H3C MSR 系列路由器

安全配置指导(V7)

杭州华三通信技术有限公司
http://www.h3c.com.cn

资料版本：6W103-20140512
产品版本：MSR-CMW710-R0105

前 言

H3C MSR 系列路由器 配置指导(V7)共分为十五本手册，介绍了 MSR 系列路由器各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例。《安全配置指导》主要介绍安全相关协议的原理和配置，包括 AAA 及用户管理、防火墙、IPSec、IKE、RADIUS、HWTACACS、802.1X、Portal、会话管理、连接限制等。

前言部分包含如下内容：

适用款型

本手册所描述的内容适用于 MSR 系列路由器中的如下款型：

款型	
MSR 2600	MSR 26-30
MSR 3600	MSR 36-10
	MSR 36-20
	MSR 36-40
	MSR 36-60
	MSR3600-28
	MSR3600-51
MSR 5600	MSR 56-60
	MSR 56-80

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
说明	对操作内容的描述进行必要的补充和说明。
窍门	配置、操作、或使用设备的技巧、小窍门。

3. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。

4. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

产品配套资料

H3C MSR 系列路由器的配套资料包括如下部分：

大类	资料名称	内容介绍
产品知识介绍	路由器产品彩页	帮助您了解产品的主要规格参数及亮点
硬件描述与安装	路由器安装指导	帮助您详细了解设备硬件规格和安装方法，指导您对设备进行安装
	MSR 系列路由器接口模块手册	帮助您详细了解单板的硬件规格
业务配置	MSR 系列路由器配置指导(V7)	帮助您掌握设备软件功能的配置方法及配置步骤
	MSR 系列路由器命令参考(V7)	详细介绍设备的命令，相当于命令字典，方便您查阅各个命令的功能
运行维护	路由器版本说明书	帮助您了解产品版本的相关信息（包括：版本配套说明、兼容性说明、特性变更说明、技术支持信息）及软件升级方法

资料获取方式

您可以通过H3C网站（www.h3c.com.cn）获取最新的产品资料：

H3C 网站与产品资料相关的主要栏目介绍如下：

- [服务支持/文档中心]：可以获取硬件安装类、软件升级类、配置类或维护类等产品资料。
- [产品技术]：可以获取产品介绍和技术介绍的文档，包括产品相关介绍、技术介绍、技术白皮书等。
- [解决方案]：可以获取解决方案类资料。
- [服务支持/软件下载]：可以获取与软件版本配套的资料。

技术支持

用户支持邮箱：service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

网址：http://www.h3c.com.cn

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 AAA

说明

设备运行于 FIPS 模式时，本特性部分配置相对于非 FIPS 模式有所变化，具体差异请见本文相关描述。有关 FIPS 模式的详细介绍请参见“安全配置指导”中的“FIPS”。

1.1 AAA简介

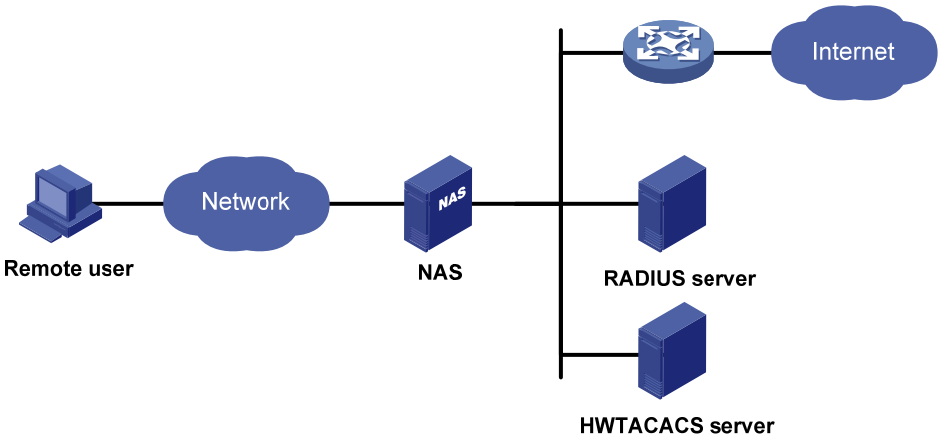
1.1.1 概述

AAA（Authentication、Authorization、Accounting，认证、授权、计费）是网络安全的一种管理机制，提供了认证、授权、计费三种安全功能。

- 认证：确认访问网络的远程用户的身份，判断访问者是否为合法的网络用户。
- 授权：对不同用户赋予不同的权限，限制用户可以使用的服务。例如，管理员授权办公用户才能对服务器中的文件进行访问和打印操作，而其它临时访客不具备此权限。
- 计费：记录用户使用网络服务过程中的所有操作，包括使用的服务类型、起始时间、数据流量等，用于收集和记录用户对网络资源的使用情况，并可以实现针对时间、流量的计费需求，也对网络起到监视作用。

AAA采用客户端/服务器结构，客户端运行于NAS（Network Access Server，网络接入服务器）上，负责验证用户身份与管理用户接入，服务器上则集中管理用户信息。AAA的基本组网结构如 图 1-1。

图1-1 AAA 基本组网结构示意图



当用户想要通过 NAS 获得访问其它网络的权利或取得某些网络资源的权利时，首先需要通过 AAA 认证，而 NAS 就起到了验证用户的作用。NAS 负责把用户的认证、授权、计费信息透传给服务器。服务器根据自身的配置对用户的身份进行判断并返回相应的认证、授权、计费结果。NAS 根据服务器返回的结果，决定是否允许用户访问外部网络、获取网络资源。

AAA 可以通过多种协议来实现，这些协议规定了 NAS 与服务器之间如何传递用户信息。目前设备支持 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）协议、HWTACACS（HW Terminal Access Controller Access Control System，HW 终端访问控制器控制系统协议）协议和 LDAP（Lightweight Directory Access Protocol，轻量级目录访问协议）协议，在实际应用中，最常使用 RADIUS 协议。

图 1-1 的AAA基本组网结构中有两台服务器，用户可以根据实际组网需求来决定认证、授权、计费功能分别由使用哪种协议类型的服务器来承担。例如，可以选择HWTACACS服务器实现认证和授权，RADIUS服务器实现计费。

当然，用户也可以只使用 AAA 提供的一种或两种安全服务。例如，公司仅仅想让员工在访问某些特定资源时进行身份认证，那么网络管理员只要配置认证服务器就可以了。但是若希望对员工使用网络的情况进行记录，那么还需要配置计费服务器。

目前，设备支持动态口令认证机制。

1.1.2 RADIUS协议简介

RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）是一种分布式的、客户端/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，常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。RADIUS 协议合并了认证和授权的过程，它定义了 RADIUS 的报文格式及其消息传输机制，并规定使用 UDP 作为封装 RADIUS 报文的传输层协议，UDP 端口 1812、1813 分别作为认证/授权、计费端口。

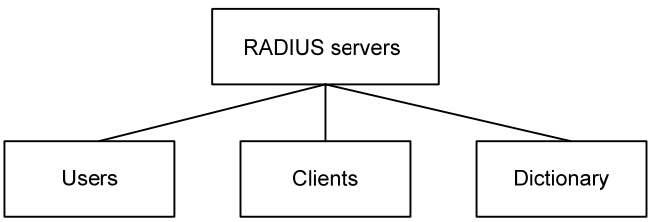
RADIUS 最初仅是针对拨号用户的 AAA 协议，后来随着用户接入方式的多样化发展，RADIUS 也适应多种用户接入方式，如以太网接入、ADSL 接入。它通过认证授权来提供接入服务，通过计费来收集、记录用户对网络资源的使用。

1. 客户端/服务器模式

- 客户端：RADIUS 客户端一般位于 NAS 上，可以遍布整个网络，负责将用户信息传输到指定的 RADIUS 服务器，然后根据服务器返回的信息进行相应处理（如接受/拒绝用户接入）。
- 服务器：RADIUS 服务器一般运行在中心计算机或工作站上，维护用户的身份信息和与其相关的网络服务信息，负责接收 NAS 发送的认证、授权、计费请求并进行相应的处理，然后给 NAS 返回处理结果（如接受/拒绝认证请求）。另外，RADIUS 服务器还可以作为一个代理，以 RADIUS 客户端的身份与其它的 RADIUS 认证服务器进行通信，负责转发 RADIUS 认证和计费报文。

RADIUS服务器通常要维护三个数据库，如 图 1-2 所示：

图1-2 RADIUS 服务器的组成



- “Users”：用于存储用户信息（如用户名、口令以及使用的协议、IP 地址等配置信息）。

- “Clients”：用于存储 RADIUS 客户端的信息（如 NAS 的共享密钥、IP 地址等）。
- “Dictionary”：用于存储 RADIUS 协议中的属性和属性值含义的信息。

2. 安全的消息交互机制

RADIUS 客户端和 RADIUS 服务器之间认证消息的交互是通过共享密钥的参与来完成的。共享密钥是一个带外传输的客户端和服务器都知道的字符串，不需要单独进行网络传输。RADIUS 报文中有一个 16 字节的验证字字段，它包含了对整个报文的数字签名数据，该签名数据是在共享密钥的参与下利用 MD5 算法计算出的。收到 RADIUS 报文的一方要验证该签名的正确性，如果报文的签名不正确，则丢弃它。通过这种机制，保证了 RADIUS 客户端和 RADIUS 服务器之间信息交互的安全性。另外，为防止用户密码在不安全的网络上传递时被窃取，在 RADIUS 报文传输过程中还利用共享密钥对用户密码进行了加密。

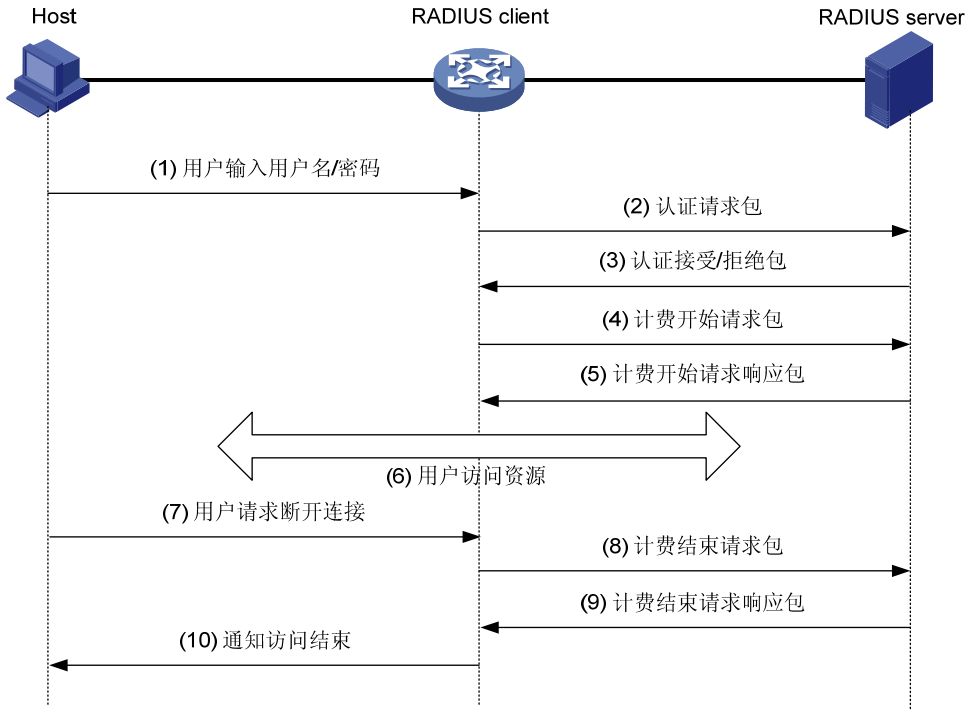
3. 用户认证机制

RADIUS 服务器支持多种方法来认证用户，例如 PAP（Password Authentication Protocol，密码验证协议）、CHAP（Challenge Handshake Authentication Protocol，质询握手验证协议）以及 EAP（Extensible Authentication Protocol，可扩展认证协议）。

4. RADIUS的基本消息交互流程

用户、RADIUS客户端和RADIUS服务器之间的交互流程如 图 1-3 所示。

图1-3 RADIUS 的基本消息交互流程



消息交互流程如下：

(1) 用户发起连接请求，向 RADIUS 客户端发送用户名和密码。

(2) RADIUS 客户端根据获取的用户名和密码，向 RADIUS 服务器发送认证请求包（Access-Request），其中的密码在共享密钥的参与下利用 MD5 算法进行加密处理。

(3) RADIUS 服务器对用户名和密码进行认证。如果认证成功，RADIUS 服务器向 RADIUS 客户端发送认证接受包（Access-Accept）；如果认证失败，则返回认证拒绝包（Access-Reject）。由于 RADIUS 协议合并了认证和授权的过程，因此认证接受包中也包含了用户的授权信息。

(4) RADIUS 客户端根据接收到的认证结果接入/拒绝用户。如果允许用户接入，则 RADIUS 客户端向 RADIUS 服务器发送计费开始请求包（Accounting-Request）。

(5) RADIUS 服务器返回计费开始响应包（Accounting-Response），并开始计费。

(6) 用户开始访问网络资源。

(7) 用户请求断开连接。

(8) RADIUS 客户端向 RADIUS 服务器发送计费停止请求包（Accounting-Request）。

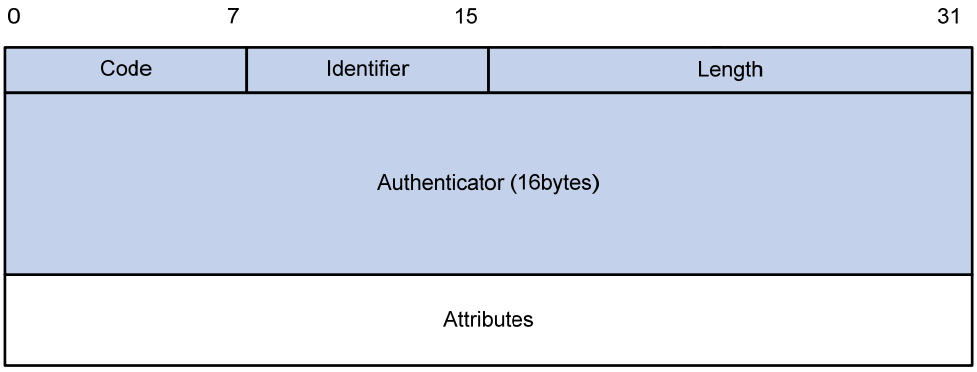
(9) RADIUS 服务器返回计费结束响应包（Accounting-Response），并停止计费。

(10) 通知用户结束访问网络资源。

5. RADIUS报文结构

RADIUS采用UDP报文来传输消息，通过定时器机制、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的正确收发。RADIUS报文结构如 图 1-4 所示。

图1-4 RADIUS 报文结构



各字段的解释如下：

(1) Code 域

长度为 1 个字节，用于说明RADIUS报文的类型，如 表 1-1 所示。

表1-1 Code 域的主要取值说明

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，请求Server对用户身份进行验证。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报文中的所有Attribute值都可以接受（即认证通过），则传输该类型报文
3	Access-Reject认证拒绝包	方向Server->Client，如果Access-Request报文中存在任何无法被接受的Attribute值（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/停止计费。该报文中的Acct-Status-Type属性用于区分计费开始请求和计费结束请求

Code	报文类型	报文说明
5	Accounting-Response 计费响应包	方向Server->Client，Server通知Client已经收到Accounting-Request报文，并且已经正确记录计费信息

(2) Identifier 域

长度为 1 个字节，用于匹配请求包和响应包，以及检测在一段时间内重发的请求包。对于类型一致且属于同一个交互过程的请求包和响应包，该 Identifier 值相同。

(3) Length 域

长度为 2 个字节，表示 RADIUS 数据包（包括 Code、Identifier、Length、Authenticator 和 Attribute）的长度，单位为字节。超过 Length 域的字节将作为填充字符被忽略。如果接收到的包的实际长度小于 Length 域的值时，则包会被丢弃。

(4) Authenticator 域

长度为 16 个字节，用于验证 RADIUS 服务器的应答报文，另外还用于用户密码的加密。Authenticator 包括两种类型：Request Authenticator 和 Response Authenticator。

(5) Attribute 域

不定长度，用于携带专门的认证、授权和计费信息。Attribute 域可包括多个属性，每一个属性都采用（Type、Length、Value）三元组的结构来表示。

- 类型（Type）：表示属性的类型。
- 长度（Length）：表示该属性（包括类型、长度和属性值）的长度，单位为字节。
- 属性值（Value）：表示该属性的信息，其格式和内容由类型决定。

表 1-2 列出了RADIUS认证、授权、计费常用的属性，这些属性由RFC 2865、RFC 2866、RFC 2867和RFC 2868 所定义。常用RADIUS标准属性的介绍请参见“1.1.8 1. 常用RADIUS标准属性”。

表1-2 RADIUS 属性

属性编号	属性名称	属性编号	属性名称
1	User-Name	45	Acct-Authentic
2	User-Password	46	Acct-Session-Time
3	CHAP-Password	47	Acct-Input-Packets
4	NAS-IP-Address	48	Acct-Output-Packets
5	NAS-Port	49	Acct-Terminate-Cause
6	Service-Type	50	Acct-Multi-Session-Id
7	Framed-Protocol	51	Acct-Link-Count
8	Framed-IP-Address	52	Acct-Input-Gigawords
9	Framed-IP-Netmask	53	Acct-Output-Gigawords
10	Framed-Routing	54	(unassigned)
11	Filter-ID	55	Event-Timestamp
12	Framed-MTU	56-59	(unassigned)
13	Framed-Compression	60	CHAP-Challenge

属性编号	属性名称	属性编号	属性名称
14	Login-IP-Host	61	NAS-Port-Type
15	Login-Service	62	Port-Limit
16	Login-TCP-Port	63	Login-LAT-Port
17	(unassigned)	64	Tunnel-Type
18	Reply-Message	65	Tunnel-Medium-Type
19	Callback-Number	66	Tunnel-Client-Endpoint
20	Callback-ID	67	Tunnel-Server-Endpoint
21	(unassigned)	68	Acct-Tunnel-Connection
22	Framed-Route	69	Tunnel-Password
23	Framed-IPX-Network	70	ARAP-Password
24	State	71	ARAP-Features
25	Class	72	ARAP-Zone-Access
26	Vendor-Specific	73	ARAP-Security
27	Session-Timeout	74	ARAP-Security-Data
28	Idle-Timeout	75	Password-Retry
29	Termination-Action	76	Prompt
30	Called-Station-Id	77	Connect-Info
31	Calling-Station-Id	78	Configuration-Token
32	NAS-Identifier	79	EAP-Message
33	Proxy-State	80	Message-Authenticator
34	Login-LAT-Service	81	Tunnel-Private-Group-id
35	Login-LAT-Node	82	Tunnel-Assignment-id
36	Login-LAT-Group	83	Tunnel-Preference
37	Framed-AppleTalk-Link	84	ARAP-Challenge-Response
38	Framed-AppleTalk-Network	85	Acct-Interim-Interval
39	Framed-AppleTalk-Zone	86	Acct-Tunnel-Packets-Lost
40	Acct-Status-Type	87	NAS-Port-Id
41	Acct-Delay-Time	88	Framed-Pool
42	Acct-Input-Octets	89	(unassigned)
43	Acct-Output-Octets	90	Tunnel-Client-Auth-id
44	Acct-Session-Id	91	Tunnel-Server-Auth-id

6. RADIUS扩展属性

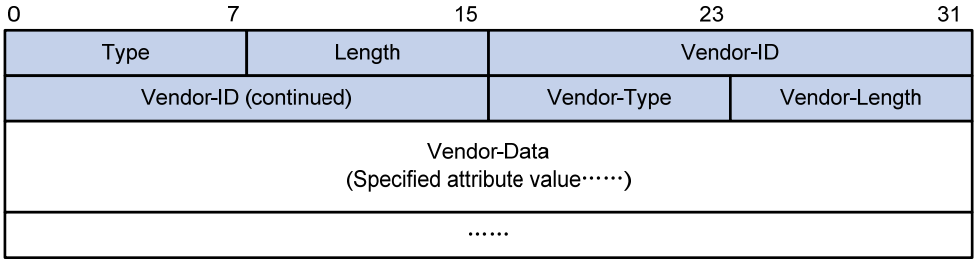
RADIUS 协议具有良好的可扩展性，RFC 2865 中定义的 26 号属性（Vendor-Specific）用于设备厂商对 RADIUS 进行扩展，以实现标准 RADIUS 没有定义的功能。

设备厂商可以在 26 号属性中封装多个自定义的（Type、Length、Value）子属性，以提供更多的扩展功能。26 号属性的格式如 图 1-5 所示：

- Vendor-ID，表示厂商代号，最高字节为 0，其余 3 字节的编码见 RFC 1700。H3C 公司的 Vendor-ID 是 25506。
- Vendor-Type，表示子属性类型。
- Vendor-Length，表示子属性长度。
- Vendor-Data，表示子属性的内容。

关于H3C RADIUS扩展属性的介绍请参见“1.1.8 2. H3C RADIUS扩展属性”。

图1-5 26 号属性的格式



1.1.3 HWTACACS协议简介

HWTACACS（HW Terminal Access Controller Access Control System，HW 终端访问控制器控制系统协议）是在 TACACS（RFC 1492）基础上进行了功能增强的安全协议。该协议与 RADIUS 协议类似，采用客户端/服务器模式实现 NAS 与 HWTACACS 服务器之间的通信。

HWTACACS 协议主要用于 PPP（Point-to-Point Protocol，点对点协议）和 VPDN（Virtual Private Dial-up Network，虚拟专用拨号网络）接入用户及终端用户的认证、授权和计费。其典型应用是对需要登录到 NAS 设备上进行操作的终端用户进行认证、授权以及对终端用户执行的操作进行记录。设备作为 HWTACACS 的客户端，将用户名和密码发给 HWTACACS 服务器进行验证，用户验证通过并得到授权之后可以登录到设备上进行操作，HWTACACS 服务器上会记录用户对设备执行过的命令。

1. HWTACACS协议与RADIUS协议的区别

HWTACACS协议与RADIUS协议都实现了认证、授权和计费功能，它们有很多相似点：结构上都采用客户端/服务器模式；都使用共享密钥对传输的用户信息进行加密；都有较好的灵活性和可扩展性。两者之间存在的主要区别如 表 1-3 所示。

表1-3 HWTACACS 协议和 RADIUS 协议区别

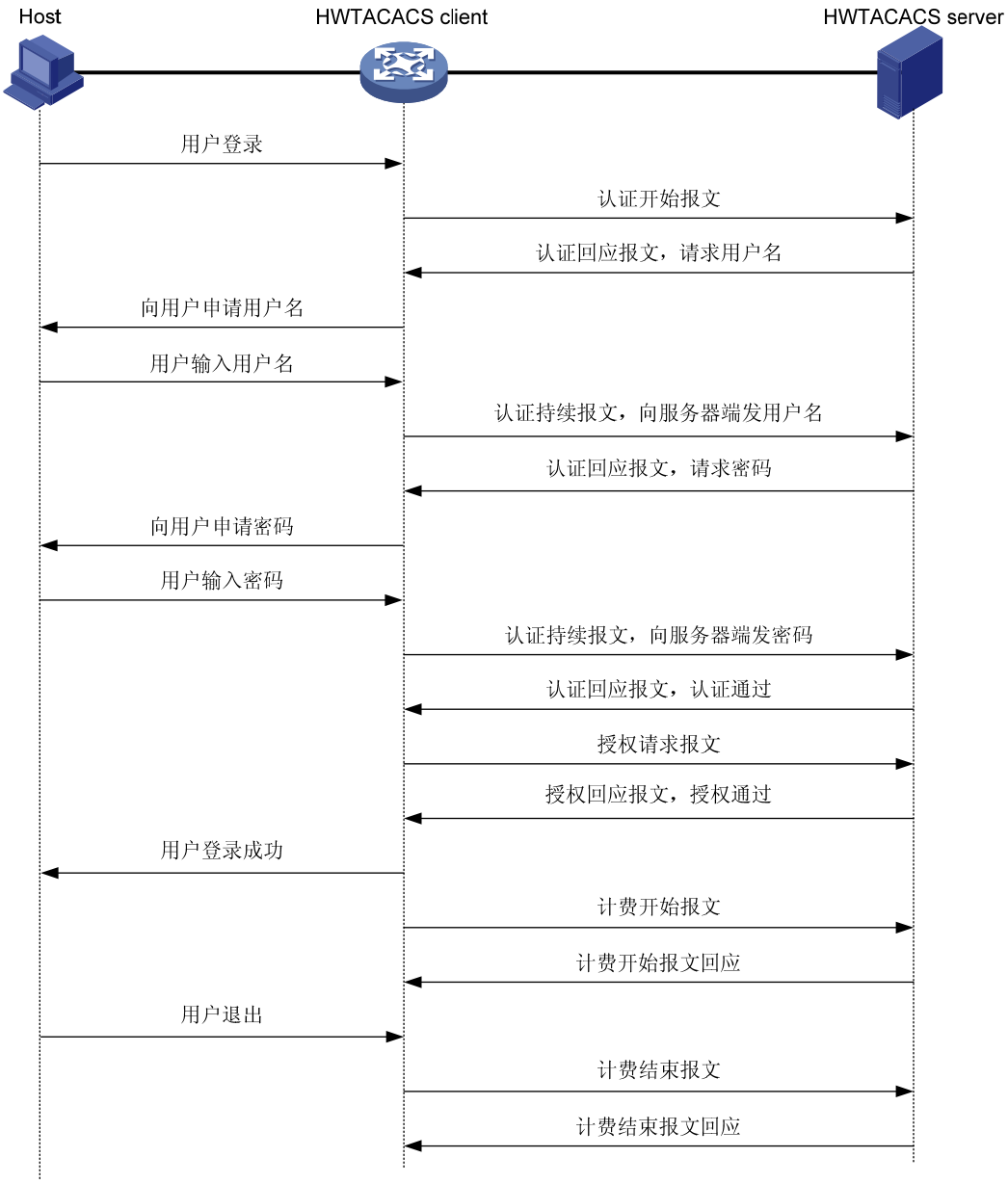
HWTACACS 协议	RADIUS 协议
使用TCP，网络传输更可靠	使用UDP，网络传输效率更高
除了HWTACACS报文头，对报文主体全部进行加密	只对认证报文中的密码字段进行加密

HWTACACS 协议	RADIUS 协议
协议报文较为复杂，认证和授权分离，使得认证、授权服务可以分离在不同的服务器上实现。例如，可以用一个HWTACACS服务器进行认证，另外一个HWTACACS服务器进行授权	协议报文比较简单，认证和授权结合，难以分离
支持对设备的配置命令进行授权使用。用户可使用的命令行受到用户角色和AAA授权的双重限制，某角色的用户输入的每一条命令都需要通过HWTACACS服务器授权，如果授权通过，命令就可以被执行	不支持对设备的配置命令进行授权使用 用户登录设备后可以使用的命令行由用户所具有的角色决定，关于用户角色的相关介绍请参见“基础配置指导”中的“RBAC”

2. HWTACACS的基本消息交互流程

下面以Telnet用户为例，说明使用HWTACACS对用户进行认证、授权和计费的过程。基本消息交互流程图如 图 1-6 所示。

图1-6 Telnet 用户认证、授权和计费流程图



基本消息交互流程如下：

(1) Telnet 用户请求登录设备。

(2) HWTACACS 客户端收到请求之后，向 HWTACACS 服务器发送认证开始报文。

(3) HWTACACS 服务器发送认证回应报文，请求用户名。

(4) HWTACACS 客户端收到回应报文后，向用户询问用户名。

(5) 用户输入用户名。

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

(7) HWTACACS 服务器发送认证回应报文，请求登录密码。

(8) HWTACACS 客户端收到回应报文，向用户询问登录密码。

(9) 用户输入密码。

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

(11) 如果认证成功，HWTACACS 服务器发送认证回应报文，指示用户通过认证。

(12) HWTACACS 客户端向 HWTACACS 服务器发送授权请求报文。

(13) 如果授权成功，HWTACACS 服务器发送授权回应报文，指示用户通过授权。

(14) HWTACACS 客户端收到授权成功报文，向用户输出设备的配置界面，允许用户登录。

(15) HWTACACS 客户端向 HWTACACS 服务器发送计费开始报文。

(16) HWTACACS 服务器发送计费回应报文，指示计费开始报文已经收到。

(17) 用户请求断开连接。

(18) HWTACACS 客户端向 HWTACACS 服务器发送计费结束报文。

(19) HWTACACS 服务器发送计费结束报文，指示计费结束报文已经收到。

1.1.4 LDAP协议简介

LDAP（Lightweight Directory Access Protocol，轻量级目录访问协议）是一种目录访问协议，用于提供跨平台的、基于标准的目录服务。它是在 X.500 协议的基础上发展起来的，继承了 X.500 的优点，并对 X.500 在读取、浏览和查询操作方面进行了改进，适合于存储那些不经常改变的数据。

LDAP 协议的典型应用是用来保存系统中的用户信息，如 Microsoft 的 Windows 操作系统就使用了 Active Directory Server（一种 LDAP 服务器软件）来保存操作系统的用户、用户组等信息，用于用户登录 Windows 时的认证和授权。

1. LDAP目录服务

LDAP 中使用目录记录并管理系统中的组织信息、人员信息以及资源信息。目录按照树型结构组织，由多个条目（Entry）组成的。条目是具有 DN（Distinguished Name，可区别名）的属性（Attribute）集合。属性用来承载各种类型的数据信息，例如用户名、密码、邮件、计算机名、联系电话等。

LDAP 协议基于 Client/Server 结构提供目录服务功能，所有的目录信息数据存储在 LDAP 服务器上。目前，Microsoft 的 Active Directory Server、IBM 的 Tivoli Directory Server 和 Sun 的 Sun ONE Directory Server 都是常用的 LDAP 服务器软件。

2. 使用LDAP协议进行认证和授权

AAA 可以使用 LDAP 协议对用户提供认证和授权服务。LDAP 协议中定义了多种操作来实现 LDAP 的各种功能，用于认证和授权的操作主要为绑定和查询。

- 绑定操作的作用有两个：一是与 LDAP 服务器建立连接并获取 LDAP 服务器的访问权限。二是用于检查用户信息的合法性。
- 查询操作就是构造查询条件，并获取 LDAP 服务器的目录资源信息的过程。

使用 LDAP 协议进行认证时，其基本的工作流程如下：

(1) LDAP 客户端使用 LDAP 服务器管理员 DN 与 LDAP 服务器进行绑定，与 LDAP 服务器建立连接并获得查询权限。

(2) LDAP 客户端使用认证信息中的用户名构造查询条件，在 LDAP 服务器指定根目录下查询此用户，得到用户的 DN。

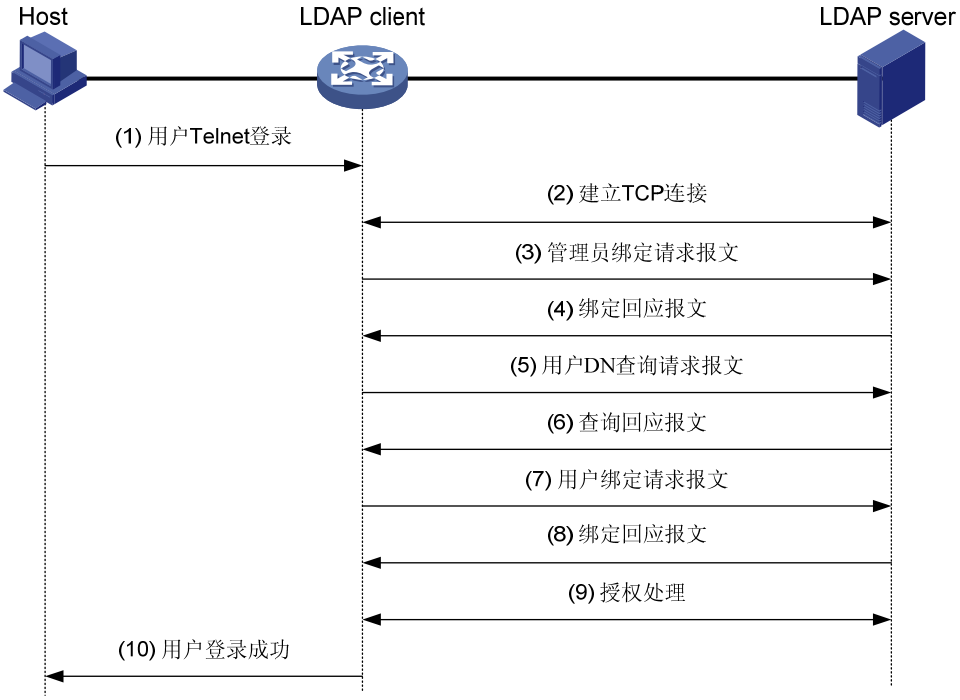
(3) LDAP 客户端使用用户 DN 和用户密码与 LDAP 服务器进行绑定，检查用户密码是否正确。

使用 LDAP 协议进行授权的过程与认证过程相似，首先必须通过与 LDAP 服务器进行绑定，建立与服务器的连接，然后在此连接的基础上通过查询操作得到用户的授权信息。与认证过程稍有不同的是，在查询用户 DN 时，除能够获得用户 DN 外，还可以获得用户信息中的授权信息。如果查询用户 DN 时便能够获得相应的授权信息，则授权过程与认证过程相同；否则还需要再次以 LDAP 服务器管理员身份与 LDAP 服务器进行绑定，并在获得相应的目录查询权限后，使用查询到的用户 DN 构造查询条件，继续对该用户的其它授权信息进行查询。

3. LDAP的基本消息交互流程

下面以Telnet用户登录设备为例，说明如何使用LDAP来对用户进行的认证和授权。基本消息交互流程如 图 1-7 所示。

图1-7 LDAP 认证的基本消息交互流程



基本消息交互流程如下：

(1) 用户发起连接请求，向 LDAP 客户端发送用户名和密码。

(2) LDAP 客户端收到请求之后，与 LDAP 服务器建立 TCP 连接。

(3) LDAP 客户端以管理员 DN 和管理员 DN 密码为参数向 LDAP 服务器发送管理员绑定请求报文（Administrator Bind Request）获得查询权限。

(4) LDAP 服务器进行绑定请求报文的处理。如果绑定成功，则向 LDAP 客户端发送绑定成功的回应报文。

(5) LDAP 客户端以输入的用户名为参数，向 LDAP 服务器发送用户 DN 查询请求报文（User DN Search Request）。

(6) LDAP 服务器收到查询请求报文后，根据报文中的查询起始地址、查询范围、以及过滤条件，对用户 DN 进行查找。如果查询成功，则向 LDAP 客户端发送查询成功的回应报文。查询得到的用户 DN 可以是一或多个。

(7) LDAP 客户端以查询得到的用户 DN 和用户输入的密码为参数，向 LDAP 服务器发送用户 DN 绑定请求报文（User DN Bind Request），检查用户密码是否正确。

(8) LDAP 服务器进行绑定请求报文的处理。

- 如果绑定成功，则向 LDAP 客户端发送绑定成功的回应报文。
- 如果绑定失败，则向 LDAP 客户端发送绑定失败的回应报文。LDAP 客户端以下一个查询到的用户 DN（如果存在的话）为参数，继续向服务器发送绑定请求，直至有一个 DN 绑定成功，或者所有 DN 均绑定失败。如果所有用户 DN 都绑定失败，则 LDAP 客户端通知用户登录失败并拒绝用户接入。

(9) LDAP 客户端与 LDAP 服务器进行授权报文的交互。如果需要使用其它方案（如 HWTACACS 等）继续进行授权，则与对应服务器进行授权报文的交互。

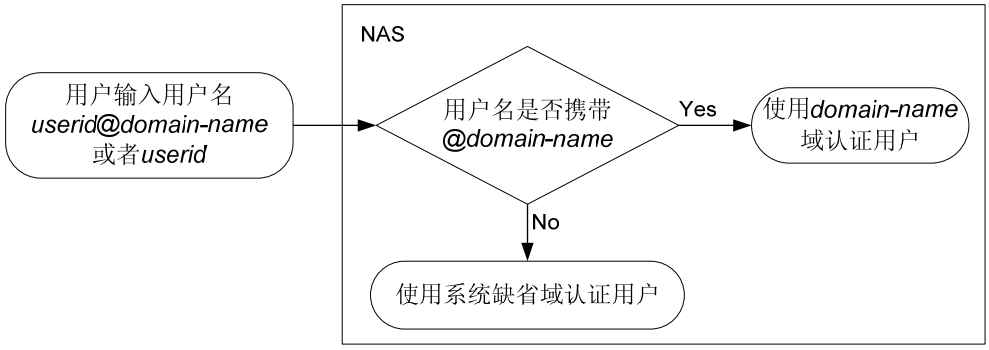
(10) 授权成功之后，LDAP 客户端通知用户登录成功。

1.1.5 设备的AAA实现

1. 基于域的用户管理

NAS对用户的管理是基于ISP（Internet Service Provider，互联网服务提供者）域的，每个用户都属于一个ISP域。一般情况下，用户所属的ISP域是由用户登录时提供的用户名决定的，如 图 1-8 所示。

图1-8 用户名决定域名



为便于对不同接入方式的用户进行区分管理，提供更为精细且有差异化的认证、授权、计费服务，AAA 将用户划分为以下几个类型：

- lan-access 用户：LAN 接入用户，如 802.1X 认证、MAC 地址认证用户。
- login 用户：登录设备用户，如 SSH、Telnet、FTP、终端接入用户（即从 Console 口、AUX 口、Async 口登录的用户）。
- Portal 接入用户。
- PPP 接入用户。

对于某些接入方式，用户最终所属的 ISP 域可由该相应的认证模块（例如 802.1X）提供命令行来指定，用于满足一定的用户认证管理策略。

2. 实现AAA的方法

在具体实现中，一个 ISP 域对应着设备上一套实现 AAA 的配置策略，它们是管理员针对该域用户制定的一套认证、授权、计费方法，可根据用户的接入特征以及不同的安全需求组合使用。

AAA 支持以下认证方法：

- 不认证：对用户非常信任，不对其进行合法性检查，一般情况下不采用这种方法。
- 本地认证：认证过程在接入设备上完成，用户信息（包括用户名、密码和各种属性）配置在接入设备上。优点是速度快，可以降低运营成本；缺点是存储信息量受设备硬件条件限制。
- 远端认证：认证过程在接入设备和远端的服务器之间完成，接入设备和远端服务器之间通过 RADIUS、HWTACACS 或 LDAP 协议通信。优点是用户信息集中在服务器上统一管理，可实现大容量、高可靠性、支持多设备的集中式统一认证。当远端服务器无效时，可配置备选认证方式完成认证。

AAA 支持以下授权方法：

- 不授权：接入设备不请求授权信息，不对用户可以使用的操作以及用户允许使用的网络服务进行授权。此时，认证通过的 login 用户只有系统所给予的缺省用户角色，其中 FTP 用户的工作目录是设备的根目录，但并无访问权限；认证通过的非 login 用户，可直接访问网络。关于缺省用户角色的详细介绍请参见“基础配置指导”中的“RBAC”。
- 本地授权：授权过程在接入设备上进行，根据接入设备上为本地用户配置的相关属性进行授权。
- 远端授权：授权过程在接入设备和远端服务器之间完成。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。RADIUS 认证成功后，才能进行授权，RADIUS 授权信息携带在认证回应报文中下发给用户。HWTACACS 协议的授权与认证相分离，在认证成功后，HWTACACS 授权信息通过授权报文进行交互。当远端服务器无效时，可配置备选授权方式完成授权。

AAA 支持以下计费方法：

- 不计费：不对用户计费。
- 本地计费：计费过程在接入设备上完成，实现了本地用户连接数的统计和限制，并没有实际的费用统计功能。
- 远端计费：计费过程在接入设备和远端的服务器之间完成。当远端服务器无效时，可配置备选计费方式完成计费。

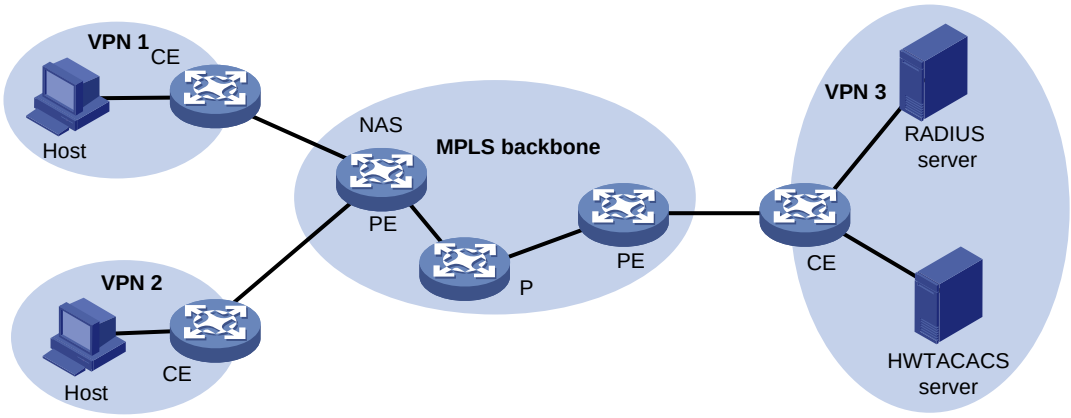
除此之外，对于 login 用户，AAA 还可以对其提供以下服务，用于提高对设备操作的安全性：

- 命令行授权：用户执行的每一条命令都需要接受授权服务器的检查，只有授权成功的命令才被允许执行。关于命令行授权的详细介绍请参考“基础配置指导”中的“配置用户通过 CLI 登录设备”。
- 命令行计费：若未开启命令行授权功能，则计费服务器对用户执行过的所有有效命令进行记录；若开启了命令行授权功能，则计费服务器仅对授权通过的命令进行记录。关于命令行计费的详细介绍请参考“基础配置指导”中的“配置用户通过 CLI 登录设备”。
- 用户角色切换认证：在不退出当前登录、不断开当前连接的前提下，用户将当前的用户角色切换为其它用户角色时，只有通过服务器的认证，该切换操作才被允许。关于用户角色切换的详细介绍请参考“基础配置指导”中的“RBAC”。

1.1.6 AAA支持MPLS L3VPN

在MPLS L3VPN组网中，要求在私网客户端业务隔离的情况下，实现对客户端的集中认证，这就需要AAA支持基于VPN多实例的报文交互。通过AAA支持MPLS L3VPN，可实现RADIUS、HWTACACS认证/授权/计费报文在MPLS L3VPN之间的交互。如 图 1-9 所示，连接客户端的PE设备作为NAS，通过MPLS L3VPN把私网客户端的认证/授权/计费信息透传给网络另一端的私网服务器，实现了对私网客户端的集中认证，且各私网的认证报文互不影响。

图1-9 AAA 支持 MPLS L3VPN 典型组网图



说明

在 MCE 设备上进行的 Portal 接入认证在本特性的配合下，也可支持多实例功能。关于 MCE 的相关介绍请见参见“MPLS 配置指导”中的“MPLS L3VPN”。关于 Portal 的相关介绍请参见“安全配置指导”中的“Portal”。

1.1.7 协议规范

与 AAA、RADIUS、HWTACACS、LDAP 相关的协议规范有：

- RFC 2865：Remote Authentication Dial In User Service (RADIUS)
- RFC 2866：RADIUS Accounting
- RFC 2867：RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC 2868：RADIUS Attributes for Tunnel Protocol Support
- RFC 2869：RADIUS Extensions
- RFC 5176：Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
- RFC 1492：An Access Control Protocol, Sometimes Called TACACS
- RFC 1777：Lightweight Directory Access Protocol
- RFC 2251：Lightweight Directory Access Protocol (v3)

1.1.8 RADIUS属性

1. 常用RADIUS标准属性

表1-4 常用 RADIUS 标准属性

属性编号	属性名称	描述
1	User-Name	需要进行认证的用户名称
2	User-Password	需要进行PAP方式认证的用户密码，在采用PAP认证方式时，该属性仅出现在Access-Request报文中
3	CHAP-Password	需要进行CHAP方式认证的用户密码的消息摘要。在采用CHAP认证方式时，该属性出现在Access-Request报文中
4	NAS-IP-Address	Server通过不同的IP地址来标识不同的Client，通常Client采用本地一个接口的IP地址来唯一的标识自己，这就是NAS-IP-Address。该属性指示当前发起请求的Client的NAS-IP-Address。该字段仅出现在Access-Request报文中
5	NAS-Port	用户接入NAS的物理端口号
6	Service-Type	用户申请认证的业务类型
7	Framed-Protocol	用户Frame类型业务的封装协议
8	Framed-IP-Address	为用户所配置的IP地址
11	Filter-ID	访问控制列表的名称
12	Framed-MTU	用户与NAS之间数据链路的MTU（Maximum Transmission Unit，最大传输单元）值。例如在802.1X的EAP方式认证中，NAS通过Framed-MTU值指示Server发送EAP报文的最大长度，防止EAP报文大于数据链路MTU导致的报文丢失
14	Login-IP-Host	用户登录设备的接口IP地址
15	Login-Service	用户登录设备时采用的业务类型
18	Reply-Message	服务器反馈给用户的纯文本描述，可用于向用户显示认证失败的原因
26	Vendor-Specific	厂商自定义的私有属性。一个报文中可以有一个或者多个私有属性，每个私有属性中可以有一个或者多个子属性
27	Session-Timeout	会话结束之前，给用户提供服务的最大时间，即用户的最大可用时长
28	Idle-Timeout	会话结束之前，允许用户持续空闲的最大时间，即用户的限制切断时间
31	Calling-Station-Id	NAS用于向Server告知标识用户的号码，在我司设备提供的lan-access业务中，该字段填充的是用户的MAC地址，采用的“HHHH-HHHH-HHHH”格式封装
32	NAS-Identifier	NAS用来向Server标识自己的名称

属性编号	属性名称	描述
40	Acct-Status-Type	计费请求报文的类型 • 1：Start • 2：Stop • 3：Interim-Update • 4：Reset-Charge • 7：Accounting-On（3GPP 中有定义） • 8：Accounting-Off （3GPP 中有定义） • 9-14：Reserved for Tunnel Accounting • 15：Reserved for Failed
45	Acct-Authentic	用户采用的认证方式，包括RADIUS，Local以及Remote
60	CHAP-Challenge	在CHAP认证中，由NAS生成的用于MD5计算的随机序列
61	NAS-Port-Type	NAS认证用户的端口的物理类型 • 15：以太网 • 16：所有种类的 ADSL • 17：Cable（有线电视电缆） • 19：WLAN-IEEE 802.11 • 201：VLAN • 202：ATM 如果在ATM或以太网端口上还划分VLAN，则该属性值为201
79	EAP-Message	用于封装EAP报文，实现RADIUS协议对EAP认证方式的支持
80	Message-Authenticator	用于对认证报文进行认证和校验，防止非法报文欺骗。该属性在RADIUS协议支持EAP认证方式被使用
87	NAS-Port-Id	用字符串来描述的认证端口信息

2. H3C RADIUS扩展属性

表1-5 H3C RADIUS 扩展属性

子属性编号	子属性名称	描述
1	Input-Peak-Rate	用户接入到NAS的峰值速率，以bps为单位
2	Input-Average-Rate	用户接入到NAS的平均速率，以bps为单位
3	Input-Basic-Rate	用户接入到NAS的基本速率，以bps为单位
4	Output-Peak-Rate	从NAS到用户的峰值速率，以bps为单位
5	Output-Average-Rate	从NAS到用户的平均速率，以bps为单位
6	Output-Basic-Rate	从NAS到用户的基本速率，以bps为单位
15	Remanent_Volume	表示该连接的剩余可用总流量。对于不同的服务器类型，此属性的单位不同

子属性编号	子属性名称	描述
20	Command	用于会话控制，表示对会话进行操作，此属性有五种取值 • 1：Trigger-Request • 2：Terminate-Request • 3：SetPolicy • 4：Result • 5：PortalClear
24	Control_Identifier	服务器重发报文的标识符，对于同一会话中的重发报文，本属性必须相同。不同的会话的报文携带的该属性值可能相同。相应的客户端响应报文必须携带该属性，其值不变 在开始、停止或中间上报流量的Accounting-Request报文中，若带有Control_Identifier属性，此时的Control_Identifier属性无实际意义
25	Result_Code	表示Trigger-Request或SetPolicy的结果，0表示成功，非0表示失败
26	Connect_ID	用户连接索引
28	Ftp_Directory	FTP用户工作目录 对于FTP用户，当RADIUS客户端作为FTP服务器时，该属性用于设置RADIUS客户端上的FTP目录
29	Exec_Privilege	EXEC用户优先级
59	NAS_Startup_Timestamp	NAS系统启动时刻，以秒为单位，表示从1970年1月1日UTC 00:00:00以来的秒数
60	Ip_Host_Addr	认证请求和计费请求报文中携带的用户IP地址和MAC地址，格式为“A.B.C.D hh:hh:hh:hh:hh:hh”，IP地址和MAC地址之间以空格分开
61	User_Notify	服务器需要透传到客户端的信息
62	User_HeartBeat	802.1X用户认证成功后下发的32字节的Hash字符串，该属性值被保存在设备的用户列表中，用于校验802.1X客户端的握手报文 该属性仅出现在Access-Accept和Accounting-Request报文中
140	User_Group	SSL VPN用户认证成功后下发的用户组，一个用户可以属于多个用户组，多个用户组之间使用分号格开。本属性用于与SSL VPN设备配合
141	Security_Level	SSL VPN用户安全认证之后下发的安全级别
201	Input-Interval-Octets	两次实时计费间隔的输入的字节差，以Byte为单位
202	Output-Interval-Octets	两次实时计费间隔的输出的字节差，以Byte为单位
203	Input-Interval-Packets	两次计费间隔的输入的包数，单位由设备上的配置决定
204	Output-Interval-Packets	两次计费间隔的输出的包数，单位由设备上的配置决定
205	Input-Interval-Gigawords	两次计费间隔的输入的字节差是4G字节的多少倍
206	Output-Interval-Gigawords	两次计费间隔的输出的字节差是4G字节的多少倍
207	Backup-NAS-IP	NAS发送RADIUS报文的备份源IP地址
255	Product_ID	产品名称

1.2 AAA配置思路及配置任务简介

在作为 AAA 客户端的接入设备（实现 NAS 功能的网络设备）上，AAA 的基本配置思路如下：

(1) 配置 AAA 方案：根据不同的组网环境，配置相应的 AAA 方案。

- 本地认证：由 NAS 自身对用户进行认证、授权和计费。需要配置本地用户，即 local user 的相关属性，包括手动添加用户的用户名和密码等。
- 远程认证：由远程 AAA 服务器来对用户进行认证、授权和计费。需要配置 RADIUS、HWTACACS 或 LDAP 方案。

(2) 配置实现 AAA 的方法：在用户所属的 ISP 域中分别指定实现认证、授权、计费的方法。其中，远程认证、授权、计费方法中均需要引用已经配置的 RADIUS、HWTACACS 或 LDAP 方案。

- 认证方法：可选择不认证（none）、本地认证（local）或远程认证（scheme）；
- 授权方法：可选择不授权（none）、本地授权（local）或远程授权（scheme）；
- 计费方法：可选择不计费（none）、本地计费（local）或远程计费（scheme）。

图1-10 AAA 基本配置思路流程图

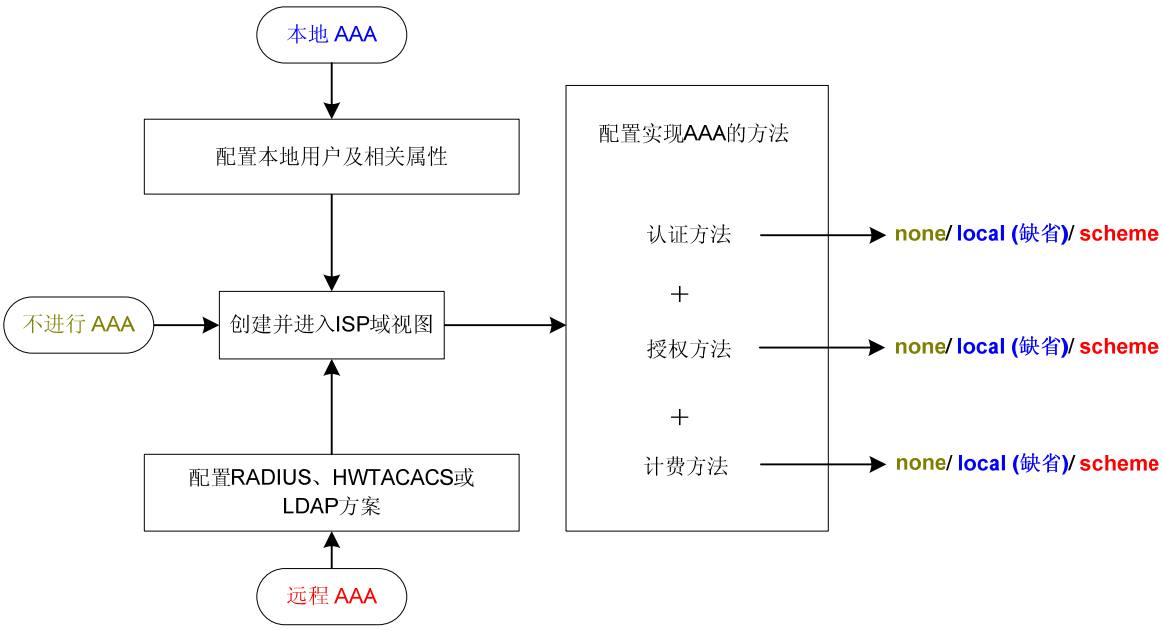


表1-6 AAA 配置任务简介

配置任务		说明	详细配置
配置AAA方案	配置本地用户	四者至少选其一	1.3.1
	配置RADIUS方案		1.3.2
	配置HWTACACS方案		1.3.3
	配置LDAP方案		1.3.4
在ISP域中配置实现AAA	创建ISP域	必选	1.4.2

配置任务		说明	详细配置
的方法	配置ISP域的属性	可选	1.4.3
	配置ISP域的AAA认证方法	三者至少选其一	1.4.4
	配置ISP域的AAA授权方法		1.4.5
	配置ISP域的AAA计费方法		1.4.6
配置RADIUS session control功能		可选	1.5
配置RADIUS DAE服务器功能		可选	1.6
配置RADIUS协议报文的DSCP优先级		可选	1.7
限制同时在线的最大用户连接数		可选	1.8

1.3 配置AAA方案

1.3.1 配置本地用户

当选择使用本地认证、本地授权、本地计费方法对用户进行认证、授权或计费时，应在设备上创建本地用户并配置相关属性。

所谓本地用户，是指在本地设备上设置的一组用户属性的集合。该集合以用户名和用户类别为用户的唯一标识。本地用户分为两类，一类是设备管理用户；另一类是网络接入用户。设备管理用户供设备管理员登录设备使用，网络接入用户供通过设备访问网络服务的用户使用。为使某个请求网络服务的用户可以通过本地认证，需要在设备上的本地用户数据库中添加相应的表项。具体步骤是，创建一个本地用户并进入本地用户视图，然后在本地用户视图下配置相应的用户属性，可配置的用户属性包括：

- 服务类型

用户可使用的网络服务类型。该属性是本地认证的检测项，如果没有用户可以使用的服务类型，则该用户无法通过认证。

支持的服务类型包括：FTP、lan-access、Portal、PPP、SSH、Telnet、Terminal。

- 用户状态

用于指示是否允许该用户请求网络服务器，包括 active 和 block 两种状态。active 表示允许该用户请求网络服务，block 表示禁止该用户请求网络服务。

- 最大用户数

使用当前用户名接入设备的最大用户数目。若当前该用户名的接入用户数已达最大值，则使用该用户名的新用户将被禁止接入。

- 所属的用户组

每一个本地用户都属于一个本地用户组，并继承组中的所有属性（密码管理属性和用户授权属性）。关于本地用户组的介绍和配置请参见“1.3.1 2. 配置用户组属性”。

- 绑定属性

用户认证时需要检测的属性，用于限制接入用户的范围。若用户的实际属性与设置的绑定属性不匹配，则不能通过认证，因此在配置绑定属性时要考虑该用户是否需要绑定某些属性。可绑定的属性包括：ISDN用户的主叫号码、用户IP地址、用户接入端口、用户MAC地址、用户所属VLAN。各属性的使用及支持情况请见 表 1-8。

- 用户授权属性

用户认证通过后，接入设备下发给用户的权限。支持的授权属性包括：ACL、PPP回呼号码、闲置切断功能、用户角色、VLAN、FTP/SFTP工作目录。各属性的支持情况请见 表 1-8。由于可配置的授权属性都有其明确的使用环境和用途，因此配置授权属性时要考虑该用户是否需要某些属性。例如，PPP接入用户不需要授权的目录，因此就不要设置PPP用户的工作目录属性。

本地用户的授权属性在用户组和本地用户视图下都可以配置，且本地用户视图下的配置优先级高于用户组视图下的配置。用户组的配置对组内所有本地用户生效。

- 密码管理属性

用户密码的安全属性，可用于对设备管理类本地用户的认证密码进行管理和控制。可设置的策略包括：密码老化时间、密码最小长度、密码组合策略、密码复杂度检查策略和用户登录尝试次数限制策略。

本地用户的密码管理属性在系统视图（具有全局性）、用户组视图和本地用户视图下都可以配置，其生效的优先级顺序由高到底依次为本地用户、用户组、全局。全局配置对所有本地用户生效，用户组的配置对组内所有本地用户生效。有关密码管理以及全局密码配置的详细介绍请参见“安全配置指导”中的“Password Control”。

表1-7 配置任务简介

配置任务	说明	详细配置
配置本地用户属性	必选	1.3.1 1.
配置用户组属性	可选	1.3.1 2.
本地用户及本地用户组显示与维护	可选	1.3.1 3.

1. 配置本地用户属性

配置本地用户属性时，有以下配置限制和指导：

- 使能全局密码管理功能（通过命令 **password-control enable**）后，设备上将不显示配置的本地用户密码。
- 如果用户线视图下登录设备的认证方式（通过命令 **authentication-mode** 设置）为 AAA（**scheme**），则用户登录设备后所能使用的命令由用户被授权的用户角色确定；如果登录设备的认证方式为不认证（**none**）或密码认证（**password**），则用户登录设备后所能使用的命令由用户线下设置的用户角色确定。对于 SSH 用户，使用公钥认证时，其所能使用的命令以与 SSH 用户同名的本地用户视图中设置的用户角色为准。关于登录设备的认证方式与用户线下的用户角色的详细介绍请参见“基础配置指导”中的“登录设备”。
- 授权属性和密码控制属性均可以在本地用户视图和用户组视图下配置，各视图下的配置优先级顺序从高到底依次为：本地用户视图-->用户组视图。

表1-8 配置本地用户的属性

操作		命令	说明
进入系统视图		**system-view**	-
添加本地用户，并进入本地用户视图		**local-user** *user-name* [**class** { **manage** | **network** }]	缺省情况下，不存在本地用户
（可选）设置本地用户的密码	对于网络接入类（**network**）本地用户	**password** { **cipher** | **simple** } *password*	网络接入类用户的密码将在加密运算后以密文的方式保存到配置文件中 设备管理类用户的密码将在哈希计算后以密文的方式保存到配置文件中 若不设置密码，则本地用户认证时无需输入密码，只要用户名有效且其它属性验证通过即可认证成功，因此为提高用户帐户的安全性，建议设置本地用户密码
	对于设备管理类（**manage**）本地用户	非FIPS模式下： **password** [{ **hash** | **simple** } *password*] FIPS模式下： **password**	
设置本地用户可以使用的服务类型	对于网络接入类（**network**）本地用户	**service-type** { **lan-access** | **portal** | **ppp** }	缺省情况下，本地用户不能使用任何服务类型
	对于设备管理类（**manage**）本地用户	非FIPS模式下： **service-type** { **ftp** | { **ssh** | **telnet** | **terminal** } * } FIPS模式下： **service-type** { **ssh** | **terminal** } *	
（可选）设置本地用户的状态		**state** { **active** | **block** }	缺省情况下，当一个本地用户被创建以后，其状态为**active**，允许该用户请求网络服务
（可选）设置使用当前本地用户名接入设备的最大用户数		**access-limit** *max-user-number*	缺省情况下，不限制使用当前本地用户名接入的用户数 由于FTP用户不支持计费，因此FTP用户不受此属性限制
（可选）设置本地用户的绑定属性		**bind-attribute** { **call-number** *call-number* [**:** *subcall-number*] | **ip** *ip-address* | **location interface** *interface-type interface-number* | **mac** *mac-address* | **vlan** *vlan-id* } *	缺省情况下，未设置本地用户的任何绑定属性 • 绑定属性 **call-number** 仅适用于 PPP 用户； • 绑定属性 **ip** 仅适用于 lan-access 类型中的 802.1X 用户； • 绑定属性 **location**、**mac** 和 **vlan** 仅适用于 lan-access 类型的用户

操作		命令	说明
（可选）设置本地用户的授权属性		**authorization-attribute** { **acl** *acl-number* | **callback-number** *callback-number* | **idle-cut** *minute* | **user-role** *role-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } *	缺省情况下，无缺省授权ACL、闲置切断时间、授权VLAN。授权FTP/SFTP/SCP用户可以访问的目录为设备的根目录，但无访问权限。由用户角色为network-admin或者level-15的用户创建的本地用户被授权用户角色network-operator • 对于ppp用户，仅授权属性**acl**、**callback-number**、**idle-cut**有效； • 对于lan-access、portal用户，仅授权属性**acl**、**idle-cut**和**vlan**有效； • 对于http、https、telnet、terminal用户，仅授权属性**user-role**有效； • 对于ssh、ftp用户，仅授权属性**user-role**和**work-directory**有效； • 对于其它类型的本地用户，所有授权属性均无效
（可选）设置设备管理类本地用户的密码管理属性	密码老化时间	**password-control aging** *aging-time*	缺省情况下，采用本地用户所属用户组的密码管理策略 仅设备管理类的本地用户支持本地用户密码管理功能
	密码最小长度	**password-control length** *length*	
	密码组合策略	**password-control composition type-number** *type-number* [**type-length** *type-length*]	
	密码的复杂度检查策略	**password-control complexity** { **same-character** | **user-name** } **check**	
	用户登录尝试次数以及登录尝试失败后的行为	**password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	
（可选）设置本地用户所属的用户组		**group** *group-name*	缺省情况下，本地用户属于系统默认创建的用户组system

2. 配置用户组属性

为了简化本地用户的配置，增强本地用户的可管理性，引入了用户组的概念。用户组是一个本地用户属性的集合，某些需要集中管理的属性可在用户组中统一配置和管理，用户组内的所有本地用户都可以继承这些属性。目前，用户组中可以管理的用户属性为授权属性。

每个新增的本地用户都默认属于一个系统自动创建的用户组 system，且继承该组的所有属性。本地用户所属的用户组可以通过本地用户视图下的 **group** 命令来修改。

表1-9 配置用户组的属性

操作		命令	说明
进入系统视图		**system-view**	-
创建用户组，并进入用户组视图		**user-group** *group-name*	缺省情况下，存在一个名称为system的用户组
设置用户组的授权属性		**authorization-attribute** { **acl** *acl-number* | **callback-number** *callback-number* | **idle-cut** *minute* | **vlan** *vlan-id* | **work-directory** *directory-name* } *	缺省情况下，未设置用户组的授权属性
（可选）设置用户组的密码管理属性	密码老化时间	**password-control aging** *aging-time*	缺省情况下，采用全局密码管理策略 全局密码管理策略的相关配置请参见“安全配置指导”中的“Password Control”
	密码最小长度	**password-control length** *length*	
	密码组合策略	**password-control composition type-number** *type-number* [**type-length** *type-length*]	
	密码的复杂度检查策略	**password-control complexity** { **same-character** | **user-name** } **check**	
	用户登录尝试次数以及登录尝试失败后的行为	**password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	

3. 本地用户及本地用户组显示与维护

完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后本地用户及本地用户组的运行情况，通过查看显示信息验证配置的效果。

表1-10 本地用户及本地用户组显示和维护

操作	命令
显示本地用户的配置信息和在线用户数的统计信息	**display local-user** [**class** { **manage** | **network** } | **idle-cut** { **disable** | **enable** } | **service-type** { **ftp** | **lan-access** | **portal** | **ppp** | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name* | **vlan** *vlan-id*]
显示本地用户组的相关配置	**display user-group** [*group-name*]

1.3.2 配置RADIUS方案

RADIUS 方案中定义了设备和 RADIUS 服务器之间进行信息交互所必需的一些参数，主要包括 RADIUS 服务器的 IP 地址、UDP 端口号、报文共享密钥、服务类型等。

1. RADIUS配置任务简介

表1-11 RADIUS 配置任务简介

配置任务	说明	详细配置
配置RADIUS服务器探测模版	可选	1.3.2 2.
创建RADIUS方案	必选	1.3.2 3.
配置RADIUS认证服务器	必选	1.3.2 4.
配置RADIUS计费服务器及相关参数	可选	1.3.2 5.
配置RADIUS报文的共享密钥	可选	1.3.2 6.
配置RADIUS方案所属的VPN	可选	1.3.2 7.
配置发送给RADIUS服务器的用户名格式和数据统计单位	可选	1.3.2 8.
配置发送RADIUS报文的最大尝试次数	可选	1.3.2 9.
配置RADIUS服务器的状态	可选	1.3.2 10.
配置发送RADIUS报文使用的源地址	可选	1.3.2 11.
配置RADIUS服务器的定时器	可选	1.3.2 12.
配置RADIUS的accounting-on功能	可选	1.3.2 13.
配置RADIUS服务器安全策略服务器的IP地址	可选	1.3.2 14.
配置RADIUS Attribute 25的CAR参数解析功能	可选	1.3.2 15.
配置RADIUS Attribute 15的检查方式	可选	1.3.2 16.
配置RADIUS的Trap功能	可选	1.3.2 17.
RADIUS显示和维护	可选	1.3.2 18.

2. 配置RADIUS服务器探测模版

RADIUS 服务器探测功能是指，设备周期性发送探测报文探测 RADIUS 服务器是否可达：如果服务器不可达，则置服务器状态为 **block**，如果服务器可达，则置服务器状态为 **active**。该探测功能不依赖于实际用户的认证过程，无论是否有用户向 RADIUS 服务器发起认证，无论是否有用户在线，设备都会自动对指定的 RADIUS 服务器进行探测，便于及时获得该服务器的可达状态。

RADIUS 服务器探测模版用于配置探测用户名以及探测周期，并且可以被 RADIUS 方案视图下的 RADIUS 服务器配置引用。只有一个 RADIUS 服务器配置中成功引用了一个已经存在的服务器探测模版，设备才会启动对该 RADIUS 服务器的探测功能。

RADIUS 服务器探测报文是一种模拟的认证请求报文，服务器探测模版中配置的探测用户名即为该探测报文中的认证用户名。设备会在配置的探测周期内选择随机时间点向引用了服务器探测模版的 RADIUS 服务器发送探测报文，且每次收到的探测应答消息仅能说明当前探测周期内该 RADIUS 服务器可达。服务器探测功能启动后，周期性的探测过程会一直执行，直到相关的配置发生变化（包括：删除该 RADIUS 服务器配置、取消对服务器探测模版的引用、删除对应的服务器探测模版、将该 RADIUS 服务器的状态手工置为 **block**、删除当前 RADIUS 方案）。

表1-12 配置 RADIUS 服务器探测模版

操作	命令	说明
进入系统视图	**system-view**	-
配置RADIUS服务器探测模版	**radius-server test-profile** *profile-name* **username** *name* [**interval** *interval*]	缺省情况下，无RADIUS服务器探测模版 系统支持最多同时存在多个RADIUS服务器探测模版

3. 创建RADIUS方案

在进行 RADIUS 的其它配置之前，必须先创建 RADIUS 方案并进入其视图。系统最多支持配置 16 个 RADIUS 方案。一个 RADIUS 方案可以同时被多个 ISP 域引用。

表1-13 创建 RADIUS 方案

操作	命令	说明
进入系统视图	**system-view**	-
创建RADIUS方案，并进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	缺省情况下，未定义RADIUS方案

4. 配置RADIUS认证服务器

由于 RADIUS 服务器的授权信息是随认证应答报文发送给 RADIUS 客户端的，RADIUS 的认证和授权功能由同一台服务器实现，因此 RADIUS 认证服务器相当于 RADIUS 认证/授权服务器。通过在 RADIUS 方案中配置 RADIUS 认证服务器，指定设备对用户进行 RADIUS 认证时与哪些服务器进行通信。

一个RADIUS方案中最多允许配置一个主认证服务器和16个从认证服务器。当主服务器不可达时，设备根据从服务器的配置顺序由先到后查找状态为 **active** 的从服务器并与之交互。建议在不需要备份的情况下，只配置主 RADIUS 认证服务器即可。

在实际组网环境中，可以指定一台服务器既作为某个 RADIUS 方案的主认证服务器，又作为另一个 RADIUS 方案的从认证服务器。

表1-14 配置 RADIUS 认证服务器

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
配置主RADIUS认证服务器	**primary authentication** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **vpn-instance** *vpn-instance-name*] *	二者至少选其一 缺省情况下，未配置主认证服务器和从认证服务器 在同一个方案中指定的主认证

操作	命令	说明
配置从RADIUS认证服务器	**secondary authentication** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **vpn-instance** *vpn-instance-name*] *	服务器和从认证服务器的IP地址、端口号和VPN参数不能完全相同，并且各从认证服务器的IP地址、端口号和VPN参数也不能完全相同

5. 配置RADIUS计费服务器及相关参数

通过在 RADIUS 方案中配置 RADIUS 计费服务器，指定设备对用户进行 RADIUS 计费时与哪些服务器进行通信。

一个RADIUS方案中最多允许配置一个主计费服务器和16个从计费服务器。当主服务器不可达时，设备根据从服务器的配置顺序由先到后查找状态为 **active** 的从服务器并与之交互。建议在不需要备份的情况下，只配置主 RADIUS 计费服务器即可。

在实际组网环境中，可以指定一台服务器既作为某个 RADIUS 方案的主计费服务器，又作为另一个 RADIUS 方案的从计费服务器。

当用户请求断开连接或者设备强行切断用户连接的情况下，设备会向 RADIUS 计费服务器发送停止计费请求。通过在设备上配置发起实时计费请求的最大尝试次数，允许设备向 RADIUS 服务器发出的实时计费请求没有得到响应的次数超过指定的最大值时切断用户连接。

目前 RADIUS 不支持对 FTP 用户进行计费。

表1-15 配置 RADIUS 计费服务器及相关参数

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
配置主RADIUS计费服务器	**primary accounting** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **vpn-instance** *vpn-instance-name*] *	二者至少选其一 缺省情况下，未配置主/从计费服务器 在同一个方案中指定的主计费服务器和从计费服务器的IP地址、端口号和VPN参数不能完全相同，并且各从计费服务器的IP地址、端口号和VPN参数也不能完全相同
配置从RADIUS计费服务器	**secondary accounting** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **vpn-instance** *vpn-instance-name*] *	
（可选）设置允许发起实时计费请求的最大尝试次数	**retry realtime-accounting** *retry-times*	缺省情况下，允许发起实时计费请求的最大尝试次数为5

6. 配置RADIUS报文的共享密钥

RADIUS 客户端与 RADIUS 服务器使用 MD5 算法并在共享密钥的参与下生成验证字，接受方根据收到报文中的验证字来判断对方报文的合法性。只有在共享密钥一致的情况下，彼此才能接收对方发来的报文并作出响应。

由于设备优先采用配置 RADIUS 认证/计费服务器时指定的报文共享密钥，因此，本配置中指定的 RADIUS 报文共享密钥仅在配置 RADIUS 认证/计费服务器时未指定相应密钥的情况下使用。

表1-16 配置 RADIUS 报文的共享密钥

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
配置RADIUS报文的共享密钥	**key** { **accounting** | **authentication** } { **cipher** | **simple** } *string*	缺省情况下，无共享密钥 必须保证设备上设置的共享密钥与RADIUS服务器上的完全一致

7. 配置RADIUS方案所属的VPN

该配置用于为 RADIUS 方案下的所有 RADIUS 服务器统一指定所属的 VPN。RADIUS 服务器所属的 VPN 也可以在配置 RADIUS 服务器的时候单独指定，且被优先使用。未单独指定所属 VPN 的服务器，则属于所在 RADIUS 方案所属的 VPN。

表1-17 配置 RADIUS 方案所属的 VPN

表1-18 操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
配置RADIUS方案所属的VPN	**vpn-instance** *vpn-instance-name*	缺省情况下，RADIUS方案属于公网

8. 配置发送给RADIUS服务器的用户名格式和数据统计单位

接入用户通常以“*userid@isp-name*”的格式命名，“@”后面的部分为 ISP 域名，设备通过该域名决定将用户归于哪个 ISP 域。由于有些较早期的 RADIUS 服务器不能接受携带有 ISP 域名的用户名，因此就需要设备首先将用户名中携带的 ISP 域名去除后再传送给该类 RADIUS 服务器。通过设置发送给 RADIUS 服务器的用户名格式，就可以选择发送 RADIUS 服务器的用户名中是否要携带 ISP 域名，以及是否保持用户输入的原始用户名格式。

设备通过发送计费报文，向 RADIUS 服务器报告在线用户的数据流量统计值，该值的单位可配，为保证 RADIUS 服务器计费的准确性，设备上设置的发送给 RADIUS 服务器的数据流或者数据包的单位应与 RADUIS 服务器上的流量统计单位保持一致。

需要注意的是，如果要在两个乃至两个以上的 ISP 域中引用相同的 RADIUS 方案，建议设置该 RADIUS 方案允许用户名中携带 ISP 域名，使得 RADIUS 服务器端可以根据 ISP 域名来区分不同的用户。

表1-19 配置发送给 RADIUS 服务器用户名格式和数据统计单位

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
设置发送给RADIUS服务器的用户名格式	**user-name-format** { **keep-original** | **with-domain** | **without-domain** }	缺省情况下，设备发送给RADIUS服务器的用户名携带有ISP域名

操作	命令	说明
设置发送给RADIUS服务器的数据流或者数据包的单位	**data-flow-format { data { byte | giga-byte | kilo-byte | mega-byte } | packet { giga-packet | kilo-packet | mega-packet | one-packet } } ***	可选 缺省情况下，数据流的单位为**byte**，数据包的单位为**one-packet**

9. 配置发送RADIUS报文的最大尝试次数

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。如果设备在应答超时定时器规定的时长内（由**timer response-timeout**命令配置）没有收到RADIUS服务器的响应，则设备有必要向RADIUS服务器重传RADIUS请求报文。如果发送RADIUS请求报文的累计次数已达到指定的最大尝试次数而RADIUS服务器仍旧没有响应，则设备将尝试与其它服务器通信，如果不存在状态为**active**的服务器，则认为本次认证或计费失败。关于RADIUS服务器状态的相关内容，请参见“1.3.2 10. 配置RADIUS服务器的状态”。

表1-20 配置发送 RADIUS 报文的最大尝试次数

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
设置发送RADIUS报文的最大尝试次数	**retry** *retry-times*	缺省情况下，发送RADIUS报文的最大尝试次数为3次

10. 配置RADIUS服务器的状态

RADIUS 方案中各服务器的状态（**active**、**block**）决定了设备向哪个服务器发送请求报文，以及设备在与当前服务器通信中断的情况下，如何转而与另外一个服务器进行交互。在实际组网环境中，可指定一个主 RADIUS 服务器和多个从 RADIUS 服务器，由从服务器作为主服务器的备份。通常情况下，设备上主从服务器的切换遵从以下原则：

- 当主服务器状态为 **active** 时，设备首先尝试与主服务器通信，若主服务器不可达，设备更改主服务器的状态为 **block**，并启动该服务器的 **quiet** 定时器，然后按照从服务器的配置先后顺序依次查找状态为 **active** 的从服务器进行认证或者计费。如果状态为 **active** 的从服务器也不可达，则将该从服务器的状态置为 **block**，同时启动该服务器的 **quiet** 定时器，并继续查找状态为 **active** 的从服务器。当服务器的 **quiet** 定时器超时，或者手动将服务器状态置为 **active** 时，该服务器将恢复为 **active** 状态。在一次认证或计费过程中，如果设备在尝试与从服务器通信时，之前已经查找过的服务器状态由 **block** 恢复为 **active**，则设备并不会立即恢复与该服务器的通信，而是继续查找从服务器。如果所有已配置的服务器都不可达，则认为本次认证或计费失败。
- 如果在认证或计费过程中删除了当前正在使用的服务器，则设备在与该服务器通信超时后，将会立即从主服务器开始依次查找状态为 **active** 的服务器并与之进行通信。
- 当主/从服务器的状态均为 **block** 时，设备不会与任何服务器进行通信。
- 只要存在状态为 **active** 的服务器，设备就仅与状态为 **active** 的服务器通信，即使该服务器不可达，设备也不会尝试与状态为 **block** 的服务器通信。

- 一旦服务器状态满足自动切换的条件，则所有 RADIUS 方案视图下该服务器的状态都会相应地变化。
- 将认证服务器的状态由 **active** 修改为 **block** 时，若该服务器引用了 RADIUS 服务器探测模板，则关闭对该服务器的探测功能；反之，将认证服务器的状态由 **block** 更改为 **active** 时，若该服务器引用了一个已存在的 RADIUS 服务器探测模板，则开启对该服务器的探测功能。

缺省情况下，设备将配置了 IP 地址的各 RADIUS 服务器的状态均置为 **active**，认为所有的服务器均处于正常工作状态，但有些情况下用户可能需要通过以下配置手工改变 RADIUS 服务器的当前状态。例如，已知某服务器故障，为避免设备认为其 **active** 而进行无意义的尝试，可暂时将该服务器状态手工置为 **block**。

表1-21 配置 RADIUS 服务器的状态

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
设置主RADIUS认证服务器的状态	**state primary authentication** { **active** | **block** }	四者可选其一 缺省情况下，RADIUS方案中配置的RADIUS服务器的状态均为**active** 设置的服务器状态不能被保存在配置文件中，可通过**display radius scheme**命令查看。设备重启后，各服务器状态将恢复为缺省状态**active**
设置主RADIUS计费服务器的状态	**state primary accounting** { **active** | **block** }	
设置从RADIUS认证服务器的状态	**state secondary authentication** [*ip-address* [*port-number* | **vpn-instance** *vpn-instance-name*] *] { **active** | **block** }	
设置从RADIUS计费服务器的状态	**state secondary accounting** [*ip-address* [*port-number* | **vpn-instance** *vpn-instance-name*] *] { **active** | **block** }	

11. 配置发送RADIUS报文使用的源地址

RADIUS 服务器上通过 IP 地址来标识接入设备，并根据收到的 RADIUS 报文的源 IP 地址是否与服务器所管理的接入设备的 IP 地址匹配，来决定是否处理来自该接入设备的认证或计费请求。若 RADIUS 服务器收到的 RADIUS 认证或计费报文的源地址在所管理的接入设备 IP 地址范围内，则会进行后续的认证或计费处理，否则直接丢弃该报文。因此，为保证认证和计费报文可被服务器正常接收并处理，接入设备上发送 RADIUS 报文使用的源地址必须与 RADIUS 服务器上指定的接入设备的 IP 地址保持一致。

通常，该地址为接入设备上与 RADIUS 服务器路由可达的接口 IP 地址，但在一些特殊的组网环境中，例如在接入设备使用 VRRP（Virtual Router Redundancy Protocol，虚拟路由器冗余协议）进行双机热备应用时，可以将该地址指定为 VRRP 上行链路所在备份组的虚拟 IP 地址。

设备发送 RADIUS 报文时，根据以下顺序查找使用的源地址：

(1) 若当前所使用的 RADIUS 方案中配置了发送 RADIUS 报文使用源地址，则使用该地址。

(2) 否则，根据当前使用的服务器所属的 VPN 查找系统视图下通过 **radius nas-ip** 命令配置的私网源地址，对于公网服务器则直接查找该命令配置的公网源地址。

(3) 若系统视图下没有配置相应的源地址，则使用通过路由查找到的报文出接口地址。

此配置可以在系统视图和 RADIUS 方案视图下进行，系统视图下的配置将对所有 RADIUS 方案生效，RADIUS 方案视图下的配置仅对本方案有效，并且具有高于前者的优先级。

表1-22 为所有 RADIUS 方案配置发送 RADIUS 报文使用的源地址

操作	命令	说明
进入系统视图	**system-view**	-
设置设备发送RADIUS报文使用的源地址	**radius nas-ip** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]	缺省情况下，未指定源地址，即以发送报文的接口地址作为源地址

表1-23 为 RADIUS 方案配置发送 RADIUS 报文使用的源地址

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
设置设备发送RADIUS报文使用的源地址	**nas-ip** { *ipv4-address* | **ipv6** *ipv6-address* }	缺省情况下，使用系统视图下由命令**radius nas-ip**指定的源地址，若系统视图下未指定源地址，则使用发送RADIUS报文的接口地址

12. 配置RADIUS服务器的定时器

在与 RADIUS 服务器交互的过程中，设备上可启动的定时器包括以下几种：

- 服务器响应超时定时器（**response-timeout**）：如果在 RADIUS 请求报文发送出去一段时间后，设备还没有得到 RADIUS 服务器的响应，则有必要重传 RADIUS 请求报文，以保证用户尽可能地获得 RADIUS 服务，这段时间被称为 RADIUS 服务器响应超时时间。
- 服务器恢复激活状态定时器（**quiet**）：当服务器不可达时，设备将该服务器的状态置为 **block**，并开启超时定时器，在设定的一定时间间隔之后，再将该服务器的状态恢复为 **active**。这段时间被称为 RADIUS 服务器恢复激活状态时长。
- 实时计费间隔定时器（**realtime-accounting**）：为了对用户实施实时计费，有必要定期向服务器发送实时计费更新报文，通过设置实时计费的时间间隔，设备会每隔设定的时间向 RADIUS 服务器发送一次在线用户的计费信息。

设置 RADIUS 服务器的定时器时，请遵循以下配置原则：

- 要根据配置的从服务器数量合理设置发送 RADIUS 报文的最大尝试次数和 RADIUS 服务器响应超时时间，避免因为超时重传时间过长，在主服务器不可达时，出现设备在尝试与从服务器通信的过程中接入模块（例如 Telnet 模块）的客户端连接已超时的现象。但是，有些接入模块的客户端的连接超时时间较短，在配置的从服务器较多的情况下，即使将报文重传次数和 RADIUS 服务器响应超时时间设置的很小，也可能会出现上述客户端超时的现象，并导致初次认证或计费失败。这种情况下，由于设备会将不可达服务器的状态设置为 **block**，在下次认证或计费时设备就不会尝试与这些状态为 **block** 的服务器通信，一定程度上缩短了查找可达服务器的时间，因此用户再次尝试认证或计费就可以成功。

- 要根据配置的从服务器数量合理设置服务器恢复激活状态的时间。如果服务器恢复激活状态时间设置得过短，就会出现设备反复尝试与状态 **active** 但实际不可达的服务器通信而导致的认证或计费频繁失败的问题；如果服务器恢复激活状态设置的过长，则会导致已经恢复激活状态的服务器暂时不能为用户提供认证或计费服务。
- 实时计费间隔的取值对设备和 RADIUS 服务器的性能有一定的相关性要求，取值小，会增加网络中的数据流量，对设备和 RADIUS 服务器的性能要求就高；取值大，会影响计费的准确性。因此要结合网络的实际情况合理设置计费间隔的大小，一般情况下，建议当用户量比较大（大于等于 1000）时，尽量把该间隔的值设置得大一些。

表1-24 设置 RADIUS 服务器的定时器

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
设置RADIUS服务器响应超时时间	**timer response-timeout** *seconds*	缺省情况下，RADIUS服务器响应超时定时器为3秒
设置服务器恢复激活状态的时间	**timer quiet** *minutes*	缺省情况下，服务器恢复激活状态前需要等待5分钟
设置实时计费间隔	**timer realtime-accounting** *minutes*	缺省情况下，实时计费间隔为12分钟

13. 配置RADIUS的accounting-on功能

使能了 accounting-on 功能后，设备会在重启后主动向 RADIUS 服务器发送 accounting-on 报文来告知自己已经重启，并要求 RADIUS 服务器停止计费且强制通过本设备上线的用户下线。该功能可用于解决设备重启后，重启前的原在线用户因被 RADIUS 服务器认为仍然在线而短时间内无法再次登录的问题。若设备发送 accounting-on 报文后 RADIUS 服务器无响应，则会在按照一定的时间间隔（**interval** *seconds*）尝试重发几次（**send** *send-times*）。分布式设备单板重启时，accounting-on 功能的实现需要和 H3C IMC 网管系统配合使用。

表1-25 配置 RADIUS 的 accounting-on 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
配置accounting-on功能	**accounting-on enable** [**interval** *seconds* | **send** *send-times*] *	缺省情况下，accounting-on功能处于关闭状态

14. 配置RADIUS安全策略服务器的IP地址

通过配置 RADIUS 安全策略服务器的 IP 地址，接入设备可以验证 IMC（Intelligent Management Center，智能管理中心）服务器发送给设备的控制报文的合法性。当接入设备收到 IMC 服务器的控制报文时，若该控制报文的源 IP 地址不是指定的安全策略服务器的 IP 地址，则接入设备认为其非

法而丢弃。若 IMC 的配置平台、认证服务器以及安全策略服务器的 IP 地址相同，则不需要在接入设备上配置 RADIUS 安全策略服务器的 IP 地址。

安全策略服务器是 H3C EAD（Endpoint Admission Defense，端点准入防御）方案中的管理与控制中心。通常，若要支持完整的 EAD 功能，建议在接入设备上通过本配置指定两个 RADIUS 安全策略服务器的 IP 地址，分别为 IMC 安全策略服务器的 IP 地址和 IMC 配置平台的 IP 地址。

表1-26 设置 RADIUS 的安全策略服务器

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
设置RADIUS安全策略服务器的IP地址	**security-policy-server** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]	缺省情况下，未指定RADIUS安全策略服务器 一个RADIUS方案中最多可以配置8个安全策略服务器IP地址

15. 配置RADIUS Attribute 25 的CAR参数解析功能

RADIUS 的 25 号属性为 class 属性，该属性由 RADIUS 服务器下发给设备，但 RFC 中并未定义具体的用途，仅规定了设备需要将服务器下发的 class 属性再原封不动地携带在计费请求报文中发送给服务器即可，同时 RFC 并未要求设备必须对该属性进行解析。目前，某些 RADIUS 服务器利用 class 属性来对用户下发 CAR 参数，为了支持这种应用，可以通过本特性来控制设备是否将 RADIUS 25 号属性解析为 CAR 参数，解析出的 CAR 参数可被用来进行基于用户的流量监管控制。

表1-27 配置 RADIUS Attribute 25 的 CAR 参数解析功能

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
开启RADIUS Attribute 25的CAR参数解析功能	**attribute 25 car**	缺省情况下，RADIUS Attribute 25的CAR参数解析功能处于关闭状态

16. 配置RADIUS Attribute 15 的检查方式

RADIUS 15 号属性为Login-Service属性，该属性携带在Access-Accept报文中，由RADIUS服务器下发给设备，表示认证用户的业务类型，例如属性值 0 表示Telnet业务。设备检查用户登录时采用的业务类型与服务器下发的Login-Service属性所指定的业务类型是否一致，如果不一致则用户认证失败 。由于RFC中并未定义SSH、FTP和Terminal这三种业务的Login-Service属性值，因此设备无法针对SSH、FTP、Terminal用户进行业务类型一致性检查，为了支持对这三种业务类型的检查，H3C为Login-Service属性定义了 表 1-28 所示的扩展取值。

表1-28 扩展的 Login-Service 属性值

属性值	描述
50	用户的业务类型为SSH
51	用户的业务类型为FTP
52	用户的业务类型为Terminal

可以通过配置设备对 RADIUS 15 号属性的检查方式，控制设备是否使用扩展的 Login-Service 属性值对用户进行业务类型一致性检查。

- 严格检查方式：设备使用标准属性值和扩展属性值对用户业务类型进行检查，对于 SSH、FTP、Terminal 用户，当 RADIUS 服务器下发的 Login-Service 属性值为对应的扩展取值时才能够通过认证。
- 松散检查方式：设备使用标准属性值对用户业务类型进行检查，对于 SSH、FTP、Terminal 用户，在 RADIUS 服务器下发的 Login-Service 属性值为 0（表示用户业务类型为 Telnet）时才能够通过认证。

由于某些 RADIUS 服务器不支持自定义的属性，无法下发扩展的 Login-Service 属性，若要使用这类 RADIUS 服务器对 SSH、FTP、Terminal 用户进行认证，建议设备上对 RADIUS 15 号属性值采用松散检查方式。

表1-29 配置 RADIUS Attribute 15 的检查方式

操作	命令	说明
进入系统视图	**system-view**	-
进入RADIUS方案视图	**radius scheme** *radius-scheme-name*	-
配置RADIUS Attribute 15的检查方式	**attribute 15 check-mode** { **loose** | **strict** }	缺省情况下，RADIUS Attribute 15 的检查方式为strict方式

17. 配置RADIUS的Trap功能

开启相应的 RADIUS Trap 功能后，RADIUS 模块会生成告警信息，用于报告该模块的重要事件：

- 当 NAS 向 RADIUS 服务器发送计费或认证请求没有收到响应时，会重传请求，当重传次数达到最大传送次数时仍然没有收到响应时，NAS 认为该服务器不可达，并发送表示 RADIUS 服务器不可达的告警信息。
- 当 **timer quiet** 定时器设定的时间到达后，NAS 将服务器的状态置为激活状态并发送表示 RADIUS 服务器可达的告警信息。
- 当 NAS 发现认证失败次数与认证请求总数的百分比超过阈值时，会发送表示认证失败次数超过阈值的告警信息。

生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

表1-30 配置 RADIUS 的 Trap 功能

操作	命令	说明
进入系统视图	**system-view**	-
开启RADIUS的Trap功能	**snmp-agent trap enable radius [accounting-server-down | authentication-error-threshold | authentication-server-down | accounting-server-up | authentication-server-up] ***	缺省情况下，所有类型的RADIUS Trap功能均处于开启状态

18. RADIUS显示和维护

完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 RADIUS 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** 命令可以清除相关统计信息。

表1-31 RADIUS 显示和维护

操作	命令
显示所有或指定RADIUS方案的配置信息	**display radius scheme** [*radius-scheme-name*]
显示RADIUS报文的统计信息	**display radius statistics**
清除RADIUS协议的统计信息	**reset radius statistics**

1.3.3 配置HWTACACS方案

1. HWTACACS配置任务简介

表1-32 HWTACACS 配置任务简介

配置任务	说明	详细配置
创建HWTACACS方案	必选	1.3.3 2.
配置HWTACACS认证服务器	必选	1.3.3 3.
配置HWTACACS授权服务器	可选	1.3.3 4.
配置HWTACACS计费服务器	可选	1.3.3 5.
配置HWTACACS报文的共享密钥	可选	1.3.3 6.
配置HWTACACS方案所属的VPN	可选	1.3.3 7.
配置发送给HWTACACS服务器的用户名格式和数据统计单位	可选	1.3.3 8.
配置发送HWTACACS报文使用的源地址	可选	1.3.3 9.
配置HWTACACS服务器的定时器	可选	1.3.3 10.
HWTACACS显示和维护	可选	1.3.3 11.

2. 创建HWTACACS方案

在进行 HWTACACS 的其它相关配置之前，必须先创建 HWTACACS 方案并进入其视图。系统最多支持配置 16 个 HWTACACS 方案。一个 HWTACACS 方案可以同时被多个 ISP 域引用。

表1-33 创建 HWTACACS 方案

操作	命令	说明
进入系统视图	**system-view**	-
创建HWTACACS方案并进入其视图	**hwtacacs scheme** *hwtacacs-scheme-name*	缺省情况下，未定义HWTACACS方案

3. 配置HWTACACS认证服务器

通过在 HWTACACS 方案中配置 HWTACACS 认证服务器，指定设备对用户进行 HWTACACS 认证时与哪个服务器进行通信。

一个 HWTACACS 方案中最多允许配置一个主认证服务器和 16 个从认证服务器。当主服务器不可达时，设备根据从服务器的配置顺序由先到后查找状态为 **active** 的从服务器并与之交互。建议在不需要备份的情况下，只配置主 HWTACACS 认证服务器即可。

在实际组网环境中，可以指定一台服务器既作为某个 HWTACACS 方案的主认证服务器，又作为另一个 HWTACACS 方案的从认证服务器。

表1-34 配置 HWTACACS 认证服务器

操作	命令	说明
进入系统视图	**system-view**	-
进入HWTACACS方案视图	**hwtacacs scheme** *hwtacacs-scheme-name*	-
配置主HWTACACS认证服务器	**primary authentication** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection** | **vpn-instance** *vpn-instance-name*] *	二者至少选其一 缺省情况下，未配置主/从认证服务器 在同一个方案中指定的主认证服务器和从认证服务器的IP地址、端口号和VPN参数不能完全相同，并且各从认证服务器的IP地址、端口号和VPN参数也不能完全相同
配置从HWTACACS认证服务器	**secondary authentication** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection** | **vpn-instance** *vpn-instance-name*] *	

4. 配置HWTACACS授权服务器

通过在 HWTACACS 方案中配置 HWTACACS 授权服务器，指定设备对用户进行 HWTACACS 授权时与哪个服务器进行通信。

一个 HWTACACS 方案中最多允许配置一个主授权服务器和 16 个从授权服务器。当主服务器不可达时，设备根据从服务器的配置顺序由先到后查找状态为 **active** 的从服务器并与之交互。建议在不需要备份的情况下，只配置主 HWTACACS 授权服务器即可。

在实际组网环境中，可以指定一台服务器既作为某个 HWTACACS 方案的主授权服务器，又作为另一个 HWTACACS 方案的从授权服务器。

表1-35 配置 HWTACACS 授权服务器

操作	命令	说明
进入系统视图	**system-view**	-
进入HWTACACS方案视图	**hwtacacs scheme** *hwtacacs-scheme-name*	-
设置主HWTACACS授权服务器	**primary authorization** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection** | **vpn-instance** *vpn-instance-name*] *	二者至少选其一 缺省情况下，未配置主/从授权服务器 在同一个方案中指定的主授权服务器和从授权服务器的IP地址、端口号和VPN参数不能完全相同，并且各从授权服务器的IP地址、端口号和VPN参数也不能完全相同
设置从HWTACACS授权服务器	**secondary authorization** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection** | **vpn-instance** *vpn-instance-name*] *	

5. 配置HWTACACS计费服务器

通过在 HWTACACS 方案中配置 HWTACACS 计费服务器，指定设备对用户进行 HWTACACS 计费时与哪个服务器进行通信。

一个 HWTACACS 方案中最多允许配置一个主计费服务器和 16 个从计费服务器。当主服务器不可达时，设备根据从服务器的配置顺序由先到后查找状态为 **active** 的从服务器并与之交互。建议在不需要备份的情况下，只配置主 HWTACACS 计费服务器即可。

在实际组网环境中，可以指定一台服务器既作为某个 HWTACACS 方案的主计费服务器，又作为另一个 HWTACACS 方案的从计费服务器。

目前 HWTACACS 不支持对 FTP 用户进行计费。

表1-36 配置 HWTACACS 计费服务器

操作	命令	说明
进入系统视图	**system-view**	-
进入HWTACACS方案视图	**hwtacacs scheme** *hwtacacs-scheme-name*	-
设置HWTACACS主计费服务器	**primary accounting** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection** | **vpn-instance** *vpn-instance-name*] **	二者至少选其一 缺省情况下，未配置主/从计费服务器 在同一个方案中指定的主计费服务器和从计费服务器的IP地址、端口号和VPN参数不能完全相同，并且各从计费服务器的IP地址、端口号和VPN参数也不能完全相同
设置HWTACACS从计费服务器	**secondary accounting** { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection** | **vpn-instance** *vpn-instance-name*] *	

6. 配置HWTACACS报文的共享密钥

HWTACACS 客户端与 HWTACACS 服务器使用 MD5 算法并在共享密钥的参与下加密 HWTACACS 报文。只有在密钥一致的情况下，彼此才能接收对方发来的报文并作出响应。

表1-37 配置 HWTACACS 报文的共享密钥

操作	命令	说明
进入系统视图	**system-view**	-
进入HWTACACS方案视图	**hwtacacs scheme** *hwtacacs-scheme-name*	-
配置HWTACACS认证、授权、计费报文的共享密钥	**key** { **accounting** | **authentication** | **authorization** } { **cipher** | **simple** } *string*	缺省情况下，无共享密钥 必须保证设备上设置的共享密钥与HWTACACS服务器上的完全一致

7. 配置HWTACACS方案所属的VPN

该配置用于指定 HWTACACS 方案所属的 VPN，即为 HWTACACS 方案下的所有 HWTACACS 服务器统一指定所属的 VPN。HWTACACS 服务器所属的 VPN 也可以在配置 HWTACACS 服务器的时候单独指定，且被优先使用。未单独指定所属 VPN 的服务器，则属于所在 HWTACACS 方案所属的 VPN。

表1-38 配置 HWTACACS 方案所属的 VPN

表1-39 操作	命令	说明
进入系统视图	**system-view**	-
进入HWTACACS方案视图	**hwtacacs scheme** *hwtacacs-scheme-name*	-
配置HWTACACS方案所属的VPN	**vpn-instance** *vpn-instance-name*	缺省情况下，HWTACACS方案属于公网

8. 配置发送给HWTACACS服务器的用户名格式和数据统计单位

接入用户通常以“*userid@isp-name*”的格式命名，“@”后面的部分为 ISP 域名，设备通过该域名决定将用户归于哪个 ISP 域的。由于有些 HWTACACS 服务器不能接受携带有 ISP 域名的用户名，因此就需要设备首先将用户名中携带的 ISP 域名去除后再传送给该类 HWTACACS 服务器。通过设置发送给 HWTACACS 服务器的用户名格式，就可以选择发送 HWTACACS 服务器的用户名中是否要携带 ISP 域名。

设备通过发送计费报文，向 HWTACACS 服务器报告在线用户的数据流量统计值，该值的单位可配，为保证 HWTACACS 服务器计费的准确性，设备上设置的发送给 HWTACACS 服务器的数据流或者数据包的单位应与 HWTACACS 服务器上的流量统计单位保持一致。

需要注意的是，如果要在两个乃至两个以上的 ISP 域中引用相同的 HWTACACS 方案，建议设置该 HWTACACS 方案允许用户名中携带 ISP 域名，使得 HWTACACS 服务器端可以根据 ISP 域名来区分不同的用户。

表1-40 配置发送给 HWTACACS 服务器的用户名格式和数据统计单位

操作	命令	说明
进入系统视图	**system-view**	-
进入HWTACACS方案视图	**hwtacacs scheme** *hwtacacs-scheme-name*	-
设置发送给HWTACACS服务器的用户名格式	**user-name-format** { **keep-original** | **with-domain** | **without-domain** }	缺省情况下，发往HWTACACS服务器的用户名带域名
设置发送给HWTACACS服务器的数据流或者数据包的单位	**data-flow-format** { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } } *	可选 缺省情况下，数据流的单位为**byte**，数据包的单位为**one-packet**

9. 配置发送HWTACACS报文使用的源地址

HWTACACS 服务器上通过 IP 地址来标识接入设备，并根据收到的 HWTACACS 报文的源 IP 地址是否与服务器所管理的接入设备的 IP 地址匹配，来决定是否处理来自该接入设备的认证、授权或计费请求。若 HWTACACS 服务器收到的 HWTACACS 认证或计费报文的源地址在所管理的接入设备 IP 地址范围内，则会进行后续的认证或计费处理，否则直接丢弃该报文。因此，为保证认证、授权和计费报文可被服务器正常接收并处理，接入设备上发送 HWTACACS 报文使用的源地址必须与 HWTACACS 服务器上指定的接入设备的 IP 地址保持一致。

通常，该地址为接入设备上与 HWTACACS 服务器路由可达的接口 IP 地址，但在一些特殊的组网环境中，例如在接入设备使用 VRRP 进行双机热备应用时，可以将该地址指定为 VRRP 上行链路所在备份组的虚拟 IP 地址。

设备发送 HWTACACS 报文时，根据以下顺序查找使用的源地址：

- 若当前所使用的 HWTACACS 方案中配置了发送 HWTACACS 报文使用源地址，则使用该地址。
- 否则，根据当前使用的服务器所属的 VPN 查找系统视图下通过 **hwtacacs nas-ip** 命令配置的私网源地址，对于公网服务器则直接查找该命令配置的公网源地址。
- 若系统视图下没有配置相应的源地址，则使用通过路由查找到的报文出接口地址。

此配置可以在系统视图和 HWTACACS 方案视图下进行，系统视图下的配置将对所有 HWTACACS 方案生效，HWTACACS 方案视图下的配置仅对本方案有效，并且具有高于前者的优先级。

表1-41 为所有 HWTACACS 方案配置发送 HWTACACS 报文使用的源地址

操作	命令	说明
进入系统视图	**system-view**	-
设置设备发送HWTACACS报文使用的源地址	**hwtacacs nas-ip** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]	缺省情况下，未指定源地址，即以发送报文的接口地址作为源地址

表1-42 为 HWTACACS 方案配置发送 HWTACACS 报文使用的源地址

操作	命令	说明
进入系统视图	**system-view**	-
进入HWTACACS方案视图	**hwtacacs scheme** *hwtacacs-scheme-name*	-
设置设备发送HWTACACS报文使用的源地址	**nas-ip** { *ipv4-address* | **ipv6** *ipv6-address* }	缺省情况下，使用系统视图下由命令**hwtacacs nas-ip**指定的源地址，若系统视图下未指定源地址，则使用发送HWTACACS报文的接口地址

10. 配置HWTACACS服务器的定时器

在与 HWTACACS 服务器交互的过程中，设备上可启动的定时器包括以下几种：

- 服务器响应超时定时器（**response-timeout**）：如果在 HWTACACS 请求报文传送出去一段时间后，设备还没有得到 HWTACACS 服务器的响应，则会将该服务器的状态置为 **block**，并向下一个 HWTACACS 服务器发起请求，以保证用户尽可能得到 HWTACACS 服务，这段时间被称为 HWTACACS 服务器响应超时时长。
- 实时计费间隔定时器（**realtime-accounting**）：为了对用户实施实时计费，有必要定期向服务器发送用户的实时计费信息，通过设置实时计费的时间间隔，设备会每隔设定的时间向 HWTACACS 服务器发送一次在线用户的计费信息。
- 服务器恢复激活状态定时器（**quiet**）：当服务器不可达时，设备将该服务器的状态置为 **block**，并开启超时定时器，在设定的一定时间间隔之后，再将该服务器的状态恢复为 **active**。这段时间被称为服务器恢复激活状态时长。

关于 HWTACACS 服务器的状态：

HWTACACS 方案中各服务器的状态（**active**、**block**）决定了设备向哪个服务器发送请求报文，以及设备在与当前服务器通信中断的情况下，如何转而与另外一个服务器进行交互。在实际组网环境中，可指定一个主 HWTACACS 服务器和多个从 HWTACACS 服务器，由从服务器作为主服务器的备份。通常情况下，设备上主从服务器的切换遵从以下原则：

- 当主服务器状态为 **active** 时，设备首先尝试与主服务器通信，若主服务器不可达，设备更改主服务器的状态为 **block**，并启动该服务器的 **quiet** 定时器，然后按照从服务器的配置先后顺序依次查找状态为 **active** 的从服务器进行认证或者计费。如果状态为 **active** 的从服务器也不可达，则将该从服务器的状态置为 **block**，同时启动该服务器的 **quiet** 定时器，并继续查找状态为 **active** 的从服务器。当服务器的 **quiet** 定时器超时，该服务器将恢复为 **active** 状态。在一次认证或计费过程中，如果设备在尝试与从服务器通信时，之前已经查找过的服务器状态由 **block** 恢复为 **active**，则设备并不会立即恢复与该服务器的通信，而是继续查找从服务器。如果所有已配置的服务器都不可达，则认为本次认证或计费失败。
- 如果在认证或计费过程中删除了当前正在使用的服务器，则设备在与该服务器通信超时后，将会立即从主服务器开始依次查找状态为 **active** 的服务器并与之进行通信。
- 当主/从服务器的状态均为 **block** 时，设备不会与任何服务器进行通信。
- 只要存在状态为 **active** 的服务器，设备就仅与状态为 **active** 的服务器通信，即使该服务器不可达，设备也不会尝试与状态为 **block** 的服务器通信。

- 一旦服务器状态满足自动切换的条件，则所有 HWTACACS 方案视图下该服务器的状态都会相应地变化。

需要注意的是，实时计费间隔的取值对设备和 HWTACACS 服务器的性能有一定的相关性要求，取值越小，对设备和 HWTACACS 服务器的性能要求越高。建议当用户量比较大（大于等于 1000）时，尽量把该间隔的值设置得大一些。

表1-43 配置 HWTACACS 服务器的定时器

操作	命令	说明
进入系统视图	**system-view**	-
进入HWTACACS方案视图	**hwtacacs scheme** *hwtacacs-scheme-name*	-
设置HWTACACS服务器响应超时时间	**timer response-timeout** *seconds*	缺省情况下，服务器响应超时时间为5秒
设置实时计费的时间间隔	**timer realtime-accounting** *minutes*	缺省情况下，实时计费间隔为12分钟
设置服务器恢复激活状态的时间	**timer quiet** *minutes*	缺省情况下，服务器恢复激活状态前需要等待5分钟

11. HWTACACS显示和维护

完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 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** 命令可以清除相关统计信息。

表1-44 HWTACACS 显示和维护

操作	命令
查看所有或指定HWTACACS方案的配置信息或统计信息	**display hwtacacs scheme** [*hwtacacs-server-name* [**statistics**]]
清除HWTACACS协议的统计信息	**reset hwtacacs statistics** { **accounting** | **all** | **authentication** | **authorization** }

1.3.4 配置LDAP方案

1. LDAP配置任务简介

表1-45 LDAP 配置任务简介

配置任务		说明	详细配置
配置LDAP服务器	创建LDAP服务器	必选	1.3.4 2.
	配置LDAP服务器IP地址	必选	1.3.4 3.
	配置LDAP版本号	可选	1.3.4 4.
	配置LDAP服务器的连接超时时间	可选	1.3.4 5.

配置任务		说明	详细配置
	配置具有管理员权限的用户属性	必选	1.3.4 6.
	配置LDAP用户属性参数	必选	1.3.4 7.
创建LDAP方案		必选	1.3.4 8.
指定LDAP认证服务器		必选	1.3.4 9.
LDAP显示和维护		可选	1.3.4 10.

2. 创建LDAP服务器

表1-46 创建 LDAP 服务器

操作	命令	说明
进入系统视图	**system-view**	-
创建LDAP服务器并进入LDAP服务器视图	**ldap server** *server-name*	缺省情况下，不存在LDAP服务器

3. 配置LDAP服务器IP地址

表1-47 配置 LDAP 服务器 IP 地址

操作	命令	说明
进入系统视图	**system-view**	-
进入LDAP服务器视图	**ldap server** *server-name*	-
配置LDAP服务器IP地址	{ **ip** *ip-address* **| ipv6** *ipv6-address* } [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]	缺省情况下，未配置LDAP服务器IP地址 LDAP服务器视图下仅能同时存在一个IPv4地址类型的LDAP服务器或一个IPv6地址类型的LDAP服务器。多次配置，后配置的生效

4. 配置LDAP版本号

配置 LDAP 认证中所支持的 LDAP 协议的版本号，目前设备支持 LDAPv2 和 LDAPv3 两个协议版本。设备上配置的 LDAP 版本号需要与服务器支持的版本号保持一致。

表1-48 配置 LDAP 版本号

操作	命令	说明
进入系统视图	**system-view**	-
进入LDAP服务器视图	**ldap server** *server-name*	-
配置LDAP版本号	**protocol-version** { **v2** | **v3** }	缺省情况下，LDAP版本号为LDAPv3 Microsoft的LDAP服务器只支持LDAPv3版本

5. 配置LDAP服务器的连接超时时间

设备向 LDAP 服务器发送绑定请求、查询请求，如果经过指定的时间后未收到 LDAP 服务器的回应，则认为本次认证、授权请求超时。若使用的 ISP 域中配置了备份的认证、授权方案，则设备会继续尝试进行其他方式的认证、授权处理，否则本次认证、授权失败。

表1-49 配置 LDAP 服务器的连接超时时间

操作	命令	说明
进入系统视图	**system-view**	-
进入LDAP服务器视图	**ldap server** *server-name*	-
配置LDAP服务器的连接超时时间	**server-timeout** *time-interval*	缺省情况下，LDAP服务器的连接超时时间为10秒

6. 配置具有管理员权限的用户属性

配置 LDAP 认证过程中绑定服务器所使用的用户 DN 和用户密码，该用户具有管理员权限。

表1-50 配置具有管理员权限的用户属性

操作	命令	说明
进入系统视图	**system-view**	-
进入LDAP服务器视图	**ldap server** *server-name*	-
配置具有管理员权限的用户DN	**login-dn** *dn-string*	缺省情况下，未配置具有管理员权限的用户DN 配置的管理员权限的用户DN必须与LDAP服务器上管理员的DN一致
配置具有管理员权限的用户密码	**login-password** { **ciper** | **simple** } *password*	缺省情况下，未配置具有管理权限的用户密码

7. 配置LDAP用户属性参数

要对用户进行身份认证，就需要以用户 DN 及密码为参数与 LDAP 服务器进行绑定，因此需要首先从 LDAP 服务器获取用户 DN。LDAP 提供了一套 DN 查询机制，在与 LDAP 服务器建立连接的基础上，按照一定的查询策略向服务器发送查询请求。该查询策略由设备上指定的 LDAP 用户属性定义，具体包括以下几项：

- 用户 DN 查询的起始节点（search-base-dn）
- 用户 DN 查询的范围（search-scope）
- 用户名称属性（user-name-attribute）
- 用户名称格式（user-name-format）
- 用户对象类型（user-object-class）

LDAP 服务器上的目录结构可能具有很深的层次，如果从根目录进行用户 DN 的查找，耗费的时间将会较长，因此必须配置用户查找的起始点 DN，以提高查找效率。

表1-51 配置 LDAP 用户属性参数

操作	命令	说明
进入系统视图	**system-view**	-
进入LDAP服务器视图	**ldap server** *server-name*	-
配置用户查询的起始DN	**search-base-dn** *base-dn*	缺省情况下，未指定用户查询的起始DN
（可选）配置用户查询的范围	**search-scope** { **all-level** | **single-level** }	缺省情况下，用户查询的范围为**all-level**
（可选）配置用户查询的用户名属性	**user-parameters user-name-attribute** { *name-attribute* | **cn** | **uid** }	缺省情况下，用户查询的用户名属性为**cn**
（可选）配置用户查询的用户名格式	**user-parameters user-name-format** { **with-domain** | **without-domain** }	缺省情况下，用户查询的用户名格式为**without-domain**
（可选）配置用户查询的自定义用户对象类型	**user-parameters user-object-class** *object-class-name*	缺省情况下，未指定自定义用户对象类型，根据使用的LDAP服务器的类型使用各服务器缺省的用户对象类型

8. 创建LDAP方案

系统最多支持配置 16 个 LDAP 方案。一个 LDAP 方案可以同时被多个 ISP 域引用。

表1-52 创建 LDAP 方案

操作	命令	说明
进入系统视图	**system-view**	-
创建LDAP方案并进入其视图	**ldap scheme** *ldap-scheme-name*	缺省情况下，未定义LDAP方案

9. 指定LDAP认证服务器

表1-53 指定 LDAP 认证服务器

操作	命令	说明
进入系统视图	**system-view**	-
进入LDAP方案视图	**ldap scheme** *ldap-scheme-name*	-
指定LDAP认证服务器	**authentication-server** *server-name*	缺省情况下，未指定LDAP认证服务器

10. LDAP显示和维护

完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 LDAP 的运行情况，通过查看显示信息验证配置的效果。

表1-54 LDAP 显示和维护

操作	命令
查看所有或指定LDAP方案的配置信息	**display ldap scheme** [*scheme-name*]

1.4 在ISP域中配置实现AAA的方法

通过在 ISP 域视图下引用预先配置的认证、授权、计费方案来实现对用户的认证、授权和计费。如果用户所属的 ISP 域下未应用任何认证、授权、计费方法，系统将使用缺省的认证、授权、计费方法，分别为本地认证、本地授权和本地计费。

1.4.1 配置准备

- 若采用本地认证方案，则请先完成本地用户的配置。有关本地用户的配置请参见“1.3.1 配置本地用户”。
- 若采用远端认证、授权或计费方案，则请提前创建RADIUS方案、HWTACACS方案或LDAP方案。有关RADIUS方案的配置请参见“1.3.2 配置RADIUS方案”。有关HWTACACS方案的配置请参见“1.3.3 配置HWTACACS方案”。有关LDAP方案的配置请参见“1.3.4 配置LDAP方案”。

1.4.2 创建ISP域

在多 ISP 的应用环境中，不同 ISP 域的用户有可能接入同一台设备。而且各 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）有可能不相同，因此有必要通过设置 ISP 域把它们区分开，并为每个 ISP 域单独配置一套 AAA 方法及 ISP 域的相关属性。

对于设备来说，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，包括一个系统缺省存在的名称为 system 的 ISP 域。如果某个用户在登录时没有提供 ISP 域名，系统将把它归于缺省的 ISP 域。系统缺省的 ISP 域可以手工修改为一个指定的 ISP 域。

用户认证时，设备将按照如下先后顺序为其选择认证域：接入模块指定的认证域-->用户名中指定的 ISP 域-->系统缺省的 ISP 域。其中，仅部分接入模块支持指定认证域，例如 802.1X、Portal、MAC 地址认证。如果根据以上原则决定的认证域在设备上不存在，但设备上为未知域名的用户指定了 ISP 域，则最终使用该指定的 ISP 域认证，否则，用户将无法认证。

需要注意的是：

- 一个 ISP 域被配置为缺省的 ISP 域后，将不能够被删除，必须首先使用命令 **undo domain default enable** 将其修改为非缺省 ISP 域，然后才可以被删除。
- 系统缺省存在的 system 域只能被修改，不能被删除。
- 一个 ISP 域被配置为未知域名的用户的 ISP 域后不能够被删除，必须首先使用命令 **undo domain if-unknown** 将其修改为非未知域名的用户的域，然后才可以被删除。

表1-55 创建 ISP 域

操作	命令	说明
进入系统视图	**system-view**	-
创建ISP域并进入其视图	**domain** *isp-name*	缺省情况下，系统存在一个名称为system的ISP域
返回系统视图	**quit**	-
（可选）手工配置缺省的ISP域	**domain default enable** *isp-name*	缺省情况下，系统缺省的ISP域为system
（可选）配置未知域名的用户的ISP域	**domain if-unknown** *isp-domain-name*	缺省情况下，没有为未知域名的用户指定ISP域

1.4.3 配置ISP域的属性

一个 ISP 域中可配置以下属性，这些属性对于接入该域的所有用户均生效：

- ISP 域的状态：通过域的状态（active、block）控制是否允许该域中的用户请求网络服务。
- 一个 ISP 域内可容纳的接入用户数：通过该属性限制接入域的用户数，使属于当前域的用户获得可靠的性能保障。
- ISP 域的用户授权属性：用户认证成功之后，对于 IP 地址池授权属性，用户优先采用服务器下发的属性值，其次采用 ISP 域下配置的属性值；对于用户闲置切断授权属性，用户优先采用 ISP 域下配置的属性值，其次采用服务器下发的属性值。
  - 用户闲置切断时间：用户上线后，设备会周期性检测用户的流量，若 ISP 域内某用户在指定的闲置检测时间内产生的流量小于指定的数据流量，则会被强制下线。
  - IP 地址池：认证成功的 PPP 用户可以从指定的地址池中分配得到一个 IP 地址。
- 设备上传到服务器的用户在线时间中保留闲置切断时间：当用户异常下线时，上传到服务器上的用户在线时间中包含了一定的闲置切断检测间隔或用户在线探测间隔（该在线探测机制目前仅 Portal 认证支持），此时服务器上记录的用户时长将大于用户实际在线时长。

表1-56 配置 ISP 域的属性

操作	命令	说明
进入系统视图	**system-view**	-
进入ISP域视图	**domain** *isp-name*	-
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**，即允许任何属于该域的用户请求网络服务
设置当前ISP域可容纳接入用户数	**access-limit enable** *max-user-number*	缺省情况下，不对当前ISP域可容纳的接入用户数作限制
设置当前ISP域下的用户授权属性	**authorization-attribute** { **idle-cut** *minute* [*flow*] | **ip-pool** *pool-name* }	未对当前ISP域下的用户设置任何授权属性，其中用户闲置切换功能处于关闭状态

操作	命令	说明
设置设备上传到服务器的用户在线时间中保留闲置切断时间	**session-time include-idle-time**	缺省情况下，设备上传到服务器的用户在线时间中扣除闲置切断时间

1.4.4 配置ISP域的AAA认证方法

配置 ISP 域的 AAA 认证方法时，需要注意的是：

- 当选择了 RADIUS 协议的认证方案以及非 RADIUS 协议的授权方案时，AAA 只接受 RADIUS 服务器的认证结果，RADIUS 授权的信息虽然在认证成功回应的报文中携带，但在认证回应的处理流程中不会被处理。
- 目前，远程方案只能支持对名称为 level-*n* 的用户角色之间的切换进行认证。当使用 HWTACACS 方案进行用户角色切换认证时，系统使用用户输入的用户角色切换用户名进行角色切换认证；当使用 RADIUS 方案进行用户角色切换认证时，系统使用 RADIUS 服务器上配置的“$enab*n*$”形式的用户名进行用户角色切换认证，其中 *n* 为用户希望切换到的用户角色 level-*n* 中的 *n*。
- FIPS 模式下不支持 **none** 认证方法。

配置前的准备工作：

(1) 确定要配置的接入方式或者服务类型。AAA 可以对不同的接入方式和服务类型配置不同的认证方案。

(2) 确定是否为所有的接入方式或服务类型配置缺省的认证方法，缺省的认证方法对所有接入用户都起作用，但其优先级低于为具体接入方式或服务类型配置的认证方法。

表1-57 配置 ISP 域的 AAA 认证方法

操作	命令	说明
进入系统视图	**system-view**	-
进入ISP域视图	**domain** *isp-name*	-
为当前ISP域配置缺省的认证方法	**authentication default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }	缺省情况下，当前ISP域的缺省认证方法为**local**
为lan-access用户配置认证方法	**authentication lan-access** { **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	缺省情况下，lan-access用户采用缺省的认证方法
为login用户配置认证方法	**authentication login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }	缺省情况下，login用户采用缺省的认证方法

操作	命令	说明
为Portal用户配置认证方法	**authentication portal** { **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	缺省情况下，Portal用户采用缺省的认证方法
为PPP用户配置认证方法	**authentication ppp** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }	缺省情况下，PPP用户采用缺省的认证方法
配置用户角色切换认证方法	**authentication super** { **hwtacacs-scheme** *hwtacacs-scheme-name* | **radius-scheme** *radius-scheme-name* } *	缺省情况下，用户角色切换认证采用缺省的认证方法

1.4.5 配置ISP域的AAA授权方法

配置 ISP 域的 AAA 授权方法时，需要注意的是：

- 目前设备暂不支持使用 LDAP 进行授权。
- 在一个 ISP 域中，只有 RADIUS 授权方法和 RADIUS 认证方法引用了相同的 RADIUS 方案，RADIUS 授权才能生效。若 RADIUS 授权未生效或者 RADIUS 授权失败，则用户认证会失败。
- FIPS 模式下不支持 **none** 授权方法。

配置前的准备工作：

(1) 确定要配置的接入方式或者服务类型，AAA 可以按照不同的接入方式和服务类型进行 AAA 授权的配置。

(2) 确定是否为所有的接入方式或服务类型配置缺省的授权方法，缺省的授权方法对所有接入用户都起作用，但其优先级低于为具体接入方式或服务类型配置的授权方法。

表1-58 配置 ISP 域的 AAA 授权方法

操作	命令	说明
进入系统视图	**system-view**	-
进入ISP域视图	**domain** *isp-name*	-
为当前ISP域配置缺省的授权方法	**authorization default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }	缺省情况下，当前ISP域的缺省授权方法为**local**
配置命令行授权方法	**authorization command** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local** [**none**] | **local** [**none**] | **none** }	缺省情况下，命令行授权采用缺省的授权方法
为lan-access用户配置授权方法	**authorization lan-access** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	缺省情况下，lan-access用户采用缺省的授权方法

操作	命令	说明
为login用户配置授权方法	**authorization login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }	缺省情况下，login用户采用缺省的授权方法
为Portal用户配置授权方法	**authorization portal** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	缺省情况下，Portal用户采用缺省的授权方法
为PPP用户配置授权方法	**authorization ppp** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }	缺省情况下，PPP用户采用缺省的授权方法

1.4.6 配置ISP域的AAA计费方法

配置 ISP 域的 AAA 认证方法时，需要注意的是：

- 不支持对 FTP 类型 login 用户进行计费。
- 本地计费仅用于配合本地用户视图下的 **access-limit** 命令来实现对本地用户连接数的限制功能。
- FIPS 模式下不支持 **none** 计费方法。

配置前的准备工作：

(1) 确定要配置的接入方式或者服务类型，AAA 可以按照不同的接入方式和服务类型进行 AAA 计费的配置。

(2) 确定是否为所有的接入方式或服务类型配置缺省的计费方法，缺省的计费方法对所有接入用户都起作用，但其优先级低于为具体接入方式或服务类型配置的计费方法。

表1-59 配置 ISP 域的 AAA 计费方法

操作	命令	说明
进入系统视图	**system-view**	-
进入ISP域视图	**domain** *isp-name*	-
为当前ISP域配置缺省的计费方法	**accounting default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }	缺省情况下，当前ISP域的缺省计费方法为**local**
配置命令行计费方法	**accounting command hwtacacs-scheme** *hwtacacs-scheme-name*	缺省情况下，命令行计费采用缺省的计费方法
为lan-access用户配置计费方法	**accounting lan-access** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	缺省情况下，lan-access用户采用缺省的计费方法

操作	命令	说明
为login用户配置计费方法	**accounting login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }	缺省情况下，login用户采用缺省的计费方法
为Portal用户配置授权方法	**accounting portal** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	缺省情况下，Portal用户采用缺省的计费方法
为PPP用户配置计费方法	**accounting ppp** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }	缺省情况下，PPP用户采用缺省的计费方法

1.5 配置RADIUS session control功能

H3C 的 IMC RADIUS 服务器使用 session control 报文向设备发送授权信息的动态修改请求以及断开连接请求。使能 RADIUS session control 功能后，设备会打开知名 UDP 端口 1812 来监听并接收 RADIUS 服务器发送的 session control 报文。

需要注意的是，该功能仅能和 H3C 的 IMC RADIUS 服务器配合使用。

表1-60 使能 RADIUS session control 服务

操作	命令	说明
进入系统视图	**system-view**	-
使能RADIUS session control功能	**radius session-control enable**	缺省情况下，RADIUS session control功能处于关闭状态

1.6 配置RADIUS DAE服务器功能

DAE（Dynamic Authorization Extensions，动态授权扩展）协议是 RFC 5176 中定义的 RADIUS 协议的一个扩展，它用于强制认证用户下线，或者更改在线用户授权信息。DAE 采用客户端/服务器通信模式，由 DAE 客户端和 DAE 服务器组成。

- DAE 客户端：用于发起 DAE 请求，通常驻留在一个 RADIUS 服务器上，也可以为一个单独的实体。
- DAE 服务器：用于接收并响应 DAE 客户端的 DAE 请求，通常为一个 NAS（Network Access Server，网络接入服务器）设备。

DAE 报文包括以下两种类型：

- DMs（Disconnect Messages）：用于强制用户下线。DAE 客户端通过向 NAS 设备发送 DM 请求报文，请求 NAS 设备按照指定的匹配条件强制用户下线。

- COA（Change of Authorization）Messages：用于更改用户授权信息。DAE 客户端通过向 NAS 设备发送 COA 请求报文，请求 NAS 设备按照指定的匹配条件更改用户授权信息。

在设备上使能 RADIUS DAE 服务后，设备将作为 RADIUS DAE 服务器在指定的 UDP 端口监听指定的 RADIUS DAE 客户端发送的 DAE 请求消息，然后根据请求消息进行用户授权信息的修改或断开用户连接，并向 RADIUS DAE 客户端发送 DAE 应答消息。

表1-61 配置 RADIUS DAE 服务器

操作	命令	说明
进入系统视图	**system-view**	-
使能RADIUS DAE服务，并进入RADIUS DAE服务器视图	**radius dynamic-author server**	缺省情况下，RADIUS DAE服务处于关闭状态
指定RADIUS DAE客户端	**client** { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**key** { **cipher** | **simple** } *string* | **vpn-instance** *vpn-instance-name*] *	缺省情况下，未指定RADIUS DAE客户端
指定RADIUS DAE服务端口	**port** *port-number*	缺省情况下，RADIUS DAE服务端口为3799

1.7 配置RADIUS报文的DSCP优先级

DSCP 携带在 IP 报文中的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。通过本命令可以指定设备发送的 RADIUS 报文携带的 DSCP 优先级的取值。配置 DSCP 优先级的取值越大，RADIUS 报文的优先级越高。

表1-62 配置 RADIUS 报文的 DSCP 优先级

操作	命令	说明
进入系统视图	**system-view**	-
配置RADIUS报文的DSCP优先级	**radius** [**ipv6**] **dscp** *dscp-value*	缺省情况下，RADIUS报文的DSCP优先级为0

1.8 限制同时在线的最大用户连接数

通过配置同时在线的最大用户连接数，可以限制采用指定登录方式（FTP、SSH、Telnet 等）同时接入设备的在线用户数。

该配置对于通过任何一种认证方式（none、password 或者 scheme）接入设备的用户都生效。

表1-63 配置同时在线的最大用户连接数

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
配置同时在线的最大用户连接数	非FIPS模式下： **aaa session-limit** { **ftp** | **http** | **https** | **ssh** | **telnet** } *max-sessions* FIPS模式下： **aaa session-limit** { **https** | **ssh** } *max-sessions*	缺省情况下，各类型用户的最大用户连接数为32

1.9 AAA显示和维护

完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 AAA 的运行情况，通过查看显示信息验证配置的效果。

表1-64 AAA 显示和维护

操作	命令
显示所有或指定ISP域的配置信息	**display domain** [*isp-name*]

1.10 AAA典型配置举例

1.10.1 SSH用户的RADIUS认证和授权配置

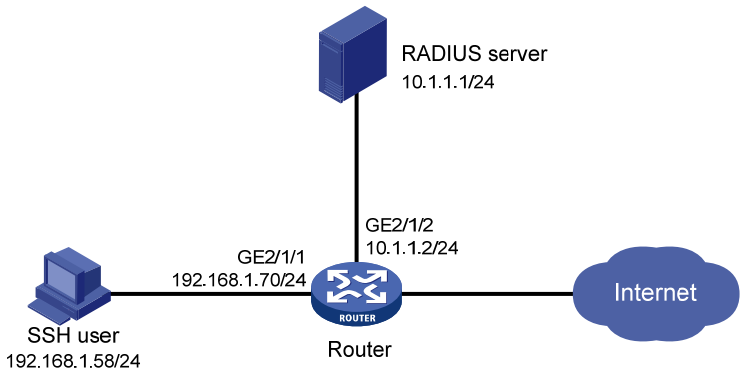
1. 组网需求

如 图 1-11 所示，SSH用户主机与Router直接相连，Router与一台RADIUS服务器相连，需要实现使用RADIUS服务器对登录Router的SSH用户进行认证和授权。

- 由一台 IMC 服务器（IP 地址为 10.1.1.1/24）担当认证/授权 RADIUS 服务器的职责；
- Router 与 RADIUS 服务器交互报文时使用的共享密钥为 expert，认证/授权、计费的端口号分别为 1812 和 1813；
- Router 向 RADIUS 服务器发送的用户名携带域名；
- SSH用户登录Router时使用RADIUS服务器上配置的用户名hello@bbb以及密码进行认证，认证通过后具有缺省的用户角色 network-operator。

2. 组网图

图1-11 SSH 用户 RADIUS 认证/授权配置组网图



3. 配置步骤

(1) 配置 RADIUS 服务器（IMC PLAT 5.0）

说明

下面以 IMC 为例（使用 IMC 版本为：IMC PLAT 5.0(E0101)、IMC UAM 5.0(E0101)），说明 RADIUS 服务器的基本配置。

增加接入设备。

登录进入 IMC 管理平台，选择“业务”页签，单击导航树中的[接入业务/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击“增加”按钮，进入增加接入设备页面。

- 设置与 Router 交互报文时使用的认证、计费共享密钥为“expert”；
- 设置认证及计费的端口号分别为“1812”和“1813”；
- 选择业务类型为“设备管理业务”；
- 选择接入设备类型为“H3C”；
- 选择或手工增加接入设备，添加 IP 地址为 10.1.1.2 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

说明

添加的接入设备 IP 地址要与 Router 发送 RADIUS 报文的源地址保持一致。缺省情况下，设备发送 RADIUS 报文的源地址是发送 RADIUS 报文的接口 IP 地址。

- 若设备上通过命令 **nas-ip** 或者 **radius nas-ip** 指定了发送 RADIUS 报文的源地址，则此处的接入设备 IP 地址就需要修改并与指定源地址保持一致。
- 若设备使用缺省的发送 RADIUS 报文的源地址，例如，本例中为接口 GigabitEthernet2/1/2 的 IP 地址 10.1.1.2，则此处接入设备 IP 地址就选择 10.1.1.2。

图1-12 增加接入设备

增加设备管理用户。

选择“用户”页签，单击导航树中的[接入用户视图/设备管理用户]菜单项，进入设备管理用户列表页面，在该页面中单击<增加>按钮，进入增加设备管理用户页面。

- 输入用户名“hello@bbb”和密码；
- 选择服务类型为“SSH”；
- 添加所管理设备的 IP 地址，IP 地址范围为“10.1.1.0～10.1.1.255”；
- 单击<确定>按钮完成操作。

说明

添加的所管理设备的 IP 地址范围要包含添加的接入设备的 IP 地址。

图1-13 增加设备管理用户

(2) 配置 Router

配置接口 GigabitEthernet2/1/1 的 IP 地址，SSH 用户将通过该地址连接 Router。

```
<Router> system-view
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] ip address 192.168.1.70 255.255.255.0
[Router-GigabitEthernet2/1/1] quit
```

配置接口 GigabitEthernet2/1/2 的 IP 地址，Router 将通过该地址与服务器通信。

```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] ip address 10.1.1.2 255.255.255.0
[Router-GigabitEthernet2/1/2] quit
```

创建本地 RSA 及 DSA 密钥对。

```
[Router] public-key local create rsa
[Router] public-key local create dsa
```

使能 SSH 服务器功能。

```
[Router] ssh server enable
```

设置 SSH 用户登录用户线的认证方式为 AAA 认证。

```
[Router] line vty 0 63
[Router-line-vty0-63] authentication-mode scheme
[Router-line-vty0-63] quit
```

使能缺省用户角色授权功能，使得认证通过后的 SSH 用户具有缺省的用户角色 network-operator。

```
[Router] role default-role enable
```

创建 RADIUS 方案 rad。

```
[Router] radius scheme rad
```

配置主认证服务器的 IP 地址为 10.1.1.1，认证端口号为 1812。

```
[Router-radius-rad] primary authentication 10.1.1.1 1812
```

配置与认证服务器交互报文时的共享密钥为明文 expert。

```
[Router-radius-rad] key authentication simple expert
```

配置向 RADIUS 服务器发送的用户名要携带域名。

```
[Router-radius-rad] user-name-format with-domain
[Router-radius-rad] quit
```

创建 ISP 域 bbb，为 login 用户配置 AAA 认证方法为 RADIUS 认证/授权、不计费。由于 RADIUS 服务器的授权信息是随认证应答报文发给 RADIUS 客户端的，所以必须保证认证和授权方案相同。

```
[Router] domain bbb
[Router-isp-bbb] authentication login radius-scheme rad
[Router-isp-bbb] authorization login radius-scheme rad
[Router-isp-bbb] accounting login none
[Router-isp-bbb] quit
```

4. 验证配置

用户向 Router 发起 SSH 连接，按照提示输入用户名 hello@bbb 及正确的密码后，可成功登录 Router，并具有用户角色 network-operator 所拥有的命令行执行权限。

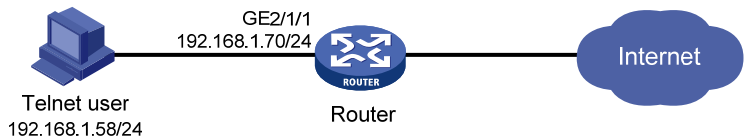
1.10.2 SSH用户的本地认证和授权配置

1. 组网需求

如 图 1-14 所示，配置Router实现对登录Router的SSH用户进行本地认证和授权，并授权该用户具有用户角色network-admin。

2. 组网图

图1-14 SSH 用户本地认证/授权配置组网图



3. 配置步骤

配置接口 GigabitEthernet2/1/1 的 IP 地址，SSH 用户将通过该地址连接 Router。

```
<Router> system-view
```

```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] ip address 192.168.1.70 255.255.255.0
[Router-GigabitEthernet2/1/1] quit
```

创建本地 RSA 及 DSA 密钥对。

```
[Router] public-key local create rsa
[Router] public-key local create dsa
```

使能 SSH 服务器功能。

```
[Router] ssh server enable
```

设置 SSH 用户登录用户线的认证方式为 AAA 认证。

```
[Router] line vty 0 63
[Router-line-vty0-63] authentication-mode scheme
[Router-line-vty0-63] quit
```

创建设备管理类本地用户 ssh。

```
[Router] local-user ssh class manage
```

配置该本地用户的服务类型为 SSH。

```
[Router-luser-manage-ssh] service-type ssh
```

配置该本地用户密码为明文 123456TESTplat&!。(若是 FIPS 模式下，只能使用交互式方式设置)

```
[Router-luser-manage-ssh] password simple 123456TESTplat&!
```

配置该本地用户的授权用户角色为 network-admin

```
[Router-luser-manage-ssh] authorization-attribute user-role network-admin
[Router-luser-manage-ssh] quit
```

创建 ISP 域 bbb，为 login 用户配置 AAA 认证方法为本地认证和本地授权。

```
[Router] domain bbb
[Router-isp-bbb] authentication login local
[Router-isp-bbb] authorization login local
[Router-isp-bbb] quit
```

4. 验证配置

用户向 Router 发起 SSH 连接，按照提示输入用户名 ssh@bbb 及正确的密码后，可成功登录 Router，并具有用户角色 network-admin 所拥有的命令行执行权限。

1.10.3 SSH用户的HWTACACS认证、授权、计费配置

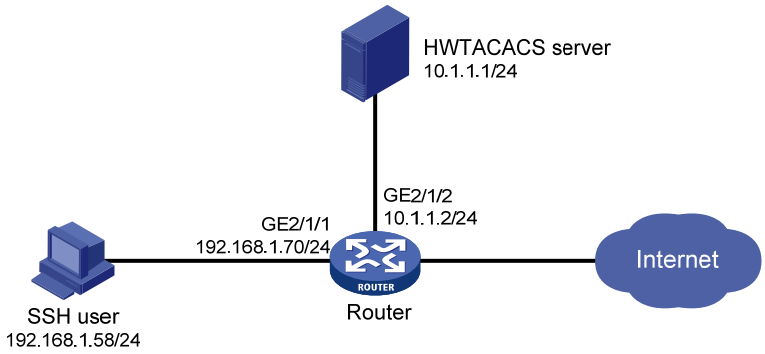
1. 组网需求

如 图 1-15 所示，配置Router实现使用HWTACACS服务器对登录Router的SSH用户进行认证、授权、计费。

- 由一台 HWTACACS 服务器担当认证、授权、计费服务器的职责，服务器 IP 地址为 10.1.1.1/24。
- Router 与认证、授权、计费 HWTACACS 服务器交互报文时的共享密钥均为 expert，向 HWTACACS 服务器发送的用户名不带域名。
- 认证通过后的 SSH 用户具有缺省的用户角色 network-operator。

2. 组网图

图1-15 SSH 用户 HWTACACS 认证、授权和计费配置组网图



3. 配置步骤

(1) 配置 HWTACACS 服务器

在 HWTACACS 服务器上设置与 Router 交互报文时的共享密钥为 expert；添加 SSH 用户名及密码。（略）

(2) 配置 Router

创建 HWTACACS 方案 hwtac。

```
<Router> system-view
[Router] hwtacacs scheme hwtac
```

配置主认证服务器的 IP 地址为 10.1.1.1，认证端口号为 49。

```
[Router-hwtacacs-hwtac] primary authentication 10.1.1.1 49
```

配置主授权服务器的 IP 地址为 10.1.1.1，授权端口号为 49。

```
[Router-hwtacacs-hwtac] primary authorization 10.1.1.1 49
```

配置主计费服务器的 IP 地址为 10.1.1.1，计费端口号为 49。

```
[Router-hwtacacs-hwtac] primary accounting 10.1.1.1 49
```

配置与认证、授权、计费服务器交互报文时的共享密钥均为明文 expert。

```
[Router-hwtacacs-hwtac] key authentication simple expert
[Router-hwtacacs-hwtac] key authorization simple expert
[Router-hwtacacs-hwtac] key accounting simple expert
```

配置向 HWTACACS 服务器发送的用户名不携带域名。

```
[Router-hwtacacs-hwtac] user-name-format without-domain
[Router-hwtacacs-hwtac] quit
```

创建 ISP 域 bbb，为 login 用户配置 AAA 认证方法为 HWTACACS 认证/授权/计费。

```
[Router] domain bbb
[Router-isp-bbb] authentication login hwtacacs-scheme hwtac
[Router-isp-bbb] authorization login hwtacacs-scheme hwtac
[Router-isp-bbb] accounting login hwtacacs-scheme hwtac
[Router-isp-bbb] quit
```

创建本地 RSA 及 DSA 密钥对。

```
[Router] public-key local create rsa
```

```
[Router] public-key local create dsa
```
使能 SSH 服务器功能。
```
[Router] ssh server enable
```
使能缺省用户角色授权功能，使得认证通过后的 SSH 用户具有缺省的用户角色 network-operator。
```
[Router] role default-role enable
```
设置 SSH 用户登录用户线的认证方式为 AAA 认证。
```
[Router] line vty 0 63
[Router-line-vty0-63] authentication-mode scheme
[Router-line-vty0-63] quit
```
配置接口 GigabitEthernet2/1/1 的 IP 地址，SSH 用户将通过该地址连接 Router。
```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] ip address 192.168.1.70 255.255.255.0
[Router-GigabitEthernet2/1/1] quit
```
配置接口 GigabitEthernet2/1/2 的 IP 地址，Router 将通过该地址与服务器通信。
```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] ip address 10.1.1.2 255.255.255.0
[Router-GigabitEthernet2/1/2] quit
```

4. 验证配置

用户向 Router 发起 SSH 连接，按照提示输入正确用户名及密码后，可成功登录 Router，并具有用户角色 network-operator 所拥有的命令行执行权限。

1.10.4 SSH用户的LDAP认证配置

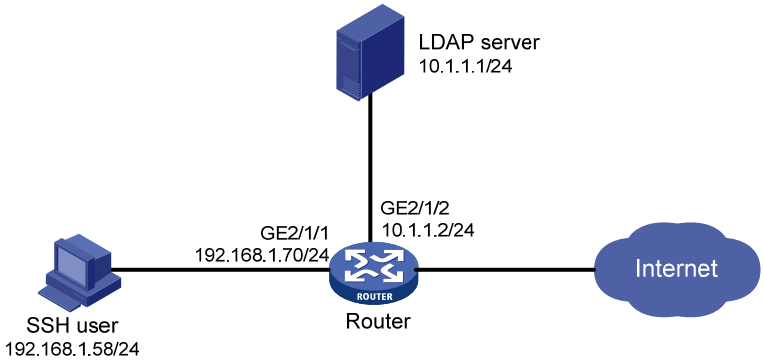
1. 组网需求

如 图 1-16 所示，配置Router实现使用LDAP服务器对登录Router的SSH用户进行认证，且认证通过后具有缺省的用户角色network-operator。

- 一台 LDAP 认证服务器与 Router 相连，服务器 IP 地址为 10.1.1.1，服务器域名为 ldap.com。
- 在 LDAP 服务器上设置管理员 administrator 的密码为 admin!123456。
- 在 LDAP 服务器上添加用户名为 aaa 的用户，密码为 ldap!123456。

2. 组网图

图1-16 SSH 用户 LDAP 认证配置组网图



3. 配置步骤

(1) 配置 LDAP 服务器

说明

本文以 Microsoft Windows 2003 Server 的 Active Directory 为例，说明该例中 LDAP 服务器的基本配置。

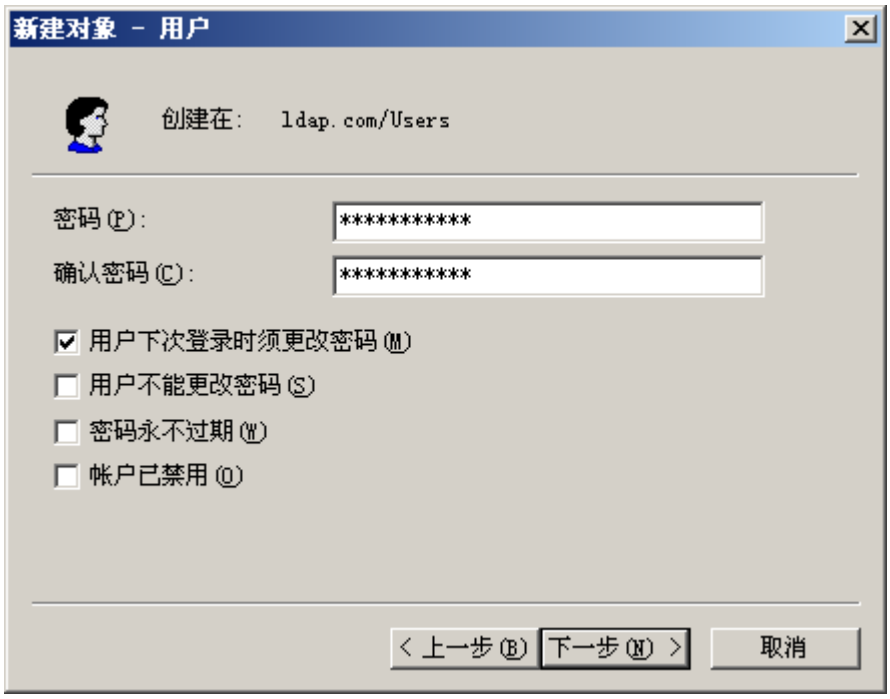
添加用户 aaa。

- 在 LDAP 服务器上，选择[开始/管理工具]中的[Active Directory 用户和计算机]，打开 Active Directory 用户管理界面；
- 在 Active Directory 用户管理界面的左侧导航树中，点击 ldap.com 节点下的“Users”按钮；
- 选择[操作/新建/用户]，打开[新建对象-用户]对话框；
- 在对话框中输入用户登录名 aaa，并单击<下一步>按钮。

图1-17 新建用户 aaa

- 在弹出的对话框的“密码”区域框内输入用户密码 ldap!123456，并单击<下一步>按钮。用户帐户的其它属性（密码的更改方式、密码的生存方式、是否禁用帐户）请根据实际情况选择配置，图中仅为示例。

图1-18 设置用户密码

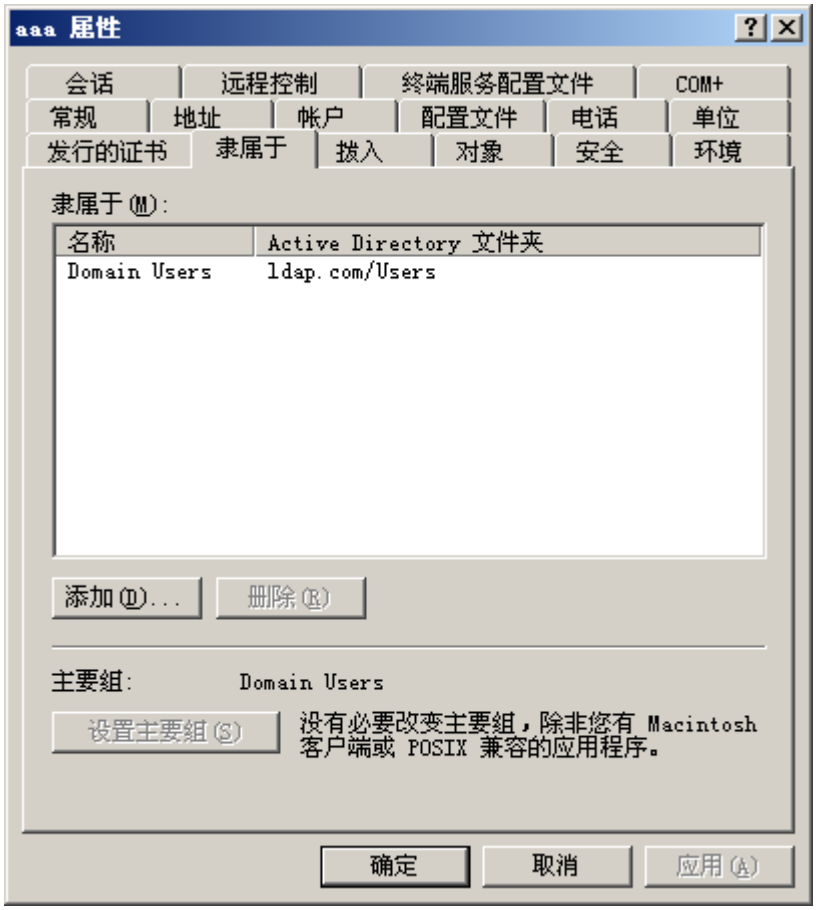


- 单击<完成>按钮，创建新用户 aaa。

将用户 aaa 加入 Users 组。

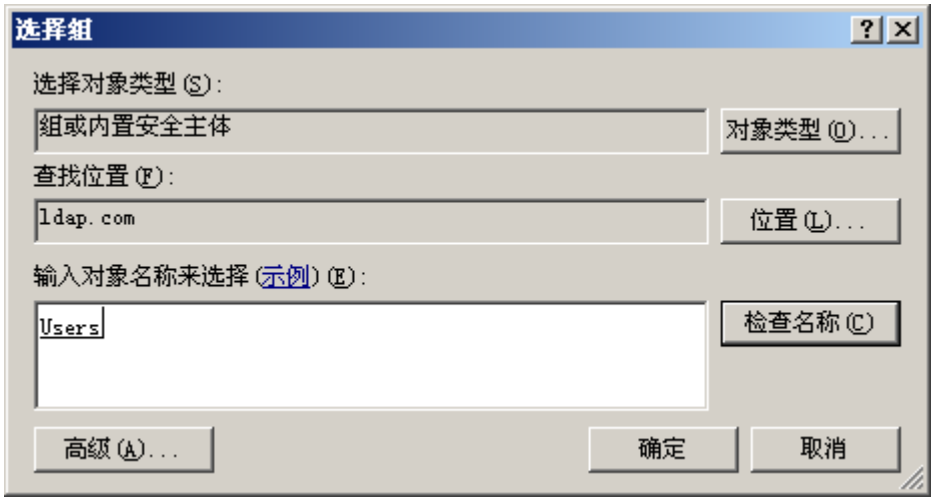
- 在 Active Directory 用户管理界面的左侧导航树中，点击 ldap.com 节点下的“Users”按钮；
- 在右侧的 Users 信息框中右键单击用户 aaa，选择“属性”项；
- 在弹出的[aaa 属性]对话框中选择“隶属于”页签，并单击<添加(D)...>按钮。

图1-19 修改用户属性



- 在弹出的[选择组]对话框中的可编辑区域框中输入对象名称“Users”，单击<确定>，完成用户 aaa 添加到 Users 组。

图1-20 添加用户 aaa 到用户组 Users



完成用户 aaa 的添加之后，还需要配置管理员用户 administrator 的密码为 admin!123456。

- 在右侧的 Users 信息框中右键单击管理员用户 administrator，选择“设置密码(S)...”项；
- 在弹出的密码添加对话框中设置管理员密码，详细过程略。

(2) 配置 Router

配置接口 GigabitEthernet2/1/1 的 IP 地址，SSH 用户将通过该地址连接 Router。

```
<Router> system-view
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] ip address 192.168.1.20 24
[Router-GigabitEthernet2/1/1] quit
```

配置接口 GigabitEthernet2/1/2 的 IP 地址，Router 将通过该地址与服务器通信。

```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] ip address 10.1.1.2 255.255.255.0
[Router-GigabitEthernet2/1/2] quit
```

生成本地 DSA 及 RSA 密钥对。

```
[Router] public-key local create dsa
[Router] public-key local create rsa
```

使能 SSH 服务器功能。

```
[Router] ssh server enable
```

设置 SSH 用户登录用户线的认证方式为 AAA 认证。

```
[Router] line vty 0 63
[Router-line-vty0-63] authentication-mode scheme
[Router-line-vty0-63] quit
```

使能缺省用户角色授权功能，使得认证通过后的 SSH 用户具有缺省的用户角色 network-operator。

```
[Router] role default-role enable
```

创建 LDAP 服务器。

```
[Router] ldap server ldap1
```

配置 LDAP 认证服务器的 IP 地址。

```
[Router-ldap-server-ldap1] ip 10.1.1.1
```

配置具有管理员权限的用户 DN。

```
[Router-ldap-server-ldap1] login-dn cn=administrator,cn=users,dc=ldap,dc=com
```

配置具有管理员权限的用户密码。

```
[Router-ldap-server-ldap1] login-password simple admin!123456
```

配置查询用户的起始目录。

```
[Router-ldap-server-ldap1] search-base-dn dc=ldap,dc=com
[Router-ldap-server-ldap1] quit
```

创建 LDAP 方案。

```
[Sysname] ldap scheme ldap1-shml
```

配置 LDAP 认证服务器。

```
[Sysname-ldap-ldap-shml] authentication-server ldap1
[Sysname-ldap-ldap1-shml] quit
```

创建 ISP 域 bbb，为 login 用户配置 AAA 认证方法为 LDAP 认证、不授权、不计费。

```
[Router] domain bbb
```

```
[Router-isp-bbb] authentication login ldap-scheme ldap1-shml
[Router-isp-bbb] authorization login none
[Router-isp-bbb] accounting login none
[Router-isp-bbb] quit
```

4. 验证配置

用户向 Router 发起 SSH 连接，按照提示输入用户名 *aaa*@bbb 及正确的密码 ldap!123456 后，可成功登录 Router，并具有用户角色 network-operator 所拥有的命令行执行权限。

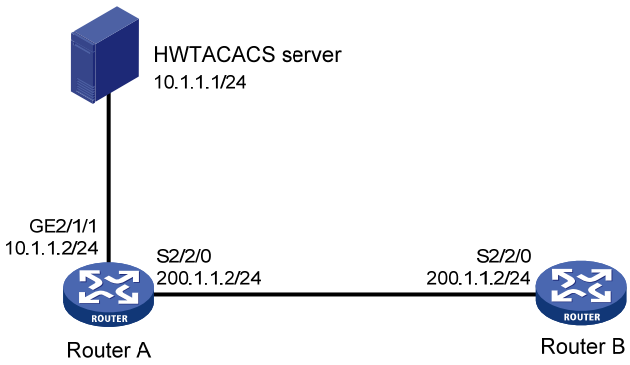
1.10.5 PPP用户的HWTACACS认证、授权、计费配置

1. 组网需求

如图 图 1-21 所示，Router A和Router B之间使用串口互连，要求Router A使用HWTACACS服务器对Router B进行PAP认证，以及使用HWTACACS服务器进行授权和计费，Router B不需要对Router A进行认证、授权和计费。

2. 组网图

图1-21 PPP 用户的 HWTACACS 认证、授权、计费组网图



3. 配置步骤

(1) 配置 HWTACACS 服务器

在 HWTACACS 服务器上设置与 Router A 交互报文时的共享密钥为 expert；添加 PPP 用户名 userb 及密码 passb，具体配置步骤略。

(2) 配置 Router A

创建 HWTACACS 方案 hwtac。

```
<RouterA> system-view
[RouterA] hwtacacs scheme hwtac
```

配置主认证、主授权、主计费服务器的 IP 地址为 10.1.1.1，认证端口号为 49，采用单连接方式。

```
[RouterA-hwtacacs-hwtac] primary authentication 10.1.1.1 49 single-connection
[RouterA-hwtacacs-hwtac] primary authorization 10.1.1.1 49 single-connection
[RouterA-hwtacacs-hwtac] primary accounting 10.1.1.1 49 single-connection
```

配置与认证、授权、计费服务器交互报文时的共享密钥均为 expert。

```
[RouterA-hwtacacs-hwtac] key authentication simple expert
[RouterA-hwtacacs-hwtac] key authorization simple expert
```

```
[RouterA-hwtacacs-hwtac] key accounting simple expert
```
配置向 HWTACACS 服务器发送的用户名不携带域名。
```
[RouterA-hwtacacs-hwtac] user-name-format without-domain
[RouterA-hwtacacs-hwtac] quit
```
创建 ISP 域 bbb，为 PPP 用户配置 AAA 认证方法为 HWTACACS 认证、授权、计费。
```
[RouterA] domain bbb
[RouterA-isp-bbb] authentication ppp hwtacacs-scheme hwtac
[RouterA-isp-bbb] authorization ppp hwtacacs-scheme hwtac
[RouterA-isp-bbb] accounting ppp hwtacacs-scheme hwtac
[RouterA-isp-bbb] quit
```
配置接口 Serial2/2/0 的封装的链路层协议为 PPP。
```
[RouterA] interface serial 2/2/0
[RouterA-Serial2/2/0] link-protocol ppp
```
配置 Router A 认证 Router B 的方式为 PAP，并使用 ISP 域 bbb 作为认证域。
```
[RouterA-Serial2/2/0] ppp authentication-mode pap domain bbb
```
配置接口的 IP 地址。
```
[RouterA-Serial2/2/0] ip address 200.1.1.1 24
```
(3) 配置 Router B

配置接口 Serial2/2/0 的封装的链路层协议为 PPP。
```
<RouterB> system-view
[RouterB] interface serial 2/2/0
[RouterB-Serial2/2/0] link-protocol ppp
```
配置 RouterB 被 Router A 以 PAP 方式认证时使用的 PAP 用户名和密码。
```
[RouterB-Serial2/2/0] ppp pap local-user userb password simple passb
```
配置接口的 IP 地址。
```
[RouterB-Serial2/2/0] ip address 200.1.1.2 24
```
4. 验证配置

以上配置完成后，通过 **display interface serial** 命令，查看接口 Serial2/1/0 的信息，发现接口的物理层和链路层的状态都是 up 状态，并且 PPP 的 LCP 和 IPCP 都是 opened 状态，说明链路的 PPP 协商已经成功，并且 Router A 和 Router B 可以互相 **ping** 通对方。

1.11 AAA常见配置错误举例

1.11.1 RADIUS认证/授权失败

1. 故障现象

用户认证/授权总是失败。

2. 故障分析

(1) 设备与 RADIUS 服务器之间存在通信故障。

(2) 用户名不是“*userid@isp-name*”的形式，或设备上没有正确配置用于认证该用户的 ISP 域。

(3) RADIUS 服务器的数据库中没有配置该用户。

(4) 用户侧输入的密码不正确。

(5) RADIUS 服务器和设备的报文共享密钥不同。

3. 处理过程

(1) 使用 **ping** 命令检查设备与 RADIUS 服务器是否可达。

(2) 使用正确形式的用户名或在设备上确保正确配置了用于该用户认证的 ISP 域。

(3) 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。

(4) 确保接入用户输入正确的密码。

(5) 检查两端的共享密钥，并确保两端一致。

1.11.2 RADIUS报文传送失败

1. 故障现象

RADIUS 报文无法传送到 RADIUS 服务器。

2. 故障分析

(1) 设备与 RADIUS 服务器之间的通信存在故障。

(2) 设备上没有设置相应的 RADIUS 服务器 IP 地址。

(3) 认证/授权和计费服务的 UDP 端口设置不正确。

(4) RADIUS 服务器的认证/授权和计费端口被其它应用程序占用。

3. 处理过程

(1) 确保线路通畅。

(2) 确保正确设置 RADIUS 服务器的 IP 地址。

(3) 确保与 RADIUS 服务器提供服务的端口号一致。

(4) 确保 RADIUS 服务器上的认证/授权和计费端口可用。

1.11.3 RADIUS计费功能异常

1. 故障现象

用户认证通过并获得授权，但是计费功能出现异常。

2. 故障分析

(1) 计费端口号设置不正确。

(2) 计费服务器和认证服务器不是同一台机器，设备却要求认证和计费功能属于同一个服务器（IP 地址相同）。

3. 处理过程

(1) 正确设置 RADIUS 计费端口号。

(2) 确保设备的认证服务器和计费服务器的设置与实际情况相同。

1.11.4 HWTACACS常见配置错误举例

HWTACACS 的常见配置错误举例与 RADIUS 基本相似，可以参考以上内容。

1.11.5 LDAP常见配置错误举例

1. 故障现象

用户认证失败。

2. 故障分析

(1) 设备与 LDAP 服务器之间存在通信故障。

(2) 配置的认证/授权服务器 IP 地址或端口号不正确。

(3) 用户名不是“*userid@isp-name*”的形式，或设备上没有正确配置用于认证该用户的 ISP 域。

(4) LDAP 服务器目录中没有配置该用户。

(5) 用户输入的密码不正确。

(6) 具有管理员权限的用户 DN 或密码没有配置。

(7) 设备上配置的用户参数（如用户名属性）与服务器上的配置不对应。

(8) 认证操作时，没有配置 LDAP 方案用户查询的起始 DN。

3. 处理过程

(1) 使用 **ping** 命令检查设备与 LDAP 服务器是否可达。

(2) 确保配置的认证服务器 IP 地址与端口号与 LDAP 服务器实际使用的 IP 地址和端口号相符。

(3) 使用正确形式的用户名或在设备上确保正确配置了用于该用户认证的 ISP 域。

(4) 检查 LDAP 服务器目录以保证该用户的配置信息确实存在。

(5) 确保输入用户密码正确。

(6) 确保配置了正确的管理员用户 DN 和密码。

(7) 确保设备上的用户参数（如用户名属性）配置与 LDAP 服务器上的配置相同。

(8) 认证操作时，确保配置了用户查询的起始 DN。

目 录

1 802.1X

说明

- 本章节主要描述了 802.1X 的相关概念及配置步骤。由于通过配置端口安全特性也可以为用户提供 802.1X 认证服务，且还可以提供 802.1X 和 MAC 地址认证的扩展和组合应用，因此在需要灵活使用以上两种认证方式的组网环境下，推荐使用端口安全特性。无特殊组网要求的情况下，无线环境中通常使用端口安全特性。在仅需要 802.1X 特性来完成接入控制的组网环境下，推荐单独使用 802.1X 特性。关于端口安全特性的详细介绍和具体配置请参见“安全配置指导”中的“端口安全”。
- 本特性仅在安装了二层交换卡的款型和 MSR3600-28/MSR 3600-51 的固定二层接口上支持。

1.1 802.1X简介

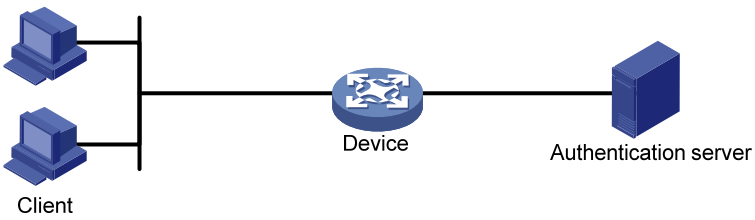
最初，提出 802.1X 协议是为解决无线局域网的网络安全问题。后来，802.1X 协议作为局域网的一种普通接入控制机制在以太网中被广泛应用，主要解决以太网内认证和安全方面的问题。

802.1X 协议是一种基于端口的网络接入控制协议，即在局域网接入设备的端口上对所接入的用户和设备进行认证，以便控制用户设备对网络资源的访问。

1.1.1 802.1X的体系结构

802.1X系统中包括三个实体：客户端（Client）、设备端（Device）和认证服务器（Authentication server），如 图 1-1 所示。

图1-1 802.1X 体系结构图



- 客户端是请求接入局域网的用户终端，由局域网中的设备端对其进行认证。客户端上必须安装支持 802.1X 认证的客户端软件。
- 设备端是局域网中控制客户端接入的网络设备，位于客户端和认证服务器之间，为客户端提供接入局域网的端口（物理端口或逻辑端口），并通过与认证服务器的交互来对所连接的客户端进行认证。
- 认证服务器用于对客户端进行认证、授权和计费，通常为 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器。认证服务器根据设备端发送来的客户端认证信息来验证客户端的合法性，并将验证结果通知给设备端，由设备端决定是否允许客户

端接入。在一些规模较小的网络环境中，认证服务器的角色也可以由设备端来代替，即由设备端对客户端进行本地认证、授权和计费。

1.1.2 802.1X对端口的控制

1. 受控/非受控端口

设备端为客户端提供的接入局域网的端口被划分为两个逻辑端口：受控端口和非受控端口。任何到达该端口的帧，在受控端口与非受控端口上均可见。

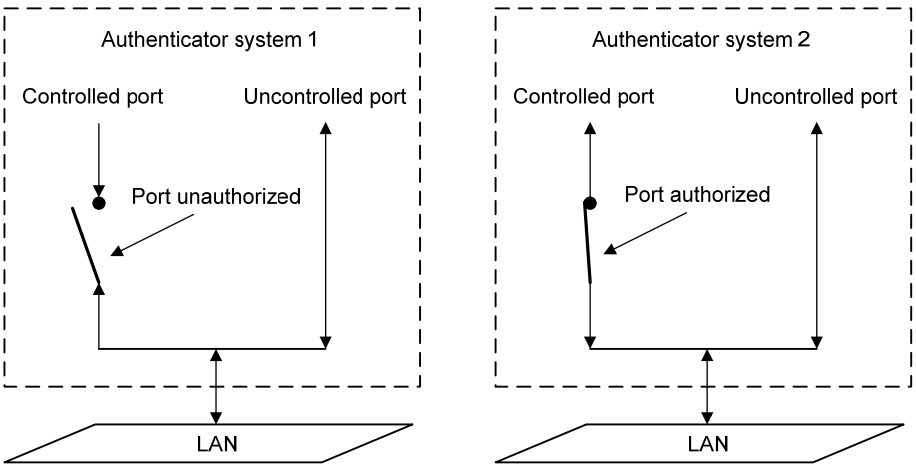
- 非受控端口始终处于双向连通状态，主要用来传递认证报文，保证客户端始终能够发出或接收认证报文。
- 受控端口在授权状态下处于双向连通状态，用于传递业务报文；在非授权状态下禁止从客户端接收任何报文。

2. 授权/非授权状态

设备端利用认证服务器对需要接入局域网的客户端进行认证，并根据认证结果（Accept 或 Reject）对受控端口的授权状态进行相应地控制。

图 1-2 显示了受控端口上不同的授权状态对通过该端口报文的影响。图中对比了两个 802.1X认证系统的端口状态。系统 1 的受控端口处于非授权状态，不允许报文通过；系统 2 的受控端口处于授权状态，允许报文通过。

图1-2 受控端口上授权状态的影响



3. 受控方向

在非授权状态下，受控端口可以处于单向受控或双向受控状态。

- 处于双向受控状态时，禁止帧的发送和接收；
- 处于单向受控状态时，禁止从客户端接收帧，但允许向客户端发送帧。

说明

目前，设备上的受控端口只能处于单向受控状态。

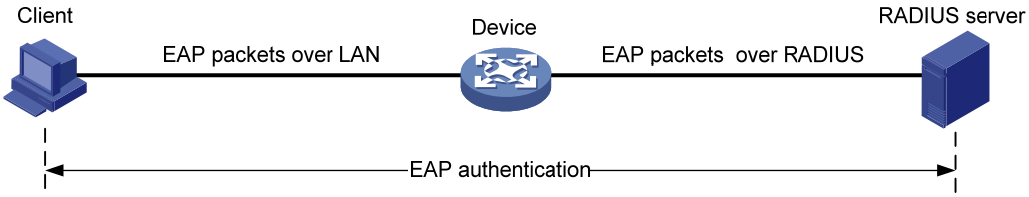
1.1.3 802.1X认证报文的交互机制

802.1X 系统使用 EAP（Extensible Authentication Protocol，可扩展认证协议）来实现客户端、设备端和认证服务器之间认证信息的交互。EAP 是一种 C/S 模式的认证框架，它可以支持多种认证方法，例如 MD5-Challenge、EAP-TLS（Extensible Authentication Protocol -Transport Layer Security，可扩展认证协议-传输层安全）、PEAP（Protected Extensible Authentication Protocol，受保护的扩展认证协议）等。在客户端与设备端之间，EAP 报文使用 EAPOL（Extensible Authentication Protocol over LAN，局域网上的可扩展认证协议）封装格式承载于数据帧中传递。在设备端与 RADIUS 服务器之间，EAP 报文的交互有 EAP 中继和 EAP 终结两种处理机制。

1. EAP中继

设备端对收到的 EAP 报文进行中继，使用 EAPOR（EAP over RADIUS）封装格式将其承载于 RADIUS 报文中发送给 RADIUS 服务器。

图1-3 EAP 中继原理示意图



该处理机制下，EAP 认证过程在客户端和 RADIUS 服务器之间进行。RADIUS 服务器作为 EAP 服务器来处理客户端的 EAP 认证请求，设备相当于一个中继，仅对 EAP 报文做中转。因此，设备处理简单，并能够支持 EAP 的各种认证方法，但要求 RADIUS 服务器支持相应的 EAP 认证方法。

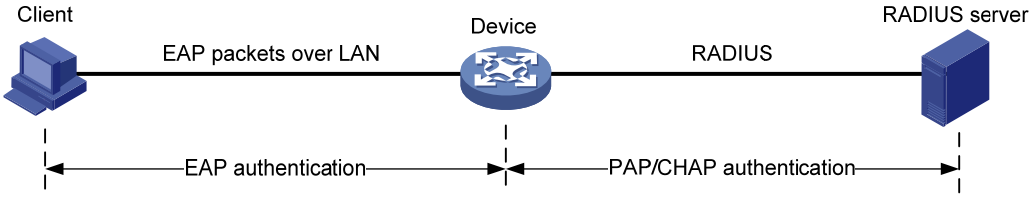
说明

在 RADIUS 服务器不能支持 EAP 认证，或者实际网络环境中未部署 RADIUS 服务器的情况下，如果希望使用 EAP 中继模式来支持多种 EAP 认证方法，则还需要在设备上配置专门的本地 EAP 服务器来协助完成 EAP 认证。

2. EAP终结

设备对 EAP 认证过程进行终结，将收到的 EAP 报文中的客户端认证信息封装在标准的 RADIUS 报文中，与服务器之间采用 PAP（Password Authentication Protocol，密码验证协议）或 CHAP（Challenge Handshake Authentication Protocol，质询握手验证协议）方法进行认证。

图1-4 EAP 终结原理示意图



该处理机制下，由于现有的 RADIUS 服务器基本均可支持 PAP 认证和 CHAP 认证，因此对服务器无特殊要求，但设备端处理较为复杂。设备端需要作为 EAP 服务器来解析与处理客户端的 EAP 报文，且目前仅能支持 MD5-Challenge 类型的 EAP 认证以及 iNode 802.1X 客户端发起的“用户名+密码”方式的 EAP 认证。

说明

如果客户端采用了 MD5-Challenge 类型的 EAP 认证，则设备端只能采用 CHAP 认证；如果 iNode 802.1X 客户端采用了“用户名+密码”方式的 EAP 认证，设备上可选择使用 PAP 认证或 CHAP 认证，从安全性上考虑，通常使用 CHAP 认证。

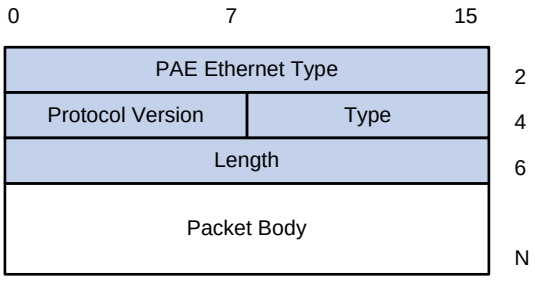
1.1.4 EAP报文的封装

1. EAPOL数据帧的封装

(1) EAPOL 数据帧的格式

EAPOL是 802.1X协议定义的一种承载EAP报文的封装技术，主要用于在局域网中传送客户端和设备端之间的EAP协议报文。EAPOL数据包的格式如 图 1-5 所示。

图1-5 EAPOL 数据包格式



- PAE Ethernet Type：表示协议类型。EAPOL 的协议类型为 0x888E。
- Protocol Version：表示 EAPOL 数据帧的发送方所支持的 EAPOL 协议版本号。
- Type：表示EAPOL数据帧类型。目前设备上支持的EAPOL数据帧类型见 表 1-1。

表1-1 EAPOL 数据帧类型

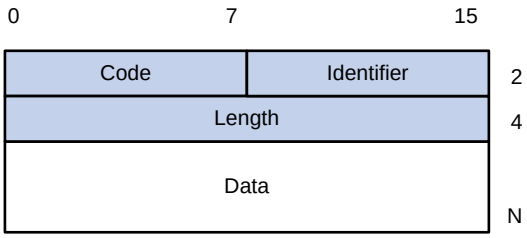
类型值	数据帧类型	说明
0x00	EAP-Packet	认证信息帧，用于承载客户端和设备端之间的EAP报文。
0x01	EAPOL-Start	认证发起帧，用于客户端向设备端发起认证请求
0x02	EAPOL-Logoff	退出请求帧，用于客户端向设备端发起下线请求

- Length：表示数据域的长度，也就是Packet Body字段的长度，单位为字节。当EAPOL数据帧的类型为 EAPOL-Start 或 EAPOL-Logoff 时，该字段值为 0，表示后面没有 Packet Body 字段。
- Packet Body：数据域的内容。

(2) EAP 报文的格式

当EAPOL数据帧的类型为EAP-Packet时，Packet Body字段的内容就是一个EAP报文，格式如 图1-6 所示。

图1-6 EAP 报文格式



- Code：EAP 报文的类型，包括 Request（1）、Response（2）、Success（3）和 Failure（4）。
- Identifier：用于匹配 Request 消息和 Response 消息的标识符。
- Length：EAP 报文的长度，包含 Code、Identifier、Length 和 Data 域，单位为字节。
- Data：EAP 报文的内容，该字段仅在 EAP 报文的类型为 Request 和 Response 时存在，它由类型域和类型数据两部分组成，例如，类型域为 1 表示 Identity 类型，类型域为 4 表示 MD5 challenge 类型。

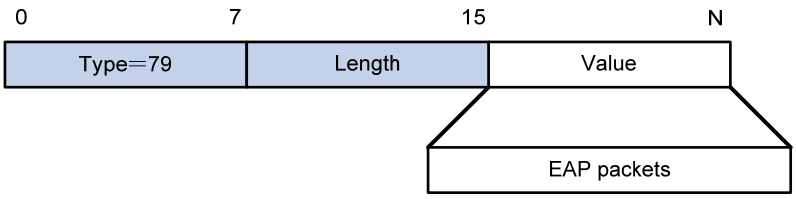
2. EAP报文在RADIUS中的封装

RADIUS 为支持 EAP 认证增加了两个属性：EAP-Message（EAP 消息）和 Message-Authenticator（消息认证码）。在含有 EAP-Message 属性的数据包中，必须同时包含 Message-Authenticator 属性。关于 RADIUS 报文格式的介绍请参见“安全配置指导”中的“AAA”的 RADIUS 协议简介部分。

(1) EAP-Message

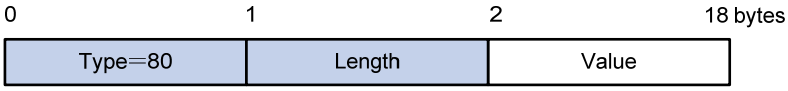
如 图 1-7 所示，EAP-Message属性用来封装EAP报文，Value域最长 253 字节，如果EAP报文长度大于 253 字节，可以对其进行分片，依次封装在多个EAP-Message属性中。

图1-7 EAP-Message 属性封装



(2) Message-Authenticator

Message-Authenticator 属性用于在 EAP 认证过程中验证携带了 EAP-Message 属性的 RADIUS 报文的完整性，避免报文被窜改。如果接收端对接收到的 RADIUS 报文计算出的完整性校验值与报文中携带的 Message-Authenticator 属性的 Value 值不一致，该报文会被认为无效而丢弃。



1.1.5 802.1X的认证触发方式

802.1X 的认证过程可以由客户端主动发起，也可以由设备端发起。

1. 客户端主动触发方式

- 组播触发：客户端主动向设备端发送 EAPOL-Start 报文来触发认证，该报文目的地址为组播 MAC 地址 01-80-C2-00-00-03。
- 广播触发：客户端主动向设备端发送 EAPOL-Start 报文来触发认证，该报文的目的地址为广播 MAC 地址。该方式可解决由于网络中有些设备不支持上述的组播报文，而造成设备端无法收到客户端认证请求的问题。

说明

目前，仅在安装了 HMIM-24GSW/24GSWP 和 HMIM-8GSW 交换卡的款型上支持广播触发方式。

2. 设备端主动触发方式

设备端主动触发方式用于支持不能主动发送 EAPOL-Start 报文的客户端，例如 Windows XP 自带的 802.1X 客户端。设备主动触发认证的方式分为以下两种：

- 组播触发：设备每隔一定时间（缺省为 30 秒）主动向客户端组播发送 Identity 类型的 EAP-Request 帧来触发认证。
- 单播触发：当设备收到源 MAC 地址未知的报文时，主动向该 MAC 地址单播发送 Identity 类型的 EAP-Request 帧来触发认证。若设备端在设置的时长内没有收到客户端的响应，则重发该报文。

1.1.6 802.1X的认证过程

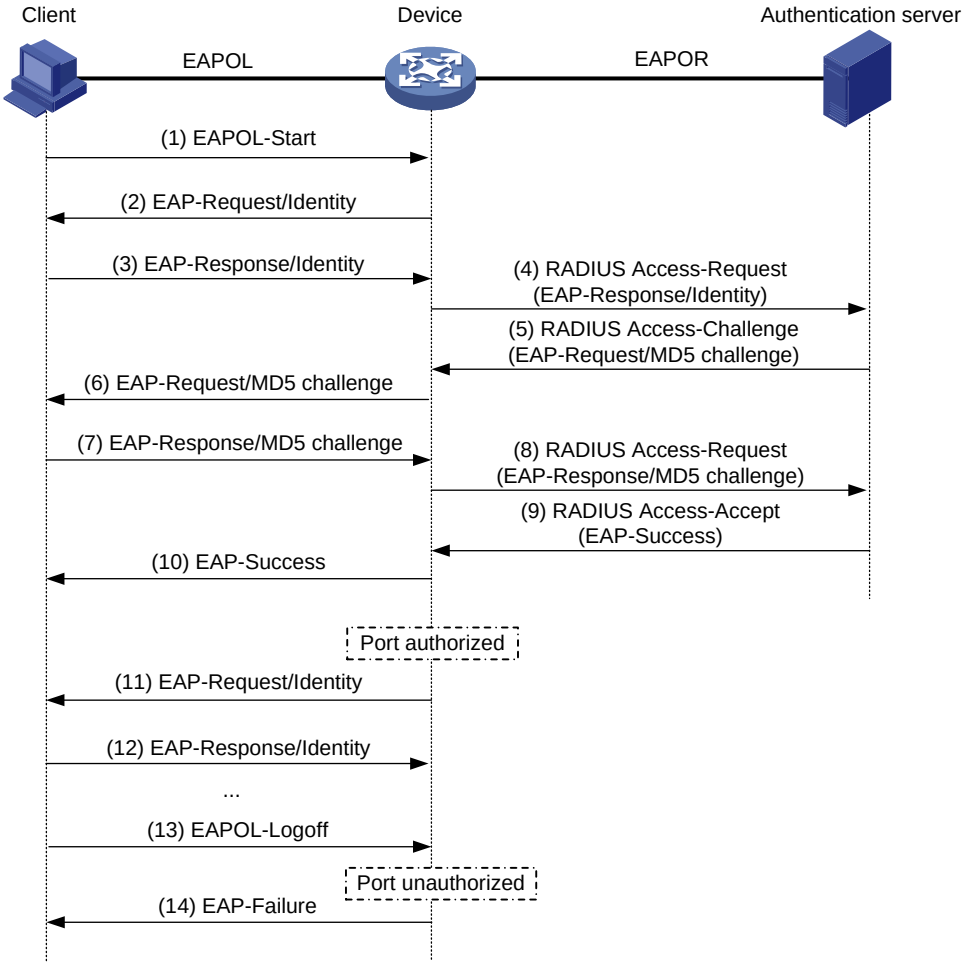
设备端支持采用 EAP 中继方式或 EAP 终结方式与远端 RADIUS 服务器交互。以下关于 802.1X 认证过程的描述，都以客户端主动发起认证为例。

1. EAP中继方式

这种方式是 IEEE 802.1X 标准规定的，将 EAP 承载在其它高层协议中，如 EAP over RADIUS，以便 EAP 报文穿越复杂的网络到达认证服务器。一般来说，需要 RADIUS 服务器支持 EAP 属性：EAP-Message 和 Message-Authenticator。

如 图 1-8 所示，以MD5-Challenge类型的EAP认证为例，具体认证过程如下。

图1-8 IEEE 802.1X 认证系统的 EAP 中继方式认证流程



(1) 当用户需要访问外部网络时打开 802.1X 客户端程序，输入用户名和密码，发起连接请求。此时，客户端程序将向设备端发出认证请求帧（EAPOL-Start），开始启动一次认证过程。

(2) 设备端收到认证请求帧后，将发出一个 Identity 类型的请求帧（EAP-Request/Identity）要求用户的客户端程序发送输入的用户名。

(3) 客户端程序响应设备端发出的请求，将用户名信息通过 Identity 类型的响应帧（EAP-Response/Identity）发送给设备端。

(4) 设备端将客户端发送的响应帧中的 EAP 报文封装在 RADIUS 报文（RADIUS Access-Request）中发送给认证服务器进行处理。

(5) RADIUS 服务器收到设备端转发的用户名信息后，将该信息与数据库中的用户名列表对比，找到该用户名对应的密码信息，用随机生成的一个 MD5 Challenge 对密码进行加密处理，同时将此 MD5 Challenge 通过 RADIUS Access-Challenge 报文发送给设备端。

(6) 设备端将 RADIUS 服务器发送的 MD5 Challenge 转发给客户端。

(7) 客户端收到由设备端传来的 MD5 Challenge 后，用该 Challenge 对密码进行加密处理，生成 EAP-Response/MD5 Challenge 报文，并发送给设备端。

(8) 设备端将此 EAP-Response/MD5 Challenge 报文封装在 RADIUS 报文（RADIUS Access-Request）中发送给 RADIUS 服务器。

(9) RADIUS 服务器将收到的已加密的密码信息和本地经过加密运算后的密码信息进行对比，如果相同，则认为该用户为合法用户，并向设备端发送认证通过报文（RADIUS Access-Accept）。

(10) 设备收到认证通过报文后向客户端发送认证成功帧（EAP-Success），并将端口改为授权状态，允许用户通过端口访问网络。

(11) 用户在线期间，设备端会通过向客户端定期发送握手报文的方法，对用户的在线情况进行监测。

(12) 客户端收到握手报文后，向设备发送应答报文，表示用户仍然在线。缺省情况下，若设备端发送的两次握手请求报文都未得到客户端应答，设备端就会让用户下线，防止用户因为异常原因下线而设备无法感知。

(13) 客户端可以发送 EAPOL-Logoff 帧给设备端，主动要求下线。

(14) 设备端把端口状态从授权状态改变成未授权状态，并向客户端发送 EAP-Failure 报文。

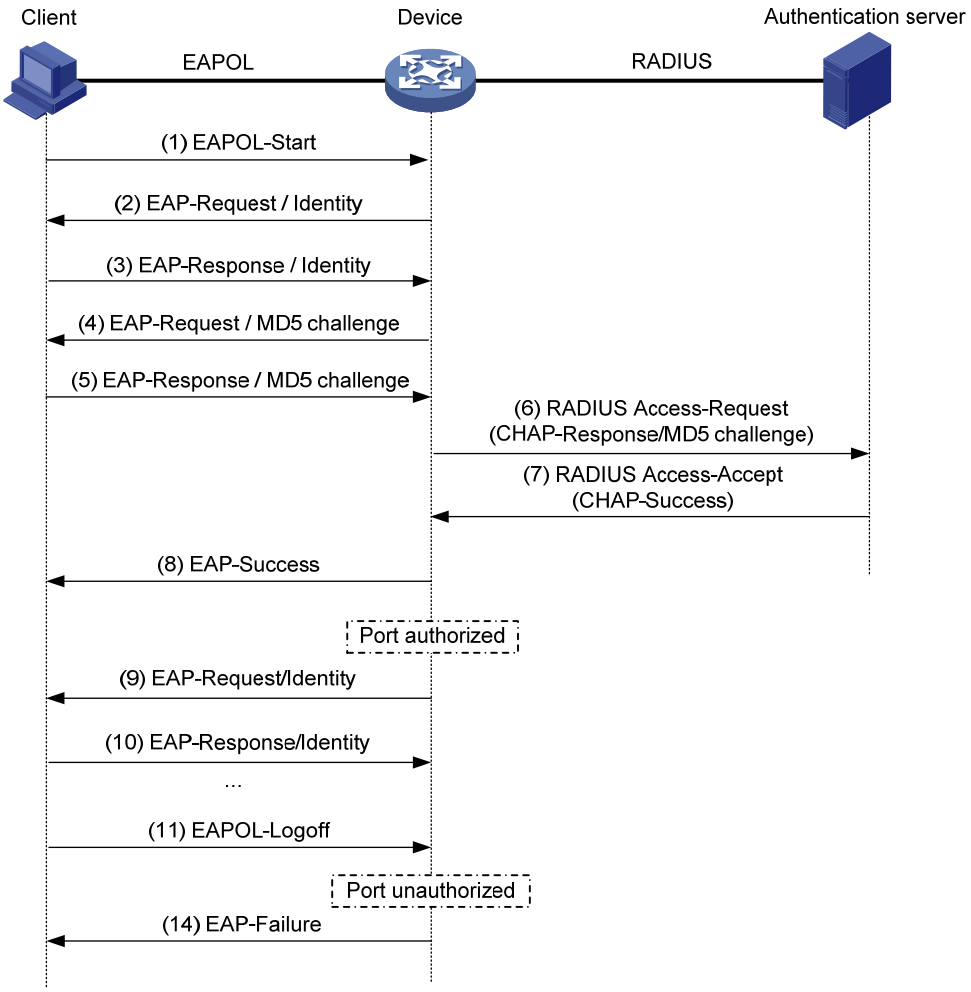
说明

EAP 中继方式下，需要保证在客户端和 RADIUS 服务器上选择一致的 EAP 认证方法，而在设备上，只需要通过 **dot1x authentication-method eap** 命令启动 EAP 中继方式即可。

2. EAP终结方式

这种方式将EAP报文在设备端终结并映射到RADIUS报文中，利用标准RADIUS协议完成认证、授权和计费。设备端与RADIUS服务器之间可以采用PAP或者CHAP认证方法。如 图 1-9 所示，以CHAP认证为例，具体的认证流程如下。

图1-9 IEEE 802.1X 认证系统的 EAP 终结方式认证流程



EAP 终结方式与 EAP 中继方式的认证流程相比，不同之处在于用来对用户密码信息进行加密处理的 MD5 challenge 由设备端生成，之后设备端会把用户名、MD5 challenge 和客户端加密后的密码信息一起发送给 RADIUS 服务器，进行相关的认证处理。

1.1.7 802.1X的接入控制方式

设备不仅支持协议所规定的基于端口的接入认证方式（Port-based），还对其进行了扩展、优化，支持基于 MAC 的接入控制方式（MAC-based）。

- 采用基于端口的接入控制方式时，只要该端口下的第一个用户认证成功后，其它接入用户无须认证就可使用网络资源，但是当第一个用户下线后，其它用户也会被拒绝使用网络。
- 采用基于 MAC 的接入控制方式时，该端口下的所有接入用户均需要单独认证，当某个用户下线后，也只有该用户无法使用网络。

1.2 802.1X支持VLAN下发

1.2.1 授权VLAN

802.1X 用户在通过远程 AAA/本地 AAA 认证时，远程 AAA 服务器/接入设备可以下发授权 VLAN 信息给用户的接入端口。

1. 远程AAA授权

该方式下，需要在服务器上指定下发给用户的授权 VLAN 信息，下发的授权 VLAN 信息可以有多种形式，包括数字型 VLAN 和字符型 VLAN，字符型 VLAN 又可分为 VLAN 名称、VLAN 组名、携带后缀的 VLAN ID（后缀用于标识是否携带 Tag）。

设备收到服务器的授权 VLAN 信息后，首先对其进行解析，只要解析成功，即以对应的方法下发授权 VLAN；如果解析不成功，则用户认证失败。

- 若认证服务器下发的授权 VLAN 信息为一个 VLAN ID 或一个 VLAN 名称，则仅当对应的 VLAN 存在，且不为动态学习到的 VLAN、保留 VLAN 时，该 VLAN 才是有效的授权 VLAN。
- 若认证服务器下发的授权 VLAN 信息为一个 VLAN 组名，则设备首先会通过组名查找该组内配置的 VLAN 列表。若查找到授权 VLAN 列表，则在这一组 VLAN 中，除动态 VLAN 以及不存在的 VLAN 之外的所有 VLAN 都有资格被授权给用户。关于 VLAN 组的相关配置，请参见“二层技术-以太网交换配置指导”中的“VLAN”。
  - 若端口上已有其它在线用户，则当端口链路类型为 Hybrid，802.1X 接入控制方式为 MAC-based，且使能了 MAC VLAN 功能时，将选择该组 VLAN 中在线用户数最少的一个 VLAN 作为当前认证用户的授权 VLAN（若在线用户数最小的 VLAN 有多个，则选择 VLAN ID 最小者）；当端口处于其它配置情况时，则查看端口上在线用户的授权 VLAN 是否存在于该组中，若存在，则将此 VLAN 授权给当前的认证用户，否则认为当前认证用户授权失败，将被强制下线。
  - 若端口上没有其它在线用户，则将该组 VLAN 中 ID 最小的 VLAN 授权给当前的认证用户。
- 若认证服务器下发的授权 VLAN 信息为一个包含若干 VLAN 编号以及若干 VLAN 名称的字符串，则设备首先将其解析为一组 VLAN ID，然后采用与解析一个 VLAN 组名相同的解析逻辑选择一个授权 VLAN。
- 若认证服务器下发的授权 VLAN 信息为一个包含若干个“VLAN ID+后缀”形式的字符串，则只有第一个不携带后缀或者携带 untagged 后缀的 VLAN 将被解析为唯一的 untagged 的授权 VLAN，其余 VLAN 都被解析为 tagged 的授权 VLAN。例如服务器下发字符串“1u 2t 3”，其中的 u 和 t 均为后缀，分别表示 untagged 和 tagged。该字符串被解析之后，VLAN 1 为 untagged 的授权 VLAN，VLAN 2 和 VLAN 3 为 tagged 的授权 VLAN。该方式下发的授权 VLAN 仅对端口链路类型为 Hybrid 或 Trunk，且 802.1X 接入控制方式为 Port-based 的端口有效。
  - 端口的缺省 VLAN 将被修改为 untagged 的授权 VLAN。若不存在 untagged 的授权 VLAN，则不修改端口的缺省 VLAN。
  - 端口将允许所有解析成功的授权 VLAN 通过。

2. 本地AAA授权

该方式下，可以通过配置本地用户的授权属性指定下发给用户的授权 VLAN 信息，且只能指定一个授权 VLAN。设备将此 VLAN 作为该本地用户的授权 VLAN。关于本地用户的相关配置，请参见“安全配置指导”中的“AAA”。

3. 不同类型的端口加入授权VLAN

无论是远程AAA授权，还是本地AAA授权，除了认证服务器下发“VLAN ID+后缀”形式的字符串之外，其它情况下设备均会根据用户认证上线的端口链路类型，按照 表 1-2 将端口加入指定的授权VLAN中。

表1-2 不同类型的端口加入授权 VLAN

接入控制方式	Access 端口	Trunk 端口	Hybrid 端口
Port-based	• 加入授权 VLAN • 缺省 VLAN 修改为授权 VLAN	• 允许授权 VLAN 通过 • 缺省 VLAN 修改为授权 VLAN	• 允许授权 VLAN 以不携带 Tag 的方式通过 • 缺省 VLAN 修改为授权 VLAN
MAC-based	• 加入第一个通过认证的用户的授权 VLAN • 缺省 VLAN 修改为第一个通过认证的用户的授权 VLAN	• 允许授权 VLAN 通过 • 缺省 VLAN 修改为第一个通过认证的用户的授权 VLAN	• 允许授权 VLAN 以不携带 Tag 的方式通过 • 若端口上开启了 MAC VLAN 功能，则根据授权 VLAN 动态地创建基于用户 MAC 的 VLAN，而端口的缺省 VLAN 并不改变 • 若端口上未开启 MAC VLAN 功能，则端口的缺省 VLAN 修改为第一个通过认证的用户的授权 VLAN
	说明：只有开启了MAC VLAN功能的端口上才允许给不同的用户MAC授权不同的VLAN。其它情况下，授权给所有用户的VLAN必须相同，否则仅第一个通过认证的用户可以成功上线。		

授权 VLAN 并不影响端口的配置。但是，授权 VLAN 的优先级高于用户配置的 VLAN，即通过认证后起作用的 VLAN 是授权 VLAN，用户配置的 VLAN 在用户下线后生效。

说明

- 对于 Hybrid 端口，不建议把将要下发或已经下发的授权 VLAN 配置为携带 Tag 的方式加入端口。
- 在启动了 802.1X 周期性重认证功能的 Hybrid 端口上，若用户在 MAC VLAN 功能开启之前上线，则 MAC VLAN 功能不能对该用户生效，即系统不会根据服务器下发的 VLAN 生成该用户的 MAC VLAN 表项，只有该在线用户重认证成功且服务器下发的 VLAN 发生变化时，MAC VLAN 功能才会对它生效。MAC VLAN 功能的详细介绍请参考“二层技术-以太网交换配置指导”中的“VLAN”。

1.2.2 802.1X Guest VLAN

802.1X Guest VLAN 功能允许用户在未认证的情况下，访问某一特定 VLAN 中的资源。这个特定的 VLAN 称之为 Guest VLAN，该 VLAN 内通常放置一些用于用户下载客户端软件或其他升级程序的服务器。

目前设备仅支持 Guest VLAN 的 Port-based 方式。

在接入控制方式为Port-based的端口上配置Guest VLAN后，若全局和端口上都使能了 802.1X，端口授权状态为auto，且端口处于激活状态，则该端口就被加入Guest VLAN，所有在该端口接入的

用户将被授权访问Guest VLAN里的资源。端口加入Guest VLAN的情况与加入授权VLAN相同，与端口链路类型有关，请参见“1.2.1 授权VLAN”的“表 1-2”。

当端口上处于Guest VLAN中的用户发起认证且失败时：如果端口配置了Auth-Fail VLAN，则该端口会被加入Auth-Fail VLAN；如果端口未配置Auth-Fail VLAN，则该端口仍然处于Guest VLAN内。关于Auth-Fail VLAN的具体介绍请参见“1.2.3 802.1X Auth-Fail VLAN”。

当端口上处于 Guest VLAN 中的用户发起认证且成功时，端口会离开 Guest VLAN，之后端口加入 VLAN 情况与认证服务器是否下发 VLAN 有关，具体如下：

- 若认证服务器下发 VLAN，则端口加入下发的 VLAN 中。用户下线后，端口离开下发的 VLAN 回到 Guest VLAN 中。
- 若认证服务器未下发 VLAN，则端口回到初始 VLAN 中。用户下线后，端口回到 Guest VLAN 中。

1.2.3 802.1X Auth-Fail VLAN

802.1X Auth-Fail VLAN 功能允许用户在认证失败的情况下访问某一特定 VLAN 中的资源，这个 VLAN 称之为 Auth-Fail VLAN。需要注意的是，这里的认证失败是认证服务器因某种原因明确拒绝用户认证通过，比如用户密码错误，而不是认证超时或网络连接等原因造成的认证失败。

目前设备仅支持 Auth-Fail VLAN 的 Port-based 方式。

在接入控制方式为Port-based的端口上配置Auth-Fail VLAN后，若该端口上有用户认证失败，则该端口会离开当前的VLAN被加入到Auth-Fail VLAN，所有在该端口接入的用户将被授权访问Auth-Fail VLAN里的资源。端口加入Auth-Fail VLAN的情况与加入授权VLAN相同，与端口链路类型有关，请参见“1.2.1 授权VLAN”的“表 1-2”。

当加入 Auth-Fail VLAN 的端口上有用户发起认证并失败，则该端口将会仍然处于 Auth-Fail VLAN 内；如果认证成功，则该端口会离开 Auth-Fail VLAN，之后端口加入 VLAN 情况与认证服务器是否下发授权 VLAN 有关，具体如下：

- 若认证服务器下发了授权 VLAN，则端口加入下发的授权 VLAN 中。用户下线后，端口会离开下发的授权 VLAN，若端口上配置了 Guest VLAN，则加入 Guest VLAN，否则加入缺省 VLAN。
- 若认证服务器未下发授权 VLAN，则端口回到缺省 VLAN 中。用户下线后，若端口上配置了 Guest VLAN，则加入 Guest VLAN，否则端口仍在缺省 VLAN 中。

1.2.4 802.1X Critical VLAN

802.1X Critical VLAN 功能允许用户在认证时，当所有认证服务器都不可达的情况下访问某一特定 VLAN 中的资源，这个 VLAN 称之为 Critical VLAN。目前，只采用 RADIUS 认证方式的情况下，在所有 RADIUS 认证服务器都不可达后，端口才会加入 Critical VLAN。若采用了其它认证方式，则端口不会加入 Critical VLAN。

目前设备仅支持 Critical VLAN 的 Port-based 方式。

在接入控制方式为Port-based的端口上配置Critical VLAN后，若该端口上有用户认证时，所有认证服务器都不可达，则该端口会被加入到Critical VLAN，之后所有在该端口接入的用户将被授权访问Critical VLAN里的资源。在用户进行重认证时，若所有认证服务器都不可达，且端口指定在此情况下强制用户下线，则该端口也会被加入到Critical VLAN。端口加入Critical VLAN的情况与加入授权VLAN相同，与端口链路类型有关，请参见“1.2.1 授权VLAN”的“表 1-2”。

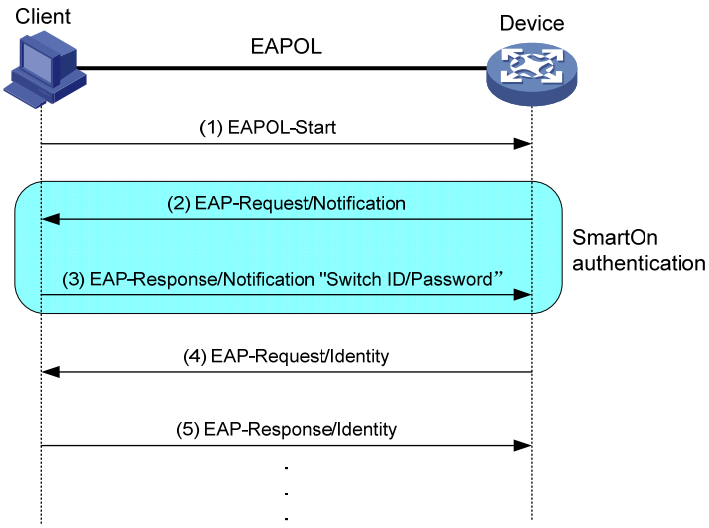
已经加入 Critical VLAN 的端口上有用户发起认证时，如果所有认证服务器不可达，则端口仍然在 Critical VLAN 内；如果服务器可达且认证失败，且端口配置了 Auth-Fail VLAN，则该端口将会加入 Auth-Fail VLAN；如果服务器可达且认证成功，则该端口加入 VLAN 的情况与认证服务器是否下发 VLAN 有关，具体如下：

- 若认证服务器下发了授权 VLAN，则端口加入下发的授权 VLAN 中。用户下线后，端口会离开下发的授权 VLAN，若端口上配置了 Guest VLAN，则加入 Guest VLAN，否则加入缺省 VLAN。
- 若认证服务器未下发授权 VLAN，则端口回缺省 VLAN 中。用户下线后，若端口上配置了 Guest VLAN，则加入 Guest VLAN，否则端口仍在缺省 VLAN 中。

1.3 802.1X SmartOn功能

SmartOn功能是为了支持NEC公司的 802.1X客户端而开发的，其基本原理如 图 1-10 所示，在开始802.1X认证请求前增加了SmartOn认证，如果SmartOn认证不成功，则不再继续进行 802.1X认证。

图1-10 开启 SmartOn 功能后 802.1X 的认证流程



开启了 SmartOn 功能的设备通过判断 Switch ID 和密码来决定用户是否能进行正常的 802.1X 认证过程：

- 只有当客户端的 Switch ID 和密码与设备上所配置的 Switch ID 和密码一致时，802.1X 的认证过程才能继续；
- 如果用户试图使用其它的 802.1X 客户端，则设备在 802.1X 认证之前就拒绝该用户的访问。

说明

安装客户端软件后，需要在 Windows 注册表中的[HKEY_LOCAL_MACHINE\SOFTWARE\Soliton Systems K.K.\SmartOn Client\Clients\1XGate]，新建两个字符串值 QX_ID 和 QX_PASSWORD，分别设置为 Switch ID 和密码，这两个值必须和设备上所配置的 Switch ID 和密码一致。

1.4 802.1X配置任务简介

表1-3 802.1X 配置任务简介

配置任务	说明	详细配置
开启802.1X特性	必选	1.5.2
配置802.1X系统的认证方法	必选	1.5.3
配置端口的授权状态	可选	1.5.4
配置端口接入控制方式	可选	1.5.5
配置端口同时接入用户数的最大值	可选	1.5.6
配置设备向接入用户发送认证请求报文的最大次数	可选	1.5.7
配置802.1X认证超时定时器	可选	1.5.8
配置在线用户握手功能	可选	1.5.9
开启认证触发功能	可选	1.5.10
配置端口的强制认证域	可选	1.5.11
配置静默功能	可选	1.5.12
配置重认证功能	可选	1.5.13
配置Guest VLAN	可选	1.5.14
配置Auth-Fail VLAN	可选	1.5.15
配置Critical VLAN	可选	1.5.16
配置802.1X支持的域名分隔符	可选	1.5.17
配置802.1X SmartOn功能	可选	1.6

1.5 配置802.1X

1.5.1 配置准备

802.1X 需要 AAA 的配合才能实现对用户的身份认证。因此，需要首先完成以下配置任务：

- 配置 802.1X 用户所属的 ISP 认证域及其使用的 AAA 方案，即本地认证方案或 RADIUS 方案。
- 如果需要通过 RADIUS 服务器进行认证，则应该在 RADIUS 服务器上配置相应的用户名和密码。
- 如果需要本地认证，则应该在设备上手动添加认证的用户名和密码。配置本地认证时，用户使用的服务类型必须设置为 **lan-access**。

说明

在 RADIUS 服务器不能支持 EAP 认证，或者使用本地认证的情况下，如果希望使用 EAP 中继模式来支持多种 EAP 认证方法，则还需要在设备上配置专门的本地 EAP 服务器来协助完成 EAP 认证。关于本地 EAP 认证以及 AAA 的具体配置请参见“安全配置指导”中的“AAA”。

1.5.2 开启 802.1X

只有同时开启全局和端口的 802.1X 后，802.1X 的配置才能在端口上生效。

开启 802.1X 时，需要注意的是：

端口上开启 802.1X 之前，请保证端口未加入聚合组或业务环回组。

表1-4 开启 802.1X

配置步骤	命令	说明
进入系统视图	**system-view**	-
开启全局的802.1X	**dot1x**	缺省情况下，全局的802.1X处于关闭状态
进入以太网接口视图	**interface** *interface-type interface-number*	-
开启端口的802.1X	**dot1x**	缺省情况下，端口的802.1X处于关闭状态

1.5.3 配置 802.1X系统的认证方法

设备上的 802.1X 系统采用的认证方法与设备对于 EAP 报文的处理机制有关，具体如下：

- 若指定 **authentication-method** 为 **eap**，则表示设备采用 EAP 中继认证方式。该方式下，设备端对客户端发送的 EAP 报文进行中继处理，并能支持客户端与 RADIUS 服务器之间所有类型的 EAP 认证方法。
- 若指定 **authentication-method** 为 **chap** 或 **pap**，则表示设备采用 EAP 终结认证方式，该方式下，设备端对客户端发送的 EAP 报文进行本地终结，并能支持与 RADIUS 服务器之间采用 CHAP 或 PAP 类型的认证方法。

表1-5 配置 802.1X 系统的认证方法

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置802.1X系统的认证方法	**dot1x authentication-method { chap | eap | pap }**	缺省情况下，设备启用EAP终结方式，并采用CHAP认证方法

说明

如果采用 EAP 中继认证方式，则设备会把客户端输入的内容直接封装后发给服务器，这种情况下 **user-name-format** 命令的设置无效，**user-name-format** 的介绍请参见“安全命令参考”中的“AAA”。

1.5.4 配置端口的授权状态

通过配置端口的授权状态，可以控制端口上接入的用户是否需要经过认证来访问网络资源。端口支持以下三种授权状态：

- 强制授权（**authorized-force**）：表示端口始终处于授权状态，允许用户不经认证即可访问网络资源。
- 强制非授权（**unauthorized-force**）：表示端口始终处于非授权状态，不允许用户进行认证。设备端不为通过该端口接入的客户端提供认证服务。
- 自动识别（**auto**）：表示端口初始状态为非授权状态，仅允许 EAPOL 报文收发，不允许用户访问网络资源；如果用户通过认证，则端口切换到授权状态，允许用户访问网络资源。这也是最常用的一种状态。

表1-6 配置端口的授权状态

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
配置端口的授权状态	**dot1x port-control** { **authorized-force** | **auto** | **unauthorized-force** }	缺省情况下，端口的授权状态为**auto**

1.5.5 配置端口接入控制方式

说明

目前，仅在安装了 HMIM-24GSW/24GSWP 和 HMIM-8GSW 交换卡的款型以及 MSR3600-28/MSR3600-51 的固定二层接口上支持基于 MAC 控制。

设备支持两种端口接入控制方式：基于端口控制（**portbased**）和基于 MAC 控制（**macbased**）。

表1-7 配置端口接入控制方式

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-

配置步骤	命令	说明
配置端口接入控制方式	**dot1x port-method** { **macbased** | **portbased** }	缺省情况下，端口采用的接入控制方式为**macbased** 若端口上同时启动了802.1X和Portal认证功能，则端口接入控制方式必须为**macbased**。关于Portal认证的相关介绍，请参考“安全配置指导”中的“Portal”

1.5.6 配置端口同时接入用户数的最大值

由于系统资源有限，如果当前端口上接入的用户过多，接入用户之间会发生资源的争用。因此限制接入用户数可以使属于当前端口的用户获得可靠的性能保障。

表1-8 配置端口同时接入用户数的最大值

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
配置端口同时接入用户数的最大值	**dot1x max-user** *user-number*	缺省情况下，端口同时接入用户数的最大值为256

1.5.7 配置设备向接入用户发送认证请求报文的最大次数

如果设备向用户发送认证请求报文后，在规定的时间里（可通过命令 **dot1x timer tx-period** 或者 **dot1x timer supp-timeout** 设定）没有收到用户的响应，则设备将向用户重发该认证请求报文，若设备累计发送认证请求报文的次数达到配置的最大值后，仍然没有得到用户响应，则停止发送认证请求。

表1-9 配置设备向接入用户发送认证请求报文的最大次数

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置设备向接入用户发送认证请求报文的最大次数	**dot1x retry** *max-retry-value*	缺省情况下，设备最多可向接入用户发送2次认证请求报文

1.5.8 配置 802.1X认证超时定时器

802.1X 认证过程中会启动多个定时器以控制客户端、设备以及 RADIUS 服务器之间进行合理、有序的交互。可配置的 802.1X 认证定时器包括以下两种：

- 客户端认证超时定时器：当设备端向客户端发送了 EAP-Request/MD5 Challenge 请求报文后，设备端启动此定时器，若在该定时器设置的时长内，设备端没有收到客户端的响应，设备端将重发该报文。

- 认证服务器超时定时器：当设备端向认证服务器发送了 RADIUS Access-Request 请求报文后，设备端启动该定时器，若在该定时器设置的时长内，设备端没有收到认证服务器的响应，设备端将重发认证请求报文。

一般情况下，无需改变认证超时定时器的值，除非在一些特殊或恶劣的网络环境下，才需要通过命令来调节。例如，用户网络状况比较差的情况下，可以适当地将客户端认证超时定时器值调大一些；还可以通过调节认证服务器超时定时器的值来适应不同认证服务器的性能差异。

表1-10 配置 802.1X 认证超时定时器

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置客户端认证超时定时器	**dot1x timer supp-timeout** *supp-timeout-value*	缺省情况下，客户端认证超时定时器的值为30秒
配置认证服务器超时定时器	**dot1x timer server-timeout** *server-timeout-value*	缺省情况下，认证服务器超时定时器的值为100秒

1.5.9 配置在线用户握手功能

开启设备的在线用户握手功能后，设备会定期（时间间隔通过命令 **dot1x timer handshake-period** 设置）向通过 802.1X 认证的在线用户发送握手报文，以定期检测用户的在线情况。如果设备连续多次（通过命令 **dot1x retry** 设置）没有收到客户端的响应报文，则会将用户置为下线状态。

在线用户握手功能处于开启状态的前提下，还可以通过开启在线用户握手安全功能，来防止在线的 802.1X 认证用户使用非法的客户端与设备进行握手报文的交互，而逃过代理检测、双网卡检测等 iNode 客户端的安全检查功能。开启了在线用户握手安全功能的设备通过检验客户端上传的握手报文中携带的验证信息，来确认用户是否使用 iNode 客户端进行握手报文的交互。如果握手检验不通过，则会将用户置为下线状态。

需要注意的是：

- 部分 802.1X 客户端不支持与设备进行握手报文的交互，因此建议在这种情况下，关闭设备的在线用户握手功能，避免该类型的在线用户因没有回应握手报文而被强制下线。
- 802.1X SmartOn 功能与在线用户握手功能互斥，建议两个功能不要同时开启。

表1-11 配置在线用户握手功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
（可选）配置握手定时器	**dot1x timer handshake-period** *handshake-period-value*	缺省情况下，握手定时器的值为15秒
进入以太网接口视图	**interface** *interface-type interface-number*	-
开启在线用户握手功能	**dot1x handshake**	缺省情况下，在线用户握手功能处于开启状态 SmartOn功能与802.1X的在线用户握手功能互斥

配置步骤	命令	说明
（可选）开启在线用户握手安全功能	**dot1x handshake secure**	缺省情况下，在线用户握手安全功能处于关闭状态

1.5.10 开启认证触发功能

端口上开启认证触发功能后，设备会主动向该端口上的客户端发送认证请求来触发认证，以支持不能主动发送 EAPOL-Start 报文来发起认证的客户端。设备提供了以下两种类型的认证触发功能：

- 组播触发功能：启用了该功能的端口会定期（间隔时间通过命令 **dot1x timer tx-period** 设置）向客户端组播发送 EAP-Request/Identity 报文来检测客户端并触发认证。
- 单播触发功能：当启用了该功能的端口收到源 MAC 地址未知的报文时，会主动向该 MAC 地址单播发送 EAP-Request/Identity 报文，若端口在指定的时间内（通过命令 **dot1x timer tx-period** 设置）没有收到客户端的响应，则重发该报文（重发次数通过命令 **dot1x retry** 设置）。

配置认证触发功能时，请参考以下配置限制和指导：

- 若端口连接的 802.1X 客户端不能主动发起认证，则需要开启组播触发功能。
- 若端口连接的 802.1X 客户端不能主动发起认证，且仅部分 802.1X 客户端需要进行认证，为避免不希望认证或已认证的 802.1X 客户端收到多余的认证触发报文，则需要开启单播触发功能。
- 对于无线局域网来说，可以由客户端主动发起认证，或由无线模块发现用户并触发认证，而不必由设备端定期发送 802.1X 的组播报文来触发。同时，组播触发报文会占用无线的通信带宽，因此建议无线局域网中的接入设备关闭组播触发功能。
- 建议组播触发功能和单播触发功能不要同时开启，以免认证报文重复发送。

表1-12 开启认证触发功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
（可选）配置用户名请求超时定时器	**dot1x timer tx-period** *tx-period-value*	缺省情况下，用户名请求超时定时器的值为30秒
进入以太网接口视图	**interface** *interface-type interface-number*	-
开启认证触发功能	**dot1x { multicast-trigger | unicast-trigger }**	缺省情况下，组播触发功能处于开启状态，单播触发功能处于关闭状态

1.5.11 配置端口的强制认证域

在端口上指定强制认证域为 802.1X 接入提供了一种安全控制策略。所有从该端口接入的 802.1X 用户将被强制使用指定的认证域来进行认证、授权和计费，从而防止用户通过恶意假冒其它域账号从本端口接入网络。另外，管理员也可以通过配置强制认证域对不同端口接入的用户指定不同的认证域，从而增加了管理员部署 802.1X 接入策略的灵活性。

表1-13 配置端口的强制认证域

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
指定端口上802.1X用户使用的强制认证域	**dot1x mandatory-domain** *domain-name*	缺省情况下，未指定802.1X用户使用的强制认证域

1.5.12 配置静默功能

当 802.1X 用户认证失败以后，设备需要静默一段时间（通过命令 **dot1x timer quiet-period** 设置）后再重新发起认证，在静默期间，设备不对 802.1X 认证失败的用户进行 802.1X 认证处理。

在网络处在风险位置，容易受攻击的情况下，可以适当地将静默定时器值调大一些，反之，可以将其调小一些来提高对用户认证请求的响应速度。

表1-14 开启静默定时器功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
（可选）配置静默定时器	**dot1x timer quiet-period** *quiet-period-value*	缺省情况下，静默定时器的值为60秒
开启静默定时器功能	**dot1x quiet-period**	缺省情况下，静默定时器功能处于关闭状态

1.5.13 配置重认证功能

端口启动了 802.1X 的周期性重认证功能后，设备会根据周期性重认证定时器设定的时间间隔（由命令 **dot1x timer reauth-period** 设置）定期向该端口在线 802.1X 用户发起重认证，以检测用户连接状态的变化、确保用户的正常在线，并及时更新服务器下发的授权属性（例如 ACL、VLAN）。

认证服务器可以通过下发 RADIUS 属性（session-timeout）来指定用户的重认证周期，且该功能不需要设备上开启周期性重认证功能来配合，属性下发成功即可生效。802.1X 用户认证通过后，如果认证服务器对该用户下发了重认证周期，则设备上配置的周期性重认证时间无效，服务器下发的重认证周期生效。认证服务器下发重认证时间的具体配置以及是否可以下发重认证周期的情况与服务器类型有关，请参考具体的认证服务器实现。

在用户名不改变的情况下，端口允许重认证前后服务器向该用户下发不同的 VLAN。

表1-15 配置重认证功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
（可选）配置周期性重认证定时器	**dot1x timer reauth-period** *reauth-period-value*	缺省情况下，周期性重认证定时器的值为3600秒
进入以太网接口视图	**interface** *interface-type interface-number*	-

配置步骤	命令	说明
开启周期性重认证功能	**dot1x re-authenticate**	缺省情况下，周期性重认证功能处于关闭状态
（可选）配置重认证服务器不可达时端口上的802.1X用户保持在线状态	**dot1x re-authenticate server-unreachable keep-online**	缺省情况下，端口上的802.1X在线用户重认证时，若认证服务器不可达，则会被强制下线

1.5.14 配置 802.1X Guest VLAN


提示

如果用户端设备发出的是携带 Tag 的数据流，且接入端口上使能了 802.1X 认证并配置了 802.1X Guest VLAN，为保证各种功能的正常使用，请为端口的缺省 VLAN 和 802.1X 的 Guest VLAN 分配不同的 VLAN ID。

配置 802.1X Guest VLAN 之前，需要进行以下配置准备：

- 创建需要配置为 Guest VLAN 的 VLAN。
- 在接入控制方式为 Port-based 的端口上，保证 802.1X 的组播触发功能处于开启状态。

表1-16 配置指定端口的 802.1X Guest VLAN

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
配置指定端口的802.1X Guest VLAN	**dot1x guest-vlan** *guest-vlan-id*	缺省情况下，端口没有配置802.1X Guest VLAN 不同的端口可以指定不同的802.1X Guest VLAN，一个端口最多只能指定一个802.1X Guest VLAN

1.5.15 配置 802.1X Auth-Fail VLAN


提示

如果用户端设备发出的是携带 Tag 的数据流，且接入端口上使能了 802.1X 认证并配置了 802.1X Auth-Fail VLAN，为保证各种功能的正常使用，请为端口的缺省 VLAN 和 802.1X 的 Auth-Fail VLAN 分配不同的 VLAN ID。

配置 802.1X Auth-Fail VLAN 之前，需要进行以下配置准备：

- 创建需要配置为 Auth-Fail VLAN 的 VLAN。

- 在接入控制方式为 Port-based 的端口上，保证 802.1X 的组播触发功能处于开启状态。

表1-17 配置指定端口的 802.1X Auth-Fail VLAN

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
配置指定端口的802.1X Auth-Fail VLAN	**dot1x auth-fail vlan** *authfail-vlan-id*	缺省情况下，端口没有配置802.1X Auth-Fail VLAN 不同的端口可以指定不同的802.1X Auth-Fail VLAN，一个端口最多只能指定一个802.1X Auth-Fail VLAN

1.5.16 配置 802.1X Critical VLAN

提示

如果用户端设备发出的是携带 Tag 的数据流，且接入端口上使能了 802.1X 认证并配置了 802.1X Critical VLAN，为保证各种功能的正常使用，请为端口的缺省 VLAN 和 802.1X 的 Critical VLAN 分配不同的 VLAN ID。

配置 802.1X Critical VLAN 之前，需要进行以下配置准备：

- 创建需要配置为 Critical VLAN 的 VLAN。
- 在接入控制方式为 Port-based 的端口上，保证 802.1X 的组播触发功能处于开启状态。

当端口加入 802.1X Critical VLAN 后，如果发现有认证服务器可达（目前，只针对 RADIUS 认证服务器不可达），则通知 802.1X 客户端进行认证。

接入控制方式为 Port-based 时，当发现有认证服务器可达后，处于 Critical VLAN 的端口会主动发送组播报文，触发端口上的客户端进行 802.1X 认证。

需要注意的是：

- 若端口已经处于 802.1X Auth-Fail VLAN，则当所有认证服务器都不可达时，端口并不会离开当前的 VLAN 而加入 802.1X Critical VLAN。
- 若端口已经处于 802.1X Guest VLAN，则当所有认证服务器都不可达时，端口会离开当前的 VLAN 并加入 802.1X Critical VLAN。

表1-1 配置指定端口的 802.1X Critical VLAN

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-

配置步骤	命令	说明
配置指定端口的802.1X Critical VLAN	**dot1x critical vlan** *vlan-id*	缺省情况下，端口没有配置802.1X Critical VLAN 不同的端口可以指定不同的802.1X Critical VLAN，一个端口最多只能指定一个802.1X Critical VLAN

1.5.17 配置 802.1X支持的域名分隔符

每个接入用户都属于一个ISP域，该域是由用户登录时提供的用户名决定的，若用户名中携带域名，则设备使用该域中的 AAA 配置对用户进行认证、授权和计费，否则使用系统中的缺省域；若设备指定了 802.1X 的强制认证域，则无论用户名中是否携带域名，设备均使用指定的强制认证域。因此，设备能够准确解析用户名中的纯用户名和域名对于为用户提供认证服务非常重要。由于不同的802.1X 客户端所支持的用户名域名分隔符不同，为了更好地管理和控制不同用户名格式的 802.1X 用户接入，需要在设备上指定 802.1X 可支持的域名分隔符。

目前，802.1X 支持的域名分隔符包括@、\和/，对应的用户名格式分别为 *username@domain-name*，*domain-name\username* 和 *username/domain-name*，其中 *username* 为纯用户名、*domain-name* 为域名。如果用户名中包含有多个域名分隔符字符，则设备仅将最后一个出现的域名分隔符识别为实际使用的域名分隔符，例如，用户输入的用户名为 123/22\@abc，设备上指定 802.1X 支持的域名分隔符为/、\，则识别出的纯用户名为@abc，域名为 123/22。

需要注意的是：

- 如果用户输入的用户名中不包含任何 802.1X 可支持的域名分隔符，则设备会认为该用户名并未携带域名，则使用系统中的缺省域对该用户进行认证。
- 若设备上指定发送给认证服务器的用户名携带域名（**user-name-format with-domain**），则发送给认证服务器的用户名包括三个部分：识别出的纯用户名、域名分隔符@、最终使用的认证域名。例如，用户输入的用户名为 123/22\@abc，指定 802.1X 支持的域名分隔符为/、\，最终使用的认证域为 xyz，则发送给认证服务器的用户名为@abc@xyz。**user-name-format** 命令的具体介绍请参考“安全命令参考”中的“AAA”。
- 为保证用户信息可在认证服务器上被准确匹配到，设备上指定的 802.1X 支持的域名分隔符必须与认证服务器支持的域名分隔符保持一致，否则可能会因为服务器匹配用户失败而导致用户认证失败。

表1-18 指定 802.1X 支持的域名分隔符

配置步骤	命令	说明
进入系统视图	**system-view**	-
指定802.1X支持的域名分隔符	**dot1x domain-delimiter** *string*	缺省情况下，仅支持域名分隔符@

1.6 配置802.1X SmartOn功能

开启了 SmartOn 功能的端口上收到 802.1X 客户端发送的 EAPOL-Start 报文，将向其回复单播的 EAP-Request/Notification 报文，并开启 SmartOn 通知请求超时定时器定时器（**dot1x smarton timer supp-timeout**）等待客户端响应的 EAP-Response/Notification 报文。若 SmartOn 通知请求超时定时器超时后客户端仍未回复，则设备会重发 EAP-Request/Notification 报文，并重新启动该定时器。当重发次数达到规定的最大次数（**dot1x smarton retry**）后，会停止对该客户端的 802.1X 认证；若在重发次数达到最大次数之前收到了该 Notification 报文的回复报文，则获取该报文中携带的 Switch ID 和 SmartOn 密码的 MD5 摘要，并与设备本地配置的 SmartOn 的 Switch ID 以及 SmartOn 密码的 MD5 摘要值比较，若相同，则继续客户端的 802.1X 认证，否则中止客户端的 802.1X 认证。

需要注意的是，802.1X SmartOn 功能与在线用户握手功能互斥，建议两个功能不要同时开启。

表1-19 配置 802.1X SmartOn 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
开启端口的SmartOn功能	**dot1x smarton**	缺省情况下，端口的SmartOn功能处于关闭状态 SmartOn功能与802.1X的在线用户握手功能互斥
退回系统视图	**quit**	-
配置SmartOn的Switch ID	**dot1x smarton switchid** *switch-string*	缺省情况下，未配置SmartOn的Switch ID
配置SmartOn密码	**dot1x smarton password** { **cipher** *cipher-string* | **simple** *plain-string* }	缺省情况下，未配置SmartOn密码
（可选）配置SmartOn通知请求超时定时器时长	**dot1x smarton timer supp-timeout**	缺省情况下，SmartOn通知请求超时定时器时长为30秒
（可选）配置重发SmartOn通知请求报文的最大次数	**dot1x smarton retry** *retries*	缺省情况下，重发SmartOn通知请求报文的最大次数为3次

1.7 802.1X显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 802.1X 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** 命令可以清除 802.1X 的统计信息。

表1-20 802.1X 显示和维护

操作	命令
显示802.1X的会话连接信息、相关统计信息或配置信息	**display dot1x** [**sessions** | **statistics**] [**interface** *interface-type interface-number*]
显示当前802.1X在线用户的详细信息（MSR 2600/MSR 3600）	**display dot1x connection** [**interface** *interface-type interface-number* | **user-mac** *mac-addr* | **user-name** *name-string*]
显示当前802.1X在线用户的详细信息（MSR 5600）	**display dot1x connection** [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-addr* | **user-name** *name-string*]
清除802.1X的统计信息	**reset dot1x statistics** [**interface** *interface-type interface-number*]
清除Guest VLAN内802.1X用户	**reset dot1x guest-vlan interface** *interface-type interface-number* [**mac-address** *mac-address*]

1.8 802.1X典型配置举例

1.8.1 802.1X认证配置举例

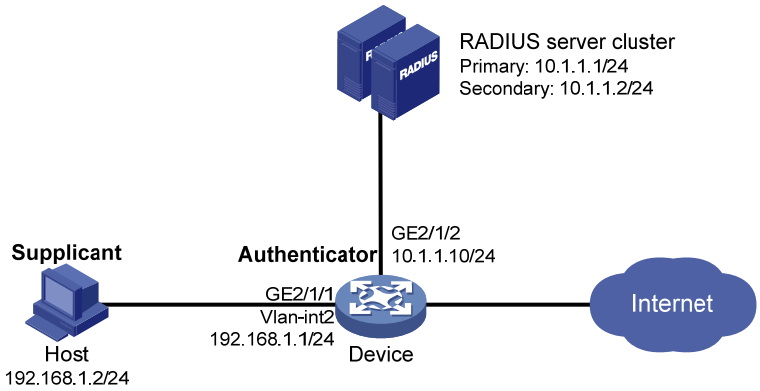
1. 组网需求

用户通过 Device 的端口 GigabitEthernet2/1/1 接入网络，设备对该端口接入的用户进行 802.1X 认证以控制其访问 Internet，具体要求如下：

- 由两台 RADIUS 服务器组成的服务器组与 Device 相连，其 IP 地址分别为 10.1.1.1/24 和 10.1.1.2/24，使用前者作为主认证/计费服务器，使用后者作为备份认证/计费服务器。
- 端口 GigabitEthernet2/1/1 下的所有接入用户均需要单独认证，当某个用户下线时，也只有该用户无法使用网络。
- 认证时，首先进行 RADIUS 认证，如果 RADIUS 服务器没有响应则进行本地认证。
- 所有接入用户都属于同一个 ISP 域 bbb。
- Device 与 RADIUS 认证服务器交互报文时的共享密钥为 name、与 RADIUS 计费服务器交互报文时的共享密钥为 money。

2. 组网图

图1-11 802.1X 认证组网图



3. 配置步骤

说明

- 下述配置步骤中包含了若干 AAA/RADIUS 协议的配置命令，关于这些命令的详细介绍请参见“安全命令参考”中的“AAA”。
- 完成 802.1X 客户端的配置。若使用 H3C iNode 802.1X 客户端，为保证备选的本地认证可成功进行，请确认 802.1X 连接属性中的“上传客户端版本号”选项未被选中。
- 完成 RADIUS 服务器的配置，添加用户帐户，保证用户的认证/授权/计费功能正常运行。

(1) 配置各接口的 IP 地址（略）

(2) 配置本地用户

添加网络接入类本地用户，用户名为 localuser，密码为明文输入的 localpass。（此处添加的本地用户的用户名和密码需要与服务器端配置的用户名和密码保持一致，本例中的 localuser 仅为示例，请根据实际情况配置）

```
<Device> system-view
[Device] local-user localuser class network
[Device-luser-network-localuser] password simple localpass
```

配置本地用户的服务类型为 lan-access。

```
[Device-luser-network-localuser] service-type lan-access
[Device-luser-network-localuser] quit
```

(3) 配置 RADIUS 方案

创建 RADIUS 方案 radius1 并进入其视图。

```
[Device] radius scheme radius1
```

配置主认证/计费 RADIUS 服务器的 IP 地址。

```
[Device-radius-radius1] primary authentication 10.1.1.1
[Device-radius-radius1] primary accounting 10.1.1.1
```

配置备份认证/计费 RADIUS 服务器的 IP 地址。

```
[Device-radius-radius1] secondary authentication 10.1.1.2
```

```
[Device-radius-radius1] secondary accounting 10.1.1.2
```

配置 Device 与认证/计费 RADIUS 服务器交互报文时的共享密钥。

```
[Device-radius-radius1] key authentication simple name
[Device-radius-radius1] key accounting simple money
```

配置发送给 RADIUS 服务器的用户名不携带域名。

```
[Device-radius-radius1] user-name-format without-domain
[Device-radius-radius1] quit
```

说明

发送给服务器的用户名是否携带域名与服务器端是否接受携带域名的用户名以及服务器端的配置有关:

- 若服务器端不接受携带域名的用户名,或者服务器上配置的用户认证所使用的服务不携带域名后缀，则 Device 上指定不携带用户名（**without-domain**）;
- 若服务器端可接受携带域名的用户名，且服务器上配置的用户认证所使用的服务携带域名后缀，则 Device 上指定携带用户名（**with-domain**）。

(4) 配置 ISP 域

创建域 bbb 并进入其视图。

```
[Device] domain bbb
```

配置 802.1X 用户使用 RADIUS 方案 radius1 进行认证、授权、计费，并采用 local 作为备选方法。

```
[Device-isp-bbb] authentication lan-access radius-scheme radius1 local
[Device-isp-bbb] authorization lan-access radius-scheme radius1 local
[Device-isp-bbb] accounting lan-access radius-scheme radius1 local
[Device-isp-bbb] quit
```

(5) 配置 802.1X

开启端口 GigabitEthernet2/1/1 的 802.1X。

```
[Device] interface gigabitethernet 2/1/1
[Device-GigabitEthernet2/1/1] dot1x
```

配置端口的 802.1X 接入控制方式为 **mac-based**（该配置可选，因为端口的接入控制在缺省情况下就是基于 MAC 地址的）。

```
[Device-GigabitEthernet2/1/1] dot1x port-method macbased
```

指定端口上接入的 802.1X 用户使用强制认证域 bbb。

```
[Device-GigabitEthernet2/1/1] dot1x mandatory-domain bbb
[Device-GigabitEthernet2/1/1] quit
```

开启全局 802.1X。

```
[Device] dot1x
```

4. 验证配置

使用命令 **display dot1x interface** 可以查看端口 GigabitEthernet2/1/1 上的 802.1X 的配置情况。当 802.1X 用户输入正确的用户名和密码成功上线后，可使用命令 **display dot1x sessions** 查看到上线用户的连接情况。

1.8.2 802.1X支持Guest VLAN、授权VLAN下发配置举例

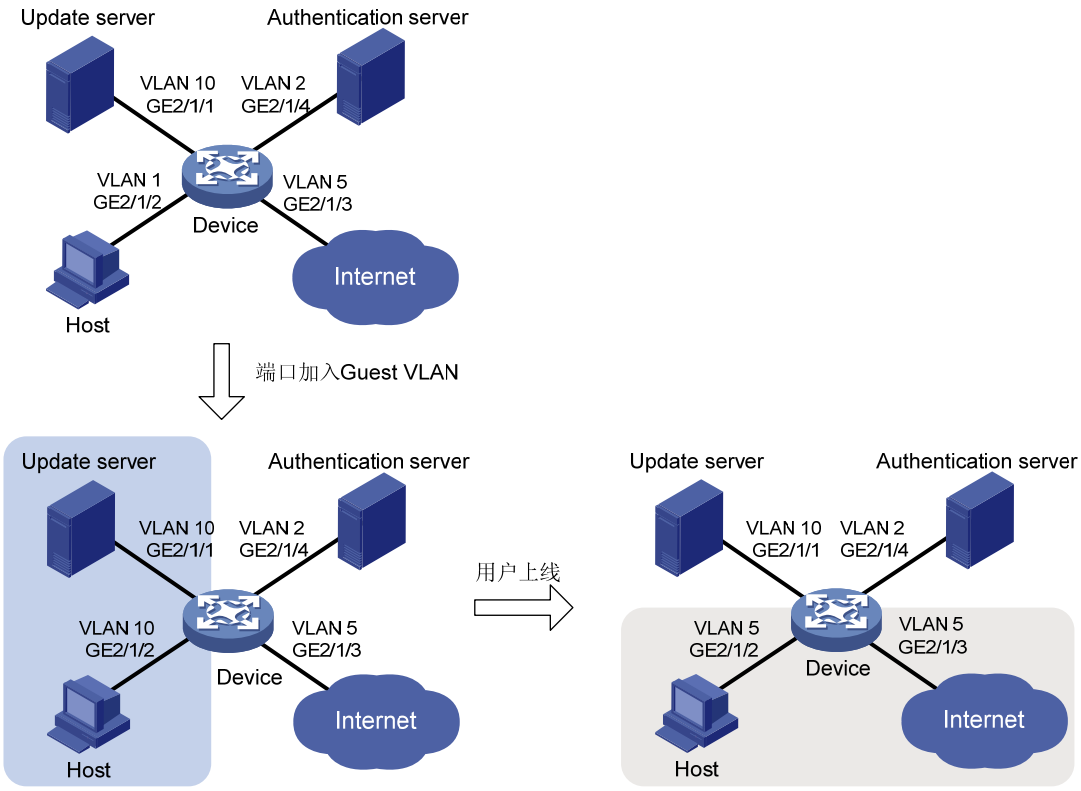
1. 组网需求

如 图 1-12 所示，一台主机通过 802.1X认证接入网络，认证服务器为RADIUS服务器。Host接入Device的端口GigabitEthernet2/1/2 在VLAN 1 内；认证服务器在VLAN 2 内；Update Server是用于客户端软件下载和升级的服务器，在VLAN 10 内；Device 连接 Internet 网络的端口 GigabitEthernet2/1/3 在VLAN 5 内。现有如下组网需求：

- 若一定的时间内端口上无客户端进行认证，则将该端口 GigabitEthernet2/1/2 加入 Guest VLAN（VLAN 10）中，此时 Host 和 Update Server 都在 VLAN 10 内，Host 可以访问 Update Server 并下载 802.1X 客户端。
- 用户认证成功上线后，认证服务器下发 VLAN 5，此时 Host 和连接 Internet 网络的端口 GigabitEthernet2/1/3 都在 VLAN 5 内，Host 可以访问 Internet。

2. 组网图

图1-12 Guest VLAN 及 VLAN 下发组网图



3. 配置步骤

说明

- 下述配置步骤中包含了若干 AAA/RADIUS 协议的配置命令，关于这些命令的详细介绍请参见“安全命令参考”中的“AAA”。
- 保证接入端口加入 Guest VLAN 或授权 VLAN 之后，802.1X 客户端能够及时更新 IP 地址，以实现与相应网络资源的互通。
- 完成 RADIUS 服务器的配置，添加用户帐户，指定要授权下发的 VLAN（本例中为 VLAN 5），并保证用户的认证/授权/计费功能正常运行。

(1) 创建 VLAN 并将端口加入对应 VLAN

```
<Device> system-view
[Device] vlan 1
[Device-vlan1] port gigabitethernet 2/1/2
[Device-vlan1] quit
[Device] vlan 10
[Device-vlan10] port gigabitethernet 2/1/1
[Device-vlan10] quit
[Device] vlan 2
[Device-vlan2] port gigabitethernet 2/1/4
[Device-vlan2] quit
[Device] vlan 5
[Device-vlan5] port gigabitethernet 2/1/3
[Device-vlan5] quit
```

(2) 配置 RADIUS 方案

创建 RADIUS 方案 2000 并进入其视图。

```
[Device] radius scheme 2000
```

配置主认证/计费 RADIUS 服务器及其共享密钥。

```
[Device-radius-2000] primary authentication 10.11.1.1 1812
[Device-radius-2000] primary accounting 10.11.1.1 1813
[Device-radius-2000] key authentication simple abc
[Device-radius-2000] key accounting simple abc
```

配置发送给 RADIUS 服务器的用户名不携带域名。

```
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

(3) 配置 ISP 域

创建域 bbb 并进入其视图。

```
[Device] domain bbb
```

配置 802.1X 用户使用 RADIUS 方案 2000 进行认证、授权、计费。

```
[Device-isp-bbb] authentication lan-access radius-scheme 2000
[Device-isp-bbb] authorization lan-access radius-scheme 2000
[Device-isp-bbb] accounting lan-access radius-scheme 2000
[Device-isp-bbb] quit
```

(4) 配置 802.1X

开启端口 GigabitEthernet2/1/2 的 802.1X。

```
[Device] interface gigabitethernet 2/1/2
[Device-GigabitEthernet2/1/2] dot1x
```

配置端口的 802.1X 接入控制的方式为 **portbased**。

```
[Device-GigabitEthernet2/1/2] dot1x port-method portbased
```

配置端口的 802.1X 授权状态为 **auto**。（此配置可选，端口的授权状态缺省为 **auto**）

```
[Device-GigabitEthernet2/1/2] dot1x port-control auto
```

配置端口的 802.1X Guest VLAN 为 VLAN10。

```
[Device-GigabitEthernet2/1/2] dot1x guest-vlan 10
[Device-GigabitEthernet2/1/2] quit
```

开启全局 802.1X。

```
[Device] dot1x
```

4. 验证配置结果

可以通过命令 **display dot1x interface** 查看端口 GigabitEthernet2/1/2 上 Guest VLAN 的配置情况。

若在指定的时间之内无客户端进行认证或者无客户端认证成功，则通过命令 **display vlan** 10 可以查看到端口 GigabitEthernet2/1/2 加入了配置的 Guest VLAN。

在用户认证成功之后，通过命令 **display interface** 可以看到用户接入的端口 GigabitEthernet2/1/2 加入了认证服务器下发的 VLAN 5 中。

1.8.3 802.1X SmartOn功能典型配置举例

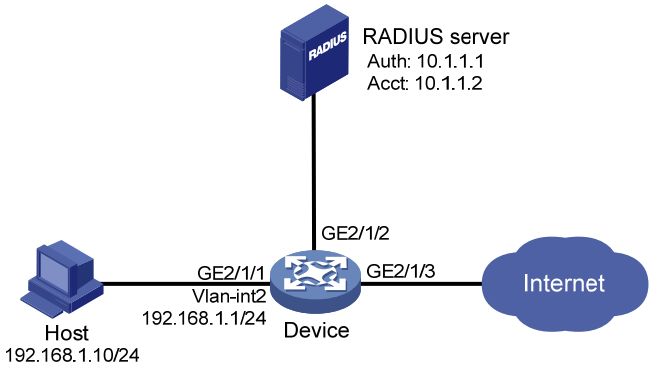
1. 组网需求

如 图 1-13 所示，某用户的工作站与Switch的端口GigabitEthernet2/1/1 相连接。Switch的管理者希望在端口上对接入用户进行 802.1X认证，以控制其访问Internet。同时，启用SmartOn功能，通过辨别Switch ID和密码来决定用户是否能进行正常的 802.1X认证过程。具体要求如下：

- SmartOn 密码为明文密码 1234，Switch ID 为 XYZ。
- SmartOn 客户端的超时时间为 40 秒。

2. 组网图

图1-13 802.1X SmartOn 典型配置组网图



3. 配置步骤

开启端口 GigabitEthernet2/1/1 的 802.1X 认证。

```
<Device> system-view
[Device] interface gigabitethernet 2/1/1
[Device-GigabitEthernet2/1/1] dot1x
```

在端口 GigabitEthernet2/1/1 上使能 SmartOn 功能。

```
[Device-GigabitEthernet2/1/1] dot1x smarton
[Device-GigabitEthernet2/1/1] quit
```

配置 SmartOn 密码为明文 1234，Switch ID 为 XYZ。

```
[Device] dot1x smarton password simple 1234
[Device] dot1x smarton switchid XYZ
```

配置 SmartOn 客户端的超时时间为 40 秒。

```
[Device] dot1x smarton timer supp-timeout 40
```

配置 RADIUS 方案。

```
[Device] radius scheme 2000
[Device-radius-2000] primary authentication 10.1.1.1 1812
[Device-radius-2000] primary accounting 10.1.1.2 1813
[Device-radius-2000] key authentication simple abc
[Device-radius-2000] key accounting simple abc
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

配置 ISP 域的 AAA 方法。

```
[Device] domain bbb
[Device-isp-bbb] authentication lan-access radius-scheme 2000
[Device-isp-bbb] authorization lan-access radius-scheme 2000
[Device-isp-bbb] accounting lan-access radius-scheme 2000
[Device-isp-bbb] quit
```

全局开启 802.1X。

```
[Device] dot1x
```

目 录

1 MAC地址认证

说明

本特性仅在安装了 HMIM-24GSW/24GSWP 和 HMIM-8GSW 交换卡的款型以及 MSR3600-28/MSR3600-51 的固定二层接口上支持。

1.1 MAC地址认证简介

1.1.1 MAC地址认证概述

MAC 地址认证是一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法，它不需要用户安装任何客户端软件。设备在启动了 MAC 地址认证的端口上首次检测到用户的 MAC 地址以后，即启动对该用户的认证操作。认证过程中，不需要用户手动输入用户名或者密码。若该用户认证成功，则允许其通过端口访问网络资源，否则该用户的 MAC 地址就被设置为静默 MAC。在静默时间内（可通过静默定时器配置），来自此 MAC 地址的用户报文到达时，设备直接做丢弃处理，以防止非法 MAC 短时间内的重复认证。

说明

若配置的静态 MAC 或者当前认证通过的 MAC 地址与静默 MAC 相同，则 MAC 地址认证失败后的 MAC 静默功能将会失效。

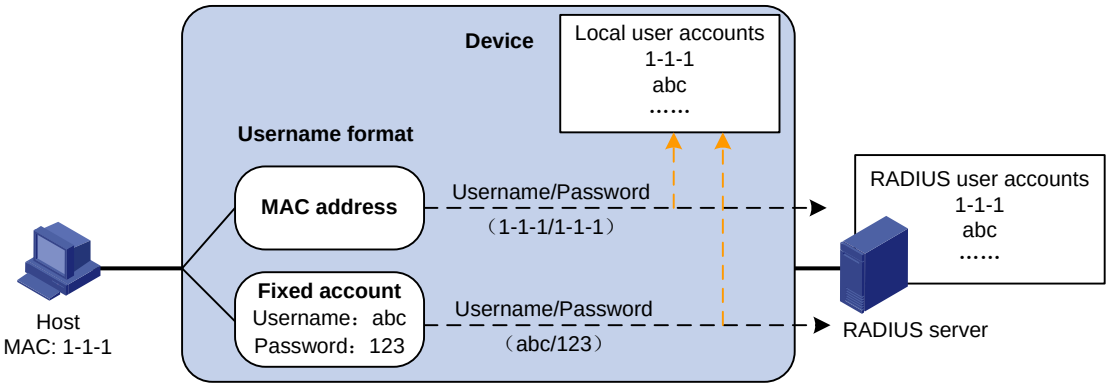
1.1.2 使用不同用户名格式的MAC地址认证

目前设备支持两种方式的 MAC 地址认证，通过 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器进行远程认证和在接入设备上进行本地认证。有关远程 RADIUS 认证和本地认证的详细介绍请参见“安全配置指导”中的“AAA”。

根据设备最终用于验证用户身份的用户名格式和内容的不同，可以将 MAC 地址认证使用的用户帐户格式分为两种类型：

- MAC 地址用户名格式：使用用户的 MAC 地址作为认证时的用户名和密码；
- 固定用户名格式：不论用户的 MAC 地址为何值，所有用户均使用设备上指定的一个固定用户名和密码替代用户的 MAC 地址作为身份信息进行认证。由于同一个端口下可以有多个用户进行认证，因此这种情况下端口上的所有 MAC 地址认证用户均使用同一个固定用户名进行认证，服务器端仅需要配置一个用户帐户即可满足所有认证用户的认证需求，适用于接入客户端比较可信的网络环境。

图1-1 不同用户名格式下的 MAC 地址认证示意图



1. RADIUS服务器认证方式进行MAC地址认证

当选用 RADIUS 服务器认证方式进行 MAC 地址认证时，设备作为 RADIUS 客户端，与 RADIUS 服务器配合完成 MAC 地址认证操作：

- 若采用 MAC 地址用户名格式，则设备将检测到的用户 MAC 地址作为用户名和密码发送给 RADIUS 服务器进行验证。
- 若采用固定用户名格式，则设备将一个已经在本地指定的 MAC 地址认证用户使用的固定用户名和对应的密码作为待认证用户的用户名和密码，发送给 RADIUS 服务器进行验证。

RADIUS 服务器完成对该用户的认证后，认证通过的用户可以访问网络。

2. 本地认证方式进行MAC地址认证

当选用本地认证方式进行 MAC 地址认证时，直接在设备上完成对用户的认证。需要在设备上配置本地用户名和密码：

- 若采用 MAC 地址用户名格式，则设备将检测到的用户 MAC 地址作为待认证用户的用户名和密码与配置的本地用户名和密码进行匹配。
- 若采用固定用户名，则设备将一个已经在本地指定的 MAC 地址认证用户使用的固定用户名和对应的密码作为待认证用户的用户名和密码与配置的本地用户名和密码进行匹配。

用户名和密码匹配成功后，用户可以访问网络。

1.2 MAC地址认证支持VLAN下发

1.2.1 授权VLAN

为了将受限的网络资源与未认证用户隔离，通常将受限的网络资源和未认证的用户划分到不同的 VLAN。MAC 地址认证支持远程 AAA 服务器/接入设备下发授权 VLAN，即当用户通过 MAC 地址认证后，远程 AAA 服务器/接入设备将指定的受限网络资源所在的 VLAN 作为授权 VLAN 下发到用户进行认证的端口。该端口被加入到授权 VLAN 中后，用户便可以访问这些受限的网络资源。

设备根据用户接入的端口链路类型，按以下三种情况将端口加入到下发的授权 VLAN 中。

- 若用户从 Access 类型的端口接入，则端口离开当前 VLAN 并加入第一个通过认证的用户的授权 VLAN 中。

- 若用户从 Trunk 类型的端口接入，则设备允许下发的授权 VLAN 通过该端口，并且修改该端口的缺省 VLAN 为第一个通过认证的用户的授权 VLAN。
- 若用户从 Hybrid 类型的端口接入，则设备允许授权下发的 VLAN 以不携带 Tag 的方式通过该端口，并且修改该端口的缺省 VLAN 为第一个通过认证的用户的授权 VLAN。需要注意的是，若该端口上使能了 MAC VLAN 功能，则设备将根据认证服务器/接入设备下发的授权 VLAN 动态地创建基于用户 MAC 地址的 VLAN，而端口的缺省 VLAN 并不改变。

1.3 MAC地址认证配置任务简介

表1-1 MAC 地址认证配置任务简介

配置任务	说明	详细配置
开启MAC地址认证	必选	1.4
配置MAC地址认证用户使用的认证域	可选	1.5
配置MAC地址认证用户名格式	可选	1.6
配置MAC地址认证定时器	可选	1.7
配置端口上最多允许同时接入的MAC地址认证用户数	可选	1.8
配置MAC地址认证延迟功能	可选	1.9
配置接口工作在MAC地址认证的多VLAN模式	可选	1.10
配置MAC地址认证的重认证不可达动作	可选	1.11

1.4 开启MAC地址认证

1. 配置准备

(1) 缺省情况下，对端口上接入的用户进行MAC地址认证时，使用系统缺省的认证域（由命令**domain default enable**指定）。若需要使用非缺省的认证域进行MAC地址认证，则需指定MAC地址认证用户使用的认证域（参见“1.5 指定MAC地址认证用户使用的认证域”），并配置该认证域。认证域的具体配置请参见“安全配置指导”中的“AAA”。

- 若采用本地认证方式，还需创建本地用户并设置其密码，且本地用户的服务类型应设置为**lan-access**。
- 若采用远程 RADIUS 认证方式，需要确保设备与 RADIUS 服务器之间的路由可达，并添加 MAC 地址认证用户帐号。

(2) 保证端口安全功能关闭。具体配置请参见“安全配置指导”中的“端口安全”。

2. 配置步骤

说明

端口上开启 MAC 地址认证之前，请保证端口未加入聚合组或业务环回组。

只有全局和端口的 MAC 地址认证均开启后，MAC 地址认证配置才能在端口上生效。

表1-2 开启 MAC 地址认证

操作	命令	说明
进入系统视图	**system-view**	-
开启全局MAC地址认证	**mac-authentication**	缺省情况下，全局的MAC地址认证处于关闭状态
进入接口视图	**interface** *interface-type interface-number*	-
开启端口MAC地址认证	**mac-authentication**	缺省情况下，端口的MAC地址认证处于关闭状态

1.5 指定MAC地址认证用户使用的认证域

为了便于接入设备的管理员更为灵活地部署用户的接入策略，设备支持指定 MAC 地址认证用户使用的认证域，可以通过以下两种配置实现：

- 在系统视图下指定一个认证域，该认证域对所有开启了 MAC 地址认证的端口生效。
- 在接口视图下指定该端口的认证域，不同的端口可以指定不同的认证域。

端口上接入的 MAC 地址认证用户将按照如下顺序选择认证域：端口上指定的认证域-->系统视图下指定的认证域-->系统缺省的认证域。关于认证域的相关介绍请参见“安全配置指导”中的“AAA”。

表1-3 指定 MAC 地址认证用户使用的认证域

配置步骤	命令	说明
进入系统视图	**system-view**	-
指定MAC地址认证用户使用的认证域	**mac-authentication domain** *domain-name*	二者至少选其一 缺省情况下，未指定MAC地址认证用户使用的认证域，使用系统缺省的认证域
	interface *interface-type interface-number* **mac-authentication domain** *domain-name*	

1.6 配置MAC地址认证用户名格式

表1-4 配置 MAC 地址认证用户名格式

操作		命令	说明
进入系统视图		**system-view**	-
配置MAC地址认证用户的用户名格式	MAC地址格式	**mac-authentication user-name-format mac-address** [{ **with-hyphen** | **without-hyphen** } [**lowercase** | **uppercase**]]	二者选其一 缺省情况下，使用用户的MAC地址作为用户名与密码，其中字母为小写，且不带连字符。
	固定用户名格式	**mac-authentication user-name-format fixed** [**account** *name*] [**password** { **cipher** | **simple** } *password*]	

1.7 配置MAC地址认证定时器

可配置的 MAC 地址认证定时器包括以下几种：

- 下线检测定时器（**offline-detect**）：用来设置用户空闲超时的时间间隔。若设备在一个下线检测定时器间隔之内，没有收到某在线用户的报文，将切断该用户的连接，同时通知 RADIUS 服务器停止对其计费。
- 静默定时器（**quiet**）：用来设置用户认证失败以后，设备停止对其提供认证服务的时间间隔。在静默期间，设备不对来自认证失败用户的报文进行认证处理，直接丢弃。静默期后，如果设备再次收到该用户的报文，则依然可以对其进行认证处理。
- 服务器超时定时器（**server-timeout**）：用来设置设备同 RADIUS 服务器的连接超时时间。在用户的认证过程中，如果到服务器超时定时器超时时设备一直没有收到 RADIUS 服务器的应答，则设备将在相应的端口上禁止此用户访问网络。

表1-5 配置 MAC 地址认证定时器

操作	命令	说明
进入系统视图	**system-view**	-
配置MAC地址认证定时器	**mac-authentication timer** { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **server-timeout** *server-timeout-value* }	缺省情况下，下线检测定时器为300秒，静默定时器为60秒，服务器超时定时器取值为100秒

1.8 配置端口上最多允许同时接入的MAC地址认证用户数

由于系统资源有限，如果当前端口下接入的用户过多，接入用户之间会发生资源的争用，因此适当地配置该值可以使端口上已经接入的用户获得可靠的性能保障。

表1-6 配置端口上最多允许同时接入的 MAC 地址认证用户数

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置端口上最多允许同时接入的MAC地址认证用户数	**mac-authentication max-user** *user-number*	缺省情况下，端口上最多允许同时接入的MAC地址认证用户数为256

1.9 配置MAC地址认证延迟功能

端口同时开启了 MAC 地址认证和 802.1X 认证的情况下，某些组网环境中希望设备对用户报文先进行 802.1X 认证。例如，有些客户端在发送 802.1X 认证请求报文之前，就已经向设备发送了其它报

文，比如 DHCP 报文，因而触发了并不期望的 MAC 地址认证。这种情况下，就可以开启端口的 MAC 地址认证延时功能。

开启端口的 MAC 地址认证延时功能之后，端口就不会在收到用户报文时立即触发 MAC 地址认证，而是会等待一定的延迟时间，若在此期间该用户一直未进行 802.1X 认证或未成功通过 802.1X 认证，则延迟时间超时后端口会对之前收到的用户报文进行 MAC 地址认证。

需要注意的是，开启了 MAC 地址认证延迟功能的接口上不建议同时配置端口安全的模式为 **mac-else-userlogin-secure** 或 **mac-else-userlogin-secure-ext**，否则 MAC 地址认证延迟功能不生效。端口安全模式的具体配置请参见“安全配置指导”中的“端口安全”。

表1-7 配置 MAC 地址认证延迟功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
开启MAC地址认证延迟功能，并指定延迟时间	**mac-authentication timer auth-delay** *time*	缺省情况下，MAC地址认证延迟功能处于关闭状态

1.10 配置接口工作在MAC地址认证的多VLAN模式

缺省情况下，如果已上线用户在属于不同 VLAN 的相同接口再次接入，设备将让原用户下线，使得该用户能够在新的 VLAN 内重新开始认证。接口工作在多 VLAN 模式下时，如果相同 MAC 地址的用户在属于不同 VLAN 的相同接口再次接入，设备将能够允许用户的流量在新的 VLAN 内通过，且允许该用户的报文无需重新认证而在多个 VLAN 中转发。

对于接入 IP 电话类用户的端口，指定接口工作在 MAC 地址认证的多 VLAN 模式，可避免 IP 电话终端的报文所携带的 VLAN tag 发生变化后，因用户流量需要重新认证带来语音报文传输质量受干扰的问题。

需要注意的是，指定接口工作在 MAC 地址认证的多 VLAN 模式之后，将不允许给该接口上的 MAC 地址认证用户下发授权 VLAN，否则用户认证失败。

表1-8 配置接口工作在 MAC 地址认证的多 VLAN 模式

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
指定接口工作在MAC地址认证的多VLAN模式	**mac-authentication host-mode multi-vlan**	缺省情况下，同一个MAC地址的用户报文在使能了MAC地址认证的相同的接口上只能在同一个VLAN中通过

1.11 配置MAC地址认证的重认证不可达动作

该功能用于控制端口上的 MAC 地址在线用户重认证时，若认证服务器不可达，设备处理在线用户的方式。在网络连通状况短时间内不良的情况下，合法用户是否会因为服务器不可达而被强制下线，需要结合实际的网络状态来调整。若配置为保持用户在线，当服务器在短时间内恢复可达，则可以避免用户频繁上下线；若配置为强制下线，当服务器可达性在短时间内不可恢复，则可避免用户在线状态长时间与实际不符。

表1-9 配置重认证服务器不可达时保持用户在线状态

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置重认证服务器不可达时端口上的MAC地址认证用户保持在线状态	**mac-authentication re-authenticate server-unreachable keep-online**	缺省情况下，端口上的MAC地址在线用户重认证时，若认证服务器不可达，则用户会被强制下线

1.12 MAC地址认证的显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 MAC 地址认证的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可以清除相关统计信息。

表1-10 MAC 地址认证的显示和维护

操作	命令
显示MAC地址认证的相关信息	**display mac-authentication** [**interface** *interface-type interface-number*]
显示MAC地址认证连接信息（MSR 2600/MSR 3600）	**display mac-authentication connection** [**interface** *interface-type interface-number* | **user-mac** *mac-addr* | **user-name** *user-name*]
显示MAC地址认证连接信息（MSR 5600）	**display mac-authentication connection** [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-addr* | **user-name** *user-name*]
清除MAC地址认证的统计信息	**reset mac-authentication statistics** [**interface** *interface-type interface-number*]

1.13 MAC地址认证典型配置举例

1.13.1 本地MAC地址认证

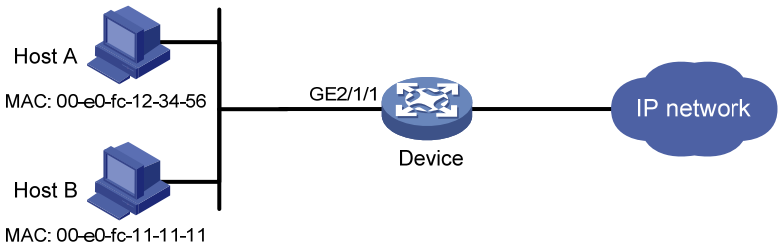
1. 组网需求

如 图 1-2 所示，某子网的用户主机与设备的端口GigabitEthernet2/1/1 相连接。

- 设备的管理者希望在端口 GigabitEthernet2/1/1 上对用户接入进行 MAC 地址认证，以控制它们对 Internet 的访问。
- 要求设备每隔 180 秒就对用户是否下线进行检测；并且当用户认证失败时，需等待 180 秒后才能对用户再次发起认证。
- 所有用户都属于 ISP 域 bbb，认证时使用本地认证的方式。
- 使用用户的 MAC 地址作用户名和密码，其中 MAC 地址带连字符、字母小写。

2. 组网图

图1-2 启动 MAC 地址认证对接入用户进行本地认证



3. 配置步骤

添加网络接入类本地接入用户。本例中添加 Host A 的本地用户，用户名和密码均为 Host A 的 MAC 地址 00-e0-fc-12-34-56，服务类型为 **lan-access**。

```
<Device> system-view
[Device] local-user 00-e0-fc-12-34-56 class network
[Device-luser-network-00-e0-fc-12-34-56] password simple 00-e0-fc-12-34-56
[Device-luser-network-00-e0-fc-12-34-56] service-type lan-access
[Device-luser-network-00-e0-fc-12-34-56] quit
```

配置 ISP 域，使用本地认证方法。

```
[Device] domain bbb
[Device-isp-bbb] authentication lan-access local
[Device-isp-bbb] quit
```

开启端口 GigabitEthernet2/1/1 的 MAC 地址认证。

```
[Device] interface gigabitethernet 2/1/1
[Device-Gigabitethernet2/1/1] mac-authentication
[Device-Gigabitethernet2/1/1] quit
```

配置 MAC 地址认证用户所使用的 ISP 域。

```
[Device] mac-authentication domain bbb
```

配置 MAC 地址认证的定时器。

```
[Device] mac-authentication timer offline-detect 180
[Device] mac-authentication timer quiet 180
```

配置 MAC 地址认证用户名格式：使用带连字符的 MAC 地址作为用户名与密码，其中字母小写。

```
[Device] mac-authentication user-name-format mac-address with-hyphen lowercase
```

开启全局 MAC 地址认证。

```
[Device] mac-authentication
```

4. 验证配置

当用户接入端口 GigabitEthernet2/1/1 之后，可以通过如下显示信息看到 Host A 成功通过认证，处于上线状态，Host B 没有通过认证，它的 MAC 地址被加入静默 MAC 列表。

```
<Device> display mac-authentication
Global MAC authentication parameters:
   MAC authentication     : Enabled
   User name format       : MAC address in lowercase(xx-xx-xx-xx-xx-xx)
           Username       : mac
           Password       : Not configured
   Offline detect period  : 180 s
   Quiet period           : 180 s
   Server timeout         : 100 s
   Authentication domain  : bbb
 Max MAC-auth users       : 1024 per slot
 Online MAC-auth users    : 0

 Silent MAC users:
          MAC address       VLAN ID  From port               Port index
          00e0-fc11-1111    8        Gigabitethernet2/1/1    1
 Gigabitethernet2/1/1 is link-up
   MAC authentication         : Enabled
   Authentication domain      : Not configured
   Auth-delay timer           : Disabled
   Re-auth server-unreachable : Logoff
   Max online users           : 256
   Authentication attempts    : successful 1, failed 0
   Current online users       : 1
          MAC address       Auth state
          00e0-fc12-3456    Authenticated
```

1.13.2 使用RADIUS服务器进行MAC地址认证

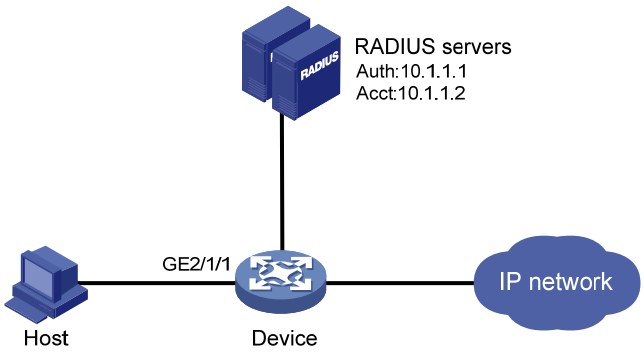
1. 组网需求

如 图 1-3 所示，用户主机Host通过端口GigabitEthernet2/1/1 连接到设备上，设备通过RADIUS服务器对用户进行认证、授权和计费。

- 设备的管理者希望在端口 GigabitEthernet2/1/1 上对用户接入进行 MAC 地址认证，以控制其对 Internet 的访问。
- 要求设备每隔 180 秒就对用户是否下线进行检测；并且当用户认证失败时，需等待 180 秒后才能对用户再次发起认证。
- 所有用户都属于域 2000，认证时采用固定用户名格式，用户名为 aaa，密码为 123456。

2. 组网图

图1-3 启动 MAC 地址认证对接入用户进行 RADIUS 认证



3. 配置步骤

说明

确保 RADIUS 服务器与设备路由可达，并成功添加了接入用户帐户：用户名为 aaa，密码为 123456。

配置 RADIUS 方案。

```
<Device> system-view
[Device] radius scheme 2000
[Device-radius-2000] primary authentication 10.1.1.1 1812
[Device-radius-2000] primary accounting 10.1.1.2 1813
[Device-radius-2000] key authentication simple abc
[Device-radius-2000] key accounting simple abc
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

配置 ISP 域的 AAA 方法。

```
[Device] domain bbb
[Device-isp-bbb] authentication default radius-scheme 2000
[Device-isp-bbb] authorization default radius-scheme 2000
[Device-isp-bbb] accounting default radius-scheme 2000
[Device-isp-bbb] quit
```

开启端口 GigabitEthernet2/1/1 的 MAC 地址认证。

```
[Device] interface gigabitethernet 2/1/1
[Device-Gigabitethernet2/1/1] mac-authentication
[Device-Gigabitethernet2/1/1] quit
```

配置 MAC 地址认证用户所使用的 ISP 域。

```
[Device] mac-authentication domain bbb
```

配置 MAC 地址认证的定时器。

```
[Device] mac-authentication timer offline-detect 180
[Device] mac-authentication timer quiet 180
```

配置 MAC 地址认证使用固定用户名格式：用户名为 aaa，密码为明文 123456。

```
[Device] mac-authentication user-name-format fixed account aaa password simple 123456
```

开启全局 MAC 地址认证。

```
[Device] mac-authentication
```

4. 验证配置

显示 MAC 地址配置信息。

```
<Device> display mac-authentication
Global MAC authentication parameters:
   MAC authentication     : Enabled
   Username format        : Fixed account
           Username       : aaa
           Password       : ******
   Offline detect period  : 180 s
   Quiet period           : 180 s
   Server timeout         : 100 s
   Authentication domain  : bbb
 Max MAC-auth users       : 1024 per slot
 Online MAC-auth users    : 1

 Silent MAC users:
          MAC address       VLAN ID  From port               Port index

 GigabitEthernet2/1/1  is link-down
   MAC authentication         : Enabled
   Authentication domain      : Not configured
   Auth-delay timer           : Disabled
   Re-auth server-unreachable : Logoff
   Max online users           : 256
   Authentication attempts    : successful 1, failed 0
   Current online users       : 0
          MAC address       Auth state
          00e0-fc12-3456    Authenticated
```

目 录

1 Portal

1.1 Portal简介

1.1.1 Portal概述

Portal 在英语中是入口的意思。Portal 认证通常也称为 Web 认证，即通过 Web 页面接受用户输入的用户名和密码，对用户进行身份认证，以达到对用户访问进行控制的目的。在采用了 Portal 认证的组网环境中，未认证用户上网时，接入设备强制用户登录到特定站点，用户可以免费访问其中的服务；当用户需要使用互联网中的其它信息时，必须在 Portal Web 服务器提供的网站上进行 Portal 认证，只有认证通过后才可以使用这些互联网中的设备或资源。

根据是否为用户主动发起认证，可以将 Portal 认证分为主动认证和强制认证两种类型：用户可以主动访问已知的 Portal Web 服务器网站，输入用户名和密码进行认证，这种开始 Portal 认证的方式称作主动认证；用户访问任意非 Portal Web 服务器网站时，被强制访问 Portal Web 服务器网站，继而开始 Portal 认证的过程称作强制认证。

Portal 认证是一种灵活的访问控制技术，可以在接入层以及需要保护的关键数据入口处实施访问控制，具有如下优势：

- 可以不安装客户端软件，直接使用 Web 页面认证，使用方便。
- 可以为运营商提供方便的管理功能和业务拓展功能，例如运营商可以在认证页面上开展广告、社区服务、信息发布等个性化的业务。
- 支持多种组网型态，例如二次地址分配认证方式可以实现灵活的地址分配策略且能节省公网 IP 地址，可跨三层认证方式可以跨网段对用户作认证。

目前，设备支持的 Portal 版本为 Portal 1.0、Portal 2.0 和 Portal 3.0。

1.1.2 Portal安全扩展功能

Portal 的安全扩展功能是指，在 Portal 身份认证的基础之上，通过强制接入终端实施补丁和防病毒策略，加强网络终端对病毒攻击的主动防御能力。具体的安全扩展功能如下：

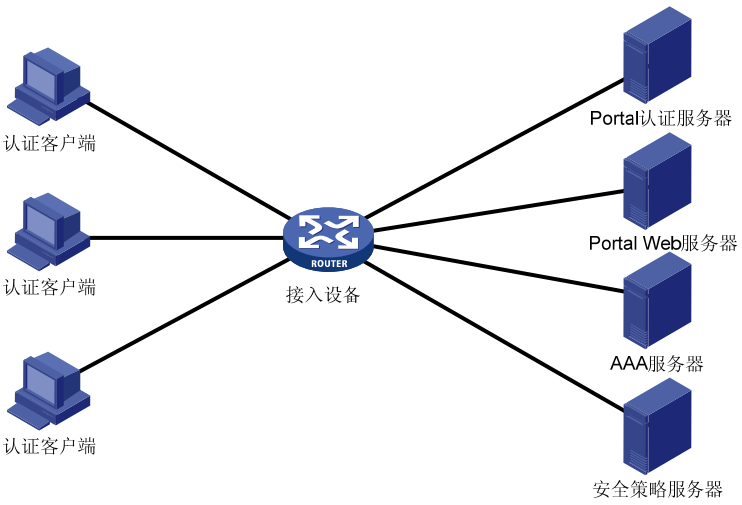
- 安全性检测：在对用户的身份认证的基础上增加了安全认证机制，可以检测接入终端上是否安装了防病毒软件、是否更新了病毒库、是否安装了非法软件、是否更新了操作系统补丁等；
- 访问资源受限：用户通过身份认证后仅仅获得访问指定互联网资源的权限，如病毒服务器、操作系统补丁更新服务器等；当用户通过安全认证后便可以访问更多的互联网资源。

安全性检测功能必须与 H3C 的 iMC 安全策略服务器以及 iNode 客户端配合使用。

1.1.3 Portal的系统组成

Portal的典型组网方式如 图 1-1 所示，它由六个基本要素组成：认证客户端、接入设备、Portal认证服务器、Portal Web服务器、AAA服务器和安全策略服务器。

图1-1 Portal 系统组成示意图



1. 认证客户端

用户终端的客户端系统，为运行 HTTP/HTTPS 协议的浏览器或运行 Portal 客户端软件的主机。对用户终端的安全性检测是通过 Portal 客户端和安全策略服务器之间的信息交流完成的。

2. 接入设备

交换机、路由器等宽带接入设备的统称，主要有三方面的作用：

- 在认证之前，将用户的所有 HTTP 请求都重定向到 Portal Web 服务器。
- 在认证过程中，与 Portal 认证服务器、AAA 服务器交互，完成身份认证/授权/计费的功能。
- 在认证通过后，允许用户访问被授权的互联网资源。

3. Portal认证服务器

接收 Portal 客户端认证请求的服务器端系统，与接入设备交互认证客户端的认证信息。

4. Portal Web服务器

负责向客户端提供 Web 认证页面，并将客户端的认证信息（用户名、密码等）提交给 Portal 认证服务器。Portal Web 服务器通常与 Portal 认证服务器是一体的，也可以是独立的服务器端系统。

5. AAA服务器

与接入设备进行交互，完成对用户的认证、授权和计费。目前 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器可支持对 Portal 用户进行认证、授权和计费，以及 LDAP（Lightweight Directory Access Protocol，轻量级目录访问协议）服务器可支持对 Portal 用户进行认证。

6. 安全策略服务器

与 Portal 客户端、接入设备进行交互，完成对用户的安全检测，并对用户进行安全授权操作。

1.1.4 Portal的基本交互过程

Portal 系统中各基本要素的交互过程如下：

(1) 未认证用户访问网络时，在 Web 浏览器地址栏中输入一个互联网的地址，那么此 HTTP 请求在经过接入设备时会被重定向到 Portal Web 服务器的 Web 认证主页上。用户也可以主动登录 Portal Web 服务器的 Web 认证主页。若需要使用 Portal 的安全扩展认证功能，则用户必须使用 H3C iNode 客户端。

(2) 用户在认证主页/认证对话框中输入认证信息后提交，Portal Web 服务器会将用户的认证信息传递给 Portal 认证服务器，由 Portal 认证服务器处理并转发给接入设备。

(2) 接入设备与 AAA 服务器交互进行用户的认证、授权和计费。

(3) 认证通过后，如果未对用户采用安全策略，则接入设备会打开用户与互联网的通路，允许用户访问互联网；如果对用户采用了安全策略，则客户端、接入设备与安全策略服务器交互，对用户的安全检测通过之后，安全策略服务器根据用户的安全性授权用户访问非受限资源。目前通过访问 Web 页面进行的 Portal 认证不能对用户实施安全策略检查，安全检查功能的实现需要与 H3C iNode 客户端配合。

说明

无论是 Web 客户端还是 H3C iNode 客户端发起的 Portal 认证，均能支持 Portal 认证穿越 NAT，即 Portal 客户端位于私网、Portal 认证服务器位于公网，接入设备上启用 NAT 功能的组网环境下，NAT 地址转换不会对 Portal 认证造成影响，但建议在此组网环境下，将发送 Portal 报文的源地址配置为接口的公网 IP 地址。

1.1.5 Portal的认证方式

Portal 支持三种认证方式：直接认证方式、二次地址分配认证方式和可跨三层认证方式。直接认证方式和二次地址分配认证方式下，认证客户端和接入设备之间没有三层转发设备；可跨三层认证方式下，认证客户端和接入设备之间可以（但不必须）跨接三层转发设备。

1. 直接认证方式

用户在认证前通过手工配置或 DHCP 直接获取一个 IP 地址，只能访问 Portal Web 服务器，以及设定的免认证地址；认证通过后即可访问网络资源。认证流程相对简单。

2. 二次地址分配认证方式

用户在认证前通过 DHCP 获取一个私网 IP 地址，只能访问 Portal Web 服务器，以及设定的免认证地址；认证通过后，用户会申请到一个公网 IP 地址，即可访问网络资源。该认证方式解决了 IP 地址规划和分配问题，对未认证通过的用户不分配公网 IP 地址。例如运营商对于小区宽带用户只在访问小区外部资源时才分配公网 IP。目前，仅 H3C iNode 客户端支持该认证方式。需要注意的是，IPv6 Portal 认证不支持二次地址分配方式。

3. 可跨三层认证方式

和直接认证方式基本相同，但是这种认证方式允许认证用户和接入设备之间跨越三层转发设备。

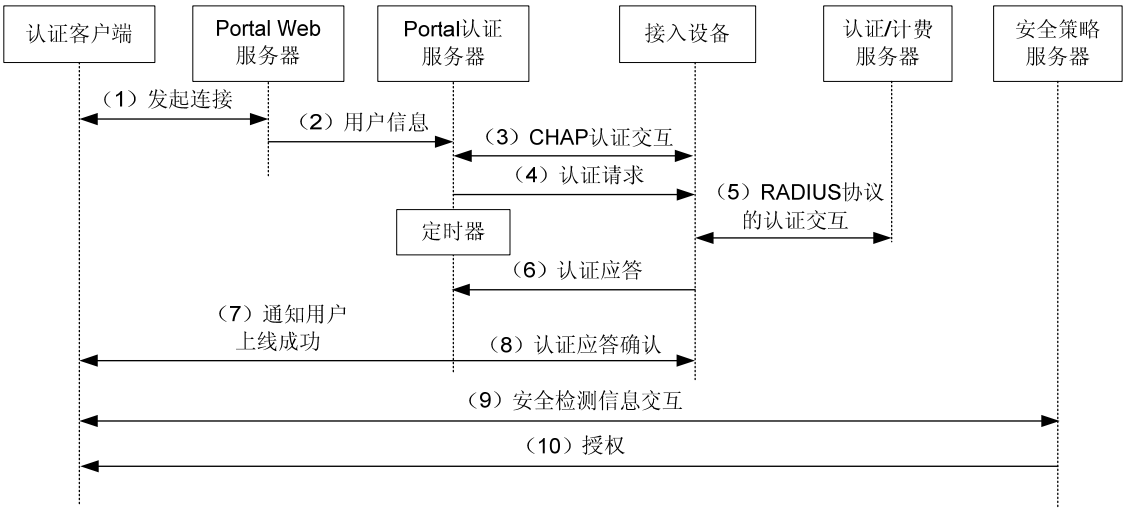
对于以上三种认证方式，IP 地址都是用户的唯一标识。接入设备基于用户的 IP 地址下发 ACL 对接口上通过认证的用户报文转发进行控制。由于直接认证和二次地址分配认证下的接入设备与用户之间未跨越三层转发设备，因此接口可以学习到用户的 MAC 地址，接入设备可以利用学习到 MAC 地址增强对用户报文转发的控制力度。

1.1.6 Portal认证流程

直接认证和可跨三层 Portal 认证流程相同。二次地址分配认证流程因为有两次地址分配过程，所以其认证流程和另外两种认证方式有所不同。

1. 直接认证和可跨三层Portal认证的流程（CHAP/PAP认证方式）

图1-2 直接认证/可跨三层 Portal 认证流程图



直接认证/可跨三层 Portal 认证流程：

(1) Portal 用户通过 HTTP 协议访问外部网络。HTTP 报文经过接入设备时，对于访问 Portal Web 服务器或设定的免认证地址的 HTTP 报文，接入设备允许其通过；对于访问其它地址的 HTTP 报文，接入设备将其重定向到 Portal Web 服务器。Portal Web 服务器提供 Web 页面供用户输入用户名和密码。

(2) Portal Web 服务器将用户输入的信息提交给 Portal 认证服务器进行认证。

(3) Portal 认证服务器与接入设备之间进行 CHAP（Challenge Handshake Authentication Protocol，质询握手验证协议）认证交互。若采用 PAP（Password Authentication Protocol，密码验证协议）认证则直接进入下一步骤。采用哪种认证交互方式由 Portal 认证服务器决定。

(3) Portal 认证服务器将用户输入的用户名和密码组装成认证请求报文发往接入设备，同时开启定时器等待认证应答报文。

(4) 接入设备与 RADIUS 服务器之间进行 RADIUS 协议报文的交互。

(5) 接入设备向 Portal 认证服务器发送认证应答报文，表示认证成功或者认证失败。

(6) Portal 认证服务器向客户端发送认证成功或认证失败报文，通知客户端认证成功（上线）或失败。

(7) 若认证成功，Portal 认证服务器还会向接入设备发送认证应答确认。若是 iNode 客户端，则还需要进行以下安全扩展功能的步骤，否则 Portal 认证过程结束，用户上线。

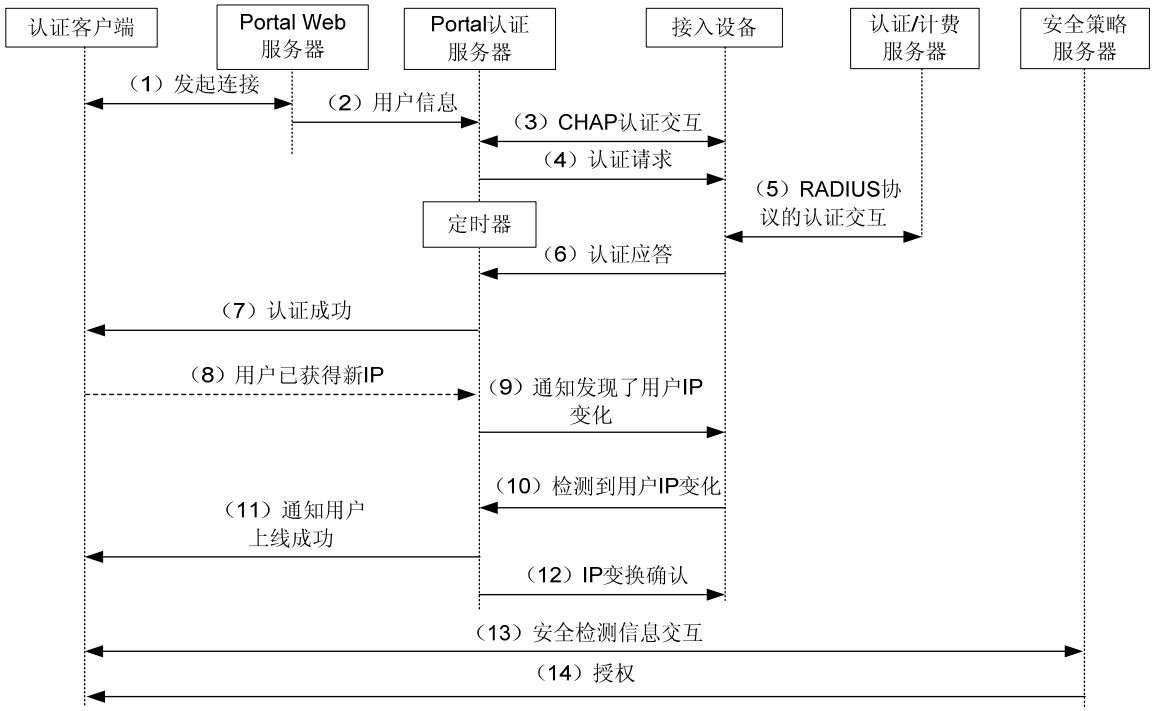
(8) 客户端和安全策略服务器之间进行安全信息交互。安全策略服务器检测客户端的安全性是否合格，包括是否安装防病毒软件、是否更新病毒库、是否安装了非法软件、是否更新操作系统补丁等。

(9) 安全策略服务器根据安全检查结果授权用户访问指定的网络资源，授权信息保存到接入设备中，接入设备将使用该信息控制用户的访问。

步骤(9)、(10)为 Portal 认证安全扩展功能的交互过程。

2. 二次地址分配认证方式的流程（CHAP/PAP认证方式）

图1-3 二次地址分配认证方式流程图



二次地址分配认证流程：

(1)～(7)同直接/可跨三层 Portal 认证中步骤（1）～（7）。

(8) 客户端收到认证通过报文后，通过 DHCP 获得新的公网 IP 地址，并通知 Portal 认证服务器用户已获得新 IP 地址。

(9) Portal 认证服务器通知接入设备客户端获得新公网 IP 地址。

(10) 接入设备通过 DHCP 模块得知用户 IP 地址变化后，通告 Portal 认证服务器已检测到用户 IP 变化。

(11) 当 Portal 认证服务器接收到客户端以及接入设备发送的关于用户 IP 变化的通告后，通知客户端上线成功。

(12) Portal 认证服务器向接入设备发送 IP 变化确认报文。

(13) 客户端和安全策略服务器之间进行安全信息交互。安全策略服务器检测客户端的安全性是否合格，包括是否安装防病毒软件、是否更新病毒库、是否安装了非法软件、是否更新操作系统补丁等。

(14) 安全策略服务器根据用户的安全性授权用户访问指定的网络资源，授权信息保存到接入设备中，接入设备将使用该信息控制用户的访问。

步骤(13)、(14)为 Portal 认证扩展功能的交互过程。

1.2 Portal配置任务简介

表1-1 Portal 配置任务简介

配置任务		说明	详细配置
配置Portal认证服务器		必选	
配置Portal Web服务器		必选	1.5
在接口上使能Portal认证		必选	1.6
在接口上引用Portal Web服务器		必选	1.7
控制Portal用户的接入	配置免认证规则	可选	1.8.1
	配置源认证网段		1.8.2
	配置目的认证网段		1.8.3
	配置Portal最大用户数		1.8.4
	指定Portal用户使用的认证域		1.8.5
配置Portal探测功能	配置Portal用户的在线探测功能	可选	1.9.1
	配置Portal认证服务器的可达性探测功能		1.9.2
	配置Portal Web服务器的可达性探测功能		1.9.3
	配置Portal用户信息同步功能		1.9.4
配置Portal用户逃生功能		可选	1.10
配置发送给Portal认证服务器的Portal报文的BAS-IP属性		可选	1.11
配置Portal用户漫游功能		可选	1.12
强制Portal用户下线		可选	1.13

1.3 配置准备

Portal 提供了一个用户身份认证和安全认证的实现方案，但是仅仅依靠 Portal 不足以实现该方案。接入设备的管理者需选择使用 RADIUS 认证方法，以配合 Portal 完成用户的身份认证。Portal 认证的配置前提：

- Portal 认证服务器、Portal Web 服务器、RADIUS 服务器已安装并配置成功。
- 若采用二次地址分配认证方式，接入设备需启动 DHCP 中继功能，另外需要安装并配置好 DHCP 服务器。
- 用户、接入设备和各服务器之间路由可达。
- 如果通过远端 RADIUS 服务器进行认证，则需要在 RADIUS 服务器上配置相应的用户名和密码，然后在接入设备端进行 RADIUS 客户端的相关设置。RADIUS 客户端的具体配置请参见“安全配置指导”中的“AAA”。

- 如果需要支持 Portal 的安全扩展功能，需要安装并配置 CAMS EAD/iMC EAD 安全策略组件。同时保证在接入设备上的 ACL 配置和安全策略服务器上配置的隔离 ACL 的编号、安全 ACL 的编号对应。接入设备上与安全策略服务器相关的配置请参见“安全配置指导”中的“AAA”。安全策略服务器的配置请参考“CAMS EAD 安全策略组件联机帮助”以及“iMC EAD 安全策略组件联机帮助”。

1.4 配置Portal认证服务器

Portal 认证服务器视图用于配置 Portal 认证服务器的相关参数，包括服务器的 IP 地址，服务器所在的 VPN 实例，设备和服务器间通信的共享密钥，服务器探测功能等。

设备支持配置多个 Portal 认证服务器。

建议不要删除正在被用户使用的 Portal 认证服务器，否则会导致设备上的在线用户无法正常下线。

设备向 Portal 认证服务器主动发送报文时使用的目的端口号（由 **port** *port-id* 配置）必须与远程 Portal 认证服务器实际使用的监听端口号保持一致。

表1-2 配置 Portal 认证服务器

操作	命令	说明
进入系统视图	**system-view**	-
创建Portal认证服务器，并进入Portal认证服务器视图	**portal server** *server-name*	缺省情况下，没有配置任何Portal认证服务器
指定Portal认证服务器的IPv4地址	**ip** *ipv4-address* [**vpn-instance** *vpn-instance-name*] [**key** { **cipher** | **simple** } *key-string*]	至少选其一 缺省情况下，没有指定Portal认证服务器的IP地址
指定Portal认证服务器的IPv6地址	**ipv6** *ipv6-address* [**vpn-instance** *vpn-instance-name*] [**key** { **cipher** | **simple** } *key-string*]	
（可选）配置接入设备主动向Portal认证服务器发送Portal报文时使用的UDP端口号	**port** *port-id*	缺省情况下，接入设备主动发送Portal报文时使用的UDP端口号为50100

1.5 配置Portal Web服务器

Portal Web 服务器是指 Portal 认证过程中向用户推送认证页面的 Web 服务器，也是设备强制重定向用户 HTTP 请求报文时所使用的 Web 服务器。Portal Web 服务器视图用于配置 Web 服务器的 URL 地址及设备重定向该 URL 地址给用户时 URL 地址所携带的参数。同时该视图还用于配置 Portal Web 服务器探测等功能。

可以配置多个 Portal Web 服务器。

表1-3 配置 Portal Web 服务器

操作	命令	说明
进入系统视图	**system-view**	-
创建Portal Web服务器，并进入Portal Web服务器视图	**portal web-server** *server-name*	缺省情况下，没有配置任何Portal Web服务器

操作	命令	说明
指定Portal Web服务器所属的VPN	**vpn-instance** *vpn-instance-name*	缺省情况下，Portal Web服务器位于公网中
指定Portal Web服务器的URL	**url** *url-string*	缺省情况下，没有指定Portal Web服务器的URL
配置设备重定向给用户的Portal Web服务器的URL中携带的参数信息	**url-parameter** *param-name* { **original-url** | **source-address** | **source-mac** | **value** *expression* }	缺省情况下，未配置设备重定向给用户的Portal Web服务器的URL中携带的参数信息

1.6 在接口上使能Portal认证

只有在接口上使能了 Portal 认证，对接入用户的 Portal 认证功能才能生效。

使能了 Portal 认证的接口上收到 Portal 报文时，首先根据报文的源 IP 地址和 VPN 信息查找本地配置的 Portal 认证服务器，若查找到相应的 Portal 认证服务器配置，则认为报文合法，并向该 Portal 认证服务器回应认证响应报文；否则，认为报文非法，将其丢弃。用户上线后，将与认证过程中使用的 Portal 认证服务器进行后续的交互。

在接口上使能 Portal 认证时，需要注意：

- 在使能 Portal 认证之前，需要保证使能 Portal 的接口已配置或者获取了合法的 IP 地址。
- 使能 IPv6 Portal 功能之前，需要保证设备支持 IPv6 ACL 和 IPv6 转发功能。
- 为使接口上的 Portal 功能生效，使能 Portal 的接口不能加入聚合组。
- 当接入设备和 Portal 用户之间跨越三层设备时，只能配置可跨三层 Portal 认证方式（**layer3**），但可跨三层 Portal 认证方式不要求接入设备和 Portal 用户之间必需跨越三层设备。
- 在二次地址分配认证方式下，接口上配置的授权 ARP 后，系统会禁止该接口动态学习 ARP 表项，只有通过 DHCP 合法分配到公网 IP 地址的用户的 ARP 报文才能够被学习。因此，为保证只有合法用户才能接入网络，建议使用二次地址分配认证方式的 Portal 认证时，接口上同时配置了授权 ARP 功能。
- IPv6 Portal 服务器不支持二次地址分配方式的 Portal 认证。
- 允许在接口上同时使能 IPv4 Portal 认证和 IPv6 Portal 认证。

表1-4 使能 Portal 认证

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	只能是三层接口
在接口上使能IPv4 Portal认证，并指定认证方式	**portal enable method** { **direct** | **layer3** | **redhcp** }	至少选其一 缺省情况下，接口上没有使能Portal认证
在接口上使能IPv6 Portal认证，并指定认证方式	**portal ipv6 enable method** { **direct** | **layer3** }	

1.7 在接口上引用Portal Web服务器

在接口上引用指定的 Portal Web 服务器后，设备会将该接口上 Portal 用户的 HTTP 请求报文重定向到该 Web 服务器。

一个接口上可以同时引用一个 IPv4 Portal Web 服务器和一个 IPv6 Portal Web 认证服务器。

表1-5 在接口上引用 Portal Web 服务器

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	只能是三层接口
在接口上引用IPv4 Portal Web服务器	**portal apply web-server** *server-name* [**fail-permit**]	至少选其一 缺省情况下，接口上没有引用任何Portal Web服务器
在接口上引用IPv6 Portal Web服务器	**portal ipv6 apply web-server** *server-name* [**fail-permit**]	

1.8 控制Portal用户的接入

1.8.1 配置免认证规则

通过配置免认证规则可以让特定的用户不需要通过 Portal 认证即可访问外网特定资源，这是由免认证规则中配置的源信息以及目的信息决定的。

免认证规则的匹配项包括 IP 地址、TCP/UDP 端口号、MAC 地址、所连接设备的接口和 VLAN，只有符合免认证规则的用户报文才不会触发 Portal 认证，因此这些报文所属的用户才可以直接访问网络资源。

配置免认证规则时，需要注意：

- 如果免认证规则中同时配置了接口和VLAN，则要求接口属于指定的VLAN，否则该规则无效。
- 相同内容的免认证规则不能重复配置，否则提示免认证规则已存在或重复。
- 无论接口上是否使能 Portal 认证，只能添加或者删除免认证规则，不能修改。

表1-6 配置基于 IP 地址的免认证规则

操作	命令	说明
进入系统视图	**system-view**	-
配置基于IPv4地址的Portal免认证规则	**portal free-rule** *rule-number* { **destination ip** { *ip-address* { *mask-length* | *mask* } | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] | **source ip** { *ip-address* { *mask-length* | *mask* } | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] } *	缺省情况下，不存在基于IPv4地址的Portal免认证规则

操作	命令	说明
配置基于IPv6地址的Portal免认证规则	**portal free-rule** *rule-number* { **destination ipv6** { *ipv6-address prefix-length* | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] | **source ipv6** { *ipv6-address prefix-length* | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] } *	缺省情况下，不存在基于IPv6地址的Portal免认证规则

表1-7 配置基于源的免认证规则

操作	命令	说明
进入系统视图	**system-view**	-
配置基于源的Portal免认证规则	**portal free-rule** *rule-number* **source** { **interface** *interface-type interface-number* | **mac** *mac-address* | **vlan** *vlan-id* } *	缺省情况下，不存在基于源的Portal免认证规则

1.8.2 配置源认证网段

通过配置源认证网段实现只允许在源认证网段范围内的用户 HTTP 报文才能触发 Portal 认证。如果未认证用户的 HTTP 报文既不满足免认证规则又不在源认证网段内，则将被接入设备丢弃。

配置源认证网段时，需要注意：

- 源认证网段配置仅对可跨三层 Portal 认证有效。
- 直接认证方式和二次地址分配认证方式下，用户与接入设备上使能 Portal 的接口在同一个网段，因此配置源认证网络没有实际意义，若配置了非用户接入的网段为源认证网段，则用户认证会失败。对于直接认证方式，接入设备认为接口上的源认证网段为任意源 IP；对于二次地址分配认证方式，接入设备认为接口上的源认证网段为接口私网 IP 决定的私网网段。
- 如果接口上同时配置了源认证网段和目的认证网段，则源认证网段的配置不会生效。
- 设备上可以配置多条源认证网段。若配置了网段地址范围有所覆盖或重叠的源认证网段，则仅其中地址范围最大（子网掩码或地址前缀最小）的一条源认证网段配置生效。

表1-8 配置 IPv4 Portal 源认证网段

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
配置IPv4 Portal源认证网段	**portal layer3 source** *ipv4-network-address* { *mask-length* | *mask* }	缺省情况下，没有配置IPv4 Portal源认证网段，表示对任意IPv4用户都进行Portal认证

表1-9 配置 IPv6 Portal 源认证网段

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置IPv6 Portal源认证网段	**portal ipv6 layer3 source** *ipv6-network-address prefix-length*	缺省情况下，没有配置IPv6 Portal源认证网段，表示对任意IPv6用户都进行Portal认证

1.8.3 配置目的认证网段

通过配置目的认证网段实现仅对要访问指定目的网段（除免认证规则中指定的目的 IP 地址或网段）的用户进行 Portal 认证，其它用户访问外部网络时无需认证。

配置目的认证网段时，需要注意：

- 如果接口下同时配置了源认证网段和目的认证网段，则源认证网段的配置无效。
- 设备上可以配置多条目的认证网段。若配置了网段地址范围有所覆盖或重叠的目的认证网段，则仅其中地址范围最大（子网掩码或地址前缀最小）的一条目的认证网段配置生效。

表1-10 配置 IPv4 Portal 目的认证网段

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置IPv4 Portal目的认证网段	**portal free-all except destination** *ipv4-network-address* { *mask-length* | *mask* }	缺省情况下，没有配置IPv4 Portal目的认证网段，表示对访问任意目的网段的用户都进行Portal认证

表1-11 配置 IPv6 Portal 目的认证网段

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置IPv6 Portal目的认证网段	**portal ipv6 free-all except destination** *ipv6-network-address prefix-length*	缺省情况下，没有配置IPv6 Portal目的认证网段，表示对访问任意目的网段的用户都进行Portal认证

1.8.4 配置Portal最大用户数

通过该配置可以控制系统中的 Portal 接入用户总数，包括 IPv4 Portal 用户和 IPv6 Portal 用户。

如果配置的 Portal 最大用户数小于当前已经在线的 Portal 用户数，则该配置可以执行成功，且在线 Portal 用户不受影响，但系统将不允许新的 Portal 用户接入。

表1-12 配置 Portal 最大用户数

操作	命令	说明
进入系统视图	**system-view**	-
配置Portal最大用户数	**portal max-user** *max-number*	缺省情况下，不限制Portal最大用户数

1.8.5 指定Portal用户使用的认证域

每个 Portal 用户都属于一个认证域，且在其所属的认证域内进行认证/授权/计费，认证域中定义了一套认证/授权/计费的策略。

通过在指定接口上配置 Portal 用户使用的认证域，使得所有从该接口接入的 Portal 用户被强制使用指定的认证域来进行认证、授权和计费。即使 Portal 用户输入的用户名中携带的域名相同，接入设备的管理员也可以通过该配置使得不同接口上接入的 Portal 用户使用不同的认证域，从而增加管理员部署 Portal 接入策略的灵活性。

从指定接口上接入的 Portal 用户将按照如下先后顺序选择认证域：接口上指定的 Portal 用户使用的 ISP 域-->用户名中携带的 ISP 域-->系统缺省的 ISP 域。关于缺省 ISP 域的相关介绍请参见“安全配置指导”中的“AAA”。

接口上可以同时指定 IPv4 Portal 用户和 IPv6 Portal 用户的认证域。

表1-13 指定 IPv4 Portal 用户使用的认证域

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
指定IPv4 Portal用户使用的认证域	**portal domain** *domain-name*	缺省情况下，未指定IPv4 Portal用户使用的认证域

表1-14 指定 IPv6 Portal 用户使用的认证域

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
指定IPv6 Portal用户使用的认证域	**portal ipv6 domain** *domain-name*	缺省情况下，未指定IPv6 Portal用户使用的认证域

1.9 配置Portal探测功能

1.9.1 配置Portal用户在线探测功能

接口上开启了 Portal 用户在线探测功能后，设备在用户上线之后，若发现在一定的时间（**idle** *time*）之内该用户无流量，则会向该用户定期（**interval** *interval*）发送探测报文来确认该用户是否在线，以便及时发现异常离线用户。

- IPv4 探测报文为 ARP 请求或 ICMP 请求，IPv6 探测报文为 ND 请求或 ICMPv6 请求。
- 若设备在指定的探测次数（**retry** *retries*）之内收到了该 Portal 用户的响应报文，则认为此用户在线。之后，继续根据指定的时间之内是否有流量来决定是否发起新的一轮探测，以持续确认该用户的在线状态。
- 若设备在指定的探测次数（**retry** *retries*）之后仍然未收到该 Portal 用户的响应报文，则认为此用户已经下线，则停止探测，并删除该用户。

需要注意的是，ARP 和 ND 方式的探测只适用于直接方式和二次地址分配方式的 Portal 认证。ICMP 方式的探测适用于所有认证方式。

表1-15 配置 IPv4 Portal 用户在线探测功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
开启IPv4 Portal用户在线探测功能	**portal user-detect type** { **arp** | **icmp** } [**retry** *retries*] [**interval** *interval*] [**idle** *time*]	缺省情况下，接口上的IPv4 Portal用户在线探测功能处于关闭状态

表1-16 配置 IPv6 Portal 用户在线探测功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
开启IPv6 Portal用户在线探测功能	**portal ipv6 user-detect type** { **icmpv6** | **nd** } [**retry** *retries*] [**interval** *interval*] [**idle** *time*]	缺省情况下，接口上的IPv6 Portal用户在线探测功能处于关闭状态

1.9.2 配置Portal认证服务器的可达性探测功能

在 Portal 认证的过程中，如果接入设备与 Portal 认证服务器的通信中断，则会导致新用户无法上线，已经在线的 Portal 用户无法正常下线的问题。为解决这些问题，需要接入设备能够及时探测到 Portal 认证服务器可达状态的变化，并能触发执行相应的操作来应对这种变化带来的影响。

开启 Portal 认证服务器的可达性探测功能后，无论是否有接口上使能了 Portal 认证，设备会定期检测 Portal 认证服务器发送的报文（例如，用户上线报文、用户下线报文、心跳报文）来判断服务器的可达状态：若设备在指定的探测超时时间（**timeout** *timeout*）内收到 Portal 报文，且验证其正确，则认为此次探测成功且服务器可达，否则认为此次探测失败，服务器不可达。

当接入设备检测到 Portal 认证服务器可达或不可达状态改变时，可执行以下一种或多种操作：

- 发送 Trap 信息：Portal 认证服务器可达或者不可达的状态改变时，向网管服务器发送 Trap 信息。Trap 信息中记录了 Portal 认证服务器名以及该服务器的当前状态。
- 发送日志：Portal 认证服务器可达或者不可达的状态改变时，发送日志信息。日志信息中记录了 Portal 认证服务器名以及该服务器状态改变前后的状态。
- Portal用户逃生：Portal认证服务器不可达时，暂时取消接口上进行的Portal认证，允许该接口接入的所有Portal用户访问网络资源。之后，若设备收到Portal认证服务器发送的报文，则恢复该端口的Portal认证功能。该功能的详细配置请参见“1.10 配置Portal用户逃生功能”。

配置 Portal 认证服务器的可达性探测功能时，需要注意：

- 目前，只有 iMC 的 Portal 认证服务器支持逃生心跳功能。为了配合该探测功能，Portal 认证服务器上必须保证逃生心跳功能处于开启状态。
- 如果同时指定了多种操作，则 Portal 认证服务器可达状态改变时系统可并发执行多种操作。

表1-17 配置 Portal 认证服务器的可达性探测功能

操作	命令	说明
进入系统视图	**system-view**	-
进入Portal认证服务器视图	**portal server** *server-name*	-
开启Portal认证服务器的可达性探测功能	**server-detect** [**timeout** *timeout*] { **log** | **trap** } *	缺省情况下，Portal服务器可达性探测功能处于关闭状态

1.9.3 配置Portal Web服务器的可达性探测功能

在 Portal 认证的过程中，如果接入设备与 Portal Web 服务器的通信中断，将无法完成整个认证过程，因此必须对 Portal Web 服务器的可达性进行探测。

由于 Portal Web 服务器用于对用户提供 Web 服务，不需要和设备交互报文，因此无法通过发送某种协议报文的方式来进行可达性检测。无论是否有接口上使能了 Portal 认证，开启了 Portal Web 服务器的可达性探测功能之后，接入设备采用模拟用户进行 Web 访问的过程来实施探测：接入设备主动向 Portal Web 服务器发起 TCP 连接，如果连接可以建立，则认为此次探测成功且服务器可达，否则认为此次探测失败。

- 探测参数
  - 探测间隔：进行探测尝试的时间间隔。
  - 失败探测的最大次数：允许连续探测失败的最大次数。若连续探测失败数目达到此值，则认为服务器不可达。
- 可达状态改变时触发执行的操作（可以选择其中一种或同时使用多种）
  - 发送 Trap 信息：Portal Web 服务器可达或者不可达的状态改变时，向网管服务器发送 Trap 信息。Trap 信息中记录了 Portal Web 服务器名以及该服务器的当前状态。
  - 发送日志：Portal Web 服务器可达或者不可达的状态改变时，发送日志信息。日志信息中记录了 Portal Web 服务器名以及该服务器状态改变前后的状态。

- Portal用户逃生：Portal Web服务器不可达时，暂时取消端口进行的Portal认证，允许该端口接入的所有Portal用户访问网络资源。之后，若Portal Web服务器可达，则恢复该端口的Portal认证功能。该功能的详细配置请参见“1.10 配置Portal用户逃生功能”。

表1-18 配置 Portal Web 服务器的可达性探测功能

操作	命令	说明
进入系统视图	**system-view**	-
进入Portal Web服务器视图	**portal web-server** *server-name*	-
开启Portal Web服务器的可达性探测功能	**server-detect** [**interval** *interval*] [**retry** *retries*] { **log** | **trap** } *	缺省情况下，Portal Web认证服务器的可达性探测功能处于关闭状态

1.9.4 配置Portal用户信息同步功能

为了解决接入设备与 Portal 认证服务器通信中断后，两者的 Portal 用户信息不一致问题，设备提供了一种 Portal 用户信息同步功能。该功能利用了 Portal 同步报文的发送及检测机制，具体实现如下：

(1) 由 Portal 认证服务器周期性地（周期为 Portal 认证服务器上指定的用户心跳间隔值）将在线用户信息通过用户同步报文发送给接入设备；

(2) 接入设备在用户上线之后，即开启用户同步检测定时器（超时时间为 **timeout** *timeout*），在收到用户同步报文后，将其中携带的用户列表信息与自己的用户列表信息进行对比，如果发现同步报文中有设备上不存在的用户信息，则将这些自己没有的用户信息反馈给 Portal 认证服务器，Portal 认证服务器将删除这些用户信息；如果发现接入设备上的某用户信息在一个用户同步报文的检测超时时间内，都未在该 Portal 认证服务器发送过来的用户同步报文中出现过，则认为 Portal 认证服务器上已不存在该用户，设备将强制该用户下线。

使用 Portal 用户信息同步功能时，需要注意：

- 只有在支持 Portal 用户心跳功能（目前仅 iMC 的 Portal 认证服务器支持）的 Portal 认证服务器的配合下，本功能才有效。为了实现该功能，还需要在 Portal 认证服务器上选择支持用户心跳功能，且服务器上配置的用户心跳间隔要小于等于设备上配置的检测超时时间。
- 在设备上删除 Portal 认证服务器时将会同时删除该服务器的用户信息同步功能配置。

表1-19 配置 Portal 用户信息同步功能

操作	命令	说明
进入系统视图	**system-view**	-
进入Portal认证服务器视图	**portal server** *server-name*	-
开启Portal用户信息同步功能	**user-sync timeout** *timeout*	缺省情况下，Portal用户信息同步功能处于关闭状态

1.10 配置Portal用户逃生功能

当接入设备探测到 Portal 认证服务器或者 Portal Web 服务器不可达时，可打开接口的网络限制，允许 Portal 用户不需经过认证即可访问网络资源，也就是通常所说的 Portal 逃生功能。

如果接口上同时开启了 Portal 认证服务器逃生功能和 Portal Web 服务器逃生功能，则当任意一个服务器不可达时，即放开接口控制，当两个服务器均恢复可达性后，再重新启动 Portal 认证功能。重新启动接口的 Portal 认证功能之后，未通过认证的用户需要通过认证之后才能访问网络资源，已通过认证的用户可继续访问网络资源。

表1-20 配置 Portal 用户逃生功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
开启Portal认证服务器不可达时的Portal用户逃生功能	**portal** [**ipv6**] **fail-permit server** *server-name*	缺省情况下，设备探测到Portal认证服务器不可达时，不允许Portal用户逃生
开启Portal Web服务器不可达时的Portal用户逃生功能	**portal** [**ipv6**] **apply web-server** *server-name* **fail-permit**	缺省情况下，设备探测到Portal Web服务器不可达时，不允许Portal用户逃生

1.11 配置发送给Portal认证服务器的Portal报文的BAS-IP属性

设备上运行 Portal 2.0 版本时，主动发送给 Portal 认证服务器的报文（例如强制用户下线报文）中必须携带 BAS-IP 属性。设备上运行 Portal 3.0 版本时，主动发送给 Portal 认证服务器的报文必须携带 BAS-IP 或者 BAS-IPv6 属性。

如果接口上使能了 IPv4 Portal 认证，则可以设置 BAS-IP 属性值；如果接口上使能了 IPv6 Portal 认证，则可以设置 BAS-IPv6 属性值。

配置此功能后，设备主动发送的通知类 Portal 报文，其源 IP 地址为配置的 BAS-IP 或 BAS-IPv6 属性值，否则为 Portal 报文出接口的 IP 地址。由于在设备进行二次地址分配认证和强制 Portal 用户下线过程中，均需要设备主动向 Portal 认证服务器发送相应的通知类 Portal 报文，因此，为了保证二次地址分配认证方式下 Portal 用户可以成功上线，以及设备可以成功通知 Portal 认证服务器用户下线，需要保证该属性值与 Portal 认证服务器上指定的设备 IP 一致。

表1-21 配置发送给 Portal 认证服务器的 Portal 报文的 BAS-IP 属性

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
配置发送给Portal认证服务器的IPv4 Portal报文的BAS-IP属性	**portal bas-ip** *ipv4-address*	缺省情况下，发送给Portal认证服务器的响应类的IPv4 Portal报文中携带的BAS-IP属性为报文的源IPv4地址，通知类IPv4 Portal报文中携带的BAS-IP属性为报文出接口的IPv4地址
配置发送给Portal认证服务器的IPv6 Portal报文的BAS-IPv6属性	**portal bas-ipv6** *ipv6-address*	缺省情况下，发送给Portal认证服务器的响应类的IPv6 Portal报文中携带的BAS-IPv6属性为报文的源IPv6地址，通知类IPv6 Portal报文中携带的BAS-IPv6属性为报文出接口的IPv6地址

1.12 配置Portal用户漫游功能

Portal 用户漫游功能允许同属一个 VLAN 的用户在 VLAN 内漫游，即只要 Portal 用户在某 VLAN 接口通过认证，则可以在该 VLAN 内的任何二层端口上访问网络资源，且移动接入端口时无须重复认证。若 VLAN 接口上未开启该功能，则在线用户在同一个 VLAN 内其它端口接入时，将无法访问外部网络资源，必须首先在原端口正常下线之后，才能在其它端口重新认证上线。

需要注意的是：

- 该功能只对通过 VLAN 接口上线的用户有效，对于通过普通三层接口上线的用户无效。
- 有用户在线的情况下，不能配置此功能。

表1-22 配置 Portal 用户漫游功能

操作	命令	说明
进入系统视图	**system-view**	-
使能Portal用户漫游功能	**portal roaming enable**	缺省情况下，Portal用户漫游功能处于关闭状态

1.13 强制Portal用户下线

通过配置强制用户下线可以终止对用户的 Portal 认证过程，或者将已经通过认证的 Portal 用户删除。

表1-23 配置强制 Portal 用户下线

操作	命令	说明
进入系统视图	**system-view**	-
强制指定的IPv4 Portal用户或所有Portal用户下线	**portal delete-user** { *ipv4-address* | **all** | **interface** *interface-type interface-number* }	-
强制指定的IPv6 Portal用户或所有的Portal用户下线	**portal delete-user** { **all** | **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }	-

1.14 Portal显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 Portal 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** 命令可以清除 Portal 统计信息。

表1-24 Portal 显示和维护

操作	命令
显示接口上用于报文匹配的Portal过滤规则信息（MSR 2600/MSR 3600）	**display portal rule** { **all** | **dynamic** | **static** } **interface** *interface-type interface-number*
显示接口下发的用于报文匹配的Portal过滤规则信息（MSR 5600）	**display portal rule** { **all** | **dynamic** | **static** } **interface** *interface-type interface-number* [**slot** *slot-id*]
显示指定接口上的Portal配置信息和Portal运行状态信息	**display portal interface** *interface-type interface-number*
显示Portal认证服务器信息	**display portal server** [*server-name*]
显示Portal Web服务器信息	**display portal web-server** [*server-name*]
显示Portal认证服务器的报文统计信息	**display portal packet statistics** [**server** *server-name*]
显示Portal用户的信息	**display portal user** { **all** | **interface** *interface-type interface-number* }
清除Portal认证服务器的报文统计信息	**reset portal packet statistics** [**server** *server-name*]

1.15 Portal典型配置举例

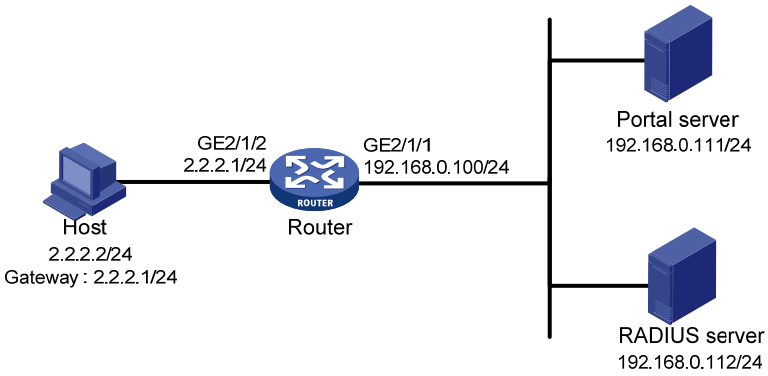
1.15.1 Portal直接认证配置举例

1. 组网需求

- 用户主机与接入设备 Router 直接相连，采用直接方式的 Portal 认证。用户通过手工配置或 DHCP 获取的一个公网 IP 地址进行认证，在通过 Portal 认证前，只能访问 Portal Web 服务器；在通过 Portal 认证后，可以使用此 IP 地址访问非受限的互联网资源。
- 采用一台 Portal 服务器承担 Portal 认证服务器和 Portal Web 服务器的职责。
- 采用 RADIUS 服务器作为认证/计费服务器。

2. 组网图

图1-4 配置 Portal 直接认证组网图



3. 配置步骤

说明

- 按照组网图配置设备各接口的 IP 地址，保证启动 Portal 之前各主机、服务器和设备之间的路由可达。
- 完成 RADIUS 服务器上的配置，保证用户的认证/计费功能正常运行。

(1) 配置 Portal server（iMC PLAT 5.0）

说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 5.0(E0101)、iMC UAM 5.0(E0101)），说明 Portal server 的基本配置。

配置 Portal 认证服务器。

登录进入 iMC 管理平台，选择“业务”页签，单击导航树中的[Portal 认证服务器管理/服务器配置]菜单项，进入服务器配置页面。

- 根据实际组网情况调整以下参数，本例中使用缺省配置。

图1-5 Portal 认证服务器配置页面

配置 IP 地址组。

单击导航树中的[Portal 认证服务器管理/IP 地址组配置]菜单项，进入 Portal IP 地址组配置页面，在该页面中单击<增加>按钮，进入增加 IP 地址组配置页面。

- 填写 IP 地址组名；
- 输入起始地址和终止地址。用户主机 IP 地址必须包含在该 IP 地址组范围内；
- 选择业务分组，本例中使用缺省的“未分组”；
- 选择 IP 地址组的类型为“普通”。

图1-6 增加 IP 地址组配置页面

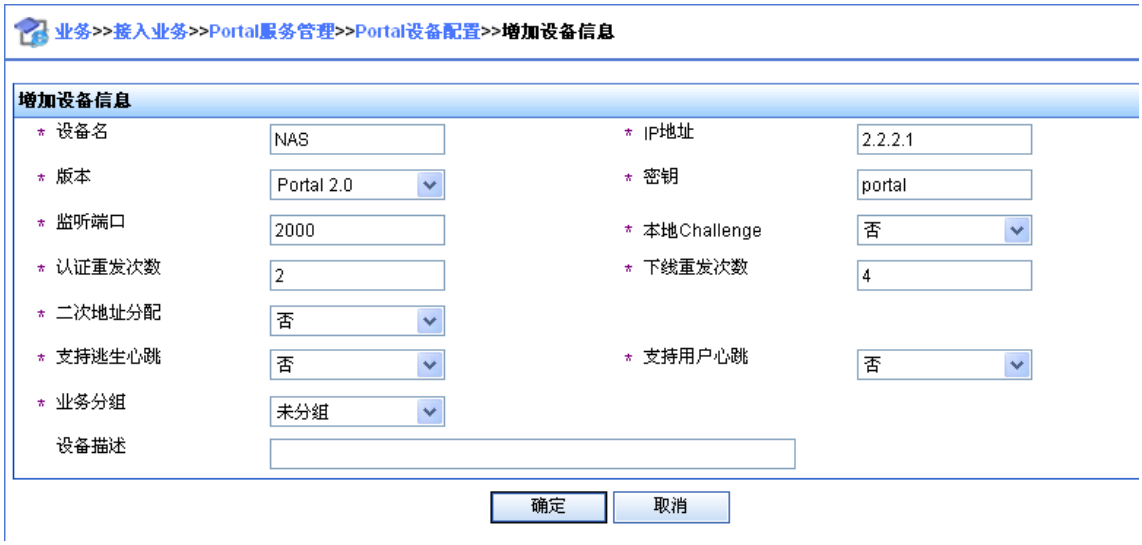
增加 Portal 设备。

单击导航树中的[Portal 认证服务器管理/设备配置]菜单项，进入 Portal 设备配置页面，在该页面中单击<增加>按钮，进入增加设备信息配置页面。

- 填写设备名；

- 指定 IP 地址为与接入用户相连的设备接口 IP；
- 输入密钥，与接入设备 Router 上的配置保持一致；
- 选择是否进行二次地址分配，本例中为直接认证，因此为否；
- 选择是否支持逃生心跳功能和用户心跳功能，本例中不支持。

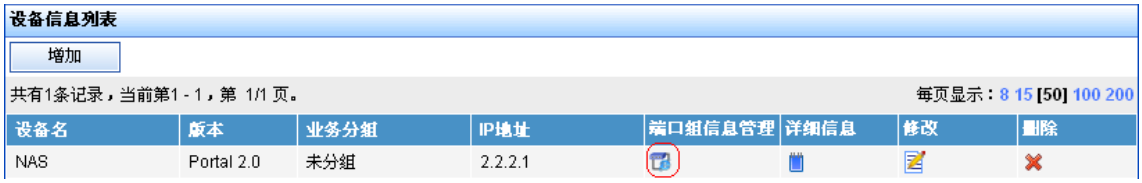
图1-7 增加设备信息配置页面



Portal 设备关联 IP 地址组

在 Portal 设备配置页面中的设备信息列表中，点击 NAS 设备的<端口组信息管理>链接，进入端口组信息配置页面。

图1-8 设备信息列表



在端口组信息配置页面中点击<增加>按钮，进入增加端口组信息配置页面。

- 填写端口组名；
- 选择 IP 地址组，用户接入网络时使用的 IP 地址必须属于所选的 IP 地址组；
- 其它参数采用缺省值。

图1-9 增加端口组信息配置页面

最后单击导航树中的[业务参数配置/系统配置手工生效]菜单项，使以上 Portal 认证服务器配置生效。

(2) 配置 Router

- 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<Router> system-view
[Router] radius scheme rs1
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Router-radius-rs1] primary authentication 192.168.0.112
[Router-radius-rs1] primary accounting 192.168.0.112
[Router-radius-rs1] key authentication simple radius
[Router-radius-rs1] key accounting simple radius
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[Router-radius-rs1] user-name-format without-domain
[Router-radius-rs1] quit
```

使能 RADIUS session control 功能。

```
[Router] radius session-control enable
```

- 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[Router] domain dm1
```

配置 ISP 域使用的 RADIUS 方案 rs1。

```
[Router-isp-dm1] authentication portal radius-scheme rs1
[Router-isp-dm1] authorization portal radius-scheme rs1
[Router-isp-dm1] accounting portal radius-scheme rs1
[Router-isp-dm1] quit
```

配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方案。

```
[Router] domain default enable dm1
```

- 配置 Portal 认证

配置 Portal 认证服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，监听 Portal 报文的端口为 50100。

```
[Router] portal server newpt
[Router-portal-server-newpt] ip 192.168.0.111 key simple portal
[Router-portal-server-newpt] port 50100
[Router-portal-server-newpt] quit
```

配置 Portal Web 服务器的 URL 为 http://192.168.0.111:8080/portal。（Portal Web 服务器的 URL 请与实际环境中的 Portal Web 服务器配置保持一致，此处仅为示例）

```
[Router] portal web-server newpt
[Router-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[Router-portal-websvr-newpt] quit
```

在接口 GigabitEthernet2/1/2 上使能直接方式的 Portal 认证。

```
[Router] interface gigabitethernet 2/1/2
[Router–GigabitEthernet2/1/2] portal enable method direct
```

在接口 GigabitEthernet2/1/2 上引用 Portal Web 服务器 newpt。

```
[Router–GigabitEthernet2/1/2] portal apply web-server newpt
```

在接口 GigabitEthernet2/1/2 上设置发送给 Portal 认证服务器的 Portal 报文中的 BAS-IP 属性值为 2.2.2.1。

```
[Router–GigabitEthernet2/1/2] portal bas-ip 2.2.2.1
[Router–GigabitEthernet2/1/2] quit
```

4. 验证配置

以上配置完成后，通过执行以下显示命令可查看 Portal 配置是否生效。

```
[Router] display portal interface gigabitethernet 2/1/2
 Portal information of GigabitEthernet2/1/2
 IPv4:
     Portal status: Enabled
     Authentication type: Direct
     Portal Web server: newpt
     Authentication domain: Not configured
     Bas-ip: 2.2.2.1
     User Detection:  Not configured
     Action for server detection:
         Server type    Server name                          Action
         --             --                                   --
     Layer3 source network:
         IP address              Mask

     Destination authenticate subnet:
         IP address              Mask
IPv6:
     Portal status: Disabled
     Authentication type: Disabled
     Portal Web server: Not configured
     Authentication domain: Not configured
```

```
    Bas-ipv6: Not configured
    User detection: Not configured
    Action for server detection:
        Server type    Server name                          Action
        --             --                                   --
    Layer3 source network:
        IP address                                          Prefix length

    Destination authenticate subnet:
        IP address                                          Prefix length
```

用户既可以使用 H3C 的 iNode 客户端，也可以通过网页方式进行 Portal 认证。用户在通过认证前，只能访问认证页面 http://192.168.0.111:8080/portal，且发起的 Web 访问均被重定向到该认证页面，在通过认证后，可访问非受限的互联网资源。

认证通过后，可通过执行以下显示命令查看 Router 上生成的 Portal 在线用户信息。

```
[Router] display portal user interface gigabitethernet 2/1/2
Total portal users:  1
Username: abc
  Portal server: newpt
  State: Online
  Authorization ACL: None
  VPN instance: --
  MAC               IP                VLAN   Interface
  0015-e9a6-7cfe    2.2.2.2           --     GigabitEthernet2/1/2
```

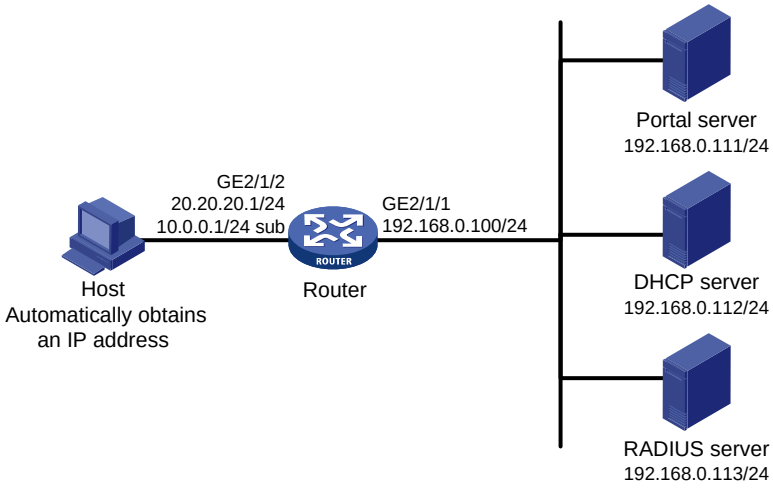
1.15.2 Portal二次地址分配认证配置举例

1. 组网需求

- 用户主机与接入设备 Router 直接相连，采用二次地址分配方式的 Portal 认证。用户通过 DHCP 服务器获取 IP 地址，Portal 认证前使用分配的一个私网地址；通过 Portal 认证后，用户申请到一个公网地址，才可以访问非受限互联网资源。
- 采用一台 Portal 服务器承担 Portal 认证服务器和 Portal Web 服务器的职责。
- 采用 RADIUS 服务器作为认证/计费服务器。

2. 组网图

图1-10 配置 Portal 二次地址分配认证组网图



3. 配置步骤

说明

- Portal 二次地址分配认证方式应用中，DHCP 服务器上需创建公网地址池（20.20.20.0/24）及私网地址池（10.0.0.0/24），具体配置略。
- Portal 二次地址分配认证方式应用中，接入设备上需要配置 DHCP 中继来配合 Portal 认证，且启动 Portal 的接口需要配置主 IP 地址（公网 IP）及从 IP 地址（私网 IP）。关于 DHCP 中继的详细配置请参见“三层技术-IP 业务配置指导”中的“DHCP 中继”。
- 请保证在 Portal 认证服务器上添加的 Portal 设备的 IP 地址为与用户相连的接口的公网 IP 地址（20.20.20.1），且与该 Portal 设备关联的 IP 地址组中的转换前地址为用户所在的私网网段（10.0.0.0/24）、转换后地址为公网网段（20.20.20.0/24）。
- 按照组网图配置设备各接口的 IP 地址，保证启动 Portal 之前各主机、服务器和设备之间的路由可达。
- 完成 RADIUS 服务器上的配置，保证用户的认证/计费功能正常运行。

在 Router 上进行以下配置。

(1) 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<Router> system-view
[Router] radius scheme rs1
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Router-radius-rs1] primary authentication 192.168.0.113
[Router-radius-rs1] primary accounting 192.168.0.113
[Router-radius-rs1] key authentication simple radius
[Router-radius-rs1] key accounting simple radius
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[Router-radius-rs1] user-name-format without-domain
[Router-radius-rs1] quit
```

使能 RADIUS session control 功能。

```
[Router] radius session-control enable
```

(2) 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[Router] domain dm1
```

配置 ISP 域的 RADIUS 方案 rs1。

```
[Router-isp-dm1] authentication portal radius-scheme rs1
[Router-isp-dm1] authorization portal radius-scheme rs1
[Router-isp-dm1] accounting portal radius-scheme rs1
[Router-isp-dm1] quit
```

配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方案。

```
[Router] domain default enable dm1
```

(3) 配置 DHCP 中继和授权 ARP

配置 DHCP 中继。

```
[Router] dhcp enable
[Router] dhcp relay client-information record
[Router] interface gigabitethernet 2/1/2
[Router–GigabitEthernet2/1/2] ip address 20.20.20.1 255.255.255.0
[Router–GigabitEthernet2/1/2] ip address 10.0.0.1 255.255.255.0 sub
[Router-GigabitEthernet2/1/2] dhcp select relay
[Router-GigabitEthernet2/1/2] dhcp relay server-address 192.168.0.112
```

使能授权 ARP 功能。

```
[Router-GigabitEthernet2/1/2] arp authorized enable
[Router-GigabitEthernet2/1/2] quit
```

(4) 配置 Portal 认证

配置 Portal 认证服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，监听 Portal 报文的端口为 50100。

```
[Router] portal server newpt
[Router-portal-server-newpt] ip 192.168.0.111 key simple portal
[Router-portal-server-newpt] port 50100
[Router-portal-server-newpt] quit
```

配置 Portal Web 服务器的 URL 为 http://192.168.0.111:8080/portal。（Portal Web 服务器的 URL 请与实际环境中的 Portal Web 服务器配置保持一致，此处仅为示例）

```
[Router] portal web-server newpt
[Router-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[Router-portal-websvr-newpt] quit
```

在接口 GigabitEthernet2/1/2 上使能二次地址方式的 Portal 认证。

```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] portal enable method redhcp
```

在接口 GigabitEthernet2/1/2 上引用 Portal Web 服务器 newpt。

```
[Router–GigabitEthernet2/1/2] portal apply web-server newpt
```

在接口 GigabitEthernet2/1/2 上设置发送给 Portal 报文中的 BAS-IP 属性值为 20.20.20.1。

```
[Router-GigabitEthernet2/1/2] portal bas-ip 20.20.20.1
[Router-GigabitEthernet2/1/2] quit
```

4. 验证配置

以上配置完成后，通过执行以下显示命令可查看 Portal 配置是否生效。

```
[Router] display portal interface gigabitethernet 2/1/2
 Portal information of GigabitEthernet2/1/2
 IPv4:
     Portal status: Enabled
     Authentication type: Redhcp
     Portal Web server: newpt
     Authentication domain: Not configured
     Bas-ip: 20.20.20.1
     User Detection:  Not configured
     Action for server detection:
         Server type    Server name                          Action
         --             --                                   --
     Layer3 source network:
         IP address              Mask

     Destination authenticate subnet:
         IP address              Mask
IPv6:
     Portal status: Disabled
     Authentication type: Disabled
     Portal Web server: Not configured
     Authentication domain: Not configured
     Bas-ipv6: Not configured
     User detection: Not configured
     Action for server detection:
         Server type    Server name                          Action
         --             --                                   --
     Layer3 source network:
         IP address                                          Prefix length

     Destination authenticate subnet:
         IP address                                          Prefix length
```

用户既可以使用 H3C 的 iNode 客户端，也可以通过网页方式进行 Portal 认证。用户在通过认证前，只能访问认证页面 http://192.168.0.111:8080/portal，且发起的 Web 访问均被重定向到该认证页面，在通过认证后，可访问非受限的互联网资源。

认证通过后，可通过执行以下显示命令查看 Router 上生成的 Portal 在线用户信息。

```
[Router] display portal user interface gigabitethernet 2/1/2
Total portal users:  1
Username: abc
  Portal server: newpt
  State: Online
  Authorization ACL: None
```

```
VPN instance: --
MAC                 IP                  VLAN    Interface
0015-e9a6-7cfe      20.20.20.2          --      GigabitEthernet2/1/2
```

1.15.3 可跨三层Portal认证配置举例

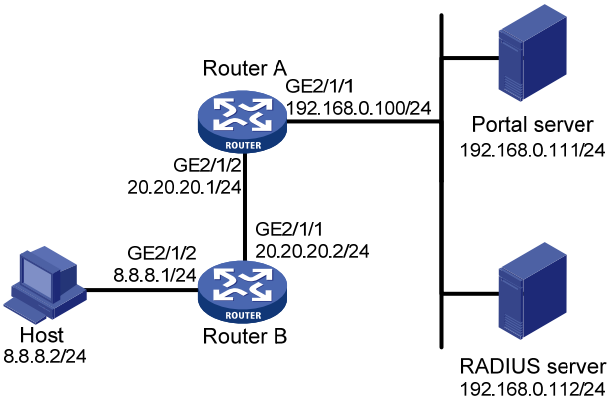
1. 组网需求

Router A 支持 Portal 认证功能。用户 Host 通过 Router B 接入到 Router A。

- 配置 Router A 采用可跨三层 Portal 认证。用户在未通过 Portal 认证前，只能访问 Portal Web 认证服务器；用户通过 Portal 认证后，可以访问非受限互联网资源。
- 采用一台 Portal 服务器承担 Portal 认证服务器和 Portal Web 服务器的职责。
- 采用 RADIUS 服务器作为认证/计费服务器。

2. 组网图

图1-11 配置可跨三层 Portal 认证组网图



3. 配置步骤

说明

- 请保证在 Portal 认证服务器上添加的 Portal 设备的 IP 地址为与用户相连的接口 IP 地址（20.20.20.1），且与该 Portal 设备关联的 IP 地址组为用户所在网段（8.8.8.0/24）。
- 按照组网图配置设备各接口的 IP 地址，保证启动 Portal 之前各主机、服务器和设备之间的路由可达。
- 完成 RADIUS 服务器上的配置，保证用户的认证/计费功能正常运行。

在 Router A 上进行以下配置。

(1) 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<RouterA> system-view
[RouterA] radius scheme rs1
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[RouterA-radius-rs1] primary authentication 192.168.0.112
```

```
[RouterA-radius-rs1] primary accounting 192.168.0.112
[RouterA-radius-rs1] key authentication simple radius
[RouterA-radius-rs1] key accounting simple radius
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[RouterA-radius-rs1] user-name-format without-domain
[RouterA-radius-rs1] quit
```

使能 RADIUS session control 功能。

```
[Router] radius session-control enable
```

(2) 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[RouterA] domain dm1
```

配置 ISP 域的 RADIUS 方案 rs1。

```
[RouterA-isp-dm1] authentication portal radius-scheme rs1
[RouterA-isp-dm1] authorization portal radius-scheme rs1
[RouterA-isp-dm1] accounting portal radius-scheme rs1
[RouterA-isp-dm1] quit
```

配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方案。

```
[Router] domain default enable dm1
```

(3) 配置 Portal 认证

配置 Portal 认证服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，监听 Portal 报文的端口为 50100。

```
[RouterA] portal server newpt
[RouterA-portal-server-newpt] ip 192.168.0.111 key simple portal
[RouterA-portal-server-newpt] port 50100
[RouterA-portal-server-newpt] quit
```

配置 Portal Web 服务器的 URL 为 http://192.168.0.111:8080/portal。（Portal Web 服务器的 URL 请与实际环境中的 Portal Web 服务器配置保持一致，此处仅为示例）

```
[Router] portal web-server newpt
[RouterA-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[RouterA-portal-websvr-newpt] quit
```

在接口 GigabitEthernet2/1/2 上使能可跨三层方式的 Portal 认证。

```
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] portal enable method layer3
```

在接口 GigabitEthernet2/1/2 上引用 Portal Web 服务器 newpt。

```
[RouterA-GigabitEthernet2/1/2] portal apply web-server newpt
```

在接口 GigabitEthernet2/1/2 上设置发送给 Portal 报文中的 BAS-IP 属性值为 20.20.20.1。

```
[RouterA-GigabitEthernet2/1/2] portal bas-ip 20.20.20.1
[RouterA-GigabitEthernet2/1/2] quit
```

Router B 上需要配置到 192.168.0.0/24 网段的缺省路由，下一跳为 20.20.20.1，具体配置略。

4. 验证配置

以上配置完成后，通过执行以下显示命令可查看 Portal 配置是否生效。

```
[Router] display portal interface gigabitethernet 2/1/2
 Portal information of GigabitEthernet2/1/2
```

```
 IPv4:
     Portal status: Enabled
     Authentication type: Layer3
     Portal Web server: newpt
     Authentication domain: Not configured
     Bas-ip: 20.20.20.1
     User Detection:  Not configured
     Action for server detection:
         Server type    Server name                          Action
         --             --                                   --
     Layer3 source network:
         IP address              Mask

     Destination authenticate subnet:
         IP address              Mask
IPv6:
     Portal status: Disabled
     Authentication type: Disabled
     Portal Web server: Not configured
     Authentication domain: Not configured
     Bas-ipv6: Not configured
     User detection: Not configured
     Action for server detection:
         Server type    Server name                          Action
         --             --                                   --
     Layer3 source network:
         IP address                                          Prefix length

     Destination authenticate subnet:
         IP address                                          Prefix length
```

用户既可以使用 H3C 的 iNode 客户端，也可以通过网页方式进行 Portal 认证。用户在通过认证前，只能访问认证页面 http://192.168.0.111:8080/portal，且发起的 Web 访问均被重定向到该认证页面，在通过认证后，可访问非受限的互联网资源。

认证通过后，可通过执行以下显示命令查看 Router 上生成的 Portal 在线用户信息。

```
[Router] display portal user interface gigabitethernet 2/1/2
Total portal users：  1
Username: abc
  Portal server: newpt
  State: Online
  Authorization ACL: None
  VPN instance: --
  MAC               IP               VLAN   Interface
  0015-e9a6-7cfe    8.8.8.2          --     GigabitEthernet2/1/2
```

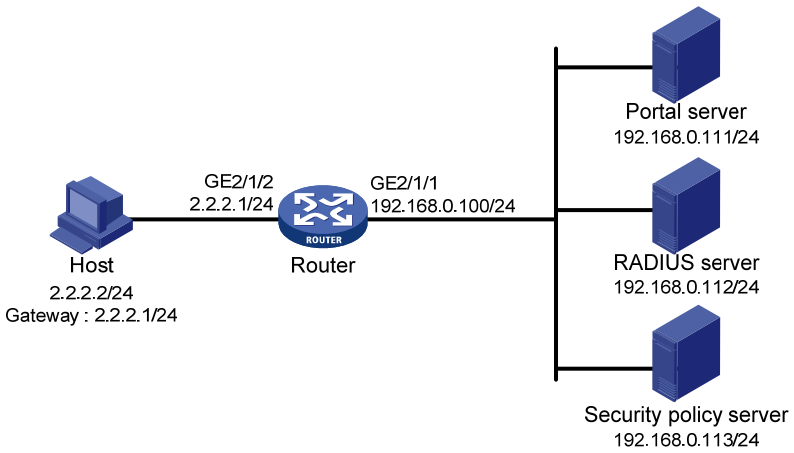
1.15.4 Portal直接认证扩展功能配置举例

1. 组网需求

- 用户主机与接入设备 Router 直接相连，采用直接方式的 Portal 认证。用户通过手工配置或 DHCP 获取的一个公网 IP 地址进行认证，在通过身份认证而没有通过安全认证时可以访问 192.168.0.0/24 网段；在通过安全认证后，可以使用此 IP 地址访问非受限互联网资源。
- 采用一台 Portal 服务器承担 Portal 认证服务器和 Portal Web 服务器的职责。
- 采用 RADIUS 服务器作为认证/计费服务器。

2. 组网图

图1-12 配置 Portal 直接认证扩展功能组网图



3. 配置步骤

说明

- 按照组网图配置设备各接口的 IP 地址，保证启动 Portal 之前各主机、服务器和设备之间的路由可达。
- 完成 RADIUS 服务器上的配置，保证用户的认证/计费功能正常运行。

在 Router 上进行以下配置。

(1) 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<Router> system-view
[Router] radius scheme rs1
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Router-radius-rs1] primary authentication 192.168.0.112
[Router-radius-rs1] primary accounting 192.168.0.112
[Router-radius-rs1] key accounting simple radius
[Router-radius-rs1] key authentication simple radius
[Router-radius-rs1] user-name-format without-domain
```

配置 RADIUS 方案的安全策略服务器 IP。

```
[Router-radius-rs1] security-policy-server 192.168.0.113
[Router-radius-rs1] quit
```

使能 RADIUS session control 功能。

```
[Router] radius session-control enable
```

(2) 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[Router] domain dm1
```

配置 ISP 域的 RADIUS 方案 rs1。

```
[Router-isp-dm1] authentication portal radius-scheme rs1
[Router-isp-dm1] authorization portal radius-scheme rs1
[Router-isp-dm1] accounting portal radius-scheme rs1
[Router-isp-dm1] quit
```

配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方案。

```
[Router] domain default enable dm1
```

(3) 配置隔离 ACL 为 3000，安全 ACL 为 3001

说明

安全策略服务器上需要将 ACL 3000 和 ACL 3001 分别指定为隔离 ACL 和安全 ACL。

```
[Router] acl number 3000
[Router-acl-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
[Router-acl-adv-3000] rule deny ip
[Router-acl-adv-3000] quit
[Router] acl number 3001
[Router-acl-adv-3001] rule permit ip
[Router-acl-adv-3001] quit
```

(4) 配置 Portal 认证

配置 Portal 认证服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，监听 Portal 报文的端口为 50100。

```
[Router] portal server newpt
[Router-portal-server-newpt] ip 192.168.0.111 key simple portal
[Router-portal-server-newpt] port 50100
[Router-portal-server-newpt] quit
```

配置 Portal Web 服务器的 URL 为 http://192.168.0.111:8080/portal。（Portal Web 服务器的 URL 请与实际环境中的 Portal Web 服务器配置保持一致，此处仅为示例）

```
[Router] portal web-server newpt
[Router-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[Router-portal-websvr-newpt] quit
```

在接口 GigabitEthernet2/1/2 上使能直接方式的 Portal 认证。

```
[Router] interface gigabitethernet 2/1/2
[Router–GigabitEthernet2/1/2] portal enable method direct
```

在接口 GigabitEthernet2/1/2 上引用 Portal Web 服务器 newpt。

```
[Router–GigabitEthernet2/1/2] portal apply web-server newpt
```

在接口 GigabitEthernet2/1/2 上设置发送给 Portal 报文中的 BAS-IP 属性值为 2.2.2.1。

```
[Router-GigabitEthernet2/1/2] portal bas-ip 2.2.2.1
[Router-GigabitEthernet2/1/2] quit
```

4. 验证配置

以上配置完成后，通过执行以下显示命令可查看 Portal 配置是否生效。

```
[Router] display portal interface gigabitethernet 2/1/2
 Portal information of GigabitEthernet2/1/2
 IPv4:
     Portal status: Enabled
     Authentication type: Direct
     Portal Web server: newpt
     Authentication domain: Not configured
     Bas-ip: 2.2.2.1
     User Detection:  Not configured
     Action for server detection:
         Server type    Server name                          Action
         --             --                                   --
     Layer3 source network:
         IP address              Mask

     Destination authenticate subnet:
         IP address              Mask
IPv6:
     Portal status: Disabled
     Authentication type: Disabled
     Portal Web server: Not configured
     Authentication domain: Not configured
     Bas-ipv6: Not configured
     User detection: Not configured
     Action for server detection:
         Server type    Server name                          Action
         --             --                                   --
     Layer3 source network:
         IP address                                          Prefix length

     Destination authenticate subnet:
         IP address                                          Prefix length
```

使用 H3C iNode 客户端的用户在通过认证前，只能访问认证页面 http://192.168.0.111:8080/portal，且发起的 Web 访问均被重定向到该认证页面。通过身份认证但未通过安全认证时，只能访问匹配 ACL 3000 的网络资源；通过身份认证以及安全认证后，可以访问匹配 ACL 3001 的互联网资源。

认证通过后，可通过执行以下显示命令查看 Router 上生成的 Portal 在线用户信息。

```
[Router] display portal user interface gigabitethernet 2/1/2
Total portal users:  1
Username: abc
  Portal server: newpt
  State: Online
  Authorization ACL: 3001
```

```
VPN instance: --
MAC                 IP                  VLAN    Interface
0015-e9a6-7cfe      2.2.2.2             --      GigabitEthernet2/1/2
```

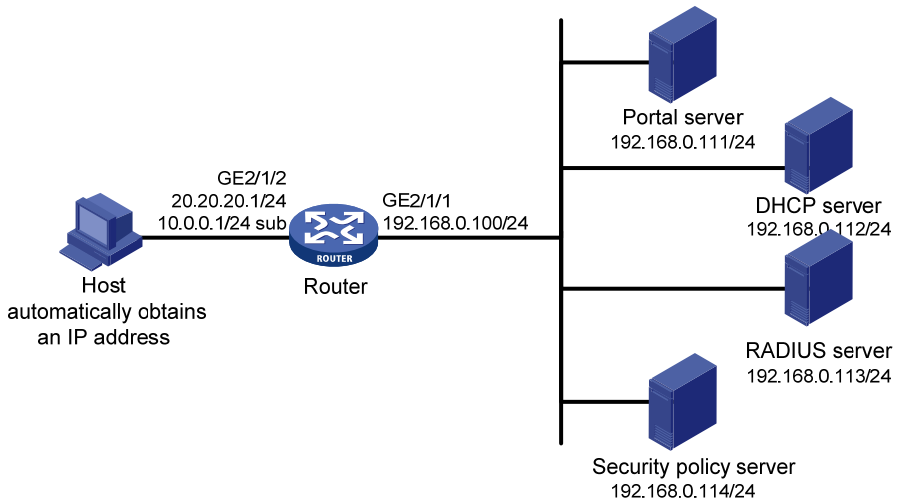
1.15.5 Portal二次地址分配认证扩展功能配置举例

1. 组网需求

- 用户主机与接入设备 Router 直接相连，采用二次地址分配方式的 Portal 认证。用户通过 DHCP 服务器获取 IP 地址，Portal 认证前使用分配的一个私网地址；通过 Portal 认证后，用户申请到一个公网地址。
- 用户在通过身份认证而没有通过安全认证时可以访问 192.168.0.0/24 网段；在通过安全认证后，可以访问非受限互联网资源。
- 采用一台 Portal 服务器承担 Portal 认证服务器和 Portal Web 服务器的职责。
- 采用 RADIUS 服务器作为认证/计费服务器。

2. 组网图

图1-13 配置 Portal 二次地址分配认证扩展功能组网图



3. 配置步骤

说明

- Portal 二次地址分配认证方式应用中，DHCP 服务器上需创建公网地址池（20.20.20.0/24）及私网地址池（10.0.0.0/24），具体配置略。
- Portal 二次地址分配认证方式应用中，接入设备需要配置 DHCP 中继来配合 Portal 认证，且启动 Portal 的接口需要配置主 IP 地址（公网 IP）及从 IP 地址（私网 IP）。关于 DHCP 中继的详细配置请参见“三层技术-IP 业务配置指导”中的“DHCP 中继”。
- 请保证在 Portal 认证服务器上添加的 Portal 设备的 IP 地址为与用户相连的接口的公网 IP 地址（20.20.20.1），且与该 Portal 设备关联的 IP 地址组中的转换前地址为用户所在的私网网段（10.0.0.0/24）、转换后地址为公网网段（20.20.20.0/24）。
- 按照组网图配置设备各接口的 IP 地址，保证启动 Portal 之前各主机、服务器和设备之间的路由可达。
- 完成 RADIUS 服务器上的配置，保证用户的认证/计费功能正常运行。

在 Router 上进行以下配置。

(1) 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<Router> system-view
[Router] radius scheme rs1
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Router-radius-rs1] primary authentication 192.168.0.113
[Router-radius-rs1] primary accounting 192.168.0.113
[Router-radius-rs1] key authentication simple radius
[Router-radius-rs1] key accounting simple radius
[Router-radius-rs1] user-name-format without-domain
```

配置 RADIUS 方案的安全策略服务器 IP。

```
[Router-radius-rs1] security-policy-server 192.168.0.114
```

使能 RADIUS session control 功能。

```
[Router-radius-rs1] radius session-control enable
[Router-radius-rs1] quit
```

使能 RADIUS session control 功能。

```
[Router] radius session-control enable
```

(2) 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[Router] domain dm1
```

配置 ISP 域的 RADIUS 方案 rs1。

```
[Router-isp-dm1] authentication portal radius-scheme rs1
[Router-isp-dm1] authorization portal radius-scheme rs1
[Router-isp-dm1] accounting portal radius-scheme rs1
[Router-isp-dm1] quit
```

配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方案。

```
[Router] domain default enable dm1
```

(3) 配置隔离 ACL 为 3000，安全 ACL 为 3001

说明

安全策略服务器上需要将 ACL 3000 和 ACL 3001 分别指定为隔离 ACL 和安全 ACL。

```
[Router] acl number 3000
[Router-acl-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
[Router-acl-adv-3000] rule deny ip
[Router-acl-adv-3000] quit
[Router] acl number 3001
[Router-acl-adv-3001] rule permit ip
[Router-acl-adv-3001] quit
```

(4) 配置 DHCP 中继和授权 ARP

配置 DHCP 中继。

```
[Router] dhcp enable
[Router] dhcp relay client-information record
[Router] interface gigabitethernet 2/1/2
[Router–GigabitEthernet2/1/2] ip address 20.20.20.1 255.255.255.0
[Router–GigabitEthernet2/1/2] ip address 10.0.0.1 255.255.255.0 sub
[Router-GigabitEthernet2/1/2] dhcp select relay
[Router-GigabitEthernet2/1/2] dhcp relay server-address 192.168.0.112
```

使能授权 ARP 功能。

```
[Router-GigabitEthernet2/1/2] arp authorized enable
[Router-GigabitEthernet2/1/2] quit
```

(5) 配置 Portal 认证

配置 Portal 认证服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，监听 Portal 报文的端口为 50100。

```
[Router] portal server newpt
[Router-portal-server-newpt] ip 192.168.0.111 key simple portal
[Router-portal-server-newpt] port 50100
[Router-portal-server-newpt] quit
```

配置 Portal Web 服务器的 URL 为 http://192.168.0.111:8080/portal。（Portal Web 服务器的 URL 请与实际环境中的 Portal Web 服务器配置保持一致，此处仅为示例）

```
[Router] portal web-server newpt
[Router-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[Router-portal-websvr-newpt] quit
```

在接口 GigabitEthernet1/0/2 上使能二次地址方式的 Portal 认证。

```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] portal enable method redhcp
```

在接口 GigabitEthernet2/1/2 上引用 Portal Web 服务器 newpt。

```
[Router–GigabitEthernet2/1/2] portal apply web-server newpt
```

在接口 GigabitEthernet2/1/2 上设置发送给 Portal 报文中的 BAS-IP 属性值为 20.20.20.1。

```
[Router-GigabitEthernet2/1/2] portal bas-ip 20.20.20.1
[Router-GigabitEthernet2/1/2] quit
```

4. 验证配置

以上配置完成后，通过执行以下显示命令可查看 Portal 配置是否生效。

```
[Router] display portal interface gigabitethernet 2/1/2
 Portal information of GigabitEthernet2/1/2
 IPv4:
     Portal status: Enabled
     Authentication type: Redhcp
     Portal Web server: newpt
     Authentication domain: Not configured
     Bas-ip: 20.20.20.1
     User Detection:  Not configured
     Action for server detection:
         Server type    Server name                          Action
         --             --                                   --
     Layer3 source network:
         IP address               Mask

     Destination authenticate subnet:
         IP address               Mask
IPv6:
     Portal status: Disabled
     Authentication type: Disabled
     Portal Web server: Not configured
     Authentication domain: Not configured
     Bas-ipv6: Not configured
     User detection: Not configured
     Action for server detection:
         Server type    Server name                          Action
         --             --                                   --
     Layer3 source network:
         IP address                                          Prefix length

     Destination authenticate subnet:
         IP address                                          Prefix length
```

使用 H3C iNode 客户端的用户在通过认证前，只能访问认证页面 http://192.168.0.111:8080/portal，且发起的 Web 访问均被重定向到该认证页面。通过身份认证但未通过安全认证时，只能访问匹配 ACL 3000 的网络资源；通过身份认证以及安全认证后，可以访问匹配 ACL 3001 的互联网资源。

认证通过后，可通过执行以下显示命令查看 Router 上生成的 Portal 在线用户信息。

```
[Router] display portal user interface gigabitethernet 2/1/2
Total portal users:  1
Username: abc
  Portal server: newpt
  State: Online
  Authorization ACL: 3001
```

```
VPN instance: --
MAC                 IP                  VLAN    Interface
0015-e9a6-7cfe      20.20.20.2          --      GigabitEthernet2/1/2
```

1.15.6 可跨三层Portal认证扩展功能配置举例

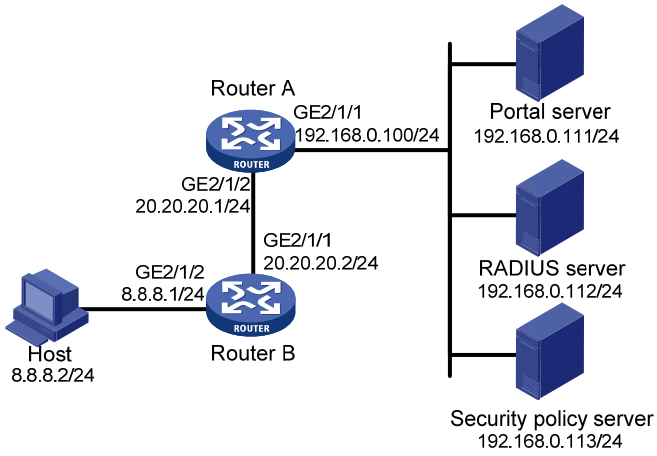
1. 组网需求

Router A 支持 Portal 认证功能。用户 Host 通过 Router B 接入到 Router A。

- 配置 Router A 采用可跨三层 Portal 认证。用户在通过身份认证而没有通过安全认证时可以访问 192.168.0.0/24 网段；在通过安全认证后，可以访问非受限互联网资源。
- 采用一台 Portal 服务器承担 Portal 认证服务器和 Portal Web 服务器的职责。
- 采用 RADIUS 服务器作为认证/计费服务器。

2. 组网图

图1-14 配置可跨三层 Portal 认证扩展功能组网图



3. 配置步骤

说明

- 请保证在 Portal 认证服务器上添加的 Portal 设备的 IP 地址为与用户相连的接口 IP 地址（20.20.20.1），且与该 Portal 设备关联的 IP 地址组为用户所在网段（8.8.8.0/24）。
- 按照组网图配置设备各接口的 IP 地址，保证启动 Portal 之前各主机、服务器和设备之间的路由可达。
- 完成 RADIUS 服务器上的配置，保证用户的认证/计费功能正常运行。

在 Router A 上进行以下配置。

(1) 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<RouterA> system-view
[RouterA] radius scheme rs1
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[RouterA-radius-rs1] primary authentication 192.168.0.112
[RouterA-radius-rs1] primary accounting 192.168.0.112
[RouterA-radius-rs1] key authentication simple radius
[RouterA-radius-rs1] key accounting simple radius
[RouterA-radius-rs1] user-name-format without-domain
```

配置 RADIUS 方案的安全策略服务器 IP。

```
[RouterA-radius-rs1] security-policy-server 192.168.0.113
[RouterA-radius-rs1] quit
```

使能 RADIUS session control 功能。

```
[RouterA] radius session-control enable
```

(2) 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[RouterA] domain dm1
```

配置 ISP 域的 RADIUS 方案 rs1。

```
[RouterA-isp-dm1] authentication portal radius-scheme rs1
[RouterA-isp-dm1] authorization portal radius-scheme rs1
[RouterA-isp-dm1] accounting portal radius-scheme rs1
[RouterA-isp-dm1] quit
```

配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方案。

```
[RouterA] domain default enable dm1
```

(3) 配置隔离 ACL 为 3000，安全 ACL 为 3001

说明

安全策略服务器上需要将 ACL 3000 和 ACL 3001 分别指定为隔离 ACL 和安全 ACL。

```
[RouterA] acl number 3000
[RouterA-acl-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
[RouterA-acl-adv-3000] rule deny ip
[RouterA-acl-adv-3000] quit
[RouterA] acl number 3001
[RouterA-acl-adv-3001] rule permit ip
[RouterA-acl-adv-3001] quit
```

(4) 配置 Portal 认证

配置 Portal 认证服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，监听 Portal 报文的端口为 50100。

```
[RouterA] portal server newpt
[RouterA-portal-server-newpt] ip 192.168.0.111 key simple portal
[RouterA-portal-server-newpt] port 50100
[RouterA-portal-server-newpt] quit
```

配置 Portal Web 服务器的 URL 为 http://192.168.0.111:8080/portal。（Portal Web 服务器的 URL 请与实际环境中的 Portal Web 服务器配置保持一致，此处仅为示例）

```
[Router] portal web-server newpt
[RouterA-portal-websvr-newpt] url http://192.168.0.111:8080/portal
```

```
[RouterA-portal-websvr-newpt] quit
```

在接口 GigabitEthernet2/1/2 上使能可跨三层方式的 Portal 认证。

```
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] portal enable method layer3
```

在接口 GigabitEthernet2/1/2 上引用 Portal Web 服务器 newpt。

```
[RouterA-GigabitEthernet2/1/2] portal apply web-server newpt
```

在接口 GigabitEthernet2/1/2 上设置发送给 Portal 报文中的 BAS-IP 属性值为 20.20.20.1。

```
[RouterA-GigabitEthernet2/1/2] portal bas-ip 20.20.20.1
[RouterA-GigabitEthernet2/1/2] quit
```

Router B 上需要配置到 192.168.0.0/24 网段的缺省路由，下一跳为 20.20.20.1，具体配置略。

4. 验证配置

以上配置完成后，通过执行以下显示命令可查看 Portal 配置是否生效。

```
[Router] display portal interface gigabitethernet 2/1/2
 Portal information of GigabitEthernet2/1/2
 IPv4:
     Portal status: Enabled
     Authentication type: Layer3
     Portal Web server: newpt
     Authentication domain: Not configured
     Bas-ip: 20.20.20.1
     User Detection:  Not configured
     Action for server detection:
         Server type    Server name                        Action
         --             --                                 --
     Layer3 source network:
         IP address              Mask

     Destination authenticate subnet:
         IP address              Mask
IPv6:
     Portal status: Disabled
     Authentication type: Disabled
     Portal Web server: Not configured
     Authentication domain: Not configured
     Bas-ipv6: Not configured
     User detection: Not configured
     Action for server detection:
         Server type    Server name                        Action
         --             --                                 --
     Layer3 source network:
         IP address                                        Prefix length

     Destination authenticate subnet:
         IP address                                        Prefix length
```

使用 H3C iNode 客户端的用户在通过认证前，只能访问认证页面 http://192.168.0.111:8080/portal，且发起的 Web 访问均被重定向到该认证页面。通过身份认证但未通过安全认证时，只能访问匹配 ACL 3000 的网络资源；通过身份认证以及安全认证后，可以访问匹配 ACL 3001 的互联网资源。

认证通过后，可通过执行以下显示命令查看 Router 上生成的 Portal 在线用户信息。

```
[Router] display portal user interface gigabitethernet 2/1/2
Total portal users:  1
Username: abc
  Portal server: newpt
  State: Online
  Authorization ACL: 3001
  VPN instance: --
  MAC                IP                 VLAN    Interface
  0015-e9a6-7cfe     8.8.8.2            --      GigabitEthernet2/1/2
```

1.15.7 Portal认证服务器探测和用户信息同步功能配置举例

1. 组网需求

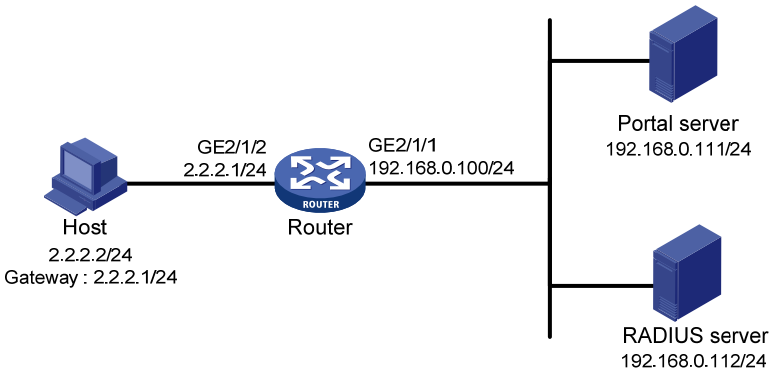
用户主机与接入设备 Router 直接相连，通过 Portal 认证接入网络，并采用一台 Portal 服务器承担 Portal 认证服务器和 Portal Web 服务器的职责，采用 RADIUS 服务器作为认证/计费服务器。

具体要求如下：

- 用户通过手工配置或 DHCP 获取的一个公网 IP 地址进行认证，在通过 Portal 认证前，只能访问 Portal 认证服务器；在通过 Portal 认证后，可以使用此 IP 地址访问非受限的互联网资源。
- 接入设备能够探测到 Portal 认证服务器是否可达，并输出可达状态变化的日志信息，在服务器不可达时（例如，网络连接中断、网络设备故障或服务器无法正常提供服务等情况），取消 Portal 认证，使得用户仍然可以正常访问网络。
- 接入设备能够与服务器定期进行用户信息的同步。

2. 组网图

图1-15 Portal 认证服务器探测和用户同步信息功能配置组网图



3. 配置思路

(1) 配置 Portal 认证服务器，并启动逃生心跳功能和用户心跳功能；

(2) 配置 RADIUS 服务器，实现正常的认证及计费功能；

(3) 接入设备通过接口 GigabitEthernet2/1/2 与用户主机直接相连，在该接口上配置直接方式的 Portal 认证；

(4) 接入设备上配置 Portal 认证服务器探测功能，在与 Portal 认证服务器的逃生心跳功能的配合下，对 Portal 认证服务器的可达状态进行探测；

(5) 接入设备上配置 Portal 用户信息同步功能，在与 Portal 认证服务器的用户心跳功能的配合下，与 Portal 认证服务器上的用户信息进行同步。

4. 配置步骤

说明

- 按照组网图配置设备各接口的 IP 地址，保证启动 Portal 之前各主机、服务器和设备之间的路由可达。
- 完成 RADIUS 服务器上的配置，保证用户的认证/计费功能正常运行。

(1) 配置 Portal 认证服务器（iMC PLAT 5.0）

说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 5.0(E0101)、iMC UAM 5.0(E0101)），说明 Portal server 的基本配置。

配置 Portal 认证服务器。

登录进入 iMC 管理平台，选择“业务”页签，单击导航树中的[Portal 认证服务器管理/服务器配置]菜单项，进入服务器配置页面。

- 配置逃生心跳间隔时长及用户心跳间隔时长；
- 其它参数使用缺省配置。

图1-16 Portal 认证服务器配置页面

配置 IP 地址组。

单击导航树中的[Portal 认证服务器管理/IP 地址组配置]菜单项，进入 Portal IP 地址组配置页面，在该页面中单击<增加>按钮，进入增加 IP 地址组配置页面。

- 填写 IP 地址组名；
- 输入起始地址和终止地址。用户主机 IP 地址必须包含在该 IP 地址组范围内；
- 选择业务分组，本例中使用缺省的“未分组”；
- 选择 IP 地址组的类型为“普通”。

图1-17 增加 IP 地址组配置页面

增加 Portal 设备。

单击导航树中的[Portal 认证服务器管理/设备配置]菜单项，进入 Portal 设备配置页面，在该页面中单击<增加>按钮，进入增加设备信息配置页面。

- 填写设备名；

- 指定 IP 地址为与接入用户相连的设备接口 IP；
- 输入密钥，与接入设备 Router 上的配置保持一致；
- 选择是否进行二次地址分配，本例中为直接认证，因此为否；
- 选择支持逃生心跳功能和用户心跳功能。

图1-18 增加设备信息配置页面

Portal 设备关联 IP 地址组

在 Portal 设备配置页面中的设备信息列表中，点击 NAS 设备的<端口组信息管理>链接，进入端口组信息配置页面。

图1-19 设备信息列表

在端口组信息配置页面中点击<增加>按钮，进入增加端口组信息配置页面。

- 填写端口组名；
- 选择 IP 地址组，用户接入网络时使用的 IP 地址必须属于所选的 IP 地址组；
- 其它参数采用缺省值。

图1-20 增加端口组信息配置页面

最后单击导航树中的[业务参数配置/系统配置手工生效]菜单项，使以上 Portal 认证服务器配置生效。

(2) 配置 Router

- 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<Router> system-view
[Router] radius scheme rs1
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Router-radius-rs1] primary authentication 192.168.0.112
[Router-radius-rs1] primary accounting 192.168.0.112
[Router-radius-rs1] key authentication simple radius
[Router-radius-rs1] key accounting simple radius
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[Router-radius-rs1] user-name-format without-domain
[Router-radius-rs1] quit
```

使能 RADIUS session control 功能。

```
[Router] radius session-control enable
```

- 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[Router] domain dm1
```

配置 ISP 域的 RADIUS 方案 rs1。

```
[Router-isp-dm1] authentication portal radius-scheme rs1
[Router-isp-dm1] authorization portal radius-scheme rs1
[Router-isp-dm1] accounting portal radius-scheme rs1
[Router-isp-dm1] quit
```

配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方案。

```
[Router] domain default enable dm1
```

- 配置 Portal 认证

配置 Portal 认证服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，监听 Portal 报文的端口为 50100。

```
[Router] portal server newpt
[Router-portal-server-newpt] ip 192.168.0.111 key simple portal
[Router-portal-server-newpt] port 50100
```

配置对 Portal 认证服务器 newpt 的探测功能：每次探测间隔时间为 40 秒，若服务器可达状态改变，则发送日志信息。

```
[Router-portal-server-newpt] server-detect timeout 40 log
```

说明

此处 **timeout** 取值应该大于等于 Portal 认证服务器的逃生心跳间隔时长。

配置对 Portal 认证服务器 newpt 的 Portal 用户信息同步功能，检测用户同步报文的时间间隔为 600 秒，如果设备中的某用户信息在 600 秒内未在该 Portal 认证服务器发送的同步报文中出现，设备将强制该用户下线。

```
[Router-portal-server-newpt] user-sync timeout 600
[Router-portal-server-newpt] quit
```

说明

此处 **timeout** 取值应该大于等于 Portal 认证服务器上的用户心跳间隔时长。

配置 Portal Web 服务器的 URL 为 http://192.168.0.111:8080/portal。（Portal Web 服务器的 URL 请与实际环境中的 Portal Web 服务器配置保持一致，此处仅为示例）

```
[Router] portal web-server newpt
[Router-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[Router-portal-websvr-newpt] quit
```

在接口 GigabitEthernet2/1/2 上使能直接方式的 Portal 认证。

```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] portal enable method direct
```

开启 Portal 认证服务器 newpt 不可达时的 Portal 用户逃生功能。

```
[Router-GigabitEthernet2/1/2] portal fail-permit server newpt
```

在接口 GigabitEthernet2/1/2 上引用 Portal Web 服务器 newpt。

```
[Router-GigabitEthernet2/1/2] portal apply web-server newpt
```

在接口 GigabitEthernet2/1/2 上设置发送给 Portal 报文中的 BAS-IP 属性值为 2.2.2.1。

```
[Router-GigabitEthernet2/1/2] portal bas-ip 2.2.2.1
[Router-GigabitEthernet2/1/2] quit
```

5. 验证配置结果

以上配置完成后，可以通过执行以下命令查看到 Portal 认证服务器的状态为 Up，说明当前 Portal 认证服务器可达。

```
[Router] display portal server newpt
Portal server: newpt
  IP                    : 192.168.0.111
  VPN instance          : Not configured
  Port                  : 50100
  Server Detection      : Timeout 40s  Action: log
  User synchronization  : Timeout 600s
  Status                : Up
```

之后，若接入设备探测到 Portal 认证服务器不可达了，可通过以上显示命令查看到 Portal 认证服务器的状态为 Down，同时，设备会输出表示服务器不可达的日志信息“Portal server newpt turns down from up.”，并取消对该接口接入的用户的 Portal 认证，使得用户可以直接访问外部网络。

1.15.8 可跨三层Portal认证支持多实例配置举例

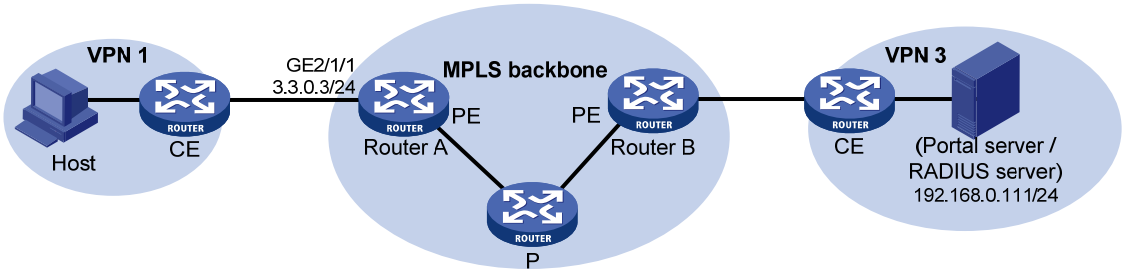
1. 组网需求

连接客户端的 PE 设备 Rourer A 对私网 VPN 1 中的用户 Host 进行 Portal 接入认证，RADIUS 服务器和 Portal 服务器位于私网 VPN 3 中。

- 配置 Rourer A 采用可跨三层 Portal 认证。用户在通过身份认证后，可以访问非受限网络资源。
- 采用一台 Portal 服务器承担 Portal 认证服务器、Portal Web 服务器和 RADIUS 服务器的职责。

2. 组网图

图1-21 配置可跨三层 Portal 认证支持多实例组网图



3. 配置步骤

说明

- 启动 Portal 之前，需要首先配置 MPLS L3VPN 功能，通过为 VPN 1 和 VPN 3 指定匹配的 VPN Target，确保 VPN 1 和 VPN 3 可以互通。本例仅介绍连接客户端的 PE 上接入认证的相关配置，其它配置请参考“MPLS 配置指导”中的“MPLS L3VPN”。
- 完成 RADIUS 服务器上的配置，保证用户的认证/计费功能正常运行。

在 Router A 上进行以下配置。

(1) 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<RouterA> system-view
[RouterA] radius scheme rs1
```

配置 RADIUS 方案所属的 VPN 实例为 vpn3。该 VPN 实例为连接服务器的接口上绑定的 VPN 实例，具体请以 Router A 上的 MPLS L3VPN 配置为准。

```
[RouterA-radius-rs1] vpn-instance vpn3
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[RouterA-radius-rs1] primary authentication 192.168.0.111
[RouterA-radius-rs1] primary accounting 192.168.0.111
[RouterA-radius-rs1] key accounting simple radius
[RouterA-radius-rs1] key authentication simple radius
```

配置向 RADIUS 服务器发送的用户名不携带域名。

```
[RouterA-radius-rs1] user-name-format without-domain
```

配置发送 RADIUS 报文使用的源地址为 3.3.0.3。

```
[RouterA-radius-rs1] nas-ip 3.3.0.3
[RouterA-radius-rs1] quit
```

使能 RADIUS session control 功能。

```
[RouterA] radius session-control enable
```

说明

建议通过命令 **nas-ip** 指定设备发送 RADIUS 报文的源地址，并与服务器上指定的接入设备 IP 保持一致，避免未指定源地址的情况下，设备选择的源地址与服务器上指定的接入设备 IP 不一致，而造成认证失败。

(2) 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[RouterA] domain dm1
```

配置 ISP 域的 RADIUS 方案 rs1。

```
[RouterA-isp-dm1] authentication portal radius-scheme rs1
[RouterA-isp-dm1] authorization portal radius-scheme rs1
[RouterA-isp-dm1] accounting portal radius-scheme rs1
[RouterA-isp-dm1] quit
```

配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方案。

```
[RouterA] domain default enable dm1
```

(3) 配置 Portal 认证

配置 Portal 认证服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，所属 VPN 实例名称为 vpn3，监听 Portal 报文的端口为 50100。

```
[RouterA] portal server newpt
[RouterA-portal-server-newpt] ip 192.168.0.111 vpn-instance vpn3 key simple portal
[RouterA-portal-server-newpt] port 50100
[RouterA-portal-server-newpt] quit
```

配置 Portal Web 服务器的 URL 为 http://192.168.0.111:8080/portal，所属 VPN 实例名称为 vpn3。（Portal Web 服务器的 URL 请与实际环境中的 Portal Web 服务器配置保持一致，此处仅为示例）

```
[RouterA] portal web-server newpt
[RouterA-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[RouterA-portal-websvr-newpt] vpn-instance vpn3
[RouterA-portal-websvr-newpt] quit
```

在接口 GigabitEthernet2/1/1 上使能可跨三层方式的 Portal 认证。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] portal enable method layer3
```

在接口 GigabitEthernet2/1/1 上引用 Portal Web 服务器 newpt。

```
[RouterA-GigabitEthernet2/1/1] portal apply web-server newpt
```

在接口 GigabitEthernet2/1/1 上设置发送给 Portal 报文中的 BAS-IP 属性值为 3.3.0.3。

```
[RouterA-GigabitEthernet2/1/1] portal bas-ip 3.3.0.3
[RouterA-GigabitEthernet2/1/1] quit
```

4. 验证配置结果

以上配置完成后，通过执行命令 **display portal server** 可查看 Portal 配置是否生效。用户认证通过后，通过执行命令 **display portal user** 查看 Router A 上生成的 Portal 在线用户信息。

```
[RouterA] display portal user all
Total portal users:  1
Username: abc
  Portal server: newpt
  State: Online
  Authorization ACL: None
  VPN instance: vpn3
  MAC                IP                VLAN   Interface
  000d-88f7-c268     3.3.0.1           --     GigabitEthernet2/1/1
```

1.16 常见配置错误举例

1.16.1 Portal用户认证时，没有弹出Portal认证页面

1. 故障现象

用户被强制去访问 Portal Web 认证服务器时没有弹出 Portal 认证页面，也没有错误提示，登录的 Portal Web 服务器页面为空白。

2. 故障分析

接入设备上配置的 Portal 密钥和 Portal 认证服务器上配置的密钥不一致，导致 Portal 认证服务器报文验证出错，Portal 认证服务器拒绝弹出认证页面。

3. 处理过程

使用 **display portal server** 命令查看接入设备上是否配置了 Portal 认证服务器密钥，若没有配置密钥，请补充配置；若配置了密钥，请在 Portal 认证服务器视图中使用 **ip** 或 **ipv6** 命令修改密钥，或者在 Portal 认证服务器上查看对应接入设备的密钥并修改密钥，直至两者的密钥设置一致。

1.16.2 接入设备上无法强制Portal用户下线

1. 故障现象

用户通过 Portal 认证后，在接入设备上使用 **portal delete-user** 命令强制用户下线失败，但是使用客户端的“断开”属性可以正常下线。

2. 故障分析

在接入设备上使用 **portal delete-user** 命令强制用户下线时，由接入设备主动发送下线通知报文到 Portal 认证服务器，Portal 认证服务器会在指定的端口监听该报文（缺省为 50100），但是接入设备发送的下线通知报文的目的端口和 Portal 认证服务器真正的监听端口不一致，故 Portal 认证服务器无法收到下线通知报文，Portal 认证服务器上的用户无法下线。

当使用客户端的“断开”属性让用户下线时，由 Portal 认证服务器主动向接入设备发送下线请求，其源端口为 50100，接入设备的下线应答报文的目的端口使用请求报文的源端口，避免了其配置上的错误，使得 Portal 认证服务器可以收到下线应答报文，从而 Portal 认证服务器上的用户成功下线。

3. 处理过程

使用 **display portal server** 命令查看接入设备对应服务器的端口，并在系统视图中使用 **portal server** 命令修改服务器的端口，使其和 Portal 认证服务器上的监听端口一致。

1.16.3 RADIUS服务器上无法强制Portal用户下线

1. 故障现象

接入设备使用 H3C 的 iMC 服务器作为 RADIUS 服务器对 Portal 用户进行身份认证，用户通过 Portal 认证上线后，管理员无法在 RADIUS 服务器上强制 Portal 用户下线。

2. 故障分析

H3C 的 iMC 服务器使用 session control 报文向设备发送断开连接请求。接入设备上监听 session control 报文的 UDP 端口缺省是关闭的，因此无法接收 RADIUS 服务器发送的 Portal 用户下线请求。

3. 处理过程

查看接入设备上的 RADIUS session control 功能是否处于开启状态，若未开启，请在系统视图下执行 **radius session control enable** 命令开启。

1.16.4 接入设备强制用户下线后，Portal认证服务器上还存在该用户

1. 故障现象

接入设备上通过命令行强制 Portal 用户下线后，Portal 认证服务器上还存在该用户。

2. 故障分析

在接入设备上使用 **portal delete-user** 命令强制用户下线时，由接入设备主动发送下线通知报文到 Portal 认证服务器，若接入设备主动发送的 Portal 报文携带的 BAS-IP/BAS-IPv6 属性值与 Portal 认证服务器上指定的设备 IP 地址不一致，Portal 认证服务器会将该下线通知报文丢弃。当接入设备尝试发送该报文超时之后，会将该用户强制下线，但 Portal 认证服务器上由于并未成功接收这样的通知报文，认为该用户依然在线。

3. 处理过程

在使能 Portal 认证的接口上配置 BAS-IP/BAS-IPv6 属性值，使其与 Portal 认证服务器上指定的设备 IP 地址保持一致。

1.16.5 二次地址分配认证用户无法成功上线

1. 故障现象

设备对用户采用二次地址分配认证方式的 Portal 认证，用户输入正确的用户名和密码，且客户端先后成功获取到了私网 IP 地址和公网的 IP 地址，但认证结果为失败。

2. 故障分析

在接入设备对用户进行二次地址分配认证过程中，当接入设备感知到客户端的 IP 地址更新之后，需要主动发送 Portal 通知报文告知 Portal 认证服务器已检测到用户 IP 变化，当 Portal 认证服务器接收到客户端以及接入设备发送的关于用户 IP 变化的通告后，才会通知客户端上线成功。若接入设备主动发送的 Portal 报文携带的 BAS-IP/BAS-IPv6 属性值与 Portal 认证服务器上指定的设备 IP 地址不一致时，Portal 认证服务器会将该 Portal 通知报文丢弃，因此会由于未及时收到用户 IP 变化的通告认为用户认证失败。

3. 处理过程

在使能 Portal 认证的接口上配置 BAS-IP/BAS-IPv6 属性值，使其与 Portal 认证服务器上指定的设备 IP 地址保持一致。

目 录

1 端口安全

说明

本特性仅在安装了二层交换卡的款型和 MSR3600-28/MSR3600-51 的固定二层接口上支持。

1.1 端口安全简介

1.1.1 概述

端口安全是一种基于 MAC 地址对网络接入进行控制的安全机制，是对已有的 802.1X 认证和 MAC 地址认证的扩充。这种机制通过检测端口收到的数据帧中的源 MAC 地址来控制非授权设备或主机对网络的访问，通过检测从端口发出的数据帧中的目的 MAC 地址来控制对非授权设备的访问。

端口安全的主要功能是通过定义各种端口安全模式，让设备学习到合法的源 MAC 地址，以达到相应的网络管理效果。启动了端口安全功能之后，当发现非法报文时，系统将触发相应特性，并按照预先指定的方式进行处理，既方便用户的管理又提高了系统的安全性。这里的非法报文是指：

- MAC 地址未被端口学习到的用户报文；
- 未通过认证的用户报文。

由于端口安全特性通过多种安全模式提供了 802.1X 和 MAC 地址认证的扩展和组合应用，因此在需要灵活使用以上两种认证方式的组网环境下，推荐使用端口安全特性。无特殊组网要求的情况下，无线环境中通常使用端口安全特性。而在仅需要 802.1X、MAC 地址认证特性来完成接入控制的组网环境下，推荐单独使用相关特性。关于 802.1X、MAC 地址认证特性的详细介绍和具体配置请参见“安全配置指导”中的“802.1X”、“MAC 地址认证”。

1.1.2 端口安全的特性

说明

目前，本特性仅在安装了 HMIM-24GSW/24GSWP 和 HMIM-8GSW 交换卡的款型以及 MSR3600-28/MSR3600-51 的固定二层接口上支持。

1. Need To Know特性（NTK）

Need To Know 特性通过检测从端口发出的数据帧的目的 MAC 地址，保证数据帧只能被发送到已经通过认证或被端口学习到的 MAC 所属的设备或主机上，从而防止非法设备窃听网络数据。

2. 入侵检测（Intrusion Protection）特性

入侵检测特性指通过检测从端口收到的数据帧的源 MAC 地址，对接收非法报文的端口采取相应的安全策略，包括端口被暂时断开连接、永久断开连接或 MAC 地址被过滤（默认 3 分钟，不可配），以保证端口的安全性。

1.1.3 端口安全模式

端口安全模式可大致分为两大类：控制 MAC 学习类和认证类。

- 控制 MAC 学习类：无需认证，包括端口自动学习 MAC 地址和禁止 MAC 地址学习两种模式。
- 认证类：利用 MAC 地址认证和 802.1X 认证机制来实现，包括单独认证和组合认证等多种模式。

配置了安全模式的端口上收到用户报文后，首先查找MAC地址表，如果该报文的源MAC地址已经存在于MAC地址表中，则端口转发该报文，否则根据端口所采用的安全模式进行相应的处理，并在发现非法报文后触发端口执行相应的安全防护措施（Need To Know、入侵检测）。缺省情况下，端口出方向的报文转发不受端口安全限制，若触发了端口Need To Know，则才受相应限制。关于各模式的具体工作机制，以及是否触发Need To Know、入侵检测的具体情况请参见 表 1-1。

表1-1 端口安全模式描述表

安全模式		工作机制	NTK/入侵检测
缺省情况	noRestrictions	表示端口的安全功能关闭，端口处于无限制状态	无效
端口控制MAC地址学习	autoLearn	端口可通过手工配置或自动学习MAC地址，这些地址将被添加到安全MAC地址表中，称之为安全MAC地址 当端口下的安全MAC地址数超过端口安全允许学习的最大安全MAC地址数后，端口模式会自动转变为secure模式。之后，该端口停止添加新的安全MAC，只有源MAC地址为安全MAC地址、通过命令**mac-address dynamic**或**mac-address static**手工配置的MAC地址的报文，才能通过该端口 该模式下，端口不会将自动学习到的MAC地址添加为MAC地址表中的动态MAC地址	可触发
	secure	禁止端口学习MAC地址，只有源MAC地址为端口上的安全MAC地址、手工配置的MAC地址的报文，才能通过该端口	
端口采用802.1X认证	userLogin	对接入用户采用基于端口的802.1X认证 此模式下，端口下的第一个802.1X用户认证成功后，其它用户无须认证就可接入	无效
	userLoginSecure	对接入用户采用基于MAC地址的802.1X认证 此模式下，端口最多只允许一个802.1X认证用户接入	可触发
	userLoginWithOUI	该模式与userLoginSecure模式类似，但端口上除了允许一个802.1X认证用户接入之外，还额外允许一个特殊用户接入，该用户报文的源MAC的OUI与设备上配置的OUI值相符 • 在用户接入方式为有线的情况下，802.1X 报文进行 802.1X 认证，非 802.1X 报文直接进行 OUI 匹配，802.1X 认证成功和 OUI 匹配成功的报文都允许通过端口； • 在用户接入方式为无线的情况下，报文首先进行 OUI 匹配，OUI 匹配失败的报文再进行 802.1X 认证，OUI 匹配成功和 802.1X 认证成功的报文都允许通过端口	
	userLoginSecureExt	对接入用户采用基于MAC的802.1X认证，且允许端口下有多个802.1X用户	

安全模式		工作机制	NTK/入侵检测
端口采用MAC地址认证	macAddressWithRadius	对接入用户采用MAC地址认证 此模式下，端口允许多个用户接入	可触发
端口采用802.1X和MAC地址认证组合认证	macAddressOrUserLoginSecure	端口同时处于userLoginSecure模式和macAddressWithRadius模式，且允许一个802.1X认证用户及多个MAC地址认证用户接入 • 在用户接入方式为有线的情况下，非 802.1X 报文直接进行 MAC 地址认证，802.1X 报文直接进行 802.1X 认证； • 在用户接入方式为无线的情况下，802.1X 认证优先级大于 MAC 地址认证：报文首先进行 802.1X 认证，如果 802.1X 认证失败再进行 MAC 地址认证	可触发
	macAddressElseUserLoginSecure	端口同时处于macAddressWithRadius模式和userLoginSecure模式，但MAC地址认证优先级大于802.1X认证。允许端口下一个802.1X认证用户及多个MAC地址认证用户接入 非802.1X报文直接进行MAC地址认证。802.1X报文先进行MAC地址认证，如果MAC地址认证失败再进行802.1X认证	
	macAddressOrUserLoginSecureExt	与macAddressOrUserLoginSecure类似，但允许端口下有多个802.1X和MAC地址认证用户	
	macAddressElseUserLoginSecureExt	与macAddressElseUserLoginSecure类似，但允许端口下有多个802.1X和MAC地址认证用户	

说明

- 除了 userLogin 模式所有款型均支持外，其余模式仅在安装了 HMIM-24GSW/24GSWP 和 HMIM-8GSW 交换卡的款型以及 MSR3600-28/MSR3600-51 的固定二层接口上支持。
- 当多个用户通过认证时，端口下所允许的最大用户数与端口安全模式相关，取端口安全所允许的最大安全 MAC 地址数与相应模式下允许认证用户数的最小值。例如，userLoginSecureExt 模式下，端口下所允许的最大用户为配置的端口安全所允许的最大安全 MAC 地址数与 802.1X 认证所允许的最大用户数的最小值。
- 手工配置 MAC 地址的具体介绍请参见“二层技术-以太网交换命令参考”中的“MAC 地址表”。

窍门

由于安全模式种类较多，为便于记忆，部分端口安全模式的名称可按如下规则理解：

- “userLogin”表示基于端口的 802.1X 认证。userLogin 之后，若携带“Secure”，则表示基于 MAC 地址的 802.1X 认证；若携带“Ext”，则示可允许多个 802.1X 用户认证成功，否则表示仅允许一个 802.1X 用户认证成功。
- “macAddress”表示 MAC 地址认证；
- “Else”之前的认证方式先被采用，失败后根据请求认证的报文协议类型决定是否转为“Else”之后的认证方式。
- “Or”连接的两种认证方式无固定生效顺序，设备根据请求认证的报文协议类型决定认证方式，但无线接入的用户先采用 802.1X 认证方式；

1.2 端口安全配置任务简介

表1-2 端口安全配置任务简介

配置任务		说明	详细配置
使能端口安全		必选	1.3
配置端口安全允许的最大安全MAC地址数		可选	1.4
配置端口安全模式		必选	1.5
配置端口安全的特性	配置Need To Know特性	根据实际组网需求选择其中一种或多种特性	1.6
	配置入侵检测模式		
配置安全MAC地址		可选	1.7
配置当前端口不应用下发的授权信息		可选	1.8
配置允许MAC迁移功能		可选	1.9

1.3 使能端口安全

在使能端口安全之前，需要关闭全局的 802.1X 和 MAC 地址认证。

当端口安全处于使能状态时，不能开启端口上的 802.1X 以及 MAC 地址认证，且不能修改 802.1X 端口接入控制方式和端口授权状态，它们只能随端口安全模式的改变由系统更改。

表1-3 使能端口安全

操作	命令	说明
进入系统视图	**system-view**	-
使能端口安全	**port-security enable**	缺省情况下，端口安全处于关闭状态

可以通过 **undo port-security enable** 命令关闭端口安全。但需要注意的是，在端口上有用户在线的情况下，关闭端口会导致在线用户会下线。

执行使能或关闭端口安全的命令后，端口上的如下配置会被自动恢复为以下缺省情况：

- 802.1X 端口接入控制方式为 **macbased**；
- 802.1X 端口的授权状态为 **auto**。

有关 802.1X 认证配置的详细介绍可参见“安全配置指导”中的“802.1X”。有关 MAC 地址认证配置的详细介绍可参见“安全配置指导”中的“MAC 地址认证”。

1.4 配置端口安全允许的最大安全MAC地址数

端口安全允许某个端口下有多个用户接入，但是允许的用户数不能超过规定的最大值。

配置端口允许的最大安全 MAC 地址数有两个作用：

- 控制端口允许接入网络的最大用户数。对于采用 802.1X、MAC 地址认证或者两者组合形式的认证类安全模式，端口允许的最大用户数取本命令配置的值与相应模式下允许认证用户数的最小值；
- 控制 autoLearn 模式下端口能够添加的最大安全 MAC 地址数。

端口安全允许的最大安全 MAC 地址数与“二层技术-以太网交换配置指导/MAC 地址表”中配置的端口最多可以学习到的 MAC 地址数无关，且不受其影响。

表1-4 配置端口安全允许的最大安全 MAC 地址数

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置端口安全允许的最大安全MAC地址数	**port-security max-mac-count** *count-value*	缺省情况下，端口安全不限制本端口可保存的最大安全MAC地址数

1.5 配置端口安全模式

1. 配置限制和指导

- 在端口安全未使能的情况下，端口安全模式可以进行配置但不会生效。
- 端口上有用户在线的情况下，改变端口的安全模式会导致在线用户会下线。

2. 配置准备

(1) 在配置端口安全模式之前，端口上首先需要满足以下条件：

- 802.1X 认证关闭。
- MAC 地址认证关闭。
- 端口未加入聚合组或业务环回组。

如果端口上已经配置了端口安全模式，则不允许开启 802.1X 认证和 MAC 地址认证。

(2) 对于 autoLearn 模式，还需要提前设置端口安全允许的最大安全 MAC 地址数。但是如果端口已经工作在 autoLearn 模式下，则无法更改端口安全允许的最大安全 MAC 地址数。

3. 配置步骤

表1-5 配置端口安全安全模式

操作	命令	说明
进入系统视图	**system-view**	-
（可选）配置允许通过认证的用户OUI值	**port-security oui index** *index-value* **mac-address** *oui-value*	该命令仅在配置**userlogin-withoui**安全模式时必选 缺省情况下，不存在允许通过认证的用户OUI值 允许通过认证的用户OUI值可以配置多个，但在端口安全模式为userLoginWithOUI时，端口除了可以允许一个802.1X的接入用户通过认证之外，仅允许一个与某OUI值匹配的用户通过认证
进入接口视图	**interface** *interface-type interface-number*	-
配置端口的安全模式	**port-security port-mode** { **autolearn** | **mac-authentication** | **mac-else-userlogin-secure** | **mac-else-userlogin-secure-ext** | **secure** | **userlogin** | **userlogin-secure** | **userlogin-secure-ext** | **userlogin-secure-or-mac** | **userlogin-secure-or-mac-ext** | **userlogin-withoui** }	缺省情况下，端口处于noRestrictions模式 当端口安全已经使能且当前端口安全模式不是noRestrictions时，若要改变端口安全模式，必须首先执行**undo port-security port-mode**命令恢复端口安全模式为noRestrictions模式


说明

OUI（Organizationally Unique Identifier，全球统一标识符）是 MAC 地址的前 24 位（二进制），是 IEEE（Institute of Electrical and Electronics Engineers，电气和电子工程师学会）为不同设备供应商分配的一个全球唯一的标识符。

1.6 配置端口安全的特性

1.6.1 配置Need To Know特性

Need To Know 特性用来限制认证端口上出方向的报文转发，可支持以下三种限制方式：

- **ntkonly**：仅允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文通过。
- **ntk-withbroadcasts**：允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文或广播地址的报文通过。

- **ntk-withmulticasts**：允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文，广播地址或组播地址的报文通过。

配置了 Need To Know 的端口在以上任何一种方式下都不允许目的 MAC 地址未知的单播报文通过。并非所有的端口安全模式都支持Need To Know特性，配置时需要先了解各模式对此特性的支持情况，具体请参见 表 1-1。

表1-6 配置 Need To Know 特性

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置端口Need To Know特性	**port-security ntk-mode** { **ntk-withbroadcasts** | **ntk-withmulticasts** | **ntkonly** }	缺省情况下，端口没有配置Need To Know特性，即所有报文都可成功发送

1.6.2 配置入侵检测特性

当设备检测到一个非法的用户通过端口试图访问网络时，入侵检测特性用于配置设备可能对其采取的安全措施，包括以下三种方式：

- **blockmac**：表示将非法报文的源 MAC 地址加入阻塞 MAC 地址列表中，源 MAC 地址为阻塞 MAC 地址的报文将被丢弃。此 MAC 地址在被阻塞 3 分钟（系统默认，不可配）后恢复正常。
- **disableport**：表示将收到非法报文的端口永久关闭。
- **disableport-temporarily**：表示将收到非法报文的端口暂时关闭一段时间。关闭时长可通过 **port-security timer disableport** 命令配置。

表1-7 配置入侵检测特性

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置入侵检测特性	**port-security intrusion-mode** { **blockmac** | **disableport** | **disableport-temporarily** }	缺省情况下，不进行入侵检测处理
退回系统视图	**quit**	-
（可选）配置系统暂时关闭端口的时间	**port-security timer disableport** *time-value*	缺省情况下，系统暂时关闭端口的时间为20秒

说明

macAddressElseUserLoginSecure 或 macAddressElseUserLoginSecureExt 安全模式下工作的端口，对于同一个报文，只有 MAC 地址认证和 802.1X 认证均失败后，才会触发入侵检测特性。

1.7 配置安全MAC地址

1. 功能简介

安全 MAC 地址是一种特殊的 MAC 地址，保存配置后重启设备，不会丢失。在同一个 VLAN 内，一个安全 MAC 地址只能被添加到一个端口上。

安全 MAC 地址可以通过以下两种途径生成：

- 由 autoLearn 安全模式下的使能端口安全功能的端口自动学习。
- 通过命令行手动添加。

缺省情况下，所有的安全 MAC 地址均不老化，除非被管理员通过命令行手工删除，或因为配置的改变（端口的安全模式被改变，或端口安全功能被关闭）而被系统自动删除。但是，安全 MAC 地址不老化会带来一些问题：合法用户离开端口后，若有非法用户仿冒合法用户源 MAC 接入，会导致合法用户不能继续接入；虽然该合法用户已离开，但仍然占用端口 MAC 地址资源，而导致其它合法用户不能接入。因此，让某一类安全 MAC 地址能够定期老化，可提高端口接入的安全性和端口资源的利用率。

表1-8 安全 MAC 地址相关属性列表

生成方式	是否可老化	配置保存机制
手工添加（未指定**sticky**关键字）	不老化，称之为静态类型的安全MAC地址	安全MAC地址在保存配置文件并重启设备后，仍然存在
手工添加（指定**sticky**关键字） 端口自动学习	可老化（老化时间可配），称之为Sticky MAC地址 • 若老化时间为 0，则表示不老化（缺省） • 若老化时间不为 0，则表示安全 MAC 地址会老化	Sticky MAC地址在保存配置文件并重启设备后，仍然存在，且其老化定时器会重新开始计时

说明

当端口下的安全MAC地址数目超过端口允许学习的最大安全MAC地址数后，该端口不会再添加新的安全MAC地址，仅接收并允许数据帧中的源MAC地址为以下两类MAC地址的报文访问网络设备：

- 安全 MAC 地址
- 通过命令 **mac-address dynamic** 或 **mac-address static** 配置的 MAC 地址

2. 配置准备

在配置安全 MAC 地址之前，需要完成以下配置任务：

- 使能端口安全功能
- 设置端口安全允许的最大 MAC 地址数
- 配置端口安全模式为 autoLearn
- 当前的接口必须允许指定的 VLAN 通过或已加入该 VLAN，且该 VLAN 已存在

3. 配置步骤

表1-9 配置安全 MAC 地址

操作	命令	说明
进入系统视图	**system-view**	-

操作		命令	说明
（可选）配置安全MAC地址的老化时间		**port-security timer autolearn aging** *time-value*	缺省情况下，安全MAC地址不会老化
配置安全MAC地址	在系统视图下	**port-security mac-address security** [**sticky**] *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*	二者选其一 缺省情况下，未配置安全MAC地址 与相同VLAN绑定的同一个MAC地址不允许同时指定为静态类型的安全MAC地址和Sticky MAC地址
	在接口视图下	**interface** *interface-type interface-number*	
		port-security mac-address security [**sticky**] *mac-address* **vlan** *vlan-id*	

1.8 配置当前端口不应用下发的授权信息

802.1X 用户或 MAC 地址认证用户通过本地认证或 RADIUS 认证时，本地设备或远程 RADIUS 服务器会把授权信息下发给用户。通过此配置可实现端口是否忽略这类下发的授权信息。

表1-10 配置当前端口不应用下发的授权信息

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置当前端口不应用RADIUS服务器或设备本地下发的授权信息	**port-security authorization ignore**	缺省情况下，端口应用RADIUS服务器或设备本地下发的授权信息

1.9 配置允许MAC迁移功能

允许 MAC 迁移功能是指，允许在线的 802.1X 用户或 MAC 地址认证用户移动到设备的其它端口上接入后可以重新认证上线。缺省情况下，如果用户从某一端口上线成功，则该用户在未从当前端口下线的情况下无法在设备的其它端口上（无论该端口是否与当前端口属于同一 VLAN）发起认证，也无法上线。若开启了允许 MAC 地址迁移功能，则允许在线用户离开当前端口在设备的其它端口上（无论该端口是否与当前端口属于同一 VLAN）发起认证。如果该用户在后接入的端口上认证成功，则当前端口会将该用户立即进行下线处理，保证该用户仅在一个端口上处于上线状态。

通常，不建议开启该功能，只有在用户漫游迁移需求的情况下建议开启此功能。

表1-11 配置允许 MAC 迁移功能

操作	命令	说明
进入系统视图	**system-view**	-
开启允许MAC迁移功能	**port-security mac-move permit**	缺省情况下，允许MAC迁移功能处于关闭状态

1.10 端口安全显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后端口安全的运行情况，通过查看显示信息验证配置的效果。

表1-12 端口安全显示和维护

操作	命令
显示端口安全的配置信息、运行情况和统计信息	**display port-security** [**interface** *interface-type interface-number*]
显示安全MAC地址信息	**display port-security mac-address security** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]
显示阻塞MAC地址信息	**display port-security mac-address block** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]

1.11 端口安全典型配置举例

1.11.1 端口安全autoLearn模式配置举例

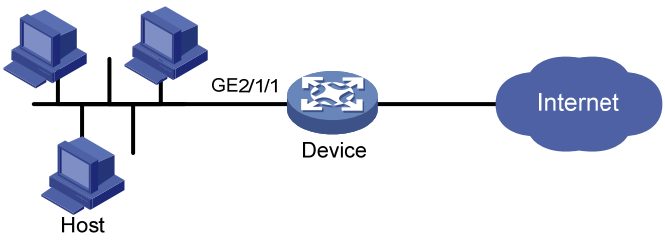
1. 组网需求

在 Device 的端口 GigabitEthernet2/1/1 上对接入用户做如下的限制：

- 允许 64 个用户自由接入，不进行认证，将学习到的用户 MAC 地址添加为 Sticky MAC 地址，老化时间为 30 分钟；
- 当安全 MAC 地址数量达到 64 后，停止学习；当再有新的 MAC 地址接入时，触发入侵检测，并将此端口关闭 30 秒。

2. 组网图

图1-1 端口安全 autoLearn 模式组网图



3. 配置步骤

使能端口安全。

```
<Device> system-view
[Device] port-security enable
```

设置安全 MAC 地址的老化时间为 30 分钟。

```
[Device] port-security timer autolearn aging 30
```

设置端口安全允许的最大安全 MAC 地址数为 64。

```
[Device] interface gigabitethernet 2/1/1
```

```
[Device-GigabitEthernet2/1/1] port-security max-mac-count 64
```
设置端口安全模式为 autoLearn。
```
[Device-GigabitEthernet2/1/1] port-security port-mode autolearn
```
设置触发入侵检测特性后的保护动作为暂时关闭端口，关闭时间为 30 秒。
```
[Device-GigabitEthernet2/1/1] port-security intrusion-mode disableport-temporarily
[Device-GigabitEthernet2/1/1] quit
[Device] port-security timer disableport 30
```
4. 验证配置

上述配置完成后，可以使用如下显示命令查看端口安全的配置情况。
```
[Device] display port-security interface gigabitethernet 2/1/1
Port security parameters:
   Port security          : Enabled
   AutoLearn aging time   : 30 min
   Disableport timeout    : 30 s
   MAC move               : Denied
   OUI value list         :

GigabitEthernet2/1/1 is link-up
   Port mode                    : autoLearn
   NeedToKnow mode              : Disabled
   Intrusion protection mode    : DisablePortTemporarily
   Max secure MAC addresses     : 64
   Current secure MAC addresses : 5
   Authorization                : Permitted
```
可以看到端口安全所允许的最大安全 MAC 地址数为 64，端口模式为 autoLearn，入侵检测保护动作为 DisablePortTemporarily，入侵发生后端口被禁用时间为 30 秒。

配置生效后，端口允许地址学习，学习到的 MAC 地址数可在上述显示信息的“Current number of secure MAC addresses”字段查看到，具体的 MAC 地址信息可以在接口视图下用 **display this** 命令查看。
```
[Device] interface gigabitethernet 2/1/1
[Device-GigabitEthernet2/1/1] display this
#
interface GigabitEthernet2/1/1
 port-security max-mac-count 64
 port-security port-mode autolearn
 port-security mac-address security sticky 0002-0000-0015 vlan 1
 port-security mac-address security sticky 0002-0000-0014 vlan 1
 port-security mac-address security sticky 0002-0000-0013 vlan 1
 port-security mac-address security sticky 0002-0000-0012 vlan 1
 port-security mac-address security sticky 0002-0000-0011 vlan 1
#
```
当学习到的 MAC 地址数达到 64 后，用命令 **display port-security interface** 可以看到端口模式变为 secure，再有新的 MAC 地址到达将触发入侵保护，可以通过命令 **display interface** 看到此端口关闭。30 秒后，端口状态恢复。此时，如果手动删除几条安全 MAC 地址后，端口安全的状态重新恢复为 autoLearn，可以继续学习 MAC 地址。

1.11.2 端口安全userLoginWithOUI模式配置举例

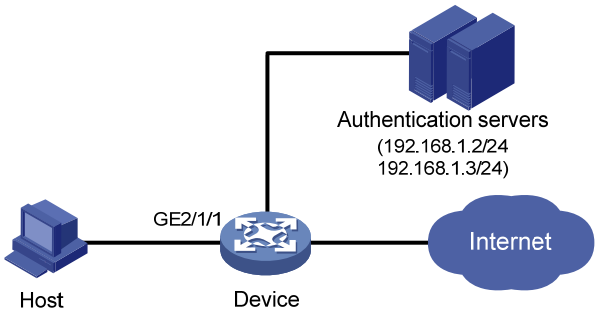
1. 组网需求

客户端通过端口 GigabitEthernet2/1/1 连接到 Device 上，Device 通过 RADIUS 服务器对客户端进行身份认证，如果认证成功，客户端被授权允许访问 Internet 资源。

- IP 地址为 192.168.1.2 的 RADIUS 服务器作为主认证服务器和从计费服务器，IP 地址为 192.168.1.3 的 RADIUS 服务器作为从认证服务器和主计费服务器。认证共享密钥为 name，计费共享密钥为 money。
- 所有接入用户都使用 ISP 域 sun 的认证/授权/计费方法，该域最多可同时接入 30 个用户；
- 系统向 RADIUS 服务器重发报文的时间间隔为 5 秒，重发次数为 5 次，发送实时计费报文的时间间隔为 15 分钟，发送的用户名不带域名。
- 端口 GigabitEthernet2/1/1 同时允许一个 802.1X 用户以及一个与指定 OUI 值匹配的设备接入。

2. 组网图

图1-2 端口安全 userLoginWithOUI 模式组网图



3. 配置步骤

说明

- 下述配置步骤包含了部分 AAA/RADIUS 协议配置命令，具体介绍请参见“安全配置指导”中的“AAA”。
- 保证客户端和 RADIUS 服务器之间路由可达。

(1) 配置 AAA

配置 RADIUS 方案。

```
<Device> system-view
[Device] radius scheme radsun
[Device-radius-radsun] primary authentication 192.168.1.2
[Device-radius-radsun] primary accounting 192.168.1.3
[Device-radius-radsun] secondary authentication 192.168.1.3
[Device-radius-radsun] secondary accounting 192.168.1.2
[Device-radius-radsun] key authentication simple name
[Device-radius-radsun] key accounting simple money
[Device-radius-radsun] timer response-timeout 5
```

```
[Device-radius-radsun] retry 5
[Device-radius-radsun] timer realtime-accounting 15
[Device-radius-radsun] user-name-format without-domain
[Device-radius-radsun] quit
```

配置 ISP 域。

```
[Device] domain sun
[Device-isp-sun] authentication lan-access radius-scheme radsun
[Device-isp-sun] authorization lan-access radius-scheme radsun
[Device-isp-sun] accounting lan-access radius-scheme radsun
[Device-isp-sun] access-limit enable 30
[Device-isp-sun] quit
```

(2) 配置 802.1X

配置 802.1X 的认证方式为 CHAP。（该配置可选，缺省情况下 802.1X 的认证方式为 CHAP）

```
[Device] dot1x authentication-method chap
```

(3) 配置端口安全

使能端口安全。

```
[Device] port-security enable
```

添加 5 个 OUI 值。（最多可添加 16 个，此处仅为示例。最终，端口仅允许一个与某 OUI 值匹配的用户通过认证）

```
[Device] port-security oui index 1 mac-address 1234-0100-1111
[Device] port-security oui index 2 mac-address 1234-0200-1111
[Device] port-security oui index 3 mac-address 1234-0300-1111
[Device] port-security oui index 4 mac-address 1234-0400-1111
[Device] port-security oui index 5 mac-address 1234-0500-1111
```

设置端口安全模式为 userLoginWithOUI。

```
[Device] interface gigabitethernet 2/1/1
[Device-GigabitEthernet2/1/1] port-security port-mode userlogin-withoui
[Device-GigabitEthernet2/1/1] quit
```

4. 验证配置

查看名称为 radsun 的 RADIUS 方案的配置信息。

```
[Device] display radius scheme radsun
RADIUS Scheme Name  : radsun
  Index : 0
  Primary Auth Server:
    IP  : 192.168.1.2                          Port: 1812
    State: Active
    VPN : Not configured
    Test profile: Not configured
  Primary Acct Server:
    IP  : 192.168.1.3                          Port: 1813
    State: Active
    VPN : Not configured
  Second Auth Server:
    IP  : 192.168.1.3                          Port: 1812
    State: Active
    VPN : Not configured
```

```
    Test profile: Not configured
  Second Acct Server:
    IP  : 192.168.1.2                              Port: 1813
    State: Active
    VPN : Not configured

  Accounting-On function                     : Disabled
    retransmission times                     : 50
    retransmission interval(seconds)         : 3
  Timeout Interval(seconds)                  : 5
  Retransmission Times                       : 5
  Retransmission Times for Accounting Update : 5
  Server Quiet Period(minutes)               : 5
  Realtime Accounting Interval(minutes)      : 15
  NAS IP Address                             : Not configured
  VPN                                        : Not configured
  User Name Format                           : without-domain
  Data flow unit                             : Million Byte
  Packet unit                                : one
  Attribute 25                               : standard
```

查看名称为 sun 的 ISP 域的配置信息。

```
[Device] display domain sun

Domain: sun
  State: Active
  Access limit: 30
  Access Count: 0
  LAN access authentication scheme:  RADIUS: radsun
  LAN access authorization  scheme:  RADIUS: radsun
  LAN access accounting     scheme:  RADIUS: radsun
  Default authentication scheme:  local
  Default authorization  scheme:  local
  Default accounting     scheme:  local
  Authorization attributes:
    Idle-cut: Disabled
  Session time: Exclude idle time
```

查看端口安全的配置信息。

```
[Device] display port-security interface gigabitethernet 2/1/1
Port security parameters:
   Port security          : Enabled
   AutoLearn aging time   : 30 min
   Disableport timeout    : 30 s
   MAC move               : Denied
   OUI value list         :
       Index :  1       Value : 123401
       Index :  2       Value : 123402
       Index :  3       Value : 123403
       Index :  4       Value : 123404
```

```
      Index :  5       Value : 123405

 GigabitEthernet2/1/1 is link-up
   Port mode                    : userLoginWithOUI
   NeedToKnow mode              : Disabled
   Intrusion protection mode    : NoAction
   Max secure MAC addresses     : 64
   Current secure MAC addresses : 1
   Authorization                : Permitted
```

配置完成后，如果有 802.1X 用户上线，则可以通过上述显示信息看到当前端口保存的 MAC 地址数为 1。还可以通过 **display dot1x** 命令查看该 802.1X 用户的在线情况。

此外，端口还允许一个 MAC 地址与 OUI 值匹配的用户通过，可以通过下述命令查看。

```
[Device] display mac-address interface gigabitethernet 2/1/1
MAC Address     VLAN ID   State          Port/NickName            Aging
1234-0300-0011  1         Learned        GE2/1/1                  Y
```

1.11.3 端口安全macAddressElseUserLoginSecure模式配置举例

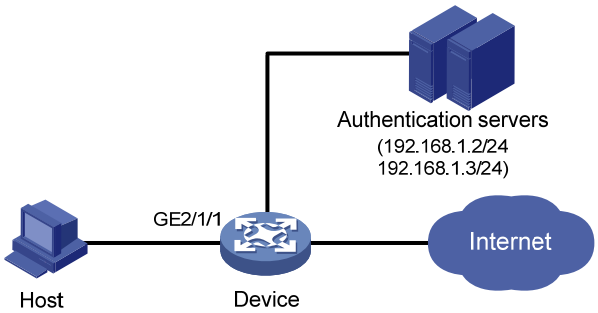
1. 组网需求

客户端通过端口 GigabitEthernet2/1/1 连接到 Device 上，Device 通过 RADIUS 服务器对客户端进行身份认证。如果认证成功，客户端被授权允许访问 Internet 资源。

- 可以有多个 MAC 认证用户接入；
- 如果是 802.1X 用户请求认证，先进行 MAC 地址认证，MAC 地址认证失败，再进行 802.1X 认证。最多只允许一个 802.1X 用户接入；
- MAC 地址认证设置用户名格式为用户 MAC 地址的形式。
- 上线的 MAC 地址认证用户和 802.1X 认证用户总和不能超过 64 个；
- 为防止报文发往未知目的 MAC 地址，启动 **ntkonly** 方式的 Need To Know 特性。

2. 组网图

图1-3 端口安全 macAddressElseUserLoginSecure 模式组网图



3. 配置步骤

说明

- RADIUS认证/计费及ISP域的配置同“1.11.2 端口安全userLoginWithOUI模式配置举例”，这里不再赘述。
- 保证接入用户和 RADIUS 服务器之间路由可达。

使能端口安全。

```
<Device> system-view
[Device] port-security enable
```

配置 MAC 认证的用户名和密码，使用带连字符“-”的 MAC 地址格式，其中字母大写。

```
[Device] mac-authentication user-name-format mac-address with-hyphen uppercase
```

配置 MAC 地址认证用户所使用的 ISP 域。

```
[Device] mac-authentication domain sun
```

配置 802.1X 的认证方式为 CHAP。（该配置可选，缺省情况下 802.1X 的认证方式为 CHAP）

```
[Device] dot1x authentication-method chap
```

设置端口安全允许的最大 MAC 地址数为 64。

```
[Device] interface gigabitethernet 2/1/1
[Device-GigabitEthernet2/1/1] port-security max-mac-count 64
```

设置端口安全模式为 macAddressElseUserLoginSecure。

```
[Device-GigabitEthernet2/1/1] port-security port-mode mac-else-userlogin-secure
```

设置端口 Need To Know 模式为 ntkonly。

```
[Device-GigabitEthernet2/1/1] port-security ntk-mode ntkonly
[Device-GigabitEthernet2/1/1] quit
```

4. 验证配置

查看端口安全的配置信息。

```
[Device] display port-security interface gigabitethernet 2/1/1
Port security parameters:
   Port security          : Enabled
   AutoLearn aging time   : 0 min
   Disableport timeout    : 30 s
   MAC move               : Denied
   OUI value list

 GigabitEthernet2/1/1 is link-up
    Port mode                   : macAddressElseUserLoginSecure
    NeedToKnow mode             : NeedToKnowOnly
    Intrusion protection mode   : NoAction
    Max secure MAC addresses    : 64
    Current secure MAC addresses : 0
    Authorization               : Permitted
```

配置完成后，如果有用户认证上线，则可以通过下述显示信息看到当前端口上的用户认证信息。

查看 MAC 地址认证信息。

```
[Device] display mac-authentication interface gigabitethernet 2/1/1
Global MAC authentication parameters:
   MAC authenticaiton     : Enabled
   User name format       : MAC address in uppercase(XX-XX-XX-XX-XX-XX)
           Username       : mac
           Password       : Not configured
   Offline detect period  : 300 s
   Quiet period           : 180 s
   Server timeout         : 100 s
   Authentication domain  : sun
 Max MAC-auth users       : 1024 per slot
 Online MAC-auth users    : 3

 Silent MAC users:
          MAC address       VLAN ID  From port               Port index

GigabitEthernet2/1/1 is link-up
   MAC authentication         : Enabled
   Authentication domain      : Not configured
   Auth-delay timer           : Disabled
   Re-auth server-unreachable : Logoff
   Guest VLAN                 : Not configured
   Critical VLAN              : Not configured
   Max online users           : 256
   Authentication attempts    : successful 3, failed 7
   Current online users       : 0
          MAC address       Auth state
          1234-0300-0011    Authenticated
          1234-0300-0012    Authenticated
          1234-0300-0013    Authenticated
```

查看 802.1X 认证信息。

```
[Device] display dot1x interface gigabitethernet 2/1/1
Global 802.1X parameters:
   802.1X authentication  : Enabled
   CHAP authentication    : Enabled
   Max-tx period          : 30 s
   Handshake period       : 15 s
   Quiet timer            : Disabled
       Quiet period       : 60 s
   Supp timeout           : 30 s
   Server timeout         : 100 s
   Reauth period          : 3600 s
   Max auth requests      : 2
   SmartOn supp timeout   : 30 s
   SmartOn retry counts   : 3
   EAD assistant function : Disabled
       EAD timeout        : 30 min
   Domain delimiter       : @
```

```
Max 802.1X users         : 1024 per slot
Online 802.1X users      : 1
GigabitEthernet2/1/1  is link-down
  802.1X authenticaiton      : Enabled
  Handshake                  : Enabled
  Handshake security         : Disabled
  Unicast trigger            : Disabled
  Periodic reauth            : Disabled
  Port role                  : Authenticator
  Authorization mode         : Auto
  Port access control        : MAC-based
  Multicast trigger          : Enabled
  Mandatory auth domain      : Not configured
  Guest VLAN                 : Not configured
  Auth-Fail VLAN             : Not configured
  Critical VLAN              : Not configured
  Re-auth server-unreachable : Logoff
  Max online users           : 256
  SmartOn                    : Disabled

  EAPOL packets: Tx 16331, Rx 102
  Sent EAP Request/Identity packets : 16316
       EAP Request/Challenge packets: 6
       EAP Success packets: 4
       EAP Failure packets: 5
  Received EAPOL Start packets : 6
           EAPOL LogOff packets: 2
           EAP Response/Identity packets : 80
           EAP Response/Challenge packets: 6
           Error packets: 0
  Online 802.1X users: 1
         MAC address         Auth state
         0002-0000-0011      Authenticated
```

此外，因为设置了 Need To Know 特性，目的 MAC 地址未知、广播和多播报文都被丢弃。

1.12 常见配置错误举例

1.12.1 端口安全模式无法设置

1. 故障现象

无法设置端口的端口安全模式。

2. 故障分析

在当前端口的端口安全模式已配置的情况下，无法直接对端口安全模式进行设置。

3. 处理过程

首先设置端口安全模式为 noRestrictions 状态，再设置新的端口安全模式。

```
[Device-GigabitEthernet2/1/1] undo port-security port-mode
```

```
[Device-GigabitEthernet2/1/1] port-security port-mode autolearn
```

1.12.2 无法配置安全MAC地址

1. 故障现象

无法配置安全 MAC 地址。

2. 故障分析

端口安全模式为非 autoLearn 时，不能对安全 MAC 地址进行设置。

3. 处理过程

设置端口安全模式为 autoLearn 状态。

```
[Device-GigabitEthernet2/1/1] undo port-security port-mode
[Device-GigabitEthernet2/1/1] port-security max-mac-count 64
[Device-GigabitEthernet2/1/1] port-security port-mode autolearn
[Device-GigabitEthernet2/1/1] port-security mac-address security 1-1-2 vlan 1
```

目 录

1 Password Control

说明

设备运行于 FIPS 模式时，本特性部分配置相对于非 FIPS 模式有所变化，具体差异请见本文相关描述。有关 FIPS 模式的详细介绍请参见“安全配置指导”中的“FIPS”。

1.1 Password Control简介

Password Control（密码管理）是设备提供的密码安全管理功能，它根据管理员定义的安全策略，对设备管理类的本地用户登录密码、super 密码的设置、老化、更新等方面进行管理，并对用户的登录状态进行控制。

说明

- 本地用户包括两种类型，设备管理类（**manage**）和网络接入类（**network**）。Password Control 功能仅对设备管理类本地用户的登录密码进行控制，对网络接入类本地用户的密码不起作用。关于本地用户类型的详细介绍，请参见“安全配置指导”中的“AAA”。
- 为了防止未授权用户的非法侵入，在进行用户角色切换时，要进行用户身份验证，即需要输入用户角色切换密码，这个密码就被称为 super 密码。关于 super 密码的详细介绍，请参见“基础配置指导”中的“RBAC”。

1.1.1 密码设置控制

1. 密码最小长度限制

管理员可以限制用户密码的最小长度。当设置用户密码时，如果输入的密码长度小于设置的最小长度，系统将不允许设置该密码。

2. 密码的组合检测功能

管理员可以设置用户密码的组成元素的组合类型，以及至少要包含每种元素的个数。密码的组成元素包括以下 4 种类型：

- [A～Z]
- [a～z]
- [0～9]
- 32 个特殊字符（空格~`!@#$%^&*()_+-={}|[]\:";'<>,./）

密码元素的组合类型有 4 种，具体涵义如下：

- 组合类型为 1 表示密码中至少包含 1 种元素；
- 组合类型为 2 表示密码中至少包含 2 种元素；

- 组合类型为 3 表示密码中至少包含 3 种元素；
- 组合类型为 4 表示密码中包含 4 种元素。

当用户设置密码时，系统会检查设定的密码是否符合配置要求，只有符合要求的密码才能设置成功。

3. 密码的复杂度检测功能

密码的复杂度越低，其被破解的可能性就越大，比如包含用户名、使用重复字符等。出于安全性考虑，管理员可以设置用户密码的复杂度检测功能，确保用户的密码具有较高的复杂度。具体实现是：配置用户密码时，系统检测输入的密码是否符合一定的复杂度要求，只有符合要求的密码才能设置成功。目前，复杂度检测功能对密码的复杂度要求包括以下两项：

- 密码中不能包含用户名或者字符顺序颠倒的用户名。例如，用户名为“abc”，那么“abc982”或者“2cba”之类的密码就不符合复杂度要求。
- 密码中不能包含连续三个或以上的相同字符。例如，密码“a111”就不符合复杂度要求。

1.1.2 密码更新与老化

1. 密码更新管理

管理员可以设置用户登录设备后修改自身密码的最小间隔时间。当用户登录设备修改自身密码时，如果距离上次修改密码的时间间隔小于配置值，则系统不允许修改密码。例如，管理员配置用户密码更新间隔时间为 48 小时，那么用户在上次修改密码后的 48 小时之内都无法成功进行密码修改操作。

有两种情况下的密码更新并不受该功能的约束：用户首次登录设备时系统要求用户修改密码；密码老化后系统要求用户修改密码。

2. 密码老化管理

密码老化时间用来限制用户密码的使用时间。当密码的使用时间超过老化时间后，需要用户更换密码。

当用户登录时，如果用户输入已经过期的密码，系统将提示该密码已经过期，需要重新设置密码。如果输入的新密码不符合要求，或连续两次输入的新密码不一致，系统将要求用户重新输入。对于 FTP 用户，密码老化后，只能由管理员修改 FTP 用户的密码；对于 Telnet、SSH、Terminal（通过 Console 口或 AUX 口登录设备）用户可自行修改密码。

3. 密码过期提醒

在用户登录时，系统判断其密码距离过期的时间是否在设置的提醒时间范围内。如果在提醒时间范围内，系统会提示该密码还有多久过期，并询问用户是否修改密码。如果用户选择修改，则记录新的密码及其设定时间。如果用户选择不修改或者修改失败，则在密码未过期的情况下仍可以正常登录。对于 FTP 用户，只能由管理员修改 FTP 用户的密码；对于 Telnet、SSH、Terminal（通过 Console 口或 AUX 口登录设备）用户可自行修改密码。

4. 密码老化后允许登录管理

管理员可以设置用户密码过期后在指定的时间内还能登录设备指定的次数。这样，密码老化的用户不需要立即更新密码，依然可以登录设备。例如，管理员设置密码老化后允许用户登录的时间为 15 天、次数为 3 次，那么用户在密码老化后的 15 天内，还能继续成功登录 3 次。

5. 密码历史记录

系统保存用户密码历史记录。当用户修改密码时，系统会要求用户设置新的密码，如果新设置的密码以前使用过，且在当前用户密码历史记录中，系统将给出错误信息，提示用户密码更改失败。另外，用户更改密码时，系统会将新设置的密码逐一与所有记录的历史密码以及当前密码比较，要求新密码至少要与旧密码有 4 字符不同，且这 4 个字符必须互不相同，否则密码更改失败。

可以配置每个用户密码历史记录的最大条数，当密码历史记录的条数超过配置的最大历史记录条数时，新的密码历史记录将覆盖该用户最老的一条密码历史记录。

由于为设备管理类本地用户配置的密码在哈希运算后以密文的方式保存，配置一旦生效后就无法还原为明文密码，因此，设备管理类本地用户的当前登录密码，不会被记录到该用户的密码历史记录中。

1.1.3 用户登录控制

1. 用户首次登录控制

当全局密码管理功能使能后，用户首次登录设备时，系统会输出相应的提示信息要求用户修改密码，否则不允许登录设备。这种情况下的修改密码不受密码更新时间间隔的限制。

2. 密码尝试次数限制

密码尝试次数限制可以用来防止恶意用户通过不断尝试来破解密码。

每次用户认证失败后，系统会将该用户加入密码管理的黑名单。可加入密码管理功能黑名单的用户包括：FTP 用户和通过 VTY 方式访问设备的用户。不会加入密码管理功能黑名单的用户包括：用户名不存在的用户、通过 Console 口或 AUX 口连接到设备的用户。

当用户连续尝试认证的失败累加次数达到设置的尝试次数时，系统对用户的后续登录行为有以下三种处理措施：

- 永久禁止该用户登录。只有管理员把该用户从密码管理的黑名单中删除后，该用户才能重新登录。
- 不对该用户做禁止，允许其继续登录。在该用户登录成功后，该用户会从密码管理的黑名单中删除。
- 禁止该用户一段时间后，再允许其重新登录。当配置的禁止时间超时或者管理员将其从密码管理的黑名单中删除，该用户才可以重新登录。

3. 用户帐号闲置时间管理

管理员可以限制用户帐号的闲置时间，禁止在闲置时间之内始终处于不活动状态的用户登录。若用户自从最后一次成功登录之后，在配置的闲置时间内再未成功登录过，那么该闲置时间到达之后此用户账号立即失效，系统不再允许使用该账号的用户登录。例如，管理员配置用户帐号的闲置时间为 60 天，如果用户名为 test 的用户自最后一次成功登录之后的 60 天内，都未成功登录过设备，那么该用户帐号 test 就会失效。

1.1.4 密码不回显

出于安全考虑，用户输入密码时，系统将不回显用户的密码。

1.1.5 日志功能

当用户成功修改密码或用户登录失败加入密码管理黑名单时，系统将会记录相应的日志。

1.2 Password Control配置任务简介

本特性的各功能可支持在多个视图下配置，各视图可支持的功能不同。而且，相同功能的命令在不同视图下或针对不同密码时有效范围有所不同，具体情况如下：

- 系统视图下的全局配置对所有本地用户密码都有效；
- 用户组视图下的配置只对当前用户组内的所有本地用户密码有效；
- 本地用户视图下的配置只对当前的本地用户密码有效；
- 为 super 密码的各管理参数所作的配置只对 super 密码有效。

对于本地用户密码的各管理参数，其生效的优先级顺序由高到低依次为本地用户视图、用户组视图、系统视图。

表1-1 Password Control 配置任务简介

配置任务	说明	详细配置
使能密码管理	必选	1.3.1
配置全局密码管理	可选	1.3.2
配置用户组密码管理	可选	1.3.3
配置本地用户密码管理	可选	1.3.4
配置super密码管理	可选	1.3.5

1.3 配置Password Control

注意

设备存储空间不足会造成以下两个影响：

- 不能使能全局密码管理功能；
- 全局密码管理功能处于使能的状态下，用户登录设备失败。

1.3.1 使能密码管理

使能全局密码管理功能，是密码管理所有配置生效的前提。若要使得具体的密码管理功能（密码老化、密码最小长度、密码历史记录、密码组合检测）生效，还需使能指定的密码管理功能。

需要注意的是，使能全局密码管理功能后：

- 设备管理类本地用户密码以及 super 密码的配置将不被显示，即无法通过相应的 **display** 命令查看到设备管理类本地用户密码以及 super 密码的配置。网络接入类本地用户密码不受密码管理功能控制，其配置显示也不受影响。

- 首次设置的设备管理类本地用户密码必须至少由四个不同的字符组成。

表1-2 使能密码管理

操作	命令	说明
进入系统视图	**system-view**	-
使能全局密码管理功能	**password-control enable**	非FIPS模式下： 缺省情况下，全局密码管理功能处于未使能状态 FIPS模式下： 缺省情况下，全局密码管理功能处开启状态，且不能关闭
（可选）使能指定的密码管理功能	**password-control { aging | composition | history | length } enable**	缺省情况下，各密码管理功能均处于使能状态

1.3.2 配置全局密码管理

系统视图下的全局密码管理参数对所有设备管理类的本地用户生效。对于密码老化时间、密码最小长度以及密码组合策略这三个功能，可分别在系统视图、用户组视图、本地用户视图下配置相关参数，其生效优先级从高到低依次为：本地用户视图->用户组视图->系统视图。

除用户登录尝试失败后的行为配置属于即时生效的配置，会在配置生效后立即影响密码管理黑名单中当前用户的锁定状态以及这些用户后续的登录之外，其它全局密码管理配置生效后仅对后续登录的用户以及后续设置的用户密码有效，不影响当前用户。

表1-3 配置全局密码管理

操作	命令	说明
进入系统视图	**system-view**	-
配置密码的老化时间	**password-control aging** *aging-time*	缺省情况下，密码的老化时间为90天
配置密码更新的最小时间间隔	**password-control update interval** *interval*	缺省情况下，密码更新的最小时间间隔为24小时
配置密码的最小长度	**password-control length** *length*	非FIPS模式下： 缺省情况下，密码的最小长度为10个字符 FIPS模式下： 缺省情况下，密码的最小长度为15个字符

操作	命令	说明
配置用户密码的组合策略	**password-control composition type-number** *type-number* [**type-length** *type-length*]	非FIPS模式下： 缺省情况下，密码元素的组合类型至少为1种，至少要包含每种元素的个数为1个 FIPS模式下： 缺省情况下，密码元素的组合类型至少为4种，至少要包含每种元素的个数为1个
配置用户密码的复杂度检查策略	**password-control complexity** { **same-character** | **user-name** } **check**	缺省情况下，不对用户密码进行复杂度检查
配置每个用户密码历史记录的最大条数	**password-control history** *max-record-num*	缺省情况下，每个用户密码历史记录的最大条数为4条
配置用户登录尝试次数以及登录尝试失败后的行为	**password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	缺省情况下，用户登录尝试次数为3次；如果用户登录失败，则1分钟后再允许该用户重新登录
配置密码过期前的提醒时间	**password-control alert-before-expire** *alert-time*	缺省情况下，密码过期前的提醒时间为7天
配置密码过期后允许用户登录的时间和次数	**password-control expired-user-login delay** *delay* **times** *times*	缺省情况下，密码过期后的30天内允许用户登录3次
配置用户帐号的闲置时间	**password-control login idle-time** *idle-time*	缺省情况下，用户帐号的闲置时间为90天

1.3.3 配置用户组密码管理

表1-4 配置用户组密码管理

操作	命令	说明
进入系统视图	**system-view**	-
创建用户组，并进入用户组视图	**user-group** *group-name*	缺省情况下，不存在任何用户组 用户组的相关配置请参见“安全配置指导”中的“AAA”
配置用户组的密码老化时间	**password-control aging** *aging-time*	缺省情况下，采用全局密码老化时间
配置用户组的密码最小长度	**password-control length** *length*	缺省情况下，采用全局密码最小长度
配置用户组的密码组合策略	**password-control composition type-number** *type-number* [**type-length** *type-length*]	缺省情况下，采用全局密码组合策略
配置用户密码的复杂度检查策略	**password-control complexity** { **same-character** | **user-name** } **check**	缺省情况下，采用全局密码复杂度检查策略
配置用户登录尝试次数以及登录尝试失败后的行为	**password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	缺省情况下，采用全局的用户登录尝试限制策略

1.3.4 配置本地用户密码管理

表1-5 配置本地用户密码管理

操作	命令	说明
进入系统视图	**system-view**	-
创建设备管理类本地用户，并进入本地用户视图	**local-user** *user-name* **class manage**	缺省情况下，不存在任何本地用户 本地用户密码管理功能仅对设备管理类的本地用户生效，对于网络接入类本地用户不起作用 本地用户的相关配置请参见“安全配置指导”中的“AAA”
配置本地用户的密码老化时间	**password-control aging** *aging-time*	缺省情况下，采用本地用户所属用户组的密码老化时间
配置本地用户的密码最小长度	**password-control length** *length*	缺省情况下，采用本地用户所属用户组的密码最小长度
配置本地用户的密码组合策略	**password-control composition type-number** *type-number* [**type-length** *type-length*]	缺省情况下，采用本地用户所属用户组的密码组合策略
配置用户密码的复杂度检查策略	**password-control complexity** { **same-character** | **user-name** } **check**	缺省情况下，采用本地用户所属用户组的密码复杂度检查策略
配置用户登录尝试次数以及登录尝试失败后的行为	**password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	缺省情况下，采用本地用户所属用户组的用户登录尝试限制策略

1.3.5 配置super密码管理

表1-6 配置 super 密码管理

操作	命令	说明
进入系统视图	**system-view**	-
配置super密码的老化时间	**password-control super aging** *aging-time*	缺省情况下，密码的老化时间为90天
配置super密码的最小长度	**password-control super length** *length*	非FIPS模式下： 缺省情况下，密码的最小长度为10个字符 FIPS模式下： 缺省情况下，密码的最小长度为15个字符

操作	命令	说明
配置super密码的组合策略	**password-control super composition type-number** *type-number* [**type-length** *type-length*]	非FIPS模式下： 缺省情况下，密码元素的组合类型至少为1种，至少要包含每种元素的个数为1个 FIPS模式下： 缺省情况下，密码元素的组合类型至少为4种，至少要包含每种元素的个数为1个

1.4 Password Control显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 Password Control 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** 命令可以清除 Password Control 统计信息。

表1-7 Password Control 显示和维护

操作	命令
显示密码管理的配置信息	**display password-control** [**super**]
显示用户认证失败后，被加入密码管理黑名单中的用户信息	**display password-control blacklist** [**user-name** *name* | **ip** *ipv4-address* | **ipv6** *ipv6-address*]
清除密码管理黑名单中的用户	**reset password-control blacklist** [**user-name** *name*]
清除用户的密码历史记录	**reset password-control history-record** [**user-name** *name* | **super** [**role** *role-name*]]

说明

当密码历史记录功能未启动时，**reset password-control history-record** 命令同样可以清除全部或者某个用户的密码历史记录。

1.5 Password Control典型配置举例

1. 组网需求

有以下密码管理需求：

- 全局密码管理策略：用户 2 次登录失败后就永久禁止登录；最小密码长度为 16 个字符，密码老化时间为 30 天；允许用户进行密码更新的最小时间间隔为 36 小时；密码过期后 60 天内允许登录 5 次；用户帐号的闲置时间为 30 天；不允许密码中包含用户名或者字符顺序颠倒的用户名；不允许密码中包含连续三个或以上相同字符；密码元素的最少组合类型为 4 种，至少要包含每种元素的个数为 4 个。

- 切换到用户角色 network-operator 时使用的 super 密码管理策略：最小密码长度为 24 个字符，密码元素的最少组合类型为 4 种，至少要包含每种元素的个数为 5 个。
- 本地 Telnet 用户 test 的密码管理策略：最小密码长度为 24 个字符，密码元素的最少组合类型为 4 种，至少要包含每种元素的个数为 5 个，密码老化时间为 20 天。

2. 配置步骤

使能全局密码管理功能。

```
<Sysname> system-view
[Sysname] password-control enable
```

配置用户 2 次登录失败后就永久禁止该用户登录。

```
[Sysname] password-control login-attempt 2 exceed lock
```

配置全局的密码老化时间为 30 天。

```
[Sysname] password-control aging 30
```

配置全局的密码的最小长度为 16。

```
[Sysname] password-control length 16
```

配置密码更新的最小时间间隔为 36 小时。

```
[Sysname] password-control update-interval 36
```

配置用户密码过期后的 60 天内允许登录 5 次。

```
[Sysname] password-control expired-user-login delay 60 times 5
```

配置用户帐号的闲置时间为 30 天。

```
[Sysname] password-control login idle-time 30
```

使能在配置的密码中检查包含用户名或者字符顺序颠倒的用户名的功能。

```
[Sysname] password-control complexity user-name check
```

使能在配置的密码中检查包含连续三个或以上相同字符的功能。

```
[Sysname] password-control complexity same-character check
```

#配置全局的密码元素的最少组合类型为 4 种，至少要包含每种元素的个数为 4 个。

```
[Sysname] password-control composition type-number 4 type-length 4
```

配置 super 密码的最小长度为 24。

```
[Sysname] password-control super length 24
```

配置 super 密码元素的最少组合类型为 4 种，至少要包含每种元素的个数为 5 个。

```
[Sysname] password-control super composition type-number 4 type-length 5
```

配置切换到用户角色 network-operator 时使用的 super 密码为明文 123456789ABGFTweuix@#$%!。

```
[Sysname] super password network-operator simple 123456789ABGFTweuix@#$%!
```

添加设备管理类本地用户 test。

```
[Sysname] local-user test class manage
```

配置本地用户的服务类型为 Telnet。

```
[Sysname-luser-manage-test] service-type telnet
```

配置本地用户的最小密码长度为 24 个字符。

```
[Sysname-luser-manage-test] password-control length 24
```

配置本地用户的密码元素的最少组合类型为 4 种，至少要包含每种元素的个数为 5 个。

```
[Sysname-luser-manage-test] password-control composition type-number 4 type-length 5
```

配置本地用户的密码老化时间为 20 天。

```
[Sysname-luser-manage-test] password-control aging 20
```

以交互式方式配置本地用户密码。

```
[Sysname-luser-manage-test] password
Password:
Confirm :
Updating user information. Please wait ... ...
[Sysname-luser-manage-test] quit
```

3. 验证配置结果

可通过如下命令查看全局密码管理的配置信息。

```
<Sysname> display password-control
 Global password control configurations:
 Password control:                     Enabled
 Password aging:                       Enabled (30 days)
 Password length:                      Enabled (16 characters)
 Password composition:                 Enabled (4 types, 4 characters per type)
 Password history:                     Enabled (max history record:4)
 Early notice on password expiration:  7 days
 Maximum login attempts:               2
 Action for exceeding login attempts:  Lock
 Minimum interval between two updates: 36 hours
 User account idle time:               30 days
 Logins with aged password:            5 times in 60 days
 Password complexity:                  Enabled (username checking)
                                       Enabled (repeated characters checking)
```

可通过如下命令查看 super 密码管理的配置信息。

```
<Sysname> display password-control super
 Super password control configurations:
 Password aging:                       Enabled (90 days)
 Password length:                      Enabled (24 characters)
 Password composition:                 Enabled (4 types, 5 characters per type)
```

可通过如下命令查看到本地用户密码管理的配置信息。

```
<Sysname> display local-user user-name test class manage
Total 1 local users matched.

Device management user test:
 State:                    Active
 Service type:             Telnet
 User group:               system
 Bind attributes:
 Authorization attributes:
  Work directory:          flash:
  User role list:          network-operator
 Password control configurations:
  Password aging:          Enabled (20 days)
  Password length:         Enabled (24 characters)
  Password composition:    Enabled (4 types, 5 characters per type)
```

目 录

1 公钥管理

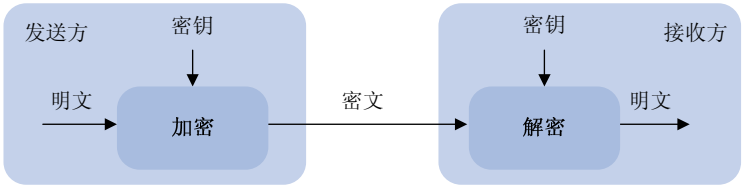
说明

设备运行于 FIPS 模式时，本特性部分配置相对于非 FIPS 模式有所变化，具体差异请见本文相关描述。有关 FIPS 模式的详细介绍请参见“安全配置指导”中的“FIPS”。

1.1 简介

如 图 1-1 所示，为了保证数据在网络中安全传输、不被攻击者非法窃听和恶意篡改，发送方在发送数据之前需要对数据进行加密处理，即通过一定的算法，利用密钥将明文数据变换为密文数据；接收方接收到密文数据后，需要对其进行解密处理，即通过一定的算法，利用密钥将密文数据恢复为明文数据，以获得原始数据。其中，密钥是一组特定的字符串，是控制明文和密文转换的唯一参数，起到“钥匙”的作用。

图1-1 加密和解密转换关系示意图



如果数据加密和解密时使用不同的密钥，则该加/解密算法称为非对称密钥算法。在非对称密钥算法中，加密和解密使用的密钥一个是对外公开的公钥，一个是由用户秘密保存的私钥，从公钥很难推算出私钥。公钥和私钥一一对应，二者统称为非对称密钥对。通过公钥（或私钥）加密后的数据只能利用对应的私钥（或公钥）进行解密。

说明

- 如果数据加密和解密时使用相同的密钥，则该加/解密算法称为对称密钥算法。使用对称密钥算法时，接收方和发送方需要获得相同的密钥，存在密钥分发的安全性问题。使用非对称密钥算法时，不存在该问题。
- 非对称密钥算法的安全性与密钥模数的长度相关。密钥模数越长，安全性越好，但是生成密钥所需的时间越长。

非对称密钥算法包括 RSA（Rivest Shamir and Adleman）、DSA（Digital Signature Algorithm，数字签名算法）和 ECDSA（Elliptic Curve Digital Signature Algorithm，椭圆曲线数字签名算法）等。非对称密钥算法主要有两个用途：

- 对发送的数据进行加/解密：发送者利用接收者的公钥对数据进行加密，只有拥有对应私钥的接收者才能使用该私钥对数据进行解密，从而可以保证数据的机密性。目前，只有 RSA 算法可以用来对发送的数据进行加/解密。
- 对数据发送者的身份进行认证：非对称密钥算法的这种应用，称为数字签名。发送者利用自己的私钥对数据进行加密，接收者利用发送者的公钥对数据进行解密，从而实现对数据发送者身份的验证。由于只能利用对应的公钥对通过私钥加密后的数据进行解密，因此根据解密是否成功，就可以判断发送者的身份是否合法，如同发送者对数据进行了“签名”。例如，用户 1 使用自己的私钥对数据进行签名后，发给用户 2，用户 2 利用用户 1 的公钥验证签名，如果签名是正确的，那么就能够确认该数据来源于用户 1。目前，RSA、DSA 和 ECDSA 都可以用于数字签名。

非对称密钥算法应用十分广泛，例如 SSH（Secure Shell，安全外壳）、SSL（Secure Sockets Layer，安全套接字层）、PKI（Public Key Infrastructure，公钥基础设施）中都利用了非对称密钥算法进行数字签名。SSH、SSL 和 PKI 的介绍，请参见“安全配置指导”中的“SSH”、“SSL”和“PKI”。

1.2 公钥管理配置任务简介

本章主要介绍如何管理非对称密钥对，包括：

- 本地非对称密钥对的管理：即管理设备自身的非对称密钥对，包括本地密钥对的生成、销毁、本地主机公钥的显示和导出。
- 远端主机公钥的管理：即将远端主机的主机公钥保存到本地设备。

完成本章中的配置后，并不能实现利用非对称密钥算法进行加/解密和数字签名，只是为其提供了必要的准备。本章中的配置只有与具体的应用（如 SSH、SSL）配合使用，才能实现利用非对称密钥算法进行加/解密或数字签名。

表1-1 公钥管理配置任务简介

配置任务		说明	详细配置
配置本地非对称密钥对	生成本地非对称密钥对	根据实际情况选择需要的配置	1.3.1
	显示或导出本地非对称密钥对中的主机公钥		1.3.2
	销毁本地非对称密钥对		1.3.3
配置远端主机的公钥			1.4

1.3 配置本地非对称密钥对

1.3.1 生成本地非对称密钥对

本地非对称密钥对分为如下几种：

- RSA：非 FIPS 模式下，生成默认名称的本地 RSA 密钥对时，将同时生成两个密钥对——服务器密钥对和主机密钥对，二者都包括一个公钥和一个私钥；生成非默认名称的本地 RSA 密钥对时，只生成一个主机密钥对。生成 RSA 密钥对时会提示用户输入密钥模数的长度，建议密钥模数的长度大于或等于 768 比特，以提高安全性。目前，只有 SSH1.5 中应用了 RSA 服

务器密钥对；FIPS 模式下，生成默认名称的本地 RSA 密钥对时，将只生成 1 个密钥对——主机密钥对，包括一个公钥和一个私钥。RSA 密钥模数的长度为 2048 比特。

- DSA：非 FIPS 模式下，生成本地 DSA 密钥对时，只生成一个主机密钥对。生成 DSA 密钥对时会提示用户输入密钥模数的长度，建议密钥模数的长度大于或等于 768 比特，以提高安全性；FIPS 模式下，DSA 密钥模数的长度为 2048 比特。
- ECDSA：生成本地 ECDSA 密钥对时，只生成一个主机密钥对。ECDSA 主机密钥的长度为 192 比特。

生成本地非对称密钥对时，需要注意：

- 生成密钥对时，通过 **name** *key-name* 参数指定的密钥对名称可以与密钥对的默认名称相同，该密钥对与不指定 **name** *key-name* 参数生成的默认名称的密钥对被视为两个不同的密钥对，可以在设备上同时存在这两个密钥对。
- 非默认名称密钥对的密钥类型和名称不能完全相同，否则需要用户确认是否覆盖原有的密钥对。不同类型的密钥，名称可以相同。
- 执行 **public-key local create** 命令后，生成的密钥对将保存在设备中，设备重启后密钥不会丢失。

表1-2 生成本地非对称密钥对

操作	命令	说明
进入系统视图	**system-view**	-
生成本地非对称密钥对	**public-key local create** { **dsa** | **ecdsa** | **rsa** } [**name** *key-name*]	缺省情况下，不存在任何本地非对称密钥对

1.3.2 显示或导出本地非对称密钥对中的主机公钥

在某些应用（如 SSH）中，为了实现远端主机采用数字签名方法对本地设备进行身份验证，用户需要将本地的主机公钥保存到远端主机上。

将本地的主机公钥保存到远端主机上，有以下三种方法：

- 如 表 1-3 所示，在本地设备上执行**public-key local export**命令按照指定格式将本地主机公钥导出到指定文件（执行命令时指定*filename*参数），并将该文件上传到远端主机上。如 表 1-7 所示，在远端主机上，通过从公钥文件中导入的方式将本地的主机公钥保存到远端设备上。
- 如 表 1-4 所示，在本地设备上执行**public-key local export**命令按照指定格式显示本地主机公钥（执行命令时不指定*filename*参数），通过拷贝粘贴等方式将显示的主机公钥保存到文件中，并将该文件上传到远端主机上。如 表 1-7 所示，在远端主机上，通过从公钥文件中导入的方式将本地的主机公钥保存到远端设备上。
- 如 表 1-5 所示，在本地设备上执行**display public-key local public**命令显示非对称密钥对中的公钥信息，并记录主机公钥数据。如 表 1-8 所示，在远端主机上，通过手工配置的方式将记录的本地主机公钥保存到远端设备上。

远端主机上的配置方法，请参见“1.4 配置远端主机的公钥”。

表1-3 按照指定格式导出本地非对称密钥对中的主机公钥

操作	命令	说明
进入系统视图	**system-view**	-
按照指定格式将本地RSA主机公钥导出到指定文件	非FIPS模式下： **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh1** | **ssh2** } *filename* FIPS模式下： **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh2** } *filename*	二者至少选其一
按照指定格式将本地DSA主机公钥导出到指定文件	**public-key local export dsa** [**name** *key-name*] { **openssh** | **ssh2** } *filename*	

表1-4 按照指定格式显示本地非对称密钥对中的主机公钥

操作	命令	说明
进入系统视图	**system-view**	-
按照指定格式显示本地RSA主机公钥	非FIPS模式下： **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh1** | **ssh2** } FIPS模式下： **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh2** }	二者至少选其一
按照指定格式显示本地DSA主机公钥	**public-key local export dsa** [**name** *key-name*] { **openssh** | **ssh2** }	

表1-5 显示本地非对称密钥对中的公钥信息

操作	命令	说明
显示本地RSA密钥对中的公钥信息	**display public-key local rsa public** [**name** *key-name*]	二者至少选其一 可以在任意视图下执行这两条命令 若执行**display public-key local rsa public**命令时，同时显示了RSA服务器密钥对和主机密钥对的公钥信息，用户只需记录主机密钥对的公钥信息
显示本地DSA密钥对中的公钥信息	**display public-key local dsa public** [**name** *key-name*]	

1.3.3 销毁本地非对称密钥对

在如下几种情况下，建议用户销毁旧的非对称密钥对，并生成新的密钥对：

- 本地设备的私钥泄露。这种情况下，非法用户可能会冒充本地设备访问网络。
- 保存密钥对的存储设备出现故障，导致设备上没有公钥对应的私钥，无法再利用旧的非对称密钥对进行加/解密和数字签名。
- 密钥对使用了较长时间，可能存在密钥泄露或破译的风险。

- 本地证书到达有效期，需要删除对应的本地密钥对。本地证书的详细介绍，请参见“安全配置指导”中的“PKI”。

表1-6 销毁本地非对称密钥对

操作	命令	说明
进入系统视图	**system-view**	-
销毁本地非对称密钥对	**public-key local destroy** { **dsa** | **ecdsa** | **rsa** } [**name** *key-name*]	-

1.4 配置远端主机的公钥

在某些应用（如 SSH）中，为了实现本地设备对远端主机的身份验证，需要在本地设备上配置远端主机的 RSA 或 DSA 主机公钥。

配置远端主机公钥的方式有如下两种：

- 从公钥文件中导入：用户事先将远端主机的公钥文件保存到本地设备（例如，通过 FTP 或 TFTP，以二进制方式将远端主机的公钥文件保存到本地设备），本地设备从该公钥文件中导入远端主机的公钥。导入公钥时，系统会自动将远端主机的公钥文件转换为 PKCS（Public Key Cryptography Standards，公共密钥加密标准）编码形式。
- 手工配置：用户事先在远端主机上查看其公钥信息，并记录远端主机公钥的内容。在本地设备上采用手工输入的方式将远端主机的公钥配置到本地。手工输入远端主机公钥时，可以逐个字符输入，也可以一次拷贝粘贴多个字符。

远端主机公钥信息的获取方法，请参见“1.3.2 显示或导出本地非对称密钥对中的主机公钥”。

说明

手工配置远端主机的公钥时，输入的主机公钥必须满足一定的格式要求。通过 **display public-key local public** 命令显示的公钥可以作为输入的公钥内容；通过其他方式（如 **public-key local export** 命令）显示的公钥可能不满足格式要求，导致主机公钥保存失败。因此，建议选用从公钥文件导入的方式配置远端主机的公钥。

表1-7 从公钥文件中导入远端主机的公钥

操作	命令	说明
进入系统视图	**system-view**	-
从公钥文件中导入远端主机的公钥	**public-key peer** *keyname* **import sshkey** *filename*	缺省情况下，设备上不存在任何远端主机公钥

表1-8 手工配置远端主机的公钥

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
指定远端主机公钥的名称，并进入公钥视图	**public-key peer** *keyname*	缺省情况下，设备上不存在任何远端主机公钥
配置远端主机的公钥	逐个字符输入或拷贝粘贴公钥内容	在输入公钥内容时，字符之间可以有空格，也可以按回车键继续输入数据。保存公钥数据时，将删除空格和回车符
退回系统视图	**peer-public-key end**	退出公钥视图时，系统自动保存配置的主机公钥

1.5 公钥管理显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后公钥管理的信息，通过查看显示信息验证配置的效果。

表1-9 公钥管理显示和维护

操作	命令
显示本地非对称密钥对中的公钥信息	**display public-key local** { **dsa** | **ecdsa** | **rsa** } **public** [**name** *key-name*]
显示保存在本地的远端主机的公钥信息	**display public-key peer** [**brief** | **name** *publickey-name*]

1.6 公钥管理典型配置举例

1.6.1 手工配置远端主机的公钥

1. 组网需求

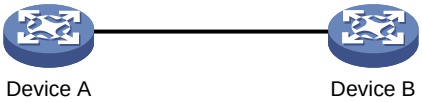
如 图 1-2 所示，为了防止非法用户访问，Device B（本地设备）采用数字签名方法对访问它的Device A（远端设备）进行身份验证。进行身份验证前，需要在Device B上配置Device A的公钥。

本例中要求：

- Device B 采用的非对称密钥算法为 RSA 算法。
- 采用手工配置方式在 Device B 上配置 Device A 的主机公钥。

2. 组网图

图1-2 手工配置远端主机的公钥组网图



3. 配置步骤

(1) 配置 Device A

在 Device A 上生成默认名称的本地 RSA 非对称密钥对，密钥模数的长度采用缺省值 1024 比特。

```
<DeviceA> system-view
[DeviceA] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.................++++++
.....................................++++++
.....++++++++
.............++++++++
Create the key pair successfully.
```

显示生成的本地 RSA 密钥对的公钥信息。

```
[DeviceA] display public-key local rsa public

=============================================
Key name: hostkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DA3B90F59237347B
   8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
   45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
   6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
   CB47440AF6BB25ACA50203010001
=============================================
Key name: serverkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2011/05/12
Key code:
   307C300D06092A864886F70D0101010500036B003068026100C9451A80F7F0A9BA1A90C7BC
   1C02522D194A2B19F19A75D9EF02219068BD7FD90FCC2AF3634EEB9FA060478DD0A1A49ACE
   E1362A4371549ECD85BA04DEE4D6BB8BE53B6AED7F1401EE88733CA3C4CED391BAE633028A
   AC41C80A15953FB22AA30203010001
```

(2) 配置 Device B

在 Device B 上配置 Device A 的主机公钥：在公钥视图输入 Device A 的主机公钥，即在 Device A 上通过 **display public-key local rsa public** 命令显示的主机公钥 hostkey 内容。

```
<DeviceB> system-view
[DeviceB] public-key peer devicea
Enter public key view. Return to system view with "peer-public-key end" command.
[DeviceB-pkey-public-key-devicea]30819F300D06092A864886F70D010101050003818D003081890
2818100DA3B90F59237347B
[DeviceB-pkey-public-key-devicea]8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027A
C8F04A827B30C2CAF79242E
[DeviceB-pkey-public-key-devicea]45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D2
88EC54A5D31EFAE4F681257
[DeviceB-pkey-public-key-devicea]6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94E
```

```
B1F2D561BF66EA27DFD4788
[DeviceB-pkey-public-key-devicea]CB47440AF6BB25ACA50203010001
```

从公钥视图退回到系统视图，并保存用户输入的公钥。

```
[DeviceB-pkey-public-key-devicea] peer-public-key end
```

4. 验证配置

显示 Device B 上保存的 Device A 的主机公钥信息。

```
[DeviceB] display public-key peer name devicea

=============================================
Key name: devicea
Key type: RSA
Key modulus: 1024
Key code:
    30819F300D06092A864886F70D010101050003818D0030818902818100DA3B90F59237347B
    8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
    45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
    6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
    CB47440AF6BB25ACA50203010001
```

通过对比可以看出，Device B 上保存的 Device A 的主机公钥信息与 Device A 实际的主机公钥信息一致。

1.6.2 从公钥文件中导入远端主机的公钥

1. 组网需求

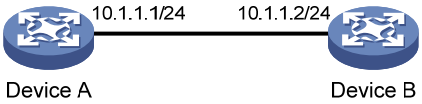
如 图 1-3 所示，为了防止非法用户访问，Device B（本地设备）采用数字签名方法对访问它的Device A（远端设备）进行身份验证。进行身份验证前，需要在Device B上配置Device A的公钥。

本例中要求：

- Device B 采用的非对称密钥算法为 RSA 算法。
- 采用从公钥文件中导入的方式在 Device B 上配置 Device A 的主机公钥。

2. 组网图

图1-3 从公钥文件中导入远端主机的公钥组网图



3. 配置步骤

(1) 在 Device A 上生成密钥对，并导出公钥

在 Device A 上生成默认名称的本地 RSA 非对称密钥对，密钥模数的长度采用缺省值 1024 比特。

```
<DeviceA> system-view
[DeviceA] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
```

```
Input the modulus length [default = 1024]:
Generating Keys...
.................++++++
.....................................++++++
.....++++++++
..............++++++++
Create the key pair successfully.
```

显示生成的本地 RSA 密钥对的公钥信息。

```
[DeviceA] display public-key local rsa public

=============================================
Key name: hostkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DA3B90F59237347B
   8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
   45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
   6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
   CB47440AF6BB25ACA50203010001
=============================================
Key name: serverkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2011/05/12
Key code:
   307C300D06092A864886F70D0101010500036B003068026100C9451A80F7F0A9BA1A90C7BC
   1C02522D194A2B19F19A75D9EF02219068BD7FD90FCC2AF3634EEB9FA060478DD0A1A49ACE
   E1362A4371549ECD85BA04DEE4D6BB8BE53B6AED7F1401EE88733CA3C4CED391BAE633028A
   AC41C80A15953FB22AA30203010001
```

将生成的默认名称的 RSA 主机公钥导出到指定文件 devicea.pub 中。

```
[DeviceA] public-key local export rsa ssh2 devicea.pub
[DeviceA] quit
```

(2) 在 Device A 上启动 FTP 服务器功能

启动 FTP 服务器功能，创建 FTP 用户（用户名为 ftp，密码为 123），并配置 FTP 用户的用户角色为 network-admin。

```
[DeviceA] ftp server enable
[DeviceA] local-user ftp
[DeviceA-luser-manage-ftp] password simple 123
[DeviceA-luser-manage-ftp] service-type ftp
[DeviceA-luser-manage-ftp] authorization-attribute user-role network-admin
[DeviceA-luser-manage-ftp] quit
```

(3) Device B 获取 Device A 的公钥文件

Device B 通过 FTP 以二进制方式从 Device A 获取公钥文件 devicea.pub。

```
<DeviceB> ftp 10.1.1.1
Connected to 10.1.1.1 (10.1.1.1).
220 FTP service ready.
User (10.1.1.1:(none)): ftp
```

```
331 Password required for ftp.
Password:
230 User logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> binary
200 TYPE is now 8-bit binary
ftp> get devicea.pub
227 Entering Passive Mode (10,1,1,1,118,252)
150 Accepted data connection
226 File successfully transferred
301 bytes received in 0.003 seconds (98.0 kbyte/s)
ftp> quit
221-Goodbye. You uploaded 0 and downloaded 1 kbytes.
221 Logout.
```

(4) Device B 从公钥文件中导入公钥

Device B 从公钥文件中导入 Device A 的主机公钥。

```
<DeviceB> system-view
[DeviceB] public-key peer devicea import sshkey devicea.pub
```

4. 验证配置

显示 Device B 上保存的 Device A 的主机公钥信息。

```
[DeviceB] display public-key peer name devicea

==============================================
Key name: devicea
Key type: RSA
Key modulus: 1024
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DA3B90F59237347B
   8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
   45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
   6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
   CB47440AF6BB25ACA50203010001
```

通过对比可以看出，Device B 上保存的 Device A 的主机公钥信息与 Device A 实际的主机公钥信息一致。

目 录

1 PKI

说明

设备运行于FIPS模式时，本特性部分配置相对于非FIPS模式有所变化，具体差异请见本文相关描述。有关 FIPS 模式的详细介绍请参见“安全配置指导”中的“FIPS”。

1.1 PKI简介

1.1.1 概述

PKI（Public Key Infrastructure，公钥基础设施）是一个利用公钥理论和技术来实现并提供信息安全服务的具有通用性的安全基础设施。

公钥体制也称为非对称密钥体制，是目前已经得到广泛应用的一种密码体制。该体制使用一个公开的密钥（公钥）和一个保密的密钥（私钥）进行信息的加密和解密，用公钥加密的信息只能用私钥解密，反之亦然。这样的一个公钥和其对应的一个私钥称为一个密钥对。公钥体制的这种特点使其可以应用于安全协议，实现数据源认证、完整性和不可抵赖性。

PKI 系统以数字证书的形式分发和使用公钥。数字证书是一个用户的身份和他所持有的公钥的结合。基于数字证书的 PKI 系统，能够为网络通信和网络交易（例如电子政务和电子商务）提供各种安全服务。

目前，我司的 PKI 特性可为安全协议 IPsec（IP Security，IP 安全）、SSL（Secure Sockets Layer，安全套接字层）提供证书管理机制。

1.1.2 相关术语

1. 数字证书

数字证书是经 CA（Certificate Authority，证书颁发机构）签名的、包含公钥及相关的用户身份信息的文件，它建立了用户身份信息与用户公钥的关联。CA 对数字证书的签名保证了证书是可信任的。数字证书的格式遵循 ITU-T X.509 国际标准，目前最常用的为 X.509 V3 标准。数字证书中包含多个字段，包括证书签发者的名称、被签发者的名称（或者称为主题）、公钥信息、CA 对证书的数字签名、证书的有效期等。

本手册中涉及四类证书：CA 证书、RA（Registration Authority，证书注册机构）证书、本地证书和对端证书。

- CA 证书是 CA 持有的证书。若 PKI 系统中存在多个 CA，则会形成一个 CA 层次结构，最上层的 CA 是根 CA，它持有一个自签名的证书（即根 CA 对自己的证书签名），下一级 CA 证书分别由上一级 CA 签发。这样，从根 CA 开始逐级签发的证书就会形成多个可信任的链状结构，每一条路径称为一个证书链。
- RA 证书是 RA 持有的证书，由 CA 签发。RA 受 CA 委托，可以为 CA 分担部分管理工作。RA 在 PKI 系统中是可选的。

- 本地证书是本设备持有的证书，由 CA 签发。
- 对端证书是其它设备持有的证书，由 CA 签发。

2. CRL（Certificate Revocation List，证书吊销列表）

由于用户名称的改变、私钥泄漏或业务中止等原因，需要存在一种方法将现行的证书吊销，即废除公钥及相关的用户身份信息的绑定关系。在 PKI 中，可以通过发布 CRL 的方式来公开证书的吊销信息。当一个或若干个证书被吊销以后，CA 签发 CRL 来声明这些证书是无效的，CRL 中会列出所有被吊销的证书的序列号。因此，CRL 提供了一种检验证书有效性的方式。

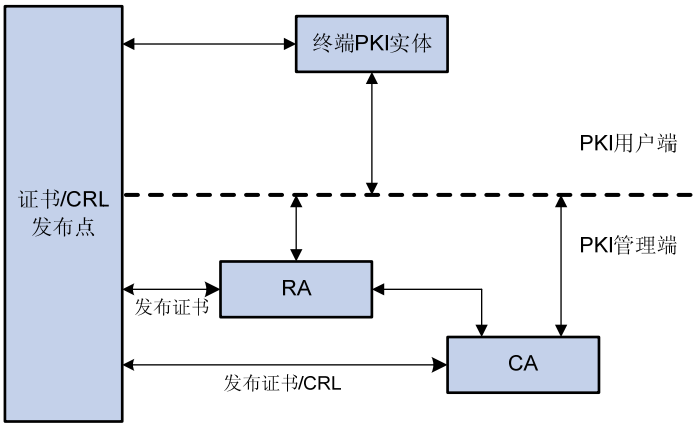
3. CA策略

CA 策略是指 CA 在受理证书请求、颁发证书、吊销证书和发布 CRL 时所采用的一套标准。通常，CA 以一种叫做 CPS（Certification Practice Statement，证书惯例声明）的文档发布其策略。CA 策略可以通过带外（如电话、磁盘、电子邮件等）或其它方式获取。由于不同的 CA 使用不同的策略，所以在选择信任的 CA 进行证书申请之前，必须理解 CA 策略。

1.1.3 体系结构

一个PKI体系由终端PKI实体、CA、RA和证书/CRL发布点四类实体共同组成，如下 图 1-1。

图1-1 PKI 体系结构图



1. 终端PKI实体

终端 PKI 实体是 PKI 服务的最终使用者，可以是个人、组织、设备（如路由器、交换机）或计算机中运行的进程，后文简称为 PKI 实体。

2. CA（Certificate Authority，证书颁发机构）

CA 是一个用于签发并管理数字证书的可信 PKI 实体。其作用包括：签发证书、规定证书的有效期和发布 CRL。

3. RA（Registration Authority，证书注册机构）

RA 是一个受 CA 委托来完成 PKI 实体注册的机构，它接收用户的注册申请，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，用于减轻 CA 的负担。建议在部署 PKI 系统时，RA 与 CA 安装在不同的设备上，减少 CA 与外界的直接交互，以保护 CA 的私钥。

4. 证书/CRL发布点

证书/CRL 发布点用于对用户证书和 CRL 进行存储和管理，并提供查询功能。通常，证书/CRL 发布点位于一个目录服务器上，该服务器可以采用 LDAP（Lightweight Directory Access Protocol，轻量级目录访问协议）协议、HTTP 等协议工作。其中，较为常用的是 LDAP 协议，它提供了一种访问发布点的方式。LDAP 服务器负责将 CA/RA 服务器传输过来的数字证书或 CRL 进行存储，并提供目录浏览服务。用户通过访问 LDAP 服务器获取自己和其他用户的数字证书或者 CRL。

1.1.4 PKI实体申请证书的工作过程

下面是一个 PKI 实体向 CA 申请本地证书的典型工作过程，其中由 RA 来完成 PKI 实体的注册：

(1) PKI 实体向 RA 提出证书申请；

(2) RA 审核 PKI 实体身份，将 PKI 实体身份信息和公钥以数字签名的方式发送给 CA；

(3) CA 验证数字签名，同意 PKI 实体的申请，并颁发证书；

(4) RA 接收 CA 返回的证书，将其发布到 LDAP 服务器（或其它形式的发布点）上以提供目录浏览服务，并通知 PKI 实体证书发布成功；

(5) PKI 实体通过 SCEP（Simple Certificate Enrollment Protocol，简单证书注册协议）从 RA 处获取证书，利用该证书可以与其它 PKI 实体使用加密、数字签名进行安全通信。

1.1.5 主要应用

PKI 技术能满足人们对网络交易安全保障的需求。PKI 的应用范围非常广泛，并且在不断发展之中，下面给出几个应用实例。

1. VPN（Virtual Private Network，虚拟专用网络）

VPN 是一种构建在公用通信基础设施上的专用数据通信网络，它可以利用网络层安全协议（如 IPsec）和建立在 PKI 上的加密与数字签名技术来获得完整性保护。

2. 安全电子邮件

电子邮件的安全也要求机密性、完整性、数据源认证和不可抵赖。目前发展很快的安全电子邮件协议 S/MIME（Secure/Multipurpose Internet Mail Extensions，安全/多用途 Internet 邮件扩充协议），是一个允许发送加密和有签名邮件的协议。该协议的实现需要依赖于 PKI 技术。

3. Web安全

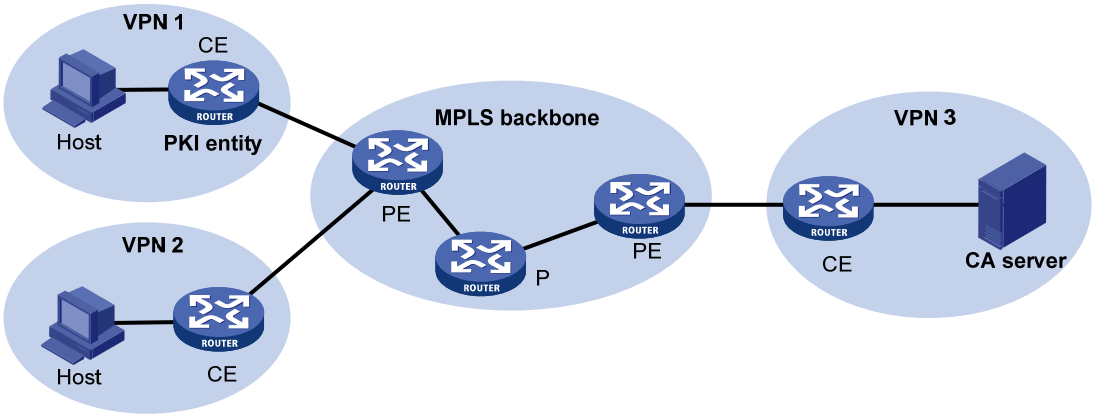
为了透明地解决 Web 的安全问题，在浏览器和服务器之间进行通信之前，先要建立 SSL 连接。SSL 协议允许在浏览器和服务器之间进行加密通信，并且利用 PKI 技术对服务器和浏览器端进行身份验证。

1.1.6 证书申请支持MPLS L3VPN

实际组网应用中，某企业的各分支机构属于不同的 VPN，且各 VPN 之间的业务相互隔离。如果各分支机构的用户要通过位于总部 VPN 中的服务器申请证书，则需要 PKI 证书申请支持 MPLS L3VPN。如 图 1-2 所示，连接客户端PKI entity的PE设备，通过MPLS L3VPN将私网客户端PKI entity的证书申请报文透传给网络另一端的CA server，CA server接收并处理证书申请信息，连接服务器端的PE设备将CA server签发的证书也通过MPLS L3VPN透传回PKI entity，满足了私网VPN业务隔离情况下的证书申请。

关于 MPLS L3VPN 的相关介绍请参见“MPLS 配置指导”中的“MPLS L3VPN”。

图1-2 证书申请支持 MPLS L3VPN



1.2 PKI配置任务简介

表1-1 PKI 配置任务简介

配置任务		说明	详细配置
配置PKI实体		必选	1.3
配置PKI域		必选	1.4
申请证书	自动申请证书	二者必选其一	1.5.1
	手工申请证书		1.5.2
停止证书申请过程		可选	1.6
手工获取证书		可选	1.7
配置证书验证		可选	1.8
配置证书和CRL的存储路径		可选	1.9
导出证书		可选	1.10
删除证书		可选	1.11
配置证书属性的访问控制策略		可选	1.12

1.3 配置PKI实体

一份证书是一个公钥与一个实体身份信息的绑定。PKI 实体的参数是 PKI 实体的身份信息，CA 根据 PKI 实体提供的身份信息来唯一标识证书申请者。

一个有效的 PKI 实体参数中必须至少包括以下参数之一：

(1) DN（Distinguished Name，识别名），包含以下参数：

- 实体通用名。对于 DN 参数，实体的通用名必须配置。

- 实体所属国家代码，用标准的两字符代码表示。例如，“CN”是中国的合法国家代码，“US”是美国的合法国家代码
- 实体所在地理区域名称
- 实体所属组织名称
- 实体所属组织部门名称
- 实体所属州省

(2) FQDN（Fully Qualified Domain Name，完全合格域名），是 PKI 实体在网络中的唯一标识

(3) IP 地址

配置 PKI 实体时，需要注意的是：

- PKI 实体的配置必须与 CA 证书颁发策略相匹配，因此建议根据 CA 证书颁发策略来配置 PKI 实体，如哪些 PKI 实体参数为必选配置，哪些为可选配置。申请者的身份信息必须符合 CA 证书颁发策略，否则证书申请可能会失败。
- Windows 2000 CA 服务器的 SCEP 插件对证书申请的数据长度有一定的限制。PKI 实体配置项超过一定数据长度时，CA 将不会响应 PKI 实体的证书申请。这种情况下如果通过离线方式提交申请，Windows 2000 CA 服务器可以完成签发。其它 CA 服务器（例如 RSA 服务器和 OpenCA 服务器）目前没有这种限制。

表1-2 配置 PKI 实体

操作	命令	说明
进入系统视图	**system-view**	-
创建一个PKI实体，并进入该PKI实体视图	**pki entity** *entity-name*	缺省情况下，无PKI实体存在 设备支持创建多个PKI实体
配置PKI实体的通用名	**common-name** *common-name-sting*	缺省情况下，未配置PKI实体的通用名
配置PKI实体所属国家代码	**country** *country-code-string*	缺省情况下，未配置PKI实体所属国家代码
配置PKI实体所在地理区域名称	**locality** *locality-name*	缺省情况下，未配置PKI实体所在地理区域名称
配置PKI实体所属组织名称	**organization** *org-name*	缺省情况下，未配置PKI实体所属组织名称
配置PKI实体所属组织部门名称	**organization-unit** *org-unit-name*	缺省情况下，未配置PKI实体所属组织部门名称
配置PKI实体所属州或省的名称	**state** *state-name*	缺省情况下，未配置PKI实体所属州或省的名称
配置PKI实体的FQDN	**fqdn** *fqdn-name-string*	缺省情况下，未配置PKI实体的FQDN
配置PKI实体的IP地址	**ip** { *ip-address* | **interface** *interface-type interface-number* }	缺省情况下，未配置PKI实体的IP地址

1.4 配置PKI域

PKI 实体在进行 PKI 证书申请操作之前需要配置一些注册信息来配合完成申请的过程。这些信息的集合就是一个 PKI 域。

PKI 域是一个本地概念，创建 PKI 域的目的是便于其它应用（比如 IKE、SSL）引用 PKI 的配置。

PKI 域中包括以下参数：

(1) 信任的 CA 名称

PKI 实体通过一个可信的 CA 来完成证书的注册及颁发的。在证书申请之前，若当前的 PKI 域中没有 CA 证书，则需要首先获取 CA 证书，获取 CA 证书之前必须指定一个信任的 CA 名称。这个名称会被作为 SCEP 消息的一部分发送给 CA 服务器。一般情况下，CA 服务器会忽略收到的 SCEP 消息中的 CA 名称的具体内容。但是如果在同一台服务器主机上配置了两个 CA，且它们的 URL 是相同的，则需要根据 PKI 域中指定的信任的 CA 名词来区分它们。设备信任的 CA 的名称只是在获取 CA 证书时使用，申请本地证书时不会用到。

(2) PKI 实体名称

向 CA 发送证书申请请求时，必须指定所使用的 PKI 实体名，以向 CA 表明自己的身份。

(3) 证书申请的注册受理机构

证书申请的受理一般由一个独立的注册机构（即 RA）来承担，它并不给用户签发证书，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，而是将其作为 CA 的一项功能而已。推荐使用独立运行的 RA 作为注册受理机构。

(4) 注册受理机构服务器的 URL

证书申请之前必须指定注册受理机构服务器的 URL，PKI 实体通过 SCEP（Simple Certificate Enrollment Protocol，简单证书注册协议）向该 URL 地址发送证书申请请求。SCEP 是专门用于与认证机构进行通信的协议。

(5) 证书申请状态的查询周期和最大次数

PKI 实体在发送证书申请后，如果 CA 手工验证申请，证书的签发会需要很长时间。在此期间，PKI 实体会定期发送状态查询，以便在证书签发后能及时获取到证书。设备上可以配置证书申请状态的查询周期和最大次数。

(6) LDAP 服务器主机名

在 PKI 系统中，可以采用 LDAP 服务器来作为证书或 CRL 发布点，这时就需要指定 LDAP 服务器的位置。

(7) 验证 CA 根证书时使用的指纹

CA 根证书的指纹，即根证书内容的散列值，该值对于每一个证书都是唯一的。PKI 域中可以指定验证 CA 根证书时使用的指纹，缺省情况下未指定该指纹。

当设备从 CA 获得根证书时，可能需要验证 CA 根证书的指纹，具体包括以下两种情况：

- 通过命令获取 CA 证书或者导入 CA 证书，如果获取到的 CA 证书链中包含了设备上没有的 CA 根证书，需要验证 CA 根证书的指纹。如果 PKI 域中指定了验证根证书的指纹，且设备获取到的 CA 根证书的指纹与在 PKI 域中指定的指纹不同，则设备将拒绝接收该 CA 根证书，继而相应的获取 CA 证书或者导入 CA 证书操作会失败；如果 PKI 域中未指定验证根证书的指纹，则会提示用户自行验证根证书指纹。

- 当 IKE 协商等应用触发设备进行本地证书申请时，如果配置的证书申请方式为自动方式，且本地没有 CA 证书，设备会自动从 CA 服务器上获取 CA 证书。如果获取到的 CA 证书链中包含了设备上没有的 CA 根证书，则需要验证 CA 根证书的指纹。如果 PKI 域中指定了验证根证书的指纹，且设备获取到的 CA 根证书的指纹与在 PKI 域中指定的指纹不同，则设备将拒绝接收该 CA 根证书，继而本地证书申请的操作会失败。如果 PKI 域中未指定验证根证书的指纹，则本地证书申请的操作会失败。

(8) 证书申请使用的密钥对

密钥对的产生是证书申请过程中重要的一步。申请过程使用了一对主机密钥：私钥和公钥。私钥由用户保留，公钥和其它信息则交由 CA 进行签名，从而产生证书。在 PKI 域中可以引用三种算法的密钥对，分别为 DSA 密钥对、RSA 密钥对。有关 DSA 和 RSA 密钥对的具体配置请参见“安全配置指导”中的“公钥管理”。申请证书前必须指定使用的密钥对，但该密钥对不必已经存在。申请过程中，如果指定的密钥对不存在，PKI 实体可以根据指定的名字、算法和密钥模数长度生成相应的密钥对。

(9) 证书的扩展用途

设备支持的证书扩展用途包括以下几种：

- IKE 使用
- SSL 客户端使用
- SSL 服务器端使用

证书申请中会带有指定的证书扩展用途，但最终签发的证书中带有哪些扩展用途，由 CA 自己的策略决定，可能与 PKI 域中指定的配置不完全一致。应用程序（例如 IKE，SSL）认证过程中是否会使用这些用途，由应用程序的策略决定。

(10) 本地 PKI 操作产生的协议报文使用的源 IP 地址

如果希望 PKI 实体操作产生的 PKI 协议报文的源 IP 地址是一个特定的地址，例如当 CA 服务器上的策略要求仅接受来自指定地址或网段的证书申请时，则需要通过配置指定该地址。

表1-3 配置 PKI 域

配置任务	命令	说明
进入系统视图	**system-view**	-
创建一个PKI域，并进入PKI域视图	**pki domain** *domain-name*	缺省情况下，不存在PKI 域
配置设备信任的CA名称	**ca identifier** *name*	获取本地证书之前，若当前的PKI域中没有CA证书，则需要首先获取CA证书。获取CA证书之前，必须配置信任的CA名称 缺省情况下，未配置信任的CA名称
指定用于申请证书的PKI实体名称	**certificate request entity** *entity-name*	缺省情况下，未指定用于申请证书的PKI实体名称
配置证书申请的注册受理机构	**certificate request from** { **ca** | **ra** }	缺省情况下，未指定证书申请的注册受理机构
配置注册受理机构服务器的URL	**certificate request url** *url-string* [**vpn-instance** *vpn-instance-name*]	缺省情况下，未指定注册受理机构服务器的URL

配置任务		命令	说明
（可选）配置证书申请状态查询的周期和最大次数		**certificate request polling** { **count** *count* | **interval** *minutes* }	缺省情况下，证书申请查询间隔为20分钟，最多查询50次
指定LDAP服务器		**ldap-server host** *hostname* [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]	需要通过LDAP协议获取证书时，此配置必选；需要通过LDAP协议获取CRL时，如果CRL的URL中未包含发布点地址信息，则此配置必选 缺省情况下，未指定LDAP服务器
配置验证CA根证书时使用的指纹		非FIPS模式下： **root-certificate fingerprint** { **md5** | **sha1** } *string* FIPS模式下： **root-certificate fingerprint sha1** *string*	当证书申请方式为自动方式时，此配置必选；当证书申请方式为手工方式时，此配置可选，若不配置，需要用户自行验证根证书指纹 缺省情况下，未指定验证根证书时使用的指纹
（二者选其一）指定证书申请时使用的密钥对	指定RSA密钥对	**public-key rsa** { { **encryption name** *encryption-key-name* [**length** *key-length*] | **signature name** *signature-key-name* [**length** *key-length*] } * | **general name** *key-name* [**length** *key-length*] }	缺省情况下，未指定所使用的密钥对
	指定DSA密钥对	**public-key dsa name** *key-name* [**length** *key-length*]	
（可选）指定证书的扩展用途		**usage** { **ike** | **ssl-client** | **ssl-server** } *	缺省情况下，证书可用于所有用途
（二者可选其一）指定PKI操作产生的协议报文使用的源IP地址		**source ip** { *ip-address* | **interface** {*interface-type interface-number* }	缺省情况下，PKI操作产生的协议报文的源IP地址为系统根据路由查找到的出接口的地址
		source ipv6 { *ipv6-address* | **interface** { *interface-type interface-number* }}	

1.5 申请证书

申请证书的过程就是 PKI 实体向 CA 自我介绍的过程。PKI 实体向 CA 提供身份信息，以及相应的公钥，这些信息将成为颁发给该 PKI 实体证书的主要组成部分。PKI 实体向 CA 提出证书申请，有离线和在线两种方式。

- 离线申请方式下，CA 允许申请方通过带外方式（如电话、磁盘、电子邮件等）向 CA 提供申请信息。
- 在线申请方式下，实体通过 SCEP 协议向 CA 提交申请信息。在线申请有自动申请和手工申请两种方式。下文将详细介绍这两种方式的具体配置。

1.5.1 自动申请证书

提示

- 申请证书之前必须保证设备的系统时钟与 CA 的时钟同步，否则设备可能会错误地认为证书不在有效期内，导致申请证书失败。调整系统时钟的方法请参见“基础配置指导”中的“设备管理”。
- 对于系统自动申请到的证书，当它们即将过期时或正式过期后，系统不会自动向 CA 发起重新申请。这种情况下，可能会由于证书过期造成应用协议的业务中断。

配置证书申请方式为自动方式后，当有应用协议与 PKI 联动时，如果应用协议中的 PKI 实体无本地证书（例如，IKE 协商采用数字签名方法进行身份认证，但在协商过程中没有发现本地证书），则 PKI 实体自动通过 SCEP 协议向 CA 发起证书申请，并在申请成功后将本地证书获取到本地保存。在证书申请之前，若当前的 PKI 域中没有 CA 证书，也会首先自动获取 CA 证书。在申请过程中，如果指定的密钥对不存在，则 PKI 实体根据 PKI 域中指定的名字、算法和长度生成相应的密钥对。需要注意的是，本地证书已存在的情况下，为保证密钥对与现存证书的一致性，不建议执行命令 **public-key local create** 或 **public-key local destroy** 创建或删除与现存证书使用的密钥对相同名称的密钥对，否则会导致现存证书不可用。若要重新申请本地证书，必须首先删除本地证书，然后再执行 **public-key local create** 命令生成新的密钥对或使用命令 **public-key local destroy** 删除旧的密钥对。有关公钥相关命令的详细介绍，请参见“安全命令参考”中的“公钥管理”。

表1-4 自动申请证书

操作	命令	说明
进入系统视图	**system-view**	-
进入PKI域视图	**pki domain** *domain-name*	-
配置证书申请为自动方式	**certificate request mode auto** [**password** { **cipher** | **simple** } *password*]	缺省情况下，证书申请为手工方式 证书申请为自动方式时，可以指定吊销证书时使用的口令 *password*，是否需要指定口令是由CA服务器的策略决定的

1.5.2 手工申请证书

提示

申请证书之前必须保证设备的系统时钟与 CA 的时钟同步，否则设备可能会错误地认为证书不在有效期内，导致申请证书失败。调整系统时钟的方法请参见“基础配置指导”中的“设备管理”。

配置证书申请方式为手工方式后，需要手工执行申请本地证书的操作。手工申请成功后，设备将把申请到的本地证书自动获取到本地保存。

1. 配置限制和指导

- 一个 PKI 域中，只能存在 DSA 或 RSA 中一种密钥算法类型的本地证书。采用 DSA 算法时，一个 PKI 域中最多只能同时申请和存在一个本地证书；采用 RSA 算法时，一个 PKI 域中最多只能同时申请和存在一个用途为签名的 RSA 算法本地证书和一个用途为加密的 RSA 算法本地证书。
- 如果一个 PKI 域中已存在一个本地证书，为保证密钥对与现存证书的一致性，不建议执行命令 **public-key local create** 或 **public-key local destroy** 创建或删除与现存证书使用的密钥对相同名称的密钥对，否则会导致现存证书不可用。若要重新申请本地证书，必须首先删除本地证书，然后再执行 **public-key local create** 命令生成新的密钥对或使用命令 **public-key local destroy** 删除旧的密钥对。有关该命令的详细介绍，请参见“安全命令参考”中的“公钥管理”。
- 如果一个 PKI 域中已存在一个本地证书，则不允许再手工执行在线证书申请操作申请一个与其互斥的证书，以避免因相关配置的修改使得证书与注册信息不匹配。若想重新申请，请先使用 **pki delete-certificate** 命令删除本地证书，然后再执行 **pki request-certificate domain** 命令。
- 当无法通过 SCEP 协议向 CA 在线申请证书时，可以首先通过执行命令 **pki request-certificate domain pkcs10** 打印出证书申请信息到终端上，或者通过执行指定 **pki request-certificate domain pkcs10 filename** 将证书申请信息保存到指定的文件中，然后再通过带外方式将这些本地证书申请信息发送给 CA 进行证书申请。

2. 配置准备

在手工申请本地证书之前，必须保证当前的 PKI 域中已经存在 CA 证书且指定了证书申请时使用的密钥对。

- PKI 域中的 CA 证书用来验证获取到的本地证书的真实性和合法性。在证书申请之前，若 PKI 域中没有 CA 证书，则需要手工获取 CA 证书。
- PKI 域中指定的密钥对用于为 PKI 实体申请本地证书，其中的公钥和其他信息交由 CA 进行签名，从而产生本地证书。

3. 配置步骤

表1-5 手工申请证书

操作	命令	说明
进入系统视图	**system-view**	-
进入PKI域视图	**pki domain** *domain-name*	-
配置证书申请为手工方式	**certificate request mode manual**	缺省情况下，证书申请为手工方式
退回系统视图	**quit**	-
手工获取CA证书	请参见1.7	-
手工申请本地证书或生成PKCS#10证书申请	**pki request-certificate domain** *domain-name* [**password** *password*] [**pkcs10** [**filename** *filename*]]	此命令不会被保存在配置文件中 执行本命令时，如果本地不存在PKI域所指定的密钥对，则系统会根据PKI域中指定的名字、算法和长度自动生成对应的密钥对

1.6 停止证书申请过程

用户可以通过此配置停止正在进行中的证书申请过程。用户在证书申请时，可能由于某种原因需要改变证书申请的一些参数，比如通用名、国家代码、FQDN 等，而此时证书申请过程正在进行，为了新的申请不与之前的申请发生冲突，建议先停止之前的申请，再进行新的申请。可以通过 **display pki certificate request-status** 命令查询正在进行中的证书申请过程。

另外，删除 PKI 域也可以停止对应的证书申请过程。

表1-6 停止证书申请过程

操作	命令	说明
进入系统视图	**system-view**	-
停止证书申请过程	**pki abort-certificate-request domain** *domain-name*	此命令不会被保存在配置文件中

1.7 手工获取证书

获取证书的目的是：将 CA 签发的与 PKI 实体所在 PKI 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 证书发布点查询的次数。

用户通过此配置可以将已存在的 CA 证书、本地证书或者外部 PKI 实体证书获取至本地保存。获取证书有两种方式：离线导入方式和在线方式。

- 离线导入方式：通过带外方式（如 FTP、磁盘、电子邮件等）取得证书，然后将其导入至本地。如果设备所处的环境中没有证书的发布点、CA 服务器不支持通过 SCEP 协议与设备交互、或者证书对应的密钥对由 CA 服务器生成，则可采用此方式获取证书。
- 在线方式：从证书发布服务器上在线获取证书并下载至本地，包括通过 SCEP 协议获取 CA 证书和通过 LDAP 协议获取本地或对端证书。

1. 配置限制和指导

- 如果本地已有 CA 证书存在，则不允许执行在线方式获取 CA 证书的操作。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，再执行获取 CA 证书的命令。
- 如果 PKI 域中已经有本地证书或对端证书，仍然允许执行在线方式获取本地证书或对端证书，获取到的证书直接覆盖已有证书。但对于 RSA 算法的证书而言，一个 PKI 域中可以存在一个签名用途的证书和一个加密用途的证书，不同用途的证书不会相互覆盖。
- 如果使能了 CRL 检查，手工获取证书时会触发 CRL 检查，如果 CRL 检查时发现待获取的证书已经吊销，则获取证书失败。
- 设备根据自身的系统时间来判断当前的证书是否还在其有效期内，设备系统时间不准确可能导致设备对于证书有效期的判断出现误差或错误，例如认为实际还在有效期内证书已过期，因此请确保设备系统时间的准确性。

2. 配置准备

获取本地证书或对端证书之前必须完成以下操作：

- 在线获取本地证书和对端证书是通过 LDAP 协议进行的，因此在线获取本地证书或对端证书之前必须完成 PKI 域中指定 LDAP 服务器的配置。
- 离线导入证书之前，需要通过 FTP、TFTP 等协议将证书文件传送到设备的存储介质中。如果设备所处的环境不允许使用 FTP、TFTP 等协议，则可以直接采用在终端上粘贴证书内容的方式导入，但是粘贴的证书必须是 PEM（Privacy Enhanced Mail，增强保密邮件）格式的，因为只有 PEM 格式的证书内容为可打印字符。
- 只有存在签发本地证书的 CA 证书链才能成功导入本地证书，这里的 CA 证书链可以是保存在 PKI 域中的，也可以是本地证书中携带的。若设备和本地证书中都没有 CA 证书链，则需要预先获取到 CA 证书链。导入对端证书时，需要满足的条件与导入本地证书相同。
- 离线导入含有被加密的密钥对的本地证书时，需要输入加密口令。请提前联系 CA 服务器管理员取得该口令。

3. 配置步骤

表1-7 手工获取证书

操作		命令	说明
进入系统视图		**system-view**	-
手工获取证书	离线导入方式	**pki import domain** *domain-name* { **der** { **ca** | **local** | **peer** } **filename** *filename* | **p12 local filename** *filename* | **pem** { **ca** | **local** | **peer** } [**filename** *filename*] }	**pki retrieve-certificate**命令不会被保存在配置文件中
	在线方式	**pki retrieve-certificate domain** *domain-name* { **ca** | **local** | **peer** *entity-name* }	

1.8 配置证书验证

在使用每一个证书之前，必须对证书进行验证。证书验证包括检查本地、CA 证书是否由可信的 CA 签发，证书是否在有效期内，证书是否未被吊销。申请证书、获取证书以及应用程序使用 PKI 功能时，都会自动对证书进行验证，因此一般不需要使用命令行手工进行证书验证。如果用户希望在没有任何前述操作的情况下单独执行证书的验证，可以手工执行证书验证。

配置证书验证时可以设置是否必须进行 CRL 检查。CRL 检查的目的是查看 PKI 实体的证书是否被 CA 吊销，若检查结果表明 PKI 实体的证书已经被吊销，那么该证书就不再被其它 PKI 实体信任。

- 如果配置为使能 CRL 检查，则需要首先从 CRL 发布点获取 CRL。PKI 域中未配置 CRL 发布点的 URL 时，从该待验证的证书中获取发布点信息：优先获取待验证的证书中记录的发布点，如果待验证的证书中没有记录发布点，则获取 CA 证书中记录的发布点（若待验证的证书为 CA 证书，则获取上一级 CA 证书中记录的发布点）。如果无法通过任何途径得到发布点，则通过 SCEP 协议获取 CRL。由于设备通过 SCEP 获取 CRL 是在获取到 CA 证书和本地证书之后进行，因此该方式下必须保证设备已经获取到 CA 证书和本地证书。使能了 CRL 检查的情况下，如果 PKI 域中不存在相应的 CRL、CRL 获取失败、或者 CRL 检查时发现待获取的证书已经吊销，则手动申请证书、获取证书的操作将会失败。
- 如果配置为不使能 CRL 检查，则不需要获取 CRL。

需要注意的是，验证一个 PKI 域中的 CA 证书时，系统会逐级验证本域 CA 证书链上的所有 CA 证书的有效性，因此需要保证设备上存在该 CA 证书链上的所有上级 CA 证书所属的 PKI 域。验证某一级 CA 证书时，系统会根据该 CA 证书的签发者名（IssuerName）查找对应的上一级 CA 证书，以及上一级 CA 证书所属的（一个或多个）PKI 域。若查找到了相应的 PKI 域，且该 PKI 域中使能了 CRL 检查，则根据该 PKI 域中的配置对待验证的 CA 证书进行吊销检查，否则不检查待验证的 CA 证书是否被吊销。检查 CA 证书链中的 CA（根 CA 除外）是否被吊销后，从根 CA 逐级验证 CA 证书链的签发关系。

1.8.1 配置使能CRL检查的证书验证

表1-8 配置使能 CRL 检查的证书验证

操作	命令	说明
进入系统视图	**system-view**	-
进入PKI域视图	**pki domain** *domain-name*	-
（可选）配置CRL发布点的URL	**crl url** *url-string* [**vpn-instance** *vpn-instance-name*]	缺省情况下，未指定CRL发布点的URL
使能CRL检查	**crl check enable**	缺省情况下，CRL检查处于开启状态
退回系统视图	**quit**	-
获取CA证书	请参见1.7	在进行本地证书验证操作之前必须首先获取CA证书
（可选）获取CRL并下载至本地	**pki retrieve-crl domain** *domain-name*	验证非根CA证书和本地证书时，如果PKI域中没有CRL，系统会自动获取CRL再进行验证；如果PKI域已经存在CRL，则可以继续获取CRL，获取到的新CRL会覆盖已有CRL 获取到的CRL不一定是本域CA签发的，但肯定是本域CA证书链上的一个CA证书签发的
验证证书的有效性	**pki validate-certificate domain** *domain-name* { **ca** | **local** }	-

1.8.2 配置不使能CRL检查的证书验证

表1-9 配置不使能 CRL 检查的证书验证

操作	命令	说明
进入系统视图	**system-view**	-
进入PKI域视图	**pki domain** *domain-name*	-
禁止CRL检查	**undo crl check enable**	缺省情况下，CRL检查处于开启状态

操作	命令	说明
退回系统视图	**quit**	-
获取CA证书	请参见1.7	在进行本地证书验证操作之前必须首先获取CA证书
验证证书的有效性	**pki validate-certificate domain** *domain-name* { **ca** | **local** }	此命令不会被保存在配置文件中

1.9 配置证书和CRL的存储路径

注意

重新配置了证书或 CRL 的存储路径后为了防止证书或 CRL 文件的丢失，重启或关闭设备前一定要保存配置。

获取到本地的证书和CRL有默认存储路径，但同时也允许用户根据自己的需要修改证书文件和CRL文件的存储路径。证书和 CRL 的存储路径可以指定为不同的路径。

修改了证书或 CRL 的存储目录后，原存储路径下的证书文件（以.cer 和.p12 为后缀的文件）和 CRL 文件（以.crl 为后缀的文件）将被移动到新路径下保存。

表1-10 配置证书和 CRL 的存储路径

操作	命令	说明
进入系统视图	**system-view**	-
配置证书和CRL的存储路径	**pki storage** { **certificates** | **crls** } *dir-path*	缺省情况下，证书和CRL的存储路径为设备存储介质上的PKI目录 对于MSR 5600，*dir-path*只能是当前主控板上的路径，不能是其它主控板上的路径

1.10 导出证书

提示

以 PKCS12 格式导出所有证书时，PKI 域中必须有本地证书，否则会导出失败。

PKI 域中已存在的 CA 证书、本地证书可以导出到文件中保存或导出到终端上显示，导出的证书可以用于证书备份或供其它设备使用。

- 导出证书时若不指定文件名，则表示要将证书导出到终端上显示，这种方式仅 PEM 格式的证书才支持。

- 导出证书时若指定文件名，则表示证书将导出到指定文件中保存。导出 RSA 算法类型的本地证书时，设备上实际保存证书的证书文件名称并不一定是用户指定的名称，它与本地证书的密钥对用途相关，具体的命名规则请参见命令手册。

表1-11 导出证书

操作	命令	说明
进入系统视图	**system-view**	-
导出DER格式的证书	**pki export domain** *domain-name* **der** { **all** | **ca** | **local** } **filename** *filename*	根据需要选择其中一个或多个
导出PKCS12格式的证书	**pki export domain** *domain-name* **p12** { **all** | **local** } **passphrase** *p12passwordstring* **filename** *filename*	
导出PEM格式的证书	**pki export domain** *domain-name* **pem** { { **all** | **local** } [{ **3des-cbc** | **aes-128-cbc** | **aes-192-cbc** | **aes-256-cbc** | **des-cbc** } *pempasswordstring*] | **ca** } [**filename** *filename*]	

1.11 删除证书

注意

删除 CA 证书时将同时删除所在 PKI 域中的本地证书、所有对端证书以及 CRL。

由 CA 颁发的证书都会设置有效期，证书生命周期的长短由签发证书的 CA 来确定。当用户的私钥被泄漏或证书的有效期快到时，应该重新申请新的证书。证书过期或希望重新申请证书时，可以通过此配置删除已经存在的本地证书、CA 证书或对端证书。

重新申请证书之前，应该先使用命令 **public-key local destroy** 删除旧的密钥对，再使用 **public-key local create** 生成新的密钥对。相关命令的详细介绍可参考“安全命令参考”中的“公钥管理”。

表1-12 配置删除证书

操作	命令	说明
进入系统视图	**system-view**	-
配置删除证书	**pki delete-certificate domain** *domain-name* { **ca** | **local** | **peer** [**serial** *serial-num*] }	如果没有指定序列号，则删除所有对端证书

1.12 配置证书访问控制策略

通过配置证书的访问控制策略，可以对安全应用中的用户访问权限进行进一步的控制，保证了与之通信的服务器端的安全性。例如，在 HTTPS（Hypertext Transfer Protocol Secure，超文本传输协议的安全版本）应用中，HTTPS 服务器可以通过引用证书访问控制策略，根据自身的安全需要对客户端的证书合法性进行检测。

一个证书访问控制策略中可以定义多个证书属性的访问控制规则（通过 **rule** 命令配置），每一个访问控制规则都与一个证书属性组关联。一个证书属性组是一系列属性规则（通过 **attribute** 命令配置）的集合，这些属性规则是对证书的颁发者名、主题名以及备用主题名进行过滤的匹配条件。

如果一个证书中的相应属性能够满足一条访问控制规则所关联的证书属性组中所有属性规则的要求，则认为该证书和该规则匹配。如果一个证书访问控制策略中有多个规则，则按照规则编号从小到大的顺序遍历所有规则，一旦证书与某一个规则匹配，则立即结束检测，不再继续匹配其它规则。

规则的匹配结果决定了证书的有效性，具体如下：

- 如果证书匹配到的规则中指定了 **permit** 关键字，则该证书将被认为通过了访问控制策略的检测且有效。
- 如果证书匹配到的规则中指定了 **deny** 关键字，则该证书将被认为未通过访问控制策略的检测且无效。
- 若遍历完所有规则后，证书没有与任何规则匹配，则该证书将因不能通过访问控制策略的检测而被认为无效。
- 若证书访问控制策略下某访问控制规则关联的证书属性组不存在，或者该证书属性组没有配置任何属性，则认为被检测的证书都能够与此规则匹配。
- 若安全应用（如 HTTPS）引用的证书访问控制策略不存在，则认为该应用中被检测的证书有效。

表1-13 配置证书访问控制策略

操作	命令	说明
进入系统视图	**system-view**	-
创建证书属性组，并进入证书属性组视图	**pki certificate attribute-group** *group-name*	缺省情况下，不存在证书属性组
（可选）配置证书颁发者名、证书主题名及备用主题名的属性规则	**attribute** *id* { **alt-subject-name** { **fqdn** | **ip** } | { **issuer-name** | **subject-name** } { **dn** | **fqdn** | **ip** } } { **ctn** | **equ** | **nctn** | **nequ**} *attribute-value*	缺省情况下，对证书颁发者名、证书主题名及备用主题名没有限制
退回系统视图	**quit**	-
创建证书访问控制策略，并进入证书访问控制策略视图	**pki certificate access-control-policy** *policy-name*	缺省情况下，不存在证书访问控制策略
配置证书属性的访问控制规则	**rule** [*id*] { **deny** | **permit** } *group-name*	缺省情况下，不存在证书属性的访问控制规则，认为所有证书都可以通过该控制策略的过滤 一个证书访问控制策略中可配置多个访问控制规则

1.13 PKI显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 PKI 的运行情况，通过查看显示信息验证配置的效果。

表1-14 PKI 显示和维护

操作	命令
显示证书内容	**display pki certificate domain** *domain-name* { **ca** | **local** | **peer** [**serial** *serial-num*] }
显示证书申请状态	**display pki certificate request-status** [**domain** *domain-name*]
显示存储在本地的CRL	**display pki crl domain** *domain-name*
显示证书属性组的配置信息	**display pki certificate attribute-group** [*group-name*]
显示证书访问控制策略的配置信息	**display pki certificate access-control-policy** [*policy-name*]

1.14 PKI典型配置举例

提示

- 当采用 Windows Server 作为 CA 时，需要安装 SCEP 插件。在这种情况下，配置 PKI 域时，需要使用 **certificate request from ra** 命令指定 PKI 实体从 RA 注册申请证书。
- 当采用 RSA Keon 软件时，不需要安装 SCEP 插件。在这种情况下，配置 PKI 域时，需要使用 **certificate request from ca** 命令指定 PKI 实体从 CA 注册申请证书。
- 当采用 OpenCA 软件时，需要启用 SCEP 功能，在这种情况下，配置 PKI 域时，需要使用 **certificate requeset from ra** 命令指定 PKI 实体从 RA 注册申请证书。

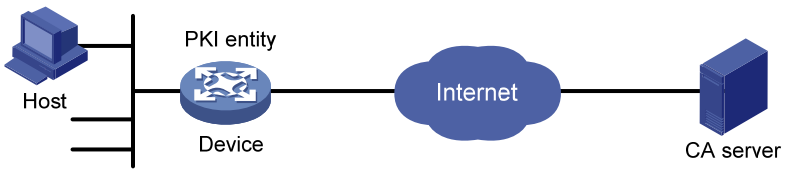
1.14.1 PKI实体向CA申请证书（采用RSA Keon CA服务器）

1. 组网需求

配置 PKI 实体 Device 向 CA 服务器申请本地证书。

2. 组网图

图1-3 PKI 实体向 CA 申请证书组网图



3. 配置步骤

(1) 配置 CA 服务器

- 创建 CA 服务器 myca

在本例中，CA 服务器上首先需要进行基本属性 Nickname 和 Subject DN 的配置。其它属性选择默认值。其中，Nickname 为可信任的 CA 名称（本例中为 myca），Subject DN 为 CA 的 DN 属性，包括 CN、OU、O 和 C。

- 配置扩展属性

基本属性配置完毕之后，还需要在生成的 CA 服务器管理页面上对“Jurisdiction Configuration”进行配置，主要内容包括：根据需要选择合适的扩展选项；启动自动颁发证书功能；添加可以自动颁发证书的地址范围。

以上配置完成之后，还需要保证设备的系统时钟与 CA 的时钟同步才可以正常使用设备来申请证书和获取 CRL。

(2) 配置 Device

- 配置 PKI 实体

配置 PKI 实体名称为 aaa，通用名为 Device。

```
<Device> system-view
[Device] pki entity aaa
[Device-pki-entity-aaa] common-name Device
[Device-pki-entity-aaa] quit
```

- 配置 PKI 域

创建并进入 PKI 域 torsa。

```
[Device] pki domain torsa
```

配置设备信任的 CA 的名称为 myca。

```
[Device-pki-domain-torsa] ca identifier myca
```

配置注册受理机构服务器的 URL，格式为 http://host:port/Issuing Jurisdiction ID。其中的 Issuing Jurisdiction ID 为 CA 服务器上生成的 16 进制字符串。

```
[Device-pki-domain-torsa] certificate request url
http://1.1.2.22:446/80f6214aa8865301d07929ae481c7ceed99f95bd
```

配置证书申请的注册受理机构为 CA。

```
[Device-pki-domain-torsa] certificate request from ca
```

指定 PKI 实体名称为 aaa。

```
[Device-pki-domain-torsa] certificate request entity aaa
```

配置 CRL 发布点位置。

```
[Device-pki-domain-torsa] crl url ldap://1.1.2.22:389/CN=myca
```

指定证书申请使用的密钥对，用途为通用，名称为 abc，密钥对长度为 1024 比特。

```
[Device-pki-domain-torsa] public-key rsa general name abc length 1024
[Device-pki-domain-torsa] quit
```

- 生成 RSA 算法的本地密钥对

```
[Device] public-key local create rsa name abc
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512,it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.........................++++++
.....................................++++++
Create the key pair successfully.
```

- 证书申请

获取 CA 证书并下载至本地。

```
[Device] pki retrieve-certificate domain torsa ca
The trusted CA's finger print is:
    MD5  fingerprint:EDE9 0394 A273 B61A F1B3 0072 A0B1 F9AB
    SHA1 fingerprint: 77F9 A077 2FB8 088C 550B A33C 2410 D354 23B2 73A8
Is the finger print correct?(Y/N):y
Retrieved the certificates successfully.
```

手工申请本地证书。（采用 RSA Keon CA 服务器申请证书时，必须指定 password 参数）

```
[Device] pki request-certificate domain torsa password 1111
Start to request the general certificate ...
……
Certificate requested successfully.
```

4. 验证配置

通过以下显示命令可以查看申请到的本地证书信息。

```
[Device] display pki certificate domain torsa local
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            15:79:75:ec:d2:33:af:5e:46:35:83:bc:bd:6e:e3:b8
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=myca
        Validity
            Not Before: Jan  6 03:10:58 2013 GMT
            Not After : Jan  6 03:10:58 2014 GMT
        Subject: CN=Device
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:ab:45:64:a8:6c:10:70:3b:b9:46:34:8d:eb:1a:
                    a1:b3:64:b2:37:27:37:9d:15:bd:1a:69:1d:22:0f:
                    3a:5a:64:0c:8f:93:e5:f0:70:67:dc:cd:c1:6f:7a:
                    0c:b1:57:48:55:81:35:d7:36:d5:3c:37:1f:ce:16:
                    7e:f8:18:30:f6:6b:00:d6:50:48:23:5c:8c:05:30:
                    6f:35:04:37:1a:95:56:96:21:95:85:53:6f:f2:5a:
                    dc:f8:ec:42:4a:6d:5c:c8:43:08:bb:f1:f7:46:d5:
                    f1:9c:22:be:f3:1b:37:73:44:f5:2d:2c:5e:8f:40:
                    3e:36:36:0d:c8:33:90:f3:9b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 CRL Distribution Points:

                Full Name:
                  DirName: CN = myca

    Signature Algorithm: sha1WithRSAEncryption
        b0:9d:d9:ac:a0:9b:83:99:bf:9d:0a:ca:12:99:58:60:d8:aa:
```

```
73:54:61:4b:a2:4c:09:bb:9f:f9:70:c7:f8:81:82:f5:6c:af:
25:64:a5:99:d1:f6:ec:4f:22:e8:6a:96:58:6c:c9:47:46:8c:
f1:ba:89:b8:af:fa:63:c6:c9:77:10:45:0d:8f:a6:7f:b9:e8:
25:90:4a:8e:c6:cc:b8:1a:f8:e0:bc:17:e0:6a:11:ae:e7:36:
87:c4:b0:49:83:1c:79:ce:e2:a3:4b:15:40:dd:fe:e0:35:52:
ed:6d:83:31:2c:c2:de:7c:e0:a7:92:61:bc:03:ab:40:bd:69:
1b:f5
```

关于获取到的 CA 证书的详细信息可以通过相应的显示命令来查看，此处略。具体内容请参考命令**display pki certificate domain**。

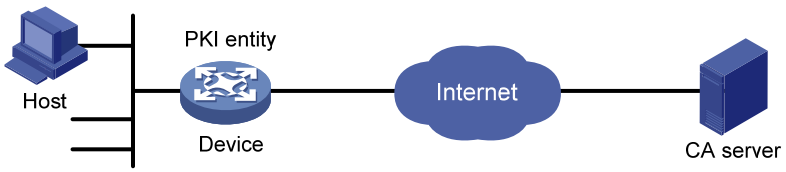
1.14.2 PKI实体向CA申请证书（采用Windows 2003 server CA服务器）

1. 组网需求

配置 PKI 实体 Device 向 CA 服务器申请本地证书。

2. 组网图

图1-4 PKI 实体向 CA 申请证书组网图



3. 配置步骤

(1) 配置 CA 服务器

- 安装证书服务器组件

打开[控制面板]/[添加/删除程序]，选择[添加/删除 Windows 组件]中的“证书服务”进行安装。安装过程中设置 CA 的名称，该名称为信任的 CA 的名称（本例中为 myca）。

- 安装 SCEP 插件

由于 Windows 2003 server 作为 CA 服务器时，缺省情况下不支持 SCEP，所以需要安装 SCEP 插件，才能使设备具备证书自动注册、获取等功能。插件安装完毕后，弹出提示框，提示框中的 URL 地址即为设备上配置的注册服务器地址。

- 修改证书服务的属性

完成上述配置后，打开[控制面板/管理工具]中的[证书颁发机构]，如果安装成功，在[颁发的证书]中将存在两个 CA 颁发给 RA 的证书。选择[CA server 属性]中的“策略模块”的属性为“如果可以的话，按照证书模板中的设置。否则，将自动颁发证书(F)。”

- 修改 IIS 服务的属性

打开[控制面板/管理工具]中的[Internet 信息服务(IIS)管理器]，将[默认网站 属性]中“主目录”的本地路径修改为证书服务保存的路径。另外，为了避免与已有的服务冲突，建议修改默认网站的 TCP 端口号为未使用的端口号（本例中为 8080）。

以上配置完成之后，还需要保证设备的系统时钟与 CA 的时钟同步才可以正常使用设备来申请证书。

(2) 配置 Device

- 配置 PKI 实体

配置 PKI 实体名称为 aaa，通用名为 test。

```
<Device> system-view
[Device] pki entity aaa
[Device-pki-entity-aaa] common-name test
[Device-pki-entity-aaa] quit
```

- 配置 PKI 域

创建并进入 PKI 域 winserver。

```
[Device] pki domain winserver
```

配置设备信任的 CA 的名称为 myca。

```
[Device-pki-domain-winserver] ca identifier myca
```

配置注册受理机构服务器的 URL，格式为 http://host:port/certsrv/mscep/mscep.dll。其中，host:port 为 CA 服务器的主机地址和端口号。

```
[Device-pki-domain-winserver] certificate request url
http://4.4.4.1:8080/certsrv/mscep/mscep.dll
```

配置证书申请的注册受理机构为 RA。

```
[Device-pki-domain-winserver] certificate request from ra
```

指定 PKI 实体名称为 aaa。

```
[Device-pki-domain-winserver] certificate request entity aaa
```

指定证书申请使用的密钥对，用途为通用，名称为 abc，密钥长度为 1024 比特。

```
[Device-pki-domain-winserver] public-key rsa general name abc length 1024
[Device-pki-domain-winserver] quit
```

- 生成 RSA 算法的本地密钥对

```
[Device] public-key local create rsa name abc
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512,it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.........................++++++
.....................................++++++
Create the key pair successfully.
```

- 证书申请

获取 CA 证书并下载至本地。

```
[Device] pki retrieve-certificate domain winserver ca
The trusted CA's finger print is:
    MD5  fingerprint:766C D2C8 9E46 845B 4DCE 439C 1C1F 83AB
    SHA1 fingerprint:97E5 DDED AB39 3141 75FB DB5C E7F8 D7D7 7C9B 97B4
Is the finger print correct?(Y/N):y
Retrieved the certificates successfully.
```

手工申请本地证书。

```
[Device] pki request-certificate domain winserver
Start to request the general certificate ...
……
Certificate requested successfully.
```

4. 验证配置

通过以下显示命令可以查看申请到的本地证书信息。

```
[Device] display pki certificate domain winserver local
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
             (Negative)01:03:99:ff:ff:ff:ff:fd:11
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=h3c
        Validity
            Not Before: Dec 24 07:09:42 2012 GMT
            Not After : Dec 24 07:19:42 2013 GMT
        Subject: CN=test
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c3:b5:23:a0:2d:46:0b:68:2f:71:d2:14:e1:5a:
                    55:6e:c5:5e:26:86:c1:5a:d6:24:68:02:bf:29:ac:
                    dc:31:41:3f:5d:5b:36:9e:53:dc:3a:bc:0d:11:fb:
                    d6:7d:4f:94:3c:c1:90:4a:50:ce:db:54:e0:b3:27:
                    a9:6a:8e:97:fb:20:c7:44:70:8f:f0:b9:ca:5b:94:
                    f0:56:a5:2b:87:ac:80:c5:cc:04:07:65:02:39:fc:
                    db:61:f7:07:c6:65:4c:e4:5c:57:30:35:b4:2e:ed:
                    9c:ca:0b:c1:5e:8d:2e:91:89:2f:11:e3:1e:12:8a:
                    f8:dd:f8:a7:2a:94:58:d9:c7:f8:1a:78:bd:f5:42:
                    51:3b:31:5d:ac:3e:c3:af:fa:33:2c:fc:c2:ed:b9:
                    ee:60:83:b3:d3:e5:8e:e5:02:cf:b0:c8:f0:3a:a4:
                    b7:ac:a0:2c:4d:47:5f:39:4b:2c:87:f2:ee:ea:d0:
                    c3:d0:8e:2c:80:83:6f:39:86:92:98:1f:d2:56:3b:
                    d7:94:d2:22:f4:df:e3:f8:d1:b8:92:27:9c:50:57:
                    f3:a1:18:8b:1c:41:ba:db:69:07:52:c1:9a:3d:b1:
                    2d:78:ab:e3:97:47:e2:70:14:30:88:af:f8:8e:cb:
                    68:f9:6f:07:6e:34:b6:38:6a:a2:a8:29:47:91:0e:
                    25:39
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment, Data Encip
herment
            X509v3 Subject Key Identifier:
                C9:BB:D5:8B:02:1D:20:5B:40:94:15:EC:9C:16:E8:9D:6D:FD:9F:34
            X509v3 Authority Key Identifier:
                keyid:32:F1:40:BA:9E:F1:09:81:BD:A8:49:66:FF:F8:AB:99:4A:30:21:9
B

            X509v3 CRL Distribution Points:
```

```
                Full Name:
                  URI:file://\\g07904c\CertEnroll\h3c.crl

            Authority Information Access:
                CA Issuers - URI:http://gc/CertEnroll/gc_h3c.crt
                CA Issuers - URI:file://\\gc\CertEnroll\gc_h3c.crt

            1.3.6.1.4.1.311.20.2:
                .0.I.P.S.E.C.I.n.t.e.r.m.e.d.i.a.t.e.O.f.f.l.i.n.e
    Signature Algorithm: sha1WithRSAEncryption
        76:f0:6c:2c:4d:bc:22:59:a7:39:88:0b:5c:50:2e:7a:5c:9d:
        6c:28:3c:c0:32:07:5a:9c:4c:b6:31:32:62:a9:45:51:d5:f5:
        36:8f:47:3d:47:ae:74:6c:54:92:f2:54:9f:1a:80:8a:3f:b2:
        14:47:fa:dc:1e:4d:03:d5:d3:f5:9d:ad:9b:8d:03:7f:be:1e:
        29:28:87:f7:ad:88:1c:8f:98:41:9a:db:59:ba:0a:eb:33:ec:
        cf:aa:9b:fc:0f:69:3a:70:f2:fa:73:ab:c1:3e:4d:12:fb:99:
        31:51:ab:c2:84:c0:2f:e5:f6:a7:c3:20:3c:9a:b0:ce:5a:bc:
        0f:d9:34:56:bc:1e:6f:ee:11:3f:7c:b2:52:f9:45:77:52:fb:
        46:8a:ca:b7:9d:02:0d:4e:c3:19:8f:81:46:4e:03:1f:58:03:
        bf:53:c6:c4:85:95:fb:32:70:e6:1b:f3:e4:10:ed:7f:93:27:
        90:6b:30:e7:81:36:bb:e2:ec:f2:dd:2b:bb:b9:03:1c:54:0a:
        00:3f:14:88:de:b8:92:63:1e:f5:b3:c2:cf:0a:d5:f4:80:47:
        6f:fa:7e:2d:e3:a7:38:46:f6:9e:c7:57:9d:7f:82:c7:46:06:
        7d:7c:39:c4:94:41:bd:9e:5c:97:86:c8:48:de:35:1e:80:14:
        02:09:ad:08
```

关于获取到的 CA 证书的详细信息可以通过相应的显示命令来查看，此处略。具体内容请参考命令 **display pki certificate domain**。

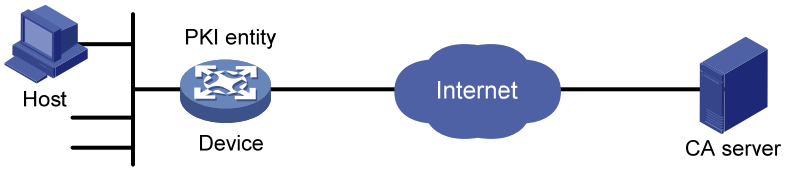
1.14.3 PKI实体向CA申请证书（采用OpenCA服务器）

1. 组网需求

配置 PKI 实体 Device 向 CA 服务器申请本地证书。

2. 组网图

图1-5 PKI 实体向 CA 申请证书组网图



3. 配置步骤

(1) 配置 CA 服务器

配置过程略，具体请参考 Open CA 服务器的相关手册。

需要注意的是：

- 使用 OpenCA 最新版本的 rpm 包进行安装，OpenCA 有多个版本，但只有 0.9.2 以后的版本才支持 SCEP，至少要安装 0.9.2 以后的版本。
- OpenCA 服务器配置完成之后，还需要保证设备的系统时钟与 CA 的时钟同步才可以正常使用设备来申请证书。

(2) 配置 Device

- 配置 PKI 实体

配置 PKI 实体，名称为 aaa、通用名为 rnd、国家码为 CN、组织名为 test、组织部门名为 software。

```
<Device> system-view
[Device] pki entity aaa
[Device-pki-entity-aaa] common-name rnd
[Device-pki-entity-aaa] country CN
[Device-pki-entity-aaa] organization test
[Device-pki-entity-aaa] organization-unit software
[Device-pki-entity-aaa] quit
```

- 配置 PKI 域

创建并进入 PKI 域 openca。

```
[Device] pki domain openca
```

配置设备信任的 CA 的名称为 myca。

```
[Device-pki-domain-openca] ca identifier myca
```

配置注册受理机构服务器的 URL。通常，格式为 http://host/cgi-bin/pki/scep。其中，host 为 OpenCA 服务器的主机地址。

```
[Device-pki-domain-openca] certificate request url http://192.168.222.218/cgi-bin/pki/scep
```

配置证书申请的注册受理机构为 RA。

```
[Device-pki-domain-openca] certificate request from ra
```

指定 PKI 实体名称为 aaa。

```
[Device-pki-domain-openca] certificate request entity aaa
```

指定证书申请使用的 RSA 密钥对，用途为通用，名称为 abc，密钥长度为 1024 比特。

```
[Device-pki-domain-openca] public-key rsa general name abc length 1024
[Device-pki-domain-openca] quit
```

- 生成 RSA 算法的本地密钥对

```
[Device] public-key local create rsa name abc
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512,it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.........................++++++
.....................................++++++
Create the key pair successfully.
```

- 证书申请

获取 CA 证书并下载至本地。

```
[Device] pki retrieve-certificate domain openca ca
The trusted CA's finger print is:
    MD5  fingerprint:5AA3 DEFD 7B23 2A25 16A3 14F4 C81C C0FA
```

```
    SHA1 fingerprint:9668 4E63 D742 4B09 90E0 4C78 E213 F15F DC8E 9122
Is the finger print correct?(Y/N):y
Retrieved the certificates successfully.
```

手工申请本地证书。

```
[Device] pki request-certificate domain openca
Start to request the general certificate ...
……
Certificate requested successfully.
```

4. 验证配置

通过以下显示命令可以查看申请到的本地证书信息。

```
[Device] display pki certificate domain openca local
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            21:1d:b8:d2:e4:a9:21:28:e4:de
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CN, L=shanghai , ST=beijing, O=OpenCA Labs, OU=mysubUnit, CN=sub-ca,
DC=pki-subdomain, DC=mydomain-sub, DC=com
        Validity
            Not Before: Jun 30 09:09:09 2011 GMT
            Not After : May  1 09:09:09 2012 GMT
        Subject: CN=rnd, O=test, OU=software, C=CN
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b8:7a:9a:b8:59:eb:fc:70:3e:bf:19:54:0c:7e:
                    c3:90:a5:d3:fd:ee:ff:c6:28:c6:32:fb:04:6e:9c:
                    d6:5a:4f:aa:bb:50:c4:10:5c:eb:97:1d:a7:9e:7d:
                    53:d5:31:ff:99:ab:b6:41:f7:6d:71:61:58:97:84:
                    37:98:c7:7c:79:02:ac:a6:85:f3:21:4d:3c:8e:63:
                    8d:f8:71:7d:28:a1:15:23:99:ed:f9:a1:c3:be:74:
                    0d:f7:64:cf:0a:dd:39:49:d7:3f:25:35:18:f4:1c:
                    59:46:2b:ec:0d:21:1d:00:05:8a:bf:ee:ac:61:03:
                    6c:1f:35:b5:b4:cd:86:9f:45
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Client, S/MIME
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection, Microsoft Smartcardlogin
Netscape Comment:
```

```
                User Certificate of OpenCA Labs
            X509v3 Subject Key Identifier:
                24:71:C9:B8:AD:E1:FE:54:9A:EA:E9:14:1B:CD:D9:45:F4:B2:7A:1B
            X509v3 Authority Key Identifier:
                keyid:85:EB:D5:F7:C9:97:2F:4B:7A:6D:DD:1B:4D:DD:00:EE:53:CF:FD:5B

            X509v3 Issuer Alternative Name:
                DNS:root@docm.com, DNS:, IP Address:192.168.154.145, IP
Address:192.168.154.138
            Authority Information Access:
                CA Issuers - URI:http://192.168.222.218/pki/pub/cacert/cacert.crt
                OCSP - URI:http://192.168.222.218:2560/
                1.3.6.1.5.5.7.48.12 - URI:http://192.168.222.218:830/

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://192.168.222.218/pki/pub/crl/cacrl.crl

    Signature Algorithm: sha256WithRSAEncryption
        5c:4c:ba:d0:a1:35:79:e6:e5:98:69:91:f6:66:2a:4f:7f:8b:
        0e:80:de:79:45:b9:d9:12:5e:13:28:17:36:42:d5:ae:fc:4e:
        ba:b9:61:f1:0a:76:42:e7:a6:34:43:3e:2d:02:5e:c7:32:f7:
        6b:64:bb:2d:f5:10:6c:68:4d:e7:69:f7:47:25:f5:dc:97:af:
        ae:33:40:44:f3:ab:e4:5a:a0:06:8f:af:22:a9:05:74:43:b6:
        e4:96:a5:d4:52:32:c2:a8:53:37:58:c7:2f:75:cf:3e:8e:ed:
        46:c9:5a:24:b1:f5:51:1d:0f:5a:07:e6:15:7a:02:31:05:8c:
        03:72:52:7c:ff:28:37:1e:7e:14:97:80:0b:4e:b9:51:2d:50:
        98:f2:e4:5a:60:be:25:06:f6:ea:7c:aa:df:7b:8d:59:79:57:
        8f:d4:3e:4f:51:c1:34:e6:c1:1e:71:b5:0d:85:86:a5:ed:63:
        1e:08:7f:d2:50:ac:a0:a3:9e:88:48:10:0b:4a:7d:ed:c1:03:
        9f:87:97:a3:5e:7d:75:1d:ac:7b:6f:bb:43:4d:12:17:9a:76:
        b0:bf:2f:6a:cc:4b:cd:3d:a1:dd:e0:dc:5a:f3:7c:fb:c3:29:
        b0:12:49:5c:12:4c:51:6e:62:43:8b:73:b9:26:2a:f9:3d:a4:
        81:99:31:89
```

关于获取到的 CA 证书的详细信息可以通过相应的显示命令来查看，此处略。具体内容请参考命令 **display pki certificate domain**。

1.14.4 NAT-PT组网中PKI实体向CA申请证书（采用RSA Keon CA服务器）

1. 组网需求

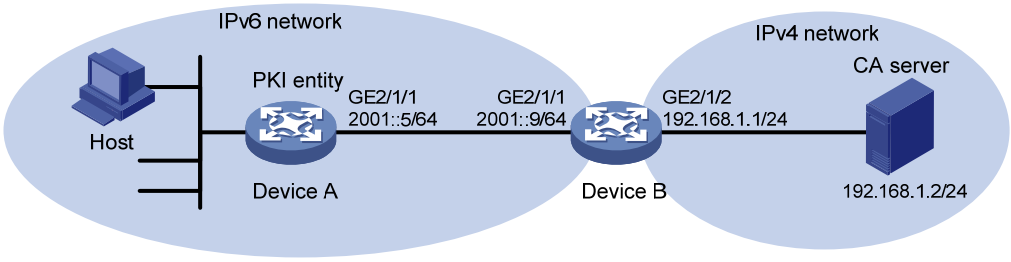
IPv6 网络内的 PKI 实体 Device A 希望与 IPv4 网络内的地址为 192.168.1.2/24 的 CA 服务器通信，以实现以下需求：

- 设备从 CA 服务器上获取 CRL，用于验证本地证书
- 设备向 CA 服务器申请本地证书

为了满足上述需求，需要在 IPv4 网络和 IPv6 网络之间部署 NAT-PT 设备 Device B，在 Device B 上配置 IPv4 侧报文静态映射和 IPv6 侧报文静态映射，使 IPv4 网络和 IPv6 网络之间可以互相访问。

2. 组网图

图1-6 NAT-PT 组网中 PKI 实体向 CA 申请证书



3. 配置步骤

(1) 配置 CA 服务器

本例CA server采用RSA Keon CA服务器，CA服务器配置参看“1.14.1 3. (1)”，并使能Local Certificate Publishing。

配置 IPv4 侧 CA 服务器到达 192.168.18.0/24 网段的静态路由（以 Windows XP 主机上的配置为例）。

```
C:\Documents and Settings\username\route add 192.16.18.0 mask 255.255.255.0 192.168.1.1
```

(2) 配置 Device B

使能 IPv6，配置接口地址，并使能接口的 NAT-PT 功能。

```
<DeviceB> system-view
[DeviceB] ipv6
[DeviceB] interface gigabitethernet 2/1/1
[DeviceB-GigabitEthernet2/1/1] ipv6 address 2001::9/64
[DeviceB-GigabitEthernet2/1/1] natpt enable
[DeviceB-GigabitEthernet2/1/1] quit
[DeviceB] interface gigabitethernet 2/1/2
[DeviceB-GigabitEthernet2/1/2] ip address 192.168.1.1 255.255.255.0
[DeviceB-GigabitEthernet2/1/2] natpt enable
[DeviceB-GigabitEthernet2/1/2] quit
```

配置 NAT-PT 前缀。

```
[DeviceB] natpt prefix 3001::
```

配置 IPv4 侧报文的静态映射。

```
[DeviceB] natpt v4bound static 192.168.1.2 3001::5
```

配置 IPv6 侧报文的静态映射。

```
[DeviceB] natpt v6bound static 2001::5 192.16.18.111
```

(3) 配置 Device A

配置到达 NAT-PT 前缀对应网段的静态路由。

```
<DeviceA> system-view
[DeviceA] ipv6 route-static 3001:: 16 2001::9
```

- 配置 PKI 实体

配置 PKI 实体名称为 aaa，通用名为 test。

```
[DeviceA] pki entity aaa
```

```
[DeviceA-pki-entity-aaa] common-name test
[DeviceA-pki-entity-aaa] quit
```

- 配置 PKI 域

创建并进入 PKI 域 torsa。

```
[DeviceA] pki domain torsa
```

配置设备信任的 CA 的名称为 myca。

```
[DeviceA-pki-domain-torsa] ca identifier myca
```

配置注册受理机构服务器的 URL，格式为 http://host:port/Issuing Jurisdiction ID，其中的 Issuing Jurisdiction ID 为 CA 服务器上生成的 16 进制字符串。

```
[DeviceA-pki-domain-torsa] certificate request url
http://[3001::5]:446/c95e970f632d27be5e8cbf80e971d9c4a9a93337
```

配置证书申请的注册受理机构为 CA。

```
[DeviceA-pki-domain-torsa] certificate request from ca
```

指定 PKI 实体名称为 aaa。

```
[DeviceA-pki-domain-torsa] certificate request entity aaa
```

配置 CRL 发布点位置。（此处不可配置 HTTP 格式的 CRL 发布点。虽然在此组网下，Device A 发出的 IPv6 报文在经过 Device B 后会被转换为 IPv4 报文，但 HTTP 报文中仍会带有 IPv6 的相关信息，RSA 服务器无法处理这种报文。OpenCA 没有这种限制。其它类型的 CA 服务器，请以实际情况为准。）

```
[DeviceA-pki-domain-torsa] crl url ldap://[3001::5]:389/CN=sslrsa,OU=sec,O=docm,C=cn
```

指定证书申请使用的密钥对，名称为 abc，用途为通用，密钥长度为 1024。

```
[DeviceA-pki-domain-torsa] public-key rsa general name abc length 1024
[DeviceA-pki-domain-torsa] quit
```

- 生成 RSA 算法的本地密钥对

```
[DeviceA] public-key local create rsa name abc
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512,it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.........................++++++
.....................................++++++
Create the key pair successfully.
```

- 证书申请

获取 CA 证书并下载至本地。

```
[DeviceA] pki retrieve-certificate domain torsa ca
The trusted CA's finger print is:
    MD5  fingerprint:EDE9 0394 A273 B61A F1B3 0072 A0B1 F9AB
    SHA1 fingerprint: 77F9 A077 2FB8 088C 550B A33C 2410 D354 23B2 73A8
Is the finger print correct?(Y/N):y
Retrieved the certificates successfully
```

获取 CRL 并下载至本地。

```
[DeviceA] pki retrieve-crl domain torsa
Retrieve CRL of the domain aaa successfully.
```

手工申请本地证书。

```
[DeviceA] pki request-certificate domain torsa password 123
Start to request the general certificate ...
……
Certificate requested successfully.
```

4. 验证配置

通过以下显示命令可以查看申请到的本地证书信息。

```
[DeviceA] display pki certificate domain torsa local
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            1a:6f:8e:6c:d6:36:b9:00:37:51:19:f5:ad:e7:30:e2
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=myca
        Validity
            Not Before: Jan  6 03:18:53 2013 GMT
            Not After : Jan  6 03:18:53 2014 GMT
        Subject: CN=test
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b8:65:45:a1:5e:21:e3:c0:c4:25:e5:26:97:25:
                    f8:91:c5:3c:76:95:2c:34:66:1a:4c:af:bc:0a:92:
                    9d:c2:79:ec:2d:eb:5a:3a:54:e1:98:e6:c1:58:ee:
                    0f:4b:84:63:51:d8:37:a5:a5:fd:7e:81:1f:d2:8c:
                    53:a3:09:3e:98:a8:51:d5:3f:3c:02:02:d3:19:51:
                    ca:6c:a0:a1:4d:07:0d:d8:09:61:6f:dd:10:e5:0f:
                    18:4d:43:e6:43:ec:54:c6:ba:2e:b5:c4:dc:ba:05:
                    53:74:e8:e9:42:ef:c6:9d:98:b7:1c:20:c7:03:a9:
                    f2:26:64:a6:ad:05:09:c8:69
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 CRL Distribution Points:

                Full Name:
                  DirName: CN = myca

    Signature Algorithm: sha1WithRSAEncryption
        6e:91:d6:74:f6:b7:60:a7:0d:c9:d8:6f:a2:c6:04:a2:d0:1b:
        23:8b:5e:3d:66:00:03:5e:15:f0:42:58:d1:8c:e3:54:8e:de:
        2f:7c:fa:f2:8b:bf:c0:c4:a0:1c:d2:04:3e:b9:39:1e:16:34:
        4a:ef:b1:10:96:60:aa:5c:c0:5a:b3:26:9d:dc:f9:57:ec:9d:
        6c:31:be:bb:af:40:a9:b1:a6:98:ca:cd:a0:f0:e7:10:4e:6e:
        b1:d8:ab:15:37:e6:83:12:21:1f:a8:c0:a8:23:1f:07:aa:0a:
        fc:be:ce:20:e4:55:79:51:8f:ec:02:12:92:23:9e:cf:14:5c:
        39:43
```

关于获取到的 CA 证书及 CRL 文件的详细信息可以通过相应的显示命令来查看，此处略。具体内容请参考命令 **display pki certificate domain** 和 **display pki crl domain**。

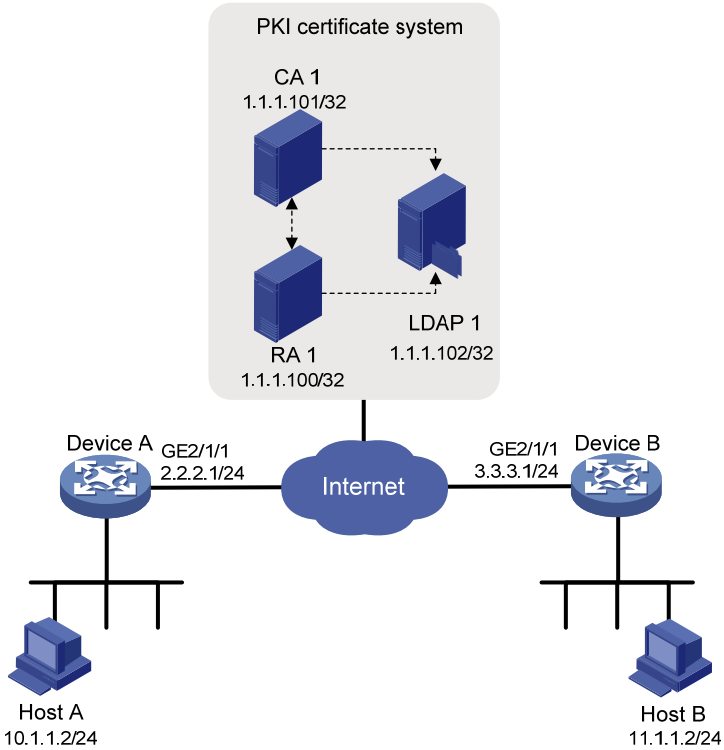
1.14.5 使用RSA数字签名方法进行IKE协商认证（采用Windows 2003 server CA服务器）

1. 组网需求

- 在 Device A 和 Device B 之间建立一个 IPsec 安全隧道对子网 10.1.1.0/24 上的主机 A 与子网 11.1.1.0/24 上的主机 B 之间的数据流进行安全保护。
- 在 Device A 和 Device B 之间使用 IKE 自动协商建立安全通信，IKE 认证策略采用 RSA 数字签名方法进行身份认证。
- Device A 和 Device B 使用相同的 CA。

2. 组网图

图1-7 使用 RSA 数字签名方法进行 IKE 协商认证组网图



3. 配置步骤

(1) 配置 CA 服务器

本例CA server采用Windows 2003 server CA服务器，CA服务器配置参看“1.14.2 3. (1)”。

(2) 配置 Device A

配置 PKI 实体。

```
<DeviceA> system-view
[DeviceA] pki entity en
[DeviceA-pki-entity-en] ip 2.2.2.1
[DeviceA-pki-entity-en] common-name devicea
```

```
[DeviceA-pki-entity-en] quit
```
配置 PKI 域参数。
```
[DeviceA] pki domain 1
[DeviceA-pki-domain-1] ca identifier CA1
[DeviceA-pki-domain-1] certificate request url http://1.1.1.100/certsrv/mscep/mscep.dll
[DeviceA-pki-domain-1] certificate request entity en
[DeviceA-pki-domain-1] ldap-server host 1.1.1.102
```
配置通过 RA 注册申请证书。
```
[DeviceA-pki-domain-1] certificate request from ra
```
指定证书申请使用的 RSA 密钥对，用途为通用，名称为 abc，密钥长度为 1024 比特。
```
[DeviceA-pki-domain-1] public-key rsa general name abc length 1024
[DeviceA-pki-domain-1] quit
```
生成 RSA 算法的本地密钥对。
```
[DeviceA] public-key local create rsa name abc
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512,it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.........................++++++
.....................................++++++
Create the key pair successfully.
```
获取 CA 证书并下载至本地。
```
[DeviceA] pki retrieve-certificate domain 1 ca
```
手工申请本地证书。
```
[DeviceA] pki request-certificate domain 1
```
配置 IKE 提议 1，使用数字签名（rsa-signature）方法为身份认证策略。
```
[DeviceA] ike proposal 1
[DeviceA-ike-proposal-1] authentication-method rsa-signature
[DeviceA-ike-proposal-1] quit
```
在 IKE profile 1 中指定 IKE 协商使用的 PKI 域。
```
[DeviceA] ike profile peer
[DeviceA-ike-profile-peer] certificate domain 1
```
(3)　配置 Device B

配置 PKI 实体。
```
<DeviceB> system-view
[DeviceB] pki entity en
[DeviceB-pki-entity-en] ip 3.3.3.1
[DeviceB-pki-entity-en] common-name deviceb
[DeviceB-pki-entity-en] quit
```
配置 PKI 域参数。（证书申请的注册机构服务器的 URL 根据所使用的 CA 服务器的不同而有所不同，这里的配置只作为示例，请根据具体情况配置。）
```
[DeviceB] pki domain 1
[DeviceB-pki-domain-1] ca identifier CA1
[DeviceB-pki-domain-1] certificate request url http://1.1.1.100/certsrv/mscep/mscep.dll
```

```
[DeviceB-pki-domain-1] certificate request entity en
[DeviceB-pki-domain-1] ldap-server host 1.1.1.102
```

配置通过 RA 注册申请证书。

```
[DeviceB-pki-domain-1] certificate request from ra
```

指定证书申请使用的 RSA 密钥对，用途为通用，名称为 abc，密钥长度为 1024 比特。

```
[DeviceB-pki-domain-1] public-key rsa general name abc length 1024
[DeviceB-pki-domain-1] quit
```

生成 RSA 算法的本地密钥对。

```
[DeviceB] public-key local create rsa name abc
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512,it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.........................++++++
.....................................++++++
Create the key pair successfully.
```

获取 CA 证书并下载至本地。

```
[DeviceB] pki retrieve-certificate ca domain 1
Retrieved the certificates successfully.
```

手工申请本地证书。

```
[DeviceB] pki request-certificate domain 1
Start to request general certificate ...
...
Certificate requested successfully.
```

配置 IKE 提议 1，使用 rsa-signature 方法为身份认证策略。

```
[DeviceB] ike proposal 1
[DeviceB-ike-proposal-1] authentication-method rsa-signature
[DeviceB-ike-proposal-1] quit
```

在 IKE profile 1 中指定 IKE 协商使用的 PKI 域。

```
[DeviceB] ike profile peer
[DeviceB-ike-profile-peer] certificate domain 1
```

说明

以上是对 IKE 协商采用 RSA 数字签名认证方法的配置，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，具体内容请参见“安全配置指导”中“IPsec”。

1.14.6 证书属性的访问控制策略应用举例

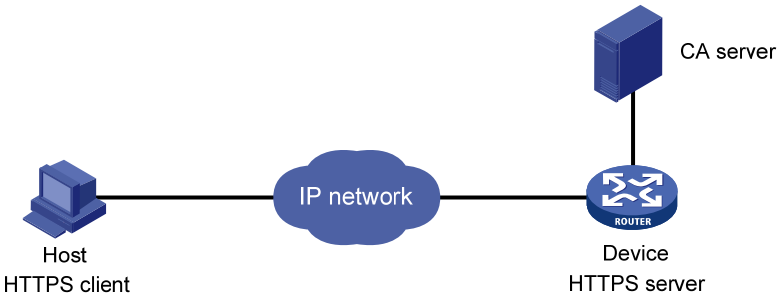
1. 组网需求

- 客户端通过 HTTPS 协议远程访问设备（HTTPS 服务器）。
- 通过 SSL 协议保证合法客户端安全登录 HTTPS 服务器。

- HTTPS 服务器要求对客户端进行身份验证，并通过制定证书访问控制策略，对客户端的证书合法性进行检测。

2. 组网图

图1-8 证书属性的访问控制策略应用组网图



3. 配置步骤

说明

- SSL 策略所引用的 PKI 域 domain1 必须首先创建。
- Device 上也需要申请一个本地证书作为 SSL 服务器端证书。

(1) 配置 HTTPS 服务器

使能 HTTPS 服务。

```
<Device> system-view
```

配置 HTTPS 服务器使用的 SSL 策略。

```
[Device] ssl server-policy abc
[Device-ssl-server-policy-abc] pki-domain domain1
[Device-ssl-server-policy-abc] client-verify enable
[Device-ssl-server-policy-abc] quit
```

(2) 配置证书属性组

配置证书属性组 mygroup1，并创建两个属性规则。规则 1 定义证书主题名的 DN 包含字符串 aabbcc；规则 2 定义证书颁发者名中的 IP 地址等于 10.0.0.1。

```
[Device] pki certificate attribute-group mygroup1
[Device-pki-cert-attribute-group-mygroup1] attribute 1 subject-name dn ctn aabbcc
[Device-pki-cert-attribute-group-mygroup1] attribute 2 issuer-name ip equ 10.0.0.1
[Device-pki-cert-attribute-group-mygroup1] quit
```

配置证书属性组 mygroup2，并创建两个属性规则。规则 1 定义证书备用主题名中的 FQDN 不包含字符串 apple；规则 2 定义证书颁发者名的 DN 包含字符串 aabbcc。

```
[Device] pki certificate attribute-group mygroup2
[Device-pki-cert-attribute-group-mygroup2] attribute 1 alt-subject-name fqdn nctn apple
[Device-pki-cert-attribute-group-mygroup2] attribute 2 issuer-name dn ctn aabbcc
[Device-pki-cert-attribute-group-mygroup2] quit
```

(3) 配置证书访问控制策略

创建访问控制策略 myacp，并定义两个访问控制规则。

```
[Device] pki certificate access-control-policy myacp
```

规则 1 定义，当证书的属性与属性组 mygroup1 里定义的属性匹配时，认为该证书无效，不能通过访问控制策略的检测。

```
[Device-pki-cert-acp-myacp] rule 1 deny mygroup1
```

规则 2 定义，当证书的属性与属性组 mygroup2 里定义的属性匹配时，认为该证书有效，可以通过访问控制策略的检测。

```
[Device-pki-cert-acp-myacp] rule 2 permit mygroup2
[Device-pki-cert-acp-myacp] quit
```

4. 验证配置

当客户端通过浏览器访问 HTTPS 服务器时，服务器端首先根据配置的证书访问控制策略检测客户端证书的有效性。已知该客户端证书的主题名的 DN 为 aabbcc，颁发者名中的 IP 地址为 1.1.1.1，备用主题名中的 FQDN 名为 banaba，由以上配置可判断匹配结果为：

- 本地证书的主题名和属性组 mygroup1 中的属性 1 匹配、颁发者名和属性组 mygroup1 中的属性 2 不匹配，因此该证书和证书属性组 mygroup1 不匹配。
- 本地证书的备用主题名属性和属性组 mygroup2 中的属性 1 匹配，颁发者名属性和属性组 mygroup2 中的属性 2 匹配，因此该证书和证书属性组 mygroup2 匹配。

该客户端的证书与访问控制策略 myacp 的规则 1 所引用的证书属性组 mygroup1 不匹配，因此规则 1 不生效；本地证书与访问控制策略 myacp 的规则 2 所引用的证书属性组 mygroup2 匹配，因此规则 2 生效，该证书可以通过访问控制策略 myacp 的检测。

通过以上检测后的合法客户端可以成功访问 HTTPS 服务器提供的网页。

1.14.7 导出、导入证书应用举例

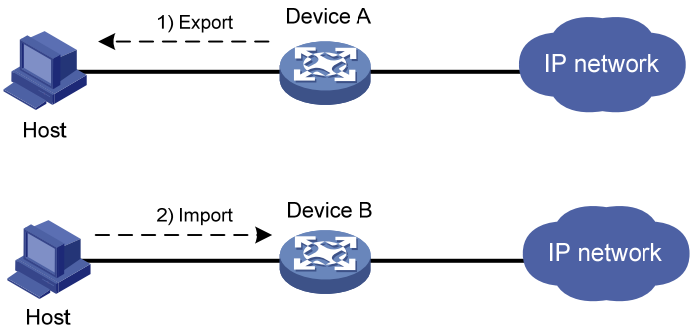
1. 组网需求

某网络中的 Device A 将要被 Device B 替换，Device A 上的 PKI 域 exportdomain 中保存了两个携带私钥的本地证书和一个 CA 证书。为保证替换后的证书可用，需要将原来 Device A 上的证书复制到 Device B 上去。具体要求如下：

- 从 Device A 上导出本地证书时，将对应的私钥数据采用 3DES_CBC 算法进行加密，加密口令为 111111。
- 来自 Device A 的证书以 PEM 编码的格式保存于 Device B 上的 PKI 域 importdomain 中。

2. 组网图

图1-9 导出、导入证书应用组网图



3. 配置步骤

(1) 从 Device A 上导出本地证书到指定文件

将 PKI 域中的 CA 证书导出到 PEM 格式的文件中，文件名为 pkicachain.pem。

```
<DeviceA> system-view
[DeviceA] pki export domain exportdomain pem ca filename pkicachain.pem
```

将 PKI 域中的本地证书导出到 PEM 格式的文件中，文件名为 pkilocal.pem。导出时对本地证书对应的私钥数据采用 3DES_CBC 算法进行加密，加密口令为 111111。

```
[DeviceA] pki export domain exportdomain pem local 3des-cbc 111111 filename pkilocal.pem
```

以上过程完成后，系统中将会生成三个 PEM 格式的证书文件，它们分别是：CA 证书文件 pkicachain.pem，带有私钥的本地签名证书文件 pkilocal.pem-signature 和带有私钥的本地加密证书文件 pkilocal.pem-encryption。

查看 PEM 格式的带有私钥的本地签名证书文件 pkilocal.pem-signature。

```
[DeviceA] quit
<DeviceA> more pkicachain.pem-sign
Bag Attributes
    friendlyName:
    localKeyID: 90 C6 DC 1D 20 49 4F 24 70 F5 17 17 20 2B 9E AC 20 F3 99 89
subject=/C=CN/O=OpenCA Labs/OU=Users/CN=subsign 11
issuer=/C=CN/L=shangdi/ST=beijing/O=OpenCA Labs/OU=docm/CN=subca1
-----BEGIN CERTIFICATE-----
MIIEgjCCA2qgAwIBAgILAJgsebpejZc5UwAwDQYJKoZIhvcNAQELBQAwZjELMAkG
…… (略)
-----END CERTIFICATE-----
Bag Attributes
    friendlyName:
    localKeyID: 90 C6 DC 1D 20 49 4F 24 70 F5 17 17 20 2B 9E AC 20 F3 99 89
Key Attributes: <No Attributes>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIICxjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIZtjSjfslJCoCAggA
…… (略)
-----END ENCRYPTED PRIVATE KEY-----
```

查看 PEM 格式的带有私钥的本地加密证书文件 pkilocal.pem-encryption。

```
<DeviceA> more pkicachain.pem-encr
```

```
Bag Attributes
    friendlyName:
    localKeyID: D5 DF 29 28 C8 B9 D9 49 6C B5 44 4B C2 BC 66 75 FE D6 6C C8
subject=/C=CN/O=OpenCA Labs/OU=Users/CN=subencr 11
issuer=/C=CN/L=shangdi/ST=beijing/O=OpenCA Labs/OU=docm/CN=subca1
-----BEGIN CERTIFICATE-----
MIIEUDCCAzigAwIBAgIKCHxnAVyzWhIPLzANBgkqhkiG9w0BAQsFADBmMQswCQYD
…… (略)
-----END CERTIFICATE-----
Bag Attributes
    friendlyName:
    localKeyID: D5 DF 29 28 C8 B9 D9 49 6C B5 44 4B C2 BC 66 75 FE D6 6C C8
Key Attributes: <No Attributes>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIICxjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI7H0mb4O7/GACAggA
…… (略)
-----END ENCRYPTED PRIVATE KEY-----
```

(2) 将 Device A 的证书文件下载到 Host

通过 FTP 将证书文件 pkicachain.pem、pkilocal.pem-sign 和 pkilocal.pem-encr 下载到 Host 上，具体过程略。

(3) 将 Host 上的证书文件上传到 Device B

通过 FTP 将证书文件 pkicachain.pem、pkilocal.pem-sign、pkilocal.pem-encr 上传到 Device B 的文件系统中，具体过程略。

(4) 在设备 Device B 上导入证书文件

关闭 CRL 检查。（是否进行 CRL 检查，请以实际的使用需求为准，此处仅为示例）

```
<DeviceB> system-view
[DeviceB] pki domain importdomain
[DeviceB-pki-domain-importdomain] undo crl check enable
```

指定证书申请使用的签名 RSA 密钥对名称为 sign，加密 RSA 密钥对名称为 encr。

```
[DeviceB-pki-domain-importdomain] public-key rsa signature name sign encryption name encr
[DeviceB-pki-domain-importdomain] quit
```

向 PKI 域中导入 CA 证书，证书文件格式为 PEM 编码，证书文件名称为 pkicachain.pem。

```
[DeviceB] pki import domain importdomain pem ca filename pkicachain.pem
```

向 PKI 域中导入本地证书，证书文件格式为 PEM 编码，证书文件名称为 pkilocal.pem-signature，证书文件中包含了密钥对。

```
[DeviceB] pki import domain importdomain pem local filename pkilocal.pem-signature
Please input the password:******
```

向 PKI 域中导入本地证书，证书文件格式为 PEM 编码，证书文件名称为 pkilocal.pem-encryption，证书文件中包含了密钥对。

```
[DeviceB] pki import domain importdomain pem local filename pkilocal.pem-encryption
Please input the password:******
```

通过以下显示命令可以查看导入到 Device B 的本地证书信息。

```
[DeviceB] display pki certificate domain importdomain local
Certificate:
    Data:
```

```
Version: 3 (0x2)
Serial Number:
    98:2c:79:ba:5e:8d:97:39:53:00
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=CN, L=shangdi, ST=beijing, O=OpenCA Labs, OU=docm, CN=subca1
Validity
    Not Before: May 26 05:56:49 2011 GMT
    Not After : Nov 22 05:56:49 2012 GMT
Subject: C=CN, O=OpenCA Labs, OU=Users, CN=subsign 11
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        Public-Key: (1024 bit)
        Modulus:
            00:9f:6e:2f:f6:cb:3d:08:19:9a:4a:ac:b4:ac:63:
            ce:8d:6a:4c:3a:30:19:3c:14:ff:a9:50:04:f5:00:
            ee:a3:aa:03:cb:b3:49:c4:f8:ae:55:ee:43:93:69:
            6c:bf:0d:8c:f4:4e:ca:69:e5:3f:37:5c:83:ea:83:
            ad:16:b8:99:37:cb:86:10:6b:a0:4d:03:95:06:42:
            ef:ef:0d:4e:53:08:0a:c9:29:dd:94:28:02:6e:e2:
            9b:87:c1:38:2d:a4:90:a2:13:5f:a4:e3:24:d3:2c:
            bf:98:db:a7:c2:36:e2:86:90:55:c7:8c:c5:ea:12:
            01:31:69:bf:e3:91:71:ec:21
        Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Basic Constraints:
        CA:FALSE
    Netscape Cert Type:
        SSL Client, S/MIME
    X509v3 Key Usage:
        Digital Signature, Non Repudiation
    X509v3 Extended Key Usage:
        TLS Web Client Authentication, E-mail Protection, Microsoft Smartcardlogin
    Netscape Comment:
        User Certificate of OpenCA Labs
    X509v3 Subject Key Identifier:
        AA:45:54:29:5A:50:2B:89:AB:06:E5:BD:0D:07:8C:D9:79:35:B1:F5
    X509v3 Authority Key Identifier:
        keyid:70:54:40:61:71:31:02:06:8C:62:11:0A:CC:A5:DB:0E:7E:74:DE:DD

    X509v3 Subject Alternative Name:
        email:subsign@docm.com
    X509v3 Issuer Alternative Name:
        DNS:subca1@docm.com, DNS:, IP Address:1.1.2.2, IP Address:2.2.1.1
    Authority Information Access:
        CA Issuers - URI:http://titan/pki/pub/cacert/cacert.crt
        OCSP - URI:http://titan:2560/
        1.3.6.1.5.5.7.48.12 - URI:http://titan:830/
```

```
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://192.168.40.130/pki/pub/crl/cacrl.crl

    Signature Algorithm: sha256WithRSAEncryption
        18:e7:39:9a:ad:84:64:7b:a3:85:62:49:e5:c9:12:56:a6:d2:
        46:91:53:8e:84:ba:4a:0a:6f:28:b9:43:bc:e7:b0:ca:9e:d4:
        1f:d2:6f:48:c4:b9:ba:c5:69:4d:90:f3:15:c4:4e:4b:1e:ef:
        2b:1b:2d:cb:47:1e:60:a9:0f:81:dc:f2:65:6b:5f:7a:e2:36:
        29:5d:d4:52:32:ef:87:50:7c:9f:30:4a:83:de:98:8b:6a:c9:
        3e:9d:54:ee:61:a4:26:f3:9a:40:8f:a6:6b:2b:06:53:df:b6:
        5f:67:5e:34:c8:c3:b5:9b:30:ee:01:b5:a9:51:f9:b1:29:37:
        02:1a:05:02:e7:cc:1c:fe:73:d3:3e:fa:7e:91:63:da:1d:f1:
        db:28:6b:6c:94:84:ad:fc:63:1b:ba:53:af:b3:5d:eb:08:b3:
        5b:d7:22:3a:86:c3:97:ef:ac:25:eb:4a:60:f8:2b:a3:3b:da:
        5d:6f:a5:cf:cb:5a:0b:c5:2b:45:b7:3e:6e:39:e9:d9:66:6d:
        ef:d3:a0:f6:2a:2d:86:a3:01:c4:94:09:c0:99:ce:22:19:84:
        2b:f0:db:3e:1e:18:fb:df:56:cb:6f:a2:56:35:0d:39:94:34:
        6d:19:1d:46:d7:bf:1a:86:22:78:87:3e:67:fe:4b:ed:37:3d:
        d6:0a:1c:0b

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            08:7c:67:01:5c:b3:5a:12:0f:2f
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CN, L=shangdi, ST=beijing, O=OpenCA Labs, OU=docm, CN=subca1
        Validity
            Not Before: May 26 05:58:26 2011 GMT
            Not After : Nov 22 05:58:26 2012 GMT
        Subject: C=CN, O=OpenCA Labs, OU=Users, CN=subencr 11
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:db:26:13:d3:d1:a4:af:11:f3:6d:37:cf:d0:d4:
                    48:50:4e:0f:7d:54:76:ed:50:28:c6:71:d4:48:ae:
                    4d:e7:3d:23:78:70:63:18:33:f6:94:98:aa:fa:f6:
                    62:ed:8a:50:c6:fd:2e:f4:20:0c:14:f7:54:88:36:
                    2f:e6:e2:88:3f:c2:88:1d:bf:8d:9f:45:6c:5a:f5:
                    94:71:f3:10:e9:ec:81:00:28:60:a9:02:bb:35:8b:
                    bf:85:75:6f:24:ab:26:de:47:6c:ba:1d:ee:0d:35:
                    75:58:10:e5:e8:55:d1:43:ae:85:f8:ff:75:81:03:
                    8c:2e:00:d1:e9:a4:5b:18:39
                Exponent: 65537 (0x10001)
        X509v3 extensions:
```

```
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Server
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            Netscape Comment:
                VPN Server of OpenCA Labs
            X509v3 Subject Key Identifier:
                CC:96:03:2F:FC:74:74:45:61:38:1F:48:C0:E8:AA:18:24:F0:2B:AB
            X509v3 Authority Key Identifier:
                keyid:70:54:40:61:71:31:02:06:8C:62:11:0A:CC:A5:DB:0E:7E:74:DE:DD

            X509v3 Subject Alternative Name:
                email:subencr@docm.com
            X509v3 Issuer Alternative Name:
                DNS:subca1@docm.com, DNS:, IP Address:1.1.2.2, IP Address:2.2.1.1
            Authority Information Access:
                CA Issuers - URI:http://titan/pki/pub/cacert/cacert.crt
                OCSP - URI:http://titan:2560/
                1.3.6.1.5.5.7.48.12 - URI:http://titan:830/

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://192.168.40.130/pki/pub/crl/cacrl.crl

    Signature Algorithm: sha256WithRSAEncryption
        53:69:66:5f:93:f0:2f:8c:54:24:8f:a2:f2:f1:29:fa:15:16:
        90:71:e2:98:e3:5c:c6:e3:d4:5f:7a:f6:a9:4f:a2:7f:ca:af:
        c4:c8:c7:2c:c0:51:0a:45:d4:56:e2:81:30:41:be:9f:67:a1:
        23:a6:09:50:99:a1:40:5f:44:6f:be:ff:00:67:9d:64:98:fb:
        72:77:9e:fd:f2:4c:3a:b2:43:d8:50:5c:48:08:e7:77:df:fb:
        25:9f:4a:ea:de:37:1e:fb:bc:42:12:0a:98:11:f2:d9:5b:60:
        bc:59:72:04:48:59:cc:50:39:a5:40:12:ff:9d:d0:69:3a:5e:
        3a:09:5a:79:e0:54:67:a0:32:df:bf:72:a0:74:63:f9:05:6f:
        5e:28:d2:e8:65:49:e6:c7:b5:48:7d:95:47:46:c1:61:5a:29:
        90:65:45:4a:88:96:e4:88:bd:59:25:44:3f:61:c6:b1:08:5b:
        86:d2:4f:61:4c:20:38:1c:f4:a1:0b:ea:65:87:7d:1c:22:be:
        b6:17:17:8a:5a:0f:35:4c:b8:b3:73:03:03:63:b1:fc:c4:f5:
        e9:6e:7c:11:e8:17:5a:fb:39:e7:33:93:5b:2b:54:72:57:72:
        5e:78:d6:97:ef:b8:d8:6d:0c:05:28:ea:81:3a:06:a0:2e:c3:
        79:05:cd:c3
```

关于导入的 CA 证书的详细信息可以通过相应的显示命令来查看，此处略。具体内容请参考命令**display pki certificate domain**。

1.15 常见配置错误举例

1.15.1 获取CA证书失败

1. 故障现象

获取 CA 证书失败。

2. 故障分析

可能有以下原因：

- 网络连接故障，如网线折断，接口松动；
- 没有设置信任的 CA 名称；
- 证书申请的注册受理机构服务器 URL 位置不正确或未配置；
- 设备的系统时钟与 CA 的时钟不同步；
- 未指定 CA 服务器可接受的 PKI 协议报文的源 IP 地址，或者指定的地址不正确；
- 指纹信息不合法。

3. 处理过程

- 排除物理连接故障；
- 查看各必配项是否都正确配置；
- 可通过 **ping** 命令测试注册服务器是否连接正常；
- 保持系统时钟与 CA 同步；
- 与 CA 服务器管理员联系，并保证配置正确的源 IP 地址；
- 在证书服务器上查看指纹信息是否合法。

1.15.2 获取本地证书失败

1. 故障现象

获取本地证书失败。

2. 故障分析

可能有以下原因：

- 网络连接故障；
- 执行获取操作之前 PKI 域中没有 CA 证书；
- 没有配置 LDAP 服务器或者配置错误；
- PKI 域没有指定申请使用的密钥对，或者指定的密钥对与待获取的本地证书不匹配；
- PKI 域中没有引用 PKI 实体配置，或 PKI 实体配置不正确；
- 使能了 CRL 检查，但是本地没有 CRL 且无法获取到 CRL；
- 未指定 CA 服务器可接受的 PKI 协议报文的源 IP 地址，或者指定的地址不正确；
- 设备时钟与 CA 服务器的时钟不同步。

3. 处理过程

- 排除物理连接故障；

- 获取或者导入 CA 证书；
- 配置正确的 LDAP 服务器；
- 在 PKI 域中指定申请使用的密钥对，生成指定的密钥对，并使其与待获取的本地证书匹配；
- PKI 域中引用正确的 PKI 实体，并正确配置该 PKI 实体；
- 获取 CRL；
- 与 CA 服务器管理员联系，并保证配置正确的源 IP 地址；
- 保持系统时钟与 CA 一致。

1.15.3 本地证书申请失败

1. 故障现象

手工申请证书失败。

2. 故障分析

可能有以下原因：

- 网络连接故障，如网线折断，接口松动；
- 执行申请操作之前 PKI 域中没有 CA 证书；
- 证书申请的注册受理机构服务器 URL 位置不正确或未配置；
- 没有配置证书申请注册受理机构或配置不正确；
- 没有配置 PKI 实体 DN 中必配参数或者配置参数不正确；
- PKI 域中没有指定证书申请使用的密钥对，或者 PKI 中指定的密钥对在申请过程中已被修改；
- 当前 PKI 域中有互斥的证书申请程序正在运行；
- 未指定 CA 服务器可接受的 PKI 协议报文的源 IP 地址，或者指定的地址不正确；
- 设备时钟与 CA 服务器的时钟不同步。

3. 处理过程

- 排除物理连接故障；
- 获取或者导入 CA 证书；
- 可通过 **ping** 命令测试注册服务器是否连接正常；
- 配置正确的证书申请注册受理机构服务器 URL；
- 查看 CA/RA 注册策略，并对相关的 PKI 实体 DN 属性进行正确配置；
- 在 PKI 域中指定证书申请使用的密钥对，或者删除设备上 PKI 域中指定的的密钥对并重新申请本地证书；
- 使用 **pki abort-certificate- request domain** 命令停止正在运行的证书申请程序；
- 与 CA 服务器管理员联系，并保证配置正确的源 IP 地址；
- 保持系统时钟与 CA 一致。

1.15.4 CRL获取失败

1. 故障现象

获取 CRL 失败。

2. 故障分析

可能有以下原因：

- 网络连接故障，如网线折断，接口松动；
- 获取 CRL 之前未先取得 CA 证书；
- 未设置 CRL 发布点位置，且不能从 PKI 域中 CA 证书或本地证书中获得正确的发布点；
- 设置的 CRL 发布点位置不正确；
- 不能获取 CRL 发布点的情况下，通过 SCEP 协议获取 CRL，但此时 PKI 域中不存在本地证书，或本地证书的密钥对已被修改，或 PKI 域中没有配置正确的证书申请 URL；
- CRL 发布点的 URL 配置中包含不完整的地址（没有主机名或主机地址）且 PKI 域中没有配置 LDAP 服务器或者配置不正确；
- CA 没有签发 CRL；
- 未指定 CA 服务器可接受的 PKI 协议报文的源 IP 地址，或者指定的地址不正确。

3. 处理过程

- 排除物理连接故障；
- 获取或导入 CA 证书；
- 设置正确 CRL 发布点位置：配置包含完整地址的 CRL 发布点的 URL 或在 PKI 域中配置正确的 LDAP 服务器；
- 在无法获取 CRL 发布点的情况下，配置正确的证书申请 URL，并保证已经获取了本地证书，且本地保存的密钥对的公钥与本地证书的公钥匹配；
- 在 CA 上发布 CRL；
- 与 CA 服务器管理员联系，并保证配置正确的源 IP 地址。

1.15.5 导入CA证书失败

1. 故障现象

导入证书失败。

2. 故障分析

可能有以下原因：

- 使能了 CRL 检查，但是本地没有 CRL 且无法获取到 CRL；
- 指定的导入格式与实际导入的文件格式不一致。

3. 处理过程

- 执行 **undo crl check enable** 命令，关闭 CRL 检查；
- 请确认导入的文件格式并选择正确的导入格式。

1.15.6 导入本地证书失败

1. 故障现象

导入证书失败。

2. 故障分析

可能有以下原因：

- PKI 域中没有 CA 证书且导入的本地证书中不含 CA 证书链；
- 使能了 CRL 检查，但是本地没有 CRL 且无法获取到 CRL；
- 指定的导入格式与实际导入的文件格式不一致；
- 设备上和证书中都没有该本地证书对应的密钥对；
- 证书已经被吊销；
- 证书不在有效期；
- 系统时钟设置错误。

3. 处理过程

- 获取或者导入 CA 证书；
- 执行 **undo crl check enable** 命令，关闭 CRL 检查，或者先获取 CRL；
- 请确认导入的文件格式并选择正确的导入格式；
- 请导入包含私钥内容的证书文件；
- 导入未被吊销的证书；
- 导入还在有效期内的证书；
- 请重新设置正确的系统时钟。

1.15.7 导出证书失败

1. 故障现象

导出证书失败。

2. 故障分析

可能有以下原因：

- 以 PKCS#12 格式导出所有证书时 PKI 域中没有本地证书；
- 用户所设置的导出路径不存在；
- 用户所设置的导出路径不合法；
- 要导出的本地证书的公钥和它所属 PKI 域中的密钥对的公钥部分不匹配；
- 设备磁盘空间已满。

3. 处理过程

- 获取或申请本地证书；
- 用 **mkdir** 命令创建用户所需路径；
- 设置正确的导出路径；
- 在 PKI 域中配置匹配的密钥对；
- 清理设备磁盘空间。

1.15.8 设置存储路径失败

1. 故障现象

设置证书或 CRL 存储路径失败。

2. 故障分析

可能有以下原因：

- 用户所设置的证书或 CRL 存储路径不存在；
- 用户所设置的证书或 CRL 存储路径不合法；
- 设备磁盘空间已满。

3. 处理过程

- 用 **mkdir** 命令创建用户所需路径；
- 设置正确的的证书或 CRL 存储路径；
- 清理设备磁盘空间。

目 录

1 IPsec

说明

设备运行于FIPS模式时，本特性部分配置相对于非FIPS模式有所变化，具体差异请见本文相关描述。有关 FIPS 模式的详细介绍请参见“安全配置指导”中的“FIPS”。

注意

若在接口上同时配置IPsec和QoS，同一个IPsec SA保护的数据流如果被QoS分类进入不同队列，会导致部分报文发送乱序。由于 IPsec 具有抗重放功能，IPsec 入方向上对于抗重放窗口之外的报文会进行丢弃，从而导致丢包现象。因此当 IPsec 与 QoS 配合使用时，必须保证 IPsec 分类与 QoS 分类规则配置保持一致。IPsec 的分类规则完全由引用的 ACL 规则确定，QoS 分类规则的配置请参考“ACL 和 QoS 配置指导”中的“QoS 配置方式”

1.1 IPsec简介

IPsec（IP Security，IP 安全）是 IETF 制定的三层隧道加密协议，它为互联网上传输的数据提供了高质量的、基于密码学的安全保证，是一种传统的实现三层 VPN（Virtual Private Network，虚拟专用网络）的安全技术。IPsec 通过在特定通信方之间（例如两个安全网关之间）建立“通道”，来保护通信方之间传输的用户数据，该通道通常称为 IPsec 隧道。

IPsec 协议不是一个单独的协议，它为 IP 层上的网络数据安全提供了一整套安全体系结构，包括安全协议 AH（Authentication Header，认证头）和 ESP（Encapsulating Security Payload，封装安全载荷）、IKE（Internet Key Exchange，互联网密钥交换）以及用于网络认证及加密的一些算法等。其中，AH 协议和 ESP 协议用于提供安全服务，IKE 协议用于密钥交换。关于 IKE 的详细介绍请参见“安全配置指导”中的“IKE”，本节不做介绍。

IPsec 提供了两大安全机制：认证和加密。认证机制使 IP 通信的数据接收方能够确认数据发送方的真实身份以及数据在传输过程中是否遭篡改。加密机制通过对数据进行加密运算来保证数据的机密性，以防数据在传输过程中被窃听。

IPsec 为 IP 层的数据报文提供的安全服务具体包括以下几种：

- 数据机密性（Confidentiality）：发送方通过网络传输用户报文前，IPsec 对报文进行加密。
- 数据完整性（Data Integrity）：接收方对发送方发送来的 IPsec 报文进行认证，以确保数据在传输过程中没有被篡改。
- 数据来源认证（Data Authentication）：接收方认证发送 IPsec 报文的发送端是否合法。
- 抗重放（Anti-Replay）：接收方可检测并拒绝接收过时或重复的 IPsec 报文。

IPsec 具有以下优点：

- 支持 IKE（Internet Key Exchange，互联网密钥交换），可实现密钥的自动协商功能，减少了密钥协商的开销。可以通过 IKE 建立和维护 SA（Security Association，安全联盟），简化了 IPsec 的使用和管理。
- 所有使用 IP 协议进行数据传输的应用系统和服务都可以使用 IPsec，而不必对这些应用系统和服务本身做任何修改。
- 对数据的加密是以数据包为单位的，而不是以整个数据流为单位，这不仅灵活而且有助于进一步提高 IP 数据包的安全性，可以有效防范网络攻击。

1.1.1 安全协议及封装模式

1. 安全协议

IPsec 包括 AH 和 ESP 两种安全协议，它们定义了对 IP 报文的封装格式以及可提供的安全服务。

- AH协议（IP协议号为 51）定义了AH头在IP报文中的封装格式，如 图 1-3 所示。AH可提供数据来源认证、数据完整性校验和抗重放功能，它能保护报文免受篡改，但不能防止报文被窃听，适合用于传输非机密数据。AH使用的认证算法有HMAC-MD5 和HMAC-SHA1。
- ESP协议（IP协议号为 50）定义了ESP头和ESP尾在IP报文中的封装格式，如 图 1-3 所示。ESP可提供数据加密、数据源认证、数据完整性校验和抗重放功能。与AH不同的是，ESP将需要保护的用户数据进行加密后再封装到IP包中，以保证数据的机密性。ESP使用的加密算法有DES、3DES、AES等。同时，作为可选项，ESP还可以提供认证服务，使用的认证算法有HMAC-MD5 和HMAC-SHA1。虽然AH和ESP都可以提供认证服务，但是AH提供的认证服务要强于ESP。

在实际使用过程中，可以根据具体的安全需求同时使用这两种协议或仅使用其中的一种。设备支持的 AH 和 ESP 联合使用的方式为：先对报文进行 ESP 封装，再对报文进行 AH 封装。

2. 封装模式

IPsec 支持两种封装模式：

- 传输模式（Transport Mode）

该模式下的安全协议主要用于保护上层协议报文，仅传输层数据被用来计算安全协议头，生成的安全协议头以及加密的用户数据（仅针对ESP封装）被放置在原IP头后面。若要求端到端的安全保障，即数据包进行安全传输的起点和终点为数据包的实际起点和终点时，才能使用传输模式。如 图 1-1 所示，通常传输模式用于保护两台主机之间的数据。

图1-1 传输模式下的 IPsec 保护

- 隧道模式（Tunnel Mode）

该模式下的安全协议用于保护整个IP数据包，用户的整个IP数据包都被用来计算安全协议头，生成的安全协议头以及加密的用户数据（仅针对ESP封装）被封装在一个新的IP数据包中。这种模式下，封装后的IP数据包有内外两个IP头，其中的内部IP头为原有的IP头，外部IP头由提供安全服务的设备添加。在安全保护由设备提供的情况下，数据包进行安全传输的起点或终点不为数据包的实际起

点和终点时（例如安全网关后的主机），则必须使用隧道模式。如 图 1-2 所示，通常隧道模式用于保护两个安全网关之间的数据。

图1-2 隧道模式下的 IPsec 保护

不同的安全协议及组合在隧道和传输模式下的数据封装形式如 图 1-3 所示。

图1-3 安全协议数据封装格式

Mode / Protocol	Transport	Tunnel
AH	IP AH Data	IP AH IP Data
ESP	IP ESP Data ESP-T	IP ESP IP Data ESP-T
AH-ESP	IP AH ESP Data ESP-T	IP AH ESP IP Data ESP-T

1.1.2 安全联盟

SA（Security Association，安全联盟）是 IPsec 的基础，也是 IPsec 的本质。IPsec 在两个端点之间提供安全通信，这类端点被称为 IPsec 对等体。SA 是 IPsec 对等体间对某些要素的约定，例如，使用的安全协议（AH、ESP 或两者结合使用）、协议报文的封装模式（传输模式或隧道模式）、认证算法（HMAC-MD5 或 HMAC-SHA1）、加密算法（DES、3DES 或 AES）、特定流中保护数据的共享密钥以及密钥的生存时间等。

SA 是单向的，在两个对等体之间的双向通信，最少需要两个 SA 来分别对两个方向的数据流进行安全保护。同时，如果两个对等体希望同时使用 AH 和 ESP 来进行安全通信，则每个对等体都会针对每一种协议来构建一个独立的 SA。

SA 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 地址和安全协议号。其中，SPI 是用于标识 SA 的一个 32 比特的数值，它在 AH 和 ESP 头中传输。

SA 有手工配置和 IKE 自动协商两种生成方式：

- 手工方式：通过命令行配置 SA 的所有信息。该方式的配置比较复杂，而且不支持一些高级特性（例如定时更新密钥），优点是可以不依赖 IKE 而单独实现 IPsec 功能。该方式主要用于需要安全通信的对等体数量较少，或小型静态的组网环境中。
- IKE 自动协商方式：对等体之间通过 IKE 协议自动协商生成 SA，并由 IKE 协议维护该 SA。该方式的配置相对比较简单，扩展能力强。在中、大型的动态网络环境中，推荐使用 IKE 自动协商建立 SA。

手工方式建立的 SA 永不老化。通过 IKE 协商建立的 SA 具有生存时间，该类型的 SA 有两种形式的生存时间：

- 基于时间的生存时间，定义了一个 SA 从建立到失效的时间；
- 基于流量的生存时间，定义了一个 SA 允许处理的最大流量。

可同时存在基于时间和基于流量两种方式的 SA 生存时间，只要 SA 的生存时间到达指定的时间或流量时，该 SA 就会失效。SA 失效前，IKE 将为 IPsec 对等体协商建立新的 SA，这样，在旧的 SA 失效前新的 SA 就已经准备好。在新的 SA 开始协商而没有协商好之前，使用当前旧的 SA 保护通信。一旦协商出新的 SA，立即采用新的 SA 保护通信。

1.1.3 认证与加密

1. 认证算法

IPsec 使用的认证算法主要是通过杂凑函数实现的。杂凑函数是一种能够接受任意长度的消息输入，并产生固定长度输出的算法，该算法的输出称为消息摘要。IPsec 对等体双方都会计算一个摘要，接收方将发送方的摘要与本地的摘要进行比较，如果二者相同，则表示收到的 IPsec 报文是完整未经篡改的，以及发送方身份合法。目前，IPsec 强制使用基于 HMAC（Hash-based Message Authentication Code，基于散列的消息鉴别码）的认证算法，包括 HMAC-MD5 和 HMAC-SHA1。其中，HMAC-MD5 算法的计算速度快，而 HMAC-SHA1 算法的安全强度高。

2. 加密算法

IPsec 使用的加密算法属于对称密钥系统，这类算法使用相同的密钥对数据进行加密和解密。目前设备的 IPsec 使用三种加密算法：

- DES：使用 56 比特的密钥对一个 64 比特的明文块进行加密。
- 3DES：使用三个 56 比特（共 168 比特）的密钥对明文块进行加密。
- AES：使用 128 比特、192 比特或 256 比特的密钥对明文块进行加密。

这三个加密算法的安全性由高到低依次是：AES、3DES、DES，安全性高的加密算法实现机制复杂，运算速度慢。

3. 加密引擎

IPsec 的认证和加/解密处理在设备上既可以通过软件实现，也可以通过硬件加密引擎实现。通过软件实现的 IPsec，由于复杂的加密/解密、认证算法会占用大量的 CPU 资源，将会影响设备整体处理效率；通过硬件加密引擎实现的 IPsec，由于复杂的算法处理由硬件完成，因此可以提高设备的处理效率。

若设备支持通过硬件加密引擎进行认证和加/解密处理，则设备会首先将需要处理的数据发送给硬件加密引擎，由硬件加密引擎对数据进行处理之后再发送回设备，最后由设备进行转发。

关于加密引擎的详细介绍请参见“安全配置指导”中的“加密引擎”。

1.1.4 IPsec实现方式

要实现建立 IPsec 隧道为两个 IPsec 对等体之间的数据提供安全保护，首先要配置相应的安全策略，通过安全策略定义哪些报文属于要保护的范围，并定义用于保护这些报文的安全参数。之后，将安全策略应用于设备的某接口上或某应用中。当 IPsec 对等体根据安全策略识别出要保护的报文时，就建立一个相应的 IPsec 隧道并将其通过该隧道发送给对端。此处的 IPsec 隧道可以是提前手工配

置或者由报文触发 IKE 协商建立。这些 IPsec 隧道实际上就是两个 IPsec 对等体之间建立的 IPsec SA。由于 IPsec SA 是单向的，因此出方向的报文由出方向的 SA 保护，入方向的报文由入方向的 SA 来保护。对端接收到报文后，首先对报文进行分析、识别，然后根据预先设定的安全策略对报文进行不同的处理（丢弃，解封装，或直接转发）。

根据 IPsec 安全策略应用方式的不同，IPsec 隧道的建立又分为两种实现方式：基于接口和基于业务。基于接口的实现方式下，通过将 IPsec 安全策略应用到设备的接口上，使得设备对通过该接口收发的数据报文依据接口上应用的安全策略进行 IPsec 保护；基于业务的实现方式下，IPsec 安全策略仅与具体的业务绑定，无论该业务的报文从设备的哪个接口发送或接收，都会被 IPsec 保护。

目前，在基于接口的 IPsec 实现方式下仅支持基于 ACL 建立 IPsec 隧道。

1. 基于ACL（Access Control List，访问控制列表）

基于 ACL 方式下，需要通过定义 ACL 来指定两个对等体之间需要被保护的数据流的范围，并需要将引用了该 ACL 的 IPsec 安全策略应用到相应的接口上。只要接口发送的报文与该接口上应用的 IPsec 安全策略中的 ACL 的 **permit** 规则匹配，就会受到出方向 IPsec SA 的保护并进行封装处理。接口接收到目的地址是本机的 IPsec 报文时，首先根据报文头里携带的 SPI 查找本地的入方向 IPsec SA，由对应的入方向 IPsec SA 进行解封装处理。解封装后的 IP 报文若能与 ACL 的 **permit** 规则匹配上则采取后续处理，否则被丢弃。

目前，设备支持的数据流的保护方式包括以下三种：

- 标准方式：一条 IPsec 隧道保护一条数据流。ACL 中的每一个规则对应的数据流分别由一条单独创建的 IPsec 隧道来保护。缺省采用该方式。
- 聚合方式：一条 IPsec 隧道保护 ACL 中定义的所有数据流。ACL 中的所有规则对应的数据流只会由一条创建的 IPsec 隧道来保护。该方式仅用于和老版本的设备互通。
- 主机方式：一条 IPsec 隧道保护一条主机到主机的数据流。ACL 中的每一个规则对应的不同主机之间的数据流分别由一条单独创建的 IPsec 隧道来保护。这种方式下，受保护的网段之间存在多条数据流的情况下，将会消耗更多的系统资源。

2. 基于业务

基于业务方式下，不需要 ACL 来限定要保护的数据流的范围，设备产生的需要 IPsec 保护的某一业务协议的所有报文都要进行封装处理，而设备接收到的不受 IPsec 保护的以及解封装失败的业务协议报文都要被丢弃。

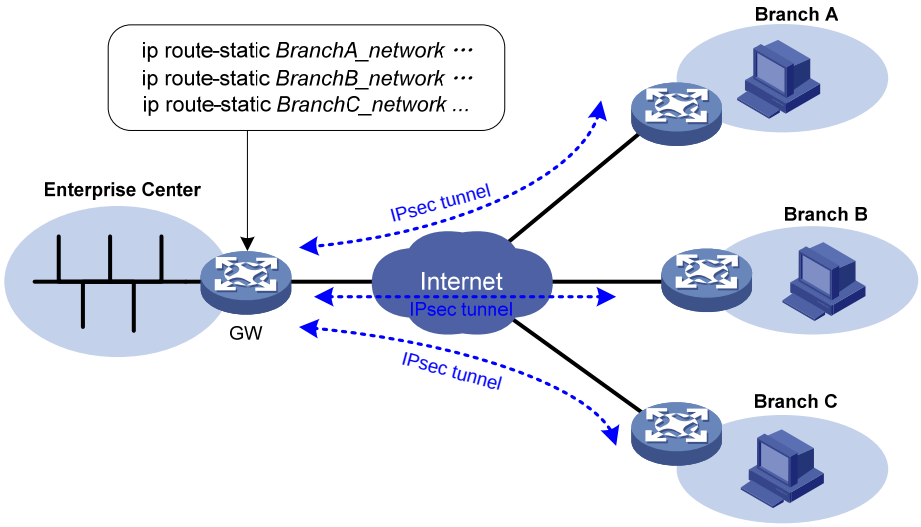
该方式可用于保护 IPv6 路由协议，目前支持保护 OSPFv3、IPv6 BGP、RIPng 路由协议。

由于 IPsec 的密钥交换机制仅仅适用于两点之间的通信保护，在广播网络一对多的情形下，IPsec 无法实现自动交换密钥，同样，由于广播网络一对多的特性，要求各设备对于接收、发送的报文均使用相同的 SA 参数（相同的 SPI 及密钥），因此该方式下必须手工配置用来保护 IPv6 路由协议报文的 IPsec SA。

1.1.5 IPsec反向路由注入功能

如 图 1-4 所示，某企业在企业分支与企业总部之间的所有流量通过IPsec进行保护，企业总部网关上需要配置静态路由，将总部发往分支的数据引到应用IPsec安全策略的接口上来。当企业分支众多或者内部网络规划发生变化时，就需要同时增加或调整总部网关上的静态路由配置，该项工作量大且容易出现配置错误。

图1-4 IPsec VPN 总部-分支组网图



RRI（Reverse Route Injection，反向路由注入）功能可以很好的解决以上问题。RRI 是一种自动添加到达 IPsec VPN 私网静态路由的机制，可以实现为受 IPsec 保护的流量自动添加静态路由的功能。如上 IPsec VPN 组网中，当企业总部侧网关设备 GW 上配置 RRI 功能后，每一个 IPsec 隧道建立之后，GW 都会自动为其添加一条相应的静态路由。通过 RRI 创建的路由表项可以在路由表中查询到，其目的地址为受保护的对端网络，下一跳地址为 IPsec 隧道的对端地址，它使得发往对端的流量被强制通过 IPsec 保护并转发。

RRI 创建的静态路由和手工配置的静态路由一样，可以向内网设备进行广播，允许内网设备选择合适的路由对 IPsec VPN 流量进行转发。

在 MPLS L3VPN 组网环境中，配置了 RRI 功能的网关设备能够依据应用 IPsec 安全策略的接口所绑定的 VPN 实例，在相应 VPN 实例的 IP 路由表中自动添加静态路由。

在大规模组网中，这种自动添加静态路由的机制可以简化用户配置，减少在企业总部网关设备上配置静态路由的工作量，并且可以根据 IPsec SA 的创建和删除进行静态路由的动态增加和删除，增强了 IPsec VPN 的可扩展性。

1.1.6 协议规范

与 IPsec 相关的协议规范有：

- RFC 2401：Security Architecture for the Internet Protocol
- RFC 2402：IP Authentication Header
- RFC 2406：IP Encapsulating Security Payload
- RFC 4552：Authentication/Confidentiality for OSPFv3

1.2 建立IPsec隧道的配置方式

注意

通常情况下，由于 IKE 协议采用 UDP 的 500 端口进行通信，IPsec 的 AH 和 ESP 协议分别使用 51 或 50 号协议来工作，因此为保障 IKE 和 IPsec 的正常运行，需要确保应用了 IKE 和 IPsec 配置的接口上没有禁止掉属于以上端口和协议的流量。

IPsec 隧道的建立有多种配置方式，请根据实际组网中对 IPsec 隧道的使用需求来选择配置方式：

- 基于ACL方式：由ACL来指定要保护的数据流范围，利用ACL的丰富配置功能，结合实际的组网环境灵活制定IPsec安全策略。该方式的配置方法为：通过配置IPsec安全策略并将IPsec安全策略绑定在接口上来完成IPsec的配置。具体配置请参见“1.3 基于ACL建立IPsec隧道”。在IPv4 网络和IPv6 网络中，基于ACL建立IPsec隧道的配置步骤相同。
- 基于业务方式：无需ACL来指定要保护的数据流，IPsec隧道直接与具体的业务绑定，保护某一业务的所有报文。目前，支持对IPv6 路由协议进行保护。该方式的配置方法为：配置手工方式的IPsec安全框架，并在IPv6 路由协议上应用安全框架来完成IPsec的配置。具体配置请参见“1.4 配置IPsec保护IPv6 路由协议”。

1.3 基于ACL建立IPsec隧道

1.3.1 基于ACL建立IPsec隧道配置任务简介

基于 ACL 建立 IPsec 隧道的基本配置思路如下：

(1) 配置 ACL：指定要保护的数据流。IPsec 不需要通过在 ACL 规则中指定 VPN 参数来保护 VPN 间的数据流。

(2) 配置 IPsec 安全提议：指定安全协议、认证算法、加密算法、封装模式等。

(3) 配置 IPsec 安全策略：一个 IPsec 安全策略是若干具有相同名字、不同顺序号的 IPsec 安全策略表项的集合。在同一个 IPsec 安全策略中，顺序号越小的 IPsec 安全策略表项优先级越高。IPsec 安全策略将要保护的数据流和 IPsec 安全提议进行了关联（即定义对何种数据流实施何种保护），并指定了 IPsec SA 的生成方式（手工方式、IKE 协商方式）、对等体 IP 地址（即保护路径的起点或终点）、所需要的密钥和 IPsec SA 的生存时间等。

(4) 在接口上应用 IPsec 安全策略。

表1-1 基于 ACL 建立 IPsec 隧道配置任务简介

配置任务		说明	详细配置
配置ACL		必选	1.3.2
配置IPsec安全提议		必选	1.3.3
配置IPsec安全策略	配置手工方式的安全策略	二者必选其一	1.3.4
	配置IKE协商方式的安全策略		1.3.5
在接口上应用IPsec安全策略		必选	1.3.6

配置任务	说明	详细配置
配置解封装后IPsec报文的ACL检查功能	可选	1.3.7
配置IPsec抗重放功能	可选	1.3.8
配置共享源接口安全策略	可选	1.3.9
配置QoS预分类功能	可选	1.3.10
配置IPsec报文日志记录功能	可选	1.3.11
设置IPsec隧道模式下封装后外层IP头的DF位	可选	1.3.12
配置IPsec反向路由注入功能	可选	1.3.13
配置IPsec告警功能	可选	1.5

1.3.2 配置ACL

1. ACL规则中关键字的使用

IPsec 通过配置 ACL 来定义需要保护的数据流。在 IPsec 应用中，ACL 规则中的 **permit** 关键字表示与之匹配的流量需要被 IPsec 保护，而 **deny** 关键字则表示与之匹配的流量不需要保护。一个 ACL 中可以配置多条规则，首个与数据流匹配上的规则决定了对该数据流的处理方式。

在IPsec安全策略中定义的ACL既可用于过滤接口入方向数据流，也可用于过滤接口出方向数据流。

- 设备出入方向的数据流都使用 IPsec 安全策略中定义的 ACL 规则来做匹配依据。具体是，出方向的数据流正向匹配ACL规则，入方向的数据流反向匹配ACL规则。例如，对于应用于IPsec安全策略中的某 ACL 规则：**rule** 0 **permit ip source** 1.1.1.0 0.0.0.255 **destination** 2.2.2.0 0.0.0.255，设备使用其正向过滤出方向上从 1.1.1.0/24 网段发往 2.2.2.0/24 网段的数据流，反向过滤入方向上从 2.2.2.0/24 网段发往 1.1.1.0/24 网段的数据流。
- 在出方向上，与 ACL 的 **permit** 规则匹配的报文将被 IPsec 保护，未匹配上任何规则或与 **deny** 规则匹配上的报文将不被 IPsec 保护。
- 在入方向上，与 ACL 的 **permit** 规则匹配上的未被 IPsec 保护的报文将被丢弃；目的地址为本机的被 IPsec 保护的报文将被进行解封装处理。缺省情况下解封装后的 IP 报文若能与 ACL 的 **permit** 规则匹配上则采取后续处理，否则被丢弃。若解封装后 IPsec 报文的 ACL 检查功能处于关闭状态，则解封装后的 IP 报文不与 ACL 匹配，直接进行后续处理。

需要注意的是：

- 仅对确实需要 IPsec 保护的数据流配置 **permit** 规则，避免盲目地使用关键字 **any**。这是因为，在一个 **permit** 规则中使用 **any** 关键字就代表所有指定范围上出方向的流量都需要被 IPsec 保护，所有对应入方向上被 IPsec 保护的报文将被接收并处理，入方向上未被 IPsec 保护的报文都将被丢弃。这种情况下，一旦入方向收到的某流量是未被 IPsec 保护的，那么该流量就会被丢弃，这会造成一些本不需要 IPsec 处理的流量丢失，影响正常的业务传输。
- 当一个安全策略下有多条优先级不同的安全策略表项时，合理使用 **deny** 规则。避免本应该与优先级较低的安全策略表项的 ACL **permit** 规则匹配而被 IPsec 保护的出方向报文，因为先与优先级较高的安全策略表项的 ACL **deny** 规则匹配上，而没有被 IPsec 保护，继而在接收端被丢弃。

下面是一个 **deny** 规则的错误配置示例。Router A 和 Router B 上分别配置如下所示的 IPsec 安全策略，当 Router A 连接的 1.1.2.0/24 网段用户访问 Router B 连接的 3.3.3.0/24 网段时，报文在 Router A 的应用了 IPsec 安全策略 testa 的出接口上优先与顺序号为 1 的安全策略表项匹配，并匹配上了 ACL 3000 的 rule 1，因此 Router A 认为它不需要 IPsec 保护，而未进行 IPsec 封装。该报文到达 Router B 后，在应用了 IPsec 安全策略 testb 的入接口上与 ACL 3001 的 rule 0 匹配，并被判断为应该受 IPsec 保护但未被保护的报文而丢弃。

Router A 上的关键配置如下：

```
acl number 3000
 rule 0 permit ip source 1.1.1.0 0.0.0.255 destination 2.2.2.0 0.0.0.255
 rule 1 deny ip
acl number 3001
 rule 0 permit ip source 1.1.2.0 0.0.0.255 destination 3.3.3.0 0.0.0.255
 rule 1 deny ip
#
ipsec policy testa 1 isakmp <---优先级高的安全策略表项
 security acl 3000
 ike-profile aa
 transform-set 1
#
ipsec policy testa 2 isakmp <---优先级低的安全策略表项
 security acl 3001
 ike-profile bb
 transform-set 1
```

Router B 上的关键配置如下：

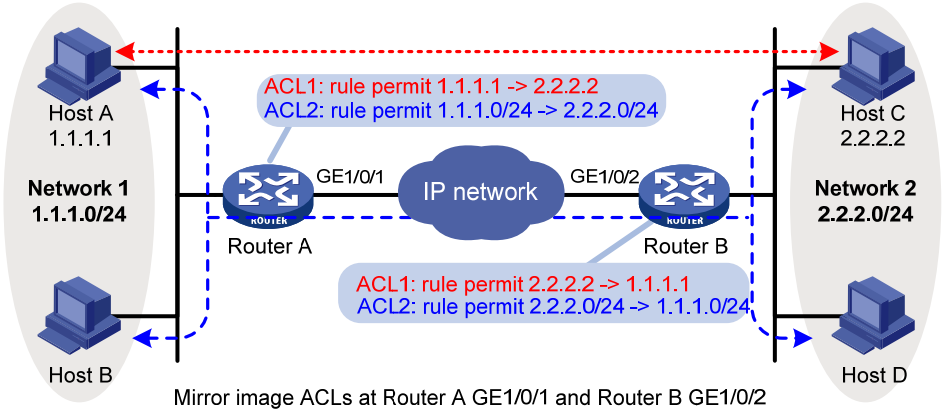
```
acl number 3001
 rule 0 permit ip source 3.3.3.0 0.0.0.255 destination 1.1.2.0 0.0.0.255
 rule 1 deny ip
#
ipsec policy testb 1 isakmp
 security acl 3001
 ike-profile aa
 transform-set 1
```

为保证 Router A 连接的 1.1.2.0/24 网段用户访问 Router B 连接的 3.3.3.0/24 网段的报文可被正确处理，建议将 Router A 上的 ACL 3000 中的 deny 规则删除。

2. ACL规则的镜像配置

为保证IPsec对等体上能够成功建立SA，建议两端设备上用于IPsec的ACL配置为镜像对称，即保证两端定义的要保护的数据流范围的源和目的尽量对称。例如，图 1-5 中Router A和Router B上的ACL配置都是完全镜像对称的，因此用于保护主机Host A与主机Host C之间、子网Network 1 与子网Network 2 之间流量的SA均可成功建立。

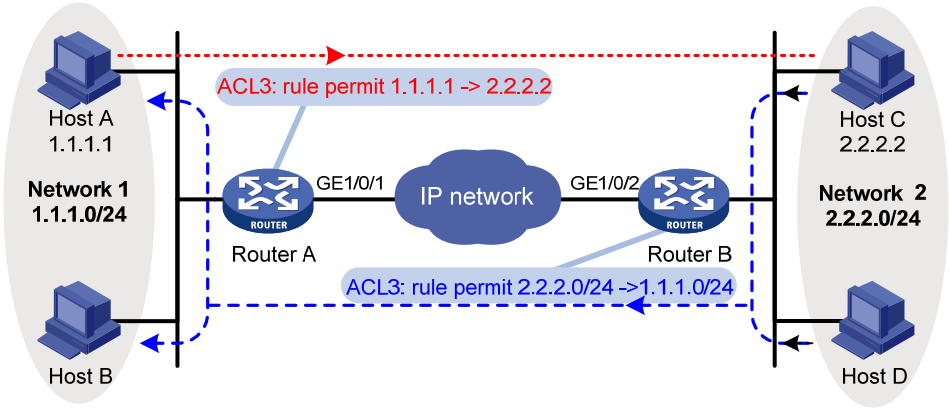
图1-5 镜像 ACL 配置



Mirror image ACLs at Router A GE1/0/1 and Router B GE1/0/2

若IPsec对等体上的ACL配置非镜像，那么只有在一端的ACL规则定义的范围是另外一端的子集时，SA协商可以成功。如 图 1-6 所示，Router A上的ACL规则允许的范围（Host A->Host C）是Router B上ACL规则允许的范围（Network 2->Network 1）的子集。

图1-6 非镜像 ACL 配置



需要注意的是，在这种 ACL 配置下，并不是任何一端发起的 SA 协商都可以成功，仅当保护范围小（细粒度）的一端向保护范围大（粗粒度）的一端发起的协商才能成功，反之则 SA 协商失败。这是因为，协商响应方要求协商发起方发送过来的数据必须在响应方可以接受的范围之内。其结果就是，从细粒度一端向粗粒度一端发送报文时，细粒度侧设备发起的 SA 协商可以成功，例如 Host A->Host C；从粗粒度一方向细粒度一方发送报文时，粗粒度侧设备发起的 SA 协商不能成功，例如 Host C->Host A、Host C->Host B、Host D->Host A 等。

1.3.3 配置IPsec安全提议

IPsec 安全提议是 IPsec 安全策略的一个组成部分，它用于定义 IPsec 需要使用的安全协议、加密/认证算法以及封装模式，为 IPsec 协商 SA 提供各种安全参数。

可对 IPsec 安全提议进行修改，但对已协商成功的 IPsec SA，新修改的安全提议并不起作用，即仍然使用原来的安全提议，只有新协商的 SA 使用新的安全提议。若要使修改对已协商成功的 IPsec SA 生效，则需要执行 **reset ipsec sa** 命令。

FIPS 模式下，若采用了 ESP 安全协议，则必须同时配置 ESP 加密算法和 ESP 认证算法。

表1-2 配置 IPsec 安全提议

操作		命令	说明
进入系统视图		**system-view**	-
创建IPsec安全提议，并进入IPsec安全提议视图		**ipsec transform-set** *transform-set-name*	缺省情况下，没有任何IPsec安全提议存在
配置IPsec安全提议采用的安全协议		**protocol** { **ah** | **ah-esp** | **esp** }	缺省情况下，采用ESP安全协议
配置安全算法	配置ESP协议采用的加密算法	非FIPS模式下： **esp encryption-algorithm { 3des-cbc | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | des-cbc | null } *** FIPS模式下： **esp encryption-algorithm { aes-cbc-128 | aes-cbc-192 | aes-cbc-256 } ***	只有采用ESP协议（**esp**或**ah-esp**）时必选 缺省情况下，ESP协议没有采用任何加密算法 此命令可以同时配置多个加密算法，算法优先级以配置顺序为准
	配置ESP协议采用的认证算法	非FIPS模式下： **esp authentication-algorithm { md5 | sha1 } *** FIPS模式下： **esp authentication-algorithm sha1**	只有采用ESP协议（**esp**或**ah-esp**）时必选 缺省情况下，ESP协议没有采用任何认证算法 此命令可以同时配置多个加密算法，算法优先级以配置顺序为准
	配置AH协议采用的认证算法	非FIPS模式下： **ah authentication-algorithm { md5 | sha1 } *** FIPS模式下： **ah authentication-algorithm sha1**	只有采用AH（**ah**或**ah-esp**）协议时必选 缺省情况下，AH协议没有采用任何认证算法 此命令可以同时配置多个加密算法，算法优先级以配置顺序为准
配置安全协议对IP报文的封装模式		**encapsulation-mode** { **transport** | **tunnel** }	缺省情况下，安全协议采用隧道模式对IP报文进行封装 传输模式必须应用于数据流的源地址和目的地址与IPsec隧道两端地址相同的情况下 若要配置应用于IPv6路由协议的手工安全策略，则该安全策略引用的安全提议仅支持传输模式的封装模式
（可选）配置使用IPsec安全策略发起协商时使用PFS特性		非FIPS模式下： **pfs { dh-group1 | dh-group2 | dh-group5 | dh-group14 | dh-group24 }** FIPS模式下： pfs dh-group14	缺省情况下，使用IPsec安全策略发起协商时不使用PFS特性 PFS（Perfect Forward Secrecy，完善的前向安全性）特性请参见“安全配置指导”中的“IKE” 发起方的PFS强度必须大于或等于响应方的PFS强度，否则协商会失败。不配置PFS特性的一端，按照对端的PFS特性要求进行IKE协商

1.3.4 配置手工方式的IPsec安全策略

1. 配置限制和指导

为保证 SA 能够成功生成，IPsec 隧道两端的配置必须符合以下要求：

- IPsec 安全策略引用的 IPsec 安全提议应采用相同的安全协议、加密/认证算法和报文封装模式。
- 当前端点的 IPv4 对端地址应与对端应用 IPsec 安全策略的接口的主 IPv4 地址保持一致；当前端点的 IPv6 对端地址应与对端应用 IPsec 安全策略的接口的第一个 IPv6 地址保持一致。
- 应分别设置 **inbound** 和 **outbound** 两个方向的 IPsec SA 参数，且保证每一个方向上的 IPsec SA 的唯一性：对于出方向 IPsec SA，必须保证三元组（对端 IP 地址、安全协议、SPI）唯一；对于入方向 IPsec SA，必须保证 SPI 唯一。
- 本端和对端 IPsec SA 的 SPI 及密钥必须是完全匹配的。即，本端的入方向 IPsec SA 的 SPI 及密钥必须和对端的出方向 IPsec SA 的 SPI 及密钥相同；本端的出方向 IPsec SA 的 SPI 及密钥必须和对端的入方向 IPsec SA 的 SPI 及密钥相同。
- 两端 IPsec SA 使用的密钥应当以相同的方式输入，即如果一端以字符串方式输入密钥，另一端必须也以字符串方式输入密钥。

2. 配置手工方式的IPsec安全策略

表1-3 配置手工方式的 IPsec 安全策略

操作	命令	说明
进入系统视图	**system-view**	-
创建一条手工方式的IPsec安全策略，并进入IPsec安全策略视图	**ipsec** { **ipv6-policy** | **policy** } *policy-name seq-number* **manual**	缺省情况下，不存在任何IPsec安全策略
（可选）配置IPsec安全策略的描述信息	**description** *text*	缺省情况下，无描述信息
指定IPsec安全策略引用的ACL	**security acl** [**ipv6**] { *acl-number* | **name** *acl-name* }	缺省情况下，IPsec安全策略没有引用任何ACL 一条安全策略只能引用一个ACL
指定IPsec安全策略所引用的安全提议	**transform-set** *transform-set-name*	缺省情况下，IPsec安全策略没有引用任何IPsec安全提议 一条手工方式的IPsec安全策略只能引用一个安全提议
指定IPsec隧道的对端IP地址	**remote-address** { *ipv4-address* | **ipv6** *ipv6-address* }	缺省情况下，未指定IPsec隧道的对端地址 IPsec隧道的本端IPv4地址为应用安全策略的接口的主IP地址；本端IPv6地址为应用安全策略的接口的第一个IPv6地址
配置IPsec SA的入方向SPI	**sa spi inbound** { **ah** | **esp** } *spi-number*	缺省情况下，不存在IPsec SA的入方向SPI

操作		命令	说明
配置IPsec SA的出方向SPI		**sa spi outbound { ah | esp }** *spi-number*	缺省情况下，不存在IPsec SA的出方向SPI
配置IPsec SA使用的密钥	配置AH协议的认证密钥（以16进制方式输入）	**sa hex-key authentication { inbound | outbound } ah { cipher | simple }** *key-value*	缺省情况下，未配置IPsec SA使用的密钥 根据本安全策略引用的安全提议中指定的安全协议，配置AH协议或ESP协议的密钥，或者两者都配置 对于ESP协议，以字符串方式输入密钥时，系统会自动地同时生成认证算法的密钥和加密算法的密钥 如果先后以不同的方式输入了密钥，则最后设定的密钥有效
	配置AH协议的认证密钥（以字符串方式输入）	**sa string-key { inbound | outbound } ah { cipher | simple }** *key-value*	
	配置ESP协议的认证密钥和加密密钥(以字符串方式输入）	**sa string-key { inbound | outbound } esp { cipher | simple }** *key-value*	
	配置ESP协议的认证密钥（以16进制方式输入）	**sa hex-key authentication { inbound | outbound } esp { cipher | simple }** *key-value*	
	配置ESP协议的加密密钥（以16进制方式输入）	**sa hex-key encryption { inbound | outbound } esp { cipher | simple }** *key-value*	

1.3.5 配置IKE协商方式的IPsec安全策略

IKE 协商方式的 IPsec 安全策略有以下两种配置方式：

- 直接配置 IPsec 安全策略：在安全策略视图中定义需要协商的各参数；
- 引用 IPsec 安全策略模板配置 IPsec 安全策略：首先在 IPsec 安全策略模板中定义需要协商的各参数，然后通过引用 IPsec 安全策略模板创建一条 IPsec 安全策略。应用了该类 IPsec 安全策略的接口不能发起协商，仅可以响应远端设备的协商请求。由于 IPsec 安全策略模板中未定义的可选参数由发起方来决定，而响应方会接受发起方的建议，因此这种方式适用于通信对端（例如对端的 IP 地址）未知的情况下，允许这些对端设备向本端设备主动发起协商。

1. 配置限制和指导

IPsec 隧道两端的配置必须符合以下要求：

- IPsec 安全策略引用的 IPsec 安全提议中应包含具有相同的安全协议、认证/加密算法和报文封装模式的 IPsec 安全提议。
- IPsec 安全策略引用的 IKE profile 参数相匹配。
- 一条 IKE 协商方式的 IPsec 安全策略中最多可以引用六个 IPsec 安全提议。IKE 协商过程中，IKE 将会在隧道两端配置的 IPsec 安全策略中查找能够完全匹配的 IPsec 安全提议。如果 IKE 在两端找不到完全匹配的 IPsec 安全提议，则 SA 不能协商成功，需要被保护的报文将被丢弃。
- IKE 协商的发起方必须配置 IPsec 隧道的对端地址，响应方可选配，且当前端点的对端地址与对端的本端地址应保持一致。

对于 IKE 协商建立的 IPsec SA，遵循以下原则：

- 采用隧道两端设置的 IPsec SA 生存时间中较小者。
- 可同时存在基于时间和基于流量两种方式的 IPsec SA 生存时间，只要到达指定的时间或指定的流量，IPsec SA 就会老化。

2. 直接配置IKE协商方式的IPsec安全策略

表1-4 直接配置 IKE 协商方式的 IPsec 安全策略

操作	命令	说明
进入系统视图	**system-view**	-
创建一条IKE协商方式的IPsec安全策略，并进入IPsec安全策略视图	**ipsec** { **ipv6-policy** | **policy** } *policy-name seq-number* **isakmp**	缺省情况下，不存在任何IPsec安全策略
（可选）配置IPsec安全策略的描述信息	**description** *text*	缺省情况下，无描述信息
指定IPsec安全策略引用的ACL	**security acl** [**ipv6**] { *acl-number* | **name** *acl-name* } [**aggregation** | **per-host**]	缺省情况下，IPsec安全策略没有指定ACL 一条IPsec安全策略只能引用一个ACL
指定IPsec安全策略引用的IPsec安全提议	**transform-set** *transform-set-name*&<1-6>	缺省情况下，IPsec安全策略没有引用任何IPsec安全提议
指定IPsec安全策略引用的IKE profile	**ike-profile** *profile-name*	缺省情况下，IPsec安全策略没有引用任何IKE profile。若系统视图下配置了IKE profile，则使用系统视图下配置的IKE profile进行性协商，否则使用全局的IKE参数进行协商 只能引用一个IKE profile，且不能引用已经被其它IPsec安全策略或IPsec安全策略模板引用的IKE profile IKE profile的相关配置请参见“安全配置指导”中的“IKE”
指定IPsec隧道的本端IP地址	**local-address** { *ipv4-address* | **ipv6** *ipv6-address* }	缺省情况下，IPsec隧道的本端IPv4地址为应用IPsec安全策略的接口的主IPv4地址，本端IPv6地址为应用IPsec安全策略的接口的第一个IPv6地址 此处指定的IPsec隧道本端IP地址必须与IKE使用的标识本端身份的IP地址一致
指定IPsec隧道的对端IP地址	**remote-address** { [**ipv6**] *host-name* | *ipv4-address* | **ipv6** *ipv6-address* }	缺省情况下，未指定IPsec隧道的对端IP地址
配置IPsec SA的生存时间	**sa duration** { **time-based** *seconds* | **traffic-based** *kilobytes* }	缺省情况下，IPsec安全策略下的IPsec SA生存时间为当前全局的IPsec SA生存时间
（可选）配置IPsec SA的空闲超时时间	**sa idle-time** *seconds*	缺省情况下，IPsec安全策略下的IPsec SA空闲超时时间为当前全局的IPsec SA空闲超时时间

操作	命令	说明
退回系统视图	**quit**	-
配置全局的IPsec SA生存时间	**ipsec sa global-duration** { **time-based** *seconds* | **traffic-based** *kilobytes* }	缺省情况下，IPsec SA基于时间的生存时间为3600秒，基于流量的生存时间为1843200千字节
（可选）开启全局的IPsec SA空闲超时功能，并配置全局IPsec SA空闲超时时间	**ipsec sa idle-time** *seconds*	缺省情况下，全局的IPsec SA空闲超时功能处于关闭状态

3. 引用IPsec安全策略模板配置IKE协商方式的IPsec安全策略

IPsec 安全策略模板与直接配置的 IKE 协商方式的 IPsec 安全策略中可配置的参数类似，但是配置较为简单，除了 IPsec 安全提议和 IKE profile 之外的其它参数均为可选。应用了引用 IPsec 安全策略模板配置的 IPsec 安全策略的接口不能发起协商，仅可以响应远端设备的协商请求。IPsec 安全策略模板中未定义的可选参数由发起方来决定，而响应方会接受发起方的建议，例如 IPsec 安全策略模板下的用于定义保护对象范围的 ACL 是可选的，该参数在未配置的情况下，相当于支持最大范围的保护，即完全接受协商发起端的 ACL 设置。这种方式配置的 IPsec 安全策略适用于通信对端（例如对端的 IP 地址）未知的情况下，允许这些对端设备向本端设备主动发起协商。

表1-5 引用 IPsec 安全策略模板配置 IKE 协商方式的 IPsec 安全策略

操作	命令	说明
进入系统视图	**system-view**	-
创建一个IPsec安全策略模板，并进入IPsec安全策略模板视图	**ipsec** { **ipv6-policy-template** | **policy-template** } *template-name seq-number*	缺省情况下，不存在任何IPsec安全策略模板
（可选）配置IPsec安全策略模板的描述信息	**description** *text*	缺省情况下，无描述信息
（可选）指定IPsec安全策略模板引用的ACL	**security acl** [**ipv6**] { *acl-number* | **name** *acl-name* } [**aggregation** | **per-host**]	缺省情况下，IPsec安全策略模板没有指定ACL 一条IPsec安全策略模板只能引用一个ACL
指定IPsec安全策略模板引用的安全提议	**transform-set** *transform-set-name*&<1-6>	缺省情况下IPsec安全策略模板没有引用任何IPsec安全提议
指定IPsec安全策略模板引用的IKE profie	**ike-profile** *profile-name*	缺省情况下，IPsec安全策略模板没有引用任何IKE profie 只能引用一个IKE profile，且不能引用已经被其它IPsec安全策略或IPsec安全策略模板引用的IKE profie IKE profile的相关配置请参见“安全配置指导”中的“IKE”

操作	命令	说明
（可选）指定IPsec隧道的本端IP地址	**local-address** { *ipv4-address* | **ipv6** *ipv6-address* }	缺省情况下，IPsec隧道的本端IPv4地址为应用IPsec安全策略的接口的主IPv4地址，本端IPv6地址为应用IPsec安全策略的接口的第一个IPv6地址 此处指定的IPsec隧道本端IP地址必须与IKE对等体使用的标识本端身份的IP地址一致
（可选）指定IPsec隧道的对端IP地址	**remote-address** { [**ipv6**] *host-name* | *ipv4-address* | **ipv6** *ipv6-address* }	缺省情况下，未指定IPsec隧道的对端IP地址
配置IPsec SA的生存时间	**sa duration** { **time-based** *seconds* | **traffic-based** *kilobytes* }	缺省情况下，IPsec安全策略模板下的IPsec SA生存时间为当前全局的IPsec SA生存时间
（可选）配置IPsec SA的空闲超时时间	**sa idle-time** *seconds*	缺省情况下，IPsec安全策略模板下的IPsec SA空闲超时时间为当前全局的IPsec SA空闲超时时间
退回系统视图	**quit**	-
配置全局的IPsec SA生存时间	**ipsec sa global-duration** { **time-based** *seconds* | **traffic-based** *kilobytes* }	缺省情况下，IPsec SA基于时间的生存时间为3600秒，基于流量的生存时间为1843200千字节
（可选）开启全局的IPsec SA空闲超时功能，并配置全局IPsec SA空闲超时时间	**ipsec sa idle-time** *seconds*	缺省情况下，全局的IPsec SA空闲超时功能处于关闭状态
引用安全策略模板创建一条IKE协商方式的安全策略	**ipsec** { **ipv6-policy** | **policy** } *policy-name seq-number* **isakmp template** *template-name*	缺省情况下，没有任何IPsec安全策略存在

1.3.6 在接口上应用IPsec安全策略

为使定义的 IPsec SA 生效，应在每个要加密的数据流和要解密的数据流所在接口上应用一个 IPsec 安全策略，以对数据进行保护。当取消 IPsec 安全策略在接口上的应用后，此接口便不再具有 IPsec 的安全保护功能。IPsec 安全策略除了可以应用到串口、以太网接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，对 GRE、L2TP 等流量进行保护。

当从一个接口发送数据时，接口将按照顺序号从小到大的顺序逐一匹配引用的 IPsec 安全策略中的每一条安全策略表项。如果数据匹配上了某一条安全策略表项引用的 ACL，则停止匹配，并对其使用当前这条安全策略表项进行处理，即根据已经建立的 IPsec SA 或者触发 IKE 协商生成的 IPsec SA 对报文进行封装处理；如果数据与所有安全策略表项引用的 ACL 都不匹配，则直接被正常转发，IPsec 不对数据加以保护。

应用了 IPsec 安全策略的接口收到数据报文时，对于目的地址是本机的 IPsec 报文，根据报文头里携带的 SPI 查找本地的 IPsec SA，并根据匹配的 IPsec SA 对报文进行解封装处理；对于那些本应该被 IPsec 保护但未被保护的报文进行丢弃。

表1-6 在接口上应用 IPsec 安全策略

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
应用IPsec安全策略	**ipsec apply** { **policy** | **ipv6-policy** } *policy-name*	缺省情况下，接口上没有应用任何IPsec安全策略 一个接口只能应用一个IPsec安全策略。IKE方式的IPsec安全策略可以应用到多个接口上，手工方式的IPsec安全策略只能应用到一个接口上
指定转发当前接口流量的业务处理板（MSR 5600）	**service slot** *slot-number*	缺省情况下，没有指定转发当前接口流量的业务处理板 仅在全局逻辑接口（例如VLAN接口、Tunnel接口）上应用IPsec安全策略时，必选

1.3.7 配置解封装后IPsec报文的ACL检查功能

在隧道模式下，接口入方向上解封装的 IPsec 报文的内部 IP 头有可能不在当前 IPsec 安全策略引用的 ACL 的保护范围内，如网络中一些恶意伪造的攻击报文就可能有此问题，所以设备需要重新检查解封装后的报文的 IP 头是否在 ACL 保护范围内。使能该功能后可以保证 ACL 检查不通过的报文被丢弃，从而提高网络安全性。

表1-7 配置解封装后 IPsec 报文的 ACL 检查功能

操作	命令	说明
进入系统视图	**system-view**	-
开启解封装后IPsec报文的ACL检查功能	**ipsec decrypt-check enable**	缺省情况下，解封装后IPsec报文的ACL检查功能处于开启状态

1.3.8 配置IPsec抗重放功能

注意

- IPsec 抗重放检测功能缺省是使能的，是否关闭该功能请根据实际需求慎重使用。
- 使用较大的抗重放窗口宽度会引起系统开销增大，导致系统性能下降，与抗重放检测用于降低系统在接收重放报文时的开销的初衷不符，因此建议在能够满足业务运行需要的情况下，使用较小的抗重放窗口宽度。
- 一般情况下，MSR 5600 直接在接收报文的单板上进行业务处理。但 IPsec 抗重放功能检测要求同一个全局虚拟接口上发送和接收的流量必须在同一个单板上处理，此时需要在该接口上通过 **sevice** 命令指定转发当前接口流量的单板。

重放报文，通常是指设备再次接收到的已经被 IPsec 处理过的报文。IPsec 通过滑动窗口（抗重放窗口）机制检测重放报文。AH 和 ESP 协议报文中带有序列号，如果收到的报文的序列号与已经解封装过的报文序列号相同，或收到的报文的序列号出现得较早，即已经超过了抗重放窗口的范围，则认为该报文为重放报文。

对重放报文的解封装无意义，并且解封装过程涉及密码学运算，会消耗设备大量的资源，导致业务可用性下降，造成了拒绝服务攻击。通过使能 IPsec 抗重放检测功能，将检测到的重放报文在解封装处理之前丢弃，可以降低设备资源的消耗。

在某些特定环境下，业务数据报文的接收顺序可能与正常的顺序差别较大，虽然并非有意的重放攻击，但会被抗重放检测认为是重放报文，导致业务数据报文被丢弃，影响业务的正常运行。因此，这种情况下就可以通过关闭 IPsec 抗重放检测功能来避免业务数据报文的错误丢弃，也可以通过适当地增大抗重放窗口的宽度，来适应业务正常运行的需要。

只有 IKE 协商的 IPsec SA 才能够支持抗重放检测，手工方式生成的 IPsec SA 不支持抗重放检测。因此该功能使能与否对手工方式生成的 IPsec SA 没有影响。

表1-8 配置 IPsec 抗重放功能

操作	命令	说明
进入系统视图	**system-view**	-
开启IPsec抗重放检测功能	**ipsec anti-replay check**	缺省情况下，IPsec抗重放检测功能处于开启状态
配置IPsec抗重放窗口宽度	**ipsec anti-replay window** *width*	缺省情况下，IPsec抗重放窗口宽度为64

1.3.9 配置共享源接口IPsec安全策略

为了提高网络的可靠性，通常核心设备到 ISP（Internet Service Provider，互联网服务提供商）都会有两条出口链路，它们互为备份或者为负载分担的关系。由于在不同的接口上应用安全策略时，各个接口将分别协商生成 IPsec SA。因此，则在主备链路切换时，接口状态的变化会触发重新进行 IKE 协商，从而导致数据流的暂时中断。这种情况下，两个接口上的 IPsec SA 就需要能够平滑切换。

通过将一个 IPsec 安全策略与一个源接口绑定，使之成为共享源接口 IPsec 安全策略，可以实现主备链路切换时受 IPsec 保护的业务流量不中断。具体机制为：应用相同 IPsec 安全策略的多个物理

接口共同使用一个指定的源接口（称为共享源接口）协商 IPsec SA，当这些物理接口对应的链路切换时，如果该源接口的状态不变化，就不会删除该接口协商出的 IPsec SA，也不需要重新触发 IKE 协商，各物理接口继续使用已有的 IPsec SA 保护业务流量。

对于本配置，有以下配置限制和注意事项：

- 只有 IKE 协商方式的 IPsec 安全策略才能配置为 IPsec 共享源接口安全策略。
- 一个 IPsec 安全策略只能与一个源接口绑定。
- 一个源接口可以同时与多个 IPsec 安全策略绑定。
- 删除与共享源接口 IPsec 安全策略绑定的共享源接口时，将使得该共享源接口 IPsec 安全策略恢复为普通 IPsec 安全策略。
- 若一个 IPsec 安全策略为共享源接口 IPsec 安全策略，但该 IPsec 安全策略中未指定隧道本端地址，则 IKE 将使用共享源接口地址作为 IPsec 隧道的本端地址进行 IKE 协商；如果共享源接口 IPsec 安全策略中指定了隧道本端地址，则将使用指定的隧道本端地址进行 IKE 协商。

表1-9 配置共享源接口 IPsec 安全策略

操作	命令	说明
进入系统视图	**system-view**	-
配置IPsec安全策略为IPsec共享源接口安全策略	**ipsec** { **ipv6-policy** | **policy** } *policy-name* **local-address** *interface-type interface-nunmber*	缺省情况下，IPsec安全策略不是共享源接口IPsec安全策略，即未将IPsec安全策略与任何源接口绑定

1.3.10 配置QoS预分类功能

当在接口上同时应用了 IPsec 安全策略与 QoS 策略时，缺省情况下，QoS 使用封装后报文的外层 IP 头信息来对报文进行分类。但如果希望 QoS 基于被封装报文的原始 IP 头信息对报文进行分类，则需要配置 QoS 预分类功能来实现。

关于 QoS 策略及 QoS 分类的相关介绍请参见“ACL 和 QoS 配置指导”中的“QoS 配置方式”。

表1-10 配置 QoS 预分类功能

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	IPsec安全策略视图	**ipsec** { **policy** | **ipv6-policy** } *policy-name seq-number* [**isakmp** | **manual**]	-
	IPsec安全策略模板视图	**ipsec** { **policy-template** | **ipv6-policy-template** } *template-name seq-number*	
开启QoS预分类功能		**qos pre-classify**	缺省情况下，QoS预分类功能处于关闭状态

1.3.11 配置IPsec报文日志信息记录功能

开启 IPsec 报文日志记录功能后，设备会在丢弃 IPsec 报文的情况下，例如入方向找不到对应的 IPsec SA、AH/ESP 认证失败、ESP 加密失败等时，输出相应的日志信息，该日志信息内容主要包括报文的源和目的 IP 地址、报文的 SPI 值、报文的序列号信息，以及设备丢包的原因。

表1-11 配置 IPsec 日志信息记录功能

操作	命令	说明
进入系统视图	**system-view**	-
开启IPsec报文日志记录功能	**ipsec logging packet enable**	缺省情况下，IPsec报文日志记录功能处于关闭状态

1.3.12 设置IPsec隧道模式下封装后外层IP头的DF位

IP 报文头中的 DF（Don't Fragment，不分片）位用于控制报文是否允许被分片。在隧道模式下，IPsec 会在原始报文外封装一个新的 IP 头，称为外层 IP 头。IPsec 的 DF 位设置功能允许用户设置 IPsec 封装后的报文外层 IP 头的 DF 位，并支持以下三种设置方式：

- **clear**：表示清除外层 IP 头的 DF 位，IPsec 封装后的报文可被分片。
- **set**：表示设置外层 IP 头的 DF 位，IPsec 封装后的报文不能被分片。
- **copy**：表示外层 IP 头的 DF 位从原始报文 IP 头中拷贝。

封装后外层 IP 头的 DF 位可以在接口视图和系统视图下分别配置，接口视图下的配置优先级高。如果接口下未设置外层 IP 头的 DF 位，则按照系统视图下的全局配置来决定如何设置封装后外层 IP 头的 DF 位。

对于本配置，有以下配置限制和注意事项：

- 该功能仅在 IPsec 的封装模式为隧道模式时有效，仅用于设置 IPsec 隧道模式封装后的外层 IP 头的 DF 位，原始报文 IP 头的 DF 位不会被修改。
- 如果有多个接口应用了共享源接口安全策略，则这些接口上必须使用相同的 DF 位设置。
- 转发报文时对报文进行分片、重组，可能会导致报文的转发延时较大。若设置了封装后 IPsec 报文的 DF 位，则不允许对 IPsec 报文进行分片，可以避免引入分片延时。这种情况下，要求 IPsec 报文转发路径上各个接口的 MTU 大于 IPsec 报文长度，否则，会导致 IPsec 报文被丢弃。如果无法保证转发路径上各个接口的 MTU 大于 IPsec 报文长度，则建议清除 DF 位。

表1-12 在接口下设置 IPsec 封装后外层 IP 头的 DF 位

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
为当前接口设置IPsec封装后外层IP头的DF位	**ipsec df-bit** { **clear** | **copy** | **set** }	缺省情况下，接口下未设置IPsec封装后外层IP头的DF位，采用全局设置的DF位

表1-13 全局设置 IPsec 封装后外层 IP 头的 DF 位

操作	命令	说明
进入系统视图	**system-view**	-
为所有接口设置IPsec封装后外层IP头的DF位	**ipsec global-df-bit** { **clear** | **copy** | **set** }	缺省情况下，IPsec封装后外层IP头的DF位从原始报文IP头中拷贝

1.3.13 配置IPsec反向路由注入功能

在企业中心侧网关设备上的 IPsec 安全策略视图/IPsec 安全策略模板视图下开启 IPsec 反向路由注入（RRI）功能后，设备会根据协商的 IPsec SA 自动生成一条静态路由，该路由的目的地址为受保护的对端私网，下一跳地址为 IPsec 隧道的对端地址。对于 RRI 生成的静态路由，可以为其配置优先级，从而更灵活地应用路由管理策略。例如：当设备上还有其他方式配置到达相同目的地的路由时，如果为它们指定相同的优先级，则可实现负载分担，如果指定不同的优先级，则可实现路由备份。同时，还可以通过修改静态路由的 Tag 值，使得设备能够在路由策略中根据 Tag 值对这些 RRI 生成的静态路由进行灵活的控制。

需要注意的是：

- 开启 RRI 功能时，会删除相应 IPsec 安全策略协商出的所有 IPsec SA。当有新的流量触发生成 IPsec SA 时，根据新协商的 IPsec 生成路由信息。
- 关闭 RRI 功能时，会删除相应 IPsec 安全策略协商出的所有 IPsec SA。
- RRI 生成的静态路由随 IPsec SA 的创建而创建，随 IPsec SA 的删除而删除。
- RRI 功能在隧道模式和传输模式下都支持。
- 若修改了 RRI 生成的静态路由的优先级或 Tag 属性，则会删除由相应 IPsec 安全策略建立的 IPsec SA 和已添加的静态路由，修改后的属性值在下次生成 IPsec SA 且添加静态路由时生效。
- 在 RRI 功能开启的情况下，对于与未指定目的 IP 地址的 ACL 规则相匹配的报文流触发协商出的 IPsec SA，设备并不会为其自动生成一条静态路由。因此，如果 IPsec 安全策略/IPsec 安全策略模板引用了此类型的 ACL 规则，则需要通过手工配置一条到达对端受保护网络的静态路由。

表1-14 配置 IPsec 反向路由注入功能

操作	命令	说明
进入系统视图	**system-view**	-
进入IPsec安全策略视图	**ipsec** { **policy** | **ipv6-policy** } *policy-name seq-number* **isakmp**	二者必选其一
进入IPsec安全策略模板视图	**ipsec** { **policy-template** | **ipv6-policy-template** } *template-name seq-number*	
开启IPsec反向路由注入功能	**reverse-route dynamic**	缺省情况下，IPsec反向路由注入功能处于关闭状态
（可选）配置IPsec反向路由功能生成的静态路由的优先级	**reverse-route preference** *number*	缺省情况下，IPsec反向路由注入功能生成的静态路由的优先级为60

操作	命令	说明
（可选）配置IPsec反向路由功能生成的静态路由的Tag值	**reverse-route tag** *tag-value*	缺省情况下，IPsec反向路由注入功能生成的静态路由的tag值为0

1.4 配置IPsec保护IPv6路由协议

1.4.1 IPsec保护IPv6 路由协议配置任务简介

使用 IPsec 安全策略建立 IPsec 隧道保护 IPv6 路由协议的基本配置思路如下：

(1) 配置 IPsec 安全提议：指定安全协议、认证算法和加密算法、封装模式等；

(2) 配置手工方式的 IPsec 安全框架：指定 SA 的 SPI 和密钥；

(3) 在路由协议上应用手工方式的 IPsec 安全框架。

表1-15 IPsec 保护 IPv6 路由协议配置任务简介

配置任务	说明	详细配置
配置IPsec安全提议	必选	1.3.3
配置手工方式的IPsec安全框架	必选	1.3.4
在路由协议上应用IPsec安全框架	必选	分别参考“三层技术-IP路由配置指导”中的“IPv6 BGP”、“OSPFv3”和“RIPng”
配置IPsec报文日志记录功能	可选	1.3.11
配置IPsec告警功能	可选	1.5

1.4.2 配置手工方式的IPsec安全框架

一个 IPsec 安全框架相当于一个 IPsec 安全策略，与 IPsec 安全策略不同的是，IPsec 安全框架由名字唯一确定，且不支持引用 ACL。IPsec 安全框架定义了对数据流进行 IPsec 保护所使用的安全提议，以及 SA 的 SPI、SA 使用的密钥。

IPsec 隧道两端的配置必须符合以下要求：

- IPsec 安全框架引用的 IPsec 安全提议应采用相同的安全协议、加密/认证算法和报文封装模式。
- 本端出方向 IPsec SA 的 SPI 和密钥必须和本端入方向 IPsec SA 的 SPI 和密钥保持一致。
- 同一个范围内的、所有设备上的 IPsec SA 的 SPI 和密钥均要保持一致。该范围与协议相关：对于 OSPF，是 OSPF 邻居之间或邻居所在的区域；对于 RIPng，是 RIPng 直连邻居之间或邻居所在的进程；对于 BGP，是 BGP 邻居之间或邻居所在的一个组。
- 两端 IPsec SA 使用的密钥应当以相同的方式输入，即如果一端以字符串方式输入密钥，另一端必须也以字符串方式输入密钥。

表1-16 配置手工方式的 IPsec 安全框架

操作		命令	说明
进入系统视图		**system-view**	-
创建一个手工方式的IPsec安全框架，并进入IPsec安全框架视图		**ipsec profile** *profile-name* **manual**	缺省情况下，没有任何IPsec安全框架存在 进入已创建的IPsec安全框架时，可以不指定协商方式**manual**
（可选）配置IPsec安全框架的描述信息		**description** *text*	缺省情况下，无描述信息
指定IPsec安全框架引用的IPsec安全提议		**transform-set** *transform-set-name*	缺省情况下，IPsec安全框架没有引用任何IPsec安全提议 要引用的IPsec安全提议所采用的封装模式必须为传输模式
配置IPsec SA的SPI		**sa spi** { **inbound** | **outbound** } { **ah** | **esp** } *spi-number*	缺省情况下，未配置IPsec SA的SPI
配置IPsec SA使用的密钥	配置AH协议的认证密钥（以16进制方式输入）	**sa hex-key authentication** { **inbound** | **outbound** } **ah** { **cipher** | **simple** } *key-value*	缺省情况下，未配置IPsec SA使用的密钥 根据本安全框架引用的安全提议中指定的安全协议，配置AH协议或ESP协议的密钥，或者两者都配置 对于ESP协议，以字符串方式输入密钥时，系统会自动地同时生成认证算法的密钥和加密算法的密钥 如果先后以不同的方式输入了密钥，则最后设定的密钥有效
	配置AH协议的认证密钥（以字符串方式输入）	**sa string-key** { **inbound** | **outbound** } **ah** { **cipher** | **simple** } *key-value*	
	配置ESP协议的认证密钥和加密密钥（以字符串方式输入）	**sa string-key** { **inbound** | **outbound** } **esp** { **cipher** | **simple** } *key-value*	
	配置ESP协议的认证密钥（以16进制方式输入）	**sa hex-key authentication** { **inbound** | **outbound** } **esp** { **cipher** | **simple** } *key-value*	
	配置ESP协议的加密密钥（以16进制方式输入）	**sa hex-key encryption** { **inbound** | **outbound** } **esp** { **cipher** | **simple** } *key-value*	

1.5 配置IPsec告警功能

开启 IPsec 的 Trap 功能后，IPsec 会生成告警信息，用于向网管软件报告该模块的重要事件。生成的告警信息将被发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

如果希望生成并输出某种类型的 IPsec 告警信息，则需要保证 IPsec 的全局告警功能以及相应类型的告警功能均处于开启状态。

表1-17 配置 IPsec 告警功能

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
开启IPsec的全局告警功能	**snmp-agent trap enable ipsec global**	缺省情况下，IPsec的全局告警功能处于关闭状态
开启IPsec的指定告警功能	**snmp-agent trap enable ipsec** [**auth-failure** | **decrypt-failure** | **encrypt-failure** | **invalid-sa-failure** | **no-sa-failure** | **policy-add** | **policy-attach** | **policy-delete** | **policy-detach** | **tunnel-start** | **tunnel-stop**] *	缺省情况下，IPsec的所有告警功能均处于关闭状态

1.6 IPsec显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 IPsec 的运行情况，通过查看显示信息认证配置的效果。

在用户视图下执行 **reset** 命令可以清除 IPsec 统计信息。

表1-18 IPsec 显示和维护

操作	命令
显示IPsec安全策略的信息	**display ipsec** { **ipv6-policy** | **policy** } [*policy-name* [*seq-number*]]
显示IPsec安全策略模板的信息	**display ipsec** { **ipv6-policy-template** | **policy-template** } [*template-name* [*seq-number*]]
显示IPsec安全框架的信息	**display ipsec profile** [*profile-name*]
显示IPsec安全提议的信息	**display ipsec transform-set** [*transform-set-name*]
显示IPsec SA的相关信息	**display ipsec sa** [**brief** | **count** | **interface** *interface-type interface-number* | { **ipv6-policy** | **policy** } *policy-name* [*seq-number*] | **profile** *policy-name* | **remote** [**ipv6**] *ip-address*]
显示IPsec处理报文的统计信息	**display ipsec statistics** [**tunnel-id** *tunnel-id*]
显示IPsec隧道的信息	**display ipsec tunnel** { **brief** | **count** | **tunnel-id** *tunnel-id* }
清除已经建立的IPsec SA	**reset ipsec sa** [{ **ipv6-policy** | **policy** } *policy-name* [*seq-number*] | **profile** *policy-name* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } | **spi** { *ipv4-address* | **ipv6** *ipv6-address* } { **ah** | **esp** } *spi-num*]
清除IPsec的报文统计信息	**reset ipsec statistics** [**tunnel-id** *tunnel-id*]

1.7 IPsec典型配置举例

1.7.1 采用手工方式建立保护IPv4 报文的IPsec隧道

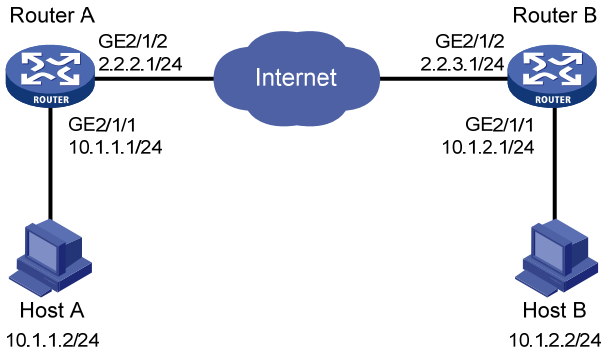
1. 组网需求

在 Router A 和 Router B 之间建立一条 IPsec 隧道，对 Host A 所在的子网（10.1.1.0/24）与 Host B 所在的子网（10.1.2.0/24）之间的数据流进行安全保护。具体要求如下：

- 封装形式为隧道模式。
- 安全协议采用 ESP 协议。
- 加密算法采用采用 128 比特的 AES，认证算法采用 HMAC-SHA1。
- 手工方式建立 IPsec SA。

2. 组网图

图1-7 保护 IPv4 报文的 IPsec 配置组网图



3. 配置步骤

(1) 配置 Router A

配置各接口的 IP 地址，具体略。

配置一个 ACL，定义要保护由子网 10.1.1.0/24 去往子网 10.1.2.0/24 的数据流。

```
<RouterA> system-view
[RouterA] acl number 3101
[RouterA-acl-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0
0.0.0.255
[RouterA-acl-adv-3101] quit
```

配置到达 Host B 所在子网的静态路由。2.2.2.3 为本例中的直连下一跳地址，实际使用中请以具体组网情况为准。

```
[RouterA] ip route-static 10.1.2.0 255.255.255.0 gigabitethernet 2/1/2 2.2.2.3
```

创建 IPsec 安全提议 tran1。

```
[RouterA] ipsec transform-set tran1
```

配置安全协议对 IP 报文的封装形式为隧道模式。

```
[RouterA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

配置采用的安全协议为 ESP。

```
[RouterA-ipsec-transform-set-tran1] protocol esp
```

配置 ESP 协议采用的加密算法为采用 128 比特的 AES，认证算法为 HMAC-SHA1。

```
[RouterA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[RouterA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterA-ipsec-transform-set-tran1] quit
```

创建一条手工方式的 IPsec 安全策略，名称为 map1，序列号为 10。

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

指定引用 ACL 3101。

```
[RouterA-ipsec-policy-manual-map1-10] security acl 3101
```
指定引用的 IPsec 安全提议为 tran1。
```
[RouterA-ipsec-policy-manual-map1-10] transform-set tran1
```
指定 IPsec 隧道对端 IP 地址为 2.2.3.1。
```
[RouterA-ipsec-policy-manual-map1-10] remote-address 2.2.3.1
```
配置 ESP 协议的出方向 SPI 为 12345，入方向 SPI 为 54321。
```
[RouterA-ipsec-policy-manual-map1-10] sa spi outbound esp 12345
[RouterA-ipsec-policy-manual-map1-10] sa spi inbound esp 54321
```
配置 ESP 协议的出方向 SA 的密钥为明文字符串 abcdefg，入方向 SA 的密钥为明文字符串 gfedcba。
```
[RouterA-ipsec-policy-manual-map1-10] sa string-key outbound esp simple abcdefg
[RouterA-ipsec-policy-manual-map1-10] sa string-key inbound esp simple gfedcba
[RouterA-ipsec-policy-manual-map1-10] quit
```
在接口 GigabitEthernet2/1/2 上应用 IPsec 安全策略 map1。
```
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ip address 2.2.2.1 255.255.255.0
[RouterA-GigabitEthernet2/1/2] ipsec apply policy map1
[RouterA-GigabitEthernet2/1/2] quit
```
(2) 配置 Router B

配置各接口的 IP 地址，具体略。

配置一个 ACL，定义要保护由子网 10.1.2.0/24 去往子网 10.1.1.0/24 的数据流。
```
<RouterB> system-view
[RouterB] acl number 3101
[RouterB-acl-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0
0.0.0.255
[RouterB-acl-adv-3101] quit
```
配置到达 Host A 所在子网的静态路由。2.2.3.3 为本例中的直连下一跳地址，实际使用中请以具体组网情况为准。
```
[RouterB] ip route-static 10.1.1.0 255.255.255.0 gigabitethernet 2/1/2 2.2.3.3
```
创建 IPsec 安全提议 tran1。
```
[RouterB] ipsec transform-set tran1
```
配置安全协议对 IP 报文的封装形式为隧道模式。
```
[RouterB-ipsec-transform-set-tran1] encapsulation-mode tunnel
```
配置采用的安全协议为 ESP。
```
[RouterB-ipsec-transform-set-tran1] protocol esp
```
配置 ESP 协议采用的加密算法为 128 比特的 AES，认证算法为 HMAC-SHA1。
```
[RouterB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[RouterB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterB-ipsec-transform-set-tran1] quit
```
创建一条手工方式的 IPsec 安全策略，名称为 use1，序列号为 10。
```
[RouterB] ipsec policy use1 10 manual
```
指定引用 ACL 3101。
```
[RouterB-ipsec-policy-manual-use1-10] security acl 3101
```

指定引用的 IPsec 安全提议为 tran1。

```
[RouterB-ipsec-policy-manual-use1-10] transform-set tran1
```

指定 IPsec 隧道对端 IP 地址为 2.2.2.1。

```
[RouterB-ipsec-policy-manual-use1-10] remote-address 2.2.2.1
```

配置 ESP 协议的出方向 SPI 为 54321，入方向 SPI 为 12345。

```
[RouterB-ipsec-policy-manual-use1-10] sa spi outbound esp 54321
[RouterB-ipsec-policy-manual-use1-10] sa spi inbound esp 12345
```

配置 ESP 协议的出方向 SA 的密钥为明文字符串 gfedcba，入方向 SA 的密钥为明文字符串 abcdefg。

```
[RouterB-ipsec-policy-manual-use1-10] sa string-key outbound esp simple gfedcba
[RouterB-ipsec-policy-manual-use1-10] sa string-key inbound esp simple abcdefg
[RouterB-ipsec-policy-manual-use1-10] quit
```

在接口 GigabitEthernet2/1/2 上应用 IPsec 安全策略 use1。

```
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] ipsec apply policy use1
[RouterB-GigabitEthernet2/1/2] quit
```

4. 验证配置

以上配置完成后，Router A 和 Router B 之间的 IPsec 隧道就建立好了，子网 10.1.1.0/24 与子网 10.1.2.0/24 之间数据流的传输将受到生成的 IPsec SA 的保护。可通过以下显示查看 Router A 上手工创建的 IPsec SA。

```
[RouterA] display ipsec sa
-------------------------------
Interface: GigabitEthernet2/1/2
-------------------------------

  -----------------------------
  IPsec policy: map1
  Sequence number: 10
  Mode: manual
  -----------------------------
    Tunnel id: 549
    Encapsulation mode: tunnel
    Path MTU: 1443
    Tunnel:
        local  address: 2.2.2.1
        remote address: 2.2.3.1
    Flow:
        as defined in ACL 3101
    [Inbound ESP SA]
      SPI: 54321 (0x0000d431)
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      No duration limit for this SA
    [Outbound ESP SA]
      SPI: 12345 (0x00003039)
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      No duration limit for this SA
```

Router B 上也会产生相应的 IPsec SA 来保护 IPv4 报文，查看方式与 Router A 同，此处略。

1.7.2 采用IKE方式建立保护IPv4 报文的IPsec隧道

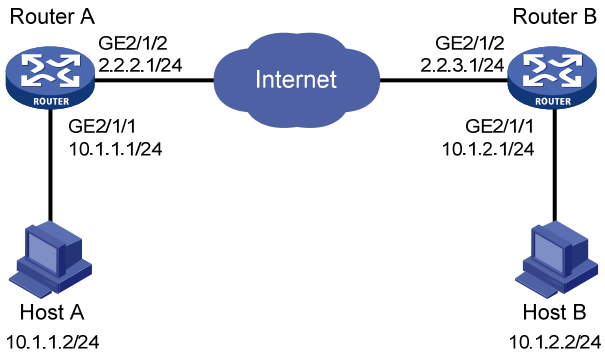
1. 组网需求

在 Router A 和 Router B 之间建立一条 IPsec 隧道，对 Host A 所在的子网（10.1.1.0/24）与 Host B 所在的子网（10.1.2.0/24）之间的数据流进行安全保护。具体要求如下：

- 封装形式为隧道模式。
- 安全协议采用 ESP 协议。
- 加密算法采用 128 比特的 AES，认证算法采用 HMAC-SHA1。
- IKE 协商方式建立 IPsec SA。

2. 组网图

图1-8 保护 IPv4 报文的 IPsec 配置组网图



3. 配置步骤

(1) 配置 Router A

配置各接口的 IP 地址，具体略。

配置一个 ACL，定义要保护由子网 10.1.1.0/24 去往子网 10.1.2.0/24 的数据流。

```
<RouterA> system-view
[RouterA] acl number 3101
[RouterA-acl-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0
0.0.0.255
[RouterA-acl-adv-3101] quit
```

配置到达 Host B 所在子网的静态路由。2.2.2.3 为本例中的直连下一跳地址，实际使用中请以具体组网情况为准。

```
[RouterA] ip route-static 10.1.2.0 255.255.255.0 gigabitethernet 2/1/2 2.2.2.3
```

创 IPsec 建安全提议 tran1。

```
[RouterA] ipsec transform-set tran1
```

配置安全协议对 IP 报文的封装形式为隧道模式。

```
[RouterA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

配置采用的安全协议为 ESP。

```
[RouterA-ipsec-transform-set-tran1] protocol esp
```

配置 ESP 协议采用的加密算法为 128 比特的 AES，认证算法为 HMAC-SHA1。

```
[RouterA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[RouterA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterA-ipsec-transform-set-tran1] quit
```

创建并配置 IKE keychain，名称为 keychain1。

```
[RouterA] ike keychain keychain1
```

配置与 IP 地址为 2.2.3.1 的对端使用的预共享密钥为明文 123456TESTplat&!。

```
[RouterA-ike-keychain-keychain1] pre-shared-key address 2.2.3.1 255.255.255.0 key simple
123456TESTplat&!
[RouterA-ike-keychain-keychain1] quit
```

创建并配置 IKE profile，名称为 profile1。

```
[RouterA] ike profile profile1
[RouterA-ike-profile-profile1] keychain keychain1
[RouterA-ike-profile-profile1] match remote identity address 2.2.3.1 255.255.255.0
[RouterA-ike-profile-profile1] quit
```

创建一条 IKE 协商方式的 IPsec 安全策略，名称为 map1，序列号为 10。

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

指定引用 ACL 3101。

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

指定引用的安全提议为 tran1。

```
[RouterA-ipsec-policy-isakmp-map1-10] transform-set tran1
```

指定 IPsec 隧道的本端 IP 地址为 2.2.2.1，对端 IP 地址为 2.2.3.1。

```
[RouterA-ipsec-policy-isakmp-map1-10] local-address 2.2.2.1
[RouterA-ipsec-policy-isakmp-map1-10] remote-address 2.2.3.1
```

指定引用的 IKE profile 为 profile1。

```
[RouterA-ipsec-policy-isakmp-map1-10] ike-profile profile1
[RouterA-ipsec-policy-isakmp-map1-10] quit
```

在接口 GigabitEthernet1/0/2 上应用安全策略 map1。

```
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ip address 2.2.2.1 255.255.255.0
[RouterA-GigabitEthernet2/1/2] ipsec apply policy map1
[RouterA-GigabitEthernet2/1/2] quit
```

(2) 配置 Router B

配置各接口的 IP 地址，具体略。

配置一个 ACL，定义要保护由子网 10.1.2.0/24 去往子网 10.1.1.0/24 的数据流。

```
<RouterB> system-view
[RouterB] acl number 3101
[RouterB-acl-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0
0.0.0.255
[RouterB-acl-adv-3101] quit
```

配置到达 Host A 所在子网的静态路由。2.2.3.3 为本例中的直连下一跳地址，实际使用中请以具体组网情况为准。

```
[RouterB] ip route-static 10.1.1.0 255.255.255.0 gigabitethernet 2/1/2 2.2.3.3
```

创建 IPsec 安全提议 tran1。

```
[RouterB] ipsec transform-set tran1
```
配置安全协议对 IP 报文的封装形式为隧道模式。
```
[RouterB-ipsec-transform-set-tran1] encapsulation-mode tunnel
```
配置采用的安全协议为 ESP。
```
[RouterB-ipsec-transform-set-tran1] protocol esp
```
配置 ESP 协议采用的加密算法为 128 比特的 AES，认证算法为 HMAC-SHA1。
```
[RouterB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[RouterB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterB-ipsec-transform-set-tran1] quit
```
创建并配置 IKE keychain，名称为 keychain1。
```
[RouterB] ike keychain keychain1
[RouterB-ike-keychain-keychain1] pre-shared-key address 2.2.2.1 255.255.255.0 key simple
123456TESTplat&!
[RouterB-ike-keychain-keychain1] quit
```
创建并配置 IKE profile， 名称为 profile1。
```
[RouterB] ike profile profile1
[RouterB-ike-profile-profile1] keychain keychain1
[RouterB-ike-profile-profile1] match remote identity address 2.2.2.1 255.255.255.0
[RouterB-ike-profile-profile1] quit
```
创建一条 IKE 协商方式的安全策略，名称为 use1，序列号为 10。
```
[RouterB] ipsec policy use1 10 isakmp
```
指定引用 ACL 3101。
```
[RouterB-ipsec-policy-isakmp-use1-10] security acl 3101
```
指定引用的 IPsec 安全提议为 tran1。
```
[RouterB-ipsec-policy-isakmp-use1-10] transform-set tran1
```
指定 IPsec 隧道的本端 IP 地址为 2.2.3.1，对端 IP 地址为 2.2.2.1。
```
[RouterB-ipsec-policy-manual-use1-10] local-address 2.2.3.1
[RouterB-ipsec-policy-manual-use1-10] remote-address 2.2.2.1
```
指定引用的 IKE 对等体为 profile1。
```
[RouterB-ipsec-policy-isakmp-use1-10] ike-profile profile1
[RouterB-ipsec-policy-isakmp-use1-10] quit
```
在接口 GigabitEthernet2/1/2 上应用 IPsec 安全策略 use1。
```
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] ip address 2.2.3.1 255.255.255.0
[RouterB-GigabitEthernet2/1/2] ipsec apply policy use1
[RouterB-GigabitEthernet2/1/2] quit
```
4. 验证配置

以上配置完成后，Router A 和 Router B 之间如果有子网 10.1.1.0/24 与子网 10.1.2.0/24 之间的报文通过，将触发 IKE 进行 IPsec SA 的协商。IKE 成功协商出 IPsec SA 后，子网 10.1.1.0/24 与子网 10.1.2.0/24 之间数据流的传输将受到 IPsec SA 的保护。可通过以下显示查看到协商生成的 IPsec SA。
```
[RouterA] display ipsec sa
-------------------------------
Interface: GigabitEthernet2/1/2
```

```
------------------------------

  ----------------------------
  IPsec policy: map1
  Sequence number: 10
  Mode: isakmp
  ----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Path MTU: 1443
    Tunnel:
        local  address: 2.2.3.1
        remote address: 2.2.2.1
    Flow:
    sour addr: 2.2.3.1/0.0.0.0  port: 0  protocol: IP
    dest addr: 2.2.2.1/0.0.0.0  port: 0  protocol: IP

    [Inbound ESP SAs]
      SPI: 3769702703 (0xe0b1192f)
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 3000/28800
      SA remaining duration (kilobytes/sec): 2300/797
      Max received sequence-number: 1
      Anti-replay check enable: N
      Anti-replay window size:
      UDP encapsulation used for NAT traversal: N
      Status: active

    [Outbound ESP SAs]
      SPI: 3840956402 (0xe4f057f2)
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 3000/28800
      SA remaining duration (kilobytes/sec): 2312/797
      Max sent sequence-number: 1
      UDP encapsulation used for NAT traversal: N
      Status: active
```

Router B 上也会产生相应的 IPsec SA 来保护 IPv4 报文，查看方式与 Router A 同，此处略。

1.7.3 采用IKE方式建立保护IPv6 报文的IPsec隧道

1. 组网需求

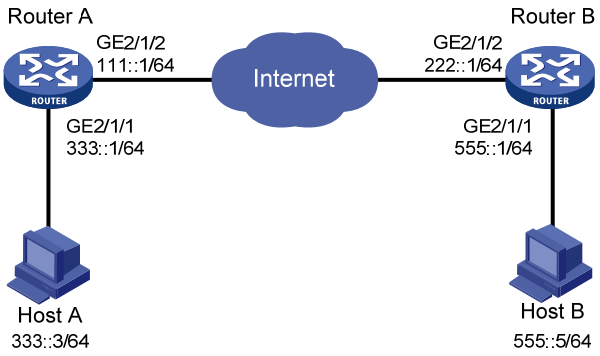
在 Router A 和 Router B 之间建立一条 IPsec 隧道，对 Host A 所在的子网（333::/64）与 Host B 所在的子网（555::/64）之间的数据流进行安全保护。具体要求如下：

- 封装形式为隧道模式。
- 安全协议采用 ESP 协议。
- 加密算法采用 128 比特的 AES，认证算法采用 HMAC-SHA1。

- IKE 协商方式建立 IPsec SA。

2. 组网图

图1-9 保护 IPv6 报文的 IPsec 配置组网图



3. 配置步骤

(1) 配置 Router A

配置各接口的 IPv6 地址，具体略。

配置一个 ACL，定义要保护由子网 333::/64 去往子网 555::/64 的数据流。

```
<RouterA> system-view
[RouterA] acl ipv6 number 3101
[RouterA-acl-adv-3101] rule permit ipv6 source 333::0 64 destination 555::0 64
[RouterA-acl-adv-3101] quit
```

配置到达 Host B 所在子网的静态路由。111::2 为本例中的直连下一跳地址，实际使用中请以具体组网情况为准。

```
[RouterA] ipv6 route-static 555::0 64 111::2
```

创建 IPsec 安全提议 tran1。

```
[RouterA] ipsec transform-set tran1
```

配置安全协议对 IP 报文的封装形式为隧道模式。

```
[RouterA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

配置采用的安全协议为 ESP。

```
[RouterA-ipsec-transform-set-tran1] protocol esp
```

配置 ESP 协议采用的加密算法为 128 比特的 AES，认证算法为 HMAC-SHA1。

```
[RouterA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[RouterA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterA-ipsec-transform-set-tran1] quit
```

创建并配置 IKE keychain，名称为 keychain1。

```
[RouterA] ike keychain keychain1
[RouterA-ike-keychain-keychain1] pre-shared-key address ipv6 222::1 64 key simple
123456TESTplat&!
[RouterA-ike-keychain-keychain1] quit
```

创建并配置 IKE profile，名称为 profile1。

```
[RouterA] ike profile profile1
[RouterA-ike-profile-profile1] keychain keychain1
```

```
[RouterA-ike-profile-profile1] match remote identity address ipv6 222::1 64
[RouterA-ike-profile-profile1] quit
```
创建一条 IKE 协商方式的 IPsec 安全策略，名称为 map1，序列号为 10。
```
[RouterA] ipsec ipv6-policy map1 10 isakmp
```
指定引用 IPv6 ACL 3101。
```
[RouterA-ipsec-ipv6-policy-isakmp-map1-10] security acl ipv6 3101
```
指定引用的 IPsec 安全提议为 tran1。
```
[RouterA-ipsec-ipv6-policy-isakmp-map1-10] transform-set tran1
```
指定 IPsec 隧道本端 IPv6 地址为 111::1，对端 IPv6 地址为 222::1。
```
[RouterA-ipsec-ipv6-policy-manual-map1-10] local-address ipv6 111::1
[RouterA-ipsec-ipv6-policy-manual-map1-10] remote-address ipv6 222::1
```
指定引用的 IKE 对等体为 profile1。
```
[RouterA-ipsec-ipv6-policy-isakmp-map1-10] ike-profile profile1
[RouterA-ipsec-ipv6-policy-isakmp-map1-10] quit
```
在接口 GigabitEthernet2/1/2 上应用 IPsec 安全策略 map1。
```
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] ipv6 address 111::1/64
[RouterA-GigabitEthernet2/1/2] ipsec apply ipv6-policy map1
[RouterA-GigabitEthernet2/1/2] quit
```
(2) 配置 Router B

配置各接口的 IPv6 地址，具体略。

配置一个 ACL，定义要保护由子网 555::/64 去往子网 333::/64 的数据流。
```
<RouterB> system-view
[RouterB] acl ipv6 number 3101
[RouterB-acl-adv-3101] rule permit ipv6 source 555::/64 destination 333::/64
[RouterB-acl-adv-3101] quit
```
配置到达 Host A 所在子网的静态路由。222::2 为本例中的直连下一跳地址，实际使用中请以具体组网情况为准。
```
[RouterB] ipv6 route-static 333::0 64 222::2
```
创建 IPsec 安全提议 tran1。
```
[RouterB] ipsec transform-set tran1
```
配置安全协议对 IP 报文的封装形式为隧道模式。
```
[RouterB-ipsec-transform-set-tran1] encapsulation-mode tunnel
```
配置采用的安全协议为 ESP。
```
[RouterB-ipsec-transform-set-tran1] protocol esp
```
配置 ESP 协议采用的加密算法为 128 比特的 AES，认证算法为 HMAC-SHA1。
```
[RouterB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[RouterB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterB-ipsec-transform-set-tran1] quit
```
创建并配置 IKE keychain，名称为 keychain1。
```
[RouterB] ike keychain keychain1
[RouterB-ike-keychain-keychain1] pre-shared-key address ipv6 111::1 64 key simple
123456TESTplat&!
[RouterB-ike-keychain-keychain1] quit
```

创建并配置 IKE profile，名称为 profile1。

```
[RouterB] ike profile profile1
[RouterB-ike-profile-profile1] keychain keychain1
[RouterB-ike-profile-profile1] match remote identity address ipv6 111::1 64
[RouterB-ike-profile-profile1] quit
```

创建一条 IKE 协商方式的 IPsec 安全策略，名称为 use1，序列号为 10。

```
[RouterB] ipsec ipv6-policy use1 10 isakmp
```

指定引用 ACL 3101。

```
[RouterB-ipsec-ipv6-policy-isakmp-use1-10] security acl 3101
```

指定引用的安全提议为 tran1。

```
[RouterB-ipsec-ipv6-policy-isakmp-use1-10] transform-set tran1
```

指定 IPsec 隧道本端 IPv6 地址为 222::1，对端 IPv6 地址为 111::1。

```
[RouterB-ipsec-ipv6-policy-manual-map1-10] local-address ipv6 222::1
[RouterB-ipsec-ipv6-policy-manual-use1-10] remote-address ipv6 111::1
```

指定引用的 IKE 对等体为 profile1。

```
[RouterB-ipsec-ipv6-policy-isakmp-use1-10] ike-profile profile1
[RouterB-ipsec-ipv6-policy-isakmp-use1-10] quit
```

在接口 GigabitEthernet2/1/2 上应用 IPsec 安全策略 use1。

```
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] ipv6 address 222::1/64
[RouterB-GigabitEthernet2/1/2] ipsec apply ipv6-policy use1
[RouterB-GigabitEthernet2/1/2] quit
```

4. 验证配置

以上配置完成后，当 Router A 和 Router B 之间有子网 333::/64 与子网 555::/64 之间的报文通过时，将触发 IKE 进行 IPsec SA 的协商。IKE 成功协商出 IPsec SA 后，子网 333::/64 与子网 555::/64 之间数据流的传输将受到 IPsec SA 的保护。可通过以下显示查看到协商生成的 IPsec SA。

```
[RouterA] display ipsec sa
-------------------------------
Interface: GigabitEthernet2/1/2
-------------------------------

  -----------------------------
  IPsec policy: map1
  Sequence number: 10
  Mode: isakmp
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Path MTU: 1423
    Tunnel:
        local  address: 111::1
        remote address: 222::1
    Flow:
    sour addr: 111::1/0      port: 0  protocol: IPv6
```

```
dest addr: 222::1/0      port: 0  protocol: IPv6

[Inbound ESP SAs]
  SPI: 3769702703 (0xe0b1192f)
  Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
  SA duration (kilobytes/sec): 3000/28800
  SA remaining duration (kilobytes/sec): 2300/797
  Max received sequence-number: 1
  Anti-replay check enable: N
  Anti-replay window size:
  UDP encapsulation used for NAT traversal: N
  Status: active

[Outbound ESP SAs]
  SPI: 3840956402 (0xe4f057f2)
  Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
  SA duration (kilobytes/sec): 3000/28800
  SA remaining duration (kilobytes/sec): 2312/797
  Max sent sequence-number: 1
  UDP encapsulation used for NAT traversal: N
  Status: active
```

Router B 上也会产生相应的 IPsec SA 来保护 IPv6 报文，查看方式与 Router A 同，此处略。

1.7.4 配置IPsec保护RIPng报文

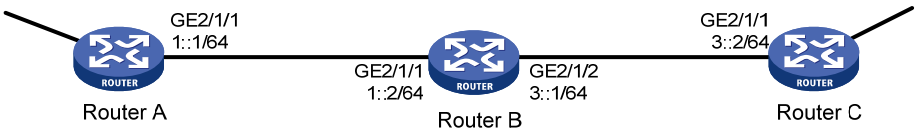
1. 组网需求

如 图 1-10 所示，Router A、Router B和Router C相连，并通过RIPng来学习网络中的IPv6 路由信息。在各设备之间建立IPsec隧道，对它们收发的RIPng报文进行安全保护。具体要求如下：

- 安全协议采用 ESP 协议；
- 加密算法采用 128 比特的 AES；
- 认证算法采用 HMAC-SHA1。

2. 组网图

图1-10 配置 IPsec 保护 RIPng 报文组网图



3. 配置思路

(1) 配置 RIPng 的基本功能

RIPng 配置的详细介绍请参考“三层技术-IP 路由配置指导”中的“RIPng”。

(2) 配置 IPsec 安全框架

需要注意的是：

- 各设备上本端出方向 SA 的 SPI 及密钥必须和本端入方向 SA 的 SPI 及密钥保持一致。
- Router A、Router B 和 Router C 上的安全策略所引用的安全提议采用的安全协议、认证/加密算法和报文封装模式要相同，而且所有设备上的 SA 的 SPI 及密钥均要保持一致。

(3) 在 RIPng 进程下或接口上应用 IPsec 安全框架

4. 配置步骤

(1) 配置 Router A

- 配置各接口的 IPv6 地址（略）
- 配置 RIPng 的基本功能

```
<RouterA> system-view
[RouterA] ripng 1
[RouterA-ripng-1] quit
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ripng 1 enable
[RouterA-GigabitEthernet2/1/1] quit
```

- 配置 IPsec 安全框架

创建并配置名为 tran1 的 IPsec 安全提议（报文封装模式采用传输模式，安全协议采用 ESP 协议，加密算法采用 128 比特的 AES，认证算法采用 HMAC-SHA1）。

```
[RouterA] ipsec transform-set tran1
[RouterA-ipsec-transform-set-tran1] encapsulation-mode transport
[RouterA-ipsec-transform-set-tran1] protocol esp
[RouterA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[RouterA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterA-ipsec-transform-set-tran1] quit
```

创建并配置名为 profile001 的 IPsec 安全框架（协商方式为手工方式，出入方向 SA 的 SPI 均为 123456，出入方向 SA 的密钥均为明文 abcdefg）。

```
[RouterA] ipsec profile profile001 manual
[RouterA-ipsec-profile-profile001] transform-set tran1
[RouterA-ipsec-profile-profile001] sa spi outbound esp 123456
[RouterA-ipsec-profile-profile001] sa spi inbound esp 123456
[RouterA-ipsec-profile-profile001] sa string-key outbound esp simple abcdefg
[RouterA-ipsec-profile-profile001] sa string-key inbound esp simple abcdefg
[RouterA-ipsec-profile-profile001] quit
```

- 在 RIPng 进程上应用 IPsec 安全框架

```
[RouterA] ripng 1
[RouterA-ripng-1] enable ipsec-profile profile001
[RouterA-ripng-1] quit
```

(2) 配置 Router B

- 配置各接口的 IPv6 地址（略）
- 配置 RIPng 的基本功能

```
<RouterB> system-view
[RouterB] ripng 1
[RouterB-ripng-1] quit
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ripng 1 enable
```

```
[RouterB-GigabitEthernet2/1/1] quit
[RouterB] interface gigabitethernet 2/1/2
[RouterB-GigabitEthernet2/1/2] ripng 1 enable
[RouterB-GigabitEthernet2/1/2] quit
```

- 配置 IPsec 安全框架

创建并配置名为 tran1 的 IPsec 安全提议（报文封装模式采用传输模式，安全协议采用 ESP 协议，加密算法采用 128 比特的 AES，认证算法采用 HMAC-SHA1）。

```
[RouterB] ipsec transform-set tran1
[RouterB-ipsec-transform-set-tran1] encapsulation-mode transport
[RouterB-ipsec-transform-set-tran1] protocol esp
[RouterB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[RouterB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterB-ipsec-transform-set-tran1] quit
```

创建并配置名为 profile001 的 IPsec 安全框架（协商方式为手工方式，出入方向 SA 的 SPI 均为 123456，出入方向 SA 的密钥均为明文 abcdefg）。

```
[RouterB] ipsec profile profile001 manual
[RouterB-ipsec-profile-profile001] transform-set tran1
[RouterB-ipsec-profile-profile001] sa spi outbound esp 123456
[RouterB-ipsec-profile-profile001] sa spi inbound esp 123456
[RouterB-ipsec-profile-profile001] sa string-key outbound esp simple abcdefg
[RouterB-ipsec-profile-profile001] sa string-key inbound esp simple abcdefg
[RouterB-ipsec-profile-profile001] quit
```

- 在 RIPng 进程上应用 IPsec 安全框架

```
[RouterB] ripng 1
[RouterB-ripng-1] enable ipsec-profile profile001
[RouterB-ripng-1] quit
```

(3) 配置 Router C

- 配置各接口的 IPv6 地址（略）
- 配置 RIPng 的基本功能

```
<RouterC> system-view
[RouterC] ripng 1
[RouterC-ripng-1] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] ripng 1 enable
[RouterC-GigabitEthernet2/1/1] quit
```

- 配置 IPsec 安全框架

创建并配置名为 tran1 的 IPsec 安全提议（报文封装模式采用传输模式，安全协议采用 ESP 协议，加密算法采用 128 比特的 AES，认证算法采用 HMAC-SHA1）。

```
[RouterC] ipsec transform-set tran1
[RouterC-ipsec-transform-set-tran1] encapsulation-mode transport
[RouterC-ipsec-transform-set-tran1] protocol esp
[RouterC-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[RouterC-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterC-ipsec-transform-set-tran1] quit
```

创建并配置名为 profile001 的 IPsec 安全框架（协商方式为手工方式，出入方向 SA 的 SPI 均为 123456，出入方向 SA 的密钥均为明文 abcdefg）。

```
[RouterC] ipsec profile profile001 manual
[RouterC-ipsec-profile-profile001] transform-set tran1
[RouterC-ipsec-profile-profile001] sa spi outbound esp 123456
[RouterC-ipsec-profile-profile001] sa spi inbound esp 123456
[RouterC-ipsec-profile-profile001] sa string-key outbound esp simple abcdefg
[RouterC-ipsec-profile-profile001] sa string-key inbound esp simple abcdefg
[RouterC-ipsec-profile-profile001] quit
```

- 在 RIPng 进程上应用 IPsec 安全框架

```
[RouterC] ripng 1
[RouterC-ripng-1] enable ipsec-policy profile001
[RouterC-ripng-1] quit
```

5. 验证配置

以上配置完成后，Router A、Router B 和 Router C 将通过 RIPng 协议学习到网络中的 IPv6 路由信息，且分别产生用于保护 RIPng 报文的 IPsec SA。

可以通过如下 **display** 命令查看 Router A 上 RIPng 的配置信息。如下显示信息表示 RIPng 进程 1 上已成功应用了 IPsec 安全框架。

```
[RouterA] display ripng 1
    RIPng process : 1
       Preference : 100
       Checkzero : Enabled
       Default Cost : 0
       Maximum number of balanced paths : 8
       Update time   :   30 sec(s)  Timeout time         :  180 sec(s)
       Suppress time :  120 sec(s)  Garbage-Collect time :  120 sec(s)
       Number of periodic updates sent : 186
       Number of trigger updates sent : 1
       IPsec profile name: profile001
```

可以通过如下命令查看 Router A 上生成的 IPsec SA。

```
[RouterA] display ipsec sa
-------------------------------
Global IPsec SA
-------------------------------

  -----------------------------
  IPsec profile: profile001
  Mode: manual
  -----------------------------
    Encapsulation mode: transport
    [Inbound ESP SA]
      SPI: 123456 (0x3039)
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      No duration limit for this SA
    [Outbound ESP SA]
```

```
SPI: 123456 (0x3039)
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
No duration limit for this SA
```

Router B 和 Router C 上也会生成相应的 IPsec SA 来保护 RIPng 报文，查看方式与 Router A 同，此处略。

1.7.5 配置IPsec反向路由注入

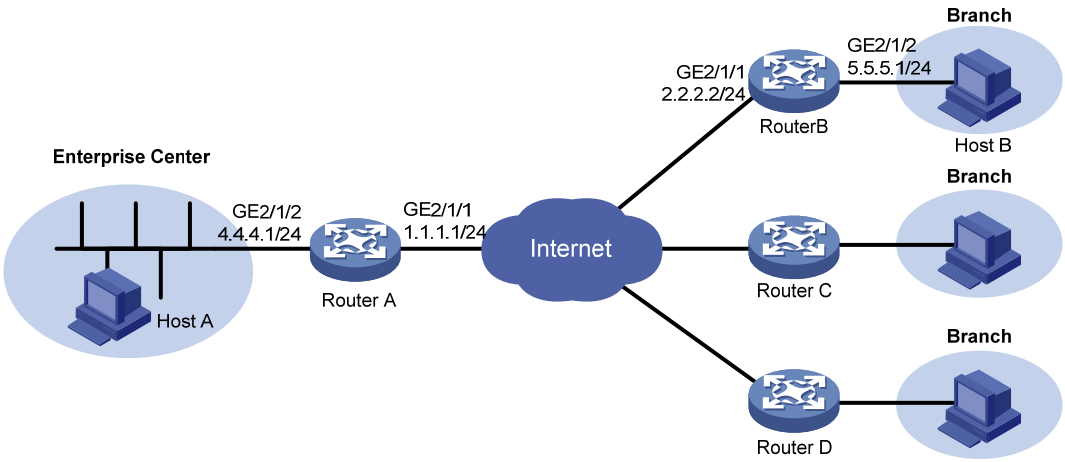
1. 组网需求

企业分支通过 IPsec VPN 接入企业总部，有如下具体需求：

- 总部网关 Router A 和各分支网关 Router B、RouterC、Router D 之间建立 IPsec 隧道，对总部网络 4.4.4.0/24 与分支网络 5.5.5.0/24 之间的数据进行安全保护。
- 使用 IKE 协商方式建立 IPsec SA，采用 ESP 安全协议，DES 加密算法，HMAC-SHA-1-96 认证算法。
- IKE 协商采用预共享密钥认证方式、3DES 加密算法、HMAC-SHA1 认证算法。
- 在 Router A 上开启 IPsec 反向路由注入功能，实现总部到分支的静态路由随 IPsec SA 的建立而动态生成。

2. 组网图

图1-11 配置 IPsec 反向路由注入功能组网图



3. 配置步骤

(1) 配置 RouterA

- 配置各接口的 IPv4 地址（略）
- 配置 IPsec 安全提议

创建并配置名为 tran1 的安全提议，采用使用 ESP 安全协议，DES 加密算法，HMAC-SHA-1-96 认证算法。

```
<RouterA> system-view
[RouterA] ipsec transform-set tran1
[RouterA-ipsec-transform-set-tran1] encapsulation-mode tunnel
[RouterA-ipsec-transform-set-tran1] protocol esp
[RouterA-ipsec-transform-set-tran1] esp encryption-algorithm des
```

```
[RouterA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterA-ipsec-transform-set-tran1] quit
```

- 配置 IPsec 安全策略模板

创建并配置名为 temp1 的 IPsec 安全策略模板，引用安全提议 tran1

```
[RouterA] ipsec policy-template temp1 1
[RouterA-ipsec-policy-template-temp1-1] transform-set tran1
```

- 配置 RRI 功能

开启 RRI 功能，指定生成的静态路由的优先级为 100、Tag 值为 1000。

```
[RouterA-ipsec-policy-template-temp1-1] reverse-route dynamic
[RouterA-ipsec-policy-template-temp1-1] reverse-route preference 100
[RouterA-ipsec-policy-template-temp1-1] reverse-route tag 1000
[RouterA-ipsec-policy-template-temp1-1] quit
```

- 配置 IKE 协商方式的 IPsec 安全策略

创建并配置名为 map1 的 IPsec 安全策略，基于安全策略模板 temp1 创建

```
[RouterA] ipsec  policy map1 10 isakmp template temp1
```

- 配置 IKE 提议

创建并配置 IKE 提议 1，指定使用预共享密钥认证方式、3DES 加密算法、HMAC-SHA1 认证算法。

```
[RouterA] ike proposal 1
[RouterA-ike-proposal-1] encryption-algorithm 3des-cbc
[RouterA-ike-proposal-1] authentication-algorithm sha
[RouterA-ike-proposal-1] authentication-method pre-share
[RouterA-ike-proposal-1] quit
```

- 配置 IKE keychain

创建并配置名为 key1 的 IKE keychain，指定与地址为 2.2.2.2 的对端使用的预共享密钥为明文 123。

```
[RouterA] ike keychain key1
[RouterA-ike-keychain-key1] pre-shared-key address 2.2.2.2 key simple 123
[RouterA-ike-keychain-key1] quit
```

- 在接口下引用 IPsec 安全策略

在接口 GigabitEthernet2/1/1 上应用 IPsec 安全策略 map1。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ipsec apply policy map1
[RouterA-GigabitEthernet2/1/1] quit
```

(2) 配置 Router B

- 配置各接口的 IPv4 地址（略）
- 配置 IPsec 安全提议

创建并配置名为 tran1 的安全提议

```
[RouterB] ipsec transform-set tran1
[RouterB-ipsec-transform-set-tran1] encapsulation-mode tunnel
[RouterB-ipsec-transform-set-tran1] protocol esp
[RouterB-ipsec-transform-set-tran1] esp encryption-algorithm des
[RouterB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterB-ipsec-transform-set-tran1] quit
```

- 配置 ACL

配置 ACL 3000，定义要保护由子网 5.5.5.0/24 去往子网 4.4.4.0/24 的数据流。

```
[RouterB] acl number 3000
[RouterB-acl-adv-3000] rule permit ip source 5.5.5.0 0.0.0.255 destination 4.4.4.0 0.0.0.255
[RouterB-acl-adv-3000] quit
```

- 配置 ISAKMP 方式的安全策略

创建并配置名为 map1 的 IPsec 安全策略，引用安全提议 tran1，引用 ACL 3000，并指定 IPsec 隧道的对端地址为 1.1.1.1。

```
[RouterB] ipsec policy map1 10 isakmp
[RouterB-ipsec-policy-isakmp-map1-10] transform-set tran1
[RouterB-ipsec-policy-isakmp-map1-10] security acl 3000
[RouterB-ipsec-policy-isakmp-map1-10] remote-address 1.1.1.1
[RouterB-ipsec-policy-isakmp-map1-10] quit
```

- 配置 IKE 提议

创建并配置 IKE 提议 1，指定预共享密钥认证方式、3DES 加密算法、HMAC-SHA1 认证算法。

```
[RouterB] ike proposal 1
[RouterB-ike-proposal-1] encryption-algorithm 3des-cbc
[RouterB-ike-proposal-1] authentication-algorithm sha
[RouterB-ike-proposal-1] authentication-method pre-share
[RouterB-ike-proposal-1] quit
```

- 配置 IKE keychain

创建并配置名为 key1 的 IKE keychain，指定与地址为 1.1.1.1 的对端使用的预共享密钥为明文 123。

```
[RouterB] ike keychain key1
[RouterB-ike-keychain-key1] pre-shared-key address 1.1.1.1 key simple 123
[RouterB-ike-keychain-key1] quit
```

- 在接口上应用 IPsec 安全策略

在接口 GigabitEthernet2/1/1 上应用 IPsec 安全策略 map1。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ipsec apply policy map1
[RouterB-GigabitEthernet2/1/1] quit
```

保证 RouterB 上存在到达对端私网网段的路由，出接口为 GigabitEthernet2/1/1。

(3) 配置 Router C、Router D

配置步骤与 Router B 类似，请参考 Router B 的配置。

4. 验证配置结果

以上配置完成后，当分支子网 5.5.5.0/24 向总部网络 4.4.4.0/24 发起数据连接时，将触发 Rouer B 和 Router A 之间进行 IKE 协商。IKE 成功协商出 IPsec SA 后，企业总部与分支子网之间的数据流传输将受到 IPsec SA 的保护。在 Router A 上可通过以下显示查看到协商生成的 IPsec SA。

```
[RouterA] display ipsec sa
------------------------------
Interface: GigabitEthernet2/1/1
------------------------------

  ----------------------------
  IPsec policy: map1
  Sequence number: 10
```

```
Mode: template
-----------------------------
  Tunnel id: 0
  Encapsulation mode: tunnel
  Perfect forward secrecy:
  Path MTU: 1463
  Tunnel:
      local  address: 1.1.1.1
      remote address: 2.2.2.2
  Flow:
  sour addr: 4.4.4.0/255.255.255.0  port: 0  protocol: ip
  dest addr: 5.5.5.0/255.255.255.0  port: 0  protocol: ip

  [Inbound ESP SAs]
    SPI: 1014286405 (0x3c74c845)
    Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3590
    Max received sequence-number: 4
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for nat traversal: N
    Status: active

  [Outbound ESP SAs]
    SPI: 4011716027 (0xef1dedbb)
    Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3590
    Max sent sequence-number: 4
    UDP encapsulation used for nat traversal: N
    Status: active
```

IPsec SA 成功建立后，在 Router A 上可以通过 **display ip routing-table verbose** 命令查看到 IPsec 反向路由注入生成的静态路由，目的地址为分支子网地址 5.5.5.0/24，下一跳为 IPsec 隧道对端地址 2.2.2.2，优先级为 100，Tag 值为 1000。Router A 和 Router C、Router D 之间的 IPsec 隧道建立成功后，Router A 上也会产生到达各分支子网的相应静态路由，此处显示略。

2 IKE

说明

若无特殊说明，本文中的 IKE 均指第 1 版本的 IKE 协议。

说明

- 设备运行于 FIPS 模式时，本特性部分配置相对于非 FIPS 模式有所变化，具体差异请见本文相关描述。有关 FIPS 模式的详细介绍请参见“安全配置指导“中的“FIPS”。

2.1 IKE简介

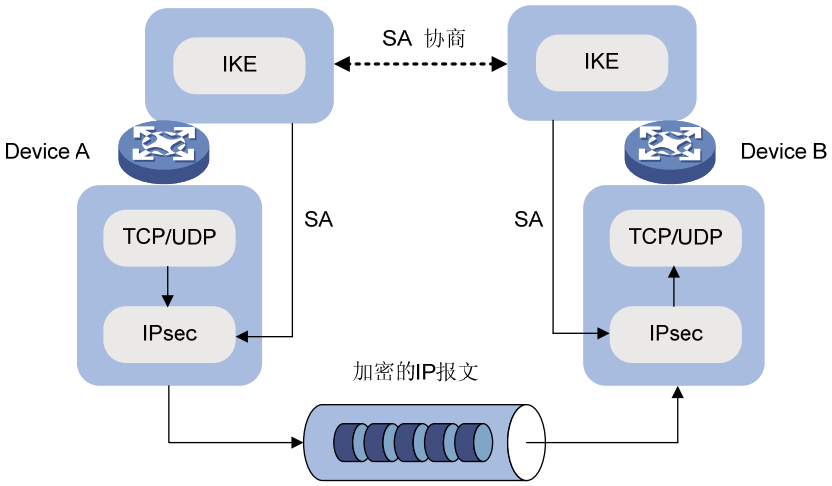
IKE（Internet Key Exchange，互联网密钥交换）协议利用 ISAKMP（Internet Security Association and Key Management Protocol，互联网安全联盟和密钥管理协议）语言定义密钥交换的过程，是一种对安全服务进行协商的手段。

用 IPsec 保护一个 IP 数据包之前，必选先建立一个安全联盟（IPsec SA），IPsec SA 可以手工创建或动态建立。IKE 为 IPsec 提供了自动建立 IPsec SA 的服务，具体有以下优点。

- IKE 首先会在通信双方之间协商建立一个安全通道（IKE SA），并在此安全通道的保护下协商建立 IPsec SA，这降低了手工配置的复杂度，简化 IPsec 的配置和维护工作。
- IKE 的精髓在于 DH（Diffie-Hellman）交换技术，它通过一系列的交换，使得通信双方最终计算出共享密钥。在 IKE 的 DH 交换过程中，每次计算和产生的结果都是不相关的。由于每次 IKE SA 的建立都运行了 DH 交换过程，因此就保证了每个通过 IKE 协商建立的 IPsec SA 所使用的密钥互不相关。
- IPsec 使用 AH 或 ESP 报文头中的顺序号实现防重放。此顺序号是一个 32 比特的值，此数溢出之前，为实现防重放，IPsec SA 需要重新建立，IKE 可以自动重协商 IPsec SA。

如 图 2-1 所示，IKE为IPsec协商建立SA，并把建立的参数交给IPsec，IPsec使用IKE建立的SA对IP报文加密或认证处理。

图2-1 IPsec 与 IKE 的关系图



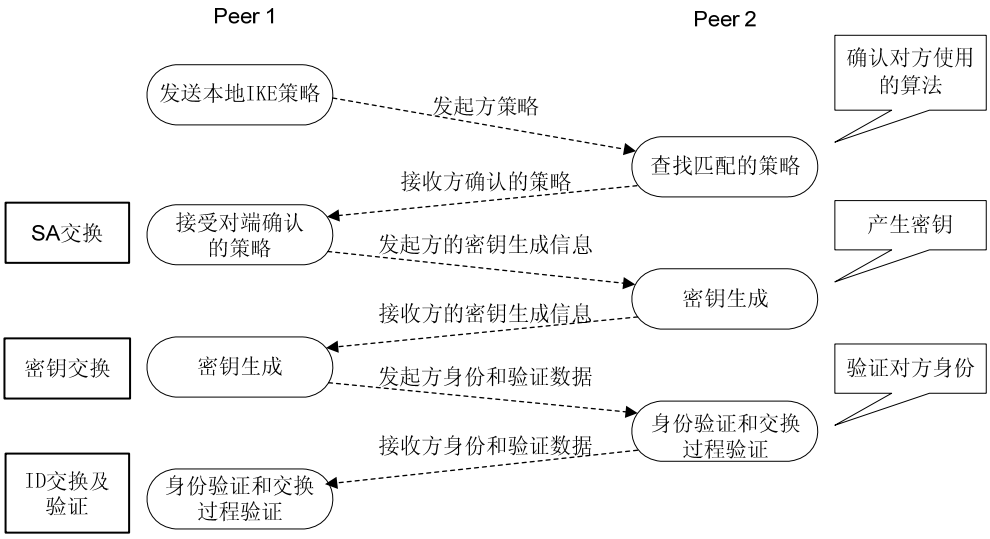
2.1.1 IKE的协商过程

IKE 使用了两个阶段为 IPsec 进行密钥协商以及建立 SA：

(1) 第一阶段，通信双方彼此间建立了一个已通过双方身份认证和对通信数据安全保护的通道，即建立一个 IKE SA（本文中提到的 IKE SA 都是指第一阶段 SA）。第一阶段有主模式（Main Mode）和野蛮模式（Aggressive Mode）两种 IKE 协商模式。

(2) 第二阶段，用在第一阶段建立的 IKE SA 为 IPsec 协商安全服务，即为 IPsec 协商 IPsec SA，建立用于最终的 IP 数据安全传输的 IPsec SA。

图2-2 主模式交换过程



如 图 2-2 所示，第一阶段主模式的IKE协商过程中包含三对消息，具体内容如下：

- 第一对消息完成了 SA 交换，它是一个协商确认双方 IKE 安全策略的过程；

- 第二对消息完成了密钥交换，通过交换 Diffie-Hellman 公共值和辅助数据（如：随机数），最终双方计算生成一系列共享密钥（例如，认证密钥、加密密钥以及用于生成 IPsec 密钥参数的密钥材料），并使其中的加密密钥和认证密钥对后续的 IKE 消息提供安全保障；
- 第三对消息完成了 ID 信息和验证数据的交换，并进行双方身份的认证。

野蛮模式交换与主模式交换的主要差别在于，野蛮模式不提供身份保护，只交换 3 条消息。在对身份保护要求不高的场合，使用交换报文较少的野蛮模式可以提高协商的速度；在对身份保护要求较高的场合，则应该使用主模式。

2.1.2 IKE的安全机制

IKE 可以在不安全的网络上安全地认证通信双方的身份、分发密钥以及建立 IPsec SA，具有以下几种安全机制。

1. 身份认证

IKE 的身份认证机制用于确认通信双方的身份。设备支持三种认证方法：预共享密钥认证、RSA 数字签名认证和 DSA 数字签名认证。

- 预共享密钥认证：通信双方通过共享的密钥认证对端身份。
- 数字签名认证：通信双方使用由 CA 颁发的数字证书向对端证明自己的身份。

2. DH算法

DH 算法是一种公共密钥算法，它允许通信双方在不传输密钥的情况下通过交换一些数据，计算出共享的密钥。即使第三方（如黑客）截获了双方用于计算密钥的所有交换数据，由于其复杂度很高，也不足以计算出双方的密钥。

3. PFS特性

PFS（Perfect Forward Secrecy，完善的前向安全性）是一种安全特性，它解决了密钥之间相互无关性的需求。由于 IKE 第二阶段协商需要从第一阶段协商出的密钥材料中衍生出用于 IPsec SA 的密钥，若攻击者能够破解 IKE SA 的一个密钥，则会非常容易得掌握其衍生出的任何 IPsec SA 的密钥。使用 PFS 特性后，IKE 第二阶段协商过程中会增加一次 DH 交换，使得 IKE SA 的密钥和 IPsec SA 的密钥之间没有派生关系，即使 IKE SA 的其中一个密钥被破解，也不会影响它协商出的其它密钥的安全性。

2.1.3 协议规范

与 IKE 相关的协议规范有：

- RFC2408：Internet Security Association and Key Management Protocol (ISAKMP)
- RFC2409：The Internet Key Exchange (IKE)
- RFC2412：The OAKLEY Key Determination Protocol

2.2 IKE配置任务简介

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。

(1) 确定 IKE 交换过程中安全保护的强度，包括认证方法、加密算法、认证算法、DH group。

- 认证方法分为预共享密钥认证和数字签名认证。预共享密钥认证机制简单、不需要证书，常在小型组网环境中使用；数字签名认证安全性更高，常在“中心—分支”模式的组网环境中使用。例如，在“中心—分支”组网中使用预共享密钥认证进行 IKE 协商时，中心侧可能需要为每个分支配置一个预共享密钥，当分支很多时，配置会很复杂，而使用数字签名认证时只需配置一个 PKI 域。
- 不同认证/加密算法的强度不同，算法强度越高，受保护数据越难被破解，但消耗的计算资源越多。
- DH group 位数越大安全性越高，但是处理速度会相应减慢。应该根据实际组网环境中对安全性和性能的要求选择合适的 DH group。

(2) 确定通信双方预先约定的预共享密钥或所属的 PKI 域。关于 PKI 的配置，请参见“安全配置指导”中的“PKI”。

(3) 确定通信双方都采用 IKE 协商模式的 IPsec 安全策略。IPsec 安全策略中若不引用 IKE profile，则使用系统视图下配置的 IKE profile 进行协商，若系统视图下没有任何 IKE profile，则使用全局的 IKE 参数进行协商。关于 IPsec 安全策略的配置，请参见“安全配置指导”中的“IPsec”。

表2-1 IKE 配置任务简介

配置任务	说明	详细配置
配置IKE profile	可选	2.3
配置IKE提议	可选 若IKE profile中需要指定IKE提议，则必配	2.4
配置IKE keychain	可选 若IKE第一阶段协商为预共享密钥认证方式，则必配	2.5
配置本端身份信息	可选	2.6
配置IKE Keepalive功能	可选	2.7
配置IKE NAT Keepalive功能	可选	2.8
配置IKE DPD探测功能	可选	2.9
配置针对无效IPsec SPI的IKE SA恢复功能	可选	2.10
配置对IKE SA数目的限制	可选	2.11
配置IKE告警功能	可选	2.12

2.3 配置IKE profile

IKE profile 中包括以下配置：

(1) 匹配对端身份的规则。响应方首先需要根据发起方的身份信息查找一个本端的 IKE profile，然后使用此 IKE profile 中的信息验证对端身份，发起方同样需要根据响应方的身份信息查找到一个 IKE profile 用于验证对端身份。对端身份信息若能满足本地某个 IKE profile 中指定的匹配规则，则该 IKE profile 为查找的结果。

(2) 根据 IKE 提议中配置的认证方法，配置 IKE keychain 或 PKI 域。

- 如果认证方法为数字签名（**dsa-signature** 或者 **rsa-signature**），则需要配置 PKI 域。
- 如果指定的认证方式为预共享密钥（**pre-share**），则需要配置 IKE keychain。

(3) 本端作为发起方时所使用的协商模式（主模式、野蛮模式）。本端作为响应方时，将自动适配发起方的协商模式。

(4) 本端作为发起方时可以使用的 IKE 提议（可指定多个），先指定的优先级高。响应方会将发起方的 IKE 提议与本端所有的 IKE 提议进行匹配，如果找到匹配项则直接使用，否则继续查找。若未查找到匹配的 IKE 提议，则协商失败。

(5) 本端身份信息。

- 如果本端的认证方式为数字签名，则可以配置任何类型的身份信息。若配置的本端身份为 IP 地址，但这个 IP 地址与本地证书中的 IP 地址不同时，设备将使用 FQDN（Fully Qualified Domain Name，完全合格域名）类型的本端身份，该身份的内容为设备的名称（可通过 **sysname** 命令配置）。
- 如果本端的认证方式为预共享密钥，则只能配置除 DN 之外的其它类型的身份信息。

(6) IKE DPD（Dead Peer Detection，对等体存活检测）功能，IKE DPD 功能用于检测协商对端是否存活。如果 IKE profile 视图下和系统视图下都配置了 DPD 功能，则 IKE profile 视图下的 DPD 配置生效，如果 IKE profile 视图下没有配置 DPD 功能，则采用系统视图下的 DPD 配置。

(7) IKE profile 的使用范围。限制 IKE profile 只能在指定的地址或指定接口的地址下使用（这里的地址指的是 IPsec 策略下配置的本端地址，若本端地址没有配置，则为引用 IPsec 策略的接口 IP 地址）。配置了 **match local address** 的 IKE profile 的优先级高于所有未配置 **match local address** 的 IKE profile。

(8) 内部 MPLS L3VPN 实例。当 IPsec 解封装后得到的报文需要继续转发到不同的 VPN 中去时，设备需要知道在哪个 VPN 实例中查找相应的路由。缺省情况下，设备在与外网相同的 VPN 中查找路由，如果不希望在与外网相同的 VPN 中查找路由去转发报文，则可以指定一个内部 VPN 实例，通过查找该内部 VPN 实例中的路由来转发报文。

(9) IKE profile 的优先级。IKE profile 的匹配优先级首先取决于其中是否配置了 **match local address**，其次决定于配置的优先级值，最后决定于配置 IKE profile 的先后顺序。

表2-2 配置 IKE profile

操作	命令	说明
进入系统视图	**system-view**	-
创建一个IKE profile，并进入IKE Profile视图	**ike profile** *profile-name*	缺省情况下，不存在IKE profile
配置匹配对端身份的规则	**match remote** { **certificate** *policy-name* | **identity** { **address** { { *ipv4-address* [*mask* | *mask-length*] | **range** *low-ipv4-address high-ipv4-address* } | **ipv6** { *ipv6-address* [*prefix-length*] | **range** *low-ipv6-address high-ipv6-address* } } [**vpn-instance** *vpn-name*] | **fqdn** *fqdn-name* | **user-fqdn** *user-fqdn-name* } }	协商双方都必须配置至少一个**match remote**规则，当对端的身份与IKE profile中配置的**match remote**规则匹配时，则使用此IKE profile中的信息与对端完成认证

操作	命令	说明
配置采用预共享密钥认证时，所使用的keychain	**keychain** *keychain-name*	二者至少选其一 缺省情况下，未指定keychain和PKI域
配置采用数字签名认证时，证书所属的PKI域	**certificate domain** *domain-name*	
配置IKE第一阶段的协商模式	非FIPS模式下： **exchange-mode** { **aggressive** | **main** } FIPS模式下： **exchange-mode main**	缺省情况下，IKE第一阶段发起方的协商模式使用主模式
配置IKE profile引用的IKE提议	**proposal** *proposal-number&<1-6>*	缺省情况下，IKE profile未引用任何IKE提议，使用系统视图下已配置的IKE提议进行IKE协商
配置本端身份信息	**local-identity** { **address** { *ipv4-address* | **ipv6** *ipv6-address* } | **dn** | **fqdn** [*fqdn-name*] | **user-fqdn** [*user-fqdn-name*] }	缺省情况下，未配置本端身份信息。此时使用系统视图下通过**ike identity**命令配置的身份信息作为本端身份信息。若两者都没有配置，则使用IP地址标识本端的身份，该IP地址为IPsec安全策略或IPsec安全策略模板应用的接口的IP地址
（可选）配置IKE DPD功能	**dpd interval** *interval-seconds* [**retry** *seconds*] { **on-demand** | **periodic** }	缺省情况下，IKE profile视图下没有配置DPD功能，采用系统视图下的DPD配置。若两者没有配置，则不进行DPD探测
（可选）配置IKE profile的使用范围	**match local address** { *interface-type interface-number* | { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-name*] }	缺省情况下，未限制IKE profile的使用范围
（可选）配置内部MPLS L3VPN实例	**inside-vpn vpn-instance** *vpn-name*	缺省情况下，IKE profile未指定内部VPN实例，即内网与外网在同一个VPN中
（可选）配置IKE profile的优先级	**priority** *number*	缺省情况下，IKE profile的优先级为100

2.4 配置IKE提议

IKE 定义了一套属性数据来描述 IKE 第一阶段使用怎样的参数来与对端进行协商。用户可以创建多条不同优先级的 IKE 提议。协商双方必须至少有一条匹配的 IKE 提议才能协商成功。

在进行 IKE 协商时，协商发起方会将自己的 IKE 提议发送给对端，由对端进行匹配。

- 若发起方使用的 IPsec 安全策略中没有引用 IKE profile，则会将当前系统中所有的 IKE 提议发送给对端，这些 IKE 提议的优先级顺序由 IKE 提议的序号决定，序号越小优先级越高；
- 若发起方的 IPsec 策略中引用了 IKE profile，则会将该 IKE profile 中引用的所有 IKE 提议发送给对端，这些 IKE 提议的优先级由引用的先后顺序决定，先引用的优先级高。

协商响应方则以对端发送的 IKE 提议优先级从高到低的顺序与本端所有的 IKE 提议进行匹配，直到找到一个匹配的提议来使用。匹配的 IKE 提议将被用来建立 IKE SA。

以上 IKE 提议的匹配原则是：协商双方具有相同的加密算法、认证方法、认证算法和 DH group 标识。匹配的 IKE 提议的 IKE SA 存活时间则取两端的最小值。

表2-3 配置 IKE 提议

操作	命令	说明
进入系统视图	**system-view**	-
创建IKE提议，并进入IKE提议视图	**ike proposal** *proposal-number*	缺省情况下，存在一个缺省的IKE提议
指定一个供IKE提议使用的加密算法	非FIPS模式下： **encryption-algorithm { 3des-cbc | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | des-cbc }** FIPS模式下： **encryption-algorithm { aes-cbc-128 | aes-cbc-192 | aes-cbc-256 }**	非FIPS模式下： 缺省情况下，IKE提议使用CBC模式的56-bit DES加密算法 FIPS模式下： 缺省情况下，IKE提议使用CBC模式的128-bit AES加密算法
指定一个供IKE提议使用的认证方法	**authentication-method { dsa-signature | pre-share | rsa-signature }**	缺省情况下，IKE提议使用预共享密钥的认证方法
指定一个供IKE提议使用的认证算法	非FIPS模式下： **authentication-algorithm { md5 | sha }** FIPS模式下： **authentication-algorithm sha**	缺省情况下，IKE提议使用HMAC-SHA1认证算法
配置IKE第一阶段密钥协商时所使用的DH密钥交换参数	非FIPS模式下： **dh { group1 | group14 | group2 | group24 | group5 }** FIPS模式下： **dh group14**	非FIPS模式下： 缺省情况下，IKE第一阶段密钥协商时所使用的DH密钥交换参数为**group1**，即768-bit的Diffie-Hellman group FIPS模式下： 缺省情况下，IKE阶段1密钥协商时所使用的DH密钥交换参数为**group14**，即2048-bit的Diffie-Hellman group
指定一个IKE提议的IKE SA存活时间	**sa duration** *seconds*	缺省情况下，IKE提议的IKE SA存活时间为86400秒

2.5 配置IKE keychain

在 IKE 需要通过预共享密钥方式进行身份认证时，协商双方需要创建并指定 IKE keychain。IKE keychain 用于配置协商双方的密钥信息，具体包括以下内容：

- 预共享密钥。IKE 协商双方配置的预共享密钥必须相同，否则身份认证会失败。以明文或密文方式设置的预共享密钥，均以密文的方式保存在配置文件中。

- IKE keychain 的使用范围。限制 keychain 的使用范围，即 IKE keychain 只能在指定的地址或指定接口对应的地址下使用(这里的地址指的是 IPsec 安全策略/IPsec 安全策略模板下配置的本端地址，若本端地址没有配置，则为引用 IPsec 安全策略的接口的 IP 地址)。
- IKE keychain 的优先级。配置了 **match local address** 的 IKE keychain 的优先级高于所有未配置 **match local address** 的 IKE keychain。即 IKE keychain 的优先级首先决定于是否配置了 **match local address**，其次取决于配置的优先级，最后决定于配置 IKE keychain 的先后顺序。

表2-4 配置 IKE keychain

操作	命令	说明
进入系统视图	**system-view**	-
创建IKE keychain，并进入IKE keychain视图	**ike keychain** *keychain-name* [**vpn-instance** *vpn-name*]	缺省情况下，不存在IKE keychain
配置预共享密钥	**pre-shared-key** { **address** { *ipv4-address* [*mask* | *mask-length*] | **ipv6** *ipv6-address* [*prefix-length*] } | **hostname** *host-name* } **key** { **cipher** *cipher-key* | **simple** *simple-key* }	缺省情况下，未配置预共享密钥
（可选）配置IKE keychain的使用范围	**match local address** { *interface-type interface-number* | { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-name*] }	缺省情况下，未限制IKE keychain的使用范围
（可选）配置IKE keychain的优先级	**priority** *number*	缺省情况下，IKE keychain的优先级为100

2.6 配置本端身份信息

本端身份信息适用于所有 IKE SA 的协商，而 IKE profile 下的 **local-identity** 仅适用于本 IKE profile。如果 IKE profile 下没有配置本端身份，则默认使用此处配置的全局本端身份。

- 如果本端采用的认证方式为数字签名，则本端配置的任何类型的身份信息都有效；
- 如果本端采用认证方式为预共享密钥，则本端除 DN 之外的其它类型的身份信息均有效。

表2-5 配置本端身份信息

操作	命令	说明
进入系统视图	**system-view**	-
配置本端身份信息	**ike identity** { **address** { *ipv4-address* | **ipv6** *ipv6-address* } | **dn** | **fqdn** [*fqdn-name*] | **user-fqdn** [*user-fqdn-name*] }	缺省情况下，使用IP地址标识本端的身份，该IP地址为IPsec安全策略或IPsec安全策略模板应用的接口地址

操作	命令	说明
（可选）配置当使用数字签名认证方式时，本端的身份总从证书的主题字段中获得	**ike signature-identity from-certificate**	缺省情况下，本端身份信息由**local-identity**或**ike identity**命令指定 在采用IPsec野蛮协商模式且使用数字签名认证方式的情况下，与仅支持使用DN类型的身份进行数字签名认证的ComwareV5设备互通时需要配置本命令

2.7 配置IKE Keepalive功能

IKE Keepalive 功能用于检测对端是否存活。在对端配置了等待 IKE Keepalive 报文的超时时间后，必须在本端配置发送 IKE Keepalive 报文的时间间隔。当对端 IKE SA 在配置的超时时间内未收到 IKE Keepalive 报文时，则删除该 IKE SA 以及由其协商的 IPsec SA。

配置 IKE Keepalive 功能时，请遵循以下配置限制和指导：

- 当有检测对方是否存活的需求时，通常建议配置 IKE DPD，不建议配置 IKE Keepalive。仅当对方不支持 IKE DPD 功能且支持 IKE Keepalive 功能时，才考虑配置 IKE Keepalive 功能。配置 IKE Keepalive 功能后，会定时检测对方是否存活，因此会额外消耗网络带宽和计算资源。
- 本端配置的 IKE Keepalive 报文的等待超时时间要大于对端发送的时间间隔。由于网络中一般不会出现超过连续三次的报文丢失，所以，本端的超时时间可以配置为对端配置的发送 IKE Keepalive 报文的时间间隔的三倍。

表2-6 配置 IKE Keepalive 功能

操作	命令	说明
进入系统视图	**system-view**	-
配置通过IKE SA向对端发送IKE Keepalive报文的时间间隔	**ike keepalive interval** *seconds*	缺省情况下，不向对端发送IKE Keepalive报文
配置本端等待对端发送IKE Keepalive报文的超时时间	**ike keepalive timeout** *seconds*	缺省情况下，永不超时，一直等待对端发送IKE Keepalive报文

2.8 配置IKE NAT Keepalive功能

在采用 IKE 协商建立的 IPsec 隧道中，可能存在 NAT 设备，由于在 NAT 设备上的 NAT 会话有一定存活时间，一旦 IPsec 隧道建立后如果长时间没有流量，对应的 NAT 会话表项会被删除，这样将导致 IPsec 隧道无法继续传输数据。为防止 NAT 表项老化，NAT 内侧的 IKE 网关设备需要定时向 NAT 外侧的 IKE 网关设备发送 NAT Keepalive 报文，以便维持 NAT 设备上对应的 IPsec 流量的会话存活，从而让 NAT 外侧的设备可以访问 NAT 内侧的设备。

表2-7 配置 IKE NAT Keepalive 功能

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
配置向对端发送NAT Keepalive报文的时间间隔	**ike nat-keepalive** *seconds*	缺省情况下，向对端发送NAT Keepalive报文的时间间隔为20秒

2.9 配置IKE DPD功能

DPD（Dead Peer Detection，对等体存活检测）用于检测对端是否存活。本端主动向对端发送 DPD 请求报文，对对端是否存活进行检测。如果本端在 DPD 报文的重传时间间隔（**retry** *seconds*）内未收到对端发送的 DPD 回应报文，则重传 DPD 请求报文，若重传两次之后仍然没有收到对端的 DPD 回应报文，则删除该 IKE SA 和对应的 IPsec SA。

配置 IKE DPD 功能时，请遵循以下配置限制和指导：

- IKE DPD 有两种模式：按需探测模式（**on-demand**）和定时探测模式（**periodic**）。一般若无特别要求，建议使用按需探测模式，在此模式下，仅在本端需要发送报文时，才会触发探测；如果需要尽快地检测出对端的状态，则可以使用定时探测模式。在定时探测模式下工作，会消耗更多的带宽和计算资源，因此当设备与大量的 IKE 对端通信时，应优先考虑使用按需探测模式。
- 如果 IKE profile 视图下和系统视图下都配置了 DPD 探测功能，则 IKE profile 视图下的 DPD 配置生效，如果 IKE profile 视图下没有配置 DPD 探测功能，则采用系统视图下的 DPD 配置。
- 建议配置的触发 IKE DPD 探测的时间间隔大于 DPD 报文的重传时间间隔，使得直到当前 DPD 探测结束才可以触发下一次 DPD 探测，DPD 在重传过程中不触发新的 DPD 探测。

以定时探测模式为例，若本端的 IKE DPD 配置如下：

ike dpd interval 10 retry 6 periodic

则，具体的探测过程为：IKE SA 协商成功之后 10 秒，本端会发送 DPD 探测报文，并等待接收 DPD 回应报文。若本端在 6 秒内没有收到 DPD 回应报文，则会第二次发送 DPD 探测报文。在此过程中总共会发送三次 DPD 探测报文，若第三次 DPD 探测报文发出后 6 秒仍没收到 DPD 回应报文，则会删除发送 DPD 探测报文的 IKE SA 及其对应的所有 IPsec SA。若在此过程中收到了 DPD 回应报文，则会等待 10 秒再次发送 DPD 探测报文。

表2-8 配置全局 IKE DPD 功能

操作	命令	说明
进入系统视图	**system-view**	-
配置IKE DPD功能	**ike dpd interval** *interval-seconds* [**retry** *seconds*] { **on-demand** | **periodic** }	缺省情况下，IKE DPD功能处于关闭状态

2.10 配置针对无效IPsec SPI的IKE SA恢复功能

当 IPsec 隧道一端的安全网关出现问题（例如安全网关重启）导致其 IPsec SA 丢失时，会造成 IPsec 流量黑洞现象：一端（接收端）的 IPsec SA 已经丢失，而另一端（发送端）还持有对应的 IPsec SA 且不断地向对端发送报文，当接收端收到发送端使用此 IPsec SA 封装的 IPsec 报文时，就会因为

找不到对应的 SA 而持续丢弃报文，形成流量黑洞。该现象造成 IPsec 通信链路长时间得不到恢复（只有等到发送端旧的 IPsec SA 生命周期超时，并重建 IPsec SA 后，两端的 IPsec 流量才能得以恢复），因此需要采取有效的 IPsec SA 恢复手段来快速恢复中断的 IPsec 通信链路。

IPsec SA 由 SPI 唯一标识，接收方根据 IPsec 报文中的 SPI 在 SA 数据库中查找对应的 IPsec SA，若接收方找不到处理该报文的 IPsec SA，则认为此报文的 SPI 无效。如果接收端当前存在 IKE SA，则会向对端发送删除对应 IPsec SA 的通知消息，发送端 IKE 接收到此通知消息后，就会立即删除此无效 SPI 对应的 IPsec SA。之后，当发送端需要继续向接收端发送报文时，就会触发两端重建 IPsec SA，使得中断的 IPsec 通信链路得以恢复；如果接收端当前不存在 IKE SA，就不会触发本端向对端发送删除 IPsec SA 的通知消息，接受端将默认丢弃无效 SPI 的 IPsec 报文，使得链路无法恢复。后一种情况下，如果使能了 IPsec 无效 SPI 恢复 IKE SA 功能，就会触发本端与对端协商新的 IKE SA 并发送删除消息给对端，从而使链路恢复正常。

由于使能此功能后，若攻击者伪造大量源 IP 地址不同但目的 IP 地址相同的无效 SPI 报文发给设备，会导致设备因忙于与无效对端协商建立 IKE SA 而面临受到 DoS（Denial of Sevice）攻击的风险。因此，建议通常不要打开 **ike invalid-spi-recovery enable** 功能。

表2-9 使能针对无效 IPsec SPI 的 IKE SA 恢复功能

操作	命令	说明
进入系统视图	**system-view**	-
使能针对无效IPsec SPI的IKE SA恢复功能	**ike invalid-spi-recovery enable**	缺省情况下，针对无效IPsec SPI的IKE SA恢复功能处于关闭状态

2.11 配置对IKE SA数目的限制

由于不同设备的能力不同，为充分利用设备的处理能力，可以配置允许同时处于协商状态的 IKE SA 的最大数，也可以配置允许建立的 IKE SA 的最大数。

若设置允许同时协商更多的 IKE SA，则可以充分利用设备处理能力，以便在设备有较强处理能力的情况下得到更高的新建性能；若设置允许同时协商较少的 IKE SA，则可以避免产生大量不能完成协商的 IKE SA，以便在设备处理能力较弱时保证一定的新建性能。

若设置允许建立更多的 IKE SA，则可以使得设备在有充足内存的情况下得到更高的并发性能；若设置允许建立较少的 IKE SA，则可以在设备没有充足内存的情况下，使得 IKE 不过多占用系统内存。

表2-10 配置对本端 IKE SA 数目的限制

操作	命令	说明
进入系统视图	**system-view**	-
配置对本端IKE SA数目的限制	**ike limit** { **max-negotiating-sa** *negotiation-limit* | **max-sa** *sa-limit* }	缺省情况下，不限制允许同时处于协商状态的IKE SA数目，也不限制允许建立的IKE SA的最大数目

2.12 配置IKE告警功能

开启 IKE 的告警功能后，IKE 会生成告警信息，用于向网管软件报告该模块的重要事件。生成的告警信息将被发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

如果希望生成并输出某种类型的 IKE 告警信息，则需要保证 IKE 的全局告警功能以及相应类型的告警功能均处于开启状态。

表2-11 配置 IKE 告警功能

操作	命令	说明
进入系统视图	**system-view**	-
开启IKE的全局告警功能	**snmp-agent trap enable ike global**	缺省情况下，IKE的告警Trap功能处于开启状态
开启IKE的指定告警功能	**snmp-agent trap enable ike** [**attr-not-support** | **auth-failure** | **cert-type-unsupport** | **cert-unavailable** | **decrypt-failure** | **encrypt-failure** | **invalid-cert-auth** | **invalid-cookie** | **invalid-id** | **invalid-proposal** | **invalid-protocol** | **invalid-sign** | **no-sa-failure** | **proposal-add** | **proposal–delete** | **tunnel-start** | **tunnel-stop** | **unsupport-exch-type**] *	缺省情况下，IKE的所有告警功能均处于开启状态

2.13 IKE显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 IKE 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** 命令可以删除 IKE SA。

表2-12 IKE 显示和维护

操作	命令
显示所有IKE提议的配置信息	**display ike proposal**
显示当前IKE SA的信息	**display ike sa** [**verbose** [**connection-id** *connection-id* | **remote-address** [**ipv6**] *remote-address* [**vpn-instance** *vpn-name*]]]
清除IKE SA	**reset ike sa** [**connection-id** *connection-id*]
清除IKE的MIB统计信息	**reset ike statistics**

2.14 IKE典型配置举例

2.14.1 IKE主模式及预共享密钥认证典型配置举例

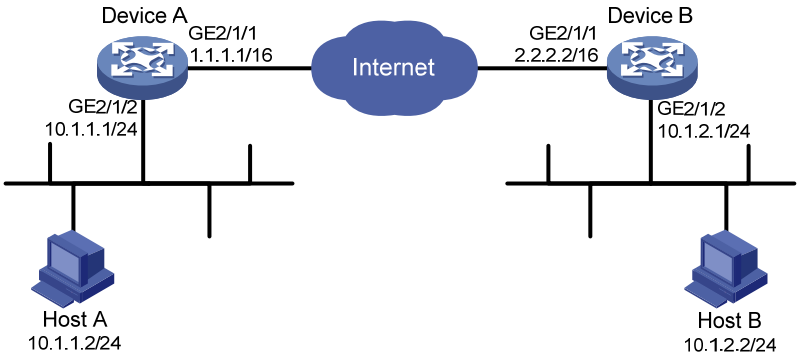
1. 组网需求

在 Device A 和 Device B 之间建立一个 IPsec 隧道，对 Host A 所在的子网（10.1.1.0/24）与 Host B 所在的子网（10.1.2.0/24）之间的数据流进行安全保护。

- Device A 和 Device B 之间采用 IKE 协商方式建立 IPsec SA。
- 使用缺省的 IKE 提议。
- 使用缺省的预共享密钥认证方法。

2. 组网图

图2-3 IKE 主模式及预共享密钥认证典型组网图



3. 配置步骤

(1) 配置 Device A

配置各接口的 IP 地址，具体略。

配置 ACL 3101，定义要保护由子网 10.1.1.0/24 去子网 10.1.2.0/24 的数据流。

```
<DeviceA> system-view
[DeviceA] acl number 3101
[DeviceA-acl-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0
0.0.0.255
[DeviceA-acl-adv-3101] quit
```

创建 IPsec 安全提议 tran1。

```
[DeviceA] ipsec transform-set tran1
```

配置安全协议对 IP 报文的封装形式为隧道模式。

```
[DeviceA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

配置采用的安全协议为 ESP。

```
[DeviceA-ipsec-transform-set-tran1] protocol esp
```

配置 ESP 协议采用的加密算法为 128 比特的 AES，认证算法为 HMAC-SHA1。

```
[DeviceA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[DeviceA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceA-ipsec-transform-set-tran1] quit
```

创建 IKE keychain，名称为 keychain1。

```
[DeviceA] ike keychain keychain1
```

配置与 IP 地址为 2.2.2.2 的对端使用的预共享密钥为明文 123456TESTplat&!。

```
[DeviceA-ike-keychain-keychain1] pre-shared-key address 2.2.2.2 255.255.255.0 key simple
123456TESTplat&!
[DeviceA-ike-keychain-keychain1] quit
```

创建 IKE profile，名称为 profile1。

```
[DeviceA] ike profile profile1
```

指定引用的 IKE keychain 为 keychain1。

```
[DeviceA-ike-profile-profile1] keychain keychain1
```

配置本端的身份信息为 IP 地址 1.1.1.1。

```
[DeviceA-ike-profile-profile1] local-identity address 1.1.1.1
```

配置匹配对端身份的规则为 IP 地址 2.2.2.2/24。

```
[DeviceA-ike-profile-profile1] match remote identity address 2.2.2.2 255.255.255.0
[DeviceA-ike-profile-profile1] quit
```

创建一条 IKE 协商方式的 IPsec 安全策略，名称为 map1，顺序号为 10。

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

配置 IPsec 隧道的对端 IP 地址为 2.2.2.2。

```
[DeviceA-ipsec-policy-isakmp-map1-10] remote-address 2.2.2.2
```

指定引用 ACL 3101。

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

指定引用的安全提议为 tran1。

```
[DeviceA-ipsec-policy-isakmp-map1-10] transform-set tran1
```

指定引用的 IKE profile 为 profile1。

```
[DeviceA-ipsec-policy-isakmp-map1-10] ike-profile profile1
[DeviceA-ipsec-policy-isakmp-map1-10] quit
```

在接口 GigabitEthernet2/1/1 上应用 IPsec 安全策略 map1。

```
[DeviceA-GigabitEthernet2/1/1] ipsec apply policy map1
[DeviceA-GigabitEthernet2/1/1] quit
```

配置到 Host B 所在子网的静态路由。

```
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 2.2.2.2
```

(2) 配置 Device B

配置各接口的 IP 地址，具体略。

配置 ACL 3101，定义要保护由子网 10.1.2.0/24 去往子网 10.1.1.0/24 的数据流。

```
<DeviceB> system-view
[DeviceB] acl number 3101
[DeviceB-acl-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0
0.0.0.255
[DeviceB-acl-adv-3101] quit
```

创建 IPsec 安全提议 tran1。

```
[DeviceB] ipsec transform-set tran1
```

配置安全协议对 IP 报文的封装形式为隧道模式。

```
[DeviceB-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

配置采用的安全协议为 ESP。

```
[DeviceB-ipsec-transform-set-tran1] protocol esp
```

配置 ESP 协议采用的加密算法为 128 比特的 AES，认证算法为 HMAC-SHA1。

```
[DeviceB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
[DeviceB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceB-ipsec-transform-set-tran1] quit
```

创建 IKE keychain，名称为 keychain1。

```
[DeviceB]ike keychain keychain1
```

配置与 IP 地址为 1.1.1.1 的对端使用的预共享密钥为明文 123456TESTplat&!。

```
[DeviceB-ike-keychain-keychain1] pre-shared-key address 1.1.1.1 255.255.255.0 key simple
123456TESTplat&!
[DeviceB-ike-keychain-keychain1] quit
```

创建 IKE profile，名称为 profile1。

```
[DeviceB] ike profile profile1
```

指定引用的 IKE keychain 为 keychain1。

```
[DeviceB-ike-profile-profile1] keychain keychain1
```

配置本端的身份信息为 IP 地址 2.2.2.2。

```
[DeviceB-ike-profile-profile1] local-identity address 2.2.2.2
```

配置匹配对端身份的规则为 IP 地址 1.1.1.1/24。

```
[DeviceB-ike-profile-profile1] match remote identity address 1.1.1.1 255.255.255.0
[DeviceB-ike-profile-profile1] quit
```

创建一条 IKE 协商方式的 IPsec 安全策略，名称为 use1，顺序号为 10。

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

配置 IPsec 隧道的对端 IP 地址为 1.1.1.1。

```
[DeviceB-ipsec-policy-isakmp-use1-10] remote-address 1.1.1.1
```

指定引用 ACL 3101。

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

指定引用的安全提议为 tran1。

```
[DeviceB-ipsec-policy-isakmp-use1-10] transform-set tran1
```

指定引用的 IKE profile 为 profile1。

```
[DeviceB-ipsec-policy-isakmp-use1-10] ike-profile profile1
[DeviceB-ipsec-policy-isakmp-use1-10] quit
```

在接口 GigabitEthernet2/1/1 上应用 IPsec 安全策略 use1。

```
[DeviceB-GigabitEthernet2/1/1] ipsec apply policy use1
```

配置到 Host A 所在子网的静态路由。

```
[DeviceB] ip route-static 10.1.1.0 255.255.255.0 1.1.1.1
```

4. 验证配置

以上配置完成后，Device A 和 Device B 之间如果有子网 10.1.1.0/24 与子网 10.1.2.0/24 之间的报文通过，将触发 IKE 协商。

可通过如下显示信息查看到 Device A 和 Device B 上的 IKE 提议。因为没有配置任何 IKE 提议，则只显示缺省的 IKE 提议。

```
[DeviceA] display ike proposal
 Priority Authentication Authentication Encryption  Diffie-Hellman Duration
```

```
              method       algorithm    algorithm       group      (seconds)
-------------------------------------------------------------------------------
default  PRE-SHARED-KEY     SHA1       AES-CBC-128     Group 1        86400

[DeviceB] display ike proposal
 Priority Authentication Authentication Encryption  Diffie-Hellman Duration
              method       algorithm    algorithm       group      (seconds)
-------------------------------------------------------------------------------
default  PRE-SHARED-KEY     SHA1       AES-CBC-128     Group 1        86400
```

可通过如下显示信息查看到 Device A 上 IKE 第一阶段协商成功后生成的 IKE SA。

```
[DeviceA] display ike sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
    1               2.2.2.2               RD           IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
```

可通过如下显示信息查看到 IKE 第二阶段协商生成的 IPsec SA。

```
[DeviceA] display ipsec sa
------------------------------
Interface: GigabitEthernet2/1/1
------------------------------

  ----------------------------
  IPsec policy: map1
  Sequence number: 10
  Mode: isakmp
  ----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect forward secrecy:
    Path MTU: 1456
    Tunnel:
        local  address: 1.1.1.1
        remote address: 2.2.2.2
    Flow:
    sour addr: 10.1.1.0/255.255.255.0  port: 0  protocol: IP
    dest addr: 10.1.2.0/255.255.255.0  port: 0  protocol: IP

    [Inbound ESP SAs]
      SPI: 3264152513 (0xc28f03c1)
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843200/3484
      Max received sequence-number:
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: active
```

```
[Outbound ESP SAs]
  SPI: 738451674 (0x2c03e0da)
  Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
  SA duration (kilobytes/sec): 1843200/3600
  SA remaining duration (kilobytes/sec): 1843200/3484
  Max received sequence-number:
  UDP encapsulation used for NAT traversal: N
  Status: active
```

Device B 上也会产生相应的 IKE SA 和 IPsec SA，查看方式与 Device A 同，此处略。

2.14.2 IKE野蛮模式及RSA数字签名认证典型配置举例

说明

设备运行于 FIPS 模式时，不支持本例。

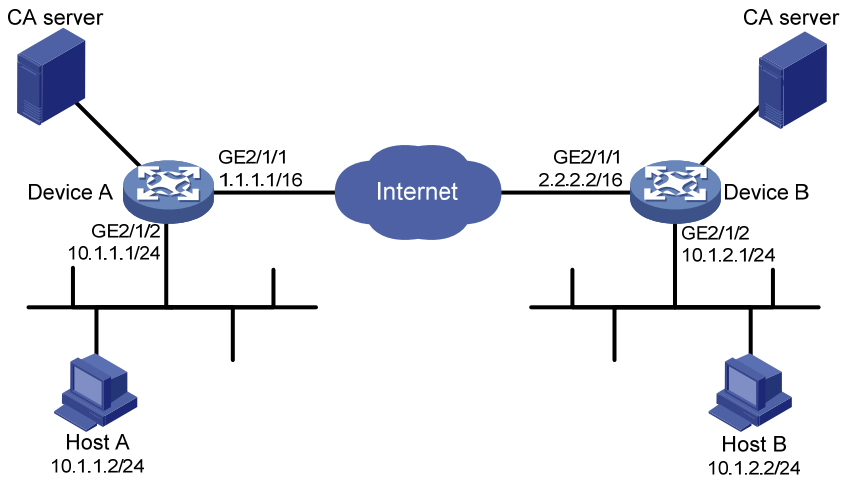
1. 组网需求

在 Device A 和 Device B 之间建立一个 IPsec 隧道，对 Host A 所在的子网（10.1.1.0/24）与 Host B 所在的子网（10.1.2.0/24）之间的数据流进行安全保护。

- Device A 和 Device B 之间采用 IKE 协商方式建立 IPsec SA。
- Device A 和 DeviceB 均使用 RSA 数字签名的认证方法。
- IKE 第一阶段的协商模式为野蛮模式。
- Device A 侧子网的 IP 地址为动态分配，因此 Device A 作为发起方。

2. 组网图

图2-4 IKE 野蛮模式及 RSA 数字签名认证典型组网图



3. 配置步骤

(1) 配置 Device A

配置各接口的 IP 地址，具体略。

配置 ACL 3101，定义要保护由子网 10.1.1.0/24 去往子网 10.1.2.0/24 的数据流。

```
<DeviceA> system-view
[DeviceA] acl number 3101
[DeviceA-acl-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0
0.0.0.255
[DeviceA-acl-adv-3101] quit
```

创建 IPsec 安全提议 tran1。

```
[DeviceA] ipsec transform-set tran1
```

配置安全协议对 IP 报文的封装形式为隧道模式。

```
[DeviceA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

配置采用的安全协议为 ESP。

```
[DeviceA-ipsec-transform-set-tran1] protocol esp
```

配置 ESP 协议采用的加密算法为 DES，认证算法为 HMAC-SHA1。

```
[DeviceA-ipsec-transform-set-tran1] esp encryption-algorithm des-cbc
[DeviceA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[DeviceA-ipsec-transform-set-tran1] quit
```

创建 PKI 实体 entity1。

```
[DeviceA] pki entity entity1
```

配置 PKI 实体的通用名。

```
[DeviceA-pki-entity-entity1] common-name routera
[DeviceA-pki-entity-entity1] quit
```

创建 PKI 域 domain1。

```
[DeviceA] pki domain domain1
```

配置证书申请模式为自动模式，并设置吊销证书时使用的口令。

```
[DeviceA-pki-domain-domain1] certificate request mode auto password simple 123
```

配置验证 CA 根证书时所使用的指纹。

```
[DeviceA-pki-domain-domain1] root-certificate fingerprint md5
50c7a2d282ea710a449eede6c56b102e
```

配置 CA 服务器名称。

```
[DeviceA-pki-domain-domain1] ca identifier 8088
```

配置实体通过 SCEP 进行证书申请的注册受理机构服务器的 URL（此处的 URL 仅为示例，请以组网环境中的实际情况为准）。

```
[DeviceA-pki-domain-domain1] certificate request url
http://192.168.222.1:446/eadbf9af4f2c4641e685f7a6021e7b298373feb7
```

配置证书申请的注册受理机构。

```
[DeviceA-pki-domain-domain1] certificate request from ca
```

配置指定用于申请证书的 PKI 实体名称。

```
[DeviceA-pki-domain-domain1] certificate request entity entity1
```

配置指定证书申请使用的 RSA 密钥对。

```
[DeviceA-pki-domain-domain1] public-key rsa general name rsa1
[DeviceA-pki-domain-domain1] quit
```

创建 IKE profile，名称为 profile1。

```
[DeviceA] ike profile profile1
```

指定引用的 PKI 域为 domain1。

```
[DeviceA-ike-profile-profile1] certificate domain domain1
```

配置第一阶段的协商模式为野蛮模式。

```
[DeviceA-ike-profile-profile1] exchange-mode aggressive
```

配置 FQDN 名 www.routera.com 作为本端的身份标识。

```
[DeviceA-ike-profile-profile1] local-identity fqdn www.routera.com
```

配置匹配对端身份的规则为 FQDN 名 www.routerb.com。

```
[DeviceA-ike-profile-profile1] match remote identity fqdn www.routerb.com
[DeviceA-ike-profile-profile1] quit
```

创建 IKE 提议 10。

```
[DeviceA] ike proposal 10
```

指定 IKE 提议使用的认证算法为 HMAC-MD5。

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

指定使用 RSA 数字签名认证方法。

```
[DeviceA-ike-proposal-10] authentication-method rsa-signature
[DeviceA-ike-proposal-10] quit
```

创建一条 IKE 协商方式的 IPsec 安全策略，名称为 map1，顺序号为 10。

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

配置 IPsec 隧道的对端 IP 地址为 2.2.2.2。

```
[DeviceA-ipsec-policy-isakmp-map1-10] remote-address 2.2.2.2
```

指定引用的安全提议为 tran1。

```
[DeviceA-ipsec-policy-isakmp-map1-10] transform-set tran1
```

指定引用 ACL 3101。

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

指定引用的 IKE profile 为 profile1。

```
[DeviceA-ipsec-policy-isakmp-map1-10] ike-profile profile1
[DeviceA-ipsec-policy-isakmp-map1-10] quit
```

在接口 GigabitEthernet2/1/1 上应用 IPsec 安全策略 map1。

```
[DeviceA-GigabitEthernet2/1/1] ipsec apply policy map1
[DeviceA-GigabitEthernet2/1/1] quit
```

配置到 Host B 所在子网的静态路由。

```
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 2.2.2.2
```

(2)　配置 Device B

配置各接口的 IP 地址，具体略。

创建 IPsec 安全提议 tran1。

```
[DeviceB] ipsec transform-set tran1
```

配置安全协议对 IP 报文的封装形式为隧道模式。

```
[DeviceB-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

配置采用的安全协议为 ESP。

```
[DeviceB-ipsec-transform-set-tran1] protocol esp
```

配置 ESP 协议采用的加密算法为 DES，认证算法为 HMAC-SHA1。

```
[DeviceB-ipsec-transform-set-tran1] esp encryption-algorithm des-cbc
[DeviceB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
```

```
[DeviceB-ipsec-transform-set-tran1] quit
```
创建 PKI 实体 entity2。
```
[DeviceB] pki entity entity2
```
配置 PKI 实体的通用名。
```
[DeviceB-pki-entity-entity2] common-name routerb
[DeviceB-pki-entity-entity2] quit
```
创建 PKI 域 domain2。
```
[DeviceB] pki domain domain2
```
配置证书申请模式为自动模式，并设置吊销证书时使用的口令。
```
[DeviceB-pki-domain-domain2] certificate request mode auto password simple 123
```
配置验证 CA 根证书时所使用的指纹。
```
[DeviceB-pki-domain-domain2] root-certificate fingerprint md5
50c7a2d282ea710a449eede6c56b102e
```
配置 CA 服务器名称。
```
[DeviceB-pki-domain-domain2] ca identifier 8088
```
配置实体通过 SCEP 进行证书申请的注册受理机构服务器的 URL（此处的 URL 仅为示例，请以组网环境中的实际情况为准）。
```
[DeviceB-pki-domain-domain2] certificate request url
http://192.168.222.1:446/eadbf9af4f2c4641e685f7a6021e7b298373feb7
```
配置证书申请的注册受理机构。
```
[DeviceB-pki-domain-domain2] certificate request from ca
```
配置指定用于申请证书的 PKI 实体名称。
```
[DeviceB-pki-domain-domain2] certificate request entity entity2
```
配置指定证书申请使用的 RSA 密钥对。
```
[DeviceB-pki-domain-domain2] public-key rsa general name rsa1
[DeviceB-pki-domain-domain2] quit
```
创建 IKE profile，名称为 profile2。
```
[DeviceB] ike profile profile2
```
配置 FQDN 名 www.routerb.com 作为本端的身份标识。
```
[DeviceB-ike-profile-profile2] local-identity identity fqdn www.routerb.com
```
配置匹配对端身份的规则为 FQDN 名 www.routera.com。
```
[DeviceB-ike-profile-profile2] match remote identity fqdn www.routera.com
[DeviceB-ike-profile-profile2] quit
```
创建 IKE 提议 10。
```
[DeviceB] ike proposal 10
```
指定 IKE 提议使用的认证算法为 HMAC-MD5。
```
[DeviceB-ike-proposal-10] authentication-algorithm md5
```
指定使用 RSA 数字签名认证方法。
```
[DeviceB-ike-proposal-10] authentication-method rsa-signature
[DeviceB-ike-proposal-10] quit
```
创建一条 IPsec 安全策略模板，名称为 template1，顺序号为 1。
```
[DeviceB] ipsec policy-template template1 1
```
指定引用的安全提议为 tran1。
```
[DeviceB-ipsec-policy-template-template1-1] transform-set tran1
```

```
[DeviceB-ipsec-policy-template-template1-1] quit
```
引用 IPsec 安全策略模板创建一条 IPsec 安全策略，名称为 use1，顺序号为 1。
```
[DeviceB] ipsec policy use1 1 isakmp template template1
```
在接口 GigabitEthernet2/1/1 上应用 IPsec 安全策略 use1。
```
[DeviceB-GigabitEthernet2/1/1] ipsec apply policy use1
[DeviceB-GigabitEthernet2/1/1] quit
```
配置到 Host A 所在子网的静态路由。
```
[DeviceB] ip route-static 10.1.1.0 255.255.255.0 1.1.1.1
```
4. 验证配置

以上配置完成后，Device A 和 Device B 之间如果有子网 10.1.1.0/24 与子网 10.1.2.0/24 之间的报文通过，将触发 IKE 协商。

可通过如下显示信息查看到 Device A 和 Device B 上的 IKE 提议。
```
[DeviceA] display ike proposal 10
 Priority Authentication Authentication Encryption  Diffie-Hellman Duration
              method       algorithm    algorithm       group      (seconds)
------------------------------------------------------------------------------
 10       RSA-SIG            MD5        DES-CBC     Group 1        5000
 default  PRE-SHARED-KEY     SHA1       DES-CBC     Group 1        86400

[DeviceB] display ike proposal 10
 Priority Authentication Authentication Encryption  Diffie-Hellman Duration
              method       algorithm    algorithm       group      (seconds)
------------------------------------------------------------------------------
 10       RSA-SIG            MD5        DES-CBC     Group 1        5000
 default  PRE-SHARED-KEY     SHA1       DES-CBC     Group 1        86400
```
可通过如下显示信息查看到 Device A 上 IKE 第一阶段协商成功后生成的 IKE SA。
```
[DeviceA] display ike sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
    1               2.2.2.2               RD           IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
```
可通过如下显示信息查看到 Device A 上自动触发获取到的 CA 证书。
```
[DeviceA] display pki certificate domain domain1 ca
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            b9:14:fb:25:c9:08:2c:9d:f6:94:20:30:37:4e:00:00
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=cn, O=rnd, OU=sec, CN=8088
        Validity
            Not Before: Sep  6 01:53:58 2012 GMT
            Not After : Sep  8 01:50:58 2015 GMT
        Subject: C=cn, O=rnd, OU=sec, CN=8088
        Subject Public Key Info:
```

```
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:de:81:f4:42:c6:9f:c2:37:7b:21:84:57:d6:42:
                    00:69:1c:4c:34:a4:5e:bb:30:97:45:2b:5e:52:43:
                    c0:49:1f:e1:d8:0f:5c:48:c2:39:69:d1:84:e4:14:
                    70:3d:98:41:28:1c:20:a1:9a:3f:91:67:78:77:27:
                    d9:08:5f:7a:c4:36:45:8b:f9:7b:e7:7d:6a:98:bb:
                    4e:a1:cb:2c:3d:92:66:bd:fb:80:35:16:c6:35:f0:
                    ff:0b:b9:3c:f3:09:94:b7:d3:6f:50:8d:83:f1:66:
                    2f:91:0b:77:a5:98:22:b4:77:ac:84:1d:03:8e:33:
                    1b:31:03:78:4f:77:a0:db:af
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha1WithRSAEncryption
        9a:6d:8c:46:d3:18:8a:00:ce:12:ee:2b:b0:aa:39:5d:3f:90:
        08:49:b9:a9:8f:0d:6e:7b:e1:00:fb:41:f5:d4:0c:e4:56:d8:
        7a:a7:61:1d:2b:b6:72:e3:09:0b:13:9d:fa:c8:fc:c4:65:a7:
        f9:45:21:05:75:2c:bf:36:7b:48:b4:4a:b9:fe:87:b9:d8:cf:
        55:16:87:ec:07:1d:55:5a:89:74:73:68:5e:f9:1d:30:55:d9:
        8a:8f:c5:d4:20:7e:41:a9:37:57:ed:8e:83:a7:80:2f:b8:31:
        57:3a:f2:1a:28:32:ea:ea:c5:9a:55:61:6a:bc:e5:6b:59:0d:
        82:16
```

可通过如下显示信息查看到 Device A 上自动触发申请到的本地证书。

```
[DeviceA] display pki certificate domain domain1 local
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            a1:f4:d4:fd:cc:54:c3:07:c4:9e:15:2d:5f:64:57:77
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=cn, O=rnd, OU=sec, CN=8088
        Validity
            Not Before: Sep 26 02:06:43 2012 GMT
            Not After : Sep 26 02:06:43 2013 GMT
        Subject: CN=devicea
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b0:a1:cd:24:6e:1a:1d:51:79:f0:2a:3e:9f:e9:
                    84:07:16:78:49:1b:7d:0b:22:f0:0a:ed:75:91:a4:
                    17:fd:c7:ef:d0:66:5c:aa:e3:2a:d9:71:12:e4:c6:
                    25:77:f0:1d:97:bb:92:a8:bd:66:f8:f8:e8:d5:0d:
                    d2:c8:01:dd:ea:e6:e0:80:ad:db:9d:c8:d9:5f:03:
                    2d:22:07:e3:ed:cc:88:1e:3f:0c:5e:b3:d8:0e:2d:
                    ea:d6:c6:47:23:6a:11:ef:3c:0f:6b:61:f0:ca:a1:
                    79:a0:b1:02:1a:ae:8c:c9:44:e0:cf:d1:30:de:4c:
                    f0:e5:62:e7:d0:81:5d:de:d3
```

```
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://xx.rsa.com:447/8088.crl

    Signature Algorithm: sha1WithRSAEncryption
        73:ac:66:f9:b8:b5:39:e1:6a:17:e4:d0:72:3e:26:9e:12:61:
        9e:c9:7a:86:6f:27:b0:b9:a3:5d:02:d9:5a:cb:79:0a:12:2e:
        cb:e7:24:57:e6:d9:77:12:6b:7a:cf:ee:d6:17:c5:5f:d2:98:
        30:e0:ef:00:39:4a:da:ff:1c:29:bb:2a:5b:60:e9:33:8f:78:
        f9:15:dc:a5:a3:09:66:32:ce:36:cd:f0:fe:2f:67:e5:72:e5:
        21:62:85:c4:07:92:c8:f1:d3:13:9c:2e:42:c1:5f:0e:8f:ff:
        65:fb:de:7c:ed:53:ab:14:7a:cf:69:f2:42:a4:44:7c:6e:90:
        7e:cd
```

可通过如下显示信息查看到 Device A 上 IKE 第二阶段协商生成的 IPsec SA。

```
[DeviceA] display ipsec sa
------------------------------
Interface: GigabitEthernet2/1/1
------------------------------

  ----------------------------
  IPsec policy: map1
  Sequence number: 10
  Mode: isakmp
  ----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect forward secrecy:
    Path MTU: 1456
    Tunnel:
        local  address: 1.1.1.1
        remote address: 2.2.2.2
    Flow:
    sour addr: 10.1.1.0/255.255.255.0  port: 0  protocol: ip
    dest addr: 10.1.2.0/255.255.255.0  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 3264152513 (0xc28f03c1)
      Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843200/3484
      Max received sequence-number:
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: active
```

```
[Outbound ESP SAs]
  SPI: 738451674 (0x2c03e0da)
  Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
  SA duration (kilobytes/sec): 1843200/3600
  SA remaining duration (kilobytes/sec): 1843200/3484
  Max received sequence-number:
  UDP encapsulation used for NAT traversal: N
  Status: active
```

Device B 上也会产生相应的 IKE SA 和 IPsec SA，并自动获取 CA 证书，自动申请本地证书，查看方式与 Device A 同，此处略。

2.14.3 IKE野蛮模式及NAT穿越典型配置举例

说明

设备运行于 FIPS 模式时，不支持本例。

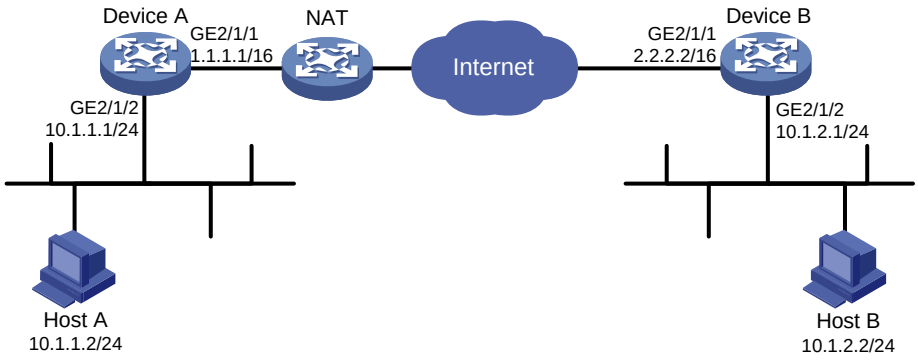
1. 组网需求

Device A 在 NAT 安全网关内网侧。要求在 Device A 和 Device B 之间建立一个 IPsec 隧道，对 Host A 所在的子网（10.1.1.0/24）与 Host B 所在的子网（10.1.2.0/24）之间的数据流进行安全保护。具体需要求如下：

- 协商双方使用缺省的 IKE 提议。
- 协商模式为野蛮模式协商。
- 第一阶段协商的认证方法为预共享密钥认证。

2. 组网图

图2-5 IKE 野蛮模式及 NAT 穿越典型组网图



3. 配置步骤

(1) 配置 Device A

配置各接口的 IP 地址，具体略。

配置 ACL 3000，定义要保护由子网 10.1.1.0/24 去往子网 10.1.2.0/24 的数据流。

```
<DeviceA> system-view
[DeviceA] acl number 3000
[DeviceA-acl-adv-3000] rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0
0.0.0.255
[DeviceA-acl-adv-3000] quit
```
创建 IPsec 安全提议 transform1。
```
[DeviceA] ipsec transform-set transform1
```
配置采用的安全协议为 ESP。
```
[DeviceA-ipsec-transform-set-transform1] protocol esp
```
配置 ESP 协议采用的加密算法为 3DES，认证算法为 HMAC-MD5。
```
[DeviceA-ipsec-transform-set-transform1] esp encryption-algorithm 3des-cbc
[DeviceA-ipsec-transform-set-transform1] esp authentication-algorithm md5
[DeviceA-ipsec-transform-set-transform1] quit
```
创建 IKE keychain，名称为 keychain1。
```
[DeviceA] ike keychain keychain1
```
配置与 IP 地址为 2.2.2.2 的对端使用的预共享密钥为明文 12345zxcvb!@#$%ZXCVB。
```
[DeviceA-ike-keychain-keychain1] pre-shared-key address 2.2.2.2 255.255.255.0 key simple
12345zxcvb!@#$%ZXCVB
[DeviceA-ike-keychain-keychain1] quit
```
创建 IKE profile，名称为 profile1。
```
[DeviceA] ike profile profile1
```
指定引用的 IKE keychain 为 keychain1。
```
[DeviceA-ike-profile-profile1] keychain keychain1
```
配置协商模式为野蛮模式。
```
[DeviceA-ike-profile-profile1] exchange-mode aggressive
```
配置本端身份为 FQDN 名称 www.devicea.com。
```
[DeviceA-ike-profile-profile1] local-identity fqdn www.devicea.com
```
配置匹配对端身份的规则为 IP 地址 2.2.2.2/24。
```
[DeviceA-ike-profile-profile1] match remote identity address 2.2.2.2 255.255.255.0
[DeviceA-ike-profile-profile1] quit
```
创建一条 IKE 协商方式的 IPsec 安全策略，名称为 policy1，顺序号为 1。
```
[DeviceA] ipsec policy policy1 1 isakmp
```
配置 IPsec 隧道的对端 IP 地址为 2.2.2.2。
```
[DeviceA-ipsec-policy-isakmp-policy1-1] remote-address 2.2.2.2
```
指定引用的安全提议为 transform1。
```
[DeviceA-ipsec-policy-isakmp-policy1-1] transform-set transform1
```
指定引用 ACL 3000。
```
[DeviceA-ipsec-policy-isakmp-policy1-1] security acl 3000
```
指定引用的 IKE profile 为 profile1。
```
[DeviceA-ipsec-policy-isakmp-policy1-1] ike-profile profile1
[DeviceA-ipsec-policy-isakmp-policy1-1] quit
```
在接口 GigabitEthernet2/1/1 上应用 IPsec 安全策略 policy1。
```
[DeviceA-GigabitEthernet2/1/1] ipsec apply policy policy1
[DeviceA-GigabitEthernet2/1/1] quit
```

配置到 Host B 所在子网的静态路由。

```
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 2.2.2.2
```

(2) 配置 Device B

配置各接口的 IP 地址，具体略。

创建 IPsec 安全提议 transform1。

```
<DeviceB> system-view
[DeviceB] ipsec transform-set transform1
```

配置采用的安全协议为 ESP。

```
[DeviceB-ipsec-transform-set-transform1] protocol esp
```

配置 ESP 协议采用的加密算法为 3DES，认证算法为 HMAC-MD5。

```
[DeviceB-ipsec-transform-set-transform1] esp encryption-algorithm 3des-cbc
[DeviceB-ipsec-transform-set-transform1] esp authentication-algorithm md5
[DeviceB-ipsec-transform-set-transform1] quit
```

创建 IKE keychain，名称为 keychain1。

```
[DeviceB]ike keychain keychain1
```

配置与 IP 地址为 1.1.1.1 的对端使用的预共享密钥为明文 12345zxcvb!@#$%ZXCVB。

```
[DeviceB-ike-keychain-keychain1] pre-shared-key address 1.1.1.1 255.255.255.0 key simple
12345zxcvb!@#$%ZXCVB
[DeviceB-ike-keychain-keychain1] quit
```

创建 IKE profile，名称为 profile1。

```
[DeviceB] ike profile profile1
```

指定引用的 IKE keychain 为 keychain1。

```
[DeviceB-ike-profile-profile1] keychain keychain1
```

配置协商模式为野蛮模式。

```
[DeviceB-ike-profile-profile1] exchange-mode aggressive
```

配置匹配对端身份的规则为 FQDN 名称 www.devicea.com。

```
[DeviceB-ike-profile-profile1] match remote identity fqdn www.devicea.com
[DeviceB-ike-profile-profile1] quit
```

创建一个 IKE 协商方式的 IPsec 安全策略模板，名称为 template1，顺序号为 1。

```
[DeviceB] ipsec policy-template template1 1
```

指定引用的安全提议为 tran1。

```
[DeviceB-ipsec-policy-template-template1-1] transform-set transform1
```

配置 IPsec 隧道的本端 IP 地址为 2.2.2.2。

```
[DeviceB-ipsec-policy-template-template1-1] local-address 2.2.2.2
```

指定引用的 IKE profile 为 profile1。

```
[DeviceB-ipsec-policy-template-template1-1] ike-profile profile1
[DeviceB-ipsec-policy-template-template1-1] quit
```

引用 IPsec 安全策略模板创建一条 IKE 协商方式的 IPsec 安全策略，名称为 policy1，顺序号为 1。

```
[DeviceB] ipsec policy policy1 1 isakmp template template1
```

在接口 GigabitEthernet2/1/1 上应用安全策略 policy1。

```
[DeviceB-GigabitEthernet2/1/1] ipsec apply policy policy1
[DeviceB-GigabitEthernet2/1/1] quit
```

4. 验证配置

以上配置完成后，子网 10.1.1.0/24 若向子网 10.1.2.0/24 发送报文，将触发 IKE 协商。

可通过如下显示信息查看到 Device A 上 IKE 第一阶段协商成功后生成的 IKE SA

```
[DeviceA] display ike sa
    Connection-ID   Remote                Flag         DOI
-------------------------------------------------------------------
    13              2.2.2.2               RD           IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
[DeviceA] display ike sa verbose
   ----------------------------------------------
   Connection ID: 13
   Outside VPN:
   Inside VPN:
   Profile: profile1
   Transmitting entity: Initiator
   ----------------------------------------------
   Local IP: 1.1.1.1
   Local ID type: FQDN
   Local ID: www.devicea.com

   Remote IP: 2.2.2.2
   Remote ID type: IPV4_ADDR
   Remote ID: 2.2.2.2

   Authentication-method: PRE-SHARED-KEY
   Authentication-algorithm: MD5
   Encryption-algorithm: 3DES-CBC

   Life duration(sec): 86400
   Remaining key duration(sec): 84565
   Exchange-mode: Aggressive
   Diffie-Hellman group: Group 1
   NAT traversal: Detected
```

可通过如下显示信息查看到 IKE 第二阶段协商生成的 IPsec SA。

```
[DeviceA] display ipsec sa
-------------------------------
Interface: GigabitEthernet2/1/1
-------------------------------

  -----------------------------
  IPsec policy: policy1
  Sequence number: 1
  Mode: isakmp
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
```

```
    Perfect forward secrecy:
    Path MTU: 1435
    Tunnel:
        local  address: 1.1.1.1
        remote address: 2.2.2.2
    Flow:
    sour addr: 10.1.1.0/255.255.255.0  port: 0  protocol: IP
    dest addr: 10.2.1.0/255.255.255.0  port: 0  protocol: IP

    [Inbound ESP SAs]
      SPI: 830667426 (0x3182faa2)
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843200/2313
      Max received sequence-number:
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for nat traversal: Y
      Status: active

    [Outbound ESP SAs]
      SPI: 3516214669 (0xd1952d8d)
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843200/2313
      Max received sequence-number:
      UDP encapsulation used for nat traversal: Y
      Status: active
```

2.15 常见错误配置举例

2.15.1 提议不匹配导致IKE SA协商失败

1. 故障现象

(1) 通过如下命令查看当前的 IKE SA 信息，发现 IKE SA 的状态（Flags 字段）为 Unknown。

```
<Sysname> display ike sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
    1               192.168.222.5         Unknown      IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
```

(2) 打开 IKE 事件和报文调试信息开关后分别可以看到如下调试信息。

IKE 事件调试信息：

```
The attributes are unacceptable.
```

IKE 报文调试信息：

```
Construct notification packet: NO_PROPOSAL_CHOSEN.
```

2. 故障分析

IKE 提议配置错误。

3. 处理过程

(1) 排查 IKE 提议相关配置。具体包括：检查两端的 IKE 提议是否匹配，即 IKE 提议中的认证方法、认证算法、加密算法是否匹配。

(2) 修改 IKE 提议的配置，使本端 IKE 提议的配置和对端匹配。

2.15.2 未正确引用IKE提议或IKE keychain导致IKE SA协商失败

1. 故障现象

(1) 通过如下命令查看当前的 IKE SA 信息，发现 IKE SA 的状态（Flags 字段）为 Unknown。

```
<Sysname> display ike sa
    Connection-ID   Remote                Flag         DOI
-------------------------------------------------------------------
    1               192.168.222.5         Unknown      IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
```

(2) 打开 IKE 事件和报文调试信息开关后分别可以看到如下调试信息。

IKE 事件调试信息：

```
Notification PAYLOAD_MALFORMED is received.
```

IKE 报文调试信息：

```
Construct notification packet: PAYLOAD_MALFORMED.
```

2. 故障分析

故障原因可能为以下两点：

(1) 匹配到的 IKE profile 中没有引用协商过程中匹配到的 IKE 提议。

通过调试信息看到：

```
Failed to find proposal 1 in profile profile1.
```

(2) 匹配到的 IKE profile 中没有引用协商过程中匹配到的 IKE keychain。

通过调试信息看到：

```
Failed to find keychain keychain1 in profile profile1.
```

3. 处理过程

(1) 检查匹配到的 IKE 提议是否在 IKE profile 下引用。以故障分析中的调试信息为例，IKE profile profile1 中需要引用 IKE proposal 1。

(2) 检查匹配到的 IKE keychain 是否在 IKE profile 下引用。以故障分析中的调试信息为例，IKE profile profile1 中需要引用 IKE keychain keychain1。

2.15.3 提议不匹配导致IPsec SA协商失败

1. 故障现象

(1) 通过 **display ike sa** 命令查看当前的 IKE SA 信息，发现 IKE SA 协商成功，其状态（Flags 字段）为 RD。但通过 **display ipsec sa** 命令查看当前的 IPsec SA 时，发现没有协商出相应的 IPsec SA。

(2) 打开 IKE 调试信息开关可以看到以下调试信息：

```
The attributes are unacceptable.
```

或者：

```
Construct notification packet: NO_PROPOSAL_CHOSEN.
```

2. 故障分析

IPsec 安全策略参数配置错误。

3. 处理过程

(1) 排查 IPsec 相关配置。具体包括：检查双方接口上应用的 IPsec 安全策略的参数是否匹配，即引用的 IPsec 安全提议的协议、加密算法和认证算法是否匹配。

(2) 修改 IPsec 安全策略配置，使本端 IPsec 安全策略的配置和对端匹配。

2.15.4 身份信息无效导致IPsec SA协商失败

1. 故障现象

(1) 通过 **display ike sa** 命令查看当前的 IKE SA 信息，发现 IKE SA 协商成功，其状态（Flags 字段）为 RD。但通过 **display ipsec sa** 命令查看当前的 IPsec SA 时，发现没有协商出相应的 IPsec SA。

(2) 打开 IKE 调试信息开关可以看到以下调试信息：

```
Notification INVALID_ID_INFORMATION is received.
```

或者：

```
Failed to get IPsec policy when renegotiating IPsec SA. Delete IPsec SA.
Construct notification packet: INVALID_ID_INFORMATION.
```

2. 故障分析

响应方 IPsec 安全策略配置错误，导致在 IKE 第二阶段协商时找不到 IPsec 安全策略，原因可能为如下几点：

(1) 通过 **display ike sa verbose** 命令查看 IKE 一阶段协商中是否找到匹配的 IKE profile。若没有找到 IKE profile，则会查找全局的 IKE 参数，因此就要求这种情况下 IPsec 安全策略中不能引用任何 IKE profile，否则协商失败。

通过如下显示信息可以看到，IKE SA 在协商过程中没有找到匹配的 IKE profile：

```
<Sysname> display ike sa verbose
   ----------------------------------------------
   Connection ID: 3
   Outside VPN:
   Inside VPN:
   Profile:
   Transmitting entity: Responder
```

```
  ---------------------------------------------
  Local IP: 192.168.222.5
  Local ID type: IPV4_ADDR
  Local ID: 192.168.222.5

  Remote IP: 192.168.222.71
  Remote ID type: IPV4_ADDR
  Remote ID: 192.168.222.71

  Authentication-method: PRE-SHARED-KEY
  Authentication-algorithm: MD5
  Encryption-algorithm: 3DES-CBC

  Life duration(sec): 86400
  Remaining key duration(sec): 85847
  Exchange-mode: Main
  Diffie-Hellman group: Group 1
  NAT traversal: Not detected
```

但在 IPsec 策略中引用了 IKE profile profile1：

```
[Sysname] display ipsec policy
-----------------------------------------
IPsec Policy: policy1
Interface: GigabitEthernet2/1/1
-----------------------------------------

  ----------------------------
  Sequence number: 1
  Mode: isakmp
  ----------------------------
  Description:
  Security data flow: 3000
  Selector mode: aggregation
  Local address: 192.168.222.5
  Remote address: 192.168.222.71
  Transform set:  transform1
  IKE profile: profile1
  SA duration(time based):
  SA duration(traffic based):
  SA idle time:
```

(2)　查看 IPsec 安全策略中引用的 ACL 配置是否正确。

例如，如发起方 ACL 流范围为网段到网段：

```
[Sysname] display acl 3000
Advanced ACL  3000, named -none-, 2 rules,
ACL's step is 5
 rule 0 permit ip source 192.168.222.0 0.0.0.255 destination 192.168.222.0 0.0.0.255
```

响应方 ACL 流范围为主机到主机：

```
[Sysname] display acl 3000
```

```
Advanced ACL  3000, named -none-, 2 rules,
ACL's step is 5
 rule 0 permit ip source 192.168.222.71 0 destination 192.168.222.5 0
```

以上配置中，响应方 ACL 规则定义的流范围小于发起方 ACL 规则定义的流范围，这会导致 IPsec SA 协商失败。

(3) IPsec 安全策略配置不完整。具体包括：没有配置对端地址、没有配置 IPsec 提议、IPsec 提议配置不完整。

例如，如下 IPsec 安全策略中没有配置隧道的对端 IP 地址，因此 IPsec 安全策略是不完整的：

```
[Sysname] display ipsec policy
-----------------------------------------
IPsec Policy: policy1
Interface: GigabitEthernet2/1/1
-----------------------------------------

  ----------------------------
  Sequence number: 1
  Mode: isakmp
  ----------------------------
  Description:
  Security data flow: 3000
  Selector mode: aggregation
  Local address: 192.168.222.5
  Remote address:
  Transform set:  transform1
  IKE profile: profile1
  SA duration(time based):
  SA duration(traffic based):
  SA idle time:
```

3. 处理过程

(1) 若在 IKE 第一阶段协商过程中没有找到 IKE profile，在响应方 IPsec 安全策略中去掉对 IKE profile 的引用。以故障分析（1）中的配置为例，需要去掉 IPsec 策略中对 IKE profile profile1 的引用。

(2) 若响应方 ACL 规则定义的流范围小于发起方 ACL 规则定义的流范围，建议修改响应方 ACL 的流范围大于或等于发起方 ACL 的流范围。以故障分析（2）中的配置为例，可以将响应方 ACL 流范围修改为：

```
[Sysname] display acl 3000
Advanced ACL  3000, named -none-, 2 rules,
ACL's step is 5
 rule 0 permit ip source 192.168.222.0 0.0.0.255 destination 192.168.222.0 0.0.0.255
```

(3) 将 IPsec 安全策略配置完整。以故障分析中的（3）中的配置为例，需要在 IPsec 安全策略中配置隧道的对端 IP 地址。

目 录

1 SSH

说明

- 设备运行于 FIPS 模式时，本特性的相关配置相对于非 FIPS 模式有所变化，具体差异请见本文相关描述。有关 FIPS 模式的详细介绍请参见“安全配置指导”中的“FIPS”。

1.1 SSH简介

SSH 是 Secure Shell（安全外壳）的简称，是一种在不安全的网络环境中，通过加密机制和认证机制，实现安全的远程访问以及文件传输等业务的网络安全协议。

SSH 协议采用了典型的客户端/服务器模式，并基于 TCP 协议协商建立用于保护数据传输的会话通道。SSH 协议有两个版本，SSH1.x 和 SSH2.0（本文简称 SSH1 和 SSH2），两者互不兼容。SSH2 在性能和安全性方面比 SSH1 有所提高。

设备既可以支持 SSH 服务器功能，接受多个 SSH 客户端的连接，也可以支持 SSH 客户端功能，允许用户通过设备与远程 SSH 服务器建立 SSH 连接。

目前，设备支持三种 SSH 应用：Stelnet、SFTP 和 SCP。

- Stelnet 是 Secure Telnet 的简称，可提供安全可靠的网络终端访问服务，使得用户可以安全登录到远程设备，且能保护远程设备不受诸如 IP 地址欺诈、明文密码截取等攻击。设备可支持 Stelnet 服务器、Stelnet 客户端功能。
- SFTP 是 Secure FTP 的简称，基于 SSH2，可提供安全可靠的网络文件传输服务，使得用户可以安全登录到远程设备上进行文件管理操作，且能保证文件传输的安全性。设备可支持 SFTP 服务器、SFTP 客户端功能。
- SCP 是 Secure Copy 的简称，基于 SSH2，可提供安全的文件复制功能。设备可支持 SCP 服务器、SCP 客户端功能。

目前，设备作为 SSH 服务器时，非 FIPS 模式下支持 SSH2 和 SSH1 两个版本，FIPS 模式下只支持 SSH2 版本；设备作为 SSH 客户端时，只支持 SSH2 版本。

1.1.1 SSH工作过程

本小节以SSH2 为例介绍SSH工作的过程，具体分为 表 1-1 所述的几个阶段，关于各阶段的详细介绍，请参见“SSH技术白皮书”。

表1-1 SSH 工作过程

阶段	说明
连接建立	SSH服务器在22号端口侦听客户端的连接请求，在客户端向服务器端发起连接请求后，双方建立一个TCP连接
版本协商	双方通过版本协商确定最终使用的SSH版本号

阶段	说明
算法协商	SSH支持多种算法，双方根据本端和对端支持的算法，协商出最终用于产生会话密钥的密钥交换算法、用于数据信息加密的加密算法、用于进行数字签名和认证的公钥算法，以及用于数据完整性保护的HMAC算法
密钥交换	双方通过DH（Diffie-Hellman Exchange）交换，动态地生成用于保护数据传输的会话密钥和用来标识该SSH连接的会话ID，并完成客户端对服务器端的身份认证
用户认证	SSH客户端向服务器端发起认证请求，服务器端对客户端进行认证
会话请求	认证通过后，SSH客户端向服务器端发送会话请求，请求服务器提供某种类型的服务（目前支持Stelnet、SFTP或SCP），即请求与服务器建立相应的会话
会话交互	会话建立后，SSH服务器端和客户端在该会话上进行数据信息的交互 该阶段，用户在客户端可以通过粘贴文本内容的方式执行命令，但文本会话不能超过2000字节，且粘贴的命令最好是同一视图下的命令，否则服务器可能无法正确执行该命令。如果粘贴的文本会话超过2000字节，可以采用将配置文件通过SFTP方式上传到服务器，利用新的配置文件重新启动的方式执行这些命令

1.1.2 SSH认证方式

设备作为 SSH 服务器可提供以下四种对客户端的认证方式：

- password 认证：利用 AAA（Authentication、Authorization、Accounting，认证、授权和计费）对客户端身份进行认证。客户端向服务器发出 password 认证请求，将用户名和密码加密后发送给服务器；服务器将认证请求解密后得到用户名和密码的明文，通过本地认证或远程认证验证用户名和密码的合法性，并返回认证成功或失败的消息。
- publickey 认证：采用数字签名的方式来认证客户端。目前，设备上可以利用 DSA 和 RSA 两种公钥算法实现数字签名。客户端发送包含用户名、公钥和公钥算法或者携带公钥信息的数字证书的 publickey 认证请求给服务器端。服务器对公钥进行合法性检查，如果不合法，则直接发送失败消息；否则，服务器利用数字签名对客户端进行认证，并返回认证成功或失败的消息。
- password-publickey 认证：对于 SSH2 版本的客户端，要求同时进行 password 和 publickey 两种方式的认证，且只有两种认证均通过的情况下，才认为客户端身份认证通过；对于 SSH1 版本的客户端，只要通过其中任意一种认证即可。
- any 认证：不指定客户端的认证方式，客户端可采用 password 认证或 publickey 认证，且只要通过其中任何一种认证即可。

关于 AAA 以及公钥相关内容的介绍请分别参考“安全配置指导”中的“AAA”和“公钥管理”。

说明

- 客户端进行 password 认证时，如果远程认证服务器要求用户进行二次密码认证，则会在发送给服务器端的认证回应消息中携带一个提示信息，该提示信息被服务器端透传给客户端，由客户端输出并要求用户再次输入一个指定类型的密码，当用户提交正确的密码并成功通过认证服务器的验证后，服务器端才会返回认证成功的消息。
- SSH1 版本的 SSH 客户端不支持 AAA 服务器发起的二次密码认证。

1.2 配置SSH服务器

1.2.1 SSH服务器配置任务简介

通过执行以下配置任务，可配置设备作为 Stelnet、SFTP 或 SCP 服务器。由于 Stelnet、SFTP 和 SCP 服务器的配置基本相同，因此除非特殊说明，本小节中使用 SSH 服务器作为 Stelnet、SFTP 和 SCP 服务器的统称。

表1-2 SSH 服务器配置任务简介

配置任务	说明	详细配置
生成本地DSA或RSA密钥对	必选	1.2.2
使能SSH服务器功能	仅对于Stelnet和SCP服务器必选	1.2.3
使能SFTP服务器功能	仅对于SFTP服务器必选	1.2.4
配置SSH客户端登录时使用的用户线	必选	1.2.5
配置客户端的公钥	采用publickey、password-publickey或any认证方式时必选	1.2.6
配置认证客户端证书的PKI域	采用publickey认证方式且客户端使用证书认证时必选 该PKI域中必须保存了用于认证客户端证书的CA证书	请参见“安全配置指导”中的“PKI配置”
配置SSH用户	采用publickey、password-publickey或any认证方式时必选 采用password认证方式时可选	1.2.7
配置SSH管理功能	可选	1.2.8

1.2.2 生成本地DSA或RSA密钥对

说明

设备运行于 FIPS 模式时，服务器端仅支持 RSA 密钥对，因此请不要生成本地的 DSA 密钥对，否则会导致用户认证失败。

服务器端的 DSA 或 RSA 密钥对有两个用途，其一是用于在密钥交换阶段生成会话密钥和会话 ID，另外一个是客户端用它来对连接的服务器进行认证。客户端验证服务器身份时，首先判断服务器发送的公钥与本地保存的服务器公钥是否一致，确认服务器公钥正确后，再使用该公钥对服务器发送的数字签名进行验证。

虽然一个客户端只会采用 DSA 和 RSA 公钥算法中的一种来认证服务器，但是由于不同客户端支持的公钥算法不同，为了确保客户端能够成功登录服务器，建议在服务器上同时生成 DSA 和 RSA 两种密钥对。

- 生成 RSA 密钥对时，将同时生成两个密钥对——服务器密钥对和主机密钥对。SSH1 利用 SSH 服务器端的服务器公钥加密会话密钥，以保证会话密钥传输的安全；SSH2 通过 DH 算法在

SSH 服务器和 SSH 客户端上生成会话密钥，不需要传输会话密钥，因此 SSH2 中没有利用服务器密钥对。

- 生成 DSA 密钥对时，只生成一个主机密钥对。SSH1 不支持 DSA 算法。

服务器端生成本地 DSA 或 RSA 密钥对，需要注意的是：

- SSH 仅支持默认名称的本地 DSA 或 RSA 密钥对，不支持指定名称的本地 DSA 或 RSA 密钥对。关于密钥对生成命令的相关介绍请参见“安全命令参考”中的“公钥管理”。
- 生成 DSA 密钥对时，要求输入的密钥模数的长度必须小于 2048 比特。

表1-3 生成本地 DSA 或 RSA 密钥对

操作	命令	说明
进入系统视图	**system-view**	-
生成本地DSA或RSA密钥对	**public-key local create** { **dsa** | **rsa** }	缺省情况下，不存在任何DSA和RSA密钥对

1.2.3 使能SSH服务器功能

该配置任务用于使能设备上的 SSH 服务器功能，使客户端能采用 SSH 协议与设备进行通信。

设备作为 SSH 服务器时，不支持 SSH1 版本的客户端发起的 SFTP 连接或 SCP 连接。

表1-4 使能 SSH 服务器功能

操作	命令	说明
进入系统视图	**system-view**	-
使能SSH服务器功能	**ssh server enable**	缺省情况下，SSH服务器功能处于关闭状态

1.2.4 使能SFTP服务器功能

该配置任务用于使能设备上的 SFTP 服务器功能，使客户端能采用 SFTP 的方式登录到设备。

表1-5 启动 SFTP 服务器功能

操作	命令	说明
进入系统视图	**system-view**	-
使能SFTP服务器功能	**sftp server enable**	缺省情况下，SFTP服务器处于关闭状态

1.2.5 配置SSH客户端登录时使用的用户线

设备支持的 SSH 客户端根据不同的应用可分为：Stelnet 客户端、SFTP 客户端和 SCP 客户端。

- Stelnet 客户端通过 VTY（Virtual Type Terminal，虚拟类型终端）用户线访问设备。因此，需要配置 Stelnet 客户端登录时采用的 VTY 用户线，使其支持 Stelnet 远程登录协议。配置将在客户端下次登录时生效。

- SFTP 客户端和 SCP 客户端不通过用户线访问设备，不需要配置登录时采用的 VTY 用户线。

表1-6 配置 Stelnet 客户端登录时使用的用户线

操作	命令	说明
进入系统视图	**system-view**	-
进入VTY用户线视图	**line vty** *number* [*ending-number*]	-
配置登录用户线的认证方式为**scheme**方式	**authentication-mode scheme**	缺省情况下，用户线认证为**password**方式 该命令的详细介绍，请参见“基础配置命令参考”中的“登录设备”

1.2.6 配置客户端的公钥

服务器在采用 publickey 方式验证客户端身份时，首先比较客户端发送的 SSH 用户名、主机公钥是否与本地配置的 SSH 用户名以及相应的客户端主机公钥一致，在确认用户名和客户端主机公钥正确后，对客户端发送的数字签名进行验证，该签名是客户端利用主机公钥对应的私钥计算出的。因此，在采用 publickey、password-publickey 或 any 认证方式时，需要在服务器端配置客户端的 DSA 或 RSA 主机公钥，并在客户端为该 SSH 用户指定与主机公钥对应的 DSA 或 RSA 主机私钥（若设备作为客户端，则在向服务器发起连接时通过指定公钥算法来实现）。

服务器端可以通过手工配置和从公钥文件中导入两种方式来配置客户端的公钥：

- 手工配置：事先在客户端上通过显示命令或其它方式查看其公钥信息，并记录客户端主机公钥的内容，然后采用手工输入的方式将客户端的公钥配置到服务器上。手工输入远端主机公钥时，可以逐个字符输入，也可以一次拷贝粘贴多个字符。这种方式要求手工输入或拷贝粘贴的主机公钥必须是未经转换的 DER（Distinguished Encoding Rules，特异编码规则）公钥编码格式。
- 从公钥文件中导入：事先将客户端的公钥文件保存到服务器上（例如，通过 FTP 或 TFTP，以二进制方式将客户端的公钥文件保存到服务器），服务器从本地保存的该公钥文件中导入客户端的公钥。导入公钥时，系统会自动将客户端公钥文件转换为 PKCS（Public Key Cryptography Standards，公共密钥加密标准）编码形式。

手工配置客户端的公钥时，输入的主机公钥必须满足一定的格式要求。通过 **display public-key local public** 命令显示的公钥可以作为输入的公钥内容；通过其他方式（如 **public-key local export** 命令）显示的公钥可能不满足格式要求，导致主机公钥保存失败。因此，建议选用从公钥文件导入的方式配置远端主机的公钥。

SSH 服务器上配置的 SSH 客户端公钥数目建议不要超过 20 个。

表1-7 手工配置客户端的公钥

操作	命令	说明
进入系统视图	**system-view**	-
进入公钥视图	**public-key peer** *keyname*	-

操作	命令	说明
配置客户端的公钥	逐个字符输入或拷贝粘贴公钥内容	在输入公钥内容时，字符之间可以有空格，也可以按回车键继续输入数据，保存公钥数据时，将删除空格和回车符 具体介绍请参见“安全配置指导”中的“公钥管理”
退回系统视图	**peer-public-key end**	-

表1-8 从公钥文件中导入客户端的公钥

操作	命令	说明
进入系统视图	**system-view**	-
从公钥文件中导入远端客户端的公钥	**public-key peer** *keyname* **import sshkey** *filename*	-

1.2.7 配置SSH用户

本配置用于创建 SSH 用户，并指定 SSH 用户的服务类型、认证方式以及对应的客户端公钥或数字证书。SSH 用户的配置与服务器端采用的认证方式有关，具体如下：

- 如果服务器采用了 publickey 认证，则必须在设备上创建相应的 SSH 用户，以及同名的本地用户（用于下发授权属性：工作目录、用户角色）。
- 如果服务器采用了 password 认证，则必须在设备上创建相应的本地用户（适用于本地认证），或在远程服务器（如 RADIUS 服务器，适用于远程认证）上创建相应的 SSH 用户。这种情况下，并不需要通过本配置创建相应的 SSH 用户，如果创建了 SSH 用户，则必须保证指定了正确的服务类型以及认证方式。
- 如果服务器采用了 password-publickey 或 any 认证，则必须在设备上创建相应的 SSH 用户，以及在设备上创建同名的本地用户（适用于本地认证）或者在远程认证服务器上创建同名的 SSH 用户（如 RADIUS 服务器，适用于远程认证）。

配置 SSH 用户时，需要注意：

- SCP 或 SFTP 用户登录时使用的工作目录与用户使用的认证方式有关。通过 publickey 或 password-publickey 认证登录服务器的用户使用的工作目录均为对应的本地用户视图下为该用户设置的工作目录；通过 password 认证登录服务器的用户，使用的工作目录为通过 AAA 授权的工作目录。
- 通过 publickey 或 password-publickey 认证登录服务器的 SSH 用户将被授予对应的本地用户视图下指定的用户角色；通过 password 认证登录服务器的 SSH 用户将被授予远程 AAA 服务器或设备本地授权的用户角色。
- 对 SSH 用户配置的修改，不会影响已经登录的 SSH 用户，仅对新登录的用户生效。
- 除 password 认证方式外，其它认证方式下均需要指定客户端的公钥或证书。
  - 对于使用公钥认证的SSH用户，服务器端必须指定客户端的公钥，且指定的公钥必须已经存在，公钥内容的配置请参见“1.2.6 配置客户端的公钥”。

- 对于使用证书认证的 SSH 用户，服务器端必须指定用于验证客户端证书的 PKI 域，PKI 域的配置请参见“安全配置指导”中的“PKI 域配置”。为保证 SSH 用户可以成功通过认证，通过 **ssh user** 命令指定的 PKI 域中必须存在用于验证客户端证书的 CA 证书。

- FIPS 模式下，设备作为 SSH 服务器不支持 any 认证和 publickey 认证方式。

关于本地用户以及远程认证的相关配置请参见“安全配置指导”中的“AAA”。

表1-9 配置 SSH 用户

操作	命令	说明
进入系统视图	**system-view**	-
创建SSH用户，并指定SSH用户的服务类型和认证方式	非FIPS模式下： **ssh user** *username* **service-type** { **all** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign** { **pki-domain** *domain-name* | **publickey** *keyname* } } FIPS模式下： **ssh user** *username* **service-type** { **all** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | **password-publickey assign** { **pki-domain** *domain-name* | **publickey** *keyname* } }	SSH服务器上最多可以创建1024个SSH用户

1.2.8 配置SSH管理功能

通过配置服务器上的 SSH 管理功能，可提高 SSH 连接的安全性。SSH 的管理功能包括：

- 设置 SSH 服务器是否兼容 SSH1 版本的客户端。
- 设置 RSA 服务器密钥对的更新时间，此配置仅对 SSH 客户端版本为 SSH1 的用户有效，SSH 的核心是密钥的协商和传输，因此密钥的管理是非常重要的，可灵活设置更新时间间隔。
- 设置 SSH 用户认证的超时时间。为了防止不法用户建立起 TCP 连接后，不进行接下来的认证，而是空占着进程，妨碍其它合法用户的正常登录，可以设置验证超时时间，如果在规定的时间内没有完成认证就拒绝该连接。
- 设置 SSH 用户请求连接的认证尝试最大次数，限制登录的重试次数，防止非法用户对用户名和密码进行恶意地猜测和破解。在 any 认证方式下，SSH 客户端通过 publickey 和 password 两种方式进行认证尝试的次数总和，不能超过配置的 SSH 连接认证尝试次数。
- 设置对 SSH 客户端的访问控制，使用 ACL 过滤向 SSH 服务器发起连接的 SSH 客户端。
- 设置 SSH 服务器向 SSH 客户端发送的报文的 DSCP 优先级。DSCP 携带在 IPv4 报文中的 ToS 字段和 IPv6 报文中的 Trafic class 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。
- 设置 SFTP 用户连接的空闲超时时间。当 SFTP 用户连接的空闲时间超过设定的阈值后，系统会自动断开此用户的连接，从而有效避免用户长期占用连接而不进行任何操作。
- 设置同时在线的最大 SSH 用户连接数。系统资源有限，当前在线 SSH 用户数超过设定的最大值时，系统会拒绝新的 SSH 连接请求。

表1-10 配置 SSH 管理功能

操作	命令	说明
进入系统视图	**system-view**	-
设置SSH服务器兼容SSH1版本的客户端	**ssh server compatible-ssh1x enable**	缺省情况下，SSH服务器兼容SSH1版本的客户端 FIPS模式下，不支持本命令
设置RSA服务器密钥对的更新时间	**ssh server rekey-interval** *hours*	缺省情况下，系统不更新RSA服务器密钥对 FIPS模式下，不支持本命令
设置SSH用户的认证超时时间	**ssh server authentication-timeout** *time-out-value*	缺省情况下，SSH用户的认证超时时间为60秒
设置SSH认证尝试的最大次数	**ssh server authentication-retries** *times*	缺省情况下，SSH连接认证尝试的最大次数为3次
设置对IPv4 SSH用户的访问控制	**ssh server acl** *acl-number*	缺省情况下，允许所有IPv4 SSH用户向设备发起SSH访问
设置对IPv6 SSH用户的访问控制	**ssh server ipv6 acl** [**ipv6**] *acl-number*	缺省情况下，允许所有IPv6 SSH用户向设备发起SSH访问
设置Pv4 SSH服务器向SSH客户端发送的报文的DSCP优先级	**ssh server dscp** *dscp-value*	缺省情况下，IPv4 SSH报文的DSCP优先级为48
设置IPv6 SSH服务器向SSH客户端发送的报文的DSCP优先级	**ssh server ipv6 dscp** *dscp-value*	缺省情况下，IPv6 SSH报文的DSCP优先级为48
设置SFTP用户连接的空闲超时时间	**sftp server idle-timeout** *time-out-value*	缺省情况下，SFTP用户连接的空闲超时时间为10分钟
设置同时在线的最大SSH用户连接数	**aaa session-limit ssh** *max-sessions*	缺省的最大SSH用户连接数为16 该值的修改不会对已经在线的用户连接造成影响，只会对新的用户连接生效 关于该命令的详细介绍，请参见“安全命令参考”中的“AAA”

1.3 配置Stelnet客户端

1.3.1 Stelnet客户端配置任务简介

表1-11 Stelnet 客户端配置任务简介

配置任务	说明	详细配置
为Stelnet客户端指定源IP地址或源接口	可选	1.3.2
建立与Stelnet服务器端的连接	必选	1.3.3

1.3.2 为Stelnet客户端指定源IP地址或源接口

Stelnet 客户端与 Stelnet 服务器通信时，缺省采用路由决定的源 IP 地址作为发送报文的源地址。如果使用本配置指定了源 IP 地址或源接口，则采用该地址与服务器进行通信。为保证 Stelnet 客户端与 Stelnet 服务器通信链路的可达性，以及增加认证业务对 SFTP 客户端的可管理性，通常建议指定 Loopback 接口或 Dialer 接口作为源接口。

表1-12 为 Stelnet 客户端指定源 IP 地址或源接口

操作		命令	说明
进入系统视图		**system-view**	-
为Stelnet客户端指定源IP地址或源接口	为Stelnet客户端指定源IPv4地址或源接口	**ssh client source** { **interface** *interface-type interface-number* | **ip** *ip-address* }	二者必选其一 缺省情况下，客户端用设备路由指定的接口地址访问Stelnet服务器
	为Stelnet客户端指定源IPv6地址或源接口	**ssh client ipv6 source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }	

1.3.3 建立与Stelnet服务器的连接

该配置任务用来启动 Stelnet 客户端程序，与远程 Stelnet 服务器建立连接，并指定公钥算法、首选加密算法、首选 HMAC 算法和首选密钥交换算法等。

Stelnet 客户端访问服务器时，需要通过本地保存的服务器端的主机公钥来验证服务器的身份。设备作为 Stelnet 客户端时，默认支持首次认证，即当 Stelnet 客户端首次访问服务器，而客户端没有配置服务器端的主机公钥时，用户可以选择继续访问该服务器，并在客户端保存该主机公钥；当用户下次访问该服务器时，就以保存的主机公钥来认证该服务器。首次认证在比较安全的网络环境中可以简化客户端的配置，但由于该方式下客户端完全相信服务器公钥的正确性，因此存在一定的安全隐患。

表1-13 建立与 Stelnet 服务器的连接

操作		命令	说明
与Stelnet服务器端建立连接	与IPv4 Stelnet服务器端建立连接	非FIPS模式下： **ssh2** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des** | **aes128 | aes256** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128 | aes256** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **publickey** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] * FIPS模式下： **ssh2** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key rsa** | **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128 | aes256** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** } | **prefer-kex dh-group14** | **prefer-stoc-cipher** { **aes128 | aes256** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** }] * [**publickey** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *	二者至少选其一 请在用户视图下执行本命令

操作		命令	说明
	与IPv6 Stelnet服务器端建立连接	非FIPS模式下： **ssh2 ipv6** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des** | **aes128 | aes256** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128 | aes256** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **publickey** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] * FIPS模式下： **ssh2 ipv6** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key rsa** | **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128 | aes256** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** } | **prefer-kex dh-group14** | **prefer-stoc-cipher** { **aes128 | aes256** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** }] * [**publickey** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *	

1.4 配置SFTP客户端

1.4.1 SFTP客户端配置任务简介

表1-14 SFTP 客户端配置任务简介

配置任务	说明	详细配置
为SFTP客户端指定源IP地址或源接口	可选	1.4.2
建立与SFTP服务器端的连接	必选	1.4.3
SFTP目录操作	可选	1.4.4
SFTP文件操作	可选	1.4.5
显示帮助信息	可选	1.4.6
终止与SFTP服务器端的连接	可选	1.4.7

1.4.2 为SFTP客户端指定源IP地址或源接口

SFTP 客户端与 SFTP 服务器通信时，缺省采用路由决定的源 IP 地址作为发送报文的源地址。如果使用本配置指定了源 IP 地址或源接口，则采用该地址与服务器进行通信。为保证 SFTP 客户端与 SFTP 服务器通信链路的可达性，以及增加认证业务对 SFTP 客户端的可管理性，通常建议指定 Loopback 接口或 Dialer 接口作为源接口。

表1-15 为 SFTP 客户端指定 IP 地址或源接口

操作		命令	说明
进入系统视图		**system-view**	-
为SFTP客户端指定源IP地址或源接口	为SFTP客户端指定源IPv4地址或源接口	**sftp client source** { **ip** *ip-address* | **interface** *interface-type interface-number* }	二者必选其一 缺省情况下，客户端用设备路由指定的接口地址访问SFTP服务器
	为SFTP客户端指定源IPv6地址或源接口	**sftp client ipv6 source** { **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }	

1.4.3 建立与SFTP服务器的连接

该配置任务用来启动 SFTP 客户端程序，与远程 SFTP 服务器建立连接，并指定公钥算法、首选加密算法、首选 HMAC 算法和首选密钥交换算法等。SFTP 客户端与服务器成功建立连接之后，用户即可进入到服务器端上的 SFTP 客户端视图下进行目录、文件等操作。

SFTP 客户端访问服务器时，需要通过本地保存的服务器端的主机公钥来验证服务器的身份。设备作为 SFTP 客户端时，默认支持首次认证，即当 SFTP 客户端首次访问服务器，而客户端没有配置服务器端的主机公钥时，用户可以选择继续访问该服务器，并在客户端保存该主机公钥；当用户下次访问该服务器时，就以保存的主机公钥来认证该服务器。首次认证在比较安全的网络环境中可以简化客户端的配置，但由于该方式下客户端完全相信服务器公钥的正确性，因此存在一定的安全隐患。

表1-16 建立与 SFTP 服务器端的连接

操作		命令	说明
与SFTP服务器建立连接，并进入SFTP客户端视图	与IPv4 SFTP服务器建立连接，并进入SFTP客户端视图	非FIPS模式下： **sftp** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des** | **aes128 | aes256** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128 | aes256** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **publickey** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-addres*}] * FIPS模式下： **sftp** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**identity-key rsa** | **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128 | aes256** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** } | **prefer-kex dh-group14** | **prefer-stoc-cipher** { **aes128 | aes256** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** }] * [**publickey** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *	二者至少选其一 请在用户视图下执行此命令
	与IPv6 SFTP服务器建立连接，并进入SFTP客户端视图	非FIPS模式下： **sftp ipv6** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des** | **aes128 | aes256** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128 | aes256** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **publickey** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-addres*}] * FIPS模式下： **sftp ipv6** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key rsa**| **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128 | aes256** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** } | **prefer-kex dh-group14** | **prefer-stoc-cipher** { **aes128 | aes256** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** }] * [**publickey** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-addres*}] *	

1.4.4 SFTP目录操作

SFTP 目录操作包括：改变或显示当前的工作路径、显示指定目录下的文件或目录信息、改变服务器上指定的文件夹的名字、创建或删除目录等操作。

表1-17 SFTP 目录操作

操作	命令	说明
进入SFTP客户端视图	具体命令请参考1.4.3	-
改变远程SFTP服务器上的工作路径	**cd** [*remote-path*]	-
返回到上一级目录	**cdup**	-
显示远程SFTP服务器上的当前工作目录	**pwd**	-
显示指定目录下的文件列表	**dir** [**-a** | **-l**] [*remote-path*]	**dir**和**ls**两条命令的作用相同
	ls [**-a** | **-l**] [*remote-path*]	
改变SFTP服务器上指定的目录的名字	**rename** *old-name new-name*	-
在远程SFTP服务器上创建新的目录	**mkdir** *remote-path*	-
删除SFTP服务器上指定的目录	**rmdir** *remote-path*	-

1.4.5 SFTP文件操作

SFTP 文件操作包括：改变文件名、下载文件、上传文件、显示文件列表和删除文件。

表1-18 SFTP 文件操作

操作	命令	说明
进入SFTP客户端视图	具体命令请参考1.4.3	-
改变SFTP服务器上指定的文件的名字	**rename** *old-name new-name*	-
从远程服务器上下载文件并存储在本地	**get** *remote-file* [*local-file*]	-
将本地的文件上传到远程SFTP服务器	**put** *local-file* [*remote-file*]	-
显示指定目录下的文件	**dir** [**-a** | **-l**] [*remote-path*]	**dir**和**ls**两条命令的作用相同
	ls [**-a** | **-l**] [*remote-path*]	
删除SFTP服务器上指定的文件	**delete** *remote-file*	**delete**和**remove**两条命令的功能相同
	remove *remote-file*	

1.4.6 显示帮助信息

本配置用于显示命令的帮助信息，如命令格式、参数配置等。

表1-19 显示客户端命令的帮助信息

操作	命令	说明
进入SFTP客户端视图	具体命令请参考1.4.3	-

操作	命令	说明
显示SFTP客户端命令的帮助信息	**help**	二者选其一 **help**和？的功能相同
	？	

1.4.7 终止与SFTP服务器的连接

表1-20 终止与 SFTP 服务器的连接

操作	命令	说明
进入SFTP客户端视图	具体命令请参考1.4.3	-
终止与SFTP服务器的连接，并退回用户视图	**bye**	三者选其一 **bye**，**exit**和**quit**三条命令的功能相同
	exit	
	quit	

1.5 配置SCP客户端

1.5.1 与远程SCP服务器传输文件

该配置任务用来启动 SCP 客户端程序，与远程 SCP 服务器建立连接，并进行安全的文件传输操作。SCP 客户端访问服务器时，需要通过本地保存的服务器端的主机公钥来验证服务器的身份。设备作为 SCP 客户端时，默认支持首次认证，即当 SCP 客户端首次访问服务器，而客户端没有配置服务器端的主机公钥时，用户可以选择继续访问该服务器，并在客户端保存该主机公钥；当用户下次访问该服务器时，就以保存的主机公钥来认证该服务器。首次认证在比较安全的网络环境中可以简化客户端的配置，但由于该方式下客户端完全相信服务器公钥的正确性，因此存在一定的安全隐患。

表1-21 与远程 SCP 服务器传输文件

操作		命令	说明
与远程SCP服务器建立连接，并进行文件传输	与远程IPv4 SCP服务器建立连接，并进行文件传输	非FIPS模式下： **scp** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des** | **aes128 | aes256** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128 | aes256** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**publickey** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] * FIPS模式下： **scp** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key rsa** | **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128 | aes256** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** } | **prefer-kex dh-group14** | **prefer-stoc-cipher** { **aes128 | aes256** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** }] * [**publickey** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *	二者至少选其一 请在用户视图下执行此命令
	与远程IPv6 SCP服务器建立连接，并进行文件传输	非FIPS模式下： **scp ipv6** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des** | **aes128 | aes256** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128 | aes256** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**publickey** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] * FIPS模式下： **scp ipv6** *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] [**identity-key rsa** | **prefer-compress zlib** | **prefer-ctos-cipher** { **aes128 | aes256** } | **prefer-ctos-hmac** { **sha1** | **sha1-96** } | **prefer-kex dh-group14** | **prefer-stoc-cipher** { **aes128 | aes256** } | **prefer-stoc-hmac** { **sha1** | **sha1-96** }] * [**publickey** *keyname* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *	

1.6 SSH显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令，可以显示配置后 SSH 的运行情况，通过查看显示信息验证配置的效果。

表1-22 SSH 显示和维护

操作	命令
显示当前为SFTP客户端设置的源IP地址或者源接口	**display sftp client source**
显示当前为Stelnet客户端设置的源IP地址或者源接口	**display ssh client source**
在SSH服务器端显示该服务器的状态信息或会话信息	**display ssh server** { **session** | **status** }
在SSH服务器端显示SSH用户信息	**display ssh user-information** [*username*]
显示本地密钥对中的公钥部分	**display public-key local** { **dsa** | **rsa** } **public** [**name** *publickey-name*]
显示保存在本地的远端主机的公钥信息	**display public-key peer** [**brief** | **name** *publickey-name*]

说明

display public-key local 和 **display public-key peer** 命令的详细介绍请参见“安全命令参考”中的“公钥管理”。

1.7 Stelnet典型配置举例

说明

举例中的设备运行于非 FIPS 模式下。若设备运行于 FIPS 模式下，支持的密钥对的模数只能为 2048 比特，因此相关的配置和显示信息也有所变化，请以设备的实际情况为准；设备作为服务器仅支持 RSA 密钥对，请不要生成 DSA 密钥对。

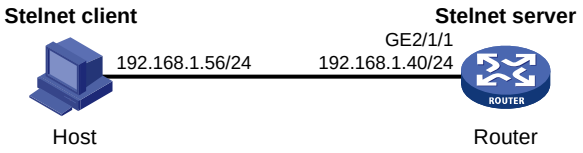
1.7.1 设备作为Stelnet服务器配置举例（password认证）

1. 组网需求

- 用户可以通过 Host 上运行的 Stelnet 客户端软件（SSH2 版本）安全地登录到 Router 上，并被授予用户角色 network-admin 进行配置管理；
- Router 采用 password 认证方式对 Stelnet 客户端进行认证，客户端的用户名和密码保存在本地。

2. 组网图

图1-1 设备作为 Stelnet 服务器配置组网图



3. 配置步骤

(1) 配置 Stelnet 服务器

生成 RSA 密钥对。

```
<Router> system-view
[Router] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[Router] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.................................+
...+................+.........+...+.
Create the key pair successfully.
```

使能 SSH 服务器功能。

```
[Router] ssh server enable
```

配置接口 GigabitEthernet2/1/1 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。

```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] ip address 192.168.1.40 255.255.255.0
[Router-GigabitEthernet2/1/1] quit
```

设置 Stelnet 客户端登录用户线的认证方式为 AAA 认证。

```
[Router] line vty 0 63
[Router-line-vty0-63] authentication-mode scheme
[Router-line-vty0-63] quit
```

创建设备管理类本地用户 client001，并设置密码为明文 aabbcc，服务类型为 SSH，用户角色为 network-admin。

```
[Router] local-user client001 class manage
[Router-luser-manage-client001] password simple aabbcc
[Router-luser-manage-client001] service-type ssh
[Router-luser-manage-client001] authorization-attribute user-role network-admin
[Router-luser-manage-client001] quit
```

配置 SSH 用户 client001 的服务器类型为 Stelnet，认证方式为 password 认证。（此步骤可以不配置）

```
[Router] ssh user client001 service-type stelnet authentication-type password
```

(2) Stelnet 客户端建立与 Stelnet 服务器的连接

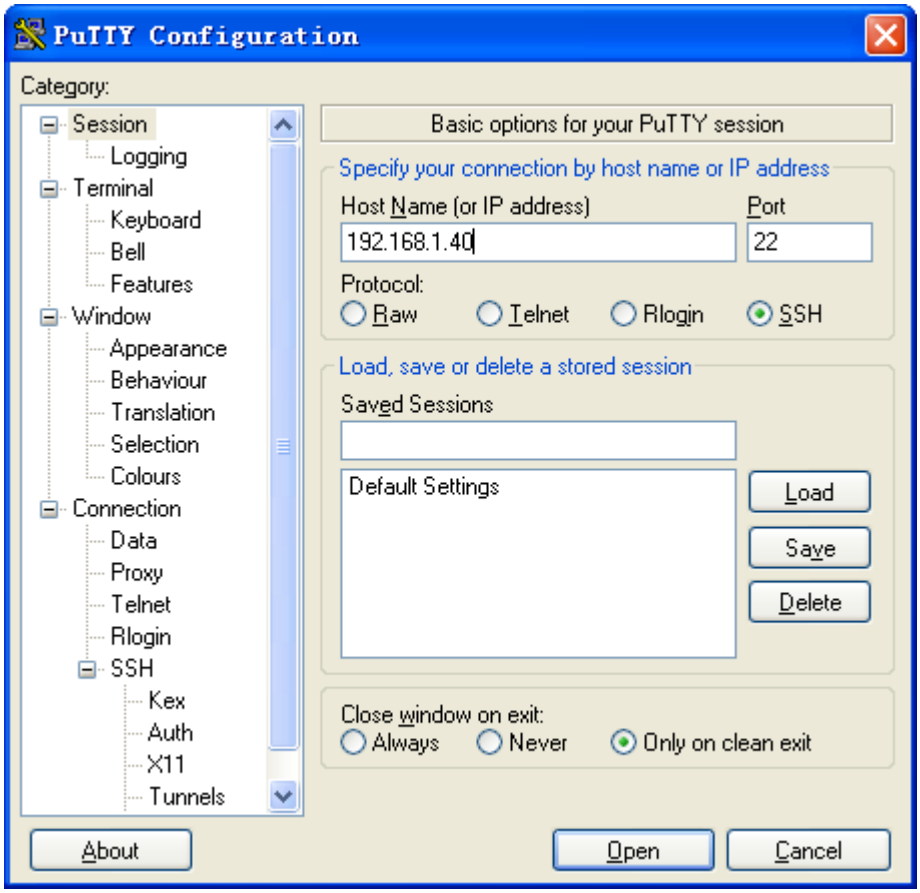
说明

Stelnet 客户端软件有很多，例如 PuTTY、OpenSSH 等。本文中仅以客户端软件 PuTTY0.58 为例，说明 Stelnet 客户端的配置方法。

建立与 Stelnet 服务器的连接。

打开PuTTY.exe程序，出现如 图 1-2 所示的客户端配置界面。在“Host Name（or IP address）”文本框中输入Stelnet服务器的IP地址为 192.168.1.40。

图1-2 Stelnet 客户端配置界面



在 图 1-2 中，单击<Open>按钮。按提示输入用户名client001 及密码aabbcc，即可进入Router的配置界面。

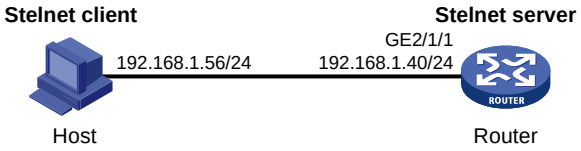
1.7.2 设备作为Stelnet服务器配置举例（publickey认证）

1. 组网需求

- 用户可以通过 Host 上运行的 Stelnet 客户端软件（SSH2 版本）安全地登录到 Router 上，并被授予用户角色 network-admin 进行配置管理；
- Router 采用 publickey 认证方式对 Stelnet 客户端进行认证，使用的公钥算法为 RSA。

2. 组网图

图1-3 设备作为 Stelnet 服务器配置组网图



3. 配置步骤

说明

- 在服务器的配置过程中需要指定客户端的公钥信息，因此需要首先完成客户端密钥对的配置，再进行服务器的配置。
- 客户端软件有很多，例如 PuTTY、OpenSSH 等。本文中仅以客户端软件 PuTTY0.58 为例，说明 Stelnet 客户端的配置方法。

(1) 配置 Stelnet 客户端

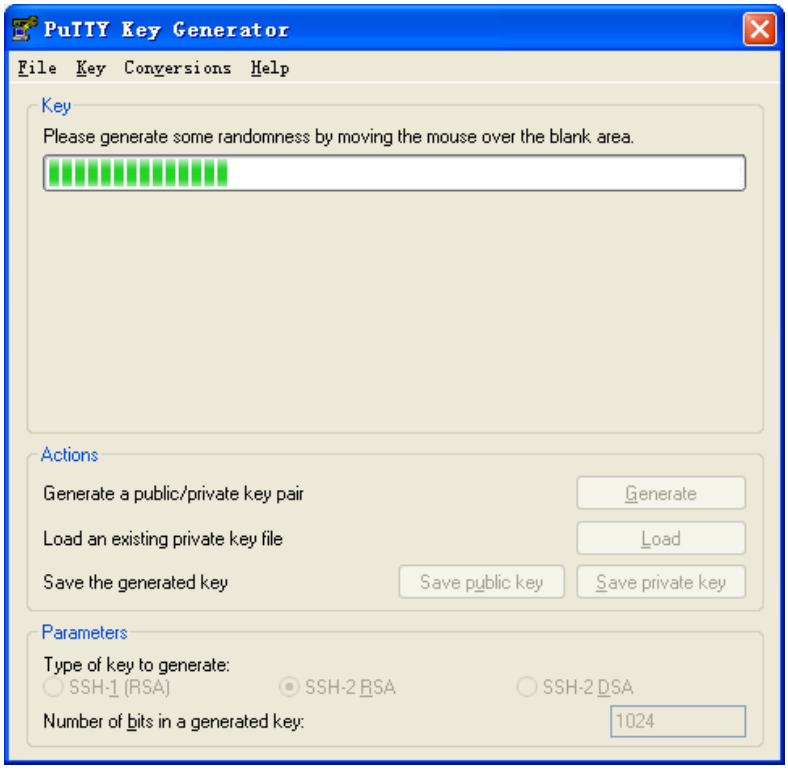
生成 RSA 密钥对。

运行 PuTTYGen.exe，在参数栏中选择“SSH-2 RSA”，点击<Generate>，产生客户端密钥对。

图1-4 生成客户端密钥（步骤 1）

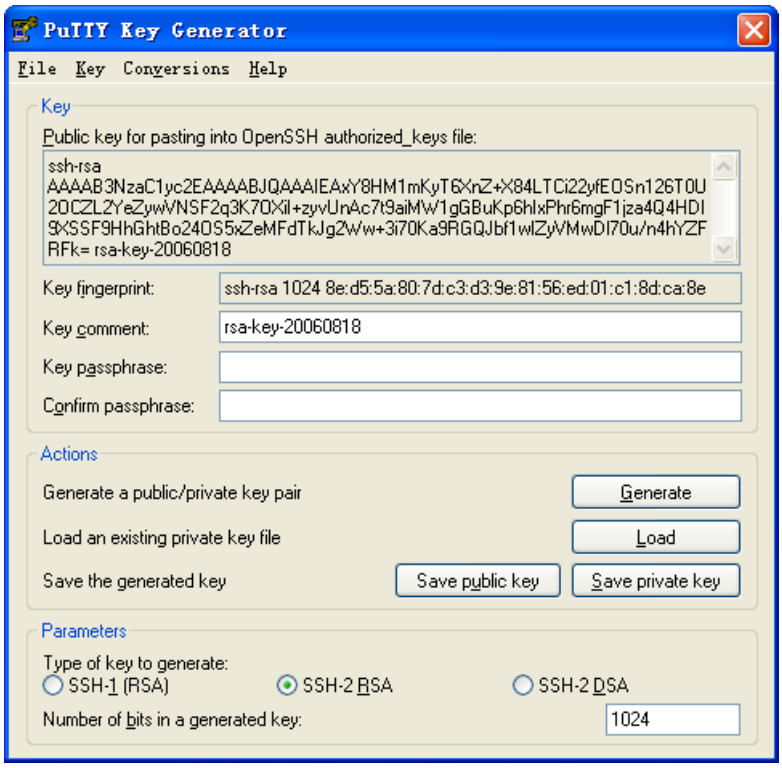
在产生密钥对的过程中需不停地移动鼠标，鼠标移动仅限于下图蓝色框中除绿色标记进程条外的地方，否则进程条的显示会不动，密钥对将停止产生，见 图 1-5。

图1-5 生成客户端密钥（步骤 2）



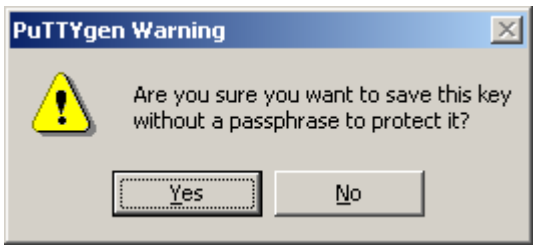
密钥对产生后，点击<Save public key>，输入存储公钥的文件名 key.pub，点击<保存>按钮。

图1-6 生成客户端密钥（步骤 3）



点击<Save private key>存储私钥，弹出警告框，提醒是否保存没做任何保护措施的私钥，点击<Yes>，输入私钥文件名为 private.ppk，点击保存。

图1-7 生成客户端密钥（步骤 4）



客户端生成密钥对后，需要将保存的公钥文件 key.pub 通过 FTP/TFTP 方式上传到服务器，具体过程略。

(2) 配置 Stelnet 服务器

生成 RSA 密钥对。

```
<Router> system-view
[Router] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
```

```
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[Router] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+................................+
...+.................+.........+...+
Create the key pair successfully.
```

使能 SSH 服务器功能。

```
[Router] ssh server enable
```

配置接口 GigabitEthernet2/1/1 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。

```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] ip address 192.168.1.40 255.255.255.0
[Router-GigabitEthernet2/1/1] quit
```

设置 Stelnet 客户端登录用户线的认证方式为 AAA 认证。

```
[Router] line vty 0 63
[Router-line-vty0-63] authentication-mode scheme
[Router-line-vty0-63] quit
```

从文件 key.pub 中导入远端的公钥，并命名为 clientkey。

```
[Router] public-key peer clientkey import sshkey key.pub
```

设置 SSH 用户 client002 的认证方式为 publickey，并指定公钥为 clientkey。

```
[Router] ssh user client002 service-type stelnet authentication-type publickey assign
publickey clientkey
```

创建设备管理类本地用户 client002，并设置服务类型为 SSH，用户角色为 network-admin。

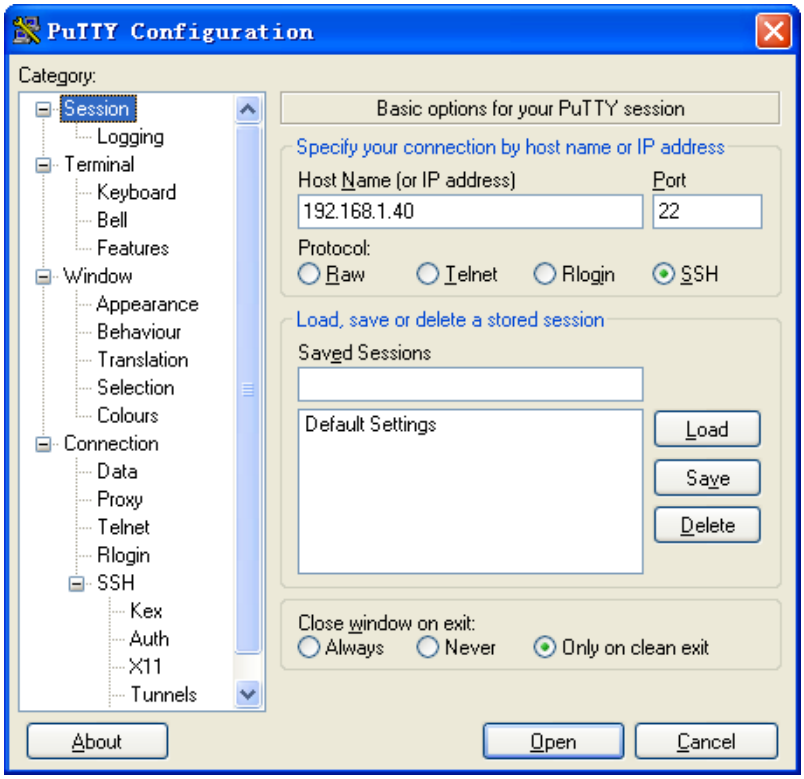
```
[Router] local-user client002 class manage
[Router-luser-manage-client002] service-type ssh
[Router-luser-manage-client002] authorization-attribute user-role network-admin
[Router-luser-manage-client002] quit
```

(3) Stelnet 客户端建立与 Stelnet 服务器的连接

指定私钥文件，并建立与 Stelnet 服务器的连接。

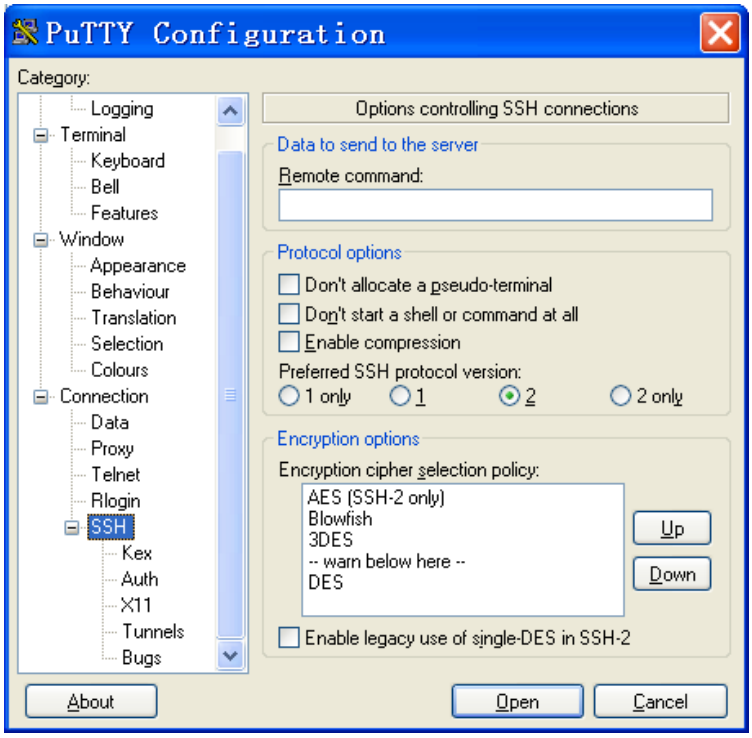
打开PuTTY.exe程序，出现如 图 1-8 所示的客户端配置界面。在“Host Name（or IP address）”文本框中输入Stelnet服务器的IP地址为 192.168.1.40。

图1-8 Stelnet 客户端配置界面（步骤 1）



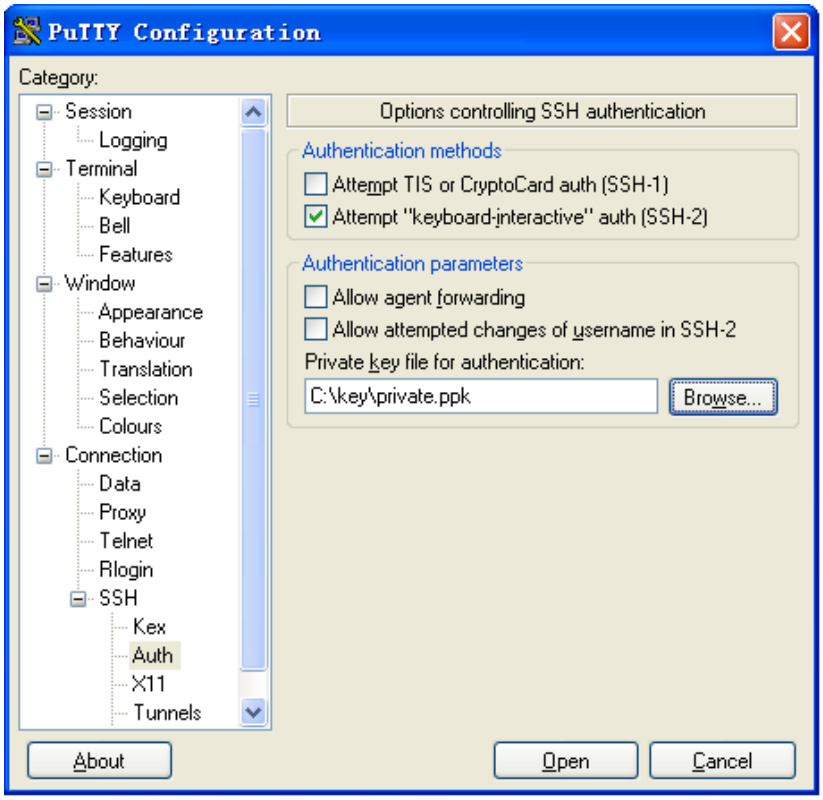
单击左侧导航栏“Connection->SSH”，出现如 图 1-9 的界面。选择“Preferred SSH protocol version”为 “2”。

图1-9 Stelnet 客户端配置界面



单击左侧导航树“Connection->SSH”下面的“Auth”（认证），出现如 图 1-10 的界面。单击<Browse…>按钮，弹出文件选择窗口。选择与配置到服务器端的公钥对应的私钥文件private.ppk。

图1-10 Stelnet 客户端配置界面（步骤 2）



如 图 1-10，单击<Open>按钮。按提示输入用户名client002，即可进入Router的配置界面。

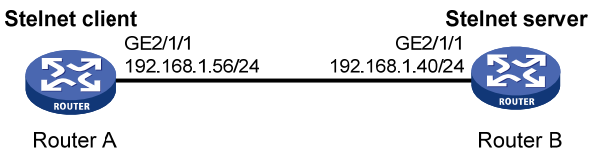
1.7.3 设备作为Stelnet客户端配置举例（password认证）

1. 组网需求

- 配置 Router A 作为 Stelnet 客户端，用户能够通过 Router A 安全地登录到 Router B 上，并被授予用户角色 network-admin 进行配置管理。
- Router B 作为 Stelnet 服务器采用 password 认证方式对 Stelnet 客户端进行认证，客户端的用户名和密码保存在 Router B 上。

2. 组网图

图1-11 设备作为 Stelnet 客户端的 password 认证配置组网图



3. 配置步骤

(1) 配置 Stelnet 服务器

生成 RSA 密钥对。

```
<RouterB> system-view
```

```
[RouterB] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[RouterB] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.................................+
...+.................+.........+...+
Create the key pair successfully.
```

使能 SSH 服务器功能。

```
[RouterB] ssh server enable
```

配置接口 GigabitEthernet2/1/1 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ip address 192.168.1.40 255.255.255.0
[RouterB-GigabitEthernet2/1/1] quit
```

设置 Stelnet 客户端登录用户线的认证方式为 AAA 认证。

```
[RouterB] line vty 0 63
[RouterB-line-vty0-63] authentication-mode scheme
[RouterB-line-vty0-63] quit
```

创建设备管理类本地用户 client001，并设置密码为明文 aabbcc，服务类型为 SSH，用户角色为 network-admin。

```
[RouterB] local-user client001 class manage
[RouterB-luser-manage-client001] password simple aabbcc
[RouterB-luser-manage-client001] service-type ssh
[RouterB-luser-manage-client001] authorization-attribute user-role network-admin
[RouterB-luser-manage-client001] quit
```

配置 SSH 用户 client001 的服务类型为 Stelnet，认证方式为 password 认证。（此步骤可以不配置）

```
[RouterB] ssh user client001 service-type stelnet authentication-type password
```

(2) Stelnet 客户端建立与 Stelnet 服务器的连接

配置接口 GigabitEthernet2/1/1 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
```

```
[RouterA-GigabitEthernet2/1/1] ip address 192.168.1.56 255.255.255.0
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] quit
```

- 客户端本地没有服务器端主机公钥，首次与服务器建立连接

建立到服务器 192.168.1.40 的 SSH 连接，选择不认证服务器的情况下继续访问服务器，并在客户端保存服务器端的本地公钥。

```
<RouterA> ssh2 192.168.1.40
Username: client001
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:y
client001@192.168.1.40's password:
```

输入正确的密码之后，即可成功登录到 Router B 上。由于选择在本地保存服务器端的主机公钥，下次用户登录 Router B 时直接输入正确密码即可成功登录。

- 客户端配置服务器端的主机公钥后，与服务器建立连接

在客户端配置 SSH 服务器端的主机公钥。在公钥视图输入服务器端的主机公钥，即在服务器端通过 **display public-key local dsa public** 命令显示的公钥内容。

```
[RouterA] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
[RouterA-pkey-public-key-key1] 308201B73082012C06072A8648CE3804013082011F0281810
0D757262C4584C44C211F18BD96E5F0
[RouterA-pkey-public-key-key1]61C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE
65BE6C265854889DC1EDBD13EC8B274
[RouterA-pkey-public-key-key1]DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B0
6FD60FE01941DDD77FE6B12893DA76E
[RouterA-pkey-public-key-key1]EBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B3
68950387811C7DA33021500C773218C
[RouterA-pkey-public-key-key1]737EC8EE993B4F2DED30F48EDACE915F0281810082269009E
14EC474BAF2932E69D3B1F18517AD95
[RouterA-pkey-public-key-key1]94184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD35D02
492B3959EC6499625BC4FA5082E22C5
[RouterA-pkey-public-key-key1]B374E16DD00132CE71B020217091AC717B612391C76C1FB2E
88317C1BD8171D41ECB83E210C03CC9
[RouterA-pkey-public-key-key1]B32E810561C21621C73D6DAAC028F4B1585DA7F42519718CC
9B09EEF0381840002818000AF995917
[RouterA-pkey-public-key-key1]E1E570A3F6B1C2411948B3B4FFA256699B3BF871221CC9C5D
F257523777D033BEE77FC378145F2AD
[RouterA-pkey-public-key-key1]D716D7DB9FCABB4ADBF6FB4FDB0CA25C761B308EF53009F71
01F7C62621216D5A572C379A32AC290
[RouterA-pkey-public-key-key1]E55B394A217DA38B65B77F0185C8DB8095522D1EF044B465E
8716261214A5A3B493E866991113B2D
[RouterA-pkey-public-key-key1]485348
[RouterA-pkey-public-key-key1] peer-public-key end
[RouterA] quit
```

建立到服务器 192.168.1.40 的 SSH 连接，并指定服务器端的主机公钥。

```
<RouterA> ssh2 192.168.1.40 publickey key1
Username: client001
```

```
client001@192.168.1.40's password:
```

输入正确的密码之后，即可成功登录到 Router B 上。

- 客户端本地已有服务器端的主机公钥，直接与服务器建立连接

```
<RouterA> ssh2 192.168.1.40
Username: client001
client001@192.168.1.40's password:
```

输入正确的密码之后，即可成功登录到 Router B 上。

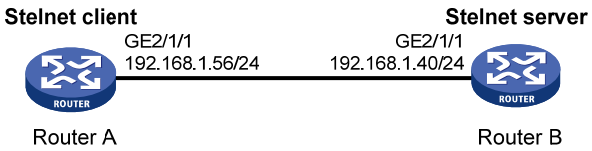
1.7.4 设备作为Stelnet客户端配置举例（publickey认证）

1. 组网需求

- 配置 Router A 作为 Stelnet 客户端，用户能够通过 Router A 安全地登录到 Router B 上，并被授予用户角色 network-admin 进行配置管理。
- Router B 作为 Stelnet 服务器采用 publickey 认证方式对 Stelnet 客户端进行认证，使用的公钥算法为 DSA。

2. 组网图

图1-12 设备作为 Stelnet 客户端配置组网图



3. 配置步骤

说明

在服务器的配置过程中需要指定客户端的公钥信息，因此需要首先完成客户端密钥对的配置，再进行服务器的配置。

---

(1) 配置 Stelnet 客户端

配置接口 GigabitEthernet2/1/1 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip address 192.168.1.56 255.255.255.0
[RouterA-GigabitEthernet2/1/1] quit
```

生成 DSA 密钥对。

```
[RouterA] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
```

```
........+......+.....+.................................+
...+.................+..........+...+
Create the key pair successfully.
```

将生成的 DSA 主机公钥导出到指定文件 key.pub 中。

```
[RouterA] public-key local export dsa ssh2 key.pub
[RouterA] quit
```

客户端生成密钥对后，需要将保存的公钥文件 key.pub 通过 FTP/TFTP 方式上传到服务器，具体过程略。

(2) 配置 Stelnet 服务器

生成 RSA 密钥对。

```
<RouterB> system-view
[RouterB] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.......................++++++
...................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[RouterB] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.................................+
...+.................+..........+...+
Create the key pair successfully.
```

使能 SSH 服务器功能。

```
[RouterB] ssh server enable
```

配置接口 GigabitEthernet2/1/1 的 IP 地址，客户端将通过该地址连接 Stelnet 服务器。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ip address 192.168.1.40 255.255.255.0
[RouterB-GigabitEthernet2/1/1] quit
```

设置 Stelnet 客户端登录用户线的认证方式为 AAA 认证。

```
[RouterB] line vty 0 63
[RouterB-line-vty0-63] authentication-mode scheme
[RouterB-line-vty0-63] quit
```

从文件 key.pub 中导入远端的公钥，并命名为 clientkey。

```
[RouterB] public-key peer clientkey import sshkey key.pub
```

设置 SSH 用户 client002 的认证方式为 publickey，并指定公钥为 clientkey。

```
[RouterB] ssh user client002 service-type stelnet authentication-type publickey assign publickey clientkey
```

创建设备管理类本地用户 client002，并设置服务类型为 SSH，用户角色为 network-admin。

```
[RouterB] local-user client002 class manage
[RouterB-luser-manage-client002] service-type ssh
[RouterB-luser-manage-client002] authorization-attribute user-role network-admin
[RouterB-luser-manage-client002] quit
```

(3) Stelnet 客户端建立与 Stelnet 服务器的连接

建立到服务器 192.168.1.40 的 SSH 连接。

```
<RouterA> ssh2 192.168.1.40
Username: client002
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
```

由于本地未保存服务器端的主机公钥，因此首次登录时只要选择继续访问服务器，即可成功登录到 Router B 上。

1.8 SFTP典型配置举例

说明

举例中的设备运行于非 FIPS 模式下。若设备运行于 FIPS 模式下，支持的密钥对的模数只能为 2048 比特，因此相关的配置和显示信息也有所变化，请以设备的实际情况为准；设备作为服务器仅支持 RSA 密钥对，请不要生成 DSA 密钥对。

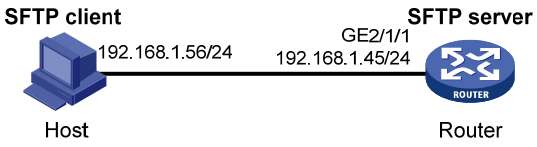
1.8.1 设备作为SFTP服务器配置举例（password认证）

1. 组网需求

- 用户可以通过 Host 上运行的 SFTP 客户端软件安全地登录到 Router 上，并被授予用户角色 network-admin 进行文件管理和文件传送操作；
- Router 采用 password 认证方式对 SFTP 客户端进行认证，客户端的用户名和密码保存在本地。

2. 组网图

图1-13 设备作为 SFTP 服务器配置组网图



3. 配置步骤

(1) 配置 SFTP 服务器

生成 RSA 密钥对。

```
<Router> system-view
[Router] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[Router] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.................................+
...+.................+..........+...+
Create the key pair successfully.
```

启动 SFTP 服务器。

```
[Router] sftp server enable
```

配置接口 GigabitEthernet2/1/1 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] ip address 192.168.1.45 255.255.255.0
[Router-GigabitEthernet2/1/1] quit
```

创建设备管理类本地用户 client002，并设置密码为明文 aabbcc，服务类型为 SSH，用户角色为 network-admin，工作目录为 flash:/。

```
[Router] local-user client002 class manage
[Router-luser-manage-client002] password simple aabbcc
[Router-luser-manage-client002] service-type ssh
[Router-luser-manage-client002] authorization-attribute user-role network-admin
work-directory flash:/
[Router-luser-manage-client002] quit
```

配置 SSH 用户认证方式为 password，服务类型为 SFTP。（此步骤可以不配置）

```
[Router] ssh user client002 service-type sftp authentication-type password
```

(2) SFTP 客户端建立与 SFTP 服务器的连接

说明

- SFTP 客户端软件有很多，本文中仅以客户端软件 PuTTY0.58 中的 PSFTP 为例，说明 SFTP 客户端的配置方法。
- PSFTP 只支持 password 认证，不支持 publickey 认证。

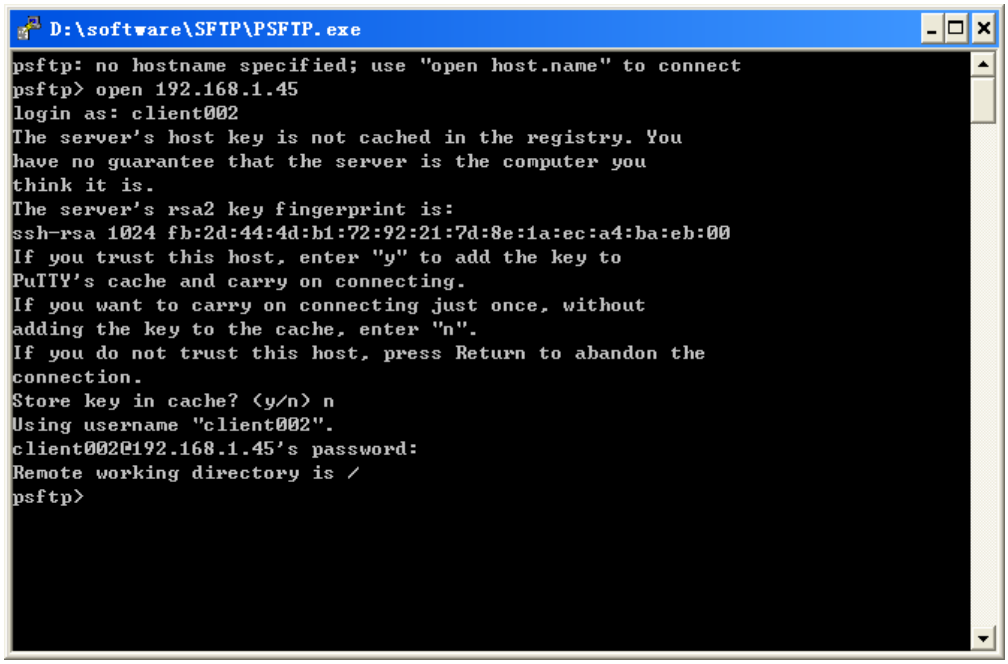
建立与 SFTP 服务器的连接。

打开psftp.exe程序，出现如 图 1-14 所示的客户端配置界面。输入如下命令：

```
open 192.168.1.45
```

根据提示输入用户名 client002、密码 aabbcc，即可登录 SFTP 服务器。

图1-14 SFTP 客户端登录界面



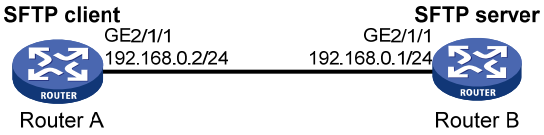
1.8.2 设备作为SFTP客户端配置举例（publickey认证）

1. 组网需求

- 配置 Router A 作为 SFTP 客户端，用户能够通过 Router A 安全地登录到 Router B 上，并被授予用户角色 network-admin 进行文件管理和文件传送等操作。
- Router B 作为 SFTP 服务器采用 publickey 认证方式对 SFTP 客户端进行认证，使用的公钥算法为 RSA。

2. 组网图

图1-15 设备作为 SFTP 客户端配置组网图



3. 配置步骤

说明

在服务器的配置过程中需要指定客户端的公钥信息，因此建议首先完成客户端密钥对的配置，再进行服务器的配置。

(1) 配置 SFTP 客户端

配置接口 GigabitEthernet2/1/1 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip address 192.168.0.2 255.255.255.0
[RouterA-GigabitEthernet2/1/1] quit
```

生成 RSA 密钥对。

```
[RouterA] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
...................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

将生成的 RSA 主机公钥导出到指定文件 pubkey 中。

```
[RouterA] public-key local export rsa ssh2 pubkey
[RouterA] quit
```

客户端生成密钥对后，需要将保存的公钥文件 pubkey 通过 FTP/TFTP 方式上传到服务器，具体过程略。

(2) 配置 SFTP 服务器

生成 RSA 密钥对。

```
<RouterB> system-view
[RouterB] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
```

```
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[RouterB] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+.................+.........+...+
Create the key pair successfully.
```

启动 SFTP 服务器。

```
[RouterB] sftp server enable
```

配置接口 GigabitEthernet2/1/1 的 IP 地址，客户端将通过该地址连接 SFTP 服务器。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ip address 192.168.0.1 255.255.255.0
[RouterB-GigabitEthernet2/1/1] quit
```

从文件 pubkey 中导入远端的公钥，并命名为 routerkey。

```
[RouterB] public-key peer routerkey import sshkey pubkey
```

设置 SSH 用户 client001 的服务类型为 SFTP，认证方式为 publickey，并指定公钥为 routerkey。

```
[RouterB] ssh user client001 service-type sftp authentication-type publickey assign
publickey routerkey
```

创建设备管理类本地用户 client001，并设置服务类型为 SSH，用户角色为 network-admin，工作目录为 flash:/。

```
[RouterB] local-user client001 class manage
[RouterB-luser-manage-client001] service-type ssh
[RouterB-luser-manage-client001] authorization-attribute user-role network-admin
work-directory flash:/
[RouterB-luser-manage-client001] quit
```

(3) SFTP 客户端建立与 SFTP 服务器的连接

与远程 SFTP 服务器建立连接，进入 SFTP 客户端视图。

```
<RouterA> sftp 192.168.0.1 identity-key rsa
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
sftp>
```

显示服务器的当前目录，删除文件 z，并检查此文件是否删除成功。

```
sftp> dir -l
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 013 z
sftp> delete z
Removing /z
sftp> dir -l
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
```

新增目录 new1，并检查新目录是否创建成功。

```
sftp> mkdir new1
sftp> dir -l
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
drwxrwxrwx    1 1        1               301 Dec 18 14:12 013 new1
```

将目录名 new1 更名为 new2，并查看是否更名成功。

```
sftp> rename new1 new2
sftp> dir
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
drwxrwxrwx    1 1        1               301 Dec 18 14:12 013 new2
```

从服务器上下载文件 pubkey2 到本地，并更名为 public。

```
sftp> get pubkey2 public
Fetching / pubkey2 to public
/pubkey2                                      100% 225     1.4KB/s   00:00
```

将本地文件 pu 上传到服务器上，更名为 puk，并查看上传是否成功。

```
sftp> put pu puk
Uploading pu to / puk
sftp> dir
-rwxrwxrwx    1 1        1               301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 012.pub
-rwxrwxrwx    1 1        1               301 Dec 18 14:12 013 puk
sftp>
```

退出 SFTP 客户端视图。

```
sftp> quit
<RouterA>
```

1.9 SCP典型配置举例

说明

举例中的设备运行于非 FIPS 模式下。若设备运行于 FIPS 模式下，支持的密钥对的模数只能为 2048 比特，因此相关的配置和显示信息也有所变化，请以设备的实际情况为准；设备作为服务器仅支持 RSA 密钥对，请不要生成 DSA 密钥对。

1.9.1 SCP文件传输配置举例（password认证）

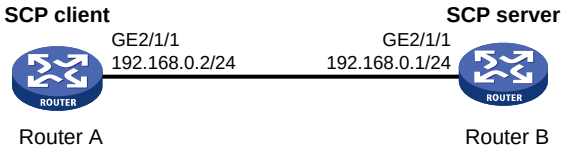
1. 组网需求

如下图所示，Router A 作为 SCP 客户端，Router B 作为 SCP 服务器。现有如下具体需求：

- 用户能够通过 Router A 安全地登录到 Router B 上，并被授予用户角色 network-admin 与 Router B 进行文件传输。
- Router B 采用 password 认证对 SCP 客户端进行认证，客户端的用户名和密码保存在 Router B 上。

2. 组网图

图1-16 SCP 文件传输配置组网图



3. 配置步骤

(1) 配置 SCP 服务器

生成 RSA 密钥对。

```
<RouterB> system-view
[RouterB] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....................++++++
.................++++++
..++++++++
............++++++++
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[RouterB] public-key local create dsa
The range of public key size is (512 ~ 2048).
```

```
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+
...+.................+..........+...+.
Create the key pair successfully.
```

使能 SSH 服务器功能。

```
[RouterB] ssh server enable
```

配置接口 GigabitEthernet2/1/1 的 IP 地址，客户端将通过该地址连接 SCP 服务器。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ip address 192.168.0.1 255.255.255.0
[RouterB-GigabitEthernet2/1/1] quit
```

创建设备管理类本地用户 client001，并设置密码为明文 aabbcc，服务类型为 SSH。

```
[RouterB] local-user client001 class manage
[RouterB-luser-manage-client001] password simple aabbcc
[RouterB-luser-manage-client001] service-type ssh
[RouterB-luser-manage-client001] authorization-attribute user-role network-admin
[RouterB-luser-manage-client001] quit
```

配置 SSH 用户 client001 的服务类型为 scp，认证方式为 password 认证。（此步骤可以不配置）

```
[RouterB] ssh user client001 service-type scp authentication-type password
```

(2) 配置 SCP 客户端

配置 GigabitEthernet2/1/1 接口的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip address 192.168.0.2 255.255.255.0
[RouterA-GigabitEthernet2/1/1] quit
[RouterA] quit
```

(3) SCP 客户端从 SCP 服务器下载文件

与远程 SCP 服务器建立连接，并下载远端的 remote.bin 文件，下载到本地后更名为 local.bin。

```
<RouterA> scp 192.168.0.1 get remote.bin local.bin
Username: client001
Connected to 192.168.0.1 ...
The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
Enter password:
18471 bytes transfered in 0.001 seconds.
```

目 录

1 SSL

说明

- 设备运行于 FIPS 模式时，本特性部分配置相对于非 FIPS 模式有所变化，具体差异请见本文相关描述。有关 FIPS 模式的详细介绍请参见“安全配置指导”中的“FIPS”。

1.1 SSL简介

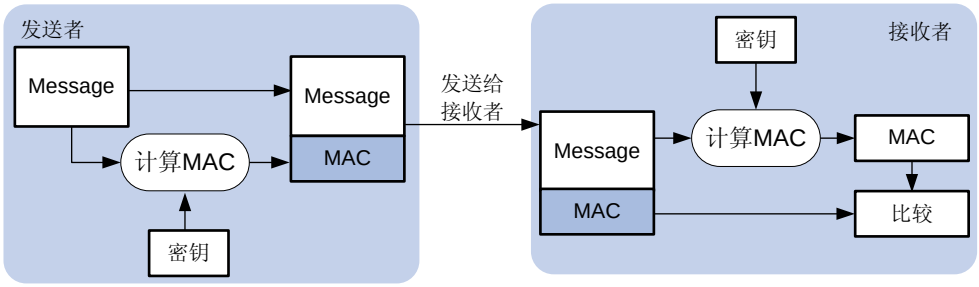
SSL（Secure Sockets Layer，安全套接字层）是一个安全协议，为基于 TCP 的应用层协议（如 HTTP）提供安全连接。SSL 协议广泛应用于电子商务、网上银行等领域，为应用层数据的传输提供安全性保证。

1.1.1 SSL安全机制

SSL 提供的安全连接可以实现如下功能：

- 保证数据传输的机密性：利用对称密钥算法对传输的数据进行加密，并利用密钥交换算法，如 RSA（Rivest Shamir and Adleman），加密传输对称密钥算法中使用的密钥。对称密钥算法、非对称密钥算法 RSA 的详细介绍请参见“安全配置指导”中的“公钥管理”。
- 验证数据源的身份：基于数字证书利用数字签名方法对 SSL 服务器和 SSL 客户端进行身份验证。SSL 服务器和 SSL 客户端通过 PKI（Public Key Infrastructure，公钥基础设施）提供的机制获取数字证书。PKI 及数字证书的详细介绍请参见“安全配置指导”中的“PKI”。
- 保证数据的完整性：消息传输过程中使用MAC（Message Authentication Code，消息验证码）来检验消息的完整性。MAC算法在密钥的参与下，将任意长度的原始数据转换为固定长度的数据，原始数据的任何变化都会导致计算出的固定长度数据发生变化。如 图 1-1 所示，利用MAC算法验证消息完整性的过程为：
  a. 发送者在密钥的参与下，利用 MAC 算法计算出消息的 MAC 值，并将其加在消息之后发送给接收者。
  b. 接收者利用同样的密钥和 MAC 算法计算出消息的 MAC 值，并与接收到的 MAC 值比较。
  c. 如果二者相同，则接收者认为报文没有被篡改；否则，认为报文在传输过程中被篡改，接收者将丢弃该报文。

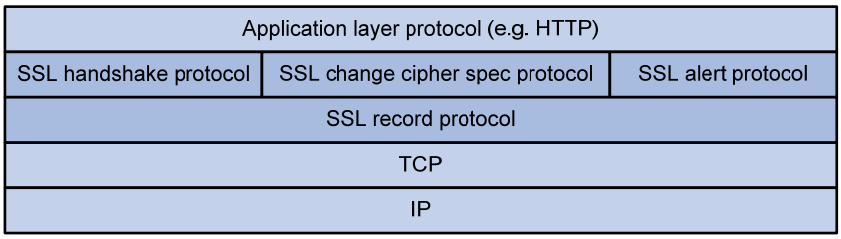
图1-1 MAC 算法示意图



1.1.2 SSL协议结构

如 图 1-2 所示，SSL协议可以分为两层：下层为SSL记录协议（SSL Record Protocol）；上层为SSL握手协议（SSL Handshake Protocol）、SSL密码变化协议（SSL Change Cipher Spec Protocol）和SSL告警协议（SSL Alert Protocol）。

图1-2 SSL 协议栈



- SSL 记录协议：主要负责对上层的数据进行分块、计算并添加 MAC、加密，最后把加密后的记录块传输给对方。
- SSL 握手协议：用来协商通信过程中使用的加密套件（数据加密算法、密钥交换算法和 MAC 算法等），实现服务器和客户端的身份验证，并在服务器和客户端之间安全地交换密钥。客户端和服务器通过握手协议建立会话。一个会话包含一组参数，主要有会话 ID、对方的数字证书、加密套件及主密钥。
- SSL 密码变化协议：客户端和服务器端通过密码变化协议通知对端，随后的报文都将使用新协商的加密套件和密钥进行保护和传输。
- SSL 告警协议：用来向对端报告告警信息，以便对端进行相应的处理。告警消息中包含告警的严重级别和描述。

1.2 SSL配置任务简介

表1-1 SSL 配置任务简介

配置任务	说明	详细配置
配置SSL服务器端策略	请在SSL服务器端进行本配置	1.3
配置SSL客户端策略	请在SSL客户端进行本配置	1.4

1.3 配置SSL服务器端策略

SSL 服务器端策略是服务器启动时使用的 SSL 参数。只有与 HTTPS（Hypertext Transfer Protocol Secure，超文本传输协议的安全版本）等应用关联后，SSL 服务器端策略才能生效。

1.3.1 SSL服务器端策略配置步骤

表1-2 配置 SSL 服务器端策略

操作	命令	说明
进入系统视图	**system-view**	-
创建SSL服务器端策略，并进入SSL服务器端策略视图	**ssl server-policy** *policy-name*	缺省情况下，设备上不存在任何SSL服务器端策略
（可选）配置SSL服务器端策略所使用的PKI域	**pki-domain** *domain-name*	缺省情况下，没有指定SSL服务器端策略所使用的PKI域 如果客户端需要对服务器端进行基于数字证书的身份验证，则必须在SSL服务器端使用本命令指定PKI域，并在该PKI域内为SSL服务器端申请本地数字证书 PKI域的创建及配置方法，请参见“安全配置指导”中的“PKI”
配置SSL服务器端策略支持的加密套件	非FIPS模式下： **ciphersuite** { **dhe_rsa_aes_128_cbc_sha** | **dhe_rsa_aes_256_cbc_sha** | **exp_rsa_des_cbc_sha** | **exp_rsa_rc2_md5** | **exp_rsa_rc4_md5** | **rsa_3des_ede_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha** | **rsa_des_cbc_sha** | **rsa_rc4_128_md5** | **rsa_rc4_128_sha** } * FIPS模式下： **ciphersuite** { **dhe_rsa_aes_128_cbc_sha** | **dhe_rsa_aes_256_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha** } *	缺省情况下，SSL服务器端策略支持所有的加密套件
配置SSL服务器上可以缓存的最大会话数目	**session cachesize** *size*	缺省情况下，SSL服务器上可以缓存的最大会话数目为500个
配置SSL服务器端要求对SSL客户端进行基于数字证书的身份验证	**client-verify enable**	缺省情况下，SSL服务器端不要求对SSL客户端进行基于数字证书的身份验证 SSL服务器端在基于数字证书对SSL客户端进行身份验证时，除了对SSL客户端发送的证书链进行验证，还要检查证书链中的除根CA证书外的每个证书是否均未被吊销

说明

目前，SSL 协议版本主要有 SSL2.0、SSL3.0 和 TLS1.0（TLS1.0 对应 SSL 协议的版本号为 3.1）。设备作为 SSL 服务器时，可以与 SSL3.0 和 TLS1.0 版本的 SSL 客户端通信，还可以识别同时兼容 SSL2.0 和 SSL3.0/TLS1.0 版本的 SSL 客户端发送的报文，并通知该客户端采用 SSL3.0/TLS1.0 版本与 SSL 服务器通信。

1.4 配置SSL客户端策略

SSL 客户端策略是客户端连接 SSL 服务器时使用的参数。只有与应用层协议，如 DDNS（Dynamic Domain Name System，动态域名系统），关联后，SSL 客户端策略才能生效。DDNS 的详细配置请参见“三层技术-IP 业务配置指导”中的“DDNS”。

表1-3 配置 SSL 客户端策略

配置任务	命令	说明
进入系统视图	**system-view**	-
创建SSL客户端策略，并进入SSL客户端策略视图	**ssl client-policy** *policy-name*	缺省情况下，设备上不存在任何SSL客户端策略
（可选）配置SSL客户端策略所使用的PKI域	**pki-domain** *domain-name*	缺省情况下，没有指定SSL客户端策略所使用的PKI域 如果服务器端需要对客户端进行基于数字证书的身份验证，则必须在SSL客户端使用本命令指定PKI域，并在该PKI域内为SSL客户端申请本地数字证书 PKI域的创建及配置方法，请参见“安全配置指导”中的“PKI”
配置SSL客户端策略支持的加密套件	非FIPS模式下： **prefer-cipher { dhe_rsa_aes_128_cbc_sha | dhe_rsa_aes_256_cbc_sha | exp_rsa_des_cbc_sha | exp_rsa_rc2_md5 | exp_rsa_rc4_md5 | rsa_3des_ede_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha | rsa_des_cbc_sha | rsa_rc4_128_md5 | rsa_rc4_128_sha }** FIPS模式下： **prefer-cipher { dhe_rsa_aes_128_cbc_sha | dhe_rsa_aes_256_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha }**	非FIPS模式下： 缺省情况下，SSL客户端策略支持的加密套件为**rsa_rc4_128_md5** FIPS模式下： 缺省情况下，SSL客户端策略支持的加密套件为**rsa_aes_128_cbc_sha**
配置SSL客户端策略使用的SSL协议版本	非FIPS模式下： **version { ssl3.0 | tls1.0 }** FIPS模式下： **version tls1.0**	缺省情况下，SSL客户端策略使用的SSL协议版本为TLS 1.0

配置任务	命令	说明
配置客户端需要对服务器端进行基于数字证书的身份验证	**server-verify enable**	缺省情况下，SSL客户端需要对SSL服务器端进行基于数字证书的身份验证

1.5 SSL显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 SSL 的运行情况，通过查看显示信息验证配置的效果。

表1-4 SSL 显示和维护

操作	命令
显示SSL服务器端策略的信息	**display ssl server-policy** [*policy-name*]
显示SSL客户端策略的信息	**display ssl client-policy** [*policy-name*]

目 录

1 ASPF配置

1.1 ASPF简介

包过滤防火墙属于静态防火墙，目前存在的问题如下：

- 对于传输层协议，配置管理员无法精确预知反向回应报文信息，因此增加了包过滤配置的难度。同时，若配置管理员配置了比较宽松的放行策略，则会增加内网被攻击的风险。
- 对于多通道的应用层协议（如 FTP 等），部分安全策略配置无法预知。
- 无法跟踪传输层和应用层的协议状态，无法检测某些来自传输层和应用层的攻击行为。
- 无法识别来自网络中伪造的 ICMP 差错报文，从而无法避免 ICMP 的恶意攻击。

因此，提出了状态防火墙——ASPF（Advanced Stateful Packet Filter，高级状态包过滤）的概念。ASPF 能够实现的主要功能有：

- 应用层协议检测：检查应用层协议信息，如报文的协议类型和端口号等信息，并且监控每一个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，以阻止恶意的入侵。
- 传输层协议检测：检测传输层协议信息（即通用 TCP/UDP 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。
- ICMP 差错报文检测：正常 ICMP 差错报文中均携带有本报文对应连接的相关信息，根据这些信息可以匹配到相应的连接。如果匹配失败，则根据当前配置决定是否丢弃该 ICMP 报文。
- TCP 连接首包检测：对 TCP 连接的首报文进行检测，查看是否为 SYN 报文，如果不是 SYN 报文则根据当前配置决定是否丢弃该报文。缺省情况下，不丢弃非 SYN 首包，适用于不需要严格 TCP 协议状态检查的组网场景。例如当防火墙设备首次加入网络时，网络中原有 TCP 连接的非首包在经过新加入的设备时如果被丢弃，会中断已有的连接，造成不好的用户体验，因此建议暂且不丢弃非 SYN 首包，等待网络拓扑稳定后，再开启非 SYN 首包丢弃功能。

在网络边界，ASPF 和包过滤防火墙协同工作，包过滤防火墙负责按照 ACL 规则进行报文过滤（阻断或放行），ASPF 负责对已放行报文进行信息记录，使已放行的报文的回应报文可以正常通过配置了包过滤防火墙的接口。因此，ASPF 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。

1.1.1 ASPF基本概念

1. 单通道协议和多通道协议

ASPF 将应用层协议划分为：

- 单通道协议：完成一次应用的全过程中，只有一个连接参与数据交互，如 SMTP、HTTP。
- 多通道协议：完成一次应用的全过程中，需要多个连接配合，即控制信息的交互和数据的传送需要通过不同的连接完成的，如 FTP。

2. 内部接口和外部接口

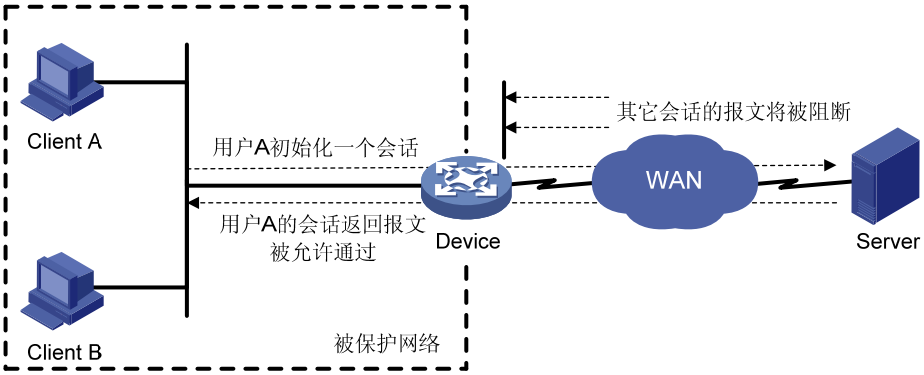
如果设备连接了内部网络和外部网络，并且要通过部署 ASPF 来保护内部网络中的主机和服务器，则设备上与内部网络连接的接口就称为内部接口，与外部网络相连的接口就称为外部接口。

若需要保护内部网络，则可以将 ASPF 应用于设备外部接口的出方向或者应用于设备内部接口的入方向。

1.1.2 ASPF检测原理

1. 应用层协议检测基本原理

图1-1 应用层协议检测基本原理示意图



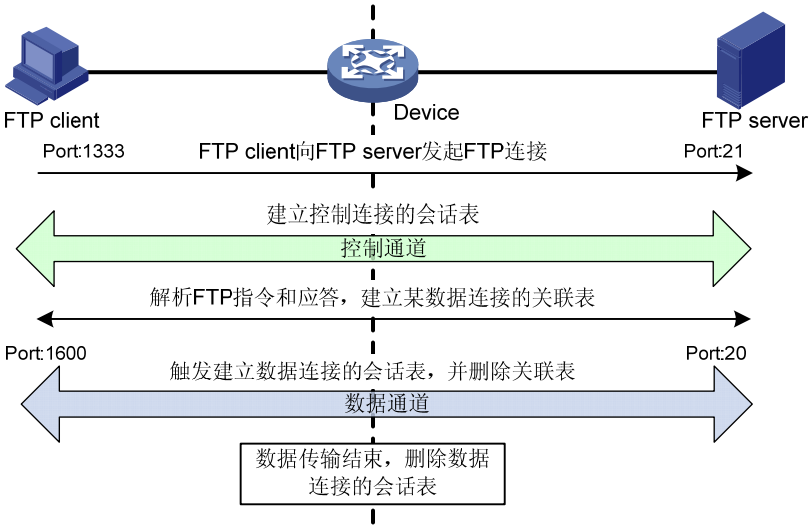
如 图 1-1 所示，为了保护内部网络，可以在边界设备上配置访问控制列表，以允许内部网络的主机访问外部网络，同时拒绝外部网络的主机访问内部网络。但是访问控制列表会将用户发起连接后返回的报文过滤掉，导致连接无法正常建立。利用ASPF的应用层协议检测可以解决此问题。

当在设备上配置了应用层协议检测后，ASPF 可以检测每一个应用层的连接，具体检测原理如下：

- 对于单通道协议，ASPF 在检测到第一个向外发送的报文时创建一个会话表项。该会话表项中记录了对应的正向报文信息和反向报文信息，用于维护会话状态并检测会话状态的转换是否正确。匹配某条会话表项的所有报文都将免于接受静态包过滤策略的检查。
- 对于多通道协议，ASPF 除了创建会话表项之外，还会根据协议的协商情况，创建一个或多个关联表项，用于关联属于同一个应用业务的不同会话。关联表项在多通道协议协商的过程中创建，在多通道协议协商完成后删除。关联表项主要用于匹配会话首报文，使已通过协商的会话报文可免于接受静态包过滤策略的检查。

单通道应用层协议（如 HTTP）的检测过程比较简单，当发起连接时建立会话表项，连接删除时随之删除会话表项即可。下面以 FTP 检测为例说明多通道应用层协议检测的过程。

图1-2 FTP 检测过程示意图



如 图 1-2 所示，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，通过协商决定在FTP server的 20 端口与FTP Client的 1600 端口之间建立数据通道，并由FTP server发起数据连接，数据传输超时或结束后数据通道删除。

FTP 检测在 FTP 连接建立到拆除过程中的处理如下：

(1) 检查 FTP client 向 FTP server 发送的 IP 报文，确认为基于 TCP 的 FTP 报文。检查端口号，确认该连接为 FTP client 与 FTP server 之间的控制连接，建立会话表项。

(2) 检查 FTP 控制连接报文，根据会话表项进行 TCP 状态检测。解析 FTP 指令，如果包含数据通道建立指令，则创建关联表项描述对应数据连接的特征。

(3) 对于返回的 FTP 控制连接报文，根据会话表项进行 TCP 状态检测，检测结果决定是否允许报文通过。

(4) FTP 数据连接报文通过设备时，将会触发建立数据连接的会话表项，并删除所匹配的关联表项。

(5) 对于返回的 FTP 数据连接报文，则通过匹配数据连接的会话表项进行 TCP 状态检测，检查结果决定是否允许报文通过。

(6) 数据连接结束时，数据连接的会话表项将被删除。FTP 连接删除时，控制连接的会话表项也会被删除。

2. 传输层协议检测基本原理

传输层协议检测是指通用 TCP/UDP 检测。通用 TCP/UDP 检测也是通过建立会话表项记录报文的传输层信息，如源地址、目的地址及端口号等，达到动态放行报文的目的。

通用 TCP/UDP 检测要求返回到 ASPF 外部接口的报文要与之前从 ASPF 外部接口发出去的报文完全匹配，即源地址、目的地址及端口号完全对应，否则返回的报文将被丢弃。因此对于 FTP 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数据连接无法建立。

1.2 ASPF配置任务简介

表1-1 ASPF 配置任务简介

配置任务	说明	详细配置
配置ASPF策略	必选	1.3
在接口上应用ASPF策略	必选	1.4

1.3 配置ASPF策略

配置 ASPF 策略时，请遵循以下配置指导：

- 在未配置应用层协议检测，直接配置 TCP 或 UDP 检测的情况下，可能会产生接收不到应答报文的情况，故建议应用层检测和 TCP/UDP 检测配合使用。
- 对于单通道协议，如 Telnet 应用，直接配置通用 TCP 检测即可实现 ASPF 功能。

表1-2 配置 ASPF 策略

操作	命令	说明
进入系统视图	**system-view**	-
创建ASPF策略，并进入ASPF策略视图	**aspf policy** *aspf-policy-number*	缺省情况下，不存在ASPF策略
（可选）为应用层或传输层协议配置ASPF检测	**detect** { **dccp** | **ftp** | **gtp** | **h323** | **icmp** | **icmpv6** | **ils** | **mgcp** | **nbt** | **pptp** | **rawip** | **rsh** | **rtsp** | **sccp** | **sctp** | **sip** | **sqlnet** | **tcp** | **tftp** | **udp** | **udp-lite** | **xdmcp** }	缺省情况下，未配置应用层和传输层协议的ASPF检测
（可选）开启ICMP差错报文丢弃功能	**icmp-error drop**	缺省情况下，不丢弃ICMP差错报文
（可选）开启非SYN的TCP首报文丢弃功能	**tcp syn-check**	缺省情况下，不丢弃非SYN的TCP首报文

1.4 在接口上应用ASPF策略

只有将定义好 ASPF 策略应用到接口的出或入方向上，才能对通过接口的特定方向的流量进行检测。在处理入接口报文时需要查找对应接口入方向的策略；在处理出接口报文时需要查找对应接口出方向的策略。如果接口应用了 ASPF 策略，所有进入或离开该接口的报文都需要与会话表项进行匹配，查找不到与之匹配的会话表项时会触发创建会话表。

如果 ASPF 与包过滤防火墙协同工作，可以在外部接口或内部接口的入方向或出方向上配置特定的 ASPF 和包过滤策略，根据特定配置，可以拒绝外部网络上的用户对内部网络的主动访问，但内部网络的用户访问外部网络时，返回的报文可以按照外部接口出方向或内部接口入方向上的 ASPF 配置进行 ASPF 检测。

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方发送的报文和响应端返回的报文经过同一接口。

表1-3 在接口上应用 ASPF 策略

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
在接口上应用ASPF策略	**aspf apply policy** *aspf-policy-number* { **inbound** | **outbound** }	缺省情况下，接口上没有应用ASPF策略

1.5 ASPF显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 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 **reset** 命令可以清除 ASPF 的统计信息。

表1-4 ASPF 显示和维护

操作	命令
查看ASPF策略配置信息及接口应用ASPF策略的信息	**display aspf all**
查看接口上的ASPF策略信息	**display aspf interface**
查看ASPF策略的配置信息	**display aspf policy** *aspf-policy-number*
查看ASPF的会话表信息	**display aspf session** [**ipv4** | **ipv6**] [**verbose**]
删除ASPF的会话表	**reset aspf session** [**ipv4** | **ipv6**]

1.6 ASPF典型配置举例

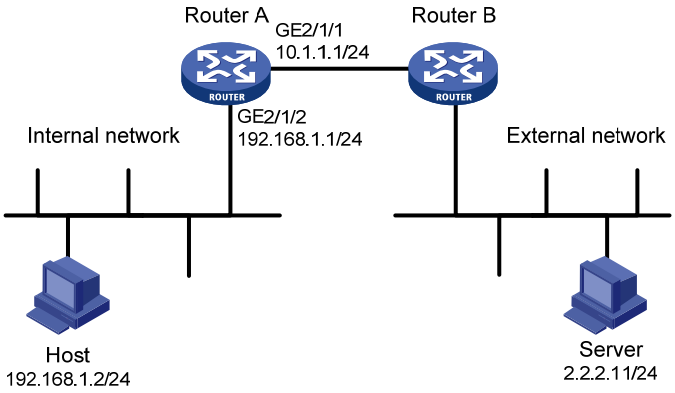
1.6.1 检测FTP应用的ASPF典型配置举例

1. 组网需求

Router A 为连接内部网络与外部网络的边界设备，内部网络中的本地用户需要访问外部网络提供的 FTP 服务。要求配置 ASPF 策略，检测通过 Router A 的 FTP 流量。如果该报文是内部网络用户发起的 FTP 连接的返回报文，则允许其通过 Router A 进入内部网络，其它报文被禁止。

2. 组网图

图1-3 检测 FTP 应用的 ASPF 典型配置组网图



3. 配置步骤

配置 ACL 3111，定义规则：拒绝所有 IP 流量进入内部网络。

```
<RouterA> system-view
[RouterA] acl number 3111
[RouterA-acl-adv-3111] rule deny ip
[RouterA-acl-adv-3111] quit
```

创建 ASPF 策略 1，配置检测应用层协议 FTP。

```
[RouterA] aspf policy 1
[RouterA-aspf-policy-1] detect ftp
[RouterA-aspf-policy-1] quit
```

在接口 GigabitEthernet2/1/1 的入方向上应用包过滤策略，拒绝所有 IP 流量进入内部网络。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] packet-filter 3111 inbound
```

在接口 GigabitEthernet2/1/1 的出方向上应用 ASPF 策略，ASPF 会为内部网络和外部网络之间的 FTP 连接创建会话表项，并允许匹配该表项的外部网络返回报文进入内部网络。

```
[RouterA-GigabitEthernet2/1/1] aspf apply policy 1 outbound
```

4. 验证配置

以上配置完成后，从 Host 向 Server 发起的 FTP 连接可正常建立，而从外部网络发起连接的报文则无法进入内部网络。在 Router A 上可以查看到已经建立的 ASPF 会话。

```
<RouterA> display aspf session ipv4
Initiator:
  Source      IP/port: 192.168.1.2/1877
  Destination IP/port: 2.2.2.11/21
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)

Total sessions found: 1
```

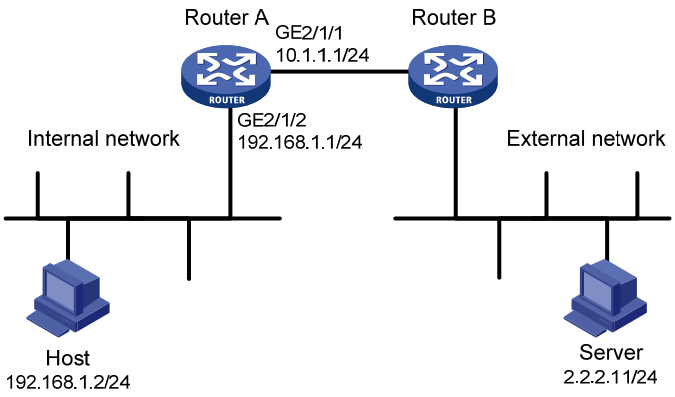
1.6.2 检测ICMP和SYN报文的ASPF典型配置举例

1. 组网需求

Router A 为连接内部网络与外部网络的边界设备，内部网络中的本地用户需要访问外部网络。为避免来自外部网络的 ICMP 和 SYN 报文的恶意攻击，要求在 Router A 上配置 ASPF 策略，实现 ICMP 差错报文检测及 TCP 非 SYN 首报文丢弃功能。

2. 组网图

图1-4 检测 ICMP 和 SYN 报文的 ASPF 典型配置组网图



3. 配置步骤

配置 ACL 3111，定义规则：拒绝所有 IP 流量进入内部网络。

```
<RouterA> system-view
[RouterA] acl number 3111
[RouterA-acl-adv-3111] rule deny ip
[RouterA-acl-adv-3111] quit
```

创建 ASPF 策略 1。

```
[RouterA] aspf policy 1
```

设置 ASPF 策略 1 丢弃 ICMP 差错报文。

```
[RouterA-aspf-policy-1] icmp-error drop
```

设置 ASPF 策略 1 丢弃非 SYN 的 TCP 首报文。

```
[RouterA-aspf-policy-1] tcp syn-check
[RouterA-aspf-policy-1] quit
```

在接口 GigabitEthernet2/1/1 的入方向上应用包过滤策略，拒绝所有 IP 流量进入内部网络。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] packet-filter 3111 inbound
```

在接口 GigabitEthernet2/1/1 的出方向上应用 ASPF 策略。

```
[RouterA-GigabitEthernet2/1/1] aspf apply policy 1 outbound
```

4. 验证配置

查看策略号为 1 的 ASPF 策略的配置信息。

```
<RouterA> display aspf policy 1
ASPF policy configuration:
  Policy number: 1
```

```
Enable ICMP error message check
Enable TCP SYN packet check
Detect these protocols:
```

通过以上配置，Router A 能够识别出来自网络中伪造的 ICMP 差错报文，可以避免 ICMP 的恶意攻击，而且非 SYN 报文的 TCP 首包也将被丢弃。

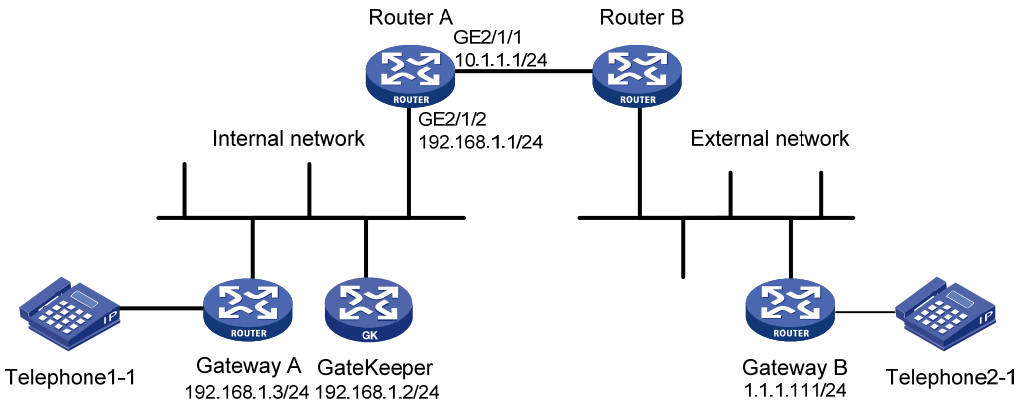
1.6.3 ASPF支持H.323 应用典型配置举例

1. 组网需求

在如 图 1-5 所示的一种常见的H.323 典型组网应用中，Router A为连接内部网络与外部网络的边界设备，外部网络中的Gateway B需要访问内部网络中的H.323 GateKeeper，并通过GateKeeper的协助，与内网中的H.323 端点Gateway A建立呼叫连接。要求配置ASPF策略，检测通过Router A的H.323 协议报文，允许外部网络设备主动访问内部网络的GateKeeper，并通过与其协商进而实现访问Gateway A，其它协议的外部网络报文均被禁止。

2. 组网图

图1-5 ASPF 支持 H.323 典型配置组网图



3. 配置步骤

配置 ACL 3200，定义规则：拒绝所有除访问 GateKeeper 之外的 IP 流量进入内部网络。

```
<RouterA> system-view
[RouterA] acl number 3200
[RouterA-acl-adv-3200] rule 0 permit ip destination 192.168.1.2 0
[RouterA-acl-adv-3200] rule 5 deny ip
[RouterA-acl-adv-3200] quit
```

创建 ASPF 策略 1，配置检测应用层协议 H.323。

```
[RouterA] aspf policy 1
[RouterA-aspf-policy-1] detect h323
[RouterA-aspf-policy-1] quit
```

在接口 GigabitEthernet2/1/1 的入方向上应用包过滤策略，拒绝所有除访问 GateKeeper 之外的流量进入内部网络。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] packet-filter 3200 inbound
```

在接口 GigabitEthernet2/1/1 的入方向上应用 ASPF 策略，ASPF 会为内部网络和外部网络之间的 H.323 连接创建会话表项，并允许匹配该表项的外部网络返回报文进入内部网络。

```
[RouterA-GigabitEthernet2/1/1] aspf apply policy 1 inbound
[RouterA-GigabitEthernet2/1/1] quit
```

4. 验证配置

以上配置完成后，从 Gateway B 向 GateKeeper 发起的 H.323 连接以及从 Gateway B 向 Gateway A 发起的 H323 连接均可正常建立，但外部网络发起的其它协议的报文则无法进入内部网络。在 Router A 上可以查看到已经建立的 ASPF 会话。

```
[RouterA] display aspf session ipv4
Initiator:
  Source      IP/port: 1.1.1.111/33184
  Destination IP/port: 192.168.1.3/32828
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: UDP(17)

Initiator:
  Source      IP/port: 1.1.1.111/1719
  Destination IP/port: 192.168.1.2/1719
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: UDP(17)

Initiator:
  Source      IP/port: 1.1.1.111/3521
  Destination IP/port: 192.168.1.2/20155
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)

Initiator:
  Source      IP/port: 1.1.1.111/33185
  Destination IP/port: 192.168.1.3/32829
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: UDP(17)

Initiator:
  Source      IP/port: 1.1.1.111/3688
  Destination IP/port: 192.168.1.2/1720
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)

Total sessions found: 5
```

目 录

1 APR配置

1.1 APR简介

APR（Application Recognition）即应用层协议识别。一些基于应用的业务（例如 QoS，ASPF）在进行报文处理时需要知道报文所属的应用层协议，APR 可以为这样的业务提供应用识别服务，并能够对接口上接收或者发送的某个应用层协议的报文进行数目和速率统计。APR 为了更好地识别报文所属的应用层协议，提供了两种应用识别方法：基于端口的应用识别和基于内容特征的应用识别。

- PBAR（Port Based Application Recognition，基于端口的应用层协议识别）：根据定义的应用层协议端口与应用的映射关系识别报文所属的应用层协议。
- 基于内容特征的应用层协议识别：提取应用报文区别于其它应用报文的特征，通过将报文的内容与特征库中的特征项进行匹配来识别报文所属的应用层协议。这种识别方式目前还不支持。

下文中的应用均指设备可以通过 APR 识别出的应用层协议。应用分为预定义应用和自定义应用两种：预定义应用由系统缺省创建；自定义应用由用户通过配置创建。

1.1.1 PBAR

PBAR（Port Based Application Recognition，基于端口的应用层协议识别）根据预定义的、自定义的端口与应用的映射关系识别出应用层协议。预定义的端口与应用的映射关系由系统预先定义，自定义的端口与应用的映射关系由用户配置进行创建。

PBAR 提供了以下两种映射机制来维护和使用自定义的端口与应用映射关系：

- 通用端口映射：对用户自定义端口号和应用层协议建立映射关系。例如：将 2121 端口映射为 FTP 协议，这样所有目的端口是 2121 的报文将被识别为 FTP 报文。
- 主机端口映射：对去往某些特定范围内主机的报文建立自定义端口号和应用层协议的映射。例如：将目的地址为 10.110.0.0/16 网段的、使用 2121 端口的报文映射为 FTP 报文。主机范围可以通过配置 ACL 或者指定主机地址、网段来确定。

1.1.2 应用组

可以将具有相似特征的应用添加到一个应用组中。一个应用组，就是若干个应用的集合。如果报文被识别为属于某个应用，而该应用又属于某个应用组，则报文相当于被识别为属于某个应用组。基于应用的业务可以对属于同一个应用组的报文做统一处理。

应用组分为预定义和自定义两种：预定义应用组由系统预先定义并包含了指定的预定义应用；自定义应用组由用户通过配置创建。一个自定义应用组中可以包含多个预定义应用和自定义应用。

1.2 配置PBAR

根据与应用层协议进行映射的对象范围的不同，可以将端口映射的配置分为以下四类：

- 通用端口映射：对于所有报文，建立端口号与应用层协议的映射关系；
- 基于 ACL 的主机端口映射：对于匹配指定 ACL 的报文，建立端口号与应用层协议的映射关系；

- 基于网段的主机端口映射：对于目的地址为指定网段的报文，建立端口号与应用层协议的映射关系；
- 基于 IP 地址的主机端口映射：对于目的地址为指定 IP 地址的报文，建立端口号与应用层协议的映射关系。

以上四类端口映射配置对于同一个报文的生效优先级从高到低依次为：基于 IP 地址、基于网段、基于 ACL、通用。而对于其中的每一类，指定传输层协议名称的配置优先级高于不指定传输层协议名称的配置。

表1-1 配置 PBAR

操作	命令	说明
进入系统视图	**system-view**	-
配置通用端口映射	**port-mapping application** *application-name* **port** *port-number* [**protocol** *protocol-name*]	至少选其一 缺省情况下，各应用层协议与其对应的知名端口号映射 配置映射关系时，如果指定的应用不存在就会创建这个应用
配置基于ACL的主机端口映射	**port-mapping application** *application-name* **port** *port-number* [**protocol** *protocol-name*] **acl** [**ipv6**] *acl-number*	
配置基于网段的主机端口映射	**port-mapping application** *application-name* **port** *port-number* [**protocol** *protocol-name*] **subnet** { **ip** *ipv4-address* { *mask-length* | *mask* } | **ipv6** *ipv6-address prefix-length* } [**vpn-instance** *vpn-instance-name*]	
配置基于IP地址的主机端口映射	**port-mapping application** *application-name* **port** *port-number* [**protocol** *protocol-name*] **host** { **ip** | **ipv6** } *start-ip-address* [*end-ip-address*] [**vpn-instance** *vpn-instance-name*]	

1.3 配置应用组

可以将具有相似特征的应用添加到一个应用组中或将一个应用组中的应用拷贝到另一个组中。设备最多可支持配置 65536 个应用组，每个应用组里最多可以包含 65536 个自定义应用。

表1-2 配置 APR 应用组

操作	命令	说明
进入系统视图	**system-view**	-
创建应用组，并进入应用组视图	**app-group** *group-name*	缺省情况下，系统中存在若干预定义应用组，可通过**display app-group pre-defined**命令查看 预定义的应用组不允许修改和删除
（可选）为自定义的应用组设置描述信息	**description** *group-description*	缺省情况下，自定义应用组的描述信息为“User-defined application group”

操作	命令	说明
在应用组中添加应用	**include application** *application-name*	缺省情况下，自定义应用组中不包含任何应用 可以通过多次执行本命令添加多个应用 添加应用时，如果对应的应用不存在就会创建这个应用
在应用组中拷贝另一个应用组中的所有应用	**copy app-group** *group-name*	可以通过多次执行本命令拷贝多个应用组里的应用

1.4 配置接口的应用统计功能

提示

接口的应用统计功能会消耗大量系统内存。当系统出现内存告警时，请关闭接口的应用统计功能。

在接口上开启应用统计功能之后，设备能够对接口上收到或者发送的报文的数目、速率按照应用层协议分别进行统计，生成的统计信息可以通过 **display application statistics** 命令查看。

表1-3 配置接口的应用统计功能

操作	命令	说明
进入系统视图	**system-view**	-
进入三层接口视图	**interface** *interface-type interface-number*	-
开启接口的应用统计功能	**application statistics enable** [**inbound** | **outbound**]	缺省情况下，接口的应用统计功能处于关闭状态 可以同时开启接口两个方向上的应用统计功能

1.5 APR显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 APR 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** 命令可以清除 APR 的统计信息。

表1-4 APR 显示和维护

操作	命令
显示应用信息	**display application** [**name** *application-name* | **pre-defined** | **user-defined**]
显示应用组信息	**display app-group** [**name** *group-name* | **pre-defined** | **user-defined**]

操作	命令
显示接口上的应用统计信息	**display application statistics** [**direction** { **inbound** | **outbound** } | **interface** *interface-type interface-number* | **name** *application-name*] *
按指定类型的统计排名显示接口应用统计信息	**display application statistics top** *number* { **bps** | **bytes** | **packets** | **pps** } **interface** *interface-type interface-number*
显示预定义的端口映射信息	**display port-mapping pre-defined**
显示自定义的端口映射信息	**display port-mapping user-defined** [**application** *application-name* | **port** *port-number*]
清除指定接口或所有接口的应用统计信息	**reset application statistics** [**interface** *interface-type interface-number*]

1.6 APR典型配置举例

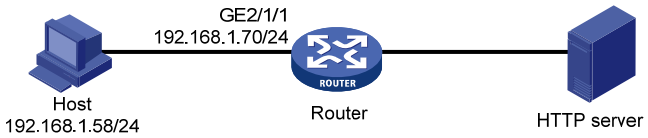
1.6.1 APR典型配置举例

1. 组网需求

主机通过 Router 与外网相连，通过配置 Router 实现丢弃主机向外部网络发送的目的端口为 8080 的 HTTP 连接报文。

2. 组网图

图1-1 APR 典型配置组网图



3. 配置步骤

创建应用组 group1，并进入应用组视图。

```
<Router> system-view
[Router] app-group group1
```

添加 HTTP 应用。

```
[Router-app-group-group1] include application http
[Router-app-group-group1] quit
```

配置 HTTP 应用层协议与 TCP 协议、端口 8080 之间的映射。

```
[Router] port-mapping application http port 8080 protocol tcp
```

定义类 classifier_1，匹配应用组 group1。

```
[Router] traffic classifier classifier_1
[Router-classifier-classifier_1] if-match app-group group1
[Router-classifier-classifier_1] quit
```

定义流行为 bdeny，动作为流量过滤（**deny**），对数据包进行丢弃。

```
[Router] traffic behavior bdeny
```

```
[Router-behavior-bdeny] filter deny
[Router-behavior-bdeny] quit
```

定义策略 1，为类 classifier_1 指定流行为 bdeny。

```
[Router] qos policy 1
[Router-qospolicy-1] classifier classifier_1 behavior bdeny
[Router-qospolicy-1] quit
```

在 GigabitEthernet2/1/1 入方向上应用 QoS 策略。

```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] qos apply policy 1 inbound
[Router-GigabitEthernet2/1/1] quit
```

4. 验证配置

以上配置完成后，主机将不能与外部网络建立 HTTP 连接。

目 录

1 会话管理

1.1 会话管理简介

会话管理是为了实现NAT（Network Address Translation，网络地址转换）、ASPF（Advanced Stateful Packet Filter，高级状态包过滤）、攻击检测及防范等基于会话进行处理的业务而抽象出来的公共功能。此功能把传输层报文之间的交互关系抽象为会话，并根据发起方和响应方的报文信息对会话进行状态更新和老化，支持多个业务特性分别对同一个业务报文进行处理。

会话管理实现的主要功能包括：

- 报文到会话的快速匹配；
- 传输层协议状态的管理；
- 报文应用层协议类型的识别；
- 按照协议状态或应用层协议类型对会话进行老化；
- 支持指定的会话维持较为长时间的连接；
- 为需要进行端口协商的应用层协议提供特殊的报文匹配；
- 支持对 ICMP/ICMPv6 差错控制报文的解析以及根据解析结果进行会话的匹配。

1.1.1 会话管理的工作原理

会话管理主要基于传输层协议对报文进行检测。其实质是通过检测传输层协议信息来对连接的状态进行跟踪，并对所有连接的状态信息进行基于会话表和关联表的统一维护和管理。

客户端向服务器发起连接请求报文的时候，系统会创建一个会话表项。该表项中记录了一个会话所对应的请求报文信息和回应报文信息，包括源 IP 地址/端口号、目的 IP 地址/端口号、传输层协议类型、应用层协议类型、会话的协议状态等。对于多通道协议（特指部分应用协议中，客户端与服务器之间需要在已有连接基础上协商新的连接来完成一个应用），会话管理还会根据协议的协商情况，创建一个或多个（由具体的应用协议决定）关联表表项，用于关联属于同一个应用的不同会话。关联表项在多通道协议协商的过程中创建，完成对多通道协议的支持后即被删除。

在实际应用中，会话管理作为公共功能，只能实现连接状态的跟踪，并不能阻止潜在的攻击报文通过。会话管理配合 ASPF 特性，可实现根据连接状态信息动态地决定是否允许数据包通过防火墙进入内部区域，以便阻止恶意的入侵。

1.1.2 会话管理在设备上的实现

目前会话管理在设备上实现的具体功能如下：

- 支持对各协议报文创建会话、更新会话状态以及根据协议状态设置老化时间。
- 支持应用层协议的端口映射（参见“安全配置指导”中的“APR”），允许为应用层协议自定义对应的非通用端口号，同时可以根据应用层协议设置不同会话老化时间。
- 支持 ICMP/ICMPv6 差错报文的映射，可以根据 ICMP/ICMPv6 差错报文携带的信息查找原始的会话。
- 支持设置长连接会话，保证指定的会话在一段较长的时间内不会被老化。

- 支持应用层协议（如 FTP）的控制通道和动态数据通道的会话管理。

1.2 配置会话管理

会话管理支持的配置包括：协议状态的会话老化时间、应用层协议的会话老化时间、长连接会话规则及删除会话。这些配置可根据实际应用需求选择进行，配置无先后顺序的要求，相互不关联。

长连接老化时间仅在 TCP 会话进入稳态（TCP-EST 状态）时生效。在会话稳态时，长连接老化时间具有最高的优先级，其次为应用层协议老化时间，最后为协议状态老化时间。

1.2.1 配置协议状态会话老化时间

提示

当会话数目过多时（大于 80 万条），建议不要将协议状态老化时间设置得过短，否则会造成设备响应速度过慢。

以下配置用于实现根据会话所处协议状态来设置会话表项的老化时间。处于某协议状态的会话，如果在该协议状态老化时间内未被任何报文匹配，则会由于老化而被系统自动删除。

表1-1 配置各协议状态的会话老化时间

操作	命令	说明
进入系统视图	**system-view**	-
配置各协议状态的会话老化时间	**session aging-time state** { **fin** | **icmp-reply** | **icmp-request** | **rawip-open** | **rawip-ready** | **syn** | **tcp-est** | **udp-open** | **udp-ready** } *time-value*	缺省情况下，各协议状态的会话老化时间为： • **syn**：30 秒 • **tcp-est**：3600 秒 • **fin**：30 秒 • **udp-open**：30 秒 • **udp-ready**：60 秒 • **icmp-request**：60 秒 • **icmp-reply**：30 秒 • **rawip-open**：30 秒 • **rawip-ready**：60 秒

1.2.2 配置应用层协议会话老化时间

提示

- 当会话数目过多时（大于 80 万条），建议不要将应用层协议会话的老化时间设置得过短，否则会造成设备响应速度过慢。
- 老化时间的修改需要结合实际的使用场景，避免过大或过小，从而影响会话协议报文的正常交互。例如，FTP 协议的会话老化时间若小于 FTP 保活报文发送的间隔，会造成 FTP 连接无法正常建立。

对于进入稳定状态的会话（TCP 会话进入 TCP-EST 状态，UDP 会话进入 UDP-READY 状态），还可以根据会话所属的应用层协议类型设置老化时间。此类会话表项如果在一定时间内未被任何报文匹配，则会按照设置的应用层协议会话老化时间老化。对于进入稳定状态的其它应用层协议的会话表项，则仍然遵循协议状态的会话老化时间进行老化。

表1-2 配置应用层协议会话老化时间

操作	命令	说明
进入系统视图	**system-view**	-
配置应用层协议的会话老化时间	**session aging-time application** { **dns** | **ftp** | **gtp** | **h225** | **h245** | **ils** | **mgcp** | **nbt** | **pptp** | **ras** | **rsh** | **rtsp** | **sccp** | **sip** | **sqlnet** | **tftp** | **xdmcp** } *time-value*	缺省情况下，各协议的会话老化时间如下： • DNS：60 秒 • FTP：3600 秒 • GTP：60 秒 • H.225：3600 秒 • H.245：3600 秒 • RAS：300 秒 • RTSP：3600 秒 • SIP：3600 秒 • TFTP：60 秒 • ILS：3600 秒 • MGCP：60 秒 • NBT：3600 秒 • PPTP：3600 秒 • RSH：60 秒 • SCCP：3600 秒 • SQLNET：600 秒 • XDMCP：3600 秒

1.2.3 配置长连接会话规则

针对进入 TCP-EST 状态的 TCP 会话，用户可以根据需要将符合指定特征的 TCP 会话设置为长连接会话。长连接会话的老化时间不会随着状态的变迁而更改，可以将其设置得比普通会话的老化时间更长，或者设置成永不老化。被设置成永不老化的长连接会话，只有当会话的发起方或响应方主动发起关闭连接请求或管理员手动删除该会话时，才会被删除。

表1-3 配置长连接会话规则

操作	命令	说明
进入系统视图	**system-view**	-
配置长连接会话规则	**session persistent acl** [**ipv6**] *acl-number* [**aging-time** *time-value*]	缺省情况下，无长连接会话规则

1.3 配置会话日志

会话日志是为满足网络管理员安全审计的需要，对用户的访问信息、用户 IP 地址的转换信息、用户的网络流量信息等进行记录，并可采用日志的格式发送给日志主机或者输出到信息中心。

存活时间或收发数目达到一定阈值的会话才会以日志的形式进行记录并输出，该阈值包括以下两种类型：

- 时间阈值：当一个会话存在的时间达到设定的时间阈值时，输出会话日志。
- 流量阈值：分为报文数阈值和字节数阈值两种。当一个会话收发的报文数或字节数达到设定的流量阈值时，输出会话日志。

同时配置了时间阈值和流量阈值的情况下，只要有一个阈值到达，就会输出相应的会话日志，并将所有的阈值统计信息清零。

同时只能有一种流量阈值有效，以最后一次配置的阈值类型为准，例如，先配置报文数阈值再配置字节数阈值，则当前有效的阈值是字节数阈值，只会输出达到字节数阈值的会话日志。

在未指定相关阈值（流量阈值、时间阈值）的情况下，若会话日志功能处于使能状态，则仅在会话表创建和删除的时候分别输出一次会话日志。

表1-4 配置会话日志功能

操作		命令	说明
进入系统视图		**system-view**	-
（可选）配置输出会话日志的时间阈值		**session log time-active** *time-value*	缺省情况下，不依据时间阈值发送会话日志
（可选）配置输出会话日志的流量阈值	配置报文数流量阈值	**session log packets-active** *packets-value*	缺省情况下，不依据报文数流量阈值发送会话日志
	配置字节数流量阈值	**session log bytes-active** *bytes-value*	缺省情况下，不依据字节数流量阈值发送会话日志
进入接口视图		**interface** *interface-type interface-number*	-
使能会话日志功能		**session log enable** { **ipv4** | **ipv6** } [**acl** *acl-number*] { **inbound** | **outbound** }	缺省情况下，会话日志功能处于关闭状态

1.4 会话管理显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后会话的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除会话统计信息。

表1-5 会话管理显示和维护

操作	命令
显示应用层协议的会话老化时间	**display session aging-time application**
显示各协议状态的会话老化时间	**display session aging-time state**
显示IPv4会话表信息（MSR 2600/MSR 3600）	**display session table** { **ipv4** | **ipv6** } [**source-ip** *source-ip*] [**destination-ip** *destination-ip*] [**verbose**]
显示IPv4会话表信息（MSR 5600）	**display session table** { **ipv4** | **ipv6** } [**slot** *slot-number*] [**source-ip** *source-ip*] [**destination-ip** *destination-ip*] [**verbose**]
显示会话统计信息（MSR 2600/MSR 3600）	**display session statistics**
显示会话统计信息（MSR 5600）	**display session statistics** [**slot** *slot-number*]
显示关联表信息（MSR 2600/MSR 3600）	**display session relation-table** { **ipv4** | **ipv6** }
显示关联表信息（MSR 5600）	**display session relation-table** { **ipv4** | **ipv6** } [**slot** *slot-number*]
删除IPv4会话表项（MSR 2600/MSR 3600）	**reset session table ipv4** [**destination-ip** *destination-ip*] [**destination-port** *destination-port*] [**protocol** { **dccp** | **icmp** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }] [**source-ip** *source-ip*] [**source-port** *source-port*] [**vpn-instance** *vpn-instance-name*]
删除IPv4会话表项（MSR 5600）	**reset session table ipv4** [**destination-ip** *destination-ip*] [**destination-port** *destination-port*] [**protocol** { **dccp** | **icmp** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }] [**slot** *slot-number*] [**source-ip** *source-ip*] [**source-port** *source-port*] [**vpn-instance** *vpn-instance-name*]
删除IPv6会话表项（MSR 2600/MSR 3600）	**reset session table ipv6** [**destination-ip** *destination-ip*] [**destination-port** *destination-port*] [**protocol** { **dccp** | **icmpv6** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }] [**source-ip** *source-ip*] [**source-port** *source-port*] [**vpn-instance** *vpn-instance-name*]
删除IPv6会话表项（MSR 5600）	**reset session table ipv6** [**destination-ip** *destination-ip*] [**destination-port** *destination-port*] [**protocol** { **dccp** | **icmpv6** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }] [**slot** *slot-number*] [**source-ip** *source-ip*] [**source-port** *source-port*] [**vpn-instance** *vpn-instance-name*]
删除所有会话项（MSR 2600/MSR 3600）	**reset session table**
删除所有会话项（MSR 5600）	**reset session table** [**slot** *slot-number*]
清除会话统计信息（MSR 2600/MSR 3600）	**reset session statistics**
清除会话统计信息（MSR 5600）	**reset session statistics** [**slot** *slot-number*]

操作	命令
删除关联表项（MSR 2600/MSR 5600）	**reset session relation-table** [**ipv4** | **ipv6**]
删除关联表项（MSR 5600）	**reset session relation-table** [**ipv4** | **ipv6**] [**slot** *slot-number*]

目 录

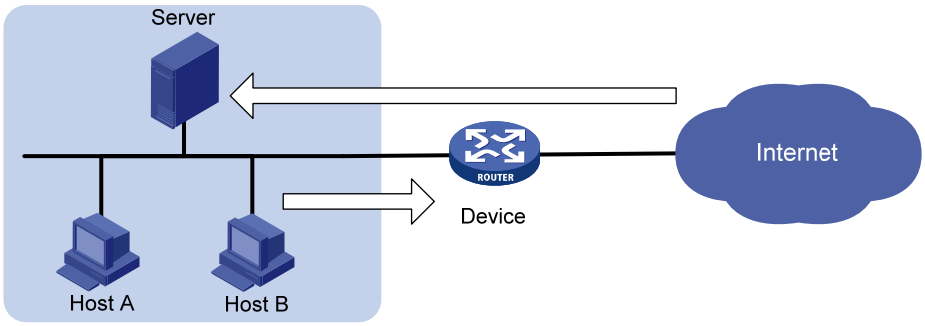
1 连接数限制

1.1 连接数限制简介

图 1-1 所示的组网环境中，通常会遇到以下两类网络问题：某内网用户在短时间内经过设备向外部网络发起大量连接，导致设备系统资源迅速消耗，其它内网用户无法正常使用网络资源；某内部服务器在短时间内接收到大量的连接请求，导致该服务器忙于处理这些连接请求，以至于不能再接受其它客户端的正常连接请求。

连接数限制通过对设备上建立的连接数进行统计和限制，能够有效解决以上问题，实现保护内部网络资源（主机或服务器）以及合理分配设备系统资源的目的。

图1-1 连接数限制组网应用示意图



1.2 连接数限制配置任务简介

表1-1 连接数限制配置任务简介

配置任务	说明	详细配置
创建连接数限制策略	必选	1.3
配置连接数限制策略	必选	1.4
应用连接数限制策略	必选	1.5

1.3 创建连接数限制策略

连接数限制策略用于定义具体的连接数限制规则，其中的规则规定了策略生效的范围和实施的参数。

表1-2 创建连接数限制策略

操作	命令	说明
进入系统视图	**system-view**	-
创建连接数限制策略，并进入连接数限制策略视图	**connection-limit { ipv6-policy | policy }** *policy-id*	缺省情况下，不存在任何连接数限制策略

1.4 配置连接数限制策略

一个连接数限制策略中可定义多条连接数限制规则，每条连接数限制规则中指定一个连接数限制的用户范围，属于该范围的用户可建立的连接数将受到该规则中指定参数的限制。当某类型的连接数达到上限值（*max-amount*）时，设备将不接受该类型的新建连接请求，直到设备上已有连接因老化而删除，使得当前该类型的连接数低于连接数下限（*min-amount*）后，才允许新建连接。对于未匹配连接数限制规则的用户所建立的连接，设备不对其连接数进行限制。

目前，连接数限制支持根据 ACL 来限定用户范围，对匹配 ACL 规则的用户连接数进行统计和限制。

设备对于某一范围内的用户连接，可根据不同的控制粒度，按照如下三种类型进行连接数限制：

- **per-destination**：按目的 IP 地址统计和限制，即到同一个目的 IP 地址的连接数目将受到指定阈值的限制。
- **per-service**：按服务统计和限制，即同一种服务（具有相同传输层协议和服务端口）的连接数目受限将受到指定阈值的限制。
- **per-source**：按源地址统计和限制，即同一个源 IP 地址发起的连接数目受限将受到指定阈值的限制。

如果在一条规则中同时指定 **per-destination**、**per-service**、**per-source** 类型中的多个，则多种统计和限制类型同时生效。例如，同时指定 **per-destination** 和 **per-service** 类型，则表示对到同一个目的地址的同一种服务的连接数进行统计和限制。若一条规则中不指定以上任何一种限制类型，则表示指定范围内的所有用户连接将整体受到指定的阈值限制。

对设备上建立的连接与某连接数限制策略进行匹配时，将按照规则编号从小到大的顺序依次遍历该策略中的所有规则，因此在配置连接限制规则时，需要从整体策略考虑，根据各规则的内容来合理安排规则的编号顺序，推荐按照限制粒度和范围由小到大的顺序来设置规则序号。

表1-3 配置连接数限制策略

操作	命令	说明
进入系统视图	**system-view**	-
进入连接数限制策略视图	**connection-limit** { **ipv6-policy** | **policy** } *policy-id*	-
配置连接数限制规则	**limit** *limit-id* **acl** [**ipv6**] { *acl-number* | **name** *acl-name* } [**per-destination** | **per-service** | **per-source**] * **amount** *max-amount min-amount*	缺省情况下，连接数策略中不存在任何规则 本命令的**ipv6**参数仅在IPv6连接数限制策略视图下存在

1.5 应用连接数限制策略

将已经配置好的连接数限制策略应用到全局或不同的接口上，实现对用户的连接数限制。接口上应用的连接数限制策略仅对本接口上处理的指定连接生效，全局应用的连接数限制策略对本设备处理的所有指定的连接生效。

如果在入接口、全局和出接口上分别应用了不同的连接数限制策略，则经过设备的连接将会依次受到入接口、全局、出接口连接数限制策略的多重限制，只要该连接的数目达到任何一处连接数上限，都不允许新建连接。

表1-4 在接口上应用连接数限制策略

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
在接口上应用连接限制策略	**connection-limit apply** { **ipv6-policy** | **policy** } *policy-id*	缺省情况下，接口上没有应用任何连接数限制策略 同一个接口上同时只能应用一个IPv4连接数限制策略和一个IPv6连接数限制策略，后配置的IPv4或IPv6连接数限制策略会覆盖已配置的对应类型的策略

表1-5 全局应用连接限制策略

操作	命令	说明
进入系统视图	**system-view**	-
全局应用连接限制策略	**connection-limit apply global** { **ipv6-policy** | **policy** } *policy-id*	缺省情况下，全局没有应用任何连接数限制策略 全局最多只能应用一个IPv4连接数限制策略和一个IPv6连接数限制策略，后配置的IPv4或IPv6连接数限制策略会覆盖已配置的对应类型的策略

1.6 连接数限制显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示连接数限制配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令清除连接数限制的相关信息。

表1-6 连接数限制显示和维护

操作	命令
显示连接数限制策略的配置信息	**display connection-limit** { **ipv6-policy | policy** } { **all** | *policy-id* }
显示连接数限制在全局或接口的统计信息（MSR 2600/MSR 3600）	**display connection-limit statistics** { **global** | **interface** *interface-type interface-number* }
显示连接数限制在全局或接口的统计信息（MSR 5600）	**display connection-limit statistics** { **global** | **interface** *interface-type interface-number* } [**slot** *slot-number*]

操作	命令
显示连接数限制在全局或接口的的统计节点列表（MSR 2600/MSR 3600）	**display connection-limit** { **ipv6-stat-nodes** | **stat-nodes** } { **global** | **interface** *interface-type interface-number* } [**destination** *destination-ip* | **service-port** *port-number* | **source** *source-ip*] * [**count**]
显示连接数限制在全局或接口的的统计节点列表（MSR 5600）	**display connection-limit** { **ipv6-stat-nodes** | **stat-nodes** } { **global** | **interface** *interface-type interface-number* } [**slot** *slot-number*] [**destination** *destination-ip* | **service-port** *port-number* | **source** *source-ip*] * [**count**]
清除连接数限制在全局或接口的统计信息（MSR 2600/MSR 3600）	**reset connection-limit statistics** { **global** | **interface** *interface-type interface-number* }
清除连接数限制在全局或接口的统计信息（MSR 5600）	**reset connection-limit statistics** { **global** | **interface** *interface-type interface-number* } [**slot** *slot-number*]

1.7 连接数限制典型配置举例

1.7.1 连接数限制典型配置举例

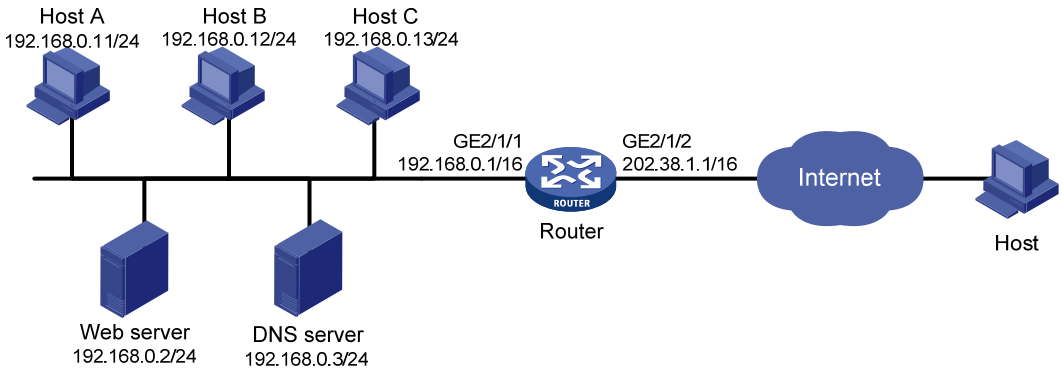
1. 组网需求

某公司拥有 202.38.1.1/24 至 202.38.1.5/24 五个公网 IP 地址，内部网络地址为 192.168.0.0/16。通过配置 NAT 使得内部网络主机可以访问 Internet，并提供两台内部服务器供外网访问。为保护内部网络及网络资源，需要进行以下限制：

- 192.168.0.0/24 网段的全部主机总共最多只能与外网建立 100000 条连接。
- 192.168.0.0/24 网段的每台主机最多只能与外网建立 100 条连接。
- 最多允许 10000 个 DNS 客户端同时向 DNS 服务器发送查询请求。
- 最多允许 10000 个 Web 客户端同时向 Web 服务器发送连接请求。

2. 组网图

图1-2 连接限制典型配置组网



3. 配置步骤

说明

内网主机访问外部网络的 NAT 配置和内部服务器的配置请参见“三层技术-IP 业务配置指导”中的“NAT”，此处不进行介绍，下面仅对连接限制的配置步骤进行详细描述。

创建 ACL 3000，定义允许内网所有主机发送的报文通过。

```
<Router> system-view
[Router] acl number 3000
[Router-acl-adv-3000] rule permit ip source 192.168.0.0 0.0.0.255
[Router-acl-adv-3000] quit
```

创建 ACL 3001，定义允许访问 Web Server 和 DNS Server 的报文通过。

```
[Router] acl number 3001
[Router-acl-adv-3001] rule permit ip destination 192.168.0.2 0
[Router-acl-adv-3001] rule permit ip destination 192.168.0.3 0
[Router-acl-adv-3001] quit
```

创建连接数限制策略 1。

```
[Router] connection-limit policy 1
```

配置连接数限制规则 1，允许匹配 ACL 3000 的全部主机总共最多只能与外网建立 100000 条连接，超过 100000 时，需要等连接数恢复到 95000 以下才允许建立新的连接。

```
[Router-connlmt-policy-1] limit 1 acl 3000 amount 100000 95000
```

配置连接数限制规则 2，允许匹配 ACL 3001 的服务器最多接受 10000 条连接请求，超过 10000 时，需要等连接数降到 9800 以下才允许建立新的连接。

```
[Router-connlmt-policy-1] limit 2 acl 3001 per-destination amount 10000 9800
[Router-connlmt-policy-1] quit
```

创建连接数限制策略 2。

```
[Router] connection-limit policy 2
```

配置连接数限制规则 1，允许匹配 ACL 3000 的每台主机最多只能与外网建立 100 条连接，超过 100 时，需要等连接数恢复到 90 以下才允许建立新的连接。

```
[Router-connlmt-policy-2] limit 1 acl 3000 per-source amount 100 90
[Router-connlmt-policy-2] quit
```

在全局应用连接数限制策略 1。

```
[Router] connection-limit apply global policy 1
```

在入接口 Gigabitethernet2/1/1 上应用连接数限制策略 2。

```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] connection-limit apply policy 2
[Router-GigabitEthernet2/1/1] quit
```

4. 验证配置结果

上述配置完成后，执行 **display connection-limit policy** 命令显示连接数限制的配置情况，具体内容如下。

```
[Router] display connection-limit policy 1
IPv4 connection limit policy 1 has been applied 1 times, and has 2 limit rules.
Limit rule list:
```

```
  Policy  Rule    StatType  HiThres  LoThres   ACL
-------------------------------------------------------------
       1     1          --   100000    95000   3000
             2         Dst    10000     9800   3001

 Application list:
     Global
[Router] display connection-limit policy 2
IPv4 connection limit policy 2 has been applied 1 times, and has 1 limit rules.
Limit rule list:
  Policy  Rule    StatType  HiThres  LoThres   ACL
-------------------------------------------------------------
       2     1         Src      100       90   3000

 Application list:
     GigabitEthernet2/1/1
```

1.8 连接限制常见配置错误举例

1.8.1 不同的连接限制规则中引用的ACL存在包含关系时，规则顺序错误

1. 故障现象

在 Router 上进行如下配置，希望限制主机 192.168.0.100/24 最多向某公网服务器发起 100 条连接请求，以及 192.168.0.0/24 网段的其他主机最多向某公网服务器发起 10 条连接请求。

```
<Router> system-view
[Router] acl number 2001
[Router-acl-basic-2001] rule permit source 192.168.0.0 0.0.0.255
[Router-acl-basic-2001] quit
[Router] acl number 2002
[Router-acl-basic-2002] rule permit source 192.168.0.100 0
[Router-acl-basic-2002] quit
[Router] connection-limit policy 1
[Router-connlmt-policy-1] limit 1 acl 2001 per-destination amount 10 5
[Router-connlmt-policy-1] limit 2 acl 2002 per-destination amount 100 10
```

实际运行过程中，主机 192.168.0.100 最多只能同时向外部网络的同一个目的地址发起 10 条连接，后续连接被拒绝。

2. 故障分析

在上述配置中，limit 1 和 limit 2 中指定的源 IP 地址范围存在包含关系，192.168.0.100 发起的连接既符合 limit 1 又符合 limit 2。由于在进行连接限制规则的匹配时，设备根据规则编号由小到大的顺序进行匹配，且以匹配到的第一条有效规则为准，因此对 192.168.0.100 向外部网络发起的连接将只按照 limit 1 进行限制，而不会使用 limit 2 来限制。

3. 处理过程

为实现本需求，需要对 limit 2 与 limit 1 的顺序重新安排，将两个规则的序号进行调换，即将限制粒度更细、限制范围更精确的规则置前。

目 录

1 对象组配置

1.1 对象组简介

对象组分为 IPv4 地址对象组、IPv6 地址对象组、服务对象组和端口对象组。这些对象组可以被域间策略、ACL 引用，作为报文匹配的条件。

- IPv4 地址对象组内可以配置 IPv4 地址对象，地址对象与 IPv4 地址绑定，用于匹配报文中的 IPv4 地址。
- IPv6 地址对象组内可以配置 IPv6 地址对象，地址对象与 IPv6 地址绑定，用于匹配报文中的 IPv6 地址。
- 端口对象组内可以配置端口对象，端口对象与协议端口号绑定，用于匹配报文中的协议端口号。
- 服务对象组内可以配置服务对象，服务对象与协议类型以及协议的特性绑定（协议特性如 TCP 或 UDP 的源端口/目的端口、ICMP 协议的消息类型/消息码等），用于匹配报文中的可承载的上层协议。

在配置对象组时，需要注意的是：

- 创建对象时指定 ID，如果指定 ID 的对象不存在，则创建一条新的对象；如果指定 ID 的对象已存在，则对原对象进行修改。
- 新创建或修改的对象不能与已有对象的内容完全相同。
- 配置嵌套对象组不能形成循环并且对象组嵌套的最大层次为 5 层。

1.2 配置IPv4地址对象组

表1-1 配置 IPv4 地址对象组

操作	命令	说明
进入系统视图	**system-view**	-
创建IPv4地址对象组，并进入对象组视图	**object-group ip address** *object-group-name*	缺省情况下，存在系统默认对象组
（可选）配置对象组的描述信息	**description** *text*	缺省情况下，没有任何描述信息
创建IPv4地址对象	[*object-id*] **network** { **host** { **address** *ip-address1* | **name** *host-name* } | **subnet** *ip-address1* { *mask-length* | *mask* } | **range** *ip-address1 ip-address2* | **group-object** *object-group-name* } }	缺省情况下，对象组内不存在任何对象。 若未指定*object-id*，系统将按照步长10从0开始，自动分配一个大于现有最大ID的最小ID。譬如现有对象的最大ID为22，那么自动分配的新ID将是30。

1.3 配置IPv6地址对象组

表1-2 配置 IPv6 地址对象组

操作	命令	说明
进入系统视图	**system-view**	-
创建IPv6地址对象组，并进入对象组视图	**object-group ipv6 address** *object-group-name*	缺省情况下，存在系统默认对象组
（可选）配置对象组的描述信息	**description** *text*	缺省情况下，没有任何描述信息
创建IPv6地址对象	[*object-id*] **network** { **host** { **address** *ipv6-address1* | **name** *host-name* } | **subnet** *ipv6-address1 prefix-length* | **range** *ipv6-address1 ipv6-address2* | **group-object** *object-group-name* }	缺省情况下，对象组内不存在任何对象。 若未指定*object-id*，系统将按照步长10从0开始，自动分配一个大于现有最大ID的最小ID。譬如现有对象的最大ID为22，那么自动分配的新ID将是30。

1.4 配置端口对象组

表1-3 配置端口对象组

操作	命令	说明
进入系统视图	**system-view**	-
创建端口对象组，并进入对象组视图	**object-group port** *object-group-name*	缺省情况下，存在系统默认对象组
（可选）配置对象组的描述信息	**description** *text*	缺省情况下，没有任何描述信息
创建端口对象	[*object-id*] **port** { { **eq** | **lt** | **gt** } *port1* | **range** *port1 port2* | **group-object** *object-group-name* }	缺省情况下，对象组内不存在任何对象。 若未指定*object-id*，系统将按照步长10从0开始，自动分配一个大于现有最大ID的最小ID。譬如现有对象的最大ID为22，那么自动分配的新ID将是30。

1.5 配置服务对象组

表1-4 配置服务对象组

操作	命令	说明
进入系统视图	**system-view**	-
创建服务对象组，并进入对象组视图	**object-group service** *object-group-name*	缺省情况下，存在系统默认对象组 缺省情况下，对象组内不存在任何对象。

操作	命令	说明
（可选）配置对象组的描述信息	**description** *text*	缺省情况下，没有任何描述信息
创建服务对象	[*object-id*] **service** { *protocol* [{ **source** { { **eq** | **lt** | **gt** } *port1* | **range** *port1 port2* } | **destination** { { **eq** | **lt** | **gt** | } *port1* | **range** *port1 port2* } } * | *icmp-type icmp-code* | *icmpv6-type icmpv6-code*] | **group-object** *object-group-name* }	缺省情况下，对象组内不存在任何对象 若未指定*object-id*，系统将按照步长10从0开始，自动分配一个大于现有最大ID的最小ID。譬如现有对象的最大ID为22，那么自动分配的新ID将是30。

1.6 对象的显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后的对象组及对象信息，通过查看显示信息验证配置的效果。

表1-5 对象组显示和维护

操作	命令
查看IPv4地址对象组的相关信息	**display object-group ip address**
查看IPv6地址对象组的相关信息	**display object-group ipv6 address**
查看端口对象组的相关信息	**display object-group port**
查看服务对象组的相关信息	**display object-group service**
查看缺省IPv4地址对象组的相关信息	**display object-group ip address default**
查看缺省IPv6地址对象组的相关信息	**display object-group ipv6 address default**
查看缺省端口对象组的相关信息	**display object-group port default**
查看缺省服务对象组的相关信息	**display object-group service default**
查看指定对象组的信息	**display object-group name** *object-group-name*

目 录

1 IP Source Guard

1.1 IP Source Guard简介

1.1.1 概述

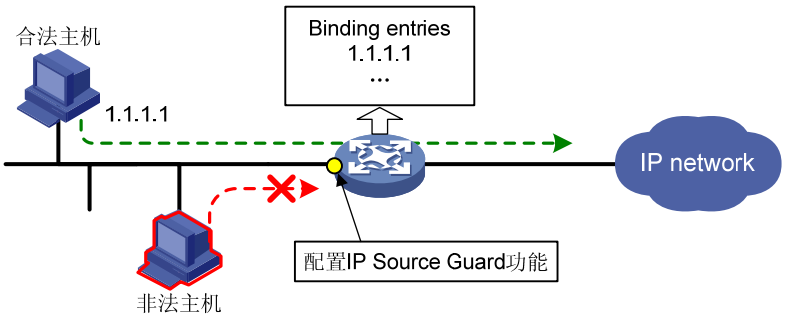
IP Source Guard 功能用于对接口收到的报文进行过滤控制，通常配置在接入用户侧的接口上，以防止非法用户报文通过，从而限制了对网络资源的非法使用（比如非法主机仿冒合法用户 IP 接入网络），提高了接口的安全性。

如 图 1-1 所示，配置了IP Source Guard功能的接口接收到用户报文后，首先查找与该接口绑定的表项（简称为绑定表项），如果报文的信息与某绑定表项匹配，则转发该报文，否则丢弃该报文。IP Source Guard可以根据报文的源IP地址、源MAC地址和VLAN标签对报文进行过滤。报文的这些特征项可单独或组合起来与接口进行绑定，形成如下几类绑定表项：

- IP 绑定表项
- MAC 绑定表项
- IP＋MAC 绑定表项
- IP＋VLAN 绑定表项
- MAC＋VLAN 绑定表项
- IP＋MAC＋VLAN 绑定表项

IP Source Guard 绑定表项可以通过手工配置和动态获取两种方式生成。

图1-1 IP Source Guard 功能示意图



说明

IP Source Guard 的绑定功能是针对接口的，一个接口配置了绑定功能后，仅对该接口接收的报文进行限制，其它接口不受影响。

1.1.2 静态配置绑定表项

说明

本特性仅在安装了 HMIM-24GSW/24GSWP 和 HMIM-8GSW 交换卡的款型以及 MSR3600-28/MSR3600-51 的固定二层接口上支持。

静态配置绑定表项是指通过命令行手工配置绑定表项，该方式适用于局域网络中主机数较少且主机使用静态配置 IP 地址的情况，比如在接入某重要服务器的接口上配置绑定表项，仅允许该接口接收与该服务器通信的报文。

IPv4 静态绑定表项用于过滤接口收到的 IPv4 报文，或者与 ARP Detection 功能配合使用检查接入用户的合法性；IPv6 静态绑定表项用于过滤接口收到的 IPv6 报文，或者与 ND Detection 功能配合使用检查接入用户的合法性。

ARP Detection 功能的详细介绍请参见“安全配置指导”中的“ARP 攻击防御”。ND Detection 功能的详细介绍请参见“安全配置指导”中的“ND 攻击防御”。

1.1.3 动态获取绑定表项

说明

本特性仅在安装了 HMIM-24GSW/24GSWP 和 HMIM-8GSW 交换卡的款型以及 MSR3600-28/MSR3600-51 的固定二层接口上支持。

动态获取绑定表项是指通过获取其它模块生成的用户信息来生成绑定表项。目前，可为 IP Source Guard 提供表项信息的模块包括 802.1X、DHCP Snooping、DHCPv6 Snooping 模块。

这种动态获取绑定表项的方式，通常适用于局域网络中主机较多，且主机使用 DHCP 动态获取 IP 地址的情况。其原理是每当局域网内的主机通过 DHCP 服务器获取到 IP 地址时，作为 DHCP Snooping 的设备上就会生成一条 DHCP Snooping 表项，并相应地增加一条 IP Source Guard 绑定表项以允许该用户访问网络。如果某个用户私自设置 IP 地址，则不会触发设备生成相应的 DHCP 表项，IP Source Guard 也不会增加相应的绑定表项，因此该用户的报文将会被丢弃。

1. IPv4 动态绑定功能

在配置了 IPv4 动态绑定功能的接口上，IP Source Guard 通过与不同的模块配合动态生成绑定表项：

- 在二层以太网端口上，IP Source Guard 可与 DHCP Snooping 配合，通过主机动态获取 IP 地址时产生的 DHCP Snooping 表项来生成动态绑定表项，并用于过滤报文。
- 在二层以太网端口上，IP Source Guard 可与 802.1X 配合，通过获取认证用户的信息来生成动态绑定表项，用于配合其它模块（例如 ARP Detection）提供相关的安全服务，而不直接用于过滤报文。

802.1X 功能的详细介绍请参见“安全配置指导”中的“802.1X”。DHCP Snooping 功能的详细介绍请参见“三层技术-IP 业务配置指导”中的“DHCP Snooping”。

2. IPv6 动态绑定功能

在配置了 IPv6 动态绑定功能的接口上，IP Source Guard 通过与 DHCPv6 Snooping 模块配合，通过主机动态获取 IPv6 地址时产生的 DHCPv6 Snooping 表项来生成动态绑定表项，并用于过滤报文。DHCPv6 Snooping 功能的详细介绍请参见“三层技术-IP 业务配置指导”的“DHCPv6 Snooping”。

1.2 IP Source Guard配置任务简介

表1-1 IPv4 绑定功能配置任务简介

配置任务	说明	详细配置
配置IPv4接口绑定功能	必选	1.3.1
配置接口的IPv4静态绑定表项	可选	1.3.2

表1-2 IPv6 绑定功能配置任务简介

配置任务	说明	详细配置
配置IPv6接口绑定功能	必选	1.4.1
配置接口的IPv6静态绑定表项	可选	1.4.2

1.3 配置IPv4绑定功能

1.3.1 配置IPv4 接口绑定功能

配置了 IPv4 接口绑定功能的接口，将打开根据绑定表项过滤报文的开关，并利用配置的 IPv4 静态绑定表项和从其它模块获取的 IPv4 动态绑定表项对接口转发的报文进行过滤或者配合其它模块提供相关的安全服务。

(1) IPv4 静态绑定表项中指定的信息均用于IP Source Guard过滤接口收到的报文，具体配置请参考“1.3.2 配置接口的IPv4 静态绑定表项”。

(2) IPv4 动态绑定表项中可能包含的内容有：MAC 地址、IP 地址、VLAN 信息、入接口信息及表项类型（DHCP Snooping、DHCP 中继等）。IP Source Guard 依据该表项中的哪些信息过滤接口收到的报文，由 IPv4 接口绑定配置决定：

- 若接口上配置动态绑定功能时绑定了源 IP 地址和 MAC 地址，则只有接口上收到的报文的源 IPv4 地址和源 MAC 地址都与某动态绑定表项匹配，该报文才能被正常转发，否则将被丢弃；
- 若接口上配置动态绑定功能时仅绑定了源 IP 地址，则只有该接口收到的报文的源 IPv4 地址与某动态绑定表项匹配，该报文才会被正常转发，否则将被丢弃；
- 若接口上配置动态绑定功能时仅绑定了源 MAC 地址，则只有该接口收到的报文的源 MAC 地址与某动态绑定表项匹配，该报文才会被正常转发，否则将被丢弃。

要实现 IPv4 动态绑定功能，请保证网络中的 DHCP Snooping 或者 DHCP 中继配置有效且工作正常。

表1-3 配置 IPv4 接口绑定功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	支持二层以太网端口
配置IPv4接口绑定功能	**ip verify source** { **ip-address** | **ip-address mac-address** | **mac-address** }	缺省情况下，接口的IPv4接口绑定功能处于关闭状态 IPv4接口绑定功能可多次配置，最后一次的配置生效

1.3.2 配置接口的IPv4 静态绑定表项

表1-4 配置接口的 IPv4 静态绑定表项

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	支持二层以太网端口
配置接口的IPv4静态绑定表项	**ip source binding** { **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]	缺省情况下，接口上无IPv4静态绑定表项 在与ARP Detection功能配合时，绑定表项中必须指定VLAN参数，且该VLAN为使能ARP Detection功能的VLAN，否则ARP报文将无法通过接口的IPv4静态绑定表项的检查。

说明

- 同一个表项不能在同一个接口上重复绑定，但可以在不同的接口上绑定。
- 安装了 HMIM-24GSW/24GSWP 和 HMIM-8GSW 交换卡的款型最多允许配置的 IPv4 静态绑定表项数量为 384，MSR3600-28/MSR3600-51 的固定二层接口上最多允许配置的 IPv4 静态绑定表项数量为 256。

1.4 配置IPv6绑定功能

1.4.1 配置IPv6 接口绑定功能

配置了 IPv6 接口绑定功能的接口，将打开根据绑定表项过滤报文的开关，并利用配置的 IPv6 静态绑定表项和从 DHCPv6 Snooping 模块获取的 IPv6 动态绑定表项对接口转发的报文进行过滤。

(1) IPv6 静态绑定表项中指定的信息均用于IP Source Guard过滤接口收到的报文，具体配置请参考“1.4.2 配置接口的IPv6 静态绑定表项”。

(2) IPv6 动态绑定表项中可能包含的信息有：MAC 地址、IP 地址、VLAN 信息、入接口信息及表项类型（DHCPv6 Snooping）。IP Source Guard 依据该表项中的哪些信息过滤接口收到的报文，由 IPv4 接口绑定配置决定：

- 若接口上配置动态绑定功能时绑定了源 IP 地址和 MAC 地址，则只有接口上收到的报文的源 IPv6 地址和源 MAC 地址都与某动态绑定表项匹配，该报文才能被正常转发，否则将被丢弃；
- 若接口上配置动态绑定功能时仅绑定了源 IP 地址，则只有该接口收到的报文的源 IPv6 地址与某动态绑定表项匹配，该报文才会被正常转发，否则将被丢弃；
- 若接口上配置动态绑定功能时仅绑定了源 MAC 地址，则只有该接口收到的报文的源 MAC 地址与某动态绑定表项匹配，该报文才会被正常转发，否则将被丢弃。

要实现 IPv6 动态绑定功能，请保证网络中的 DHCPv6 Snooping 配置有效且工作正常。

表1-5 配置 IPv6 接口绑定功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	支持二层以太网端口
配置IPv6接口绑定功能	**ipv6 verify source** { **ip-address** | **ip-address mac-address** | **mac-address** }	缺省情况下，接口的IPv6接口绑定功能处于关闭状态 IPv6接口绑定功能可多次配置，最后一次的配置生效。

1.4.2 配置接口的IPv6 静态绑定表项

表1-6 配置接口的 IPv6 静态绑定表项

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	支持二层以太网端口
配置接口的IPv6静态绑定表项	**ipv6 source binding** { **ip-address** *ipv6-address* | **ip-address** *ipv6-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]	缺省情况下，接 口上无IPv6静态绑定表项 在与ND Detection功能配合时，绑定表项中必须指定VLAN参数，且该VLAN为使能ND Detection功能的VLAN，否则ND报文将无法通过接口的IPv6静态绑定表项的检查。

说明

- 同一个表项不能在同一个接口上重复绑定，但可以在不同接口上绑定。
- 安装了 HMIM-24GSW/24GSWP 和 HMIM-8GSW 交换卡的款型最多允许配置的 Ipv6 静态绑定表项数量为 384，MSR3600-28/MSR3600-51 的固定二层接口上最多允许配置的 Ipv6 静态绑定表项数量为 256。

1.5 IP Source Guard显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 IP Source Guard 的运行情况，通过查看显示信息验证配置的效果。

表1-7 IP Source Guard 显示和维护（IPv4）

操作	命令
显示IPv4绑定表项信息（MSR 2600/MSR 3600）	**display ip source binding** [**static** | [**vpn-instance** *vpn-instance-name*] [**dhcp-snooping** | **dot1x**]] [**ip-address** *ip-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]
显示IPv4绑定表项信息（MSR 5600）	**display ip source binding** [**static** | [**vpn-instance** *vpn-instance-name*] [**dhcp-snooping** | **dot1x**]] [**ip-address** *ip-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

表1-8 IP Source Guard 显示和维护（IPv6）

操作	命令
显示IPv6绑定表项信息（MSR 2600/MSR 3600）	**display ipv6 source binding** [**static** | [**vpn-instance** *vpn-instance-name*] [**dhcpv6-snooping**]] [**ip-address** *ipv6-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]
显示IPv6绑定表项信息（MSR 5600）	**display ipv6 source binding** [**static** | [**vpn-instance** *vpn-instance-name*] [**dhcpv6-snooping**]] [**ip-address** *ipv6-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

1.6 IP Source Guard典型配置举例

1.6.1 IPv4 静态绑定表项配置举例

1. 组网需求

如 图 1-2 所示，Host A、Host B分别与Device B的接口GigabitEthernet2/1/2、GigabitEthernet2/1/1相连；Host C与Device A的接口GigabitEthernet2/1/2 相连。Device B接到Device A的接口GigabitEthernet2/1/1 上。各主机均使用静态配置的IP地址。

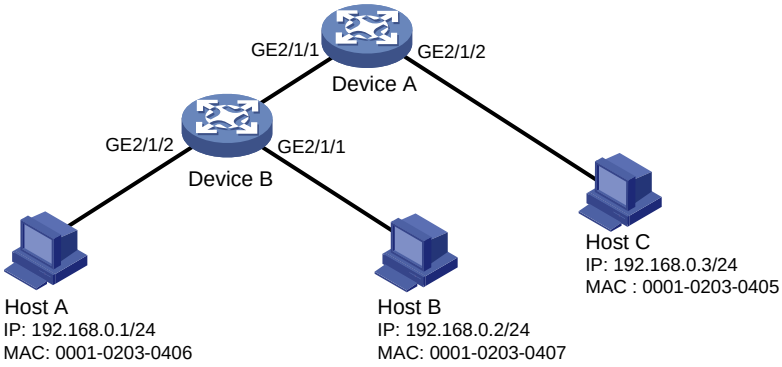
要求通过在 Device A 和 Device B 上配置 IPv4 静态绑定表项，满足以下各项应用需求：

- Device A 的接口 GigabitEthernet2/1/2 上只允许 Host C 发送的 IP 报文通过。

- Device A 的接口 GigabitEthernet2/1/1 上只允许 Host A 发送的 IP 报文通过。
- Device B 的接口 GigabitEthernet2/1/1 上允许 Host B 发送的 IP 报文通过。

2. 组网图

图1-2 配置静态绑定表项组网图



3. 配置步骤

(1) 配置 Device A

配置各接口的 IP 地址（略）。

在接口 GigabitEthernet2/1/2 上配置 IPv4 接口绑定功能，绑定源 IP 地址和 MAC 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 2/1/2
[DeviceA-GigabitEthernet2/1/2] ip verify source ip-address mac-address
```

配置 IPv4 静态绑定表项，在 Device A 的 GigabitEthernet1/0/2 上只允许 MAC 地址为 0001-0203-0405、IP 地址为 192.168.0.3 的数据终端 Host C 发送的 IP 报文通过。

```
[DeviceA-GigabitEthernet2/1/2] ip source binding ip-address 192.168.0.3 mac-address
0001-0203-0405
[DeviceA-GigabitEthernet2/1/2] quit
```

在接口 GigabitEthernet2/1/1 上配置 IPv4 接口绑定功能，绑定源 IP 地址和 MAC 地址。

```
[DeviceA] interface gigabitethernet 2/1/1
[DeviceA-GigabitEthernet2/1/1] ip verify source ip-address mac-address
```

配置在 Device A 的 GigabitEthernet2/1/1 上只允许 MAC 地址为 0001-0203-0406、IP 地址为 192.168.0.1 的数据终端 Host A 发送的 IP 报文通过。

```
[DeviceA-GigabitEthernet2/1/1] ip source binding ip-address 192.168.0.1 mac-address
0001-0203-0406
[DeviceA-GigabitEthernet2/1/1] quit
```

(2) 配置 Device B

配置各接口的 IP 地址（略）。

在接口 GigabitEthernet2/1/2 上配置 IPv4 接口绑定功能，绑定源 IP 地址和 MAC 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 2/1/2
[DeviceB-GigabitEthernet2/1/2] ip verify source ip-address mac-address
[DeviceB-GigabitEthernet2/1/2] quit
```

在接口 GigabitEthernet2/1/1 上配置 IPv4 接口绑定功能，绑定源 IP 地址和 MAC 地址。

```
[DeviceB] interface gigabitethernet 2/1/1
[DeviceB-GigabitEthernet2/1/1] ip verify source ip-address mac-address
```

配置 IPv4 静态绑定表项，在 Device B 的 GigabitEthernet2/1/1 上允许 MAC 地址为 0001-0203-0407 的数据终端 Host B 发送的 IP 报文通过。

```
[DeviceB] interface gigabitethernet 2/1/1
[DeviceB-GigabitEthernet2/1/1] ip source binding mac-address 0001-0203-0407
[DeviceB-GigabitEthernet2/1/1] quit
```

4. 验证配置

在 Device A 上显示 IPv4 静态绑定表项，可以看出以上配置成功。

```
<DeviceA> display ip source binding static
Total entries found: 2
IP Address      MAC Address    Interface               VLAN Type
192.168.0.1     0001-0203-0405 GE2/1/2                 N/A  Static
192.168.0.3     0001-0203-0406 GE2/1/1                 N/A  Static
```

在 Device B 上显示 IPv4 静态绑定表项，可以看出以上配置成功。

```
<DeviceB> display ip source binding static
Total entries found: 2
IP Address      MAC Address    Interface               VLAN Type
N/A             0001-0203-0407 GE2/1/1                 N/A  Static
```

1.6.2 与DHCP Snooping配合的IPv4 动态绑定功能配置举例

1. 组网需求

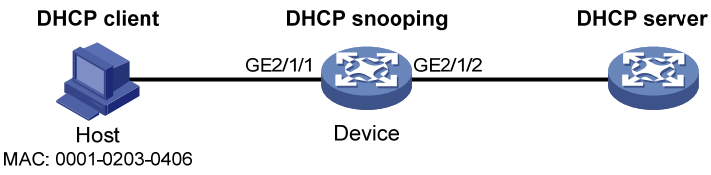
DHCP 客户端通过 Device 的接口 GigabitEthernet2/1/1 接入网络，通过 DHCP 服务器获取 IPv4 地址。

具体应用需求如下：

- Device 上使能 DHCP Snooping 功能，保证客户端从合法的服务器获取 IP 地址，且记录客户端 IPv4 地址及 MAC 地址的绑定关系。
- 在接口 GigabitEthernet2/1/1 上启用 IPv4 动态绑定功能，利用动态生成的 DHCP Snooping 表项过滤接口接收的报文，只允许通过 DHCP 服务器动态获取 IP 地址的客户端接入网络。DHCP 服务器的具体配置请参见“三层技术-IP 业务配置指导”中的“DHCP 服务器”。

2. 组网图

图1-3 配置与 DHCP Snooping 配合的 IPv4 动态绑定功能组网图



3. 配置步骤

(1) 配置 DHCP Snooping

配置各接口的 IP 地址（略）。

开启 DHCP Snooping 功能。

```
<Device> system-view
[Device] dhcp snooping enable
```

设置与 DHCP 服务器相连的接口 GigabitEthernet2/1/2 为信任接口。

```
[Device] interface gigabitethernet2/1/2
[Device-GigabitEthernet2/1/2] dhcp snooping trust
[Device-GigabitEthernet2/1/2] quit
```

(2) 配置 IPv4 接口绑定功能

配置接口 GigabitEthernet2/1/1 的 IPv4 接口绑定功能，绑定源 IP 地址和 MAC 地址，并启用接口的 DHCP Snooping 表项记录功能。

```
[Device] interface gigabitethernet 2/1/1
[Device-GigabitEthernet2/1/1] ip verify source ip-address mac-address
[Device-GigabitEthernet2/1/1] dhcp snooping binding record
[Device-GigabitEthernet2/1/1] quit
```

4. 验证配置

显示接口 GigabitEthernet2/1/1 从 DHCP Snooping 获取的动态表项。

```
[Device] display ip source binding dhcp-snooping
Total entries found: 1
IP Address      MAC Address    Interface               VLAN Type
192.168.0.1     0001-0203-0406 GE2/1/1                 1    DHCP snooping
```

从以上显示信息可以看出，接口 GigabitEthernet2/1/1 在配置 IPv4 接口绑定功能之后根据 DHCP Snooping 表项产生了动态绑定表项。

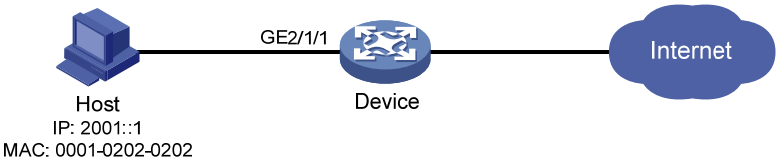
1.6.3 IPv6 静态绑定表项配置举例

1. 组网需求

IPv6 客户端通过 Device 的接口 GigabitEthernet2/1/1 接入网络。要求在 Device 上配置 IPv6 静态绑定表项，使得接口 GigabitEthernet2/1/1 上只允许 Host（MAC 地址为 0001-0202-0202、IPv6 地址为 2001::1）发送的 IPv6 报文通过。

2. 组网图

图1-4 配置 IPv6 静态绑定表项组网图



3. 配置步骤

在接口 GigabitEthernet2/1/1 上配置 IPv6 接口绑定功能，绑定源 IP 地址和 MAC 地址。

```
<Device> system-view
[Device] interface gigabitethernet 2/1/1
[Device-GigabitEthernet2/1/1] ipv6 verify source ip-address mac-address
```

在接口 GigabitEthernet2/1/1 上配置 IPv6 静态绑定表项，绑定源 IP 地址和 MAC 地址，只允许 IPv6 地址为 2001::1 且 MAC 地址为 00-01-02-02-02-02 的 IPv6 报文通过。

```
[Device-GigabitEthernet2/1/1] ipv6 source binding ip-address 2001::1 mac-address
0001-0202-0202
[Device-GigabitEthernet2/1/1] quit
```

4. 验证配置

在 Device 上显示 IPv6 静态绑定表项，可以看出以上配置成功。

```
[Device] display ipv6 source binding static
Total entries found: 1
IPv6 Address         MAC Address    Interface              VLAN Type
2001::1              0001-0202-0202 GE2/1/1                N/A  Static
```

1.6.4 与DHCPv6 Snooping配合的IPv6 动态绑定表项配置举例

1. 组网需求

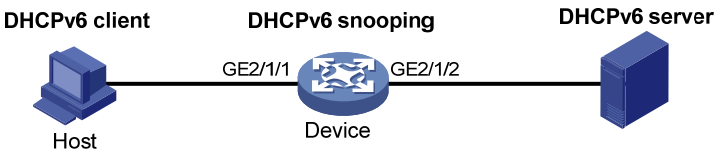
DHCPv6 客户端通过 Device 的接口 GigabitEthernet2/1/1 接入网络，通过 DHCPv6 服务器获取 IPv6 地址。

具体应用需求如下：

- Device 上使能 DHCPv6 Snooping 功能，保证客户端从合法的服务器获取 IP 地址，且记录客户端 IPv6 地址及 MAC 地址的绑定关系。
- 在接口 GigabitEthernet2/1/1 上启用 IPv6 动态绑定功能，利用动态生成的 DHCPv6 Snooping 表项过滤接口接收的报文，只允许通过 DHCPv6 服务器动态获取 IP 地址的客户端接入网络。

2. 组网图

图1-5 配置与 DHCPv6 Snooping 配合的 IPv6 动态绑定功能组网图



3. 配置步骤

(1) 配置 DHCPv6 Snooping

全局使能 DHCPv6 Snooping 功能。

```
<Device> system-view
[Device] ipv6 dhcp snooping enable
```

配置接口 GigabitEthernet2/1/2 为信任接口。

```
[Device] interface gigabitethernet 2/1/2
[Device-GigabitEthernet2/1/2] ipv6 dhcp snooping trust
[Device-GigabitEthernet2/1/2] quit
```

(2) 配置 IPv6 接口绑定功能

配置接口 GigabitEthernet2/1/1 的 IPv6 接口绑定功能，绑定源 IP 地址和 MAC 地址，并启用接口的 DHCPv6 Snooping 表项记录功能。

```
[Device] interface gigabitethernet 2/1/1
```

```
[Device-GigabitEthernet2/1/1] ipv6 verify source ip-address mac-address
[Device-GigabitEthernet2/1/1] ipv6 dhcp snooping binding record
[Device-GigabitEthernet2/1/1] quit
```

4. 验证配置

客户端通过 DHCPv6 server 成功获取 IP 地址之后，通过执行以下命令可查看到已生成的 IPv6 动态绑定表项信息。

```
[Device] display ipv6 source binding dhcpv6-snooping
Total entries found: 1
IPv6 Address         MAC Address    Interface               VLAN Type
2001::1              040a-0000-0001 GE2/1/1                 1    DHCPv6 snooping
```

从以上显示信息可以看出，IP Source Guard 通过获取接口 GigabitEthernet2/1/1 上产生的 DHCPv6 Snooping 表项成功生成了 IPv6 动态绑定表项。

目 录

1 ARP攻击防御

1.1 ARP攻击防御简介

ARP 协议有简单、易用的优点，但是也因为其没有任何安全机制而容易被攻击发起者利用。

- 攻击者可以仿冒用户、仿冒网关发送伪造的 ARP 报文，使网关或主机的 ARP 表项不正确，从而对网络进行攻击。
- 攻击者通过向设备发送大量目标 IP 地址不能解析的 IP 报文，使得设备试图反复地对目标 IP 地址进行解析，导致 CPU 负荷过重及网络流量过大。
- 攻击者向设备发送大量 ARP 报文，对设备的 CPU 形成冲击。

关于 ARP 攻击报文的特点以及 ARP 攻击类型的详细介绍，请参见“ARP 攻击防范技术白皮书”。

目前 ARP 攻击和 ARP 病毒已经成为局域网安全的一大威胁，为了避免各种攻击带来的危害，设备提供了多种技术对攻击进行防范、检测和解决。

下面将详细介绍一下这些技术的原理以及配置。

1.2 ARP攻击防御配置任务简介

表1-1 ARP 攻击防御配置任务简介

配置任务			说明	详细配置
防止泛洪攻击	配置ARP防止IP报文攻击功能	配置ARP源抑制功能	可选 建议在网关设备上配置本功能	1.3
		配置ARP黑洞路由功能	可选 建议在网关设备上配置本功能	
	配置源MAC地址固定的ARP攻击检测功能		可选 建议在网关设备上配置本功能	1.4
防止仿冒用户、仿冒网关攻击	配置ARP报文源MAC地址一致性检查功能		可选 建议在网关设备上配置本功能	1.5
	配置ARP主动确认功能		可选 建议在网关设备上配置本功能	1.6
	配置授权ARP功能		可选 建议在网关设备上配置本功能	1.7
	配置ARP Detection功能		可选 建议在接入设备上配置本功能	1.8
	配置ARP自动扫描、固化功能		可选 建议在网关设备上配置本功能	1.9
	配置ARP网关保护功能		可选 建议在接入设备上配置本功能	1.10

配置任务		说明	详细配置
	配置ARP过滤保护功能	可选 建议在接入设备上配置本功能	1.11

1.3 配置ARP防止IP报文攻击功能

1.3.1 ARP防止IP报文攻击功能简介

如果网络中有主机通过向设备发送大量目标 IP 地址不能解析的 IP 报文来攻击设备，则会造成下面的危害：

- 设备向目的网段发送大量 ARP 请求报文，加重目的网段的负载。
- 设备会试图反复地对目标 IP 地址进行解析，增加了 CPU 的负担。

为避免这种 IP 报文攻击所带来的危害，设备提供了下列两个功能：

- ARP 源抑制功能：如果发送攻击报文的源是固定的，可以采用 ARP 源抑制功能。开启该功能后，如果网络中每 5 秒内从某 IP 地址向设备某接口发送目的 IP 地址不能解析的 IP 报文超过了设置的阈值，则设备将不再处理由此 IP 地址发出的 IP 报文直至该 5 秒结束，从而避免了恶意攻击所造成的危害。
- ARP 黑洞路由功能：无论发送攻击报文的源是否固定，都可以采用 ARP 黑洞路由功能。开启该功能后，一旦接收到目标 IP 地址不能解析的 IP 报文，设备立即产生一个黑洞路由，使得设备在一段时间内将去往该地址的报文直接丢弃。等待黑洞路由老化时间过后，如有报文触发则再次发起解析，如果解析成功则进行转发，否则仍然产生一个黑洞路由将去往该地址的报文丢弃。这种方式能够有效地防止 IP 报文的攻击，减轻 CPU 的负担。

1.3.2 配置ARP防止IP报文攻击功能

1. 配置ARP源抑制功能

表1-2 配置 ARP 源抑制功能

操作	命令	说明
进入系统视图	**system-view**	-
使能ARP源抑制功能	**arp source-suppression enable**	缺省情况下，ARP源抑制功能处于关闭状态
配置ARP源抑制的阈值	**arp source-suppression limit** *limit-value*	缺省情况下，ARP源抑制的阈值为10

2. 配置ARP黑洞路由功能

表1-3 配置 ARP 黑洞路由功能

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
使能ARP黑洞路由功能	**arp resolving-route enable**	缺省情况下，ARP黑洞路由功能处于开启状态

1.3.3 ARP防止IP报文攻击显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 ARP 源抑制的运行情况，通过查看显示信息验证配置的效果。

表1-4 ARP 防止 IP 报文攻击显示和维护

操作	命令
显示ARP源抑制的配置信息	**display arp source-suppression**

1.3.4 ARP防止IP报文攻击配置举例

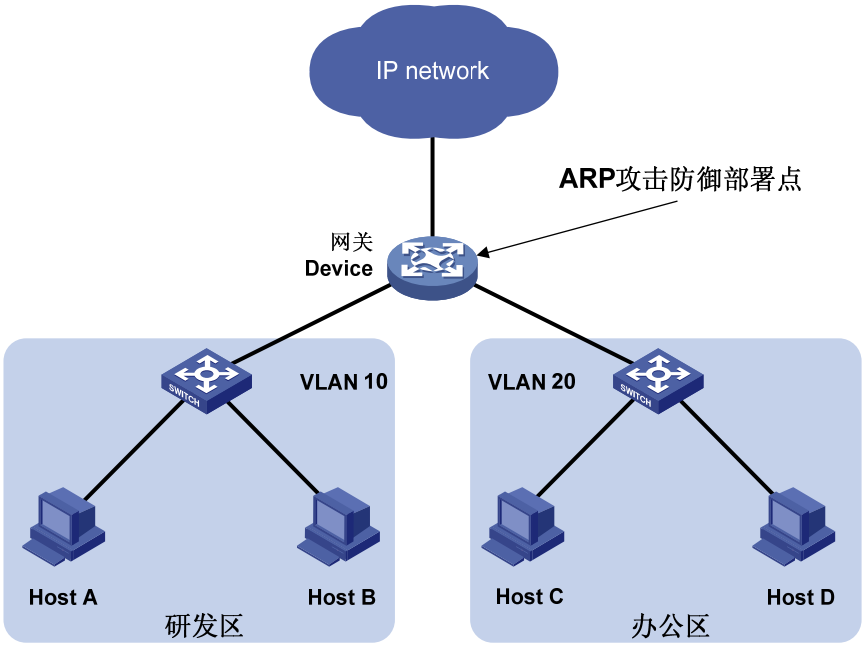
1. 组网需求

某局域网内存在两个区域：研发区和办公区，分别属于VLAN 10 和VLAN 20，通过接入交换机连接到网关Device，如 图 1-1 所示。

网络管理员在监控网络时发现办公区存在大量 ARP 请求报文，通过分析认为存在 IP 泛洪攻击，为避免这种 IP 报文攻击所带来的危害，可采用 ARP 源抑制功能和 ARP 黑洞路由功能。

2. 组网图

图1-1 ARP 防止 IP 报文攻击配置组网图



3. 配置思路

对攻击报文进行分析，如果发送攻击报文的源地址是固定的，采用 ARP 源抑制功能。在 Device 上做如下配置：

- 使能 ARP 源抑制功能；
- 配置 ARP 源抑制的阈值为 100，即当每 5 秒内的 ARP 请求报文的流量超过 100 后，对于由此 IP 地址发出的 IP 报文，设备不允许其触发 ARP 请求，直至 5 秒后再处理。

如果发送攻击报文的源地址是不固定的，则采用 ARP 黑洞路由功能，在 Device 上配置 ARP 黑洞路由功能。

4. 配置步骤

- 配置 ARP 源抑制功能

使能 ARP 源抑制功能，并配置 ARP 源抑制的阈值为 100。

```
<Device> system-view
[Device] arp source-suppression enable
[Device] arp source-suppression limit 100
```

- 配置 ARP 黑洞路由功能

使能 ARP 黑洞路由功能。

```
[Device] arp resolving-route enable
```

1.4 配置源MAC地址固定的ARP攻击检测功能

1.4.1 源MAC地址固定的ARP攻击检测功能简介

本特性根据 ARP 报文的源 MAC 地址对上送 CPU 的 ARP 报文进行统计，在 5 秒内，如果收到同一源 MAC 地址（源 MAC 地址固定）的 ARP 报文超过一定的阈值，则认为存在攻击，系统会将此 MAC 地址添加到攻击检测表项中。在该攻击检测表项老化之前，如果设置的检查模式为过滤模式，则会打印日志信息并且将该源 MAC 地址发送的 ARP 报文过滤掉；如果设置的检查模式为监控模式，则只打印日志信息，不会将该源 MAC 地址发送的 ARP 报文过滤掉。

对于网关或一些重要的服务器，可能会发送大量 ARP 报文，为了使这些 ARP 报文不被过滤掉，可以将这类设备的 MAC 地址配置成保护 MAC 地址，这样，即使该设备存在攻击也不会被检测、过滤。

1.4.2 配置源MAC地址固定的ARP攻击检测功能

表1-5 配置源 MAC 地址固定的 ARP 攻击检测功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
使能源MAC地址固定的ARP攻击检测功能，并选择检查模式	**arp source-mac { filter | monitor }**	缺省情况下，源MAC地址固定的ARP攻击检测功能处于关闭状态
配置源MAC地址固定的ARP报文攻击检测的阈值	**arp source-mac threshold** *threshold-value*	缺省情况，源MAC地址固定的ARP报文攻击检测阈值为30
配置源MAC地址固定的ARP攻击检测表项的老化时间	**arp source-mac aging-time** *time*	缺省情况下，源MAC地址固定的ARP攻击检测表项的老化时间为300秒，即5分钟

配置步骤	命令	说明
（可选）配置保护MAC地址	**arp source-mac exclude-mac** *mac-address*&<1-n>	缺省情况下，没有配置任何保护MAC地址 n的值为64

说明

对于已添加到源 MAC 地址固定的 ARP 攻击检测表项中的 MAC 地址，在等待设置的老化时间后，会重新恢复成普通 MAC 地址。

1.4.3 源MAC地址固定的ARP攻击检测显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后源 MAC 地址固定的 ARP 攻击检测的运行情况，通过查看显示信息验证配置的效果。

表1-6 源 MAC 地址固定的 ARP 攻击检测显示和维护

操作	命令
显示检测到的源MAC地址固定的ARP攻击检测表项（MSR 2600/MSR 3600）	**display arp source-mac** [**interface** *interface-type interface-number*]
显示检测到的源MAC地址固定的ARP攻击检测表项（MSR 5600）	**display arp source-mac** { **slot** *slot-number* | **interface** *interface-type interface-number* }

1.4.4 源MAC地址固定的ARP攻击检测功能配置举例

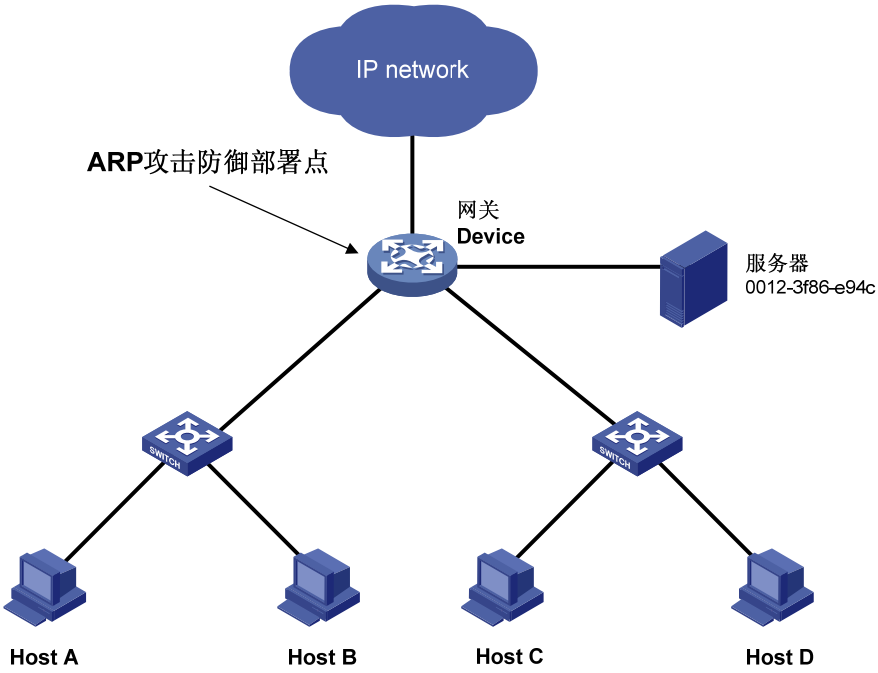
1. 组网需求

某局域网内客户端通过网关与外部网络通信，网络环境如 图 1-2 所示。

网络管理员希望能够防止因恶意用户对网关发送大量 ARP 报文，造成设备瘫痪，并导致其它用户无法正常地访问外部网络；同时，对于正常的大量 ARP 报文仍然会进行处理。

2. 组网图

图1-2 源 MAC 地址固定的 ARP 攻击检测功能配置组网图



3. 配置思路

如果恶意用户发送大量报文的源MAC地址是使用客户端合法的MAC地址，并且源MAC是固定的，可以在网关上进行如下配置：

- 使能源 MAC 固定 ARP 攻击检测功能，并选择过滤模式；
- 配置源 MAC 固定 ARP 报文攻击检测的阈值；
- 配置源 MAC 固定的 ARP 攻击检测表项的老化时间；
- 配置服务器的 MAC 为保护 MAC，使服务器可以发送大量 ARP 报文。

4. 配置步骤

使能源 MAC 固定 ARP 攻击检测功能，并选择过滤模式。

```
<Device> system-view
[Device] arp source-mac filter
```

配置源 MAC 固定 ARP 报文攻击检测阈值为 30 个。

```
[Device] arp source-mac threshold 30
```

配置源 MAC 地址固定的 ARP 攻击检测表项的老化时间为 60 秒。

```
[Device] arp source-mac aging-time 60
```

配置源 MAC 固定攻击检查的保护 MAC 地址为 0012-3f86-e94c。

```
[Device] arp source-mac exclude-mac 0012-3f86-e94c
```

1.5 配置ARP报文源MAC地址一致性检查功能

1.5.1 ARP报文源MAC地址一致性检查功能简介

ARP 报文源 MAC 地址一致性检查功能主要应用于网关设备上，防御以太网数据帧首部中的源 MAC 地址和 ARP 报文中的源 MAC 地址不同的 ARP 攻击。

配置本特性后，网关设备在进行 ARP 学习前将对 ARP 报文进行检查。如果以太网数据帧首部中的源 MAC 地址和 ARP 报文中的源 MAC 地址不同，则认为是攻击报文，将其丢弃；否则，继续进行 ARP 学习。

1.5.2 配置ARP报文源MAC地址一致性检查功能

表1-7 配置 ARP 报文源 MAC 地址一致性检查功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
使能ARP报文源MAC地址一致性检查功能	**arp valid-check enable**	缺省情况下，ARP报文源MAC地址一致性检查功能处于关闭状态

1.6 配置ARP主动确认功能

1.6.1 ARP主动确认功能简介

ARP 的主动确认功能主要应用于网关设备上，防止攻击者仿冒用户欺骗网关设备。

启用 ARP 主动确认功能后，设备在新建或更新 ARP 表项前需进行主动确认，防止产生错误的 ARP 表项。关于工作原理的详细介绍请参见“ARP 攻击防范技术白皮书”。使能严格模式后，ARP 主动确认功能执行更严格的检查，新建 ARP 表项前，需要本设备先对其 IP 地址发起 ARP 解析，解析成功后才能触发正常的主动确认流程，在主动确认流程成功后，才允许设备学习该表项。

1.6.2 配置ARP主动确认功能

表1-8 配置 ARP 主动确认功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
使能ARP主动确认功能	**arp active-ack [strict] enable**	缺省情况下，ARP主动确认功能处于关闭状态

1.7 配置授权ARP功能

1.7.1 授权ARP功能简介

所谓授权 ARP（Authorized ARP），就是动态学习 ARP 的过程中，只有和 DHCP 服务器生成的租约或 DHCP 中继生成的安全表项一致的 ARP 报文才能够被学习。关于 DHCP 服务器和 DHCP 中继的介绍，请参见“三层技术-IP 业务配置指导”中的“DHCP 服务器”和“DHCP 中继”。

使能接口的授权 ARP 功能后，系统会禁止该接口学习动态 ARP 表项，可以防止用户仿冒其他用户的 IP 地址或 MAC 地址对网络进行攻击，保证只有合法的用户才能使用网络资源，增加了网络的安全性。

1.7.2 配置授权ARP功能

表1-9 配置授权 ARP 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入三层以太网接口/三层以太网子接口/三层聚合接口/三层聚合子接口视图	**interface** *interface-type interface-number*	
使能授权ARP功能	**arp authorized enable**	缺省情况下，接口下的授权ARP功能处于关闭状态

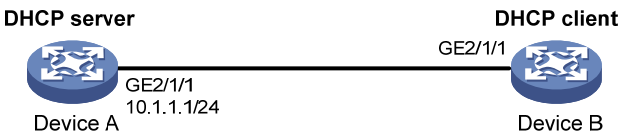
1.7.3 授权ARP功能在DHCP服务器上的典型配置举例

1. 组网需求

- Device A 是 DHCP 服务器，为同一网段中的客户端动态分配 IP 地址，地址池网段为 10.1.1.0/24。通过在接口 GigabitEthernet2/1/1 上启用授权 ARP 功能来保证客户端的合法性。
- Device B 是 DHCP 客户端，通过 DHCP 协议从 DHCP 服务器获取 IP 地址。

2. 组网图

图1-3 授权 ARP 功能典型配置组网图



3. 配置步骤

(1) 配置 Device A

配置接口的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 2/1/1
[DeviceA-GigabitEthernet2/1/1] ip address 10.1.1.1 24
```

```
[DeviceA-GigabitEthernet2/1/1] quit
```

使能 DHCP 服务。

```
[DeviceA] dhcp enable
[DeviceA] dhcp server ip-pool 1
[DeviceA-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.0
[DeviceA-dhcp-pool-1] quit
```

进入三层以太网接口视图。

```
[DeviceA] interface gigabitethernet 2/1/1
```

使能接口授权 ARP 功能。

```
[DeviceA-GigabitEthernet2/1/1] arp authorized enable
[DeviceA-GigabitEthernet2/1/1] quit
```

(2) 配置 Device B

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 2/1/1
[DeviceB-GigabitEthernet2/1/1] ip address dhcp-alloc
[DeviceB-GigabitEthernet2/1/1] quit
```

(3) Device B 获得 Device A 分配的 IP 后，在 Device A 查看授权 ARP 信息。

```
[DeviceA] display arp all
  Type: S-Static   D-Dynamic   O-Openflow   M-Multiport  I-Invalid
IP Address       MAC Address     VLAN     Interface          Aging  Type
10.1.1.2         0012-3f86-e94c  N/A      GE2/1/1            20     D
```

从以上信息可以获知 Device A 为 Device B 动态分配的 IP 地址为 10.1.1.2。

此后，Device B 与 Device A 通信时采用的 IP 地址、MAC 地址等信息必须和授权 ARP 表项中的一致，否则将无法通信，保证了客户端的合法性。

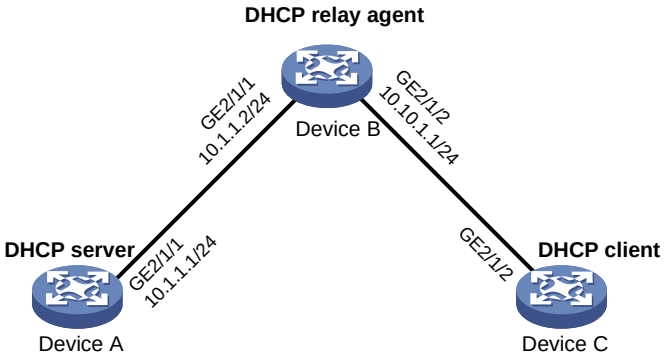
1.7.4 授权ARP功能在DHCP中继上的典型配置举例

1. 组网需求

- Device A 是 DHCP 服务器，为不同网段中的客户端动态分配 IP 地址，地址池网段为 10.10.1.0/24。
- Device B 是 DHCP 中继，通过在接口 GigabitEthernet2/1/2 上启用授权 ARP 功能来保证客户端的合法性。
- Device C 是 DHCP 客户端，通过 DHCP 中继从 DHCP 服务器获取 IP 地址。

2. 组网图

图1-4 授权 ARP 功能典型配置组网图



3. 配置步骤

(1) 配置 Device A

配置接口的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 2/1/1
[DeviceA-GigabitEthernet2/1/1] ip address 10.1.1.1 24
[DeviceA-GigabitEthernet2/1/1] quit
```

启用 DHCP 服务。

```
[DeviceA] dhcp enable
[DeviceA] dhcp server ip-pool 1
[DeviceA-dhcp-pool-1] network 10.10.1.0 mask 255.255.255.0
[DeviceA-dhcp-pool-1] gateway-list 10.10.1.1
[DeviceA-dhcp-pool-1] quit
[DeviceA] ip route-static 10.10.1.0 24 10.1.1.2
```

(2) 配置 Device B

启用 DHCP 服务。

```
<DeviceB> system-view
[DeviceB] dhcp enable
```

配置接口的 IP 地址。

```
[DeviceB] interface gigabitethernet 2/1/1
[DeviceB-GigabitEthernet2/1/1] ip address 10.1.1.2 24
[DeviceB-GigabitEthernet2/1/1] quit
[DeviceB] interface gigabitethernet 2/1/2
[DeviceB-GigabitEthernet2/1/2] ip address 10.10.1.1 24
```

配置 GigabitEthernet2/1/2 接口工作在 DHCP 中继模式。

```
[DeviceB-GigabitEthernet2/1/2] dhcp select relay
```

配置 DHCP 服务器的地址。

```
[DeviceB-GigabitEthernet2/1/2] dhcp relay server-address 10.1.1.1
```

启用接口授权 ARP 功能。

```
[DeviceB-GigabitEthernet2/1/2] arp authorized enable
[DeviceB-GigabitEthernet2/1/2] quit
```

开启 DHCP 中继用户地址表项记录功能。

```
[DeviceB] dhcp relay client-information record
```

(3) 配置 Device C

```
<DeviceC> system-view
[DeviceC] ip route-static 10.1.1.0 24 10.10.1.1
[DeviceC] interface gigabitethernet 2/1/2
[DeviceC-GigabitEthernet2/1/2] ip address dhcp-alloc
[DeviceC-GigabitEthernet2/1/2] quit
```

4. 验证配置

Device C 获得 Device A 分配的 IP 后，在 Device B 查看授权 ARP 信息。

```
[DeviceB] display arp all
  Type: S-Static   D-Dynamic   O-Openflow   M-Multiport  I-Invalid
IP Address       MAC Address     VLAN     Interface          Aging Type
10.10.1.2        0012-3f86-e94c  N/A      GE2/1/2             20    D
```

从以上信息可以获知 Device A 为 Device C 动态分配的 IP 地址为 10.10.1.2。

此后，Device C 与 Device B 通信时采用的 IP 地址、MAC 地址等信息必须和授权 ARP 表项中的一致，否则将无法通信，保证了客户端的合法性。

1.8 配置ARP Detection功能

说明

- 本特性仅在安装了二层交换卡的款型上支持。
- 文中的交换机指的是安装了二层以太网接口模块的路由器。

1.8.1 ARP Detection功能简介

ARP Detection 功能主要应用于接入设备上，对于合法用户的 ARP 报文进行正常转发，否则直接丢弃，从而防止仿冒用户、仿冒网关的攻击。

ARP Detection 包含三个功能：用户合法性检查、ARP 报文有效性检查、ARP 报文强制转发。

1. 用户合法性检查

对于 ARP 信任接口，不进行用户合法性检查；对于 ARP 非信任接口，需要进行用户合法性检查，以防止仿冒用户的攻击。

用户合法性检查是根据 ARP 报文中源 IP 地址和源 MAC 地址检查用户是否是所属 VLAN 所在接口上的合法用户，包括基于 IP Source Guard 静态绑定表项的检查、基于 DHCP Snooping 表项的检查。只要符合四者中的任何一个，就认为该 ARP 报文合法，进行转发。如果所有检查都没有找到匹配的表项，则认为是非法报文，直接丢弃。

IP Source Guard 静态绑定表项通过 **ip source binding** 命令生成，详细介绍请参见“安全配置指导”中的“IP Source Guard”。DHCP Snooping 安全表项通过 DHCP Snooping 功能自动生成，详细介绍请参见“三层技术-IP 业务配置指导”中的“DHCP Snooping”。

2. ARP报文有效性检查

对于 ARP 信任接口，不进行报文有效性检查；对于 ARP 非信任接口，需要根据配置对 MAC 地址和 IP 地址不合法的报文进行过滤。可以选择配置源 MAC 地址、目的 MAC 地址或 IP 地址检查模式。

- 源 MAC 地址的检查模式：会检查 ARP 报文中的源 MAC 地址和以太网报文头中的源 MAC 地址是否一致，一致则认为有效，否则丢弃报文；
- 目的 MAC 地址的检查模式（只针对 ARP 应答报文）：会检查 ARP 应答报文中的目的 MAC 地址是否为全 0 或者全 1，是否和以太网报文头中的目的 MAC 地址一致。全 0、全 1、不一致的报文都是无效的，需要被丢弃；
- IP 地址检查模式：会检查 ARP 报文中的源 IP 或目的 IP 地址，如全 1、或者组播 IP 地址都是不合法的，需要被丢弃。对于 ARP 应答报文，源 IP 和目的 IP 地址都进行检查；对于 ARP 请求报文，只检查源 IP 地址。

3. ARP报文强制转发

对于从 ARP 信任接口接收到的 ARP 报文不受此功能影响，按照正常流程进行转发；对于从 ARP 非信任接口接收到的并且已经通过用户合法性检查的 ARP 报文的处理过程如下：

- 对于 ARP 请求报文，通过信任接口进行转发；
- 对于 ARP 应答报文，首先按照报文中的以太网目的 MAC 地址进行转发，若在 MAC 地址表中没有查到目的 MAC 地址对应的表项，则将此 ARP 应答报文通过信任接口进行转发。

说明

- ARP 报文强制转发功能不支持目的 MAC 地址为多端口 MAC 的情况。
- 如果既配置了报文有效性检查功能，又配置了用户合法性检查功能，那么先进行报文有效性检查，然后进行用户合法性检查。

1.8.2 配置ARP Detection功能

1. 配置用户合法性检查功能

配置用户合法性检查功能时，必须至少配置 IP Source Guard 静态绑定表项、DHCP Snooping 功能、802.1X 功能和 OUI MAC 地址检查四者之一，否则所有从 ARP 非信任接口收到的 ARP 报文都将被丢弃。

在配置 IP Source Guard 静态绑定表项时，必须指定 VLAN 参数，否则 ARP 报文将无法通过基于 IP Source Guard 静态绑定表项的检查。

表1-10 配置用户合法性检查功能

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
使能ARP Detection功能	**arp detection enable**	缺省情况下，ARP Detection功能处于关闭状态，即不进行用户合法性检查
退回系统视图	**quit**	-

操作	命令	说明
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
（可选）将不需要进行用户合法性检查的接口配置为ARP信任接口	**arp detection trust**	缺省情况下，接口为ARP非信任接口

2. 配置ARP报文有效性检查功能

表1-11 配置 ARP 报文有效性检查功能

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
使能ARP Detection功能	**arp detection enable**	缺省情况下，ARP Detection功能处于关闭状态，即不进行用户合法性检查
退回系统视图	**quit**	-
使能ARP报文有效性检查功能	**arp detection validate** { **dst-mac** | **ip** | **src-mac** } *	缺省情况下，ARP报文有效性检查功能处于关闭状态
进入二层以太网接口视图	**interface** *interface-type interface-number*	-
（可选）将不需要进行ARP报文有效性检查的接口配置为ARP信任接口	**arp detection trust**	缺省情况下，接口为ARP非信任接口

3. 配置ARP报文强制转发功能

进行下面的配置之前，需要保证已经配置了用户合法性检查功能。

表1-12 配置 ARP 报文强制转发功能

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
使能ARP报文强制转发功能	**arp restricted-forwarding enable**	缺省情况下，ARP报文强制转发功能处于关闭状态

1.8.3 ARP Detection显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 ARP Detection 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，用户可以执行 **reset** 命令清除 ARP Detection 的统计信息。

表1-13 ARP Detection 显示和维护

操作	命令
显示使能了ARP Detection功能的VLAN	**display arp detection**
显示ARP Detection功能报文检查的丢弃计数的统计信息	**display arp detection statistics** [**interface** *interface-type interface-number*]
清除ARP Detection的统计信息	**reset arp detection statistics** [**interface** *interface-type interface-number*]

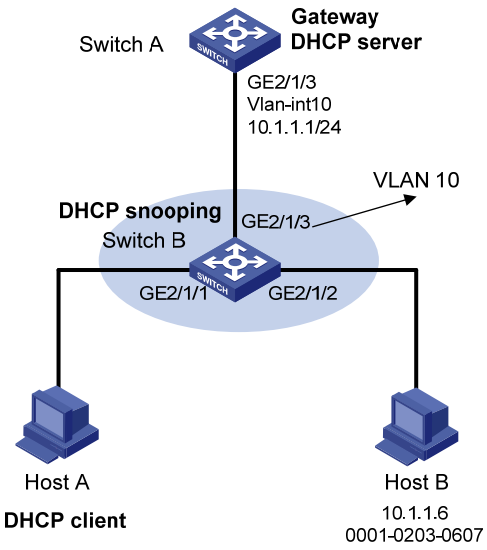
1.8.4 用户合法性检查和报文有效性检查配置举例

1. 组网需求

- Switch A 是 DHCP 服务器；
- Host A 是 DHCP 客户端；用户 Host B 的 IP 地址是 10.1.1.6，MAC 地址是 0001-0203-0607。
- Switch B 是 DHCP Snooping 设备，在 VLAN 10 内启用 ARP Detection 功能，对 DHCP 客户端和用户进行用户合法性检查和报文有效性检查。

2. 组网图

图1-5 配置用户合法性检查和报文有效性检查组网图



3. 配置步骤

(1) 配置组网图中所有接口属于 VLAN 及 Switch A 对应 VLAN 接口的 IP 地址（略）

(2) 配置 DHCP 服务器 Switch A

配置 DHCP 地址池 0。

```
<SwitchA> system-view
[SwitchA] dhcp enable
[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

(3) 配置 DHCP 客户端 Host A 和用户 Host B（略）

(4) 配置设备 Switch B

启用 DHCP Snooping 功能。

```
<SwitchB> system-view
[SwitchB] dhcp snooping enable
[SwitchB] interface gigabitethernet 2/1/3
[SwitchB-GigabitEthernet2/1/3] dhcp snooping trust
[SwitchB-GigabitEthernet2/1/3] quit
```

在接口 GigabitEthernet2/1/1 上启用 DHCP Snooping 表项记录功能。

```
[SwitchB] interface gigabitethernet 2/1/1
[SwitchB-GigabitEthernet2/1/1] dhcp snooping binding record
[SwitchB-GigabitEthernet2/1/1] quit
```

使能 ARP Detection 功能，对用户合法性进行检查。

```
[SwitchB] vlan 10
[SwitchB-vlan10] arp detection enable
```

接口状态缺省为非信任状态，上行接口配置为信任状态，下行接口按缺省配置。

```
[SwitchB-vlan10] interface gigabitethernet 2/1/3
[SwitchB-GigabitEthernet2/1/3] arp detection trust
[SwitchB-GigabitEthernet2/1/3] quit
```

在接口 GigabitEthernet2/1/2 上配置 IP Source Guard 静态绑定表项。

```
[SwitchB] interface gigabitethernet 2/1/2
[SwitchB-GigabitEthernet2/1/2] ip source binding ip-address 10.1.1.6 mac-address
0001-0203-0607 vlan 10
[SwitchB-GigabitEthernet2/1/2] quit
```

配置进行报文有效性检查。

```
[SwitchB] arp detection validate dst-mac ip src-mac
```

完成上述配置后，对于接口 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 收到的 ARP 报文，先进行报文有效性检查，然后基于 IP Source Guard 静态绑定表项、DHCP Snooping 安全表项进行用户合法性检查。

1.8.5 ARP报文强制转发配置举例

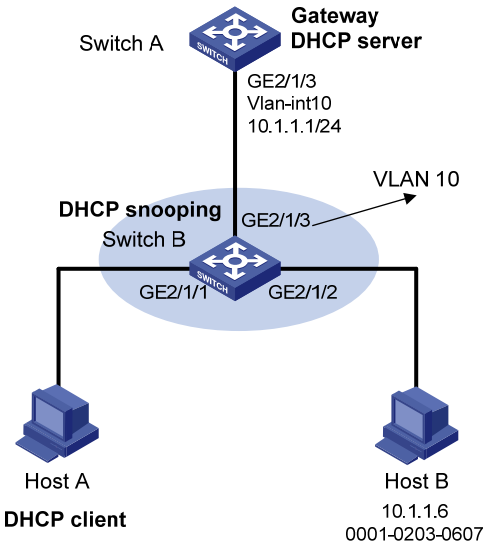
1. 组网需求

- Switch A 是 DHCP 服务器。
- Host A 是 DHCP 客户端；用户 Host B 的 IP 地址是 10.1.1.6，MAC 地址是 0001-0203-0607。
- Host A 和 Host B 在设备 Switch B 上端口隔离，但是均和网关 Switch A 相通，GigabitEthernet2/1/1、GigabitEthernet2/1/2、GigabitEthernet2/1/3 均属于 VLAN 10。
- Switch B 是 DHCP Snooping 设备，在 VLAN 10 内启用 ARP Detection 功能，对 DHCP 客户端和用户进行保护，保证合法用户可以正常转发报文，否则丢弃。

要求：Switch B 在启用 ARP Detection 功能后，对于 ARP 广播请求报文仍然能够进行端口隔离。

2. 组网图

图1-6 配置 ARP 报文强制转发组网图



3. 配置步骤

(1) 配置组网图中所有接口属于 VLAN 及 Switch A 对应 VLAN 接口的 IP 地址（略）

(2) 配置 DHCP 服务器 Switch A

配置 DHCP 地址池 0。

```
<SwitchA> system-view
[SwitchA] dhcp enable
[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

(3) 配置 DHCP 客户端 Host A 和用户 Host B（略）

(4) 配置设备 Switch B

配置 DHCP Snooping 功能。

```
<SwitchB> system-view
[SwitchB] dhcp snooping enable
[SwitchB] interface gigabitethernet 2/1/3
[SwitchB-GigabitEthernet2/1/3] dhcp snooping trust
[SwitchB-GigabitEthernet2/1/3] quit
```

使能 ARP Detection 功能，对用户合法性进行检查。

```
[SwitchB] vlan 10
[SwitchB-vlan10] arp detection enable
```

配置上行接口为信任状态，下行接口为缺省配置（非信任状态）。

```
[SwitchB-vlan10] interface gigabitethernet 2/1/3
[SwitchB-GigabitEthernet2/1/3] arp detection trust
[SwitchB-GigabitEthernet2/1/3] quit
```

在接口 GigabitEthernet2/1/2 上配置 IP Source Guard 静态绑定表项。

```
[SwitchB] interface gigabitethernet 2/1/2
```

```
[SwitchB-GigabitEthernet2/1/2] ip source binding ip-address 10.1.1.6 mac-address
0001-0203-0607 vlan 10
[SwitchB-GigabitEthernet2/1/2] quit
```

配置进行报文有效性检查。

```
[SwitchB] arp detection validate dst-mac ip src-mac
```

配置端口隔离。

```
[SwitchB] port-isolate group 1
[SwitchB] interface gigabitethernet 2/1/1
[SwitchB-GigabitEthernet2/1/1] port-isolate enable group 1
[SwitchB-GigabitEthernet2/1/1] quit
[SwitchB] interface gigabitethernet 2/1/2
[SwitchB-GigabitEthernet2/1/2] port-isolate enable group 1
[SwitchB-GigabitEthernet2/1/2] quit
```

完成上述配置后，对于接口 GigabitEthernet2/1/1 和 GigabitEthernet2/1/2 收到的 ARP 报文，先进行报文有效性检查，然后基于 IP Source Guard 静态绑定表项、DHCP Snooping 安全表项进行用户合法性检查。但是，Host A 发往 Switch A 的 ARP 广播请求报文，由于通过了用户合法性检查，所以能够被转发到 Host B，端口隔离功能失效。

配置 ARP 报文强制转发功能。

```
[SwitchB] vlan 10
[SwitchB-vlan10] arp restricted-forwarding enable
[SwitchB-vlan10] quit
```

此时，Host A 发往 Switch A 的合法 ARP 广播请求报文只能通过信任接口 GigabitEthernet1/0/3 转发，不能被 Host B 接收到，端口隔离功能可以正常工作。

1.9 配置ARP自动扫描、固化功能

1.9.1 ARP自动扫描、固化功能简介

ARP 自动扫描功能一般与 ARP 固化功能配合使用：

- 启用 ARP 自动扫描功能后，设备会对局域网内的邻居自动进行扫描（向邻居发送 ARP 请求报文，获取邻居的 MAC 地址，从而建立动态 ARP 表项）。
- ARP 固化功能用来将当前的 ARP 动态表项（包括 ARP 自动扫描生成的动态 ARP 表项）转换为静态 ARP 表项。通过对动态 ARP 表项的固化，可以有效防止攻击者修改 ARP 表项。

说明

建议在网吧这种环境稳定的小型网络中使用这两个功能。

1.9.2 配置ARP自动扫描、固化功能

配置 ARP 自动扫描、固化功能时，需要注意：

- 对于已存在 ARP 表项的 IP 地址不进行扫描。
- 扫描操作可能比较耗时，用户可以通过<Ctrl_C>来终止扫描（在终止扫描时，对于已经收到的邻居应答，会建立该邻居的动态 ARP 表项）。

- 固化后的静态 ARP 表项与配置产生的静态 ARP 表项相同。
- 固化生成的静态 ARP 表项数量同样受到设备可以支持的静态 ARP 表项数目的限制，由于静态 ARP 表项数量的限制可能导致只有部分动态 ARP 表项被固化。

表1-14 配置 ARP 自动扫描、固化功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
启动ARP自动扫描功能	**arp scan** [*start-ip-address* **to** *end-ip-address*]	-
退回系统视图	**quit**	-
配置ARP固化功能	**arp fixup**	-

说明

- 通过 **arp fixup** 命令将当前的动态 ARP 表项转换为静态 ARP 表项后，后续学习到的动态 ARP 表项可以通过再次执行 **arp fixup** 命令进行固化。
- 通过固化生成的静态 ARP 表项，可以通过命令行 **undo arp** *ip-address* [*vpn-instance-name*] 逐条删除，也可以通过命令行 **reset arp all** 或 **reset arp static** 全部删除。

1.10 配置ARP网关保护功能

说明

- 本特性仅在安装了二层交换卡的款型上支持。
- 文中的交换机指的是安装了二层以太网接口模块的路由器。

1.10.1 ARP网关保护功能简介

在设备上不与网关相连的接口上配置此功能，可以防止伪造网关攻击。

在接口上配置此功能后，当接口收到 ARP 报文时，将检查 ARP 报文的源 IP 地址是否和配置的被保护网关的 IP 地址相同。如果相同，则认为此报文非法，将其丢弃；否则，认为此报文合法，继续进行后续处理。

1.10.2 配置ARP网关保护功能

配置 ARP 网关保护功能，需要注意：

- 每个接口最多支持配置 8 个被保护的网关 IP 地址。
- 不能在同一接口下同时配置命令 **arp filter source** 和 **arp filter binding**。

- 本功能与 ARP Detection、MFF、ARP Snooping 功能配合使用时，先进行本功能检查，本功能检查通过后才会进行其他配合功能的处理。

表1-15 配置 ARP 网关保护功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口	**interface** *interface-type interface-number*	
开启ARP网关保护功能，配置被保护的网关IP地址	**arp filter source** *ip-address*	缺省情况下，ARP网关保护功能处于关闭状态

1.10.3 ARP网关保护功能配置举例

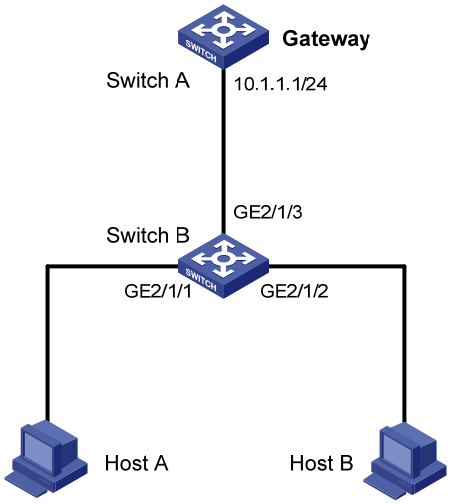
1. 组网需求

与 Switch B 相连的 Host B 进行了仿造网关 Switch A（IP 地址为 10.1.1.1）的 ARP 攻击，导致与 Switch B 相连的设备与网关 Switch A 通信时错误发往了 Host B。

要求：通过配置防止这种仿造网关攻击。

2. 组网图

图1-7 配置 ARP 网关保护功能组网图



3. 配置步骤

在 Switch B 上配置 ARP 网关保护功能。

```
<SwitchB> system-view
[SwitchB] interface gigabitethernet 2/1/1
[SwitchB-GigabitEthernet2/1/1] arp filter source 10.1.1.1
[SwitchB-GigabitEthernet2/1/1] quit
[SwitchB] interface gigabitethernet 2/1/2
[SwitchB-GigabitEthernet2/1/2] arp filter source 10.1.1.1
```

完成上述配置后，对于 Host B 发送的伪造的源 IP 地址为网关 IP 地址的 ARP 报文将会被丢弃，不会再被转发。

1.11 配置ARP过滤保护功能

说明

- 本特性仅在安装了二层交换卡的款型上支持。
- 文中的交换机指的是安装了二层以太网接口模块的路由器。

1.11.1 ARP过滤保护功能简介

本功能用来限制接口下允许通过的 ARP 报文，可以防止仿冒网关和仿冒用户的攻击。

在接口上配置此功能后，当接口收到 ARP 报文时，将检查 ARP 报文的源 IP 地址和源 MAC 地址是否和允许通过的 IP 地址和 MAC 地址相同：

- 如果相同，则认为此报文合法，继续进行后续处理；
- 如果不相同，则认为此报文非法，将其丢弃。

1.11.2 配置ARP过滤保护功能

配置 ARP 过滤保护功能，需要注意：

- 每个接口最多支持配置 8 组允许通过的 ARP 报文的源 IP 地址和源 MAC 地址。
- 不能在同一接口下同时配置命令 **arp filter source** 和 **arp filter binding**。
- 本功能与 ARP Detection、ARP Snooping 功能配合使用时，先进行本功能检查，本功能检查通过后才会进行其他配合功能的处理。

表1-16 配置 ARP 过滤保护功能

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网接口视图	**interface** *interface-type interface-number*	
开启ARP过滤保护功能，配置允许通过的ARP报文的源IP地址和源MAC地址	**arp filter binding** *ip-address mac-address*	缺省情况下，ARP过滤保护功能处于关闭状态

1.11.3 ARP过滤保护功能配置举例

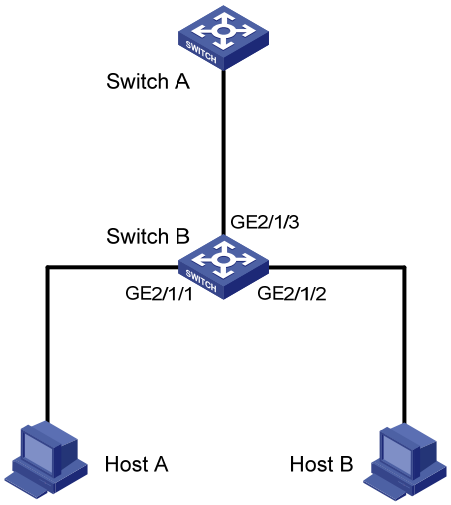
1. 组网需求

- Host A 的 IP 地址为 10.1.1.2，MAC 地址为 000f-e349-1233。
- Host B 的 IP 地址为 10.1.1.3，MAC 地址为 000f-e349-1234。

- 限制 Switch B 的 GigabitEthernet2/1/1、GigabitEthernet2/1/2 接口只允许指定用户接入，不允许其他用户接入。

2. 组网图

图1-8 配置 ARP 过滤保护功能组网图



3. 配置步骤

配置 Switch B 的 ARP 过滤保护功能。

```
<SwitchB> system-view
[SwitchB] interface gigabitethernet 2/1/1
[SwitchB-GigabitEthernet2/1/1] arp filter binding 10.1.1.2 000f-e349-1233
[SwitchB-GigabitEthernet2/1/1] quit
[SwitchB] interface gigabitethernet 2/1/2
[SwitchB-GigabitEthernet2/1/2] arp filter binding 10.1.1.3 000f-e349-1234
```

完成上述配置后，接口 GigabitEthernet2/1/1 收到 Host A 发出的源 IP 地址为 10.1.1.2、源 MAC 地址为 000f-e349-1233 的 ARP 报文将被允许通过，其他 ARP 报文将被丢弃；接口 GigabitEthernet2/1/2 收到 Host B 发出的源 IP 地址为 10.1.1.3、源 MAC 地址为 000f-e349-1234 的 ARP 报文将被允许通过，其他 ARP 报文将被丢弃。

目 录

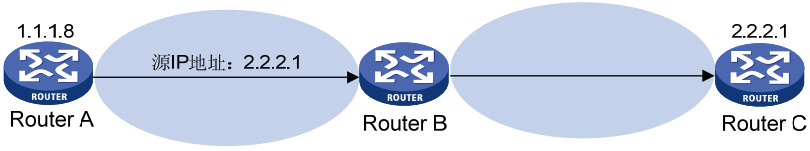
1 uRPF

1.1 uRPF简介

uRPF（Unicast Reverse Path Forwarding，单播反向路径转发）是一种单播逆向路由查找技术，用来防范基于源地址欺骗的攻击手段，例如基于源地址欺骗的 DoS（Denial of Service，拒绝服务）攻击和 DDoS（Distributed Denial of Service，分布式拒绝服务）攻击。

对于使用基于 IP 地址验证的应用来说，基于源地址欺骗的攻击手段可能导致未被授权用户以他人，甚至是管理员的身份获得访问系统的权限。因此即使响应报文没有发送给攻击者或其它主机，此攻击方法也可能会造成对被攻击对象的破坏。

图1-1 源地址欺骗攻击示意图



如 图 1-1 所示，攻击者在Router A上伪造并向Router B发送大量源地址为 2.2.2.1 的报文，Router B响应这些报文并向真正的“2.2.2.1”（Router C）回复报文。因此这种非法报文对Router B和Router C都造成了攻击。如果此时网络管理员错误地切断了Router C的连接，可能会导致网络业务中断甚至更严重的后果。

攻击者也可以同时伪造不同源地址的攻击报文或者同时攻击多个服务器，从而造成网络阻塞甚至网络瘫痪。

uRPF 可以有效防范上述攻击。一般情况下，设备在收到报文后会根据报文的目的地址对报文进行转发或丢弃。而 uRPF 可以在转发表中查找报文源地址对应的接口是否与报文的入接口相匹配，如果不匹配则认为源地址是伪装的并丢弃该报文，从而有效地防范网络中基于源地址欺骗的恶意攻击行为的发生。

1.1.2 uRPF检查方式

uRPF 检查有严格（strict）型和松散（loose）型两种。

1. 严格型uRPF检查

不仅检查报文的源地址是否在转发表中存在，而且检查报文的入接口与转发表是否匹配。

在一些特殊情况下（如非对称路由，即设备上行流量的入接口和下行流量的出接口不相同），严格型 uRPF 检查会错误地丢弃非攻击报文。

一般将严格型 uRPF 检查布置在 ISP 的用户端和 ISP 端之间。

2. 松散型uRPF检查

仅检查报文的源地址是否在转发表中存在，而不再检查报文的入接口与转发表是否匹配。

松散型 uRPF 检查可以避免错误的拦截合法用户的报文，但是也容易忽略一些攻击报文。

一般将松散型 uRPF 检查布置在 ISP-ISP 端。另外，如果用户无法保证路由对称，可以使用松散型 uRPF 检查。

1.1.3 uRPF技术优点

1. 支持与缺省路由的配合使用

当设备上配置了缺省路由后，会导致 uRPF 根据转发表检查源地址时，所有源地址都能查到下一跳。针对这种情况，支持用户配置 uRPF 是否允许匹配缺省路由。如果允许匹配缺省路由（配置 **allow-default-route**），则当 uRPF 查询转发表得到的结果是缺省路由时，认为查到了匹配的表项；如果不允许匹配缺省路由，则当 uRPF 查询转发表得到的结果是缺省路由时，认为没有查到匹配的表项。

缺省情况下，如果 uRPF 查询转发表得到的结果是缺省路由，则按没有查到表项处理，丢弃报文。运营商网络边缘位置一般不会有缺省路由指向客户侧设备，所以一般不需要配置 **allow-default-route**。如果在客户侧边缘设备接口上面启用 uRPF，这时往往会有缺省路由指向运营商，此时需要配置 **allow-default-route**。

2. 支持与链路层检查配合使用

严格型 uRPF 检查中还可以进一步进行链路层检查，即用源地址查转发表得到的下一跳地址再查一次 ARP 表，确保报文的源 MAC 地址和查到的 ARP 表项中的 MAC 地址一样才允许报文通过。

链路层检查功能对于运营商用一个三层以太网接口接入大量 PC 机用户时部署非常合适。

松散型 uRPF 检查不支持链路层检查功能。

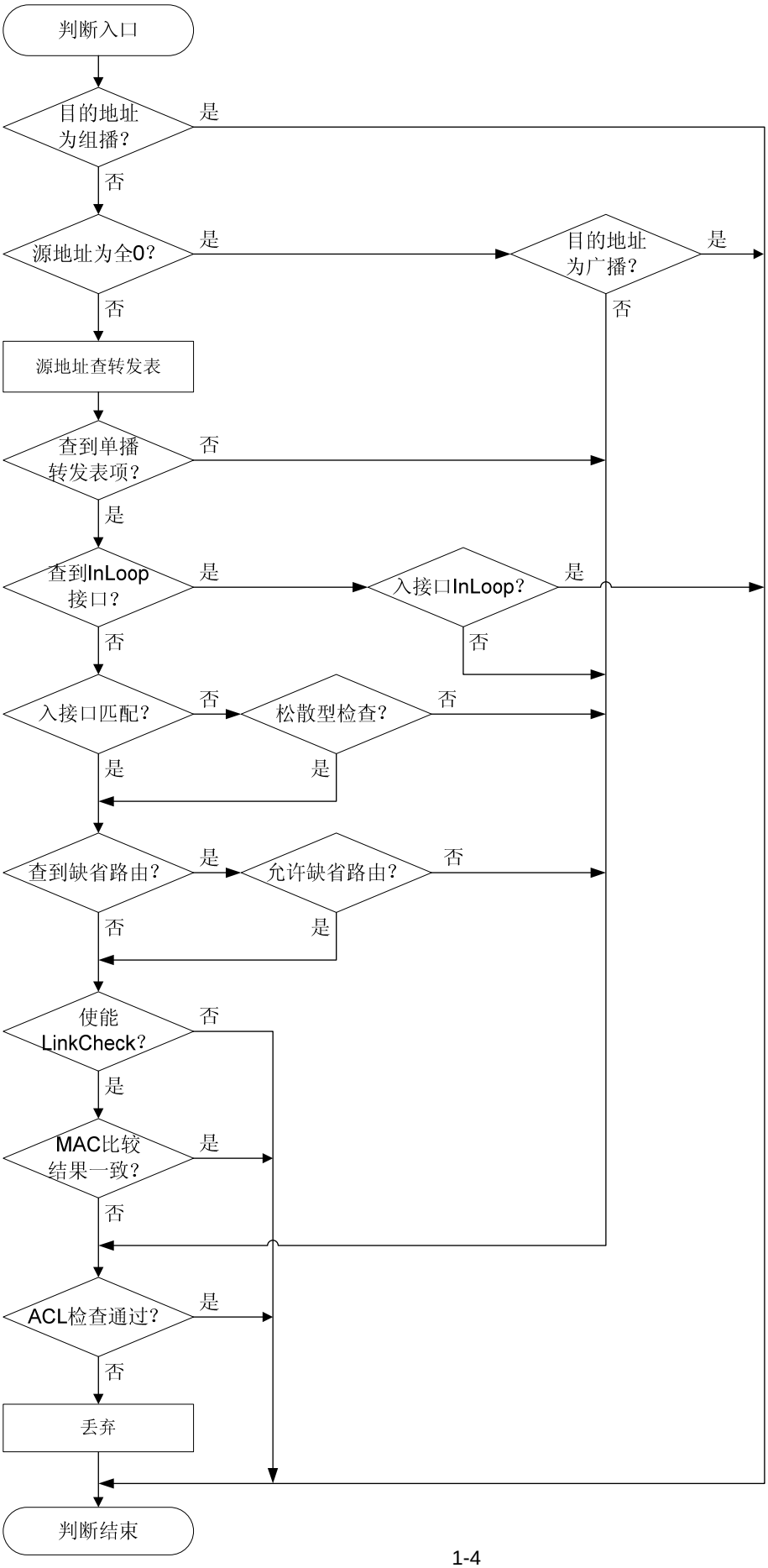
3. 支持与ACL的配合使用

如果用户确认具有某些特征的报文是合法报文，则可以在 ACL 中指定这些报文，那么这些报文在逆向路由不存在的情况下，不做丢弃处理，按正常报文进行转发。

1.1.4 uRPF处理流程

uRPF的处理流程如 图 1-2 所示。

图1-2 uRPF 处理流程图


判断入口
目的地址为组播?
是
否
源地址为全0?
是
目的地址为广播?
是
否
否
源地址查转发表
查到单播转发表项?
否
是
查到InLoop接口?
是
入接口InLoop?
是
否
否
入接口匹配?
否
松散型检查?
否
是
是
查到缺省路由?
是
允许缺省路由?
否
否
是
使能LinkCheck?
否
是
MAC比较结果一致?
是
否
ACL检查通过?
是
否
丢弃
判断结束

(1) 检查地址合法性：

- 对于目的地址是组播地址的报文，直接放行。
- 对于源地址是全零地址的报文，如果目的地址是广播，则放行（源地址为 0.0.0.0，目的地址为 255.255.255.255 的报文，可能是 DHCP 或者 BOOTP 报文，不做丢弃处理）；如果目的地址不是广播，则进入步骤（7）。
- 对于不是上述情况的报文，则进入步骤（2）。

(2) 检查报文的源地址在转发表中是否存在匹配的单播路由：如果在转发表中查找失败（源地址是非单播地址则会匹配到非单播路由），则进入步骤（7），否则进入步骤（3）；

(3) 如果转发表中匹配的是上送本机路由，即查到 InLoop 接口，则检查报文入接口是否是 InLoop 接口：如果是，则直接放行，否则进入步骤(7)；如果转发表中匹配的不是上送本机路由则继续步骤(4)；

(4) 如果转发表中匹配的是缺省路由，则检查用户是否配置了允许匹配缺省路由（参数 **allow-default-route**）：如果没有配置，则进入步骤（7），否则进入步骤（5）；如果转发表中匹配的不是缺省路由，则进入步骤（5）；

(5) 检查报文源地址与入接口是否匹配。反向查找报文出接口（反向查找是指查找以该报文源 IP 地址为目的 IP 地址的报文的出接口）或者缺省路由的出接口：如果其中至少有一个出接口和报文的入接口相匹配，则进入步骤（6）；如果不匹配，则查看是否是松散型检查，如果是，则报文检查通过，否则说明是严格型检查，进入步骤（7）；

(6) 检查用户是否配置了对链路层信息进行检查（参数 **link-check**）：如果没有配置，则认为报文通过检查，进行正常的转发。如果已经配置，则根据转发表中的下一跳查询 ARP 表，并比较 IP 报文源 MAC 地址与 ARP 表中的 MAC 地址是否一致。如果两者一致，则报文通过检查；如果查询失败或两者不一致，则进入步骤（7）；

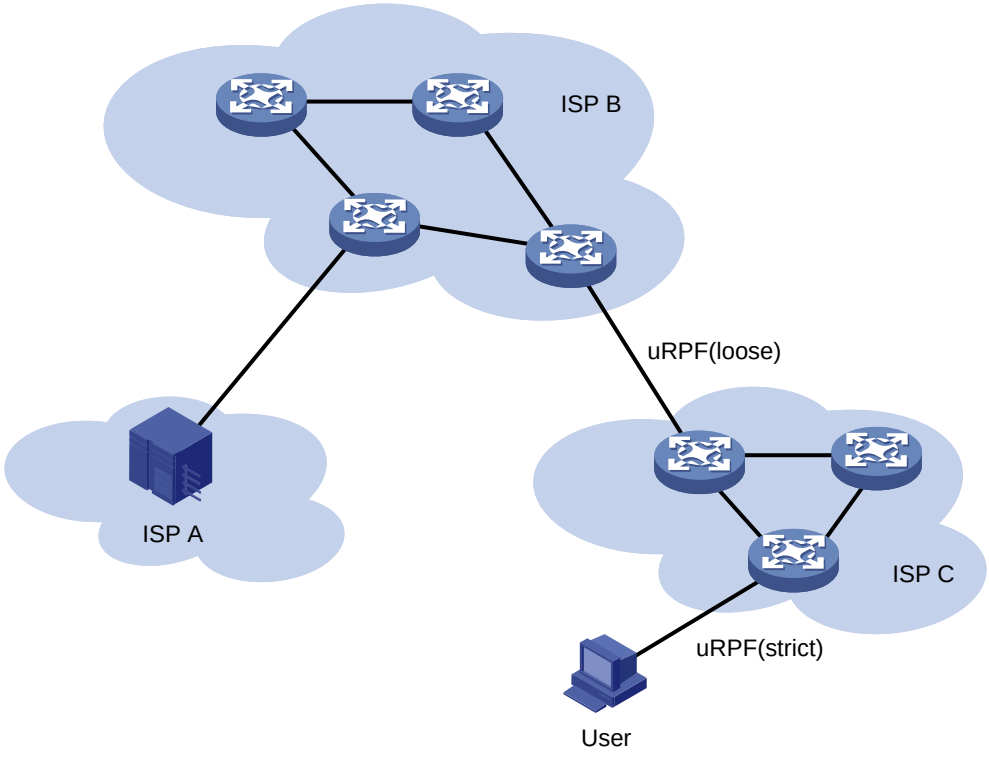
(7) ACL 检查流程。如果报文符合 ACL，则报文继续进行正常的转发（此类报文称为被抑制丢弃的报文）；否则报文被丢弃。

说明

组播报文不进行 uRPF 检查。

1.1.5 uRPF典型组网应用

图1-3 uRPF 典型组网应用



通常在 ISP 上配置 uRPF，在 ISP 与用户端，配置严格型 uRPF 检查，在 ISP 与 ISP 端，配置松散型 uRPF 检查。

如果有特殊用户，或者具有一定特征，需要特殊处理的报文，可以配置 ACL 规则。

1.2 配置uRPF

配置 uRPF 时，需要注意：

- uRPF 检查仅对接口收到的报文有效。
- 如果在接口下打开 uRPF 功能，用户可以通过 **display ip interface** 命令查看 uRPF 功能丢弃报文的统计信息（uRPF Information：Drops 表示被丢弃的报文数目；Suppressed drops 表示被抑制丢弃的报文数目）。
- 配置松散型 uRPF 检查时不建议配置 **allow-default-route** 参数，否则可能导致防攻击能力失效。

表1-1 配置接口 uRPF

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
在接口下打开uRPF功能	**ip urpf** { **loose** [**allow-default-route**] [**acl** *acl-number*] | **strict** [**allow-default-route**] [**acl** *acl-number*] [**link-check**] }	缺省情况下，uRPF功能处于关闭状态

1.3 uRPF显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置 uRPF 后的运行情况，通过查看显示信息验证配置的效果。

表1-2 uRPF 显示和维护

配置步骤	命令
显示uRPF的配置应用情况（MSR 2600/MSR 3600）	**display ip urpf** [**interface** *interface-type interface-number*]
显示uRPF的配置应用情况（MSR 5600）	**display ip urpf** [**interface** *interface-type interface-number*] [**slot** *slot-number*]

1.4 uRPF典型配置举例

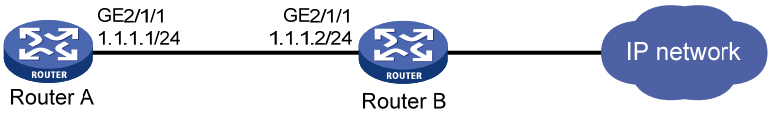
1.4.1 uRPF配置举例

1. 组网需求

- 客户路由器 Router A 与 ISP 路由器 Router B 直连，在 Router B 的接口 GigabitEthernet2/1/1 上配置严格型 uRPF 检查，源地址能够匹配 ACL 2010 的报文在任何情况下都能通过检查。
- 在 Router A 的接口 GigabitEthernet2/1/1 上配置严格型 uRPF 检查，同时允许匹配缺省路由。

2. 组网图

图1-4 uRPF 配置举例组网图



3. 配置步骤

(1) 配置 Router B

配置 ACL 2010，允许 10.1.1.0/24 网段的流量通过 uRPF 检查。

```
<RouterB> system-view
[RouterB] acl number 2010
[RouterB-acl-basic-2010] rule permit source 10.1.1.0 0.0.0.255
[RouterB-acl-basic-2010] quit
```

配置接口 GigabitEthernet2/1/1 的 IP 地址。

```
[RouterB] interface gigabitethernet 2/1/1
```

```
[RouterB-GigabitEthernet2/1/1] ip address 1.1.1.2 255.255.255.0
```

在接口 GigabitEthernet2/1/1 上配置严格型 uRPF 检查。

```
[RouterB-GigabitEthernet2/1/1] ip urpf strict acl 2010
```

(2) 配置 Router A

配置接口 GigabitEthernet2/1/1。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip address 1.1.1.1 255.255.255.0
```

在接口 GigabitEthernet2/1/1 上配置严格型 uRPF 检查，同时允许匹配缺省路由。

```
[RouterA-GigabitEthernet2/1/1] ip urpf strict allow-default-route
```

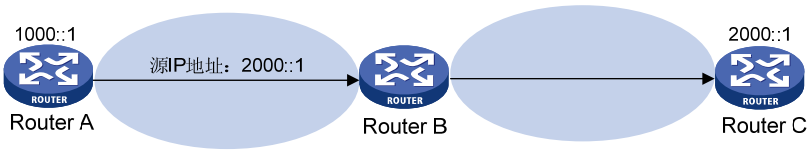
2 IPv6 uRPF

2.1 IPv6 uRPF简介

uRPF（Unicast Reverse Path Forwarding，单播反向路径转发）是一种单播逆向路由查找技术，用来防范基于源地址欺骗的攻击手段，例如基于源地址欺骗的 DoS（Denial of Service，拒绝服务）攻击和 DDoS（Distributed Denial of Service，分布式拒绝服务）攻击。

对于使用基于 IP 地址验证的应用来说，基于源地址欺骗的攻击手段可能导致未被授权用户以他人，甚至是管理员的身份获得访问系统的权限。因此即使响应报文没有发送给攻击者或其它主机，此攻击方法也可能会造成对被攻击对象的破坏。

图2-1 源地址欺骗攻击示意图



如 图 2-1 所示，攻击者在Router A上伪造并向Router B发送大量源地址为 2000::1 的报文，Router B响应这些报文并向真正的“2000::1”（Router C）回复报文。因此这种非法报文对Router B和Router C都造成了攻击。如果此时网络管理员错误地切断了Router C的连接，可能会导致网络业务中断甚至更严重的后果。

攻击者也可以同时伪造不同源地址的攻击报文或者同时攻击多个服务器，从而造成网络阻塞甚至网络瘫痪。

uRPF 可以有效防范上述攻击。一般情况下，设备在收到报文后会根据报文的目的地址对报文进行转发或丢弃。而 uRPF 可以在转发表中查找报文源地址对应的接口是否与报文的入接口相匹配，如果不匹配则认为源地址是伪装的并丢弃该报文，从而有效地防范网络中基于源地址欺骗的恶意攻击行为的发生。

2.1.2 IPv6 uRPF检查方式

IPv6 uRPF 检查有严格（strict）型和松散（loose）型两种。

1. 严格型IPv6 uRPF检查

不仅检查报文的源地址是否在 IPv6 转发表中存在，而且检查报文的入接口与 IPv6 转发表是否匹配。在一些特殊情况下（如非对称路由，即设备上行流量的入接口和下行流量的出接口不相同），严格型 IPv6 uRPF 检查会错误地丢弃非攻击报文。

一般将严格型 IPv6 uRPF 检查布置在 ISP 的用户端和 ISP 端之间。

2. 松散型IPv6 uRPF检查

仅检查报文的源地址是否在 IPv6 转发表中存在，而不再检查报文的入接口与 IPv6 转发表是否匹配。松散型 IPv6 uRPF 检查可以避免错误的拦截合法用户的报文，但是也容易忽略一些攻击报文。

一般将松散型 IPv6 uRPF 检查布置在 ISP-ISP 端。另外，如果用户无法保证路由对称，可以使用松散型 IPv6 uRPF 检查。

2.1.3 IPv6 uRPF技术优点

1. 支持与缺省路由的配合使用

当设备上配置了缺省路由后，会导致 IPv6 uRPF 根据 IPv6 转发表检查源地址时，所有源地址都能查到下一跳。针对这种情况，支持用户配置 IPv6 uRPF 是否允许匹配缺省路由。如果允许匹配缺省路由（配置 **allow-default-route**），则当 IPv6 uRPF 查询 IPv6 转发表得到的结果是缺省路由时，认为查到了匹配的表项；如果不允许匹配缺省路由，则当 IPv6 uRPF 查询 IPv6 转发表得到的结果是缺省路由时，认为没有查到匹配的表项。

缺省情况下，如果 IPv6 uRPF 查询 IPv6 转发表得到的结果是缺省路由，则按没有查到表项处理，丢弃报文。

运营商网络边缘位置一般不会有缺省路由指向客户侧设备，所以一般不需要配置 **allow-default-route**。如果在客户侧边缘设备接口上面启用 IPv6 uRPF，这时往往会有缺省路由指向运营商，此时需要配置 **allow-default-route**。

2. 支持与ACL的配合使用

如果用户确认具有某些特征的报文是合法报文，则可以在 IPv6 ACL 中指定这些报文，那么这些报文在逆向路由不存在的情况下，不做丢弃处理，按正常报文进行转发。

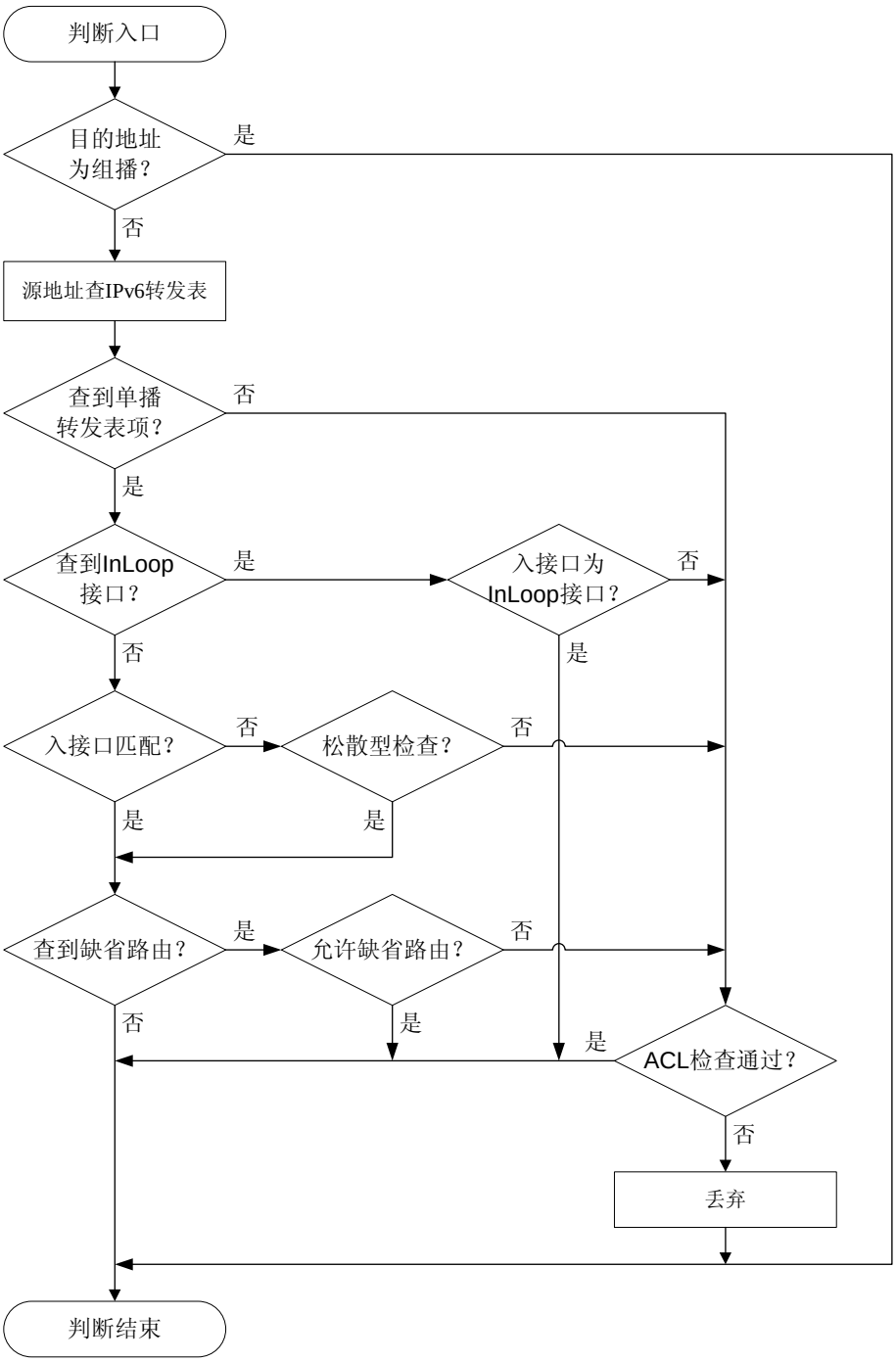
2.1.4 IPv6 uRPF处理流程


说明

组播报文不进行 IPv6 uRPF 检查。

IPv6 uRPF的处理流程如 图 2-2 所示。

图2-2 IPv6 uRPF 处理流程图



(1) 检查地址合法性：对于目的地址是组播地址的报文直接放行。否则，进入步骤（2）；

(2) 检查报文的源地址在 IPv6 转发表中是否存在匹配的单播路由：如果在 IPv6 转发表中查找失败（源地址是非单播地址则会匹配到非单播路由），则进入步骤（6），否则进入步骤（3）；

(3) 如果 IPv6 转发表中匹配的是上送本机路由，则检查报文入接口是否是 InLoop 接口：如果是，则直接放行，否则进入步骤（6）；如果 IPv6 转发表中匹配的不是上送本机路由则继续步骤（4）；如果源地址是 Link-Local 地址，倘若这个地址是入接口的地址，并且入接口不是 InLoop 接口则进入步骤（6），否则直接放行；

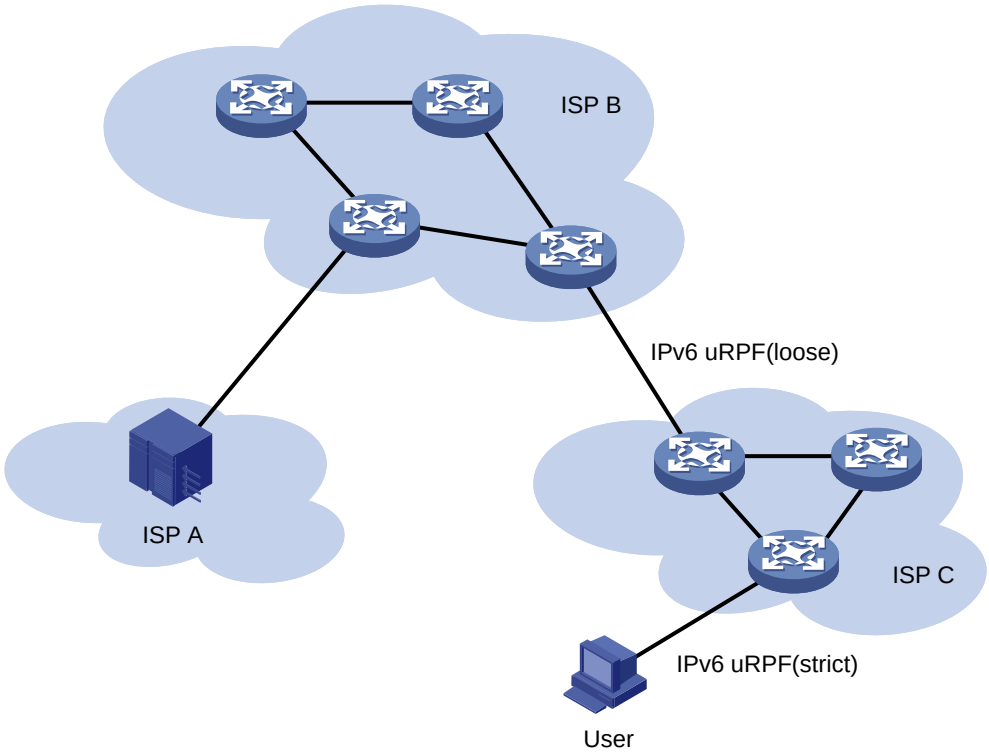
(4) 检查报文源地址与入接口是否匹配：反向查找报文出接口（反向查找是指查找以该报文源 IPv6 地址为目的 IPv6 地址的报文的出接口）或者缺省路由的出接口，如果其中至少有一个出接口和报文的入接口相匹配，则进入步骤（5）；如果不匹配，则查看是否是松散型检查，如果是，则进入步骤（5），否则说明是严格型检查，进入步骤（6）；

(5) 如果 IPv6 转发表中匹配的是缺省路由，则检查用户是否配置了允许匹配缺省路由（参数 **allow-default-route**），如果没有配置，则进入步骤（6），否则处理结束报文正常转发；如果 IPv6 转发表中匹配的不是缺省路由，则处理结束报文正常转发；

(6) IPv6 ACL 检查流程。如果报文符合 IPv6 ACL，则报文继续进行正常的转发（此类报文称为被抑制丢弃的报文）；否则报文被丢弃。

2.1.5 IPv6 uRPF典型组网应用

图2-3 IPv6 uRPF 典型组网应用



通常在 ISP 上配置 uRPF，在 ISP 与用户端，配置严格型 IPv6 uRPF 检查，在 ISP 与 ISP 端，配置松散型 IPv6 uRPF 检查。

如果有特殊用户，或者具有一定特征，需要特殊处理的报文，可以配置 IPv6 ACL 规则。

2.2 配置IPv6 uRPF

表2-1 配置接口 IPv6 uRPF

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入接口视图	**interface** *interface-type interface-number*	-
在接口下打开IPv6 uRPF功能	**ipv6 urpf** { **loose** | **strict** } [**allow-default-route**] [**acl** *acl-number*]	缺省情况下，IPv6 uRPF功能处于关闭状态

说明

- IPv6 uRPF 检查仅对接口收到的报文有效。
- 如果在接口下打开 IPv6 uRPF 功能，用户可以通过 **display ipv6 interface** 命令查看 IPv6 uRPF 功能丢弃报文的统计信息（IPv6 uRPF Information: Drops 表示被丢弃的报文数目；Suppressed drops 表示被抑制丢弃的报文数目）。
- 配置松散型 IPv6 uRPF 检查时不建议配置 **allow-default-route** 参数，否则可能导致防攻击能力失效。

2.3 IPv6 uRPF显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置 IPv6 uRPF 后的运行情况，通过查看显示信息验证配置的效果。

表2-2 IPv6 uRPF 显示和维护

配置步骤	命令
显示IPv6 uRPF的配置应用情况（MSR 2600/MSR 3600）	**display ipv6 urpf** [**interface** *interface-type interface-number*]
显示IPv6 uRPF的配置应用情况（MSR 5600）	**display ipv6 urpf** [**interface** *interface-type interface-number*] [**slot** *slot-number*]

2.4 IPv6 uRPF典型配置举例

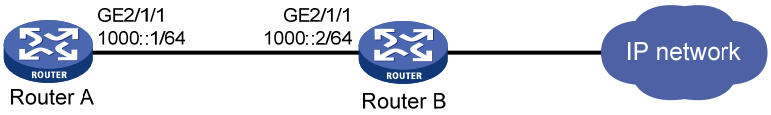
2.4.1 IPv6 uRPF配置举例

1. 组网需求

- 客户路由器 Router A 与 ISP 路由器 Router B 直连，在 Router B 的接口 GigabitEthernet2/1/1 上配置严格型 IPv6 uRPF 检查，源地址能够匹配 IPv6 ACL 2010 的报文在任何情况下都能通过检查。
- 在 Router A 的接口 GigabitEthernet2/1/1 上配置严格型 IPv6 uRPF 检查，同时允许匹配缺省路由。

2. 组网图

图2-4 IPv6 uRPF 配置举例组网图



3. 配置步骤

(1) 配置 Router B

配置 IPv6 ACL 2010，允许 1010::/64 网段的流量通过 IPv6 uRPF 检查。

```
<RouterB> system-view
[RouterB] acl ipv6 number 2010
[RouterB-acl-basic-2010] rule permit source 1010:: 64
[RouterB-acl-basic-2010] quit
```

配置接口 GigabitEthernet2/1/1 的 IPv6 地址。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] ipv6 address 1000::2/64
```

在接口 GigabitEthernet2/1/1 上配置严格型 IPv6 uRPF 检查。

```
[RouterB-GigabitEthernet2/1/1] ipv6 urpf strict acl 2010
```

(2) 配置 Router A

配置接口 GigabitEthernet2/1/1。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] ip address 1000::1/64
```

在接口 GigabitEthernet2/1/1 上配置严格型 IPv6 uRPF 检查，同时允许匹配缺省路由。

```
[RouterA-GigabitEthernet2/1/1] ipv6 urpf strict allow-default-route
```

目 录

1 加密引擎

1.1 加密引擎简介

加密引擎是专门用于提供数据加/解密服务的硬件及软件的统称，具体分为硬件加密引擎和软件加密引擎两种类型。

- 硬件加密引擎是集成在 CPU 上的协处理器或者硬件加密卡，由于使用硬件进行加/解密处理，因此具有加速加密的能力，可以提高设备的处理效率。硬件加密引擎的开关状态可由配置控制；
- 软件加密引擎是设备上所有软件加密算法的集合，通过系统自身的软件算法进行加/解密处理。软件加密引擎一直处于开启状态，不可配。

当硬件加密引擎处于开启状态时，设备优先选择硬件加密引擎执行加/解密功能，若设备不支持硬件加密引擎或者其上的所有硬件加密引擎均不支持业务模块所要求的算法时，设备会选择软件加密引擎执行相应的加/解密功能；当硬件加密引擎处于关闭状态时，设备只能选择软件加密引擎执行加/解密功能。

加密引擎可以为 IPsec 等需要加密的业务模块服务，与业务模块的交互过程是：各业务模块将需要加/解密的数据发送给加密引擎，加密引擎对数据进行加/解密处理，然后加密引擎将处理后的数据发送回各业务模块。

1.2 配置硬件加密引擎

硬件加密引擎默认是开启的，可以通过 **crypto-engine accelerator disable** 命令关闭该功能。关闭硬件加密引擎会严重影响加/解密性能，因此仅允许在测试、调试或故障排除的环境下关闭，正常情况下不建议关闭该功能。

硬件加密引擎的开启或关闭状态的改变对业务模块的影响由业务模块决定，例如，对于 IPsec 业务来说，硬件加密引擎状态的改变只对新建立的 IPsec SA 有影响，已建的 IPsec SA 仍旧使用之前选择的加密引擎来处理。因此，建议在开启或关闭硬件加密引擎之后，使用 **reset ipsec sa** 命令将当前已有的 IPsec SA 删除，使得所有新建立的 IPsec SA 都将使用新选择的加密引擎处理流程来处理。

表1-1 配置硬件加密引擎

操作	命令	说明
进入系统视图	**system-view**	-
关闭硬件加密引擎	**crypto-engine accelerator disable**	缺省情况下，硬件加密引擎处于开启状态
开启硬件加密引擎	**undo crypto-engine accelerator disable**	

1.3 加密引擎显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示加密引擎的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除加密引擎的统计信息。

表1-2 会话管理显示和维护

操作	命令
显示加密引擎的基本信息	**display crypto-engine**
显示加密引擎的统计信息（MSR 2600/MSR 3600）	**display crypto-engine statistics** [**engine-id** *engine-id*]
显示加密引擎的统计信息（MSR 5600）	**display crypto-engine statistics** [**engine-id** *engine-id* **slot** *slot-number*]
清除加密引擎的统计计数（MSR 2600/MSR 3600）	**reset crypto-engine statistics** [**engine-id** *engine-id*]
清除加密引擎的统计计数（MSR 5600）	**reset crypto-engine statistics** [**engine-id** *engine-id* **slot** *slot-number*]

目 录

1 FIPS

1.1 FIPS简介

FIPS（Federal Information Processing Standards，联邦信息处理标准）140-2 是 NIST（National Institute of Standard and Technology，美国标准与技术研究所）颁布的针对密码算法安全的一个标准，它规定了一个安全系统中的密码模块应该满足的安全性要求。FIPS 140-2 定义了四个安全级别：Level 1、Level 2、Level 3 和 Level 4，它们安全等级依次递增，可广泛适用于密码模块的各种应用环境。目前，设备支持 Level 2 级别的 FIPS 140-2。

若无特殊说明，本文中的 FIPS 即表示 FIPS 140-2。

1.2 配置限制和指导

- 执行 **fips mode enable** 命令之后，系统会提示用户选择启动方式，若用户未在 30 秒内作出选择，则系统默认用户采用了手动启动方式。
- 设备重启进入 FIPS 模式之前，系统会自动删除所有非 FIPS 模式下配置的密钥对和不符合 FIPS 标准（密钥位数小于 2048 位，签名 HSAH 算法为 MD5）的数字证书。因此，由非 FIPS 模式切换到 FIPS 模式后，用户将无法直接通过 SSH 方式登录设备。若需要进行 SSH 登录，必须先在 FIPS 模式下，通过 Console/AUX/Async 口登录设备，并创建 SSH 服务器所需的密钥对，才能支持 SSH 用户登录。
- 登录 FIPS 模式下的设备时使用的用户密码必须符合 Password Control 密码管理策略，例如必须符合一定的密码长度策略、密码复杂度策略以及密码老化策略等。其中，密码的老化时间策略需要关注。当密码的使用时间超过老化时间后，系统会要求用户及时更换密码。一般设备的出厂系统时间比较早，等到进入 FIPS 模式之后再去调整正确的系统时间很可能会导致登录密码在下一次登录系统时过期。因此，如果选择自动重启方式进入 FIPS 模式，则建议在执行 **fips mode enable** 命令之前设置正确的系统时间；如果选择手动重启方式进入 FIPS 模式，则建议在配置本地用户名和密码之前设置正确的系统时间。
- 如果采用手动重启方式进入 FIPS 模式，在保存当前配置并设置为下次启动配置文件后，必须首先删除二进制类型的下次启动配置文件，然后再重启设备。如果不删除二进制类型的下次启动配置文件，则设备使用二进制配置文件启动时，FIPS 模式下不支持的命令（如果存在于配置文件中）也会被恢复，从而影响 FIPS 模式下系统的正常运行。
- 执行 **fips mode enable** 命令之后到系统重启之前的这个时间段，系统将进入一个准备进入 FIPS 模式之前的中间状态，若选择手动方式重启，则不建议在这个时间段执行除 **reboot**、**save** 以及相应的配置准备之外的其它命令，否则可能会不能达到预期的执行效果。
- FIPS 模式下的配置支持配置回滚，FIPS 模式与非 FIPS 模式之间的配置也支持配置回滚。需要注意的是，对 FIPS 模式与非 FIPS 模式之间的配置执行回滚操作后，建议删除登录设备的本地用户并重新设置登录设备的本地用户（包括密码、用户角色和服务类型等属性），然后保存当前配置并设置为下次启动配置文件，最后重启设备。重启之后，回滚后的配置才能生效。此过程期间，请勿退出系统或进行其它操作，否则可能会登录失败。

- 为保证自动重启方式进入的 FIPS 模式与非 FIPS 模式之间的配置成功进行回滚，设备进入 FIPS 模式后请首先保存配置，然后进行其它操作；为保证自动重启方式进入的非 FIPS 模式与 FIPS 模式之间的配置成功进行回滚，设备进入非 FIPS 模式后请首先保存配置，然后进行其它操作。

1.3 配置FIPS模式

1.3.1 进入FIPS模式

使能 FIPS 模式并重启设备之后，设备会运行于支持 FIPS 140-2 标准的工作模式下。在该工作模式下，系统将具有更为严格的安全性要求，并会对密码模块进行相应的自检处理，以确认其处于正常运行状态。

进入 FIPS 模式的设备同时也符合 CC（Common Criteria，公共准则）中的 NDPP（Network Device Protection Profile，网络设备保护特性）定义的功能要求。

系统提供了两种启动选择来进入 FIPS 模式：自动重启方式和手动重启方式。

1. 自动重启方式

该方式下，系统自动创建一个 FIPS 缺省配置文件（名称为 fips-startup.cfg），同时将其指定为下次启动配置文件，在要求用户完成配置下次登录设备所需的用户名和密码之后，自动使用 FIPS 缺省配置文件重启。具体步骤如下：

(1) 用户使能 FIPS 模式。

(2) 用户手工选择自动重启。如果在以下的输入过程中想退出配置流程，可以使用组合键<Ctrl+C>中断配置流程。配置流程中断后，已输入的使能 FIPS 模式的命令将不被执行。

(3) 用户手工配置登录 FIPS 模式的设备时所使用的用户名和密码。该用户将会成为 FIPS 模式中安全管理员（Crypto Officer），其密码必须是大写字母、小写字母、数字以及特殊字符的组合，且最小长度为 15 位。

(4) 用户成功设置安全管理员用户名和登录密码之后，系统自动使用指定的启动配置文件重启。

(5) 系统进入 FIPS 模式。用户只能通过步骤（3）设置的用户名和密码登录运行于 FIPS 模式的设备。

2. 手动重启方式

该方式下，系统不自动创建进入 FIPS 模式的下次启动配置文件，需要用户手工完成进入 FIPS 模式所需的所有必要配置之后，手工重启设备。具体步骤如下：

(1) 用户完成以下配置准备，主要包括：

- 使能全局 Password Control 功能。
- 设置全局 Password Control 密码组合类型的个数为 4，每种类型至少 1 个字符。
- 设置全局 Password Control 的密码最小长度为 15。
- 添加设备管理类本地用户，设置密码、用户角色和服务类型。本地用户的密码需要符合以上 Password Control 配置的限制，用户角色必须是 network-admin，服务类型为 terminal。
- 删除不符合 FIPS 标准的本地用户服务类型（Telnet、HTTP 和 FTP）。

(2) 用户使能 FIPS 模式。

(3) 用户手工选择手动重启。

(4) 用户手工保存当前配置文件并设置为下次启动配置文件。

(5) 用户手工删除二进制类型的下次启动配置文件（文件名后缀为“.mdb”）。

(6) 重启设备。

(7) 系统进入 FIPS 模式。用户只能通过步骤（1）设置的本地用户名和密码登录处于 FIPS 模式的设备。

表1-1 使能 FIPS 模式

操作	命令	说明
进入系统视图	**system-view**	-
使能FIPS模式	**fips mode enable**	缺省情况下，FIPS模式处于关闭状态

1.3.2 FIPS模式下的配置变化

系统进入 FIPS 模式，设备上的以下功能将发生变化：

- 仅支持 **scheme** 类型的用户登录认证方式。
- FTP/TFTP 服务器和客户端功能被禁用。
- Telnet 服务器和客户端功能被禁用。
- HTTP 服务器功能被禁用。
- SNMPv1 和 SNMPv2c 版本的 SNMP 功能被禁用，只允许使用 SNMPv3 版本。
- SSL 服务器功能只支持 TLS1.0 协议。
- SSH 服务器功能不兼容 SSHv1 客户端，不支持 DSA 类型的密钥对。
- 仅支持生成 2048 位的 RSA 密钥对和 2048 位的 DSA 密钥对。因此设备作为服务器时，若要求对客户端进行公钥认证，则客户端的密钥对也需要为 2048 位，否则服务器将会拒绝客户端的连接。
- SSH、SNMPv3、IPsec 和 SSL 不支持 DES、3DES、RC4、MD5 算法。
- 不能关闭全局 Password Control 功能，即 **undo password control enable** 命令执行后不生效。
- 部分特性中的密码设置将具有更严格的安全性要求：
  - AAA 服务器的共享密钥、IKE 协商的预共享密钥、SNMPv3 用户的认证密钥都必须满足固定的要求：密码最小长度为 15，密码元素的最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符）。
  - 设备管理类本地用户的密码和用户角色切换密码受 Password Control 密码策略的管理，缺省要求为：密码最小长度为 15，密码元素的最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符）。

1.3.3 退出FIPS模式

关闭 FIPS 模式并重启设备之后，设备会返回到非 FIPS 的工作模式下。在该工作模式下，系统将不再具有 FIPS 模式所需的安全性要求，也不会对密码模块进行相应的自检处理。

系统提供了两种启动方式来退出 FIPS 模式：

- 自动重启方式：系统自动创建一个非 FIPS 缺省配置文件（名称为 non-fips-startup.cfg），同时将其指定为下次启动配置文件，之后自动使用非 FIPS 缺省配置文件重启。重启之后，当前登录用户不需要输入任何信息即可直接登录到非 FIPS 模式的系统。
- 手动重启方式：系统不自动创建进入非 FIPS 模式的下次启动配置文件，需要用户手工完成进入非 FIPS 模式所需的所有必要配置之后，手工重启设备。重启之后，当前登录用户需要根据配置的登录认证方式输入相应的用户信息登录到非 FIPS 模式的系统。

从 FIPS 模式切换到非 FIPS 模式时，登录设备的缺省认证方式如下，用户也可根据实际情况修改登录认证方式：

- 通过 VTY 用户线登录设备时的缺省认证方式为 **password**。
- 若设备同时支持 Console 口和 AUX 口，则通过 Console 口登录设备时的缺省认证方式为 **none**，通过 AUX 口登录设备时的缺省认证方式为 **password**。
- 若设备支持 Console 口或 AUX 口之一，则通过 Console 口和通过 AUX 口登录设备时的缺省认证方式均为 **none**。

关闭 FIPS 模式之后、选择手动重启设备之前，需要注意的是：

- 对于当前远程登录的用户，若要登录非 FIPS 模式，则必须在不退出当前用户线的情况下，重新设置登录设备的认证方式为 **scheme**，并设置对应的登录用户和密码（也可使用当前的登录用户和密码）。
- 对于当前通过 Console/AUX/Async 口登录的用户，若要登录非 FIPS 模式的系统：
  - 如果使用 **password** 登录认证方式，则还需要设置相应的认证方式为 **password**，并设置对应的登录密码。
  - 如果使用 **scheme** 登录认证方式，则需要设置相应的认证方式为 **scheme**，并设置对应的登录用户和密码（也可使用当前的登录用户和密码）。
  - 如果使用 **none** 登录认证方式，则需要设置相应的认证方式为 **none**。

表1-2 关闭 FIPS 模式

操作	命令	说明
进入系统视图	**system-view**	-
关闭FIPS模式	**undo fips mode enable**	缺省情况下，FIPS模式处于关闭状态

1.4 FIPS密码算法自检处理

FIPS 模式处于使能状态之后，为确保密码算法模块的功能正常运行，系统会进行一定的自检处理，具体包括启动自检、条件自检。启动自检失败后，自检进程所在的单板自动重启。条件自检失败后，自检进程所在的单板不重启，但系统会输出密码算法自检失败的提示信息。

设备运行过程当中，当用户或管理员需要确认当前 FIPS 模式下的系统中的密码算法模块是否正常工作时，可以通过执行命令来手工触发系统进行密码算法自检工作。手工自检失败后，整个设备会自动重启。

注意

如果自检失败，请联系用服工程师解决。

1.4.1 启动自检（Power-up Self-tests）

启动自检是在设备启动过程中对 FIPS 允许使用的密码算法进行的自检。启动自检也称为已知结果的自检，即使用密码算法对已知的密钥和明文进行运算，如果运算结果与已知结果相同，则表示该算法的启动自检通过，否则表示自检失败。

启动自检又分为以下几种类型，具体内容如 表 1-3 所示。

表1-3 启动自检列表

启动自检类型	自检操作
软件加密算法自检	对以下软件加密算法进行自检： • DSA（签名和验证） • RSA（签名和验证） • RSA（加密和解密） • AES • 3DES • SHA1 • HMAC-SHA1 • 随机数生成算法
加密引擎自检	在支持加密引擎的设备上，对以下加密引擎使用的算法进行自检： • SHA1 • HMAC-SHA1 • AES • RSA（签名和验证） • RSA（加密和解密） • DSA（签名和验证） • 随机数生成算法

1.4.2 条件自检（Conditional Self-tests）

条件自检是在非对称密码模块和随机数生成模块被使用时进行的自检，具体包括以下两种测试：

- 密钥对有效性测试：生成 DSA/RSA 非对称密钥对时进行的自检，具体为，首先使用公钥加密任意一段明文，然后使用对应的私钥对生成的密文进行解密，如果解密成功，则表示自检通过，否则自检失败。
- 随机数连续性测试：生成随机数的过程中进行的自检，如果前后两次生成的随机数不同，则表示自检通过，否则自检失败。该自检过程也会在生成 DSA/RSA 非对称密钥对时进行。

1.4.3 手工触发密码算法自检

手工触发的密码算法自检内容与设备启动时自动进行的启动自检（Power-up Self-tests）内容相同。该自检失败后，设备会自动重启。

表1-1 手工触发密码算法自检

操作	命令	说明
进入系统视图	**system-view**	-
手工触发密码算法自检	**fips self-test**	-

1.5 FIPS显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 FIPS 模式的状态，通过查看显示信息验证配置的效果。

表1-2 FIPS 的显示和维护

操作	命令
显示FIPS模式的状态	**display fips status**

1.6 FIPS典型配置举例

1.6.1 自动重启设备进入FIPS模式

1. 组网需求

自动重启设备进入 FIPS 模式，并采用 Console/AUX/Async 口登录 FIPS 模式的设备。

2. 配置步骤

若要保存当前配置，请在使能 FIPS 模式之前，执行 **save** 命令。

使能 FIPS 模式，并选择自动重启方式进入 FIPS 模式。设置用户名为 root，对应的密码为 12345zxcvb!@#$%ZXCVB。

```
<Sysname> system-view
[Sysname] fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
Reboot the device automatically? [Y/N]:y
The system will create a new startup configuration file for FIPS mode. After you set the login
username and password for FIPS mode, the device will reboot automatically.
Enter username(1-55 characters):root
Enter password(15-63 characters):
Confirm password:
Waiting for reboot... After reboot, the device will enter FIPS mode.
```

3. 验证结果

重启设备后，输入用户名 root 和对应的密码。首次登录时，系统会提示重置密码。重置密码成功后，进入 FIPS 模式的系统。重置的密码必须是大写字母、小写字母、数字以及特殊字符的组合，最小长度为 15 位，且需要与旧密码不同（具体要求请见系统提示）。

```
Press ENTER to get started.
login: root
Password:
First login or password reset. For security reason, you need to change your password. Please enter your password.
old password:
new password:
confirm:
Updating user information. Please wait ... ...
…（略）
<Sysname>
```

显示当前 FIPS 模式状态。

```
<Sysname> display fips status
FIPS mode is enabled.
```

查看缺省的配置文件内容。

```
<Sysname> more fips-startup.cfg
#
 password-control enable
#
local-user root class manage
 service-type terminal
 authorization-attribute user-role network-admin
#
 fips mode enable
#
return

<Sysname>
```

1.6.2 手动重启设备进入FIPS模式

1. 组网需求

手动重启设备进入 FIPS 模式，并采用 Console/AUX/Async 方式登录 FIPS 模式的设备。

2. 配置步骤

使能全局 Password Control 功能。

```
<Sysname> system-view
[Sysname] password-control enable
```

设置全局 Password Control 密码组合类型的个数为 4，每种类型至少一个字符。

```
[Sysname] password-control composition type-number 4 type-length 1
```

设置全局 Password Control 的密码最小长度为 15。

```
[Sysname] password-control length 15
```

添加设备管理类本地用户：用户名为 test、密码为 12345zxcvb!@#$%ZXCVB、用户角色为 network-admin，服务类型为 Terminal。

```
[Sysname] local-user test class manage
[Sysname-luser-manage-test] password simple 12345zxcvb!@#$%ZXCVB
[Sysname-luser-manage-test] authorization-attribute user-role network-admin
[Sysname-luser-manage-test] service-type terminal
[Sysname-luser-manage-test] quit
```

使能 FIPS 模式，并选择手动重启方式进入 FIPS 模式。

```
[Sysname] fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
Reboot the device automatically? [Y/N]:n
Change the configuration to meet FIPS mode requirements, save the configuration to the
next-startup configuration file, and then reboot to enter FIPS mode.
```

将当前配置保存到存储介质的根目录，并将该文件设置为下次启动配置文件。

```
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to device successfully.
[Sysname] quit
```

删除二进制类型的下次启动配置文件。

```
<Sysname> delete flash:/startup.mdb
Delete flash:/startup.mdb?[Y/N]:y
Deleting file flash:/startup.mdb...Done.
```

重启设备。

```
<Sysname> reboot
```

3. 验证结果

重启设备后，输入用户名 test 和对应的密码首次登录时，系统会提示重置密码。重置密码成功后，进入 FIPS 模式的系统。重置的密码必须是大写字母、小写字母、数字以及特殊字符的组合，最小长度为 15 位，且需要与旧密码不同（具体要求请见系统提示）。

```
Press ENTER to get started.
login: test
Password:
First login or password reset. For security reason, you need to change your pass
word. Please enter your password.
old password:
new password:
confirm:
Updating user information. Please wait ... ...
…（略）
<Sysname>
```

显示当前 FIPS 模式状态，可见设备工作在 FIPS 模式下。

```
<Sysname> display fips status
FIPS mode is enabled.
```

1.6.3 自动重启设备退出FIPS模式

1. 组网需求

当前用户已使用 Console/AUX/Async 口登录到 FIPS 模式，要求自动重启设备退出 FIPS 模式。

2. 配置步骤

关闭 FIPS 模式。

```
[Sysname] undo fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
The system will create a new startup configuration file for non-FIPS mode and then reboot automatically. Continue? [Y/N]:y
Waiting for reboot... After reboot, the device will enter non-FIPS mode.
```

3. 验证结果

重启设备后，用户可直接进入系统。

```
<Sysname>
```

显示当前 FIPS 模式状态。

```
<Sysname> display fips status
FIPS mode is disabled.
```

1.6.4 手动重启设备退出FIPS模式

1. 组网需求

当前用户已使用 SSH 远程登录到 FIPS 模式，用户名为 test、密码为 12345zxcvb!@#$%ZXCVB，要求手动重启设备退出 FIPS 模式。

2. 配置步骤

关闭 FIPS 模式。

```
[Sysname] undo fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
The system will create a new startup configuration file for non-FIPS mode, and then reboot automatically. Continue? [Y/N]:n
Change the configuration to meet non-FIPS mode requirements, save the configuration to the next-startup configuration file, and then reboot to enter non-FIPS mode.
```

设置登录 VTY 用户线的登录认证方式为 **scheme**。

```
[Sysname] line vty 0 63
[Sysname-line-vty0-63] authentication-mode scheme
```

将当前配置保存到存储介质的根目录，并将该文件设置为下次启动配置文件。

```
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to device successfully.
[Sysname] quit
```

删除二进制类型的下次启动配置文件。

```
<Sysname> delete flash:/startup.mdb
Delete flash:/startup.mdb?[Y/N]:y
Deleting file flash:/startup.mdb...Done.
```

重启设备。

```
<Sysname> reboot
```

3. 验证结果

重启设备后，输入用户名 test 和对应的密码 12345zxcvb!@#$%ZXCVB，进入非 FIPS 模式的系统。

```
Press ENTER to get started.
login: test
Password:
Last successfully login time:…
（略）
<Sysname>
```

显示当前 FIPS 模式状态，可见设备工作在非 FIPS 模式下。

```
<Sysname> display fips status
FIPS mode is disabled.
```

目 录

1 攻击检测及防范

1.1 攻击检测及防范简介

攻击检测及防范是一个重要的网络安全特性，它通过分析经过设备的报文的内容和行为，判断报文是否具有攻击特征，并根据配置对具有攻击特征的报文执行一定的防范措施，例如输出告警日志、丢弃报文、加入黑名单或客户端验证列表。

本特性能够检测单包攻击、扫描攻击和泛洪攻击等多种类型的网络攻击，并能对各类型攻击采取合理的防范措施。

1.2 攻击检测及防范的类型

1.2.1 单包攻击

单包攻击也称为畸形报文攻击，主要包括以下三种类型：

- 攻击者通过向目标系统发送带有攻击目的的 IP 报文，如分片重叠的 IP 报文、TCP 标志位非法的报文，使得目标系统在处理这样的 IP 报文时出错、崩溃；
- 攻击者可以通过发送正常的报文，如 ICMP 报文、特殊类型的 IP option 报文，来干扰正常网络连接或探测网络结构，给目标系统带来损失；
- 攻击者还可通过发送大量无用报文占用网络带宽，造成拒绝服务攻击。

设备可以对 表 1-1 中所列的各单包攻击行为进行有效防范。

表1-1 单包攻击类型及说明列表

单包攻击类型	说明
ICMP redirect	攻击者向用户发送ICMP重定向报文，更改用户主机的路由表，干扰用户主机正常的IP报文转发。
ICMP unreachable	某些系统在收到不可达的ICMP报文后，对于后续发往此目的地的报文判断为不可达并切断对应的网络连接。攻击者通过发送ICMP不可达报文，达到切断目标主机网络连接的目的。
ICMP type	ICMP报文中，type值的表示不同含义的报文，接收者需要根据不同的类型进行响应，攻击者通过构造特定type类型的ICMP报文来达到影响系统正常处理报文等目的。
ICMPv6 type	ICMPv6报文中，type值的表示不同含义的报文，接收者需要根据不同的类型进行响应，攻击者通过构造特定type类型的ICMPv6报文来达到影响系统正常处理报文等目的。
Land	攻击者向目标主机发送大量源IP地址和目的IP地址都是目标主机自身的TCP SYN报文，使得目标主机的半连接资源耗尽，最终不能正常工作。
Large ICMP	某些主机或设备收到超大的报文，会引起内存分配错误而导致协议栈崩溃。攻击者通过发送超大ICMP报文，让目标主机崩溃，达到攻击目的。
Large ICMPv6	某些主机或设备收到超大的报文，会引起内存分配错误而导致协议栈崩溃。攻击者通过发送超大ICMPv6报文，让目标主机崩溃，达到攻击目的。

单包攻击类型	说明
IP option	攻击者利用IP报文中的异常选项的设置，达到探测网络结构的目的，也可由于系统缺乏对错误报文的处理而造成系统崩溃。
Fragment	攻击者通过向目标主机发送分片偏移小于5的分片报文，导致主机对分片报文进行重组时发生错误而造成系统崩溃。
Impossible	攻击者通过向目标主机发送源IP地址和目的IP地址相同的报文，造成主机系统处理异常。
Tiny fragment	攻击者构造一种特殊的IP分片来进行微小分片的攻击，这种报文首片很小，未能包含完整的传输层信息，因此能够绕过某些包过滤防火墙的过滤规则，达到攻击目标网络的目的。
Smurf	攻击者向目标网络发送ICMP应答请求，该请求包的目的地址设置为目标网络的广播地址，这样该网络中的所有主机都会对此ICMP应答请求作出答复，导致网络阻塞，从而达到令目标网络中主机拒绝服务的攻击目的。
TCP Flag	不同操作系统对于非常规的TCP标志位有不同的处理。攻击者通过发送带有非常规TCP标志的报文探测目标主机的操作系统类型，若操作系统对这类报文处理不当，攻击者便可达到使目标主机系统崩溃的目的。
Traceroute	攻击者连续发送TTL从1开始递增的目的端口号较大的UDP报文，报文每经过一个路由器，其TTL都会减1，当报文的TTL为0时，路由器会给报文的源IP设备发送一个TTL超时的ICMP报文，攻击者借此来探测网络的拓扑结构。
Winnuke	攻击者向安装（或使用）Windows系统的特定目标的NetBIOS端口（139）发送OOB（Out-Of-Band，带外）数据包，这些攻击报文的指针字段与实际的位置不符，从而引起一个NetBIOS片断重叠，致使已与其他主机建立连接的目标主机在处理这些数据的时候系统崩溃。
UDP Bomb	攻击者发送畸形的UDP报文，其IP首部中的报文总长度大于IP首部长度与UDP首部中标识的UDP数据长度之和，可能造成收到此报文的系统处理数据时越界访问非法内存，导致系统异常。
UDP Snork	攻击者向Windows系统发送目的端口为135（Windows定位服务）源端口为135、7或19（UDP Chargen服务）的报文，使被攻击系统不断应答报文，最终耗尽CPU资源。
UDP Fraggle	攻击者通过向目标网络发送UDP端口为7的ECHO报文或者UDP端口为19的Chargen报文，令网络产生大量无用的应答报文，占满网络带宽，达到攻击目的。
Teardrop	攻击者通过发送大量分片重叠的报文，致使服务器对这些报文进行重组时造成重叠，因而丢失有效的数据。
Ping of death	攻击者构造标志位为最后一片且长度大于65535的ICMP报文发送给目标主机，可能导致系统处理数据时越界访问非法内存，造成系统错误甚至系统崩溃。

1.2.2 扫描攻击

扫描攻击是指，攻击者运用扫描工具对网络进行主机地址或端口的扫描，通过准确定位潜在目标的位置，探测目标系统的网络拓扑结构和开放的服务端口，为进一步侵入目标系统做准备。

- IP Sweep 攻击

攻击者发送大量目的 IP 地址变化的探测报文，通过收到的回应报文来确定活跃的目标主机，以便针对这些主机进行下一步的攻击。

- Port scan 攻击

攻击者获取了活动目标主机的 IP 地址后，向目标主机发送大量目的端口变化的探测报文，通过收到的回应报文来确定目标主机开放的服务端口，然后针对活动目标主机开放的服务端口选择合适的攻击方式或攻击工具进行进一步的攻击。

- 分布式 Port scan 攻击

攻击者控制多台主机，分别向特定目标主机发送探测报文，通过收集所有被控制的主机的回应报文，确定目标主机开启的服务端口，以便进一步实施攻击。

1.2.3 泛洪攻击

泛洪攻击是指攻击者在短时间内向目标系统发送大量的虚假请求，导致目标系统疲于应付无用信息，从而无法为合法用户提供正常服务，即发生拒绝服务。

设备支持对以下几种泛洪攻击进行有效防范：

- SYN flood 攻击

根据 TCP 协议，服务器收到 SYN 报文后需要建立半连接并回应 SYN ACK 报文，然后等待客户端的 ACK 报文来建立正式连接。由于资源的限制，操作系统的 TCP/IP 协议栈只能允许有限个 TCP 连接。攻击者向服务器发送大量伪造源地址的 SYN 报文后，由于攻击报文是伪造的，服务器不会收到客户端的 ACK 报文，从而导致服务器上遗留了大量无效的半连接，耗尽其系统资源，使正常的用户无法访问，直到半连接超时。

- ACK flood 攻击

ACK 报文为只有 ACK 标志位置位的 TCP 报文，服务器收到 ACK 报文时，需要查找对应的连接。若攻击者发送大量这样的报文，服务器需要进行大量的查询工作，消耗正常处理的系统资源，影响正常的报文处理。

- SYN-ACK flood 攻击

由于 SYN ACK 报文为 SYN 报文的后续报文，服务器收到 SYN ACK 报文时，需要查找对应的 SYN 报文。若攻击者发送大量这样的报文，服务器需要进行大量的查询工作，消耗正常处理的系统资源，影响正常的报文处理。

- FIN flood 攻击

FIN 报文用于关闭 TCP 连接。若攻击者向服务器发送大量的伪造的 FIN 报文，可能会使服务器关闭掉正常的连接。同时，服务器收到 FIN 报文时，需要查找对应的连接，大量的无效查询操作会消耗系统资源，影响正常的报文处理。

- RST flood 攻击

RST 报文为 TCP 连接的复位报文，用于在异常情况下关闭 TCP 连接。如果攻击者向服务器发送大量伪造的 RST 报文，可能会使服务器关闭正常的 TCP 连接。另外，服务器收到 RST 报文时，需要查找对应的连接，大量的无效查询操作会消耗系统资源，影响正常的报文处理。

- DNS flood 攻击

DNS 服务器收到任何 DNS Query 报文时都会试图进行域名解析并且回复该 DNS 报文。攻击者通过构造并向 DNS 服务器发送大量虚假 DNS Query 报文，占用 DNS 服务器的带宽或计算资源，使得正常的 DNS Query 得不到处理。

- HTTP flood 攻击

HTTP 服务器收到 HTTP GET 命令时可能进行一系列复杂的操作，包括字符串搜索、数据库遍历、数据组装、格式化转换等等，这些操作会消耗大量系统资源，因此当 HTTP 请求的速率超过了服务

器的处理能力时，服务器就无法正常提供服务。攻击者通过构造并发送大量虚假 HTTP GET 请求，使服务器崩溃，无法响应正常的用户请求。

- ICMP flood 攻击

ICMP flood 攻击是指，攻击者在短时间内向特定目标发送大量的 ICMP 请求报文（例如 ping 报文），使其忙于回复这些请求，致使目标系统负担过重而不能处理正常的业务。

- ICMPv6 flood 攻击

ICMPv6 flood 攻击是指，攻击者在短时间内向特定目标发送大量的 ICMPv6 请求报文（例如 ping 报文），使其忙于回复这些请求，致使目标系统负担过重而不能处理正常的业务。

- UDP flood 攻击

UDP flood 攻击是指，攻击者在短时间内向特定目标发送大量的 UDP 报文，占用目标主机的带宽，致使目标主机不能处理正常的业务。

1.3 黑名单功能

黑名单功能是根据报文的源 IP 地址进行报文过滤的一种攻击防范特性。同基于 ACL（Access Control List，访问控制列表）的包过滤功能相比，黑名单进行报文匹配的方式更为简单，可以实现报文的高速过滤和有效屏蔽。

黑名单可以由设备动态或由用户手工进行添加、删除，具体机制如下：

- 动态添加黑名单是与扫描攻击防范功能配合实现的，动态生成的黑名单表项会在一定的时间之后老化。当设备根据报文的行为特征检测到某特定 IP 地址的扫描攻击企图之后，便将攻击者的 IP 地址自动加入黑名单，之后该 IP 地址发送的报文会被设备过滤掉。
- 手动配置的黑名单表项分为永久黑名单表项和非永久黑名单表项。永久黑名单表项建立后，一直存在，除非用户手工删除该表项。非永久黑名单表项的老化时间由用户指定，超出老化时间后，设备会自动将该黑名单表项删除。

1.4 客户端验证功能

1.4.1 TCP客户端验证功能（TCP Client verify）

TCP 客户端验证功能用来防御服务器受到的 SYN flood，ACK flood，SYN-ACK flood，FIN flood，RST flood 等攻击。启用了 TCP 客户端验证功能的设备称为 TCP proxy，它位于客户端和服务器之间，能够对客户端与服务器之间的 TCP 连接进行代理。当设备检测到有服务器受到相关泛洪攻击时，TCP proxy 即将该服务器 IP 地址添加为动态受保护的 IP 地址，并对所有向该受保护服务器发起的 TCP 连接的协商报文进行处理，通过对客户端发起的 TCP 连接进行验证，达到保护服务器免受各种 TCP 泛洪攻击的目的。

TCP 客户端验证支持两种验证模式：

- Safe Reset：是指仅对 TCP 连接的正向握手报文进行处理，也称为单向代理模式。
- SYN Cookie：是指对 TCP 连接的正向和反向所有报文都进行处理，也称为双向代理模式。

用户可以根据实际的组网情况选择不同的代理模式。例如：在如 图 1-1 所示的组网中，从客户端发出的报文经过TCP proxy，而从服务器端发出的报文不经过TCP proxy，此时只能使用Safe Reset方式；在如 图 1-2 所示的组网中，从客户端发出的报文经和从服务器端发出的报文都经过TCP proxy，此时两种验证模式都可以使用。

图1-1 Safe Reset 组网

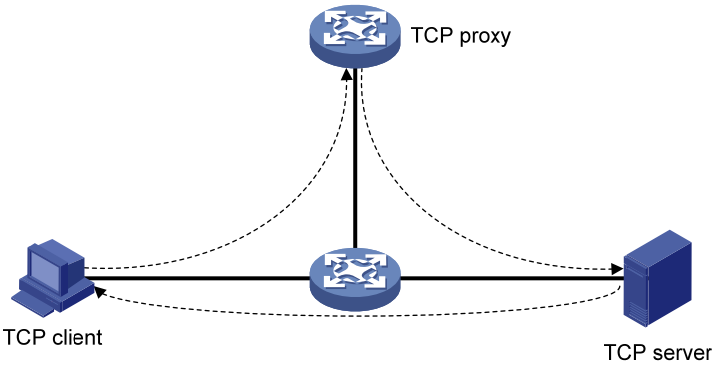
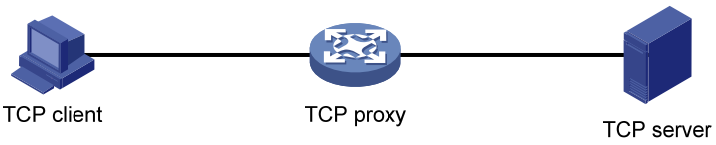


图1-2 通用组网

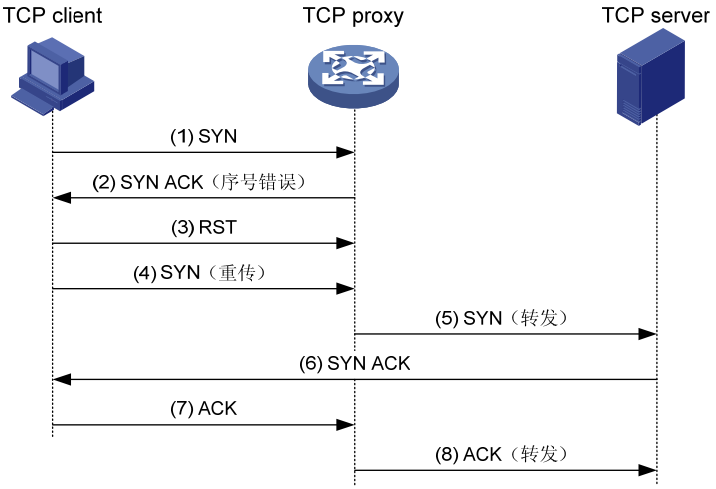


TCP Client verify 处理流程：

- Safe Reset

Safe Reset代理模式下，TCP Client verify的处理流程如 图 1-3 所示。

图1-3 Safe Reset 模式的 TCP Client verify 处理流程



TCP proxy 收到某客户端发来的与受保护服务器（匹配某个受保护 IP 地址表项）建立 TCP 连接的请求（SYN 报文）后，先代替服务器向客户端回应序号错误的 SYN ACK 报文。如果 TCP proxy 收到客户端回应的正确 RST 报文，则认为该 TCP 连接请求通过 TCP 代理的验证。此后一定时间内，TCP proxy 收到来自该客户端的 TCP 报文后，直接将其转发给服务器，允许客户端和服务器之间直接建立 TCP 连接。

一般而言，应用服务器不会主动对客户端发起恶意连接，因此服务器响应客户端的报文可以不需要经过 TCP proxy 的检查。TCP Client verify 仅需要对客户端发往应用服务器的报文进行实时监控，

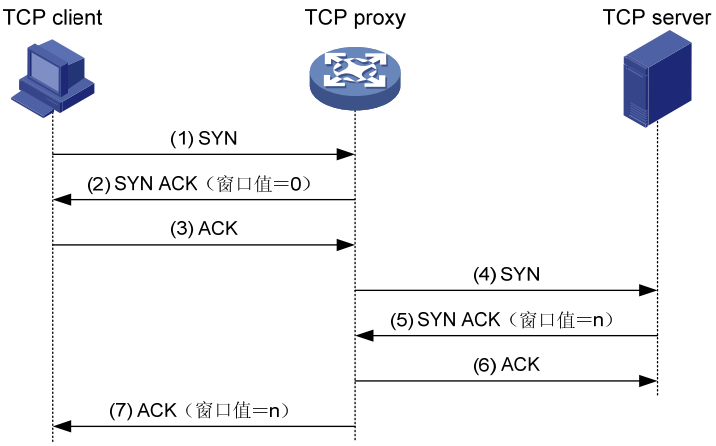
服务器响应客户端的报文可以根据实际需要选择是否经过 TCP proxy，因此 Safe Reset 模式能够支持更灵活的组网方式。

由于 TCP proxy 对客户端发起的 TCP 连接进行了干预，因此 Safe Reset 模式的实现要求客户端的实现严格遵守 TCP 协议栈的规定，如果客户端的 TCP 协议栈实现不完善，即便是合法用户，也可能由于未通过 TCP proxy 的严格检查而无法访问服务器。而且，该方式依赖于客户端向服务器发送 RST 报文后再次发起请求的功能，因此启用 TCP Client verify 后，客户端发起的每个 TCP 连接的建立时间会有相应增加。

- SYN Cookie

SYN Cookie模式下，TCP Client verify的处理流程如 图 1-4 所示。

图1-4 SYN Cookie 模式的 TCP Client verify 处理流程



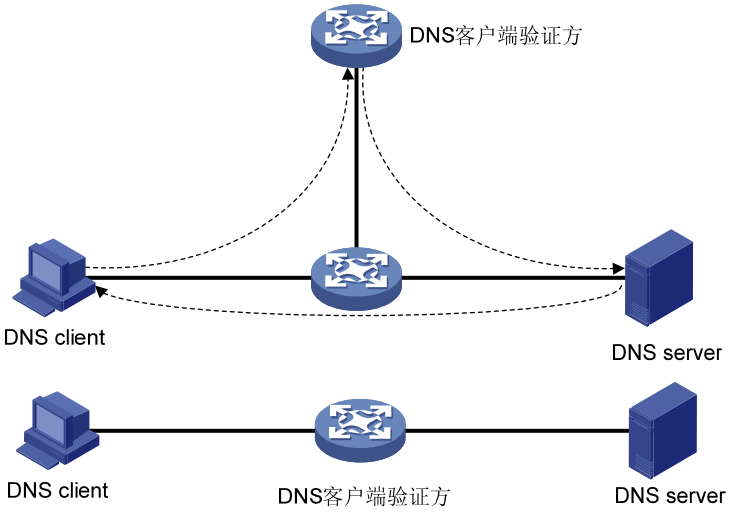
TCP proxy 收到某客户端发来的与受保护服务器建立 TCP 连接的请求（SYN 报文）后，先代替服务器向客户端回应正常的 SYN ACK 报文（窗口值为 0）。如果收到客户端回应的 ACK 报文，则认为该 TCP 连接请求通过 TCP 代理的验证。之后，TCP Client verify 再代替客户端向服务器发送 SYN 报文，并通过三次握手与服务器建立 TCP 连接。因此，在客户端和 TCP proxy、TCP proxy 和服务器之间会建立两个 TCP 连接，而且两个 TCP 连接使用的序号不同。

SYN Cookie 模式下，TCP proxy 作为虚拟的服务器与客户端交互，同时也作为虚拟的客户端与服务器交互，在为服务器过滤掉恶意连接报文的同时保证了常规业务的正常运行。但该方式要求 TCP proxy 必须部署在所保护的服务器入口和出口的关键路径上，且要保证所有客户端向服务器发送的报文以及服务器向客户端回应的报文都需要经过该设备。

1.4.2 DNS 客户端验证（DNS Client verify）

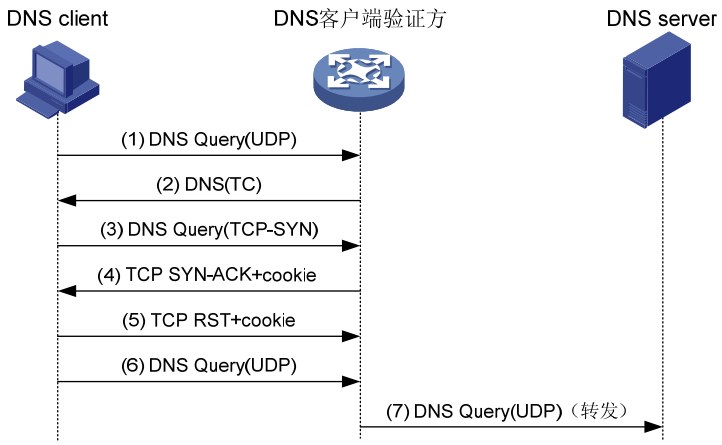
DNS客户端验证功能用来防御服务器受到的DNS flood攻击。如 图 1-5 所示的两种类型的组网中，启用了DNS 客户端验证功能的设备位于客户端和服务器之间，均能够对客户端与服务器之间的DNS连接进行代理。当设备检测到有服务器受到DNS flood攻击时，即将该服务器IP地址添加为动态受保护的IP地址，并对所有向该受保护服务器发起的DNS Query进行处理，通过对客户端发起的DNS连接进行验证，达到保护服务器免受DNS flood攻击的目的。

图1-5 DNS 客户端验证组网



DNS Client verify 处理流程：

图1-6 DNS Client verify 处理流程



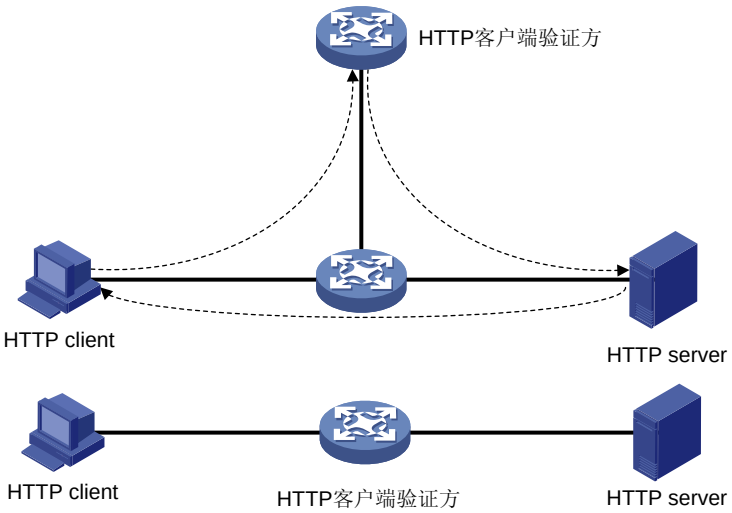
DNS 客户端验证设备收到某客户端发送的 UDP 类型的 DNS Query 报文（目的地址匹配受保护 IP 表项）后，先代替服务器向客户端回应 DNS Truncate（TC）报文，要求客户端以 TCP 方式进行域名请求。如果是合法客户端，则它收到 DNS Truncate 报文之后会向 DNS 客户端验证设备发送目的端口为 53 的 TCP SYN 报文。DNS 客户端验证设备收到此报文后，先代替服务器向客户端回应序号错误的 SYN ACK 报文，之后，如果能够收到客户端回应的 RST 报文，则认为该客户端通过了 DNS 客户端验证。对于通过了 DNS 验证的客户端，设备直接转发其后续报文，不对报文进行处理。

由于 DNS Client verify 对客户端发起的 DNS 请求进行了干预，因此要求客户端的实现严格遵守 TCP/IP 协议栈以及 DNS 协议的规定，如果客户端的协议栈实现不完善，即便是合法用户，也可能由于未通过 DNS Client verify 的严格检查而无法访问服务器。而且，该方式依赖于客户端向服务器发送 RST 报文后再次发起请求的功能，因此启用 DNS Client verify 后，正常客户端发起的首个 DNS 请求的响应时间会有相应增加。

1.4.3 HTTP客户端验证（HTTP Client verify）

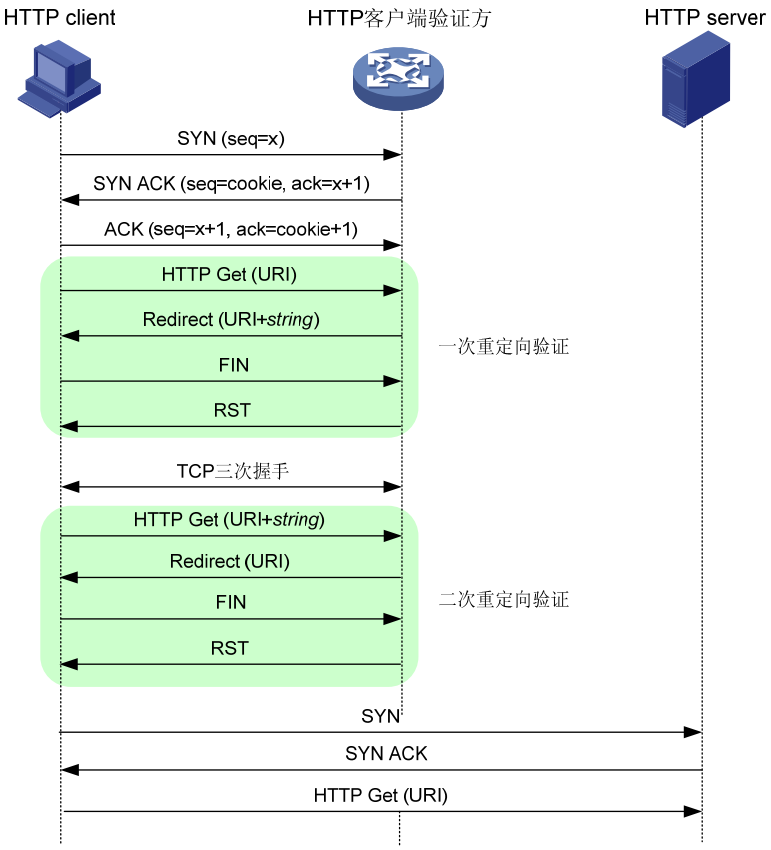
HTTP客户端验证功能用来防御服务器受到HTTP flood攻击。如 图 1-7 所示的两种类型的组网中，启用了HTTP 客户端验证功能的设备位于客户端和服务器之间，均能够对客户端与服务器之间的HTTP GET请求进行代理。当设备检测到有服务器受到HTTP flood攻击时，即将该服务器IP地址添加为动态受保护的IP地址，并对所有向该受保护服务器发起的HTTP GET请求报文进行处理，通过对客户端发起的HTTP GET请求进行两次重定向方式的验证，达到保护服务器免受HTTP flood攻击的目的。

图1-7 HTTP 客户端验证组网



HTTP Client verify 处理流程：

图1-8 HTTP Client verify 处理流程



HTTP客户端验证设备收到某客户端发送的HTTP GET报文（目的地址匹配受保护IP表项）后，首先以TCP Proxy的Syn cookie方式进行验证（详见“1.4.1 TCP客户端验证功能（TCP Client verify）”）。TCP验证通过后，将进行HTTP两次重定向验证，具体流程见 图 1-8。第二次HTTP重定向验证通过时，会将该客户端加入到信任IP表项中，该客户端的后续HTTP GET请求报文将被直接进行透传。

1.5 攻击检测及防范配置任务简介

表1-2 攻击检测及防范配置任务简介

配置任务		说明	详细配置
创建攻击防范策略		必选	1.6.1
配置攻击防范策略	配置单包攻击防范策略	必选 各类型的攻击防范功能之间没有先后顺序，可根据实际组网需求，配置其中的一种或多种	1.6.2 1.
	配置扫描攻击防范策略		1.6.2 2.
	配置泛洪攻击防范策略		1.6.2 3.
	配置攻击防范例外列表	可选	1.6.3
在接口上应用攻击防范策略		二者至少选其一	1.6.4

配置任务		说明	详细配置
在本机应用攻击防范策略		应用在接口的策略仅对接口生效 应用在本机的策略对所有目的地址为本机的报文均有效	1.6.5
配置单包攻击防范日志的非聚合输出功能		可选	1.6.6
配置客户端验证	配置TCP Client verify	可选 可单独使用，也可与SYN flood、SYN-ACK flood、RST flood、FIN flood、ACK flood攻击防范策略配合使用	1.6.6
	配置DNS Client verify	可选 可单独使用，也可与DNS flood攻击防范策略配合使用	1.8
	配置HTTP Client verify	可选 可单独使用，也可与HTTP flood攻击防范策略配合使用	1.9
配置黑名单		可选 可单独使用，也可与扫描攻击防范策略配合使用	1.10

1.6 配置攻击防范

1.6.1 创建攻击防范策略

在配置攻击防范之前，必须首先创建一个攻击防范策略，并进入该攻击防范策略视图。在该视图下，可以定义一个或多个用于检测攻击的特征项，以及对检测到的攻击报文所采取的防范措施。

表1-3 创建攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
创建一个攻击防范策略，并进入攻击防范策略视图	**attack-defense policy** *policy-number*	缺省情况下，不存在任何攻击防范策略

1.6.2 配置攻击防范策略

在一个攻击防范策略中，可以根据实际的网络安全需求来配置策略中的具体内容，主要包括针对攻击类型指定检测条件及采取的防范措施。

不同类型的攻击防范策略在配置内容上有所不同，下面将按照攻击类型（单包攻击、扫描攻击、泛洪攻击）分别进行介绍。

1. 配置单包攻击防范策略

单包攻击防范主要通过分析经过设备的报文特征来判断报文是否具有攻击性，一般应用在设备连接外部网络的接口上，且仅对应用了攻击防范策略的接口上的入方向报文有效。若设备检测到某报文具有攻击性，则默认会输出告警日志，另外还可以根据配置将检测到的攻击报文做丢弃处理。

表1-4 配置单包攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入攻击防范策略视图	**attack-defense policy** *policy-number*	-
开启指定类型单包攻击报文的特征检测，并设置攻击防范的处理行为	**signature detect** { **fraggle** | **fragment** | **impossible** | **ip-option-abnormal** | **land** | **large-icmp** | **large-icmpv6** | **ping-of-death** | **smurf** | **snork** | **tcp-all-flags** | **tcp-fin-only** | **tcp-invalid-flags** | **tcp-null-flag** | **tcp-syn-fin** | **teardrop** | **tiny-fragment** | **traceroute** | **udp-bomb** | **winnuke** } [**action** { { **drop** | **logging** } * | **none** }] **signature detect icmp-type** { *icmp-type-value* | **address-mask-reply** | **address-mask-request** | **destination-unreachable** | **echo-reply** | **echo-request** | **information-reply** | **information-request** | **parameter-problem** | **redirect** | **source-quench** | **time-exceeded** | **timestamp-reply** | **timestamp-request** } [**action** { { **drop** | **logging** } * | **none** }] **signature detect icmpv6-type** { *icmpv6-type-value* | **destination-unreachable** | **echo-reply** | **echo-request** | **group-query** | **group-reduction** | **group-report** | **packet-too-big** | **parameter-problem** | **time-exceeded** } [**action** { { **drop** | **logging** } * | **none** }] **signature detect ip-option** { *option-code* | **internet-timestamp** | **loose-source-routing** | **record-route** | **route-alert** | **security** | **stream-id** | **strict-source-routing** } [**action** { { **drop** | **logging** } * | **none** }]	至少选其一 缺省情况下，所有类型的单包攻击的特征检测均处于关闭状态
（可选）配置启动Large ICMP攻击防范的ICMP报文长度的最大值	**signature** { **large-icmp** | **large-icmpv6** } **max-length** *length*	缺省情况下，ICMP报文和ICMPv6报文长度的最大值均为4000字节
（可选）配置对不同级别的单包攻击报文的处理方式	**signature level** { **high** | **info** | **low** | **medium** } **action** { { **drop** | **logging** } * | **none** }	缺省情况下，对**info**和**low**级别的单包攻击的处理行为是发送日志；对**medium**和**high**级别的单包攻击的处理行为是发送日志并丢包

配置步骤	命令	说明
（可选）开启指定级别单包攻击报文的特征检测	**signature level** { **high** | **info** | **low** | **medium** } **detect**	缺省情况下，未开启任何级别的单包攻击报文的特征检测

2. 配置扫描攻击防范策略

扫描攻击防范主要通过监测网络使用者向目标系统发起连接的速率来检测其探测行为，一般应用在设备连接外部网络的三层接口上，且仅对应用了攻击防范策略的三层接口上的入方向报文有效。若设备监测到某 IP 地址主动发起的连接速率达到或超过了一定阈值，则可以根据配置输出告警日志、丢弃来自该 IP 地址的后续报文，或者将检测到的攻击者的源 IP 地址加入黑名单。

若指定的扫描攻击的处理行为为加入黑名单，则需要开启全局或接口上的黑名单过滤功能来配合。

表1-5 配置扫描攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入攻击防范策略视图	**attack-defense policy** *policy-number*	-
开启指定级别的扫描攻击防范	**scan detect level** { **high** | **low** | **medium** } **action** { { **block-source** [**timeout** *minutes*] | **drop** } | **logging** } *	缺省情况下，扫描攻击防范处于关闭状态
（可选）开启全局黑名单过滤功能	**blacklist global enable**	缺省情况下，全局黑名单过滤功能处于关闭状态 全局黑名单过滤功能对所有接口都生效
进入三层接口视图	**interface** *interface-type interface-number*	-
（可选）在接口上开启黑名单过滤功能	**blacklist enable**	缺省情况下，接口上的黑名单过滤功能处于关闭状态

3. 配置泛洪攻击防范策略

泛洪攻击防范主要用于保护服务器，通过监测向服务器发起连接请求的速率来检测各类泛洪攻击，一般应用在设备连接外部网络的接口上，且仅对应用了攻击防范策略的接口上的入方向报文有效。在接口上应用了泛洪攻击防范策略后，接口处于攻击检测状态，当它监测到向某服务器发送报文的速率持续达到或超过了指定的触发阈值时，即认为该服务器受到了攻击，则进入攻击防范状态，并根据配置启动相应的防范措施（输出告警日志、对后续新建连接的报文进行丢弃处理或者进行客户端验证）。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

为保护指定 IP 地址，攻击防范策略中支持基于 IP 地址的攻击防范配置。对于所有非受保护 IP 地址，可以统一开启攻击防范检测，并采用全局的参数设置来进行保护。

(1) 配置 SYN flood 攻击防范策略

表1-6 配置 SYN flood 攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入攻击防范策略视图	**attack-defense policy** *policy-number*	-
对所有非受保护IP地址开启SYN flood攻击防范检测	**syn-flood detect non-specific**	缺省情况下，未对所有非受保护IP地址开启SYN flood攻击防范检测
配置SYN flood攻击防范的全局触发阈值	**syn-flood threshold** *threshold-value*	缺省情况下，SYN flood攻击防范的全局触发阈值为1000
配置SYN flood攻击防范的全局处理行为	**syn-flood action** { **client-verify** | **drop** | **logging** } *	缺省情况下，不对检测到的SYN flood攻击采取任何措施
开启对指定IP地址的SYN flood攻击防范检测，并配置触发阈值和处理行为	**syn-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **client-verify** | **drop** | **logging** } *]	缺省情况下，未对任何指定IP地址配置SYN flood攻击防范检测

(2) 配置 ACK flood 攻击防范策略

表1-7 配置 ACK flood 攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入攻击防范策略视图	**attack-defense policy** *policy-number*	-
对所有非受保护IP地址开启ACK flood攻击防范检测	**ack-flood detect non-specific**	缺省情况下，未对所有非受保护IP地址开启ACK flood攻击防范检测
配置ACK flood攻击防范全局触发阈值	**ack-flood threshold** *threshold-value*	缺省情况下，ACK flood攻击防范的全局触发阈值为1000
配置ACK flood攻击防范的全局处理行为	**ack-flood action** { **client-verify** | **drop** | **logging** } *	缺省情况下，不对检测到的ACK flood攻击采取任何措施
开启对指定IP地址的ACK flood攻击防范检测，并配置触发阈值和处理行为	**ack-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **client-verify** | **drop** | **logging** } *]	缺省情况下，未对任何指定IP地址配置ACK flood攻击防范检测

(3) 配置 SYN-ACK flood 攻击防范策略

表1-8 配置 SYN-ACK flood 攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入攻击防范策略视图	**attack-defense policy** *policy-number*	-

配置步骤	命令	说明
对所有非受保护IP地址开启SYN-ACK flood攻击防范检测	**syn-ack-flood detect non-specific**	缺省情况下，未对所有非受保护IP地址开启SYN-ACK flood攻击防范检测
配置SYN-ACK flood攻击防范的全局触发阈值	**syn-ack-flood threshold** *threshold-value*	缺省情况下，SYN-ACK flood攻击防范的全局触发阈值为1000
配置SYN-ACK flood攻击防范的全局处理行为	**syn-ack-flood action** { **client-verify** | **drop** | **logging** } *	缺省情况下，不对检测到的SYN-ACK flood攻击采取任何措施
开启对指定IP地址的SYN-ACK flood攻击防范检测，并配置触发阈值和处理行为	**syn-ack-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **client-verify** | **drop** | **logging** } *]	缺省情况下，未对任何指定IP地址配置SYN-ACK flood攻击防范检测

(4) 配置 FIN flood 攻击防范策略

表1-9 配置 FIN flood 攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入攻击防范策略视图	**attack-defense policy** *policy-number*	-
对所有非受保护IP地址开启FIN flood攻击防范检测	**fin-flood detect non-specific**	缺省情况下，未对所有非受保护IP地址开启FIN flood攻击防范检测
配置FIN flood攻击防范的全局触发阈值	**fin-flood threshold** *threshold-value*	缺省情况下，FIN flood攻击防范的全局触发阈值为1000
配置FIN flood攻击防范的全局处理行为	**fin-flood action** { **client-verify** | **drop** | **logging** } *	缺省情况下，不对检测到的FIN flood攻击采取任何措施
开启对指定IP地址的FIN flood攻击防范检测，并配置触发阈值和处理行为	**fin-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **client-verify** | **drop** | **logging** } *]	缺省情况下，未对任何指定IP地址配置FIN flood攻击防范检测

(5) 配置 RST flood 攻击防范策略

表1-10 配置 RST flood 攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入攻击防范策略视图	**attack-defense policy** *policy-number*	-
对所有非受保护IP地址开启RST flood攻击防范检测	**rst-flood detect non-specific**	缺省情况下，未对所有非受保护IP地址开启RST flood攻击防范检测
配置RST flood攻击防范检测阈值	**rst-flood threshold** *threshold-value*	缺省情况下，RST flood攻击防范的全局触发阈值为1000

配置步骤	命令	说明
配置全局的RST flood攻击防范的全局处理行为	**rst-flood action** { **client-verify** | **drop** | **logging** } *	缺省情况下，不对检测到的RST flood攻击采取任何措施
开启对指定IP地址的RST flood攻击防范检测，并配置触发阈值和处理行为	**rst-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **client-verify** | **drop** | **logging** } *]	缺省情况下，未对任何指定IP地址配置RST flood攻击防范检测

(6) 配置 ICMP flood 攻击防范策略

表1-11 配置 ICMP flood 攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入攻击防范策略视图	**attack-defense policy** *policy-number*	-
对所有非受保护IPv4地址开启ICMP flood攻击防范检测	**icmp-flood detect non-specific**	缺省情况下，未对任何非受保护IPv4地址开启ICMP flood攻击防范检测
配置ICMP flood攻击防范的全局触发阈值	**icmp-flood threshold** *threshold-value*	缺省情况下，ICMP flood攻击防范的全局触发阈值为1000
配置ICMP flood攻击防范的全局处理动作	**icmp-flood action** { **drop** | **logging** } *	缺省情况下，不对检测到的ICMP flood攻击采取任何措施
开启对指定IPv4地址的RST flood攻击防范检测，并配置触发阈值和处理行为	**icmp-flood detect ip** *ip-address* [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **drop** | **logging** } *]	缺省情况下，未对任何指定IPv4地址配置ICMP flood 攻击防范触发阈值

(7) 配置 ICMPv6 flood 攻击防范策略

表1-12 配置 ICMP flood 攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入攻击防范策略视图	**attack-defense policy** *policy-number*	-
对所有非受保护IPv6地址开启ICMPv6 flood攻击防范检测	**icmpv6-flood detect non-specific**	缺省情况下，未对任何非受保护IPv6地址开启ICMPv6 flood攻击防范检测
配置ICMPv6 flood攻击防范的全局触发阈值	**icmpv6-flood threshold** *threshold-value*	缺省情况下，ICMPv6 flood攻击防范的全局触发阈值为1000
配置ICMPv6 flood攻击防范的全局处理行为	**icmpv6-flood action** { **drop** | **logging** } *	缺省情况下，不对检测到的ICMPv6 flood攻击采取任何防范措施

配置步骤	命令	说明
开启对指定IPv6地址的ICMPv6 flood攻击防范检测，并配置触发阈值和处理行为	**icmpv6-flood detect ipv6** *ipv6-address* [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **drop** | **logging** } *]	缺省情况下，未对任何指定IPv6地址配置ICMPv6 flood攻击防范检测

(8) 配置 UDP flood 攻击防范策略

表1-13 配置 UDP flood 攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入攻击防范策略视图	**attack-defense policy** *policy-number*	-
对所有非受保护IP地址开启UDP flood攻击防范检测	**udp-flood detect non-specific**	缺省情况下，未对所有非受保护IP地址开启UDP flood攻击防范检测
配置UDP flood攻击防范的全局触发阈值	**udp-flood threshold** *threshold-value*	缺省情况下，UDP flood攻击防范的全局触发阈值为1000
配置UDP flood攻击防范检测的全局处理行为	**udp-flood action** { **drop** | **logging** } *	缺省情况下，不对检测到的UDP flood攻击进行任何处理
开启对指定IP地址的UDP flood攻击防范检测，并配置触发阈值和处理行为	**udp-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**threshold** *threshold-value*] [**action** { **client-verify** | **drop** | **logging** } *]	缺省情况下，未对任何指定IP地址配置UDP flood攻击防范检测

(9) 配置 DNS flood 攻击防范策略

表1-14 配置 DNS flood 攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入攻击防范策略视图	**attack-defense policy** *policy-number*	-
对所有非受保护IP地址开启DNS flood攻击防范检测	**dns-flood detect non-specific**	缺省情况下，未对所有非受保护IP地址开启DNS flood攻击防范检测
配置DNS flood攻击防范的全局触发阈值	**dns-flood threshold** *threshold-value*	缺省情况下，DNS flood攻击防范的全局触发阈值为1000
（可选）配置DNS flood攻击防范的全局检测端口号	**dns-flood port** *port-list*	缺省情况下，DNS flood攻击防范的全局检测端口号为53
配置对DNS flood攻击防范的全局处理行为	**dns-flood action** { **client-verify** | **drop** | **logging** } *	缺省情况下，不对检测到的DNS flood攻击采取任何措施

配置步骤	命令	说明
开启对指定IP地址的DNS flood攻击防范检测，并配置触发阈值和处理行为	**dns-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**port** *port-list*] [**threshold** *threshold-value*] [**action** { **client-verify** | **drop** | **logging** } *]	缺省情况下，未对任何指定IP地址配置DNS flood攻击防范检测

(10) 配置 HTTP flood 攻击防范策略

表1-15 配置 HTTP flood 攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入攻击防范策略视图	**attack-defense policy** *policy-number*	-
对所有非受保护IP地址开启HTTP flood攻击防范检测	**http-flood detect non-specific**	缺省情况下，未对所有非受保护IP地址开启HTTP flood攻击防范检测
配置HTTP flood攻击防范的全局触发阈值	**http-flood threshold** *threshold-value*	缺省情况下，HTTP flood攻击防范的全局触发阈值为1000
（可选）配置HTTP flood攻击防范的全局检测端口号	**http-flood port** *port-list*	缺省情况下，HTTP flood攻击防范的全局检测端口号为80
配置对HTTP flood攻击防范的全局处理行为	**http-flood action** { **client-verify** | **drop** | **logging** } *	缺省情况下，不对检测到的HTTP flood攻击采取任何措施
开启对指定IP地址的HTTP flood攻击防范检测，并配置触发阈值和处理行为	**http-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**port** *port-list*] [**threshold** *threshold-value*] [**action** { **client-verify** | **drop** | **logging** } *]	缺省情况下，未对任何指定IP地址配置HTTP flood攻击防范检测

1.6.3 配置攻击防范例外列表

攻击防范例外列表用于过滤不需要进行攻击防范检测的主机报文，与指定的 ACL permit 规则匹配的报文将不会受到任何类型的攻击防范检测。该配置用于过滤某些被信任的安全主机发送的报文，可以有效的减小误报率，并提高服务器处理效率。

表1-16 配置攻击防范例外列表

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入攻击防范策略视图	**attack-defense policy** *policy-number*	-

配置步骤	命令	说明
配置攻击防范例外列表	**exempt acl** [**ipv6**] { *acl-number* | **name** *acl-name* }	缺省情况下，应用了攻击防范策略的接口收到的所有报文都需要进行攻击防范检测

1.6.4 在三层接口上应用攻击防范策略

通过下面的配置，使已配置的攻击防范策略在具体的三层接口上生效。

表1-17 配置在三层接口上应用攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入三层接口视图	**interface** *interface-type interface-number*	-
配置在三层接口上应用攻击防范策略	**attack-defense apply policy** *policy-number*	缺省情况下，接口上未应用任何攻击防范策略

1.6.5 在本机应用攻击防范策略

通过在本机上应用攻击防范策略提高对目的地址为本机的攻击报文的处理效率。

当接口和本机均应用了攻击防范策略时，先进行接口上攻击防范策略的检测，若报文未被丢弃，则还会进行本机上攻击防范策略的检测。需要注意的是，对于目的地址是本机且将要进行快速转发流程处理的报文，则只进行本机攻击防范策略的检测。

表1-18 配置在本机应用攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置在本机应用攻击防范策略	**attack-defense local apply policy** *policy-number*	缺省情况下，本机未应用任何攻击防范策略

1.6.6 配置单包攻击防范日志的非聚合输出功能

对日志进行聚合输出是指，在一定时间内，对在同一个接口上检测到的相同攻击类型、相同攻击防范动作、相同的源/目的地址以及属于相同 VPN 的单包攻击的所有日志聚合成一条日志输出。

通常不建议开启单包攻击防范的日志非聚合输出功能，因为在单包攻击较为频繁的情况下，它会导致大量日志信息输出，占用控制台的显示资源。

表1-19 配置单包攻击防范日志的非聚合输出功能

配置步骤	命令	说明
进入系统视图	**system-view**	-

配置步骤	命令	说明
开启对单包攻击防范日志的非聚合输出功能	**attack-defense signature log non-aggregate**	缺省情况下，单包攻击防范的日志信息经系统聚合后再输出

1.7 配置TCP客户端验证

通过在设备连接外部网络的接口上使能 TCP 客户端验证功能，可以保护内部网络中的应用服务器免受 SYN flood 攻击。TCP 客户端验证功能有两种工作方式：

- 手工添加受保护 IP 地址：当设备检测到来自某客户端的首个目的地址为配置的受保护 IP 地址的 SYN 报文后，将对该客户端的新建 TCP 连接的协商报文进行合法性检查。
- 自动添加受保护 IP 地址：当设备检测到某服务器受到了 SYN flood、SYN-ACK flood、RST flood、FIN flood、ACK flood 攻击时，会根据配置启动相应的防范措施。若防范措施配置为对攻击报文进行 TCP 客户端验证，则设备会将该服务器 IP 地址添加到受保护 IP 表项中，并按照指定的 TCP 客户端验证代理模式，对后续新建 TCP 连接的协商报文进行合法性检查。

通过合法性检查的 TCP 客户端的 IP 地址将被加入信任 IP 地址列表中，之后设备将放行来自该 IP 地址的 TCP 报文。

表1-20 配置 TCP 客户端验证

配置步骤		命令	说明
进入系统视图		**system-view**	-
（可选）配置TCP客户端验证的受保护IP地址		**client-verify tcp protected** { **ip** *destination-ip-address* | **ipv6** *destination-ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**port** *port-number*]	缺省情况下，不存在任何受保护IP地址，即TCP客户端验证功能未保护任何IP地址
进入三层接口视图		**interface** *interface-type interface-number*	-
使能接口上的TCP客户端验证功能	单向代理模式	**client-verify tcp enable mode safe-reset**	二者选其一 缺省情况下，接口上的TCP客户端验证功能处于关闭状态
	双向代理模式	**client-verify tcp enable** [**mode syn-cookie**]	

1.8 配置DNS客户端验证

通过在设备连接外部网络的接口上使能 DNS 客户端验证功能，可以保护内部网络中的应用服务器免受 DNS flood 攻击。DNS 客户端验证功能有两种工作方式：

- 手工添加受保护 IP 地址：当设备检测到来自某客户端的首个目的地址为配置的受保护 IP 地址的 DNS Query 报文时，对该客户端发送的 DNS 报文进行合法性检查。
- 自动添加受保护 IP 地址：当设备检测到某服务器受到了 DNS flood 攻击时，会根据配置启动相应的防范措施。若防范措施配置为对攻击报文进行 DNS 客户端验证，则设备会将该服务器 IP 地址添加到受保护 IP 表项中，并对后续的 DNS Query 请求报文进行合法性检查。

通过合法性检查的 DNS 客户端的 IP 地址将被加入信任 IP 地址列表中，之后设备将放行来自该 IP 地址的 DNS 报文。

表1-21 配置 DNS 客户端验证

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置DNS客户端验证的受保护IP地址	**client-verify dns protected** { **ip** *destination-ip-address* | **ipv6** *destination-ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**port** *port-number*]	缺省情况下，不存在任何受保护IP地址，即DNS客户端验证功能未保护任何IP地址
进入三层接口视图	**interface** *interface-type interface-number*	-
使能接口上的DNS 客户端验证功能	**client-verify dns enable**	缺省情况下，接口上的DNS客户端验证功能处于关闭状态

1.9 配置HTTP客户端验证

通过在设备连接外部网络的接口上使能 HTTP 客户端验证功能，可以保护内部网络中的应用服务器免受 HTTP flood 攻击。HTTP 客户端验证功能有两种工作方式：

- 手工添加受保护 IP 地址：当设备检测到来自某客户端的首个目的地址为配置的受保护 IP 地址的 HTTP Get 报文时，对该客户端发送的 HTTP 报文进行合法性检查。
- 自动添加受保护 IP 地址：当设备监测到某服务器受到了 HTTP flood 攻击时，会根据配置启动相应的防范措施。若防范措施配置为对攻击报文进行 HTTP 客户端验证，则设备会将该服务器 IP 地址添加到受保护 IP 表项中，并对后续的 HTTP Get 请求报文进行合法性检查。

通过合法性检查的 HTTP 客户端的 IP 地址将被加入信任 IP 地址列表中，之后设备将放行来自该 IP 地址的 HTTP 报文。

表1-22 配置 HTTP 客户端验证

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置HTTP客户端验证的受保护IP地址	**client-verify http protected** { **ip** *destination-ip-address* | **ipv6** *destination-ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**port** *port-number*]	缺省情况下，不存在任何受保护IP地址，即HTTP客户端验证功能未保护任何IP地址
进入三层接口视图	**interface** *interface-type interface-number*	-
配置接口上的HTTP客户端验证功能	**client-verify http enable**	缺省情况下，接口上的HTTP客户端验证功能处于关闭状态

1.10 配置黑名单

通过配置黑名单功能可以对来自指定 IP 地址的报文进行过滤。

黑名单的配置包括开启黑名单过滤功能和添加黑名单表项。若全局的黑名单过滤功能处于开启状态，则所有接口上的黑名单过滤功能均处于开启状态。若全局的黑名单过滤功能处于关闭状态，则需要开启指定接口上的黑名单过滤功能。添加黑名单表项的同时可以选择配置黑名单表项的老化时间，若不配置，那么该黑名单表项永不老化，除非用户手动将其删除。

黑名单表项除了可以手工添加之外，还可以通过扫描攻击防范自动添加。具体来讲就是，在黑名单功能使能的前提下，若配置了扫描攻击防范策略及相应的黑名单添加功能，则可以将检测到的扫描攻击方IP地址添加到黑名单中。扫描攻击防范添加的黑名单必定会老化，老化时间可配。关于扫描攻击防范的相关配置请参见“1.6.2 2. 配置扫描攻击防范策略”。

表1-23 配置黑名单

配置步骤	命令	说明
进入系统视图	**system-view**	-
（可选）开启全局黑名单过滤功能	**blacklist global enable**	缺省情况下，全局黑名单功能处于关闭状态
（可选）添加IPv4黑名单表项	**blacklist ip** *source-ip-address* [**vpn-instance** *vpn-instance-name*] [**timeout** *minutes*]	缺省情况下，无IPv4黑名单表项
（可选）添加IPv6黑名单表项	**blacklist ipv6** *source-ipv6-address* [**vpn-instance** *vpn-instance-name*] [**timeout** *minutes*]	缺省情况下，无IPv6黑名单表项
（可选）使能黑名单日志功能	**blacklist logging enable**	缺省情况下，黑名单日志功能处于关闭状态
进入接口视图	**interface** *interface-type interface-number*	-
开启接口上的黑名单过滤功能	**blacklist enable**	缺省情况下，接口上的黑名单功能处于关闭状态

1.11 攻击检测及防范显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后攻击检测及防范的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可以清除攻击检测及防范的统计信息。

表1-24 攻击检测及防范配置的显示和维护

操作	命令
显示接口上的攻击防范统计信息（MSR 2600/MSR 3600）	**display attack-defense statistics interface** *interface-type interface-number*

操作	命令
显示接口上的攻击防范统计信息（MSR 5600）	**display attack-defense statistics interface** *interface-type interface-number* [**slot** *slot-number*]
显示本机攻击防范统计信息（MSR 2600/MSR 3600）	**display attack-defense statistics local**
显示本机攻击防范统计信息（MSR 5600）	**display attack-defense statistics local** [**slot** *slot-number*]
显示攻击防范策略的配置信息	**display attack-defense policy** [*policy-name*]
显示扫描攻击者的IPv4信息（MSR 2600/MSR 3600）	**display attack-defense scan attacker ip** [**interface** *interface-type interface-number*]
显示扫描攻击者的IPv4信息（MSR 5600）	**display attack-defense scan attacker ip** [**interface** *interface-type interface-number* [**slot** *slot-number*]]
显示扫描攻击者的IPv6信息（MSR 2600/MSR 3600）	**display attack-defense scan attacker ipv6** [**interface** *interface-type interface-number*]
显示扫描攻击者的IPv6信息（MSR 5600）	**display attack-defense scan attacker ipv6** [**interface** *interface-type interface-number* [**slot** *slot-number*]]
显示扫描攻击被攻击者的IPv4信息（MSR 2600/MSR 3600）	**display attack-defense scan victim ip** [**interface** *interface-type interface-number*]
显示扫描攻击被攻击者的IPv4信息（MSR 5600）	**display attack-defense scan victim ip** [**interface** *interface-type interface-number* [**slot** *slot-number*]]
显示扫描攻击被攻击者的IPv6信息（MSR 2600/MSR 3600）	**display attack-defense scan victim ipv6** [**interface** *interface-type interface-number*]
显示扫描攻击被攻击者的IPv6信息（MSR 5600）	**display attack-defense scan victim ipv6** [**interface** *interface-type interface-number* [**slot** *slot-number*]]
显示IPv4 flood攻击防范统计信息（MSR 2600/MSR 3600）	**display attack-defense** { **ack-flood** | **dns-flood** | **fin-flood** | **flood** | **http-flood** | **icmp-flood** | **rst-flood** | **syn-flood** | **syn-ack-flood** | **udp-flood** } **statistics ip** [*ip-address* [**vpn** *vpn-instance*]] [**count**] [**interface** *interface-type interface-number* | **local**]
显示IPv4 flood攻击防范统计信息（MSR 5600）	**display attack-defense** { **ack-flood** | **dns-flood** | **fin-flood** | **flood** | **http-flood** | **icmp-flood** | **rst-flood** | **syn-flood** | **syn-ack-flood** | **udp-flood** } **statistics ip** [*ip-address* [**vpn** *vpn-instance*]] [**count**] [[**interface** *interface-type interface-number* | **local**] [**slot** *slot-number*]]
显示IPv6 flood攻击防范统计信息（MSR 2600/MSR 3600）	**display attack-defense** { **ack-flood** | **dns-flood** | **fin-flood** | **flood** | **http-flood** | **icmpv6-flood** | **rst-flood** | **syn-flood** | **syn-ack-flood** | **udp-flood** } **statistics ipv6** [*ip-address* [**vpn** *vpn-instance*]] [**count**] [**interface** *interface-type interface-number* | **local**]
显示IPv6 flood攻击防范统计信息（MSR 5600）	**display attack-defense** { **ack-flood** | **dns-flood** | **fin-flood** | **flood** | **http-flood** | **icmpv6-flood** | **rst-flood** | **syn-flood** | **syn-ack-flood** | **udp-flood** } **statistics ipv6** [*ip-address* [**vpn** *vpn-instance*]] [**count**] [[**interface** *interface-type interface-number* | **local**] [**slot** *slot-number*]]
显示flood攻击防范的IPv4类型的受保护IP表项（MSR 2600/MSR 3600）	**display attack-defense policy** *policy-name* { **ack-flood** | **dns-flood** | **fin-flood** | **flood** | **http-flood** | **icmp-flood** | **rst-flood** | **syn-flood** | **udp-flood** } **ip** [*ip-address* [**vpn** *vpn-instance*]] [**count**]

操作	命令
显示flood攻击防范的IPv4类型的受保护IP表项（MSR 5600）	**display attack-defense policy** *policy-name* { **ack-flood** | **dns-flood** | **fin-flood** | **flood** | **http-flood** | **icmp-flood** | **rst-flood** | **syn-flood** | **udp-flood** } **ip** [*ip-address* [**vpn** *vpn-instance*]] [**slot** *slot-number*]] [**count**]
显示flood攻击防范的IPv6类型的受保护IP表项（MSR 2600/MSR 3600）	**display attack-defense policy** *policy-name* { **ack-flood** | **dns-flood** | **fin-flood** | **flood** | **http-flood** | **icmpv6-flood** | **rst-flood** | **syn-flood** | **udp-flood** } **ipv6** [*ip-address* [**vpn** *vpn-instance*]] [**count**]
显示flood攻击防范的IPv6类型的受保护IP表项（MSR 5600）	**display attack-defense policy** *policy-name* { **ack-flood** | **dns-flood** | **fin-flood** | **flood** | **http-flood** | **icmpv6-flood** | **rst-flood** | **syn-flood** | **udp-flood** } **ipv6** [*ip-address* [**vpn** *vpn-instance*]] [**slot** *slot-number*]] [**count**]
显示IPv4黑名单信息（MSR 2600/MSR 3600）	**display blacklist ip** [*source-ip-address* [**vpn-instance** *vpn-instance-name*]] [**count**]
显示IPv4黑名单信息（MSR 5600）	**display blacklist ip** [*source-ip-address* [**vpn-instance** *vpn-instance-name*]] [**slot** *slot-number*] [**count**]
显示IPv6黑名单信息（MSR 2600/MSR 3600）	**display blacklist ipv6** [*source-ip-address* [**vpn-instance** *vpn-instance-name*]] [**count**]
显示IPv6黑名单信息（MSR 5600）	**display blacklist ipv6** [*source-ip-address* [**vpn-instance** *vpn-instance-name*]] [**slot** *slot-number*] [**count**]
显示客户端验证的IPv4类型的受保护IP表项（MSR 2600/MSR 3600）	**display client-verify** { **dns** | **http** | **tcp** } **protected ip** [*ip-address* [**vpn** *vpn-instance*]] [**port** *port-number*] [**count**]
显示客户端验证的IPv4类型的受保护IP表项（MSR 5600）	**display client-verify** { **dns** | **http** | **tcp** } **protected ip** [*ip-address* [**vpn** *vpn-instance*]] [**port** *port-number*] [**slot** *slot-number*]] [**count**]
显示客户端验证的IPv6类型的受保护IP表项（MSR 2600/MSR 3600）	**display client-verify** { **dns** | **http** | **tcp** } **protected ipv6** [*ip-address* [**vpn** *vpn-instance*]] [**port** *port-number*] [**count**]
显示客户端验证的IPv6类型的受保护IP表项（MSR 5600）	**display client-verify** { **dns** | **http** | **tcp** } **protected ipv6** [*ip-address* [**vpn** *vpn-instance*]] [**port** *port-number*] [**slot** *slot-number*]] [**count**]
显示客户端验证的IPv4类型的信任IP表项（MSR 2600/MSR 3600）	**display client-verify** { **dns** | **http** | **tcp** } **trusted ip** [*ipv6-address* [**vpn** *vpn-instance*]] [**count**]
显示客户端验证的IPv4类型的信任IP表项（MSR 5600）	**display client-verify** { **dns** | **http** | **tcp** } **trusted ip** [*ipv6-address* [**vpn** *vpn-instance*]] [**count**] [**slot** *slot-number*]]
显示客户端验证的IPv6类型的信任IP表项（MSR 2600/MSR 3600）	**display client-verify** { **dns** | **http** | **tcp** } **trusted ipv6** [*ipv6-address* [**vpn** *vpn-instance*]] [**count**]
显示客户端验证的IPv6类型的信任IP表项（MSR 5600）	**display client-verify** { **dns** | **http** | **tcp** } **trusted ipv6** [*ipv6-address* [**vpn** *vpn-instance*]] [**count**] [**slot** *slot-number*]]
清除接口上的攻击防范统计信息	**reset attack-defense statistics interface** *interface-type interface-number*
清除flood攻击防范受保护IP表项的统计信息	**reset attack-defense policy** *policy-name* **flood protected** { **ip** | **ipv6** } **statistics**
清除本机攻击防范的统计信息	**reset attack-defense statistics local**
清除IPv4动态黑名单表项	**reset blacklist ip** { *source-ip-address* [**vpn-instance** *vpn-instance-name*] | **all** }

操作	命令
清除IPv6动态黑名单表项	**reset blacklist ipv6** { *source-ip-address* [**vpn-instance** *vpn-instance-name*] | **all** }
清除黑名单表项的统计信息	**reset blacklist statistics**
清除受Client verify保护的IP表项的统计信息	**reset client-verify** { **dns** | **http** | **tcp** } **protected** { **ip** | **ipv6** } **statistics**
清除所有客户端通过验证的信任IP列表	**reset client-verify** { **dns** | **http** | **tcp** } **trusted** { **ip** | **ipv6** }

1.12 攻击检测及防范典型配置举例

1.12.1 配置攻击防范

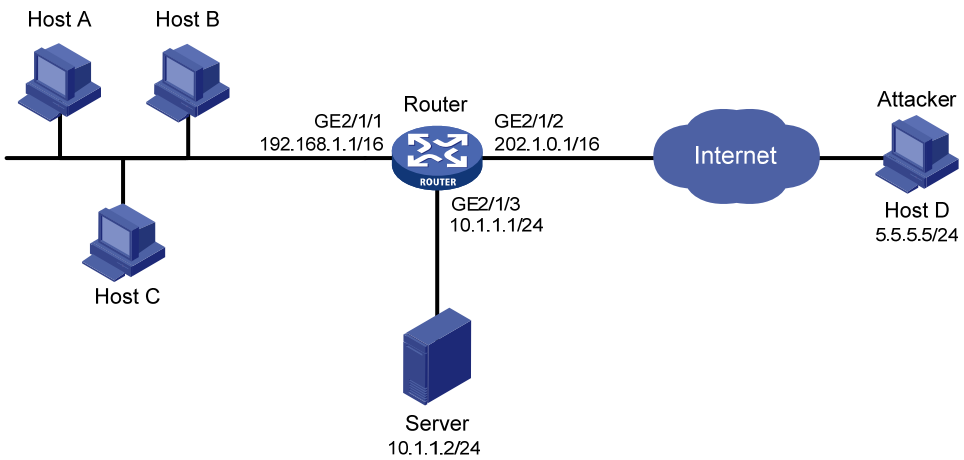
1. 组网需求

Router 上的接口 GigbitEthernet2/1/1 与内部网络连接，接口 GigbitEthernet2/1/2 与外部网络连接，接口 GigbitEthernet2/1/3 与一台内部服务器连接。现有如下安全需求：

- 为防范外部网络对内部网络主机的 Smurf 攻击和扫描攻击，需要在接口 GigabitEthernet2/1/2 上开启 Smurf 攻击防范和扫描攻击防范。具体要求为：启动扫描攻击防范的连接速率阈值为每秒 4500 个连接数；将扫描攻击者添加到黑名单中（老化时间为 10 分钟）；检测到 Smurf 攻击或扫描攻击后，输出告警日志。
- 为防范外部网络对内部服务器的 SYN flood 攻击，需要在接口 GigabitEthernet2/1/2 上开启 SYN flood 攻击防范。具体要求为：当设备监测到向内部服务器每秒发送的 SYN 报文数持续达到或超过 5000 时，输出告警日志并丢弃攻击报文。

2. 组网图

图1-9 接口上的攻击防范配置典型组网图



3. 配置步骤

配置各接口的 IP 地址，略。

开启全局黑名单过滤功能。

```
<Router> system-view
[Router] blacklist global enable
```
创建攻击防范策略 a1。
```
[Router] attack-defense policy a1
```
开启 Smurf 单包攻击报文的特征检测，配置处理行为为输出告警日志。
```
[Router-attack-defense-policy-a1] signature detect smurf action logging
```
开启低防范级别的扫描攻击防范，配置处理行为输出告警日志以及阻断并将攻击者的源 IP 地址加入黑名单表项。
```
[Router-attack-defense-policy-a1] scan detect level low action logging block-source
[Router-attack-defense-policy-a1] quit
```
在接口 GigabitEthernet2/1/2 上应用攻击防范策略 a1。
```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] attack-defense apply policy a1
[Router-GigabitEthernet2/1/2] quit
```
创建攻击防范策略 a2。
```
[Router] attack-defense policy a2
```
配置 SYN flood 攻击防范的全局触发阈值为 4500。
```
[Router-attack-defense-policy-a2] syn-flood threshold 4500
```
配置对 SYN flood 攻击防范的全局处理行为输出告警日志并丢弃攻击报文。
```
[Router-attack-defense-policy-a2] syn-flood action logging drop
```
为保护 IP 地址为 10.1.1.2 的内部服务器，配置针对 IP 地址 10.1.1.2 的 SYN flood 攻击防范参数，触发阈值为 5000。
```
[Router-attack-defense-policy-a2] syn-flood detect ip 10.1.1.2 threshold 5000
[Router-attack-defense-policy-a2] quit
```
在接口 GigabitEthernet2/1/2 上应用攻击防范策略 a2。
```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] attack-defense apply policy a2
[Router-GigabitEthernet2/1/2] quit
```

4. 验证配置

完成以上配置后，可以通过 **display attack-defense policy** 命令查看配置的攻击防范策略 a1 和 a2 的具体内容。

查看攻击防范策略 a1 的配置信息。
```
[Router] display attack-defense policy a1
          Attack-defense Policy Information
------------------------------------------------------------------------------
Policy name                         : a1
Applied list                        : GE2/1/2
------------------------------------------------------------------------------
Exempt IPv4 ACL                     : Not configured
Exempt IPv6 ACL                     : Not configured
------------------------------------------------------------------------------
  Actions: CV-Client verify  BS-Block source  L-Logging  D-Drop  N-None
```

Signature attack defense configuration:

Signature name	Defense	Level	Actions
Fragment	Disabled	low	L
Impossible	Disabled	medium	L,D
Teardrop	Disabled	medium	L,D
Tiny fragment	Disabled	low	L
IP option abnormal	Disabled	medium	L,D
Smurf	Enabled	medium	L
Traceroute	Disabled	low	L
Ping of death	Disabled	medium	L,D
Large ICMP	Disabled	info	L
Max length	4000 bytes		
Large ICMPv6	Disabled	info	L
Max length	4000 bytes		
TCP invalid flags	Disabled	medium	L,D
TCP null flag	Disabled	medium	L,D
TCP all flags	Disabled	medium	L,D
TCP SYN-FIN flags	Disabled	medium	L,D
TCP FIN only flag	Disabled	medium	L,D
TCP Land	Disabled	medium	L,D
Winnuke	Disabled	medium	L,D
UDP Bomb	Disabled	medium	L,D
UDP Snork	Disabled	medium	L,D
UDP Fraggle	Disabled	medium	L,D
IP option record route	Disabled	info	L
IP option internet timestamp	Disabled	info	L
IP option security	Disabled	info	L
IP option loose source routing	Disabled	info	L
IP option stream ID	Disabled	info	L
IP option strict source routing	Disabled	info	L
IP option route alert	Disabled	info	L
ICMP echo request	Disabled	info	L
ICMP echo reply	Disabled	info	L
ICMP source quench	Disabled	info	L
ICMP destination unreachable	Disabled	info	L
ICMP redirect	Disabled	info	L
ICMP time exceeded	Disabled	info	L
ICMP parameter problem	Disabled	info	L
ICMP timestamp request	Disabled	info	L
ICMP timestamp reply	Disabled	info	L
ICMP information request	Disabled	info	L
ICMP information reply	Disabled	info	L
ICMP address mask request	Disabled	info	L
ICMP address mask reply	Disabled	info	L
ICMPv6 echo request	Disabled	info	L
ICMPv6 echo reply	Disabled	info	L
ICMPv6 group membership query	Disabled	info	L
ICMPv6 group membership report	Disabled	info	L

```
ICMPv6 group membership reduction  Disabled     info              L
ICMPv6 destination unreachable     Disabled     info              L
ICMPv6 time exceeded               Disabled     info              L
ICMPv6 parameter problem           Disabled     info              L
ICMPv6 packet too big              Disabled     info              L

Scan attack defense configuration:
 Defense : Enabled
 Level   : low
 Actions : L,BS(10)

Flood attack defense configuration:
Flood type      Global thres(pps)  Global actions  Service ports   Non-specific
SYN flood       1000(default)      -               -               Disabled
ACK flood       1000(default)      -               -               Disabled
SYN-ACK flood   1000(default)      -               -               Disabled
RST flood       1000(default)      -               -               Disabled
FIN flood       1000(default)      -               -               Disabled
UDP flood       1000(default)      -               -               Disabled
ICMP flood      1000(default)      -               -               Disabled
ICMPv6 flood    1000(default)      -               -               Disabled
DNS flood       1000(default)      -               53              Disabled
HTTP flood      1000(default)      -               80              Disabled

Flood attack defense for protected IP addresses:
 Address                 VPN instance Flood type    Thres(pps) Actions Ports
```

查看攻击防范策略 a2 的配置信息。

```
[Router] display attack-defense policy a2
          Attack-defense Policy Information
-------------------------------------------------------------------------
Policy name                         : a2
Applied list                        : GE2/1/2
-------------------------------------------------------------------------
Exempt IPv4 ACL                     : Not configured
Exempt IPv6 ACL                     : Not configured
-------------------------------------------------------------------------
  Actions: CV-Client verify  BS-Block source  L-Logging  D-Drop  N-None

Signature attack defense configuration:
Signature name                      Defense      Level             Actions
Fragment                            Disabled     low               L
Impossible                          Disabled     medium            L,D
Teardrop                            Disabled     medium            L,D
Tiny fragment                       Disabled     low               L
IP option abnormal                  Disabled     medium            L,D
Smurf                               Disabled     medium            L,D
Traceroute                          Disabled     low               L
Ping of death                       Disabled     medium            L,D
```

```
Large ICMP                          Disabled     info             L
  Max length                        4000 bytes
Large ICMPv6                        Disabled     info             L
  Max length                        4000 bytes
TCP invalid flags                   Disabled     medium           L,D
TCP null flag                       Disabled     medium           L,D
TCP all flags                       Disabled     medium           L,D
TCP SYN-FIN flags                   Disabled     medium           L,D
TCP FIN only flag                   Disabled     medium           L,D
TCP Land                            Disabled     medium           L,D
Winnuke                             Disabled     medium           L,D
UDP Bomb                            Disabled     medium           L,D
UDP Snork                           Disabled     medium           L,D
UDP Fraggle                         Disabled     medium           L,D
IP option record route              Disabled     info             L
IP option internet timestamp        Disabled     info             L
IP option security                  Disabled     info             L
IP option loose source routing      Disabled     info             L
IP option stream ID                 Disabled     info             L
IP option strict source routing     Disabled     info             L
IP option route alert               Disabled     info             L
ICMP echo request                   Disabled     info             L
ICMP echo reply                     Disabled     info             L
ICMP source quench                  Disabled     info             L
ICMP destination unreachable        Disabled     info             L
ICMP redirect                       Disabled     info             L
ICMP time exceeded                  Disabled     info             L
ICMP parameter problem              Disabled     info             L
ICMP timestamp request              Disabled     info             L
ICMP timestamp reply                Disabled     info             L
ICMP information request            Disabled     info             L
ICMP information reply              Disabled     info             L
ICMP address mask request           Disabled     info             L
ICMP address mask reply             Disabled     info             L
ICMPv6 echo request                 Disabled     info             L
ICMPv6 echo reply                   Disabled     info             L
ICMPv6 group membership query       Disabled     info             L
ICMPv6 group membership report      Disabled     info             L
ICMPv6 group membership reduction   Disabled     info             L
ICMPv6 destination unreachable      Disabled     info             L
ICMPv6 time exceeded                Disabled     info             L
ICMPv6 parameter problem            Disabled     info             L
ICMPv6 packet too big               Disabled     info             L

Scan attack defense configuration:
 Defense : Disabled
 Level   : -
 Actions : -
```

```
Flood attack defense configuration:
Flood type      Global thres(pps)  Global actions  Service ports   Non-specific
SYN flood       4500               L,D             -               Disabled
ACK flood       1000(default)      -               -               Disabled
SYN-ACK flood   1000(default)      -               -               Disabled
RST flood       1000(default)      -               -               Disabled
FIN flood       1000(default)      -               -               Disabled
UDP flood       1000(default)      -               -               Disabled
ICMP flood      1000(default)      -               -               Disabled
ICMPv6 flood    1000(default)      -               -               Disabled
DNS flood       1000(default)      -               53              Disabled
HTTP flood      1000(default)      -               80              Disabled

Flood attack defense for protected IP addresses:
 Address                 VPN instance Flood type    Thres(pps) Actions Ports
 10.1.1.2                --           SYN-FLOOD     5000       -       -
```

如果接口 GigabitEthernet2/1/2 上收到 Smurf 攻击报文，设备输出告警日志；如果接口 GigabitEthernet2/1/2 上收到扫描攻击报文，设备会输出告警日志，并将攻击者的 IP 地址加入黑名单；如果接口 GigabitEthernet2/1/3 上收到的 SYN flood 攻击报文超过触发阈值，则设备会输出告警日志，并将受到攻击的主机地址添加到 TCP 客户端验证的受保护 IP 列表中，同时丢弃攻击报文。

之后，可以通过 **display attack-defense statistics interface** 命令查看各接口上攻击防范的统计信息。

查看接口 GE2/1/2 上攻击防范的统计信息。

```
<Router> display attack-defense statistics interface GE2/1/2
Attack policy name: a1
Scanning attack defense statistics:
 AttackType                      AttackTimes Dropped
 Port scan                       2           0
 IP sweep                        3           0
 Distribute port scan            1           0
Flood attack defense statistics:
 AttackType                      AttackTimes Dropped
 SYN flood                       1           5000
Signature attack defense statistics:
 AttackType                      AttackTimes Dropped
 Smurf                           1           0
```

若有扫描攻击发生，还可以通过 **display blacklist** 命令查看由扫描攻击防范自动添加的黑名单信息。

查看由扫描攻击防范自动添加的黑名单信息。

```
[Router] display blacklist ip
IP address      VPN instance   DS-Lite tunnel peer  Type    TTL(sec) Dropped
5.5.5.5         --             --                   Dynamic 600      353452
```

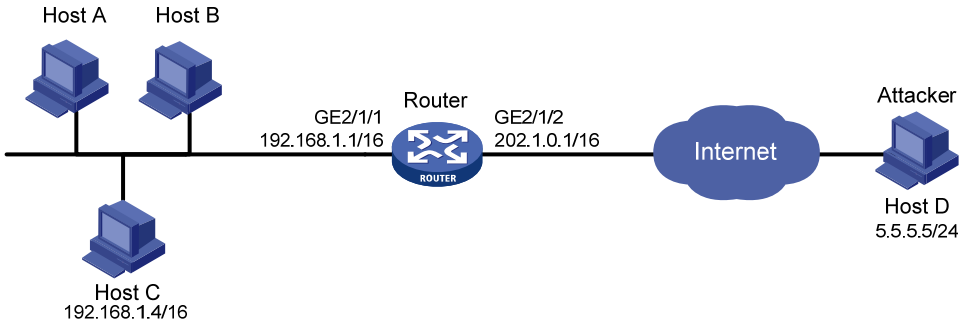
1.12.2 黑名单配置举例

1. 组网需求

网络管理员通过流量分析发现外部网络中存在一个攻击者 Host D，需要将来自 Host D 的报文在 Router 上永远过滤掉。另外，网络管理员为了暂时控制内部网络 Host C 的访问行为，需要将 Router 上收到的 Host C 的报文阻止 50 分钟。

2. 组网图

图1-10 黑名单配置典型组网图



3. 配置步骤

配置各接口的 IP 地址，略。

开启全局黑名单过滤功能。

```
<Router> system-view
[Router] blacklist global enable
```

将 Host D 的 IP 地址 5.5.5.5 添加到黑名单列表中，；老化时间使用缺省情况（永不老化）。

```
[Router] blacklist ip 5.5.5.5
```

将 Host C 的 IP 地址 192.168.1.4 添加到黑名单列表中，老化时间为 50 分钟。

```
[Router] blacklist ip 192.168.1.4 timeout 50
```

4. 验证配置

完成以上配置后，可以通过 **display blacklist** 命令查看已添加的黑名单信息。

```
<Router> display blacklist ip
IP address      VPN instance   DS-Lite tunnel peer  Type    TTL(sec) Dropped
5.5.5.5         --             --                   Manual  Never    0
192.168.1.4     --             --                   Manual  2989     0
```

配置生效后，Router 对来自 Host D 的报文一律进行丢弃处理，除非管理员认为 Host D 不再是攻击者，通过 **undo blacklist ip 5.5.5.5** 将其从黑名单中删除；如果 Router 接收到来自 Host C 的报文，则在 50 分钟之内，一律对其进行丢弃处理，50 分钟之后，才进行正常转发。

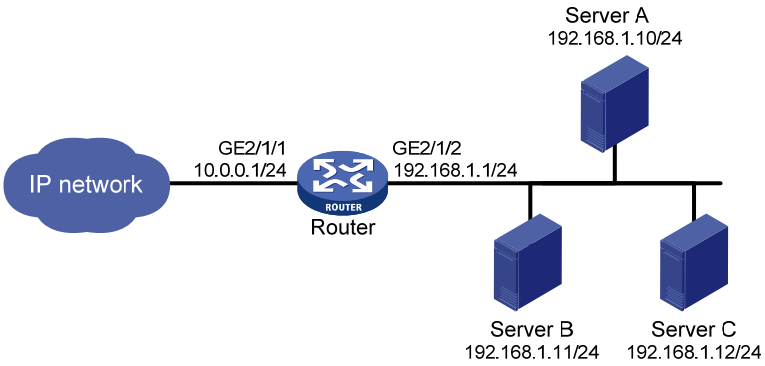
1.12.3 TCP客户端验证配置举例

1. 组网需求

在 Router 上配置 TCP 客户端验证功能，保护内网服务器不会受到外网非法用户的 SYN flood 攻击，并要求在客户端与服务器之间进行双向代理。

2. 组网图

图1-11 TCP 客户端验证配置组网图



3. 配置步骤

配置各接口的 IP 地址，略。

创建攻击防范策略 a1。

```
<Router> system-view
[Router] attack-defense policy a1
```

对所有非受保护 IP 地址开启 SYN flood 攻击防范检测。

```
[Router-attack-defense-policy-a1] syn-flood detect non-specific
```

配置 SYN flood 攻击防范的全局触发阈值为 10000。

```
[Router-attack-defense-policy-a1] syn-flood threshold 10000
```

配置 SYN flood 攻击防范的全局处理行为为添加到 TCP 客户端验证的受保护 IP 列表中以及输出告警日志。

```
[Router-attack-defense-policy-a1] syn-flood action logging client-verify
[Router-attack-defense-policy-a1] quit
```

在接口 GigabitEthernet2/1/1 上应用攻击防范策略 a1。

```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] attack-defense apply policy a1
[Router-GigabitEthernet2/1/1] quit
```

在接口 GigabitEthernet2/1/1 上开启 TCP 客户端验证的双向代理功能。

```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] client-verify tcp enable mode syn-cookie
[Router-GigabitEthernet2/1/1] quit
```

4. 验证配置结果

以上配置完成之后，若有针对服务器的 SYN flood 攻击发生时，可以通过 **display client-verify tcp protected ip** 命令查看受攻击的服务器的 IP 地址被添加为动态受保护 IP。

```
[Router] display client-verify tcp protected ip
IP address           VPN instance     Port  Type    TTL(min) Requested  Authenticated
192.168.1.10         --               any   Dynamic 30       20         12
```

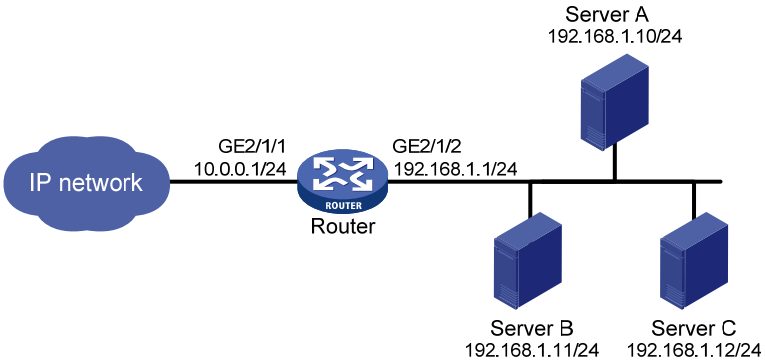
1.12.4 DNS客户端验证配置举例

1. 组网需求

在Router上配置DNS客户端验证功能，保护内网服务器不会受到外网非法用户的DNS flood攻击。

2. 组网图

图1-12 DNS 客户端验证配置组网图



3. 配置步骤

配置各接口的 IP 地址，略。

创建攻击防范策略 a1。

```
<Router> system-view
[Router] attack-defense policy a1
```

对所有非受保护 IP 地址开启 DNS flood 攻击防范检测。

```
[Router-attack-defense-policy-a1] dns-flood detect non-specific
```

配置 DNS flood 攻击防范的的全局触发阈值为 10000。

```
[Router-attack-defense-policy-a1] dns-flood threshold 10000
```

配置 DNS flood 攻击防范的全局处理行为为添加到 DNS 客户端验证的受保护 IP 列表中以及输出告警日志。

```
[Router-attack-defense-policy-a1] dns-flood action logging client-verify
[Router-attack-defense-policy-a1] quit
```

在接口 GigabitEthernet2/1/1 上应用攻击防范策略 a1。

```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] attack-defense apply policy a1
[Router-GigabitEthernet2/1/1] quit
```

在接口 GigabitEthernet2/1/1 上开启 DNS 客户端验证功能。

```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] client-verify dns enable
[Router-GigabitEthernet2/1/1] quit
```

4. 验证配置

以上配置完成之后，若有针对服务器的 DNS flood 攻击发生时，可以通过 **display client-verify dns protected ip** 命令查看受攻击的服务器的 IP 地址被添加为动态受保护 IP。

```
[Router] display client-verify dns protected ip
IP address          VPN instance     Port  Type    TTL(min) Requested  Authenticated
```

```
192.168.1.10          --                53     Dynamic 30        20           12
```

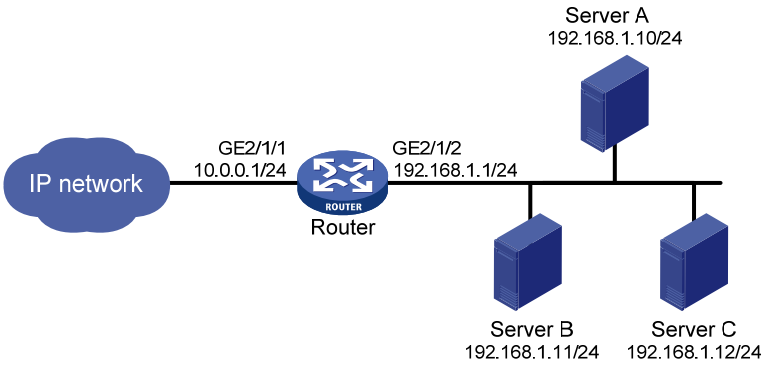
1.12.5 配置HTTP客户端验证

1. 组网需求

在 Router 上配置 HTTP 客户端验证功能，保护内网服务器不会受到外网非法用户的 HTTP flood 攻击。

2. 组网图

图1-13 HTTP 客户端验证配置组网图



3. 配置步骤

配置各接口的 IP 地址，略。

创建攻击防范策略 a1。

```
<Router> system-view
[Router] attack-defense policy a1
```

对所有非受保护 IP 地址开启 HTTP flood 攻击防范检测。

```
[Router-attack-defense-policy-a1] http-flood detect non-specific
```

配置 HTTP flood 攻击防范的全局触发阈值为 10000。

```
[Router-attack-defense-policy-a1] http-flood threshold 10000
```

配置 HTTP flood 攻击防范的全局处理行为添加到 HTTP 客户端验证的受保护 IP 列表中以及输出告警日志。

```
[Router-attack-defense-policy-a1] http-flood action logging client-verify
[Router-attack-defense-policy-a1] quit
```

在接口 GigabitEthernet2/1/1 上应用攻击防范策略 a1。

```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] attack-defense apply policy a1
[Router-GigabitEthernet2/1/1] quit
```

在接口 GigabitEthernet2/1/1 上使能 HTTP 客户端验证功能。

```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] client-verify http enable
[Router-GigabitEthernet2/1/1] quit
```

4. 验证配置

以上配置完成之后，若有针对服务器的 HTTP flood 攻击发生时，可以通过 **display client-verify http protected ip** 命令查看受攻击的服务器的 IP 地址被添加为动态受保护 IP。

```
[Router] display client-verify http protected ip
IP address           VPN instance     Port  Type    TTL(min) Requested  Authenticated
192.168.1.10         --               8080  Dynamic 30       20          12
```