作模式包括传输模式和隧道模式。

对同一数据流，对等体两端必须设置相同的协议、算法和操作模式。另外，对于两个安全网关（例如 VRP 路由器间）实施 IPSec，建议采用隧道模式，以隐藏实际通信的源和目的 IP 地址。

因此，请先根据需要配置好一个安全提议，以便下一步将数据流和安全提议相关联。

(3) 定义安全策略或安全策略组

安全策略规定了对什么样的数据流采用什么样的安全提议。一条安全策略由“名字”和“顺序号”共同唯一确定。安全策略分为手工安全策略和 IKE 协商安全策略，前者需要用户手工配置密钥、SPI、SA 的生存周期等参数，在隧道模式下还需要手工配置安全隧道两个端点的 IP 地址；后者则由 IKE 自动协商生成这些参数。

安全策略组是所有具有相同名字、不同顺序号的安全策略的集合。在同一个安全策略组中，顺序号越小的安全策略，优先级越高。

(4) 接口实施安全策略

在接口上应用安全策略组，安全策略组中的所有安全策略同时应用在这个接口上，从而实现对流经这个接口的不同的数据流进行不同的安全保护。

5.2 IPSec 配置

1. IPSec 主要配置

(1) 配置访问控制列表

(2) 定义安全提议

- 创建安全提议（包括 IPSec 安全提议和加密卡安全提议两种类型）
- 指定加密卡安全提议使用的加密卡（仅用于加密卡）
- 选择安全协议
- 选择安全算法
- 选择报文封装形式

(3) 创建安全策略

包括手工创建安全策略和用 IKE 创建安全策略。

手工创建安全策略：

- 手工创建安全策略
- 在安全策略中引用安全提议
- 在安全策略中引用访问控制列表
- 配置隧道的起点和终点
- 配置安全联盟的 SPI
- 配置安全联盟使用的密钥

用 IKE 创建安全策略：

- 用 IKE 创建安全策略
- 在安全策略中引用安全提议
- 在安全策略中引用访问控制列表
- 在安全策略中引用 IKE 对等体
- 配置安全联盟生存周期（可选）
- 配置协商时使用的 PFS 特性

在安全策略中可以根据需要引用 IPSec 安全提议或加密卡安全提议。

(4) 配置安全策略模板（可选）

(5) 在接口上应用安全策略

(6) 配置取消对 next payload 域的检查（可选）

2. 加密卡配置（可选）

(1) 使能加密卡

(2) 使能 VRP 主体软件备份

(3) 配置加密卡快转功能

(4) 配置加密卡的简单网管操作

5.2.1 定义访问控制列表

用于 IPSec 的访问控制列表的作用不同于在防火墙中所介绍的访问控制列表。一般的访问控制列表是用来决定一个接口上哪些数据可通过，哪些要被拒绝；而 IPSec 是根据访问控制列表中的规则来确定哪些报文需要安全保护，哪些报文不需要安全保护，故用于 IPSec 的访问控制列表可称为加密访问控制列表。加密访问控制列表匹配（**permit**）的报文将被保护，加密访问控制列表拒绝（**deny**）的报文将不被保护。加密访问控制列表既可用于加密入口数据流，也可用于加密出口数据流。

具体配置请参见1.4.3 2. 访问控制列表。

在本地和远端路由器上定义的加密访问控制列表必须是相对应的（即互为镜像），这样在某一端加密的数据才能在对端上被解密。例如：

本端：

```
acl number 3101
rule 1 permit ip source 173.1.1.1 0.255.255.255 destination 173.2.2.2
0.255.255.255
```

对端：

```
acl number 3101
rule 1 permit ip source 173.2.2.2 0.255.255.255 destination 173.1.1.1
0.255.255.255
```

📖 说明：

- IPSec 对访问控制列表（ACL）中 **permit** 的数据流进行保护，因此建议用户精确地配置 ACL，只对确实需要 IPSec 保护的数据流配置 **permit**，避免盲目地使用关键字 **any**。
- 建议用户将本端和对端的 ACL 配置成互为镜像。
- VRP3.4 Release0010 之后的版本和 VRP1.7、VRP3.4 Release0010 之前的版本（含 Release0010）在实现 IPSec 时，对流的匹配方式不同：

VRP1.7 及 VRP3.4Release0010 之前的版本对每个 ACL 中的所有 rule 只建立一个 ipsec sa，每个流都在 ACL 中去匹配，不支持 display ipsec tunnel 命令。

VR3.4eleasexxx 之后的版本对每个 ACL 中的每个 rule 建立一个 ipsec sa 和 ipsec tunnel，每个流都会和 tunnel 中的流去匹配。

当这样的两个版本互通时，需要在两端路由器上都配置多个 ACL，每个 ACL 下仅配置一条 rule，否则会导致 IPSec SA 无法建立。

当用户使用 **display acl** 命令来浏览路由器的访问控制列表，所有扩展 IP 访问控制列表都将显示在命令的输出中，即同时包括了用于通信过滤和用于加密的扩展 IP 访问控制列表，该命令的输出信息不区分这两种不同用途的扩展访问控制列表。

5.2.2 定义安全提议

安全提议保存 IPSec 需要使用的特定安全性协议以及加密/验证算法，为 IPSec 协商安全联盟提供各种安全参数。为了能够成功的协商 IPSec 的安全联盟，两端必须使用相同的安全提议。

安全提议的配置包括：

- 定义安全提议
- 指定加密卡安全提议使用的加密卡（仅适用于加密卡）
- 选择安全协议
- 选择安全算法
- 设置安全协议对 IP 报文的封装模式

1. 创建安全提议

安全提议是用于实施 IPSec 保护而采用的安全协议、算法、报文封装形式的一个组合。一条安全策略通过引用一个或多个安全提议来确定采用的安全协议、算法和报文封装形式。在安全策略引用一个安全提议之前，这个安全提议必须已经建立。最多能够创建 50 个安全提议。

可对安全提议进行修改，但对已协商成功的安全联盟，新修改的安全提议并不起作用，即安全联盟仍然使用原来的安全提议（除非使用 **reset ipsec sa** 或 **reset encrypt-card sa** 命令重置），只有新协商的安全联盟将使用新的安全提议。

请在系统视图下进行下列配置。

表5-1 配置安全提议

操作	命令
创建安全提议并进入安全提议视图（适用于 VRP 主体软件 IPSec）	**ipsec proposal** *proposal-name*
删除安全提议（适用于 VRP 主体软件 IPSec）	**undo ipsec proposal** *proposal-name*
创建加密卡安全提议并进入加密卡安全提议视图（适用于加密卡）	**ipsec card-proposal** *proposal-name*
删除加密卡安全提议（适用于加密卡）	**undo ipsec card-proposal** *proposal-name*

缺省情况下，未配置加密卡安全提议。

2. 指定加密卡安全提议使用的加密卡（仅适用于加密卡）

当使用加密卡进行数据处理时，需要在加密卡安全提议模式下指定使用加密卡的槽位号。每一个模块化路由器最多可以支持四块加密卡。同一块加密卡可以在不同的加密卡安全提议中使用。

请在加密卡提议视图下进行下列配置。

表5-2 指定加密卡安全提议使用的加密卡的槽位

操作	命令
指定加密卡安全提议使用的加密卡	**use encrypt-card** [*slot-id*]
取消加密卡安全提议使用的加密卡	**undo use encrypt-card** [*slot-id*]

缺省情况下，加密卡安全提议没有使用任何加密卡。

3. 选择报文封装形式

在安全提议中需要指定报文封装模式，安全隧道的两端所选择的 IP 报文封装模式必须一致。

请在安全提议视图或加密卡安全提议视图下进行下列配置。

表5-3 选择报文封装形式

操作	命令
设置安全协议对 IP 报文的封装形式	**encapsulation-mode** { **transport**	**tunnel** }
恢复缺省报文封装形式	**undo encapsulation-mode**

通常，在两个安全网关（路由器）之间，总是使用隧道模式。而在两台主机之间的通讯，或者是一台主机和一个安全网关之间的通讯（例如网关工作站和一台路由器之间的网管通讯，此时安全网关相对于网关数据来说是接收主机）选择传输模式。

缺省情况下采用 **tunnel**，即隧道模式。

4. 选择安全协议

安全提议中需要选择所采用的安全协议。目前可选的安全协议有 AH 和 ESP，也可指定同时使用 AH 与 ESP。安全隧道两端所选择的安全协议必须一致。

请在安全提议或加密卡安全提议视图下进行下列配置。

表5-4 选择安全协议

操作	命令
设置安全提议采用的安全协议	**transform** { **ah**	**ah-esp**	**esp** }
恢复缺省的安全协议	**undo transform**

缺省情况下采用 **esp**，即 RFC2406 规定的 ESP 协议。

5. 选择安全算法

不同的安全协议可以采用不同的验证算法和加密算法。目前，AH 支持 MD5 和 SHA-1 验证算法；ESP 协议支持 MD5、SHA-1 验证算法和 DES、3DES、AES 加密算法。

请在安全提议或加密卡安全提议视图下进行下列配置。

表5-5 选择安全算法

操作	命令
设置 ESP 协议采用的加密算法	**esp encryption-algorithm** { **3des** | **des** | **aes** }
设置 ESP 协议不对报文进行加密	**undo esp encryption-algorithm**
设置 ESP 协议采用的验证算法	**esp authentication-algorithm** { **md5** | **sha1** }
设置 ESP 协议不对报文进行验证	**undo esp authentication-algorithm**
设置 AH 协议采用的验证算法	**ah authentication-algorithm** { **md5** | **sha1** }
恢复 AH 协议缺省的验证算法	**undo ah authentication-algorithm**

ESP 协议允许对报文同时进行加密和验证，或只加密，或只验证。注意，**undo esp authentication-algorithm** 命令不是恢复验证算法为缺省算法，而是设置验证算法为空，即不验证。当加密算法为空时，**undo esp authentication-algorithm** 命令失效。AH 协议没有加密的功能，只对报文进行验证。**undo ah authentication-algorithm** 命令用来恢复 AH 协议缺省验证算法（**md5**）。在安全隧道的两端设置的安全策略所引用的安全提议必须设置成采用同样的验证算法和/或加密算法。

VRP 主体软件及加密卡中 ESP 协议支持的安全加密算法有三种：**des、3des 和 aes**；支持的安全认证算法有 **hmac-md5** 和 **hmac-sha1**。

VRP 主机软件及加密卡中 AH 协议支持的认证算法有 **hmac-md5** 和 **hmac-sha1** 两种。

缺省情况下，ESP 协议采用的加密算法是 **des**，采用的验证算法是 **md5**；AH 协议采用的验证算法是 **md5**。

📖 说明：

必须首先通过 **transform** 命令选择了相应的安全协议后，该安全协议所需的安全算法才可配置。例如，如果使用 **transform** 命令选择了 **esp**，那么只有 ESP 所需的安全算法才可配置，而 AH 所需的安全算法则不能配置。

5.2.3 创建安全策略

安全策略规定了对什么样的数据流采用什么样的安全提议。安全策略分为手工安全策略和 IKE 协商安全策略，前者需要用户手工配置密钥、SPI 等参数，在隧道模式下还需要手工配置安全隧道两个端点的 IP 地址；后者则由 IKE 自动协商生成这些参数。

📖 说明：

本节将全面介绍安全策略的各项配置，包括手工协商方式所需的配置和 IKE 协商所需的配置。对于仅用于某种协商方式下的配置，会特别标明；没有特别标明的配置项，则表示手工方式和 IKE 协商方式下均需配置。

---

1. 手工创建安全策略

(1) 手工创建安全策略

一旦安全策略已经创建，就不能再修改它的协商方式。例如：创建了 **manual** 方式的安全策略，就不能修改成 **isakmp** 方式，而必须先删除这条安全策略然后再重新创建。

请在系统视图下进行下列配置。

表5-6 创建安全策略

操作	命令
用手工方式创建安全联盟的安全策略	**ipsec policy** *policy-name seq-number* **manual**
修改安全联盟的安全策略	**ipsec policy** *policy-name seq-number* **manual**
删除安全策略	**undo ipsec policy** *policy-name* [*seq-number*]

具有相同名字、不同顺序号的安全策略共同构造一个安全策略组，在一个安全策略组中最大可以设置 100 条安全策略。并且，所有安全策略的总数也不能超过 100。在一个安全策略组中，顺序号越小的安全策略，优先级越高。

缺省情况下没有安全策略存在。

(2) 配置在安全策略中引用安全提议

安全策略通过引用安全提议来确定采用的安全协议、算法和报文封装形式。在引用一个安全提议之前，这个安全提议必须已经建立。

请在安全策略视图下进行下列配置。

表5-7 在安全策略中应用安全提议

操作	命令
设置安全策略所引用的安全提议	**proposal** *proposal-name1* [*proposal-name2*... *proposal-name6*]
取消安全策略引用的安全提议	**undo proposal**

通过手工（**manual**）方式建立安全联盟，一条安全策略只能引用一个安全，并且如果已经设置了安全提议，必须先取消原先的安全提议才能设置新的安全提议。在安全隧道的两端设置的安全策略所引用的安全提议必须设置成采用同样的安全协议、算法和报文封装形式。

(3) 配置在安全策略引用的访问控制列表

安全策略引用访问控制列表，IPSec 根据该访问控制列表中的规则来确定哪些报文需要安全保护，哪些报文不需要安全保护：访问控制列表匹配（**permit**）的报文被保护，访问控制列表拒绝（**deny**）的报文不被保护。

请在安全策略视图下进行下列配置。

表5-8 设置安全策略引用的访问控制列表

操作	命令
设置安全策略引用的访问控制列表	**security acl** *acl-number*
取消安全策略引用的访问控制列表	**undo security acl**

一条安全策略只能引用一条访问控制列表，如果设置安全策略引用了多于一个访问控制列表，最后配置的那条访问控制列表才有效。

(4) 配置隧道的起点与终点

通常人们把应用安全策略的通道称为“ 安全隧道 ”。安全隧道是建立在本端和对端网关之间，所以必须正确设置本端地址和对端地址才能成功地建立起一条安全隧道。

请在安全策略视图下进行下列配置。

表5-9 配置隧道的起点与终点

操作	命令
设置安全策略的本端地址	**tunnel local** *ip-address*
删除在安全策略中设定的本端地址	**undo tunnel local** *ip-address*
设置安全策略的对端地址	**tunnel remote** *ip-address*
删除安全策略中设置的对端地址	**undo tunnel remote** *ip-address*

对于 **manual** 方式的安全策略，必须正确设置本端地址和对端地址才能成功地建立一条安全隧道，而 **isakmp** 方式的安全策略则不需要配置本端和对端地址，通过安全联盟自动协商可以获得。

(5) 配置安全联盟的 SPI

此配置任务仅用于 **manual** 方式的安全策略。用下列命令手工配置安全联盟的 SPI，实现手工创建安全联盟（对于 **isakmp** 方式的安全策略，不需要手工配置，IKE 将自动协商安全联盟的 SPI 并创建安全联盟）。

请在安全策略视图下进行下列配置。

表5-10 配置安全联盟的 SPI

操作	命令
配置安全联盟的 SPI	**sa spi** { **inbound** | **outbound** } { **ah** | **esp** } *spi-number*
删除安全联盟的 SPI	**undo sa spi** { **inbound** | **outbound** } { **ah** | **esp** }

在为系统配置安全联盟时，必须分别设置 **inbound** 和 **outbound** 两个方向安全联盟的参数。

在安全隧道的两端设置的安全联盟参数必须是完全匹配的。本端的入方向安全联盟的 SPI 必须和对端的出方向安全联盟的 SPI 一样；本端的出方向安全联盟的 SPI 必须和对端的入方向安全联盟的 SPI 一样。

(6) 配置安全联盟使用的密钥

此配置任务仅用于 **manual** 方式的安全策略，用如下命令手工输入安全联盟的密钥（对于采用 **isakmp** 协商方式的安全策略，无需手工配置密钥，IKE 将自动协商安全联盟的密钥）。

请在安全策略视图下进行下列配置。

表5-11 配置安全联盟使用的密钥

操作	命令
配置协议的验证密钥（以 16 进制方式输入）	**sa authentication-hex** { **inbound** | **outbound** } { **ah** | **esp** } *hex-key*
配置协议的验证密钥（以字符串方式输入）	**sa string-key** { **inbound** | **outbound** } { **ah** | **esp** } *string-key*
配置 ESP 协议的加密密钥（以 16 进制方式输入）	**sa encryption-hex** { **inbound** | **outbound** } **esp** *hex-key*
删除设置的安全联盟的参数	**undo string-key** { **inbound** | **outbound** } { **ah** | **esp** } **undo sa authentication-hex** { **inbound** | **outbound** } { **ah** | **esp** } **undo encryption-hex** { **inbound** | **outbound** } **esp**

在安全隧道的两端设置的安全联盟参数必须是完全匹配的。本端的入方向安全联盟的 SPI 及密钥必须和对端的出方向安全联盟的 SPI 及密钥一样；本端的出方向安全联盟的 SPI 及密钥必须和对端的入方向安全联盟的 SPI 及密钥一样。

如果分别以两种方式输入了密钥，则最后设定的密钥有效。在安全隧道的两端，应当以相同的方式输入密钥。如果一端以字符串方式输入密钥，另一端以 16 进制方式输入密钥，则不能正确地建立安全隧道。

2. 用 IKE 创建安全策略联盟

IKE 创建安全策略联盟的配置包括：

- 用 IKE 创建安全策略联盟
- 配置安全策略引用的访问控制列表
- 指定安全隧道的终点
- 配置安全策略中引用的安全提议
- 配置安全联盟的生存时间

(1) 用 IKE 创建安全策略

请在系统视图下进行下列配置。

表5-12 创建安全策略

操作	命令
用 IKE 创建安全策略，进入安全策略视图	**ipsec policy** *policy-name seq-number* **isakmp**
用 IKE 并采用策略模板动态创建安全策略	**ipsec policy** *policy-name seq-number* **isakmp** [**template** *template-name*]
修改通过 IKE 协商建立的安全策略	**ipsec policy** *policy-name seq-number* **isakmp**
删除安全策略	**undo ipsec policy** *policy-name* [*seq-number*]

若采用策略模板动态创建安全策略，则必须预先定义策略模板，策略模板的定义请参见5.2.4 配置安全策略模板。

(2) 配置在安全策略中引用安全提议

安全策略通过引用安全提议来确定采用的安全协议、算法和报文封装形式。在引用一个安全提议之前，这个安全提议必须已经建立。

请在安全策略视图下进行下列配置。

表5-13 在安全策略中应用安全提议

操作	命令
设置安全策略所引用的安全提议	**proposal** *proposal-name1* [*proposal-name2*... *proposal-name6*]
取消安全策略引用的安全提议	**undo proposal**

通过手工（**manual**）方式建立安全联盟，一条安全策略只能引用一个安全提议，并且如果已经设置了安全提议，必须先取消原先的安全提议才能设置新的安全提议。在安全隧道的两端设置的安全策略所引用的安全提议必须设置成采用同样的安全协议、算法和报文封装形式。

(3) 配置在安全策略引用的访问控制列表

安全策略引用访问控制列表，IPSec 根据该访问控制列表中的规则来确定哪些报文需要安全保护，哪些报文不需要安全保护：访问控制列表匹配（**permit**）的报文被保护，访问控制列表拒绝（**deny**）的报文不被保护。

请在安全策略视图下进行下列配置。

表5-14 设置安全策略引用的访问控制列表

操作	命令
设置安全策略引用的访问控制列表	**security acl** *acl-number*
取消安全策略引用的访问控制列表	**undo security acl**

一条安全策略只能引用一条访问控制列表，如果设置安全策略引用了多于一个访问控制列表，最后配置的那条访问控制列表才有效。

通过 IKE（**isakmp**）协商建立安全联盟，一条安全策略最多可以引用六个安全提议，IKE 协商将在安全隧道的两端搜索能够完全匹配的安全提议。如果 IKE 在两端找不到完全匹配的安全提议，则安全联盟不能建立，需要被保护的报文将被丢弃。

(4) 配置在安全策略中引用 IKE 对等体

对于 IKE 协商方式，无需象手工方式那样配置对等体、SPI 和密钥等参数，IKE 将自动协商这些它们，因而仅需要将安全策略和 IKE Peer 关联即可。

请在安全策略视图下进行下列配置。

表5-15 设置安全策略引用的访问控制列表

操作	命令
在安全策略中引用 ike 对等体。	**ike-peer** *peer-name*
取消在安全策略中引用 ike 对等体。	**undo ike-peer** *peer-name*

📖 说明：

本章仅介绍了 IPSec 对 IKE Peer 的引用，实际在 IKE Peer 视图下还需要进行一些 IKE 相关参数的设置，包括 IKE 的协商模式、ID 类型、NAT 穿越、共享密钥、对端地址和对端名称等。有关 IKE Peer 的配置，请参考下一章的内容。

(5) 配置安全联盟的生存周期（可选）

(a) 配置全局的安全联盟生存周期

所有在安全策略视图下没有单独配置生存周期的安全联盟，都采用全局生存周期。IKE 为 IPSec 协商建立安全联盟时，采用本地设置的和对端提议的生存周期中较小的一个。

有两种类型的生存周期：“ 基于时间 ”的生存周期和“ 基于流量 ”的生存周期。无论哪一种类型的生存周期先到期，安全联盟都会失效。安全联盟快要失效前，IKE 将为 IPSec 协商建立新的安全联盟，这样在旧的安全联盟失效时新的安全联盟就已经准备好。

请在系统视图下进行下列配置。

表5-16 配置全局的安全联盟生存周期

操作	命令
设置全局的安全联盟（SA）生存周期	**ipsec sa global-duration** { **traffic-based** *kilobytes* | **time-based** *seconds* }
恢复全局的安全联盟（SA）生存周期为缺省值	**undo ipsec sa global-duration** { **traffic-based** | **time-based** }

改变全局生存周期，不会影响单独配置了自己的生存周期的安全策略，也不会对已经建立的安全联盟产生影响，但是在以后的 IKE 协商中会用于建立新的安全联盟。

生存周期只对通过 **isakmp** 方式建立的安全联盟有效，对通过 **manual** 方式建立的安全联盟没有生存周期的限制，即手工建立的安全联盟永远不会失效。

(b) 配置安全联盟的生存周期

为安全策略设置单独的安全联盟生存周期，如果没有单独设置生存周期，则采用设定的全局生存周期。

IKE 为 IPSec 协商建立安全联盟时，采用本地设置的和对端提议的生存周期中较小的一个。

请在安全策略视图下进行下列配置。

表5-17 配置安全联盟生存周期

操作	命令
设置安全策略安全联盟的生存周期	**sa duration** { **traffic-based** *kilobytes* | **time-based** *seconds* }
恢复使用设定的全局生存周期	**undo sa duration** { **traffic-based** | **time-based** }

改变生存周期，不会影响已经建立的安全联盟，但是在以后的 IKE 协商中会用于建立新的安全联盟。

(6) 配置协商时使用的 PFS 特性（可选）

PFS（Perfect Forward Secrecy，完善的前向安全性）是一种安全特性，指一个密钥被破解，并不影响其他密钥的安全性，因为这些密钥间没有派生关系。此特性是通过在 IKE 阶段 2 的协商中增加密钥交换来实现的。

请在安全策略视图下进行下列配置。

表5-18 设置协商时使用的 PFS 特性

操作	命令
设置协商时使用的 PFS 特性	**pfs** { **dh-group1** | **dh-group2** }
设置在协商时不使用 PFS 特性	**undo pfs**

IKE 在使用此安全策略发起一个协商时，进行一个 PFS 交换。如果本端指定了 PFS，对端在发起协商时必须是 PFS 交换。本端和对端指定的 DH 组必须一致，否则协商会失败。

1024-bit Diffie-Hellman 组（**group2**）比 768-bit Diffie-Hellman 组（**group1**）提供更高的安全性，但是需要更长的计算时间。

缺省情况下没有 PFS 特性。

5.2.4 配置安全策略模板

在采用 IKE 方式创建安全策略时，除直接在安全策略视图下直接配置安全策略外，还可以通过引用安全策略模板来创建安全策略。在这种情况下，我们应先在安全策略模板中配置好所有的安全策略。

安全策略模板的配置与普通的安全策略配置相似，首先创建一个策略模板，然后配置模板的参数。

请在系统视图下进行下列配置。

表5-19 创建安全策略模板

操作	命令
创建/修改 IPsec 安全策略模板	**ipsec policy-template** *template-name seq-number*
删除安全策略模板	**undo ipsec policy-template** *policy-template-name* [*seq-number*]

执行上面的创建命令，会进入 IPsec 策略模板视图，在此视图下，可以配置策略模板的参数。

📖 说明：

安全策略模板可配置的参数与 isakmp 方式的 IPsec 安全策略相同，只是很多参数是可选的。必须配置的参数只有 IPsec 安全提议，而隧道对端地址、保护的数据流、PFS 特性可以不配置。但需要注意：如果配置了这些参数中的一个或几个，则在协商时这些参数必须匹配。

在策略模板配置完成后，还需要使用如下命令引用所定义的策略模板：

表5-20 引用安全策略模板

操作	命令
引用 IPsec 安全策略模板	**ipsec policy** *policy-name seq-number* **template** *template-name*

当某一个安全策略引用了安全策略模板后，就不能够再进入其安全策略视图下配置或修改安全策略了，只能进入安全策略模板视图下配置或修改。

注意：不能用应用策略模板的安全策略来发起安全联盟的协商，但可以响应协商。

5.2.5 在接口上应用安全策略组

为使定义的安全联盟生效，应在每个要加密的出站数据、解密的入站数据所在接口（逻辑的或物理的）上应用一个安全策略组，由这个接口根据所配置的安全策略组和对端加密路由器配合进行报文的加密处理。当安全策略组被从接口上删除后，此接口便不再具有 IPSec 的安全保护功能。

请在接口视图下进行下列配置。

表5-21 应用安全策略组

操作	命令
应用安全策略组	**ipsec policy** *policy-name*
取消应用的安全策略组	**undo ipsec policy**

一个接口只能应用一个安全策略组，一个安全策略组可以应用到多个接口上。但手工方式配置的安全策略只能应用到一个接口。

当从一个接口发送报文时，将按照从小到大的顺序号查找安全策略组中每一条安全策略。如果报文匹配了一条安全策略引用的访问控制列表，则使用这条安全策略对报文进行处理；如果报文没有匹配安全策略引用的访问控制列表，则继续查找下一条安全策略；如果报文对所有安全策略引用的访问控制列表都不匹配，则报文直接被发送（IPSec 不对报文加以保护）。

华为 3COM 公司实现的 IPSec 安全策略除了可以应用到串口、以太网口等实际物理接口上之外，还能够应用到 Tunnel、Virtual Template 等虚接口上。这样就可以根据实际组网要求，在如 GRE、L2TP 等隧道上应用 IPSec。

5.2.6 配置取消对 next payload 域的检查

next-payload 是指在 IKE 协商报文（由几个 payload 组装而成）的最后一个 payload 的通用头中 Next Payload 域。按协议规定该域必须为 0，但某些公司的设备会将该域赋其它值，为增强设备的互通性，可以通过 **ike next-payload check disabled** 命令取消 IPSec 协商过程对该域的检查。

表5-22 配置取消对 next payload 域的检查

操作	命令
配置在 IPSec 协商过程中取消对最后一个 payload 的 next payload 域的检查	**ike next-payload check disabled**
恢复缺省设置	**undo ike next-payload check disabled**

缺省情况下，检查 next payload 域。

5.2.7 加密卡可选配置

加密卡的主要配置与 IPSec 的配置过程相同，请参见本章的前面各节，以下为加密卡的可选配置，请根据需要进行选配。

1. 进入加密卡接口视图并且使能加密卡

当路由器上有多块加密卡在并行工作时，可以通过 **undo shutdown** 和 **shutdown** 命令灵活的管理各加密卡。根据应用的需要可以将该加密卡设置为不可用状态（禁止该加密卡进行数据处理）或可用状态，便于维护管理和调试。对处于 **shutdown** 状态下的加密卡执行 **undo shutdown** 命令将复位并初始化该加密卡。

可以通过 **interface encrypt** 命令进入相应槽位的加密卡，并且在加密卡视图下完成使能/禁止加密卡的操作。

请在系统视图下完成下面配置。

表5-23 进入加密卡接口视图

操作	命令
进入加密卡接口视图	**interface encrypt** [*slot-id*]

请在加密卡接口视图下进行下列配置。

表5-24 使能/禁止加密卡

操作	命令
使能加密卡	**undo shutdown**
禁用加密卡	**shutdown**

缺省情况下，使能所有加密卡。

2. 使能 VRP 主体软件备份

对于应用于加密卡侧的安全联盟，只要该加密卡工作状态正常，IPSec 处理就由状态正常的加密卡进行处理。当该加密卡状态异常时，则无法完成 IPSec 处理。此时如果已经开启主机备份处理开关，并且 VRP 主体软件 IPSec 模块支持该安全联盟所使用的加密/认证算法，则由 VRP 主体软件 IPSec 模块替代加密卡进行 IPSec 处理；若 VRP 主体软件 IPSec 模块不支持该安全联盟使用的算法，则报文被丢弃。

请在系统视图下进行下列配置。

表5-25 使能/禁用主机备份处理

操作	命令
使能主机备份处理	**encrypt-card backuped**
禁用主机备份处理	**undo encrypt-card backuped**

缺省情况下，禁用主机备份处理。

3. 配置加密卡快转功能

加密卡快转指的是对于[SourIP, SourPort, DestIP, DestPort, Prot] 五元组相同的一系列报文，路由器在接收或发送第一个报文时就会创建一个快转表项，之后符合此表项的所有报文都会直接被发往加密卡进行加密或解密，然后再由加密卡发往目的出口，这样省去了对每个报文逐一进行从 IP 到 IPSec 的处理，加速了处理过程。

请在系统视图下进行如下配置。

表5-26 配置加密卡快转功能

操作	命令
使能加密卡快转功能	**encrypt-card fast-switch**
关闭加密卡快转功能	**undo encrypt-card fast-switch**

缺省情况下，关闭加密卡快转功能。

4. 配置加密卡的简单网管操作

为了更加便于管理和维护，加密卡支持通过 SNMP 协议远程管理。通过与路由器的网管功能结合，可以在网管终端查询加密卡的状态并监控 TRAP 信息。其中可监控的 TRAP 信息包括加密卡的复位信息、状态变迁信息以及报文处理过程中的异常丢包信息等。

该命令在系统视图下进行如下配置。

表5-27 使能/关闭加密卡 trap 信息开关

操作	命令
使能加密卡 trap 信息开关	**snmp-agent trap enable encrypt-card**
关闭加密卡 trap 信息开关	**undo snmp-agent trap enable encrypt-card**

缺省情况下加密卡 trap 信息开关是关闭的。

5.3 IPSec 显示与调试

5.3.1 VRP 主体软件 IPSec 的显示与调试

1. IPSec 显示与调试

IPSec 提供以下命令显示安全联盟、安全联盟生存周期、安全提议、安全策略的信息以及 IPSec 处理的报文的统计信息。

display 命令可在所有视图下进行操作，**debugging** 命令只能在用户视图下操作。

表5-28 IPSec 显示与调试

操作	命令
显示安全联盟的相关信息	**display ipsec sa** [**brief** | **remote** *ip-address* | **policy** *policy-name* [*seq-number*] | **duration**]
显示 IPSec 处理报文的统计信息	**display ipsec statistics**
显示安全提议的信息	**display ipsec proposal** [*proposal-name*]
显示安全策略的信息	**display ipsec policy** [**brief** | **name** *policy-name* [*seq-number*]]

操作	命令
显示安全策略模板的信息	**display ipsec policy-template** [**brief** | **name** *policy-name* [*seq-number*]]
打开 IPSec 的调试功能	**debugging ipsec** { **sa** | **packet** [**policy** *policy-name* [*seq-number*] | **parameters** *ip-address protocol spi-number*] | **misc** }
禁止 IPSec 的调试功能	**undo debugging ipsec** { **sa** | **packet** [**policy** *policy-name* [*seq-number*] | **parameters** *ip-address protocol spi-number*] | **misc** }

2. 清除 IPSec 的报文统计信息

此配置任务清除 IPSec 的报文统计信息，所有的统计信息都被设置成零。

请在用户视图下进行下列操作。

表5-29 清除 IPSec 的报文统计信息

操作	命令
清除 IPSec 的报文统计信息	**reset ipsec statistics**

3. 删除安全联盟

此配置任务删除已经建立的安全联盟（无论是手工建立的还是通过 IKE 协商建立的）。如果未指定参数，则删除所有的安全联盟。

请在用户视图下进行下列操作。

表5-30 删除安全联盟

操作	命令
删除安全联盟	**reset ipsec sa** [**remote** *ip-address* | **policy** *policy-name* [*seq-number*] | **parameters** *dest-address protocol spi*]

对于通过 IKE 协商建立的安全联盟，被删除后如果有报文重新触发 IKE 协商，IKE 将重新协商建立安全联盟。

对于手工建立的安全联盟，被删除后系统会根据手工设置的参数立即创建新的安全联盟。

如果指定参数 **parameters**，由于安全联盟是成对出现的，删除了一个方向安全联盟，另一个方向安全联盟也随之被删除。

5.3.2 加密卡 IPSec 的显示与调试

1. 加密卡 IPSec 的显示与调试

加密卡可以提供下面的命令用来显示安全联盟信息、统计信息、系统日志、接口信息以及主机备份信息。

display 命令可在所用视图下操作，而 **debugging** 命令则只能在用户视图下操作。具体显示和调试命令如下表所示：

表5-31 加密卡的显示和调试命令

操作	命令
显示加密卡安全联盟的相关信息	**display encrypt-card sa** [*slot-id*]
显示加密卡处理报文的统计信息	**display encrypt-card statistics** [*slot-id*]
显示加密卡统计的系统日志信息	**display encrypt-card syslog** [*slot-id*]
显示加密卡的接口信息	**display interface encrypt** [*slot-id*]
显示加密卡的快转表项	**display encrypt-card fast-switch**
打开加密卡信息、报文、安全联盟、命令、错误及其它信息的调试开关	**debugging encrypt-card** {{**all** | **command** | **error** | **misc** | **packet** | **sa**} [*slot-id*]
禁止加密卡信息、报文、安全联盟、命令、错误及其它信息的调试开关	**undo debugging encrypt-card** {{**all** | **command** | **error** | **misc** | **packet** | **sa**} [*slot-id*]
打开加密卡侧 VRP 主体测试软件的调试开关	**debugging encrypt-card host** { **all** | **packet** | **sa** | **command** | **error** | **misc** } [*slot-id*]
禁止加密卡侧 VRP 主体测试软件的调试开关	**undo debugging encrypt-card host** { **all** | **packet** | **sa** | **command** | **error** | **misc** } [*slot-id*]

2. 清除加密卡的统计信息

此配置命令清除加密卡上的统计信息，如果不指定加密卡的槽位号，则清除路由器上所有加密卡的统计信息。

请在用户视图下进行下列配置。

表5-32 清除加密卡的统计信息

操作	命令
清除加密卡的统计信息	**reset counters interface encrypt** [*slot-id*]

3. 清除加密卡侧的安全联盟

此配置命令清除加密卡侧已配置的安全联盟（无论是手工创建的还是 IKE 协商创建的，如果不指定加密卡的槽位号，则清除路由器上所有加密卡的安全联盟。

请在用户视图下进行下列配置。

表5-33 清除加密卡侧的安全联盟

操作	命令
清除加密卡侧联盟	**reset encrypt-card sa** [*slot-id*]

4. 清除加密卡侧的报文统计信息

此命令用来清除加密卡侧所有的统计信息的计数器，其中包括数据包统计、字节数统计、丢包统计、认证失败统计、错误 SA 统计、非法加密卡安全提议统计、非法协议统计等信息。

请在用户视图下进行下面配置。

表5-34 清除加密卡报文统计信息

操作	命令
清除加密卡侧报文统计信息	**reset encrypt-card statistics** [*slot-id*]

5. 清除加密卡系统日志信息

此命令用来清除加密卡侧的日志统计信息。加密卡的日志中记录了到清除命令下发前对加密卡所做的关键操作的信息。

请在用户视图下进行下面配置。

表5-35 清除加密卡日志统计信息

操作	命令
清除加密卡侧日志信息	**reset encrypt-card syslog** [*slot-id*]

5.4 IPSec 典型配置案例

5.4.1 采用 manual 方式建立安全联盟的配置

1. 组网需求

在 Router A 和 Router B 之间建立一个安全隧道，对 PC A 代表的子网（10.1.1.x）与 PC B 代表的子网（10.1.2.x）之间的数据流进行安全保护。安全协议采用 ESP 协议，加密算法采用 DES，验证算法采用 SHA1-HMAC-96。

2. 组网图

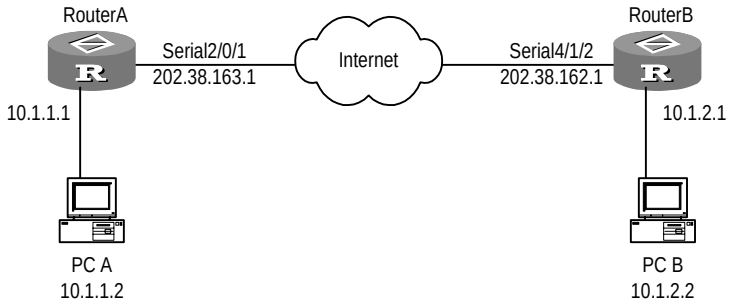

图5-2 IPSec 配置组网图

3. 配置步骤

(1) 配置 Router A

配置一个访问控制列表，定义由子网 10.1.1.x 去子网 10.1.2.x 的数据流。

```
[Quidway] acl number 3101
[Quidway-acl-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination
10.1.2.0 0.0.0.255
[Quidway-acl-adv-3101] rule deny ip source any destination any
```

配置到 PC B 的静态路由。

```
[Quidway] ip route-static 10.1.2.0 255.255.255.0 202.38.162.1
```

创建名为 tran1 的安全提议。

```
[Quidway] ipsec proposal tran1
```

报文封装形式采用隧道视图。

```
[Quidway-ipsec-proposal-tran1] encapsulation-mode tunnel
```

安全协议采用 ESP 协议。

```
[Quidway-ipsec-proposal-tran1] transform esp
```

选择算法。

```
[Quidway-ipsec-proposal-tran1] esp encryption-algorithm des
[Quidway-ipsec-proposal-tran1] esp authentication-algorithm sha1
```

退回到系统视图。

```
[Quidway-ipsec-proposal-tran1] quit
```

创建一条安全策略，协商方式为 manual。

```
[Quidway] ipsec policy map1 10 manual
```

引用访问控制列表。

```
[Quidway-ipsec-policy-manual-map1-10] security acl 3101
```

引用安全提议。

```
[Quidway-ipsec-policy-manual-map1-10] proposal tran1
```

设置对端地址。

```
[Quidway-ipsec-policy-manual-map1-10] tunnel remote 202.38.162.1
```

设置本端地址。

```
[Quidway-ipsec-policy-manual-map1-10] tunnel local 202.38.163.1
```

设置 SPI。

```
[Quidway-ipsec-policy-manual-map1-10] sa spi outbound esp 12345
[Quidway-ipsec-policy-manual-map1-10] sa spi inbound esp 54321
```

设置密钥。

```
[Quidway-ipsec-policy-manual-map1-10] sa string-key outbound esp abcdefg
[Quidway-ipsec-policy-manual-map1-10] sa string-key inbound esp gfedcba
```

退回到系统视图。

```
[Quidway-ipsec-policy-manual-map1-10] quit
```

进入串口配置视图。

```
[Quidway] interface serial 12/0/1
```

配置串口的 IP 地址。

```
[Quidway-Serial2/0/1] ip address 202.38.163.1 255.0.0.0
```

在串口上应用安全策略组。

```
[Quidway-Serial2/0/1] ipsec policy map1
```

(2) 配置 Router B

配置一个访问控制列表，定义由子网 10.1.2.x 去子网 10.1.1.x 的数据流。

```
[Quidway] acl number 3101
[Quidway-acl-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination
10.1.1.0 0.0.0.255
[Quidway] rule deny ip source any destination any
```

配置到 PC A 的静态路由。

```
[Quidway] ip route-static 10.1.1.0 255.255.255.0 202.38.163.1
```

创建名为 tran1 的安全提议。

```
[Quidway] ipsec proposal tran1
```

报文封装形式采用隧道模式。

```
[Quidway-ipsec-proposal-tran1] encapsulation-mode tunnel
```

安全协议采用 ESP 协议。

```
[Quidway-ipsec-proposal-tran1] transform esp
```

选择算法。

```
[Quidway-ipsec-proposal-tran1] esp encryption-algorithm des
[Quidway-ipsec-proposal-tran1] esp authentication-algorithm sha1
```

退回到系统视图。

```
[Quidway-ipsec-proposal-tran1] quit
```

创建一条安全策略，协商方式为 manual。

```
[Quidway] ipsec policy use1 10 manual
```

引用访问控制列表。

```
[Quidway-ipsec-policyl-manual-use1-10] security acl 3101
```

引用安全提议。

```
[Quidway-ipsec-policyl-manual-use1-10] proposal tran1
```

设置对端地址。

```
[Quidway-ipsec-policyl-manual-use1-10] tunnel remote 202.38.163.1
```

设置本端地址。

```
[Quidway-ipsec-policyl-manual-use1-10] tunnel local 202.38.162.1
```

设置 SPI 。

```
[Quidway-ipsec-policyl-manual-use1-10] sa spi outbound esp 54321
[Quidway-ipsec-policyl-manual-use1-10] sa spi inbound esp 12345
```

设置密钥。

```
[Quidway-ipsec-policyl-manual-use1-10] sa string-key outbound esp gfedcba
[Quidway-ipsec-policyl-manual-use1-10] sa string-key inbound esp abcdefg
```

退回到系统视图。

```
[Quidway-ipsec-policyl-manual-use1-10] quit
```

进入串口配置视图。

```
[Quidway] interface serial 4/1/2
```

配置串口的 IP 地址。

```
[Quidway-Serial4/1/2] ip address 202.38.162.1 255.0.0.0
```

在串口上应用安全策略组。

```
[Quidway-Serial4/1/2] ipsec policy use1
```

以上配置完成后，Router A 和 Router B 之间的安全隧道就建立好了，子网 10.1.1.x 与子网 10.1.2.x 之间的数据流将被加密传输。

5.4.2 采用 isakmp 方式建立安全联盟的配置

1. 组网需求

如上例图所示，在 Router A 和 Router B 之间建立一个安全隧道，对 PC A 代表的子网（10.1.1.x）与 PC B 代表的子网（10.1.2.x）之间的数据流进行安全保护。安全协议采用 ESP 协议，加密算法采用 DES，验证算法采用 SHA1-HMAC-96。

2. 组网图

见图 5-1。

3. 配置步骤

(1) 配置 Router A

配置一个访问控制列表，定义由子网 10.1.1.x 去子网 10.1.2.x 的数据流。

```
[Quidway] acl number 3101
[Quidway-acl-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[Quidway-acl-adv-3101] rule deny ip source any destination any
```

配置到 PC B 的静态路由。

```
[Quidway] ip route-static 10.1.2.0 255.255.255.0 202.38.162.1
```

创建名为 tran1 的安全提议。

```
[Quidway] ipsec proposal tran1
```

报文封装形式采用隧道模式。

```
[Quidway-ipsec-proposal-tran1] encapsulation-mode tunnel
```

安全协议采用 ESP 协议。

```
[Quidway-ipsec-proposal-tran1] transform esp
```

选择算法。

```
[Quidway-ipsec-proposal-tran1] esp encryption-algorithm des
[Quidway-ipsec-proposal-tran1] esp authentication-algorithm sha1
```

退回到系统视图。

```
[Quidway-ipsec-proposal-tran1] quit
```

配置 IKE 对等体。

```
[Quidway] ike peer peer
[Quidway-ike-peer-peer] pre-shared-key abcde
[Quidway-ike-peer-peer] remote- address 202.38.162.1
```

创建一条安全策略，协商方式为 isakmp。

```
[Quidway] ipsec policy map1 10 isakmp
```

引用安全提议。

```
[Quidway-ipsec-policy-isakmp-map1-10] proposal tran1
```

引用访问控制列表。

```
[Quidway-ipsec-policy-isakmp-map1-10] security acl 3101
```

引用 IKE 对等体。

```
[Quidway-ipsec-policy-isakmp-map1-10] ike-peer peer
```

退回到系统视图。

```
[Quidway-ipsec-policy-isakmp-map1-10] quit
```

进入串口配置视图。

```
[Quidway] interface serial 2/0/1
```

配置串口的 IP 地址。

```
[Quidway-Serial2/0/1] ip address 202.38.163.1 255.0.0.0
```

在串口上应用安全策略组。

```
[Quidway-Serial2/0/1] ipsec policy map1
```

退回到系统视图。

```
[Quidway-Serial2/0/1] quit
```

(2) 配置 Router B

配置一个访问控制列表，定义由子网 10.1.2.x 去子网 10.1.1.x 的数据流。

```
[Quidway] acl number 3101
[Quidway-acl-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination
10.1.1.0 0.0.0.255
[Quidway-acl-adv-3101] rule deny ip source any destination any
```

配置到 PC A 的静态路由。

```
[Quidway] ip route-static 10.1.1.0 255.255.255.0 202.38.163.1
```

创建名为 tran1 的安全提议。

```
[Quidway] ipsec proposal tran1
```

报文封装形式采用隧道模式。

```
[Quidway-ipsec-proposal-tran1] encapsulation-mode tunnel
```

安全协议采用 ESP 协议。

```
[Quidway-ipsec-proposal-tran1] transform esp
```

选择算法。

```
[Quidway-ipsec-proposal-tran1] esp encryption-algorithm des
[Quidway-ipsec-proposal-tran1] esp authentication-algorithm sha1
```

退回到系统视图。

```
[Quidway-ipsec-proposal-tran1] quit
```

配置 IKE 对等体。

```
[Quidway] ike peer peer
[Quidway-ike-peer-peer] pre-shared-key abcde
[Quidway-ike-peer-peer] remote-address 202.38.163.1
```

创建一条安全策略，协商方式为 isakmp。

```
[Quidway] ipsec policy use1 10 isakmp
```

引用访问控制列表。

```
[Quidway-ipsec-policy-isakmp-use1-10] security acl 3101
```

引用安全提议。

```
[Quidway-ipsec-policy-isakmp-use1-10] proposal tran1
```

引用 IKE 对等体。

```
[Quidway-ipsec-policy-isakmp-map1-10] ike-peer peer
```

退回到系统视图。

```
[Quidway-ipsec-policy-isakmp-use1-10] quit
```

进入串口配置视图。

```
[Quidway] interface serial 4/1/2
```

配置串口的 IP 地址。

```
[Quidway-Serial4/1/2] ip address 202.38.162.1 255.0.0.0
```

在串口上应用安全策略组。

```
[Quidway-Serial4/1/2] ipsec policy use1
```

退回到系统视图。

```
[Quidway-Serial4/1/2] quit
```

以上配置完成后，Router A 和 Router B 之间如果有子网 10.1.1.x 与子网 10.1.2.x 之间的报文通过，将触发 IKE 进行协商建立安全联盟。IKE 协商成功并创建了安全联盟后，子网 10.1.1.x 与子网 10.1.2.x 之间的数据流将被加密传输。

5.4.3 使用加密卡进行加/解密和认证

1. 组网需求

在路由器 A 和路由器 B 之间建立一个安全隧道对 PC A 代表的子网（10.1.1.0/24）与 PC B 代表的子网（10.1.2.0/24）之间的数据流进行安全保护。使用手工方式建立安全联盟，安全协议采用 ESP 协议，加密算法采用 DES，认证算法采用 sha1-hmac-96。

2. 组网图

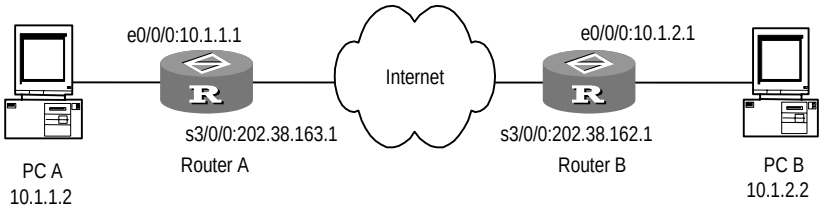

图5-3 使用加密卡建立安全隧道组网图

3. 配置步骤

(1) 配置 Router A

配置一个访问列表，定义由子网 10.1.1.0/24 去子网 10.1.2.0/24 的数据流。

```
[Router] acl 3001
[Router-acl-3001] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[Router-acl-3001] rule deny ip source any destination any
[Router-acl-3001] quit
```

创建名为 trans1 的加密卡安全提议

```
[Router] ipsec card-proposal tran1
```

指定 trans1 加密卡安全提议使用的加密卡槽位为 1/0/0

```
[Router-ipsec-card-proposal-tran1] use encrypt-card 1/0/0
```

报文封装形式采用隧道模式。

```
[Router-ipsec-card-proposal-tran1] encapsulation-mode tunnel
```

安全协议采用 ESP 协议。

```
[Router-ipsec-card-proposal-tran1] transform esp
```

选择算法。

```
[Router-ipsec-card-proposal-tran1] esp encryption-algorithm des
[Router-ipsec-card-proposal-tran1] esp authentication-algorithm sha1-hmac-96
```

退回到系统视图。

```
[Router-ipsec-card-proposal-tran1] quit
```

创建一条安全策略，协商方式为 manual。

```
[Router] ipsec policy policy1 10 manual
```

引用访问列表。

```
[Router-ipsec-policy-policy1-10] security acl 3001
```

设置对端地址。

```
[Router-ipsec-policy-policy1-10] tunnel remote 202.38.162.1
```

设置本端地址。

```
[Router-ipsec-policy-policy1-10] tunnel local 202.38.163.1
```

引用加密卡安全提议。

```
[Router-ipsec-policy-policy1-10] proposal tran1
```

设置 SPI。

```
[Router-ipsec-policy-policy1-10] sa outbound esp spi 12345
[Router-ipsec-policy-policy1-10] sa inbound esp spi 54321
```

设置密钥。

```
[Router-ipsec-policy-policy1-10] sa outbound esp string-key abcdefg
[Router-ipsec-policy-policy1-10] sa inbound esp string-key gfedcba
```

退回到系统视图。

```
[Router-ipsec-policy-policy1-10] quit
```

进入以太网口视图，配置 IP 地址。

```
[Router] interface Ethernet0/0/0
[Router-Ethernet0/0/0] ip address 10.1.1.1 255.255.255.0
```

进入串口视图，配置 IP 地址。

```
[Router-Ethernet0/0/0] interface serial 3/0/0
[Router-Serial3/0/0] ip address 202.38.163.1 255.255.255.0
```

在串口上应用安全策略组。

```
[Router-Serial3/0/0] ipsec policy policy1
[Router-Serial3/0/0] quit
```

配置去 10.1.2.0/24 网段的静态路由。

```
[Router] ip route-static 10.1.2.0 255.255.255.0 202.38.162.1
```

(2) 配置 Router B

配置一个访问列表，定义由子网 10.1.2.0/24 去子网 10.1.1.0/24 的数据流。

```
[Router] acl 3000
[Router-acl-3000] rule permit ip source 10.1.2.0 0.0.0.255 destination
10.1.1.0 0.0.0.255
[Router-acl-3000] rule deny ip source any destination any
[Router-acl-3000] quit
```

创建名为 tran1 的加密卡安全提议。

```
[Router] ipsec card-proposal tran1
```

指定 trans1 加密卡安全提议使用的加密卡的槽位号 1/0/0。

```
[Router-ipsec-card-proposal-tran1] use encrypt-card 1/0/0
```

报文封装形式采用隧道模式。

```
[Router-ipsec-card-proposal-tran1] encapsulation-mode tunnel
```

安全协议采用 ESP 协议。

```
[Router-ipsec-card-proposal-tran1] transform esp
```

选择算法。

```
[Router-ipsec-card-proposal-tran1] esp encryption-algorithm des
[Router-ipsec-card-proposal-tran1] esp authentication-algorithm
sha1-hmac-96
```

退回到系统视图。

```
[Router-ipsec-card-proposal-tran1] quit
```

创建一条安全策略，协商方式为 manual。

```
[Router] ipsec policy map1 10 manual
```

引用访问列表。

```
[Router-ipsec-policy-map1-10] security acl 3000
```

设置对端地址。

```
[Router-ipsec-policy-map1-10] tunnel remote 202.38.163.1
```

设置本端地址。

```
[Router-ipsec-policy-map1-10] tunnel local 202.38.162.1
```

引用加密卡安全提议。

```
[Router-ipsec-policy-map1-10] proposal tran1
```

设置 SPI。

```
[Router-ipsec-policy-map1-10] sa outbound esp spi 54321
[Router-ipsec-policy-map1-10] sa inbound esp spi 12345
```

设置密钥。

```
[Router-ipsec-policy-map1-10] sa outbound esp string-key gfedcba
[Router-ipsec-policy-map1-10] sa inbound esp string-key abcdefg
```

退回到系统视图。

```
[Router-ipsec-policy-map1-10] quit
```

进入以太网口视图，配置 IP 地址。

```
[Router] interface Ethernet0/0/0
[Router-Ethernet0/0/0] ip address 10.1.2.1 255.255.255.0
```

进入串口视图，配置 IP 地址。

```
[Router-Ethernet0/0/0] interface serial 3/0/0
[Router-Serial3/0/0] ip address 202.38.162.1 255.255.255.0
```

在串口上应用安全策略组。

```
[Router-Serial3/0/0] ipsec policy map1
[Router-Serial3/0/0] quit
```

#配置去 10.1.1.x 网段的静态路由。

```
[Router] ip route-static 10.1.1.0 255.255.255.0 202.38.163.1
```

第6章 IKE 配置

6.1 IKE 协议简介

6.1.1 IKE 协议概述

在实施 IPSec 的过程中，可以使用因特网密钥交换 IKE（Internet Key Exchange）协议来建立安全联盟，该协议建立在由 Internet 安全联盟和密钥管理协议 ISAKMP（Internet Security Association and Key Management Protocol）定义的框架上。IKE 为 IPSec 提供了自动协商交换密钥、建立安全联盟的服务，能够简化 IPSec 的使用和管理。

网络安全包括两层含义：其一是内部网的安全，其二是在公共网络中进行数据交换的安全。实现前者的手段有防火墙、地址转换（NAT）等。后者如正在兴起的 IPSec（IP Security），IPSec 提供了在 IP 层对报文实施加密的保护手段。IPSec 的安全联盟可以通过手工配置的方式建立，但是当网络中结点增多时，手工配置将非常困难，而且难以保证安全性。这时就要使用 IKE 自动地进行安全联盟建立与密钥交换的过程。

IKE 具有一套自保护机制，可以在不安全的网络上安全地分发密钥、验证身份、建立 IPSec 安全联盟。

IKE 的安全机制包括：

- DH（Diffie-Hellman）交换及密钥分发。Diffie-Hellman 算法是一种公共密钥算法。通信双方在不传送密钥的情况下通过交换一些数据，计算出共享的密钥。加密的前提是交换加密数据的双方必须要有共享的密钥。IKE 的精髓在于它永远不在不安全的网络上直接传送密钥，而是通过一系列数据的交换，最终计算出双方共享的密钥。即使第三者（如黑客）截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥。
- 完善的前向安全性（Perfect Forward Secrecy，PFS）。PFS 特性是一种安全特性，指一个密钥被破解，并不影响其他密钥的安全性，因为这些密钥间没有派生关系。对于 IPsec，是通过在 IKE 阶段 2 协商中增加一次密钥交换来实现的。
- 身份验证。身份验证确认通信双方的身份。对于 pre-shared key 验证方法，验证字用来作为一个输入产生密钥，验证字不同是不可能在双方产生相同的密钥的。验证字是验证双方身份的关键。
- 身份保护。身份数据在密钥产生之后加密传送，实现了对身份数据的保护。

IKE 使用了两个阶段为 IPSec 进行密钥协商并建立安全联盟：第一阶段，通信各方彼此间建立了一个已通过身份验证和安全保护的通道，此阶段的交换建立了一个 ISAKMP 安全联盟，即 ISAKMP SA；第二阶段，用在第一阶段建立的安全通道为 IPSec 协商安全服务，即为 IPSec 协商具体的安全联盟，建立 IPSec SA，IPSec SA 用于最终的 IP 数据安全传送。

从下图我们可以看出 IKE 和 IPSec 的关系。

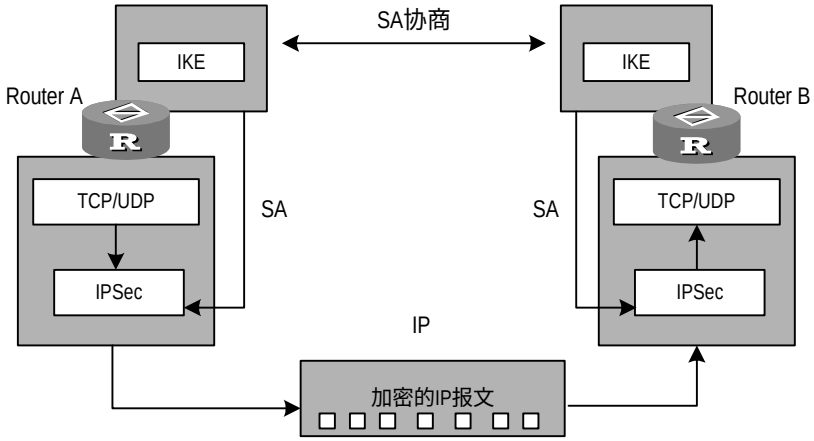

图6-1 IKE 和 IPSec 的关系图

另外，为了使 IKE 支持目前广泛应用的通过 ADSL 及拨号方式构建 VPN 的方案中的特殊情况——即局端设备的 IP 地址为固定分配的，用户端设备的 IP 地址为动态获取的情况，在 IKE 阶段的协商模式中增加了 IKE 野蛮模式，它可以选择根据协商发起端的 IP 地址或者 ID 来查找对应的身份验证字，并最终完成协商。IKE 野蛮模式相对于主模式来说更加灵活，能够支持协商发起端为动态 IP 地址的情况。

在 IPSec/IKE 组建的 VPN 隧道中，若存在 NAT 网关设备，且 NAT 网关设备对 VPN 业务数据流进行了 NAT 转换的话，则必须配置 IPSec/IKE 的 NAT 穿越功能。该功能删去了 IKE 协商过程中对 UDP 端口号的验证过程，同时实现了对 VPN 隧道中 NAT 网关设备的发现功能，即如果发现 NAT 网关设备，则将在之后的 IPSec 数据传输中使用 UDP 封装（即将 IPSec 报文封装到 IKE 协商所使用的 UDP 连接隧道里）的方法，避免了 NAT 网关对 IPSec 报文进行篡改（NAT 网关设备将只能够修改最外层的 IP 和 UDP 报文头，对 UDP 报文封装的 IPSec 报文将不作修改），从而保证了 IPSec 报文的完整性（IPSec 数据加密解密验证过程中要求报文原封不动地被传送到接收端）。

以上两个特性在 ADSL+IPSec 的组网方式中一般联合使用，解决了在企业网宽带接入方式下 IP 地址不固定、公网中需要穿越 NAT 等问题，为企业网以 ADSL 宽带接入替代原有的专线方式提供了安全的解决方案。

6.1.2 IKE 配置前准备工作

进行 IKE 配置之前，用户需要确定以下几个因素，以便配置过程的顺利进行：

- 确定 IKE 交换过程中算法的强度，即确定安全保护的强度（包括身份验证方法、加密算法、验证算法、DH 组）：不同的算法的强度不同，强度越高的算法，受保护数据越难被破解，但消耗的计算资源越多。一般来说，密钥越长的算法强度越高。
- 确定通信双方预先约定的身份验证字。

6.2 IKE 的配置

IKE 主要配置包括：

(1) 配置本端安全网关的名字

(2) 定义 IKE 安全提议

- 创建 IKE 安全提议
- 选择加密算法
- 选择验证方法
- 选择验证算法
- 选择 Diffie-Hellman 组标识
- 配置 ISAKMP SA 生存周期（可选）

(3) 配置 IKE 对等体

- 创建 IKE 对等体
- 配置 IKE 协商模式
- 配置身份验证字
- 配置本端安全网关 ID 的类型
- 配置 ike 协商过程中使用的
- 配置安全网关的 IP 地址
- 配置 NAT 穿越功能
- 配置 IKE 对等体的子网类型

(4) 配置 Keepalive 定时器参数

- 配置发送 Keepalive 报文的时间间隔
- 配置等待 Keepalive 报文的超时时间

这里的“安全网关”指配置了 IPSec/IKE 的设备（可以是网关或路由器）。

6.2.1 配置本端安全网关的名字

当 IKE 协商的发起端使用网关名字进行协商时（即配置了 **id-type name**），本端需要配置命令 **ike local**-name。

请在系统视图下进行下列配置。

表6-1 配置本端安全网关名字

操作	命令
配置本端安全网关的名字。	**ike local-name** *id*
恢复本端安全网关设备的缺省名字。	**undo ike local-name**

6.2.2 定义 IKE 安全提议

1. 创建 IKE 安全提议

IKE 提议定义了一套属性数据来描述 IKE 协商怎样进行安全通信。配置 IKE 提议包括创建 IKE 提议、选择加密算法、选择验证方法、选择验证算法、选择 Diffie-Hellman 组标识和设置安全联盟生存周期。

用户可以按照优先级创建多条 IKE 提议，但是协商双方必须至少有一条匹配的 IKE 提议才能协商成功。

此配置任务定义一个 IKE 提议。配置的 IKE 提议将被用来建立安全通道。

请在系统视图下进行下列配置。

表6-2 创建 IKE 提议

操作	命令
创建 IKE 安全提议	**ike proposal** *proposal-number*
删除 IKE 安全提议	**undo ike proposal** *proposal-number*

执行 **ike proposal** 命令会进入 IKE 提议视图。在 IKE 提议视图下可以配置加密算法、验证算法、组标识、生存周期和验证方法。

proposal-number 为 IKE 提议序号，取值为 1～100。该序号同时表示优先级，数值越小，优先级越高。可以为进行 IKE 协商的每一端配置多条提议，在协商时将从优先级最高的提议开始匹配一条双方都相同的提议，匹配的原则是：协商双方具有相同的加密算法、验证算法、验证方法和 DH 组标识。

系统提供一条缺省的 IKE 提议，具有最低的优先级，此缺省提议具有缺省的加密算法、验证算法、组标识、生存周期和验证方法。

IKE 提议需要定义的参数见下文。

2. 选择加密算法

此配置任务指定一个 IKE 提议使用的加密算法。

请在 IKE 提议视图下进行下列配置。

表6-3 选择加密算法

操作	命令
选择加密算法	**encryption-algorithm** { **des-cbc**| **3des-cbc** }
设置加密算法为缺省值	**undo encryption-algorithm**

缺省情况下使用 CBC 模式的 56-bit DES 加密算法。

3. 选择验证方法

当前 IKE 认证算法只有两种选择：预共享密钥（pre-shared-key）和 PKI（rsa-signature）方法。

请在 IKE 提议视图下进行下列配置。

表6-4 选择验证方法

操作	命令
选择验证方法	**authentication-method** { **pre-share**	**rsa-signature** }
设置验证方法为缺省值	**undo authentication-method**

📖 说明：

关于 PKI 的配置，请参考本手册中的“ PKI 配置 ”。

4. 选择验证算法

此配置任务指定一个 IKE 提议使用的验证算法。

请在 IKE 提议视图下进行下列配置。

表6-5 选择验证算法

操作	命令
选择验证算法	**authentication-algorithm** { **md5**	**sha** }
设置验证算法为缺省值	**undo authentication-algorithm**

缺省情况下使用 SHA-1 验证算法。

5. 选择 Diffie-Hellman 组标识

此配置任务指定一个 IKE 提议使用的 Diffie-Hellman 组标识。

请在 IKE 提议视图下进行下列配置。

表6-6 选择 DH 组标识

操作	命令
选择 Diffie-Hellman 组标识	**dh** { **group1** | **group2** }
设置 Diffie-Hellman 组标识为缺省值	**undo dh**

缺省情况下指定为 **group1**，即 768-bit 的 Diffie-Hellman 组。

6. 配置 ISAKMP SA 生存周期

此配置任务指定一个 IKE 提议使用的 ISAKMP SA 生存周期。

请在 IKE 提议视图下进行下列配置。

表6-7 设置 ISAKMP SA 生存周期

操作	命令
设置 ISAKMP SA 生存周期	**sa duration** *seconds*
设置生存周期为缺省值	**undo sa duration**

如果 **duration** 时间超时，ISAKMP SA 将自动更新。生存周期可以设定为 60 到 604800 秒之间的一个值。因为 IKE 协商需要进行 DH 计算，在低端路由器上需要经过较长的时间，为使 ISAKMP SA 的更新不影响安全通信，建议设置 **duration** 大于 10 分钟。

SA 在设定的生存周期超时前会提前协商另一个 SA 来替换旧的 SA。在新的 SA 还没有协商完之前，依然使用旧的 SA；在新的 SA 建立后，将立即使用新的 SA，而旧的 SA 在生存周期超时时被自动清除。

缺省情况下，ISAKMP SA 生存周期为 86400 秒（一天）。

6.2.3 配置 ike 对等体

1. 创建 IKE 对等体

请在系统视图下进行下列配置。

表6-8 配置 ike 对等体

操作	命令
配置一个 ike 对等体并进入 ike peer 视图。	**ike peer** *peer-name*
删除一个 ike 对等体。	**undo ike peer** *peer-name*

2. 配置 IKE 协商模式

请在 ike-peer 视图下进行下列配置。

表6-9 配置协商模式

操作	命令
配置 ike 阶段的协商模式。	**exchange-mode** [**aggressive** | **main**]
恢复 ike 阶段缺省的协商模式。	**undo exchange-mode**

缺省情况下使用主模式。

📖 说明：

当安全隧道一端的 IP 地址为动态获取时，必须将 IKE 阶段的协商模式配置为野蛮模式。

3. 配置身份验证字

请在 ike-peer 视图下进行下列配置。

表6-10 配置身份验证字

操作	命令
配置 ike 阶段协商所使用的身份验证字	**pre-shared-key** *key*
取消 ike 阶段协商所使用的身份验证字	**undo pre-shared-key**

4. 配置 ike 协商过程中使用的 ID 类型

请在 ike-peer 视图下进行下列配置。

表6-11 配置 ike 协商过程中使用的 ID 类型

操作	命令
选择 ike 阶段的协商过程中使用 ID 的类型。	**id-type** [**ip** | **name**]
恢复 ike 阶段的协商过程中使用的 ID 类型的缺省设置。	**undo id-type**

缺省情况下使用 ip 地址作为 ike 协商过程中使用的 ID 类型。

在主模式方式下只能使用 IP 地址作为 ike 协商过程中使用的 ID。在野蛮模式下，可以选择 IP 地址或者名字来作为 ike 协商过程中使用的 ID。

5. 指定对端安全网关设备的 ID

当 IKE 协商的发起端使用网关名字进行协商时（即配置了 **id-type name**），发起端会发送自己名字给对端来标识自己的身份，而对端使用 **remote-name** *name* 来验证发起端，故此时 *name* 应与发起端网关上使用 ike local-name 命令所配的名字保持一致。

请在 ike-peer 视图下进行下列配置。

表6-12 指定对端安全网关设备

操作	命令
指定一个对端安全网关设备。	**remote-name** *name*
删除对端安全网关设备。	**undo remote--name**

6. 配置本端及对端安全网关设备的 IP 地址

当 IKE 协商的发起端使用地址进行协商时（即配置了 **id-type ip**），发起端会发送自己的 IP 地址给对端来标识自己的身份，而对端使用 remote-address *ip-address* 来验证发起端，故此时 *ip-address* 应与发起端上 local-address 命令所配的 IP 地址保持一致。

请在 ike-peer 视图下进行下列配置。

表6-13 配置安全网关设备的 IP 地址

操作	命令
配置本端安全网关的 IP 地址。	**local-address** *ip-address*
删除本端安全网关的 IP 地址。	**undo local-address**
配置对端安全网关的 IP 地址。	**remote-address** *ip-address*
删除对端安全网关的 IP 地址。	**undo remote-address**

一般情况下命令 **local-address** 不需要配置，只有当用户需要指定特殊的本端网关地址时（如指定 loopback 接口地址）才需要配置这条命令。

7. 配置 NAT 穿越功能

在IPSec/IKE组建的VPN隧道中，若存在NAT安全网关设备，则必须配置IPSec/IKE的 NAT 穿越功能。

请在 ike-peer 视图下进行下列配置。

表6-14 配置 IKE/IPSec 的 NAT 穿越功能

操作	命令
配置 IKE/IPSec 的 NAT 穿越功能。	**nat-traversal**
取消 IKE/IPSec 的 NAT 穿越功能。	**undo nat-traversal**

为了节省 IP 地址空间，ISP 经常会在公网中加入 NAT 网关，以便于将私有 IP 地址分配给用户，此时可能会导致 IPSec/IKE 隧道的两端一端为公网地址，另一端为私网地址，所以必须在私网侧配置 NAT 穿越，保证隧道能够正常协商建立。

8. 配置子网类型

这两条命令仅在与 NETSCREEN 的设备互通时使用。

请在 ike-peer 视图下进行下列配置。

表6-15 配置 IKE 对等体的子网类型

操作	命令
配置本端网关的子网类型	**local** { **multi-subnet** | **single-subnet** }
恢复缺省的子网类型	**undo local**
配置对端网关的子网类型	**peer** { **multi-subnet** | **single-subnet** }
恢复缺省的子网类型	**undo peer**

缺省为 **single-subnet**。

9. 配置最大连接数

请在 ike-peer 视图下进行下列配置。

表6-16 配置最大连接数

操作	命令
配置最大连接数	**max-connections** *number*
恢复最大连接数的缺省值	**undo max-connections**

缺省情况下，最大连接数为 1。

6.2.4 配置 Keepalive 定时器

1. 配置发送 Keepalive 报文的时间间隔

配置通过 ISAKMP SA 向对端发送 Keepalive 报文的时间间隔。

请在系统视图下进行下列配置。

表6-17 设置发送 Keepalive 报文的时间间隔

操作	命令
设置 ISAKMP SA 向对端发送 Keepalive 报文的时间间隔	**ike sa keepalive-timer interval** *seconds*
设置使该功能失效	**undo ike sa keepalive-timer interval**

IKE 通过此报文维护该条 ISAKMP SA 的链路状态。一般在对端使用命令 **ike sa keepalive-timer timeout** 配置了超时时间时，必须在本端配置此 Keepalive 报文发送时间间隔。当对端在配置的超时时间内未收到此 Keepalive 报文时，如果该

ISAKMP SA带有TIMEOUT标记，则删除该ISAKMP SA以及由其协商的IPSec SA；否则，将其标记为 TIMEOUT。所以在配置时需使配置的超时时间比 Keepalive 报文发送时间长。

缺省情况下，此功能无效。

2. 配置等待 Keepalive 报文的超时时间

配置一个 ISAKMP SA 等待 Keepalive 报文的超时时间。

请在系统视图下进行下列配置。

表6-18 设置等待 Keepalive 报文的超时时间

操作	命令
设置 ISAKMP SA 等待 Keepalive 报文的超时时间	**ike sa keepalive-timer timeout** *seconds*
设置使该功能失效	**undo ike sa keepalive-timer timeout**

IKE 通过此报文维护该条 ISAKMP SA 的链路状态。如果在配置的超时时间内未收到对端的 Keepalive 报文，如果该 ISAKMP SA 带有 TIMEOUT 标记，则删除该 ISAKMP SA 以及由其协商的 IPSec SA；否则，将其标记为 TIMEOUT。所以在配置时需使配置的超时时间比 Keepalive 报文发送时间长。

在网络上一般不会出现超过连续三次的报文丢失，所以配置超时时间时可以采用对端配置的 Keepalive 报文发送时间间隔的三倍。

缺省情况下，此功能无效。

6.3 IKE 显示与调试

IKE 提供以下命令显示当前所有安全联盟的状态和每个 IKE 提议配置的参数。**display** 命令可在所有视图下进行下列操作，**debugging** 命令只能在用户视图下操作，**reset** 命令请在用户视图下进行操作。

表6-19 IKE 显示与调试

操作	命令
显示当前已建立的安全通道	**display ike sa**
显示每个 IKE 提议配置的参数	**display ike proposal**
显示 IKE 对等体的相关配置信息	**display ike peer**
删除安全隧道	**reset ike sa** [*connection-id*]
打开 IKE 的调试信息	**debugging ike** { **error** | **exchange** | **message** | **misc**| **transport** }

操作	命令
关闭 IKE 的调试信息	**undo debugging ike** { **error** | **exchange** | **message** | **misc**| **transport** }

在删除指定的安全通道时，需要指定 SA 的 *connection-id*，*通过命令* display ike sa 可以显示目前的安全联盟的 *connection-id* 信息。针对同一个安全通道（即相同的对端），分别有阶段 1 的信息和阶段 2 的信息。

删除本地的安全联盟时，如果阶段 1 的 ISAKMP SA 还存在，将在此安全联盟的保护下向对端发送删除消息，通知对方清除安全联盟数据库。

如果未指定 *connection-id*，所有的阶段 1 的 SA 都会被删除。

安全通道与安全联盟是完全不同的两个概念，安全通道是一个两端可以互通的通道，而 IPSec SA 则是一个单向的连接，所以安全通道是由一对或几对安全联盟组成的。

6.4 IKE 典型配置案例

6.4.1 IKE 典型配置组网应用

1. 组网需求

- 主机 1 与 2 之间进行安全通信，在安全网关 A 与 B 之间使用 IKE 自动协商建立安全通道。
- 在安全网关 A 上配置一条 IKE 提议，其优先级为 10，网关 B 使用缺省的 IKE 提议。
- 为使用 pre-shared key 验证方法的提议配置验证字。

2. 组网图

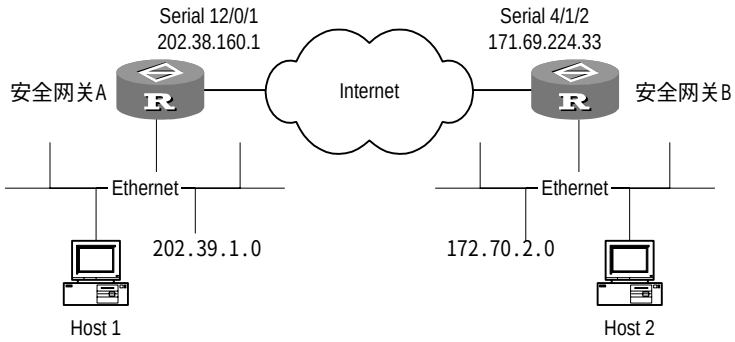

图6-2 IKE 配置举例组网图

3. 配置步骤

(1) 配置安全网关 A

配置 IKE 对等体。

```
[Quidway] ike peer peer
[Quidway-ike-peer-peer] pre-shared-key abcde
[Quidway-ike-peer-peer] remote-address 171.69.224.33
```

配置一条 IKE 提议 10。

```
[Quidway] ike proposal 10
```

指定 IKE 提议使用的验证算法为 MD5。

```
[Quidway-ike-proposal-10] authentication-algorithm md5
```

使用 pre-shared key 验证方法。

```
[Quidway-ike-proposal-10] authentication-method pre-share
```

设置 ISAKMP SA 生存周期 5000 秒。

```
[Quidway-ike-proposal-10] sa duration 5000
```

(2) 配置安全网关 B

配置 IKE 对等体。

```
[Quidway] ike peer peer
[Quidway-ike-peer-peer] pre-shared-key abcde
[Quidway-ike-peer-peer] remote address 202.38.160.1
```

以上配置可以保证网关 A 和 B 之间进行 IKE 协商。由于网关 A 配置的提议是 proposal 10，使用 authentication-algorithm md5，但网关 B 上只有一条缺省的 IKE 提议，默认是 authentication-algorithm sha。在进行提议匹配的时候，从优先级最高的提议开始，因为网关 B 上没有和网关 A 上提议 10 相匹配的提议，所以双方能够匹配的只有缺省的 IKE 提议。另外，在进行提议匹配的时候，duration 是不用进行匹配的，生存周期由 IKE 协商发起方决定。

关于 IPSec 的相应配置请参考 IPSec 配置举例。

6.4.2 IKE 野蛮模式及 NAT 穿越的组网应用

1. 组网需求

- 分公司 LAN 通过专线接入总公司内部网， RouterA 的 S0/0/0 口为固定 IP 地址，RouterB 动态获取 IP 地址。
- 分公司自动获得的 IP 地址为私有 IP 地址，RouterA 的 S0/0/0 口的 IP 地址也为私网地址，故 RouterA、RouterB 上需要配置 NAT 穿越功能。
- 为了保证信息安全采用 IPSec/IKE 方式创建安全隧道。

📖 说明：

为突出 IKE 野蛮模式及 NAT 穿越的配置，本例中的路由器采用串口通过 Internet 互联，并将一端配置为自动获取 IP 地址。实际应用中的拨号方式及宽带接入方式，均可以参考此例。

2. 组网图

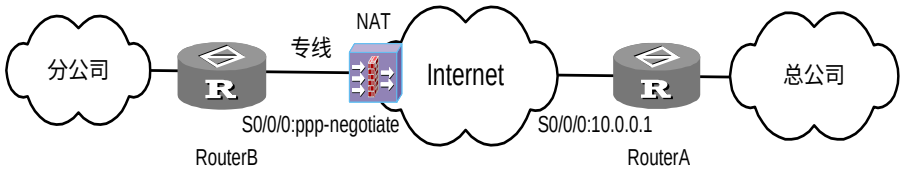

图6-3 IKE 野蛮模式及 NAT 穿越的典型配置案例

3. 配置步骤

(1) 配置 RouterA

配置本端安全网关设备的名字。

```
[RouterA] ike local-name routera
```

配置 acl。

```
[RouterA] acl number 3101 match-order auto
[RouterA -acl-adv-3101] rule permit ip source any destination any
```

配置地址池。

```
[RouterA] ip pool 1 10.0.0.2 10.0.0.10
```

配置 IKE 对等体 peer。

```
[RouterA] ike peer peer
[RouterA -ike-peer-peer] exchange-mode aggressive
[RouterA -ike-peer-peer] pre-shared-key abc
[RouterA -ike-peer-peer] id-type ip
[RouterA -ike-peer-peer] remote-name routerb
[RouterA -ike-peer-peer] nat traversal
```

创建 IPSec 安全提议 prop。

```
[RouterA] ipsec proposal prop
[RouterA-ipsec-proposal-prop] encapsulation-mode tunnel
[RouterA-ipsec-proposal-prop] transform esp
[RouterA-ipsec-proposal-prop] esp encryption-algorithm des
[RouterA-ipsec-proposal-prop] esp authentication-algorithm sha1
```

创建安全策略 policy 并指定通过 IKE 协商建立安全联盟。

```
[RouterA] ipsec policy policy 10 isakmp
```

配置安全策略 policy 引用 ike 对等体 peer。

```
[RouterA-ipsec-policy-isakmp-policy-10] ike-peer peer
```

配置安全策略 policy 引用访问控制列表 3101。

```
[RouterA-ipsec-policy-isakmp-policy-10] security acl 3101
```

配置安全策略 policy 引用 IPSec 安全提议 prop。

```
[RouterA-ipsec-policy-isakmp-policy-10] proposal prop
```

进入串口 S0/0/0 并配置 IP 地址。

```
[RouterA] interface Serial0/0/0
[RouterA -Serial0/0/0] ip address 10.0.0.1 255.255.0.0
```

配置串口 S0/0/0 引用安全策略组 policy。

```
[RouterA -Serial0/0/0] ipsec policy policy
[RouterA -Serial0/0/0] remote address pool 1
```

(2) 配置 RouterB

配置本端安全网关设备的名字。

```
[RouterB] ike local-name routerb
```

配置 acl。

```
[RouterB] acl number 3101 match-order auto
[RouterB -acl-adv-3101] rule permit ip source any destination any
```

配置 IKE 对等体 peer。

```
[RouterB] ike peer peer
[RouterB -ike-peer-peer] exchange-mode aggressive
[RouterB -ike-peer-peer] pre-shared-key abc
[RouterB -ike-peer-peer] id-type name
[RouterB -ike-peer-peer] remote-ip 10.0.0.1
[RouterB -ike-peer-peer] nat traversal
```

创建 IPSec 安全提议 prop。

```
[RouterB] ipsec proposal prop
[RouterB-ipsec-proposal-prop] encapsulation-mode tunnel
[RouterB-ipsec-proposal-prop] transform esp
[RouterB-ipsec-proposal-prop] esp encryption-algorithm des
[RouterB-ipsec-proposal-prop] esp authentication-algorithm sha1
```

创建安全策略 policy 并指定通过 IKE 协商建立安全联盟。

```
[RouterB] ipsec policy policy 10 isakmp
```

配置安全策略 policy 引用 ike 对等体 peer。

```
[RouterB-ipsec-policy-isakmp-policy-10] ike-peer peer
```

配置安全策略 policy 引用访问控制列表 3101。

```
[RouterB-ipsec-policy-isakmp-policy-10] security acl 3101
```

配置安全策略 policy 引用 IPSec 安全提议 prop。

```
[RouterB-ipsec-policy-isakmp-policy-10] proposal prop
```

进入串口 S0/0/0 并配置接口动态协商 IP 地址。

```
[RouterB] interface Serial0/0/0
[RouterB-Serial0/0/0] ip address ppp-negotiate
```

配置串口 S0/0/0 引用安全策略组 policy。

```
[RouterB-Serial0/0/0] ipsec policy policy
```

6.4.3 ADSL 与 IPSec/IKE 相结合的组网应用

1. 组网需求

本例将 IPSec 和 ADSL 相结合，是目前实际中广泛应用的典型案例。

- 分公司局域网内所有 PC 以 RouterB 的以太网口，RouterB 通过 ADSL 卡直接连接公网的 DSLAM 接入端，作为 PPPoEoA 的 client 端。总公司地址也为私网地址，RouterB 动态获得的 IP 地址也为私网地址，故 RouterA、RouterB 都需要配置 NAT 穿越。
- 总公司局域网通过 RouterA 接入到 ATM 网络，作为 PPPoEoA 的 Server 端，为分公司局域网内的主机分配 IP 地址。
- 为了保证信息安全采用 IPSec/IKE 方式创建安全隧道。

2. 组网图

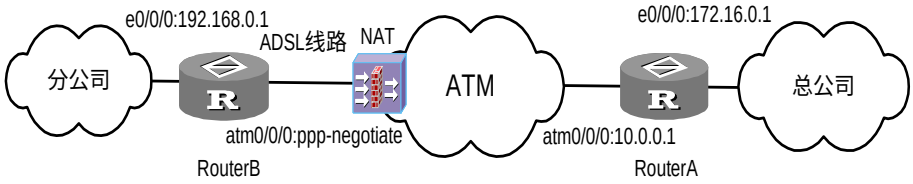

图6-4 ADSL 与 IPSec/IKE 相结合的组网应用

3. 配置步骤

(1) 配置 RouterA

在本地数据库中填加需验证的用户名及口令。

```
[RouterA] local-user test@adsl
[RouterA-luser-test@adsl] password simple 123456
```

配置 adsl 域用户。

```
[Quidway] domain adsl
[Quidway-isp-adsl] scheme local
[Quidway-isp-adsl] ip pool 80 192.168.38.66 192.168.38.78
```

配置本端安全网关设备名称。

```
[RouterA] ike local-name routera
```

配置 acl。

```
[RouterA] acl number 3101
[RouterA-acl-adv-3101] rule 0 permit ip source 172.16.0.0 0.0.255.255
destination 192.168.0.0 0.0.255.255
```

配置 IKE 对等体 peer。

```
[RouterA] ike peer peer
[RouterA-ike-peer-peer] exchange-mode aggressive
[RouterA-ike-peer-peer] pre-shared-key abc
[RouterA-ike-peer-peer] id-type ip
[RouterA-ike-peer-peer] remote-name routerb
[RouterA-ike-peer-peer] nat traversal
```

创建 IPSec 安全提议 prop。

```
[RouterA] ipsec proposal prop
[RouterA-ipsec-proposal-prop] encapsulation-mode tunnel
[RouterA-ipsec-proposal-prop] transform esp
[RouterA-ipsec-proposal-prop] esp encryption-algorithm des
[RouterA-ipsec-proposal-prop] esp authentication-algorithm sha1
```

创建安全策略 policy 并指定通过 IKE 协商建立安全联盟。

```
[RouterA] ipsec policy policy 10 isakmp
```

配置安全策略 policy 引用 ike 对等体 peer。

```
[RouterA-ipsec-policy-isakmp-policy-10] ike-peer peer
```

配置安全策略 policy 引用访问控制列表 3101。

```
[RouterA-ipsec-policy-isakmp-policy-10] security acl 3101
```

配置安全策略 policy 引用 IPSec 安全提议 prop。

```
[RouterA-ipsec-policy-isakmp-policy-10] proposal prop
```

创建 VT，设置验证方式为 CHAP 及 PAP，配置 IP 地址。

```
[RouterA] interface Virtual-Template0
[RouterA-Virtual-Template0] ppp authentication-mode chap domain adsl
[RouterA-Virtual-Template0] ppp authentication-mode pap
[RouterA-Virtual-Template0] ip address 10.0.0.1 255.255.0.0
[RouterA-Virtual-Template0] remote address pool 80
[RouterA-Virtual-Template0] ipsec policy policy
```

```
[RouterA-Virtual-Template0] remote address pool 80
```

设置 VE 口。

```
[RouterA] interface virtual-ethernet1/0/0
```

在 VE 接口上使能 PPPoE Server。

```
[RouterA-Virtual-Ethernet1/0/0] pppoe-server bind virtual-template 0
[RouterA-Virtual-Ethernet1/0/0] mac-address 0022-0022-00c1
```

对 ATM 口进行配置。

```
[RouterA] interface atm2/0/0
[RouterA-Atm1/0/0] pvc 0/32
[RouterA-atm-pvc-Atm1/0/0-0/32] map bridge vrtual-ethernet1/0/0
```

配置以太网口。

```
[RouterA-Ethernet0/0/0] ip address 172.16.0.1 255.255.0.0
```

配置到分公司局域网的静态路由。

```
[RouterA] ip route-static 192.168.0.0 255.255.0.0 10.0.0.1
```

(2) 配置 RouterB

配置本端安全网关的名称。

```
[RouterB] ike local-name routerb
```

配置拨号访问控制列表。

```
[RouterB] dialer-rule 1 ip permit
```

配置 acl。

```
[RouterB] acl number 3101
[RouterB-acl-adv-3101] rule 0 permit ip source 192.168.0.0 0.0.255.255
destination 172.16.0.0 0.0.255.255
```

配置 IKE 对等体 peer。

```
[RouterB] ike peer peer
[RouterB-ike-peer-peer] exchange-mode aggressive
[RouterB-ike-peer-peer] pre-shared-key abc
[RouterB-ike-peer-peer] id-type name
[RouterB-ike-peer-peer] remote-address 10.0.0.1
[RouterB-ike-peer-peer] nat traversal
```

创建 IPSec 安全提议 prop。

```
[RouterB] ipsec proposal prop
[RouterB-ipsec-proposal-prop] dh group2
[RouterB-ipsec-proposal-prop] esp encryption-algorithm 3des
```

创建安全策略 policy 并指定通过 IKE 协商建立安全联盟。

```
[RouterB] ipsec policy policy 10 isakmp
```

配置安全策略 policy 引用 ike 对等体 peer。

```
[RouterB-ipsec-policy-isakmp-policy-10] ike-peer peer
```

配置安全策略 policy 引用访问控制列表 3101。

```
[RouterB-ipsec-policy-isakmp-policy-10] security acl 3101
```

配置安全策略 policy 引用 IPSec 安全提议 prop。

```
[RouterB-ipsec-policy-isakmp-policy-10] proposal prop
```

配置拨号访问控制列表。

```
[RouterB] dialer-rule 1 ip permit
```

创建 Dialer0，进行拨号和 PPP 认证的相关配置，并配置 TCP 分片策略。

```
[RouterB] interface Dialer0
[RouterB-Dialer0] link-protocol ppp
[RouterB-Dialer0] ppp chap user test@adsl
[RouterB-Dialer0] ppp chap password simple 123456
[RouterB-Dialer0] ppp pap local-user test@adsl password simple 123456
[RouterB-Dialer0] ip address ppp-negotiate
[RouterB-Dialer0] dialer user quidway
[RouterB-Dialer0] dialer-group 1
[RouterB-Dialer0] dialer bundle 1
[RouterB-Dialer0] ipsec policy policy
[RouterB-Dialer0] tcp mss 1200
```

配置到 Dialer0 口的静态路由。

```
[RouterB] ip route-static 172.16.0.0 255.255.0.0 Dialer 0
```

配置以太网口。

```
[RouterB] interface Ethernet0/0/0
[RouterB-Ethernet0/0] mtu 1450
[RouterB-Ethernet0/0] ip address 192.168.0.1 255.255.0.0
```

创建 VE 接口。

```
[RouterB] interface Virtual-Ethernet0
```

对 adsl 卡的 atm 口进行配置。

```
[RouterB] interface Atm1/0/0
[RouterB -Atm1/0/0] pvc 0/100
[RouterB-Atm1/0/0] map bridge Virtual-Ethernet0
```

配置 VE 口。

```
[RouterB] interface virtual-ethernet2/0/0
[RouterB-Virtual-Ethernet2/0/0] pppoe-client dial-bundle-number 1
[RouterB-Virtual-Ethernet2/0/0] mac-address 0011-0022-0012
```

6.5 IKE 故障诊断与排错

配置参数建立 IPSec 安全通道时，可以打开 IKE 的 Error 调试开关，帮助我们查找配置问题。其命令是：

```
<Quidway> debugging ike error
```

故障之一：非法用户身份信息

故障排除：用户身份信息是发起 IPSec 通信的用户用来标识自己的数据。在实际应用中我们可以通过用户身份标识实现对不同的数据流建立不同的安全通道进行保护。目前我们是通过用户的 IP 地址来标识用户。

可以看到调试信息：

```
got NOTIFY of type INVALID_ID_INFORMATION
```

或者

```
drop message from A.B.C.D due to notification type INVALID_ID_INFORMATION
```

检查协商两端接口上配置的安全策略中的 ACL 内容是否相容。建议用户将两端的 ACL 配置成互为镜像的。ACL 镜像的含义请参考 IPSec 配置中“ 配置访问控制列表 ”内容。

故障之二：提议不匹配

故障排除：

可以看到调试信息：

```
got NOTIFY of type NO_PROPOSAL_CHOSEN
```

或者：

```
drop message from A.B.C.D due to notification type NO_PROPOSAL_CHOSEN
```

协商双方没有可以匹配的提议。对于阶段 1，检查 IKE proposal 是否有与对方匹配的。对于阶段 2 协商，检查双方接口上应用的 IPsec 安全策略的参数是否匹配，引用的 IPsec 安全提议的协议、加密算法和验证算法是否有匹配的。

故障之三：无法建立安全通道

故障排除：实际应用中有时会发现在不稳定的网络状态下，安全通道无法建立或者存在安全通道却无法通信，而且检查双方的 ACL 的配置正确，也有匹配的提议。

这种情况一般是安全通道建立好以后，有一方的路由器重启造成的。解决办法：

- 使用 **display ike sa** 命令检查双方是否都已建立阶段 1 的 SA。
- 使用 **display ipsec sa policy** 命令查看接口上的安全策略是否已建立了 IPSec SA。
- 根据以上两步的结果查看，如果有一方存在的 SA 在另一方不存在的情况，使用 **reset ike sa** 命令清除错误存在的 SA，重新发起协商。

第7章 PKI 配置

7.1 PKI 简介

7.1.1 概述

公钥基础设施（Public Key Infrastructure，简称 PKI）是通过使用公开密钥技术和数字证书来确保系统信息安全并负责验证数字证书持有者身份的一种体系，它是一套软硬件系统和安全策略的集合，提供了一整套安全机制。PKI 采用证书进行公钥管理，通过第三方的可信任机构，把用户的公钥和用户的其他标识信息捆绑在一起，以在网上验证用户的身份。PKI 为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便的使用加密和数字签名技术，从而保证网上数据的机密性、完整性、有效性。数据的机密性是指数据在传输过程中，不能被非授权者偷看；数据的完整性是指数据在传输过程中不能被非法篡改；数据的有效性是指数据不能被否认。

一个 PKI 系统由公开密钥密码技术、证书认证机构、注册机构、数字证书和相应的 PKI 存储库共同组成。

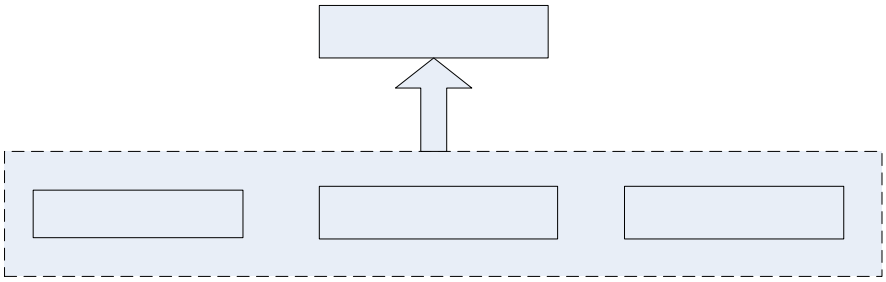

图7-1 PKI 组成框图

其中，认证机构用于签发并管理证书；注册机构用于个人身份审核、证书废除列表管理等；PKI 存储库用于对证书和日志等信息进行存储和管理，并提供一定的查询功能；数字证书是 PKI 应用信任的基础，是 PKI 系统的安全凭据。数字证书又称为公共密钥证书 PKC（Public Key Certificate），是基于公共密钥技术发展起来的一种主要用于验证的技术，它是一个经证书认证中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件，可作为各类实体在网上进行信息交流及商务活动的身份证明。证书是有生命期的，在证书生成时指定，认证中心也可以在证书的有效期到来前吊销证书，结束证书的生命期。

7.1.2 相关术语

- 公钥密码算法：是指加密密钥和解密密钥为两个不同密钥的密码算法，用户产生一对密钥：将其中的一个向外界公开，称为公钥；另一个则自己保留，称为私钥。密钥对中任一密钥加密的信息只能用另一密钥进行解密，因此它们常用于签名和加密。在通信过程中，发送方用自己的私钥对信息进行签名，接受方可以用发送方的公钥验证其签名；发送方也可以用接受方的公钥对信息进行加密，而也只有相应接受方的私钥能够对其解密。
- 认证机构（CA，Certificate Authority）：是一个向个人、计算机或任何其它实体颁发证书的可信实体。CA 受理证书申请，根据证书管理策略验证申请人的信息，然后用其私钥对证书进行签名，并颁发该证书。
- 注册机构（RA，Registration Authority）：RA 是 CA 的延伸，一方面向 CA 转发实体传输过来的证书申请请求，另一方面向目录服务器转发 CA 颁发的数字证书和证书撤消列表，以提供目录浏览和查询服务。
- 轻量级目录访问协议（LDAP，Light-weight Directory Access Protocol）服务器：LDAP 提供了一种访问 PKI 数据库（Repository）的方式，通过该协议来访问并管理 PKI 信息。LDAP 服务器提供目录浏览服务，负责将注册机构服务器传输过来的用户信息以及数字证书加入到 LDAP 服务器上。这样用户通过访问 LDAP 服务器就能够得到自己和其他用户的数字证书。
- 证书废除列表（CRL，Certificate Revocation Lists）：证书具有一定的寿命，另外由于泄露密钥、业务终止等原因，CA 也可通过称为证书吊销的过程来缩短这一寿命。一个证书一旦被撤消，证书中心就要公布 CRL 来声明该证书是无效的，并列出被认为不能再使用的证书的序列号。CRL 为应用程序和其它系统提供了一种检验证书有效性的方式，它们存储在数据库（LDAP 服务器）中，提供了一种通知用户和其他应用的中心管理方式。

7.1.3 主要应用

PKI 作为一组在分布式计算系统中利用公钥技术和 X.509 证书所提供的安全服务，可以为各种目的颁发证书，如 Web 用户身份验证、Web 服务器身份验证、使用安全/多用途 Internet 邮件扩充协议（S/MIME，Secure/Multipurpose Internet Mail Extensions）的安全电子邮件、虚拟专用网络（VPN，Virtual Private Network ）、IP 安全性(IP Security)、因特网密钥交换协议（IKE，Internet Key Exchange）、安全套接字协议层/事务层安全性（SSL/TLS，Secure Sockets Layer/Transaction Layer Security）和代码签名。证书还可以由一个 CA 颁发给另一个 CA，以建立证书层次结构。

7.1.4 配置任务列表

针对一个使用 PKI 的网络，配置 PKI 的目的就是为指定的设备向 CA 申请一个本地证书并进行证书的有效性验证。配置任务包括：

- PKI 证书申请配置
- PKI 证书验证配置
- 显示和调试配置

7.2 证书申请配置

7.2.1 证书申请概述

证书申请就是实体向 CA 自我介绍的过程，实体向 CA 提供身份信息，该信息随后将成为所颁发证书的一部分。CA 根据一套标准受理申请，对证书申请者的信用度、申请证书的目的、身份的真实可靠性等问题进行审查，确保证书与身份绑定的正确性。该标准可能要求进行脱机的、非自动的带外方式（如电话、磁盘、电子邮件等）身份验证。如果申请被成功受理，CA 随后将向该用户颁发证书，同时将用户的一些公开信息和证书放到 LDAP 服务器上提供目录浏览服务。用户随后可以到指定位置下载自己的公钥数字证书，也可以通过 LDAP 服务器获得其他用户的公钥数字证书。根据 PKI 证书管理策略，实现本地证书申请的配置任务包括：

- 进入 PKI 域视图
- 指定信任的 CA
- 配置证书申请的服务器
- 配置实体命名空间
- 创建本地公、私密钥对
- 配置查询证书申请处理状态的重发间隔和次数
- 配置证书申请模式
- 手工申请证书
- 证书获取

7.2.2 进入 PKI 域视图

PKI 域是将信任同一第三方可信任机构的一组 PKI 用户进行统一管理，即组内的每个成员只需同 CA 建立单一的信任关系即可，无需每位成员之间互相建立成对的信任关系，这样大大减轻了系统负荷，极大加强了 PKI 证书体系的扩展能力。

在配置域参数之前，必须首先进入 PKI 域视图。

请在系统视图下进行下列配置。

表7-1 进入 PKI 域视图

操作	命令
指定 PKI 域名并进入域视图	**pki domain** *name*
删除指定的 PKI 域及域内的所有配置信息	**undo pki domain** *name*

缺省情况下，未指定 PKI 域名。

📖 说明：

一个设备有可能从属于两个或多个 PKI 域，对于 PKI 应该能针对每一个域有其单独的配置信息，所以采用 PKI 域视图进行域参数的配置。但目前一个设备只支持一个 PKI 域，所以若在域已存在的情况下使用新域名，则需使用相应的 undo 命令删除旧域。

7.2.3 配置信任的 CA

在申请证书时，是通过为主体提供担保的另一个可信实体认证中心来完成注册颁发的。认证中心是公钥基础设施的核心，有了大家信任的认证中心，用户才能放心方便的使用公钥技术带来的安全服务。

请在 PKI 域视图下，进行下列配置。

表7-2 指定信任的 CA

操作	命令
指定本设备信任 CA 的名称	**ca identifier** *name*
删除本设备信任 CA 的名称	**undo ca identifier**

缺省情况下，未指定本设备信任的 CA。

📖 说明：

CA 在受理证书请求（以及颁发证书、吊销证书和发布 CRL）时所采用的一套标准被称为 CA 策略。通常，CA 以一种叫做证书惯例声明（CPS，Certification Practice Statement）的文档发布其策略，CA 策略可以通过带外或其他方式获取。由于不同的 CA 使用不同的方法验证公钥与主体之间的绑定，所以在选择信任的 CA 进行证书申请之前，理解其策略是非常重要的。

CA 标识只是在获取 CA 证书时使用，申请本地证书时不会用到。

7.2.4 配置申请证书的服务器

1. 配置证书申请的注册受理机构

注册管理一般由一个独立的注册机构（即 RA）来承担，它接受用户的注册申请，审查用户的申请资格，并决定是否同意 CA 给其签发数字证书。注册机构并不给用户签发证书，而只是对用户进行资格审查。有时 PKI 把注册管理的职能交给 CA 来完成，而不设立独立运行的 RA，但这并不是取消了 PKI 的注册功能，而只是将其作为 CA 的一项功能而已。

请在 PKI 域视图下，进行下列配置。

表7-3 选择证书申请注册机构

操作	命令
指定证书注册申请的受理机构	**certificate request from** { **ca** | **ra** } **entity** *entity-name*
删除证书注册申请的受理机构	**undo certificate request from** { **ca** | **ra** }

缺省情况下，未指定证书注册申请的受理机构。

PKI 安全策略推荐使用 RA 作为注册审理机构。

📖 说明：

实体 *entity-name* 的相关信息，请参阅7.2.5 实体命名空间部分。

2. 配置申请证书的服务器位置

证书申请之前必须指定注册服务器位置 URL，随后实体可通过简单证书注册协议（SCEP，Simple Certification Enrollment Protocal）向该服务器提出证书申请，SCEP 是专门用于与认证权威机构进行通信的协议。

请在 PKI 域视图下，进行下列配置。

表7-4 指定申请证书的服务器位置

操作	命令
设置证书申请注册机构的位置	**certificate request url** *string*
删除证书申请注册机构的位置	**undo certificate request url**

缺省情况下，未指定证书申请机构的服务器位置。

3. 配置 LDAP 服务器地址

在 PKI 系统中，用户的证书和 CRL 信息的存储是一个非常核心的问题。一般采用 LDAP 目录服务器，用来分发证书和 CRL。

请在 PKI 域视图下，进行下列配置。

表7-5 指定 LDAP 服务器地址

操作	命令
指定 LDAP 服务器 IP 地址	**ldap server ip** *ip-address* [**port** *port-num*] [**version** *version-number*]
删除 LDAP 服务器 IP 地址	**undo ldap server ip**

缺省情况下，未指定 LDAP 服务器地址及端口，LDAP 版本为 2。

7.2.5 配置实体命名空间

1. 命名空间概述

在构建 PKI 时，要考虑的一个重要的问题便是实体的命名空间（Name Space）。在一份证书中，必须证明公钥及其所有者的姓名是一致的，每个 CA 都要用它认为重要的信息对一个实体进行细致的描述。这里可以通过唯一的标识符（或称 DN-distinguished name）来唯一确定单个主体，它由许多部分组成，如用户通用名、组织单位、国家或者证书持有人的姓名等信息。DN 在网络上应该是唯一的。

本章介绍了进入 PKI 实体视图后如何对实体的 DN 相关信息进行配置，内容包括:

- 定义 PKI 实体名称
- 配置实体 FQDN
- 配置实体所属国家
- 配置实体所属州省
- 配置实体所在地理区域
- 配置实体所属组织名称
- 配置实体所属组织部门
- 配置实体通用名
- 配置实体 IP 地址

📖 说明：

实体的配置信息必须与 CA 证书颁发策略相匹配，以确认实体 DN 配置任务，如哪些实体参数必须配置，哪些可选配，否则证书申请可能会失败。

---

2. 定义 PKI 实体名称

PKI 实体视图提供了配置实体 DN 各项属性的平台。

请在系统视图下进行下列配置。

表7-6 配置实体名称

操作	命令
配置实体名称，并进入该实体视图	**pki entity** *name-str*
删除此实体名称及该实体参数	**undo pki entity** *name-str*

缺省情况下，未指定实体名称。

📖 说明：

实体名称必须与注册受理机构配置 **certificate request from** { **ca** | **ra** } **entity** *entity-name* 中指定的 *entity-name* 一致，否则该实体的证书申请会失败。*name-str* 只是用来方便引用，不用于证书的任何字段。

3. 配置实体的 FQDN 名称

FQDN（Fully Qualified Domain Name）是实体在网络中的唯一标识，如 Email 地址，一般形式为：user.domain，可被解析为 IP 地址。FQDN 与指定实体 IP 地址的功能相同，可选配。

请在 PKI 实体视图下进行下列配置。

表7-7 实体 FQDN 配置

操作	命令
配置实体 FQDN 名称	**fqdn** *name-str*
删除此实体 FQDN 名称	**undo fqdn**

缺省情况下，未指定实体 FQDN。

4. 配置实体所属国家

请在 PKI 实体视图下进行下列配置。

表7-8 实体所属国家配置

操作	命令
配置实体所属国家代码	**country** *country-code-str*
删除此实体所属国家代码	**undo country**

缺省情况下，未指定实体所属国家。

📖 说明：

代码用标准的 2 字符代码。例如：CN 是中国的合法国家代码，US 是美国的合法国家代码。

5. 配置实体所属州省

在 PKI 实体视图下进行下列配置。

表7-9 实体所属州省配置

操作	命令
配置实体所属州省	**state** *state-str*
删除此实体所属州省	**undo state**

缺省情况下，未指定实体所属州省。

6. 配置实体所在地理区域

在 PKI 实体视图下进行下列配置。

表7-10 实体所在地理区域配置

操作	命令
配置实体所在地理区域	**locality** *locality-str*
删除此实体所在地理区域	**undo locality**

缺省情况下，未指定实体所在地理区域。

7. 配置实体所属组织名称

在 PKI 实体视图下进行下列配置。

表7-11 实体所属组织配置

操作	命令
配置实体所属组织名称	**organization** *org-str*
删除此实体所属组织名称	**undo organization**

缺省情况下，未指定实体所属组织。

8. 配置实体所属组织部门

可以使用这个可选择的字段在同一个单位内区分不同的部门。

请在 PKI 实体视图下进行下列配置。

表7-12 实体所属部门配置

操作	命令
配置实体所属组织部门	**organizational-unit** *org-unit-str*
删除此实体所属组织部门	**undo organizational-unit**

缺省情况下，未指定实体所属部门。

9. 配置实体的通用名

请在 PKI 实体视图下进行下列配置。

表7-13 实体通用名配置

操作	命令
配置实体通用名	**common-name** *name-str*
删除此实体通用名	**undo common-name**

缺省情况下，未指定实体的通用名。

10. 配置实体的 IP 地址

与指定实体 FQDN 的功能相同，可选配。

请在 PKI 实体视图下进行下列配置。

表7-14 实体 IP 地址配置

操作	命令
配置实体 IP 地址	**ip** *ip-address*
删除此实体 IP 地址	**undo ip**

缺省情况下，未指定实体 IP 地址。

7.2.6 创建公、私密钥对

密钥对的产生是证书申请过程中重要的一步，它使用了一对密钥：私钥和公钥。私钥由用户保留；公钥和其他信息则交于 CA 中心进行签名，从而产生证书。另外，每一个由 CA 颁发的证书都会有有效期，证书生命周期的长短由签发证书的 CA 中心来确定。当用户的私钥被泄漏或证书的有效期快到时，用户应该删除旧的密钥对，产生新的密钥对，重新申请新的证书。

该配置任务用来产生本地密钥对。如果此时已经有了 RSA 密钥，系统提示是否替换原有密钥。产生的密钥对的命名方式为：路由器名称+host。主机密钥的最小长度为 512 位，最大长度为 2048 位。

请在系统视图下进行下列配置。

表7-15 创建和销毁本地 RSA 密钥对

操作	命令
创建本地 RSA 密钥对	**rsa local-key-pair create**
销毁本地 RSA 密钥对	**rsa local-key-pair destroy**

缺省情况下，本地没有 RSA 密钥对，需要用户创建。

⚠ 注意：

- 当本地证书已存在时，为保证密钥对与现存证书的一致性，不应执行创建密钥对命令，必须删除本地证书后方可执行该命令生成新的密钥对。
- 若本地已有 RSA 密钥对，则创建的新密钥对将覆盖掉旧密钥对。
- 这两个密钥对本来是提供给 SSH 使用，其中本地服务器密钥对周期性由本地服务器改变；主机密钥对不变。申请证书时我们使用的是主机密钥对。

7.2.7 配置查询证书申请处理状态的重发间隔和次数

实体在发送证书申请后，如果 CA 采用手工验证申请，会需要很长时间才能发布证书，在此期间，客户端需要定期发送状态查询，以便在证书签发后能及时获取到证书。

请在 PKI 域视图下，进行下列配置。

表7-16 配置证书申请状态查询的重发间隔和次数

操作	命令
配置证书申请状态查询重发间隔和次数	**certificate request polling** {**interval** *minutes* | **count** *count* }
恢复证书申请状态查询重发间隔和次数为缺省值	**undo certificate request polling** {**interval** | **count** }

缺省情况下，证书申请状态查询重发次数为 50，间隔为 20 分钟。

7.2.8 配置证书申请模式

证书申请有手工发起和自动发起方式。如果是自动方式，则在本地没有自己的证书时自动通过 SCEP 协议进行申请，而且在证书快要过期时自动申请新的证书。如果为手工方式，则需要手工完成各项证书申请工作。

请在 PKI 域视图下，进行下列配置。

表7-17 证书申请模式

操作	命令
配置证书获取方式	**certificate request mode** { **manual** | **auto** }
恢复证书获取方式为缺省值	**undo certificate request mode**

缺省情况下，证书申请为手工方式。

7.2.9 手工申请证书

完整的证书请求由用户公钥和相关登记信息构成，在完成以上配置后，即可向 PKI 注册认证机构发起申请本地证书请求。

请在任意视图下进行下列操作。

表7-18 证书申请操作

操作	命令
证书申请操作	**pki request certificate** *domain-name* [*password*] [**pem**]

⚠ 注意：

- 如果本地证书已存在，不允许再执行证书申请操作，避免因相关配置的修改使得证书与登记信息不匹配。若想重新申请，请先使用 **pki delete certificate** 命令删除存储于本地的 CA 证书与本地证书，然后再执行此申请命令。
- 当出现无法通过 SCEP 协议向 CA 申请证书的异常情况时，可以使用可选参数 pem 打印出本地的证书请求信息，用户保存该信息，并将该信息通过带外方式发送给 CA 进行证书请求。
- 证书申请之前必须保证实体的时钟必须与 CA 同步，否则申请的证书的有效期会出现异常。
- 该操作不被保存在配置中。

7.2.10 手工获取证书

这里证书获取的目的有两个：其一是将 CA 签发的证书中与本安全域有关的证书存放到本地，以提高证书的查询效率，减少向 PKI 证书存储库查询的次数；其二是为证书的验证做好准备。

下载数字证书时如果选择参数 local，则下载本地证书，如果参数为 ca，则下载 ca 的证书。

请在任意视图下进行下列操作。

表7-19 证书获取操作

操作	命令
获取证书并下载至本地	**pki retrieval certificate** { **local** | **ca** } **domain** *domain-name*

⚠ 注意：

- 如果本地已有 CA 证书存在，则不允许执行获取 CA 证书操作，避免因相关配置的修改使得证书与登记信息不匹配。若想重新获取，请先使用 **pki delete certificate** 命令删除 CA 证书与本地证书后，再执行此获取命令。
- 该操作不被保存在配置中。

7.3 证书验证配置

7.3.1 证书验证配置任务列表

在数据通信的各个环节，通信双方都需验证相应证书的有效性。证书验证的目的也就是检查一个证书的有效性。验证证书需要作签发时间、签发者信息以及证书的有效性几方面的验证。证书验证的核心就是检查 CA 在证书上的签名，并确定证书仍在有效期内，而且未被废除。由于人们相信 CA 不会发行伪造证书，所以含有它的真实签名的任何证书都可得到验证。比如你收到的一封邮件，邮件中附有一个包含公共密钥的证书，而该邮件使用了私有密钥加密，为了确定该用户是否合法持有该证书并且证书没有过期（通过 CRL 判断），以及该证书是否值得信任，就必须验证证书是否有效。

要实现证书验证功能，一般需要完成以下配置及操作任务:

- 配置 CRL 发布点位置
- 配置 CRL 更新周期
- 配置是否必须检查 CRL

- 获取 CRL
- 证书验证

7.3.2 配置 CRL 发布点位置

请在 PKI 域视图下进行下列配置。

表7-20 CRL 发布点位置配置

操作	命令
指定 CRL 发布点位置	**crl url** *url-string*
删除 CRL 发布点位置	**undo crl url**

缺省情况下，未指定 CRL 发布点位置。

7.3.3 配置 CRL 更新周期

CRL 的更新周期是指本地从 CRL 存储服务器上下载 CRL 的时间间隔。

请在 PKI 域视图下进行下列配置。

表7-21 CRL 更新周期配置

操作	命令
设置更新 CRL 的周期	**crl update period** {**default** | *days*}
恢复更新 CRL 的周期为缺省值	**undo crl update period**

缺省情况下，根据 CRL 的有效期进行更新。

📖 说明：

手工配置的 CRL 更新时间将优先于 CRL 中指明的更新时间。

7.3.4 配置是否必须检查 CRL

配置证书验证时可以设置是否必须进行 CRL 检查。如果配置为 **enable**，则检验证书的有效性，必须通过 CRL 判断。可以直接在 CA 中心进行验证，也可以将 CRL 下载到本地进行验证。如果为 **disable**，则不进行检查。

请在 PKI 域视图进行下列配置。

表7-22 CRL 是否必须检查配置

操作	命令
必须进行 CRL 检查	**crl check enable**
不进行 CRL 检查	**crl check disable**

缺省情况下，必须进行 CRL 检查。

7.3.5 获取 CRL

在完成以上配置后，即可在任意视图下发起 CRL 获取操作。下载 CRL 目的是验证当前本地所获得证书的合法性。

请在任意视图下进行下列操作。

表7-23 CRL 获取操作

操作	命令
获取 CRL 并下载至本地	**pki retrieval crl domain** *domain-name*

📖 说明：

该操作不被保存在配置中。

7.3.6 验证证书

用户可以检查一个证书的有效性。如果使用参数 local，则验证本地证书。如果参数为 ca，则验证 ca 的证书。

请在任意视图下进行下列操作。

表7-24 证书验证操作

操作	命令
检验本地证书的有效性	**pki validation certificate** { **local** | **ca** } **domain** *domain-name*

📖 说明：

该操作不被保存在配置中。

7.4 显示和调试

1. 证书显示

证书成功获取后，用户可以通过下面的操作，显示下载到本地的 CA 签名的证书内容。证书格式及内容遵循 X.509 标准，包含关于用户及 CA 自身的各种信息，如：能唯一标识用户的姓名及其他标识信息，如个人的 email 地址、证书持有者的公钥、签发个人证书的认证机构的名称、个人证书的序列号和个人证书的有效期（证书有效起止日期）等。

请在任意视图下进行下列操作。

表7-25 PKI 显示和调试操作

操作	命令
显示证书内容	**display pki certificate** [**local** | **ca** | **request-status**] [**domain** *domain-name*]

2. CRL 显示

CRL 成功获取后，用户可以通过下面的操作，显示和查看下载到本地的 CRL 内容。CRL 内容遵循 X.509 标准，包含的内容有： CRL 的版本号、签名算法、证书签发机构名、此次签发时间、下次签发时间、用户公钥信息、签名算法、签名值、序列号、撤销日期等。

请在任意视图下进行下列操作。

表7-26 PKI 显示和调试操作

操作	命令
显示 CRL 内容	**display pki crl** [**domain** *domain-name*]

3. 配置显示及调试

在配置过程中，可执行 display current 命令显示当前的 PKI 配置情况。在证书操作过程中，可打开 PKI 调试开关对相应证书操作进行监控和诊断。

请在任意视图下进行下列操作。

表7-27 PKI 显示和调试操作

操作	命令
查看 PKI 配置信息	**display current**
打开 PKI 调试开关	**debugging pki** { **verify** | **request** | **retrieval** | **error** }
关闭 PKI 调试开关	**undo debugging pki** { **verify** | **request** | **retrieval** | **error** }

缺省情况下，PKI 调试开关全部关闭。

7.5 典型配置举例

7.5.1 使用 PKI 证书方法进行 IKE 协商认证

1. 组网需求

在路由器 A 和路由器 B 之间建立一个 IPSec 安全隧道对 PC A 代表的子网（10.1.1.x）与 PC B 代表的子网（10.1.2.x）之间的数据流进行安全保护。路由器 A 和路由器 B 之间使用 IKE 自动协商建立安全通信，IKE 认证策略采用 PKI 证书体系进行身份认证。

图 1-2 中假设路由器 A 和路由器 B 使用不同的 CA（可以相同，根据实际情况确定）。

2. 组网图

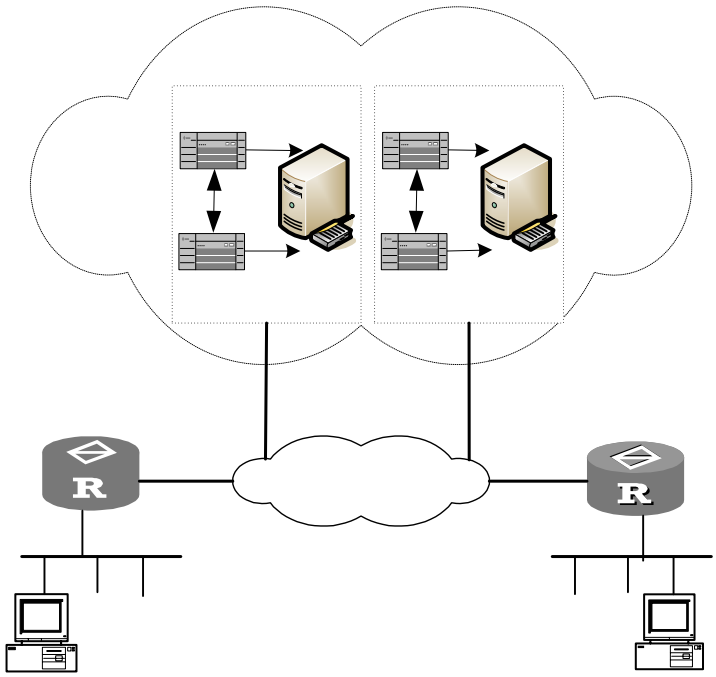

图7-2 PKI 进行 IKE 协商认证的组网图

3. 配置步骤

(1) 路由器 A 配置:

在路由器 A 上使用缺省的 IKE 策略，并配置使用 PKI（rsa-signature）方法为身份认证策略。

```
[RouterA] ike proposal 1
```

```
[RouterA-ike-proposal-1] authentication-method rsa-signature
[RouterA-ike-proposal-1] quit
```

PKI 域参数配置。

```
[RouterA]pki domain 1
[RouterA-pki-domain-1] ca identifier CA1
[RouterA-pki-domain-1] certificate request url
http://1.1.1.100/certsrv/mscep/mscep.dll
[RouterA-pki-domain-1] certificate request from ra entity en
[RouterA-pki-domain-1] ldap server ip 1.1.1.102
```

CRL 发布点位置配置（若 CRL 必须检查为 disable，则无需配置）。

```
[RouterA-pki-domain-1] crl url ldap://1.1.1.102
```

实体 DN 配置。

```
[RouterA] pki entity en
[RouterA-pki-entity-en] ip 202.38.163.1
[RouterA-pki-entity-en] common-name RouterA
```

用 RSA 算法生成本地的密钥对。

```
[RouterA-pki-entity-en] rsa local-key-pair create
```

证书申请

```
[RouterA-pki-entity-en] pki retrieval certificate ca domain 1
[RouterA-pki-entity-en] pki request  certificate 1
```

(2) 路由器 B 配置:

在路由器 B 上使用缺省的 IKE 策略，并配置使用 PKI（rsa-signature）方法为身份认证策略。

```
[RouterB] ike proposal 1
[RouterB-ike-proposal-1] authentication-method rsa-signature
[RouterB-ike-proposal-1] quit
```

PKI 域参数配置。

```
[RouterB]pki domain 1
[RouterB -pki-domain-1] ca identifier CA2
[RouterB-pki-domain-1] certificate request url
http://2.1.1.100/certsrv/mscep/mscep.dll
[RouterB -pki-domain-1] certificate request from ra entity en
[RouterB -pki-domain-1] ldap server ip 2.1.1.102
```

CRL 发布点配置（若 CRL 必须检查为 disable，则无需配置）。

```
[RouterB -pki-domain-1] crl url ldap://2.1.1.102
```

实体 DN 配置。

```
[RouterB] pki entity en
```

```
[RouterB -pki-entity-en] ip 202.38.162.1
[RouterB -pki-entity-en] common-name RouterB
```

用 RSA 算法生成本地的密钥对。

```
[RouterB -pki-entity-en] rsa local-key-pair create
```

证书申请

```
[RouterB -pki-entity-en] pki retrieval certificate ca domain 1
[RouterB -pki-entity-en] pki request  certificate 1
```

📖 说明：

以上是对 IKE 协商采用 PKI 身份认证方法的配置，若希望建立 IPSec 安全通道进行安全通信，还需要进行 IPSec 的相应配置，具体内容请参考“ IPSec 配置 ”章和“ IKE 配置 ” 章中的配置。

7.6 证书故障诊断与排除

7.6.1 故障之一：获取 CA 的证书失败

故障排除：发出手工 CA 证书请求时失败，可能有以下原因：

(1) 软件原因

- 没有设置信任的 CA 名称。
- SCEP 证书请求的服务器 URL 位置不正确或未配置，可通过 ping 命令测试服务器是否连接正常。
- 没有设置证书注册机构。

(2) 硬件原因

- 网络连接是否有故障，如网线折断，接口松动。

7.6.2 故障之二：本地证书申请失败

故障排除：路由器配置完 PKI 域参数、实体 DN、创建了新 RSA 密钥对后，发出手工证书请求时失败，可能有以下原因：

(1) 软件原因

- 申请之前没有先获取 CA/RA 的证书。
- 未创建密钥对或目前的密钥对已有证书。
- 没有设置信任的 CA 名称。
- SCEP 证书请求的服务器 URL 位置不正确或未配置，可通过 ping 命令测试服务器是否连接正常。

- 没有设置证书注册机构。
- 没有配置实体 DN 中必配属性，可通过查看 CA/RA 注册策略选择相关的属性进行配置。

(2) 硬件原因

- 网络连接是否有故障，如网线折断，接口松动。

7.6.3 故障之三：CRL 获取失败

故障排除：获取 CRL 发生失败，可能有以下原因：

(1) 软件原因

- 获取 CRL 之前未先取得本地证书。
- 未设置 LDAP 服务器的 IP 地址。
- 未设置 CRL 分布点位置。
- LDAP 服务器版本配置错误。

(2) 硬件原因

- 网络连接是否有故障，如网线折断，接口松动。