



H3C S5500-HI 系列以太网交换机

安全配置指导

杭州华三通信技术有限公司
<http://www.h3c.com.cn>

资料版本: 6W102-20131220
产品版本: Release 52xx 系列

Copyright © 2013 杭州华三通信技术有限公司及其许可者 版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

H3C、**H3C**、H3CS、H3CIE、H3CNE、Aolynk、、H³Care、、IRF、NetPilot、Netflow、SecEngine、SecPath、SecCenter、SecBlade、Comware、ITCMM、HUASAN、华三均为杭州华三通信技术有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。**H3C** 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，**H3C** 尽全力在本手册中提供准确的信息，但是 **H3C** 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前言

H3C S5500-HI 系列以太网交换机配置指导共分为十一本手册，介绍了 S5500-HI 系列以太网交换机 Release52xx 系列软件版本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》主要介绍了各种安全业务特性的原理及配置方法，包括 AAA、802.1X、MAC 地址认证、Portal 认证等接入认证特性，以及 IP Source Guard、ARP 攻击防御等安全防护特性。

前言部分包含如下内容：

- [读者对象](#)
- [新增及修改特性说明](#)
- [本书约定](#)
- [产品配套资料](#)
- [资料获取方式](#)
- [技术支持](#)
- [资料意见反馈](#)

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

新增及修改特性说明

本手册对应 S5500-HI 系列以太网交换机的 Release52xx 系列软件版本，各版本间特性差异如下：

- Release5206 与 Release5203 版本相比，新增、修改了部分特性，具体请参见 [表 1](#)。
- Release5203 与 Release5101 版本相比，新增、修改了部分特性，具体请参见 [表 2](#)。

表1 Release5206 与 Release5203 版本间特性差异

配置指导	新增及修改特性
AAA	新增特性：支持多备份HWTACACS服务器
MAC地址认证	新增特性：配置MAC地址认证支持多VLAN模式
IP Source Guard	新增特性：基于802.1X认证的IP Source Guard动态表项获取功能
ARP攻击防御	新增特性：ARP Detection日志功能

表2 Release5203 与 Release5101 版本间特性差异

配置指导	新增及修改特性
AAA	新增特性： - 配置ISP域优先级 - 配置RADIUS报文的DSCP优先级 - 配置主/从RADIUS认证/授权服务器状态探测功能 - RADIUS/HWTACACS认证、授权、计费报文的共享密钥支持以密文方式配置 - 指定与RADIUS客户端通信的共享密钥支持以密文方式配置 修改特性：设置本地用户的密码 删除特性：设置本地用户密码的显示方式
802.1X	新增特性： - 配置802.1X认证的Critical VLAN - 配置802.1X支持的域名分隔符 - 配置端口发送802.1X协议报文不带Tag - 配置MAC地址认证用户进行802.1X认证的最大尝试次数 - 支持VLAN组下发
MAC地址认证	新增特性： - 配置 MAC 地址认证的 Critical VLAN - 配置 MAC 地址认证延时时间
Portal	新增特性： - 配置Portal支持IPv6功能 - 指定与Portal服务器通信的共享密钥支持以密文方式配置
Triple	无
端口安全	无
User Profile	无
Password Control	修改特性：清除所有密码管理黑名单中的用户
HABP	无
公钥管理	无
PKI	新增特性：用密文方式配置吊销证书时使用的密码
IPsec	新增特性： - 支持基于 ACL 建立 IPsec 安全隧道 - 支持 IKE
SSH2.0	新增特性： - 配置 SCP 功能 - 配置 SSH 服务器发送报文的 DSCP 优先级 - 配置 Stelnet 客户端发送报文的 DSCP 优先级 - 配置 SFTP 客户端发送报文的 DSCP 优先级

配置指导	新增及修改特性
SSL	无
TCP攻击防御	无
IP Source Guard	变更特性：IPv4/IPv6端口绑定表项数目的最大值
ARP攻击防御	新增特性：配置用户合法性检查的规则
ND攻击防御	无
URPF	无
MFF	无
SAVI	新增特性：配置SAVI绑定表项延迟时间
黑名单	无
FIPS	FIPS相关配置为本版本新增特性

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。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 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. 图形界面格式约定

格 式	意 义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[]	带方括号“[]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 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。

4. 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。

5. 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 S5500-HI 系列以太网交换机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	产品彩页	帮助您了解产品的主要规格参数及亮点
	技术白皮书	帮助您了解产品和特性功能，对于特色及复杂技术从细节上进行介绍
硬件介绍及安装	安全兼容性手册	列出产品的兼容性声明，并对兼容性和安全的细节进行说明
	H3C 设备防雷安装指导手册	帮助您了解防雷接地设计和工程安装方法，以保证交换机具有良好的抗雷击性能
	快速安装指南	指导您对设备进行初始安装，通常针对最常用的情况，减少您的检索时间

大类	资料名称	内容介绍
	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
	风扇安装手册	帮助您了解产品支持的可插拔风扇模块的外观、功能、规格、安装及拆卸方法
	电源手册	帮助您了解产品支持的可插拔电源模块的外观、功能、规格、安装及拆卸方法
	RPS电源用户手册	帮助您了解产品支持的RPS电源的外观、功能、规格
	H3C低端系列以太网交换机RPS电源选购指南	帮助您了解各种RPS电源适用的交换机产品型号及RPS电源配套电缆的相关规格
	接口模块扩展卡用户手册	帮助您了解该接口模块扩展卡的外观、规格、安装及拆卸方法
	H3C低端系列以太网交换机可插拔模块手册	帮助您了解产品支持的可插拔模块类型、外观和规格
	H3C可插拔SFP[SFP+][XFP]模块安装指南	帮助您掌握SFP/SFP+/XFP模块的正确安装方法，避免因操作不当而造成器件损坏
业务配置	配置指导	帮助您掌握设备软件功能的配置方法及配置步骤
	命令参考	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	故障处理手册	指导您快速定位并处理软件故障
	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）

010-62982107

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配置	1-1
1.1 AAA简介	1-1
1.1.1 概述	1-1
1.1.2 RADIUS协议简介	1-2
1.1.3 HWTACACS协议简介	1-7
1.1.4 基于域的用户管理	1-9
1.1.5 设备的RADIUS服务器功能	1-10
1.1.6 AAA支持多实例	1-11
1.1.7 协议规范	1-12
1.1.8 RADIUS属性	1-12
1.2 AAA配置思路及配置任务简介	1-15
1.3 配置AAA方案	1-17
1.3.1 配置本地用户	1-17
1.3.2 配置RADIUS方案	1-21
1.3.3 配置HWTACACS方案	1-35
1.4 在ISP域中配置实现AAA的方法	1-43
1.4.1 配置准备	1-43
1.4.2 创建ISP域	1-43
1.4.3 配置ISP域的属性	1-43
1.4.4 配置ISP域的AAA认证方法	1-45
1.4.5 配置ISP域的AAA授权方法	1-46
1.4.6 配置ISP域的AAA计费方法	1-48
1.5 配置强制切断用户连接	1-50
1.6 配置NAS-ID与VLAN的绑定	1-50
1.7 配置双机热备模式下的设备ID	1-50
1.8 配置设备作为RADIUS服务器	1-51
1.8.1 RADIUS服务器功能配置任务简介	1-51
1.8.2 配置RADIUS用户	1-51
1.8.3 指定RADIUS客户端	1-52
1.9 AAA显示和维护	1-53
1.10 AAA典型配置举例	1-1
1.10.1 Telnet用户的HWTACACS认证、授权、计费配置	1-1
1.10.2 Telnet用户的local认证、HWTACACS授权、RADIUS计费配置	1-2

1.10.3 SSH/Telnet用户的RADIUS认证和授权配置	1-4
1.10.4 Portal用户的RADIUS认证、授权和计费配置	1-7
1.10.5 802.1X用户的RADIUS认证、授权和计费配置	1-15
1.10.6 Telnet用户的HWTACACS级别切换认证配置	1-22
1.10.7 设备作为RADIUS服务器对Telnet用户进行接入认证	1-25
1.11 AAA常见配置错误举例	1-27
1.11.1 RADIUS认证/授权失败	1-27
1.11.2 RADIUS报文传送失败	1-28
1.11.3 RADIUS计费功能异常	1-28
1.11.4 HWTACACS常见配置错误举例	1-28

1 AAA配置

1.1 AAA简介



说明

- 设备运行于 FIPS 模式时，本特性的部分配置相对于非 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”。
- 本章中典型配置举例中的配置，如无特殊说明，均以设备运行在非 FIPS 模式下的命令行为准。

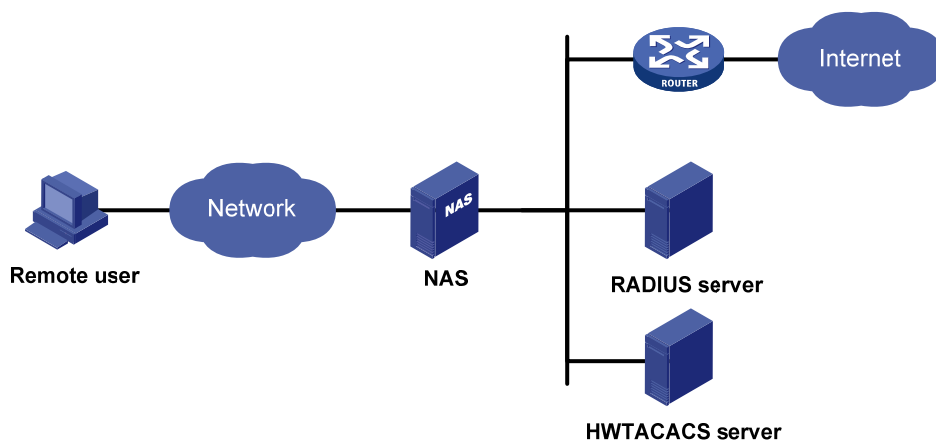
1.1.1 概述

AAA 是 Authentication、Authorization、Accounting（认证、授权、计费）的简称，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。例如用户成功登录服务器后，管理员可以授权用户对服务器中的文件进行访问和打印操作。
- 计费：记录用户使用网络服务中的所有操作，包括使用的服务类型、起始时间、数据流量等，它不仅是一种计费手段，也对网络安全起到了监视作用。

AAA一般采用客户机/服务器结构，客户端运行于NAS（Network Access Server，网络接入服务器）上，服务器上则集中管理用户信息。NAS对于用户来讲是服务器端，对于服务器来说是客户端。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



当用户想要通过某网络与 NAS 建立连接，从而获得访问其它网络的权利或取得某些网络资源的权利时，NAS 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（RADIUS

服务器或 HWTACACS 服务器), RADIUS 协议或 HWTACACS 协议规定了 NAS 与服务器之间如何传递用户信息。

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的时候进行身份认证, 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。

AAA 可以通过多种协议来实现, 目前设备支持基于 RADIUS 协议、HWTACACS 协议来实现 AAA, 在实际应用中, 最常使用 RADIUS 协议。

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。该协议定义了 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、计费端口)。

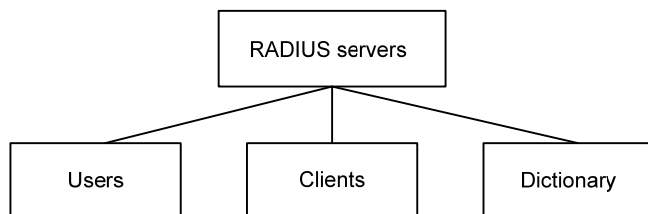
RADIUS 最初仅是针对拨号用户的 AAA 协议, 后来随着用户接入方式的多样化发展, RADIUS 也适应多种用户接入方式, 如以太网接入、ADSL 接入。它通过认证授权来提供接入服务, 通过计费来收集、记录用户对网络资源的使用。

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, 负责传输用户信息到指定的 RADIUS 服务器, 然后根据从服务器返回的信息进行相应处理 (如接受/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, 维护相关的用户认证和网络服务访问信息, 负责接收用户连接请求并认证用户, 然后给客户端返回所有需要的信息 (如接受/拒绝认证请求)。

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. 安全和认证机制

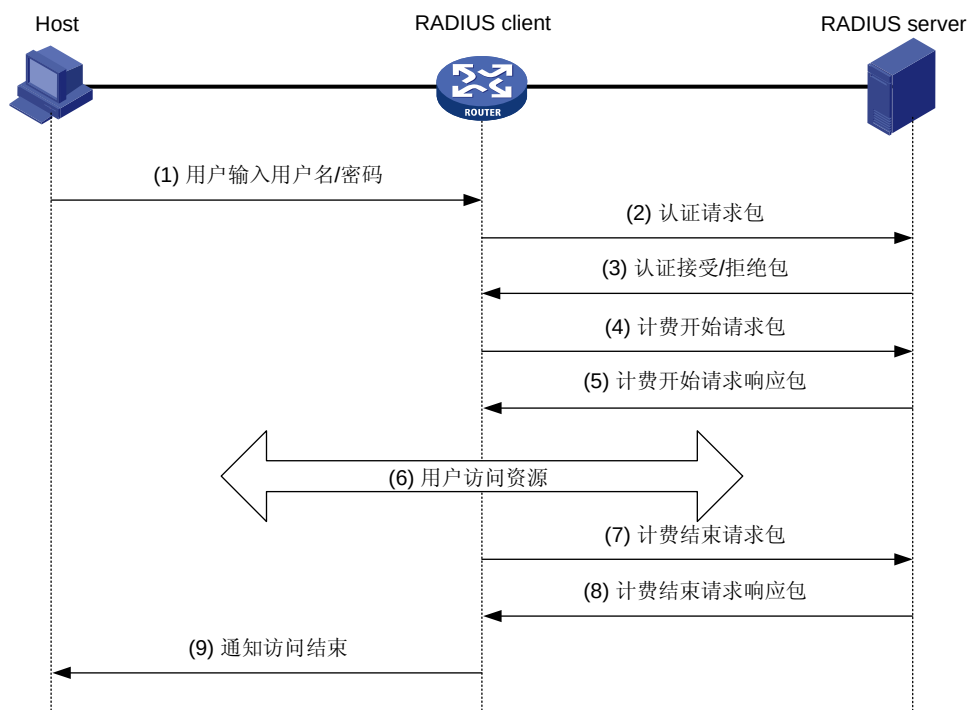
RADIUS 客户端和 RADIUS 服务器之间认证消息的交互是通过共享密钥的参与来完成的，并且共享密钥不能通过网络来传输，增强了信息交互的安全性。另外，为防止用户密码在不安全的网络上传递时被窃取，在传输过程中对密码进行了加密。

RADIUS 服务器支持多种方法来认证用户。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。

3. 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：

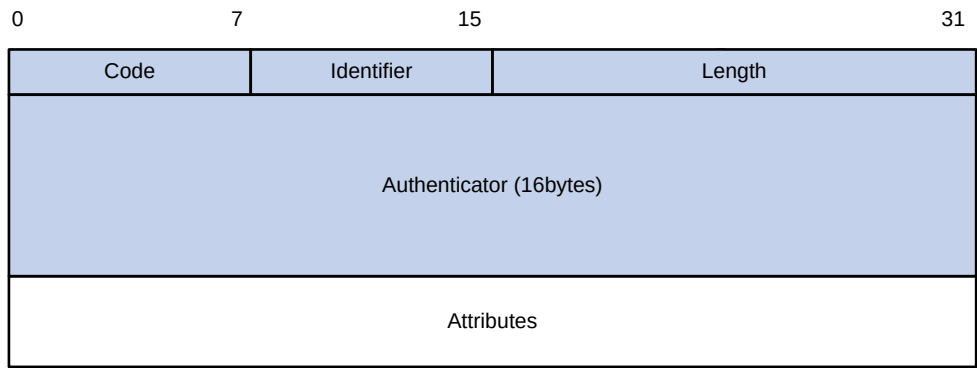
- (1) 用户发起连接请求，向 RADIUS 客户端发送用户名和密码。
- (2) RADIUS 客户端根据获取的用户名和密码，向 RADIUS 服务器发送认证请求包（Access-Request），其中的密码在共享密钥的参与下由 MD5 算法进行加密处理。
- (3) RADIUS 服务器对用户名和密码进行认证。如果认证成功，RADIUS 服务器向 RADIUS 客户端发送认证接受包（Access-Accept）；如果认证失败，则返回认证拒绝包（Access-Reject）。由于 RADIUS 协议合并了认证和授权的过程，因此认证接受包中也包含了用户的授权信息。
- (4) RADIUS 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，RADIUS 客户端向 RADIUS 服务器发送计费停止请求包（Accounting-Request）。

- (8) RADIUS 服务器返回计费结束响应包（Accounting-Response），并停止计费。
- (9) 用户结束访问网络资源。

4. RADIUS报文结构

RADIUS采用UDP报文来传输消息,通过定时器管理机制、重传机制、备用服务器机制,确保RADIUS服务器和客户端之间交互消息的正确收发。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, 由Server判断是否接入该用户。该报文中必须包含User-Name属性, 可选包含NAS-IP-Address、User-Password、NAS-Port等属性
2	Access-Accept认证接受包	方向Server->Client, 如果Access-Request报文中的所有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, 由该报文中的Acct-Status-Type属性区分计费开始请求和计费结束请求
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。类型一致的请求包和响应包的 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,范围从 20~4096。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,提供请求和响应报文的配置细节。Attribute 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), 1 个字节,取值为 1~255,用于表示属性的类型,表 1-2 列出了 RADIUS 认证、 授权、计费常用的属性。
- 长度 (Length), 表示该属性 (包括类型、长度和属性) 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和长度决定,最大长度为 253 字 节。

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
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

属性编号	属性名称	属性编号	属性名称
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



说明

- [表 1-2](#) 中所列的属性由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](#)”。

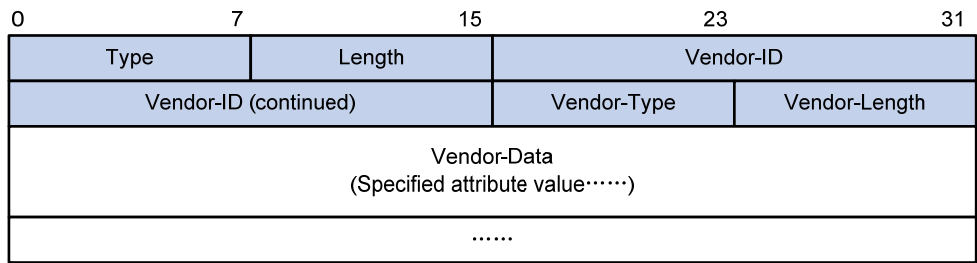
5. RADIUS扩展属性

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。

设备厂商可以封装多个自定义的“(Type、Length、Value)”子属性来扩展RADIUS。如 [图 1-5](#) 所示，26 号属性报文内封装的子属性包括以下四个部分：

- 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。H3C RADIUS扩展属性的介绍请参见“[1.1.8 2. H3C RADIUS扩展属性](#)”。
- 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。

图1-5 包括扩展属性的 RADIUS 报文片断



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，点到点协议）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、计费的功能，它们有很多相似点：结构上都采用客户端/服务器模式；都使用公共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

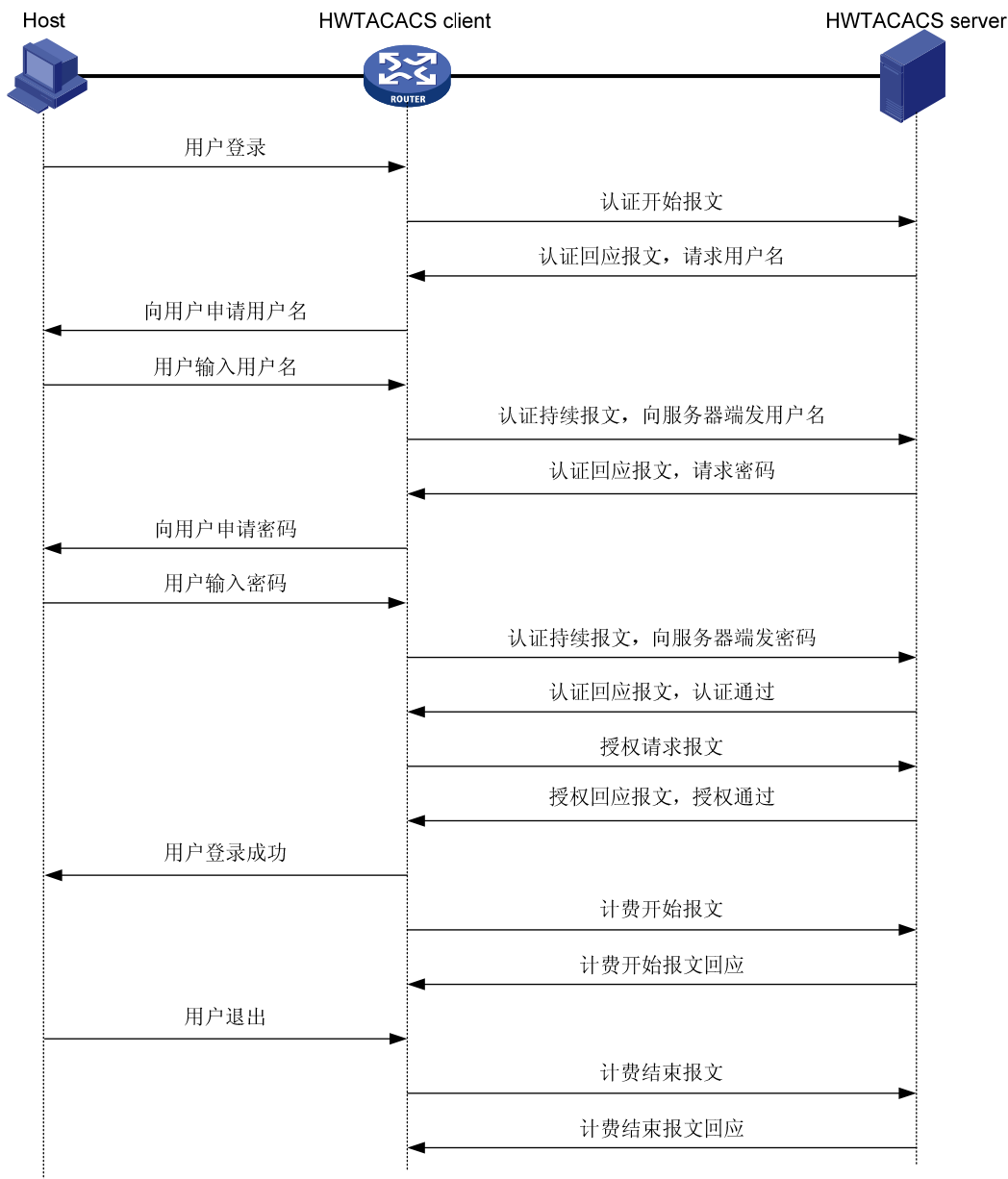
HWTACACS 协议	RADIUS 协议
使用TCP，网络传输更可靠	使用UDP，网络传输效率更高
除了HWTACACS报文头，对报文主体全部进行加密	只对验证报文中的密码字段进行加密
协议报文较为复杂，认证和授权分离，使得认证、授权服务可以分离在不同的安全服务器上实现。例如，可以用一个HWTACACS服务器进行认证，另外一个HWTACACS服务器进行授权	协议报文比较简单，认证和授权结合，难以分离

HWTACACS 协议	RADIUS 协议
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级别和AAA授权的双重限制，某一级别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级别决定，用户只能使用缺省级别等于/低于用户级别的命令行

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



在整个过程中的基本消息交互流程如下：

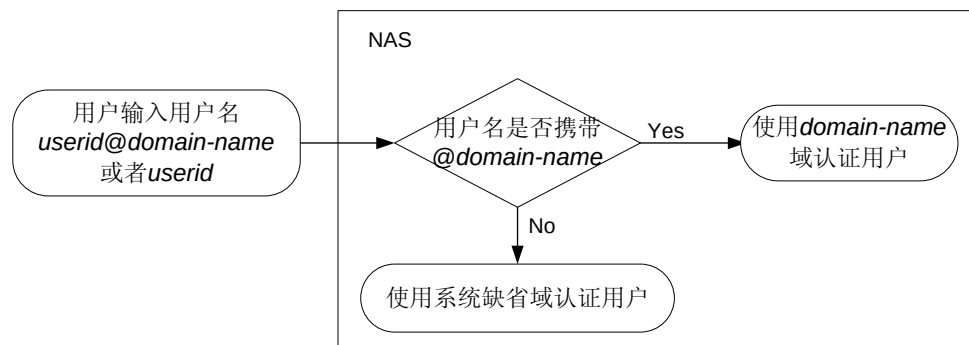
- (1) Telnet 用户请求登录设备。
- (2) HWTACACS 客户端收到请求之后，向 HWTACACS 服务器发送认证开始报文。
- (3) HWTACACS 服务器发送认证回应报文，请求用户名。
- (4) HWTACACS 客户端收到回应报文后，向用户询问用户名。
- (5) 用户输入用户名。
- (6) HWTACACS 客户端收到用户名后，向 HWTACACS 服务器发送认证持续报文，其中包括了用户名。
- (7) HWTACACS 服务器发送认证回应报文，请求登录密码。
- (8) HWTACACS 客户端收到回应报文，向用户询问登录密码。
- (9) 用户输入密码。
- (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) 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) HWTACACS 服务器发送授权回应报文，指示用户通过授权。
- (14) HWTACACS 客户端收到授权回应成功报文，向用户输出设备的配置界面。
- (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 基于域的用户管理

一个 ISP（Internet Service Provider，互联网服务提供商）域是由属于同一个 ISP 的用户构成的群体。

NAS 对用户的管理是基于 ISP 域的，每个接入用户都属于一个 ISP 域。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 1-7](#) 所示。

图1-7 用户名决定域名



用户的认证、授权、计费都是在相应的 ISP 域视图下应用预先配置的认证、授权、计费方案来实现的。AAA 有缺省的认证、授权、计费方案，分别为本地认证、本地授权、本地计费。如果用户所属的 ISP 域下未应用任何认证、授权、计费方案，系统将使用缺省的认证、授权、计费方案。

为便于对不同接入方式的用户进行区分管理，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、Web、FTP、终端接入用户。
- Portal 接入用户。

用户登录设备后，AAA 还可以对其提供以下服务，用于提高用户登录后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：用户执行过的所有命令或被成功授权执行的命令，会被计费服务器进行记录。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”。
- 级别切换认证：在不退出当前登录、不断开当前连接的前提下，用户将自身的用户级别由低向高切换的时候，需要通过服务器的认证，级别切换操作才被允许。关于用户级别切换的详细介绍请参考“基础配置指导”中的“CLI”。

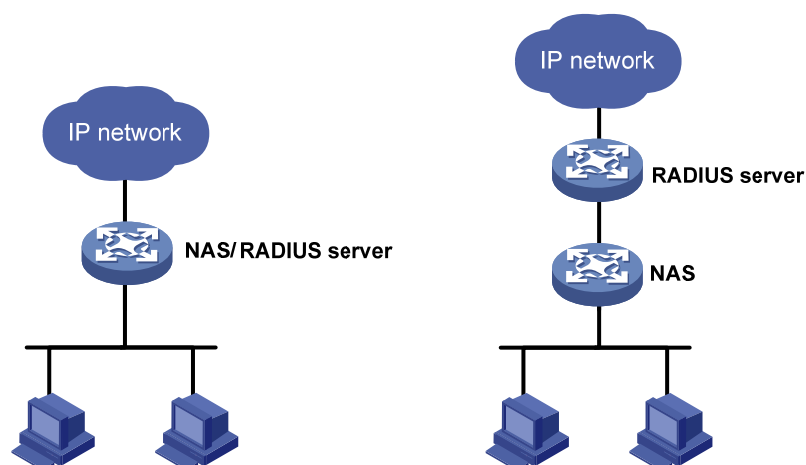
AAA 支持在 ISP 域视图下针对不同的接入方式配置不同的认证、授权、计费的方法（一组不同的认证/授权/计费方案），具体的配置步骤请参见“[1.4 在 ISP 域中配置实现 AAA 的方法](#)”。

1.1.5 设备的 RADIUS 服务器功能

通常，RADIUS 的服务器端位于中心计算机或工作站上，RADIUS 的客户端位于 NAS 上。若网络设备上能够实现 RADIUS 服务器的功能，则该网络设备就可以作为 RADIUS 服务器端与 RADIUS 的客户端配合完成用户的认证、授权和计费等功能。这种情况下，如 [图 1-8](#) 所示，RADIUS 的客户端和 RADIUS 的服务器端既可以集中位于同一台设备上，也可以分别位于不同的设备上。

设备支持 RADIUS 服务器功能给 RADIUS 的应用提供了更多便利，一方面，使得用户组网方式更加灵活，另一方面，可减少用户专门部署 RADIUS 服务器的组网成本。该功能常被应用于集群网络结构中，通过在汇聚层的管理设备上配置 RADIUS 服务器功能，并在接入层的成员设备上部署相应的认证方案，实现对用户的认证、授权。

图1-8 设备作为 RADIUS 服务器典型组网图



设备作为 RADIUS 服务器可以实现如下功能：

- 用户信息管理：支持创建、修改或删除用户信息。用户信息包括用户名、口令、权限、过期时间，以及用户描述信息等。
- RADIUS 客户端信息管理：支持创建、删除 RADIUS 客户端。RADIUS 客户端以 IP 地址为标识，并具有共享密钥等属性。RADIUS 服务器通过配置指定被管理的 RADIUS 客户端，并只处理来自其管理范围内的客户端的 RADIUS 报文，对其它报文直接作丢弃处理。共享密钥用于保证 RADIUS 客户端和 RADIUS 服务器端通信的安全性。
- 支持 RADIUS 协议的认证和授权功能（暂不支持计费功能）。

作为 RADIUS 服务器的设备接收到 RADIUS 报文后，首先检查 RADIUS 客户端是否在可管理的范围内，并使用共享密钥检验报文的合法性，然后依次检查用户帐号是否存在、用户口令是否正确，并根据 RADIUS 服务器的配置检查用户的其它属性是否满足要求，例如帐号是否在有效期内等因素，最后决定是否允许用户通过认证，并对认证通过的用户授予对应的权限。



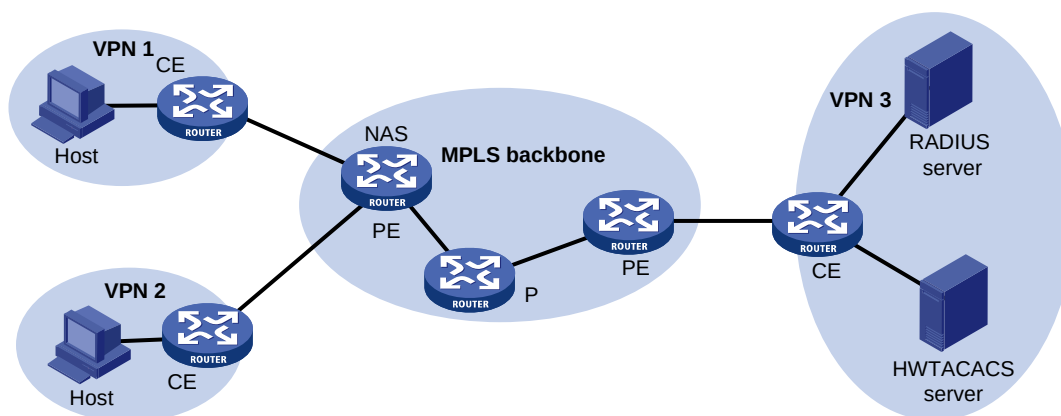
说明

在标准的 RADIUS 协议中，RADIUS 服务器的认证端口为 UDP 端口 1812，我司设备作为 RADIUS 服务器时认证端口为 UDP 端口 1645。因此，在 RADIUS 客户端上配置 RADIUS 方案时，需要指定认证服务器的认证端口号为 1645。

1.1.6 AAA支持多实例

在MPLS VPN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支持基于多实例的报文交互。通过AAA支持多实例，可实现RADIUS、HWTACACS认证/授权/计费报文在MPLS VPN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 VPN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 支持多实例典型组网图





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 的相关介绍请参见“MPLS 配置指导”中的“MCE”。

1.1.7 协议规范

与 AAA、RADIUS、HWTACACS 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 1492: An Access Control Protocol, Sometimes Called TACACS

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 • 2: 802.1X 认证 • 10: MAC 地址认证
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

属性编号	属性名称	描述
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
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
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服务器的时候，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客户端的握手机制 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隔开。本属性用于SSL VPN设备的配合
141	Security_Level	SSL VPN用户安全认证之后下发的安全级别

子属性 编号	子属性名称	描述
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：根据需要配置本地或远程认证方案。

- 本地认证：需要配置本地用户，即 local user 的相关属性，包括手动添加认证的用户名和密码等；
- 远程认证：需要配置 RADIUS、HWTACACS 方案，并在服务器上配置相应的用户属性。

(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。

- 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

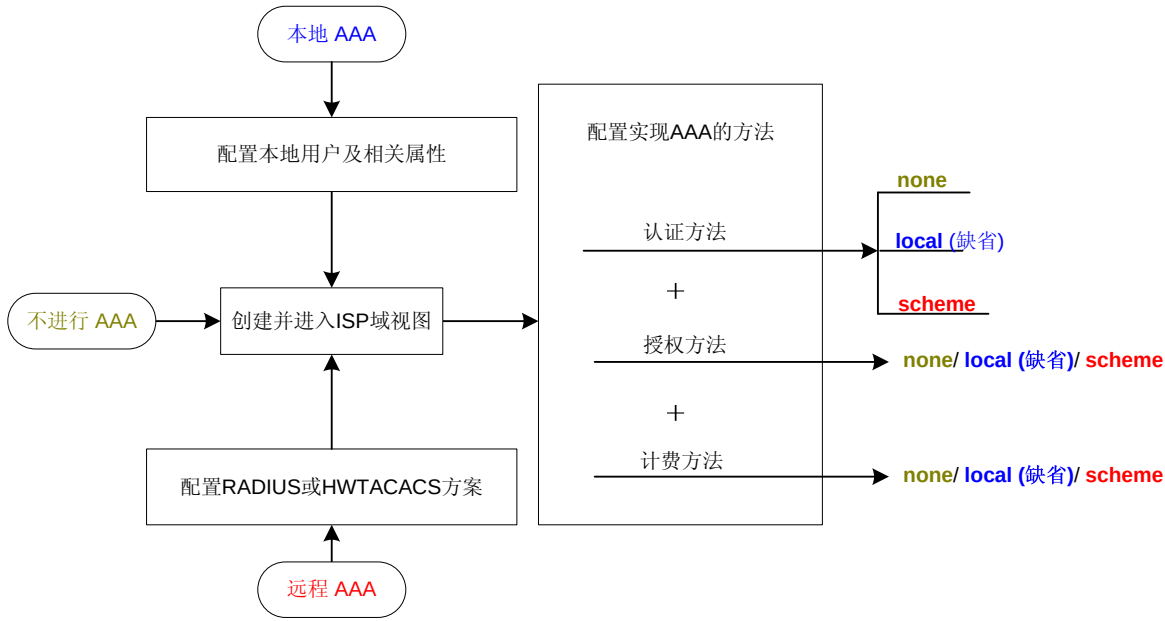


表1-6 AAA 配置任务简介

配置任务		说明	详细配置
配置AAA方案	配置本地用户	至少选其一	1.3.1
	配置RADIUS方案		1.3.2
	配置HWTACACS方案		1.3.3
在ISP域中配置实现AAA的方法	创建ISP域	必选	1.4.2
	配置ISP域的属性	可选	1.4.3
	配置ISP域的AAA认证方法	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
配置强制切断用户		可选	1.5
配置NAS-ID与VLAN的绑定		可选	1.6
配置双机热备模式下的设备ID		可选	1.7
配置设备作为RADIUS服务器		可选	1.8

 说明

对于 Login 用户，只有配置登录用户界面的认证方式为 **scheme**，这类用户登录设备才会采用 AAA 处理。有关登录用户界面认证方式的命令介绍请参见“基础配置命令参考”中的“登录交换机”。

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。该集合以用户名为用户的唯一标识。为使某个请求网络服务的用户可以通过本地认证，需要在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。

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

- 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。

- 生效时间及有效期

用户帐户开始生效的时间以及有效期截止的时间。接入设备仅允许帐户处于有效期内的用户通过认证。有用户临时需要接入网络时，可以通过建立有一定有效期的来宾帐户控制用户的临时访问。

- 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 3. 配置用户组属性](#)”。

- 密码管理属性

用户密码的安全属性，可用于对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。

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低依次为本地用户、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”。

- 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

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。

用户认证通过后，接入设备下发给用户的权限。可支持的授权属性包括：**ACL**、闲置切换功能、用户级别、用户角色、**User Profile**、**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。

1. 本地用户配置任务简介

表1-7 本地用户配置任务简介

配置任务	说明	详细配置
配置本地用户属性	必选	1.3.1 2.
配置用户组属性	可选	1.3.1 3.
本地用户及本地用户组显示与维护	可选	1.3.1 4.

2. 配置本地用户属性

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	必选 缺省情况下，系统中没有任何本地用户
设置本地用户的密码	非FIPS模式下： password [[hash] { cipher simple } password] FIPS模式下： password	可选 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 仅支持Password Control特性的设备上才支持不指定任何参数的交互式密码配置方式
设置本地用户可以使用的服务类型	非FIPS模式下： service-type { ftp lan-access { ssh telnet terminal } * portal web } FIPS模式下： service-type { lan-access { ssh terminal } * portal web }	必选 缺省情况下，系统不对本地用户授权任何服务
设置本地用户的状态	state { active block }	可选 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
设置本地用户名可容纳的最大接入用户数	access-limit max-user-number	可选 缺省情况下，不限制当前本地用户名可容纳的接入用户数 FTP用户不受此属性限制

操作		命令	说明
设置本地用户的密码管理属性	老化时间	password-control aging <i>aging-time</i>	可选 缺省情况下，采用本地用户所属用户组的密码老化时间，若用户组未配置该值，则采用全局配置
	密码最小长度	password-control length <i>length</i>	可选 缺省情况下，采用本地用户所属用户组的密码最小长度，若用户组未配置该值，则采用全局配置
	密码组合策略	password-control composition type-number <i>type-number</i> [type-length <i>type-length</i>]	可选 缺省情况下，采用本地用户所属用户组的密码组合策略，若用户组未配置该值，则采用全局配置
设置本地用户的绑定属性		bind-attribute { ip <i>ip-address</i> location port <i>slot-number subslot-number port-number</i> mac <i>mac-address</i> vlan <i>vlan-id</i> } *	可选 缺省情况下，未设置本地用户的任何绑定属性
设置本地用户的授权属性		authorization-attribute { acl <i>acl-number</i> idle-cut <i>minute</i> level <i>level</i> user-profile <i>profile-name</i> user-role { guest guest-manager security-audit } vlan <i>vlan-id</i> work-directory <i>directory-name</i> } *	可选 缺省情况下，未设置本地用户的任何授权属性 对于 lan-access 用户，仅授权属性 acl 、 idle-cut 、 user-profile 和 vlan 有效； 对于 portal 用户，仅授权属性 acl 、 user-profile 和 vlan 有效； 对于 ssh 、 terminal 、 web 用户，仅授权属性 level 有效； 对于 ftp 用户，仅授权属性 level 和 work-directory 有效； 对于 telnet 用户，仅授权属性 level 和 user-role 有效； 对于其它类型的本地用户，所有授权属性均无效
设置本地用户的生效时间		validity-date <i>time</i>	可选 缺省情况下，未设置本地用户的生效时间
设置本地用户的有效期		expiration-date <i>time</i>	可选 缺省情况下，未设置本地用户的有效期
设置本地用户所属的用户组		group <i>group-name</i>	可选 缺省情况下，本地用户属于系统默认用户组 system



说明

- 密码控制属性相关命令的具体介绍请参见“安全命令参考”中的“Password Control”。
- 本地用户的 **access-limit** 命令只在该用户采用了本地计费方法的情况下生效。
- 如果登录设备的认证方式（通过命令 **authentication-mode** 设置）为 AAA（**scheme**），则用户登录系统后所能访问的命令级别由用户被授权的级别确定；如果配置登录设备的认证方式为不认证（**none**）或采用密码认证（**password**），则用户登录系统后所能访问的命令级别由用户界面所能访问的命令级别确定。对于 SSH 用户，使用公钥认证时，其所能使用的命令以用户界面上设置的级别为准。关于登录设备的认证方式与用户界面所能访问的命令级别的详细介绍请参见“基础配置指导”中的“登录交换机”。
- 除本地用户视图下可以配置授权 User Profile 之外，用户组视图及 ISP 域视图下也可以配置授权 User Profile，各视图下的配置优先级顺序从高到低依次为：本地用户视图-->用户组视图-->ISP 视图。关于 User Profile 的详细介绍请参见“安全配置指导”中的“User Profile”。
- 系统中只剩一个角色为安全日志管理员的本地用户时，该本地用户就不能被删除，而且也不能修改或删除该本地用户的安全日志管理员角色，除非再指定一个新的用户为安全日志管理员。

3. 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内容包括本地用户的密码管理属性和授权属性。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使用本地用户视图下的 **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	必选
设置用户组的密码控制属性	老化时间	password-control aging aging-time	可选 缺省情况下，采用全局老化时间
	密码最小长度	password-control length length	可选 缺省情况下，采用全局密码长度
	密码组合策略	password-control composition type-number type-number [type-length type-length]	可选 缺省情况下，采用全局密码组合策略
设置用户组的授权属性		authorization-attribute { acl acl-number idle-cut minute level level user-profile profile-name vlan vlan-id work-directory directory-name } *	可选 缺省情况下，未设置用户组的授权属性

操作	命令	说明
设置用户组的来宾可选属性	group-attribute allow-guest	可选 缺省情况下，用户组不具有来宾可选属性，来宾用户管理员在Web界面上创建的来宾用户不能加入该用户组



说明
密码控制属性相关命令的具体介绍请参见“安全命令参考”中的“Password Control”。

4. 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
显示本地用户相关信息	display local-user [<i>idle-cut</i> { disable enable }] [<i>service-type</i> { ftp lan-access portal ssh telnet terminal web }] [<i>state</i> { active block }] [<i>user-name</i> <i>user-name</i> <i>vlan</i> <i>vlan-id</i>] [<i>slot</i> <i>slot-number</i>] [[{ begin exclude include } <i>regular-expression</i>]]
显示本地用户组的相关信息	display user-group [<i>group-name</i>] [[{ begin exclude include } <i>regular-expression</i>]]

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须的一些参数。当创建一个新的 RADIUS 方案之后，需要对属于此方案的 RADIUS 服务器的 IP 地址、UDP 端口号和报文共享密钥进行设置，这些服务器包括认证/授权和计费服务器，而每种服务器又有主服务器和从服务器的区别。每个 RADIUS 方案的属性包括：主服务器的 IP 地址、从服务器的 IP 地址、共享密钥以及 RADIUS 服务器类型等。

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
创建RADIUS方案	必选	1.3.2 2.
配置RADIUS认证/授权服务器	必选	1.3.2 3.
配置RADIUS计费服务器及相关参数	可选	1.3.2 4.
配置RADIUS报文的共享密钥	可选	1.3.2 5.
配置RADIUS方案所属的VPN	可选	1.3.2 6.
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 7.

配置任务	说明	详细配置
配置支持的RADIUS服务器的类型	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.
配置发送RADIUS报文使用的备份源地址	可选	1.3.2 12.
配置RADIUS服务器的定时器	可选	1.3.2 13.
配置RADIUS的accounting-on功能	可选	1.3.2 14.
配置RADIUS服务器的安全策略服务器	可选	1.3.2 15.
配置RADIUS Attribute 25的CAR参数解析功能	可选	1.3.2 16.
配置RADIUS的Trap功能	可选	1.3.2 17.
使能RADIUS客户端的监听端口	可选	1.3.2 18.
配置RADIUS报文的DSCP优先级	可选	1.3.2 19.
RADIUS显示和维护	可选	1.3.2 20.

2. 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。

表1-12 创建 RADIUS 方案

操作	命令	说明
进入系统视图	system-view	-
创建RADIUS方案并进入其视图	radius scheme <i>radius-scheme-name</i>	必选 缺省情况下，未定义RADIUS方案



说明

一个 RADIUS 方案可以同时被多个 ISP 域引用。

3. 配置RADIUS认证/授权服务器

通过在 RADIUS 方案中配置 RADIUS 认证/授权服务器，指定设备对用户进行 RADIUS 认证/授权时与哪些服务器进行通信。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，故不能也不需要单独配置 RADIUS 授权服务器。若在 RADIUS 方案中同时配置了主认证/授权服务器和从认证/授权服务器，则当设备判断主认证/授权服务器不可达时，将使用从认证/授权服务器进行认证、授权。建议在不需要备份的情况下，只配置主 RADIUS 认证/授权服务器即可。

配置认证/授权服务器时可以同时配置服务器状态探测功能，即周期性发送探测报文探测该认证/授权服务器是否可达：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**。服务器状态探测功能具有实时性，可及时将服务器状态通知给相关认证模块，例如，可与 802.1X Critical VLAN 的端口恢复功能相配合，一旦发现服务器可达，则立即触发用户进行认证。

表1-13 配置 RADIUS 认证/授权服务器

操作	命令	说明
进入系统视图	system-view	-
进入RADIUS方案视图	radius scheme <i>radius-scheme-name</i>	-
配置主RADIUS认证/授权服务器	primary authentication { <i>ip-address</i> ipv6 <i>ipv6-address</i> } [<i>port-number</i> key [cipher simple] <i>key</i> probe username name [interval <i>interval</i>] vpn-instance <i>vpn-instance-name</i>] *	二者至少选其一 缺省情况下，未配置主认证/授权服务器和从认证/授权服务器
配置从RADIUS认证/授权服务器	secondary authentication { <i>ip-address</i> ipv6 <i>ipv6-address</i> } [<i>port-number</i> key [cipher simple] <i>key</i> probe username name [interval <i>interval</i>] vpn-instance <i>vpn-instance-name</i>] *	



说明

- 在实际组网环境中，可以指定一台 RADIUS 服务器作为主认证/授权服务器，并指定多台（最多 16 台）RADIUS 服务器作为从认证/授权服务器；也可以指定一台服务器既作为某个方案的主认证/授权服务器，又作为另一个方案的从认证/授权服务器。
- 在同一个方案中指定的主认证/授权服务器和从认证/授权服务器的 IP 地址不能相同，并且各从服务器的 IP 地址也不能相同，否则将提示配置不成功。
- 主服务器和从服务器的 IP 地址版本必须保持一致，并且各从服务器的 IP 地址版本也必须保持一致；认证/授权服务器和计费服务器的 IP 地址版本也必须保持一致。

4. 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。若在 RADIUS 方案中同时配置了主计费服务器和从计费服务器，则当设备判断主计费服务器不可达时，将使用从计费服务器进行计费。建议在不需要备份的情况下，只配置主 RADIUS 计费服务器即可。

用户上线之后，设备应该尽量与 RADIUS 服务器同步切断用户连接，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。

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，通过在设备上使能停止计费报文缓存功能，将其缓存在本机上，然后发送直到 RADIUS 计费服务器产生响应，或者在发起停止计费请求的尝试次数达到指定的最大值后将其丢弃。

表1-14 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 { <i>ip-address</i> ipv6 <i>ipv6-address</i> } [<i>port-number</i> key [<i>cipher</i> simple] <i>key</i> vpn-instance <i>vpn-instance-name</i>] *	二者至少选其一
配置从RADIUS计费服务器	secondary accounting { <i>ip-address</i> ipv6 <i>ipv6-address</i> } [<i>port-number</i> key [<i>cipher</i> simple] <i>key</i> vpn-instance <i>vpn-instance-name</i>] *	缺省情况下，未配置主/从计费服务器
设置允许发起实时计费请求的最大尝试次数	retry realtime-accounting <i>retry-times</i>	可选 缺省情况下，允许发起实时计费请求的最大尝试次数为5
使能停止计费报文缓存功能	stop-accounting-buffer enable	可选 缺省情况下，允许设备缓存没有得到响应的停止计费请求报文
设置允许发起停止计费请求的最大尝试次数	retry stop-accounting <i>retry-times</i>	可选 缺省情况下，允许发起停止计费请求的最大尝试次数为500

说明

- 在实际组网环境中，可以指定一台 RADIUS 服务器作为主计费服务器，并指定多台（最多 16 台）RADIUS 服务器作为从计费服务器；也可以指定一台服务器既作为某个方案的主计费服务器，又作为另一个方案的从计费服务器。
- 如果在线用户正在使用的计费服务器被删除，则设备将无法发送用户的实时计费请求和停止计费请求，且停止计费报文不会被缓存到本地。
- 主计费服务器和从计费服务器的 IP 地址不能相同，并且各从计费服务器的 IP 地址也不能相同，否则将提示配置不成功。
- 目前 RADIUS 不支持对 FTP 用户进行计费。
- 主服务器和从服务器的 IP 地址版本必须保持一致，并且各从服务器的 IP 地址版本也必须保持一致；计费服务器和认证/授权服务器的 IP 地址版本也必须保持一致。

5. 配置RADIUS报文的共享密钥

RADIUS 客户端与 RADIUS 服务器使用 MD5 算法来加密 RADIUS 报文，并在共享密钥的参与下生成验证字来验证对方报文的合法性。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。

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

表1-15 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 <i>radius-scheme-name</i>	-
配置RADIUS认证/授权或计费报文的共享密钥	key { accounting authentication } [cipher simple] key	必选 缺省情况下，无密钥



说明

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。

6. 配置RADIUS方案所属的VPN

该配置用于为 RADIUS 方案下的所有认证/授权/计费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 认证/授权/计费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1-16 配置 RADIUS 方案所属的 VPN

表1-17 操作	命令	说明
进入系统视图	system-view	-
进入RADIUS方案视图	radius scheme <i>radius-scheme-name</i>	-
配置RADIUS方案所属的VPN	vpn-instance <i>vpn-instance-name</i>	必选

7. 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 域的。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 域名去除后再发送给该类 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。

设备通过周期性地发送计费更新报文，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 RADIUS 服务器上的流量统计单位保持一致。

表1-18 配置发送给 RADIUS 服务器的数据相关属性

操作	命令	说明
进入系统视图	system-view	-
进入RADIUS方案视图	radius scheme <i>radius-scheme-name</i>	-

操作	命令	说明
设置发送给RADIUS服务器的用户名格式	user-name-format { keep-original with-domain without-domain }	可选 缺省情况下，设备发送给RADIUS服务器的用户名携带有ISP域名
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



说明

- 如果指定某个 RADIUS 方案不允许用户名中携带有 ISP 域名，那么请不要在两个乃至两个以上的 ISP 域中同时设置使用该 RADIUS 方案，否则，会出现虽然实际用户不同（在不同的 ISP 域中）、但 RADIUS 服务器认为用户相同（因为传送到它的用户名相同）的错误。
- 对于级别切换认证，命令 **user-name-format keep-original** 与 **user-name-format without-domain** 的执行效果一样，即发送给 RADIUS 服务器的用户名都不携带 ISP 域名。

8. 配置支持的RADIUS服务器的类型

通过指定设备支持 RADIUS 服务器类型，决定设备与 RADIUS 服务器之间可交互的 RADIUS 协议类型：

- 若指定 **extended** 类型的 RADIUS 服务器，则设备与 RADIUS 服务器将按照私有 RADIUS 协议的规程和报文格式进行交互。
- 若指定 **standard** 类型的 RADIUS 服务器，则设备与 RADIUS 服务器将按照标准 RADIUS 协议（RFC 2865/2866 或更新）的规程和报文格式进行交互。

使用 CAMS/iMC 服务器时，RADIUS 服务器类型应选择 **extended** 类型。使用其它第三方 RADIUS 服务器时，RADIUS 服务器类型可以选择 **standard** 类型或 **extended** 类型。

需要注意的是，若使用设备作为 RADIUS 服务器对 login 用户进行认证，则此处的 RADIUS 服务器类型必须指定为 **standard**。

表1-19 配置支持的 RADIUS 服务器的类型

操作	命令	说明
进入系统视图	system-view	-
进入RADIUS方案视图	radius scheme <i>radius-scheme-name</i>	-
设置设备支持的RADIUS服务器类型	server-type { extended standard }	可选 缺省情况下，设备支持的RADIUS服务器类型为 standard



说明

当设备支持的 RADIUS 服务器类型被更改时，设备会将发送到 RADIUS 服务器的数据流的单位（**data-flow-format**）恢复为缺省配置。

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RADIUS服务器在应答超时定时器规定的时长内（由**timer response-timeout**命令配置）没有响应设备，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超过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 <i>radius-scheme-name</i>	-
设置发送RADIUS报文的最大尝试次数	retry <i>retry-times</i>	可选 缺省情况下，发送RADIUS报文的最大尝试次数为3次



说明

- 发送 RADIUS 报文的最大尝试次数与 RADIUS 服务器应答超时时间的乘积不能超过 75 秒。
- RADIUS服务器应答超时时间的配置请参考命令“[13. 配置RADIUS服务器的定时器](#)”。

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 **timer 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 **timer quiet** 定时器，并继续查找状态为 **active** 的从服务器。当服务器的 **timer quiet** 定时器超时，或者设备收到该服务器的认证/计费应答报文时，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，主服务器状态由 **block** 恢复为 **active**，则设备并不会立

即恢复与主服务器的通信，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。

- 一个用户的计费流程开始之后，设备就不会再与其它的计费服务器通信，即该用户的实时计费报文和停止计费报文只会发往当前使用的计费服务器。如果当前使用的计费服务器被删除，则实时计费和停止计费报文都将无法发送。
- 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** 的服务器进行通信。
- 当主/从服务器的状态均为 **block** 时，设备仅与主服务器通信，若主服务器可达，则主服务器状态变为 **active**，否则保持不变。
- 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。
- 设备收到服务器的认证或计费应答报文后会将与报文源 IP 地址相同且状态为 **block** 的认证或计费服务器的状态更改为 **active**。

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** 而可能进行的无意义尝试，可暂时将该服务器状态手工置为 **block** 来满足此需求。

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/授权服务器的状态	state primary authentication { active block }	可选 缺省情况下，RADIUS方案中配置了IP地址的各RADIUS服务器的状态均为 active
设置主RADIUS计费服务器的状态	state primary accounting { active block }	
设置从RADIUS认证/授权服务器的状态	state secondary authentication [ip ipv4-address ipv6 ipv6-address] { active block }	
设置从RADIUS计费服务器的状态	state secondary accounting [ip ipv4-address ipv6 ipv6-address] { active block }	



说明

- **state** 命令设置的服务器状态属于动态信息，不能被保存在配置文件中，设备重启后，配置了 IP 地址的服务器状态恢复为缺省状态 **active**。
- 可通过执行 **display radius scheme** 命令查看各服务器的当前状态。
- 可通过 **timer quiet** 命令来设置服务器恢复激活状态的时间，当该参数取值为 0 时，若当前用户使用的认证或计费服务器不可达，则设备并不会切换它的状态，而是保持其为 **active**，并且将使用该服务器的用户认证或计费的报文发送给下一个状态为 **active** 的服务器，而后续其它用户的认证请求报文仍然可以发送给该服务器进行处理。

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，则才会进行后续的认证或计费处理，否则直接对其做丢弃处理。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，例如接入设备与 RADIUS 服务器之间存在 NAT (Network Address Translation, 网络地址转换) 设备时，需要将该地址指定为转换后的公网 IP 地址；在接入设备使用 VRRP (Virtual Router Redundancy Protocol, 虚拟路由冗余协议) 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，首先判断当前所使用的 RADIUS 方案中是否通过 **nas-ip** 命令配置了发送 RADIUS 报文使用源地址，若配置存在，则使用该地址作为发送 RADIUS 报文使用的源地址，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 **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。若系统视图下配置了相应的源地址，则使用该地址作为发送 RADIUS 报文使用的源地址，否则，使用通过路由查找到的报文出接口地址作为发送 RADIUS 报文使用的源地址。

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 { <i>ip-address</i> ipv6 <i>ipv6-address</i> } [vpn-instance <i>vpn-instance-name</i>]	必选 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 <i>radius-scheme-name</i>	-
设置设备发送RADIUS报文使用的源地址	nas-ip { <i>ip-address</i> ipv6 <i>ipv6-address</i> }	必选 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

12. 配置发送RADIUS报文使用的备份源地址

在双机热备的组网环境中，主设备通过与 RADIUS 服务器交互对 Portal 用户进行认证，并负责将生成的 Portal 在线用户数据通过备份链路同步给备用设备，而备用设备只接收和处理主设备发送的同步消息。

当主设备发生故障时，由于服务器不知道备用设备的源地址，因此不会主动向备用设备发送 RADIUS 报文。为解决这个问题，需要将备用设备发送 RADIUS 报文使用的源地址发给服务器，使得服务器也主动向备用设备发送 RADIUS 报文，备用设备发送 RADIUS 报文的源地址就是通过在主用设备上配置发送 RADIUS 报文使用的备份源地址告知服务器的。

设备选择发送 RADIUS 报文使用的备份源地址时，首先判断当前所使用的 RADIUS 方案中是否通过 **nas-backup-ip** 命令配置了发送 RADIUS 报文使用备份源地址，若配置存在，则将该地址作为对端设备发送 RADIUS 报文使用的源地址发给服务器，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-backup-ip** 命令配置的私网备份源地址，对于公网服务器则直接查找该命令配置的公网备份源地址。若系统视图下配置了相应的备份源地址，则使用该地址作为备份源地址，否则，不向服务器发送备份源地址。

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1-24 为所有 RADIUS 方案配置发送 RADIUS 报文使用的备份源地址

操作	命令	说明
进入系统视图	system-view	-
设置设备发送RADIUS报文使用的备份源地址	radius nas-backup-ip <i>ip-address</i> [vpn-instance <i>vpn-instance-name</i>]	必选 缺省情况下，未指定备份源地址

表1-25 为 RADIUS 方案配置发送 RADIUS 报文使用的备份源地址

操作	命令	说明
进入系统视图	system-view	-
进入RADIUS方案视图	radius scheme <i>radius-scheme-name</i>	-

操作	命令	说明
设置设备发送RADIUS报文使用的备份源地址	nas-backup-ip <i>ip-address</i>	必选 缺省情况下，未指定备份源地址



说明

设备发送 RADIUS 报文使用的备份源地址仅在双机热备环境下生效，而且，此地址必须指定为对端发送 RADIUS 报文使用的源地址。

13. 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（认证/授权请求或计费请求）传送出去一段时间后，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，以保证用户确实能够得到 RADIUS 服务，这段时间被称为 RADIUS 服务器响应超时时长。
- 服务器恢复激活状态定时器（**quiet**）：当服务器不可达时，状态变为 **block**，设备会与其它状态为 **active** 的服务器交互，并开启超时定时器，在设定的一定时间间隔之后，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。

表1-26 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 <i>radius-scheme-name</i>	-
设置RADIUS服务器响应超时时间	timer response-timeout <i>seconds</i>	可选 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 <i>minutes</i>	可选 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 <i>minutes</i>	可选 缺省情况下，实时计费间隔为12分钟



说明

- 发送 RADIUS 报文的最大尝试次数与 RADIUS 服务器响应超时时间的乘积必须小于各接入类型的客户端连接超时时间，且不能超过 75 秒。比如对于语音类型的接入用户，因为其客户端连接

超时时间为 10 秒，所以 RADIUS 服务器的响应超时时间与发送 RADIUS 请求报文的最大尝试次数的乘积必须小于 10 秒；对于 Telnet 接入类型的用户，其客户端连接超时时间为 30 秒，所以此乘积必须小于 30 秒。否则会造成计费停止报文不能被缓存，以及主备服务器不能切换的问题。具体接入客户端连接超时时间请参考相关接入手册。

- 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的过短，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。
- RADIUS 各类报文重传次数的最大值配置请参考命令 **retry**。

14. 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，则会按照一定的时间间隔（**interval seconds**）尝试重发几次（**send send-times**）。

表1-27 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 <i>radius-scheme-name</i>	-
配置accounting-on功能	accounting-on enable [interval seconds send send-times] *	必选 缺省情况下，accounting-on功能处于关闭状态，accounting-on报文重发时间间隔为3秒，accounting-on报文重发次数为50次



说明

accounting-on 功能需要和 H3C CAMS 或 H3C iMC 网管系统配合使用。

15. 配置RADIUS安全策略服务器的IP地址

H3C EAD 方案的核心是整合与联动，其中的安全策略服务器是 EAD 方案中的管理与控制中心，它作为一个软件的集合，兼具用户管理、安全策略管理、安全状态评估、安全联动控制以及安全事件审计等功能。

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 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。

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将 RADIUS 安全策略服务器的 IP 地址分别指定为 iMC 安全策略服务器的 IP 地址和 iMC 配置平台的 IP 地址。

表1-28 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 <i>radius-scheme-name</i>	-
设置RADIUS安全策略服务器的IP地址	security-policy-server ip-address	必选 缺省情况下，未指定RADIUS安全策略服务器

16. 配置对RADIUS Attribute 25 进行CAR参数解析

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1-29 配置对 RADIUS Attribute 25 进行 CAR 参数解析

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



说明

本功能是否需要配置与两个前提条件有关：一是设备是否支持 CAR 参数的下发，另外一个 RADIUS 服务器是否支持利用 class 属性进行 CAR 参数的下发，具体情况请以设备和服务器的实际情况为准。

17. 配置RADIUS的Trap功能

通过配置 RADIUS 的 Trap 功能，控制 NAS 触发输出相应的 Trap 信息，具体包括以下两种：

- RADIUS 服务器可达状态改变时输出 Trap 信息。具体包括两种情况：当 NAS 向 RADIUS 服务器发送计费或认证请求无响应的次数达到指定的发送 RADIUS 报文的最大尝试次数时，NAS 认为服务器不可达，会置服务器状态为 **block** 并输出 Trap 信息；当 NAS 收到状态不可达的服务器发送的报文时，则认为服务器状态可达，会置服务器状态为 **active** 并输出 Trap 信息。
- 认证失败次数与认证请求次数的百分比超过一定阈值时输出 Trap 信息。该阈值目前只能够通过 MIB 方式进行配置，取值范围为 1%~100%，缺省为 30%。由于正常情况下，认证失败的比率较小，如果 NAS 触发输出了该类 Trap 信息，则管理员可能需要确认配置是否正确或设备与服务器的通信是否正常，并通过排查配置或网络问题来保证用户认证过程的正常运行。

表1-30 配置 RADIUS 的 Trap 功能

操作	命令	说明
进入系统视图	system-view	-
使能RADIUS的Trap功能	radius trap { accounting-server-down authentication-error-threshold authentication-server-down }	必选 缺省情况下，RADIUS的Trap功能处于关闭状态

18. 使能RADIUS客户端的监听端口

通过以下配置可以打开 RADIUS 客户端的 RADIUS 报文监听端口，使能后的端口才可以接收和发送 RADIUS 报文。在不需要使用 RADIUS 认证功能时，为避免收到恶意的 RADIUS 攻击报文，建议关闭设备上 RADIUS 客户端的监听端口。

表1-31 使能 RADIUS 客户端的监听端口

操作	命令	说明
进入系统视图	system-view	-
使能RADIUS客户端的监听端口	radius client enable	可选 缺省情况下，监听端口处于使能状态

19. 配置RADIUS报文的DSCP优先级

在 IPv4 和 IPv6 报文头中，包含一个 8bit 的字段，用于标识 IP 报文的服务类型。在 IPv4 报文中，这个字段称为 ToS 字段；在 IPv6 报文中，称为 Traffic class 字段。RFC 2474 对这 8 个 bit 进行了

定义，将前 6 个 bit 定义为 DSCP 优先级，最后 2 个 bit 作为保留位。在报文传输的过程中，DSCP 优先级可以被网络设备识别，并作为报文传输优先程度的参考。

表1-32 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IPv4 RADIUS报文的DSCP优先级	radius dscp dscp-value	可选 缺省情况下，IPv4 RADIUS报文的DSCP优先级为0
配置IPv6 RADIUS报文的DSCP优先级	radius ipv6 dscp dscp-value	可选 缺省情况下，IPv6 RADIUS报文的DSCP优先级为0

20. 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1-33 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 [<i>radius-scheme-name</i>] [<i>slot slot-number</i>] [{ begin exclude include } <i>regular-expression</i>]
显示RADIUS报文的统计信息	display radius statistics [<i>slot slot-number</i>] [{ begin exclude include } <i>regular-expression</i>]
显示缓存的没有得到响应的停止计费请求报文	display stop-accounting-buffer { radius-scheme <i>radius-scheme-name</i> session-id <i>session-id</i> time-range <i>start-time stop-time</i> user-name <i>user-name</i> } [<i>slot slot-number</i>] [{ begin exclude include } <i>regular-expression</i>]
清除RADIUS协议的统计信息	reset radius statistics [<i>slot slot-number</i>]
清除缓存中的没有得到响应的停止计费请求报文	reset stop-accounting-buffer { radius-scheme <i>radius-scheme-name</i> session-id <i>session-id</i> time-range <i>start-time stop-time</i> user-name <i>user-name</i> } [<i>slot slot-number</i>]

1.3.3 配置HWTACACS方案

 说明

有用户在线时，不能删除 HWTACACS 方案，并且不能修改 HWTACACS 服务器 IP 地址。

1. HWTACACS配置任务简介

表1-34 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	必选	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服务器的数据相关属性	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

HWTACACS 的配置是以 HWTACACS 方案为单位进行的。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。

表1-35 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	hwtaacs scheme <i>hwtaacs-scheme-name</i>	必选 缺省情况下，未定义 HWTACACS方案



说明

系统最多支持配置 16 个 HWTACACS 方案。只有未被引用的方案才可以被删除。

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。若在 HWTACACS 方案中同时配置了主认证服务器和从认证服务器，则当设备判断主认证服务器不可达时，将使用从认证服务器进行认证。**Release 5206** 及以上版本支持一个 HWTACACS 方案中配置一个主认证服务器和最多 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。

表1-36 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 <i>hwtacacs-scheme-name</i>	-
配置主HWTACACS认证服务器	primary authentication <i>ip-address</i> [<i>port-number</i> key [cipher simple] key vpn-instance <i>vpn-instance-name</i>] *	二者至少选其一 缺省情况下, 未配置主/从认证服务器
配置从HWTACACS认证服务器	secondary authentication <i>ip-address</i> [<i>port-number</i> key [cipher simple] key vpn-instance <i>vpn-instance-name</i>] *	仅Release 5206及以上版本支持参数 key [cipher simple] key



说明

- 在实际组网环境中, 可以指定一台 HWTACACS 服务器既作为某个方案的主认证服务器, 又作为另一个方案的从认证服务器。
- 主认证服务器和从认证服务器的 IP 地址不能相同, 否则将提示配置不成功。
- 只有当没有活跃的用于发送认证报文的 TCP 连接使用该认证服务器时, 才允许删除该服务器。

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。若在 HWTACACS 方案中同时配置了主授权服务器和从授权服务器, 则当设备判断主授权服务器不可达时, 将使用从授权服务器进行授权。Release 5206 及以上版本支持一个 HWTACACS 方案中配置一个主授权服务器和最多 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。

表1-37 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 <i>hwtacacs-scheme-name</i>	-
设置主HWTACACS授权服务器	primary authorization <i>ip-address</i> [<i>port-number</i> key [cipher simple] key vpn-instance <i>vpn-instance-name</i>] *	二者至少选其一 缺省情况下, 未配置主/从授权服务器
设置从HWTACACS授权服务器	secondary authorization <i>ip-address</i> [<i>port-number</i> key [cipher simple] key vpn-instance <i>vpn-instance-name</i>] *	仅Release 5206及以上版本支持参数 key [cipher simple] key



说明

- 在实际组网环境中，可以指定一台 HWTACACS 服务器既作为某个方案的主授权服务器，又作为另一个方案的从授权服务器。
- 主授权服务器和从授权服务器的 IP 地址不能相同，否则将提示配置不成功。
- 只有当没有活跃的用于发送授权报文的 TCP 连接使用该授权服务器时，才允许删除该服务器。

5. 配置HWTACACS计费服务器及相关参数

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。若在 HWTACACS 方案中同时配置了主计费服务器和从计费服务器，则当设备判断主计费服务器不可达时，将使用从计费服务器进行授权。Release 5206 及以上版本支持一个 HWTACACS 方案中配置一个主计费服务器和最多 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。

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 HWTACACS 计费服务器发送停止计费请求报文，通过在设备上使能停止计费报文缓存功能，将其缓存在本机上，然后发送直到 HWTACACS 计费服务器产生响应，或者在发送停止计费请求报文的尝试次数达到指定的最大值后将其丢弃。

表1-38 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 <i>hwtacacs-scheme-name</i>	-
设置HWTACACS主计费服务器	primary accounting <i>ip-address</i> [<i>port-number</i> key [cipher simple] key vpn-instance <i>vpn-instance-name</i>] *	二者至少选其一 缺省情况下，未配置主/从计费服务器
设置HWTACACS从计费服务器	secondary accounting <i>ip-address</i> [<i>port-number</i> key [cipher simple] key vpn-instance <i>vpn-instance-name</i>] *	仅Release 5206及以上版本支持 参数 key [cipher simple] key
使能停止计费报文缓存功能	stop-accounting-buffer enable	可选 缺省情况下，使能停止计费报文缓存功能
设置允许发送停止计费请求报文的最大尝试次数	retry stop-accounting <i>retry-times</i>	可选 缺省情况下，允许发送停止计费请求报文的最大尝试次数为100



说明

- 在实际组网环境中，可以指定一台 HWTACACS 服务器既作为某个方案的主计费服务器，又作为另一个方案的从计费服务器。
- 主计费服务器和从计费服务器的 IP 地址不能相同，否则将提示配置不成功。
- 只有当没有活跃的用于发送计费报文的 TCP 连接使用该计费服务器时，才允许删除该服务器。
- 目前 HWTACACS 不支持对 FTP 用户进行计费。

6. 配置HWTACACS报文的共享密钥

HWTACACS 客户端与 HWTACACS 服务器使用 MD5 算法来加密 HWTACACS 报文，并在共享密钥的参与下生成验证字来验证对方报文的合法性。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1-39 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 <i>hwtacacs-scheme-name</i>	-
配置HWTACACS认证、授权、计费报文的共享密钥	key { accounting authentication authorization } [cipher simple] key	必选 缺省情况下，无密钥



说明

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 方案下的所有认证/授权/计费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 认证/授权/计费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1-40 配置 HWTACACS 方案所属的 VPN

操作	命令	说明
进入系统视图	system-view	-
进入HWTACACS方案视图	hwtacacs scheme <i>hwtacacs-scheme-name</i>	-
配置HWTACACS方案所属的VPN	vpn-instance <i>vpn-instance-name</i>	必选

8. 配置发送给HWTACACS服务器的数据相关属性

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。

设备通过周期性地发送计费更新报文，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。

表1-41 配置发送给 HWTACACS 服务器的数据相关属性

操作	命令	说明
进入系统视图	system-view	-
进入HWTACACS方案视图	hwtacacs scheme <i>hwtacacs-scheme-name</i>	-
设置发送给HWTACACS服务器的用户名格式	user-name-format { keep-original with-domain without-domain }	可选 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



说明

- 如果 HWTACACS 服务器不接受带域名的用户名，可以配置将用户名的域名去除后再传送给 HWTACACS 服务器。
- 对于级别切换认证，命令 **user-name-format keep-original** 与 **user-name-format without-domain** 的效果一样，发送给 HWTACACS 服务器的用户名都不携带 ISP 域名。

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，则才会进行后续的认证或计费处理，否则直接对其做丢弃处理。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 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，例如接入设备与 HWTACACS 服务器之间存在 NAT 设备时，需要将该地址指定为转换后

的公网 IP 地址；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，首先判断当前所使用的 HWTACACS 方案中是否通过 **nas-ip** 命令配置了发送 HWTACACS 报文使用源地址，若配置存在，则使用该地址作为发送 HWTACACS 报文使用的源地址，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。若系统视图下配置了相应的源地址，则使用该地址作为发送 HWTACACS 报文使用的源地址，否则，使用通过路由查找到的报文出接口地址作为发送 HWTACACS 报文使用的源地址。

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1-42 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 ip-address [vpn-instance vpn-instance-name]	必选 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1-43 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 <i>hwtacacs-scheme-name</i>	-
设置设备发送HWTACACS报文使用的源地址	nas-ip ip-address	必选 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

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（认证/授权请求或计费请求）传送出去一段时间后，设备还没有得到 HWTACACS 服务器的响应，则有必要重传 HWTACACS 请求报文，以保证用户确实能够得到 HWTACACS 服务，这段时间被称为 HWTACACS 服务器响应超时时长。
- 主服务器恢复激活状态定时器（**quiet**）：当主服务器不可达时，状态变为 **block**，设备会与状态为 **active** 的从服务器交互，并开启超时定时器，在设定的一定时间间隔之后，将主服务器的状态恢复为 **active**。这段时间被称为主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。如果服务器对实时计费报文没有正常响应，设备也不会强制切断在线用户。

表1-44 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	hwtaacs scheme <i>hwtaacs-scheme-name</i>	-
设置HWTACACS服务器响应超时时间	timer response-timeout seconds	可选 缺省情况下，服务器响应超时时间为5秒
设置主服务器恢复激活状态的时间	timer quiet minutes	可选 缺省情况下，主服务器恢复激活状态前需要等待5分钟
设置实时计费的时间间隔	timer realtime-accounting minutes	可选 缺省情况下，实时计费间隔为12分钟



说明

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。

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1-45 HWTACACS 协议显示和维护

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 hwtaacs [<i>hwtaacs-server-name</i> [statistics]] [slot slot-number] [{ begin exclude include } <i>regular-expression</i>]
显示缓存的没有得到响应的停止计费请求报文	display stop-accounting-buffer hwtaacs-scheme <i>hwtaacs-scheme-name</i> [slot slot-number] [{ begin exclude include } <i>regular-expression</i>]
清除HWTACACS协议的统计信息	reset hwtaacs statistics { accounting all authentication authorization } [slot slot-number]
清除缓存中的没有得到响应的停止计费请求报文	reset stop-accounting-buffer hwtaacs-scheme <i>hwtaacs-scheme-name</i> [slot slot-number]

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。每个 ISP 域中都有缺省的认证、授权、计费方法，分别为本地认证、本地授权、本地计费，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。

1.4.1 配置准备

- 若采用本地认证方案，则请保证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。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](#)”。

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。

表1-46 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 <i>isp-name</i>	必选
返回系统视图	quit	-
手工配置缺省的ISP域	domain default enable <i>isp-name</i>	可选 缺省情况下，系统缺省的ISP域为 system



说明

配置为缺省的 ISP 域不能够被删除，除非首先使用命令 **undo domain default enable** 将其修改为非缺省 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：

- 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。

- 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。
- 闲置切断：用户上线后，若域内某用户连续闲置的时长超过指定的闲置检测时间，设备会强制该用户下线。
- 自助服务器定位功能：通过该属性使得用户可以对自己的帐号和密码进行管理和控制。
缺省授权 **User Profile**：若认证服务器未对认证成功用户下发授权 **User Profile**，则系统会使用当前域中指定的 **User Profile** 作为用户的授权 **User Profile**，用户的访问行为将受到该 **User Profile** 中预设配置的限制。
- 域优先级：配置 **ISP** 域优先级，在用户认证通过后，可以根据登录时提供的携带有 **ISP** 域名的用户名（**userid@domain-name**）来设置该用户 **IP** 报文的 **DSCP** 值，这样可以区分同一种认证方案中不同 **ISP** 域的报文。根据 **IP** 报文的 **DSCP** 值不同，通过策略路由功能指定不同的下一跳，从而使不同 **ISP** 域用户认证成功后的报文走向不同。策略路由相关配置可参考“三层技术-**IP** 路由配置指导”中的“策略路由配置”。



配置 **ISP** 域优先级功能仅适用于认证方法为三层 **Portal** 认证的情况，以区分三层 **Portal** 认证时在同一种认证方案中不同 **ISP** 域的 **IP** 报文。三层 **Portal** 认证相关配置可参考“安全配置指导”中的“**Portal** 配置”。

表1-47 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 }	可选 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的限制	access-limit enable max-user-number	可选 缺省情况下，不对当前 ISP 域可容纳的接入用户数作限制
设置用户闲置切断功能	idle-cut enable minute	可选 缺省情况下，用户闲置切断功能处于关闭状态 此命令目前只对 lan-access 服务类型的用户有效
设置自助服务器定位功能	self-service-url enable url-string	可选 缺省情况下，自助服务器定位功能处于关闭状态
配置当前 ISP 域的缺省授权 User Profile	authorization-attribute user-profile profile-name	可选 缺省情况下，当前 ISP 域无缺省授权 User Profile

操作	命令	说明
配置当前ISP域优先级	dscp <i>dscp-value</i>	可选 缺省情况下，未配置ISP域的DSCP优先级



说明

- 关于 User Profile 的详细介绍请参见“安全配置指导”中的“User Profile”。
- 自助服务器定位功能需要与支持自助服务的 RADIUS 服务器配合使用，如 CAMS/iMC。

1.4.4 配置ISP域的AAA认证方法

在 AAA 中，认证、授权和计费是三个独立的业务流程。认证的职责是完成各接入或服务请求的用户名 / 密码 / 用户信息的交互认证过程，它不会下发授权信息给请求用户，也不会触动计费的流程。

AAA 支持以下认证方法：

- 不认证 (**none**)：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 (**local**)：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 (**scheme**)：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 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，可配置本地认证或者不认证作为备选认证方式完成认证。目前，仅 **lan-access** 用户的远端认证可支持不认证作为备选认证方法。

在 AAA 中，可以只使用认证，而不使用授权或计费。如果用户没有进行任何配置，则 ISP 域的缺省认证方法为 **local**。

配置前的准备工作：

- (1) 如果用户使用 RADIUS、HWTACACS 认证，则需要先配置要引用的 RADIUS、HWTACACS 方案；如果使用 **local** 或 **none** 认证，则不需要配置方案。
- (2) 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，并且从配置上限制了用户接入时使用的认证协议。
- (3) 确定是否为所有的接入方式或服务类型配置认证方法。

表1-48 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 <i>isp-name</i>	-

操作	命令	说明
为当前ISP域配置缺省的认证方法	authentication default { hwtacacs-scheme <i>hwtacacs-scheme-name</i> [local] local none radius-scheme <i>radius-scheme-name</i> [local] }	可选 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 { local none radius-scheme <i>radius-scheme-name</i> [local none] }	可选 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 <i>hwtacacs-scheme-name</i> [local] local none radius-scheme <i>radius-scheme-name</i> [local] }	可选 缺省情况下，login用户采用缺省的认证方法
为Portal用户配置认证方法	authentication portal { local none radius-scheme <i>radius-scheme-name</i> [local] }	可选 缺省情况下，Portal用户采用缺省的认证方法
配置级别切换认证方法	authentication super { hwtacacs-scheme <i>hwtacacs-scheme-name</i> radius-scheme <i>radius-scheme-name</i> }	可选 缺省情况下，级别切换认证采用缺省的认证方法



说明

- **authentication default** 命令配置的认证方法不区分用户类型，即对所有类型的用户都起作用。此配置的优先级低于具体接入方式的配置。
- 当选择 RADIUS 认证方案时，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。
- 如果配置 AAA 认证方法时指定了参数 **radius-scheme radius-scheme-name local**、**hwtacacs-scheme hwtacacs-scheme-name local**，则 **local** 为远端服务器没有正常响应后的备选认证方法。
- 如果 **local** 或者 **none** 作为第一认证方法，那么只能采用本地认证或者不进行认证，不能同时采用远程认证方法。
- 当使用 HWTACACS 方案进行级别切换认证时，系统默认使用登录用户名进行用户级别切换认证；当使用 RADIUS 方案进行级别切换认证时，系统使用 RADIUS 服务器上配置的“\$enab+level/\$”形式的用户名替换登录用户名进行用户级别切换认证，其中 *level* 为用户希望切换到的级别。例如，用户希望切换到级别 3，输入的用户名为“user1”，在要求携带域名认证的情况下，系统使用用户名“\$enab3@domain_name\$”进行用户级别切换认证，否则使用“\$enab3\$”进行用户级别切换认证。

1.4.5 配置ISP域的AAA授权方法

在 AAA 中，授权是一个和认证、计费同级别的独立流程，其职责是发送授权请求给所配置的授权服务器，授权通过后向用户下发授权信息。在 ISP 域的 AAA 配置中，授权方法为可选配置。

AAA 支持以下授权方法：

- **不授权 (none)**: 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 (通过 **Console** 口或者 **Telnet**、**FTP** 访问设备的用户) 只有系统所给予的 **0** 级别的命令行访问权限, 其中 **FTP** 用户可访问设备的根目录; 认证通过的非 **Login** 用户, 可直接访问网络。
- **本地授权 (local)**: 授权过程在接入设备上, 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 (scheme)**: 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, 可配置本地授权或直接授权作为备选授权方式完成授权。

如果用户没有进行任何配置, 则 **ISP** 域的缺省授权方法为 **local**。

配置前的准备工作:

- (1) 如果用户要使用 **HWTACACS** 授权, 则需要先配置要引用的 **HWTACACS** 方案; 如果是 **RADIUS** 授权, 只有在认证和授权方法中引用相同的 **RADIUS** 方案, 授权才起作用。
- (2) 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, 并且从配置上正确限制了接入所能使用的授权协议。
- (3) 确定是否为所有的接入方式或服务类型配置授权方法。

表1-49 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 <i>isp-name</i>	-
为当前 ISP 域配置缺省的授权方法	authorization default { hwtacacs-scheme <i>hwtacacs-scheme-name</i> [local] local none radius-scheme <i>radius-scheme-name</i> [local] }	可选 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 <i>hwtacacs-scheme-name</i> [local none] local none }	可选 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 radius-scheme <i>radius-scheme-name</i> [local none] }	可选 缺省情况下, lan-access 用户采用缺省的授权方法
为 login 用户配置授权方法	authorization login { hwtacacs-scheme <i>hwtacacs-scheme-name</i> [local] local none radius-scheme <i>radius-scheme-name</i> [local] }	可选 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 radius-scheme <i>radius-scheme-name</i> [local] }	可选 缺省情况下, Portal 用户采用缺省的授权方法



说明

- **authorization default** 命令配置的授权方法不区分用户类型，即对所有类型的用户都起作用。此配置的优先级低于具体接入方式的配置。
- 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。对于所有 RADIUS 授权失败的情况，RADIUS 服务器返回给 NAS 的原因为服务器没有响应。
- 如果配置 AAA 授权方法时指定了参数 **radius-scheme radius-scheme-name local**、**hwtacacs-scheme hwtacacs-scheme-name [local | none]**，则 **local** 或 **none** 为远端服务器没有正常响应后的备选授权方法。
- **local** 或者 **none** 作为第一授权方法时，没有备选授权方式，只能采用本地授权或者直接授权。

1.4.6 配置ISP域的AAA计费方法

在 AAA 中，计费是一个和认证、授权同级别的独立流程，其职责为发送计费开始 / 更新 / 结束请求给所配置的计费服务器。计费不是必须使用的。在 ISP 域的 AAA 配置中，允许不配置计费方法。如果不配置计费方法，则 ISP 域的缺省计费方法为 **local**。

AAA 支持以下计费方法：

- 不计费（**none**）：不对用户计费。
- 本地计费（**local**）：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。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。
- 远端计费（**scheme**）：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，可配置本地计费或不计费作为备选计费方式完成计费。

配置前的准备工作：

- (1) 如果用户要使用 RADIUS 或 HWTACACS 计费，则需要先配置要引用的 RADIUS 方案或 HWTACACS 方案；如果要使用 **local** 或 **none** 计费，则不需要配置方案。
- (2) 确定要配置的接入方式或者服务类型，AAA 可以支持为按照不同的接入方式和服务类型进行 AAA 计费的配置，并且从配置上正确限制了接入所能使用的计费协议。
- (3) 确定是否为所有的接入方式或服务类型配置计费方法。

表1-50 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	-

操作	命令	说明
打开计费可选开关	accounting optional	可选 缺省情况下,ISP域的计费可选开关处于关闭状态 对用户进行计费时,若发现没有可用的计费服务器或与计费服务器通信失败,在计费开关打开的情况下,用户可继续使用网络资源,否则用户会被强制下线
为当前ISP域配置缺省的计费方法	accounting default { hwtacacs-scheme hwtacacs-scheme-name [local] local none radius-scheme radius-scheme-name [local] }	可选 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	可选 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 radius-scheme radius-scheme-name [local none] }	可选 缺省情况下,lan-access用户采用缺省的计费方法
为login用户配置计费方法	accounting login { hwtacacs-scheme hwtacacs-scheme-name [local] local none radius-scheme radius-scheme-name [local] }	可选 缺省情况下,login用户采用缺省的计费方法
为Portal用户配置计费方法	accounting portal { local none radius-scheme radius-scheme-name [local] }	可选 缺省情况下,Portal用户采用缺省的计费方法



说明

- 在计费可选开关打开的情况下,本地用户的连接数限制功能不生效。
- accounting default** 命令配置的计费方法不区分用户类型,即对所有类型的用户都起作用。此配置的优先级低于具体接入方式的配置。
- 如果配置 AAA 计费方法时指定了参数 **radius-scheme radius-scheme-name local** 或 **hwtacacs-scheme hwtacacs-scheme-name local**,则 **local** 为远端服务器没有正常响应后的备选计费方法。
- 如果 **local** 或者 **none** 作为第一计费方法,那么只能采用本地认证或者不进行计费,不能同时采用远程计费方法。
- login 类型的接入中 FTP 方式不支持计费流程。

1.5 配置强制切断用户连接

表1-51 配置强制切断用户连接

操作	命令	说明
进入系统视图	system-view	-
强制切断指定AAA用户的连接	cut connection { access-type { dot1x mac-authentication portal } all domain isp-name interface interface-type interface-number ip ip-address mac mac-address ucibindex ucib-index user-name user-name vlan vlan-id } [slot slot-number]	必选 此命令目前只对lan-access、Portal服务类型的用户有效

1.6 配置NAS-ID与VLAN的绑定

用户的接入 VLAN 可标识用户的接入位置，而在某些应用环境中，网络运营商需要使用接入设备发送给 RADIUS 服务器的 NAS-Identifier 属性值来标识用户的接入位置，因此接入设备上需要建立用户接入 VLAN 与指定的 NAS-ID 之间的绑定关系。这样，当用户上线时，设备会将与用户接入 VLAN 匹配的 NAS-ID 填充在 RADIUS 请求报文中的 NAS-Identifier 属性中发送给 RADIUS 服务器。

表1-52 配置 NAS-ID 与 VLAN 的绑定

操作	命令	说明
进入系统视图	system-view	-
创建NAS-ID Profile，并进入NAS-ID-Profile视图	aaa nas-id profile profile-name	必选 本NAS-ID Profile将被使能Portal的接口进行引用，具体应用请参见“安全配置指导”中的“Portal”
设置NAS-ID 与VLAN的绑定关系	nas-id nas-identifier bind vlan vlan-id	必选 缺省情况下，未设置任何绑定关系

1.7 配置双机热备模式下的设备ID

设备 ID 是设备工作在双机热备环境中的一个标志，为保证设备上的 Portal 业务备份可以正常工作，互为备份的两台设备上必须配置不同编号的设备 ID。目前，设备 ID 的编号取值只能为 1 和 2。关于 Portal 双机热备的详细介绍请参考“安全配置指导”中的“Portal”。

表1-53 配置双机热备模式下的设备 ID

操作	命令	说明
进入系统视图	system-view	-

操作	命令	说明
配置双机热备模式下的设备ID	nas device-id <i>device-id</i>	必选 缺省情况下，设备工作在单机模式下，无设备ID



说明

- 配置或改变设备 ID 后，设备上所有在线用户均会被强制下线。因此需慎重操作，并建议该配置成功执行后，保存配置并重启设备。
- 由于设备 ID 是设备运行在双机模式下的标志，因此单机运行的环境下不需要在设备上对此配置。

1.8 配置设备作为RADIUS服务器

1.8.1 RADIUS服务器功能配置任务简介

表1-54 RADIUS 服务器功能配置任务简介

配置任务	说明	详细配置
配置RADIUS用户	必选	1.8.2
指定RADIUS客户端	必选	1.8.3

1.8.2 配置RADIUS用户

所谓 RADIUS 用户，是指在支持 RADIUS 服务器功能的设备上设置的一组用户属性的集合。该集合以用户名为用户的唯一标识。

为使某个请求网络服务的用户可以通过 RADIUS 认证，需要在设备上的 RADIUS 用户数据库中添加相应的 RADIUS 用户。具体步骤是，创建一个 RADIUS 用户并进入 RADIUS 服务器用户视图，然后在该视图下配置相应的用户属性。可配置的用户属性包括：用户密码、授权属性、帐户有效期和用户描述信息。

表1-55 配置 RADIUS 用户

操作	命令	说明
进入系统视图	system-view	-
创建RADIUS用户并进入RADIUS服务器用户视图	radius-server user <i>user-name</i>	必选 缺省情况下，不存在任何RADIUS用户

操作	命令	说明
配置RADIUS用户密码	password [cipher simple] <i>password</i>	可选 缺省情况下，未设置RADIUS用户的密码
配置RADIUS用户的授权属性	authorization-attribute { acl <i>acl-number</i> vlan <i>vlan-id</i> } *	可选 缺省情况下，未配置任何授权信息
配置RADIUS用户的有效期	expiration-date <i>time</i>	可选 缺省情况下，未配置用户的有效期，设备不进行用户有效期的检查
配置RADIUS用户的描述信息	description <i>text</i>	可选 缺省情况下，未配置任何描述信息



说明

通过命令 **authorization-attribute** 可以为 RADIUS 用户设置授权 ACL 以及授权 VLAN 属性。当用户通过认证后，RADIUS 服务器将这些属性下发到 RADIUS 客户端（即 NAS）上，NAS 根据下发的 VLAN/ACL 控制用户的访问权限。若 NAS 上不存在对应的 ACL，则 ACL 下发失败，该用户将被强制下线；若 NAS 上不存在对应的 VLAN，则 NAS 首先创建 VLAN，而后将连接用户的端口或用户加入授权 VLAN。

1.8.3 指定RADIUS客户端

RADIUS 服务器上使用 IP 地址来标识被管理的 RADIUS 客户端。RADIUS 服务器只处理来自其管理范围内的客户端的 RADIUS 报文，对其它报文直接作丢弃处理。本配置用来指定要管理的 RADIUS 客户端的 IP 地址，以及与 RADIUS 客户端通信的共享密钥。

表1-56 指定 RADIUS 客户端

操作	命令	说明
进入系统视图	system-view	-
指定RADIUS客户端	radius-server client-ip <i>ip-address</i> [key [cipher simple] <i>string</i>]	必选 缺省情况下，未指定任何RADIUS客户端



说明

- RADIUS 服务器上指定的 RADIUS 客户端 IP 地址必须和 RADIUS 客户端上配置的发送 RADIUS 报文的源 IP 地址保持一致。
- RADIUS 服务器上指定的共享密钥必须和 RADIUS 客户端上配置的与 RADIUS 服务器通信的共享密钥保持一致。

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1-57 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 [<i>isp-name</i>] [{ begin exclude include } <i>regular-expression</i>]
显示AAA用户连接的相关信息	display connection [access-type { dot1x mac-authentication portal } domain <i>isp-name</i> interface <i>interface-type</i> <i>interface-number</i> ip <i>ip-address</i> mac <i>mac-address</i> ucibindex <i>ucib-index</i> user-name <i>user-name</i> vlan <i>vlan-id</i>] [slot <i>slot-number</i>] [{ begin exclude include } <i>regular-expression</i>]

1.10 AAA典型配置举例

1.10.1 Telnet用户的HWTACACS认证、授权、计费配置

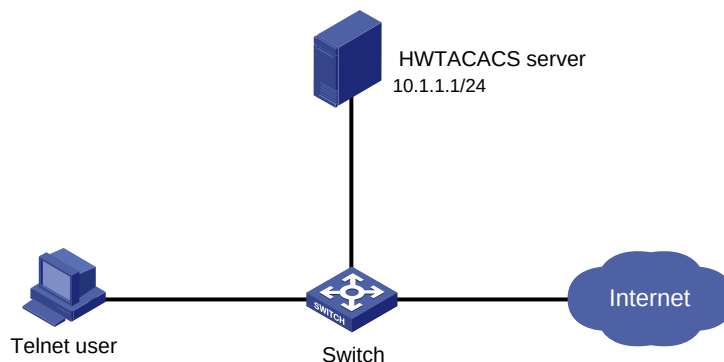
1. 组网需求

如下图所示，Telnet 用户主机与 Switch 直接相连，Switch 与一台 HWTACACS 服务器相连，需要实现 HWTACACS 服务器对登录 Switch 的 Telnet 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。
- Switch 与 HWTACACS 服务器交互报文时的共享密钥为 expert，向 HWTACACS 服务器发送的用户名中不带域名。

2. 组网图

图1-11 Telnet 用户远端 HWTACACS 认证、授权和计费配置组网图



3. 配置步骤

配置各接口的 IP 地址（略）。

开启 Switch 的 Telnet 服务器功能。

```
<Switch> system-view
```

```
[Switch] telnet server enable
```

配置 Telnet 用户登录采用 AAA 认证方式。

```
[Switch] user-interface vty 0 4
```

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

```
[Switch-ui-vty0-4] quit
```

创建 HWTACACS 方案 hwtac。

```
[Switch] 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。

```
[Switch-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。

```
[Switch-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。

```
[Switch-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 expert。

```
[Switch-hwtacacs-hwtac] key authentication simple expert
```

```
[Switch-hwtacacs-hwtac] key authorization simple expert
```

```
[Switch-hwtacacs-hwtac] key accounting simple expert
```

配置向 HWTACACS 服务器发送的用户名不携带域名。

```
[Switch-hwtacacs-hwtac] user-name-format without-domain
```

```
[Switch-hwtacacs-hwtac] quit
```

配置 ISP 域的 AAA 方法。

```
[Switch] domain bbb
```

```
[Switch-isp-bbb] authentication login hwtacacs-scheme hwtac
```

```
[Switch-isp-bbb] authorization login hwtacacs-scheme hwtac
```

```
[Switch-isp-bbb] accounting login hwtacacs-scheme hwtac
```

```
[Switch-isp-bbb] quit
```

4. 验证配置结果

用户向 Switch 发起 Telnet 连接，在 Telnet 客户端按照提示输入正确的用户名和密码后，可成功进入 Switch 的用户界面。在 Switch 上可以通过 **display connection** 命令查看到 AAA 用户的连接信息。

1.10.2 Telnet用户的local认证、HWTACACS授权、RADIUS计费配置

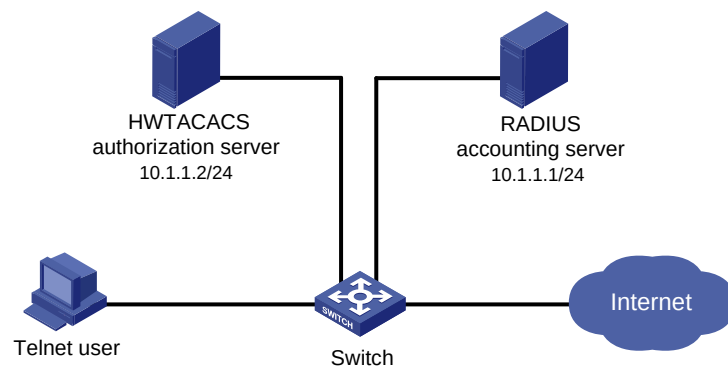
1. 组网需求

如下图所示，Telnet 用户主机与 Switch 直接相连，Switch 分别与一台 RADIUS 服务器和一台 HWTACACS 服务器相连，需要实现对登录 Switch 的 Telnet 用户进行 local 认证，HWTACACS 授权和 RADIUS 计费。

- 一台 HWTACACS 服务器(担当授权服务器的职责)与 Switch 相连,服务器 IP 地址为 10.1.1.2。Switch 与授权 HWTACACS 服务器交互报文时的共享密钥为 expert，发送给 HWTACACS 服务器的用户名中不带域名。
- 一台 RADIUS 服务器（担当计费服务器的职责）与 Switch 相连，服务器 IP 地址为 10.1.1.1。Switch 与计费 RADIUS 服务器交互报文时的共享密钥为 expert。

2. 组网图

图1-12 Telnet 用户 local 认证、HWTACACS 授权和 RADIUS 计费配置组网图



3. 配置步骤

配置各接口的 IP 地址（略）。

开启 Switch 的 Telnet 服务器功能。

```
<Switch> system-view
```

```
[Switch] telnet server enable
```

配置 Telnet 用户登录采用 AAA 认证方式。

```
[Switch] user-interface vty 0 4
```

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

```
[Switch-ui-vty0-4] quit
```

配置 HWTACACS 方案。

```
[Switch] hwtacacs scheme hwtac
```

```
[Switch-hwtacacs-hwtac] primary authorization 10.1.1.2 49
```

```
[Switch-hwtacacs-hwtac] key authorization expert
```

```
[Switch-hwtacacs-hwtac] user-name-format without-domain
```

```
[Switch-hwtacacs-hwtac] quit
```

配置 RADIUS 方案。

```
[Switch] radius scheme rd
```

```
[Switch-radius-rd] primary accounting 10.1.1.1 1813
```

```
[Switch-radius-rd] key accounting expert
```

```
[Switch-radius-rd] server-type extended
```

```
[Switch-radius-rd] user-name-format without-domain
```

```
[Switch-radius-rd] quit
```

创建本地用户 hello。

```
[Switch] local-user hello
```

```
[Switch-luser-hello] service-type telnet
```

```
[Switch-luser-hello] password simple hello
```

```
[Switch-luser-hello] quit
```

配置 ISP 域的 AAA 方法。

```
[Switch] domain bbb
```

```
[Switch-isp-bbb] authentication login local
```

```
[Switch-isp-bbb] authorization login hwtacacs-scheme hwtac
```

```
[Switch-isp-bbb] accounting login radius-scheme rd
```

```
[Switch-isp-bbb] quit
```

4. 验证配置结果

用户向 Switch 发起 Telnet 连接，在 Telnet 客户端按照提示输入用户名 `hello@bbb` 和正确的密码后，可成功进入 Switch 的用户界面。在 Switch 上可以通过 **display connection** 命令查看到 AAA 用户的连接信息。

1.10.3 SSH/Telnet用户的RADIUS认证和授权配置



说明

Telnet 用户与 SSH 用户通过 RADIUS 服务器进行认证/授权的配置方法类似，下面的描述以 SSH 用户的远端认证为例。

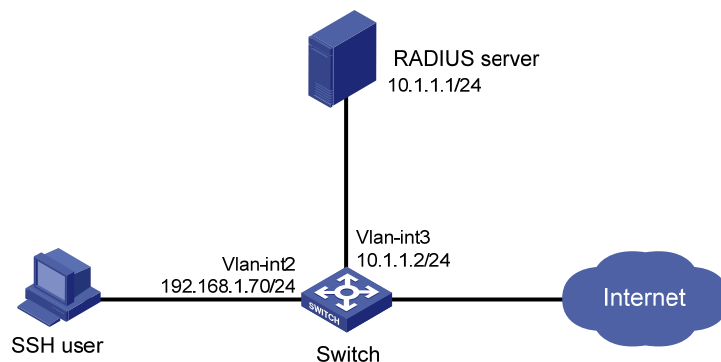
1. 组网需求

如 图 1-13 所示，Telnet用户主机与Switch直接相连，Switch与一台RADIUS服务器相连，需要实现对登录Switch的Telnet用户进行RADIUS认证。

- 由一台 CAMS/iMC 服务器担当认证/授权 RADIUS 服务器的职责，服务器 IP 地址为 10.1.1.1/24。
- Switch 与 RADIUS 服务器交互报文时使用的共享密钥为 expert，向 RADIUS 服务器发送的用户名带域名。服务器根据用户名携带的域名来区分提供给用户的服务。
- SSH 用户登录 Switch 时使用 RADIUS 服务器上配置的用户名 hello@bbb 以及密码进行认证，认证通过后的用户级别为 3。

2. 组网图

图1-13 SSH 用户 RADIUS 认证/授权配置组网图



3. 配置步骤

(1) 配置 RADIUS 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 RADIUS server 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 Switch 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；
- 单击<确定>按钮完成操作。

 说明

添加的接入设备 IP 地址要与 Switch 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 Vlan-interface3 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1-14 增加接入设备

 业务 >> 接入业务 >> 接入设备配置 >> 增加接入设备

接入配置

* 共享密钥

expert

* 计费端口

1813

接入设备类型

H3C

业务分组

未分组

* 认证端口

1812

业务类型

设备管理业务

组网方式

不启用混合组网

接入区域

无

设备列表

选择

手工增加

全部清除

请单击下方的<确定>按钮完成配置。

共有1条记录。

设备名称	设备IP地址	设备型号	删除
	10.1.1.2		

确定

取消

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，进入增加设备管理页面。

- 输入用户名“hello@bbb”和密码；
- 选择服务类型为“SSH”；
- 设置 EXEC 权限级别为“3”，该值为 SSH 用户登录系统后的用户级别（缺省为 0）；
- 增加所管理设备的 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。

图1-15 增加设备管理用户

用户 >> 设备管理用户 >> 增加设备管理用户

增加设备管理用户

设备管理用户基本信息

* 帐号名

hello@bbb

?

* 用户密码

.....

* 密码确认

.....

服务类型

SSH

▼

EXEC权限级别

3

?

绑定的用户IP地址列表

增加

删除

未找到符合条件的记录。

☐	起始IP地址	结束IP地址	删除

所管理设备IP地址列表

增加

删除

共有1条记录。

☐	起始IP地址	结束IP地址	删除
☐	10.1.1.0	10.1.1.255	✖

确定

取消

(2) 配置 Switch

配置 VLAN 接口 2 的 IP 地址，SSH 客户端将通过该地址连接 SSH 服务器。

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
```

配置 VLAN 接口 3 的 IP 地址，Switch 将通过该地址与服务器通信。

```
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Switch-Vlan-interface3] quit
```

生成 RSA 及 DSA 密钥对，并启动 SSH 服务器。

```
[Switch] public-key local create rsa
[Switch] public-key local create dsa
[Switch] ssh server enable
```

配置 SSH 用户登录采用 AAA 认证方式。

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
```

配置用户远程登录 Switch 的协议为 SSH。

```

[Switch-ui-vty0-4] protocol inbound ssh
[Switch-ui-vty0-4] quit
# 创建 RADIUS 方案 rad。
[Switch] 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。
[Switch-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 expert。
[Switch-radius-rad] key authentication expert
# 配置向 RADIUS 服务器发送的用户名携带域名。
[Switch-radius-rad] user-name-format with-domain
# 配置 RADIUS 服务器的服务类型。使用 CAMS/iMC 服务器时，RADIUS 服务器类型应选择 extended。
[Switch-radius-rad] server-type extended
[Switch-radius-rad] quit
# 配置 ISP 域的 AAA 方法。
[Switch] domain bbb
[Switch-isp-bbb] authentication login radius-scheme rad
[Switch-isp-bbb] authorization login radius-scheme rad
[Switch-isp-bbb] quit

```

4. 验证配置结果

用户向 Switch 发起 SSH 连接，在 SSH 客户端按照提示输入用户名 `hello@bbb` 及正确的密码后，可成功进入 Switch 的用户界面，并可以使用级别为 0、1、2、3 的命令。

可以通过如下命令查看到 AAA 用户的连接信息。

```

[Switch] display connection

Index=1      ,Username=hello@bbb
IP=192.168.1.58
IPv6=N/A
Total 1 connection(s) matched.

```

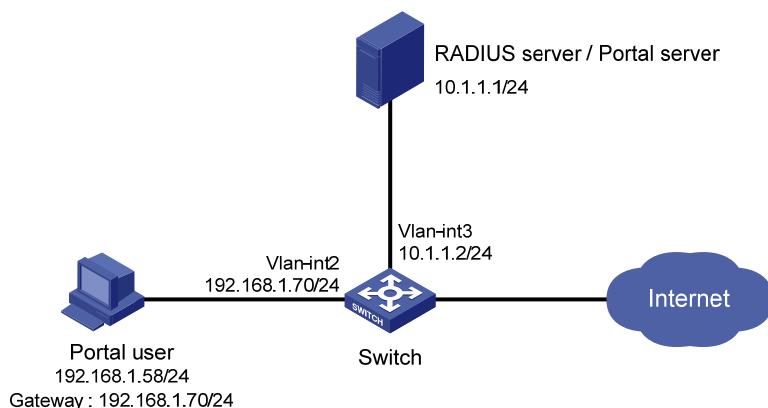
1.10.4 Portal用户的RADIUS认证、授权和计费配置

1. 组网需求

- 用户主机与接入设备 Switch 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 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。
- 使用 RADIUS 服务器作为认证/计费服务器。（本例中，RADIUS 服务器和 Portal 服务器位于同一台服务器主机上）；
- Switch 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，向 RADIUS 服务器发送的用户名携带域名。
- 对 Portal 用户进行包月方式计费，费用为 120 元/月，以月为周期对用户上网服务的使用量按时长进行统计，允许每月最大上网使用量为 120 个小时。

2. 组网图

图1-16 Portal 用户 RADIUS 认证、授权和计费配置组网图



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。

(1) 配置 RADIUS 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)、iMC CAMS 5.0(E0101)），说明 RADIUS server 和 Portal server 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 Switch 交互报文时的认证、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“LAN 接入业务”；
- 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 Switch 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 Vlan-interface3 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1-17 增加接入设备

 **业务 >> 接入业务 >> 接入设备配置 >> 增加接入设备**

接入配置			
* 共享密钥	expert	* 认证端口	1812
* 计费端口	1813	业务类型	LAN接入业务
接入设备类型	H3C	组网方式	不启用混合组网
业务分组	未分组	接入区域	无

设备列表			
选择	手工增加	全部清除	请单击下方的<确定>按钮完成配置。
共有1条记录。			
设备名称	设备IP地址	设备型号	删除
	10.1.1.2		X

增加计费策略。

选择“业务”页签，单击导航树中的[计费业务/计费策略管理]菜单项，进入计费策略管理页面，在该页面中单击<增加>按钮，进入计费策略配置页面。

- 输入计费策略名称“UserAcct”；
- 选择计费策略模板为“包月类型计费”；
- 设置包月基本信息：计费方式为“按时长”、计费周期为“月”、周期内固定费用为“120 元”；
- 设置包月使用量限制：允许每月最大上网使用量为 120 个小时。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图1-18 增加计费策略

业务 >> 计费业务 >> 计费策略管理 >> 增加计费策略

计费策略配置

基本信息

* 策略名称

UserAcct

计费策略模板

包月类型计费

业务分组

未分组

策略描述

包月基本信息

计费方式

按时长

计费周期类型

月

* 周期内固定费用

120

元

包月使用量限制设置

周期内限制量

120

?

周期内限制单位

小时

确定

取消

增加服务配置。

选择“业务”页签，单击导航树中的[接入业务/服务配置管理]菜单项，进入服务器配置管理页面，在该页面中单击<增加>按钮，进入增加服务配置页面。

- 输入服务名为“Portal-auth/acct”、服务后缀为“dm1”，此服务后缀为 Portal 用户使用的认证域。指定服务后缀的情况下，RADIUS 方案中必须指定向服务器发送的用户名中携带域名；
- 选择计费策略为“UserAcct”；
- 本配置页面中还有其它服务配置选项，请根据实际情况选择配置；
- 单击<确定>按钮完成操作。

图1-19 增加服务配置

业务 >> 接入业务 >> 服务配置管理 >> 增加服务配置

增加服务配置

基本信息

* 服务名

Portal-auth/acct

服务后缀

dm1

* 业务分组

未分组

计费策略

UserAcct

计费周期开始类型

自适应

计费周期开始日期

不限

☐ 自适应连续扣费 ☒ 首次计费周期按全周期计费 ☐ 首次计费周期按天计费 ☐ 首次计费周期免周期费

服务描述

LDAP优先级

☒ 可申请 ?

增加接入用户。

选择“用户”页签，单击导航树中的[接入用户视图/所有接入用户]菜单项，进入接入用户列表页面，在该页面中单击<增加>按钮，进入增加接入用户页面。

- 选择或者手工增加用户姓名为“hello”；
- 输入帐号名“portal”和密码；
- 选择该用户所关联的接入服务为“Portal-auth/acct”；
- 本配置页面中还有其它服务配置选项，请根据实际情况选择配置；
- 单击<确定>按钮完成操作。

图1-20 增加接入用户

用户 >> 所有接入用户 >> 增加接入用户

帮助

接入用户

接入信息

* 用户姓名

hello

选择

增加用户

* 帐号名

portal

☐快速认证用户

☐主机名用户

* 密码

.....

* 密码确认

.....

☒允许用户修改密码

☐启用用户密码控制策略

☐下次登录须修改密码

失效日期

最大闲置时长

分钟

在线数量限制

1

帐号类型

预付费

* 预付金额

120元

自助充值

允许

登录提示信息

接入服务

	服务名	服务后缀	状态	计费策略	分配IP地址
☒	Portal-auth/acct	dm1	可申请	UserAcct	

(2) 配置 Portal server（iMC PLAT 5.0）

配置 Portal 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 服务器管理/服务器配置]菜单项，进入服务器配置页面。

- 输入 Portal 认证主页地址，形式为 http://ip:port/portal，其中 ip 和 port 在安装 iMC UAM 的时候确定，port 一般使用缺省值 8080 即可；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图1-21 Portal 服务器配置页面

业务>>接入业务>>Portal服务管理 >> 服务器配置

Portal服务器配置

基本信息

* 日志级别

信息

* 报文请求超时时长

5

秒

* 逃生心跳间隔时长

20

秒

* 用户心跳间隔时长

5

分钟

Portal主页

http://10.1.1.1:8080/portal

高级信息

服务类型列表

增加

共有0条记录。

服务类型标识	服务类型	删除

确定

配置 IP 地址组。

单击导航树中的[Portal 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。

- 输入 IP 地址组名为 “Portal_user” ；
- 输入起始地址为 “192.168.1.1”、终止地址为 “192.168.1.255”。用户主机 IP 地址必须包含在该 IP 地址组范围内；
- 选择类型为 “普通” ；
- 单击<确定>按钮完成操作。

图1-22 增加 IP 地址组配置页面

业务>>接入业务>>Portal服务管理>>Portal IP地址组配置>>增加IP地址组

增加IP地址组

* IP地址组名

Portal_user

* 起始地址

192.168.1.1

* 终止地址

192.168.1.255

业务分组

未分组

* 类型

普通

确定取消

增加 Portal 设备。

单击导航树中的[Portal 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。

- 输入设备名为“NAS”；
- 输入 IP 地址为“192.168.1.70”，该地址为与接入用户相连的设备接口 IP 地址；
- 输入密钥为“portal”，该密钥与接入设备 Switch 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”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图1-23 增加设备信息配置页面

业务>>接入业务>>Portal服务管理>>Portal设备配置>>增加设备信息

增加设备信息

* 设备名

NAS

* IP地址

192.168.1.70

* 版本

Portal 2.0

* 密钥

portal

* 监听端口

2000

* 本地Challenge

否

* 认证重发次数

2

* 下线重发次数

4

* 二次地址分配

否

* 支持逃生心跳

否

* 支持用户心跳

否

* 业务分组

未分组

设备描述

确定

取消

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1-24 设备信息列表

业务>>接入业务>>Portal服务管理 >> 设备配置

设备信息查询

设备名

版本

业务分组

查询

重置

设备信息列表

增加

共有1条记录，当前第1 - 1，第 1/1 页。 每页显示：8 15 [50] 100 200

设备名	版本	业务分组	IP地址	端口组信息管理	详细信息	修改	删除
NAS	Portal 2.0	未分组	192.168.1.70				

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。

- 输入端口组名为“group”；
- 选择 IP 地址组为“Portal_user”，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，并单击<确定>按钮完成操作。

图1-25 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 服务器配置生效。

(3) 配置 Switch

- 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<Switch> system-view
[Switch] radius scheme rs1
```

配置 RADIUS 方案的服务器类型。使用 CAMS/iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[Switch-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Switch-radius-rs1] primary authentication 10.1.1.1
[Switch-radius-rs1] primary accounting 10.1.1.1
[Switch-radius-rs1] key authentication expert
[Switch-radius-rs1] key accounting expert
```

配置发送给 RADIUS 服务器的用户名携带 ISP 域名。

```
[Switch-radius-rs1] user-name-format with-domain
[Switch-radius-rs1] quit
```

- 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[Switch] domain dm1
```

配置 ISP 域的 RADIUS 方案 rs1。

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
```

```
[Switch-isp-dm1] authorization portal radius-scheme rs1
[Switch-isp-dm1] accounting portal radius-scheme rs1
[Switch-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法。

```
[Switch] domain default enable dm1
```

• 配置 Portal 认证

配置 Portal 服务器：名称为 newpt，IP 地址为 10.1.1.1，密钥为 portal，端口为 50100，URL 为 http://10.1.1.1:8080/portal。

```
[Switch] portal server newpt ip 10.1.1.1 key portal port 50100 url
http://10.1.1.1:8080/portal
```

在与用户 Host 相连的接口上使能 Portal 认证。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] portal server newpt method direct
[Switch-Vlan-interface2] quit
```

4. 验证配置结果

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://10.1.1.1:8080/portal，且发起的 Web 访问请求均被重定向到该认证页面，通过认证后，即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 Switch 上生成的 Portal 在线用户信息。

```
[Switch] display portal user interface vlan-interface 2
Index:19
State:ONLINE
SubState:NONE
ACL:NONE
Work-mode:stand-alone
MAC                IP                Vlan  Interface
-----
0015-e9a6-7cfe     192.168.1.58      2     Vlan-interface2
Total 1 user(s) matched, 1 listed.
```

可以通过如下命令查看到 AAA 用户的连接信息。

```
[Switch] display connection

Index=20 ,Username=portal@dm1
IP=192.168.1.58
IPv6=N/A
MAC=00-15-E9-A6-7C-FE
```

```
Total 1 connection(s) matched.
```

1.10.5 802.1X用户的RADIUS认证、授权和计费配置

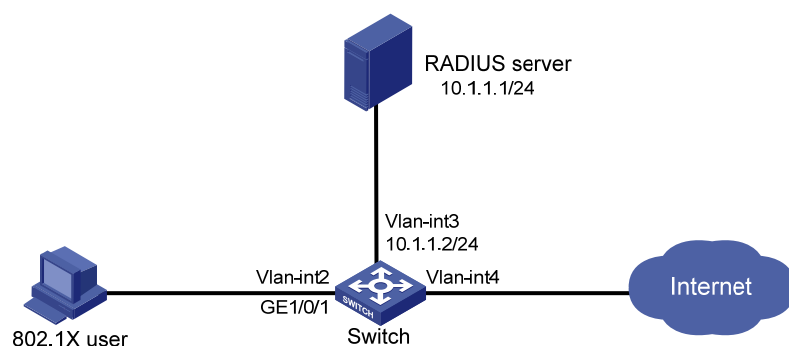
1. 组网需求

在 [图 1-26](#) 所示的组网环境中，需要实现使用 RADIUS 服务器对通过 Switch 接入的 802.1X 用户进行认证、授权和计费。

- 在接入端口 GigabitEthernet1/0/1 上对接入用户进行 802.1X 认证, 并采用基于 MAC 地址的接入控制方式, 即该端口下的所有用户都需要单独认证;
- Switch 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, 向 RADIUS 服务器发送的用户名携带域名;
- 用户认证时使用的用户名为 dot1x@bbb。
- 用户认证成功后, 认证服务器授权下发 VLAN 4, 将用户所在端口加入该 VLAN, 允许用户访问该 VLAN 中的网络资源。
- 对 802.1X 用户进行包月方式计费, 费用为 120 元/月, 以月为周期对用户上网服务的使用量按时长进行统计, 允许每月最大上网使用量为 120 个小时。

2. 组网图

图1-26 802.1X 用户 RADIUS 认证、授权和计费配置组网图



3. 配置步骤



说明

请按照组网图完成端口和 VLAN 的配置, 并保证在用户通过认证后能够自动或者手动更新 IP 地址与授权 VLAN 中的资源互通。

(1) 配置 RADIUS 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)、iMC CAMS 5.0(E0101)), 说明 RADIUS server 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 Switch 交互报文时的认证、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“LAN 接入业务”;

- 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 Switch 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。

- 若设备使用缺省的发送 RADIUS 报文的源地址，例如，本例中为接口 Vlan-interface3 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。
- 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。

图1-27 增加接入设备

业务 >> 接入业务 >> 接入设备配置 >> 增加接入设备

接入配置			
* 共享密钥	expert	* 认证端口	1812
* 计费端口	1813	业务类型	LAN接入业务
接入设备类型	H3C	组网方式	不启用混合组网
业务分组	未分组	接入区域	无

设备列表			
选择	手工增加	全部清除	请单击下方的<确定>按钮完成配置。
共有1条记录。			
设备名称	设备IP地址	设备型号	删除
	10.1.1.2		✖

增加计费策略。

选择“业务”页签，单击导航树中的[计费业务/计费策略管理]菜单项，进入计费策略管理页面，在该页面中单击<增加>按钮，进入计费策略配置页面。

- 输入计费策略名称“UserAcct”；
- 选择计费策略模板为“包月类型计费”；
- 设置包月基本信息：计费方式为“按时长”、计费周期为“月”、周期内固定费用为“120 元”；
- 设置包月使用量限制：允许每月最大上网使用量为 120 个小时。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图1-28 增加计费策略

业务 >> 计费业务 >> 计费策略管理 >> 增加计费策略

计费策略配置

基本信息

* 策略名称

UserAcct

计费策略模板

包月类型计费

业务分组

未分组

策略描述

包月基本信息

计费方式

按时长

计费周期类型

月

* 周期内固定费用

120

元

包月使用量限制设置

周期内限制量

120

周期内限制单位

分钟

确定

取消

- # 增加服务配置。
- 选择“业务”页签，单击导航树中的[接入业务/服务配置管理]菜单项，进入服务器配置管理页面，在该页面中单击<增加>按钮，进入增加服务配置页面。
- 输入服务名为“Dot1x auth”、服务后缀为“bbb”，此服务后缀为 802.1X 用户使用的认证域。指定服务后缀的情况下，RADIUS 方案中必须指定向服务器发送的用户名中携带域名；
 - 选择计费策略为“UserAcct”；
 - 配置授权下发的 VLAN ID 为“4”；
 - 本配置页面中还有其它服务配置选项，请根据实际情况选择配置；
 - 单击<确定>按钮完成操作。

图1-29 增加服务配置

业务 >> 接入业务 >> 服务配置管理 >> 增加服务配置

增加服务配置

基本信息

* 服务名

Dot1x auth

服务后缀

bbb

* 业务分组

未分组

计费策略

UserAcct

计费周期开始类型

自适应

计费周期开始日期

不限

☐ 自适应连续扣费

☒ 首次计费周期按全周期计费

☐ 首次计费周期按天计费

☐ 首次计费周期免周期费

服务描述

LDAP优先级

☒ 可申请

授权信息

* 接入时段

无

分配IP地址

否

下行速率

Kbps

上行速率

Kbps

优先级

☐ 启用RSA认证

证书认证

☒ 不启用

☐ EAP证书认证

☐ WAP证书认证

认证证书类型

EAP-TLS认证

☒ 下发VLAN

4

☐ 下发User Profile

☐ 下发用户组

☐ 下发ACL

增加接入用户。

选择“用户”页签，单击导航树中的[接入用户视图/所有接入用户]菜单项，进入接入用户列表页面，在该页面中单击<增加>按钮，进入增加接入用户页面。

- 选择或者手工增加用户姓名为“test”；
- 输入帐号名“dot1x”和密码；
- 选择该用户所关联的接入服务为“Dot1x auth”；
- 本配置页面中还有其它服务配置选项，请根据实际情况选择配置；
- 单击<确定>按钮完成操作。

1-19

图1-30 增加接入用户

用户 >> 所有接入用户 >> 增加接入用户

帮助

接入用户

接入信息

* 用户姓名

test

选择

增加用户

* 帐号名

dot1x

☐ 快速认证用户

☐ 主机名用户

* 密码

.....

* 密码确认

.....

☒ 允许用户修改密码

☐ 启用用户密码控制策略

☐ 下次登录须修改密码

失效日期

最大闲置时长

分钟

在线数量限制

1

帐号类型

预付费

* 预付金额

0

元

自助充值

允许

登录提示信息

接入服务

	服务名	服务后缀	状态	计费策略	分配IP地址
☒	Dot1x auth	bbb	可申请	UserAcct	

(2) 配置 Switch

● 配置 RADIUS 方案

创建名字为 rad 的 RADIUS 方案并进入该方案视图。

```
<Switch> system-view
```

```
[Switch] radius scheme rad
```

配置 RADIUS 方案的服务器类型。使用 CAMS/iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[Switch-radius-rad] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Switch-radius-rad] primary authentication 10.1.1.1
```

```
[Switch-radius-rad] primary accounting 10.1.1.1
```

```
[Switch-radius-rad] key authentication expert
```

```
[Switch-radius-rad] key accounting expert
```

配置发送给 RADIUS 服务器的用户名携带 ISP 域名。

```
[Switch-radius-rad] user-name-format with-domain
```

```
[Switch-radius-rad] quit
```

● 配置认证域

创建并进入名字为 bbb 的 ISP 域。

```
[Switch] domain bbb
```

配置 ISP 域的 RADIUS 方案 rad。

```
[Switch-isp-bbb] authentication lan-access radius-scheme rad
```

```
[Switch-isp-bbb] authorization lan-access radius-scheme rad
```

```
[Switch-isp-bbb] accounting lan-access radius-scheme rad
```

```
[Switch-isp-bbb] quit
```

配置系统缺省的 ISP 域 bbb，所有接入用户共用此缺省域认证和计费方式。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法。

```
[Switch] domain default enable bbb
```

- 配置 802.1X 认证

开启全局 802.1X 认证。

```
[Switch] dot1x
```

开启端口 GigabitEthernet1/0/1 的 802.1X 认证。

```
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] dot1x
```

```
[Switch-GigabitEthernet1/0/1] quit
```

设置接入控制方式（该命令可以不配置，因为端口的接入控制在缺省情况下就是基于 MAC 地址的）。

```
[Switch] dot1x port-method macbased interface gigabitethernet 1/0/1
```

4. 验证配置结果



说明

- 若使用 Windows XP 的 802.1X 客户端，则需要正确设置此连接的网络属性：在网络属性的“验证”页签中，确保选中“启用此网络的 IEEE 802.1x 验证”，并选择要用于此连接的 EAP 认证类型为“MD5-质询”。
- 若使用 iNode 802.1X 客户端，则无需启用任何高级认证选项。

对于使用 iNode 802.1X 客户端的用户，在客户端的用户属性中输入正确的用户名“dot1x@bbb”和密码后，通过主动发起连接可成功通过认证；对于使用 Windows XP 802.1X 客户端的用户，在系统自动弹出的认证对话框中输入正确的用户名“dot1x@bbb”和密码后，可成功通过认证。认证通过后，服务器向该用户所在端口授权下发了 VLAN 4。

可以通过如下命令查看到 AAA 用户的连接信息。

```
[Switch] display connection
```

```
Slot: 1
```

```
Index=22 , Username=dot1x@bbb
```

```
IP=192.168.1.58
```

```
IPv6=N/A
```

```
MAC=0015-e9a6-7cfe
```

```
Total 1 connection(s) matched on slot 1.
```

```
Total 1 connection(s) matched.
```

可以通过如下命令查看该连接的详细信息，其中授权下发 VLAN 为 VLAN 4。

```
[Switch] display connection ucibindex 22
```

```
Slot: 1
```

```
Index=22 , Username=dot1x@bbb
```

```
IP=192.168.1.58
```

```
IPv6=N/A
```

```
MAC=0015-e9a6-7cfe
```

```
Access=8021X , AuthMethod=CHAP
```

```
Port Type=Ethernet, Port Name=GigabitEthernet1/0/1
```

```
Initial VLAN=2, Authorization VLAN=4
```

```
ACL Group=Disable
```

```
User Profile=N/A
```

```
CAR=Disable
```

```
Priority=Disable
Start=2011-04-26 19:41:12 ,Current=2011-04-26 19:41:25 ,Online=00h00m14s
Total 1 connection matched.
```

1.10.6 Telnet用户的HWTACACS级别切换认证配置

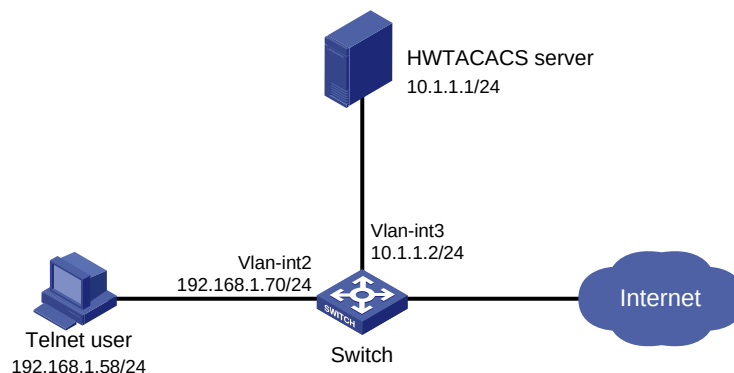
1. 组网需求

如 图 1-31 所示，Telnet用户主机与Switch直接相连，Switch与一台HWTACACS服务器相连，需要配置Switch实现对登录Switch的Telnet用户进行用户级别切换认证。具体要求如下：

Telnet 用户登录 Switch 时进行本地认证，登录后所能访问的命令级别为 0 级，当进行由低到高的用户级别切换时，首先使用 HWTACACS 认证，若 AAA 配置无效或者 HWTACACS 服务器没有响应则转为 **local** 认证。

2. 组网图

图1-31 Telnet 用户远端 HWTACACS 用户级别切换认证配置组网图



3. 配置思路

在交换机上的配置思路如下：

- (1) 配置 Telnet 用户登录采用 AAA 认证方式 (**scheme**)，并且使用 AAA 中的本地认证。
 - 创建 ISP 域 **bbb**，配置 Telnet 用户登录时采用的 **login** 认证方法为 **local**。
 - 创建本地用户，配置 Telnet 用户登录密码及登录后的用户级别。
- (2) Telnet 用户进行由低到高的用户级别切换时，首先使用 HWTACACS 认证，若 AAA 配置无效或者 HWTACACS 服务器没有响应则转为本地认证。
 - 配置用户级别切换认证方式为 **scheme local**。
 - 配置 HWTACACS 方案 **hwtac**，指定 HWTACACS 服务器 IP 地址及与其进行交互的相关参数（HWTACACS 协议报文交互时使用的共享密钥，Switch 发送给 HWTACACS 服务器的用户名不带域名）。在 ISP 域 **bbb** 下配置级别切换认证方法为 **hwtac**。
 - 配置采用本地认证方式时的级别切换密码。

在 HWTACACS server 上需要添加用于级别切换认证的用户名和密码。

4. 配置步骤

(1) 配置 Switch

配置 VLAN 接口 2 的 IP 地址，Telnet 客户端将通过该地址连接 Switch。

```

<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
# 配置 VLAN 接口 3 的 IP 地址，Switch 将通过该地址与服务器通信。
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Switch-Vlan-interface3] quit
# 开启 Switch 的 Telnet 服务器功能。
[Switch] telnet server enable
# 配置 Telnet 用户登录采用 AAA 认证方式。
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
[Switch-ui-vty0-4] quit
# 配置进行由低到高的用户级别切换时的级别切换认证方式为 scheme local。（首先使用 HWTACACS 认证，若 AAA 配置无效或者 HWTACACS 服务器没有响应则转为本地认证）
[Switch] super authentication-mode scheme local
# 创建 HWTACACS 方案 hwtac。
[Switch] 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。
[Switch-hwtacacs-hwtac] primary authentication 10.1.1.1 49
# 配置与认证服务器交互报文时的共享密钥为 expert。
[Switch-hwtacacs-hwtac] key authentication simple expert
# 配置向 HWTACACS 服务器发送的用户名不携带域名。
[Switch-hwtacacs-hwtac] user-name-format without-domain
[Switch-hwtacacs-hwtac] quit
# 创建 ISP 域 bbb。
[Switch] domain bbb
# 配置 Telnet 用户登录认证方法为本地认证。
[Switch-isp-bbb] authentication login local
# 配置用户级别切换认证方法为 hwtac。
[Switch-isp-bbb] authentication super hwtacacs-scheme hwtac
[Switch-isp-bbb] quit
# 创建本地 Telnet 用户 test。
[Switch] local-user test
[Switch-luser-test] service-type telnet
[Switch-luser-test] password simple aabbcc
# 指定 Telnet 用户登录系统后所能访问的命令级别为 0 级。
[Switch-luser-test] authorization-attribute level 0
[Switch-luser-test] quit
# 配置用户级别切换认证方式为本地认证时，切换用户级别使用的密码为 654321。
[Switch] super password simple 654321
[Switch] quit

```

(2) 配置 HWTACACS server



说明

下面以 ACSv4.0 为例，说明该例中 HWTACACS server 的基本配置。

在 HWTACACS server 上添加用户 test，对该用户的高级属性进行设置。

- 设置 Enable Password 为 enabpass;
- 设置 Max Privilege 为 Level 3，表示用户级别切换到 1~3 时均使用密码 enabpass 进行认证。

图1-32 设置 Telnet 用户的高级属性

Advanced TACACS+ Settings

TACACS+ Enable Control:

☐ Use Group Level Setting

☐ No Enable Privilege

☒ Max Privilege for any AAA Client

Level 3

TACACS+ Enable Password

☐ Use CiscoSecure PAP password

☐ Use external database password

Windows Database

☒ Use separate password

Password

Confirm Password

TACACS+ Outbound Password
(Used for SendPass and SendAuth clients such as routers)

Password

Confirm Password

5. 验证配置结果

(1) Telnet 用户建立与 Switch 的连接

在 Telnet 客户端按照提示输入用户名 test@bbb 及密码 aabbcc，即可进入 Switch 的用户界面，且所只能访问级别为 0 级的命令。

```
<Switch> telnet 192.168.1.70
Trying 192.168.1.70 ...
Press CTRL+K to abort
Connected to 192.168.1.70 ...
```

```
*****
* Copyright (c) 2004-2011 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
*****
```

Login authentication

Username:test@bbb

Password:

<Switch> ?

User view commands:

```
cluster  Run cluster command
display  Display current system information
ping     Ping function
quit     Exit from current command view
ssh2     Establish a secure shell client connection
super    Set the current user priority level
telnet   Establish one TELNET connection
tracert  Trace route function
```

(2) 切换用户级别

在当前的用户界面下执行切换用户级别到 3 级的命令，按照提示输入 HWTACACS 级别切换认证密码 enabpass，若认证成功即可将当前 Telnet 用户的级别切换到 3 级。

<Switch> super 3

Password:

User privilege level is 3, and only those commands can be used
whose level is equal or less than this.

Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE

若 ACS 服务器无响应，按照提示输入本地级别切换认证密码 654321，若认证成功即可将当前 Telnet 用户的级别切换到 3 级。

<Switch> super 3

Password: <——此处需输入 HWTACACS 级别切换认证密码

Error: Invalid configuration or no response from the authentication server.

Info: Change authentication mode to local.

Password: <——此处需输入本地级别切换认证密码

User privilege level is 3, and only those commands can be used
whose level is equal or less than this.

Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE

1.10.7 设备作为RADIUS服务器对Telnet用户进行接入认证

1. 组网需求

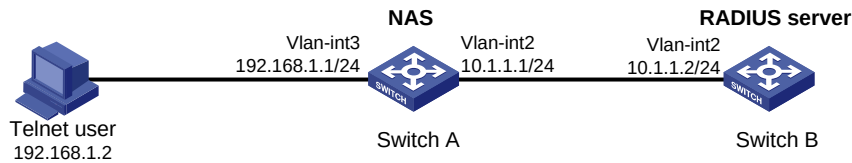
Telnet 用户与 Switch A 相连，Switch A 作为 NAS 对 Telnet 用户进行接入认证。具体要求如下：

- Switch B 作为 RADIUS 服务器对用户进行认证、授权，服务器 IP 地址为 10.1.1.2/24、认证端口号为 1645。

- NAS 与 RADIUS 认证、授权服务器交互报文时的共享密钥均为 abc，向 RADIUS 服务器发送的用户名中不带域名。

2. 组网图

图1-33 设备作为 RADIUS 服务器对 Telnet 用户进行接入认证组网图



3. 配置步骤

配置各接口的 IP 地址，具体配置过程略。

(1) 配置 NAS

开启 Switch A 的 Telnet 服务器功能。

```
<SwitchA> system-view
```

```
[SwitchA] telnet server enable
```

配置 Telnet 用户登录采用 AAA 认证方式。

```
[SwitchA] user-interface vty 0 4
```

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

```
[SwitchA-ui-vty0-4] quit
```

创建 RADIUS 方案 rad。

```
[SwitchA] radius scheme rad
```

配置主认证服务器的 IP 地址为 10.1.1.2，认证端口号为 1645，共享密钥为 abc。

```
[SwitchA-radius-rad] primary authentication 10.1.1.2 1645 key abc
```

配置发送给 RADIUS 服务器的用户名不带 ISP 域名。

```
[SwitchA-radius-rad] user-name-format without-domain
```

配置发送 RADIUS 报文使用的源 IP 地址为 10.1.1.1。

```
[SwitchA-radius-rad] nas-ip 10.1.1.1
```

```
[SwitchA-radius-rad] quit
```

创建 ISP 域 bbb。

```
[SwitchA] domain bbb
```

配置 Telnet 用户使用的 RADIUS 认证方案为 rad。

```
[SwitchA-isp-bbb] authentication login radius-scheme rad
```

配置 Telnet 用户使用的 RADIUS 授权方案为 rad。

```
[SwitchA-isp-bbb] authorization login radius-scheme rad
```

配置 Telnet 用户的计费方案为 none。

```
[SwitchA-isp-bbb] accounting login none
```

配置 RADIUS 服务器的服务类型为 **standard**。使用设备作为服务器对 login 用户进行认证时，RADIUS 服务器类型应配置为 **standard**。

```
[SwitchA-isp-bbb] server-type standard
```

```
[SwitchA-isp-bbb] quit
```

配置系统缺省 ISP 域为 bbb，使得用户名中未携带域名的用户可使用 bbb 域进行认证。

```
[SwitchA] domain default enable bbb
```

(2) 配置 RADIUS server

创建名称为 aaa 的 RADIUS 用户，并进入该用户视图。

```
<SwitchB> system-view
```

```
[SwitchB] radius-server user aaa
```

指定用户 aaa 的密码为明文 aabbcc。

```
[SwitchB-rdsuser-aaa] password simple aabbcc
```

```
[SwitchB-rdsuser-aaa] quit
```

配置 RADIUS 客户端 IP 为 10.1.1.1，共享密钥为明文 abc。

```
[SwitchB] radius-server client-ip 10.1.1.1 key simple abc
```

4. 验证配置结果

用户 aaa 向 Switch A 发起 Telnet 连接，按照提示输入用户名 aaa@bbb（或不携带域名的 aaa）及密码 aabbcc 后，可成功通过认证，并进入 Switch A 的用户界面。在 Switch A 上可查看到已在线 Telnet 用户的连接情况。

```
<SwitchA> display connection
```

```
Index=1      ,Username=aaa@bbb
```

```
IP=192.168.1.2
```

```
IPv6=N/A
```

```
Total 1 connection(s) matched.
```

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 服务器之间的存在通信故障。
- (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/授权服务器不是同一台机器，设备却要求认证/授权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/授权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。

目 录

1 802.1X配置	1-1
1.1 802.1X简介	1-1
1.1.1 802.1X的体系结构	1-1
1.1.2 802.1X对端口的控制	1-2
1.1.3 802.1X认证报文的交互机制	1-3
1.1.4 EAP报文的封装	1-4
1.1.5 802.1X的认证触发方式	1-6
1.1.6 802.1X的认证过程	1-6
1.1.7 802.1X的接入控制方式	1-9
1.2 802.1X扩展功能	1-10
1.2.1 支持Tag/Untag VLAN下发	1-10
1.2.2 支持VLAN组下发	1-10
1.2.3 Guest VLAN	1-11
1.2.4 Auth-Fail VLAN	1-12
1.2.5 802.1X认证的Critical VLAN	1-12
1.2.6 支持ACL下发	1-13
1.3 802.1X配置任务简介	1-13
1.4 配置 802.1X	1-14
1.4.1 配置准备	1-14
1.4.2 开启 802.1X特性	1-14
1.4.3 配置 802.1X系统的认证方法	1-15
1.4.4 配置端口的授权状态	1-15
1.4.5 配置端口接入控制方式	1-16
1.4.6 配置端口同时接入用户数的最大值	1-17
1.4.7 配置设备向接入用户发送认证请求报文的最大次数	1-17
1.4.8 配置 802.1X认证超时定时器	1-17
1.4.9 配置在线用户握手功能	1-18
1.4.10 开启认证触发功能	1-19
1.4.11 配置端口的强制认证域	1-20
1.4.12 配置静默功能	1-20
1.4.13 配置重认证功能	1-21
1.4.14 配置端口发送 802.1X协议报文不带Tag	1-21
1.4.15 配置MAC地址认证用户进行 802.1X认证的最大尝试次数	1-22

1.4.16 配置VLAN组	1-22
1.4.17 配置Guest VLAN	1-23
1.4.18 配置Auth-Fail VLAN	1-24
1.4.19 配置Critical VLAN	1-25
1.4.20 配置 802.1X支持的域名分隔符	1-27
1.5 802.1X显示和维护	1-27
1.6 802.1X典型配置举例	1-28
1.6.1 802.1X认证配置举例	1-28
1.6.2 802.1X认证配合Guest VLAN、VLAN下发配置举例	1-31
1.6.3 802.1X认证配合下发ACL配置举例	1-33
2 802.1X支持EAD快速部署配置	2-1
2.1 802.1X支持EAD快速部署简介	2-1
2.1.1 概述	2-1
2.1.2 实现机制	2-1
2.2 配置EAD快速部署	2-1
2.2.1 配置准备	2-1
2.2.2 配置Free IP	2-2
2.2.3 配置用户HTTP访问的重定向URL	2-2
2.2.4 配置EAD规则的老化时间	2-3
2.3 EAD快速部署显示和维护	2-3
2.4 EAD快速部署典型配置举例	2-3
2.5 常见配置错误举例	2-5
2.5.1 用户通过浏览器访问外部网络不能正确重定向	2-5

1 802.1X配置



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。而在仅需要 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”。

1.1 802.1X简介

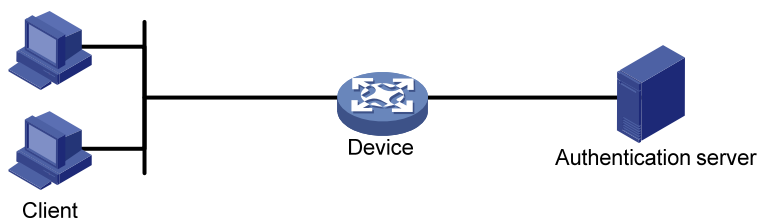
最初，IEEE802 LAN/WAN 委员会为解决无线局域网的网络安全问题，提出了 802.1X 协议。后来，802.1X 协议作为局域网的一个普通接入控制机制在以太网中被广泛应用，主要解决以太网内认证和安全方面的问题。

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设备进行认证，以便用户设备控制对网络资源的访问。

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设备，它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。

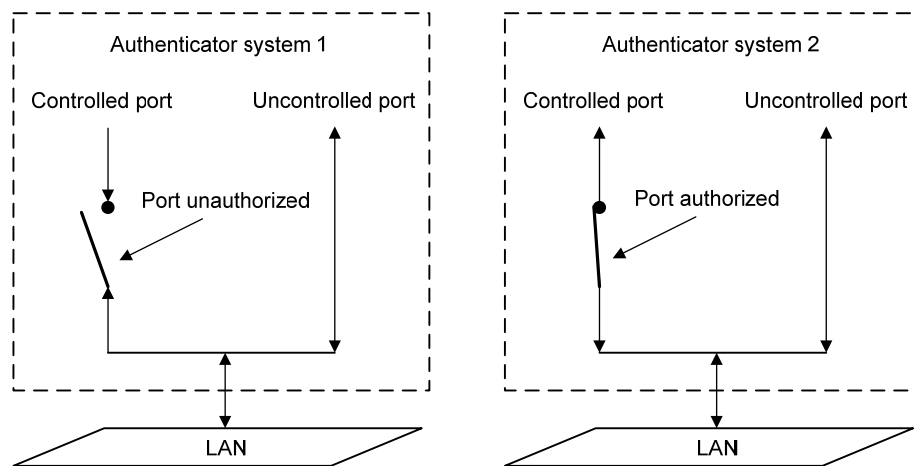
- 非受控端口始终处于双向连通状态，主要用来传递 EAPOL 协议帧，保证客户端始终能够发出或接收认证报文。
- 受控端口在授权状态下处于双向连通状态，用于传递业务报文；在非授权状态下禁止从客户端接收任何报文。

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。

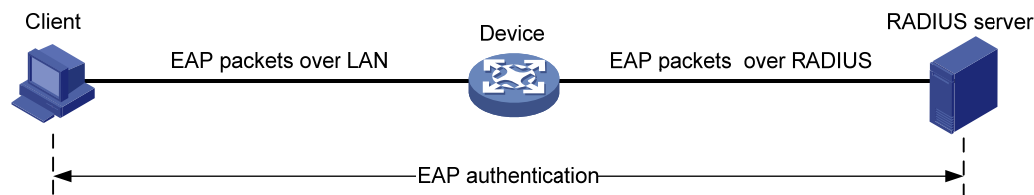
1.1.3 802.1X认证报文的交互机制

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、PEAP 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 报文的交互有以下两种处理机制。

1. EAP中继

设备对收到的 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 服务器进行认证。

图1-3 EAP 中继原理示意图

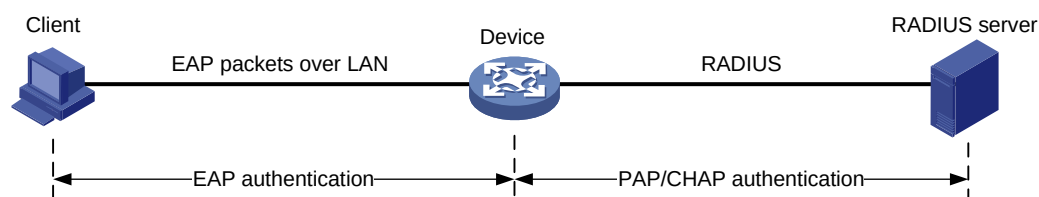


该处理机制下，EAP 认证过程在客户端和 RADIUS 服务器之间进行，RADIUS 服务器作为 EAP 服务器来处理客户端的 EAP 认证请求，设备相当于一个代理，仅对 EAP 报文做中转，因此设备处理简单，并能够支持 EAP 的各种认证方法，但要求 RADIUS 服务器支持相应的 EAP 认证方法。

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，但设备处理较为复杂，它需要作为 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。

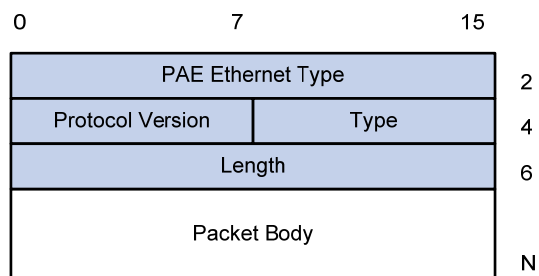
1.1.4 EAP报文的封装

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报文的封装协议，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

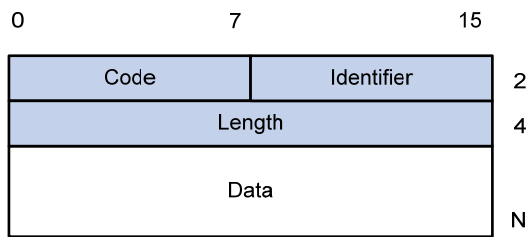
类型值	数据帧类型	说明
0x00	EAP-Packet	认证信息帧，用于承载客户端和设备端之间的EAP报文。 • 在终结方式下，该帧中的客户端认证信息会被设备端重新封装并承载于 RADIUS 报文中发送给认证服务器 • 在中继方式下，该帧承载的 EAP 报文会被设备端直接封装在 RADIUS 报文的 EAP 属性中发送给认证服务器
0x01	EAPOL-Start	认证发起帧，用于客户端向设备端发起认证请求
0x02	EAPOL-Logoff	退出请求帧，用于客户端向设备端发起下线请求

- 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。

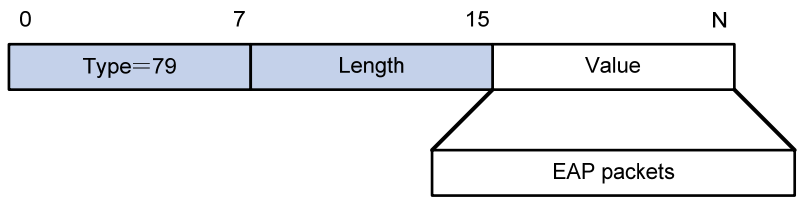
2. EAP报文在RADIUS中的封装

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。

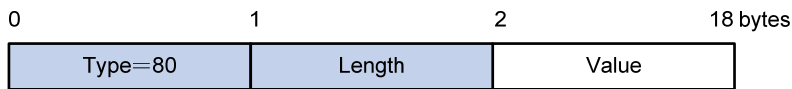
图1-7 EAP-Message 属性封装



(2) Message-Authenticator

如 [图 1-8](#)所示，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，避免报文被篡改。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。

图1-8 Message-Authenticator 属性封装



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，而造成认证设备无法收到客户端认证请求的问题。



说明

目前，iNode 的 802.1X 客户端可支持广播触发方式。

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 N 秒(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

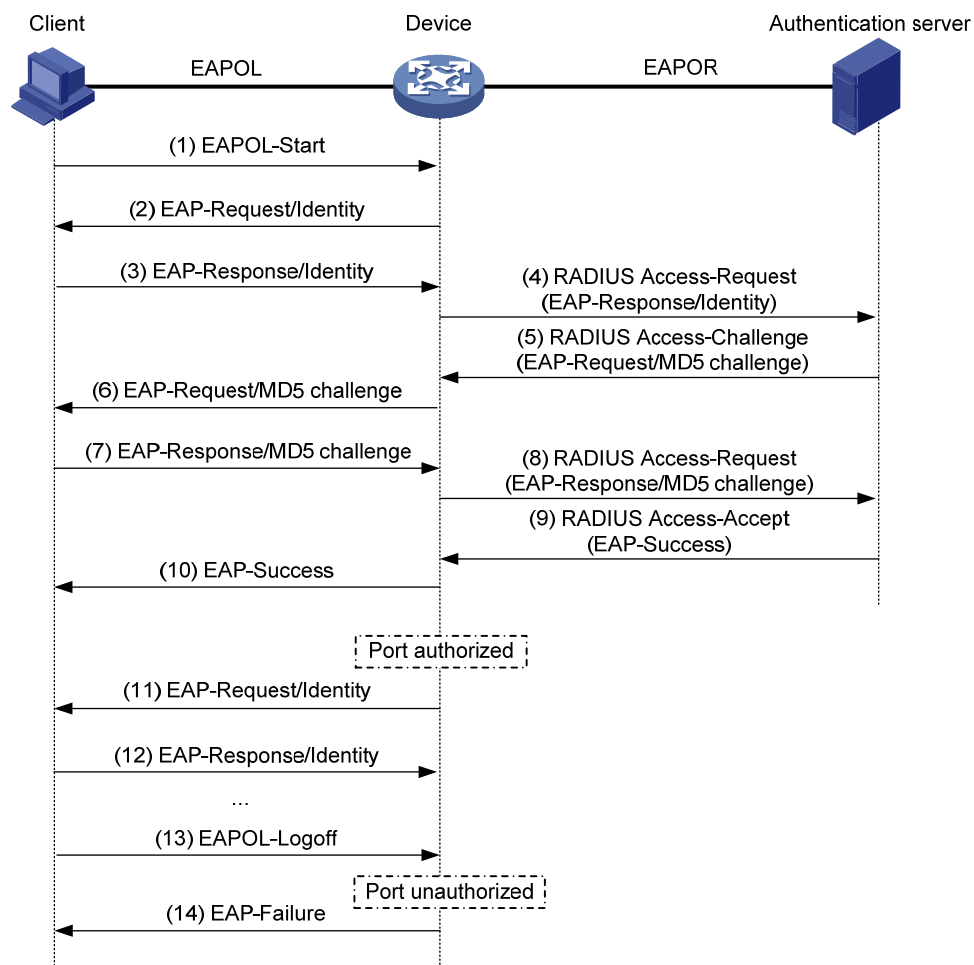
802.1X 系统支持采用 EAP 中继方式或 EAP 终结方式与远端 RADIUS 服务器交互。以下关于两种认证方式的过程描述，都以客户端主动发起认证为例。

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，以便扩展认证协议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，分别用来封装 EAP 报文及对携带 EAP-Message 的 RADIUS 报文进行保护。

下面以MD5-Challenge认证方法为例介绍基本业务流程，认证过程如 [图 1-9](#) 所示。

图1-9 IEEE 802.1X 认证系统的 EAP 中继方式业务流程



- (1) 当用户需要访问外部网络时打开 802.1X 客户端程序,输入已经申请、登记过的用户名和密码,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中对比, 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 对密码部分进行加密处理, 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。
-



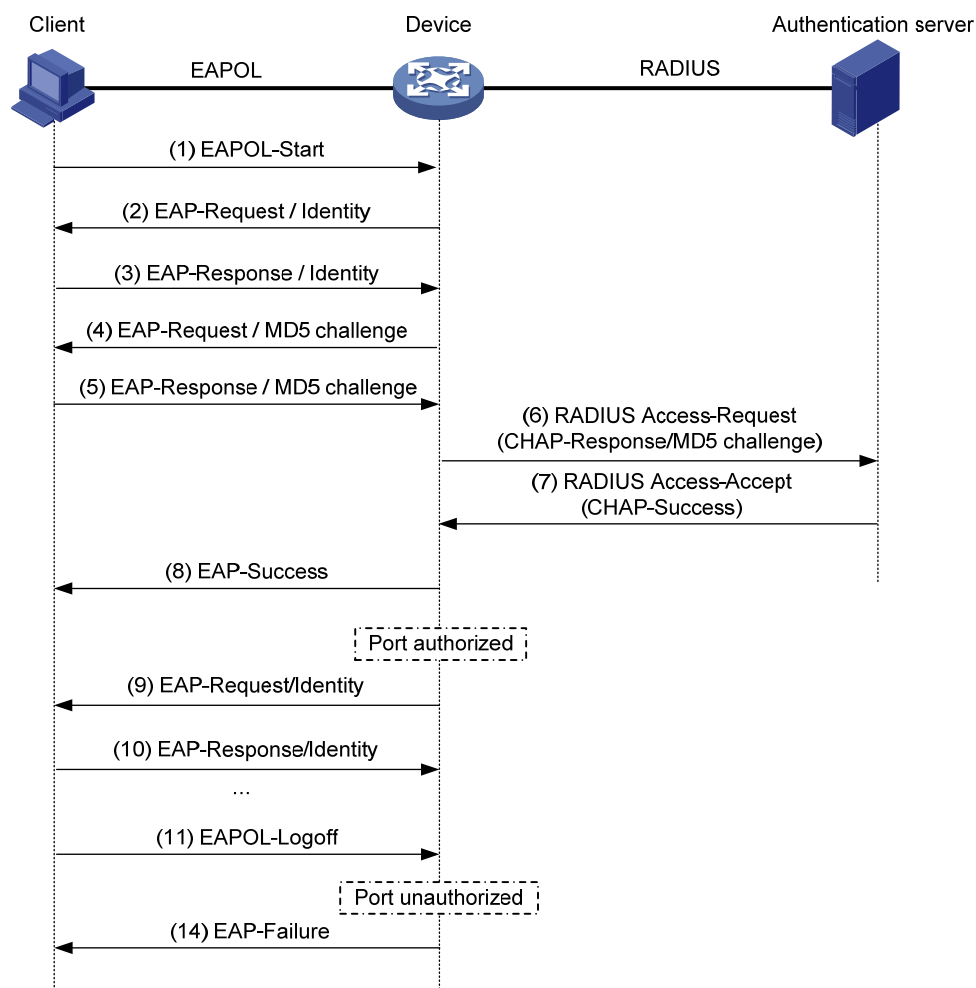
说明

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。下面以CHAP认证方法为例介绍基本业务流程, 如 [图 1-10](#) 所示。

图1-10 IEEE 802.1X 认证系统的 EAP 终结方式业务流程



EAP 终结方式与 EAP 中继方式的认证流程相比，不同之处在于步骤(4)中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）。

- 当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，当某个用户下线时，也只有该用户无法使用网络。

1.2 802.1X扩展功能

1.2.1 支持Tag/Untag VLAN下发

802.1X 用户在服务器上通过认证时，服务器会把授权信息传送给设备端。如果服务器上指定了授权给该用户的 VLAN 以及该 VLAN 的下发方式（Tag 或 Untag），则服务器发送给设备的授权信息中将含有下发的 VLAN 信息，设备根据用户认证上线的端口链路类型，按以下三种情况将端口加入下发 VLAN 中。

表1-2 不同类型的端口加入下发的 VLAN

接入控制方式	Access 端口	Trunk 端口	Hybrid 端口
Port-based	端口离开用户配置的 VLAN，加入下发的VLAN（该VLAN必须为Untag下发的VLAN）	端口允许下发的VLAN通过，并且将缺省VLAN修改为Untag下发的VLAN	端口允许下发的VLAN通过，并且将缺省VLAN修改为Untag下发的VLAN
MAC-based	端口离开用户配置的 VLAN，加入第一个通过认证的用户的下发VLAN（该VLAN必须为Untag下发的VLAN）	端口允许下发的VLAN通过，并且将缺省VLAN修改为为第一个通过认证的用户Untag下发的VLAN	端口允许下发的VLAN通过 - 若端口上开启了 MAC VLAN 功能，则根据下发的 VLAN 动态地创建基于用户 MAC 的 VLAN，而端口的缺省 VLAN ID 并不改变 - 若端口上未开启 MAC VLAN 功能，则端口的缺省 VLAN ID 修改为为第一个通过认证的用户 Untag 下发的 VLAN 的 VLAN ID

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

说明

- 对于 Access 端口，不支持下发带 Tag 的 VLAN。
- 对于 Trunk 端口和 Hybrid 端口，若服务器下发的是带 Tag 的 VLAN，不改变该端口的缺省 VLAN。
- 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 支持VLAN组下发

802.1X 用户在服务器上通过认证时，服务器会把授权信息传送给设备端。如果服务器上指定了授权给该用户的下发 VLAN，则服务器发送给设备的授权信息中将含有下发的 VLAN 信息，设备将用户认证上线的端口加入到下发的 VLAN 中。

支持 VLAN 下发功能下发的是 VLAN ID 或 VLAN 名，仅支持下发特定的 VLAN。而支持 VLAN 组下发功能可以在设备上配置 VLAN 组，认证服务器下发 VLAN 组名，认证服务器下发 VLAN 组名后，接入设备选择该 VLAN 组中的一个 VLAN ID 作为授权 VLAN。

接入设备从 VLAN 组中选择授权 VLAN ID 的原则：

- (1) 优先选择 VLAN 下成员用户少的 VLAN 做当前用户的授权 VLAN；
- (2) 如果 VLAN 下成员用户一样多，首先查询到的 VLAN（按 VLAN ID 从小到大的查询顺序）作为当前用户的授权 VLAN。

举例如下：VLAN 组内包括 VLAN2、VLAN3 两个 VLAN ID，如果已有 3 个用户认证成功后授权 VLAN 3，有 2 个用户认证成功后授权 VLAN 2，那么接下来认证成功用户，则授权 VLAN 2。

通过下发 VLAN 组，可以均衡每个 VLAN 下的用户数，用于减少 VLAN 内广播报文，提高效率。

1.2.3 Guest VLAN

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。根据端口的接入控制方式不同，Guest VLAN 的生效情况有所不同。

(1) 端口的接入控制方式为 Port-based

在接入控制方式为 Port-based 的端口上配置 Guest VLAN 后，若在一定的时间内（默认 90 秒），该端口上无客户端进行认证，则该端口将被加入 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。不同链路类型的端口加入 Guest VLAN 的情况有所不同，具体情况与端口加入服务器下发的 VLAN 类似，请参见“[1.2.1 支持 Tag/Untag VLAN 下发](#)”。

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“[1.2.4 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 回到初始 VLAN 中，该初始 VLAN 为端口加入 Guest VLAN 之前所在的 VLAN。
- 若认证服务器未下发 VLAN，则端口回到初始 VLAN 中。用户下线后，端口仍在该初始 VLAN 中。

(2) 端口的接入控制方式为 MAC-based

在接入控制方式为 MAC-based 的端口上配置 Guest VLAN 后，端口上未认证的用户被授权访问 Guest VLAN 里的资源。

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，则认证失败的用户将被加入 Auth-Fail VLAN；如果端口未配置 Auth-Fail VLAN，则该用户将仍然处于 Guest VLAN 内。

当端口上处于 Guest VLAN 中的用户发起认证且成功时，设备会根据认证服务器是否下发 VLAN 决定将该用户加入到下发的 VLAN 中，或回到加入 Guest VLAN 之前端口所在的初始 VLAN。

1.2.4 Auth-Fail VLAN

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。

根据端口的接入控制方式不同，Auth-Fail VLAN 的生效情况有所不同。

(1) 端口的接入控制方式为 Port-based

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 的情况与加入授权下发 VLAN 相同，与端口链路类型有关。

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 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，端口会离开下发的 VLAN 回到初始 VLAN 中，该初始 VLAN 为端口加入 Auth-Fail VLAN 之前所在的 VLAN。
- 若认证服务器未下发 VLAN，则端口回到初始 VLAN 中。用户下线后，端口仍在该初始 VLAN 中。

(2) 端口的接入控制方式为 MAC-based

在接入控制方式为 MAC-based 的端口上配置 Auth-Fail VLAN 后，该端口上认证失败的用户将被授权访问 Auth-Fail VLAN 里的资源。

当 Auth-Fail VLAN 中的用户再次发起认证时，如果认证成功，则设备会根据认证服务器是否下发 VLAN 决定将该用户加入到下发的 VLAN 中，或回到加入 Auth-Fail VLAN 之前端口所在的初始 VLAN；如果认证失败，则该用户仍然留在该 VLAN 中。

1.2.5 802.1X认证的Critical VLAN

802.1X 认证的 Critical VLAN 功能允许用户在进行 802.1X 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 802.1X 认证的 Critical VLAN。

1. 端口加入 802.1X认证的Critical VLAN

根据端口的接入控制方式不同，Critical VLAN 的生效情况有所不同。

(1) 端口的接入控制方式为 Port-based

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。端口加入 Critical VLAN 的情况与加入授权下发 VLAN 相同，与端口链路类型有关。

(2) 端口的接入控制方式为 MAC-based

在接入控制方式为 MAC-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，则端口将允许 Critical VLAN 通过，用户将被授权访问 Critical VLAN 里的资源。

2. 端口退出 802.1X认证的Critical VLAN

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；如果满足以下任意一个条件，端口将会离开 Critical VLAN：

- 认证用户的 ISP 域中新增认证服务器（且该服务器可达）。
- 配置了 RADIUS 认证服务器探测功能，且探测结果表示某认证服务器可达。
- 收到 RADIUS 服务器回应报文。

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 VLAN，则端口加入下发的 VLAN 中。用户下线后，端口会离开下发的 VLAN 回到初始 VLAN 中，该初始 VLAN 为端口加入 Critical VLAN 之前所在的 VLAN。
- 若认证服务器未下发 VLAN，则端口回到初始 VLAN 中。用户下线后，端口仍在该初始 VLAN 中。



说明

- 只采用 RADIUS 认证方式的情况下，在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。
- RADIUS 服务器相关的配置请参见“安全配置指导”中的“AAA”。

1.2.6 支持ACL下发

802.1X 支持 ACL（Access Control List，访问控制列表）下发功能提供了对上线用户访问网络资源的过滤与控制功能。当用户上线时，如果 RADIUS 服务器上指定了要下发给该用户的授权 ACL，则设备会根据服务器下发的授权 ACL 对用户所在端口的数据流进行过滤，仅允许 ACL 规则中允许的数据流通过该端口。由于服务器上指定的是授权 ACL 的编号，因此还需要在设备上创建该 ACL 并配置该对应的 ACL 规则。管理员可以通过改变服务器的授权 ACL 设置或设备上对应的 ACL 规则来改变用户的访问权限。

1.3 802.1X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	1.4.2
配置802.1X系统的认证方法	若采用EAP中继模式， 则必选 若采用EAP终结模式， 则可选	1.4.3
配置端口的授权状态	可选	1.4.4
配置端口接入控制方式	可选	1.4.5
配置端口同时接入用户数的最大值	可选	1.4.6
配置设备向接入用户发送认证请求报文的最大次数	可选	1.4.7
配置802.1X认证超时定时器	可选	1.4.8

配置任务	说明	详细配置
配置在线用户握手功能	可选	1.4.9
开启认证触发功能	可选	1.4.10
配置端口的强制认证域	可选	1.4.11
配置静默功能	可选	1.4.12
配置重认证功能	可选	1.4.13
配置端口发送802.1X协议报文不带Tag	可选	1.4.14
配置MAC地址认证用户进行802.1X认证的最大尝试次数	可选	1.4.15
配置VLAN组	可选	1.4.16
配置Guest VLAN	可选	1.4.17
配置Auth-Fail VLAN	可选	1.4.18
配置Critical VLAN	可选	1.4.19
配置802.1X支持的域名分隔符	可选	1.4.20

1.4 配置802.1X

1.4.1 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**。

1.4.2 开启 802.1X特性



说明

- 在用户端设备发送不携带 Tag 数据流的情况下，若接入端口配置了 Voice VLAN 功能，则端口的 802.1X 功能不生效。关于 Voice VLAN 特性请参见“二层技术-以太网交换配置指导”中的“Voice VLAN”。
- 端口启动 802.1X 与端口加入聚合组及端口加入业务环回组互斥。
- 端口开启 BPDU 拦截功能后，对收到的 802.1X 报文会进行丢弃，因此请不要同时开启端口的 BPDU 拦截功能和 802.1X 功能。

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

表1-4 开启 802.1X 特性

配置步骤		命令	说明
进入系统视图		system-view	-
开启全局的802.1X特性		dot1x	必选 缺省情况下，全局的802.1X特性为关闭状态
开启端口的802.1X特性	在系统视图下	dot1x interface interface-list	二者必选其一 缺省情况下，端口的802.1X特性为关闭状态
	在以太网端口视图下	interface interface-type interface-number	
		dot1x	

1.4.3 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：

- EAP 中继方式下，设备端对客户端发送的 EAP 报文进行中继处理，设备上需指定 **authentication-method** 为 **eap** 来启用 EAP 中继方式，并支持客户端与 RADIUS 服务器之间所有类型的 EAP 认证方法。
- EAP 终结方式下，设备端对客户端发送的 EAP 报文进行本地终结，设备上需指定 **authentication-method** 为 **chap** 或 **pap** 来启用 EAP 终结方式，并支持与 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 }	可选 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”。

1.4.4 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；如果认证通过，则端口切换到授权状态，允许用户访问网络资源。这也是最常见的情况。

在系统视图和以太网端口视图下均可进行端口授权状态的配置，前者可针对多个端口，后者仅针对当前端口。若在不同视图下先后对同一个端口的授权状态进行了配置，则最后执行的配置生效。

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	-
配置端口的授权状态	在系统视图下	dot1x port-control { authorized-force auto unauthorized-force } [interface interface-list]	二者可选其一 缺省情况下，端口的授权状态为 auto
	在以太网端口视图下	interface interface-type interface-number	
		dot1x port-control { authorized-force auto unauthorized-force }	

1.4.5 配置端口接入控制方式

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**）。在系统视图和以太网端口视图下均可进行端口接入控制方式的配置，前者可针对多个端口，后者仅针对当前端口。若在不同视图下先后对同一个端口的接入控制方式进行了配置，则最后执行的配置生效。

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	-
配置端口接入控制方式	在系统视图下	dot1x port-method { macbased portbased } [interface interface-list]	二者可选其一 缺省情况下，802.1X在端口上进行接入控制方式为 macbased
	在以太网端口视图下	interface interface-type interface-number	
		dot1x port-method { macbased portbased }	



说明

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”。

1.4.6 配置端口同时接入用户数的最大值

在系统视图和以太网端口视图下均可进行端口接入用户数最大值的配置，前者可针对多个端口，后者仅针对当前端口。若在不同视图下先后对同一个端口的最大接入用户数进行了配置，则最后执行的配置生效。

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	-
配置端口同时接入用户数的最大值	在系统视图下	dot1x max-user user-number [interface interface-list]	二者可选其一 缺省情况下，端口同时接入用户数的最大值为2048
	在以太网端口视图下	interface interface-type interface-number	
		dot1x max-user user-number	

1.4.7 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，在规定的时间内（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	可选 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

1.4.8 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接入用户、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。

表1-10 配置 802.1X 定时器参数

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 <i>supp-timeout-value</i>	可选 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 <i>server-timeout-value</i>	可选 缺省情况下，认证服务器超时定时器的值为100秒



说明

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。

1.4.9 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：在线用户握手安全功能的实现依赖于在线用户握手功能。为使在线用户握手安全功能生效，请保证在线用户握手功能处于开启状态。

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	-
配置握手定时器	dot1x timer handshake-period <i>handshake-period-value</i>	可选 缺省情况下，握手定时器的值为15秒
进入以太网端口视图	interface interface-type <i>interface-number</i>	-
开启在线用户握手功能	dot1x handshake	可选 缺省情况下，在线用户握手功能处于开启状态

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



说明

- 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。
- 建议在线用户握手安全功能与 iNode 客户端以及 iMC 服务器配合使用，以保证该功能可以正常运行。

1.4.10 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。该功能用于支持不能主动发起认证的客户端。
- 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）。该功能适用于客户端不支持主动认证，且仅部分客户端需要进行认证的组网环境，可避免不希望认证或已认证的客户端收到多余的认证触发报文。

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	-
配置用户名请求超时定时器	dot1x timer tx-period tx-period-value	可选 缺省情况下，用户名请求超时定时器的值为30秒
进入以太网端口视图	interface interface-type interface-number	-
开启认证触发功能	dot1x { multicast-trigger unicast-trigger }	可选 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



说明

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。

1.4.11 配置端口的强制认证域

配置端口的强制认证域（mandatory domain）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	-
进入以太网端口视图	interface <i>interface-type interface-number</i>	-
配置端口的强制认证域	dot1x mandatory-domain <i>domain-name</i>	必选 缺省情况下，未定义强制认证域

1.4.12 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，设备不进行 802.1X 认证的相关处理。

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	-
配置静默定时器	dot1x timer quiet-period <i>quiet-period-value</i>	可选 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	必选 缺省情况下，静默定时器功能处于关闭状态



说明

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。

1.4.13 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、User Profile）。

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	-
配置周期性重认证定时器	dot1x timer reauth-period <i>reauth-period-value</i>	可选 缺省情况下，周期性重认证定时器的值为3600秒
进入以太网端口视图	interface <i>interface-type</i> <i>interface-number</i>	-
开启周期性重认证功能	dot1x re-authenticate	必选 缺省情况下，周期性重认证功能处于关闭状态



说明

- 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内容的 VLAN；但是，若重认证前端口下发了 VLAN，而重认证后未下发 VLAN，则重认证失败，用户下线，反之同样处理。
- 当端口向在线的 802.1X 用户发起重认证或者重认证过程中发现没有可达的服务器时，如果该端口上配置了 Critical VLAN，则重认证将会中止，用户保持在线；如果端口上没有配置 Critical VLAN，则在线用户将会下线。

1.4.14 配置端口发送 802.1X协议报文不带Tag

EAPOL 是 802.1X 协议定义的一种承载 EAP 报文的封装协议，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。由于 EAPOL 封装不带 VLAN Tag，因此若服务器上指定了授权给用户的 VLAN 以带 Tag 的方式下发，为了保证 802.1X 协议报文在用户与设备之间正常交互，需要在设备连接用户的端口上配置端口发送 802.1X 协议报文不带 Tag 功能。

表1-16 配置端口发送 802.1X 协议报文不带 Tag

配置步骤	命令	说明
进入系统视图	system-view	-
进入二层以太网端口视图	interface <i>interface-type</i> <i>interface-number</i>	-
配置端口发送802.1X协议报文不带Tag	dot1x eapol untag	可选 缺省情况下，端口发送的802.1X协议报文是否携带Tag由端口配置决定

1.4.15 配置MAC地址认证用户进行 802.1X认证的最大尝试次数

当端口上开启了 MAC 地址认证和 802.1X 认证的情况下，若已经通过 MAC 地址认证的客户端向设备发送了 EAP 报文请求进行 802.1X 认证，缺省情况下，设备允许其进行 802.1X 认证。若该用户通过了 802.1X 认证，则以 802.1X 用户的身份上线；若该用户未通过 802.1X 认证，则后续可能还会进行多次 802.1X 认证尝试（取决于客户端配置）。若设备并不希望此类用户多次进行无意义的 802.1X 认证尝试，则可以通过本命令限制认证失败的次数。

表1-17 配置 MAC 地址认证用户进行 802.1X 认证的最大尝试次数

操作	命令	说明
进入系统视图	system-view	-
进入二层以太网端口视图	interface <i>interface-type</i> <i>interface-number</i>	-
配置MAC地址认证用户进行802.1X认证的最大尝试次数	dot1x attempts max-fail <i>unsuccessful-attempts</i>	必选

1.4.16 配置VLAN组

VLAN 组由用户创建生成，用户可将多个 VLAN ID 加入同一个 VLAN 组中。

表1-18 配置 VLAN 组

操作	命令	说明
进入系统视图	system-view	-
创建VLAN组，并进入VLAN组视图	vlan-group <i>group-name</i>	必选 缺省情况下，不存在VLAN组
添加VLAN到指定VLAN组中	vlan-list <i>vlan-list</i>	必选 缺省情况下，VLAN组里没有VLAN成员



说明

如果将配置为 Super VLAN 的 VLAN 配置为 VLAN 组成员，那么在用户认证成功后，从 VLAN 组中选择授权 VLAN 时，设备将自动忽略此 VLAN。

1.4.17 配置 Guest VLAN



注意

- 配置 Guest VLAN 时，请不要同时使能 **ip verify source dot1x** 命令，以免造成用户不能正常访问该 VLAN 中的资源，关于 **ip verify source dot1x** 命令详细内容请参见“安全命令参考”中的“IP Source Guard”。
- 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 Guest VLAN，为保证各种功能的正常使用，请为 Voice VLAN、端口的缺省 VLAN 和 802.1X 的 Guest VLAN 分配不同的 VLAN ID。
- 如果某个 VLAN 被指定为 Super VLAN，则该 VLAN 不能被指定为某个端口的 Guest VLAN；同样，如果某个 VLAN 被指定为某个端口的 Guest VLAN，则该 VLAN 不能被指定为 Super VLAN。关于 Super VLAN 的详细内容请参见“二层技术-以太网交换配置指导”中的“Super VLAN”。

配置 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。
- 在接入控制方式为 MAC-based 的端口上，保证端口类型为 Hybrid，端口上的 MAC VLAN 功能处于使能状态，且不建议将指定的 Guest VLAN 修改为携带 Tag 的方式。MAC VLAN 功能的具体配置请参考“二层技术-以太网交换配置指导”中的“VLAN”。

表1-19 配置 Guest VLAN

配置步骤		命令	说明
进入系统视图		system-view	-
配置指定端口的 Guest VLAN	在系统视图下	dot1x guest-vlan guest-vlan-id [interface interface-list]	二者必选其一 缺省情况下，端口没有配置 Guest VLAN 不同的端口可以配置不同的 Guest VLAN，但一个端口最多只能配置一个 Guest VLAN
	在以太网端口视图下	interface interface-type <i>interface-number</i>	
		dot1x guest-vlan guest-vlan-id	



说明

- 802.1X 认证过程中，当 802.1X 客户端无法在设备给其分配的 VLAN 发生变化时（加入或离开 802.1X 的授权 VLAN、Guest VLAN、Auth-Fail VLAN 或 Critical VLAN）触发自身的 IP 地址更新，建议用户通过释放 IP 或修复网络连接的方式解决这个问题。H3C iNode 客户端没有此问题。
- 在接入控制方式为 MAC-based 的端口上同时配置了 802.1X 认证的 Guest VLAN 与 MAC 地址认证的 Guest VLAN 时，则仅 802.1X 认证的 Guest VLAN 有效，即用户触发 MAC 地址认证且失败后，不会加入 MAC 地址认证的 Guest VLAN，若未触发或者未成功通过 802.1X 认证，则将始终处于 802.1X 认证的 Guest VLAN 中（若端口上还配置了 802.1X 认证的 Auth-Fail VLAN，则用户认证失败后加入 Auth-Fail VLAN）。关于 MAC 地址认证 Guest VLAN 的介绍请参见“安全配置指导”中的“MAC 地址认证”。
- 在接入控制方式为 MAC-based 的端口上生成的 Guest VLAN 表项会覆盖已生成的阻塞 MAC 表项，但如果端口因检测到非法报文而关闭，则 802.1X 的 Guest VLAN 功能无法生效。关于端口入侵检测关闭功能的具体介绍请参见“安全配置指导”中的“端口安全”。

1.4.18 配置Auth-Fail VLAN



注意

- 配置 Auth-Fail VLAN 时，请不要同时使能 **ip verify source dot1x** 命令，以免造成用户不能正常访问该 VLAN 中的资源，关于 **ip verify source dot1x** 命令详细内容请参见“安全命令参考”中的“IP Source Guard”。
- 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 Auth-Fail VLAN，为保证各种功能的正常使用，请为 Voice VLAN、端口的缺省 VLAN 和 802.1X 的 Auth-Fail VLAN 分配不同的 VLAN ID。
- 如果某个 VLAN 被指定为 Super VLAN，则该 VLAN 不能被指定为某个端口的 Auth-Fail VLAN；同样，如果某个 VLAN 被指定为某个端口的 Auth-Fail VLAN，则该 VLAN 不能被指定为 Super VLAN。关于 Super VLAN 的详细内容请参见“二层技术-以太网交换配置指导”中的“Super VLAN”。

配置 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。
- 在接入控制方式为 MAC-based 的端口上，保证端口类型为 Hybrid，端口上的 MAC VLAN 功能处于使能状态，且不建议将指定的 Auth-Fail VLAN 修改为携带 Tag 的方式。MAC VLAN 功能的具体配置请参考“二层技术-以太网交换配置指导”中的“VLAN”。

表1-20 配置 Auth-Fail VLAN

配置步骤	命令	说明
进入系统视图	system-view	-

配置步骤	命令	说明
进入以太网端口视图	interface <i>interface-type interface-number</i>	-
配置指定端口的Auth-Fail VLAN	dot1x auth-fail vlan <i>authfail-vlan-id</i>	必选 缺省情况下，端口没有配置Auth-Fail VLAN 不同的端口可以配置不同的Auth-Fail VLAN，但一个端口最多只能配置一个Auth-Fail VLAN

说明

- 802.1X 认证过程中，当 802.1X 客户端无法在设备给其分配的 VLAN 发生变化时（加入或离开 802.1X 的授权 VLAN、Guest VLAN、Auth-Fail VLAN 或 Critical VLAN）触发自身的 IP 地址更新，建议用户通过释放 IP 或修复网络连接的方式解决这个问题。H3C iNode 客户端没有此问题。
- 在接入控制方式为 MAC-based 的端口上同时配置了 802.1X 认证 Auth-Fail VLAN 与 MAC 地址认证的 Guest VLAN 时，若用户首先进行 MAC 地址认证且失败，则加入 MAC 地址认证的 Guest VLAN 中，之后若该用户再进行 802.1X 认证且失败，则会离开 MAC 地址认证的 Guest VLAN 而加入 802.1X 认证的 Auth-Fail VLAN 中；若用户首先进行 802.1X 认证且失败，之后除非成功通过 MAC 地址认证或者 802.1X 认证，否则会一直位于 802.1X 认证的 Auth-Fail VLAN 中。
- 在接入控制方式为 MAC-based 的端口上生成的 Auth-Fail VLAN 表项会覆盖已生成的阻塞 MAC 表项，但如果端口因检测到非法报文而关闭，则 802.1X 的 Auth-Fail VLAN 功能无法生效。关于端口入侵检测关闭功能的具体介绍请参见“安全配置指导”中的“端口安全”。

1.4.19 配置Critical VLAN

注意

- 配置 Critical VLAN 时，请不要同时使能 **ip verify source dot1x** 命令，以免造成用户不能正常访问该 VLAN 中的资源，关于 **ip verify source dot1x** 命令详细内容请参见“安全命令参考”中的“IP Source Guard”。
- 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 Critical VLAN，为保证各种功能的正常使用，请为 Voice VLAN、端口的缺省 VLAN 和 802.1X 的 Critical VLAN 分配不同的 VLAN ID。
- 如果某个 VLAN 被指定为 Super VLAN，则该 VLAN 不能被指定为某个端口的 Critical VLAN；同样，如果某个 VLAN 被指定为某个端口的 Critical VLAN，则该 VLAN 不能被指定为 Super VLAN。关于 Super VLAN 的详细内容请参见“二层技术-以太网交换配置指导”中的“Super VLAN”。

配置 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。
- 在接入控制方式为 MAC-based 的端口上，保证端口类型为 Hybrid，端口上的 MAC VLAN 功能处于使能状态，且不建议将指定的 Critical VLAN 修改为携带 Tag 的方式。MAC VLAN 功能的具体配置请参考“二层技术-以太网交换配置指导”中的“VLAN”。

当端口加入 Critical VLAN 后，如果发现有认证服务器可达，可通过配置端口的恢复动作为 **reinitialize** 来通知 802.1X 客户端进行认证。根据端口的接入控制方式不同，具体实现有所不同：

- 接入控制方式为 MAC-based 时，当发现有认证服务器可达后，处于 Critical VLAN 的端口会主动向已加入 Critical VLAN 的 MAC 地址发送单播报文触发其进行 802.1X 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。

表1-21 配置 Critical VLAN

配置步骤	命令	说明
进入系统视图	system-view	-
进入二层以太网端口视图	interface interface-type interface-number	-
配置指定端口的Critical VLAN	dot1x critical vlan vlan-id	必选 缺省情况下，端口没有配置 Critical VLAN 不同的端口可以配置不同的 Critical VLAN，但一个端口最多只能配置一个Critical VLAN
配置指定端口的恢复动作	dot1x critical recovery-action reinitialize	可选 缺省情况下，设备检测到服务器恢复为可达状态后，端口仅仅离开Critical VLAN，不会对用户主动进行认证



说明

- 802.1X 认证过程中，当 802.1X 客户端无法在设备给其分配的 VLAN 发生变化时（加入或离开 802.1X 的授权 VLAN、Guest VLAN、Auth-Fail VLAN 或 Critical VLAN）触发自身的 IP 地址更新，建议用户通过释放 IP 或修复网络连接的方式解决这个问题。H3C iNode 客户端没有此问题。
- 若端口已经位于 802.1X 的 Guest VLAN 或 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 Critical VLAN。
- 若端口已经位于 MAC 地址认证的 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 Critical VLAN。

1.4.20 配置 802.1X支持的域名分隔符

设备对用户的管理是基于 ISP 域的，每个接入用户都属于一个 ISP 域。用户所属的 ISP 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，则设备仅将第一个出现的域名分隔符识别为实际使用的域名分隔符，其它字符都被认为是域名中的一部分，例如，用户输入的用户名为 123/22\@abc，则认为纯用户名为 123，域名分隔符为/，域名为 22\@abc。

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，则使用系统中的强制认证域或缺省域对该用户进行认证。

表1-22 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	可选 缺省情况下，仅支持域名分隔符@



说明

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中携带该用户输入的域名（若原始用户名携带域名），或携带最终使用的认证域的域名（若原始用户名中未携带域名），并采用设备上指定的 802.1X 支持的域名分隔符，若设备上指定了多个域名分隔符，则选择的优先级由高到低依次为@、/、\。另外，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。相关命令的具体介绍请参考“安全命令参考”中的“AAA”。

1.5 802.1X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1-23 802.1X 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-list] [{ begin exclude include } regular-expression]
清除802.1X的统计信息	reset dot1x statistics [interface interface-list]

1.6 802.1X典型配置举例

1.6.1 802.1X认证配置举例

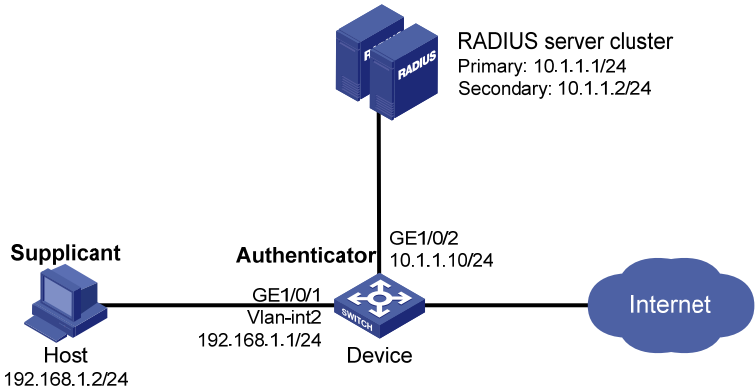
1. 组网需求

用户通过 Device 的端口 GigabitEthernet1/0/1 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 GigabitEthernet1/0/1 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；计费时，如果 RADIUS 计费失败则切断用户连接使其下线。
- 所有接入用户都属于同一个 ISP 域 aabbcc.net，该域中最多可容纳 30 个用户。
- 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
```

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

```
[Device-luser-localuser] password simple localpass
```

启动闲置切断功能,并指定正常连接时用户空闲时间超过 20 分钟,则切断其连接。

```
[Device-luser-localuser] authorization-attribute idle-cut 20
```

```
[Device-luser-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 name
```

```
[Device-radius-radius1] key accounting 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 **aabbcc.net** 并进入其视图。

```
[Device] domain aabbcc.net
```

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-aabbcc.net] authentication lan-access radius-scheme radius1 local
```

```
[Device-isp-aabbcc.net] authorization lan-access radius-scheme radius1 local
```

```
[Device-isp-aabbcc.net] accounting lan-access radius-scheme radius1 local
```

配置该域最多可容纳 30 个用户。

```
[Device-isp-aabbcc.net] access-limit enable 30
```

启动闲置切断功能,并指定正常连接时用户空闲时间超过 20 分钟,则切断其连接。

```
[Device-isp-aabbcc.net] idle-cut enable 20
```

```
[Device-isp-aabbcc.net] quit
```

指定域 **aabbcc.net** 为缺省的 ISP 域。如果用户在登录时没有提供 ISP 域名,系统将把它归于该缺省的 ISP 域。

```
[Device] domain default enable aabbcc.net
```

(5) 配置 802.1X

开启全局 802.1X 特性。

```
[Device] dot1x
```

开启指定端口 **GigabitEthernet1/0/1** 的 802.1X 特性。

```
[Device] interface gigabitethernet 1/0/1
```

```
[Device-GigabitEthernet1/0/1] dot1x
```

```
[Device-GigabitEthernet1/0/1] quit
```

配置基于 MAC 地址的接入控制方式 (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] dot1x port-method macbased interface gigabitethernet 1/0/1
```

4. 验证配置结果

使用命令 **display dot1x interface gigabitethernet 1/0/1** 可以查看 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通过 RADIUS 认证上线后,可使用命令 **display connetion** 查看到上线用户的连接情况。若 RADIUS 服务器无响应,则进行本地认证。

1.6.2 802.1X认证配合Guest VLAN、VLAN下发配置举例

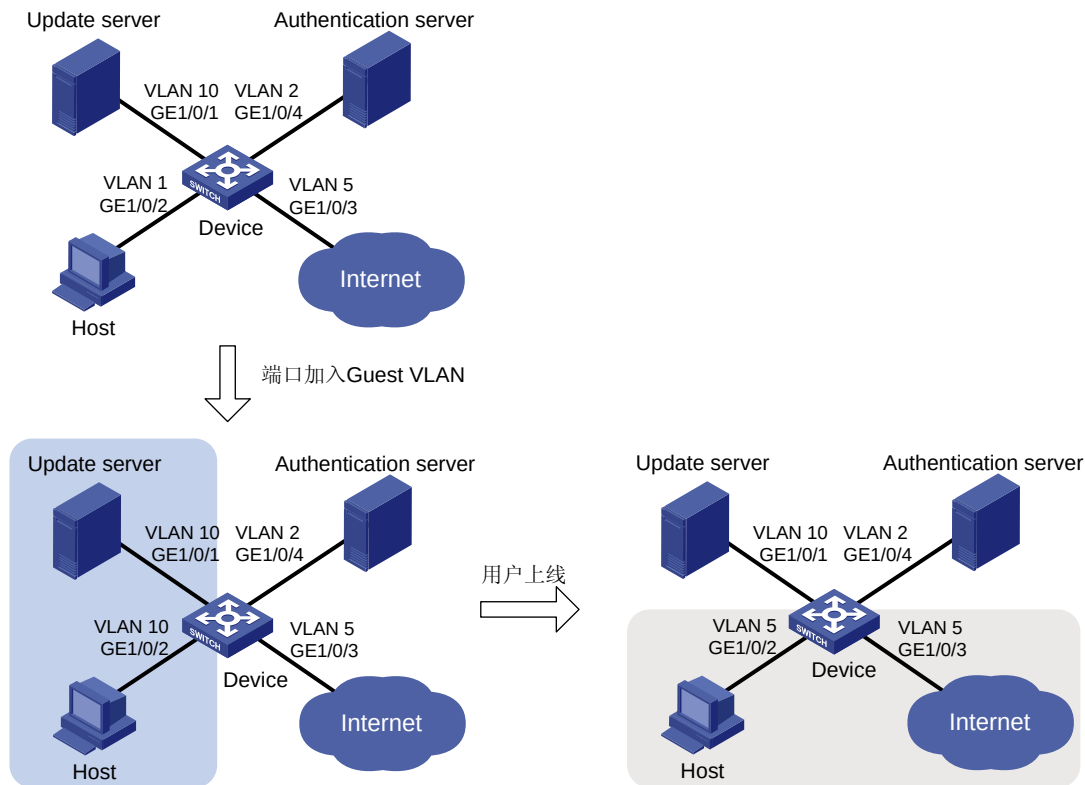
1. 组网需求

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GigabitEthernet1/0/2 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 GigabitEthernet1/0/3 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 GigabitEthernet1/0/2 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 GigabitEthernet1/0/3 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 1/0/2
[Device-vlan1] quit
[Device] vlan 10
[Device-vlan10] port gigabitethernet 1/0/1
[Device-vlan10] quit
[Device] vlan 2
[Device-vlan2] port gigabitethernet 1/0/4
[Device-vlan2] quit
[Device] vlan 5
[Device-vlan5] port gigabitethernet 1/0/3
[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 abc
[Device-radius-2000] key accounting 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

开启全局 802.1X 特性。

```
[Device] dot1x
```

开启指定端口的 802.1X 特性。

```
[Device] interface gigabitethernet 1/0/2
```

```
[Device-GigabitEthernet1/0/2] dot1x
```

配置端口上进行接入控制的方式为 **portbased**。

```
[Device-GigabitEthernet1/0/2] dot1x port-method portbased
```

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

```
[Device-GigabitEthernet1/0/2] dot1x port-control auto
```

```
[Device-GigabitEthernet1/0/2] quit
```

配置指定端口的 Guest VLAN。

```
[Device] dot1x guest-vlan 10 interface gigabitethernet 1/0/2
```

4. 验证配置结果

通过命令 **display dot1x interface gigabitethernet 1/0/2** 可以查看端口 GigabitEthernet1/0/2 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 GigabitEthernet1/0/2 加入了配置的 Guest VLAN。

在用户认证成功之后，通过 **display interface gigabitethernet 1/0/2** 可以看到用户接入的端口 GigabitEthernet1/0/2 加入了认证服务器下发的 VLAN 5 中。

1.6.3 802.1X认证配合下发ACL配置举例

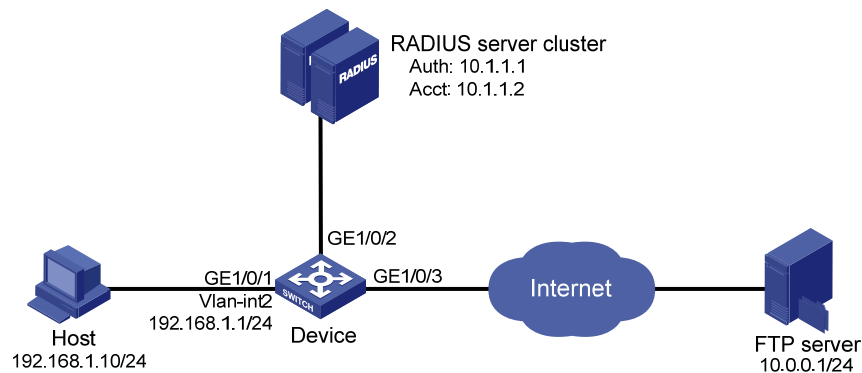
1. 组网需求

用户通过 Device 的端口 GigabitEthernet1/0/1 接入网络，Device 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：

- 使用 RADIUS 服务器 10.1.1.1/24 作为认证/授权服务器，RADIUS 服务器 10.1.1.2/24 作为计费服务器；
- 通过认证服务器下发 ACL，禁止上线的 802.1X 用户在工作日的工作时间（8:00~18:00）访问 IP 地址为 10.0.0.1/24 的 FTP 服务器。

2. 组网图

图1-13 下发 ACL 典型组网图



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,并保证接入端口加入 Guest VLAN 或授权 VLAN 之后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 ACL (本例中为 ACL 3000),并保证用户的认证/授权/计费功能正常运行。

配置各接口的 IP 地址 (略)。

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

配置 ISP 域的 AAA 方法。

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

配置名为 ftp 的时间段,其时间范围为每周工作日的 8 点到 18 点。

```
[Device] time-range ftp 8:00 to 18:00 working-day
```

配置 ACL 3000,拒绝用户在工作日的工作时间内访问 FTP 服务器 10.0.0.1 的报文通过。

```
[Device] acl number 3000
```

```
[Device-acl-adv-3000] rule 0 deny ip destination 10.0.0.1 0 time-range ftp
[Device-acl-adv-3000] quit
# 开启全局 802.1X 特性。
[Device] dot1x
# 开启指定端口的 802.1X 特性。
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x
```

4. 验证配置结果

当用户认证成功上线后，在工作日的工作时间 Ping FTP 服务器。

```
C:\>ping 10.0.0.1
```

```
Pinging 10.0.0.1 with 32 bytes of data:
```

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
Ping statistics for 10.0.0.1:
```

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

由以上过程可知，用户无法 ping 通 FTP 服务器，说明认证服务器下发的 ACL 已对该用户生效。

2 802.1X支持EAD快速部署配置

2.1 802.1X支持EAD快速部署简介

2.1.1 概述

EAD（Endpoint Admission Defense，端点准入防御）作为一个网络端点接入控制方案，它通过安全客户端、安全策略服务器、接入设备以及第三方服务器的联动，加强了对用户的集中管理，提升了网络的整体防御能力。但是在实际的应用过程中 EAD 客户端的部署工作量很大，例如，需要网络管理员手动为每一个 EAD 客户端下载、升级客户端软件，这在 EAD 客户端数目较多的情况下给管理员带来了操作上的不便。

802.1X 认证支持的 EAD 快速部署功能就可以解决以上问题，它允许未通过认证的 802.1X 用户访问一个特定的 IP 地址段，并可以将用户发起的 HTTP 访问请求重定向到该 IP 地址段中的一个指定的 URL，实现用户自动下载并安装 EAD 客户端的目的。

2.1.2 实现机制

802.1X 支持的 EAD 快速部署是通过以下两个功能配合实现的。

1. 未认证用户可访问免认证网段（Free IP）

802.1X 终端用户在认证成功之前，可以访问一个免认证的 IP 地址段，也称为 Free IP。该 IP 地址段中可以配置一个或多个特定服务器，用于提供 EAD 客户端的下载升级或者动态地址分配等服务。

2. 用户HTTP访问URL的重定向

802.1X 终端用户在认证成功之前，如果使用浏览器访问网络，设备会将用户访问的 URL 重定向到已配置的 URL（例如，重定向到 EAD 客户端下载界面），这样只要用户打开浏览器，就必须进入管理员预设的界面。提供重定向 URL 的服务器必须位于用户受限访问的特定网段内。

2.2 配置EAD快速部署



说明

目前，MAC 地址认证和端口安全特性不支持 EAD 的快速部署功能，全局使能 MAC 认证或端口安全功能将会使 EAD 快速部署功能失效。

2.2.1 配置准备

- 开启全局 802.1X 特性
- 开启指定端口的 802.1X 特性，并指定端口的授权模式为 **auto**

2.2.2 配置Free IP

配置 Free IP 之后，EAD 的快速部署功能将立即处于使能状态。未通过认证的 802.1X 终端用户可以访问该 IP 地址段中的网络资源。

表2-1 配置用户可访问的免认证网段

配置步骤	命令	说明
进入系统视图	system-view	-
配置Free IP	dot1x free-ip ip-address { mask-address mask-length }	必选 缺省情况下，未定义Free IP



说明

- MAC 地址认证、端口安全功能均与 Free IP 配置互斥。
- 在同时配置了 Free IP 与 Guest VLAN 功能、Auth-Fail VLAN 功能的情况下，请保证 Free IP 为 Guest VLAN 和 Auth-Fail VLAN 可允许访问的网络资源。这种情况下，用户只能访问 Free IP，不能访问其它资源。
- 未通过 802.1X 认证的用户若要通过外网的 DHCP 服务器动态获得 IP 地址，则需要保证该 DHCP 服务器的 IP 地址在配置的 Free IP 内。

2.2.3 配置用户HTTP访问的重定向URL

终端用户在 802.1X 认证成功之前（包括认证失败）发起的 HTTP 访问请求都会被设备重定向到本命令配置的 URL。

表2-2 配置用户 HTTP 访问的重定向 URL

配置步骤	命令	说明
进入系统视图	system-view	-
配置用户HTTP访问的重定向URL	dot1x url url-string	必选 缺省情况下，未定义重定向URL



说明

- 重定向的 URL 必须处于 Free IP 网段内，否则无法实现重定向。
- 二层 Portal 功能与重定向功能互斥。

2.2.4 配置EAD规则的老化时间

EAD 快速部署功能通过制订 EAD 规则（通常为 ACL 规则）来给予未通过认证的终端用户受限制的网络访问权限，在用户认证成功后，所占用的 ACL 将被释放。由于设备支持的 ACL 数量有限，当大量用户同时上线时，ACL 资源将迅速被占用，如果没有用户认证成功，将出现 ACL 数量不足的情况，这样会导致一部分新接入的用户无法上线。

管理员可以通过配置 EAD 规则的老化时间来控制用户对 ACL 资源的占用，当用户访问网络时该定时器即开始计时，在定时器超时或者用户下载客户端并成功通过认证之后，该用户所占用的 ACL 资源即被删除，这样那些在老化时间内未进行任何操作的用户所占用的 ACL 资源会及时得到释放。在接入用户数量较多时，可以将超时时间适当缩短，以提高 ACL 的使用效率。

表2-3 配置 EAD 规则老化超时时间

配置步骤	命令	说明
进入系统视图	system-view	-
配置EAD规则老化时间	dot1x timer ead-timeout ead-timeout-value	可选 缺省情况下，EAD规则老化时间为30分钟

2.3 EAD快速部署显示和维护

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 EAD 快速部署的运行情况，通过查看显示信息验证配置的效果。

表2-4 EAD 快速部署显示和维护

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-list]

2.4 EAD快速部署典型配置举例

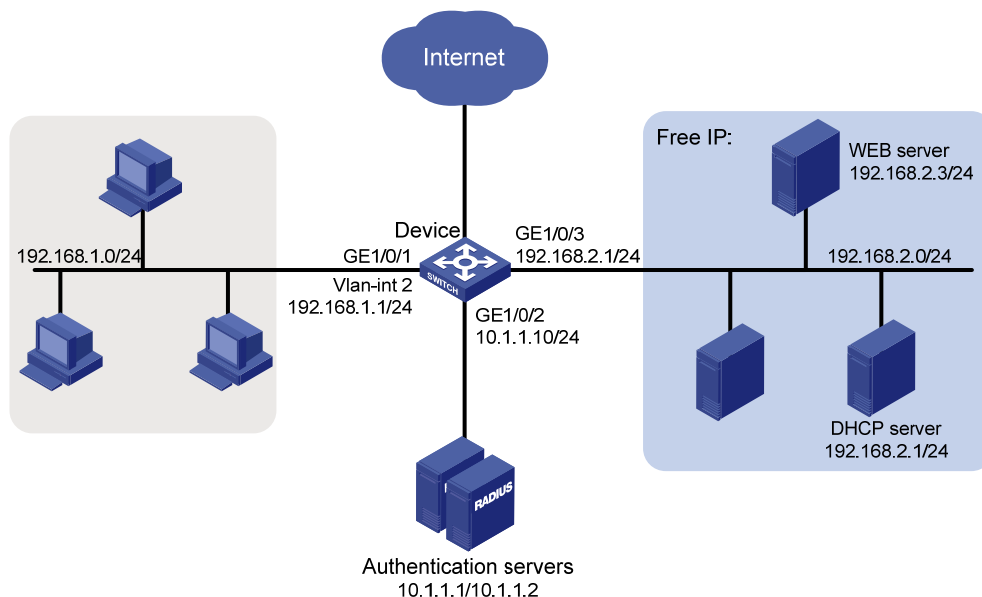
1. 组网需求

某公司用户主机通过 Device 接入 Internet，并通过 DHCP 服务器动态获取 IP 地址。目前，公司部署 EAD 解决方案，要求所有用户主机通过 802.1X 认证上网，因此需要所有主机上安装配套的 802.1X 客户端。由于网络中的用户主机数量较大，为减轻网络管理员安装以及升级 802.1X 客户端的工作量，在 192.168.2.0/24 网段部署一台 Web 服务器专门提供客户端软件下载。具体要求如下：

- 未进行 802.1X 认证或者 802.1X 认证失败的用户，只能访问 192.168.2.0/24 网段，并可通过该网段内的 DHCP 服务器动态获取 192.168.1.0/24 网段的 IP 地址。
- 未进行 802.1X 认证或者 802.1X 认证失败的用户通过浏览器访问非 192.168.2.0/24 网段的外部网络时，用户访问的页面均会被 Device 重定向至管理员预设的 Web 服务器页面，该 Web 服务器页面将提示用户进行 802.1X 客户端的下载。
- 用户成功通过 802.1X 认证之后，可正常访问网络。

2. 组网图

图2-1 EAD 快速部署典型配置组网图



3. 配置步骤



说明

- 完成 DHCP 服务器的配置，保证用户可成功获取 192.168.1.0/24 网段的 IP 地址。
- 完成 Web 服务器的配置，保证用户可成功登录预置的 Web 页面进行 802.1X 客户端的下载。
- 完成认证服务器的配置，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 DHCP 中继

使能 DHCP 服务。

```
<Device> system-view
```

```
[Device] dhcp enable
```

配置 DHCP 服务器的地址。

```
[Device] dhcp relay server-group 1 ip 192.168.2.2
```

配置接口 Vlan-interface2 工作在 DHCP 中继模式。

```
[Device] interface vlan-interface 2
```

```
[Device-Vlan-interface2] dhcp select relay
```

配置接口 Vlan-interface2 对应 DHCP 服务器组 1。

```
[Device-Vlan-interface2] dhcp relay server-select 1
```

```
[Device-Vlan-interface2] quit
```

(3) 配置 RADIUS 方案和 ISP 域

请参见“[1.6.1 802.1X认证配置举例](#)”。

(4) 配置 802.1X

配置 Free IP。

```
[Device] dot1x free-ip 192.168.2.0 24
```

配置 IE 访问的重定向 URL。

```
[Device] dot1x url http://192.168.2.3
```

开启全局 802.1X 特性。

```
[Device] dot1x
```

开启指定端口的 802.1X 特性。

```
[Device] interface gigabitethernet 1/0/1
```

```
[Device-GigabitEthernet1/0/1] dot1x
```

4. 验证配置结果

以上配置完成之后，执行命令 **display dot1x** 可以查看 802.1X 的配置情况。用户主机成功获得 DHCP 服务器分配的 IP 地址之后，在 Windows XP 操作系统的主机上执行 **ping Free IP** 中的地址，可验证在 802.1X 认证成功之前是否可以访问免认证网段 192.168.2.0/24。

```
C:\>ping 192.168.2.3
```

```
Pinging 192.168.2.3 with 32 bytes of data:
```

```
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
```

```
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
```

```
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
```

```
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 192.168.2.3:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

用户在 802.1X 认证成功之前，通过浏览器访问任何非 Free IP 的外部网站地址时，都会被重定向到 Web server 页面，此页面提供 802.1X 客户端的下载服务。需要注意的是，地址栏内输入的地址应该为非 Free IP 地址才有效，例如 3.3.3.3 或者 <http://3.3.3.3>。

2.5 常见配置错误举例

2.5.1 用户通过浏览器访问外部网络不能正确重定向

1. 故障现象

用户在浏览器中输入地址，但该 HTTP 访问不能被正确重定向到指定的 URL 服务器。

2. 故障分析

- 用户在浏览器地址栏内输入了字符串类型的地址。由于用户主机使用的操作系统首先会将这个字符串地址作为名字进行网络地址解析，如果解析不成功通常会以非 X.X.X.X 形式的网络地址发送 ARP 请求，这样的请求不能进行重定向；
- 用户在 IE 地址栏内输入了 Free IP 内的任意地址。设备会认为用户试图访问 Free IP 内的某台主机，而不对其进行重定向，即使这台主机不存在；

- 用户在配置和组网时没有将服务器加入 **Free IP**，或者配置的 **URL** 为不存在的地址，或者该 **URL** 指向的服务器没有提供 **Web** 服务。

3. 处理过程

- 地址栏内输入的地址应该为 **X.X.X.X**（点分十进制格式）的非 **Free IP** 地址才有效。
- 确保设备及服务器上的配置正确且有效。

目 录

1 MAC地址认证配置	1-1
1.1 MAC地址认证简介	1-1
1.1.1 MAC地址认证概述	1-1
1.1.2 使用不同用户名格式的MAC地址认证	1-1
1.1.3 MAC地址认证定时器	1-2
1.1.4 和MAC地址认证配合使用的特性	1-3
1.2 MAC地址认证配置任务简介	1-4
1.3 MAC地址认证基本配置	1-4
1.3.1 配置准备	1-4
1.3.2 配置过程	1-4
1.4 配置MAC地址认证用户使用的认证域	1-6
1.5 配置MAC地址认证的Guest VLAN	1-6
1.5.1 配置准备	1-7
1.5.2 配置Guest VLAN	1-7
1.6 配置MAC地址认证的Critical VLAN	1-7
1.6.1 配置准备	1-8
1.6.2 配置Critical VLAN	1-8
1.7 配置MAC地址认证延时时间	1-8
1.8 配置MAC地址认证支持多VLAN模式（仅R5206及以上版本支持）	1-9
1.9 MAC地址认证的显示和维护	1-9
1.10 MAC地址认证典型配置举例	1-10
1.10.1 本地MAC地址认证	1-10
1.10.2 使用RADIUS服务器进行MAC地址认证	1-11
1.10.3 下发ACL典型配置举例	1-13

1 MAC地址认证配置

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 地址就被添加为静默 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。

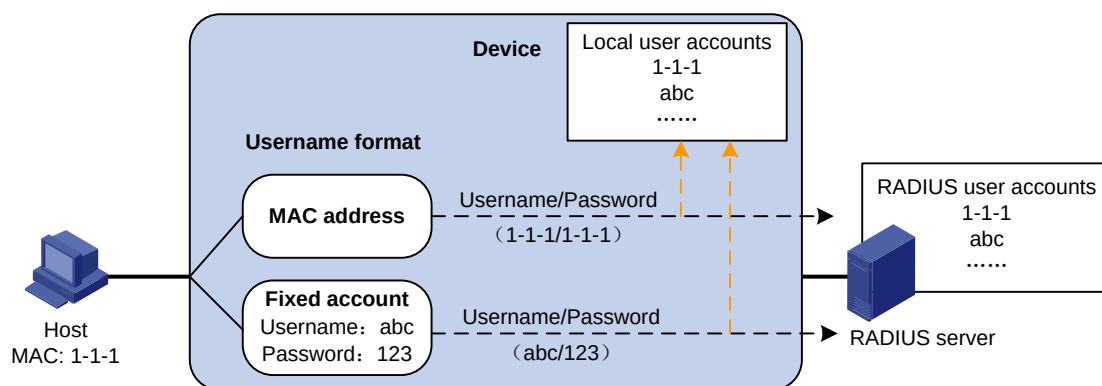
1.1.2 使用不同用户名格式的MAC地址认证

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名格式分为两种类型：

- **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



2. 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。

3. 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。

1.1.3 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。如果在两个时间间隔之内，某在线用户没有流量通过设备，设备将切断该用户的连接，同时通知 RADIUS 服务器，停止对该用户的计费。
- 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，设备不对来自该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。

1.1.4 和MAC地址认证配合使用的特性

1. 支持VLAN下发

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用户划分到不同的 VLAN。MAC 地址认证支持认证服务器（远程或本地）授权下发 VLAN 功能，即当用户通过 MAC 地址认证后，认证服务器将指定的受限网络资源所在的 VLAN 作为授权 VLAN 下发到用户认证的端口。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 并加入下发的授权 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 为下发的授权 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 为下发的授权 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下发的授权 VLAN 动态地创建基于用户 MAC 的 VLAN，而端口的缺省 VLAN 并不改变。

2. 支持ACL下发

从认证服务器（远程或本地）下发的 ACL 被称为授权 ACL，它为用户访问网络提供了良好的过滤条件设置功能。MAC 地址认证支持认证服务器授权下发 ACL 功能，即当用户通过 MAC 地址认证后，如果认证服务器上配置了授权 ACL，则设备会根据服务器下发的授权 ACL 对用户所在端口的数据流进行控制。为使下发的授权 ACL 生效，需要提前在设备上配置相应的 ACL 规则。而且在用户访问网络的过程中，可以通过改变服务器的授权 ACL 设置来改变用户的访问权限。

3. MAC地址认证的Guest VLAN

Guest 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，比如获取客户端软件，升级客户端或执行其他一些用户升级程序。这个 VLAN 称之为 Guest VLAN。

如果接入用户的端口上配置了 Guest VLAN，则该端口上认证失败的用户会被加入 Guest VLAN，且设备允许 Guest VLAN 以不携带 Tag 的方式通过该端口，即该用户被授权访问 Guest VLAN 里的资源。若 Guest VLAN 中的用户再次发起认证未成功，则该用户将仍然处于 Guest VLAN 内；若认证成功，则会根据认证服务器是否下发授权 VLAN 决定是否将用户加入到下发的授权 VLAN 中，在认证服务器未下发授权 VLAN 的情况下，用户回到加入 Guest VLAN 之前端口所在的 VLAN。

4. MAC地址认证的Critical VLAN

MAC 地址认证的 Critical VLAN 功能允许用户在进行 MAC 地址认证时，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 MAC 地址认证的 Critical VLAN。

端口上配置 Critical VLAN 后，若该端口上有用户进行 MAC 地址认证时，当所有认证服务器都不可达，则用户将被授权访问 Critical VLAN 里的资源。

如果满足以下任意一个条件，端口将会离开 Critical VLAN：

- 认证用户的 ISP 域中新增认证服务器（且该服务器可达）。
- 配置了 RADIUS 认证服务器探测功能，且探测结果表示某认证服务器可达。
- 收到 RADIUS 服务器回应报文。



说明

- 只采用 RADIUS 认证方式的情况下，在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。
- RADIUS 服务器相关的配置请参见“安全配置指导”中的“AAA”。

1.2 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
MAC地址认证基本配置	必选	1.3
配置MAC地址认证用户使用的认证域	可选	1.4
配置MAC地址认证的Guest VLAN	可选	1.5
配置MAC地址认证的Critical VLAN	可选	1.6
配置MAC地址认证延时时间	可选	1.7
配置MAC地址认证支持多VLAN模式（仅R5206及以上版本支持）	可选	1.8

1.3 MAC地址认证基本配置

1.3.1 配置准备

- 创建并配置 ISP 域。
- 若采用本地认证方式，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。



说明

创建本地用户或添加远程用户帐号时，需要注意这些用户的用户名必须与设备上指定的 MAC 地址认证用户名格式保持一致。

1.3.2 配置过程

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

1. 配置全局MAC地址认证

表1-2 配置全局 MAC 地址认证

操作	命令	说明
进入系统视图	system-view	-
启动全局的MAC地址认证特性	mac-authentication	必选 缺省情况下，全局的MAC地址认证特性为关闭状态
配置MAC地址认证定时器	mac-authentication timer { offline-detect <i>offline-detect-value</i> quiet <i>quiet-value</i> server-timeout <i>server-timeout-value</i> }	可选 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
配置MAC地址认证用户的用户名格式	mac-authentication user-name-format { fixed [account name] [password { cipher simple } <i>password</i>] mac-address [{ with-hyphen without-hyphen } [lowercase uppercase]] }	可选 缺省情况下，使用用户的源MAC地址做用户名与密码，其中字母为小写，MAC地址不带连字符“-”



说明

全局 MAC 地址认证与 802.1X 的 EAD 快速部署功能互斥，开启全局 MAC 地址认证将会使 802.1X 的 EAD 快速部署功能失效。

2. 配置端口MAC地址认证

表1-3 配置端口 MAC 地址认证

配置步骤		命令	说明
进入系统视图		system-view	-
开启端口MAC地址认证特性	系统视图	mac-authentication interface <i>interface-list</i>	二者必选其一 缺省情况下，端口的MAC地址认证特性为关闭状态
	以太网端口视图	interface <i>interface-type interface-number</i>	
		mac-authentication	
配置端口同时可容纳接入的MAC地址认证用户数量的最大值		mac-authentication max-user <i>user-number</i>	可选 端口同时可容纳接入用户数量的最大值为2048



说明

端口启动 MAC 地址认证与端口加入聚合组及端口加入业务环回组互斥。

1.4 配置MAC地址认证用户使用的认证域

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。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，该认证域对所有使能了 MAC 地址认证的端口生效。
- 在以太网端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。

如果系统视图和以太网端口视图下都指定了认证域，则端口优先采用本端口上指定的认证域。

表1-4 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
	interface interface-type interface-number mac-authentication domain domain-name	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



说明

端口上接入的 MAC 地址认证用户将按照如下先后顺序选择认证域：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”。

1.5 配置MAC地址认证的Guest VLAN



注意

- 若在 802.1X 接入控制方式为 MAC-based 的端口上同时配置了 802.1X 认证的 Guest VLAN 与 MAC 地址认证的 Guest VLAN，则仅 802.1X 认证的 Guest VLAN 生效，因此建议在配置 MAC 地址认证的 Guest VLAN 之前，确认是否配置了 802.1X 认证的 Guest VLAN。关于 802.1X 的 Guest VLAN 介绍请参见“安全配置指导”中的“802.1X”。
- MAC 地址认证 Guest VLAN 功能的优先级高于端口安全中端口入侵检测的阻塞 MAC 功能，低于端口入侵检测的端口关闭功能，因此在开启了端口安全入侵检测的端口关闭功能时，MAC 地址认证的 Guest VLAN 功能不生效。关于端口入侵检测功能的具体介绍请参见“安全配置指导”中的“端口安全”。
- 如果某个 VLAN 被指定为 Super VLAN，则该 VLAN 不能被指定为某个端口的 Guest VLAN；同样，如果某个 VLAN 被指定为某个端口的 Guest VLAN，则该 VLAN 不能被指定为 Super VLAN。关于 Super VLAN 的详细内容请参见“二层技术-以太网交换配置指导”中的“Super VLAN”。

1.5.1 配置准备

- 开启 MAC 地址认证特性。
- 端口的 MAC VLAN 功能已经使能。
- 已经创建需要配置为 Guest VLAN 的 VLAN。

1.5.2 配置Guest VLAN

表1-5 配置 Guest VLAN

配置步骤	命令	说明
进入系统视图	system-view	-
进入以太网端口视图	interface <i>interface-type</i> <i>interface-number</i>	-
配置MAC认证的Guest VLAN	mac-authentication guest-vlan <i>guest-vlan-id</i>	必选 缺省情况下，没有配置MAC认证的 Guest VLAN



说明

- MAC 地址认证过程中，当客户端无法在设备给其分配的 VLAN 发生变化时（加入或离开 MAC 地址认证的授权 VLAN、Guest VLAN 或 Critical VLAN）触发自身的 IP 地址更新，建议用户通过释放 IP 或修复网络连接的方式解决这个问题。
- 不同的端口可以配置不同的 Guest VLAN，但一个端口只能配置一个 Guest VLAN。
- MAC 地址认证 Guest VLAN 功能的优先级高于 MAC 地址认证的静默 MAC 功能，即认证失败的用户可访问指定的 Guest VLAN 中的资源，且该用户的 MAC 地址不会被加入静默 MAC。

1.6 配置MAC地址认证的Critical VLAN



注意

- MAC 地址认证 Critical VLAN 功能的优先级高于端口安全中端口入侵检测的阻塞 MAC 功能，低于端口入侵检测的端口关闭功能，因此在开启了端口安全入侵检测的端口关闭功能时，MAC 地址认证的 Critical VLAN 功能不生效。关于端口入侵检测功能的具体介绍请参见“安全配置指导”中的“端口安全”。
- 如果某个 VLAN 被指定为 Super VLAN，则该 VLAN 不能被指定为某个端口的 Critical VLAN；同样，如果某个 VLAN 被指定为某个端口的 Critical VLAN，则该 VLAN 不能被指定为 Super VLAN。关于 Super VLAN 的详细内容请参见“二层技术-以太网交换配置指导”中的“Super VLAN”。

1.6.1 配置准备

- 开启 MAC 地址认证特性。
- 端口的 MAC VLAN 功能已经使能。
- 已经创建需要配置为 Critical VLAN 的 VLAN。

1.6.2 配置Critical VLAN

表1-6 配置 Critical VLAN

配置步骤	命令	说明
进入系统视图	system-view	-
进入二层以太网端口视图	interface <i>interface-type</i> <i>interface-number</i>	-
配置MAC认证的Critical VLAN	mac-authentication critical vlan <i>critical-vlan-id</i>	必选 缺省情况下，没有配置MAC认证的 Critical VLAN



说明

- MAC 地址认证过程中，当客户端无法在设备给其分配的 VLAN 发生变化时（加入或离开 MAC 地址认证的授权 VLAN、Guest VLAN 或 Critical VLAN）触发自身的 IP 地址更新，建议用户通过释放 IP 或修复网络连接的方式解决这个问题。
- 不同的端口可以配置不同的 Critical VLAN，但一个端口只能配置一个 Critical VLAN。
- MAC 地址认证 Critical VLAN 功能的优先级高于 MAC 地址认证的静默 MAC 功能，即当认证服务器都不可达时，认证失败的用户可访问指定的 Critical VLAN 中的资源，且该用户的 MAC 地址不会被加入静默 MAC。

1.7 配置MAC地址认证延时时间

在端口上同时启用了 802.1X 认证和 MAC 地址认证功能的情况下，可以通过启用 MAC 地址认证延时触发功能达到优先触发 802.1X 认证的目的。具体是否需要启用此功能，可以根据实际组网情况进行相应设置。

表1-7 配置 MAC 地址认证延时时间

配置步骤	命令	说明
进入系统视图	system-view	-
进入二层以太网端口视图	interface <i>interface-type</i> <i>interface-number</i>	-
配置MAC地址认证延时的时间	mac-authentication timer auth-delay <i>time</i>	必选 缺省情况下，MAC地址认证不延时

1.8 配置MAC地址认证支持多VLAN模式（仅R5206及以上版本支持）

缺省情况下，端口上开启 MAC 地址认证功能后，若用户认证通过，则端口将记录用户 MAC 地址与 VLAN 的对应关系，后继收到的源 MAC 地址为该 MAC 的报文，若 MAC 地址和 VLAN 的对应关系符合记录，则正常转发；若收到源 MAC 地址相同，但 VLAN 不同的报文，则将该报文上送 CPU，重新触发 MAC 地址认证，认证成功后，端口刷新 MAC 地址与 VLAN 的对应关系。

这种机制下当一台 IP 电话通过 MAC 地址认证后，可以在相应的 VLAN 内转发语音报文，但后续该 IP 电话如果发送了 untag 的非语音报文，则该报文会因在其它 VLAN 内转发而触发重新认证，后续语音报文再次通过端口时，也因为 VLAN 变化而需要重新认证。为了解决这种端口反复认证带来的语音报文传输质量受干扰的问题，可配置 MAC 地址认证支持多 VLAN 模式。

开启该功能后，当端口收到的报文的源 MAC 地址与已通过认证的用户的 MAC 地址一致，但 MAC 地址与 VLAN 的对应关系与记录不一致时，系统会增加这一条新的 MAC 地址与 VLAN 的对应关系的记录，从而实现允许该用户相同 MAC 地址的报文同时在多个 VLAN 中转发的目的。

需要注意的是：目前设备最多支持相同 MAC 地址认证的报文同时在 5 个 VLAN 内转发。

表1-8 配置 MAC 地址认证支持多 VLAN 模式

操作	命令	说明
进入系统视图	system-view	-
进入二层以太网端口视图	interface interface-type interface-number	-
配置MAC地址认证支持多VLAN模式	mac-authentication host-mode multi-vlan	必选 缺省情况下，MAC地址认证不支持多VLAN模式，即相同MAC地址的用户报文在当前端口下只能同时在一个VLAN中认证通过

1.9 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1-9 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-list] [{ begin exclude include } regular-expression]
清除MAC地址认证的统计信息	reset mac-authentication statistics [interface interface-list]

1.10 MAC地址认证典型配置举例

1.10.1 本地MAC地址认证

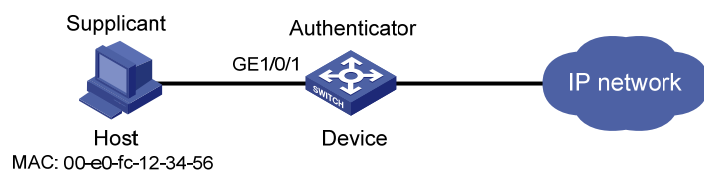
1. 组网需求

如 图 1-2 所示，某用户的工作站与以太网设备的端口GigabitEthernet1/0/1 相连接。

- 设备的管理者希望在端口 GigabitEthernet1/0/1 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：aabbcc.net，认证时使用本地认证的方式。
- 使用用户的 MAC 地址做用户名和密码，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

(1) 配置本地 MAC 地址认证

添加本地接入用户。用户名和密码均为接入用户的 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
[Device-luser-00-e0-fc-12-34-56] password simple 00-e0-fc-12-34-56
[Device-luser-00-e0-fc-12-34-56] service-type lan-access
[Device-luser-00-e0-fc-12-34-56] quit
```

配置 ISP 域，使用本地认证方法。

```
[Device] domain aabbcc.net
[Device-isp-aabbcc.net] authentication lan-access local
[Device-isp-aabbcc.net] quit
```

开启全局 MAC 地址认证特性。

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

开启端口 GigabitEthernet1/0/1 的 MAC 地址认证特性。

```
[Device] mac-authentication interface gigabitethernet 1/0/1
```

配置 MAC 地址认证用户所使用的 ISP 域。

```
[Device] mac-authentication domain aabbcc.net
```

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
(2) 验证配置结果
# 显示 MAC 地址配置信息。
<Device> display mac-authentication
MAC address authentication is enabled.
User name format is MAC address in lowercase, like xx-xx-xx-xx-xx-xx
Fixed username:mac
Fixed password:not configured
    Offline detect period is 180s
    Quiet period is 180s.
    Server response timeout value is 100s
    The max allowed user number is 2048 per slot
    Current user number amounts to 1
    Current domain is aabbcc.net
Silent Mac User info:
    MAC Addr          From Port          Port Index
GigabitEthernet1/0/1 is link-up
    MAC address authentication is enabled
    Authenticate success: 1, failed: 0
    Max number of on-line users is 2048
    Current online user number is 1
    MAC Addr          Authenticate state      Auth Index
    00e0-fc12-3456    MAC_AUTHENTICATOR_SUCCESS    29
# 用户认证成功后，可通过如下显示命令查看上线用户的连接信息。
<Device> display connection
Slot: 1
Index=29 ,Username=00-e0-fc-12-34-56@aabbcc.net
IP=N/A
IPv6=N/A
MAC=00e0-fc12-3456

Total 1 connection(s) matched on slot 1.
Total 1 connection(s) matched.
```

1.10.2 使用RADIUS服务器进行MAC地址认证

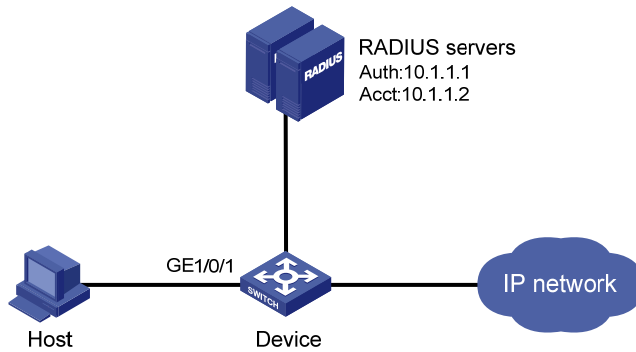
1. 组网需求

如 [图 1-3](#) 所示，用户主机Host通过端口GigabitEthernet1/0/1 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 GigabitEthernet1/0/1 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。

(1) 配置使用 RADIUS 服务器进行 MAC 地址认证

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

配置 ISP 域的 AAA 方法。

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

开启全局 MAC 地址认证特性。

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

开启端口 GigabitEthernet1/0/1 的 MAC 地址认证特性。

```
[Device] mac-authentication interface gigabitethernet 1/0/1
```

配置 MAC 地址认证用户所使用的 ISP 域。

```
[Device] mac-authentication domain 2000
```

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
```

(2) 验证配置结果

```
# 显示 MAC 地址配置信息。
```

```
<Device> display mac-authentication  
MAC address authentication is enabled.  
User name format is fixed account  
Fixed username:aaa  
Fixed password: *****  
Offline detect period is 180s  
Quiet period is 180s.  
Server response timeout value is 100s  
The max allowed user number is 2048 per slot  
Current user number amounts to 1  
Current domain is 2000  
Silent Mac User info:  
MAC ADDR          From Port          Port Index  
GigabitEthernet1/0/1 is link-up  
MAC address authentication is enabled  
Authenticate success: 1, failed: 0  
Max number of on-line users is 2048  
Current online user number is 1  
MAC ADDR          Authenticate state      Auth Index  
00e0-fc12-3456    MAC_AUTHENTICATOR_SUCCESS    29  
# 用户认证成功后，可通过如下显示命令查看上线用户的连接信息。  
<Device> display connection  
Slot: 1  
Index=29 ,Username=aaa@2000  
IP=N/A  
IPv6=N/A  
MAC=00e0-fc12-3456  
  
Total 1 connection(s) matched on slot 1.  
Total 1 connection(s) matched.
```

1.10.3 下发ACL典型配置举例

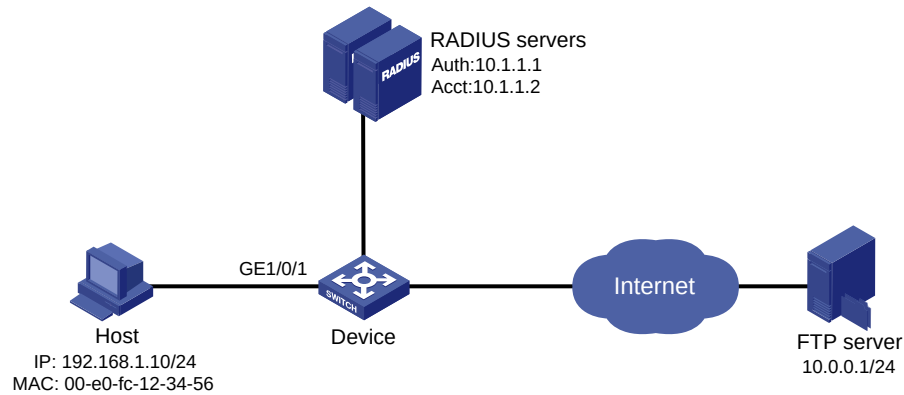
1. 组网需求

如 [图 1-4](#) 所示，用户主机Host通过端口GigabitEthernet1/0/1 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，Internet网络中有一台FTP服务器，IP地址为 10.0.0.1。现有如下组网需求：

- 在端口 GigabitEthernet1/0/1 上对用户接入进行 MAC 地址认证，以控制其对 Internet 的访问。认证时使用用户的源 MAC 地址做用户名和密码，其中 MAC 地址带连字符、字母小写。
- 当用户认证成功上线后，允许用户访问除 FTP 服务器之外的 Internet 资源。

2. 组网图

图1-4 下发 ACL 典型配置组网图



3. 配置步骤



说明

- 确保 RADIUS 服务器与设备路由可达。
- 由于该例中使用了 MAC 地址认证的缺省用户名和密码，即使用户的源 MAC 地址做用户名与密码，因此还要保证 RADIUS 服务器上正确添加了接入用户帐户：用户名为 00-e0-fc-12-34-56，密码为 00-e0-fc-12-34-56。
- 指定 RADIUS 服务器上的授权 ACL 为设备上配置的 ACL 3000。

(1) 配置授权 ACL

配置 ACL 3000，拒绝目的 IP 地址为 10.0.0.1 的报文通过。

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 0 deny ip destination 10.0.0.1 0
[Sysname-acl-adv-3000] quit
```

(2) 配置使用 RADIUS 服务器进行 MAC 地址认证

配置 RADIUS 方案。

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

配置 ISP 域的 AAA 方法。

```
[Sysname] domain 2000
[Sysname-isp-2000] authentication default radius-scheme 2000
[Sysname-isp-2000] authorization default radius-scheme 2000
[Sysname-isp-2000] accounting default radius-scheme 2000
```

```
[Sysname-isp-2000] quit
# 开启全局 MAC 地址认证特性。
[Sysname] mac-authentication
# 配置 MAC 地址认证用户所使用的 ISP 域。
[Sysname] mac-authentication domain 2000
# 配置 MAC 地址认证用户名格式：使用带连字符的 MAC 地址做用户名与密码，其中字母小写。
[Sysname] mac-authentication user-name-format mac-address with-hyphen lowercase
# 开启指定端口的 MAC 地址认证特性。
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication
```

(3) 验证配置结果

用户 Host 认证成功后，通过在设备上执行 **display connection** 命令可以查看到已上线用户信息。

```
[Sysname-GigabitEthernet1/0/1] display connection
Slot: 1
Index=9 , Username=00-e0-fc-12-34-56@2000
IP=N/A
IPv6=N/A
MAC=00e0-fc12-3456
```

```
Total 1 connection(s) matched on slot 1.
```

```
Total 1 connection(s) matched.
```

用户通过 **ping** FTP 服务器，可以验证认证服务器下发的 ACL 3000 是否生效。

```
C:\>ping 10.0.0.1
```

```
Pinging 10.0.0.1 with 32 bytes of data:
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Ping statistics for 10.0.0.1:
```

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

目 录

1 Portal配置	1-1
1.1 Portal简介	1-1
1.1.1 Portal概述	1-1
1.1.2 Portal扩展功能	1-1
1.1.3 Portal的系统组成	1-1
1.1.4 使用本地Portal服务器的Portal认证系统	1-3
1.1.5 Portal的认证方式	1-4
1.1.6 Portal支持EAP认证	1-5
1.1.7 二层Portal认证过程	1-5
1.1.8 三层Portal认证过程	1-6
1.1.9 Portal支持双机热备	1-10
1.1.10 Portal支持多实例	1-11
1.2 Portal配置任务简介	1-12
1.3 配置准备	1-13
1.4 指定Portal服务器	1-14
1.4.1 指定二层Portal认证的本地Portal服务器监听IP地址	1-14
1.4.2 指定三层Portal认证的Portal服务器	1-14
1.5 配置本地Portal服务器	1-15
1.5.1 自定义认证页面文件	1-15
1.5.2 配置本地Portal服务器	1-18
1.6 使能Portal认证	1-19
1.6.1 使能二层Portal认证	1-19
1.6.2 使能三层Portal认证	1-19
1.7 控制Portal用户的接入	1-20
1.7.1 配置免认证规则	1-20
1.7.2 配置源认证网段	1-21
1.7.3 配置Portal最大用户数	1-22
1.7.4 指定Portal用户使用的认证域	1-22
1.7.5 配置二层Portal认证支持Web代理	1-23
1.7.6 配置Portal用户认证端口的自动迁移功能	1-24
1.8 配置Portal认证的Auth-Fail VLAN	1-24
1.9 配置接口发送RADIUS报文的相关属性	1-25
1.9.1 配置接口的NAS-Port-Type	1-25

1.9.2 配置接口的NAS-ID Profile	1-26
1.10 配置接口发送Portal报文使用的源地址	1-26
1.11 配置Portal支持双机热备	1-27
1.12 指定Portal用户认证成功后认证页面的自动跳转目的网站地址	1-29
1.13 配置Portal探测功能	1-29
1.13.1 配置二层Portal用户在线检测功能	1-29
1.13.2 配置Portal服务器探测功能	1-30
1.13.3 配置Portal用户信息同步功能	1-31
1.14 强制Portal用户下线	1-32
1.15 Portal显示和维护	1-32
1.16 Portal典型配置举例	1-33
1.16.1 Portal直接认证配置举例	1-33
1.16.2 Portal二次地址分配认证配置举例	1-38
1.16.3 可跨三层Portal认证配置举例	1-40
1.16.4 Portal直接认证扩展功能配置举例	1-42
1.16.5 Portal二次地址分配认证扩展功能配置举例	1-44
1.16.6 可跨三层Portal认证方式扩展功能配置举例	1-46
1.16.7 Portal支持双机热备配置举例	1-48
1.16.8 Portal服务器探测和用户同步功能配置举例	1-56
1.16.9 可跨三层Portal认证支持多实例配置举例	1-62
1.16.10 配置二层Portal认证	1-64
1.17 常见配置错误举例	1-67
1.17.1 接入设备和Portal服务器上的密钥不一致	1-67
1.17.2 接入设备上服务器端口配置错误	1-68

1 Portal配置

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，一般将 Portal 认证网站称为门户网站。

未认证用户上网时，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，必须在门户网站进行认证，只有认证通过后才可以使用互联网资源。

用户可以主动访问已知的 Portal 认证网站，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。反之，如果用户试图通过 HTTP 访问其他外网，将被强制访问 Portal 认证网站，从而开始 Portal 认证过程，这种方式称作强制认证。

Portal 业务可以为运营商提供方便的管理功能，门户网站可以开展广告、社区服务、个性化的业务等，使宽带运营商、设备提供商和内容服务提供商形成一个产业生态系统。

1.1.2 Portal扩展功能

Portal 的扩展功能主要是指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。具体扩展功能如下：

- 安全性检测：在 Portal 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部分互联网资源（受限资源）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（非受限资源）。

1.1.3 Portal的系统组成

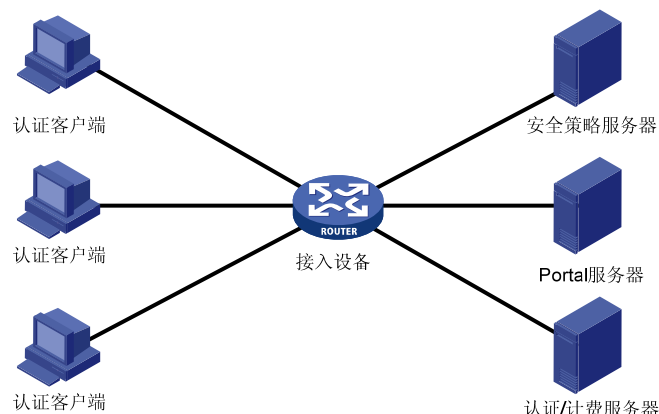
Portal的典型组网方式如 [图 1-1](#) 所示，它由五个基本要素组成：认证客户端、接入设备、Portal服务器、认证/计费服务器和安全策略服务器。



说明

Portal 服务器可以是接入设备之外的独立实体，也可以是存在于接入设备之内的内嵌实体，本文称之为“本地 Portal 服务器”，因此下文除对本地支持的 Portal 服务器做特殊说明之外，其它所有 Portal 服务器均指独立的 Portal 服务器，请勿混淆。

图1-1 Portal 系统组成示意图



1. 认证客户端

安装于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。对接入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 服务器。
- 在认证过程中，与 Portal 服务器、安全策略服务器、认证/计费服务器交互，完成身份认证/安全认证/计费的功能。
- 在认证通过后，允许用户访问被管理员授权的互联网资源。

3. Portal服务器

接收 Portal 客户端认证请求的服务器端系统，提供免费门户服务和基于 Web 认证的界面，与接入设备交互认证客户端的认证信息。

4. 认证/计费服务器

与接入设备进行交互，完成对用户的认证和计费。

5. 安全策略服务器

与 Portal 客户端、接入设备进行交互，完成对用户的安全认证，并对用户进行授权操作。

以上五个基本要素的交互过程为：

- (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 服务器的 Web 认证主页上；若需要使用 Portal 的扩展认证功能，则用户必须使用 Portal 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 服务器会将用户的认证信息传递给接入设备；
- (3) 然后接入设备再与认证/计费服务器通信进行认证和计费；
- (4) 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。



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 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 报文的源地地址配置为接口的公网 IP 地址。
 - 目前支持 Portal 认证的远端认证/计费服务器为 RADIUS (Remote Authentication Dial-In User Service, 远程认证拨号用户服务) 服务器。
 - 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。
-

1.1.4 使用本地Portal服务器的Portal认证系统

1. 系统组成

本地Portal服务器功能是指,Portal认证系统中不采用外部独立的Portal服务器,而由接入设备实现Portal服务器功能。这种情况下,Portal认证系统仅包括三个基本要素:认证客户端、接入设备和认证/计费服务器,如 [图 1-2](#) 所示。由于设备支持Web用户直接认证,因此就不需要部署额外的Portal服务器,增强了Portal认证的通用性。

图1-2 使用本地 Portal 服务器的 Portal 系统组成示意图



说明

- 使用本地 Portal 服务器的 Portal 认证系统不支持 Portal 扩展功能,因此不需要部署安全策略服务器。
 - 内嵌本地 Portal 服务器的接入设备实现了简单的 Portal 服务器功能,仅能给用户提供通过 Web 方式登录、下线的基本功能,并不能完全替代独立的 Portal 服务器。
-

2. 认证客户端和本地Portal服务器之间的交互协议

认证客户端和内嵌本地 Portal 服务器的接入设备之间可以采用 HTTP 和 HTTPS 协议通信。若客户端和接入设备之间交互 HTTP 协议,则报文以明文形式传输,安全性无法保证;若客户端和接入设备之间交互 HTTPS 协议,则报文基于 SSL 提供的安全机制以密文的形式传输,数据的安全性有保障。

3. 本地Portal服务器支持用户自定义认证页面

本地 Portal 服务器支持由用户自定义认证页面的内容,即允许用户编辑一套认证页面的 HTML 文件,并在压缩之后保存至设备的存储设备中。该套自定义页面中包括六个认证页面:登录页面、登录成

功页面、在线页面、下线成功页面、登录失败页面和系统忙页面。本地 Portal 服务器根据不同的认证阶段向客户端推出对应的认证页面，若不自定义，则分别推出系统提供的缺省认证页面。



说明

关于认证页面文件的自定义规范请参见“[1.5.1 自定义认证页面文件](#)”。

1.1.5 Portal 的认证方式

不同的组网方式下，可采用的 Portal 认证方式不同。按照网络中实施 Portal 认证的网络层次来分，Portal 的认证方式分为两种：二层认证方式和三层认证方式。

1. 二层认证方式

这种方式支持在接入设备连接用户的二层端口上开启 Portal 认证功能，只允许源 MAC 地址通过认证的用户才能访问外部网络资源。目前，该认证方式仅支持本地 Portal 认证，即接入设备作为本地 Portal 服务器向用户提供 Web 认证服务。

另外，该方式还支持服务器下发授权 VLAN 和将认证失败用户加入认证失败 VLAN 功能（三层认证方式不支持）。

2. 三层认证方式

这种方式支持在接入设备连接用户的三层接口上开启 Portal 认证功能。三层接口 Portal 认证又可分为三种不同的认证方式：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；可跨三层认证方式下，认证客户端和接入设备之间可以跨接三层转发设备。

(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 服务器，以及设定的免费访问地址；认证通过后即可访问网络资源。认证流程相对二次地址较为简单。

(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 服务器，以及设定的免费访问地址；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。



说明

- 使用本地 Portal 服务器的 Portal 认证不支持二次地址分配认证方式。
- 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

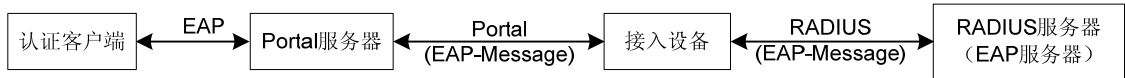
间未跨越三层转发设备，因此接口可以学习到用户的 MAC 地址，接入设备可以利用学习到 MAC 地址增强对用户报文转发的控制力度。

1.1.6 Portal支持EAP认证

在对接入用户身份可靠性要求较高的网络应用中，传统的基于用户名和口令的用户身份验证方式存在一定的安全问题，基于数字证书的用户身份验证方式通常被用来建立更为安全和可靠的网络接入认证机制。

EAP（Extensible Authentication Protocol，可扩展认证协议）可支持多种基于数字证书的认证方式（例如 EAP-TLS），它与 Portal 认证相配合，可共同为用户提供基于数字证书的接入认证服务。

图1-3 Portal 支持 EAP 认证协议交互示意图



如 图 1-3 所示，在Portal支持EAP认证的实现中，客户端与Portal服务器之间交互EAP认证报文，Portal服务器与接入设备之间交互携带EAP-Message属性的Portal协议报文，接入设备与RADIUS服务器之间交互携带EAP-Message属性的RADIUS协议报文，由具备EAP服务器功能的RADIUS服务器处理EAP-Message属性中封装的EAP报文，并给出EAP认证结果。整个EAP认证过程中，接入设备只是对Portal服务器与RADIUS服务器之间的EAP-Message属性进行透传，并不对其进行任何处理，因此接入设备上无需任何额外配置。

说明

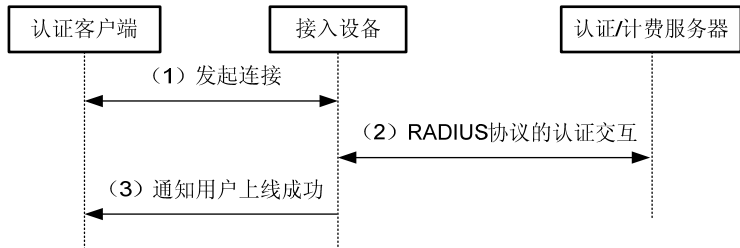
- 该功能仅能与 iMC 的 Portal 服务器以及 iNode Portal 客户端配合使用。
- 目前，仅使用远程 Portal 服务器的三层 Portal 认证支持 EAP 认证。

1.1.7 二层Portal认证过程

1. 二层Portal认证流程

目前，二层 Portal 认证只支持本地 Portal 认证，即由接入设备作为本地 Portal 服务器向用户提供 Web 认证服务，具体认证过程如下。

图1-4 二层 Portal 认证流程图



- (1) Portal 用户通过 HTTP 协议发起认证，HTTP 报文经过配置了本地 Portal 服务器的接入设备的端口时会被重定向到本地 Portal 服务器的监听 IP 地址，本地 Portal 服务器提供 Web 页面供

用户输入用户名和密码来进行认证且支持 HTTP 和 HTTPS 协议的认证请求。该本地 Portal 服务器的监听 IP 地址为接入设备上一个与用户之间路由可达的三层接口 IP 地址（通常为 Loopback 接口 IP）。

- (2) 接入设备与 RADIUS 服务器之间进行 RADIUS 协议报文的交互，对用户身份进行验证。
- (3) 如果 RADIUS 认证成功，则接入设备上的本地 Portal 服务器向客户端发送登录成功页面，通知客户端认证（上线）成功。

2. 支持下发授权VLAN

二层 Portal 认证支持认证服务器下发授权 VLAN。当用户通过 Portal 认证后，如果认证服务器上配置了下发 VLAN 功能，那么认证服务器会将授权 VLAN 信息下发给接入设备，由接入设备将认证成功的用户加入对应的授权 VLAN 中，则端口上会生成该用户 MAC 对应的 MAC VLAN 表项，若该 VLAN 不存在，则接入设备首先创建 VLAN，而后将用户加入授权 VLAN 中。

通过支持下发授权 VLAN，可实现对已认证用户可访问网络资源的控制。

3. 支持Auth-Fail VLAN

Auth-Fail VLAN 功能允许用户在认证失败的情况下，可以访问某一特定 VLAN 中的资源，比如病毒补丁服务器，存储客户端软件或杀毒软件的服务器，进行升级客户端或执行其他一些用户升级程序。这个 VLAN 称之为 Auth-Fail VLAN。

二层 Portal 认证支持基于 MAC 的 Auth-Fail VLAN，如果接入用户的端口上配置了 Auth-Fail VLAN，则端口上会基于认证失败的 MAC 地址生成相应的 MAC VLAN 表项，认证失败的用户将会被加入 Auth-Fail VLAN 中。加入 Auth-Fail VLAN 中的用户可以访问该 VLAN 中的非 HTTP 资源，但用户的所有 HTTP 访问请求会被重定向到接入设备上认证，若用户仍然没有通过认证，则将继续处于 Auth-Fail VLAN 内；若认证成功，则回到加入 Auth-Fail VLAN 之前端口所在的 VLAN。处于 Auth-Fail VLAN 中的用户，若在指定时间（默认 90 秒）内无流量通过接入端口，则将离开该 VLAN，回到端口的初始 VLAN。



说明

用户加入授权 VLAN 或 Auth-Fail VLAN 后，需要自动申请或者手动更新客户端 IP 地址，以保证可以与授权 VLAN 或 Auth-Fail VLAN 中的资源互通。

4. 支持ACL下发

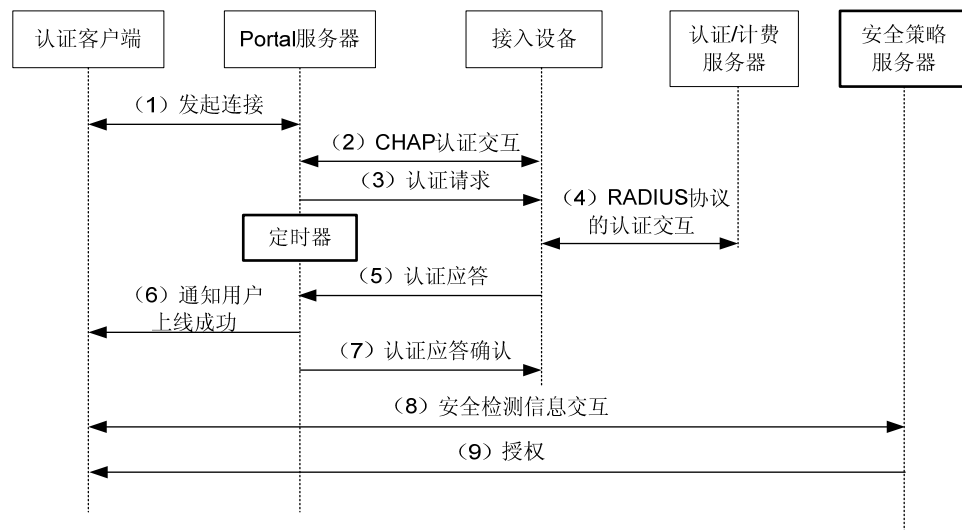
ACL（Access Control List，访问控制列表）提供了控制用户访问网络资源和限制用户访问权限的功能。当用户上线时，如果服务器上配置了授权 ACL，则设备会根据服务器下发的授权 ACL 对用户所在端口的数据流进行控制；在服务器上配置授权 ACL 之前，需要在设备上配置相应的规则。管理员可以通过改变服务器的授权 ACL 设置或设备上对应的 ACL 规则来改变用户的访问权限。

1.1.8 三层Portal认证过程

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1-5 直接认证/可跨三层 Portal 认证流程图



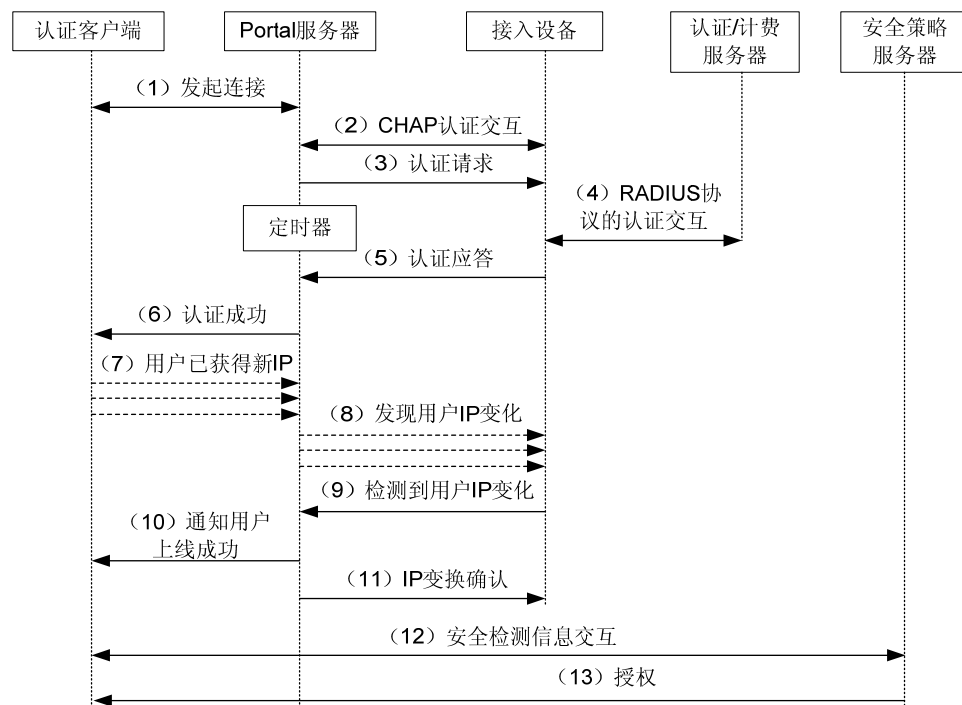
直接认证/可跨三层 Portal 认证流程：

- (1) Portal 用户通过 HTTP 协议发起认证请求。HTTP 报文经过接入设备时，对于访问 Portal 服务器或设定的免费访问地址的 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 服务器。Portal 服务器提供 Web 页面供用户输入用户名和密码来进行认证。
- (2) Portal 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。
- (3) Portal 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 服务器发送认证应答报文。
- (6) Portal 服务器向客户端发送认证通过报文，通知客户端认证（上线）成功。
- (7) Portal 服务器向接入设备发送认证应答确认。
- (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接入终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用户的安全性授权用户访问非受限资源，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(8)、(9)为 Portal 认证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1-6 二次地址分配认证方式流程图



二次地址分配认证流程：

(1)~(6)同直接/可跨三层 Portal 认证中步骤（1）~（6）。

(7) 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 服务器用户已获得新 IP 地址。

(8) Portal 服务器通知接入设备客户端获得新公网 IP 地址。

(9) 接入设备通过检测 ARP 协议报文发现了用户 IP 变化，并通告 Portal 服务器已检测到用户 IP 变化。

(10) Portal 服务器通知客户端上线成功。

(11) Portal 服务器向接入设备发送 IP 变化确认报文。

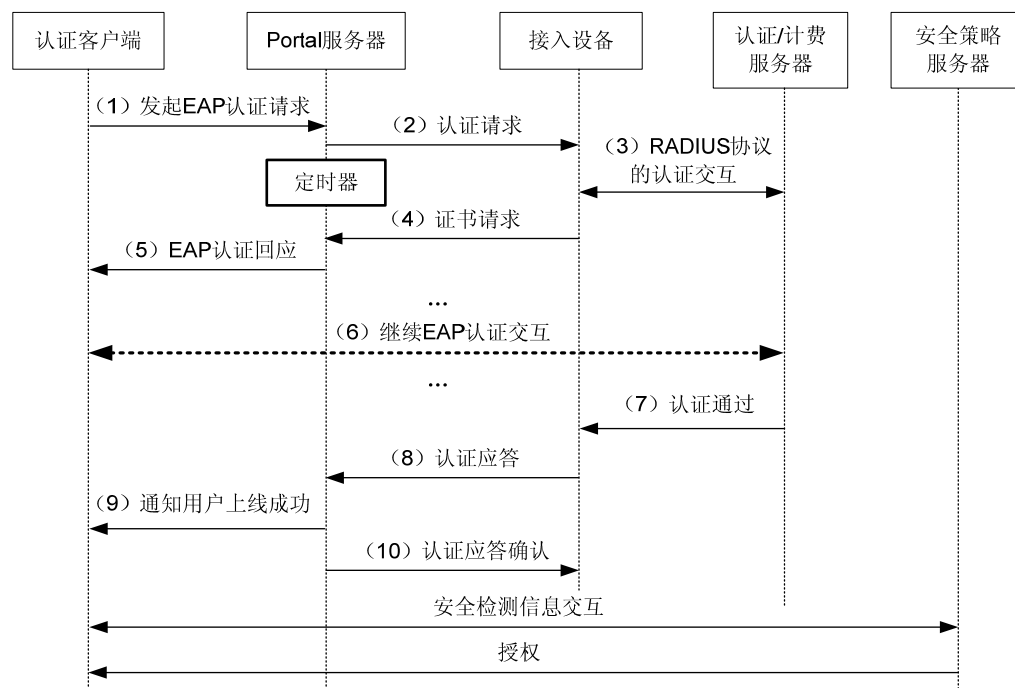
(12) 客户端和安全策略服务器之间进行安全信息交互。安全策略服务器检测接入终端的安全性是否合格，包括是否安装防病毒软件、是否更新病毒库、是否安装了非法软件、是否更新操作系统补丁等。

(13) 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，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(12)、(13)为 Portal 认证扩展功能的交互过程。

3. Portal支持EAP认证流程

图1-7 Portal 支持 EAP 认证流程图



支持 EAP 认证的 Portal 认证流程如下（各 Portal 认证方式下 EAP 认证的处理流程相同，此处仅以直接方式的 Portal 认证为例）：

- (1) Portal 客户端发起 EAP 认证请求，向 Portal 服务器发送 Identity 类型的 EAP 请求报文。
- (2) Portal 服务器向接入设备发送 Portal 认证请求报文，同时开启定时器等待 Portal 认证应答报文，该认证请求报文中包含若干个 EAP-Message 属性，这些属性用于封装 Portal 客户端发送的 EAP 报文，并可携带客户端的证书信息。
- (3) 接入设备接收到 Portal 认证请求报文后，构造 RADIUS 认证请求报文与 RADIUS 服务器进行认证交互，该 RADIUS 认证请求报文的 EAP-Message 属性值由接入设备收到的 Portal 认证请求报文中的 EAP-Message 属性值填充。
- (4) 接入设备根据 RADIUS 服务器的回应信息向 Portal 服务器发送证书请求报文，该报文中同样会包含若干个 EAP-Message 属性，可用于携带 RADIUS 服务器的证书信息，这些属性值由 RADIUS 认证回应报文中的 EAP-Message 属性值填充。
- (5) Portal 服务器接收到证书请求报文后，向 Portal 客户端发送 EAP 认证回应报文，直接将 RADIUS 服务器响应报文中的 EAP-Message 属性值透传给 Portal 客户端。
- (6) Portal 客户端继续发起的 EAP 认证请求，与 RADIUS 服务器进行后续的 EAP 认证交互，期间 Portal 认证请求报文可能会出现多次。后续认证过程与第一个 EAP 认证请求报文的交互过程类似，仅 EAP 报文类型会根据 EAP 认证阶段发展有所变化，此处不再详述。
- (7) EAP 认证通过后，RADIUS 服务器向接入设备发送认证通过响应报文，该报文的 EAP-Message 属性中封装了 EAP 认证成功报文（EAP-Success）。
- (8) 接入设备向 Portal 服务器发送认证应答报文，该报文的 EAP-Message 属性中封装了 EAP 认证成功报文。

(9) Portal 服务器根据认证应答报文中的认证结果通知 Portal 客户端认证成功。

(10) Portal 服务器向接入设备发送认证应答确认。

后续为 Portal 认证扩展功能的交互过程，可参考 CHAP/PAP 认证方式下的认证流程介绍，此处略。

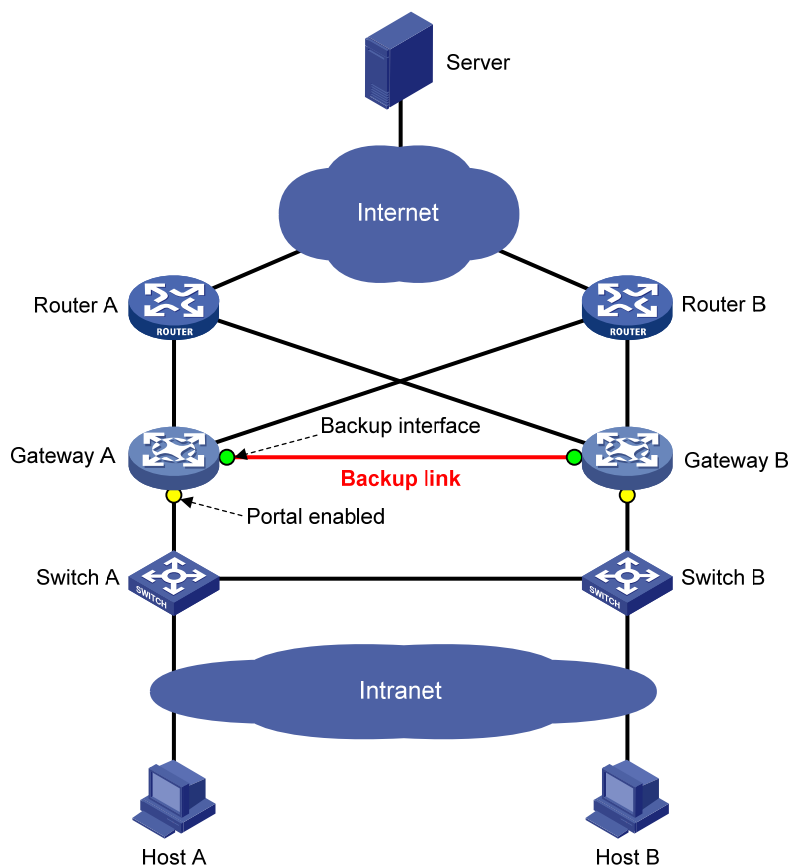
1.1.9 Portal支持双机热备

1. 概述

在当前的组网应用中，用户对网络可靠性的要求越来越高，特别是在一些重点的业务入口或接入点上需要保证网络业务的不间断性。双机热备技术可以保证这些关键业务节点在单点故障的情况下，信息流仍然不中断。

所谓双机热备，其实是双机业务备份。在两台设备上分别指定相同的备份 VLAN，专用于传输双机热备相关的报文。在设备正常工作时，对业务信息进行主备同步；在设备故障后，利用 VRRP 机制实现业务流量切换到备份设备，由备份设备继续处理业务，从而保证了当前的业务不被中断。关于双机热备的详细介绍请参见“可靠性配置指导”中的“双机热备”。

图1-8 双机热备组网图



如 图 1-8 所示，在一个典型的Portal双机热备组网环境中，用户通过Portal认证接入网络，为避免接入设备单机故障的情况下造成的Portal业务中断，接入设备提供了Portal支持双机热备功能。该功能是指，接入设备Gateway A和Gateway B通过备份链路互相备份两台设备上的Portal在线用户信息，实现当其中一台设备发生故障时，另外一台设备可以对新的Portal用户进行接入认证，并能够保证所有已上线Portal用户的正常数据通信。



说明

备份链路对于部分双机热备设备不是必须的，只要保证互为备份的设备上存在相同的 VLAN 专用于传输双机热备相关的报文。若组网中配置了专门的备份链路，则需要将两台设备上连接备份链路的物理接口加入备份 VLAN 中。

2. 基本概念

(1) 设备的工作状态

- 独立运行状态：设备未与其它设备建立备份连接时所处的一种稳定状态。
- 同步运行状态：设备与对端设备之间成功建立备份连接，可以进行数据备份时所处的一种稳定状态。

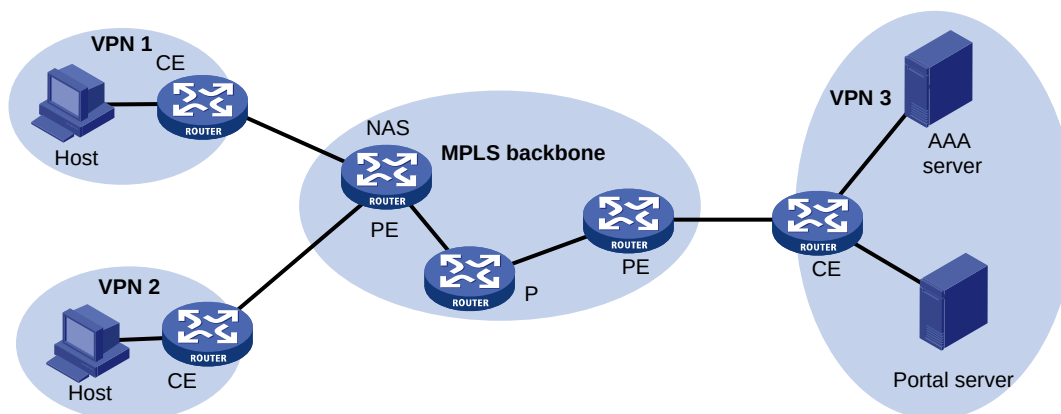
(2) 用户的工作模式

- **Stand-alone**：表示用户数据只在一台设备上存在。当前设备处于独立运行状态，或者当前设备处于同步运行状态但用户数据还未同步。
- **Primary**：表明用户是由本端设备上线，用户数据由本端设备生成。本端设备处于同步运行状态，可以处理并接收服务器发送的报文。
- **Secondary**：表明用户是由对端设备上线，用户数据是由对端设备同步到本端设备上的。本端设备处于同步运行状态，只接收并处理同步消息，不处理服务器发送的报文。

1.1.10 Portal支持多实例

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 Portal 用户要通过位于总部 VPN 中的服务器进行统一认证，则需要 Portal 支持多实例。通过 Portal 支持多实例，可实现 Portal 认证报文通过 MPLS VPN 进行交互。如下图所示，连接客户端的 PE 设备作为 NAS，通过 MPLS VPN 将私网客户端的 Portal 认证报文透传给网络另一端的私网服务器，并在 AAA 支持多实例的配合下，实现对私网 VPN 客户端的 Portal 接入认证，满足了私网 VPN 业务隔离情况下的客户端集中认证，且各私网的认证报文互不影响。

图1-9 Portal 支持多实例典型组网图





说明

- 在 MCE 设备上进行的 Portal 接入认证也可支持多实例功能。关于 MCE 的相关介绍请参见“MPLS 配置指导”中的“MCE”。
- 关于 AAA 支持多实例的相关介绍请参见“安全配置指导”中的“AAA”。
- 本特性不支持多 VPN 间的地址重叠。

1.2 Portal配置任务简介

表1-1 二层 Portal 配置任务简介

配置任务		说明	详细配置
指定二层Portal认证的本地Portal服务器IP地址		必选	1.4.1
配置本地Portal服务器	自定义认证页面	可选	1.5.1
	配置本地Portal服务器	必选	1.5.2
使能二层Portal		必选	1.6.1
控制Portal用户的接入	配置免认证规则	可选	1.7.1
	配置Portal最大用户数		1.7.3
	指定Portal用户使用的认证域		1.7.4
	配置二层Portal支持Web代理		1.7.5
	配置Portal用户认证端口的自动迁移功能		1.7.6
配置Portal认证的Auth-Fail VLAN		可选	1.8
指定Portal用户认证成功后认证页面的自动跳转目的网站地址		可选	1.12
配置二层Portal用户的在线检测功能		可选	1.13.1
强制Portal用户下线		可选	1.14

表1-2 三层 Portal 配置任务简介

配置任务		说明	详细配置
指定三层Portal认证的Portal服务器监听IP地址		必选	1.4.2
使能三层Portal		必选	1.6.2
控制Portal用户的接入	配置免认证规则	可选	1.7.1
	配置源认证网段		1.7.2
	配置Portal最大用户数		1.7.3
	指定Portal用户使用的认证域		1.7.4

配置任务		说明	详细配置
配置接口发送RADIUS报文的相关属性	配置接口的NAS-Port-Type	可选	1.9.1
	配置接口的NAS-ID Profile		1.9.2
配置接口发送Portal报文使用的源地址		可选	1.10
配置Portal支持双机热备		可选	1.11
指定Portal用户认证成功后认证页面的自动跳转目的网站地址		可选	1.12
配置Portal探测功能	配置Portal服务器探测功能	可选	1.13.2
	配置Portal用户信息同步功能		1.13.3
强制Portal用户下线		可选	1.14

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 服务器、RADIUS 服务器已安装并配置成功。本地 Portal 认证无需单独安装 Portal 服务器。
- 若采用二次地址分配认证方式，接入设备需启动 DHCP 中继的安全地址匹配检查功能，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 的扩展功能，需要安装并配置 CAMS EAD/iMC EAD。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受限资源 ACL 号、非受限资源 ACL 号对应。接入设备上的安全策略服务器配置请参见“安全配置指导”中的“AAA”。



说明

- 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/iMC EAD 安全策略组件联机帮助。
- 受限资源 ACL、非受限资源 ACL 分别对应安全策略服务器中的隔离 ACL 与安全 ACL。
- 如果接入设备上的授权 ACL 配置被修改，则修改后的 ACL 不对已经在线的 Portal 用户生效，只能对新上线的 Portal 用户有效。
- 为保证 Portal 认证可正常进行，请将接入设备系统名称的长度限制在 16 个字符以内。

1.4 指定Portal服务器

1.4.1 指定二层Portal认证的本地Portal服务器监听IP地址

二层 Portal 认证使用本地 Portal 服务器，因此需要将设备上一个与 Portal 客户端路由可达的三层接口 IP 地址指定为本地 Portal 服务器的监听 IP 地址，并强烈建议使用设备上空闲的 Loopback 接口的 IP 地址，利用 LoopBack 接口状态稳定的优点，避免因接口故障导致用户无法打开认证页面的问题。另外，由于发送到 LoopBack 接口的报文不会被转发到网络中，当请求上线的用户数目较大时，可减轻对系统性能的影响。

表1-3 指定二层 Portal 认证的本地 Portal 服务器监听 IP 地址

操作	命令	说明
进入系统视图	system-view	-
指定二层Portal认证的本地Portal服务器监听IP地址	portal local-server ip ip-address	必选 缺省情况下，没有指定本地Portal服务器的监听IP地址



说明

已配置的本地 Portal 服务器监听 IP 地址仅在二层 Portal 认证未在任何端口上使能时才可以被删除或修改。

1.4.2 指定三层Portal认证的Portal服务器

本配置用于指定 Portal 服务器的相关参数，主要包括服务器 IP 地址、共享加密密钥、服务器端口号以及服务器提供的 Web 认证地址。

表1-4 指定三层 Portal 认证的 Portal 服务器

操作	命令	说明
进入系统视图	system-view	-
指定三层Portal认证的Portal服务器	portal server server-name { ip ipv4-address [key [cipher simple] key-string port port-id url url-string vpn-instance vpn-instance-name] * ipv6 ipv6-address [key [cipher simple] key-string port port-id url url-string] * }	必选 缺省情况下，没有指定三层Portal认证的Portal服务器



说明

- 已配置的 Portal 服务器参数仅在该 Portal 服务器未被接口引用时才可以被删除或修改。
- 为保证设备能够向 MPLS VPN 私网中的 Portal 服务器发送报文，指定 Portal 服务器时需指定服务器所属的 VPN 且必须和该服务器所在的 VPN 保持一致。

1.5 配置本地Portal服务器

本特性用于配合 Portal 本地认证，且仅在使用本地 Portal 服务器时必配。使用本地 Portal 服务器进行认证时，本地 Portal 服务器负责向用户推出认证页面。认证页面的内容和样式可自定义，若未配置自定义认证页面，则向用户推出系统提供的缺省认证页面。

1.5.1 自定义认证页面文件

用户自定义的认证页面为 HTML 文件的形式，压缩后保存在本地设备的存储设备中。每套认证页面可包括六个主索引页面（登录页面、登录成功页面、登录失败页面、在线页面、系统忙页面、下线成功页面）及其页面元素（认证页面需要应用的各种文件，如 Logon.htm 页面中的 back.jpg），每个主索引页面可以引用若干页面元素。若用户只自定义了部分主索引页面，则其余主索引页面使用系统提供的缺省认证页面。

用户在自定义这些页面时需要遵循一定的规范，否则会影响本地 Portal 服务器功能的正常使用和系统运行的稳定性。

1. 文件名规范

主索引页面文件名不能自定义，必须使用 [表 1-5](#) 中所列的固定文件名。

表1-5 认证页面文件名

主索引页面	文件名
登录页面	logon.htm
登录成功页面	logonSuccess.htm
登录失败页面	logonFail.htm
在线页面 用于提示用户已经在线	online.htm
系统忙页面 用于提示系统忙或者该用户正在登录过程中	busy.htm
下线成功页面	logoffSuccess.htm



说明

主索引页面文件之外的其他文件名可由用户自定义，但需注意文件名和文件目录名中不能含有中文且不区分大小写。

2. 页面请求规范

本地 Portal 服务器只能接受 Get 请求和 Post 请求。

- Get 请求用于获取认证页面中的静态文件，其内容不能为递归内容。例如，Logon.htm 文件中包含了 Get ca.htm 文件的内容，但 ca.htm 文件中又包含了对 Logon.htm 的引用，这种递归引用是不允许的。
- Post 请求用于用户提交用户名和密码以及用户执行登录、下线操作。

3. Post请求中的属性规范

(1) 认证页面中表单（Form）的编辑必须符合以下原则：

- 认证页面可以含有多个 Form，但是必须有且只有一个 Form 的 action=logon.cgi，否则无法将用户信息送到本地 Portal 服务器。
- 用户名属性固定为"PtUser"，密码属性固定为"PtPwd"。
- 需要有用于标记用户登录还是下线的属性"PtButton"，取值为"Logon"表示登录，取值为"Logoff"表示下线。
- 登录 Post 请求必须包含"PtUser"，"PtPwd"和"PtButton"三个属性。
- 下线 Post 请求必须包含"PtButton"这个属性。

(2) 需要包含登录 Post 请求的页面有 logon.htm 和 logonFail.htm。

logon.htm 页面脚本内容的部分示例：

```
<form action=logon.cgi method = post >
<p>User name:<input type="text" name = "PtUser" style="width:160px;height:22px"
maxlength=64>
<p>Password :<input type="password" name = "PtPwd" style="width:160px;height:22px"
maxlength=32>
<p><input type=SUBMIT value="Logon" name = "PtButton" style="width:60px;"
onclick="form.action=form.action+location.search;>
</form>
```

(3) 需要包含下线 Post 请求的页面有 logonSuccess.htm 和 online.htm。

online.htm 页面脚本内容的部分示例：

```
<form action=logon.cgi method = post >
<p><input type=SUBMIT value="Logoff" name="PtButton" style="width:60px;">
</form>
```

4. 页面文件压缩及保存规范

- 完成所有认证页面的编辑之后，必须按照标准 Zip 格式将其压缩到一个 Zip 文件中，该 Zip 文件的文件名只能包含字母、数字和下划线。缺省认证页面文件必须以 defaultfile.zip 为文件名保存。
- 压缩后的 Zip 文件中必须直接包含认证页面，不允许存在间接目录。

- 压缩生成的 Zip 文件可以通过 FTP 或 TFTP 的方式上传至设备,并保存在设备的指定目录下。
缺省认证页面文件必须保存在设备的根目录下, 非缺省认证页面文件可以保存在设备根目录下或者根目录的 portal 目录下。

Zip 文件保存目录示例:

```
<Sysname> dir
Directory of flash:/portal/
 0      -rw-          1405  Feb 28 2011 15:53:31  2.zip
 1      -rw-          1405  Feb 28 2011 15:53:20  1.zip
 2      -rw-          1405  Feb 28 2011 15:53:39  3.zip
 3      -rw-          1405  Feb 28 2011 15:53:44  4.zip
2540 KB total (1319 KB free)
```

5. 页面文件大小和内容规范

为了方便系统推出自定义的认证页面, 认证页面在文件大小和内容上需要有如下限制:

- 每套页面(包括主索引页面文件及其页面元素)压缩后的 Zip 文件大小不能超过 500K 字节。
- 每个单独页面(包括单个主索引页面文件及其页面元素)压缩前的文件大小不能超过 50K 字节。
- 页面元素只能包含 HTML、JS、CSS 和图片之类的静态内容。

6. 关闭登录成功/在线页面后强制用户下线

用户认证成功后, 系统会推出登录成功页面(文件名为 logonSuccess.htm), 认证通过后再次通过登录页面进行认证操作, 系统会推出在线页面(文件名为 online.htm)。若希望用户关闭这两个页面的同时, 触发设备执行强制当前在线用户下线的操作, 就需要按照如下要求在这两个页面文件的脚本文件中增加如下内容。

- (1) 添加对 JS 文件“pt_private.js”的引用;
- (2) 添加触发页面卸载的函数“pt_unload()”;
- (3) 添加 Form 的提交事件处理函数“pt_submit()”;
- (4) 添加页面加载的初始化函数“pt_init()”。

需要在 logonSuccess.htm 和 online.htm 页面脚本中增加的内容如示例中突出显示部分:

```
<html>
<head>
<script type="text/javascript" language="javascript" src="pt_private.js"></script>
</head>
<body onload="pt_init();" onbeforeunload="return pt_unload();">
... ..
<form action=logon.cgi method = post onsubmit="pt_submit()">
... ..
</body>
</html>
```

7. 认证成功后认证页面自动跳转

若要支持认证成功后自定义认证页面的自动跳转功能, 即认证页面会在用户认证成功后自动跳转到设备指定的网站页面, 则需要按照如下要求在认证页面 logon.htm 和 logonSuccess.htm 的脚本文件中做如下改动。

- (1) 将 logon.htm 文件中的 Form 的 target 值设置为“blank”。

修改的脚本内容如下突出显示部分所示：

```
<form method=post action=logon.cgi target="blank">
```

(2) logonSuccess.htm 文件添加页面加载的初始化函数 “pt_init()”。

增加的脚本内容如下突出显示部分所示：

```
<html>
<head>
<title>LogonSucceeded</title>
<script type="text/javascript" language="javascript" src="pt_private.js"></script>
</head>
<body onload="pt_init();" onbeforeunload="return pt_unload();">
...
</body>
</html>
```

 说明

- 推荐使用 IE6.0 版本以上的浏览器。
- 需要用户浏览器设置为允许弹出窗口，或者将设备的 IP 地址设置为允许弹出的网站地址。若浏览器禁止弹出窗口，则关闭登录成功或在线页面时会提示用户无法下线，用户可以点击“取消”回到原页面。
- 目前，仅 IE 浏览器、Firefox 浏览器和 Safari 浏览器支持关闭登录成功/在线页面后的强制用户下线功能，而其它浏览器（例如 Chrome 浏览器、Opera 浏览器等）均不支持该功能。
- 刷新登录成功/在线页面或者使该页面跳转到别的网站上时都会触发强制用户下线事件。

1.5.2 配置本地Portal服务器

在本配置任务中，通过指定 Portal 客户端和本地 Portal 服务器的之间采用的通信协议（HTTP 或 HTTPS），接入设备上的本地 Portal 服务器功能才能生效。

1. 配置准备

若指定本地 Portal 服务器支持的协议类型为 HTTPS，则需要首先完成以下配置：

- 配置 PKI 策略，并成功申请本地证书和 CA 证书，具体配置请参见“安全配置指导”中的“PKI”。
- 配置 SSL 服务器端策略，并指定使用已配置的 PKI 域。具体配置请参见“安全配置指导”中的“SSL”。

由于指定本地 Portal 服务器支持的协议类型时，本地 Portal 服务器将同时加载已保存在根目录的缺省认证页面文件，因此若需要使用自定义的缺省认证页面文件，则需要首先完成对它的编辑和保存工作，否则使用系统默认的缺省认证页面。

2. 配置本地Portal服务器

表1-6 配置本地 Portal 服务器

操作	命令	说明
进入系统视图	system-view	-

操作	命令	说明
配置本地Portal服务器支持的协议类型，并同时加载缺省认证页面文件	portal local-server { http https server-policy policy-name }	必选 缺省情况下，本地Portal服务器不支持任何协议类型
配置本地Portal服务器缺省认证页面的欢迎信息	portal server banner banner-string	可选 缺省情况下，无Web页面欢迎信息

1.6 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。

1.6.1 使能二层Portal认证

在使能二层 Portal 认证之前，需要满足以下要求：

- 已经指定了本地 Portal 服务器的监听 IP 地址；
- 未在任何接口上使能三层 Portal 认证。

表1-7 使能二层 Portal 认证

操作	命令	说明
进入系统视图	system-view	-
进入二层以太网端口视图	interface interface-type interface-number	-
在端口上使能二层Portal认证	portal local-server enable	必选 缺省情况下，未使能二层Portal认证



说明

- 为使二层端口上的 Portal 认证功能正常运行，不建议端口上同时使能端口安全、802.1X 的 Guest VLAN 或 802.1X 的 EAD 快速部署功能。
- 若要支持授权 VLAN 下发功能，则需要在端口上使能 MAC VLAN 功能。

1.6.2 使能三层Portal认证

在使能三层 Portal 认证之前，需要满足以下要求：

- 使能 Portal 的接口已配置或者获取了合法的 IP 地址；
- 使能 Portal 的接口未加入聚合组；
- 接口上引用的 Portal 服务器名已经存在；
- 未在任何端口上使能二层 Portal 认证。

表1-8 使能三层 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	-
在接口上使能三层Portal认证	portal server server-name method { direct layer3 redhcp }	必选 缺省情况下，没有使能三层Portal认证



说明

- 加入聚合组的三层接口不能使能 Portal，反之亦然。
- 设备向 Portal 服务器主动发送报文时使用的目的端口号必须与远程 Portal 服务器实际使用的端口号保持一致。
- 已配置的 Portal 服务器及其参数仅在该 Portal 服务器未被接口引用时才可以被删除或修改。
- 对于跨三层设备支持 Portal 认证的应用只能配置可跨三层 Portal 认证方式（**portal server server-name method 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，允许用户在未通过 Portal 认证时以公网地址向外发送报文，但相应的回应报文则受限制。
- 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使用 IPv4 Portal 服务器的三层 Portal 认证和使用 IPv6 Portal 服务器的三层 Portal 认证。但是，不允许同时使能使用相同 IP 协议的 Portal 服务器的三层 Portal 认证。

1.7 控制Portal用户的接入

1.7.1 配置免认证规则

通过配置免认证规则(**free-rule**)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。

对于二层 Portal 认证，只能配置从任意源地址（即 **source any**）到任意或指定目的地址的免认证规则。配置了到指定目的地址的免认证规则后，用户不需要通过 Portal 认证即可访问指定目的网段或地址的网络资源，且用户访问这些资源的 HTTP 请求不会被重定向到 Portal 认证页面上。通常，可以将一些提供特定服务器资源（例如软件升级服务器）的 IP 地址指定为免认证规则的目的 IP，便于二层 Portal 用户在免认证的情况下获取特定的服务资源。

表1-9 配置免认证规则

操作	命令	说明
进入系统视图	system-view	-
配置Portal的免认证规则	<pre>portal free-rule rule-number { destination { any ip { ip-address mask { mask-length netmask } any } [tcp tcp-port-number udp udp-port-number] } source { any [interface interface-type interface-number ip { ip-address mask { mask-length mask } any } [tcp tcp-port-number udp udp-port-number] mac mac-address vlan vlan-id] * } } *</pre> <pre>portal free-rule rule-number { destination { any ipv6 { ipv6-address prefix-length any } } source { any [interface interface-type interface-number ipv6 { ipv6-address prefix-length any } mac mac-address vlan vlan-id] * } } *</pre>	二者至少选其一



说明

- 如果免认证规则中同时配置了 **vlan** 和 **interface** 项，则要求 **interface** 属于该 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。
- 加入聚合组的二层接口不能被指定为免认证规则的源接口，反之亦然。

1.7.2 配置源认证网段



说明

本特性仅三层 Portal 认证支持。

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。

表1-10 配置源认证网段

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
配置源认证网段	portal auth-network { <i>ipv4-network-address</i> { <i>mask-length</i> <i>mask</i> } ipv6 <i>ipv6-network-address</i> <i>prefix-length</i> }	可选 缺省情况下，源IPv4认证网段为0.0.0.0/0，源IPv6认证网段为::/0，表示对来自任意网段的用户都进行Portal认证



说明

- 源认证网段配置仅对可跨三层 Portal 认证有效。直接认证方式的认证网段为任意源 IP，二次地址分配方式的认证网段为由接口私网 IP 决定的私网网段。
- 可通过多次执行本命令，配置多个源认证网段。

1.7.3 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。

表1-11 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 <i>max-number</i>	必选 缺省情况下，S5500-28SC-HI和S5500-52SC-HI交换机的Portal最大用户数为1000；本系列交换机其它机型，Portal最大用户数为3000



说明

- 交换机实际下发的 Portal 最大的用户数和设备的 ACL 资源有关。
- 如果配置的 Portal 最大用户数小于当前已经在线的 Portal 用户数，则该命令可以执行成功，且在线 Portal 用户不受影响，但系统将不允许新的 Portal 用户接入。

1.7.4 指定Portal用户使用的认证域

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对不同接口指定不同的认证域，从而增加了管理员部署 Portal 接入策略的灵活性。

表1-12 指定 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 <i>interface-type</i> <i>interface-number</i>	-
指定Portal用户使用的认证域	portal domain [ipv6] <i>domain-name</i>	必选 缺省情况下,未指定Portal用户使用的认证域



说明

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 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”。

1.7.5 配置二层Portal认证支持Web代理

对于二层 Portal 认证,缺省情况下,设备不支持配置了 Web 代理服务器的用户浏览器发起的 Portal 认证。若用户使用配置了 Web 代理服务器的浏览器上网,则用户的这类 HTTP 请求报文将被丢弃,而不能触发 Portal 认证。这种情况下,网络管理员可以通过在设备上添加 Web 代理服务器端口号,来允许使用 Web 代理服务器的用户浏览器发起的 HTTP 请求也可以触发 Portal 认证。

表1-13 配置允许触发 Portal 认证的 Web 代理服务器端口

配置步骤	命令	说明
进入系统视图	system-view	-
添加允许触发Portal认证的Web代理服务器端口	portal web-proxy port <i>port-number</i>	必选 缺省情况下,不存在允许触发Portal认证的Web代理服务器端口



说明

- 如果用户浏览器采用 WPAD (Web Proxy Auto-Discovery, Web 代理服务器自动发现) 方式自动配置 Web 代理,则不仅需要网络管理员在设备上添加 Web 代理服务器端口,还需要配置免认证规则,允许目的 IP 为 WPAD 主机 IP 地址的用户报文免认证。
- 除了网络管理员需要在设备上添加指定的 Web 代理服务器端口,还需要用户在浏览器上将设备的本地 Portal 服务器监听 IP 地址配置为 Web 代理服务器的例外地址,避免 Portal 用户发送给本地 Portal 服务器的 HTTP 报文被发送到 Web 代理服务器上,从而影响正常的 Portal 认证。

1.7.6 配置Portal用户认证端口的自动迁移功能



说明

本特性仅二层 Portal 认证支持。

在用户和设备之间存在 Hub、二层交换机或 AP 的组网环境下，若在线用户在未下线的情况下从同一设备上的当前认证端口离开并迁移到其它使能了二层 Portal 的认证端口上接入时，由于原端口上仍然存在该用户的认证信息，因此设备默认不允许用户在新端口上认证上线。

开启本功能后，设备允许在线用户离开当前端口后在新端口上上线，具体分为以下两种情况：

- 若原认证端口状态未 **down**，且用户先后接入的两个端口属于同一个 **VLAN**，则用户不需要重新认证就能够继续以在线状态在新的端口上访问网络，并按照新的端口信息继续计费；
- 若原认证端口状态变为 **down**，或者原认证端口状态未 **down** 但是两个认证端口所属的 **VLAN** 不同，则设备会将用户在原端口上的认证信息删除掉，并要求用户在新端口上重新进行认证。

表1-14 配置 Portal 用户认证端口的自动迁移功能

配置步骤	命令	说明
进入系统视图	system-view	-
开启Portal用户认证端口的自动迁移功能	portal move-mode auto	必选 缺省情况下，Portal用户认证端口的自动迁移功能处于关闭状态



说明

用户迁移到新端口上之后，若设备发现该用户具有授权属性（例如授权 **VLAN**），则设备会尝试在新的端口上添加该用户的授权信息，若授权信息添加失败，设备会删除原端口上的用户信息，要求用户重新进行认证。

1.8 配置Portal认证的Auth-Fail VLAN



说明

本特性仅二层 Portal 认证支持。

通过该配置可以指定 Portal 用户认证失败后加入的 **VLAN**。

进行本配置之前，请首先创建需要配置为 Auth-Fail VLAN 的 **VLAN**。

表1-15 配置 Portal 认证的 Auth-Fail VLAN

配置步骤	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	-
配置端口的Portal认证的Auth-Fail VLAN	portal auth-fail vlan authfail-vlan-id	必选 缺省情况下，端口没有配置 Portal认证的Auth-Fail VLAN

 说明

- 为使端口的 Portal 认证的 Auth-Fail VLAN 生效，还必须使能端口上的 MAC VLAN 功能。MAC VLAN 功能的具体配置请参考“二层技术-以太网交换配置指导”中的“VLAN”。
- 不同的端口可以配置不同的 Portal 认证的 Auth-Fail VLAN，但一个端口最多只能配置一个 Portal 认证的 Auth-Fail VLAN。
- 端口上 Portal 认证失败产生的 MAC VLAN 表项不会覆盖已存在的其它认证方式产生的 MAC VLAN 表项。

1.9 配置接口发送RADIUS报文的相关属性

 说明

本特性仅三层 Portal 认证支持。

1.9.1 配置接口的NAS-Port-Type

RADIUS 标准属性 NAS-Port-Type 用于表示用户接入的端口类型。当接口上有 Portal 用户上线时候，若该接口上配置了 NAS-Port-Type，则使用本命令配置的值作为向 RADIUS 服务器发送的 RADIUS 请求报文的 NAS-Port-Type 属性值，否则使用接入设备获取到的用户接入的端口类型填充该属性。若作为 Portal 认证接入设备的 BAS（Broadband Access Server，宽带接入服务器）与 Portal 客户端之间跨越了多个网络设备，则可能无法正确获取到接入用户的实际端口信息，例如对于 Portal 认证接入的无线客户端，BAS 获取到的接入端口类型有可能是设备上认证该用户的有线接口类型。因此，为保证 BAS 能够向 RADIUS 服务器正确传递用户的接入端口信息，需要网络管理员在了解用户的实际接入环境后，通过本命令指定相应的 NAS-Port-Type。

表1-16 配置接口的 NAS-Port-Type

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 <i>interface-type</i> <i>interface-number</i>	-
配置接口的NAS-Port-Type	portal nas-port-type { ethernet wireless }	必选 缺省情况下，未指定接口的NAS-Port-Type

1.9.2 配置接口的NAS-ID Profile

在某些组网环境下，依靠 VLAN 来确定用户的接入位置，网络运营商需要使用 NAS-Identifier 来标识用户的接入位置。当接口上有 Portal 用户上线时，若该接口上指定了 NAS-ID Profile，则接入设备会根据指定的 Profile 名字和用户接入的 VLAN 来获取与此 VLAN 绑定的 NAS-ID，此 NAS-ID 的值将作为向 RADIUS 服务器发送的 RADIUS 请求报文中的 NAS-Identifier 属性值。

本特性中指定的 Profile 名字用于标识 VLAN 和 NAS-ID 的绑定关系，该绑定关系由 AAA 中的 **nas-id id-value bind vlan vlan-id** 命令生成，有关该命令的具体情况请参见“安全命令参考”中的“AAA”。

在接口上未指定 NAS-ID Profile 或指定的 Profile 中没有找到匹配的绑定关系的情况下，使用设备名作为接口的 NAS-ID。

表1-17 配置接口的 NAS-ID Profile

操作	命令	说明
进入系统视图	system-view	-
创建NAS-ID Profile，并进入NAS-ID-Profile视图	aaa nas-id profile <i>profile-name</i>	必选 该命令的具体情况请参见“安全命令参考”中的“AAA”
设置NAS-ID与VLAN的绑定关系	nas-id nas-identifier bind vlan <i>vlan-id</i>	必选 该命令的具体情况请参见“安全命令参考”中的“AAA”
退出当前视图	quit	-
进入接口视图	interface <i>interface-type</i> <i>interface-number</i>	-
指定接口的NAS-ID Profile	portal nas-id-profile <i>profile-name</i>	必选 缺省情况下，未指定NAS-ID Profile

1.10 配置接口发送Portal报文使用的源地址



说明

本特性仅三层 Portal 认证支持。

通过在使能 Portal 的接口上配置发送 Portal 报文使用的源地址，可以保证接入设备以此 IP 地址为源地址向 Portal 服务器发送报文，且 Portal 服务器向接入设备回应的报文以此 IP 地址为目的地址。

表1-18 配置接口发送 Portal 报文使用的源地址

操作	命令	说明
进入系统视图	system-view	-
进入接口视图	interface <i>interface-type</i> <i>interface-number</i>	-
配置接口发送Portal报文使用的源地址	portal nas-ip { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> }	可选 缺省情况下，未指定接口发送Portal报文使用的源地址，即以接入用户的接口地址作为发送Portal报文的源地址 在NAT组网环境下，此地址建议配置为接口的公网IP地址

1.11 配置Portal支持双机热备



说明

本特性仅三层 Portal 认证支持。

为实现 Portal 支持双机热备，在保证实现业务流量切换的 VRRP 机制工作正常的前提下，还需要完成以下配置任务：

- 指定备份 Portal 业务所涉及的接口，本文简称为业务备份接口，并在该业务备份接口上使能 Portal。
- 配置业务备份接口所属的 Portal 备份组，两台设备上有备份关系的业务备份接口属于同一个 Portal 备份组。
- 配置双机热备模式下的设备 ID，保证设备上用户的全局唯一性，该设备 ID 必须不同于对端的设备 ID。
- 配置设备发送 RADIUS 报文的备份源 IP 地址，使得对端设备也能够收到服务器发送的报文。备份源 IP 地址必须指定为对端设备发送 RADIUS 报文使用的源 IP 地址。（此配置可选）
- 指定备份 VLAN，并使能双机热备功能，相关配置请参考“可靠性配置指导”的“双机热备”。

对端设备上也需要完成以上配置，才能保证双机热备环境下的 Portal 业务备份正常进行。

当双机工作状态由独立运行状态转换为同步运行状态，且 Portal 备份组已生效时，两台设备上已经上线的 Portal 用户数据会开始进行相互的备份。

表1-19 配置 Portal 支持双机热备

操作	命令	说明
进入系统视图	system-view	-
进入接口视图	interface <i>interface-type</i> <i>interface-number</i>	-

操作	命令	说明
配置业务备份接口所属的Portal备份组	portal backup-group group-id	必选 缺省情况下，业务备份接口不属于任何Portal备份组 相互备份的两台设备上业务备份接口所属的Portal备份组必须相同
退回系统视图	quit	-
配置双机热备模式下的设备ID	nas device-id device-id	必选 缺省情况下，设备运行在单机模式下，无设备ID 具体配置请参考“安全命令参考”中的“AAA”
指定设备发送RADIUS报文使用的备份源IP地址	radius nas-backup-ip ip-address	二者可选其一
	radius scheme radius-scheme-name nas-backup-ip ip-address	缺省情况下，未指定发送RADIUS报文使用的备份源IP地址 若将设备发送RADIUS报文使用的源IP地址指定为VRRP上行链路所在备份组的虚拟IP地址，则不需要本配置 具体配置请参考“安全命令参考”中的“AAA”

说明

- 双机热备模式下，设备不支持业务备份接口使能二次地址方式的 Portal 认证。
- 工作于双机热备模式下的任何一台设备上的用户被强制下线，都会导致另外一台设备上的相同用户信息同时被删除。设备和 Portal 服务器上均可执行强制用户下线操作，例如，设备上可通过执行命令 **cut connetion**、**portal delete-user** 来强制用户下线。
- 互为备份的两台设备上的 AAA 及 Portal 的相关配置必须保持一致，比如两台设备上都必须配置相同的 Portal 服务器。

注意

- 由于配置或改变设备的设备 ID 会导致设备上所有在线用户被强制下线，因此需慎重操作，并建议该配置成功执行后，保存配置并重启设备。
- 在双机热备运行的情况下，不要删除已配置的备份源 IP 地址，否则可能会导致备份设备上的在线用户无法收到服务器发送的报文。

1.12 指定Portal用户认证成功后认证页面的自动跳转目的网站地址

未认证用户上网时，首先会主动或被强制登录到 Portal 认证页面进行认证，当用户输入正确的认证信息且认证成功后，若设备上指定了认证页面的自动跳转目的网站地址，则认证成功的用户将在一定的时间间隔（由 **wait-time** 参数配置）之后被强制登录到该指定的目的网站页面。

表1-20 指定 Portal 用户认证成功后认证页面的自动跳转目的 URL

配置步骤	命令	说明
进入系统视图	system-view	-
指定Portal用户认证成功后认证页面的自动跳转目的网站地址	portal redirect-url <i>url-string</i> [wait-time <i>period</i>]	必选 缺省情况下，用户认证成功后认证页面将会跳转到用户初始访问的网站页面



说明

- 对于三层远程 Portal 认证,该特性需要与支持自动跳转页面功能的 iMC Portal 服务器配合使用。
- wait-time** 参数只对本地 Portal 认证有效，对于远程 Portal 认证无效。
- 本地 Portal 认证时，若用户初始访问的页面 URL 长度超过 255 个字符，则在未指定跳转目的网站地址的情况下，用户认证成功之后的认证页面无法返回到初始页面。

1.13 配置Portal探测功能

1.13.1 配置二层Portal用户在线检测功能



说明

本特性仅二层 Portal 认证支持。

二层端口上有 Portal 用户上线后，设备会启动一个用户在线检测定时器，定期对该端口上的所有在线用户的 MAC 地址表项进行检测，查看定时器超时前该用户是否有报文发送到设备上(该用户 MAC 地址表项是否被命中过)，来确认该用户是否在线，以便及时发现异常离线用户。若发现某用户 MAC 地址表项已经被老化或检测间隔内未收到过该用户的报文，则认为一次检测失败，连续两次检测失败后，设备会强制该用户下线。

表1-21 配置二层 Portal 用户在线检测时间间隔

操作	命令	说明
进入系统视图	system-view	-
进入接口视图	interface <i>interface-type</i> <i>interface-number</i>	-

操作	命令	说明
配置二层Portal用户在线检测时间间隔	portal offline-detect interval <i>offline-detect-interval</i>	必选 缺省情况下，二层Portal用户在线检测时间间隔为300秒

1.13.2 配置Portal服务器探测功能



说明

本特性仅三层 Portal 认证支持。

在 Portal 认证的过程中，如果接入设备与 Portal 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 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。例如，当接入设备发现 Portal 服务器不可达时，可打开网络限制，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，该功能为一种灵活的用户接入方案。

通过配置本特性，设备可以对指定 Portal 服务器的可达状态进行探测，具体配置包括如下几项：

(1) 探测方式（可以选择其中一种或同时使用两种）

- 探测 HTTP 连接：接入设备定期向 Portal 服务器的 HTTP 服务端口发起 TCP 连接，若连接成功建立则表示此服务器的 HTTP 服务已开启，就认为一次探测成功且服务器可达。若连接失败则认为一次探测失败。
- 探测 Portal 心跳报文：支持 Portal 逃生心跳功能的 Portal 服务器（目前仅 iMC 支持）会定期向接入设备发送 Portal 心跳报文，设备通过检测此报文来判断服务器的可达状态：若设备在指定的周期内收到 Portal 心跳报文或者其它认证报文，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。

(2) 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。

(3) 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：Portal 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 服务器名以及该服务器的当前状态。
- 发送日志：Portal 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 服务器名以及该服务器状态改变前后的状态。
- 打开网络限制（Portal 逃生）：Portal 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，若设备收到 Portal 服务器的心跳报文，或者收到其它认证报文（上线报文、下线报文等），则恢复该端口的 Portal 认证功能。

对于以上配置项，可根据实际情况进行组合使用，但需要注意以下几点：

- 如果同时指定了两种探测方式，则只要使用任何一种探测方式进行探测的失败次数达到最大值就认为服务器不可达。在服务器不可达状态下，只有使用两种探测方式的探测都成功才能认为服务器恢复为可达状态。
- 如果同时指定了多种操作，则 Portal 服务器可达状态改变时系统可并发执行多种操作。
- 对指定 Portal 服务器配置的探测功能，只有接口上使能了 Portal 认证并引用该 Portal 服务器之后才能生效。

表1-22 配置 Portal 服务器探测功能

操作	命令	说明
进入系统视图	system-view	-
配置对Portal服务器的探测功能	portal server server-name server-detect method { http portal-heartbeat } * action { log permit-all trap } * [interval interval] [retry retries]	必选 缺省情况下，未配置对Portal服务器的探测功能 本命令中指定的Portal服务器必须已经存在



说明

只有对于支持 Portal 逃生心跳功能（目前仅 iMC 的 Portal 服务器支持）的 Portal 服务器，**portal-heartbeat** 类型的探测方法才有效。为了配合此类型的探测，还需要在 Portal 服务器上选择支持逃生心跳功能，并要求此处的 **interval** 与 **retry** 参数值的乘积大于等于 Portal 服务器上的逃生心跳间隔时长，其中 **interval** 取值最好大于 Portal 服务器的逃生间隔时长。

1.13.3 配置Portal用户信息同步功能



说明

本特性仅三层 Portal 认证支持。

为了解决接入设备与 Portal 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 服务器周期性地（周期为 Portal 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) 接入设备检测到该用户同步报文后，将其中携带的用户信息与自己的用户信息进行对比，如果发现同步报文中存在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 服务器，Portal 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连续 N（N 为 **retry** 参数的取值）个周期内，都未在该 Portal 服务器发送过来的用户同步报文中出现过，则认为 Portal 服务器上已不存在该用户，设备将强制该用户下线。

表1-23 配置 Portal 用户同步功能

操作	命令	说明
进入系统视图	system-view	-
配置Portal用户同步功能	portal server server-name user-sync [interval interval] [retry retries]	必选 缺省情况下，未配置Portal用户同步功能 本命令中指定的Portal服务器必须已经存在 只有在指定的Portal服务器已经在接口上使能的情况下，本功能才能生效



说明

- 只有在支持 Portal 用户心跳功能(目前仅 iMC 的 Portal 服务器支持)的 Portal 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 服务器上选择支持用户心跳功能，并要求此处的 **interval** 与 **retry** 参数值的乘积应该大于等于 Portal 服务器上的用户心跳间隔时长，其中 **interval** 取值最好大于 Portal 服务器的用户心跳间隔时长。
- 对于设备上多余的用户信息，即在 N 个周期后被判定为 Portal 服务器上已不存在的用户信息，设备会在第 N + 1 个周期内的某时刻将其删除掉。

1.14 强制Portal用户下线

通过配置强制用户下线可以终止对指定 IP 地址用户的认证过程，或者将已经通过认证的指定 IP 地址的用户删除。

表1-24 配置强制用户下线

操作	命令	说明
进入系统视图	system-view	-
强制接入设备上的用户下线	portal delete-user { <i>ipv4-address</i> all interface <i>interface-type interface-number</i> ipv6 <i>ipv6-address</i> }	必选

1.15 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1-25 Portal 显示和维护

操作	命令
显示接口上Portal的ACL信息	display portal acl { all dynamic static } interface interface-type interface-number [{ begin exclude include } regular-expression]
显示接口上Portal的连接统计信息	display portal connection statistics { all interface interface-type interface-number } [{ begin exclude include } regular-expression]
显示Portal的免认证规则信息	display portal free-rule [rule-number] [{ begin exclude include } regular-expression]
显示指定接口的Portal配置信息	display portal interface interface-type interface-number [{ begin exclude include } regular-expression]
显示本地Portal服务器信息	display portal local-server [{ begin exclude include } regular-expression]
显示Portal服务器信息	display portal server [server-name] [{ begin exclude include } regular-expression]
显示接口上Portal服务器的统计信息	display portal server statistics { all interface interface-type interface-number } [{ begin exclude include } regular-expression]
显示TCP仿冒统计信息	display portal tcp-cheat statistics [{ begin exclude include } regular-expression]
显示Portal用户的信息	display portal user { all interface interface-type interface-number } [{ begin exclude include } regular-expression]
清除接口上Portal的连接统计信息	reset portal connection statistics {all interface interface-type interface-number }
清除接口上Portal服务器的统计信息	reset portal server statistics { all interface interface-type interface-number }
清除TCP仿冒统计信息	reset portal tcp-cheat statistics

1.16 Portal典型配置举例

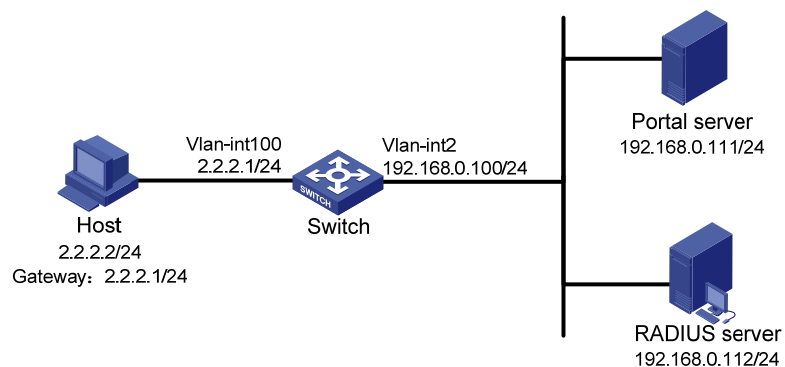
1.16.1 Portal直接认证配置举例

1. 组网需求

- 用户主机与接入设备 Switch 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 服务器；在通过 Portal 认证后，可以使用此 IP 地址访问非受限互联网资源。
- 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 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 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 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1-11 Portal 服务器配置页面

业务>>接入业务>>Portal服务管理 >> 服务器配置

Portal服务器配置

基本信息

* 日志级别

信息

* 逃生心跳间隔时长

20

秒

* 报文请求超时时长

5

秒

* 用户心跳间隔时长

5

分钟

Portal主页

http://192.168.0.111:8080/portal

高级信息

服务类型列表

增加

共有0条记录。

服务类型标识	服务类型	删除

确定

配置 IP 地址组。

单击导航树中的[Portal 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1-12 增加 IP 地址组配置页面

业务>>接入业务>>Portal服务管理>>Portal IP地址组配置>>增加IP地址组

增加IP地址组

* IP地址组名

Portal_user

* 起始地址

2.2.2.1

* 终止地址

2.2.2.255

业务分组

未分组

* 类型

普通

确定 取消

增加 Portal 设备。

单击导航树中的[Portal 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 Switch 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1-13 增加设备信息配置页面

业务>>接入业务>>Portal服务管理>>Portal设备配置>>增加设备信息

增加设备信息

* 设备名

NAS

* 版本

Portal 2.0

* 监听端口

2000

* 认证重发次数

2

* 二次地址分配

否

* 支持逃生心跳

否

* 业务分组

未分组

设备描述

* IP地址

2.2.2.1

* 密钥

portal

* 本地Challenge

否

* 下线重发次数

4

* 支持用户心跳

否

确定

取消

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1-14 设备信息列表

设备信息列表							
增加							
共有1条记录，当前第1 - 1，第 1/1 页。					每页显示：8 15 [50] 100 200		
设备名	版本	业务分组	IP地址	端口组信息管理	详细信息	修改	删除
NAS	Portal 2.0	未分组	2.2.2.1				

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1-15 增加端口组信息配置页面

业务>>接入业务>>Portal服务管理>>Portal设备配置>>端口组信息配置 >> 增加端口组信息

增加端口组信息			
* 端口组名	group	* 提示语言	动态检测
* 开始端口	0	* 终止端口	55555
* 协议类型	HTTP	* 快速认证	否
* 是否NAT	否	* 错误透传	是
* 认证方式	CHAP认证	* IP地址组	Portal_user
* 心跳间隔	10 分钟	* 心跳超时	30 分钟
用户域名		端口组描述	
用户属性类型		缺省认证页面	index_default.jsp
缺省认证类型	网页身份认证		

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 服务器配置生效。

(2) 配置 Switch

● 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<Switch> system-view
```

```
[Switch] radius scheme rs1
```

配置 RADIUS 方案的服务器类型。使用 CAMS/iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[Switch-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Switch-radius-rs1] primary authentication 192.168.0.112
```

```
[Switch-radius-rs1] primary accounting 192.168.0.112
```

```
[Switch-radius-rs1] key authentication simple radius
```

```
[Switch-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。

```
[Switch-radius-rs1] user-name-format without-domain
```

```
[Switch-radius-rs1] quit
```

● 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[Switch] domain dm1
```

配置 ISP 域的 AAA 方法。

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
```

```
[Switch-isp-dm1] authorization portal radius-scheme rs1
```

```
[Switch-isp-dm1] accounting portal radius-scheme rs1
```

```
[Switch-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认证和计费方法。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法。

```
[Switch] domain default enable dm1
```

- 配置 Portal 认证

配置 Portal 服务器: 名称为 newpt, IP 地址为 192.168.0.111, 密钥为明文 portal, 端口为 50100, URL 为 <http://192.168.0.111:8080/portal>。(Portal 服务器的 URL 请与实际环境中的 Portal 服务器配置保持一致, 此处仅为示例)

```
[Switch] portal server newpt ip 192.168.0.111 key simple portal port 50100  
url http://192.168.0.111:8080/portal
```

在与用户 Host 相连的接口上使能 Portal 认证。

```
[Switch] interface vlan-interface 100
```

```
[Switch-Vlan-interface100] portal server newpt method direct
```

```
[Switch] quit
```

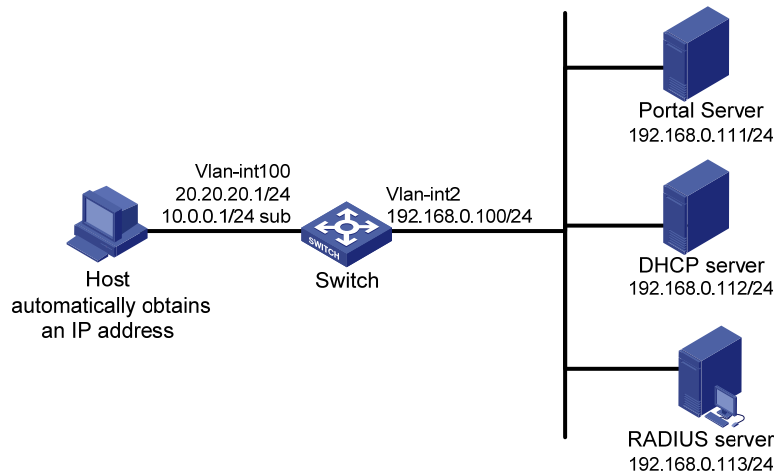
1.16.2 Portal二次地址分配认证配置举例

1. 组网需求

- 用户主机与接入设备 Switch 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 RADIUS 服务器作为认证/计费服务器。

2. 组网图

图1-16 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 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 Switch 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。

```
<Switch> system-view
```

```
[Switch] radius scheme rs1
```

配置 RADIUS 方案的服务器类型。使用 CAMS/iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[Switch-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Switch-radius-rs1] primary authentication 192.168.0.113
```

```
[Switch-radius-rs1] primary accounting 192.168.0.113
```

```
[Switch-radius-rs1] key authentication simple radius
```

```
[Switch-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。

```
[Switch-radius-rs1] user-name-format without-domain
```

```
[Switch-radius-rs1] quit
```

(2) 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[Switch] domain dm1
```

配置 ISP 域的 AAA 方法。

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
```

```
[Switch-isp-dm1] authorization portal radius-scheme rs1
```

```
[Switch-isp-dm1] accounting portal radius-scheme rs1
```

```
[Switch-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认证和计费方法。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法。

```
[Switch] domain default enable dm1
```

(3) 配置 Portal 认证

配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，端口为 50100，URL 为 http://192.168.0.111:8080/portal（请根据 Portal 服务器的实际情况配置，此处仅为示例）。

```
[Switch] portal server newpt ip 192.168.0.111 key simple portal port 50100 url  
http://192.168.0.111:8080/portal
```

配置 DHCP 中继，并启动 DHCP 中继的安全地址匹配检查功能。

```
[Switch] dhcp enable  
[Switch] dhcp relay server-group 0 ip 192.168.0.112  
[Switch] interface vlan-interface 100  
[Switch-Vlan-interface100] ip address 20.20.20.1 255.255.255.0  
[Switch-Vlan-interface100] ip address 10.0.0.1 255.255.255.0 sub  
[Switch-Vlan-interface100] dhcp select relay  
[Switch-Vlan-interface100] dhcp relay server-select 0  
[Switch-Vlan-interface100] dhcp relay address-check enable
```

在与用户 Host 相连的接口上使能 Portal 认证。

```
[Switch-Vlan-interface100] portal server newpt method redhcp  
[Switch-Vlan-interface100] quit
```

1.16.3 可跨三层 Portal 认证配置举例

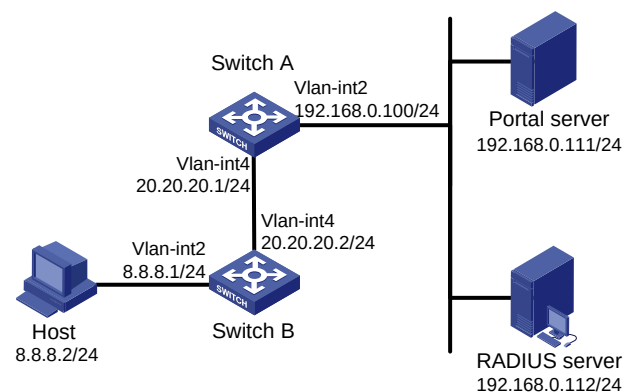
1. 组网需求

Switch A 支持 Portal 认证功能。用户 Host 通过 Switch B 接入到 Switch A。

- 配置 Switch 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 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 RADIUS 服务器作为认证/计费服务器。

2. 组网图

图1-17 配置可跨三层 Portal 认证组网图



3. 配置步骤



说明

- 请保证在 Portal 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 Switch 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。

```
<SwitchA> system-view
```

```
[SwitchA] radius scheme rs1
```

配置 RADIUS 方案的服务器类型。使用 CAMS/iMC 服务器时, RADIUS 服务器类型应选择 **extended**。

```
[SwitchA-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[SwitchA-radius-rs1] primary authentication 192.168.0.112
```

```
[SwitchA-radius-rs1] primary accounting 192.168.0.112
```

```
[SwitchA-radius-rs1] key authentication simple radius
```

```
[SwitchA-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。

```
[SwitchA-radius-rs1] user-name-format without-domain
```

```
[SwitchA-radius-rs1] quit
```

(2) 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[SwitchA] domain dm1
```

配置 ISP 域的 AAA 方法。

```
[SwitchA-isp-dm1] authentication portal radius-scheme rs1
```

```
[SwitchA-isp-dm1] authorization portal radius-scheme rs1
```

```
[SwitchA-isp-dm1] accounting portal radius-scheme rs1
```

```
[SwitchA-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认证和计费方法。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法。

```
[SwitchA] domain default enable dm1
```

(3) 配置 Portal 认证

配置 Portal 服务器: 名称为 newpt, IP 地址为 192.168.0.111, 密钥为明文 portal, 端口为 50100, URL 为 <http://192.168.0.111:8080/portal> (请根据 Portal 服务器的实际情况配置, 此处仅为示例)。

```
[SwitchA] portal server newpt ip 192.168.0.111 key simple portal port 50100
```

```
url http://192.168.0.111:8080/portal
```

在与 Switch B 相连的接口上使能 Portal 认证。

```
[SwitchA] interface vlan-interface 4
[SwitchA-Vlan-interface4] portal server newpt method layer3
[SwitchA-Vlan-interface4] quit
```

Switch 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。

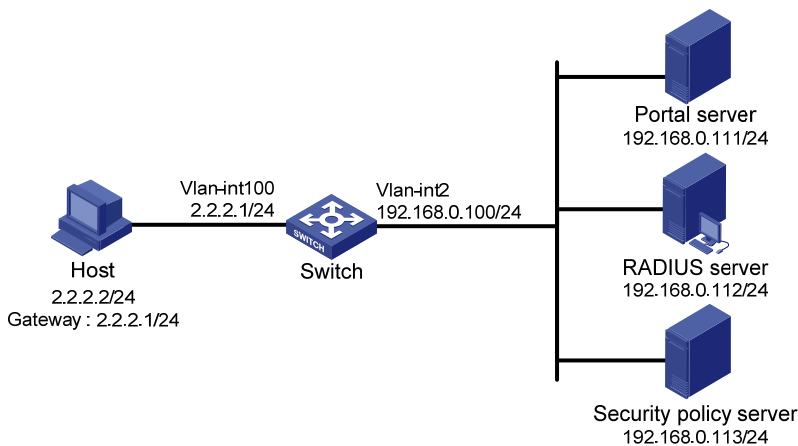
1.16.4 Portal直接认证扩展功能配置举例

1. 组网需求

- 用户主机与接入设备 Switch 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，可以访问非受限互联网资源。
- 采用 RADIUS 服务器作为认证/计费服务器。

2. 组网图

图1-18 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 Switch 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。

```
<Switch> system-view
```

```
[Switch] radius scheme rs1
```

配置 RADIUS 方案的服务器类型。使用 CAMS/iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[Switch-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Switch-radius-rs1] primary authentication 192.168.0.112
```

```
[Switch-radius-rs1] primary accounting 192.168.0.112
```

```
[Switch-radius-rs1] key accounting simple radius
```

```
[Switch-radius-rs1] key authentication simple radius
```

```
[Switch-radius-rs1] user-name-format without-domain
```

配置 RADIUS 方案的安全策略服务器。

```
[Switch-radius-rs1] security-policy-server 192.168.0.113
```

```
[Switch-radius-rs1] quit
```

(2) 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[Switch] domain dm1
```

配置 ISP 域的 AAA 方法。

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
```

```
[Switch-isp-dm1] authorization portal radius-scheme rs1
```

```
[Switch-isp-dm1] accounting portal radius-scheme rs1
```

```
[Switch-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法。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法。

```
[Switch] domain default enable dm1
```

(3) 配置受限资源对应的 ACL 为 3000，非受限资源对应的 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。

```
[Switch] acl number 3000
```

```
[Switch-acl-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
```

```
[Switch-acl-adv-3000] rule deny ip
```

```
[Switch-acl-adv-3000] quit
```

```
[Switch] acl number 3001
```

```
[Switch-acl-adv-3001] rule permit ip
```

```
[Switch-acl-adv-3001] quit
```

(4) 配置 Portal 认证

配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，端口为 50100，URL 为 <http://192.168.0.111:8080/portal>（请根据 Portal 服务器的实际情况配置，此处仅为示例）。

```
[Switch] portal server newpt ip 192.168.0.111 key simple portal port 50100
```

url <http://192.168.0.111:8080/portal>

在与用户 Host 相连的接口上使能 Portal 认证。

```
[Switch] interface vlan-interface 100
```

```
[Switch-Vlan-interface100] portal server newpt method direct
```

```
[Switch] quit
```

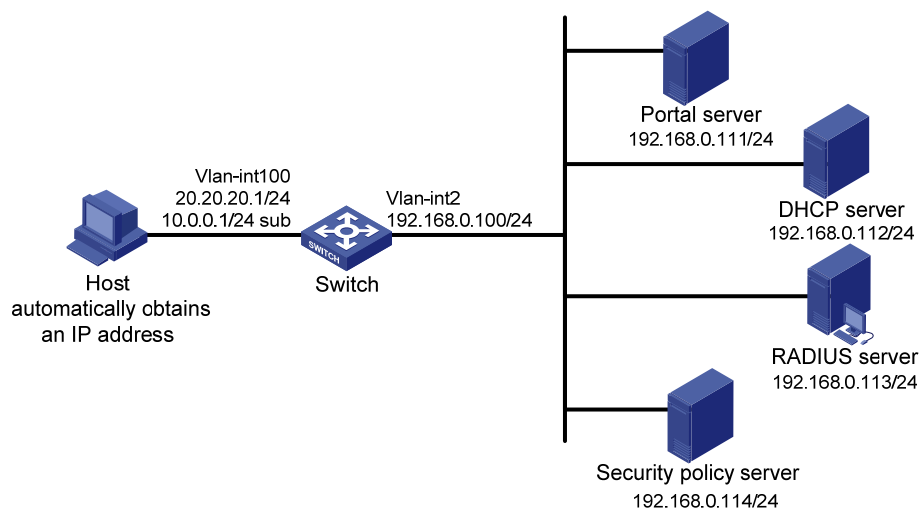
1.16.5 Portal二次地址分配认证扩展功能配置举例

1. 组网需求

- 用户主机与接入设备 Switch 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;用户通过安全认证后,可以访问非受限互联网资源。
- 采用 RADIUS 服务器作为认证/计费服务器。

2. 组网图

图1-19 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 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 Switch 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。

```
<Switch> system-view
```

```
[Switch] radius scheme rs1
```

配置 RADIUS 方案的服务器类型。使用 CAMS/iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[Switch-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Switch-radius-rs1] primary authentication 192.168.0.113
```

```
[Switch-radius-rs1] primary accounting 192.168.0.113
```

```
[Switch-radius-rs1] key accounting simple radius
```

```
[Switch-radius-rs1] key authentication simple radius
```

```
[Switch-radius-rs1] user-name-format without-domain
```

配置 RADIUS 方案的安全策略服务器。

```
[Switch-radius-rs1] security-policy-server 192.168.0.114
```

```
[Switch-radius-rs1] quit
```

(2) 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[Switch] domain dm1
```

配置 ISP 域的 AAA 方法。

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
```

```
[Switch-isp-dm1] authorization portal radius-scheme rs1
```

```
[Switch-isp-dm1] accounting portal radius-scheme rs1
```

```
[Switch-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认证和计费方法。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法。

```
[Switch] domain default enable dm1
```

(3) 配置受限资源对应的 ACL 为 3000，非受限资源对应的 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。

```
[Switch] acl number 3000
```

```
[Switch-acl-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
```

```
[Switch-acl-adv-3000] rule deny ip
```

```
[Switch-acl-adv-3000] quit
```

```
[Switch] acl number 3001
```

```
[Switch-acl-adv-3001] rule permit ip
```

```
[Switch-acl-adv-3001] quit
```

(4) 配置 Portal 认证

配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，端口为 50100，URL 为 http://192.168.0.111:8080/portal（请根据 Portal 服务器的实际情况配置，此处仅为示例）。

```
[Switch] portal server newpt ip 192.168.0.111 key simple portal port 50100
url http://192.168.0.111:8080/portal
# 配置 DHCP 中继, 并启动 DHCP 中继的安全地址匹配检查功能。
[Switch] dhcp enable
[Switch] dhcp relay server-group 0 ip 192.168.0.112
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 20.20.20.1 255.255.255.0
[Switch-Vlan-interface100] ip address 10.0.0.1 255.255.255.0 sub
[Switch-Vlan-interface100] dhcp select relay
[Switch-Vlan-interface100] dhcp relay server-select 0
[Switch-Vlan-interface100] dhcp relay address-check enable
# 在与用户 Host 相连的接口上使能 Portal 认证。
[Switch-Vlan-interface100] portal server newpt method redhcp
[Switch-Vlan-interface100] quit
```

1.16.6 可跨三层Portal认证方式扩展功能配置举例

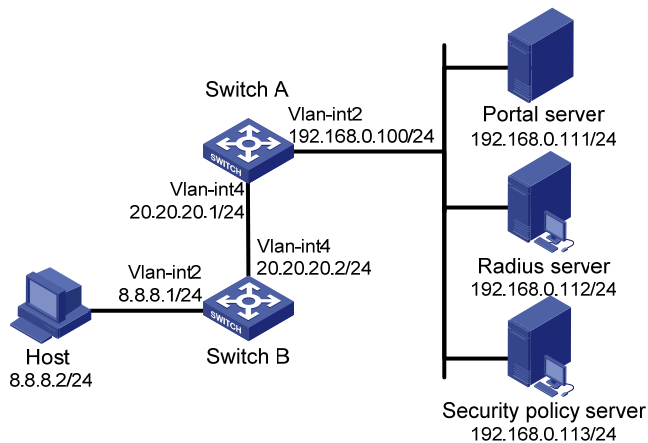
1. 组网需求

Switch A 支持 Portal 认证功能。用户 Host 通过 Switch B 接入到 Switch A。

- 配置 Switch 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 RADIUS 服务器作为认证/计费服务器。

2. 组网图

图1-20 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 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 Switch 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。

```
<SwitchA> system-view
```

```
[SwitchA] radius scheme rs1
```

配置 RADIUS 方案的服务器类型。使用 CAMS/iMC 服务器时, RADIUS 服务器类型应选择 **extended**。

```
[Switch-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[SwitchA-radius-rs1] primary authentication 192.168.0.112
```

```
[SwitchA-radius-rs1] primary accounting 192.168.0.112
```

```
[SwitchA-radius-rs1] key accounting simple radius
```

```
[SwitchA-radius-rs1] key authentication simple radius
```

```
[SwitchA-radius-rs1] user-name-format without-domain
```

配置 RADIUS 方案的安全策略服务器。

```
[SwitchA-radius-rs1] security-policy-server 192.168.0.113
```

```
[SwitchA-radius-rs1] quit
```

(2) 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[SwitchA] domain dm1
```

配置 ISP 域的 AAA 方法。

```
[SwitchA-isp-dm1] authentication portal radius-scheme rs1
```

```
[SwitchA-isp-dm1] authorization portal radius-scheme rs1
```

```
[SwitchA-isp-dm1] accounting portal radius-scheme rs1
```

```
[SwitchA-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认证和计费方法。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法。

```
[SwitchA] domain default enable dm1
```

(3) 配置受限资源对应的 ACL 为 3000, 非受限资源对应的 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。

```
[SwitchA] acl number 3000
[SwitchA-acl-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
[SwitchA-acl-adv-3000] rule deny ip
[SwitchA-acl-adv-3000] quit
[SwitchA] acl number 3001
[SwitchA-acl-adv-3001] rule permit ip
[SwitchA-acl-adv-3001] quit
```

(4) 配置 Portal 认证

配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，端口为 50100，URL 为 http://192.168.0.111:8080/portal（请根据 Portal 服务器的实际情况配置，此处仅为示例）。

```
[SwitchA] portal server newpt ip 192.168.0.111 key simple portal port 50100 url
http://192.168.0.111:8080/portal
```

在与 Switch B 相连的接口上使能 Portal 认证。

```
[SwitchA] interface vlan-interface 4
[SwitchA-Vlan-interface4] portal server newpt method layer3
[SwitchA-Vlan-interface4] quit
```

Switch 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。

1.16.7 Portal支持双机热备配置举例

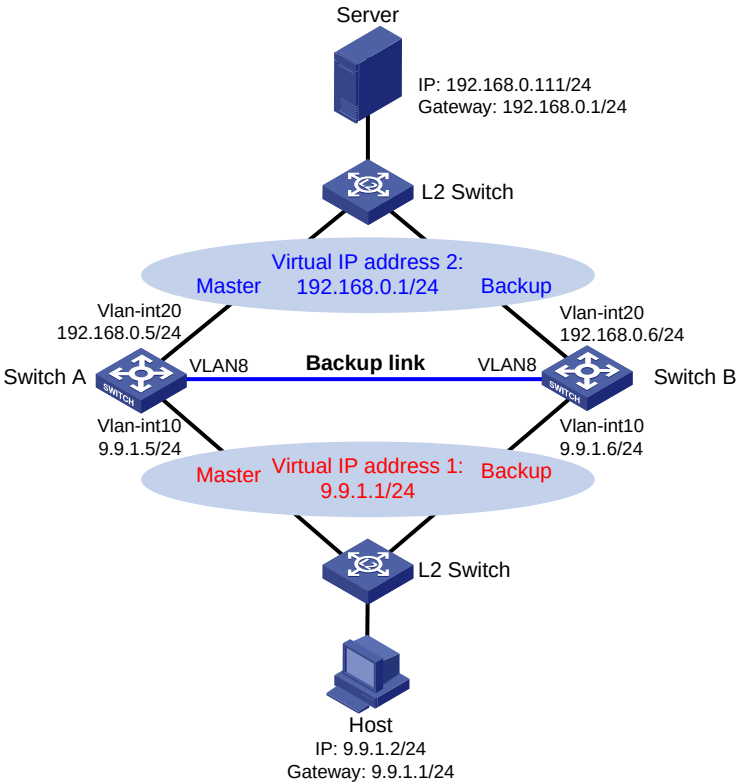
1. 组网需求

接入设备 Switch A 和 Switch B 之间存在备份链路，使用 VRRP 协议实现双机热备的流量切换，且两台设备均支持 Portal 认证功能。现要求 Switch A 和 Switch B 支持双机热备运行情况下的 Portal 用户数据备份，具体为：

- Switch A 正常工作的情况下，Host 通过 Switch A 进行 Portal 认证接入到外网。Switch A 发生故障的情况下，Host 通过 Switch B 接入到外网，并且在 VRRP 监视上行链路接口功能的配合下，保证业务流量切换不被中断。
- 采用 RADIUS 服务器作为认证/计费服务器。（本例中 Portal 服务器和 RADIUS 服务器的功能均由 Server 实现）
- Switch A 和 Switch B 之间通过单独的链路传输双机热备报文，且指定专用于双机热备的 VLAN 为 VLAN 8。

2. 组网图

图1-21 配置 Portal 支持双机热备组网图



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。
- 保证启动 Portal 之前主机可以分别通过 Switch A 和 Switch B 访问认证服务器。
- 配置 VRRP 备份组 1 和 VRRP 备份组 2 分别实现下行、上行链路的备份。VRRP 配置的相关介绍请参见“可靠性配置指导”中的“VRRP”。
- 双机热备配置的相关介绍请参见“可靠性配置指导”中的“双机热备”。

(1) 配置 Portal 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 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 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1-22 Portal 服务器配置页面

业务>>接入业务>>Portal服务器管理 >> 服务器配置

Portal服务器配置

基本信息

* 日志级别

信息

* 逃生心跳间隔时长

20

秒

* 报文请求超时时长

5

秒

* 用户心跳间隔时长

5

分钟

Portal主页

http://192.168.0.111:8080/portal

高级信息

服务类型列表

增加

共有0条记录。

服务类型标识	服务类型	删除

确定

配置 IP 地址组。

单击导航树中的[Portal 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”。

1-50

图1-23 增加 IP 地址组配置页面

业务>>接入业务>>Portal服务管理>>Portal IP地址组配置>>增加IP地址组

增加IP地址组

* IP地址组名	Portal_user
* 起始地址	9.9.1.1
* 终止地址	9.9.1.255
业务分组	未分组
* 类型	普通

增加 Portal 设备。

单击导航树中的[Portal 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；
- 指定主机 IP 地址为使能 Portal 的接口所在的 VRRP 组的虚拟 IP 地址；
- 输入密钥，与接入设备 Switch 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1-24 增加设备信息配置页面

业务>>接入业务>>Portal服务管理>>Portal设备配置>>增加设备信息

增加设备信息

* 设备名	NAS	* IP地址	9.9.1.1
* 版本	Portal 2.0	* 密钥	portal
* 监听端口	2000	* 本地Challenge	否
* 认证重发次数	2	* 下线重发次数	4
* 二次地址分配	否	* 支持用户心跳	否
* 支持逃生心跳	否		
* 业务分组	未分组		
设备描述			

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1-25 设备信息列表

设备信息列表							
增加							
共有1条记录，当前第1 - 1，第 1/1 页。				每页显示：8 15 [50] 100 200			
设备名	版本	业务分组	IP地址	端口组信息管理	详细信息	修改	删除
NAS	Portal 2.0	未分组	9.9.1.1				

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1-26 增加端口组信息配置页面


[业务](#)>>[接入业务](#)>>[Portal服务管理](#)>>[Portal设备配置](#)>>[端口组信息配置](#) >> 增加端口组信息

增加端口组信息

* 端口组名	group	* 提示语言	动态检测
* 开始端口	0	* 终止端口	zzzzz
* 协议类型	HTTP	* 快速认证	否
* 是否NAT	否	* 错误透传	是
* 认证方式	CHAP认证	* IP地址组	Portal_user
* 心跳间隔	10 分钟	* 心跳超时	30 分钟
用户域名		端口组描述	
用户属性类型		缺省认证页面	index_default.jsp
缺省认证类型	网页身份认证		

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 服务器配置生效。

(2) 配置 Switch A

• 配置 VRRP

创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 9.9.1.1。

```
<SwitchA> system-view
```

```
[SwitchA] interface vlan-interface 10
```

```
[SwitchA-Vlan-interface10] vrrp vrid 1 virtual-ip 9.9.1.1
```

配置 VLAN 接口 10 在 VRRP 备份组 1 中的优先级为 200。

```
[SwitchA-Vlan-interface10] vrrp vrid 1 priority 200
```

在 VLAN 接口 10 上配置监视 VLAN 接口 20，当 VLAN 接口 20 状态为 Down 或 Removed 时，VLAN 接口 10 在备份组 1 中的优先级降低 150。

```
[SwitchA-Vlan-interface10] vrrp vrid 1 track interface vlan-interface20 reduced 150
```

```
[SwitchA-Vlan-interface10] quit
```

```

# 创建 VRRP 备份组 2，并配置 VRRP 备份组 2 的虚拟 IP 地址为 192.168.0.1。
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] vrrp vrid 2 virtual-ip 192.168.0.1
# 配置 VLAN 接口 20 在 VRRP 备份组 2 中的优先级为 200。
[SwitchA-Vlan-interface20] vrrp vrid 2 priority 200
# 在 VLAN 接口 20 上配置监视 VLAN 接口 10，当 VLAN 接口 10 状态为 Down 或 Removed 时，
VLAN 接口 20 在备份组 2 中的优先级降低 150。
[SwitchA-Vlan-interface20] vrrp vrid 2 track interface vlan-interface10 reduced 150
[SwitchA-Vlan-interface20] quit
• 配置 RADIUS 方案
# 创建名字为 rs1 的 RADIUS 方案并进入该方案视图。
[SwitchA] radius scheme rs1
# 配置 RADIUS 方案的服务器类型。使用 CAMS/iMC 服务器时，RADIUS 服务器类型应选择
extended。
[SwitchA-radius-rs1] server-type extended
# 配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。
[SwitchA-radius-rs1] primary authentication 192.168.0.111
[SwitchA-radius-rs1] primary accounting 192.168.0.111
[SwitchA-radius-rs1] key authentication simple expert
[SwitchA-radius-rs1] key accounting simple expert
# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。（可选，请根据实际应用需求调整）
[SwitchA-radius-rs1] user-name-format without-domain
[SwitchA-radius-rs1] quit
• 配置认证域
# 创建并进入名字为 dm1 的 ISP 域。
[SwitchA] domain dm1
# 配置 ISP 域的 AAA 方法。
[SwitchA-isp-dm1] authentication portal radius-scheme rs1
[SwitchA-isp-dm1] authorization portal radius-scheme rs1
[SwitchA-isp-dm1] accounting portal radius-scheme rs1
[SwitchA-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法。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法。
[SwitchA] domain default enable dm1
• 配置接口使能 Portal
# 配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，端口为 50100，
URL 为 http://192.168.0.111:8080/portal。（Portal 服务器的 URL 请与实际环境中的 Portal 服务器配
置保持一致，此处仅为示例）
[SwitchA] portal server newpt ip 192.168.0.111 key simple portal port 50100 url
http://192.168.0.111:8080/portal
# 在与用户 Host 相连的接口上使能 Portal 认证。
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] portal server newpt method layer3
# 指定发送 Portal 报文的源 IP 地址为 VRRP 组 1 的虚拟 IP 地址 9.9.1.1。

```

```
[SwitchA-Vlan-interface10] portal nas-ip 9.9.1.1
```

- 配置 Portal 支持双机热备

配置 VLAN 接口 10 属于 Portal 备份组 1。

```
[SwitchA-Vlan-interface10] portal backup-group 1
```

```
[SwitchA-Vlan-interface10] quit
```

配置双机热备模式下的设备 ID 为 1。

```
[SwitchA] nas device-id 1
```

配置发送 RADIUS 报文的源 IP 地址为 VRRP 组 2 的虚拟 IP 地址 192.168.0.1。

```
[SwitchA] radius nas-ip 192.168.0.1
```



说明

请保证 RADIUS 服务器上成功添加了 IP 地址为 192.168.0.1 的接入设备。

- 配置双机热备

配置备份 VLAN 为 VLAN 8。

```
[SwitchA] dmbk vlan 8
```

使能双机热备功能，且支持对称路径。

```
[SwitchA] dmbk enable backup-type symmetric-path
```

(3) 配置 Switch B

- 配置 VRRP

创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 9.9.1.1。

```
<SwitchB> system-view
```

```
[SwitchB-Vlan-interface10] vrrp vrid 1 virtual-ip 9.9.1.1
```

配置 VLAN 接口 10 在 VRRP 备份组 1 中的优先级为 150。

```
[SwitchB-Vlan-interface10] vrrp vrid 1 priority 150
```

```
[SwitchB-Vlan-interface10] quit
```

创建 VRRP 备份组 2，并配置 VRRP 备份组 2 的虚拟 IP 地址为 192.168.0.1。

```
[SwitchB] interface vlan-interface 20
```

```
[SwitchB-Vlan-interface20] vrrp vrid 2 virtual-ip 192.168.0.1
```

配置 VLAN 接口 20 在 VRRP 备份组 2 中的优先级为 150。

```
[SwitchB-Vlan-interface20] vrrp vrid 2 priority 150
```

```
[SwitchB-Vlan-interface20] quit
```

- 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
[SwitchA] radius scheme rs1
```

配置 RADIUS 方案的服务器类型。使用 CAMS/iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[SwitchB-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[SwitchB-radius-rs1] primary authentication 192.168.0.111
```

```
[SwitchB-radius-rs1] primary accounting 192.168.0.111
```

```
[SwitchB-radius-rs1] key authentication simple expert
```

```
[SwitchB-radius-rs1] key accounting simple expert
# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。(可选, 请根据实际应用需求调整)
[SwitchB-radius-rs1] user-name-format without-domain
[SwitchB-radius-rs1] quit
```

- 配置认证域

```
# 创建并进入名字为 dm1 的 ISP 域。
[SwitchB] domain dm1
# 配置 ISP 域的 AAA 方法。
[SwitchB-isp-dm1] authentication portal radius-scheme rs1
[SwitchB-isp-dm1] authorization portal radius-scheme rs1
[SwitchB-isp-dm1] accounting portal radius-scheme rs1
[SwitchB-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认证和计费方法。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法。
[SwitchB] domain default enable dm1
```

- 配置接口使能 Portal

```
# 配置 Portal 服务器: 名称为 newpt, IP 地址为 192.168.0.111, 密钥为明文 portal, 端口为 50100,
# URL 为 http://192.168.0.111:8080/portal。(Portal 服务器的 URL 请与实际环境中的 Portal 服务器配
# 置保持一致, 此处仅为示例)
[SwitchB] portal server newpt ip 192.168.0.111 key simple portal port 50100 url
http://192.168.0.111:8080/portal
# 在与用户 Host 相连的接口上使能 Portal 认证。
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] portal server newpt method layer3
# 指定发送 Portal 报文的源 IP 地址为 VRRP 组 1 的虚拟 IP 地址 9.9.1.1。
[SwitchA-Vlan-interface10] portal nas-ip 9.9.1.1
```

- 配置 Portal 支持双机热备

```
# 配置 VLAN 接口 10 属于 Portal 备份组 1。
[SwitchB-Vlan-interface10] portal backup-group 1
[SwitchB-Vlan-interface10] quit
# 配置双机热备模式下的设备 ID 为 2。
[SwitchB] nas device-id 2
# 配置发送 RADIUS 报文的源 IP 地址为 VRRP 组 2 的虚拟 IP 地址 192.168.0.1。
[SwitchB] radius nas-ip 192.168.0.1
```



说明

请保证 RADIUS 服务器上成功添加了 IP 地址为 192.168.0.1 的接入设备。

- 配置双机热备

```
# 配置备份 VLAN 为 VLAN 8。
[SwitchB] dmbk vlan 8
# 使能双机热备功能。
[SwitchB] dmbk enable backup-type symmetric-path
```

4. 验证配置结果

用户 Host 从 Switch A 成功上线后, 在 Switch A 和 Switch B 上均可以通过命令 **display portal user** 查看该用户的认证情况。

```
[SwitchA] display portal user all
```

```
Index:3
```

```
State:ONLINE
```

```
SubState:NONE
```

```
ACL:NONE
```

```
Work-mode: primary
```

```
VPN instance:NONE
```

MAC	IP	Vlan	Interface

000d-88f8-0eac	9.9.1.2	10	Vlan-interface10

```
Total 1 user(s) matched, 1 listed.
```

```
[SwitchB] display portal user all
```

```
Index:2
```

```
State:ONLINE
```

```
SubState:NONE
```

```
ACL:NONE
```

```
Work-mode: secondary
```

```
VPN instance:NONE
```

MAC	IP	Vlan	Interface

000d-88f8-0eac	9.9.1.2	10	Vlan-interface10

```
Total 1 user(s) matched, 1 listed.
```

通过以上显示信息可以看到, Switch A 和 Switch B 上均有 Portal 用户 Host 的信息, 且 Switch A 上的用户模式为 **primary**, Switch B 上的用户模式为 **secondary**, 表示该用户是由 Switch A 上线并被同步到 Switch B 上的。

1.16.8 Portal服务器探测和用户同步功能配置举例

1. 组网需求

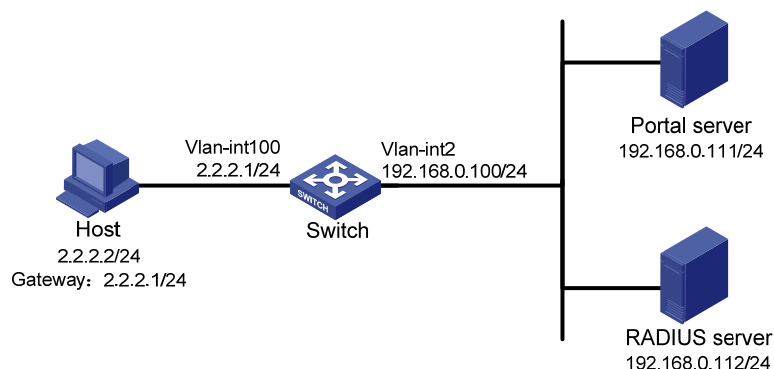
用户主机与接入设备 Switch 直接相连, 通过 Portal 认证接入网络, 并采用 RADIUS 服务器作为认证/计费服务器。

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 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 服务器是否可达, 并输出可达状态变化的 Trap 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1-27 Portal 服务器探测和用户同步功能配置组网图



3. 配置思路

- (1) 配置 Portal 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 Vlan-int100 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 服务器探测功能，在与 Portal 服务器的逃生心跳功能的配合下，对 Portal 服务器的可达状态进行探测；
- (5) 接入设备上配置 Portal 用户同步功能，在与 Portal 服务器的用户心跳功能的配合下，与 Portal 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 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 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 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1-28 Portal 服务器配置页面

业务>>接入业务>>Portal服务管理 >> 服务器配置

Portal服务器配置

基本信息

* 日志级别

信息

* 报文请求超时时长

5

秒 ?

* 逃生心跳间隔时长

20

秒 ?

* 用户心跳间隔时长

5

分钟 ?

Portal主页

http://192.168.0.111:8080/portal

高级信息

服务类型列表

增加

共有0条记录。

服务类型标识	服务类型	删除

确定

配置 IP 地址组。

单击导航树中的[Portal 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1-29 增加 IP 地址组配置页面

业务>>接入业务>>Portal服务管理>>Portal IP地址组配置>>增加IP地址组

增加IP地址组

* IP地址组名

Portal_user

* 起始地址

2.2.2.1

* 终止地址

2.2.2.255

业务分组

未分组

* 类型

普通

确定

取消

增加 Portal 设备。

单击导航树中的[Portal 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 Switch 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1-30 增加设备信息配置页面

业务>>接入业务>>Portal服务管理>>Portal设备配置>>增加设备信息

增加设备信息

* 设备名

NAS

* IP地址

2.2.2.1

* 版本

Portal 2.0

* 密钥

portal

* 监听端口

2000

* 本地Challenge

否

* 认证重发次数

2

* 下线重发次数

4

* 二次地址分配

否

* 支持逃生心跳

是

* 支持用户心跳

是

* 业务分组

未分组

设备描述

确定

取消

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1-31 设备信息列表

设备信息列表							
增加							
共有1条记录，当前第1 - 1，第 1/1 页。				每页显示：8 15 [50] 100 200			
设备名	版本	业务分组	IP地址	端口组信息管理	详细信息	修改	删除
NAS	Portal 2.0	未分组	2.2.2.1				

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1-32 增加端口组信息配置页面

业务>>接入业务>>Portal服务管理>>Portal设备配置>>端口组信息配置 >> 增加端口组信息

增加端口组信息			
* 端口组名	group	* 提示语言	动态检测
* 开始端口	0	* 终止端口	zzzzz
* 协议类型	HTTP	* 快速认证	否
* 是否NAT	否	* 错误透传	是
* 认证方式	CHAP认证	* IP地址组	Portal_user
* 心跳间隔	10 分钟	* 心跳超时	30 分钟
用户域名		端口组描述	
用户属性类型			
缺省认证类型	网页身份认证	缺省认证页面	index_default.jsp

确定 取消

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 服务器配置生效。

(2) 配置 Switch

• 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<Switch> system-view
```

```
[Switch] radius scheme rs1
```

配置 RADIUS 方案的服务器类型。使用 CAMS/iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[Switch-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Switch-radius-rs1] primary authentication 192.168.0.112
```

```
[Switch-radius-rs1] primary accounting 192.168.0.112
```

```
[Switch-radius-rs1] key authentication simple radius
```

```
[Switch-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。

```
[Switch-radius-rs1] user-name-format without-domain
```

```
[Switch-radius-rs1] quit
```

• 配置认证域

创建并进入名字为 dm1 的 ISP 域。

```
[Switch] domain dm1
```

配置 ISP 域的 AAA 方法。

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
```

```
[Switch-isp-dm1] authorization portal radius-scheme rs1
```

```
[Switch-isp-dm1] accounting portal radius-scheme rs1
```

```
[Switch-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认证和计费方法。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法。

```
[Switch] domain default enable dm1
```

- 使能 Portal 认证

配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为明文 portal，端口为 50100，URL 为 http://192.168.0.111:8080/portal。（Portal 服务器的 URL 请与实际环境中的 Portal 服务器配置保持一致，此处仅为示例）

```
[Switch] portal server newpt ip 192.168.0.111 key simple portal port 50100 url  
http://192.168.0.111:8080/portal
```

在与用户 Host 相连的接口上使能 Portal 认证。

```
[Switch] interface vlan-interface 100  
[Switch-Vlan-interface100] portal server newpt method direct  
[Switch-Vlan-interface100] quit
```

- 配置 Portal 服务器探测功能

配置对 Portal 服务器 newpt 的探测功能：探测方式为探测 Portal 心跳报文，每次探测间隔时间为 40 秒，若连续二次探测均失败，则发送服务器不可达的 Trap 信息，并打开网络限制，允许未认证用户访问网络。

```
[Switch] portal server newpt server-detect method portal-heartbeat action trap permit-all  
interval 40 retry 2
```



说明

此处 interval 与 retry 的乘积应该大于等于 Portal 服务器的逃生心跳间隔时长，且推荐 interval 取值大于 Portal 服务器的逃生心跳间隔时长。

- 配置 Portal 用户信息同步功能

配置对 Portal 服务器 newpt 的 Portal 用户同步功能，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连续两个探测周期内都未在该 Portal 服务器发送的同步报文中出现，设备将强制该用户下线。

```
[Switch] portal server newpt user-sync interval 600 retry 2
```



说明

此处 interval 与 retry 的乘积应该大于等于 Portal 服务器上的用户心跳间隔时长，且推荐 interval 取值大于 Portal 服务器的用户心跳间隔时长。

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 Portal 服务器的状态。

```
<Switch> display portal server newpt
```

Portal server:

1)newpt:

IP : 192.168.0.111

Key : *****

Port : 50100

URL : http://192.168.0.111:8080/portal
Status : Up

1.16.9 可跨三层Portal认证支持多实例配置举例

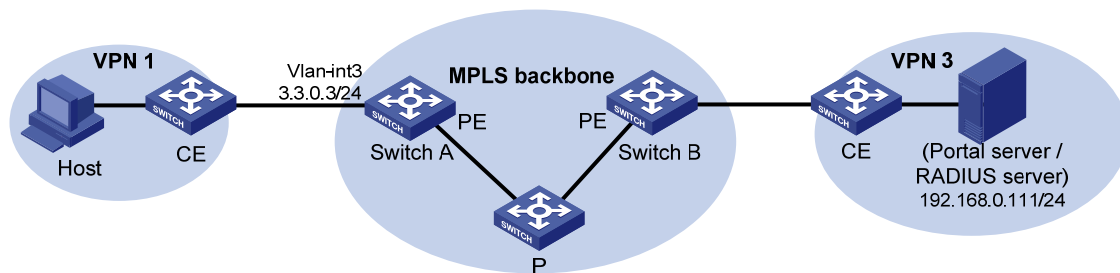
1. 组网需求

连接客户端的 PE 设备 Switch 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 Switch 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。
- RADIUS 服务器和 Portal 服务器由同一台服务器承担。

2. 组网图

图1-33 配置三层 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。本例仅介绍客户端 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 Switch 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。

```
<SwitchA> system-view
```

```
[SwitchA] radius scheme rs1
```

配置 RADIUS 方案所属的 VPN 实例为 vpn3。

```
[SwitchA-radius-rs1] vpn-instance vpn3
```

配置 RADIUS 方案的服务器类型。使用 CAMS/iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[Switch-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[SwitchA-radius-rs1] primary authentication 192.168.0.111
```

```
[SwitchA-radius-rs1] primary accounting 192.168.0.111
```

```
[SwitchA-radius-rs1] key accounting simple radius
[SwitchA-radius-rs1] key authentication simple radius
# 配置向 RADIUS 服务器发送的用户名不携带域名。
[SwitchA-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。
[SwitchA-radius-rs1] nas-ip 3.3.0.3
[SwitchA-radius-rs1] quit
```



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。

```
[SwitchA] domain dm1
```

配置 ISP 域的 AAA 方法。

```
[SwitchA-isp-dm1] authentication portal radius-scheme rs1
```

```
[SwitchA-isp-dm1] authorization portal radius-scheme rs1
```

```
[SwitchA-isp-dm1] accounting portal radius-scheme rs1
```

```
[SwitchA-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法。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法。

```
[SwitchA] domain default enable dm1
```

(3) 配置 Portal 认证

配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，所属的 VPN 为 vpn3，密钥为明文 portal，端口为 50100，URL 为 http://192.168.0.111:8080/portal。

```
[SwitchA] portal server newpt ip 192.168.0.111 vpn-instance vpn3 key simple portal port 50100
url http://192.168.0.111:8080/portal
```

在与客户端相连的接口上使能 Portal 认证。

```
[SwitchA] interface vlan-interface 3
```

```
[SwitchA-Vlan-interface3] portal server newpt method layer3
```

```
[SwitchA-Vlan-interface3] quit
```

4. 验证配置结果

以上配置完成后，通过执行命令 **display portal interface** 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 Switch A 上生成的 Portal 在线用户信息。

```
[SwitchA] display portal user all
```

```
Index:2
```

```
State:ONLINE
```

```
SubState:NONE
```

```
ACL:NONE
```

```
Work-mode:stand-alone
```

```
VPN instance:vpn1
```

MAC	IP	Vlan	Interface
000d-88f7-c268	3.3.0.1	3	Vlan-interface3

Total 1 user(s) matched, 1 listed.

1.16.10 配置二层Portal认证

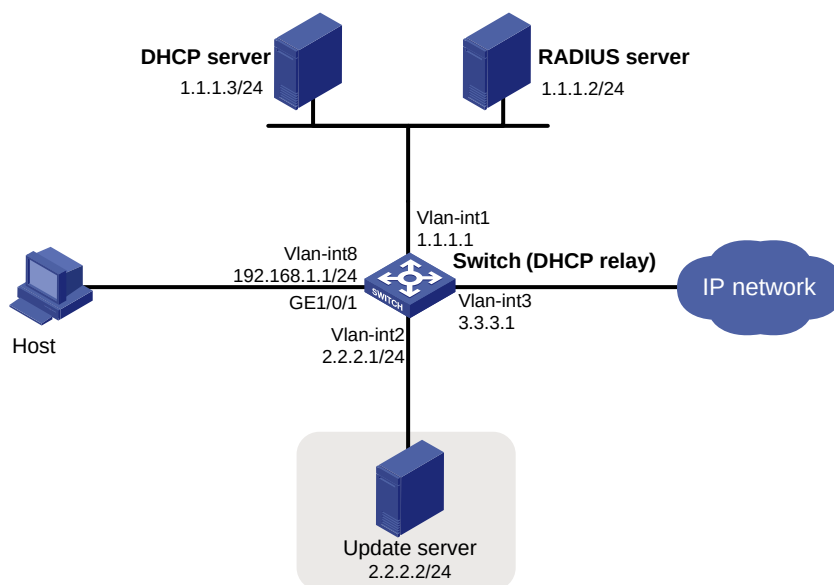
1. 组网需求

用户主机与接入设备 Switch 直接相连，接入设备在端口 GigabitEthernet1/0/1 上对用户进行二层 Portal 认证。具体要求如下：

- 使用远程 RADIUS 服务器进行认证、授权和计费；
- 使用远程 DHCP 服务器为用户分配 IP 地址；
- 本地 Portal 认证服务器的监听 IP 地址为 4.4.4.4，设备向 Portal 用户推出自定义的认证页面，并使用 HTTPS 传输认证数据；
- 认证成功用户可被授权加入 VLAN 3；
- 认证失败的用户将被加入 VLAN 2，允许访问其中的 Update 服务器资源；
- Host 通过 DHCP 动态获取 IP 地址，认证前使用 192.168.1.0/24 网段的 IP 地址，认证成功后使用 3.3.3.0/24 网段的 IP 地址，认证失败后使用 2.2.2.0/24 网段的 IP 地址。

2. 组网图

图1-34 配置二层 Portal 认证组网图



3. 配置步骤



说明

- 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 服务器的配置, 保证用户的认证/授权/计费功能正常运行。本例中, RADIUS 服务器上需要配置一个 Portal 用户 (帐户名为 userpt), 并配置授权 VLAN。
 - 完成 DHCP 服务器的配置, 主要包括: 指定为 Portal 客户端分配的 IP 地址范围 (192.168.1.0/24、3.3.3.0/24、2.2.2.0/24); 指定客户端的默认网关地址 (192.168.1.1、3.3.3.1、2.2.2.1), 并将 Update server 地址 (2.2.2.2) 排除在可分配的 IP 地址范围外; 确定分配给客户端的 IP 地址的租约期限 (建议尽量取较小的值, 以缩短认证状态变化后 IP 地址更新的时间); 保证 DHCP server 上具有到达客户端主机的路由。
 - 由于 DHCP 服务器与 DHCP 客户端不在同一个网段, 因此需要在客户端所在的网段设置 DHCP 中继。关于 DHCP 中继的详细介绍请参见“三层技术-IP 业务配置指导”中的“DHCP 中继”。
-

(1) 配置 Portal 认证

配置各以太网端口加入 VLAN 及对应 VLAN 接口的 IP 地址 (略)。

完成 PKI 域 pkidm 的配置, 并成功申请本地证书和 CA 证书, 具体配置请参见“安全配置指导”中的“PKI”。

完成自定义缺省认证页面文件的编辑, 并将其以 defaultfile 为名称压缩为一个 Zip 文件之后保存在设备根目录下。

配置 SSL 服务器端策略 sslsvr, 指定使用的 PKI 域为 pkidm。

```
<Switch> system-view
[Switch] ssl server-policy sslsvr
[Switch-ssl-server-policy-sslsvr] pki pkidm
[Switch-ssl-server-policy-sslsvr] quit
```

配置本地 Portal 服务器支持 HTTPS 协议, 并引用 SSL 服务器端策略 sslsvr。

```
[Switch] portal local-server https server-policy sslsvr
```

配置 Loopback 接口 12 的 IP 地址为 4.4.4.4。

```
[Switch] interface loopback 12
[Switch-LoopBack12] ip address 4.4.4.4 32
[Switch-LoopBack12] quit
```

指定二层 Portal 认证的本地 Portal 服务器监听 IP 地址为 4.4.4.4。

```
[Switch] portal local-server ip 4.4.4.4
```

在端口 GigabitEthernet1/0/1 上使能 Portal 认证, 并配置认证失败的 VLAN 为 VLAN 2。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type hybrid
[Switch-GigabitEthernet1/0/1] mac-vlan enable
[Switch-GigabitEthernet1/0/1] portal local-server enable
[Switch-GigabitEthernet1/0/1] portal auth-fail vlan 2
[Switch-GigabitEthernet1/0/1] quit
```

(2) 配置 RADIUS 方案

创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
[Switch] radius scheme rs1
```

配置 RADIUS 方案的服务器类型。使用 CAMS/iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[Switch-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Switch-radius-rs1] primary authentication 1.1.1.2
```

```
[Switch-radius-rs1] primary accounting 1.1.1.2
```

```
[Switch-radius-rs1] key accounting simple radius
```

```
[Switch-radius-rs1] key authentication simple radius
```

```
[Switch-radius-rs1] quit
```

(3) 配置认证域

创建并进入名字为 triple 的 ISP 域。

```
[Switch] domain triple
```

配置 ISP 域的 AAA 方法。

```
[Switch-isp-triple] authentication portal radius-scheme rs1
```

```
[Switch-isp-triple] authorization portal radius-scheme rs1
```

```
[Switch-isp-triple] accounting portal radius-scheme rs1
```

```
[Switch-isp-triple] quit
```

配置系统缺省的 ISP 域 triple，所有接入用户共用此缺省域认证和计费方法。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法。

```
[Switch] domain default enable triple
```

(4) 配置 DHCP 中继

使能 DHCP 服务。

```
[Switch] dhcp enable
```

配置 DHCP 服务器的地址。

```
[Switch] dhcp relay server-group 1 ip 1.1.1.3
```

配置 VLAN 接口 8 工作在 DHCP 中继模式。

```
[Switch] interface vlan-interface 8
```

```
[Switch-Vlan-interface8] dhcp select relay
```

配置 VLAN 接口 8 对应 DHCP 服务器组 1。

```
[Switch-Vlan-interface8] dhcp relay server-select 1
```

```
[Switch-Vlan-interface8] quit
```

配置 VLAN 接口 2 工作在 DHCP 中继模式。

```
[Switch] interface vlan-interface 2
```

```
[Switch-Vlan-interface2] dhcp select relay
```

配置 VLAN 接口 2 对应 DHCP 服务器组 1。

```
[Switch-Vlan-interface2] dhcp relay server-select 1
```

```
[Switch-Vlan-interface2] quit
```

配置 VLAN 接口 3 工作在 DHCP 中继模式。

```
[Switch] interface vlan-interface 3
```

```
[Switch-Vlan-interface3] dhcp select relay
```

配置 VLAN 接口 3 对应 DHCP 服务器组 1。

```
[Switch-Vlan-interface3] dhcp relay server-select 1
```

```
[Switch-Vlan-interface3] quit
```

4. 验证配置结果

用户 userpt 未进行 Web 访问之前，位于初始 VLAN（VLAN 8）中，并被分配 192.168.1.0/24 网段中的 IP 地址。当用户通过 Web 浏览器访问外部网络时，其 Web 请求均被重定向到认证页面 <https://4.4.4.4/portal/logon.htm>。用户根据网页提示输入正确的用户名和密码后，能够成功通过 Portal 认证。通过认证的用户将会离开初始 VLAN（VLAN 8），并加入授权 VLAN（VLAN 3）。可通过 **display connection ucibindex** 命令查看已在线用户的详细信息。

```
<Switch> display connection ucibindex 30
Slot: 1
Index=30 , Username=userpt@triple
MAC=0015-e9a6-7cfe
IP=192.168.1.2
IPv6=N/A
Access=PORTAL ,AuthMethod=PAP
Port Type=Ethernet,Port Name=GigabitEthernet1/0/1
Initial VLAN=8, Authorization VLAN=3
ACL Group=Disable
User Profile=N/A
CAR=Disable
Priority=Disable
Start=2009-11-26 17:40:02 ,Current=2009-11-26 17:48:21 ,Online=00h08m19s
Total 1 connection matched.
```

可以通过 **display mac-vlan all** 命令查看到认证成功用户的 MAC VLAN 表项，该表项中记录了加入授权 VLAN 的 MAC 地址与端口上生成的基于 MAC 的 VLAN 之间的对应关系。

```
[Switch] display mac-vlan all
The following MAC VLAN addresses exist:
S:Static D:Dynamic
MAC ADDR          MASK                VLAN ID   PRIO   STATE
-----
0015-e9a6-7cfe    ffff-ffff-ffff    3         0      D
Total MAC VLAN address count:1
```

若用户认证失败，将被加入 VLAN 2 中，端口上生成的 MAC VLAN 表项及 IP 地址分配情况的查看方式同上，此处略。

1.17 常见配置错误举例

1.17.1 接入设备和Portal服务器上的密钥不一致

1. 故障现象

用户被强制去访问 Portal 服务器时没有弹出 Portal 认证页面，也没有错误提示，登录的 Portal 认证服务器 Web 页面为空白。

2. 故障分析

接入设备上配置的 Portal 密钥和 Portal 服务器上配置的密钥不一致，导致 Portal 服务器报文验证出错，Portal 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配置的 Portal 服务器密钥，并在系统视图中使用 **portal server** 命令修改密钥，或者在 Portal 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。

1.17.2 接入设备上服务器端口配置错误

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 Portal 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请求报文到 Portal 服务器，Portal 服务器默认的报文监听端口为 50100，但是因为接入设备上配置的服务器监听端口错误（不是 50100），即其发送的下线请求报文的端口和 Portal 服务器真正的监听端口不一致，故 Portal 服务器无法收到下线请求报文，Portal 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 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 服务器可以收到下线应答报文，从而 Portal 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 服务器上的监听端口一致。

目 录

1 Triple认证配置	1-1
1.1 Triple认证简介	1-1
1.1.1 产生背景	1-1
1.1.2 认证机制	1-1
1.1.3 扩展功能	1-2
1.2 Triple认证配置任务简介	1-3
1.3 Triple认证典型配置举例	1-3
1.3.1 Triple认证基本功能配置举例	1-3
1.3.2 Triple认证配合VLAN下发及Auth-Fail VLAN功能配置举例	1-6

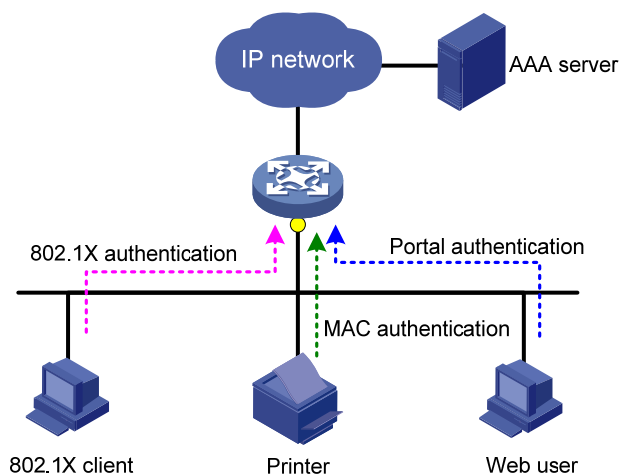
1 Triple认证配置

1.1 Triple认证简介

1.1.1 产生背景

在客户端形式多样的网络环境中，不同客户端支持的接入认证方式有所不同，如 [图 1-1](#) 所示，有的客户端只能进行MAC地址认证（比如打印机终端）；有的主机安装了 802.1X客户端软件，可以进行 802.1X认证；有的用户主机只希望通过Web访问进行Portal认证。为了灵活地适应这种网络环境中的多种认证需求，需要在接入用户的端口上对三种认证方式进行统一部署，使得用户可以选择任何一种适合的认证机制来进行认证，且只需要成功通过一种方式的认证即可实现接入，无需通过多种认证。

图1-1 Triple 认证典型应用组网图



Triple 认证方案可满足以上需求，允许在设备的二层端口上同时开启 Portal 认证、MAC 地址认证和 802.1X 认证功能，使得选用其中任意一种方式进行认证的客户端均可通过该端口接入网络。



说明

关于 802.1X、MAC 地址认证、Portal 认证的详细介绍请分别参考“安全配置指导”中的“802.1X”、“MAC 地址认证”和“Portal”。

1.1.2 认证机制

当端口上同时开启了 802.1X 认证、MAC 地址认证和 Portal 认证功能后，不同类型的客户端报文可触发的不同的认证过程：

- 客户端网卡接入网络时，如果发送 ARP 报文或者 DHCP 报文（广播报文），则首先触发 MAC 地址认证，若 MAC 地址认证成功，则后续无需其它认证；若 MAC 地址认证失败，则后续允许触发 802.1X 或者 Portal 认证。
- 如果客户端使用系统自带的 802.1X 客户端或者第三方客户端软件发送 EAP 报文，或者在设备开启单播触发功能的情况下客户端发送任意报文，则触发 802.1X 认证。
- 如果客户端发送 HTTP 报文，则触发 Portal 认证。

端口允许多种认证过程同时进行，且某一种认证失败不会影响同时进行的其它认证过程。一旦客户端通过某一种认证，设备将立即中止同时进行的其它认证过程。之后，端口是否允许该客户端触发其它认证过程的情况有所不同：

- 客户端通过 802.1X 认证或者 Portal 认证后，将不能再触发其它认证。
- 客户端通过 MAC 地址认证后，将不能再触发 Portal 认证，但是允许触发 802.1X 认证。若 802.1X 认证成功，则端口上后生成的 802.1X 认证用户信息会覆盖已存在的 MAC 地址认证用户信息。

1.1.3 扩展功能

在同时使能了三种认证方式的端口上，还支持以下扩展功能：

1. 授权VLAN下发

服务器向通过认证的用户所在的端口下发授权 VLAN，端口将用户加入对应的授权 VLAN 中。

2. 认证失败的VLAN

用户认证失败后，端口将认证失败的用户加入已配置的认证失败的 VLAN 中。

- 对于 802.1X 和 Portal 用户，认证失败的 VLAN 为端口上配置 Auth-Fail VLAN。
- 对于 MAC 地址认证用户，认证失败的 VLAN 为端口上配置的 Guest VLAN。



说明

允许在同一个端口上配置不同类型的认证失败的 VLAN，但最终端口上认证失败的用户所加入的 VLAN 与用户所经历的认证失败类型有关，通常情况下为用户第一次认证失败后加入的 VLAN，但如果用户进行了 802.1X 认证且失败了，则用户会立刻离开之前已经加入的认证失败的 VLAN 而加入端口上配置的 802.1X 认证失败的 VLAN。

3. ACL下发

设备能够根据服务器下发的授权 ACL 对通过认证的用户所在端口的数据流进行控制；在服务器上配置授权 ACL 之前，需要在设备上配置相应的规则。管理员可以通过改变服务器的授权 ACL 设置或设备上对应的 ACL 规则来改变用户的访问权限。

4. 在线用户探测功能

- 对于 Portal 用户，通过开启用户在线检测定时器来探测用户是否在线，检测时间间隔可配；
- 对于 802.1X 认证用户，通过开启端口上的在线用户握手功能或者重认证功能来探测用户是否在线，探测时间间隔可配置；

- 对于 MAC 地址认证用户，通过开启下线检测定时器，来探测用户是否在线，检测时间间隔可配置。



说明

关于各扩展功能的详细介绍请分别参考“安全配置指导”中的“802.1X”、“MAC 地址认证”、“Portal 认证”。

1.2 Triple认证配置任务简介

表1-1 Triple 认证配置任务简介

配置任务	说明		详细配置
配置802.1X认证	三者至少选其一	必须为基于MAC的接入控制方式（ macbased ）； 不建议使用Guest VLAN功能	具体配置请参考“安全配置指导”的“802.1X”
配置MAC地址认证		-	具体配置请参考“安全配置指导”的“MAC地址认证”
配置Portal认证		仅支持二层Portal认证的相关功能	具体配置请参考“安全配置指导”的“Portal”

1.3 Triple认证典型配置举例

1.3.1 Triple认证基本功能配置举例

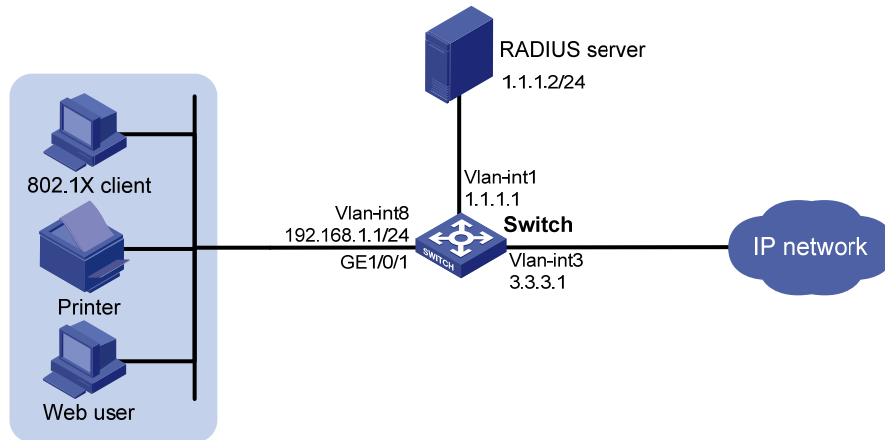
1. 组网需求

在如 [图 1-3](#) 所示的组网环境中，用户通过接入设备Switch接入网络，要求在Switch的二层端口上对所有用户进行统一认证，且只要用户通过 802.1X认证、Portal认证、MAC地址认证中的任何一种认证，即可接入网络。具体需求如下：

- 客户端上静态配置属于 192.168.1.0/24 网段的 IP 地址；
- 使用远程 RADIUS 服务器进行认证、授权和计费，且发送给 RADIUS 服务器的用户名不携带 ISP 域名；
- 本地 Portal 认证服务器的监听 IP 地址为 4.4.4.4，设备向 Portal 用户推出系统默认的认知页面，并使用 HTTP 传输认证数据。

2. 组网图

图1-2 Triple 认证基本功能配置组网图



3. 配置步骤



说明

- 保证启动 Portal 之前各主机、服务器和设备之间的路由可达。
- 保证 Web 用户的主机上有与本地 Portal 服务器监听 IP 地址可达的路由表项。
- 完成 RADIUS 服务器的配置，保证用户的认证/授权/计费功能正常运行。本例中，RADIUS 服务器上配置一个 802.1X 用户（帐户名为 userdot），一个 Portal 用户（帐户名为 userpt），以及一个 MAC 地址认证用户（帐户名、密码均为 Printer 的 MAC 地址 001588f80dd7）。

(1) 配置 Portal 认证

配置端口属于 VLAN 及对应 VLAN 接口的 IP 地址（略）。

配置本地 Portal 服务器支持 HTTP 协议。

```
<Switch> system-view
```

```
[Switch] portal local-server http
```

配置 Loopback 接口 0 的 IP 地址为 4.4.4.4。

```
[Switch] interface loopback 0
```

```
[Switch-LoopBack0] ip address 4.4.4.4 32
```

```
[Switch-LoopBack0] quit
```

指定二层 Portal 认证的本地 Portal 服务器监听 IP 地址为 4.4.4.4。

```
[Switch] portal local-server ip 4.4.4.4
```

在端口 GigabitEthernet 1/0/1 上使能二层 Portal 认证。

```
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] portal local-server enable
```

```
[Switch-GigabitEthernet1/0/1] quit
```

(2) 配置 802.1X 认证

全局使能 802.1X 认证。

```
[Switch] dot1x
```

在端口 GigabitEthernet1/0/1 上使能 802.1X 认证（必须为基于 MAC 的接入控制方式）。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x port-method macbased
[Switch-GigabitEthernet1/0/1] dot1x
[Switch-GigabitEthernet1/0/1] quit
```

(3) 配置 MAC 地址认证

全局使能 MAC 地址认证。

```
[Switch] mac-authentication
# 在端口 GigabitEthernet 1/0/1 上使能 MAC 地址认证。
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-authentication
[Switch-GigabitEthernet1/0/1] quit
```

(4) 配置 RADIUS 方案

创建并进入名字为 rs1 的 RADIUS 方案视图。

```
[Switch] radius scheme rs1
# 配置 RADIUS 方案的服务器类型。使用 iMC 服务器时，RADIUS 服务器类型应选择 extended。
[Switch-radius-rs1] server-type extended
# 配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。
[Switch-radius-rs1] primary authentication 1.1.1.2
[Switch-radius-rs1] primary accounting 1.1.1.2
[Switch-radius-rs1] key authentication radius
[Switch-radius-rs1] key accounting radius
# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。
[Switch-radius-rs1] user-name-format without-domain
[Switch-radius-rs1] quit
```

(5) 配置认证域

创建并进入名字为 triple 的 ISP 域。

```
[Switch] domain triple
# 为所有类型的用户配置缺省的 AAA 方案。
[Switch-isp-triple] authentication default radius-scheme rs1
[Switch-isp-triple] authorization default radius-scheme rs1
[Switch-isp-triple] accounting default radius-scheme rs1
[Switch-isp-triple] quit
```

配置系统缺省的 ISP 域为 triple。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。

```
[Switch] domain default enable triple
```

4. 验证配置结果

用户 userdot 通过 802.1X 客户端发起认证，输入正确的用户名和密码后，可成功通过 802.1X 认证；Web 用户 userpt 通过 Web 浏览器访问外部网络，其 Web 请求均被重定向到认证页面 <http://4.4.4.4/portal/logon.htm>。用户根据网页提示输入正确的用户名和密码后，能够成功通过 Portal 认证；打印机接入网络后，可成功通过 MAC 地址认证。

可通过 **display connection** 命令查看已在线用户的信息。

```
[Switch] display connection
```

```
Slot: 1
Index=30 , Username=userpt@triple
IP=192.168.1.2
IPv6=N/A
MAC=0015-e9a6-7cfe
Index=31 , Username=userdot@triple
IP=192.168.1.3
IPv6=N/A
MAC=0002-0002-0001
Index=32 , Username=001588f80dd7@triple
IP=192.168.1.4
IPv6=N/A
MAC=0015-88f8-0dd7

Total 3 connection(s) matched on slot 1.
Total 3 connection(s) matched.
```

1.3.2 Triple认证配合VLAN下发及Auth-Fail VLAN功能配置举例

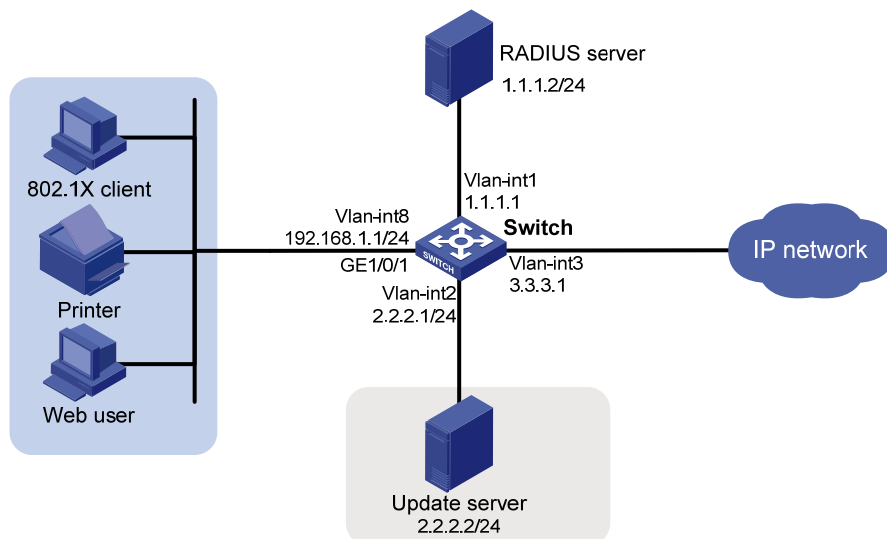
1. 组网需求

在如 [图 1-3](#) 所示的组网环境中，用户通过接入设备Switch接入网络，要求在Switch的二层端口上对所有用户进行统一认证，且只要用户通过 802.1X认证、Portal认证、MAC地址认证中的任何一种认证，即可接入网络。具体需求如下：

- Portal 用户通过 DHCP 动态获取 IP 地址，认证前使用 192.168.1.0/24 网段的 IP 地址，认证成功后使用 3.3.3.0/24 网段的 IP 地址，认证失败后使用 2.2.2.0/24 网段的 IP 地址；（DHCP 服务器可由接入设备充当也可外置，本例中由接入设备提供 DHCP 服务）
- 802.1X 用户在认证前使用手工配置的 192.168.1.0/24 网段的 IP 地址，认证成功后通过 DHCP 动态获取 3.3.3.0/24 网段的 IP 地址，认证失败后使用手工配置的 2.2.2.0/24 网段的 IP 地址。
- 打印机成功接入网络后通过 DHCP 获取一个与它的 MAC 地址静态绑定的 IP 地址 3.3.3.111/24；
- 使用远程 RADIUS 服务器进行认证、授权和计费，且发送给 RADIUS 服务器的用户名不携带 ISP 域名；
- 本地 Portal 认证服务器的监听 IP 地址为 4.4.4.4，设备向 Portal 用户推出自定义的认证页面，并使用 HTTPS 传输认证数据；
- 认证成功的用户可被授权加入服务器上指定的 VLAN 3；
- 认证失败的用户将被加入接入设备上配置的 VLAN 2，允许访问其中的 Update 服务器资源。

2. 组网图

图1-3 Triple 认证配合 VLAN 下发及 Auth-Fail VLAN 功能配置组网图



3. 配置步骤



说明

- 保证启动 Portal 之前各主机、服务器和设备之间的路由可达。
- 若使用外置 DHCP 服务器，保证用户在认证前后可成功获取 DHCP 服务器分配的 IP 地址。
- 完成 RADIUS 服务器的配置，保证用户的认证/授权/计费功能正常运行。本例中，RADIUS 服务器上配置一个 802.1X 用户（帐户名为 userdot），一个 Portal 用户（帐户名为 userpt），以及一个 MAC 地址认证用户（帐户名、密码均为 Printer 的 MAC 地址 001588f80dd7），并配置授权 VLAN（VLAN 3）。
- 完成 PKI 域 pkidm 的配置，并成功申请本地证书和 CA 证书，具体配置请参见“安全配置指导”中的“PKI”。
- 完成自定义缺省认证页面文件的编辑，并将其以 defaultfile 为名称压缩为一个 Zip 文件之后保存在设备根目录下。

(1) 配置 DHCP 服务

配置端口属于 VLAN 及对应 VLAN 接口的 IP 地址（略）。

使能 DHCP 服务。

```
<Switch> system-view
```

```
[Switch] dhcp enable
```

配置不参与自动分配的 Update server 的 IP 地址。

```
[Switch] dhcp server forbidden-ip 2.2.2.2
```

配置 DHCP 地址池 1 的属性（地址池范围、地址租用期限、网关地址）。建议配置较小的地址租用期限，以缩短客户端认证成功或失败后重新获取 IP 地址的时间。

```
[Switch] dhcp server ip-pool 1
```

```
[Switch-dhcp-pool-1] network 192.168.1.0 mask 255.255.255.0
[Switch-dhcp-pool-1] expired day 0 hour 0 minute 1
[Switch-dhcp-pool-1] gateway-list 192.168.1.1
[Switch-dhcp-pool-1] quit
```

配置 DHCP 地址池 2 的属性（地址池范围、地址租用期限、网关地址）。建议配置较小的地址租用期限，以缩短客户端认证成功后重新获取 IP 地址的时间。

```
[Switch] dhcp server ip-pool 2
[Switch-dhcp-pool-2] network 2.2.2.0 mask 255.255.255.0
[Switch-dhcp-pool-2] expired day 0 hour 0 minute 1
[Switch-dhcp-pool-2] gateway-list 2.2.2.1
[Switch-dhcp-pool-2] quit
```

配置 DHCP 地址池 3 的属性（地址池范围、地址租用期限、网关地址）。建议配置较小的地址租用期限，以缩短客户端下线后重新获取 IP 地址的时间。

```
[Switch] dhcp server ip-pool 3
[Switch-dhcp-pool-3] network 3.3.3.0 mask 255.255.255.0
[Switch-dhcp-pool-3] expired day 0 hour 0 minute 1
[Switch-dhcp-pool-3] gateway-list 3.3.3.1
[Switch-dhcp-pool-3] quit
```



说明

一般情况下，为缩小客户端认证状态改变之后更新 IP 地址的时间，建议配置较小的地址租约期限，使得前一个状态的 IP 地址租约尽快过期，以触发新的 IP 地址申请。但是，地址租用期限的配置还要考虑客户端的实现，例如 iNode 的 802.1X 客户端就可以选择在断开连接之后自动更新客户端 IP 地址，而不必等待租约过期来重获 IP 地址，因此实际应用中需要根据当前组网环境合理调整取值。

配置 DHCP 地址池 4，将 MAC 地址为 0015-e9a6-7cfe 的打印机与 IP 地址 3.3.3.111/24 绑定。

```
[Switch] dhcp server ip-pool 4
[Switch-dhcp-pool-4] static-bind ip-address 3.3.3.111 mask 255.255.255.0
[Switch-dhcp-pool-4] static-bind mac-address 0015-e9a6-7cfe
[Switch-dhcp-pool-4] quit
```

(2) 配置 Portal 认证

配置 SSL 服务器端策略 sslsvr，指定使用的 PKI 域为 pkidm。

```
[Switch] ssl server-policy sslsvr
[Switch-ssl-server-policy-sslsvr] pki pkidm
[Switch-ssl-server-policy-sslsvr] quit
```

配置本地 Portal 服务器支持 HTTPS 协议，并引用 SSL 服务器端策略 sslsvr。

```
[Switch] portal local-server https server-policy sslsvr
```

配置 Loopback 接口 12 的 IP 地址为 4.4.4.4。

```
[Switch] interface loopback 12
[Switch-LoopBack12] ip address 4.4.4.4 32
[Switch-LoopBack12] quit
```

指定二层 Portal 认证的本地 Portal 服务器监听 IP 地址为 4.4.4.4。

```
[Switch] portal local-server ip 4.4.4.4
```

在端口 GigabitEthernet 1/0/1 上使能二层 Portal 认证，并配置认证失败的 VLAN 为 VLAN 2。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type hybrid
[Switch-GigabitEthernet1/0/1] mac-vlan enable
[Switch-GigabitEthernet1/0/1] portal local-server enable
[Switch-GigabitEthernet1/0/1] portal auth-fail vlan 2
[Switch-GigabitEthernet1/0/1] quit
```

(3) 配置 802.1X 认证

全局使能 802.1X 认证。

```
[Switch] dot1x
```

在端口 GigabitEthernet 1/0/1 上使能 802.1X 认证（必须为基于 MAC 的接入控制方式），并配置认证失败的 VLAN 为 VLAN 2。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x port-method macbased
[Switch-GigabitEthernet1/0/1] dot1x
[Switch-GigabitEthernet1/0/1] dot1x auth-fail vlan 2
[Switch-GigabitEthernet1/0/1] quit
```

(4) 配置 MAC 地址认证

全局使能 MAC 地址认证。

```
[Switch] mac-authentication
```

在端口 GigabitEthernet 1/0/1 上使能 MAC 地址认证，并配置认证失败的 VLAN 为 VLAN 2。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-authentication
[Switch-GigabitEthernet1/0/1] mac-authentication guest-vlan 2
[Switch-GigabitEthernet1/0/1] quit
```

(5) 配置 RADIUS 方案

创建并进入名字为 rs1 的 RADIUS 方案视图。

```
[Switch] radius scheme rs1
```

配置 RADIUS 方案的服务器类型。使用 iMC 服务器时，RADIUS 服务器类型应选择 **extended**。

```
[Switch-radius-rs1] server-type extended
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Switch-radius-rs1] primary authentication 1.1.1.2
[Switch-radius-rs1] primary accounting 1.1.1.2
[Switch-radius-rs1] key authentication radius
[Switch-radius-rs1] key accounting radius
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[Switch-radius-rs1] user-name-format without-domain
[Switch-radius-rs1] quit
```

(6) 配置认证域

创建并进入名字为 triple 的 ISP 域。

```
[Switch] domain triple
```

为所有类型的用户配置缺省的 AAA 方案。

```
[Switch-isp-triple] authentication default radius-scheme rs1
[Switch-isp-triple] authorization default radius-scheme rs1
[Switch-isp-triple] accounting default radius-scheme rs1
```

```
[Switch-isp-triple] quit
```

配置系统缺省的 ISP 域为 **triple**。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。

```
[Switch] domain default enable triple
```

4. 验证配置结果

用户 **userdot** 通过 802.1X 客户端发起认证，输入正确的用户名和密码后，可成功通过 802.1X 认证；Web 用户 **userpt** 通过 Web 浏览器访问外部网络，其 Web 请求均被重定向到认证页面 <https://4.4.4.4/portal/logon.htm>。用户根据网页提示输入正确的用户名和密码后，能够成功通过 Portal 认证；打印机接入网络后，可成功通过 MAC 地址认证。

可通过 **display connection** 命令查看已在线用户的信息。

```
[Switch] display connection
```

```
Slot: 1
```

```
Index=30 , Username=userpt@triple
```

```
IP=192.168.1.2
```

```
IPv6=N/A
```

```
MAC=0015-e9a6-7cfe
```

```
Index=31 , Username=userdot@triple
```

```
IP=3.3.3.2
```

```
IPv6=N/A
```

```
MAC=0002-0002-0001
```

```
Index=32 , Username=001588f80dd7@triple
```

```
IP=N/A
```

```
IPv6=N/A
```

```
MAC=0015-88f8-0dd7
```

```
Total 3 connection(s) matched on slot 1.
```

```
Total 3 connection(s) matched.
```

可以通过 **display mac-vlan all** 命令查看到认证成功用户的 MAC VLAN 表项，该表项中记录了加入授权 VLAN 的 MAC 地址与端口上生成的基于 MAC 的 VLAN 之间的对应关系。

```
[Switch] display mac-vlan all
```

```
The following MAC VLAN addresses exist:
```

```
S:Static D:Dynamic
```

MAC ADDR	MASK	VLAN ID	PRIO	STATE

0015-e9a6-7cfe	ffff-ffff-ffff	3	0	D

0002-0002-0001	ffff-ffff-ffff	3	0	D

0015-88f8-0dd7	ffff-ffff-ffff	3	0	D

```
Total MAC VLAN address count:3
```

可通过 **display dhcp server ip-in-use** 命令查看设备为在线用户分配的 IP 地址信息。

```
[Switch] display dhcp server ip-in-use all
```

```
Pool utilization: 0.59%
```

IP address	Client-identifier/ Hardware address	Lease expiration	Type
3.3.3.111	0015-88f8-0dd7	Dec 15 2009 17:40:52	Auto:COMMITTED
3.3.3.2	0002-0002-0001	Dec 15 2009 17:41:02	Auto:COMMITTED
3.3.3.3	0015-e9a6-7cfe	Unlimited	Manual

--- total 3 entry ---

若用户认证失败，将被加入 **VLAN 2** 中，端口上生成的 **MAC VLAN** 表项及 **IP** 地址分配情况的查看方式同上，此处略。

目 录

1 端口安全配置	1-1
1.1 端口安全简介	1-1
1.1.1 概述	1-1
1.1.2 端口安全的特性	1-1
1.1.3 端口安全模式	1-1
1.1.4 端口安全对Guest VLAN和Auth-Fail VLAN的支持	1-3
1.2 端口安全配置任务简介	1-4
1.3 使能端口安全功能	1-4
1.3.1 配置准备	1-4
1.3.2 使能端口安全功能	1-4
1.4 配置端口安全允许的最大MAC地址数	1-5
1.5 配置端口安全模式	1-6
1.5.1 配置准备	1-6
1.5.2 配置端口安全模式	1-6
1.6 配置端口安全的特性	1-7
1.6.1 配置Need To Know特性	1-7
1.6.2 配置入侵检测特性	1-8
1.6.3 配置Trap特性	1-8
1.7 配置安全MAC地址	1-9
1.7.2 配置准备	1-10
1.7.3 配置安全MAC地址	1-10
1.8 配置当前端口不应用下发的授权信息	1-11
1.9 端口安全显示和维护	1-11
1.10 端口安全典型配置举例	1-12
1.10.1 端口安全autoLearn模式配置举例	1-12
1.10.2 端口安全userLoginWithOUI模式配置举例	1-14
1.10.3 端口安全macAddressElseUserLoginSecure模式配置举例	1-18
1.11 常见配置错误举例	1-21
1.11.1 端口安全模式无法设置	1-21
1.11.2 无法配置端口安全MAC地址	1-21
1.11.3 用户在线情况下无法更换端口安全模式	1-22

1 端口安全配置

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。



说明

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。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，推荐单独使用以上两个特性。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

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。

3. Trap特性

Trap 特性是指当端口有特定的数据包（由非法入侵，用户上下线等原因引起）传送时，设备将会发送 Trap 信息，便于网络管理员对这些特殊的行为进行监控。

1.1.3 端口安全模式

基本的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,否则根据端口所在安全模式进行相应的处理(学习、认证),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)或发送Trap告警。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。这些新的MAC地址被称为安全MAC,并被添加到安全MAC地址表中 当端口下的安全MAC地址数超过端口安全允许学习的最大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、手工配置的MAC地址的报文,才能通过该端口 该模式下,端口禁止学习动态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	
	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	
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 在用户接入方式为有线的情况下,非802.1X报文进行MAC地址认证,802.1X报文直接进行802.1X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; 在用户接入方式为有线的情况下,非802.1X报文进行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	

安全模式		工作机制	NTK/入侵检测
	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

- 当多个用户通过认证时，端口下所允许的最大用户数根据不同的端口安全模式，取端口安全所允许的最大 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 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，部分端口安全模式名称的构成可按如下规则理解：

- “userLogin”表示基于端口的 802.1X 认证；
- “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；
- 携带“Secure”的 userLogin 表示基于 MAC 地址的 802.1X 认证。
- 携带“Ext”表示可允许多个 802.1X 用户认证成功，不携带则表示仅允许一个 802.1X 用户认证成功。

1.1.4 端口安全对Guest VLAN和Auth-Fail VLAN的支持

802.1X 认证的 Guest VLAN 是指允许用户在未认证的情况下，可以访问的指定 VLAN。802.1X 的 Auth-Fail VLAN 与 MAC 地址认证的 Guest VLAN 是指允许用户在认证失败的情况下，可以访问的指定 VLAN。

- 对于支持 802.1X 认证的安全模式来说，可配置 Guest VLAN 和 Auth-Fail VLAN。关于 802.1X 认证的 Guest VLAN 和 Auth-Fail VLAN 的具体介绍请参见“安全配置指导”中的“802.1X”。
- 对于支持 MAC 地址认证的安全模式来说，可配置 Guest VLAN。关于 MAC 地址认证 Guest VLAN 的具体介绍请参见“安全配置指导”中的“MAC 地址认证”。



说明

若端口上同时配置了 802.1X 认证的 Auth-Fail VLAN 与 MAC 地址认证的 Guest VLAN，则后生成的 Auth-Fail VLAN 表项会覆盖先生成的 Guest VLAN 表项，但后生成的 Guest VLAN 表项不能覆盖先生成的 Auth-Fail VLAN 表项。

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
使能端口安全功能		必选	1.3
配置端口安全允许的最大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	可选 根据实际组网需求选择其中一种或多种特性	1.6
	配置入侵检测特性		
	配置Trap特性		
配置安全MAC地址		可选	1.7
配置当前端口不应用服务器下发的授权信息		可选	1.8

1.3 使能端口安全功能

1.3.1 配置准备

在使能端口安全功能之前，需要关闭全局的 802.1X 和 MAC 地址认证功能。

1.3.2 使能端口安全功能

表1-3 使能端口安全功能

操作	命令	说明
进入系统视图	system-view	-
使能端口安全功能	port-security enable	必选 缺省情况下，端口安全功能处于关闭状态



注意

执行使能或关闭端口安全功能的命令后，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**。
- 端口安全模式为 **noRestrictions**。

当端口安全功能处于使能状态时，端口上的 802.1X 功能以及 MAC 地址认证功能将不能被手动开启，且 802.1X 端口接入控制方式和端口接入控制模式也不能被修改，只能随端口安全模式的改变由系统更改。

在端口上有用户在线的情况下，端口安全功能无法关闭。



说明

- 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 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。最终端口上允许接入的用户数为此处配置的最大 MAC 地址数和相应认证类安全模式下允许的用户数的较小值；
- 控制 **autoLearn** 模式下端口能够添加的最大安全 MAC 地址数。

表1-4 配置端口安全允许的最大 MAC 地址数

操作	命令	说明
进入系统视图	system-view	-
进入二层以太网端口视图	interface <i>interface-type interface-number</i>	-
配置端口安全允许的最大 MAC 地址数	port-security max-mac-count <i>count-value</i>	必选 缺省情况下，最大MAC地址数不受限制



说明

端口安全允许的最大 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。

1.5 配置端口安全模式

1.5.1 配置准备

在配置端口安全模式之前，端口上需要满足以下条件：

- 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。

（如果以上条件不满足，则系统会提示错误信息，且不能进行端口安全模式的配置；如果端口上已经配置了端口安全模式，则以上配置就不允许改变。）

- 对于 autoLearn 模式，还需要提前设置端口安全允许的最大 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 MAC 地址数。



说明

- 在端口安全功能未使能的情况下，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，端口安全模式无法改变。

1.5.2 配置端口安全模式

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	-
配置允许通过认证的用户 OUI 值	port-security oui oui-value index index-value	可选 缺省情况下，没有配置允许通过认证的用户 OUI 值 该命令仅在配置 userlogin-withoui 安全模式时必选
进入二层以太网端口视图	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 }	必选 缺省情况下，端口处于 noRestrictions 模式



说明

- OUI (Organizationally Unique Identifier) 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。
- 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，仅允许其中一个 OUI 值所属的用户通过认证。
- 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。

1.6 配置端口安全的特性

1.6.1 配置Need To Know特性

该功能用来限制认证端口上出方向的报文转发。即，用户通过认证后，以此 MAC 为目的地址的报文都可以正常转发。可以设置以下三种方式：

- **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。

表1-6 配置 Need To Know 特性

操作	命令	说明
进入系统视图	system-view	-
进入二层以太网端口视图	interface <i>interface-type</i> <i>interface-number</i>	-
配置端口Need To Know 特性	port-security ntk-mode { ntk-withbroadcasts ntk-withmulticasts ntkonly }	必选 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



说明

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。

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，该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	-
进入二层以太网端口视图	interface <i>interface-type</i> <i>interface-number</i>	-
配置入侵检测特性	port-security intrusion-mode { blockmac disableport disableport-temporarily }	必选 缺省情况下，不进行入侵检测处理
退回系统视图	quit	-
配置系统暂时关闭端口连接的时间	port-security timer disableport <i>time-value</i>	可选 缺省情况下，系统暂时关闭端口连接的时间为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。

1.6.3 配置Trap特性

该特性用于端口上发生关键事件时触发告警开关输出对应的 Trap 信息，包括以下几种情况：

- **addresslearned**：端口学习到新 MAC 地址时发出告警信息。
- **dot1xlogfailure/dot1xlogon/dot1xlogoff**：802.1X 用户认证失败/认证成功/下线时发出告警日志。
- **raimlogfailure/raimlogon/raimlogoff**：MAC 地址认证用户认证失败/认证成功/下线时发出告警信息。
- **intrusion**：发现非法报文时发出告警信息。

表1-8 配置 Trap 特性

操作	命令	说明
进入系统视图	system-view	-

操作	命令	说明
打开指定告警信息的开关	port-security trap { addresslearned dot1xlogfailure dot1xlogoff dot1xlogon intrusion ralmlogfailure ralmlogoff ralmlogon }	必选 缺省情况下，所有告警信息的开关处于关闭状态

1.7 配置安全MAC地址

安全 MAC 地址是一种特殊的 MAC 地址，不会因为端口状态的变化而被丢失。在同一个 VLAN 内，一个安全 MAC 地址只能被添加到一个端口上，利用该特点，可以实现同一 VLAN 内 MAC 地址与端口的绑定。

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，比如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；或者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。我们将这类可老化的安全 MAC 地址称为 Sticky MAC。

表1-9 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	老化机制
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	无
手工添加（指定 sticky 关键字）	可老化（老化时间可配），称之为 Sticky MAC 地址	• 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。（缺省） • 动态类型的安全 MAC 地址不能被保存在配置文件中，设备重启后会被丢失	• 定时老化（缺省） • 无流量老化 说明：无论是 Sticky MAC 地址还是动态类型的安全 MAC 地址，均遵循此老化机制
端口自动学习	• 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 地址可通过配置转换为动态类型的 MAC 地址		



说明

- 动态类型的安全 MAC 地址与 Sticky MAC 地址可通过配置相互转换，两者本质相同，仅配置保存方式不同。
- 无流量老化方式下，设备会定期检测（检测周期不可配）端口上的安全 MAC 地址是否有流量产生，若某安全 MAC 地址在配置的 Sticky MAC 地址老化时间内没有任何流量产生，则才会被老化。
- 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 地址为安全 MAC 地址的报文和源 MAC 地址为手工配置的 MAC 地址的报文访问网络设备。

1.7.2 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

1.7.3 配置安全MAC地址

表1-10 配置安全 MAC 地址

操作		命令	说明
进入系统视图		system-view	-
配置安全MAC地址的老化时间		port-security timer autolearn aging <i>time-value</i>	可选 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] <i>mac-address interface interface-type interface-number vlan vlan-id</i>	二者必选其一 缺省情况下，未配置安全MAC地址
	在二层以太网端口视图下	interface <i>interface-type interface-number</i>	
		port-security mac-address security [sticky] <i>mac-address vlan vlan-id</i>	
		quit	
进入二层以太网端口视图		interface <i>interface-type interface-number</i>	-
配置安全地址的老化方式为无流量老化		port-security mac-address aging-type inactivity	可选 缺省情况下，安全MAC地址按照固定时间进行老化，即在配置的安全MAC地址的老化时间到达后立即老化
将Sticky MAC地址设置为动态类型的安全MAC地址		port-security mac-address dynamic	可选 缺省情况下，Sticky MAC地址能够被保存在配置文件中，设备重启后也不会丢失



说明

- 无流量老化方式下，设备会定期检测（检测周期固定，不可配）端口上的安全 MAC 地址是否有流量产生，若某安全 MAC 地址在配置的安全 MAC 地址老化时间内没有任何流量产生，则才会被老化。
- 动态类型的安全 MAC 地址不会被保存在配置文件中，可通过执行 **display port-security mac-address security** 命令查看到，设备重启之后会丢失。

1.8 配置当前端口不应用下发的授权信息

802.1X 用户或 MAC 地址认证用户在 RADIUS 服务器或设备上通过认证时，服务器或设备会把授权信息下发给用户。通过此配置可实现基于端口是否忽略 RADIUS 服务器或设备本地下发的授权信息。

表1-11 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	-
进入二层以太网端口视图	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	必选 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 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-list] [{ begin exclude include } regular-expression]
显示安全 MAC 地址信息	display port-security mac-address security [interface interface-type interface-number] [vlan vlan-id] [count] [{ begin exclude include } regular-expression]
显示阻塞 MAC 地址信息	display port-security mac-address block [interface interface-type interface-number] [vlan vlan-id] [count] [{ begin exclude include } regular-expression]

1.10 端口安全典型配置举例

1.10.1 端口安全autoLearn模式配置举例

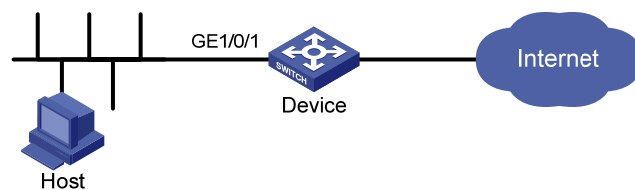
1. 组网需求

在 Device 的端口 GE1/0/1 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 安全 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

(1) 具体的配置步骤

```
<Device> system-view
```

使能端口安全功能。

```
[Device] port-security enable
```

设置 Sticky MAC 地址的老化时间为 30 分钟。

```
[Device] port-security timer autolearn aging 30
```

打开入侵检测 Trap 开关。

```
[Device] port-security trap intrusion
```

```
[Device] interface gigabitethernet 1/0/1
```

设置端口安全允许的最大 MAC 地址数为 64。

```
[Device-GigabitEthernet1/0/1] port-security max-mac-count 64
```

设置端口安全模式为 autoLearn。

```
[Device-GigabitEthernet1/0/1] 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-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
```

```
[Device-GigabitEthernet1/0/1] quit
```

```
[Device] port-security timer disableport 30
```

(2) 验证配置结果

上述配置完成后，可以用 **display** 命令显示端口安全配置情况，如下：

```
[Device] display port-security interface gigabitethernet 1/0/1
```

```
Equipment port-security is enabled
```

```
Intrusion trap is enabled
```

```
AutoLearn aging time is 30 minutes
```

Disableport Timeout: 30s
OUI value:

```
GigabitEthernet1/0/1 is link-up
  Port mode is autoLearn
  NeedToKnow mode is disabled
  Intrusion Protection mode is DisablePortTemporarily
  Max MAC address number is 64
  Stored MAC address number is 0
  Authorization is permitted
  Security MAC address learning mode is sticky
  Security MAC address aging type is absolute
```

可以看到端口安全所允许的最大 MAC 数为 64，端口模式为 autoLearn，入侵检测 Trap 开关打开，入侵保护动作为 DisablePortTemporarily，入侵发生后端口禁用时间为 30 秒。

配置完成后，允许地址学习，学习到的 MAC 地址数可以用上述命令显示，如学习到 5 个，那么存储的安全 MAC 地址数就为 5，可以在端口视图下用 **display this** 命令查看学习到的 MAC 地址，如：

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
  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，Trap 信息如下：

```
#Jan 14 10:39:47:135 2011 Device PORTSEC/4/VIOLATION: Trap1.3.6.1.4.1.25506.2.26.1.
3.2<hh3cSecureViolation>:
  An intrusion occurs!
  IfIndex: 9437185
  Port: 9437185
  MAC Addr: 00:02:00:00:00:32
  VLAN ID: 1
  IfAdminStatus: 1
```

并且可以通过下述命令看到端口安全将此端口关闭：

```
[Device-GigabitEthernet1/0/1] display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 current state: DOWN ( Port Security Disabled )
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-cb00-5558
Description: GigabitEthernet1/0/1 Interface
.....
```

30 秒后，端口状态恢复：

```
[Device-GigabitEthernet1/0/1] display interface gigabitethernet 1/0/1
```

```
GigabitEthernet1/0/1 current state: UP
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-cb00-5558
Description: GigabitEthernet1/0/1 Interface
.....
```

此时，如手动删除几条安全 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。

1.10.2 端口安全userLoginWithOUI模式配置举例

1. 组网需求

客户端通过端口 `GE1/0/1` 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。

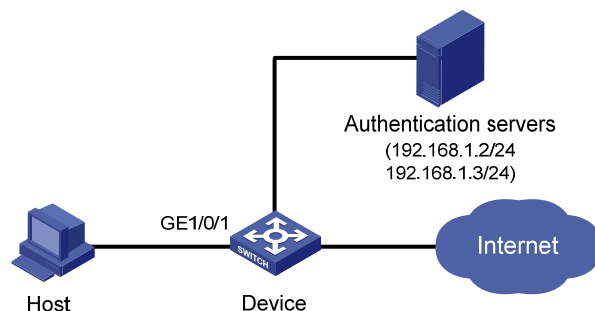
- IP 地址为 192.168.1.2 的 RADIUS 服务器作为主认证/备份计费服务器，IP 地址为 192.168.1.3 的 RADIUS 服务器作为备份认证/主计费服务器。认证共享密钥为 `name`，计费共享密钥为 `money`。
- 所有接入用户都使用 ISP 域 `sun` 的缺省认证/授权/计费方案，该域最多可容纳 30 个用户；
- 系统向 RADIUS 服务器重发报文的时间间隔为 5 秒，重发次数为 5 次，发送实时计费报文的时间间隔为 15 分钟，发送的用户名不带域名。

Device 的管理者希望对接入用户的端口 `GE1/0/1` 做如下限制：

- 允许一个 802.1X 用户上线；
- 最多可以配置 16 个 OUI 值，还允许端口上有一个与 OUI 值匹配的 MAC 地址用户通过。

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”。
- 客户端和 RADIUS 服务器之间路由可达，认证相关的配置略。

(1) 具体的配置步骤

- 配置 RADIUS 协议

```
<Device> system-view
```

配置 RADIUS 方案。

```
[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 name
[Device-radius-radsun] key accounting 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 default radius-scheme radsun
[Device-isp-sun] authorization default radius-scheme radsun
[Device-isp-sun] accounting default radius-scheme radsun
[Device-isp-sun] access-limit enable 30
[Device-isp-sun] quit
```

- 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
```

- 配置端口安全特性

使能端口安全功能。

```
[Device] port-security enable
```

添加 5 个 OUI 值。

```
[Device] port-security oui 1234-0100-1111 index 1
[Device] port-security oui 1234-0200-1111 index 2
[Device] port-security oui 1234-0300-1111 index 3
[Device] port-security oui 1234-0400-1111 index 4
[Device] port-security oui 1234-0500-1111 index 5
[Device] interface gigabitethernet 1/0/1
```

设置端口安全模式为 userLoginWithOUI。

```
[Device-GigabitEthernet1/0/1] port-security port-mode userlogin-withoui
[Device-GigabitEthernet1/0/1] quit
```

(2) 验证配置结果

查看名为 radsun 的 RADIUS 方案的配置信息：

```
[Device] display radius scheme radsun
```

SchemeName : radsun

Index : 1

Type : standard

Primary Auth Server:

IP: 192.168.1.2

Port: 1812

State: active


```

Encryption Key : N/A
VPN instance   : N/A
Probe username : N/A
Probe interval : N/A
Primary Acct Server:
  IP: 192.168.1.3                               Port: 1813   State: active
  Encryption Key : N/A
  VPN instance   : N/A
Second Auth Server:
  IP: 192.168.1.3                               Port: 1812   State: active
  Encryption Key : N/A
  VPN instance   : N/A
  Probe username : N/A
  Probe interval : N/A
Second Acct Server:
  IP: 192.168.1.2                               Port: 1813   State: active
  Encryption Key : N/A
  VPN instance   : N/A
Auth Server Encryption Key : *****
Acct Server Encryption Key : *****
Accounting-On packet disable, send times : 5 , interval : 3s
Interval for timeout(second)                : 5
Retransmission times for timeout              : 5
Interval for realtime accounting(minute)      : 15
Retransmission times of realtime-accounting packet : 5
Retransmission times of stop-accounting packet : 500
Quiet-interval(min)                          : 5
Username format                              : without-domain
Data flow unit                               : Byte
Packet unit                                  : one

```

查看名为 sun 的 ISP 域的配置信息:

```

[Device] display domain sun
  Domain : sun
  State : Active
  Access-limit : 30
  Accounting method : Required
  Default authentication scheme : radius:radsun
  Default authorization scheme : radius:radsun
  Default accounting scheme : radius:radsun
  Domain User Template:
  Idle-cut : Disabled
  Self-service : Disabled
  Authorization attributes:

```

查看端口安全的配置信息:

```

[Device] display port-security interface gigabitethernet 1/0/1
Equipment port-security is enabled
Trap is disabled

```

Disableport Timeout: 20s

OUI value:

Index is 1, OUI value is 123401
Index is 2, OUI value is 123402
Index is 3, OUI value is 123403
Index is 4, OUI value is 123404
Index is 5, OUI value is 123405

GigabitEthernet1/0/1 is link-up

Port mode is userLoginWithOUI
NeedToKnow mode is disabled
Intrusion Protection mode is NoAction
Max MAC address number is not configured
Stored MAC address number is 0
Authorization is permitted
Security MAC address learning mode is sticky
Security MAC address aging type is absolute

配置完成后，如果有 802.1X 用户上线，则可以看到存储的安全 MAC 地址数为 1。还可以通过下述命令查看 802.1X 用户的情况：

[Device] display dot1x interface gigabitethernet 1/0/1

Equipment 802.1X protocol is enabled
CHAP authentication is enabled
EAD quick deploy is disabled

Configuration: Transmit Period 30 s, Handshake Period 15 s
Quiet Period 60 s, Quiet Period Timer is disabled
Supp Timeout 30 s, Server Timeout 100 s
Reauth Period 3600 s
The maximal retransmitting times 2

EAD quick deploy configuration:

EAD timeout: 30m

The maximum 802.1X user resource number is 2048 per slot

Total current used 802.1X resource number is 1

GigabitEthernet1/0/1 is link-up

802.1X protocol is enabled
Handshake is enabled
Handshake secure is disabled
802.1X unicast-trigger is enabled
Periodic reauthentication is disabled
The port is an authenticator
Authentication Mode is Auto
Port Control Type is Mac-based
802.1X Multicast-trigger is enabled
Mandatory authentication domain: NOT configured
Guest VLAN: NOT configured
Auth-Fail VLAN: NOT configured

Critical VLAN: NOT configured
Critical recovery-action: NOT configured
Max number of on-line users is 2048

EAPOL Packet: Tx 16331, Rx 102
Sent EAP Request/Identity Packets : 16316
 EAP Request/Challenge Packets: 6
 EAP Success Packets: 4, Fail Packets: 5
Received EAPOL Start Packets : 6
 EAPOL LogOff Packets: 2
 EAP Response/Identity Packets : 80
 EAP Response/Challenge Packets: 6
 Error Packets: 0

1. Authenticated user : MAC address: 0002-0000-0011

Controlled User(s) amount to 1

此外，端口还允许一个与 OUI 值匹配的 MAC 地址的用户通过，可以通过下述命令查看：

[Device] display mac-address interface gigabitethernet 1/0/1

MAC ADDR	VLAN ID	STATE	PORT INDEX	AGING TIME(s)
1234-0300-0011	1	Learned	GigabitEthernet1/0/1	AGING

--- 1 mac address(es) found ---

1.10.3 端口安全macAddressElseUserLoginSecure模式配置举例

1. 组网需求

客户端通过端口 GE1/0/1 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。

Device 的管理者希望对接入用户的端口 GE1/0/1 做如下的限制：

- 可以有多个 MAC 认证用户上线；
- 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。802.1X 用户限制为 1 个；
- MAC 地址认证用户使用 MAC 地址作为用户名和密码，其中 MAC 地址带连字符、字母小写；
- 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 Need To Know 特性。

2. 组网图

同 [图 1-2](#) 所示。

3. 配置步骤



说明

- RADIUS 认证/计费及 ISP 域的配置同 [1.10.2](#)，这里不再赘述。
- 接入用户和 RADIUS 服务器之间路由可达，认证相关的配置略。

(1) 具体的配置步骤

```
<Device> system-view
```

使能端口安全功能。

```
[Device] port-security enable
```

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
```

配置 MAC 地址认证用户所使用的 ISP 域。

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

```
[Device] interface gigabitethernet 1/0/1
```

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-GigabitEthernet1/0/1] port-security max-mac-count 64
```

设置端口安全模式为 macAddressElseUserLoginSecure。

```
[Device-GigabitEthernet1/0/1] port-security port-mode mac-else-userlogin-secure
```

设置端口 Need To Know 模式为 ntkonly。

```
[Device-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
```

```
[Device-GigabitEthernet1/0/1] quit
```

(2) 验证配置结果

查看端口安全的配置信息：

```
[Device] display port-security interface gigabitethernet 1/0/1
```

```
Equipment port-security is enabled
```

```
Trap is disabled
```

```
Disableport Timeout: 20s
```

```
OUI value:
```

```
GigabitEthernet1/0/1 is link-up
```

```
Port mode is macAddressElseUserLoginSecure
```

```
NeedToKnow mode is NeedToKnowOnly
```

```
Intrusion Protection mode is NoAction
```

```
Max MAC address number is 64
```

```
Stored MAC address number is 0
```

```
Authorization is permitted
```

```
Security MAC address learning mode is sticky
```

```
Security MAC address aging type is absolute
```

查看 MAC 地址认证情况：

```
[Device] display mac-authentication interface gigabitethernet 1/0/1
```

```
MAC address authentication is enabled.
```

```
User name format is MAC address in lowercase, like xx-xx-xx-xx-xx-xx
```

```
Fixed username: mac
```

```
Fixed password: not configured
```

```
Offline detect period is 60s
```

```
Quiet period is 5s
```

```
Server response timeout value is 100s
```

The max allowed user number is 2048 per slot
Current user number amounts to 3
Current domain is mac

Silent MAC User info:

MAC Addr	From Port	Port Index
GigabitEthernet1/0/1 is link-up		
MAC address authentication is enabled		
Authenticate success: 3, failed: 7		
Max number of on-line users is 2048		
Current online user number is 3		
MAC ADDR	Authenticate state	Auth Index
1234-0300-0011	MAC_AUTHENTICATOR_SUCCESS	13
1234-0300-0012	MAC_AUTHENTICATOR_SUCCESS	14
1234-0300-0013	MAC_AUTHENTICATOR_SUCCESS	15

查看 802.1X 认证情况:

<Device> display dot1x interface gigabitethernet 1/0/1

Equipment 802.1X protocol is enabled

CHAP authentication is enabled

EAD quick deploy is disabled

Configuration: Transmit Period 30 s, Handshake Period 15 s
Quiet Period 60 s, Quiet Period Timer is disabled
Supp Timeout 30 s, Server Timeout 100 s
The maximal retransmitting times 2

EAD quick deploy configuration:

EAD timeout: 30m

Total maximum 802.1X user resource number is 2048 per slot

Total current used 802.1X resource number is 1

GigabitEthernet1/0/1 is link-up

802.1X protocol is enabled

Handshake is enabled

Handshake secure is disabled

802.1X unicast-trigger is enabled

Periodic reauthentication is disabled

The port is an authenticator

Authentication Mode is Auto

Port Control Type is Mac-based

802.1X Multicast-trigger is enabled

Mandatory authentication domain: NOT configured

Guest VLAN: NOT configured

Auth-Fail VLAN: NOT configured

Critical VLAN: NOT configured

Critical recovery-action: NOT configured

Max number of on-line users is 2048

EAPOL Packet: Tx 16331, Rx 102

Sent EAP Request/Identity Packets : 16316

EAP Request/Challenge Packets: 6

EAP Success Packets: 4, Fail Packets: 5

Received EAPOL Start Packets : 6

EAPOL LogOff Packets: 2

EAP Response/Identity Packets : 80

EAP Response/Challenge Packets: 6

Error Packets: 0

1. Authenticated user : MAC address: 0002-0000-0011

Controlled User(s) amount to 1

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。

1.11 常见配置错误举例

1.11.1 端口安全模式无法设置

1. 故障现象

无法配置端口安全模式。

```
[Device-GigabitEthernet1/0/1] port-security port-mode autolearn
```

Error:When we change port-mode, we should first change it to noRestrictions, then change it to the other.

2. 故障分析

在当前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。

```
[Device-GigabitEthernet1/0/1] undo port-security port-mode
```

```
[Device-GigabitEthernet1/0/1] port-security port-mode autolearn
```

1.11.2 无法配置端口安全MAC地址

1. 故障现象

无法配置端口安全 MAC 地址。

```
[Device-GigabitEthernet1/0/1] port-security mac-address security 1-1-2 vlan 1
```

Error: Security MAC address configuration failed.

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-GigabitEthernet1/0/1] undo port-security port-mode
```

```
[Device-GigabitEthernet1/0/1] port-security max-mac-count 64
```

```
[Device-GigabitEthernet1/0/1] port-security port-mode autolearn
[Device-GigabitEthernet1/0/1] port-security mac-address security 1-1-2 vlan 1
```

1.11.3 用户在线情况下无法更换端口安全模式

1. 故障现象

802.1X 或 MAC 地址认证用户在线的情况下，更换端口安全模式失败。

```
[Device-GigabitEthernet1/0/1] undo port-security port-mode
Error:Cannot configure port-security for there is 802.1X user(s) on line on port
GigabitEthernet1/0/1.
```

2. 故障分析

有 802.1X 或 MAC 认证用户在线的情况下，禁止更换端口安全模式。

3. 处理过程

断开端口与用户的连接后再进行端口安全模式更换，可以通过 **cut** 命令强制切断连接。

```
[Device-GigabitEthernet1/0/1] quit
[Device] cut connection interface gigabitethernet 1/0/1
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] undo port-security port-mode
```

目 录

1 User Profile配置	1-1
1.1 User Profile简介	1-1
1.2 User Profile配置任务简介	1-1
1.3 创建User Profile	1-2
1.3.1 配置准备	1-2
1.3.2 创建User Profile	1-2
1.4 配置User Profile	1-2
1.5 激活User Profile	1-3
1.6 User Profile显示和维护	1-3

1 User Profile配置

1.1 User Profile简介

User Profile（用户配置文件）提供一个配置模板，能够保存预设配置（一系列配置的集合）。用户可以根据不同的应用场景为 User Profile 配置不同的内容，比如 QoS（Quality of Service，服务质量）策略等。

用户访问设备时，需要先进行身份认证（目前支持 802.1X 和 Portal 两种接入认证方式）。在认证过程中，认证服务器会先匹配用户名和密码，匹配成功后再将与用户绑定的 User Profile 名称下发给设备，设备会立即启用 User Profile 里配置的具体内容。只有用户名和密码匹配，并且 User Profile 下的配置均应用成功，设备才认为用户通过了认证。因此，当用户通过认证上线后，其访问行为将受到 User Profile 的限制。当用户下线时，系统会自动禁用 User Profile 下的配置项，从而取消 User Profile 对用户的限定。因此，User Profile 适用于限制上线用户的访问行为，没有用户上线（可能是没有用户接入、或者用户没有通过认证、或者用户下线）时，User Profile 是预设配置，并不生效。

使用 User Profile 之后，可以：

- 更精确地利用系统资源。比如，使用 User Profile 之前，只能基于接口/VLAN/全局等应用 QoS 策略，这个 QoS 策略限制的是一群用户（从指定接口/VLAN 接入的用户，甚至设备的所有接入用户）；使用 User Profile 之后，可以基于用户应用 QoS 策略，这个 QoS 策略针对的是单个用户。
- 更灵活地限制用户访问系统资源。比如，使用 User Profile 之前，只能基于 QoS 策略对当前接口的所有流进行流量监管，当用户的物理位置移动时（比如从另一个接口接入），则需要先取消旧的接入接口下的流量监管功能，再在新的接入接口下配置流量监管功能；使用 User Profile 之后，可以基于用户进行流量监管，只要用户上线，认证服务器会自动下发相应的 User Profile（配置了 QoS 策略），当用户下线，系统会自动取消相应的配置，不需要再进行手工调整。

1.2 User Profile配置任务简介

表1-1 User Profile 配置任务简介

配置任务	说明	详细配置
创建User Profile	必选	1.3
配置User Profile	必选	1.4
激活User Profile	必选	1.5

1.3 创建User Profile

1.3.1 配置准备

在创建 User Profile 之前，需配置认证参数。User Profile 特性支持 802.1X 和 Portal 两种接入认证方式，用户在访问网络时可以根据当前的网络规划选择一种方式进行认证。但需要在客户端、本设备和认证服务器上进行相应的配置（比如用户名、密码、认证方案、域以及 User Profile 和用户的绑定关系等）。

1.3.2 创建User Profile

表1-2 创建 User Profile

操作	命令	说明
进入系统视图	system-view	-
创建User Profile并进入相应的user-profile视图	user-profile <i>profile-name</i>	必选 如果指定的User Profile已经存在,则直接进入相应的user-profile视图，不需要再创建User Profile 进入user-profile视图后,下面进行的配置只在User Profile处于激活状态，且用户成功上线后才生效

1.4 配置User Profile

User Profile 创建之后，需要在 User Profile 视图下配置具体的内容才能对上线用户进行限制。用户可以通过在 User Profile 视图下应用 QoS 策略来实现多种流量管理功能。

表1-3 基于上线用户应用 QoS 策略

操作	命令	说明
进入系统视图	system-view	-
进入user-profile视图	user-profile <i>profile-name</i>	必选 进入user-profile视图后,下面进行的配置只在User Profile处于激活状态，且用户成功上线后才生效
应用关联的策略	qos apply policy <i>policy-name</i> { inbound outbound }	必选 inbound 是对设备入方向的上线用户流量（即上线用户发送的流量）应用策略； outbound 是对设备出方向的上线用户流量（即上线用户接收到的流量）应用策略



说明

- 如果 User Profile 处于激活状态，既不能修改策略的内容（包括流分类引用的 ACL 规则），也不能删除已经应用到此 User Profile 的策略。
- user-profile 视图下应用的策略中的流行为只支持 **remark**、**car**、**filter** 三种动作。
- user-profile 视图下应用的策略不能为空策略，因为应用空策略的 User Profile 不能被激活。
- 关于 QoS 策略的相关配置命令，请参见“ACL 和 QoS 配置指导”中的“QoS 配置方式”。

1.5 激活 User Profile

User Profile 创建后，必须被激活，User Profile 下的配置才能生效。如果不激活 User Profile，会导致被绑定的用户认证失败，不能上线。

表1-4 激活 User Profile

操作	命令	说明
进入系统视图	system-view	-
激活已创建的 User Profile	user-profile profile-name enable	必选 缺省情况下，创建的 User Profile 处于未激活状态



注意

- User Profile 被激活后，不允许修改 User Profile 下的配置，需要禁用后才可以被修改或删除。
- 禁用 User Profile 将导致使用该 User Profile 用户强制下线。

1.6 User Profile 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 User Profile 的运行情况，通过查看显示信息验证配置的效果。

表1-5 User Profile 显示和维护

操作	命令
显示当前已创建的全部 User Profile 的信息	display user-profile [{ begin exclude include } regular-expression]

目 录

1 Password Control配置	1-1
1.1 Password Control简介	1-1
1.2 Password Control配置任务简介	1-4
1.3 配置Password Control	1-4
1.3.1 使能密码管理	1-4
1.3.2 配置全局密码管理	1-6
1.3.3 配置用户组密码管理	1-7
1.3.4 配置本地用户密码管理	1-7
1.3.5 配置super密码管理	1-8
1.3.6 以交互式方式设置本地用户密码	1-8
1.4 Password Control显示和维护	1-9
1.5 Password Control典型配置举例	1-9

1 Password Control配置



说明

- 设备运行于 FIPS 模式时，本特性的部分配置相对于非 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”。
- 本章中典型配置举例中的配置，如无特殊说明，均以设备运行在非 FIPS 模式下的命令行为准。

1.1 Password Control简介

Password Control（密码管理）是本地认证服务器提供的密码安全功能，它根据管理员设置的安全策略对用户的登录密码、super 密码和用户的登录状态进行控制。密码管理功能实现的密码安全策略包括：

1. 密码最小长度限制

根据系统安全需求不同，管理员可以设置用户密码的最小长度。当用户设置用户密码时，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，此时将显示出错信息，提醒用户重新输入密码。

2. 密码更新间隔时间管理

管理员可以根据系统安全需求，设置用户登录设备后修改自身密码的最小间隔时间。当非管理级别的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。这样可以有效防止登录用户频繁进行修改密码的操作。



说明

- 该功能对管理级别的用户不生效。关于用户级别的详细介绍请参见“基础配置指导”中的“CLI”。
- 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。

3. 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超时时，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。

4. 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。



说明

在密码老化管理和密码过期提醒这两项功能中，不允许 FTP 用户更改密码，只能通过管理员修改 FTP 用户的密码；允许 Telnet、SSH、Terminal 用户自行修改密码。

5. 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。这样允许密码过期的用户登录设备时不需要立即更新密码。

6. 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，旧的密码将被记录下来，形成该用户的密码历史记录。如果用户新设置的密码以前被使用过，系统将给出错误提示，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与密码历史记录以及当前密码相比较，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。

7. 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黑名单。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，通过设置可以有三种选择：

- 永久禁止该用户登录。只有管理员把该用户从密码管理黑名单中删除后，该用户才能重新登录。
- 不对该用户做禁止，允许其继续登录。在该用户登录成功或者密码管理黑名单的老化时间（系统规定为 1 分钟）超时后，该用户会从该黑名单中被删除。
- 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。



说明

- 密码管理的黑名单的最大条数为 1024。不存在的用户进行登录认证时将失败，但不将该用户加入黑名单中。
- FTP 用户和通过 VTY 方式访问设备的用户在认证失败后，会被加入密码管理的黑名单。
- 通过 Console 口连接到设备的用户，由于系统无法获得其 IP 地址，且通过这两种方式访问设备的用户已经具备了一定的权限和安全性，所以认证失败后不会被加入密码管理的黑名单。

8. 密码的组合检测功能

根据系统安全需求不同，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：

- [A~Z]
- [a~z]
- [0~9]
- 32 个特殊字符（空格~`!@#\$%^&*()_+~={}|~\:"';'<>.,/）

密码元素的组合级别为 1~4 级，级别表示设置密码时至少要包含的密码元素种类数目：

- 1 表示密码中至少包含 1 种元素；
- 2 表示密码中至少包含 2 种元素；
- 3 表示密码中至少包含 3 种元素；
- 4 表示密码中包含 4 种元素。

当用户设定或修改密码时，系统检查设定的密码是否符合配置要求。如果不符合，将给出错误提示。

9. 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：配置本地用户密码时，系统检测输入的密码是否符合一定的复杂度要求，如果不符合复杂度要求，则提示密码配置失败。目前，复杂度检测功能对密码的复杂度要求包括：

- 密码中不能包含用户名或者颠倒的用户名。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。

10. 密码回显为“*”

出于安全考虑，用户输入的密码中的每个字符均以“*”显示。

11. 认证超时管理

认证超时管理只针对 Telnet 用户。

认证过程的时间为：从服务器获得用户名到该用户的密码验证结束的时间。用户如果在规定时间内没有完成认证，则认证失败，用户连接将被断开。

12. 用户帐号闲置时间管理

根据系统安全需求，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用户账号登录。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。

13. 日志功能

系统对用户成功修改密码事件和用户登录失败加入密码管理的黑名单事件有相应的日志记录。

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和 **super** 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。

上述四者之间的优先级关系如下：

- 对于本地用户密码的各管理参数来说，其生效的优先级顺序由高到底依次为本地用户视图、用户组视图、系统视图。
- 对于 **super** 密码的各管理参数来说，系统优先采用单独为 **super** 密码所作的单独配置；如果没有为 **super** 密码进行单独配置时，采用全局配置。

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
以交互式方式设置本地用户密码	可选	1.3.6

1.3 配置Password Control

1.3.1 使能密码管理

使能密码管理功能包括两个部分：

- (1) 使能全局密码管理功能。只有使能全局密码管理功能后，密码管理相关的配置才能生效。
- (2) 使能指定的密码管理功能。某些密码安全策略在使能全局密码管理功能后，还需要单独使能指定的密码管理功能才能生效。这些密码管理功能包括：
 - 密码老化管理
 - 密码最小长度管理
 - 密码历史记录管理
 - 密码组合检测管理功能

表1-2 使能密码管理

操作	命令	说明
进入系统视图	system-view	-

操作	命令	说明
使能全局密码管理功能	password-control enable	必选 缺省情况下，全局密码管理功能处于未使能状态
使能指定的密码管理功能	password-control { aging composition history length } enable	可选 缺省情况下，各密码管理功能均处于使能状态



说明

- 使能了全局密码管理功能后，设备上已配置的本地用户密码将不被显示，即无法通过相应的 **display** 命令查看本地用户密码。
- 使能了全局密码管理功能后，为保证用户密码符合安全要求，Telnet、SSH、Terminal 用户首次登录设备时，系统会提示用户进行密码修改。由于 FTP 用户没有交互修改密码的功能，故开启此功能后，需要管理员在设备上对 FTP 用户密码进行修改，否则 FTP 用户无法正常登录。



注意

- 未使能全局密码管理功能时：没有用户密码历史记录，用户新配置的密码可以和当前密码相同。
- 使能了全局密码管理功能，但密码历史记录功能未使能时：没有用户密码历史记录，用户新配置的密码可以和当前密码相同。
- 使能了全局密码管理功能，并使能了密码历史记录管理功能时：用户更改密码时，系统会将新设置的密码与密码历史记录以及当前密码相比较，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。



注意

- 未使能全局密码管理功能时：密码的最小长度为 1 个字符。
- 使能了全局密码管理功能，未使能密码最小长度管理功能时：非 FIPS 模式下密码的最小长度为 4 个字符；FIPS 模式下密码的最小长度为 8 个字符。密码中至少有四个字符不同。
- 使能了全局密码管理功能，并通过 **password-control length enable** 命令使能了密码最小长度管理功能时：密码的最小长度为 n 个字符。（n 为通过 **password-control length length** 命令配置的密码最小长度）。

1.3.2 配置全局密码管理

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 <i>aging-time</i>	可选 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 password update interval <i>interval</i>	可选 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 <i>length</i>	可选 缺省情况下，密码的最小长度为10个字符
配置用户密码的组合策略	password-control composition type-number <i>policy-type</i> [type-length <i>type-length</i>]	可选 非FIPS模式的缺省情况下，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模式的缺省情况下，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	可选 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 <i>max-record-num</i>	可选 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 <i>login-times</i> [exceed { lock unlock lock-time <i>time</i> }]	可选 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
配置密码老化前的提醒时间	password-control alert-before-expire <i>alert-time</i>	可选 缺省情况下，密码老化前的提醒时间为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 <i>delay</i> times <i>times</i>	可选 缺省情况下，密码过期后的30天内允许用户登录3次
配置用户认证的超时时间	password-control authentication-timeout <i>authentication-timeout</i>	可选 缺省情况下，用户认证的超时时间为60秒
配置用户帐号的闲置时间	password-control login idle-time <i>idle-time</i>	可选 缺省情况下，用户帐号的闲置时间为90天



注意

用户登录尝试失败后的行为的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，而其它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。

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 <i>group-name</i>	-
配置用户组的密码老化时间	password-control aging <i>aging-time</i>	可选 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 <i>length</i>	可选 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 <i>type-number</i> [type-length <i>type-length</i>]	可选 缺省情况下，采用全局密码组合策略

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	-
创建本地用户，并进入本地用户视图	local-user <i>user-name</i>	-
配置本地用户的密码老化时间	password-control aging <i>aging-time</i>	可选 缺省情况下，采用本地用户所属用户组的密码老化时间，若用户组未配置该值，则采用全局配置
配置本地用户的密码最小长度	password-control length <i>length</i>	可选 缺省情况下，采用本地用户所属用户组的密码最小长度，若用户组未配置该值，则采用全局配置
配置本地用户的密码组合策略	password-control composition type-number <i>type-number</i> [type-length <i>type-length</i>]	可选 缺省情况下，采用本地用户所属用户组的密码组合策略，若用户组未配置该值，则采用全局配置

1.3.5 配置super密码管理



说明

- 系统命令行采用分级保护方式：命令行级别由低到高被划分为访问级、监控级、系统级、管理级 4 个级别。同时对登录用户划分等级，分为 4 级，分别与上述的命令行级别对应，即不同级别的用户登录后，只能使用等于或低于自己级别的命令。
- 为了防止未授权用户的非法侵入，在从低级别用户切换到高级别用户时，要进行用户身份验证，即需要输入高级别用户密码，这个高级别的密码就被称为 super 密码。关于 super 密码的详细介绍，请参见“基础配置指导”中的“CLI”。

表1-6 配置 super Password Control

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 <i>aging-time</i>	可选 缺省情况下，采用全局密码老化时间
配置super密码的最小长度	password-control super length <i>length</i>	可选 缺省情况下，采用全局密码最小长度
配置super密码的组合策略	password-control super composition <i>type-number type-number [type-length type-length]</i>	可选 缺省情况下，采用全局密码组合策略

1.3.6 以交互式方式设置本地用户密码

以交互方式设置本地用户密码时会要求用户在输入本地密码后进行密码确认。

表1-7 以交互式方式设置本地用户密码

操作	命令	说明
进入系统视图	system-view	-
创建本地用户，并进入本地用户视图	local-user <i>user-name</i>	-
以交互式方式设置本地用户密码	password	必选

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1-8 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] [[{ begin exclude include } <i>regular-expression</i>]
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 <i>name</i> ip <i>ipv4-address</i> ipv6 <i>ipv6-address</i>] [[{ begin exclude include } <i>regular-expression</i>]
清除密码管理黑名单中的用户	reset password-control blacklist [all user-name <i>name</i>]
清除用户的密码历史记录	reset password-control history-record [user-name <i>name</i> super [level <i>level</i>]]



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; 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颠倒用户名; 不允许密码中包含连续三个或以上字符。
- **super** 密码管理策略: 密码元素的最少组合类型为 3 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 12 个字符, 密码元素的最少组合类型为 2 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
```

```

# 配置密码更新的最小时间间隔为 36 小时。
[Sysname] password-control password 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 super 密码元素的最少组合类型为 3 种，至少要包含每种元素的个数为 5 个。
[Sysname] password-control super composition type-number 3 type-length 5
# 配置 super 密码。
[Sysname] super password level 3 simple 12345ABGFTweuix
# 添加本地用户 test。
[Sysname] local-user test
# 配置本地用户的服务类型为 Telnet。
[Sysname-luser-test] service-type telnet
# 配置本地用户的最小密码长度为 12 个字符。
[Sysname-luser-test] password-control length 12
# 配置本地用户的密码元素的最少组合类型为 2 种，至少要包含每种元素的个数为 5 个。
[Sysname-luser-test] password-control composition type-number 2 type-length 5
# 配置本地用户的密码老化时间为 20 天。
[Sysname-luser-test] password-control aging 20
# 以交互式方式配置本地用户密码。
[Sysname-luser-test] password
Password:*****
Confirm :*****
Updating user(s) information, please wait.....
[Sysname-luser-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 (10 characters)
  Password composition:            Enabled (1 types, 1 characters per type)
  Password history:                Enabled (max history record:4)
  Early notice on password expiration: 7 days
  User authentication timeout:     60 seconds
  Maximum failed login attempts:   2 times
  Login attempt-failed action:     Lock
  Minimum password update time:    36 hours

```

```
User account idle-time:          30 days
Login with aged password:       5 times in 60 day(s)
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 (30 days)
Password length:               Enabled (10 characters)
Password composition:          Enabled (3 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
The contents of local user test:
State:                         Active
ServiceType:                   telnet
Access-limit:                  Disable          Current AccessNum: 0
User-group:                     system
Bind attributes:
Authorization attributes:
Password aging:                 Enabled (20 days)
Password length:               Enabled (12 characters)
Password composition:          Enabled (2 types, 5 characters per type)
Total 1 local user(s) matched.
```

目 录

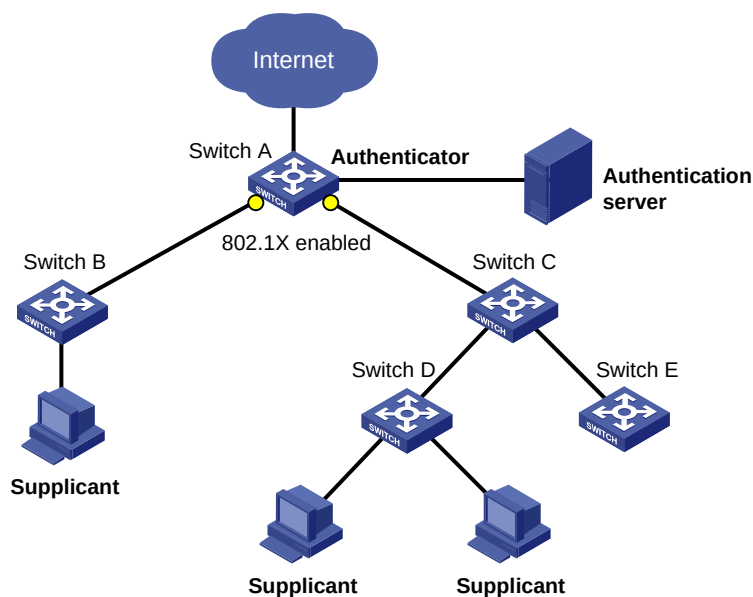
1 HABP配置.....	1-1
1.1 HABP简介	1-1
1.2 HABP配置	1-2
1.2.1 配置HABP server.....	1-2
1.2.2 配置HABP client	1-2
1.3 HABP显示和维护	1-3
1.4 HABP典型配置举例.....	1-3

1 HABP配置

1.1 HABP简介

HABP（HW Bypass Protocol，HW 旁路认证协议）是一种链路层应用协议，工作在 MAC 层之上，其主要作用是让启用 802.1X 或 MAC 地址认证的接入设备的下游设备免认证。

图1-1 802.1X 认证典型组网图



如 [图 1-1](#) 所示，802.1X 认证端设备 Switch A 下挂接入设备 Switch B 和 Switch C。在 Switch A 及其连接下游设备的端口上启动 802.1X 认证，终端用户可以通过主机上的 802.1X 客户端进行认证。在这种情况下，如果网络设备 Switch B 和 Switch D 之间也需要通信，则它们之间的报文在经过 Switch A 的时候就必须通过 802.1X 认证。但是设备上通常不支持 802.1X 客户端，所以需要一种简单的机制让网络设备绕过 802.1X 认证。

HABP 特性就可以解决以上问题，能帮助一些链路层报文穿过 802.1X 和 MAC 地址认证，在不影响认证体系正常功能的情况下，实现非终端用户的网络连接设备穿过认证，完成必要的网络设备间协议通信的功能。

HABP 协议采用 Server/Client 结构，每台设备同一时间只能成为一种角色，Server 或 Client。HABP server 一般应该在 802.1X 或 MAC 地址认证端设备上启动，例如上图中的 Switch A；HABP client 应该在下挂的交换机上启动，例如上图中的 Switch B、Switch C、Switch D 和 Switch E。通常 Server 会定期向 Client 发送 HABP 请求报文，收集下挂交换机 MAC 地址，形成 HABP 表项。而 Client 会对请求报文进行应答，同时向下层交换机转发 HABP 请求报文。所有的 HABP 报文只能在一个指定的 VLAN 内转发。HABP server 和 HABP client 通过该 VLAN 实现内部通信。



注意

- 在一个集群中，当使能了 802.1X 或 MAC 地址认证功能的成员设备还下挂有其它成员设备时，必须在该成员设备上开启 HABP server 功能，否则管理设备将无法对其下挂的成员设备进行管理。
- 关于集群功能的具体介绍请参见“网络管理和监控配置指导”中的“集群管理”。

1.2 HABP配置

1.2.1 配置HABP server

HABP server 一般是在认证端（开启了 802.1X 或 MAC 地址认证功能）设备上启动。开启该功能后，HABP server 就会定期（发送时间间隔可配）向连接的 HABP client 发送 HABP 请求报文，通过 HABP client 的响应报文来收集下挂交换机的 MAC 地址信息。HABP 报文在 HABP server 上的指定 VLAN 内传播。

表1-1 配置 HABP server

操作	命令	说明
进入系统视图	system-view	-
使能HABP功能	habp enable	可选 缺省情况下，HABP功能处于使能状态
设置HABP功能的模式为 Server模式，同时指定HABP报文在指定的VLAN内传播	habp server vlan <i>vlan-id</i>	必选 缺省情况下，HABP功能工作在 Client模式下
设置发送HABP请求报文的时间间隔	habp timer <i>interval</i>	可选 缺省情况下，发送HABP请求报文的时间间隔为20秒



说明

HABP server 上指定的传播 HABP 报文的 VLAN 必须与 HABP client 所属的 VLAN 保持一致。

1.2.2 配置HABP client

HABP client 是在认证端设备下挂的设备上启动。HABP client 收到 HABP server 的请求报文后，通过发送响应报文向 HABP server 告知本设备的 MAC 地址等信息，并向下层交换机转发该 HABP 请求报文。HABP 报文在 HABP client 所属的指定 VLAN 内传播。

表1-2 配置 HABP Client

操作	命令	说明
进入系统视图	system-view	-
使能HABP功能	habp enable	可选 缺省情况下，HABP功能处于使能状态
设置HABP功能的模式为Client模式	undo habp server	可选 缺省情况下，HABP功能工作在Client模式下
设置HABP client所属的VLAN	habp client vlan <i>vlan-id</i>	可选 缺省情况下，HABP Client所属的VLAN为VLAN 1



说明

HABP client 所属的 VLAN 必须与 HABP server 上指定的传播 HABP 报文的 VLAN 保持一致。

1.3 HABP显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令都可以显示配置后 HABP 的运行情况。

表1-3 HABP 显示和维护

操作	命令
显示HABP特性的配置信息和状态	display habp [{ begin exclude include } <i>regular-expression</i>]
显示HABP的MAC地址表信息	display habp table [{ begin exclude include } <i>regular-expression</i>]
显示HABP报文的统计信息	display habp traffic [{ begin exclude include } <i>regular-expression</i>]

1.4 HABP典型配置举例

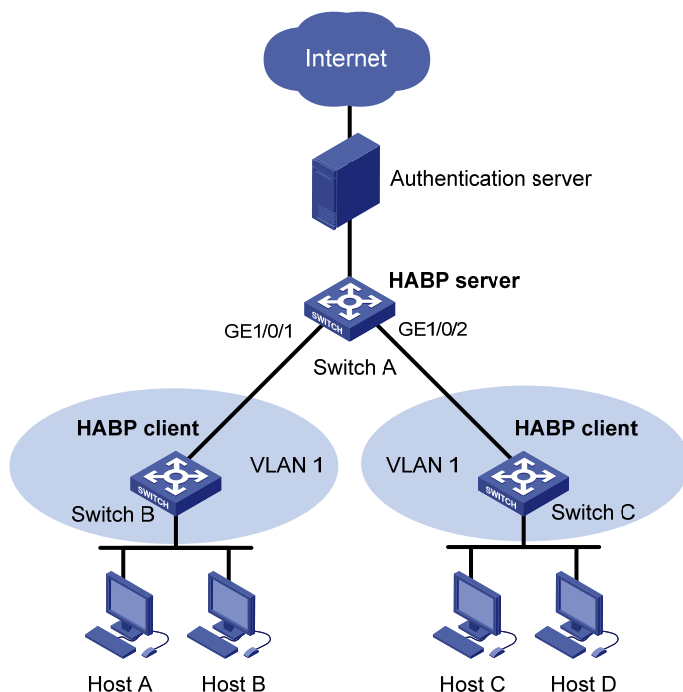
1. 组网需求

如 [图 1-2](#) 所示，Switch A下挂用户接入设备Switch B和Switch C。为了便于对接入用户（Host A～Host D）进行集中认证，在Switch A上开启 802.1X功能。

- 为满足 Switch B 和 Switch C 之间的通信需求，需要在 Switch A 上启动 HABP server 功能，在 Switch B 和 Switch C 上启动 HABP client 功能，并指定 HABP 报文在 VLAN 1 内传播。
- HABP server 以 50 秒的时间间隔周期性地向 VLAN 1 内的 HABP client 发送 HABP 请求报文。

2. 组网图

图1-2 HABP 典型配置组网图



3. 配置步骤

(1) 配置 Switch A

配置 802.1X 相关功能，具体请参见“安全配置指导”中的“802.1X”，此处略。

在 Switch A 上使能 HABP。（此配置可选，缺省情况下 HABP 功能处于使能状态）

```
<SwitchA> system-view
```

```
[SwitchA] habp enable
```

配置 HABP 工作在 Server 模式下，并指定 HABP 报文在 VLAN 1 内传播。

```
[SwitchA] habp server vlan 1
```

配置发送 HABP 请求报文的时间间隔为 50 秒。

```
[SwitchA] habp timer 50
```

(2) 配置 Switch B

在 Switch B 上使能 HABP。（此配置可选，缺省情况下 HABP 功能处于使能状态）

```
<SwitchA> system-view
```

```
[SwitchB] habp enable
```

配置 HABP 工作在 Client 模式下。（此配置可选，缺省情况下 HABP 工作在 Client 模式下）

```
[SwitchB] undo habp server
```

配置 HABP Client 所属的 VLAN，指定 HABP 报文在 VLAN 1 内传播。（此配置可选，缺省情况下 HABP Client 属于 VLAN 1）

```
[SwitchB] habp client vlan 1
```

(3) 配置 Switch C

配置步骤同 Switch B，此处略。

(4) 验证配置结果

可以通过此显示命令查看 HABP 相关配置信息。

```
<SwitchA> display habp
```

Global HABP information:

HABP Mode: Server

Sending HABP request packets every 50 seconds

Bypass VLAN: 1

可以通过此显示命令查看 MAC 地址表项的学习情况。

```
<SwitchA> display habp table
```

MAC	Holdtime	Receive Port
001f-3c00-0030	53	GigabitEthernet1/0/2
001f-3c00-0031	53	GigabitEthernet1/0/1

目 录

1 公钥管理配置	1-1
1.1 简介	1-1
1.2 公钥管理配置任务简介	1-2
1.3 配置本地的非对称密钥对	1-2
1.3.1 生成本地非对称密钥对	1-2
1.3.2 显示或导出本地非对称密钥对中的主机公钥	1-3
1.3.3 销毁本地非对称密钥对	1-4
1.4 配置远端主机的公钥	1-5
1.5 公钥管理显示和维护	1-6
1.6 公钥管理典型配置举例	1-6
1.6.1 手工配置远端主机的公钥	1-6
1.6.2 从公钥文件中导入远端主机的公钥	1-8

1 公钥管理配置



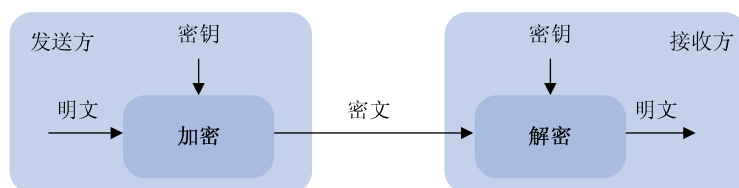
说明

- 设备运行于 FIPS 模式时，本特性的部分配置相对于非 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”。
- 本章中典型配置举例中的配置，如无特殊说明，均以设备运行在非 FIPS 模式下的命令行为准。

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



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。

非对称密钥算法包括 RSA（Rivest Shamir and Adleman）和 DSA（Digital Signature Algorithm，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 和 DSA 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“SSH2.0”、“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
配置本地的非对称密钥对	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
配置远端主机的主机公钥			1.4

1.3 配置本地的非对称密钥对

1.3.1 生成本地非对称密钥对

- 非 FIPS 模式下，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，二者都包括一个公钥和一个私钥。非 FIPS 模式下，RSA 服务器密钥和主机密钥模数的最小长度均为 512 比特，最大长度为 2048 比特，缺省长度为 1024 比特。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。FIPS 模式下，生成 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。
- 非 FIPS 模式下，生成 DSA 密钥对时，只生成一个主机密钥对。DSA 主机密钥模数的最小长度为 512 比特，最大长度为 2048 比特，缺省长度为 1024 比特。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 密钥模数的最小长度为 1024 比特，最大长度为 2048 比特，缺省长度为 1024 比特。

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 rsa }	必选 缺省情况下，不存在任何非对称密钥对



说明

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。

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）应用中，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：

- 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。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。
- 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。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。
- 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。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。

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 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 [{ begin exclude include } regular-expression]	二者至少选择其一 在任意视图下执行
显示本地DSA密钥对中的公钥信息	display public-key local dsa public [{ begin exclude include } regular-expression]	



说明

执行 **display public-key local rsa public** 命令后，会同时显示 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。

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 { openssh ssh1 ssh2 } FIPS模式下： public-key local export rsa { openssh ssh2 }	二者至少选择其一
按照指定格式显示本地 DSA 主机公钥	public-key local export dsa { openssh ssh2 }	

表1-5 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 { openssh ssh1 ssh2 } filename FIPS模式下： public-key local export rsa { openssh ssh2 } filename	二者至少选择其一
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 { openssh ssh2 } filename	

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 rsa }	必选

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：

- 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。
- 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。



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。
- 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](#)”。
- 设备上最多可以配置 20 个远端主机的公钥。

表1-7 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	-
指定远端主机公钥的名称，并进入公钥视图	public-key peer keyname	必选
进入公钥编辑视图	public-key-code begin	-
配置远端主机的公钥	逐个字符输入或拷贝粘贴公钥内容	必选 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

操作	命令	说明
退回公钥视图，并保存配置的主机公钥	public-key-code end	必选 退出公钥编辑视图时，系统自动保存配置的主机公钥
退回系统视图	peer-public-key end	-

表1-8 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	必选

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 rsa } public [[{ begin exclude include } regular-expression]
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] [[{ begin exclude include } regular-expression]

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

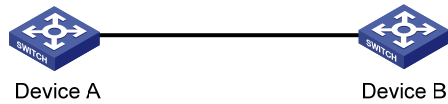
如 [图 1-2](#) 所示，为了防止非法用户访问，Device B 采用数字签名方法对访问它的 Device A 进行身份验证。进行身份验证前，需要在 Device B 上配置 Device A 的公钥。

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 RSA 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 size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
```

```
++++++
++++++
+++++++
+++++++
```

显示生成的 RSA 密钥对的公钥信息。

```
[DeviceA] display public-key local rsa public
```

```
=====
Time of Key pair created: 09:50:06 2012/03/07
Key name: HOST_KEY
Key type: RSA Encryption Key
=====
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100D90003FA95F5A44A2A2CD3F814F985
4C4421B57CAC64CFE4782A87B0360B600497D87162D1F398E6E5E51E5E353B3A9AB16C9E766BD995C669A78
4AD597D0FB3AA9F7202C507072B19C3C50A0D7AD3994E14ABC62DB125035EA326470034DC078B2BAA3BC3BCA
80AAB5EE01986BD1EF64B42F17CCAE4A77F1EF999B2BF9C4A10203010001
```

```
=====
Time of Key pair created: 09:50:07 2012/03/07
Key name: SERVER_KEY
Key type: RSA Encryption Key
=====
Key code:
307C300D06092A864886F70D0101010500036B003068026100999089E7AEE9802002D9EB2D0433B87BB6158E
35000AFB3FF310E42F109829D65BF70F7712507BE1A3E0BC5C2C03FAAF00DFDDC63D004B4490DACBA3CFA9E8
4B9151BDC7EECE1C8770D961557D192DE2B36CAF9974B7B293363BB372771C2C1F0203010001
```

(2) 配置 Device B

在 Device B 上配置 Device A 的主机公钥: 在公钥编辑视图输入 Device A 的主机公钥, 即在 Device A 上通过 **display public-key local dsa public** 命令显示的主机公钥 HOST_KEY 内容。

```
<DeviceB> system-view
[DeviceB] public-key peer devicea
Public key view: return to System View with "peer-public-key end".
[DeviceB-pkey-public-key] public-key-code begin
Public key code view: return to last view with "public-key-code end".
[DeviceB-pkey-key-code] 30819F300D06092A864886F70D010101050003818D0030818902818100D90003FA95F5A44A2A2CD3F814F9854C4421B57CAC64CFFE4782A87B0360B600497D87162D1F398E6E5E51E5E353B3A9AB16C9E766BD995C669A784AD597D0FB3AA9F7202C507072B19C3C50A0D7AD3994E14ABC62DB125035EA326470034DC078B2BAA3BC3BCA80AAB5EE01986BD1EF64B42F17CCAE4A77F1EF999B2BF9C4A10203010001
[DeviceB-pkey-key-code] public-key-code end
[DeviceB-pkey-public-key] peer-public-key end
# 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 Module: 1024
=====
Key Code:
30819F300D06092A864886F70D010101050003818D0030818902818100D90003FA95F5A44A2A2CD3F814F985
4C4421B57CAC64CFFE4782A87B0360B600497D87162D1F398E6E5E51E5E353B3A9AB16C9E766BD995C669A78
4AD597D0FB3AA9F7202C507072B19C3C50A0D7AD3994E14ABC62DB125035EA326470034DC078B2BAA3BC3BCA
80AAB5EE01986BD1EF64B42F17CCAE4A77F1EF999B2BF9C4A10203010001
```

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

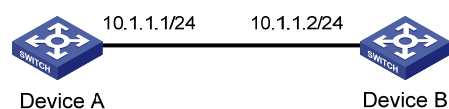
如 [图 1-3](#) 所示, 为了防止非法用户访问, Device B 采用数字签名方法对访问它的 Device A 进行身份验证。进行身份验证前, 需要在 Device B 上配置 Device A 的公钥。

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 RSA 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 size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
```

```
++++++
++++++
+++++++
+++++++
```

显示生成的 RSA 密钥对的公钥信息。

```
[DeviceA] display public-key local rsa public
```

```
=====
```

```
Time of Key pair created: 09:50:06 2012/03/07
```

```
Key name: HOST_KEY
```

```
Key type: RSA Encryption Key
```

```
=====
```

```
Key code:
```

```
30819F300D06092A864886F70D010101050003818D0030818902818100D90003FA95F5A44A2A2CD3F814F985
4C4421B57CAC64CFE4782A87B0360B600497D87162D1F398E6E5E51E5E353B3A9AB16C9E766BD995C669A78
4AD597D0FB3AA9F7202C507072B19C3C50A0D7AD3994E14ABC62DB125035EA326470034DC078B2BAA3BC3BCA
80AAB5EE01986BD1EF64B42F17CCAE4A77F1EF999B2BF9C4A10203010001
```

```
=====
```

```
Time of Key pair created: 09:50:07 2012/03/07
```

```
Key name: SERVER_KEY
```

```
Key type: RSA Encryption Key
```

```
=====
```

```
Key code:
```

```
307C300D06092A864886F70D0101010500036B0030680261009999089E7AEE9802002D9EB2D0433B87BB6158E
35000AFB3FF310E42F109829D65BF70F7712507BE1A3E0BC5C2C03FAAF00DFDDC63D004B4490DACBA3CFA9E8
4B9151BDC7EECE1C8770D961557D192DE2B36CAF9974B7B293363BB372771C2C1F0203010001
```

将生成的 RSA 主机公钥 HOST_KEY 导出到指定文件 devicea.pub 中。

```
[DeviceA] public-key local export rsa ssh2 devicea.pub
```

(2) 在 Device A 上启动 FTP 服务器功能

启动 FTP 服务器功能，并创建 FTP 用户，用户名为 ftp，密码为 123，用户级别为 3（以便 FTP 用户具有足够的权限执行 FTP 操作）。

```
[DeviceA] ftp server enable
```

```
[DeviceA] local-user ftp
```

```
[DeviceA-luser-ftp] password simple 123
```

```
[DeviceA-luser-ftp] service-type ftp
```

```
[DeviceA-luser-ftp] authorization-attribute level 3
[DeviceA-luser-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
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 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.
[ftp] binary
200 Type set to I.
[ftp] get devicea.pub
227 Entering Passive Mode (10,1,1,1,5,148).
125 BINARY mode data connection already open, transfer starting for /devicea.pub.
226 Transfer complete.
FTP: 299 byte(s) received in 0.189 second(s), 1.00Kbyte(s)/sec.
[ftp]quit
221 Server closing.
```

(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
# 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 Module: 1024
=====
```

Key Code:

```
30819F300D06092A864886F70D010101050003818D0030818902818100D90003FA95F5A44A2A2CD3F814F985
4C4421B57CAC64CFFE4782A87B0360B600497D87162D1F398E6E5E51E5E353B3A9AB16C9E766BD995C669A78
4AD597D0FB3AA9F7202C507072B19C3C50A0D7AD3994E14ABC62DB125035EA326470034DC078B2BAA3BC3BCA
80AAB5EE01986BD1EF64B42F17CCAE4A77F1EF999B2BF9C4A10203010001
```

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配置.....	1-1
1.1 PKI简介	1-1
1.1.1 概述	1-1
1.1.2 相关术语	1-1
1.1.3 体系结构	1-2
1.1.4 PKI的工作过程.....	1-3
1.1.5 主要应用	1-3
1.2 PKI配置任务简介.....	1-3
1.3 配置实体DN.....	1-4
1.4 配置PKI域.....	1-5
1.5 PKI证书申请	1-7
1.5.1 自动申请证书	1-7
1.5.2 手工申请证书	1-8
1.6 手工获取证书.....	1-9
1.7 配置PKI证书验证	1-10
1.7.1 配置使能CRL检查的证书验证.....	1-10
1.7.2 配置不使能CRL检查的PKI证书验证	1-11
1.8 销毁本地RSA密钥对	1-11
1.9 删除证书	1-12
1.10 配置证书属性的访问控制策略	1-12
1.11 PKI显示和维护	1-12
1.12 PKI典型配置举例.....	1-13
1.12.1 PKI实体向CA申请证书（采用RSA Keon CA服务器）	1-13
1.12.2 PKI实体向CA申请证书（采用Windows 2003 server CA服务器）	1-16
1.12.3 证书属性的访问控制策略应用举例	1-19
1.13 常见配置错误举例	1-21
1.13.1 获取CA证书失败	1-21
1.13.2 本地证书申请失败.....	1-21
1.13.3 CRL获取失败	1-22

1 PKI配置

1.1 PKI简介

1.1.1 概述

PKI (Public Key Infrastructure, 公钥基础设施) 是一个利用公共密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。

公共密钥体制也称为非对称密钥体制, 是目前应用最广泛的一种加密体制, 在这一体制中, 它使用一个非对称的密钥对, 分别是一个公开的加密密钥 (公钥) 和一个保密的解密密钥 (私钥), 用公钥加密的信息只能用私钥解密, 反之亦然。由于公钥是公开的, 需要在网上传送, 故公钥的管理问题就是公共密钥体制所需要解决的关键问题。

目前, PKI 系统中引出的数字证书机制就是一个很好的解决方案。基于公共密钥技术的数字证书是一个用户的身份和他所持有的公钥的结合, 它是使用 PKI 系统的用户建立安全通信的信任基础。

基于数字证书的 PKI 系统, 能够为网络通信和网络交易, 特别是电子政务和电子商务业务, 透明地提供一整套安全服务, 主要包括身份认证、保密、数据完整性和不可否认性。

目前, 我司的 PKI 可为安全协议 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

数字证书是一个经 CA (Certificate Authority, 证书颁发机构) 签名的、包含公开密钥及相关的用户身份信息文件, 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的合法性和权威性。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。一个数字证书中包含多个字段, 包括证书签发者的名称、主体的公钥信息、CA 对证书的数字签名、证书的有效期等。

本手册中涉及两类证书: 本地 (local) 证书和 CA (Certificate Authority) 证书。本地证书是 CA 签发给用户的数字证书; CA 证书是 CA 自身的证书。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, 它拥有一个 CA “自签名” 的证书。

2. 证书废除列表 (CRL, Certificate Revocation List)

由于用户姓名的改变、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撤销, 即撤销公开密钥及相关的用户身份信息的绑定关系。在 PKI 中, 所使用的这种方法为证书废除列表。任何一个证书被废除以后, CA 就要发布 CRL 来声明该证书是无效的, 并列出所有被废除的证书的序列号。CRL 提供了一种检验证书有效性的方式。

当一个 CRL 的撤销信息过多时会导致 CRL 的发布规模变得非常庞大, 且随着 CRL 大小的增加, 网络资源的使用性能也会随之下降。为了避免这种情况, 允许一个 CA 的撤销信息通过多个 CRL 发布出来, 并且使用 CRL 发布点来指出这些小 CRL 的位置。

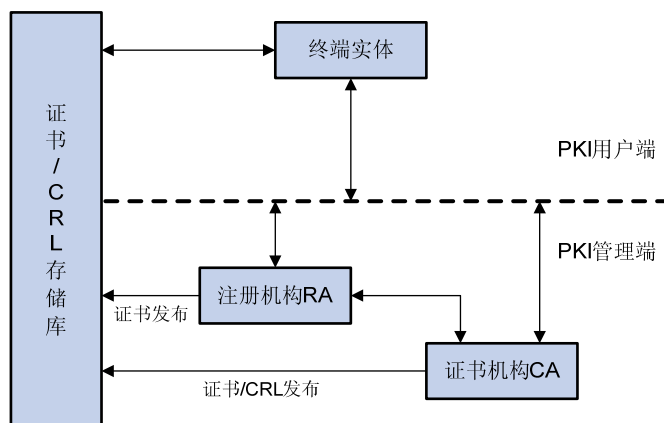
3. CA策略

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被称为 CA 策略。通常，CA 以一种叫做证书惯例声明（CPS，Certification Practice Statement）的文档发布其策略，CA 策略可以通过带外（如电话、磁盘、电子邮件等）或其他方式获取。由于不同的 CA 使用不同的方法验证公开密钥与实体之间的绑定，所以在选择信任的 CA 进行证书申请之前，必须理解 CA 策略，从而指导对实体进行相应的配置。

1.1.3 体系结构

一个PKI体系由终端实体、证书机构、注册机构和PKI存储库四类实体共同组成，如下 [图 1-1](#)。

图1-1 PKI 体系结构图



1. 终端实体

终端实体是 PKI 产品或服务的最终使用者，可以是个人、组织、设备或计算机中运行的进程。

2. 证书颁发机构（CA，Certificate Authority）

CA 是 PKI 的信任基础，是一个用于签发并管理数字证书的可信实体。其作用包括：发放证书、规定证书的有效期和通过发布 CRL 确保必要时可以废除证书。

3. 证书注册机构（RA，Registration Authority）

RA 是 CA 的延伸，可作为 CA 的一部分，也可以独立。RA 功能包括个人身份审核、CRL 管理、密钥对产生和密钥对备份等。PKI 国际标准推荐由一个独立的 RA 来完成注册管理的任务，这样可以增强应用系统的安全性。

4. PKI存储库

PKI 存储库包括 LDAP（Lightweight Directory Access Protocol，轻量级目录访问协议）服务器和普通数据库，用于对用户申请、证书、密钥、CRL 和日志等信息进行存储和管理，并提供一定的查询功能。

LDAP 提供了一种访问 PKI 存储库的方式，通过该协议来访问并管理 PKI 信息。LDAP 服务器负责将 RA 服务器传输过来的用户信息以及数字证书进行存储，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。

1.1.4 PKI的工作过程

针对一个使用 PKI 的网络，配置 PKI 的目的就是为指定的实体向 CA 申请一个本地证书，并由设备对证书的有效性进行验证。下面是 PKI 的工作过程：

- (1) 实体向 RA 提出证书申请；
- (2) RA 审核实体身份，将实体身份信息和公开密钥以数字签名的方式发送给 CA；
- (3) CA 验证数字签名，同意实体的申请，颁发证书；
- (4) RA 接收 CA 返回的证书，发送到 LDAP 服务器（或其它形式的发布点）以提供目录浏览服务，并通知实体证书发行成功；
- (5) 实体获取证书，利用该证书可以与其它实体使用加密、数字签名进行安全通信；
- (6) 实体希望撤消自己的证书时，向 CA 提交申请。CA 批准实体撤消证书，并更新 CRL，发布到 LDAP 服务器（或其它形式的发布点）。

1.1.5 主要应用

PKI 技术的广泛应用能满足人们对网络交易安全保障的需求。作为一种基础设施，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. 虚拟专用网络（VPN，Virtual Private Network）

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，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机密性保护。

2. 安全电子邮件

电子邮件的安全也要求机密、完整、认证和不可否认，而这些都可以利用 PKI 技术来实现。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，在两个实体进行通信之前，先要建立 SSL(Secure Sockets Layer，安全套接字层)连接，以此实现对应用层透明的安全通信。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 技术使用基于数字签名的方法对服务器和浏览器端进行身份验证。

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
配置实体DN		必选	1.3
配置PKI域		必选	1.4
PKI证书申请	自动申请证书	二者必选其一	1.5.1
	手工申请证书		1.5.2
手工获取证书		可选	1.6

配置任务	说明	详细配置
配置PKI证书验证	可选	1.7
销毁本地RSA密钥对	可选	1.8
删除证书	可选	1.9
配置证书属性的访问控制策略	可选	1.10

1.3 配置实体DN

一份证书是一个公开密钥与一个身份的绑定，而身份必须与一个特定的 PKI 实体相关联。实体 DN（Distinguished Name，识别名）的参数是实体的身份信息，CA 根据实体提供的身份信息来唯一标识证书申请者。

实体 DN 的参数包括：

- 实体通用名
- 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 FQDN（Fully Qualified Domain Name，完全合格域名），是实体在网络中的唯一标识，由一个主机名和域名组成，可被解析为 IP 地址。例如，www 是一个主机名，whatever.com 是一个域名，则 www.whatever.com 就是一个 FQDN。
- 实体 IP 地址
- 实体所在地理区域名称
- 实体所属组织名称
- 实体所属部门名称
- 实体所属州省



说明

实体 DN 的配置必须与 CA 证书颁发策略相匹配，以确认实体 DN 的配置任务，如哪些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。

表1-2 配置实体 DN

操作	命令	说明
进入系统视图	system-view	-
创建一个实体，并进入该实体视图	pki entity <i>entity-name</i>	必选 缺省情况下，无实体存在
配置实体通用名	common-name <i>name</i>	可选 缺省情况下，未配置实体的通用名

操作	命令	说明
配置实体所属国家代码	country <i>country-code-str</i>	可选 缺省情况下，未配置实体所属国家代码
配置实体FQDN	fqdn <i>name-str</i>	可选 缺省情况下，未配置实体FQDN
配置实体IP地址	ip <i>ip-address</i>	可选 缺省情况下，未配置实体IP地址
配置实体所在地理区域名称	locality <i>locality-name</i>	可选 缺省情况下，未配置实体所在地理区域
配置实体所属组织名称	organization <i>org-name</i>	可选 缺省情况下，未配置实体所属组织
配置实体所属部门名称	organization-unit <i>org-unit-name</i>	可选 缺省情况下，未配置实体所属部门
配置实体所属州省	state <i>state-name</i>	可选 缺省情况下，未配置实体所属州省



说明

Windows 2000 CA 服务器对证书申请的数据长度有一定的限制。实体 DN 配置项超过一定数据长度时，申请证书没有回应。

1.4 配置PKI域

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实体的 PKI 域。

PKI 域是一个本地概念，因此创建 PKI 域的目的是便于其它应用引用 PKI 的配置，比如 SSL 等。一个设备上配置的 PKI 域对 CA 和其它设备是不可见的，每一个 PKI 域有单独的域参数配置信息。

PKI 域中包括以下参数：

- 信任的 CA 名称

在申请证书时，是通过一个可信实体认证机构，来完成实体证书的注册颁发，因此必须指定一个信任的 CA 名称。

- 实体名称

向 CA 发送证书申请请求时，必须指定所使用的实体名，以向 CA 表明自己的身份。

- 证书申请的注册机构

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。注册机构并不给用户签发证书，而只是对用户进行资格审查。有时 PKI 把注册管理的职能交给 CA 来完成，而不设立独立运行的 RA，但这并

不是取消了 PKI 的注册功能，而只是将其作为 CA 的一项功能而已。PKI 推荐独立使用 RA 作为注册审理机构。

- 注册服务器的 URL

证书申请之前必须指定注册服务器的 URL，随后实体可通过简单证书注册协议（SCEP，Simple Certification Enrollment Protocol）向该服务器提出证书申请，SCEP 是专门用于与认证机构进行通信的协议。

- 证书申请状态查询的周期和次数

实体在发送证书申请后，如果 CA 采用手工验证申请，证书的发布会需要很长时间。在此期间，客户端需要定期发送状态查询，以便在证书签发后能及时获取到证书。客户端可以配置证书申请状态的查询周期和次数。

- LDAP 服务器 IP 地址

在 PKI 系统中，用户的证书和 CRL 信息的存储是一个非常核心的问题。一般采用 LDAP 服务器来存储证书和 CRL，这时就需要指定 LDAP 服务器的位置。

- 验证根证书时使用的指纹

当设备从 CA 获得根证书时，需要验证 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。如果 CA 根证书的指纹与在 PKI 域中配置的指纹不同，则设备将拒绝接收根证书。

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 <i>domain-name</i>	必选
配置信任的CA名称	ca identifier <i>name</i>	必选 缺省情况下，未配置信任的CA名称
指定实体名称	certificate request entity <i>entity-name</i>	必选 缺省情况下，未指定实体名称 指定的实体名称必须已创建
配置证书申请的注册受理机构	certificate request from { <i>ca</i> <i>ra</i> }	必选 缺省情况下，未指定证书申请的注册受理机构
配置注册服务器URL	certificate request url <i>url-string</i>	必选 缺省情况下，未指定注册服务器URL
配置证书申请状态查询的周期和次数	certificate request polling { <i>count count</i> <i>interval minutes</i> }	可选 缺省情况下，证书申请状态查询周期为20分钟，每一个周期内查询50次
配置LDAP服务器	ldap-server ip <i>ip-address</i> [port <i>port-number</i>] [version <i>version-number</i>]	可选 缺省情况下，未指定LDAP服务器

配置任务	命令	说明
配置验证根证书时使用的指纹	root-certificate fingerprint { md5 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



说明

- 目前一台设备只支持同时创建两个 PKI 域。
- 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。
- 目前，注册服务器 URL 的配置不支持域名解析。

1.5 PKI证书申请

证书申请就是实体向 CA 自我介绍的过程。实体向 CA 提供身份信息，以及相应的公开密钥，这些信息将成为颁发给该实体证书的主要组成部分。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。

在线证书申请有手工发起和自动发起两种方式。

1.5.1 自动申请证书

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，如果应用协议中的实体无本地证书，则实体自动通过 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。

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 [key-length key-length password { cipher simple } password] *	必选 缺省情况下，证书申请为手工方式



说明

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业务的中断。

1.5.2 手工申请证书

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工作。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 证书和密钥对。

- 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。若 PKI 域中没有 CA 证书,则需要手工获取 CA 证书。
- 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,公钥和其他信息则交由 CA 中心进行签名,从而产生证书。若 PKI 域中不存在密钥对,则需要生成本地密钥对。有关 RSA 密钥对的具体配置请参见“安全配置指导”中的“公钥管理”。

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	可选 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 1.6	必选
生成本地RSA密钥对	public-key local create rsa	必选 缺省情况下,本地没有RSA密钥对
手工申请本地证书	pki request-certificate domain domain-name [password] [pkcs10 [filename filename]]	必选



说明

- 若本地证书已存在，为保证密钥对与现存证书的一致性，不应执行创建密钥对命令，必须在删除本地证书后再执行 **public-key local create** 命令生成新的密钥对。有关 **public-key local create** 命令的详细介绍，请参见“安全命令参考”中的“公钥管理”。
- 创建的新密钥对将覆盖旧密钥对。若本地已有 RSA 密钥对，执行 **public-key local create** 命令时，系统会提示是否替换原有密钥对。
- 如果本地证书已存在，则不允许再执行证书申请操作，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** 命令删除存储于本地的 CA 证书与本地证书，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，可以首先通过执行指定参数 **pkcs10** 的命令 **pki request-certificate domain** 打印出本地的证书申请信息，或者通过执行指定 **pkcs10 filename filename** 参数的该命令将证书申请信息直接保存到本地的指定文件中，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。
- 证书申请之前必须保证实体时钟与 CA 的时钟同步，否则申请证书的有效期会出现异常。
- **pki request-certificate domain** 配置不能被保存在配置文件中。

1.6 手工获取证书

用户通过此配置可以将已存在的 CA 证书、本地证书获取至本地。获取证书有两种方式：离线方式和在线方式。离线方式下获取证书需要通过带外方式（如 FTP、磁盘、电子邮件等）取得证书，然后将其导入至本地。

获取证书的目的有两个：

- 将 CA 签发的与实体所在安全域有关的证书存放到本地，以提高证书的查询效率，减少向 PKI 证书存储库查询的次数。
- 为证书的验证做好准备。

在线获取本地证书之前必须完成 LDAP 服务器的配置。

表1-6 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	在线方式	pki retrieval-certificate { ca local } domain domain-name	二者必选其一
	离线方式导入证书	pki import-certificate { ca local } domain domain-name { der p12 pem } [filename filename]	



注意

- 如果本地已有 CA 证书存在，则不允许执行手工获取 CA 证书的操作，避免因相关配置的修改使得证书与注册信息不匹配。若想重新获取，请先使用 **pki delete-certificate** 命令删除 CA 证书与本地证书后，再执行此命令。
- pki retrieval-certificate** 配置不能被保存在配置文件中。
- 为保证设备上已申请的证书可用，请确保设备当前系统时间处于证书的有效期限范围之内。

1.7 配置PKI证书验证

在使用每一个证书之前，必须对证书进行验证。证书验证包括对签发时间、签发者信息以及证书的有效性几方面进行验证。证书验证的核心是检查 CA 在证书上的签名，并确定证书仍在有效期内，而且未被废除，因此在进行证书验证操作之前必须首先获取 CA 证书。

配置证书验证时可以设置是否必须进行 CRL 检查。

- 如果配置为使能 CRL 检查，则检验证书的有效性，必须通过 CRL 判断。因此，在进行证书有效性验证之前，除了获取 CA 证书还必须获取 CRL 并下载至本地；
- 如果配置为不使能 CRL 检查，则仅需要获取 CA 证书来判断证书的有效性。

1.7.1 配置使能CRL检查的证书验证

表1-7 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 <i>domain-name</i>	-
配置CRL发布点的URL	crl url <i>url-string</i>	可选 缺省情况下，未指定CRL发布点的URL
配置CRL的更新周期	crl update-period <i>hours</i>	可选 缺省情况下，根据CRL文件中的下次更新域进行更新
使能CRL检查	crl check enable	可选 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 1.6	必选
获取CRL并下载至本地	pki retrieval-crl <i>domain</i> <i>domain-name</i>	必选
检验证书的有效性	pki validate-certificate { <i>ca</i> <i>local</i> } <i>domain</i> <i>domain-name</i>	必选



说明

- CRL 的更新周期是指本地从 CRL 存储服务器下载 CRL 的时间间隔。手工配置的 CRL 更新周期将优先于 CRL 文件中指定的更新时间。
- **pki retrieval-crl domain** 命令不能被保存在配置文件中。

1.7.2 配置不使能CRL检查的PKI证书验证

表1-8 配置不使能 CRL 检查的 PKI 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	crl check disable	必选 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 1.6	必选
检验证书的有效性	pki validate-certificate { ca local } domain domain-name	必选

1.8 销毁本地RSA密钥对

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 中心来确定。当用户的私钥被泄漏或证书的有效快到时，用户应该删除旧的密钥对，产生新的密钥对，重新申请新的证书。通过此配置用户可以销毁本地 RSA 密钥对。

表1-9 销毁本地 RSA 密钥对

操作	命令	说明
进入系统视图	system-view	-
销毁本地RSA密钥对	public-key local destroy rsa	必选



说明

命令 **public-key local destroy** 的详细介绍可参考“安全命令参考”中的“公钥管理”。

1.9 删除证书

证书过期或希望重新申请证书，可以通过此配置删除一个已经存在的本地证书或 CA 证书。

表1-10 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 { ca local } domain <i>domain-name</i>	必选

1.10 配置证书属性的访问控制策略

通过配置证书属性的访问控制策略，可以对用户的访问权限进行进一步的控制，保证了与之通信的服务器的安全性。

表1-11 配置证书属性的访问控制策略

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 <i>group-name</i>	必选 缺省情况下，不存在证书属性组
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 } <i>attribute-value</i>	可选 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	-
创建证书属性访问控制策略，并进入证书属性访问控制策略视图	pki certificate access-control-policy <i>policy-name</i>	必选 缺省情况下，不存在证书属性访问控制策略
配置证书属性控制规则	rule [id] { deny permit } group-name	必选 缺省情况下，不存在证书属性控制规则 <i>group-name</i> 必须是已存在的证书属性组的名称

1.11 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1-12 PKI 显示和维护

操作	命令
显示证书内容或证书申请状态	display pki certificate { { ca local } domain <i>domain-name</i> request-status } [{ begin exclude include } <i>regular-expression</i>]
显示CRL内容	display pki crl domain <i>domain-name</i> [{ begin exclude include } <i>regular-expression</i>]
显示证书属性组的信息	display pki certificate attribute-group { <i>group-name</i> all } [{ begin exclude include } <i>regular-expression</i>]
显示证书属性访问控制策略的信息	display pki certificate access-control-policy { <i>policy-name</i> all } [{ begin exclude include } <i>regular-expression</i>]

1.12 PKI典型配置举例



注意

- 当采用 Windows Server 作为 CA 时，需要安装 SCEP 插件。此时，配置 PKI domain 时，需要使用 **certificate request from ra** 命令指定实体从 RA 注册申请证书。
- 当采用 RSA Keon 软件时，不需要安装 SCEP 插件。此时，配置 PKI domain 时，需要使用 **certificate request from ca** 命令指定实体从 CA 注册申请证书。
- 如下典型配置举例中的配置，均以设备运行在非 FIPS 模式下的命令行为准。

1.12.1 PKI实体向CA申请证书（采用RSA Keon CA服务器）

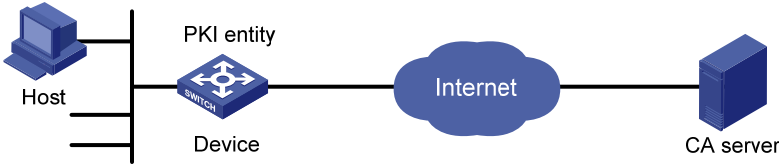
1. 组网需求

在作为 PKI 实体的设备 Device 上进行相关配置，实现以下需求：

- 设备向 CA 服务器申请本地证书
- 获取 CRL 为证书验证做准备

2. 组网图

图1-2 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，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。

- 配置 CRL 发布

CA 服务器的基本配置完成之后，需要进行 CRL 的相关配置。

本例中选择 CRL 的发布方式为 HTTP，自动生成 CRL 发布点的 URL 为 <http://4.4.4.133:447/myca.crl>。

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

- 配置实体命名空间

配置实体名称为 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 域参数

创建并进入 PKI 域 torsa。

```
[Device] pki domain torsa
```

配置可信任的 CA 名称为 myca。

```
[Device-pki-domain-torsa] ca identifier myca
```

配置注册服务器 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://4.4.4.133:446/c95e970f632d27be5e8cbf80e971d9c4a9a93337
```

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 http://4.4.4.133:447/myca.crl
[Device-pki-domain-torsa] quit
```

- 用 RSA 算法生成本地密钥对

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

The range of public key size is (512 ~ 2048).

NOTES: If the key modulus is greater than 512,

It will take a few minutes.

Press CTRL+C to abort.

Input the bits in the modulus [default = 1024]:

Generating Keys...

```
+++++
+++++
+++++
+++++
```

- 证书申请

获取 CA 证书并下载至本地。

```
[Device] pki retrieval-certificate ca domain torsa
```

Retrieving CA/RA certificates. Please wait a while.....

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

Saving CA/RA certificates chain, please wait a moment.....

CA certificates retrieval success.

获取 CRL 并下载至本地。

```
[Device] pki retrieval-crl domain torsa
```

Connecting to server for retrieving CRL. Please wait a while.....

CRL retrieval success!

手工申请本地证书。

```
[Device] pki request-certificate domain torsa challenge-word
```

Certificate is being requested, please wait.....

```
[Device]
```

Enrolling the local certificate, please wait a while.....

Certificate request Successfully!

Saving the local certificate to device.....

Done!

4. 验证配置结果

通过以下显示命令可以查看获取的本地证书信息。

```
[Device] display pki certificate local domain torsa
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

9A96A48F 9A509FD7 05FFF4DF 104AD094

Signature Algorithm: sha1WithRSAEncryption

Issuer:

C=cn

O=org

OU=test

CN=myca

Validity

Not Before: Jan 8 09:26:53 2012 GMT

Not After : Jan 8 09:26:53 2012 GMT

Subject:

CN=device


```

Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (1024 bit)
    Modulus (1024 bit):
      00D67D50 41046F6A 43610335 CA6C4B11
      F8F89138 E4E905BD 43953BA2 623A54C0
      EA3CB6E0 B04649CE C9CDDD38 34015970
      981E96D9 FF4F7B73 A5155649 E583AC61
      D3A5C849 CBDE350D 2A1926B7 0AE5EF5E
      D1D8B08A DBF16205 7C2A4011 05F11094
      73EB0549 A65D9E74 0F2953F2 D4F0042F
      19103439 3D4F9359 88FB59F3 8D4B2F6C
      2B
    Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 CRL Distribution Points:
      URI:http://4.4.4.133:447/myca.crl

```

```

Signature Algorithm: sha1WithRSAEncryption
  836213A4 F2F74C1A 50F4100D B764D6CE
  B30C0133 C4363F2F 73454D51 E9F95962
  EDE9E590 E7458FA6 765A0D3F C4047BC2
  9C391FF0 7383C4DF 9A0CCFA9 231428AF
  987B029C C857AD96 E4C92441 9382E798
  8FCC1E4A 3E598D81 96476875 E2F86C33
  75B51661 B6556C5E 8F546E97 5197734B
  C8C29AC7 E427C8E4 B9AAF5AA 80A75B3C

```

关于获取的 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 ca domain** 和 **display pki crl domain**。

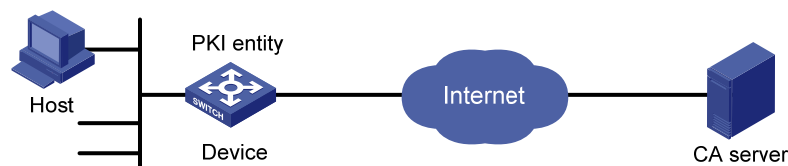
1.12.2 PKI实体向CA申请证书（采用Windows 2003 server CA服务器）

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1-3 PKI 实体向 CA 申请证书组网图



3. 配置步骤

(1) 配置 CA 服务器

- 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 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。

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

- 配置实体命名空间

配置实体名称为 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 域参数

创建并进入 PKI 域 torsa。

```
[Device] pki domain torsa
```

配置可信任的 CA 名称为 myca。

```
[Device-pki-domain-torsa] ca identifier myca
```

配置注册服务器 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-torsa] 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-torsa] certificate request from ra
```

指定实体名称为 aaa。

```
[Device-pki-domain-torsa] certificate request entity aaa
```

- 用 RSA 算法生成本地密钥对

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

The range of public key size is (512 ~ 2048).

NOTES: If the key modulus is greater than 512,

It will take a few minutes.

Press CTRL+C to abort.

Input the bits in the modulus [default = 1024]:

Generating Keys...

+++++

```
+++++
+++++
+++++
```

- 证书申请

获取 CA 证书并下载至本地。

```
[Device] pki retrieval-certificate ca domain torsa
Retrieving CA/RA certificates. Please wait a while.....
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

```
Saving CA/RA certificates chain, please wait a moment.....
CA certificates retrieval success.
```

手工申请本地证书。

```
[Device] pki request-certificate domain torsa challenge-word
Certificate is being requested, please wait.....
[Device]
Enrolling the local certificate,please wait a while.....
Certificate request Successfully!
Saving the local certificate to device.....
Done!
```

4. 验证配置结果

通过以下显示命令可以查看获取的本地证书信息。

```
[Device] display pki certificate local domain torsa
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            48FA0FD9 00000000 000C
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:
            CN=myca
        Validity
            Not Before: Feb 21 12:32:16 2012 GMT
            Not After : Feb 21 12:42:16 2012 GMT
        Subject:
            CN=device
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
            Modulus (1024 bit):
                00A6637A 8CDEA1AC B2E04A59 F7F6A9FE
                5AEE52AE 14A392E4 E0E5D458 0D341113
                0BF91E57 FA8C67AC 6CE8FEBB 5570178B
                10242FDD D3947F5E 2DA70BD9 1FAF07E5
```

```

1D167CE1 FC20394F 476F5C08 C5067DF9
CB4D05E6 55DC11B6 9F4C014D EA600306
81D403CF 2D93BC5A 8AF3224D 1125E439
78ECEFE1 7FA9AE7B 877B50B8 3280509F
6B
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
B68E4107 91D7C44C 7ABCE3BA 9BF385F8 A448F4E1
X509v3 Authority Key Identifier:
keyid:9D823258 EADFEFA2 4A663E75 F416B6F6 D41EE4FE

X509v3 CRL Distribution Points:
URI:http://l00192b/CertEnroll/CA%20server.crl
URI:file://\\l00192b\CertEnroll\CA server.crl

Authority Information Access:
CA Issuers - URI:http://l00192b/CertEnroll/l00192b_CA%20server.crt
CA Issuers - URI:file://\\l00192b\CertEnroll\l00192b_CA server.crt

1.3.6.1.4.1.311.20.2:
.O.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
81029589 7BFA1CBD 20023136 B068840B
..... (略)

```

关于获取的 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 ca domain**。

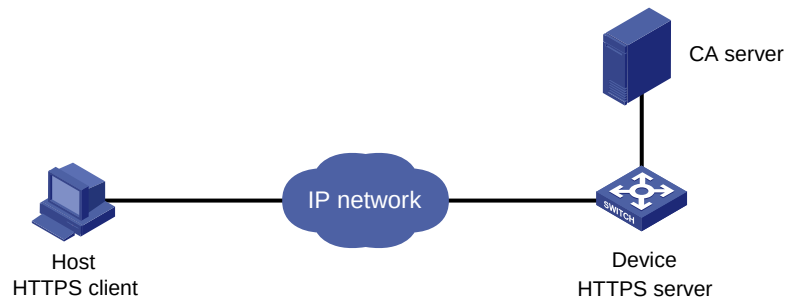
1.12.3 证书属性的访问控制策略应用举例

1. 组网需求

- 客户端通过 HTTPS（Hypertext Transfer Protocol Secure，超文本传输协议的安全版本）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。
- 为 HTTPS 服务器制定证书属性的访问控制策略，对客户端的访问权限进行控制。

2. 组网图

图1-4 证书属性的访问控制策略应用组网图



3. 配置步骤



说明

- SSL 配置的相关内容请参见“安全配置指导”中的“SSL”。
- HTTPS 配置的相关内容请参见“基础配置指导”中的“配置通过 Web 网管登录设备”。
- SSL策略所引用的PKI域必须首先创建，PKI域参数的具体配置请参见 [1.12.1](#) 中的“配置PKI域参数”。

(1) 配置 HTTPS 服务器

配置 HTTPS 服务器使用的 SSL 策略。

```
<Device> system-view
[Device] ssl server-policy myssl
[Device-ssl-server-policy-mysl] pki-domain 1
[Device-ssl-server-policy-mysl] client-verify enable
[Device-ssl-server-policy-mysl] 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

配置访问控制策略 **myacp**，并建立两个控制规则。

```
[Device] pki certificate access-control-policy myacp
[Device-pki-cert-acp-myacp] rule 1 deny mygroup1
[Device-pki-cert-acp-myacp] rule 2 permit mygroup2
[Device-pki-cert-acp-myacp] quit
(4) 配置 HTTPS 服务器与相关策略进行关联，并启动 HTTPS 服务器
# 配置指定 HTTPS 服务器的 SSL 策略为 myssl。
[Device] ip https ssl-server-policy myssl
# 配置指定 HTTPS 服务器的证书访问控制策略为 myacp。
[Device] ip https certificate access-control-policy myacp
# 启动 HTTPS 服务器。
[Device] ip https enable
```

1.13 常见配置错误举例

1.13.1 获取CA证书失败

1. 故障现象

获取 CA 证书时失败。

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；
- 设备的系统时钟与 CA 的时钟不同步。

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；
- 配置证书申请注册受理机构；
- 保持系统时钟与 CA 同步。

1.13.2 本地证书申请失败

1. 故障现象

手工证书请求失败。

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；
- 申请之前没有先获取 CA 证书；
- 当前的密钥对已经绑定证书；

- 没有设置信任的 CA 名称；
- 证书申请的注册服务器 URL 位置不正确或未配置；
- 没有配置证书申请注册受理机构；
- 没有配置实体 DN 中必配参数。

3. 处理过程

- 排除物理连接故障；
- 获取 CA 证书；
- 重新创建密钥对；
- 配置信任的 CA 名称；
- 可通过 **ping** 命令测试注册服务器是否连接正常；
- 配置证书申请注册受理机构；
- 可通过查看 CA/RA 注册策略选择相关的实体 DN 属性进行配置。

1.13.3 CRL获取失败

1. 故障现象

获取 CRL 发生失败。

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 LDAP 服务器的 IP 地址；
- 未设置 CRL 发布点位置；
- LDAP 服务器版本配置错误。
- CRL 发布点的域名解析失败

3. 处理过程

- 排除物理连接故障；
- 获取 CA 证书；
- 设置 LDAP 服务器的 IP 地址；
- 设置 CRL 发布点位置；
- 重新配置 LDAP 版本。
- 确保能够正常访问 DNS 服务器，并且保证 DNS 服务器能够解析配置的 CRL 发布点域名。

目 录

1 IPsec.....	1-1
1.1 IPsec简介	1-1
1.1.1 IPsec基本概念	1-2
1.1.2 使用IPsec保护IPv6 路由协议	1-4
1.1.3 协议规范	1-4
1.2 建立IPsec隧道的配置方式	1-4
1.3 基于ACL建立IPsec安全隧道	1-5
1.3.1 IPsec隧道限制说明	1-5
1.3.2 IPsec配置任务简介	1-5
1.3.3 配置访问控制列表	1-6
1.3.4 配置安全提议	1-7
1.3.5 配置安全策略	1-8
1.3.6 在接口上应用安全策略组	1-12
1.3.7 配置会话空闲超时时间	1-13
1.3.8 使能解封装后IPsec报文的ACL检查功能	1-13
1.3.9 配置IPsec抗重放功能	1-14
1.3.10 配置报文信息预提取功能	1-15
1.4 配置IPsec保护IPv6 路由协议	1-15
1.5 IPsec显示和维护	1-16
1.6 IPsec典型配置举例	1-17
1.6.1 采用IKE方式建立保护IPv4 报文的IPsec安全隧道	1-17
1.6.2 配置IPsec保护RIPng报文	1-19
2 IKE.....	2-1
2.1 IKE简介	2-1
2.1.1 IKE的安全机制	2-1
2.1.2 IKE的交换过程	2-1
2.1.3 IKE在IPsec中的作用	2-2
2.1.4 IPsec与IKE的关系	2-3
2.1.5 协议规范	2-3
2.2 IKE配置任务简介	2-3
2.3 配置本端安全网关的名字	2-4
2.4 配置IKE安全提议	2-4

2.5 配置IKE对等体	2-5
2.6 配置Keepalive定时器	2-7
2.7 配置NAT Keepalive定时器	2-8
2.8 配置对等体存活检测	2-8
2.9 配置取消对next payload域的检查	2-9
2.10 IKE显示和维护	2-9
2.11 IKE典型配置举例	2-10
2.12 常见错误配置举例	2-13
2.12.1 非法用户身份信息	2-13
2.12.2 提议不匹配	2-13
2.12.3 无法建立安全隧道	2-13
2.12.4 ACL配置错误	2-14

1 IPsec



说明

- 本节所涉及的路由器和路由器图标，代表了一般意义下的路由器或运行了路由协议的交换机。
- 处于 IRF 状态的交换机不支持 IPsec 自动协商方式。
- 设备仅在 FIPS 模式下，支持 IKE 相关配置。关于 FIPS 模式的介绍，请参见“安全配置指导”中的“FIPS”。

1.1 IPsec简介

IPsec (IP Security) 是 IETF 制定的三层隧道加密协议，它为 Internet 上传输的数据提供了高质量的、可互操作的、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。特定的通信方之间通过建立 IPsec 隧道来传输用户的私有数据，并在 IP 层提供了以下安全服务：

- 数据机密性 (Confidentiality)：IPsec 发送方在通过网络传输包前对包进行加密。
- 数据完整性 (Data Integrity)：IPsec 接收方对发送方发送来的包进行认证，以确保数据在传输过程中没有被篡改。
- 数据来源认证 (Data Authentication)：IPsec 在接收端可以认证发送 IPsec 报文的发送端是否合法。
- 防重放 (Anti-Replay)：IPsec 接收方可检测并拒绝接收过时或重复的报文。

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) 的服务，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。

IPsec 协议不是一个单独的协议，它给出了应用于 IP 层上网络数据安全的一整套体系结构，包括网络认证协议 AH (Authentication Header, 认证头)、ESP (Encapsulating Security Payload, 封装安全载荷)、IKE (Internet Key Exchange, 互联网密钥交换) 和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。

IPsec 提供了两种安全机制：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。

设备可支持 IPsec 对 IPv4 报文和 IPv6 报文的保护。

1.1.1 IPsec基本概念

1. 安全协议

AH 协议和 ESP 协议的功能及工作原理如下：

- AH 协议（IP 协议号为 51）定义了认证的应用方法，提供数据源认证、数据完整性校验和防报文重放功能，它能保护通信免受篡改，但不能防止窃听，适合用于传输非机密数据。AH 的工作原理是在每一个数据包上添加一个身份验证报文头，此报文头插在标准 IP 包头后面，对数据提供完整性保护。可选的认证算法有 MD5（Message Digest）、SHA-1（Secure Hash Algorithm）等。
- ESP 协议（IP 协议号为 50）定义了加密和可选认证的应用方法，提供加密、数据源认证、数据完整性校验和防报文重放功能。ESP 的工作原理是在每一个数据包的标准 IP 包头后面添加一个 ESP 报文头，并在数据包后面追加一个 ESP 尾。与 AH 协议不同的是，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。常见的加密算法有 DES、3DES、AES 等。同时，作为可选项，用户可以选择 MD5、SHA-1 算法保证报文的完整性和真实性。

在实际进行 IP 通信时，可以根据实际安全需求同时使用这两种协议或选择使用其中的一种。AH 和 ESP 都可以提供认证服务，不过，AH 提供的认证服务要强于 ESP。同时使用 AH 和 ESP 时，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，封装之后的报文从内到外依次是原始 IP 报文、ESP 头、AH 头和外部 IP 头。

2. 安全联盟（Security Association, SA）

IPsec 在两个端点之间提供安全通信，端点被称为 IPsec 对等体。

SA 是 IPsec 的基础，也是 IPsec 的本质。SA 是通信对等体间对某些要素的约定，例如，使用哪种协议（AH、ESP 还是两者结合使用）、协议的封装模式（传输模式和隧道模式）、加密算法（DES、3DES 和 AES）、特定流中保护数据的共享密钥以及密钥的生存周期等。建立 SA 的方式有手工配置和 IKE 自动协商两种。

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 由一个三元组来标识，这个三元组包括 SPI（Security Parameter Index，安全参数索引）、目的 IP 地址、安全协议号（AH 或 ESP）。

SPI 是用于唯一标识 SA 的一个 32 比特数值，它在 AH 和 ESP 头中传输。在手工配置 SA 时，需要手工指定 SPI 的取值。使用 IKE 协商产生 SA 时，SPI 将随机生成。

通过 IKE 协商建立的 SA 具有生存周期，手工方式建立的 SA 永不老化。IKE 协商建立的 SA 的生存周期有两种定义方式：

- 基于时间的生存周期，定义了一个 SA 从建立到失效的时间；
- 基于流量的生存周期，定义了一个 SA 允许处理的最大流量。

生存周期到达指定的时间或指定的流量，SA 就会失效。SA 失效前，IKE 将为 IPsec 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，继续使用旧的 SA 保护通信。在新的 SA 协商好之后，则立即采用新的 SA 保护通信。

3. 封装模式

IPsec 有如下两种工作模式：

- 隧道(tunnel)模式：用户的整个 IP 数据包被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被封装在一个新的 IP 数据包中。通常，隧道模式应用在两个安全网关之间的通讯。
- 传输(transport)模式：只是传输层数据被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被放置在原 IP 包头后面。通常，传输模式应用在两台主机之间的通讯，或一台主机和一个安全网关之间的通讯。

不同的安全协议在tunnel和transport模式下的数据封装形式如 [图 1-1](#) 所示。

图1-1 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

4. 认证算法与加密算法

(1) 认证算法

认证算法的实现主要是通过杂凑函数。杂凑函数是一种能够接受任意长的消息输入，并产生固定长度输出的算法，该输出称为消息摘要。IPsec 对等体计算摘要，如果两个摘要是相同的，则表示报文是完整未经篡改的。IPsec 使用两种认证算法：

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

MD5 算法的计算速度比 SHA-1 算法快，而 SHA-1 算法的安全强度比 MD5 算法高。

(2) 加密算法

加密算法实现主要通过对称密钥系统，它使用相同的密钥对数据进行加密和解密。目前设备的 IPsec 实现三种加密算法：

- DES（Data Encryption Standard）：使用 56bit 的密钥对一个 64bit 的明文块进行加密。
- 3DES（Triple DES）：使用三个 56bit 的 DES 密钥（共 168bit 密钥）对明文进行加密。
- AES（Advanced Encryption Standard）：使用 128bit、192bit 或 256bit 密钥长度的 AES 算法对明文进行加密。

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。对于普通的安全要求，DES 算法就可以满足需要。

5. 协商方式

有如下两种协商方式建立 SA：

- 手工方式（manual）配置比较复杂，创建 SA 所需的全部信息都必须手工配置，而且不支持一些高级特性（例如定时更新密钥），但优点是可以不依赖 IKE 而单独实现 IPsec 功能。
- IKE 自动协商（isakmp）方式相对比较简单，只需要配置好 IKE 协商安全策略的信息，由 IKE 自动协商来创建和维护 SA。

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

6. 安全隧道

安全隧道是建立在本端和对端之间可以互通的一个通道，它由一对或多对 SA 组成。

1.1.2 使用IPsec保护IPv6 路由协议

使用 IPsec 保护 IPv6 路由协议是指，使用 AH/ESP 协议对 IPv6 路由协议报文进行加/解封装处理，并为其提供认证和加密的安全服务，目前支持 OSPFv3、IPv6 BGP、RIPng 路由协议。

IPsec 对 IPv6 路由协议报文进行保护的处理方式和目前基于接口的 IPsec 处理方式不同，是基于业务的 IPsec，即 IPsec 保护某一业务的所有报文。该方式下，设备产生的所有需要 IPsec 保护的 IPv6 路由协议报文都要被进行加封装处理，而设备接收到的不受 IPsec 保护的以及解封装（解密或验证）失败的 IPv6 路由协议报文都要被丢弃。

在基于接口的 IPsec 处理方式下，设备对配置了 IPsec 安全功能的接口上发送的每个报文都要判断是否进行 IPsec 处理。目前，该方式采用基于 ACL 的 IPsec 的实现，只要到达接口的报文与该接口的 IPsec 安全策略中的 ACL 规则匹配，就会受到 IPsec 保护。

相对于基于接口的 IPsec，基于业务的 IPsec 既不需要 ACL 来限定要保护的流的范围，也不需要指定 IPsec 隧道的起点与终点，IPsec 安全策略仅与具体的业务绑定，不管业务报文从设备的哪个接口发送出去都会被 IPsec 保护。

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，因此必须使用手工配置密钥的方式。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，目前仅支持手工安全策略生成的 SA 对 IPv6 路由协议报文进行保护。

1.1.3 协议规范

与 IPsec 相关的协议规范有：

- RFC2401: Security Architecture for the Internet Protocol
- RFC2402: IP Authentication Header
- RFC2406: IP Encapsulating Security Payload
- RFC4552: Authentication/Confidentiality for OSPFv3

1.2 建立IPsec隧道的配置方式

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，通过配置安全策略并将安全策略绑定在实际的物理接口上来完成IPsec的配置。这种方式可以利用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。具体配置请参见“[1.3 基于ACL建立IPsec安全隧道](#)”。

- 基于业务方式：IPsec安全策略直接与具体的业务绑定，保护某一业务的所有报文，无需ACL或者路由来指定要保护的数据流。目前，支持对IPv6 路由协议的保护。通过配置手工方式的IPsec安全策略，并在IPv6 路由协议上应用安全策略来完成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安全隧道

1.3.1 IPsec隧道限制说明

目前，设备通过ACL来识别由IPsec隧道保护的流量时，受保护的流量只能是源地址或目的地址为本机的报文。例如：可配置IPsec隧道对设备发送给日志服务器的日志信息进行保护。ACL中定义的匹配转发流量的规则不生效，IPsec不会对设备转发的任何数据流和语音流进行保护。关于IPsec中ACL规则的定义请参见“[1.3.3 配置访问控制列表](#)”。

1.3.2 IPsec配置任务简介

基于 ACL 建立 IPsec 安全隧道的基本配置思路如下：

- (1) 通过配置访问控制列表，用于匹配需要保护的数据流；
- (2) 通过配置安全提议，指定安全协议、认证算法和加密算法、封装模式等；
- (3) 通过配置安全策略，将要保护的数据流和安全提议进行关联（即定义对何种数据流实施何种保护），并指定 SA 的协商方式、对等体 IP 地址（即保护路径的起/终点）、所需要的密钥和 SA 的生存周期等；
- (4) 最后在设备接口上应用安全策略即可完成 IPsec 隧道的配置。

表1-1 IPsec 配置任务简介

配置任务		说明	详细配置
IPsec基本配置	配置访问控制列表	必选	1.3.3
	配置安全提议		1.3.4
	配置安全策略		1.3.5
	在接口上应用安全策略组		1.3.6
配置会话空闲超时时间		可选	1.3.7
使能解封装后IPsec报文的ACL检查开关		可选	1.3.8
配置IPsec抗重放功能		可选	1.3.9
配置报文信息预提取功能		可选	1.3.10



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。

1.3.3 配置访问控制列表

ACL（Access Control List，访问控制列表）是用来实现流识别功能的。网络设备为了过滤报文，需要配置一系列的匹配条件对报文进行分类，当设备的端口接收到报文后，即根据当前端口上应用的 ACL 规则对报文进行分析、识别之后，根据预先设定的策略对报文进行不同的处理。

1. ACL规则中关键字的使用

IPsec 通过配置 ACL 来定义需要过滤的数据流。在 IPsec 的应用中，ACL 规则中的 **permit** 关键字表示与之匹配的流量需要被 IPsec 保护，而规则中的 **deny** 关键字则表示与之匹配的那些流量不需要保护。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，如果该规则为 **permit**，则该规则就定义了需要建立 SA 来保护的数据流量的范围。

在 IPsec 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 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。
- 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 IPsec 报文将被进行解封装处理，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，否则丢弃。

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保护的 IPsec 报文将被接收并处理，入方向上未被保护的 IPsec 报文将被丢弃。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，影响正常的业务流传输。
- 合理使用 **deny** 规则，尤其是在一个安全策略下有多条优先级不同的子安全策略时，避免本应该与优先级较低的子安全策略的 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子安全策略的 ACL **deny** 规则匹配上，而在接收端被当作未被 IPsec 保护的报文丢弃。
- 在交换机上给 IPsec 使用的 ACL 不能与其它业务共享，并且 ACL 中的规则要对称，否则某些情况下 IPsec 只能保护单一方向的数据流。

2. ACL规则的配置

为保证 SA 的成功建立，建议将 IPsec 对等体上的访问控制列表镜像配置，即保证两端要保护的数据流范围是镜像的。

若 IPsec 对等体上的访问控制列表配置非镜像，那么只有一种情况下，SA 的协商是可以建立的。这种情况就是，一端的访问控制列表规则定义的范围是另外一端的子集。但需要注意的是，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起的协商是可以成功的；从粗粒度一方向细粒度一方发起的协商是不能成功的。

3. 数据流的保护方式

目前，设备支持的数据流的保护方式为标准方式：即一条隧道保护一条数据流。ACL 中的每一个规则对应的数据流都会由一条单独创建的隧道来保护。



说明

- ACL 的具体配置请参见“ACL 和 QoS 配置指导”中的“ACL”。
- 若在接口上同时使能 IPsec 和 QoS，同一个 IPsec 安全联盟的数据流如果被 QoS 分类进入不同队列，会导致部分报文发送乱序。由于 IPsec 具有防重放功能，IPsec 入方向上对于防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 结合使用时，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”。

1.3.4 配置安全提议

安全提议是安全策略的一个组成部分，它用于保存 IPsec 需要使用的特定安全协议、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。

表1-2 配置安全提议

操作		命令	说明
进入系统视图		system-view	-
创建安全提议，并进入安全提议视图		ipsec proposal <i>proposal-name</i>	必选 缺省情况下，没有任何安全提议存在
配置安全提议采用的安全协议		transform { ah ah-esp esp }	可选 缺省情况下，采用ESP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 aes [key-length] des } FIPS模式下： esp encryption-algorithm aes [key-length]	可选 非FIPS模式的缺省情况下，ESP协议采用DES加密算法 FIPS模式的缺省情况下，ESP协议缺省采用AES-128加密算法
	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	可选 非FIPS模式的缺省情况下，ESP协议采用MD5认证算法 FIPS模式的缺省情况下，ESP协议缺省采用SHA1认证算法
	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	可选 非FIPS模式的缺省情况下，AH协议采用MD5认证算法 FIPS模式的缺省情况下，AH协议缺省采用SHA1认证算法

操作	命令	说明
配置安全协议对IP报文的封装形式	encapsulation-mode { transport tunnel }	可选 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安全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



说明

- 可对安全提议进行修改，但对已协商成功的 SA，新修改的安全提议并不起作用，即 SA 仍然使用原来的安全提议（除非使用 **reset ipsec sa** 命令重置），只有新协商的 SA 将使用新的安全提议。
- 只有选择了相应的安全协议后，该安全协议所需的安全算法才可配置。例如，如果使用 **transform** 命令选择了 **esp**，那么只有 ESP 所需的安全算法才可配置，而 AH 所需的安全算法则不能配置。ESP 协议允许对报文同时进行加密和认证，或只加密，或只认证。FIPS 模式下，ESP 必须同时使用加密和认证。

1.3.5 配置安全策略

安全策略规定了对什么样的数据流采用什么样的安全提议。一条安全策略由“名字”和“顺序号”共同唯一确定。

安全策略分为手工安全策略和 IKE 协商安全策略：

- 手工配置方式：需要用户手工配置密钥、SPI 等参数，在隧道模式下还需要手工配置安全隧道两个端点的 IP 地址；
- IKE 协商方式：由 IKE 自动协商生成各参数。（仅在 FIPS 模式下支持）

1. 手工配置安全策略

(1) 配置准备

手工配置安全策略时，除完成该安全策略需要引用的访问控制列表及安全提议的配置之外，为保证 SA 的协商成功，安全隧道两端的配置必须符合以下要求：

- 安全策略引用的安全提议应采用相同的安全协议、安全算法和报文封装形式；
- 当前端点的对端地址与对端的本端地址应保持一致；
- 应分别设置出方向 SA 和入方向 SA 的参数，且保证 SA 的唯一性，即不同 SA 必须对应不同的 SPI；
- 本端和对端 SA 的 SPI 及密钥必须是完全匹配的。即，本端的入方向 SA 的 SPI 及密钥必须和对端的出方向 SA 的 SPI 及密钥相同；本端的出方向 SA 的 SPI 及密钥必须和对端的入方向 SA 的 SPI 及密钥相同；

- 两端 SA 使用的密钥应当以相同的方式输入。即，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。而且，任何一端出入方向的 SA 使用的密钥也应当以相同的方式输入。
- 对于要应用于 IPv6 路由协议的安全策略，无需配置访问控制列表和隧道地址，但是应该符合以下要求：
- 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；
 - 同一个范围内的，所有设备上的安全策略所引用的安全提议采用的安全协议、安全算法和报文封装形式要相同，而且所有设备上的 SA 的 SPI 及密钥均要保持一致。该范围与协议相关：对于 OSPFv3，是 OSPFv3 邻居之间或一个 OSPFv3 区域内；对于 RIPng，是 RIPng 直连邻居之间或一个 RIPng 进程内；对于 IPv6 BGP，是 IPv6 BGP 邻居之间或一个对等体组内。

(2) 手工配置安全策略

表1-3 手工配置安全策略

操作		命令	说明
进入系统视图		system-view	-
用手工方式创建一条安全策略，并进入安全策略视图		ipsec policy <i>policy-name</i> seq-number manual	必选 缺省情况下，没有任何安全策略存在
配置安全策略引用的访问控制列表		security acl <i>acl-number</i>	若安全策略要应用于IPv6路由协议，则无需此配置，其它情况必选 缺省情况下，安全策略没有指定访问控制列表
配置安全策略所引用的安全提议		proposal <i>proposal-name</i>	必选 缺省情况下，安全策略没有引用任何安全提议
配置隧道的起点与终点	配置安全隧道的本端地址	tunnel local <i>ip-address</i>	若安全策略要应用于IPv6路由协议，则无需此配置，其它情况必选 缺省情况下，没有配置安全隧道的本端地址和对端地址
	配置安全隧道的对端地址	tunnel remote <i>ip-address</i>	
配置SA的安全参数索引参数		sa spi { inbound outbound } { ah esp } spi-number	必选 缺省情况下，不存在SA的安全参数索引
配置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 authentication-hex { inbound outbound } ah [cipher string-key simple hex-key]	二者必选其一 FIPS模式下不支持 sa string-key 命令
	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] string-key	
	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] string-key	至少选其一 以字符串方式输入密钥时，系统会自动地同时生成认证算

操作	命令	说明
配置ESP协议的认证密钥(以16进制方式输入)	sa authentication-hex { inbound outbound } esp [cipher string-key simple hex-key]	法的密钥和加密算法的密钥 FIPS模式下不支持 sa string-key 命令
配置ESP协议的加密密钥(以16进制方式输入)	sa encryption-hex { inbound outbound } esp [cipher string-key simple hex-key]	



说明

- 一条安全策略只能引用一条访问控制列表，如果设置安全策略引用了多于一个访问控制列表，最后引用的那条访问控制列表才有效。
- 通过手工方式建立 SA，一条安全策略只能引用一个安全提议，并且如果已经引用了安全提议，必须先取消原先的安全提议才能引用新的安全提议。
- 在为系统配置 SA 时，必须分别设置 **inbound** 和 **outbound** 两个方向 SA 的参数。同时，为保证 SA 的唯一性，不同 SA 必须对应不同的 SPI，且设备上同一个方向上的 SPI 必须不同。
- 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。
- 对于手工方式创建的安全策略，不能直接修改它的创建方式，而必须先删除该安全策略然后再重新创建。

2. 配置使用IKE协商方式的安全策略（仅在FIPS模式下支持）

在采用 IKE 方式配置安全策略时，目前仅支持直接配置安全策略，即：在安全策略视图中定义需要协商的各参数。

(1) 配置准备

在配置 IKE 协商安全策略之前，需要完成以下配置：

- 配置所引用的访问控制列表和安全提议。
- 配置IKE对等体。具体配置请参见“[2.5 配置IKE对等体](#)”。

为保证 IKE 协商成功，安全策略中所有配置的参数必须在本端和对端相匹配。

(2) 直接配置使用 IKE 协商方式的安全策略

表1-4 直接配置使用 IKE 协商方式的安全策略

操作	命令	说明
进入系统视图	system-view	-
创建一条安全策略，并进入安全策略视图	ipsec policy <i>policy-name</i> <i>seq-number</i> isakmp	必选 缺省情况下，没有安全策略存在
配置用于描述安全策略的IPsec连接名	connection-name <i>name</i>	可选 缺省情况下，无IPsec连接名

操作	命令	说明
配置安全策略引用的访问控制列表	security acl <i>acl-number</i>	必选 缺省情况下，安全策略没有指定访问控制列表
配置安全策略所引用的安全提议	proposal <i>proposal-name</i> <1-6>	必选 缺省情况下，安全策略没有引用任何提议
在安全策略中引用IKE对等体	ike-peer <i>peer-name</i>	必选
配置使用此安全策略发起协商时使用PFS特性	pfs { dh-group2 dh-group5 dh-group14 }	可选 缺省情况下，安全策略发起协商时没有使用PFS特性 PFS（Perfect Forward Secrecy，完善的前向安全性）特性请参见“ 2.1.1 IKE的安全机制 ”
配置SA的生存周期	sa duration { time-based seconds traffic-based kilobytes }	可选 缺省情况下，安全策略的SA生存周期为当前全局的SA生存周期值
使能安全策略	policy enable	可选 缺省情况下，安全策略处于使能状态
退回系统视图	quit	-
配置全局SA的生存周期	ipsec sa global-duration { time-based seconds traffic-based kilobytes }	可选 缺省情况下，SA基于时间的生存周期为3600秒，基于流量的生存周期为1843200千字节



说明

- 一条安全策略只能引用一条访问控制列表，如果设置安全策略引用了多于一个访问控制列表，最后配置的那条访问控制列表才有效。
- 通过 IKE 协商建立 SA，一条安全策略最多可以引用六个安全提议，IKE 协商将在安全隧道的两端搜索能够完全匹配的安全提议。如果 IKE 在两端找不到完全匹配的安全提议，则 SA 不能建立，需要被保护的报文将被丢弃。
- IKE 在使用安全策略发起一个协商时，可以进行一个 PFS 交换。如果本端配置了 PFS 特性，则发起协商的对端也必须配置 PFS 特性，而且本端和对端指定的 DH 组必须一致，否则协商会失败。
- 所有在安全策略视图下没有单独配置生存周期的 SA，都采用全局生存周期。IKE 为 IPsec 协商建立 SA 时，采用本地设置的和对端提议的生存周期中较小的一个。
- 对于 IKE 方式创建的安全策略，不能直接修改它的创建方式，而必须先删除该安全策略然后再重新创建。

1.3.6 在接口上应用安全策略组



说明

本特性仅在 FIPS 模式下支持。

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

为使定义的 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（逻辑的或物理的）上应用一个安全策略组，以对数据进行保护。当取消安全策略组在接口上的应用后，此接口便不再具有 IPsec 的安全保护功能。

当从一个接口发送数据时，将按照从小到大的顺序号查找安全策略组中每一条安全策略。如果数据匹配了一条安全策略引用的访问控制列表，则使用这条安全策略对数据进行处理；如果数据没有匹配安全策略引用的访问控制列表，则继续查找下一条安全策略；如果数据与所有安全策略引用的访问控制列表都不匹配，则直接被发送（IPsec 不对数据加以保护）。

表1-5 在接口上应用安全策略组

操作	命令	说明
进入系统视图	system-view	-
进入接口视图	interface <i>interface-type</i> <i>interface-number</i>	-
应用指定的安全策略组	ipsec policy <i>policy-name</i>	必选



说明

- 目前，设备上的安全策略只支持在 Vlan 接口或三层以太网接口下配置。
- 一个接口只能应用一个安全策略组。交换机上同一个安全策略不允许应用到多个接口上，通过手工创建的安全策略只能应用到一个接口上。

1.3.7 配置会话空闲超时时间



说明

本特性仅在 FIPS 模式下支持。

数据包首次匹配 IPsec 策略后创建 IPsec 会话，并根据匹配结果创建 IPsec 会话表项，会话表项中记录了报文的五元组（源 IP 地址、目的 IP 地址、协议号、源端口、目的端口）和匹配的 IPsec 隧道。

IPsec 会话的删除由 IPsec 会话的空闲超时时间决定。IPsec 会话在超过它的空闲超时时间之后，被自动删除。

属于该会话的后续数据流根据报文的五元组，来查找会话表项。如果找到匹配的会话表项，则根据会话表项中的隧道信息来处理；如果没有找到匹配的会话表项，则按照 IPsec 原来的处理流程来处理，即从接口下查找策略组、策略，最后查找匹配的隧道来处理。

IPsec 流程中增加的会话处理机制，节省了大量的中间匹配过程，提高了 IPsec 的转发效率。

表1-6 配置会话空闲超时时间

操作	命令	说明
进入系统视图	system-view	-
配置IPsec会话的空闲超时时间	ipsec session idle-time seconds	可选 缺省情况下，IPsec会话的空闲超时时间为300秒

1.3.8 使能解封装后IPsec报文的ACL检查功能



说明

本特性仅在 FIPS 模式下支持。

在隧道模式下，对于解封装之后的入方向 IPsec 报文，有可能出现报文的内部 IP 头不在当前安全策略配置的 ACL 保护范围内的情况，如网络中恶意构造的攻击报文头可能不在此范围，所以需要重新检查报文内部 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 使能解封装后 IPsec 报文的 ACL 检查功能

操作	命令	说明
进入系统视图	system-view	-
使能解封装后IPsec报文的ACL检查功能	ipsec decrypt check	可选 缺省情况下，解封装后IPsec报文的ACL检查功能处于使能状态

1.3.9 配置IPsec抗重放功能



说明

本特性仅在 FIPS 模式下支持。

通常，重放报文是指已经处理过的报文。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，如果收到报文的序列号与已经解封装过的报文序列号相同，或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。

由于对重放报文的解封装无实际作用，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，实际上构成了拒绝服务攻击。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。

另外，在某些特定环境下，业务数据报文的序列号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。

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	-
使能IPsec抗重放检测功能	ipsec anti-replay check	可选 缺省情况下，IPsec抗重放检测功能处于使能状态
配置IPsec抗重放窗口宽度	ipsec anti-replay window width	可选 缺省情况下，IPsec抗重放窗口宽度为32



说明

- 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。



说明

按照 IPsec 协议，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与对手工方式生成的 IPsec SA 没有影响。

1.3.10 配置报文信息预提取功能



说明

本特性仅在 FIPS 模式下支持。

当在接口上同时应用了 IPsec 策略与 QoS 策略时，缺省情况下，QoS 使用被封装报文的外层 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，则需要配置报文信息预提取功能来实现。

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1-9 配置报文信息预提取功能

操作	命令	说明
进入系统视图	system-view	-
进入安全策略视图	ipsec policy <i>policy-name</i> <i>seq-number</i> [isakmp manual]	二者必选其一
配置报文信息预提取功能	qos pre-classify	必选 缺省情况下，报文信息预提取功能处于关闭状态

1.4 配置IPsec保护IPv6路由协议

使用 IPsec 安全策略建立 IPsec 安全隧道保护 IPv6 路由协议的基本配置思路如下：

- (1) 配置安全提议：指定安全协议、认证算法和加密算法、封装模式等；
- (2) 配置手工方式的安全策略：指定 SA 的 SPI 和密钥；
- (3) 在路由协议上应用安全策略。

表1-10 IPsec 虚拟隧道接口配置任务简介

配置任务	说明	详细配置
配置安全提议	必选	1.3.4
配置手工方式的安全策略	必选 无需配置访问控制列表和隧道地址	1.3.5 1.
在路由协议上应用安全策略	必选	分别参考“三层技术-IP路由配置指导”中的“IPv6 BGP”、“OSPFv3”和“RIPng”

1.5 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1-11 IPsec 显示和维护

操作	命令
显示安全策略的信息	display ipsec policy [<i>brief</i> <i>name policy-name</i> [<i>seq-number</i>]] [{ <i>begin</i> <i>exclude</i> <i>include</i> } <i>regular-expression</i>]
显示安全提议的信息	display ipsec proposal [<i>proposal-name</i>] [{ <i>begin</i> <i>exclude</i> <i>include</i> } <i>regular-expression</i>]
显示SA的相关信息	display ipsec sa [<i>brief</i> <i>policy policy-name</i> [<i>seq-number</i>]] <i>remote ip-address</i> [{ <i>begin</i> <i>exclude</i> <i>include</i> } <i>regular-expression</i>]
显示IPsec会话的信息	display ipsec session [<i>tunnel-id integer</i>] [{ <i>begin</i> <i>exclude</i> <i>include</i> } <i>regular-expression</i>]
显示IPsec处理报文的统计信息	display ipsec statistics [<i>tunnel-id integer</i>] [{ <i>begin</i> <i>exclude</i> <i>include</i> } <i>regular-expression</i>]
显示IPsec隧道的信息	display ipsec tunnel [{ <i>begin</i> <i>exclude</i> <i>include</i> } <i>regular-expression</i>]
清除已经建立的SA	reset ipsec sa [<i>parameters dest-address protocol spi</i> <i>policy policy-name</i> [<i>seq-number</i>]] <i>remote ip-address</i>]
清除设备上IPsec隧道的会话	reset ipsec session [<i>tunnel-id integer</i>]
清除IPsec的报文统计信息	reset ipsec statistics



说明

display ipsec session 和 **reset ipsec session** 命令仅在 FIPS 模式下支持。

1.6 IPsec典型配置举例

1.6.1 采用IKE方式建立保护IPv4 报文的IPsec安全隧道

1. 组网需求

- 如 图 1-2 所示，在Switch A和Switch B之间建立一个安全隧道，对Switch A与Switch B之间的数据流进行安全保护。
- 安全协议采用 ESP 协议，加密算法采用 AES-CBC-128，认证算法采用 HMAC-SHA1-96。

2. 组网图

图1-2 IPsec 配置组网图



3. 配置步骤

(1) 配置 Switch A

配置 Vlan-interface1 接口的 IP 地址。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 2.2.2.1 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

配置一个访问控制列表，定义由 Switch A 去 Switch B 的数据流。

```
[SwitchA] acl number 3101
[SwitchA-acl-adv-3101] rule 0 permit ip source 2.2.2.1 0 destination 2.2.3.1 0
[SwitchA-acl-adv-3101] rule 5 permit ip source 2.2.3.1 0 destination 2.2.2.1 0
[SwitchA-acl-adv-3101] quit
```

创建名为 tran1 的安全提议。

```
[SwitchA] ipsec proposal tran1
# 报文封装形式采用隧道模式。
[SwitchA-ipsec-proposal-tran1] encapsulation-mode tunnel
# 安全协议采用 ESP 协议。
[SwitchA-ipsec-proposal-tran1] transform esp
# 选择算法。
[SwitchA-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchA-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchA-ipsec-proposal-tran1] quit
```

配置 IKE 对等体。

```
[SwitchA] ike peer peer
[SwitchA-ike-peer-peer] pre-shared-key Ab12<><>
[SwitchA-ike-peer-peer] remote-address 2.2.3.1
[SwitchA-ike-peer-peer] quit
```

创建一条安全策略，协商方式为 isakmp。

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

```
# 引用安全提议。
[SwitchA-ipsec-policy-isakmp-map1-10] proposal tran1
# 引用访问控制列表。
[SwitchA-ipsec-policy-isakmp-map1-10] security acl 3101
# 引用 IKE 对等体。
[SwitchA-ipsec-policy-isakmp-map1-10] ike-peer peer
[SwitchA-ipsec-policy-isakmp-map1-10] quit
# 在 Vlan-interface1 接口上应用安全策略组。
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ipsec policy map1
```

(2) 配置 Switch B

```
# 配置 Vlan-interface1 接口的 IP 地址。
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 2.2.3.1 255.255.255.0
[SwitchB-Vlan-interface1] quit
# 配置一个访问控制列表，定义由 Switch B 去 Switch A 的数据流。
[SwitchB] acl number 3101
[SwitchB-acl-adv-3101] rule 0 permit ip source 2.2.3.1 0 destination 2.2.2.1 0
[SwitchB-acl-adv-3101] rule 5 permit ip source 2.2.2.1 0 destination 2.2.3.1 0
[SwitchB-acl-adv-3101] quit
# 创建名为 tran1 的安全提议。
[SwitchB] ipsec proposal tran1
# 报文封装形式采用隧道模式。
[SwitchB-ipsec-proposal-tran1] encapsulation-mode tunnel
# 安全协议采用 ESP 协议。
[SwitchB-ipsec-proposal-tran1] transform esp
# 选择算法。
[SwitchB-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchB-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchB-ipsec-proposal-tran1] quit
# 配置 IKE 对等体。
[SwitchB] ike peer peer
[SwitchB-ike-peer-peer] pre-shared-key Ab12<><>
[SwitchB-ike-peer-peer] remote-address 2.2.2.1
[SwitchB-ike-peer-peer] quit
# 创建一条安全策略，协商方式为 isakmp。
[SwitchB] ipsec policy use1 10 isakmp
# 引用访问控制列表。
[SwitchB-ipsec-policy-isakmp-use1-10] security acl 3101
# 引用安全提议。
[SwitchB-ipsec-policy-isakmp-use1-10] proposal tran1
# 引用 IKE 对等体。
[SwitchB-ipsec-policy-isakmp-use1-10] ike-peer peer
```

```
[SwitchB-ipsec-policy-isakmp-use1-10] quit
# 在 Vlan-interface1 接口上应用安全策略组。
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ipsec policy use1
```

4. 验证配置结果

以上配置完成后，Switch A 和 Switch B 之间如果有报文发送，将触发 IKE 进行协商建立 SA。IKE 协商成功并创建了 SA 后，Switch A 和 Switch B 之间的数据流将被加密传输。

1.6.2 配置IPsec保护RIPng报文



说明

IPsec 保护其它 IPv6 路由协议（OSPFv3、IPv6 BGP）的具体配置与本例类似，具体内容请参考“三层技术-IP 路由配置指导”中的“OSPFv3”和“IPv6 BGP”。

1. 组网需求

如 图 1-3 所示，Switch A、Switch B 和 Switch C 相连，并通过 RIPng 来学习网络中的 IPv6 路由信息。具体组网要求如下：

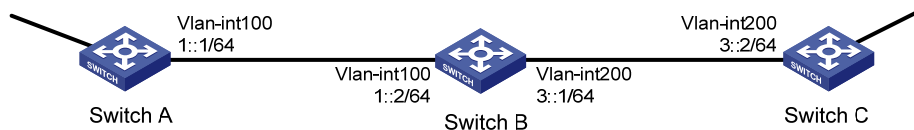
- 在各设备之间建立 IPsec 安全隧道，对它们收发的 RIPng 报文进行安全保护；
- 安全协议采用 ESP 协议，加密算法采用 DES，认证算法采用 HMAC-SHA1-96。

配置思路：

- 配置 RIPng 的基本功能
- 配置手工方式的 IPsec 安全策略
- 在 RIPng 进程下或接口上应用 IPsec 安全策略（进程下配置的 IPsec 安全策略对该进程的所有报文有效，接口下的 IPsec 安全策略只对接口的报文有效）

2. 组网图

图1-3 配置 IPsec 保护 RIPng 报文组网图



3. 配置步骤



说明

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”。

(1) 配置 Switch A

- 配置各接口的 IPv6 地址（略）
- 配置 RIPng 的基本功能

```
<SwitchA> system-view
```

```
[SwitchA] ripng 1
[SwitchA-ripng-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ripng 1 enable
[SwitchA-Vlan-interface100] quit
```

- 配置 IPsec 安全策略

创建并配置名为 tran1 的安全提议（报文封装形式采用传输模式，安全协议采用 ESP 协议，加密算法采用 DES，认证算法采用 HMAC-SHA1-96）。

```
[SwitchA] ipsec proposal tran1
[SwitchA-ipsec-proposal-tran1] encapsulation-mode transport
[SwitchA-ipsec-proposal-tran1] transform esp
[SwitchA-ipsec-proposal-tran1] esp encryption-algorithm des
[SwitchA-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchA-ipsec-proposal-tran1] quit
```

创建并配置名为 policy001 的安全策略（协商方式为 manual，出入方向 SA 的 SPI 均为 123456，出入方向 SA 的密钥均为 abcdefg）。

```
[SwitchA] ipsec policy policy001 10 manual
[SwitchA-ipsec-policy-manual-policy001-10] proposal tran1
[SwitchA-ipsec-policy-manual-policy001-10] sa spi outbound esp 123456
[SwitchA-ipsec-policy-manual-policy001-10] sa spi inbound esp 123456
[SwitchA-ipsec-policy-manual-policy001-10] sa string-key outbound esp abcdefg
[SwitchA-ipsec-policy-manual-policy001-10] sa string-key inbound esp abcdefg
[SwitchA-ipsec-policy-manual-policy001-10] quit
```

- 在 RIPng 进程上应用 IPsec 安全策略

```
[SwitchA] ripng 1
[SwitchA-ripng-1] enable ipsec-policy policy001
[SwitchA-ripng-1] quit
```

(2) 配置 Switch B

- 配置各接口的 IPv6 地址（略）

- 配置 RIPng 的基本功能

```
<SwitchB> system-view
[SwitchB] ripng 1
[SwitchB-ripng-1] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ripng 1 enable
[SwitchB-Vlan-interface200] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ripng 1 enable
[SwitchB-Vlan-interface100] quit
```

- 配置 IPsec 安全策略

创建并配置名为 tran1 的安全提议（报文封装形式采用传输模式，安全协议采用 ESP 协议，加密算法采用 DES，认证算法采用 HMAC-SHA1-96）。

```
[SwitchB] ipsec proposal tran1
[SwitchB-ipsec-proposal-tran1] encapsulation-mode transport
[SwitchB-ipsec-proposal-tran1] transform esp
[SwitchB-ipsec-proposal-tran1] esp encryption-algorithm des
```

```
[SwitchB-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchB-ipsec-proposal-tran1] quit
# 创建并配置名为 policy001 的安全策略（协商方式为 manual，出入方向 SA 的 SPI 均为 123456，出入方向 SA 的密钥均为 abcdefg）。
```

```
[SwitchB] ipsec policy policy001 10 manual
[SwitchB-ipsec-policy-manual-policy001-10] proposal tran1
[SwitchB-ipsec-policy-manual-policy001-10] sa spi outbound esp 123456
[SwitchB-ipsec-policy-manual-policy001-10] sa spi inbound esp 123456
[SwitchB-ipsec-policy-manual-policy001-10] sa string-key outbound esp abcdefg
[SwitchB-ipsec-policy-manual-policy001-10] sa string-key inbound esp abcdefg
[SwitchB-ipsec-policy-manual-policy001-10] quit
```

- 在 RIPng 进程上应用 IPsec 安全策略

```
[SwitchB] ripng 1
[SwitchB-ripng-1] enable ipsec-policy policy001
[SwitchB-ripng-1] quit
```

(3) 配置 Switch C

- 配置各接口的 IPv6 地址（略）
- 配置 RIPng 的基本功能

```
<SwitchC> system-view
[SwitchC] ripng 1
[SwitchC-ripng-1] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] ripng 1 enable
[SwitchC-Vlan-interface200] quit
```

- 配置 IPsec 安全策略

创建并配置名为 tran1 的安全提议（报文封装形式采用传输模式，安全协议采用 ESP 协议，加密算法采用 DES，认证算法采用 HMAC-SHA1-96）。

```
[SwitchC] ipsec proposal tran1
[SwitchC-ipsec-proposal-tran1] encapsulation-mode transport
[SwitchC-ipsec-proposal-tran1] transform esp
[SwitchC-ipsec-proposal-tran1] esp encryption-algorithm des
[SwitchC-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchC-ipsec-proposal-tran1] quit
```

创建并配置名为 policy001 的安全策略（协商方式为 manual，出入方向 SA 的 SPI 均为 123456，出入方向 SA 的密钥均为 abcdefg）。

```
[SwitchC] ipsec policy policy001 10 manual
[SwitchC-ipsec-policy-manual-policy001-10] proposal tran1
[SwitchC-ipsec-policy-manual-policy001-10] sa spi outbound esp 123456
[SwitchC-ipsec-policy-manual-policy001-10] sa spi inbound esp 123456
[SwitchC-ipsec-policy-manual-policy001-10] sa string-key outbound esp abcdefg
[SwitchC-ipsec-policy-manual-policy001-10] sa string-key inbound esp abcdefg
[SwitchC-ipsec-policy-manual-policy001-10] quit
```

- 在 RIPng 进程上应用 IPsec 安全策略

```
[SwitchC] ripng 1
[SwitchC-ripng-1] enable ipsec-policy policy001
[SwitchC-ripng-1] quit
```

4. 验证配置结果

以上配置完成后，Switch A、Switch B 和 Switch 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 SA。

可以通过如下 **display** 命令查看 Switch 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 策略，且携带了有效的 SPI 值。

```
<SwitchA> 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 policy name: policy001, SPI: 123456
```

可以通过如下 **display** 命令查看 Switch A 上生成的 SA。

```
<SwitchA> display ipsec sa
=====
Protocol: RIPng
=====

-----
IPsec policy name: "policy001"
sequence number: 10
mode: manual
-----

connection id: 1
encapsulation mode: transport
perfect forward secrecy:
tunnel:
flow:

[inbound ESP SAs]
  spi: 123456 (0x3039)
  proposal: ESP-ENCRYPT-DES ESP-AUTH-SHA1
  No duration limit for this sa

[outbound ESP SAs]
  spi: 123456 (0x3039)
  proposal: ESP-ENCRYPT-DES ESP-AUTH-SHA1
  No duration limit for this sa
```

Switch B 和 Switch C 上也会生成相应的 SA 来保护 RIPng 报文，查看方式与 Switch A 同，此处略。

2 IKE



说明

设备仅在 FIPS 模式下，支持 IKE。关于 FIPS 模式的介绍，请参见“安全配置指导”中的“FIPS”。

2.1 IKE简介

在实施 IPsec 的过程中，可以使用 IKE（Internet Key Exchange，因特网密钥交换）协议来建立 SA，该协议建立在由 ISAKMP（Internet Security Association and Key Management Protocol，互联网安全联盟和密钥管理协议）定义的框架上。IKE 为 IPsec 提供了自动协商交换密钥、建立 SA 的服务，能够简化 IPsec 的使用和管理，大大简化 IPsec 的配置和维护工作。

IKE 不是在网络上直接传输密钥，而是通过一系列数据的交换，最终计算出双方共享的密钥，并且即使第三方截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥。

2.1.1 IKE的安全机制

IKE 具有一套自保护机制，可以在不安全的网络上安全地认证身份、分发密钥、建立 IPsec SA。

1. 数据认证

数据认证有如下两方面的概念：

- 身份认证：身份认证确认通信双方的身份。支持两种认证方法：预共享密钥（pre-shared-key）认证和基于 PKI 的数字签名（rsa-signature）认证。
- 身份保护：身份数据在密钥产生之后加密传送，实现了对身份数据的保护。

2. DH

DH（Diffie-Hellman，交换及密钥分发）算法是一种公共密钥算法。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，也不足以计算出真正的密钥。所以，DH 交换技术可以保证双方能够安全地获得公有信息。

3. PFS

PFS（Perfect Forward Secrecy，完善的前向安全性）特性是一种安全特性，指一个密钥被破解，并不影响其他密钥的安全性，因为这些密钥间没有派生关系。对于 IPsec，是通过在 IKE 阶段 2 协商中增加一次密钥交换来实现的。PFS 特性是由 DH 算法保障的。

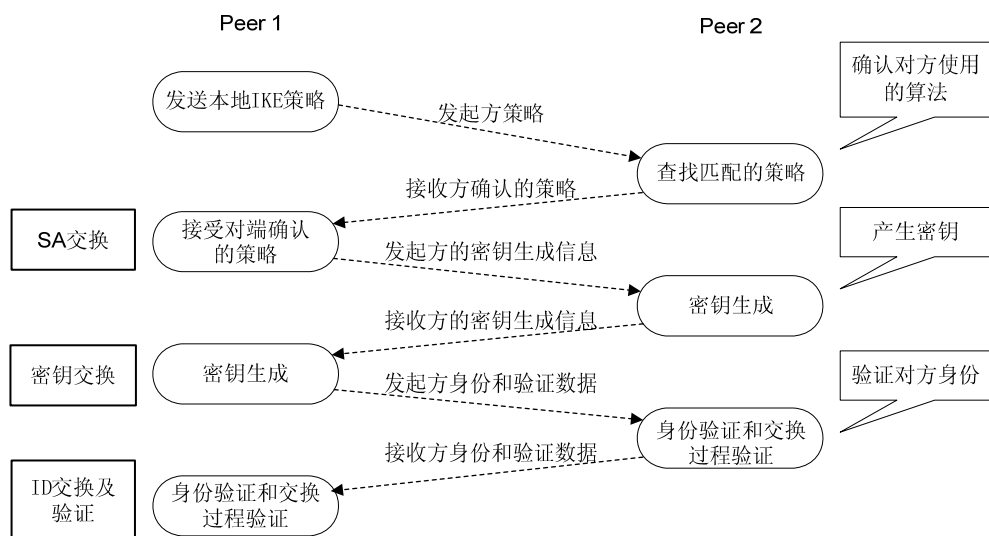
2.1.2 IKE的交换过程

IKE 使用了两个阶段为 IPsec 进行密钥协商并建立 SA：

- (1) 第一阶段，通信各方彼此间建立了一个已通过身份认证和安全保护的通道，即建立一个 ISAKMP SA。

- (2) 第二阶段,用在第一阶段建立的安全隧道为 IPsec 协商安全服务,即为 IPsec 协商具体的 SA,建立用于最终的 IP 数据安全传输的 IPsec SA。

图2-1 主模式交换过程



如 [图 2-1](#) 所示, 第一阶段主模式的IKE协商过程中包含三对消息:

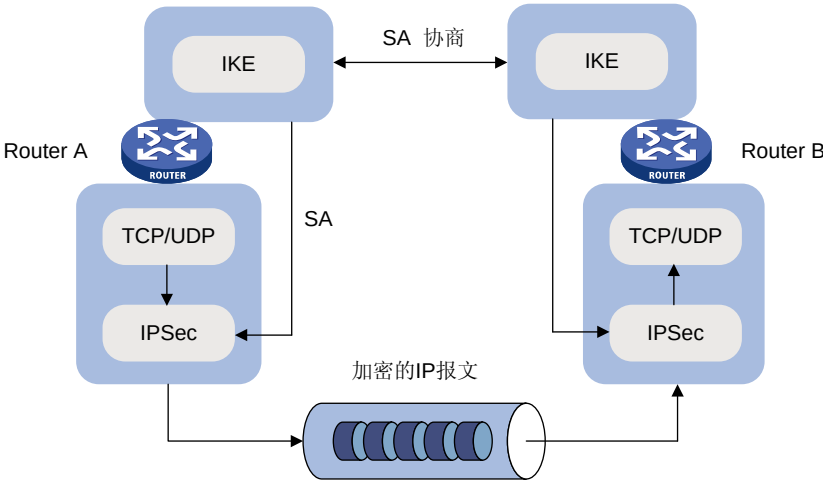
- 第一对叫 SA 交换, 是协商确认有关安全策略的过程;
- 第二对消息叫密钥交换, 交换 Diffie-Hellman 公共值和辅助数据 (如: 随机数), 密钥材料在这个阶段产生;
- 最后一对消息是 ID 信息和认证数据交换, 进行身份认证和对整个第一阶段交换内容的认证。

2.1.3 IKE在IPsec中的作用

- 因为有了 IKE, IPsec 很多参数 (如: 密钥) 都可以自动建立, 降低了手工配置的复杂度。
- IKE 协议中的 DH 交换过程, 每次的计算和产生的结果都是不相关的。每次 SA 的建立都运行 DH 交换过程, 保证了每个 SA 所使用的密钥互不相关。
- IPsec 使用 AH 或 ESP 报文头中的序列号实现防重放。此序列号是一个 32 比特的值, 此数溢出后, 为实现防重放, SA 需要重新建立, 这个过程需要 IKE 协议的配合。
- 对安全通信的各方身份的认证和管理, 将影响到 IPsec 的部署。IPsec 的大规模使用, 必须有 CA (Certificate Authority, 证书颁发机构) 或其他集中管理身份数据的机构的参与。
- IKE 提供端与端之间动态认证。

2.1.4 IPsec与IKE的关系

图2-2 IPsec 与 IKE 的关系图



从 [图 2-2](#) 中我们可以看出IKE和IPsec的关系：

- IKE 是 UDP 之上的一个应用层协议，是 IPsec 的信令协议；
- IKE 为 IPsec 协商建立 SA，并把建立的参数及生成的密钥交给 IPsec；
- IPsec 使用 IKE 建立的 SA 对 IP 报文加密或认证处理。

2.1.5 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。

- 确定 IKE 交换过程中算法的强度，即确定安全保护的强度（包括身份认证方法、加密算法、认证算法、DH 组）：不同的算法的强度不同，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。一般来说，密钥越长的算法强度越高。
- 确定通信双方预先约定的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”。

表2-1 IKE 配置任务简介

配置任务	说明	详细配置
配置本端安全网关的名字	可选	2.3

配置任务	说明	详细配置
配置IKE安全提议	可选 若IKE对等体中需要指定IKE安全提议，则必配	2.4
配置IKE对等体	必选	2.5
配置Keepalive定时器	可选	2.6
配置NAT Keepalive定时器	可选	2.7
配置对等体存活检测	可选	2.8
配置取消对next payload域的检查	可选	2.9

2.3 配置本端安全网关的名字

当IKE协商的发起端使用安全网关名字进行协商时(即配置了 **id-type name** 或 **id-type user-fqdn**)，本端需要配置本端安全网关的名字，该名字既可以在系统视图下进行配置，也可以在IKE对等体视图下配置，若IKE对等体视图下未配置本端安全网关的名字，则采用系统视图下的配置。

表2-2 配置本端安全网关名字

操作	命令	说明
进入系统视图	system-view	-
配置本端安全网关的名字	ike local-name name	可选 缺省情况下，使用设备名作为本端安全网关的名字

2.4 配置IKE安全提议

IKE安全提议定义了一套属性数据来描述IKE协商怎样进行安全通信。用户可以创建多条不同优先级的IKE提议，优先级由IKE提议的序号表示，数值越小，优先级越高。

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安全提议发送给对端，由对端进行匹配，协商响应方则从自己优先级最高（序号最小）的IKE提议开始，按照优先级顺序与对端发送的安全提议进行匹配，直到找到一个匹配的安全提议来使用。匹配的IKE提议将被用来建立安全隧道。

以上IKE安全提议的匹配原则是：协商双方具有相同的加密算法、认证方法、认证算法和DH组标识。匹配的IKE提议的ISAKMP SA存活时间则取两端的最小值。

缺省情况下，系统提供一条缺省的IKE提议。此缺省的IKE提议具有最低的优先级，具有缺省的加密算法、认证方法、认证算法、DH组标识和ISAKMP SA存活时间。

表2-3 配置IKE安全提议

操作	命令	说明
进入系统视图	system-view	-

操作	命令	说明
创建IKE提议, 并进入IKE提议视图	ike proposal <i>proposal-number</i>	必选
指定一个供IKE提议使用的加密算法	encryption-algorithm aes-cbc [<i>key-length</i>]	可选 缺省情况下, IKE缺省提议使用AES-CBC-128加密算法
指定一个供IKE提议使用的认证方法	authentication-method { pre-share rsa-signature }	可选 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	authentication-algorithm sha	可选 缺省情况下, IKE提议使用SHA1认证算法
配置IKE阶段1密钥协商时所使用的DH密钥交换参数	dh { group2 group5 group14 }	可选 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 group2 , 即1024-bit的Diffie-Hellman组
指定一个IKE提议的ISAKMP SA存活时间	sa duration <i>seconds</i>	可选 缺省情况下, IKE提议的ISAKMP SA存活时间为86400秒



说明

如果存活时间超时, ISAKMP SA 将自动更新。因为 IKE 协商需要进行 DH 计算, 在低端设备上需要经过较长的时间, 为使 ISAKMP SA 的更新不影响安全通信, 建议设置存活时间大于 10 分钟。

2.5 配置IKE对等体

在采用 IKE 方式配置安全策略时, 需要指定 IKE 对等体。IKE 对等体中主要包括以下配置:

- 本端作为发起方时所使用的协商模式 (主模式)。本端作为响应方时, 将自动适配发起方的协商模式。
- 本端作为发起方时可以使用的 IKE 安全提议 (可指定多个)。本端作为响应方时, 将使用系统视图下已经配置的安全提议与对端发送的安全提议进行协商。
- 根据 IKE 提议使用的认证方法不同, 选择所使用的预共享密钥或者 PKI 域。
- 本端在 IKE 第一阶段协商时, 所使用的 ID 类型 (IP 地址、FQDN 名、User FQDN 名)。在预共享密钥认证的主模式下, 只能使用 IP 地址类型的 ID。
- 本端安全网关的名字或 IP 地址。一般情况下本端安全网关的 IP 地址不需要配置, 只有要指定特殊的本端安全网关地址时 (如指定 **loopback** 接口地址) 才需要配置。
- 对端安全网关的名字或 IP 地址。若本端作为发起方, 则需要配置对端安全网关名字或对端安全网关 IP 地址, 它们用于发起方在协商过程中寻找对端。

- NAT 穿越功能。当 IPsec/IKE 隧道中存在 NAT 设备时，导致隧道一端为公网地址，另一端为私网地址，则必须在隧道两端均配置 NAT 穿越功能，保证隧道能够正常协商建立。
- 用于 IKE 对等体存活状态检测的 DPD 名称。

表2-4 配置 IKE 对等体

操作		命令	说明
进入系统视图		system-view	-
创建一个IKE对等体，并进入IKE-Peer视图		ike peer <i>peer-name</i>	必选
配置IKE第一阶段的协商模式		exchange-mode main	可选 缺省情况下，IKE阶段的协商模式使用主模式
配置IKE对等体引用的IKE安全提议		proposal <i>proposal-number</i> <1-6>	可选 缺省情况下，IKE对等体未引用任何IKE安全提议，使用系统视图下已配置的IKE安全提议进行IKE协商
配置采用预共享密钥认证时，所使用的预共享密钥		pre-shared-key [cipher simple] <i>key</i>	二者必选其一 根据IKE提议使用的认证方法选择其中一个配置
配置采用数字签名认证时，证书所属的PKI域		certificate domain <i>domain-name</i>	
选择IKE第一阶段的协商过程中使用ID的类型		id-type { ip name user-fqdn }	可选 缺省情况下，使用IP地址作为IKE协商过程中使用的ID
配置本端及对端安全网关的名字	配置本端安全网关的名字	local-name <i>name</i>	可选 对端使用 remote-name 配置的网关名字应与IKE协商发起端所配置的本端安全网关名字保持一致 缺省情况下，未定义本端安全网关的名字，使用系统视图下本端安全网关的名字
	配置对端安全网关的名字	remote-name <i>name</i>	
配置本端及对端安全网关的IP地址	配置本端安全网关的IP地址	local-address <i>ip-address</i>	可选 对端使用 remote-address 配置的IP地址应与IKE协商发起端使用 local-address 命令所配的网关IP地址保持一致 缺省情况下，IKE协商时的本端网关IP地址使用应用安全策略的接口的主IP地址
	配置对端安全网关的IP地址	remote-address { <i>hostname</i> [dynamic] <i>low-ip-address</i> [<i>high-ip-address</i>] }	

操作	命令	说明
配置IKE/IPsec的NAT穿越功能	nat traversal	可选 在IPsec/IKE组建的VPN隧道中，若存在NAT安全网关设备，则必须配置IPsec/IKE的NAT穿越功能 缺省情况下，没有配置NAT穿越功能
为IKE对等体应用一个DPD	dpd dpd-name	可选 缺省情况下，IKE对等体没有应用DPD 关于DPD的配置请参见“ 2.8 配置对等体存活检测 ”



说明

修改IKE对等体配置之后，要执行命令 **reset ipsec sa**、**reset ike sa** 来清除原有的IPsec SA与IKE SA，否则重新协商SA会失败。

2.6 配置Keepalive定时器

IKE通过Keepalive报文维护ISAKMP SA的链路状态。一般在对端配置了等待Keepalive报文的超时时间后，必须在本端配置此Keepalive报文发送时间间隔。当对端在配置的超时时间内未收到此Keepalive报文时，如果该ISAKMP SA带有TIMEOUT标记，则删除该ISAKMP SA以及由其协商的IPsec SA；否则，将其标记为TIMEOUT。

表2-5 配置Keepalive定时器

操作	命令	说明
进入系统视图	system-view	-
配置ISAKMP SA向对端发送Keepalive报文的时间间隔	ike sa keepalive-timer interval seconds	必选 缺省情况下，ISAKMP SA不向对端发送Keepalive报文
配置ISAKMP SA等待对端发送Keepalive报文的超时时间	ike sa keepalive-timer timeout seconds	必选 缺省情况下，ISAKMP SA不向对端发送Keepalive报文



说明

本端配置的 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 Keepalive 报文发送时间间隔的三倍。

2.7 配置 NAT Keepalive 定时器

在 IPsec/IKE 组建的 VPN 隧道中，若存在 NAT 安全网关设备，需配置 NAT 穿越功能来实现 NAT 穿越，但由于在 NAT 网关上的 NAT 映射会话有一定存活时间，因此一旦安全隧道建立后如果长时间没有报文穿越，NAT 会话表项会被删除，这样将导致在 NAT 网关外侧的隧道无法继续传输数据。为防止 NAT 表项老化，NAT 网关内网侧的 ISAKMP SA 会以一定的时间间隔向对端发送 NAT Keepalive 报文，以维持 NAT 会话的存活。

表2-6 配置 NAT Keepalive 定时器

操作	命令	说明
进入系统视图	system-view	-
配置 ISAKMP SA 向对端发送 NAT Keepalive 报文的时间间隔	ike sa nat-keepalive-timer interval seconds	必选 缺省情况下，ISAKMP SA 向对端发送 NAT Keepalive 报文的时间间隔为 20 秒

2.8 配置对等体存活检测

DPD (Dead Peer Detection, 对等体存活检测) 用于 IKE 对等体存活状态检测。启动 DPD 功能后，当本端需要向对端发送 IPsec 报文时，若判断当前距离最后一次收到对端 IPsec 报文已经超过触发 DPD 的时间间隔 (**interval-time interval-time**)，则触发 DPD 查询，本端主动向对端发送 DPD 请求报文，对 IKE 对等体是否存活进行检测。如果本端在 DPD 报文的重传时间间隔 (**time-out time-out**) 内未收到对端发送的 DPD 响应报文，则重传 DPD 请求，缺省重传两次之后，若仍然没有收到对端的 DPD 响应报文，则删除该 IKE SA 和对应的 IPsec SA。

DPD 和 Keepalive 的区别：

- Keepalive 定期发送查询；
- DPD 只在要发送加密报文前并且长时间（触发 DPD 的时间间隔）未收到对端 IPsec 报文时发送查询。

表2-7 配置对等体存活检测

操作	命令	说明
进入系统视图	system-view	-
创建一个 DPD，并进入 DPD 视图	ike dpd dpd-name	必选

操作	命令	说明
配置触发DPD的时间间隔	interval-time <i>interval-time</i>	可选 缺省情况下，触发DPD的时间间隔为10秒
配置DPD报文的重传时间间隔	time-out <i>time-out</i>	可选 缺省情况下，DPD报文的重传时间间隔为5秒

2.9 配置取消对next payload域的检查

next payload 域是在 IKE 协商报文（由几个 payload 组装而成）的最后一个 payload 的通用头中的一个域。按协议规定如果当前载荷处于消息的最后，该域必须为 0，但某些公司的设备会将该域赋其它值，为增强设备的互通性，可以通过下面的配置取消 IKE 协商过程对该域的检查。

表2-8 配置取消对 next payload 域的检查

操作	命令	说明
进入系统视图	system-view	-
配置在IKE协商过程中取消对next payload域的检查	ike next-payload check disabled	必选 缺省情况下，在IPsec协商过程中对next payload域进行检查

2.10 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 建立的安全隧道。

表2-9 IKE 显示和维护

操作	命令
显示DPD配置的参数	display ike dpd [<i>dpd-name</i>] [[{ begin exclude include } <i>regular-expression</i>]]
显示IKE对等体配置的参数	display ike peer [<i>peer-name</i>] [[{ begin exclude include } <i>regular-expression</i>]]
显示当前IKE SA的信息	display ike sa [verbose [connection-id <i>connection-id</i> remote-address <i>remote-address</i>]] [[{ begin exclude include } <i>regular-expression</i>]]
显示每个IKE提议配置的参数	display ike proposal [[{ begin exclude include } <i>regular-expression</i>]]
清除IKE建立的安全隧道	reset ike sa [<i>connection-id</i>]

2.11 IKE典型配置举例

1. 组网需求

- 在 Switch A 和 Switch B 之间建立一个安全隧道，对 Switch A 与 Switch B 之间的数据流进行安全保护。
- 在 Switch A 上配置一条 IKE 提议，其提议号为 10，使用的认证算法为 SHA1。Switch B 使用缺省的 IKE 提议。
- 使用预共享密钥的认证方法。

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



说明

请保证 Switch A 与 Switch B 之间路由可达。

(1) 配置安全网关 Switch A

配置 Vlan-interface1 的 IP 地址。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-vlan-interface1] ip address 1.1.1.1 255.255.255.0
[SwitchA-vlan-interface1] quit
```

配置 ACL 3101，定义由 Switch A 去 Switch B 的数据流。

```
[SwitchA] acl number 3101
[SwitchA-acl-adv-3101] rule 0 permit ip source 1.1.1.1 0 destination 2.2.2.2 0
[SwitchA-acl-adv-3101] rule 1 permit ip source 2.2.2.2 0 destination 1.1.1.1 0
[SwitchA-acl-adv-3101] quit
```

配置安全提议 tran1。

```
[SwitchA] ipsec proposal tran1
# 报文封装形式采用隧道模式。
[SwitchA-ipsec-proposal-tran1] encapsulation-mode tunnel
# 安全协议采用 ESP 协议。
[SwitchA-ipsec-proposal-tran1] transform esp
# 选择 ESP 协议采用的加密算法和认证算法。
[SwitchA-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchA-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchA-ipsec-proposal-tran1] quit
```

创建一条 IKE 提议 10。

```

[SwitchA] ike proposal 10
# 指定 IKE 提议使用的认证算法为 SHA1。
[SwitchA-ike-proposal-10] authentication-algorithm sha
# 使用预共享密钥认证方法。
[SwitchA-ike-proposal-10] authentication-method pre-share
# 配置 ISAKMP SA 的存活时间为 5000 秒。
[SwitchA-ike-proposal-10] sa duration 5000
[SwitchA-ike-proposal-10] quit
# 创建 IKE 对等体。
[SwitchA] ike peer peer
# 配置 IKE 对等体引用 IKE 安全提议 10。
[SwitchA-ike-peer-peer] proposal 10
# 配置预共享密钥。
[SwitchA-ike-peer-peer] pre-shared-key Ab12<><>
# 配置对端安全网关的 IP 地址。
[SwitchA-ike-peer-peer] remote-address 2.2.2.2
[SwitchA-ike-peer-peer] quit
# 创建一条安全策略，协商方式为 isakmp。
[SwitchA] ipsec policy map1 10 isakmp
# 引用安全提议。
[SwitchA-ipsec-policy-isakmp-map1-10] proposal tran1
# 引用访问控制列表。
[SwitchA-ipsec-policy-isakmp-map1-10] security acl 3101
# 引用 IKE 对等体。
[SwitchA-ipsec-policy-isakmp-map1-10] ike-peer peer
[SwitchA-ipsec-policy-isakmp-map1-10] quit
# 在 Vlan-interface1 上应用安全策略组。
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ipsec policy map1
(2) 配置安全网关 Switch B

```

```

# 配置 Vlan-interface1 的 IP 地址。
<SwitchB> system-view
[SwitchB] interface Vlan-interface1
[SwitchB-Vlan-interface1] ip address 2.2.2.2 255.255.255.0
[SwitchB-Vlan-interface1] quit
# 配置 ACL 3101，定义由 Switch B 去 Switch A 的数据流。
[SwitchB] acl number 3101
[SwitchB-acl-adv-3101] rule 0 permit ip source 2.2.2.2 0 destination 1.1.1.0 0
[SwitchB-acl-adv-3101] rule 1 permit ip source 1.1.1.1 0 destination 2.2.2.2 0
[SwitchB-acl-adv-3101] quit
# 创建安全提议 tran1。
[SwitchB] ipsec proposal tran1
# 报文封装形式采用隧道模式。
[SwitchB-ipsec-proposal-tran1] encapsulation-mode tunnel

```

```

# 安全协议采用 ESP 协议。
[SwitchB-ipsec-proposal-tran1] transform esp
# 选择 ESP 协议采用的加密算法和认证算法。
[SwitchB-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchB-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchB-ipsec-proposal-tran1] quit
# 创建一条 IKE 提议 10。
[SwitchB] ike proposal 10
# 指定 IKE 提议使用的认证算法为 SHA1。
[SwitchB-ike-proposal-10] authentication-algorithm sha
# 使用预共享密钥认证方法。
[SwitchB-ike-proposal-10] authentication-method pre-share
# 配置 ISAKMP SA 的存活时间为 5000 秒。
[SwitchB-ike-proposal-10] sa duration 5000
[SwitchB-ike-proposal-10] quit
# 创建 IKE 对等体。
[SwitchB] ike peer peer
# 配置 IKE 对等体引用 IKE 安全提议 10。
[SwitchB-ike-peer-peer] proposal 10
# 配置预共享密钥。
[SwitchB-ike-peer-peer] pre-shared-key Ab12<><>
# 配置对端安全网关的 IP 地址。
[SwitchB-ike-peer-peer] remote-address 1.1.1.1
[SwitchB-ike-peer-peer] quit
# 创建一条安全策略，协商方式为 isakmp。
[SwitchB] ipsec policy use1 10 isakmp
# 引用安全提议。
[SwitchB-ipsec-policy-isakmp-use1-10] proposal tran1
# 引用访问控制列表。
[SwitchB-ipsec-policy-isakmp-use1-10] security acl 3101
# 引用 IKE 对等体。
[SwitchB-ipsec-policy-isakmp-use1-10] ike-peer peer
[SwitchB-ipsec-policy-isakmp-use1-10] quit
# 在 Vlan-interface1 上应用安全策略组。
[SwitchB] interface Vlan-interface1
[SwitchB-Vlan-interface1] ipsec policy use1

```

4. 验证配置结果

以上配置完成后，Switch A 和 Switch B 之间如果有报文发送，将触发 IKE 协商。在进行 IKE 提议匹配的时候，从优先级最高的提议开始匹配，在进行提议匹配的时候，存活时间是不用进行匹配的，它由 IKE 协商双方决定。

2.12 常见错误配置举例

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

```
<Switch> debugging ike error
```

2.12.1 非法用户身份信息

1. 故障现象

非法用户身份信息

2. 故障分析

用户身份信息是发起 IPsec 通信的用户用来标识自己的数据。在实际应用中我们可以通过用户身份标识实现对不同的数据流建立不同的安全隧道进行保护。目前我们是通过用户的 IP 地址和名字来标识用户。

可以看到调试信息：

```
got NOTIFY of type INVALID_ID_INFORMATION
```

或者

```
drop message from A.B.C.D due to notification type INVALID_ID_INFORMATION
```

3. 处理过程

检查协商两端接口上配置的安全策略中的 ACL 内容是否相容。建议用户将两端的 ACL 配置成互为镜像的。ACL 镜像的含义请参考 IPsec 配置中“配置访问控制列表”内容。

2.12.2 提议不匹配

1. 故障现象

提议不匹配

2. 故障分析

可以看到调试信息：

```
got NOTIFY of type NO_PROPOSAL_CHOSEN
```

或者：

```
drop message from A.B.C.D due to notification type NO_PROPOSAL_CHOSEN
```

协商双方没有可以匹配的提议。

3. 处理过程

对于阶段 1，检查 IKE proposal 是否有与对方匹配的。对于阶段 2 协商，检查双方接口上应用的 IPsec 安全策略的参数是否匹配，引用的 IPsec 安全提议的协议、加密算法和认证算法是否有匹配的。

2.12.3 无法建立安全隧道

1. 故障现象

无法建立安全隧道

2. 故障分析

实际应用中有时会发现在不稳定的网络状态下，安全隧道无法建立或者存在安全隧道却无法通信，而且检查双方的 ACL 的配置正确，也有匹配的提议。

这种情况一般是安全隧道建立好以后，有一方的设备重启造成的。

3. 处理过程

- 使用 **display ike sa** 命令检查双方是否都已建立阶段 1 的 SA。
- 使用 **display ipsec sa policy** 命令查看接口上的安全策略是否已建立了 IPsec SA。
- 根据以上两步的结果查看，如果有一方存在的 SA 在另一方上不存在，请先使用 **reset ipsec sa** 命令清除双方不对称存在的 IPsec SA，再使用 **reset ike sa** 命令清除双方不对称存在的 IKE SA，并重新发起协商。

2.12.4 ACL配置错误

1. 故障现象

ACL 配置错误，导致协商成功之后数据流不通

2. 故障分析

多台设备之间先后建立不同的安全隧道，出现同一设备有不同对端的情况。若此设备不配置 ACL 规则，则分别由对端发起报文来与之建立保护粒度不同的安全隧道。由于安全隧道的优先级由它们创建的顺序决定，当这一设备的出方向报文首先匹配到较粗粒度的安全隧道时，将导致此设备无法与其它较细粒度对端互通。

3. 处理过程

为避免这种情况发生，当同一设备有不同对端时，建议用户在此设备上配置 ACL 来区别数据流，且与不同对端尽量避免配置有重复范围的 ACL 子规则。若需要有重复范围的子规则，应该将细粒度的子规则配置为较高的优先级。

目 录

1 SSH2.0 配置	1-1
1.1 SSH2.0 简介	1-1
1.1.1 概述	1-1
1.1.2 SSH工作过程	1-1
1.1.3 SSH支持VPN多实例	1-4
1.2 配置设备作为SSH服务器	1-4
1.2.1 SSH服务器配置任务简介	1-4
1.2.2 生成DSA或RSA密钥	1-5
1.2.3 使能SSH服务器功能	1-5
1.2.4 配置SSH客户端登录时的用户界面	1-6
1.2.5 配置客户端的公钥	1-7
1.2.6 配置SSH用户并指定服务类型和认证方式	1-8
1.2.7 配置服务器上的SSH管理功能	1-9
1.2.8 配置SSH服务器发送报文的DSCP优先级	1-10
1.3 配置设备作为SSH客户端	1-11
1.3.1 SSH客户端配置任务简介	1-11
1.3.2 为SSH客户端指定源IP地址或源接口	1-11
1.3.3 配置SSH客户端是否支持首次认证	1-11
1.3.4 建立SSH客户端和服务器的连接	1-13
1.3.5 配置SSH客户端发送报文的DSCP优先级	1-13
1.4 SSH协议显示和维护	1-14
1.5 设备作为SSH服务器配置举例	1-15
1.5.1 password认证配置举例	1-15
1.5.2 publickey认证配置举例	1-17
1.6 设备作为SSH客户端配置举例	1-22
1.6.1 password认证配置举例	1-22
1.6.2 publickey认证配置举例	1-25
2 SFTP配置	2-1
2.1 SFTP简介	2-1
2.2 配置设备作为SFTP服务器	2-1
2.2.1 配置准备	2-1
2.2.2 启动SFTP服务器	2-1

2.2.3 配置SFTP用户连接的空闲超时时间	2-2
2.3 配置设备作为SFTP客户端	2-2
2.3.1 为SFTP客户端指定源IP地址或源接口	2-2
2.3.2 建立与SFTP服务器的连接	2-3
2.3.3 SFTP目录操作	2-3
2.3.4 SFTP文件操作	2-4
2.3.5 显示帮助信息	2-4
2.3.6 终止与远程SFTP服务器的连接	2-5
2.3.7 配置SFTP客户端发送报文的DSCP优先级	2-5
2.4 设备作为SFTP客户端配置举例	2-6
2.5 设备作为SFTP服务器配置举例	2-9
3 SCP配置	3-1
3.1 SCP简介	3-1
3.2 配置设备作为SCP服务器	3-1
3.3 配置设备作为SCP客户端	3-1
3.4 SCP服务典型配置举例	3-2
3.4.1 设备作为SCP客户端配置举例	3-2
3.4.2 设备作为SCP服务器配置举例	3-3

1 SSH2.0 配置



说明

- 设备运行于 FIPS 模式时，本特性的部分配置相对于非 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”。
- 本章中典型配置举例中的配置，如无特殊说明，均以设备运行在非 FIPS 模式下的命令行为准。

1.1 SSH2.0简介

1.1.1 概述

SSH 是 Secure Shell（安全外壳）的简称。用户通过一个不能保证安全的网络环境远程登录到设备时，SSH 可以利用加密和强大的认证功能提供安全保障，保护设备不受诸如 IP 地址欺诈、明文密码截取等攻击。

设备支持 SSH 服务器功能，可以接受多个 SSH 客户端的连接。同时，设备还支持 SSH 客户端功能，允许用户与支持 SSH 服务器功能的设备建立 SSH 连接，从而实现从本地设备通过 SSH 登录到远程设备上。



说明

- 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，仅支持 SSH2 版本；设备作为 SSH 客户端时，只支持 SSH2 版本。
- 如无特殊说明，文中的 SSH 均指 SSH2。

1.1.2 SSH工作过程

在整个通讯过程中，为实现 SSH 的安全连接，服务器端与客户端要经历如下五个阶段：

表1-1 SSH 服务器端与客户端建立连接的五个阶段

阶段	说明	详细内容
版本号协商阶段	SSH目前包括SSH1和SSH2两个版本，双方通过版本协商确定使用的版本	1.1.1 1.
密钥和算法协商阶段	SSH支持多种算法，双方根据本端和对端支持的算法，协商出最终使用的算法，并通过DH交换，生成相同的会话密钥和会话ID	1.1.2 2.
认证阶段	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	1.1.2 3.
会话请求阶段	认证通过后，SSH客户端向服务器端发送会话请求	1.1.2 4.

阶段	说明	详细内容
交互会话阶段	会话请求通过后，SSH服务器端和客户端进行信息的交互	1.1.2 5.

1. 版本号协商阶段

具体步骤如下：

- (1) 服务器打开端口 22，等待客户端连接。
- (2) 客户端向服务器端发起 TCP 初始连接请求。
- (3) TCP 连接建立后，服务器向客户端发送第一个报文，包括版本标志字符串，格式为“SSH-<主协议版本号>.<次协议版本号>.<软件版本号>”，协议版本号由主版本号和次版本号组成，软件版本号主要是为调试使用。
- (4) 客户端收到报文后，首先解析该数据包，通过与服务器端的协议版本号进行对比，决定要使用的协议版本号。如果服务器端的协议版本号比自己的低，且客户端能支持服务器端的低版本，就使用服务器端的低版本协议号，否则使用自己的协议版本号。然后，客户端回应服务器一个报文，包含了客户端决定使用的协议版本号。
- (5) 服务器比较客户端发来的版本号，如果服务器支持该版本，则使用该版本，并进入密钥和算法协商阶段，否则，版本协商失败，服务器端断开 TCP 连接。



说明

上述报文都是采用明文方式传输的。

2. 密钥和算法协商阶段

具体步骤如下：

- (1) 服务器端和客户端分别发送算法协商报文给对端，报文中包含自己支持的公钥算法列表、加密算法列表、MAC（Message Authentication Code，消息验证码）算法列表、压缩算法列表等。
- (2) 服务器端和客户端根据对端和本端支持的算法列表得出最终使用的算法。任何一种算法协商失败，都会导致服务器端和客户端的算法协商过程失败，服务器将断开与客户端的连接。
- (3) 服务器端和客户端利用 DH 交换（Diffie-Hellman Exchange）算法、主机密钥对等参数，生成会话密钥和会话 ID，并完成客户端对服务器身份的验证。

通过以上步骤，服务器端和客户端就取得了相同的会话密钥和会话 ID。对于后续传输的数据，两端都会使用会话密钥进行加密和解密，保证了数据传送的安全。会话 ID 用来标识一个 SSH 连接，在认证阶段，会话 ID 还会用于两端的认证过程。



注意

在密钥和算法协商阶段之前，服务器端需要生成 DSA 或 RSA 密钥对，他们不仅用于生成会话密钥和会话 ID，还用于客户端验证服务器身份。DSA 和 RSA 密钥对的详细介绍请参见“安全配置指导”中的“公钥管理”。

3. 认证阶段

SSH 提供两种认证方法：

- **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；服务器将该信息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。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信息。
- **publickey 认证**：采用数字签名的方法来认证客户端。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。

对于 SSH2，除了上述两种认证方法外，还提供了 **password-publickey** 认证和 **any** 认证：

- **password-publickey 认证**：指定客户端版本为 SSH2 的用户认证方式为必须同时进行 **password** 和 **publickey** 两种认证；客户端版本为 SSH1 的用户认证方式为只要进行其中一种认证即可。
- **any 认证**：不指定用户的认证方式，用户既可以采用 **password** 认证，也可以采用 **publickey** 认证。

认证阶段的具体步骤如下：

- 客户端向服务器端发送认证请求，认证请求中包含用户名、认证方法（**password** 认证或 **publickey** 认证）、与该认证方法相关的内容（如：**password** 认证时，内容为密码）。
- 服务器端对客户端进行认证，如果认证失败，则向客户端发送认证失败消息，其中包含可以再次认证的方法列表。
- 客户端从认证方法列表中选取一种认证方法再次进行认证。
- 该过程反复进行，直到认证成功或者认证次数达到上限，服务器关闭连接为止。



说明

设备作为 SSH 服务器发起的二次密码认证，仅 SSH2 及以后版本的 SSH 客户端才能支持。

4. 会话请求阶段

认证通过后，客户端向服务器发送会话请求。服务器等待并处理客户端的请求。请求被成功处理后，服务器会向客户端回应 **SSH_MSG_SUCCESS** 包，SSH 进入交互会话阶段；否则回应 **SSH_MSG_FAILURE** 包，表示服务器处理请求失败或者不能识别请求。

5. 交互会话阶段

会话请求成功后，连接进入交互会话阶段。在这个阶段，数据被双向传送。客户端将要执行的命令加密后传给服务器，服务器接收到报文，解密后执行该命令，将执行的结果加密发送给客户端，客户端将接收到的结果解密后显示到终端上。



说明

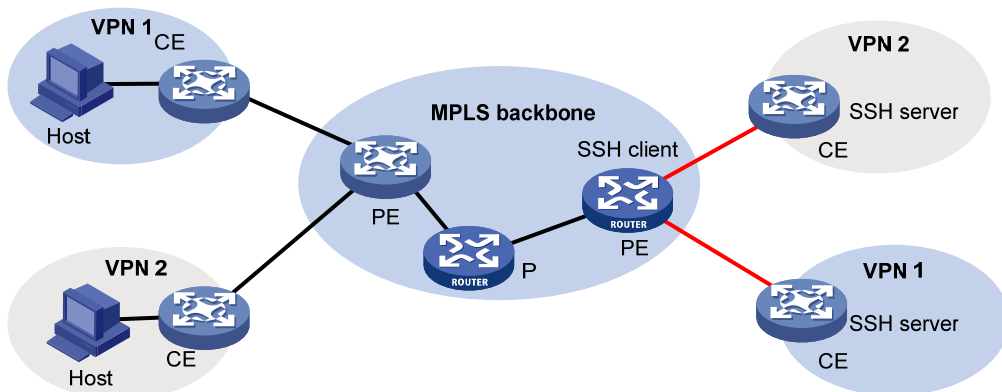
- 交互会话阶段,用户在客户端可以通过粘贴文本会话的方式执行命令,但文本会话不能超过 2000 字节,且粘贴的命令最好是同一视图下的命令,否则服务器可能无法正确执行该命令。
- 如果粘贴的文本会话超过 2000 字节,可以采用将配置文件通过 SFTP (Secure FTP, 安全的 FTP) 方式上传到服务器,利用新的配置文件重新启动的方式执行这些命令。

1.1.3 SSH支持VPN多实例

通过 SSH 连接支持 VPN 多实例功能,可实现设备作为 SSH 客户端时,与位于 MPLS VPN 中的 SSH 服务器之间建立连接。

如下图所示,私网 VPN 1 和 VPN 2 中的用户通过 PE 接入 MPLS 骨干网,各 VPN 之间的业务相互隔离。在 PE 设备上开启 SSH 客户端功能后,通过 MPLS VPN 功能和 SSH 连接支持 VPN 多实例功能,可以对各 VPN 中开启 SSH 服务器功能的 CE 设备进行访问,实现从 PE 设备到 CE 设备的安全登录和日志文件传输等功能。

图1-1 SSH 支持 VPN 多实例组网应用图



1.2 配置设备作为SSH服务器

1.2.1 SSH服务器配置任务简介

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DSA或RSA密钥	可选	1.2.2
使能SSH服务器功能	必选	1.2.3
配置SSH客户端登录时的用户界面	必选	1.2.4

配置任务	说明	详细配置
配置客户端的公钥	对于采用publickey认证的SSH用户为必选 对于采用password认证的SSH用户为可选	1.2.5
配置SSH用户并指定服务类型和认证方式	可选	1.2.6
配置服务器上的SSH管理功能	可选	1.2.7
配置SSH服务器发送报文的DSCP优先级	可选	1.2.8

1.2.2 生成DSA或RSA密钥

服务器端的 DSA 或 RSA 密钥对，用于在密钥和算法协商阶段生成会话密钥和会话 ID，以及客户端认证服务器。

表1-3 生成 DSA 或 RSA 密钥

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 }	必选 缺省情况下，不存在任何DSA和RSA密钥对



说明

- **public-key local create** 命令的详细介绍请参见“安全命令参考”中的“公钥管理”。
- SSH 用户登录设备时，若设备未配置本地 DSA 或 RSA 密钥，可以自动生成 RSA 密钥对。
- 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，建议在服务器上生成 DSA 和 RSA 两种密钥对。
- 通过 **public-key local create rsa** 命令生成 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，二者都包括一个公钥和一个私钥。SSH1 中利用 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 中通过 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。
- 通过 **public-key local create dsa** 命令生成 DSA 密钥对时，只生成一个主机密钥对。SSH1 中不支持 DSA 算法。

1.2.3 使能SSH服务器功能

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	-

操作	命令	说明
使能SSH服务器功能	ssh server enable	必选 缺省情况下，SSH服务器功能处于关闭状态



设备作为 SCP 服务器时，同一时间只允许有一个 SCP 用户访问 SCP 服务器。

1.2.4 配置SSH客户端登录时的用户界面

SSH 客户端通过 VTY 用户界面访问设备。因此，需要配置 SSH 客户端登录时采用的 VTY 用户界面，使其支持 SSH 远程登录协议。配置结果在客户端下次请求登录时生效。

表1-5 配置 SSH 客户端登录时的用户界面

操作	命令	说明
进入系统视图	system-view	-
进入一个或多个VTY用户界面视图	user-interface vty number [<i>ending-number</i>]	-
配置登录用户界面的认证方式为 scheme 方式	authentication-mode scheme	必选 缺省情况下，用户界面认证为 password 方式
配置所在用户界面支持SSH协议	protocol inbound { all ssh }	可选 缺省情况下，系统支持所有的协议，即支持Telnet和SSH



- **authentication-mode** 命令和 **protocol inbound** 命令的详细介绍，请参见“基础配置命令参考”中的“登录设备”。
- 如果在该用户界面上配置支持的协议是 SSH，为确保配置成功，请务必配置登录用户界面的认证方式为 **authentication-mode scheme**（采用 AAA 认证）。
- 如果某用户界面已经配置成支持 SSH 协议，则无法更改用户界面的认证方式，除非先取消用户界面支持 SSH 协议。

1.2.5 配置客户端的公钥



说明

本配置适用于采用 **publickey** 认证的 SSH 用户，采用 **password** 认证的 SSH 用户，不必进行本配置。

如果 SSH 用户采用 **publickey** 认证方式登录服务器，则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，以便服务器端采用数字签名对客户端进行验证。

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：

- 手工配置客户端的公钥：采用手工输入或拷贝粘贴的方式将客户端的公钥配置到服务器上。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。
- 从公钥文件中导入客户端的公钥：自动将客户端公钥文件中的客户端公钥转换为 PKCS（Public Key Cryptography Standards，公共密钥加密标准）编码的形式导入到服务器上。这种方式需要事先将客户端的公钥文件通过 FTP/TFTP 以二进制（binary）方式传输到服务器上。



说明

建议选用从公钥文件导入的方式配置客户端公钥。

表1-6 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 <i>keyname</i>	-
进入公钥编辑视图	public-key-code begin	-
配置客户端的公钥	直接输入公钥内容	必选 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
退回公钥视图，并保存配置的主机公钥	public-key-code end	- 退出公钥编辑视图时，系统自动保存配置的公钥密钥
退回系统视图	peer-public-key end	-

表1-7 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SSH用户的公钥	public-key peer keyname import sshkey filename	必选



说明

关于客户端的公钥的配置介绍，请参见“安全配置指导”中的“公钥管理”。

1.2.6 配置SSH用户并指定服务类型和认证方式



说明

- 对于使用 **publickey** 认证方式登录设备的用户，必须在设备上创建相应的 SSH 用户、并指定服务器类型、认证方式以及客户端的公钥。
- 对于使用 **password** 认证方式登录设备的用户，用户的账号信息配置在设备或者远程认证服务器（如 RADIUS 服务器）上（前者适用于本地认证，后者适用于远程认证），并不要求在设备上通过本配置创建相应的 SSH 用户。如果创建了相应的 SSH 用户，则必须保证该服务类型以及认证方式正确。关于本地及远程认证的相关配置请参见“安全配置指导”中的“AAA”。

通过本配置，可以在创建 SSH 用户的同时，指定 SSH 用户的服务类型和认证方式：

- 服务类型：**Stelnet**、**SFTP**和**SCP**。**Stelnet**即Secure Telnet，安全的Telnet服务，详细内容请参见“[2.1 SFTP简介](#)”；**SCP**详细内容请参见“[3.1 SCP简介](#)”。
- 认证方式：**password** 认证、**publickey** 认证、**password-publickey** 认证、**any** 认证。

表1-8 配置 SSH 用户并指定服务类型和认证方式

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	SSH用户的服务 类型为 stelnet 非FIPS模式下： ssh user username service-type stelnet authentication-type { password { any password-publickey publickey } assign publickey keyname } FIPS模式下： ssh user username service-type stelnet authentication-type { password password-publickey assign publickey keyname }	二者必选其一

操作	命令	说明
SSH用户的服务类型为 all 、 scp 或 sftp	非FIPS模式下： ssh user username service-type { all scp sftp } authentication-type { password { any password-publickey publickey } assign publickey keyname work-directory directory-name } FIPS模式下： ssh user username service-type { all scp sftp } authentication-type { password password-publickey assign publickey keyname work-directory directory-name }	



注意

- 对于 AAA 用户，即使没有创建对应的 SSH 用户，只要能够通过 AAA 认证，且设置的服务类型为 SSH，则该用户仍然可以通过 password 认证方式登录服务器。
- SSH1 不支持服务类型 **scp** 与 **sftp**。如果客户端采用 SSH1 版本登录服务器，则必须在服务器上配置服务类型为 **stelnet** 或者 **all**。否则，客户端无法登录服务器。
- SCP 与 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。只采用 **publickey** 认证方式的用户，使用的工作目录为通过 **ssh user** 命令为该用户设置的工作目录；只采用 **password** 认证方式的用户，使用的工作目录为通过 AAA 授权的工作目录；同时采用 **publickey** 和 **password** 两种认证方式的用户，使用的工作目录为通过 **ssh user** 命令为该用户设置的工作目录。
- 配置的认证方式和用户公钥，对于已经登录的 SSH 用户不会生效，只在 SSH 用户下次登录时生效。



说明

- FIPS 模式下，SSH 服务器不支持 any 认证或 **publickey** 认证方式。
- 仅使用 **publickey** 认证方式的用户登录服务器后，可以访问的命令级别为在用户界面上通过 **user privilege level** 命令配置的级别。
- 使用 **password** 认证方式的用户登录服务器后，用户可以访问的命令级别由 AAA 来授权。

1.2.7 配置服务器上的SSH管理功能

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
- 设置 SSH 用户认证的超时时间
- 设置 SSH 用户请求连接的认证尝试次数

通过定时更新服务器密钥以及对用户认证时间、认证次数的限制，可以防止恶意地对密钥和用户名的猜测和破解，从而提高了 SSH 连接的安全性。

表1-9 配置服务器上的 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]	可选 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	可选 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	可选 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	可选 缺省情况下，SSH连接认证尝试的最大次数为3次



说明

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 **ssh server authentication-retries** 命令配置的 SSH 连接认证尝试次数，否则，客户端认证失败，无法登录 SSH 服务器。

1.2.8 配置SSH服务器发送报文的DSCP优先级

在 IPv4 和 IPv6 报文头中，包含一个 8bit 的字段，用于标识 IP 报文的的服务类型。在 IPv4 报文中，这个字段称为 ToS 字段；在 IPv6 报文中，称为 Traffic class 字段。RFC 2474 对这 8 个 bit 进行了定义，将前 6 个 bit 定义为 DSCP 优先级，最后 2 个 bit 作为保留位。在报文传输的过程中，DSCP 优先级可以被网络设备识别，并作为报文传输优先程度的参考。

用户可以对 SSH 服务器发送报文的 DSCP 优先级进行配置。

表1-10 配置 SSH 服务器发送报文的 DSCP 优先级

操作	命令	说明
进入系统视图	system-view	-
配置SSH服务器发送Pv4报文的DSCP优先级	ssh server dscp dscp-value	可选 缺省情况下，SSH服务器发送Pv4报文的DSCP优先级为16

操作	命令	说明
配置SSH服务器发送IPv6报文的DSCP优先级	ssh server ipv6 dscp dscp-value	可选 缺省情况下，SSH服务器发送IPv6报文的DSCP优先级为0

1.3 配置设备作为SSH客户端

1.3.1 SSH客户端配置任务简介

表1-11 SSH 客户端配置任务简介

配置任务	说明	详细配置
为SSH客户端指定源IP地址或源接口	可选	1.3.2
配置SSH客户端是否支持首次认证	可选	1.3.3
建立SSH客户端和服务端端的连接	必选	1.3.4
配置SSH客户端发送报文的DSCP优先级	可选	1.3.5

1.3.2 为SSH客户端指定源IP地址或源接口

用户可以通过以下配置，为 SSH 客户端指定源 IP 地址或者源接口，这样客户端可以用指定的 IP 地址或接口地址访问 SSH 服务器，增加了业务的可管理性。

表1-12 为 SSH 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SSH客户端指定源IP地址或源接口	为SSH客户端指定源IPv4地址或源接口 ssh 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SSH服务器
	为SSH客户端指定源IPv6地址或源接口 ssh client ipv6 source { ipv6 ipv6-address interface interface-type interface-number }	

1.3.3 配置SSH客户端是否支持首次认证

当设备作为 SSH 客户端和服务端连接时，可以设置 SSH 客户端对访问的 SSH 服务器是否进行首次认证。

- 如果支持首次认证，则当 SSH 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。

- 如果不支持首次认证，则当客户端没有配置服务器端的主机公钥时，客户端将拒绝访问该服务器。用户必须事先将要访问的服务器端的主机公钥配置在本地，同时指定要连接的服务器端的主机公钥名称，以便客户端对连接的服务器进行认证。

1. 配置SSH客户端支持首次认证

表1-13 配置 SSH 客户端支持首次认证

操作	命令	说明
进入系统视图	system-view	-
设置SSH客户端对访问的SSH服务器进行首次认证	ssh client first-time [enable]	可选 缺省情况下，客户端进行首次认证

2. 配置SSH客户端不支持首次认证

如果配置 SSH 客户端不支持首次认证，则需要在客户端配置服务器端的主机公钥，并为要连接的服务器指定主机公钥名称，

表1-14 配置 SSH 客户端不支持首次认证

操作	命令	说明
进入系统视图	system-view	-
设置SSH客户端对访问的SSH服务器不进行首次认证	undo ssh client first-time	必选 缺省情况下，客户端进行首次认证
配置服务器端的主机公钥	请参见 “ 1.2.5 配置客户端的公钥 ”	必选 在客户端配置服务器端主机公钥的方法，与在服务器端配置客户端公钥的方法相同
在客户端上指定要连接的服务器端的主机公钥名称	ssh client authentication server server assign publickey keyname	必选

1.3.4 建立SSH客户端和服务端端的连接

表1-15 建立 SSH 客户端和服务端端的连接

操作	命令	说明
建立SSH客户端和IPv4服务器端的连接，并指定公钥算法、客户端和服务器的首选加密算法、首选HMAC算法和首选密钥交换算法	非FIPS模式下： <pre>ssh2 server [port-number] [vpn-instance vpn-instance-name] [identity-key { dsa rsa } prefer-ctos-cipher { 3des aes128 des } prefer-ctos-hmac { md5 md5-96 sha1 sha1-96 } prefer-kex { dh-group-exchange dh-group1 dh-group14 } prefer-stoc-cipher { 3des aes128 des } prefer-stoc-hmac { md5 md5-96 sha1 sha1-96 } } *</pre> FIPS模式下： <pre>ssh2 server [port-number] [vpn-instance vpn-instance-name] [identity-key rsa 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 } } *</pre>	二者必选其一 必须在用户视图下执行本命令
	非FIPS模式下： <pre>ssh2 ipv6 server [port-number] [vpn-instance vpn-instance-name] [identity-key { dsa rsa } prefer-ctos-cipher { 3des aes128 des } prefer-ctos-hmac { md5 md5-96 sha1 sha1-96 } prefer-kex { dh-group-exchange dh-group1 dh-group14 } prefer-stoc-cipher { 3des aes128 des } prefer-stoc-hmac { md5 md5-96 sha1 sha1-96 } } *</pre> FIPS模式下： <pre>ssh2 ipv6 server [port-number] [vpn-instance vpn-instance-name] [identity-key rsa 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 } } *</pre>	

1.3.5 配置SSH客户端发送报文的DSCP优先级

在 IPv4 和 IPv6 报文头中，包含一个 8bit 的字段，用于标识 IP 报文的服务类型。在 IPv4 报文中，这个字段称为 ToS 字段；在 IPv6 报文中，称为 Traffic class 字段。RFC 2474 对这 8 个 bit 进行了定义，将前 6 个 bit 定义为 DSCP 优先级，最后 2 个 bit 作为保留位。在报文传输的过程中，DSCP 优先级可以被网络设备识别，并作为报文传输优先程度的参考。

用户可以对 SSH 客户端发送报文的 DSCP 优先级进行配置。

表1-16 配置 SSH 客户端发送报文的 DSCP 优先级

操作	命令	说明
进入系统视图	system-view	-
配置SSH客户端发送IPv4报文的DSCP优先级	ssh client dscp dscp-value	可选 缺省情况下, SSH客户端发送IPv4报文的DSCP优先级为16
配置SSH客户端发送IPv6报文的DSCP优先级	ssh client ipv6 dscp dscp-value	可选 缺省情况下, SSH客户端发送IPv6报文的DSCP优先级为0

1.4 SSH协议显示和维护

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1-17 SSH 协议显示和维护

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 [{ begin exclude include } <i>regular-expression</i>]
显示当前为SSH客户端设置的源IP地址或者源接口	display ssh client source [{ begin exclude include } <i>regular-expression</i>]
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 { status session } [{ begin exclude include } <i>regular-expression</i>]
在SSH客户端显示客户端保存的服务器端的主机公钥和服务器的对应关系	display ssh server-info [{ begin exclude include } <i>regular-expression</i>]
在SSH服务器端显示SSH用户信息	display ssh user-information [<i>username</i>] [{ begin exclude include } <i>regular-expression</i>]
显示本地密钥对中的公钥部分	display public-key local { dsa rsa } public [{ begin exclude include } <i>regular-expression</i>]
显示保存在本地的远端主机的公钥信息	display public-key peer [brief name <i>publickey-name</i>] [{ begin exclude include } <i>regular-expression</i>]



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“公钥配置”。

1.5 设备作为SSH服务器配置举例

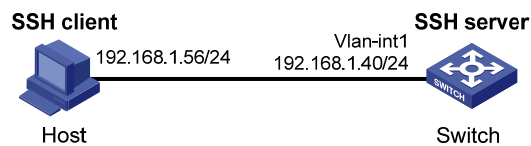
1.5.1 password认证配置举例

1. 组网需求

如 图 1-2，配置Host（SSH客户端）与Switch建立本地连接。Host采用SSH协议登录到Switch上，以保证数据信息交换的安全。SSH用户采用的认证方式为password认证，用户名和密码保存在Switch上。

2. 组网图

图1-2 SSH password 认证配置组网图



3. 配置步骤

(1) 配置 SSH 服务器

生成 RSA 密钥对。

```
<Switch> system-view
[Switch] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
+++++++
+++++++
+++++
+++++++
```

生成 DSA 密钥对。

```
[Switch] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
```

```
+++++++
+++++++
```

启动 SSH 服务器。

```
[Switch] ssh server enable
```

配置 VLAN 接口 1 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface1] quit
# 设置 SSH 客户端登录用户界面的认证方式为 AAA 认证。
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] authentication-mode scheme
# 设置 Switch 上远程用户登录协议为 SSH。
[Switch-ui-vty0-15] protocol inbound ssh
[Switch-ui-vty0-15] quit
# 创建本地用户 client001，并设置用户访问的命令级别为 3。
[Switch] local-user client001
[Switch-luser-client001] password simple aabbcc
[Switch-luser-client001] service-type ssh
[Switch-luser-client001] authorization-attribute level 3
[Switch-luser-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）
[Switch] ssh user client001 service-type stelnet authentication-type password
```

(2) SSH 客户端建立与 SSH 服务器的连接



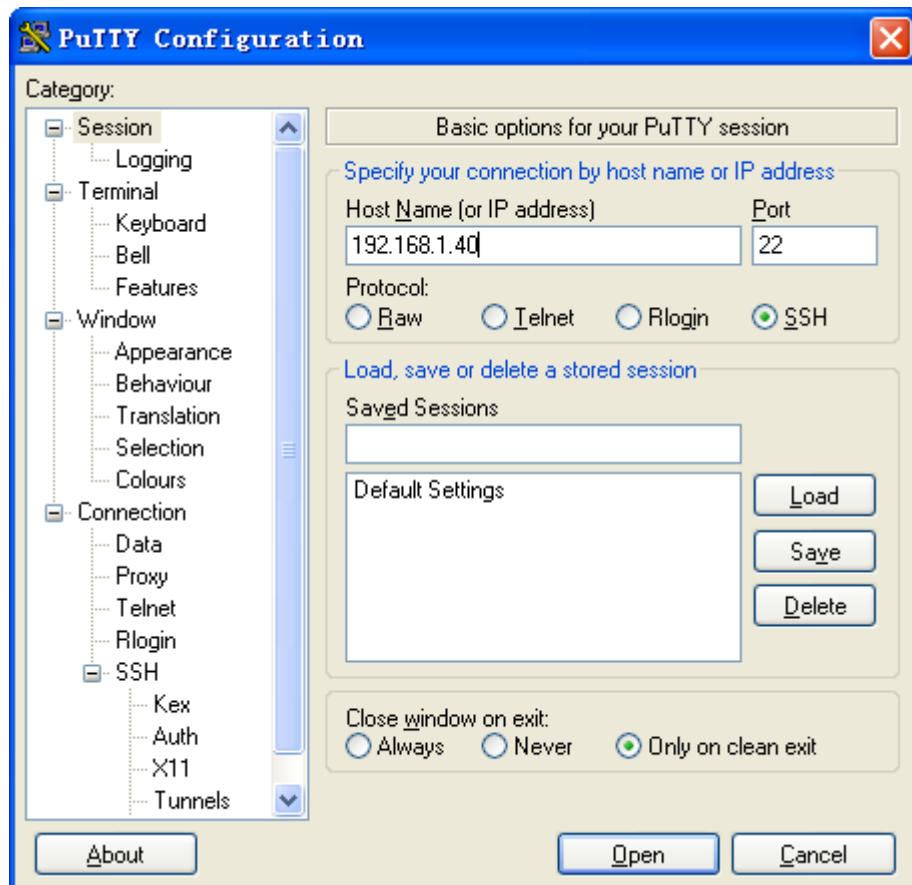
说明

SSH 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 SSH 客户端的配置方法。

建立与 SSH 服务器端的连接。

打开PuTTY.exe程序，出现如 [图 1-3](#) 所示的客户端配置界面。在“Host Name (or IP address)”文本框中输入SSH服务器的IP地址为 192.168.1.40。

图1-3 SSH 客户端配置界面（1）



在 图 1-3 中，单击<Open>按钮。按提示输入用户名client001 及密码aabbcc，即可进入Switch的配置界面。

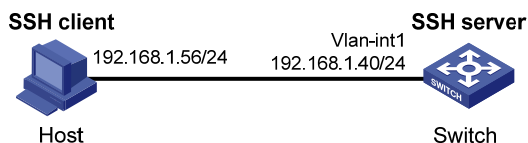
1.5.2 publickey认证配置举例

1. 组网需求

如 图 1-4，配置Host（SSH客户端）与Switch建立本地连接。Host采用SSH协议登录到Switch上，以保证数据信息交换的安全。SSH用户采用的认证方式为publickey认证，公钥算法为RSA。

2. 组网图

图1-4 SSH publickey 配置组网图



3. 配置步骤



说明

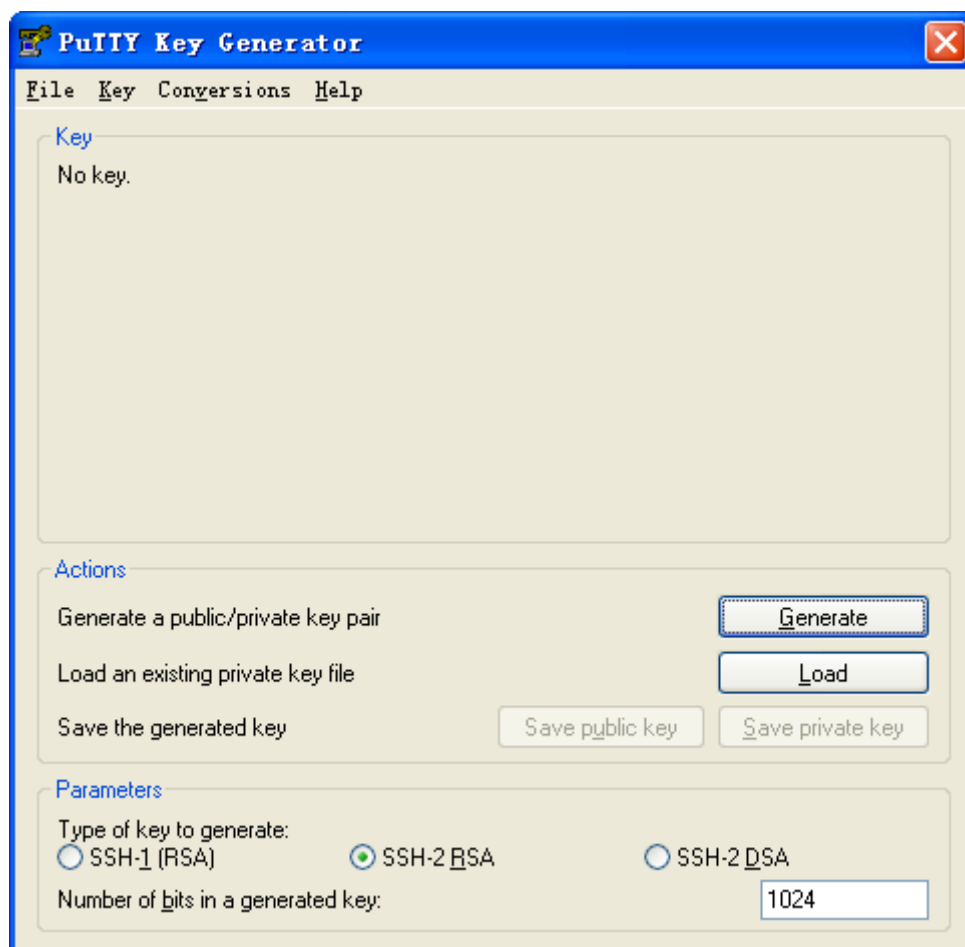
在服务器的配置过程中需要指定客户端的公钥信息，因此建议首先完成客户端密钥对的配置，再进行服务器的配置。

(1) 配置 SSH 客户端

生成 RSA 密钥对。

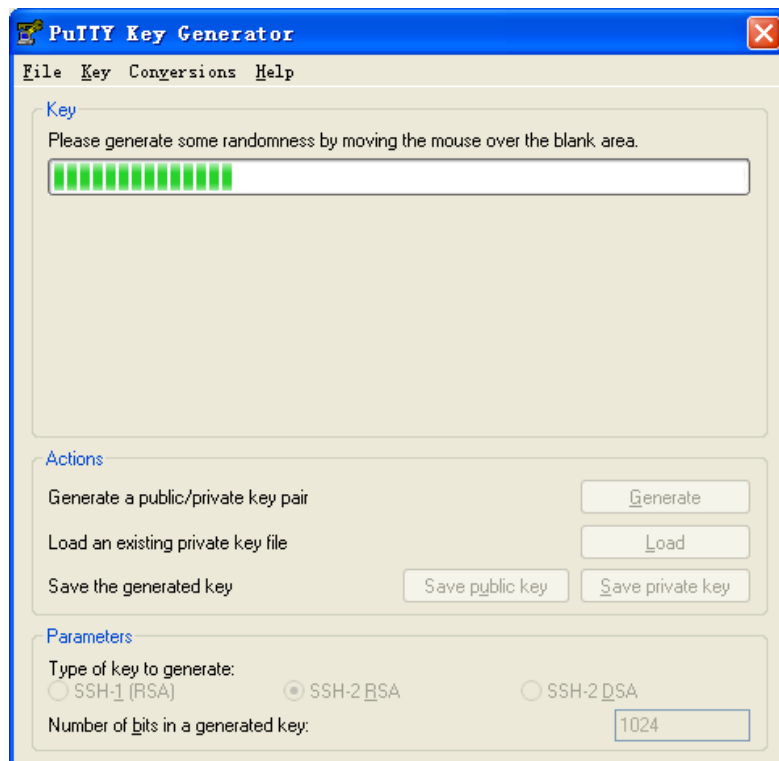
在客户端运行 PuTTYGen.exe，在参数栏中选择“SSH-2 RSA”，点击<Generate>，产生客户端密钥对。

图1-5 生成客户端密钥（1）



在产生密钥对的过程中需不停的移动鼠标，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 1-6](#)。

图1-6 生成客户端密钥（2）



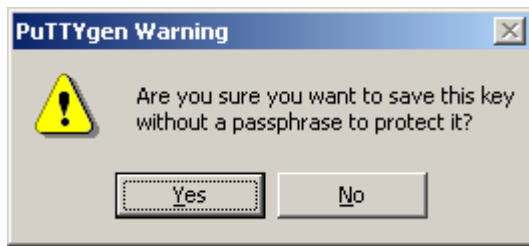
密钥对产生后，点击<Save public key>，输入存储公钥的文件名 key.pub，点击<保存>按钮。

图1-7 生成客户端密钥（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私钥，点击<Yes>，输入私钥文件名为 **private.ppk**，点击保存。

图1-8 生成客户端密钥（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。

(2) 配置 SSH 服务器

生成 RSA 密钥对。

```
<Switch> system-view
[Switch] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
```

```
+++++++
+++++
+++++
+++++
```

生成 DSA 密钥对。

```
[Switch] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
```

```
+++++
+++++
```

启动 SSH 服务器。

```
[Switch] ssh server enable
```

配置 VLAN 接口 1 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface1] quit
```

设置用户接口上认证模式为 AAA 认证。

```
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] authentication-mode scheme
```

设置 Switch 上远程用户登录协议为 SSH。

```
[Switch-ui-vty0-15] protocol inbound ssh
```

设置用户能访问的命令级别为 3。

```
[Switch-ui-vty0-15] user privilege level 3
```

```
[Switch-ui-vty0-15] quit
```

从文件 key.pub 中导入远端的公钥，并命名为 Switch001。

```
[Switch] public-key peer Switch001 import sshkey key.pub
```

设置 SSH 用户 client002 的认证方式为 publickey，并指定公钥为 Switch001。

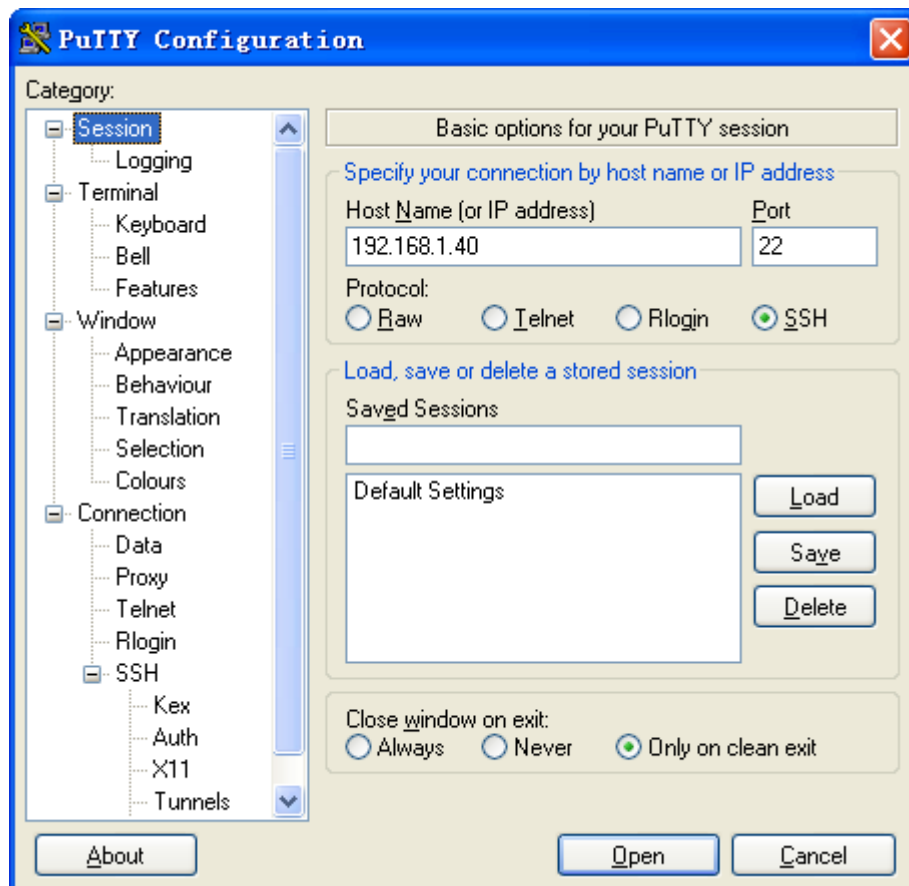
```
[Switch] ssh user client002 service-type stelnet authentication-type publickey assign  
publickey Switch001
```

(3) SSH 客户端建立与 SSH 服务器的连接

指定私钥文件，并建立与 SSH 服务器的连接。

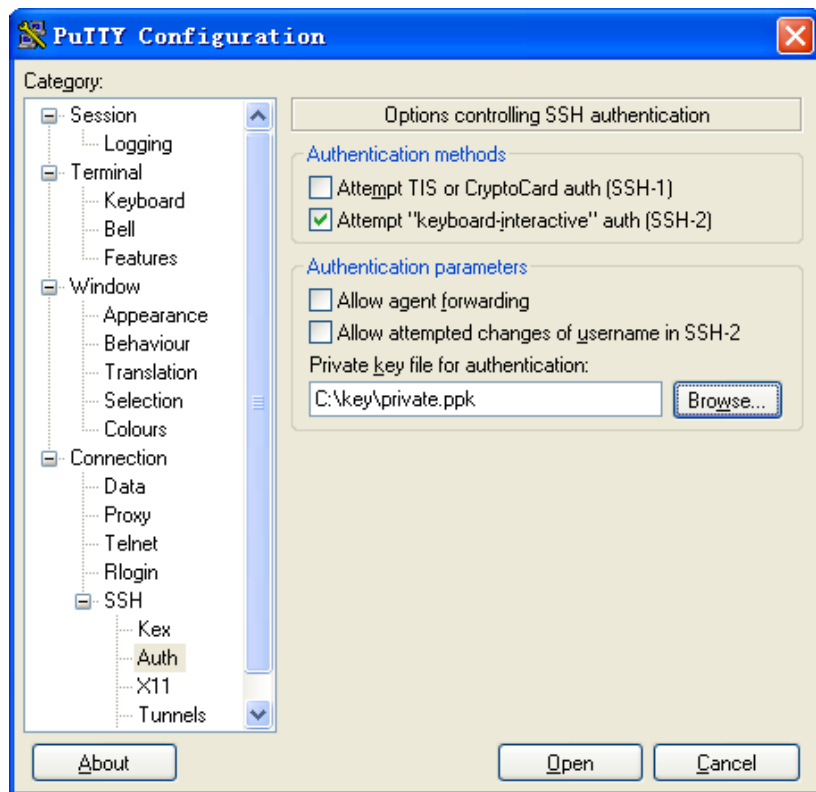
打开PuTTY.exe程序，出现如 图 1-9 所示的客户端配置界面。在“Host Name (or IP address)”文本框中输入SSH服务器的IP地址为 192.168.1.40。

图1-9 SSH 客户端配置界面（1）



单击左侧导航栏“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 SSH 客户端配置界面（2）



如 图 1-10，单击<Open>按钮。按提示输入用户名client002，即可进入Switch的配置界面。

1.6 设备作为SSH客户端配置举例

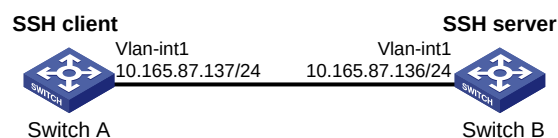
1.6.1 password认证配置举例

1. 组网需求

如 图 1-11，配置Switch A作为客户端，采用SSH协议登录到Switch B上。SSH用户采用的认证方式为password认证，用户名为client001，密码为aabbcc。

2. 组网图

图1-11 设备作为 SSH 客户端配置组网图



3. 配置步骤

(1) 配置 SSH 服务器

生成 RSA 密钥对。

```
<SwitchB> system-view
```

```

[SwitchB] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
+++++++
+++++++
+++++
+++++++
# 生成 DSA 密钥对。
[SwitchB] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
+++++++
+++++++
# 启动 SSH 服务器。
[SwitchB] ssh server enable
# 配置 VLAN 接口 1 的 IP 地址，客户端将通过该地址连接 SSH 服务器。
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[SwitchB-Vlan-interface1] quit
# 设置 SSH 客户端登录用户界面的认证方式为 AAA 认证。
[SwitchB] user-interface vty 0 15
[SwitchB-ui-vty0-15] authentication-mode scheme
# 设置 Switch B 上远程用户登录协议为 SSH。
[SwitchB-ui-vty0-15] protocol inbound ssh
[SwitchB-ui-vty0-15] quit
# 创建本地用户 client001。
[SwitchB] local-user client001
[SwitchB-luser-client001] password simple aabbcc
[SwitchB-luser-client001] service-type ssh
[SwitchB-luser-client001] authorization-attribute level 3
[SwitchB-luser-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）
[SwitchB] ssh user client001 service-type stelnet authentication-type password
(2) SSH 客户端建立与 SSH 服务器的连接
# 配置 VLAN 接口 1 的 IP 地址。
<SwitchA> system-view
[SwitchA] interface vlan-interface 1

```

```
[SwitchA-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[SwitchA-Vlan-interface1] quit
[SwitchA] quit
```

- 如果客户端支持首次认证，则可以直接与服务器建立连接。

建立到服务器 10.165.87.136 的 SSH 连接。

```
<SwitchA> ssh2 10.165.87.136
Username: client001
Trying 10.165.87.136 ...
Press CTRL+K to abort
Connected to 10.165.87.136 ...
```

```
The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
Enter password:
```

输入正确的密码之后，即可成功登录到 Switch B 上。

- 如果客户端不支持首次认证，则需要进行如下配置。

配置客户端对服务器不进行首次认证。

```
[SwitchA] undo ssh client first-time
```

在客户端配置 SSH 服务器端的主机公钥。在公钥编辑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。

```
[SwitchA] public-key peer key1
[SwitchA-pkey-public-key] public-key-code begin
[SwitchA-pkey-key-code]308201B73082012C06072A8648CE3804013082011F0281810
0D757262C4584C44C211F18BD96E5F0
[SwitchA-pkey-key-code]61C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE
65BE6C265854889DC1EDBD13EC8B274
[SwitchA-pkey-key-code]DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B0
6FD60FE01941DDD77FE6B12893DA76E
[SwitchA-pkey-key-code]EBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B3
68950387811C7DA33021500C773218C
[SwitchA-pkey-key-code]737EC8EE993B4F2DED30F48EDACE915F0281810082269009E
14EC474BAF2932E69D3B1F18517AD95
[SwitchA-pkey-key-code]94184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD35D02
492B3959EC6499625BC4FA5082E22C5
[SwitchA-pkey-key-code]B374E16DD00132CE71B020217091AC717B612391C76C1FB2E
88317C1BD8171D41ECB83E210C03CC9
[SwitchA-pkey-key-code]B32E810561C21621C73D6DAAC028F4B1585DA7F42519718CC
9B09EEF0381840002818000AF995917
[SwitchA-pkey-key-code]E1E570A3F6B1C2411948B3B4FFA256699B3BF871221CC9C5D
F257523777D033BEE77FC378145F2AD
[SwitchA-pkey-key-code]D716D7DB9FCABB4ADBF6FB4FDB0CA25C761B308EF53009F71
01F7C62621216D5A572C379A32AC290
[SwitchA-pkey-key-code]E55B394A217DA38B65B77F0185C8DB8095522D1EF044B465E
8716261214A5A3B493E866991113B2D
[SwitchA-pkey-key-code]485348
[SwitchA-pkey-key-code] public-key-code end
[SwitchA-pkey-public-key] peer-public-key end
```

```
# 指定服务器 10.165.87.136 对应的主机公钥名称为 key1。
[SwitchA] ssh client authentication server 10.165.87.136 assign publickey key1
[SwitchA] quit
# 建立到服务器 10.165.87.136 的 SSH 连接。
<SwitchA> ssh2 10.165.87.136
Username: client001
Trying 10.165.87.136
Press CTRL+K to abort
Connected to 10.165.87.136...
Enter password:
输入正确的密码之后，即可成功登录到 Switch B 上。
```

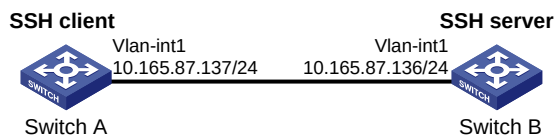
1.6.2 publickey认证配置举例

1. 组网需求

如 图 1-12，配置Switch A作为客户端，采用SSH协议登录到Switch B上。SSH用户采用的认证方式为publickey认证，公钥算法为DSA。

2. 组网图

图1-12 设备作为 SSH 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 SSH 客户端

配置 VLAN 接口 1 的 IP 地址。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

生成 DSA 密钥对。

```
[SwitchA] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
```



```

Input the bits of the modulus[default = 1024]:
Generating Keys...
+++++
+++++
# 将生成的 DSA 主机公钥导出到指定文件 key.pub 中。
[SwitchA] public-key local export dsa ssh2 key.pub
[SwitchA] 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。
(2) 配置 SSH 服务器
# 生成 RSA 密钥对。
<SwitchB> system-view
[SwitchB] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
+++++
+++++
+++++
+++++
# 生成 DSA 密钥对。
[SwitchB] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
+++++
+++++
# 启动 SSH 服务器。
[SwitchB] ssh server enable
# 配置 VLAN 接口 1 的 IP 地址，客户端将通过该地址连接 SSH 服务器。
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[SwitchB-Vlan-interface1] quit
# 设置 SSH 客户端登录用户界面的认证方式为 AAA 认证。
[SwitchB] user-interface vty 0 15
[SwitchB-ui-vty0-15] authentication-mode scheme
# 设置 Switch B 上远程用户登录协议为 SSH。
[SwitchB-ui-vty0-15] protocol inbound ssh
# 设置用户能访问的命令级别为 3。
[SwitchB-ui-vty0-15] user privilege level 3
[SwitchB-ui-vty0-15] quit

```

从文件 **key.pub** 中导入远端的公钥。

```
[SwitchB] public-key peer Switch001 import sshkey key.pub
```

设置 SSH 用户 **client002** 的认证方式为 **publickey**，并指定公钥为 **Switch001**。

```
[SwitchB] ssh user client002 service-type stelnet authentication-type publickey assign  
publickey Switch001
```

(3) SSH 客户端建立与 SSH 服务器的连接

建立到服务器 **10.165.87.136** 的 SSH 连接。

```
<SwitchA> ssh2 10.165.87.136
```

```
Username: client002
```

```
Trying 10.165.87.136 ...
```

```
Press CTRL+K to abort
```

```
Connected to 10.165.87.136 ...
```

```
The Server is not authenticated. Continue? [Y/N]:y
```

```
Do you want to save the server public key? [Y/N]:n
```

之后，用户就可成功登录到 **Switch B** 上。

2 SFTP配置

2.1 SFTP简介

SFTP 是 Secure FTP 的简称，是 SSH 2.0 中新增的功能。

SFTP 建立在 SSH 连接的基础之上，它使得远程用户可以安全地登录设备，进行文件管理和文件传送等操作，为数据传输提供了更高的安全保障。同时，由于设备支持作为客户端的功能，用户可以从本地设备安全登录到远程设备上，进行文件的安全传输。

通过SSH连接支持VPN多实例功能，作为SFTP客户端的设备可与位于MPLS VPN中的SFTP服务器之间建立连接。关于该功能的详细介绍，请参考 [1.1.3 SSH支持VPN多实例](#)。

2.2 配置设备作为SFTP服务器

2.2.1 配置准备

- 已经完成SSH服务器的配置，具体配置步骤请参见“[1.2 配置设备作为SSH服务器](#)”。
- SSH用户的服务类型设置为sftp或者all。具体配置步骤请参见“[1.2.6 配置SSH用户并指定服务类型和认证方式](#)”。

2.2.2 启动SFTP服务器

该配置任务用于启动 SFTP 服务，使客户端能用 SFTP 的方式登录到服务器。

表2-1 启动 SFTP 服务器

操作	命令	说明
进入系统视图	system-view	-
启动SFTP服务器	sftp server enable	必选 缺省情况下，SFTP服务器处于关闭状态



说明

- 设备作为 SFTP 服务器时，同时只能有一个用户访问 SFTP 服务器。如果以 WinSCP 作为 SFTP 客户端，则无法直接编辑服务器上的文件，需要采用将服务器上的文件下载到本地，在本地修改后上传到服务器的方式实现对文件的编辑。
- 设备作为 SFTP 服务器时，对客户端的访问操作有级别限制：如果要对设备的文件系统执行写操作（比如上传、删除、创建/删除文件夹），则必须将 SFTP 登录用户的级别设置为 3；如果要对设备的文件系统执行查看和上传操作（不能覆盖和删除文件），则可以将 SFTP 登录用户的级别设置为 2；如果执行其它操作（比如普通的查看操作），则 SFTP 登录用户的级别不受限制，可以为 0~3 中的任意级别。

2.2.3 配置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。

表2-2 配置 SFTP 用户连接的空闲超时时间

操作	命令	说明
进入系统视图	system-view	-
设置SFTP用户连接的空闲超时时间	sftp server idle-timeout time-out-value	可选 缺省情况下，SFTP用户连接的空闲超时时间为10分钟

2.3 配置设备作为SFTP客户端

2.3.1 为SFTP客户端指定源IP地址或源接口

用户可以通过以下配置，使 SFTP 客户端只能使用指定接口的 IP 地址或指定 IP 地址作为源地址建立与 SFTP 服务器的连接，增加了业务的可管理性。

表2-3 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	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
	sftp client ipv6 source { ipv6 ipv6-address interface interface-type interface-number }	

2.3.2 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，并进入到 SFTP 客户端视图。

表2-4 建立与 SFTP 服务器的连接

操作	命令	说明
与远程SFTP服务器建立连接，并进入SFTP客户端视图	与远程IPv4 SFTP服务器建立连接，并进入SFTP客户端视图 非FIPS模式下： <pre>sftp server [port-number] [vpn-instance vpn-instance-name] [identity-key { dsa rsa } prefer-ctos-cipher { 3des aes128 des } prefer-ctos-hmac { md5 md5-96 sha1 sha1-96 } prefer-kex { dh-group-exchange dh-group1 dh-group14 } prefer-stoc-cipher { 3des aes128 des } prefer-stoc-hmac { md5 md5-96 sha1 sha1-96 }] *</pre> FIPS模式下： <pre>sftp ipv6 server [port-number] [vpn-instance vpn-instance-name] [identity-key rsa 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 }] *</pre>	必选其一 请在用户视图下执行此命令
	与远程IPv6 SFTP服务器建立连接，并进入SFTP客户端视图 非FIPS模式下： <pre>sftp ipv6 server [port-number] [vpn-instance vpn-instance-name] [identity-key { dsa rsa } prefer-ctos-cipher { 3des aes128 des } prefer-ctos-hmac { md5 md5-96 sha1 sha1-96 } prefer-kex { dh-group-exchange dh-group1 dh-group14 } prefer-stoc-cipher { 3des aes128 des } prefer-stoc-hmac { md5 md5-96 sha1 sha1-96 }] *</pre> FIPS模式下： <pre>sftp ipv6 server [port-number] [vpn-instance vpn-instance-name] [identity-key rsa 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 }] *</pre>	

2.3.3 SFTP目录操作

SFTP 目录操作包括：改变或显示当前的工作目录、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。

表2-5 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 2.3.2	必选 请在用户视图下执行此命令

操作	命令	说明
改变远程SFTP服务器上的工作路径	cd [<i>remote-path</i>]	可选
返回到上一级目录	cdup	可选
显示远程SFTP服务器上的当前工作目录	pwd	可选
显示指定目录下的文件列表	dir [-a -l] [<i>remote-path</i>]	可选
	ls [-a -l] [<i>remote-path</i>]	dir 和 ls 两条命令的作用相同
改变SFTP服务器上指定的目录的名字	rename <i>oldname newname</i>	可选
在远程SFTP服务器上创建新的目录	mkdir <i>remote-path</i>	可选
删除SFTP服务器上指定的目录	rmdir <i>remote-path</i> &<1-10>	可选

2.3.4 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、删除文件。

表2-6 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 2.3.2	必选 请在用户视图下执行此命令
改变SFTP服务器上指定的文件的名字	rename <i>old-name new-name</i>	可选
从远程服务器上下载文件并存储在本地	get <i>remote-file</i> [<i>local-file</i>]	可选
将本地的文件上传到远程SFTP服务器	put <i>local-file</i> [<i>remote-file</i>]	可选
显示指定目录下的文件	dir [-a -l] [<i>remote-path</i>]	可选
	ls [-a -l] [<i>remote-path</i>]	dir 和 ls 两条命令的作用相同
删除SFTP服务器上指定的文件	delete <i>remote-file</i> &<1-10>	可选
	remove <i>remote-file</i> &<1-10>	delete 和 remove 两条命令的功能相同

2.3.5 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2-7 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 2.3.2	必选 请在用户视图下执行此命令
显示SFTP客户端命令的帮助信息	help [all <i>command-name</i>]	必选

2.3.6 终止与远程SFTP服务器的连接

表2-8 终止与远程 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 2.3.2	必选 请在用户视图下执行此命令
终止与远程SFTP服务器的连接，并退回用户视图	bye	必选其一 bye 、 exit 和 quit 三条命令的功能相同
	exit	
	quit	

2.3.7 配置SFTP客户端发送报文的DSCP优先级

在 IPv4 和 IPv6 报文头中，包含一个 8bit 的字段，用于标识 IP 报文的服务类型。在 IPv4 报文中，这个字段称为 ToS 字段；在 IPv6 报文中，称为 Traffic class 字段。RFC 2474 对这 8 个 bit 进行了定义，将前 6 个 bit 定义为 DSCP 优先级，最后 2 个 bit 作为保留位。在报文传输的过程中，DSCP 优先级可以被网络设备识别，并作为报文传输优先程度的参考。

用户可以对 SFTP 客户端发送报文的 DSCP 优先级进行配置。

表2-9 配置 SFTP 客户端发送报文的 DSCP 优先级

操作	命令	说明
进入系统视图	system-view	-
配置SFTP客户端发送IPv4报文的DSCP优先级	sftp client dscp <i>dscp-value</i>	可选 缺省情况下，SFTP客户端发送IPv4报文的DSCP优先级为16
配置SFTP客户端发送IPv6报文的DSCP优先级	sftp client ipv6 dscp <i>dscp-value</i>	可选 缺省情况下，SFTP客户端发送IPv6报文的DSCP优先级为8

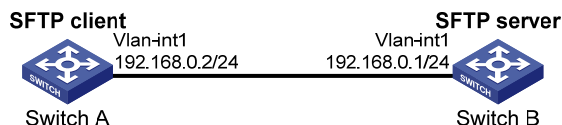
2.4 设备作为SFTP客户端配置举例

1. 组网需求

如 图 2-1，Switch A和Switch B之间建立SSH连接，Switch A作为SFTP客户端登录到Switch B，进行文件管理和文件传送等操作。SSH用户采用的认证方式为publickey认证，公钥算法为RSA。

2. 组网图

图2-1 设备作为 SFTP 客户端组网图



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 VLAN 接口 1 的 IP 地址。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 192.168.0.2 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

生成 RSA 密钥对。

```
[SwitchA] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
```

```
+++++++
+++++
+++++
+++++
```

将生成的 RSA 主机公钥导出到指定文件 pubkey 中。

```
[SwitchA] public-key local export rsa ssh2 pubkey
[SwitchA] 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。

(2) 配置 SFTP 服务器

生成 RSA 密钥对。


```

<SwitchB> system-view
[SwitchB] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
+++++++
+++++++
+++++
+++++++
# 生成 DSA 密钥对。
[SwitchB] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
+++++++
+++++++
# 启动 SSH 服务器。
[SwitchB] ssh server enable
# 启动 SFTP 服务器。
[SwitchB] sftp server enable
# 配置 VLAN 接口 1 的 IP 地址，客户端将通过该地址连接 SSH 服务器。
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[SwitchB-Vlan-interface1] quit
# 设置 SSH 客户端登录用户界面的认证方式为 AAA 认证。
[SwitchB] user-interface vty 0 15
[SwitchB-ui-vty0-15] authentication-mode scheme
# 设置 Switch B 上远程用户登录协议为 SSH。
[SwitchB-ui-vty0-15] protocol inbound ssh
[SwitchB-ui-vty0-15] quit
# 从文件 pubkey 中导入远端的公钥。
[SwitchB] public-key peer Switch001 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 Switch001，
  工作目录为 flash:/。
[SwitchB] ssh user client001 service-type sftp authentication-type publickey assign
  publickey Switch001 work-directory flash:/
(3) SFTP 客户端建立与 SFTP 服务器端的连接
# 与远程 SFTP 服务器建立连接，进入 SFTP Client 视图。
<SwitchA> sftp 192.168.0.1 identity-key rsa
Input Username: client001

```

```
Trying 192.168.0.1 ...
Press CTRL+K to abort
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
```

```
sftp-client>
```

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-client> dir
-rwxrwxrwx  1 noone  nogroup  1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone  nogroup   225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup   283 Aug 24 07:39 pubkey
drwxrwxrwx  1 noone  nogroup    0 Sep 01 06:22 new
-rwxrwxrwx  1 noone  nogroup   225 Sep 01 06:55 pub
-rwxrwxrwx  1 noone  nogroup    0 Sep 01 08:00 z
```

```
sftp-client> delete z
```

The following File will be deleted:

/z

Are you sure to delete it? [Y/N]:y

This operation may take a long time.Please wait...

File successfully Removed

```
sftp-client> dir
-rwxrwxrwx  1 noone  nogroup  1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone  nogroup   225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup   283 Aug 24 07:39 pubkey
drwxrwxrwx  1 noone  nogroup    0 Sep 01 06:22 new
-rwxrwxrwx  1 noone  nogroup   225 Sep 01 06:55 pub
```

新增目录 new1，并检查新目录是否创建成功。

```
sftp-client> mkdir new1
```

New directory created

```
sftp-client> dir
-rwxrwxrwx  1 noone  nogroup  1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone  nogroup   225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup   283 Aug 24 07:39 pubkey
drwxrwxrwx  1 noone  nogroup    0 Sep 01 06:22 new
-rwxrwxrwx  1 noone  nogroup   225 Sep 01 06:55 pub
drwxrwxrwx  1 noone  nogroup    0 Sep 02 06:30 new1
```

将目录名 new1 更名为 new2，并查看是否更名成功。

```
sftp-client> rename new1 new2
```

File successfully renamed

```
sftp-client> dir
-rwxrwxrwx  1 noone  nogroup  1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone  nogroup   225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup   283 Aug 24 07:39 pubkey
drwxrwxrwx  1 noone  nogroup    0 Sep 01 06:22 new
-rwxrwxrwx  1 noone  nogroup   225 Sep 01 06:55 pub
```

```

drwxrwxrwx  1 noone  nogroup          0 Sep 02 06:33 new2
# 从服务器上下载文件 pubkey2 到本地，并更名为 public。
sftp-client> get pubkey2 public
Remote file:/pubkey2 ---> Local file: public
Downloading file successfully ended
# 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-client> put pu puk
Local file:pu ---> Remote file: /puk
Uploading file successfully ended
sftp-client> dir
-rwxrwxrwx  1 noone  nogroup          1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone  nogroup           225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup           283 Aug 24 07:39 pubkey
drwxrwxrwx  1 noone  nogroup           0 Sep 01 06:22 new
drwxrwxrwx  1 noone  nogroup           0 Sep 02 06:33 new2
-rwxrwxrwx  1 noone  nogroup           283 Sep 02 06:35 pub
-rwxrwxrwx  1 noone  nogroup           283 Sep 02 06:36 puk
sftp-client>
# 退出 SFTP。
sftp-client> quit
Bye
Connection closed.
<SwitchA>

```

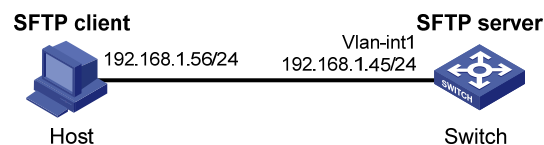
2.5 设备作为SFTP服务器配置举例

1. 组网需求

如 图 2-2，Host和Switch之间建立SSH连接，Host作为SFTP客户端登录到Switch，进行文件管理和文件传送等操作，用户名为client002，密码为aabbcc，用户名和密码保存在本地设备上。

2. 组网图

图2-2 设备作为 SFTP 服务器组网图



3. 配置步骤

(1) 配置 SFTP 服务器

```

# 生成 RSA 密钥对。
<Switch> system-view
[Switch] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.

```

```

Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
+++++++
+++++++
+++++
+++++++
# 生成 DSA 密钥对。
[Switch] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
+++++++
+++++++
# 启动 SSH 服务器。
[Switch] ssh server enable
# 启动 SFTP 服务器。
[Switch] sftp server enable
# 配置 VLAN 接口 1 的 IP 地址，客户端将通过该地址连接 SSH 服务器。
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.45 255.255.255.0
[Switch-Vlan-interface1] quit
# 设置 SSH 客户端登录用户界面的认证方式为 AAA 认证。
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] authentication-mode scheme
# 设置 Switch 上远程用户登录协议为 SSH。
[Switch-ui-vty0-15] protocol inbound ssh
[Switch-ui-vty0-15] quit
# 创建本地用户 client002。
[Switch] local-user client002
[Switch-luser-client002] password simple aabbcc
[Switch-luser-client002] service-type ssh
[Switch-luser-client002] quit
# 配置 SSH 用户认证方式为 password，服务类型为 SFTP。
[Switch] 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 2-3](#) 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2-3 SFTP 客户端登录界面

```
D:\software\SFTP\PSFTP.exe
psftp: no hostname specified; use "open host.name" to connect
psftp> open 192.168.1.45
login as: client002
The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1024 fb:2d:44:4d:b1:72:92:21:7d:8e:1a:ec:a4:ba:eb:00
If you trust this host, enter "y" to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? <y/n> n
Using username "client002".
client002@192.168.1.45's password:
Remote working directory is /
psftp> _
```

3 SCP配置

3.1 SCP简介

SCP 是 Secure Copy 的简称，提供安全的文件复制功能。目前仅支持基于 SSH 2.0 的文件复制。SCP 建立在 SSH 连接的基础之上，设备作为 SCP 服务器时，可使得远程用户安全地登录设备，进行文件上传或下载操作；设备作为 SCP 客户端时，用户可以从本地设备安全登录到远程服务器，进行文件的安全传输。

3.2 配置设备作为SCP服务器

- 具体配置步骤请参见“[1.2 配置设备作为SSH服务器](#)”。
- SSH用户的服务类型设置为**scp**或者**all**。具体配置步骤请参见“[1.2.6 配置SSH用户并指定服务类型和认证方式](#)”。



说明

设备作为 SCP 服务器时，同时仅允许有一个 FTP、SFTP 或 SCP 用户访问 SCP 服务器。

3.3 配置设备作为SCP客户端

该配置任务用来启动 SCP 客户端程序，与远程 SCP 服务器传输文件。

表3-1 建立与 SCP 服务器的连接

操作		命令	说明
与远程 SCP 服务器传输文件	向远程IPv4 SCP服务器上 传文件	非FIPS模式下： <pre>scp server [port-number] put source-file-path [destination-file-path] [identity-key { dsa rsa } prefer-ctos-cipher { 3des aes128 des } prefer-ctos-hmac { md5 md5-96 sha1 sha1-96 } prefer-kex { dh-group-exchange dh-group1 dh-group14 } prefer-stoc-cipher { 3des aes128 des } prefer-stoc-hmac { md5 md5-96 sha1 sha1-96 }] *</pre> FIPS模式下： <pre>scp server [port-number] put source-file-path [destination-file-path] [identity-key rsa 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 }] *</pre>	四者必 选其一 请在用 户视图 下执行 此命令

操作	命令	说明
从远程IPv4 SCP服务器下 载文件	非FIPS模式下： <pre>scp server [port-number] get source-file-path [destination-file-path] [identity-key { dsa rsa } prefer-ctos-cipher { 3des aes128 des } prefer-ctos-hmac { md5 md5-96 sha1 sha1-96 } prefer-kex { dh-group-exchange dh-group1 dh-group14 } prefer-stoc-cipher { 3des aes128 des } prefer-stoc-hmac { md5 md5-96 sha1 sha1-96 }] *</pre> FIPS模式下： <pre>scp server [port-number] get source-file-path [destination-file-path] [identity-key rsa 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 }] *</pre>	
向远程IPv6 SCP服务器上 传文件	非FIPS模式下： <pre>scp ipv6 server [port-number] put source-file-path [destination-file-path] [identity-key { dsa rsa } prefer-ctos-cipher { 3des aes128 des } prefer-ctos-hmac { md5 md5-96 sha1 sha1-96 } prefer-kex { dh-group-exchange dh-group1 dh-group14 } prefer-stoc-cipher { 3des aes128 des } prefer-stoc-hmac { md5 md5-96 sha1 sha1-96 }] *</pre> FIPS模式下： <pre>scp ipv6 server [port-number] put source-file-path [destination-file-path] [identity-key rsa 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 }] *</pre>	
从远程IPv6 SCP服务器下 载文件	非FIPS模式下： <pre>scp ipv6 server [port-number] get source-file-path [destination-file-path] [identity-key { dsa rsa } prefer-ctos-cipher { 3des aes128 des } prefer-ctos-hmac { md5 md5-96 sha1 sha1-96 } prefer-kex { dh-group-exchange dh-group1 dh-group14 } prefer-stoc-cipher { 3des aes128 des } prefer-stoc-hmac { md5 md5-96 sha1 sha1-96 }] *</pre> FIPS模式下： <pre>scp ipv6 server [port-number] get source-file-path [destination-file-path] [identity-key rsa 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 }] *</pre>	

3.4 SCP服务典型配置举例

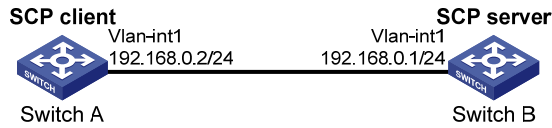
3.4.1 设备作为SCP客户端配置举例

1. 组网需求

如 [图 3-1](#)，Switch A作为SCP客户端从Switch B下载文件remote.bin，用户采用的认证方式为password认证，用户名为test。

2. 组网图

图3-1 设备作为 SCP 客户端组网图



3. 配置步骤

(1) 配置 SCP 客户端

配置 VLAN 接口 1 的 IP 地址。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 192.168.0.2 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

(2) 下载文件

下载远端的 remote.bin 文件，下载到本地后更名为 local.bin。

```
<SwitchA> scp 192.168.0.1 get remote.bin local.bin
Username: test
Trying 192.168.0.1 ...
Press CTRL+K to abort
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.
```

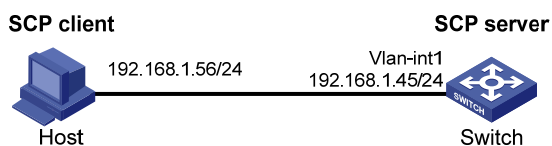
3.4.2 设备作为SCP服务器配置举例

1. 组网需求

如 图 3-2，Host和Switch之间建立SSH连接，Host作为SCP客户端与SCP服务器Switch传输文件。所使用的用户名为test，密码为aabbcc，用户名和密码保存在本地设备上。

2. 组网图

图3-2 设备作为 SCP 服务器组网图



3. 配置步骤

(1) 配置 SCP 服务器

生成 RSA 密钥对。


```

<Switch> system-view
[Switch] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
+++++++
+++++++
+++++
+++++++
# 生成 DSA 密钥对。
[Switch] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
+++++++
+++++++
# 启动 SSH 服务器。
[Switch] ssh server enable
# 配置 VLAN 接口 1 的 IP 地址，客户端将通过该地址连接 SSH 服务器。
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.45 255.255.255.0
[Switch-Vlan-interface1] quit
# 设置 SSH 客户端登录用户界面的认证方式为 AAA 认证。
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] authentication-mode scheme
# 设置 SSH 客户端登录用户界面支持包括 SSH 在内的所有协议。
[Switch-ui-vty0-15] protocol inbound all
[Switch-ui-vty0-15] quit
# 创建本地用户 test。
[Switch] local-user test
[Switch-luser-test] password simple aabbcc
[Switch-luser-test] service-type ssh
[Switch-luser-test] quit
# 配置 SSH 用户认证方式为 password，服务类型为 SCP。
[Switch] ssh user test service-type scp authentication-type password

```

目 录

1 SSL配置.....	1-1
1.1 SSL简介	1-1
1.1.1 SSL安全机制	1-1
1.1.2 SSL协议结构	1-2
1.2 SSL配置任务简介	1-2
1.3 配置SSL服务器端策略	1-3
1.3.1 SSL服务器端策略配置步骤.....	1-3
1.3.2 SSL服务器端策略典型配置举例	1-4
1.4 配置SSL客户端策略	1-6
1.5 SSL显示和维护	1-7
1.6 常见配置错误举例	1-8
1.6.1 SSL握手失败	1-8

1 SSL配置



说明

设备运行于 FIPS 模式时，本特性的部分配置相对于非 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

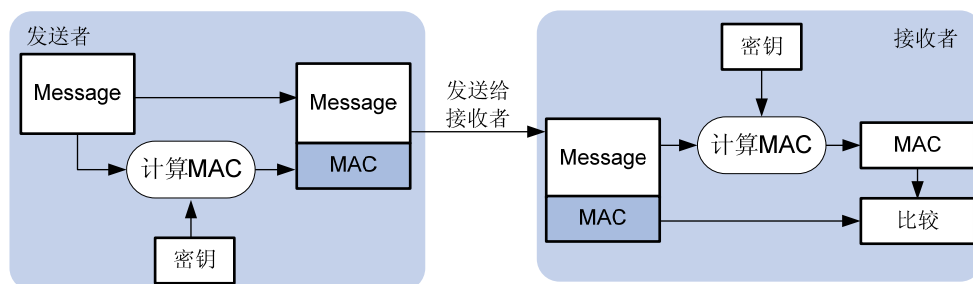
SSL（Secure Sockets Layer，安全套接字层）是一个安全协议，为基于 TCP 的应用层协议提供安全连接，如 SSL 可以为 HTTP 协议提供安全连接。SSL 协议广泛应用于电子商务、网上银行等领域，为网络上数据的传输提供安全性保证。

1.1.1 SSL安全机制

SSL 提供的安全连接可以实现：

- 连接的私密性：利用对称加密算法对传输数据进行加密，并利用密钥交换算法——RSA（Rivest Shamir and Adleman）加密传输对称密钥算法中使用的密钥。
- 身份验证：基于证书利用数字签名方法对服务器和客户端进行身份验证。SSL 服务器和客户端通过 PKI（Public Key Infrastructure，公钥基础设施）提供的机制从 CA（Certificate Authority，认证颁发机构）获取证书。
- 连接的可靠性：消息传输过程中使用基于密钥的 MAC（Message Authentication Code，消息验证码）来检验消息的完整性。MAC 是将密钥和任意长度的数据转换为固定长度数据的一种算法。利用 MAC 算法验证消息完整性的过程如 [图 1-1](#) 所示。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。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。如果二者相同，则报文没有改变；否则，报文在传输过程中被修改，接收者将丢弃该报文。

图1-1 MAC 算法示意图





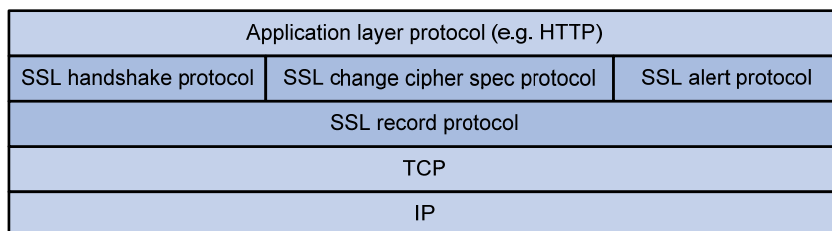
说明

- 对称密钥算法、非对称密钥算法 RSA 及数字签名的详细介绍请参见“安全配置指导”中的“公钥管理”；
- PKI 及证书、CA 的详细介绍请参见“安全配置指导”中的“PKI”。

1.1.2 SSL协议结构

如 图 1-2 所示，SSL协议本身可以分为两层：底层为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警告协议（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，最后把记录块传输给对方。
- SSL 握手协议：是 SSL 协议非常重要的组成部分，用来协商通信过程中使用的加密套件（对称加密算法、密钥交换算法和 MAC 算法等）、在服务器和客户端之间安全地交换密钥，实现服务器和客户端的身份验证。客户端和服务端通过握手协议建立一个会话。会话包含一组参数，主要有会话 ID、对方的证书、加密套件（包括密钥交换算法、数据加密算法和 MAC 算法）及主密钥。
- SSL 密码变化协议：客户端和服务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 警告协议：用来允许一方向另一方报告告警信息。消息中包含告警的严重级别和描述。

1.2 SSL配置任务简介

SSL 服务器和客户端需要配置的参数不同，下面将分别介绍 SSL 服务器端策略和 SSL 客户端策略的配置方法。

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	必选	1.3
配置SSL客户端策略	可选	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 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 <i>policy-name</i>	必选
配置SSL服务器端策略所使用的PKI域	pki-domain <i>domain-name</i>	可选 缺省情况下，没有配置SSL服务器端策略所使用的PKI域，SSL服务器自己生成证书，而无需从CA获取证书 指定使用的PKI域后，SSL服务器将通过该PKI域获取服务器端的证书 PKI域配置方法的详细介绍，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 [<i>rsa_3des_edc_cbc_sha</i> <i>rsa_aes_128_cbc_sha</i> <i>rsa_aes_256_cbc_sha</i> <i>rsa_des_cbc_sha</i> <i>rsa_rc4_128_md5</i> <i>rsa_rc4_128_sha</i>] * FIPS模式下： ciphersuite [<i>dhe_rsa_aes_128_cbc_sha</i> <i>dhe_rsa_aes_256_cbc_sha</i> <i>rsa_aes_128_cbc_sha</i> <i>rsa_aes_256_cbc_sha</i>] *	可选 缺省情况下，SSL服务器端策略支持所有的加密套件
配置服务器端SSL握手连接保持时间	handshake timeout <i>time</i>	可选 缺省情况下，服务器端SSL握手连接保持时间是3600秒
配置SSL连接关闭模式	close-mode <i>wait</i>	可选 缺省情况下，关闭模式为非 <i>wait</i> 模式
配置缓存的最大会话数目和会话缓存的超时时间	session { <i>cachesize size</i> <i>timeout time</i> } *	可选 缺省情况下，缓存的最大会话数目为500个，会话缓存的超时时间为3600秒
配置SSL服务器端要求对SSL客户端进行基于证书的身份验证	client-verify <i>enable</i>	可选 缺省情况下，SSL服务器端不要求对SSL客户端进行基于证书的身份验证

操作	命令	说明
使能SSL客户端弱认证功能	client-verify weaken	可选 缺省情况下,未使能SSL客户端弱认证功能 只有通过 client-verify enable 命令配置SSL服务器端要求对SSL客户端进行基于证书的身份验证后,本命令才会生效

说明

- 如果服务器端需要对客户端进行基于证书的身份验证,即配置了 **client-verify enable** 命令,则必须先为 SSL 客户端申请本地证书。
- 目前,SSL 协议版本主要有 SSL2.0、SSL3.0 和 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。

1.3.2 SSL服务器端策略典型配置举例

1. 组网需求

用户可以通过 Web 页面访问和控制设备。为了防止非法用户访问和控制设备,提高设备管理的安全性,设备要求用户以 HTTPS (Hypertext Transfer Protocol Secure, 超文本传输协议的安全版本) 的方式登录 Web 页面,利用 SSL 协议实现用户身份验证,并保证传输的数据不被窃听和篡改。

为了满足上述需求,需要进行如下配置:

- 配置 Device 作为 HTTPS 服务器,并为 Device 申请证书。
- 为 HTTPS 客户端 Host 申请证书,以便 Device 验证其身份。

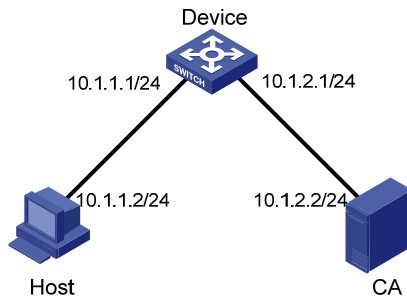
其中,负责为 Device 和 Host 颁发证书的认证机构为 CA server。

说明

- 本配置举例中,采用 Windows Server 作为 CA,在 CA 上需要安装 SCEP (Simple Certificate Enrollment Protocol, 简单证书注册协议) 插件。
- 进行下面的配置之前,需要确保 Device、Host、CA 之间路由可达。

2. 组网图

图1-3 SSL 服务器端策略组网图



3. 配置步骤

(1) 配置 HTTPS 服务器 Device

配置 PKI 实体 en，指定实体的通用名为 http-server1、FQDN 为 ssl.security.com。

```
<Device> system-view
[Device] pki entity en
[Device-pki-entity-en] common-name http-server1
[Device-pki-entity-en] fqdn ssl.security.com
[Device-pki-entity-en] quit
```

配置 PKI 域 1，指定信任的 CA 名称为 ca server、注册服务器的 URL 为 http://10.1.2.2/certsrv/mscep/mscep.dll、证书申请的注册受理机构为 RA、实体名称为 en。

```
[Device] pki domain 1
[Device-pki-domain-1] ca identifier ca server
[Device-pki-domain-1] certificate request url http://10.1.2.2/certsrv/mscep/mscep.dll
[Device-pki-domain-1] certificate request from ra
[Device-pki-domain-1] certificate request entity en
[Device-pki-domain-1] quit
```

生成本地的 RSA 密钥对。

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

获取 CA 的证书。

```
[Device] pki retrieval-certificate ca domain 1
```

为 Device 申请证书。

```
[Device] pki request-certificate domain 1
```

创建一个名为 myssl 的 SSL 服务器端策略。

```
[Device] ssl server-policy myssl
```

配置 SSL 服务器端策略使用的 PKI 域名为 1。

```
[Device-ssl-server-policy-myssl] pki-domain 1
```

配置服务器端需要验证客户端身份。

```
[Device-ssl-server-policy-myssl] client-verify enable
[Device-ssl-server-policy-myssl] quit
```

配置 HTTPS 服务使用的 SSL 策略为 myssl。

```
[Device] ip https ssl-server-policy myssl
```

```
# 使能 HTTPS 服务。
[Device] ip https enable
# 创建本地用户 usera，密码为 123，服务类型为 Web。
[Device] local-user usera
[Device-luser-usera] password simple 123
[Device-luser-usera] service-type web
```

(2) 配置 HTTPS 客户端 Host

在 Host 上打开 IE 浏览器，输入网址 `http://10.1.2.2/certsrv`，根据提示为 Host 申请证书。

(3) 验证配置结果

在 Host 上打开 IE 浏览器，输入网址 `https://10.1.1.1`，选择 CA server 为 Host 颁发的证书，即可打开 Device 的 Web 登录页面。在登录页面，输入用户名 `usera`，密码 `123`，则可进入 Device 的 Web 配置页面，实现对 Device 的访问和控制。

 说明

- PKI 配置命令的详细介绍请参见“安全命令参考”中的“PKI”；
- **public-key local create rsa** 命令的详细介绍请参见“安全命令参考”中的“公钥管理”；
- HTTPS 的详细介绍，请参见“基础配置指导”中的“配置通过 Web 网管登录设备”。

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。只有与应用层协议关联后，SSL 客户端策略才能生效。

表1-3 配置 SSL 客户端策略

操作	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 <i>policy-name</i>	必选
配置SSL客户端策略所使用的PKI域	pki-domain <i>domain-name</i>	可选 缺省情况下，没有配置SSL客户端策略所使用的PKI域 指定使用的PKI域后，SSL客户端将通过该PKI域获取客户端的证书 PKI域配置方法的详细介绍，请参见“安全配置指导”中的“PKI”

操作	命令	说明
配置SSL客户端策略的首选加密套件	非FIPS模式下： <pre>prefer-cipher { 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 }</pre> FIPS模式下： <pre>prefer-cipher { dhe_rsa_aes_128_cbc_sha dhe_rsa_aes_256_cbc_sha rsa_aes_128_cbc_sha rsa_aes_256_cbc_sha }</pre>	可选 缺省情况下，SSL客户端策略的首选加密套件为 rsa_rc4_128_md5
配置SSL客户端策略使用的SSL协议版本	非FIPS模式下： <pre>version { ssl3.0 tls1.0 }</pre> FIPS模式下： <pre>version tls1.0</pre>	可选 缺省情况下，SSL客户端策略使用的SSL协议版本号为TLS 1.0
使能基于证书的SSL服务器身份验证	server-verify enable	可选 缺省情况下，需要进行基于证书的SSL服务器身份验证



说明

如果服务器端需要对客户端进行基于证书的身份验证，则必须先在SSL客户端所属的PKI域内为SSL客户端申请本地证书。

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 { <i>policy-name</i> all } [{ begin exclude include } <i>regular-expression</i>]
显示SSL客户端策略的信息	display ssl client-policy { <i>policy-name</i> all } [{ begin exclude include } <i>regular-expression</i>]

1.6 常见配置错误举例

1.6.1 SSL握手失败

1. 故障现象

设备作为 SSL 服务器时，与 SSL 客户端握手失败。

2. 故障分析

SSL 握手失败，可能有以下原因：

- 客户端配置了必须对服务器端进行身份验证，但 SSL 服务器端证书不存在，或者证书不能被信任；
- 服务器端配置了必须对客户端进行身份验证，但 SSL 客户端的证书不存在或不能被信任；
- SSL 服务器端和客户端没有匹配的加密套件。

3. 故障排除

(1) 使用 **debugging ssl** 命令查看调试信息：

- 如果客户端配置了必须对服务器端进行身份验证，而 SSL 服务器端的证书不存在，请为 SSL 服务器申请证书；如果服务器端证书不能被信任，请在 SSL 客户端安装为 SSL 服务器颁发证书的 CA 服务器根证书，或服务器向 SSL 客户端信任的 CA 服务器重新申请证书；
- 如果服务器端配置了必须对客户端进行身份验证，而 SSL 客户端的证书不存在或不能被信任，请为客户端申请并安装证书。

(1) 使用 **display ssl server-policy** 命令查看 SSL 服务器端策略支持的加密套件。如果 SSL 服务器端和客户端没有匹配的加密套件，请用 **ciphersuite** 命令修改 SSL 服务器支持的加密套件。

目 录

1 TCP攻击防御配置	1-1
1.1 TCP攻击防御简介	1-1
1.2 配置SYN Cookie功能	1-1
1.3 TCP攻击防御显示和维护	1-2

1 TCP攻击防御配置

1.1 TCP攻击防御简介

攻击者可以利用 TCP 连接的建立过程对设备进行攻击。为了避免上述攻击带来的危害，设备提供了 SYN Cookie 功能。

下面将详细介绍该功能的工作原理以及配置过程。

1.2 配置SYN Cookie功能

一般情况下，TCP 连接的建立需要经过三次握手，即：

- (1) TCP 连接请求的发起者向目标服务器发送 SYN 报文；
- (2) 目标服务器收到 SYN 报文后，建立处于 SYN_RECEIVED 状态的 TCP 半连接，并向发起者回复 SYN ACK 报文，等待发起者的回应；
- (3) 发起者收到 SYN ACK 报文后，回应 ACK 报文，这样 TCP 连接就建立起来了。

利用 TCP 连接的建立过程，一些恶意的攻击者可以进行 SYN Flood 攻击。攻击者向服务器发送大量请求建立 TCP 连接的 SYN 报文，而不回应服务器的 SYN ACK 报文，导致服务器上建立了大量的 TCP 半连接。从而，达到耗费服务器资源，使服务器无法处理正常业务的目的。

SYN Cookie 功能用来防止 SYN Flood 攻击。当服务器收到 TCP 连接请求时，不建立 TCP 半连接，而直接向发起者回复 SYN ACK 报文。服务器接收到发起者回应的 ACK 报文后，才建立连接，并进入 ESTABLISHED 状态。通过这种方式，可以避免在服务器上建立大量的 TCP 半连接，防止服务器受到 SYN Flood 攻击。

表1-1 配置 SYN Cookie 功能

操作	命令	说明
进入系统视图	system-view	-
使能SYN Cookie功能	tcp syn-cookie enable	必选 缺省情况下，SYN Cookie功能处于使能状态

说明

- 如果启用了在建立 TCP 连接时进行 MD5 认证的功能，则 SYN Cookie 功能不会生效。取消在建立 TCP 连接时进行 MD5 认证功能后，之前配置的 SYN Cookie 功能会自动生效。关于在建立 TCP 连接时进行 MD5 认证功能的介绍，请参见“三层技术-IP 路由配置指导”中“BGP”手册中“配置 BGP 建立 TCP 连接时进行 MD5 认证”章节的内容。
- 使能 SYN Cookie 功能后，建立 TCP 连接时只协商最大报文段长度选项，而不协商窗口缩放因子和时间戳选项。

1.3 TCP攻击防御显示和维护

在任意视图下执行 **display tcp status** 命令可以显示所有 TCP 连接的状态,用户可以通过显示信息随时监控 TCP 连接。

表1-2 TCP 攻击防御显示和维护

操作	命令
显示所有TCP连接的状态	display tcp status [{ begin exclude include } <i>regular-expression</i>]

目 录

1 IP Source Guard配置	1-1
1.1 IP Source Guard简介	1-1
1.1.1 概述	1-1
1.1.2 静态绑定表项	1-1
1.1.3 动态获取绑定表项	1-2
1.2 配置IPv4 绑定功能	1-3
1.2.1 配置IPv4 端口绑定功能	1-3
1.2.2 配置IPv4 静态绑定表项	1-4
1.2.3 配置IPv4 绑定表项数目的最大值	1-5
1.3 配置IPv6 绑定功能	1-6
1.3.1 配置IPv6 端口绑定功能	1-6
1.3.2 配置IPv6 静态绑定表项	1-7
1.3.3 配置IPv6 绑定表项数目的最大值	1-8
1.4 IP Source Guard显示和维护	1-9
1.5 IP Source Guard典型配置举例	1-9
1.5.1 IPv4 静态绑定表项配置举例	1-9
1.5.2 与DHCP Snooping配合的IPv4 端口绑定功能配置举例	1-11
1.5.3 与DHCP Relay配合的IPv4 端口绑定功能配置举例	1-13
1.5.4 IPv6 静态绑定表项配置举例	1-14
1.5.5 与DHCPv6 Snooping配合的IPv6 端口绑定功能配置举例	1-14
1.5.6 与ND Snooping配合的IPv6 端口绑定功能配置举例	1-16
1.5.7 全局地址绑定配置举例	1-17
1.6 常见配置错误举例	1-18
1.6.1 静态绑定表项配置和端口绑定功能配置失败	1-18

1 IP Source Guard配置

1.1 IP Source Guard简介

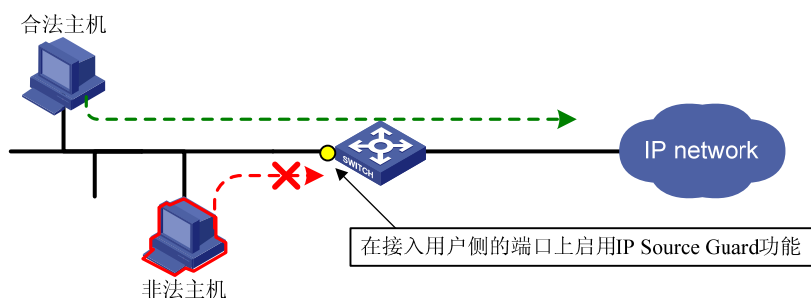
1.1.1 概述

通过在设备接入用户侧的端口上启用 IP Source Guard 功能，可以对端口收到的报文进行过滤控制，防止非法报文通过端口，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），提高了端口的安全性。

IP Source Guard 在端口上用于过滤报文的特征项包括：源 IP 地址、源 MAC 地址。这些特征项可单独或组合起来与端口进行绑定，形成绑定表项，具体包括：IP、MAC、IP+MAC。

如 图 1-1 所示，配置了 IP Source Guard 的端口接收到报文后查找 IP Source Guard 绑定表项，如果报文中的特征项与绑定表项中记录的特征项匹配，则端口转发该报文，否则做丢弃处理。绑定功能是针对端口的，一个端口配置了绑定功能后，仅该端口被限制，其他端口不受该绑定影响。

图1-1 IP Source Guard 功能示意图



1.1.2 静态绑定表项

通过手工配置产生绑定表项来完成端口的控制功能，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端口上配置绑定表项，仅允许该端口接收或者发送与该服务器通信的报文。

- IPv4 静态表项：使用手工配置的 IPv4 静态绑定表项来过滤端口收到的 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 静态表项：使用手工配置的 IPv6 静态绑定表项来过滤端口收到的 IPv6 报文，或者与 ND Detection 功能配合使用检查接入用户的合法性。



说明

- ARP Detection 功能的详细介绍请参考“安全配置指导”中的“ARP 攻击防御”。
- ND Detection 功能的详细介绍请参考“安全配置指导”中的“ND 攻击防御”。

静态绑定表项又包括全局静态绑定表项和端口静态绑定表项两种类型，这两种绑定表项的作用范围不同。

1. 全局静态绑定表项

全局静态绑定表项是在系统视图下配置的绑定了 IP 地址和 MAC 地址的表项，这类表项在设备的所有端口上生效，允许端口正常转发 IP 地址和 MAC 地址均与全局静态绑定表项匹配的报文，其它报文是否可以被正常转发由端口上配置的静态绑定表项来决定。全局静态绑定表项适用于防御主机仿冒攻击，可有效过滤攻击者通过仿冒合法用户主机的 IP 地址或者 MAC 地址向设备发送的伪造 IP 报文。

2. 端口静态绑定表项

端口静态绑定是在端口上配置的绑定了 IP 地址、MAC 地址以及相关组合的表项，这类表项仅在当前端口上生效。只有端口收到的报文的 IP 地址、MAC 地址与端口上配置的绑定表项的各参数完全匹配时，报文才可以在该端口被正常转发，其它报文都不能被转发，该表项适用于检查端口上接入用户的合法性。

1.1.3 动态获取绑定表项

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、DHCP 中继和 ND Snooping。

根据 DHCP 的相关表项动态生成绑定表项来完成端口控制功能，通常适用于局域网络中主机较多，并且采用 DHCP 进行动态主机配置的情况。其原理是每当 DHCP 为用户分配 IP 地址而生成一条 DHCP 表项时，端口绑定功能就相应地增加一条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，因此端口绑定功能也不会增加相应的访问规则来允许该用户访问网络。

根据 802.1X 的相关表项动态生成绑定表项来完成端口控制功能，通常适用于局域网络中使用 802.1X 客户端认证的情况。当 802.1X 客户端支持上传 IP 地址时，设备可以根据 802.1X 的相关表项动态生成绑定表项来过滤端口收到的 IPv4 报文。当 802.1X 客户端不支持上传 IP 地址时，802.1X 功能必须与 DHCP Snooping 功能或者 ARP Snooping 功能配合使用，通过 DHCP Snooping 或者 ARP Snooping 记录表项生成 802.1X 安全表项，再动态生成绑定表项来过滤端口收到的 IPv4 报文。同时，为防止某个用户私自修改 IP 地址，配置 802.1X 用户 IP 地址冻结功能，使得首次获取并保存了 802.1X 上线用户的 IP 地址之后，不会随着该用户 IP 地址的变化而更新 IP Source Guard 动态绑定表中用户的 IP 地址。

- IPv4 动态绑定：根据 802.1X、DHCP Snooping 表项或 DHCP Relay 表项动态生成绑定表项来过滤端口收到的 IPv4 报文；
- IPv6 动态绑定：根据 DHCPv6 Snooping 表项或 ND Snooping 表项动态生成绑定表项来过滤端口收到的 IPv6 报文。



说明

- 仅 R5206 及以上版本支持基于 802.1X 认证的 IP Source Guard 动态表项获取功能。
- 802.1X 功能的详细介绍请参见“安全配置指导”中的“802.1X”。
- DHCP Snooping 和 DHCP Relay 功能的详细介绍请参考“三层技术-IP 业务配置指导”中的“DHCP 中继”。
- DHCPv6 Snooping 功能的详细介绍请参考“三层技术-IP 业务配置指导”中的“DHCPv6 Snooping”。
- ND Snooping 功能的详细介绍请参考“三层技术-IP 业务配置指导”中的“IPv6 基础”。

1.2 配置IPv4绑定功能



说明

加入聚合组或加入业务环回组的端口上不能配置 IP Source Guard 功能，反之亦然。

1.2.1 配置IPv4 端口绑定功能

配置了 IPv4 端口绑定功能的端口，可利用配置的 IPv4 静态绑定表项和从 DHCP 模块获取的 IPv4 动态绑定表项对端口转发的报文进行过滤：

- IPv4 静态绑定表项的配置请参考“[1.2.2 配置IPv4 静态绑定表项](#)”。
- 在二层以太网端口上，IP Source Guard 可与 DHCP Snooping 配合，通过获取 IP 地址动态分配时产生的 DHCP Snooping 表项来生成动态绑定表项；
- 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。
- 在 VLAN 接口上，IP Source Guard 可与 DHCP Relay 配合，通过获取 IP 地址跨网段动态分配时产生的 DHCP Relay 表项来生成动态绑定表项。

动态绑定表项中可能包含的内容有：MAC 地址、IP 地址、VLAN 信息、入端口信息及表项类型（DHCP Snooping 或 DHCP Relay），其中 MAC 地址、IP 地址和 VLAN 信息的包含情况由动态绑定配置决定。IP Source Guard 把这些动态绑定表项下发到端口后，可对端口上转发的报文进行过滤。

表1-1 配置 IPv4 端口绑定功能

操作	命令	说明
进入系统视图	system-view	-
开启全局的802.1X	dot1x	可选 缺省情况下，全局的802.1X处于关闭状态
进入接口视图	interface interface-type interface-number	-

操作	命令	说明
开启端口的802.1X	dot1x	可选 缺省情况下，端口的802.1X特性为关闭状态
配置802.1X用户IP地址冻结功能	dot1x user-ip freeze	可选 缺省情况下，端口首次获取且保存了802.1X上线用户的IP地址之后，会随着用户IP地址的变化而更新保存的用户IP地址。
配置基于802.1X认证的IP Source Guard动态表项获取功能	ip verify source dot1x	可选 缺省情况下，端口上未配置IPv4端口绑定功能
配置IPv4端口绑定功能	ip verify source { ip-address ip-address mac-address mac-address }	必选 缺省情况下，端口上未配置IPv4端口绑定功能



说明

- IPv4 端口绑定功能中所指的“接口”可以为二层以太网端口、VLAN 接口或端口组。
- 接口下的 IPv4 端口绑定功能可多次配置，最后一次的配置生效。
- 若要通过获取 DHCP 相关表项来生成动态绑定表项，请保证网络中的 DHCP Snooping 或 DHCP Relay 配置有效且工作正常，DHCP Snooping 配置的具体介绍请参见“三层技术-IP 业务配置指导”中的“DHCP Snooping”，DHCP Relay 配置的具体介绍请参见“三层技术-IP 业务配置指导”中的“DHCP 中继”。
- 虽然 IP Source Guard 的动态表项是通过获取 DHCP 的相关表项而生成，但生成的 IP Source Guard 动态绑定表项数目并不与对应的 DHCP 表项数目保持一致，实际使用过程中，请以 IP Source Guard 实际生成的表项数目为准。

1.2.2 配置IPv4 静态绑定表项

IPv4 静态绑定表项包括全局IPv4 静态绑定表项和端口IPv4 静态绑定表项。IPv4 静态绑定表项只能在配置了IPv4 端口绑定功能的端口上生效，端口绑定功能的具体配置请参见“[1.2.1 配置IPv4 端口绑定功能](#)”。

静态绑定表项与端口绑定功能配合使用时，端口静态绑定表项和动态绑定表项的优先级高于全局静态绑定表项，即端口优先使用端口上的静态或动态绑定表项对收到的报文进行匹配，若匹配失败，再与全局静态绑定表项进行匹配。

1. 配置全局IPv4 静态绑定表项

全局静态绑定表项中定义了端口允许转发的报文的 IP 地址和 MAC 地址，对所有端口都生效。

表1-2 配置全局 IPv4 静态绑定表项

操作	命令	说明
进入系统视图	system-view	-

操作	命令	说明
配置全局IPv4静态绑定表项	ip source binding ip-address ip-address mac-address mac-address	必选 缺省情况下，无全局IPv4静态绑定表项

2. 配置端口IPv4 静态绑定表项

表1-3 配置端口 IPv4 静态绑定表项

操作	命令	说明
进入系统视图	system-view	-
进入二层以太网端口视图	interface interface-type interface-number	-
配置端口的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]	必选 缺省情况下，端口上无IPv4静态绑定表项



说明

- 一个表项不能在同一个端口上重复绑定，但可以在不同端口上绑定。
- 当 IPv4 静态绑定表项与 IP Source Guard 功能配合时，静态绑定表项中的 VLAN 参数不作为过滤报文的特征项，VLAN 参数指定与否，不影响 IP Source Guard 功能对报文的过滤结果。
- 在 IPv4 静态绑定表项与 ARP Detection 功能配合时，静态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 IPv4 静态绑定表项的检查。关于 ARP Detection 功能的相关配置请参见“安全配置指导”中的“ARP 攻击防御”。
- 配置静态表项时，如果系统中已经存在相同内容的动态表项，则新添加的静态表项将会覆盖已有的动态表项。

1.2.3 配置IPv4 绑定表项数目的最大值

IPv4 绑定表项数目的最大值用于限制端口上允许添加的 IPv4 静态绑定表项和 IPv4 动态绑定表项的数量总和。当端口上的 IPv4 绑定表项数目达到指定的最大值时，端口将不再允许添加新的 IPv4 绑定表项。

表1-4 配置 IPv4 绑定表项数目的最大值

操作	命令	说明
进入系统视图	system-view	-
进入二层以太网端口视图	interface interface-type interface-number	-

操作	命令	说明
配置IPv4绑定表项数目的最大值	ip verify source max-entries <i>number</i>	可选 缺省情况下，对于S5500-28SC-HI和S5500-52SC-HI，端口上IPv4绑定表项的最大值为640；对于本系列交换机其它机型，端口上IPv4绑定表项数目的最大值为2048



说明

如果要配置的 IPv4 绑定表项数目的最大值小于当前端口上已存在的 IPv4 绑定表项总数，则该最大值可以配置成功，且原有的表项不受影响，但端口将不再允许新增 IPv4 绑定表项，除非端口上的 IPv4 绑定表项数目减少到小于此最大值。

1.3 配置IPv6绑定功能



说明

加入聚合组或加入业务环回组的端口上不能配置 IP Source Guard 功能，反之亦然。

1.3.1 配置IPv6 端口绑定功能

配置了 IPv6 端口绑定功能的端口，利用配置的 IPv6 静态绑定表项和从 DHCP 模块或 ND 模块获取的 IPv6 动态绑定表项对端口转发的报文进行过滤：

- IPv6 静态绑定表项的配置请参考“[1.3.2 配置IPv6 静态绑定表项](#)”。
- 在二层以太网端口上，IP Source Guard 可与 DHCPv6 Snooping 配合，通过获取 IPv6 地址动态分配时产生的 DHCPv6 Snooping 表项来生成动态绑定表项。
- 在二层以太网端口上，IP Source Guard 可与 ND Snooping 配合，通过获取动态产生的 ND Snooping 表项来生成动态绑定表项。

动态绑定表项中可能包含的内容有：MAC 地址、IPv6 地址、VLAN 信息、入端口信息及表项类型（DHCPv6 Snooping 或 ND Snooping），其中 MAC 地址、IPv6 地址和 VLAN 信息的包含情况由端口绑定配置决定。IP Source Guard 把这些动态绑定表项下发到端口后，可对端口上转发的报文进行过滤。

表1-5 配置 IPv6 端口绑定功能

操作	命令	说明
进入系统视图	system-view	-
进入二层以太网端口、端口组视图	interface <i>interface-type interface-number</i>	-

操作	命令	说明
配置IPv6端口绑定功能	ipv6 verify source { ipv6-address ipv6-address mac-address mac-address }	必选 缺省情况下，端口上未配置IPv6端口绑定功能

说明

- 若要通过获取 DHCP 或 ND 相关表项来生成动态绑定表项，请保证网络中的 DHCPv6 Snooping 或 ND Snooping 配置有效且工作正常，配置的具体介绍请分别参见“三层技术-IP 业务配置指导”中的“DHCPv6”和“三层技术-IP 业务配置指导”中的“IPv6 基础”。
- IPv6 端口绑定功能可多次配置，最后一次的配置生效。
- 若设备上同时配置了 ND Snooping 和 DHCPv6 Snooping，通常会首先生成 DHCPv6 Snooping 表项，因此 IP Source Guard 会使用先生成的 DHCPv6 Snooping 表项来过滤端口报文。
- 虽然 IP Source Guard 的动态表项是通过获取 DHCP 的相关表项而生成，但生成的 IP Source Guard 动态绑定表项数目并不与对应的 DHCP 表项数目保持一致，实际使用过程中，请以 IP Source Guard 实际生成的表项数目为准。

1.3.2 配置IPv6 静态绑定表项

IPv6 静态绑定功能包括全局IPv6 静态绑定功能和端口IPv6 静态绑定功能。IPv6 静态绑定表项只能在配置了IPv6 端口绑定功能的端口上生效，端口绑定功能的具体配置请参见“[1.3.1 配置IPv6 端口绑定功能](#)”。

IPv6 静态绑定表项与 IPv6 端口绑定功能配合使用时，端口 IPv6 静态绑定表项和 IPv6 动态绑定表项的优先级高于全局 IPv6 静态绑定表项，即端口优先使用端口上的 IPv6 静态或动态绑定表项对收到的报文进行匹配，若匹配失败，再与全局 IPv6 静态绑定表项进行匹配。

1. 配置全局IPv6 静态绑定表项

全局 IPv6 静态绑定表项中定义了端口允许转发的报文的 IP 地址和 MAC 地址，对所有端口都生效。

表1-6 配置全局 IPv6 静态绑定表项

操作	命令	说明
进入系统视图	system-view	-
配置全局IPv6静态绑定表项	ipv6 source binding ipv6-address ipv6-address mac-address mac-address	必选 缺省情况下，无全局IPv6静态绑定表项

2. 配置端口IPv6 静态绑定表项

表1-7 配置端口 IPv6 静态绑定表项

操作	命令	说明
进入系统视图	system-view	-
进入二层以太网端口视图	interface <i>interface-type interface-number</i>	-
配置端口的IPv6静态绑定表项	ipv6 source binding { ipv6-address <i>ipv6-address</i> ipv6-address <i>ipv6-address</i> mac-address <i>mac-address</i> mac-address <i>mac-address</i> } [vlan <i>vlan-id</i>]	必选 缺省情况下，端口上无 IPv6静态绑定表项



说明

- 同一个表项不能在同一个端口上重复绑定，但可以在不同端口上绑定。
- 绑定表项中的 MAC 地址不能为全 0、全 F（广播 MAC）和组播 MAC。绑定表项中的 IPv6 地址必须为单播地址，不能为全 0 地址、组播地址、环回地址。
- 当 IPv6 静态绑定表项与 IP Source Guard 功能配合时，静态绑定表项中的 VLAN 参数不作为过滤报文的特征项，VLAN 参数指定与否，不影响 IP Source Guard 功能对报文的过滤结果。
- 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 IPv6 静态绑定表项的检查。关于 ND Detection 功能的相关配置请参见“安全配置指导”中的“ND 攻击防御”。
- 配置静态表项时，如果系统中已经存在相同内容的动态表项，则新添加的静态表项将会覆盖已有的动态表项。

1.3.3 配置IPv6 绑定表项数目的最大值

IPv6 绑定表项数目的最大值用于限制端口上允许添加的 IPv6 静态绑定表项和 IPv6 动态绑定表项的数量总和。当端口上的 IPv6 绑定表项数目达到指定的最大值时，端口将不再允许添加新的 IPv6 绑定表项。

表1-8 配置 IPv6 绑定表项数目的最大值

操作	命令	说明
进入系统视图	system-view	-
进入二层以太网端口视图	interface <i>interface-type interface-number</i>	-
配置IPv6绑定表项数目的最大值	ipv6 verify source max-entries <i>number</i>	可选 缺省情况下，对于S5500-28SC-HI和S5500-52SC-HI，端口上IPv6绑定表项的最大值为640；对于本系列交换机其它机型，端口上IPv6绑定表项数目的最大值为2048



说明

如果要配置的 IPv6 绑定表项数目的最大值小于当前端口上已存在的 IPv6 绑定表项总数，则该最大值可以配置成功，且原有的表项不受影响，但端口将不再允许新增 IPv6 绑定表项，除非端口上的 IPv6 绑定表项数目减少到小于最大值。

1.4 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1-9 IP Source Guard 显示和维护（IPv4）

操作	命令
显示静态绑定表项信息	display ip source binding static [interface <i>interface-type interface-number</i> ip-address <i>ip-address</i> mac-address <i>mac-address</i>] [slot <i>slot-number</i>] [{ begin exclude include } <i>regular-expression</i>]
显示绑定表项信息	display ip source binding [interface <i>interface-type interface-number</i> ip-address <i>ip-address</i> mac-address <i>mac-address</i>] [slot <i>slot-number</i>] [{ begin exclude include } <i>regular-expression</i>]

表1-10 IP Source Guard 显示和维护（IPv6）

操作	命令
显示IPv6静态绑定表项信息	display ipv6 source binding static [interface <i>interface-type interface-number</i> ipv6-address <i>ipv6-address</i> mac-address <i>mac-address</i>] [slot <i>slot-number</i>] [{ begin exclude include } <i>regular-expression</i>]
显示IPv6绑定表项信息	display ipv6 source binding [interface <i>interface-type interface-number</i> ipv6-address <i>ipv6-address</i> mac-address <i>mac-address</i>] [slot <i>slot-number</i>] [{ begin exclude include } <i>regular-expression</i>]

1.5 IP Source Guard典型配置举例

1.5.1 IPv4 静态绑定表项配置举例

1. 组网需求

如 [图 1-2](#) 所示，Host A与Host B分别与Device B的端口GigabitEthernet1/0/2、GigabitEthernet1/0/1 相连；Host C与Device A的端口GigabitEthernet1/0/2 相连。Device B接到Device A的端口 GigabitEthernet1/0/1 上。各主机均使用静态配置的IP地址。

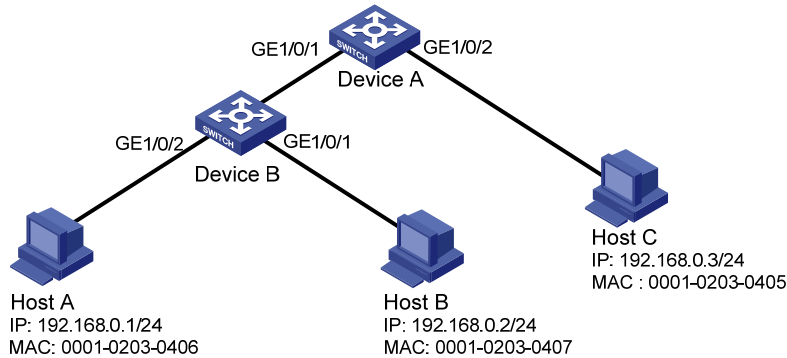
通过在 Device A 和 Device B 上配置 IPv4 静态绑定表项，可以满足以下各项应用需求：

- Device A 的端口 GigabitEthernet1/0/2 上只允许 Host C 发送的 IP 报文通过。
- Device A 的端口 GigabitEthernet1/0/1 上只允许 Host A 发送的 IP 报文通过。
- Device B 的端口 GigabitEthernet1/0/2 上只允许 Host A 发送的 IP 报文通过。

- Device B 的端口 GigabitEthernet1/0/1 上只允许使用 IP 地址 192.168.0.2/24 的主机发送的 IP 报文通过，即允许 Host B 更换网卡后仍然可以使用该 IP 地址与 Host A 互通。

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

在端口 GigabitEthernet1/0/2 上配置 IPv4 端口绑定功能，绑定源 IP 地址和 MAC 地址。

```
<DeviceA> system-view
```

```
[DeviceA] interface gigabitethernet 1/0/2
```

```
[DeviceA-GigabitEthernet1/0/2] ip verify source ip-address mac-address
```

配置 IPv4 静态绑定表项，只允许 MAC 地址为 0001-0203-0405、IP 地址为 192.168.0.3 的 Host C 发送的 IP 报文通过端口 GigabitEthernet1/0/2。

```
[DeviceA] interface gigabitethernet 1/0/2
```

```
[DeviceA-GigabitEthernet1/0/2] ip source binding ip-address 192.168.0.3 mac-address 0001-0203-0405
```

```
[DeviceA-GigabitEthernet1/0/2] quit
```

在端口 GigabitEthernet1/0/1 上配置 IPv4 端口绑定功能，绑定源 IP 地址和 MAC 地址。

```
[DeviceA] interface gigabitethernet 1/0/1
```

```
[DeviceA-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

配置 IPv4 静态绑定表项，只允许 MAC 地址为 0001-0203-0406、IP 地址为 192.168.0.1 的 Host A 发送的 IP 报文通过端口 GigabitEthernet1/0/1。

```
[DeviceA] interface gigabitethernet 1/0/1
```

```
[DeviceA-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
```

```
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 配置 Device B

在端口 GigabitEthernet1/0/2 上配置 IPv4 端口绑定功能，绑定源 IP 地址和 MAC 地址。

```
<DeviceB> system-view
```

```
[DeviceB] interface gigabitethernet1/0/2
```

```
[DeviceB-GigabitEthernet1/0/2] ip verify source ip-address mac-address
```

配置 IPv4 静态绑定表项，只允许 MAC 地址为 0001-0203-0406、IP 地址为 192.168.0.1 的 Host A 发送的 IP 报文通过端口 GigabitEthernet1/0/2。


```
[DeviceB-GigabitEthernet1/0/2] ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
```

```
[DeviceB-GigabitEthernet1/0/2] quit
```

在 GigabitEthernet1/0/1 上配置 IPv4 端口绑定功能，绑定源 IP 地址。

```
[DeviceB] interface gigabitethernet 1/0/1
```

```
[DeviceB-GigabitEthernet1/0/1] ip verify source ip-address
```

配置 IPv4 静态绑定表项，只允许 IP 地址为 192.168.0.2 的主机发送的 IP 报文通过端口 GigabitEthernet1/0/1。

```
[DeviceB-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.2
```

```
[DeviceB-GigabitEthernet1/0/1] quit
```

4. 验证配置结果

在 Device A 上显示 IPv4 静态绑定表项配置成功。

```
[DeviceA] display ip source binding static
```

Total entries found: 2

MAC Address	IP Address	VLAN	Interface	Type
0001-0203-0405	192.168.0.3	N/A	GE1/0/2	Static
0001-0203-0406	192.168.0.1	N/A	GE1/0/1	Static

在 Device B 上显示 IPv4 静态绑定表项配置成功。

```
[DeviceB] display ip source binding static
```

Total entries found: 2

MAC Address	IP Address	VLAN	Interface	Type
0001-0203-0406	192.168.0.1	N/A	GE1/0/2	Static
N/A	192.168.0.2	N/A	GE1/0/1	Static

1.5.2 与DHCP Snooping配合的IPv4 端口绑定功能配置举例

1. 组网需求

Device 通过端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别与客户端 Host 和 DHCP server 相连。

具体应用需求如下：

- Host 通过 DHCP server 获取 IP 地址。
- Device 上使能 DHCP Snooping 功能，记录 Host 的 DHCP Snooping 表项。
- 在端口 GigabitEthernet1/0/1 上启用 IPv4 端口绑定功能，利用记录的 DHCP Snooping 表项过滤端口转发的报文，仅允许通过 DHCP server 动态获取 IP 地址的客户端可以接入网络。

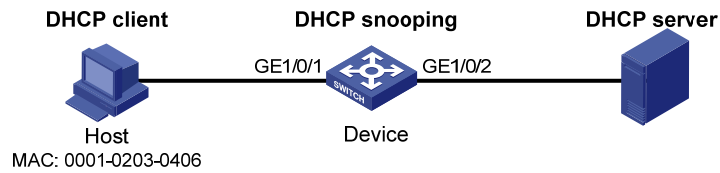


说明

DHCP server 的具体配置请参考“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 端口绑定功能组网图



3. 配置步骤

(1) 配置 DHCP Snooping

开启 DHCP Snooping 功能。

```
<Device> system-view
```

```
[Device] dhcp-snooping
```

设置与 DHCP server 相连的端口 GigabitEthernet1/0/2 为信任端口。

```
[Device] interface gigabitethernet 1/0/2
```

```
[Device-GigabitEthernet1/0/2] dhcp-snooping trust
```

```
[Device-GigabitEthernet1/0/2] quit
```

(2) 配置 IPv4 端口绑定功能

配置端口 GigabitEthernet1/0/1 的 IPv4 端口绑定功能，绑定源 IP 地址和 MAC 地址。

```
[Device] interface gigabitethernet 1/0/1
```

```
[Device-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

```
[Device-GigabitEthernet1/0/1] quit
```

4. 验证配置结果

显示端口 GigabitEthernet1/0/1 上的绑定表项信息。

```
[Device] display ip source binding
```

Total entries found: 1

MAC Address	IP Address	VLAN	Interface	Type
0001-0203-0406	192.168.0.1	1	GE1/0/1	DHCP-SNP

显示 DHCP Snooping 已有的动态表项，查看其是否和端口 GigabitEthernet1/0/1 获取的动态表项一致。

```
[Device] display dhcp-snooping
```

DHCP snooping is enabled.

The client binding table for all untrusted ports.

Type : D--Dynamic , S--Static , R--Recovering

Type	IP Address	MAC Address	Lease	VLAN	SVLAN	Interface
D	192.168.0.1	0001-0203-0406	86335	1	N/A	GigabitEthernet1/0/1

--- 1 dhcp-snooping item(s) found ---

从以上显示信息可以看出，端口 GigabitEthernet1/0/1 在配置 IPv4 端口绑定功能之后根据获取的 DHCP Snooping 表项产生了端口绑定表项。

1.5.3 与DHCP Relay配合的IPv4 端口绑定功能配置举例

1. 组网需求

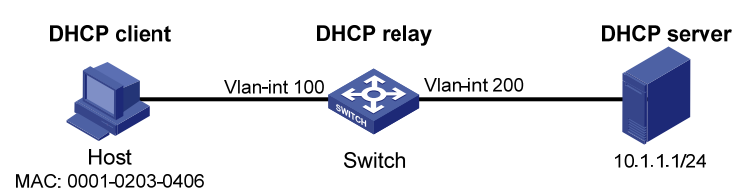
Switch 通过接口 Vlan-interface100 和 Vlan-interface200 分别与客户端 Host 和 DHCP server 相连。Switch 上使能 DHCP Relay 功能。

具体应用需求如下：

- Host（MAC 地址为 0001-0203-0406）通过 DHCP relay 从 DHCP server 上获取 IP 地址。
- 在接口 Vlan-interface100 上启用 IPv4 端口绑定功能，利用 Switch 上生成的 DHCP Relay 表项过滤端口转发的报文，仅允许通过 DHCP server 动态获取 IP 地址的客户端可以接入网络。

2. 组网图

图1-4 配置端口绑定功能组网图



3. 配置步骤

(1) 配置 IPv4 端口绑定功能

配置各接口的 IP 地址（略）。

在接口 Vlan-interface100 上配置 IPv4 端口绑定功能，绑定源 IP 地址和 MAC 地址。

```
<Switch> system-view
[Switch] vlan 100
[Switch-Vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip verify source ip-address mac-address
[Switch-Vlan-interface100] quit
```

(2) 配置 DHCP Relay

使能 DHCP 服务。

```
[Switch] dhcp enable
```

配置 DHCP 服务器的地址。

```
[Switch] dhcp relay server-group 1 ip 10.1.1.1
```

配置接口 Vlan-interface100 工作在 DHCP 中继模式。

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] dhcp select relay
# 配置接口 Vlan-interface100 对应服务器组 1。
[Switch-Vlan-interface100] dhcp relay server-select 1
[Switch-Vlan-interface100] quit
```

4. 验证配置结果

显示生成的 IPv4 绑定表项信息。

```
[Switch] display ip source binding
```

Total entries found: 1

MAC Address	IP Address	VLAN	Interface	Type
0001-0203-0406	192.168.0.1	100	Vlan100	DHCP-RLY

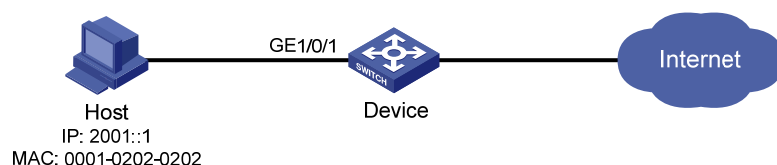
1.5.4 IPv6 静态绑定表项配置举例

1. 组网需求

IPv6 客户端通过 Device 的端口 GigabitEthernet1/0/1 接入网络。要求在 Device 上配置 IPv6 静态绑定表项，使得端口 GigabitEthernet1/0/1 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1-5 配置 IPv6 静态绑定表项组网图



3. 配置步骤

在端口 GigabitEthernet1/0/1 上配置 IPv6 端口绑定功能，绑定源 IP 地址和 MAC 地址。

```
<Device> system-view
```

```
[Device] interface gigabitethernet1/0/1
```

```
[Device-GigabitEthernet1/0/1] ipv6 verify source ipv6-address mac-address
```

在端口 GigabitEthernet1/0/1 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-GigabitEthernet1/0/1] ipv6 source binding ipv6-address 2001::1 mac-address 0001-0202-0202
```

```
[Device-GigabitEthernet1/0/1] quit
```

4. 验证配置结果

在 Device 上显示 IPv6 静态绑定表项配置成功。

```
[Device] display ipv6 source binding static
```

Total entries found: 1

MAC Address	IP Address	VLAN	Interface	Type
0001-0202-0202	2001::1	N/A	GE1/0/1	Static-IPv6

1.5.5 与DHCPv6 Snooping配合的IPv6 端口绑定功能配置举例

1. 组网需求

DHCPv6 客户端通过 Device 的端口 GigabitEthernet1/0/1 接入网络，通过 DHCPv6 server 获取 IPv6 地址。

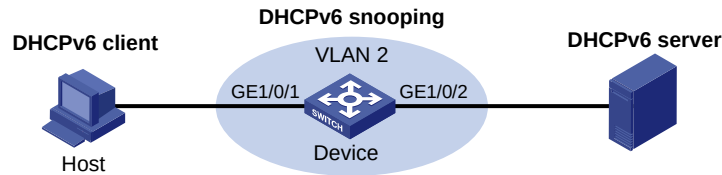
具体应用需求如下：

- 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。

- 在端口 GigabitEthernet1/0/1 上启用 IPv6 动态绑定功能，利用动态获取的 DHCPv6 Snooping 表项过滤端口转发的报文，只允许通过 DHCPv6 server 动态获取 IP 地址的客户端接入网络。

2. 组网图

图1-6 配置与 DHCPv6 Snooping 配合的 IPv6 端口绑定功能组网图



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
```

在 VLAN 2 内使能 DHCPv6 Snooping 功能。

```
[Device] vlan 2
```

```
[Device-vlan2] ipv6 dhcp snooping vlan enable
```

```
[Device] quit
```

配置端口 GigabitEthernet1/0/2 为信任端口。

```
[Device] interface gigabitethernet 1/0/2
```

```
[Device-GigabitEthernet1/0/2] ipv6 dhcp snooping trust
```

```
[Device-GigabitEthernet1/0/2] quit
```

(2) 配置 IPv6 动态绑定功能

配置端口 GigabitEthernet1/0/1 的 IPv6 动态绑定功能，绑定源 IP 地址和 MAC 地址。

```
[Device] interface gigabitethernet 1/0/1
```

```
[Device-GigabitEthernet1/0/1] ipv6 verify source ipv6-address mac-address
```

```
[Device-GigabitEthernet1/0/1] quit
```

4. 验证配置结果

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
```

```
Total entries found: 1
```

MAC Address	IP Address	VLAN	Interface	Type
040a-0000-0001	2001::1	2	GE1/0/1	DHCPv6-SNP

显示 DHCPv6 Snooping 已有的动态表项，查看其是否和端口 GigabitEthernet1/0/1 生成的 IPv6 动态绑定表项一致。

```
[Device] display ipv6 dhcp snooping user-binding dynamic
```

IP Address	MAC Address	Lease	VLAN	Interface
2001::1	040a-0000-0001	286	2	GigabitEthernet1/0/1

```

--- 1 DHCPv6 snooping item(s) found ---

```

从以上显示信息可以看出，IP Source Guard 通过获取端口 GigabitEthernet1/0/1 上产生的 DHCPv6 Snooping 表项成功生成了 IPv6 动态绑定表项。

1.5.6 与ND Snooping配合的IPv6 端口绑定功能配置举例

1. 组网需求

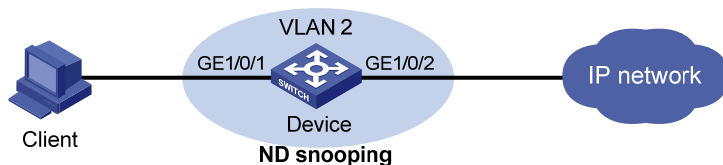
IPv6 客户端通过 Device 的端口 GigabitEthernet1/0/1 接入网络。

具体应用需求如下：

- Device 上使能 ND Snooping 功能，通过侦听 DAD NS 消息来建立 ND Snooping 表项。
- 在端口 GigabitEthernet1/0/1 上启用 IPv6 端口绑定功能，利用动态获取的 ND Snooping 表项过滤端口收到的报文，只允许合法获取 IPv6 地址的客户端可以接入网络。

2. 组网图

图1-7 配置与 ND Snooping 配合的 IPv6 端口绑定功能组网图



3. 配置步骤

(1) 配置 ND Snooping

在 VLAN 2 内使能 ND Snooping 功能。

```
<Device> system-view
[Device] vlan 2
[Device-vlan2] ipv6 nd snooping enable
[Device-vlan2] quit
```

(2) 配置 IPv6 端口绑定功能

在端口 GigabitEthernet1/0/1 上配置 IPv6 端口绑定功能，绑定源 IP 地址和 MAC 地址。

```
[Device] interface gigabitethernet1/0/1
[Device-GigabitEthernet1/0/1] ipv6 verify source ipv6-address mac-address
[Device-GigabitEthernet1/0/1] quit
```

4. 验证配置结果

在 Device 上显示生成的 IPv6 绑定表项信息。

```
[Device] display ipv6 source binding
```

Total entries found: 1

MAC Address	IP Address	VLAN	Interface	Type
040a-0000-0001	2001::1	2	GE1/0/1	ND-SNP

显示 ND Snooping 已有的动态表项，查看其是否和端口 GigabitEthernet1/0/1 获取的 IPv6 端口绑定表项一致。

```
[Device] display ipv6 nd snooping
```

IPv6 Address	MAC Address	VID	Interface	Aging Status
2001::1	040a-0000-0001	2	GE1/0/1	25 Bound

---- Total entries: 1 ----

从以上显示信息可以看出，IP Source Guard 通过获取端口 GigabitEthernet1/0/1 上产生的 ND Snooping 表项成功生成了 IPv6 动态绑定表项。

1.5.7 全局地址绑定配置举例

1. 组网需求

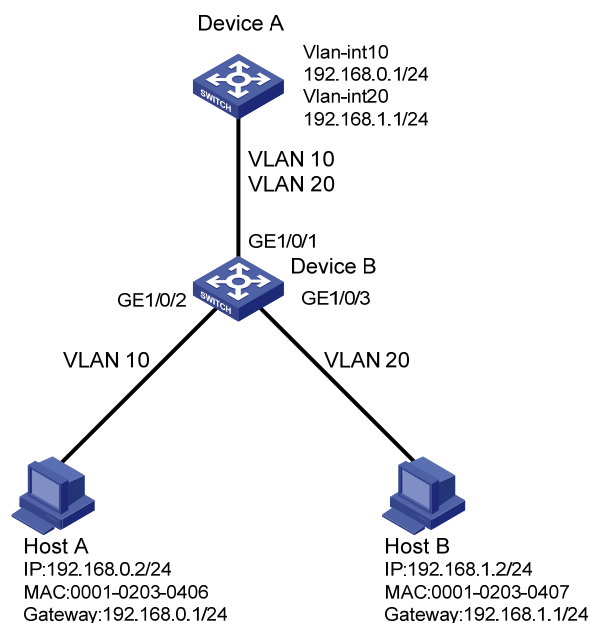
Device A 为汇聚设备，Device B 为接入设备，VLAN 10 中的 Host A 与 VLAN 20 中的 Host B 通过 Device A 进行通信。

具体应用需求如下：

- Device B 上阻止仿冒 Host A 和 Host B 的 IP 报文通过。
- Host A 和 Host B 之间的报文可在 Device B 上正常转发。

2. 组网图

图1-8 全局地址绑定典型配置组网图



3. 配置步骤

创建 VLAN 10，并将端口 GigabitEthernet1/0/2 加入 VLAN 10。

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] port gigabitethernet1/0/2
[DeviceB-vlan10] quit
```

创建 VLAN 20，并将端口 GigabitEthernet1/0/3 加入 VLAN 20。

```
[DeviceB] vlan 20
[DeviceB-vlan20] port gigabitethernet1/0/3
[DeviceB-vlan20] quit
```

将端口 GigabitEthernet1/0/1 的链路类型配置为 Trunk，并允许 VLAN 10 和 VLAN 20 的报文通过。

```
[DeviceB] interface gigabitethernet1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 10 20
[DeviceB-GigabitEthernet1/0/1] quit
# 在端口 GigabitEthernet1/0/2 和端口 GigabitEthernet1/0/3 上分别配置 IPv4 端口绑定功能，绑定
源 IP 地址和 MAC 地址。
[DeviceB] interface gigabitethernet1/0/2
[DeviceB-GigabitEthernet1/0/2] ip verify source ip-address mac-address
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet1/0/3
[DeviceB-GigabitEthernet1/0/3] ip verify source ip-address mac-address
[DeviceB-GigabitEthernet1/0/3] quit
# 配置全局静态绑定表项，阻止仿冒 Host A（IP 地址：192.168.0.2、MAC 地址：0001-0203-0406）
和 Host B（IP 地址：192.168.1.2、MAC 地址：0001-0203-0407）的 IP 报文通过。
[DeviceB] ip source binding ip-address 192.168.0.2 mac-address 0001-0203-0406
[DeviceB] ip source binding ip-address 192.168.1.2 mac-address 0001-0203-0407
```

4. 验证配置结果

在 Device 上显示配置的 IPv4 静态绑定表项信息。

```
[DeviceB] display ip source binding static
Total entries found: 2
  MAC Address      IP Address      VLAN   Interface      Type
  0001-0203-0406   192.168.0.2     N/A    N/A            Static
  0001-0203-0407   192.168.1.2     N/A    N/A            Static
```

以上配置完成后，Host A 和 Host B 能够成功 ping 通对方。

1.6 常见配置错误举例

1.6.1 静态绑定表项配置和端口绑定功能配置失败

1. 故障现象

在端口上配置静态绑定表项、配置端口绑定功能均失败。

2. 故障分析

IP Source Guard 功能不能在加入聚合组或加入业务环回组的端口上配置。

3. 处理过程

将端口退出已加入的聚合组或业务环回组。

目 录

1 ARP攻击防御配置	1-1
1.1 ARP攻击防御简介	1-1
1.2 ARP攻击防御配置任务简介	1-1
1.3 配置ARP防止IP报文攻击功能	1-2
1.3.1 ARP防止IP报文攻击功能简介	1-2
1.3.2 配置ARP防止IP报文攻击功能	1-2
1.3.3 ARP防止IP报文攻击显示和维护	1-3
1.3.4 ARP防止IP报文攻击配置举例	1-3
1.4 配置ARP报文限速功能	1-5
1.4.1 ARP报文限速功能简介	1-5
1.4.2 配置ARP报文限速功能	1-5
1.5 配置源MAC地址固定的ARP攻击检测功能	1-6
1.5.1 源MAC地址固定的ARP攻击检测功能简介	1-6
1.5.2 配置源MAC地址固定的ARP攻击检测功能	1-6
1.5.3 源MAC地址固定的ARP攻击检测显示和维护	1-7
1.5.4 源MAC地址固定的ARP攻击检测功能配置举例	1-7
1.6 配置ARP报文源MAC地址一致性检查功能	1-8
1.6.1 ARP报文源MAC地址一致性检查功能简介	1-8
1.6.2 配置ARP报文源MAC地址一致性检查功能	1-8
1.7 配置ARP主动确认功能	1-9
1.7.1 ARP主动确认功能简介	1-9
1.7.2 配置ARP主动确认功能	1-9
1.8 配置ARP Detection功能	1-9
1.8.1 ARP Detection功能简介	1-9
1.8.2 配置ARP Detection功能	1-11
1.8.3 ARP Detection显示和维护	1-13
1.8.4 用户合法性检查配置举例	1-13
1.8.5 用户合法性检查和报文有效性检查配置举例	1-15
1.8.6 ARP报文强制转发配置举例	1-16
1.9 配置ARP自动扫描、固化功能	1-18
1.9.1 ARP自动扫描、固化功能简介	1-18
1.9.2 配置ARP自动扫描、固化功能	1-18
1.10 配置ARP网关保护功能	1-19

1.10.1 ARP网关保护功能简介	1-19
1.10.2 配置ARP网关保护功能	1-19
1.10.3 ARP网关保护功能配置举例	1-20
1.11 配置ARP过滤保护功能	1-21
1.11.1 ARP过滤保护功能简介	1-21
1.11.2 配置ARP过滤保护功能	1-21
1.11.3 ARP过滤保护功能配置举例	1-21

1 ARP攻击防御配置



说明

ARP 攻击防御功能中所指的“接口”为三层口，包括 VLAN 接口、三层以太网端口等。三层以太网端口是指被配置为三层模式的以太网端口，有关以太网端口模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口配置”。

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 and 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ARP报文限速功能		可选 建议在接入设备上配置本功能	1.4
	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	1.5
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	1.6
	配置ARP主动确认功能		可选 建议在网关设备上配置本功能	1.7

配置任务		说明	详细配置
	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：

- 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，以每 5 秒为单位时间，当在 5 秒的单位时间内由某特定主机发出 IP 报文触发的 ARP 请求报文的数量超过设置的阈值，那么对这台主机随后发出的所有 IP 报文，设备不允许其再触发 ARP 请求，并丢弃这些 IP 报文。直至这 5 秒结束后，设备允许这台主机重新触发 ARP 请求，并重复以上的操作，从而避免了恶意攻击所造成的危害。
- 如果发送攻击报文的源不固定，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	必选 缺省情况下，ARP源抑制功能处于关闭状态

操作	命令	说明
配置ARP源抑制的阈值	arp source-suppression limit <i>limit-value</i>	可选 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	-
使能ARP黑洞路由功能	arp resolving-route enable	必选 缺省情况，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 源抑制显示和维护

操作	命令
显示ARP源抑制的配置信息	display arp source-suppression [{ begin exclude include } regular-expression]

1.3.4 ARP防止IP报文攻击配置举例

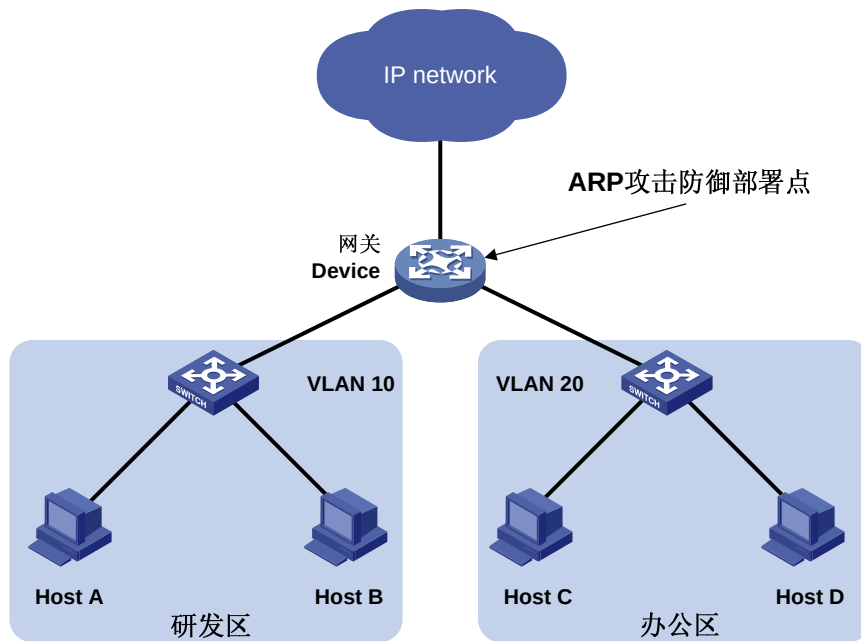
1. 组网需求

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：

- (1) 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。
- (2) 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

- (1) 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
```

- (2) 配置 ARP 黑洞路由功能

使能 ARP 黑洞路由功能。

```
<Device> system-view
[Device] arp resolving-route enable
```

1.4 配置ARP报文限速功能

1.4.1 ARP报文限速功能简介

ARP 报文限速功能是指对上送 CPU 的 ARP 报文进行限速，可以防止大量 ARP 报文对 CPU 进行冲击。例如，在配置了 ARP Detection 功能后，设备会将收到的 ARP 报文重定向到 CPU 进行检查，这样引入了新的问题：如果攻击者恶意构造大量 ARP 报文发往设备，会导致设备的 CPU 负担过重，从而造成其他功能无法正常运行甚至设备瘫痪，这个时候可以启用 ARP 报文限速功能来控制上送 CPU 的 ARP 报文的速率。

推荐用户在配置了 ARP Detection、ARP Snooping 或者发现有 ARP 泛洪攻击的情况下，使用 ARP 报文限速功能。

1.4.2 配置ARP报文限速功能

使能 ARP 报文限速功能后，当端口上收到的 ARP 报文速率超过用户设定的限速值时，设备就会发送 ARP 超速的 Trap 和 Log 信息。为防止过多的 Trap 和 Log 信息干扰用户工作，用户可以设定信息的发送时间间隔。当用户设定的时间间隔超时时，设备将这个时间间隔内的超速峰值作为 Trap 和 Log 的速率值打印出来。

需要注意的是，只有开启了 ARP 报文限速的 Trap 功能后，才会生成 Trap 报文。

生成的 Trap 和 Log 报文将被发送到设备的信息中心，通过设置信息中心的参数，最终决定 Trap 和 Log 报文的输出规则（即是否允许输出以及输出方向）。（有关信息中心参数的配置请参见“网络管理和监控配置指导”中的“信息中心”。）

表1-5 配置 ARP 报文限速功能

操作	命令	说明
进入系统视图	system-view	-
开启ARP报文限速Trap功能	snmp-agent trap enable arp rate-limit	可选 缺省情况下，ARP报文限速Trap功能处于开启状态
配置当端口上的ARP报文速率超过用户设定的限速值时，设备发送Trap和Log的时间间隔	arp rate-limit interval seconds information	可选 缺省情况下，设备发送ARP超速Trap和Log的时间间隔为60秒
进入二层以太网端口/二层聚合接口视图	interface interface-type interface-number	-
配置ARP报文限速功能	arp rate-limit { disable rate pps drop }	必选 缺省情况下，ARP报文限速功能处于关闭状态



说明

- 如果在二层聚合接口上配置了 ARP 报文限速功能,则只要聚合成员端口上的 ARP 报文速率超过用户设定的限速值,就会发送 Trap 和 Log 信息。
- **snmp-agent trap enable arp rate-limit** 命令的详细介绍请参见“网络管理和监控命令参考 /SNMP”中的 **snmp-agent trap enable** 命令。

1.5 配置源MAC地址固定的ARP攻击检测功能

1.5.1 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 地址进行统计,在 5 秒内,如果收到同一源 MAC 地址的 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 Log 信息并且将该源 MAC 地址发送的 ARP 报文过滤掉;如果设置的模式为监控模式,则只打印 Log 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 MAC 地址存在攻击也不会被检测、过滤。

只对上送 CPU 的 ARP 报文进行统计。

1.5.2 配置源MAC地址固定的ARP攻击检测功能

表1-6 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 anti-attack source-mac { filter monitor }	必选 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 anti-attack source-mac threshold threshold-value	可选 缺省情况下,源MAC固定ARP报文攻击检测阈值为50
配置源MAC地址固定的ARP攻击检测表项的老化时间	arp anti-attack source-mac aging-time time	可选 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
配置保护MAC地址	arp anti-attack source-mac exclude-mac mac-address&<1-10>	可选 缺省情况下,没有配置任何保护MAC地址



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。

1.5.3 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1-7 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	display arp anti-attack source-mac { slot <i>slot-number</i> interface <i>interface-type</i> <i>interface-number</i> } [{ begin exclude include } <i>regular-expression</i>]

1.5.4 源MAC地址固定的ARP攻击检测功能配置举例

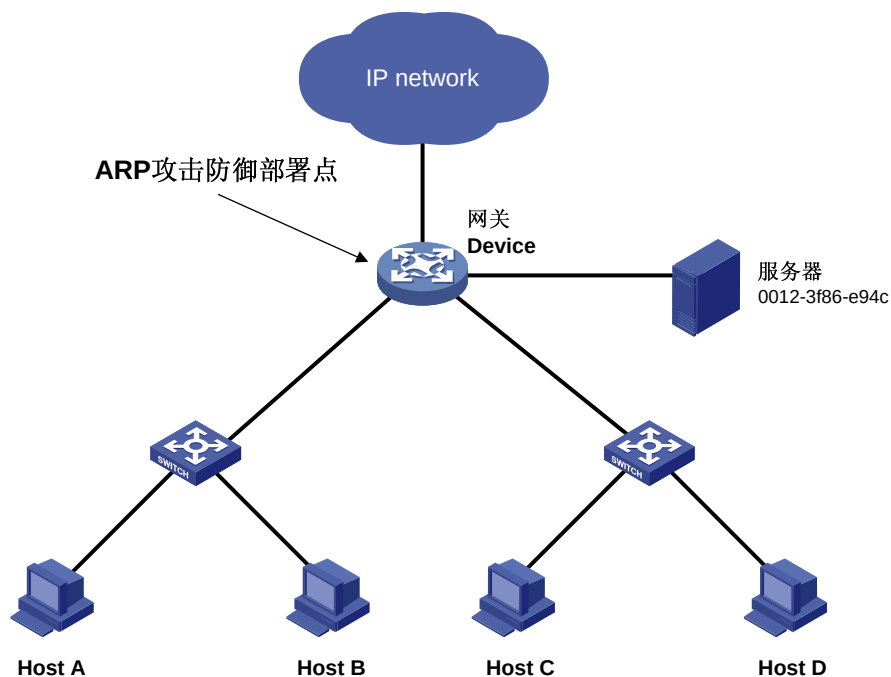
1. 组网需求

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 anti-attack source-mac filter
# 配置源 MAC 固定 ARP 报文攻击检测阈值为 30 个。
[Device] arp anti-attack 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 anti-attack 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 anti-attack source-mac exclude-mac 0012-3f86-e94c
```

1.6 配置ARP报文源MAC地址一致性检查功能

1.6.1 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。

1.6.2 配置ARP报文源MAC地址一致性检查功能

表1-8 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 anti-attack valid-check enable	必选 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

1.7 配置ARP主动确认功能

1.7.1 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”。

1.7.2 配置ARP主动确认功能

表1-9 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 anti-attack active-ack enable	必选 缺省情况下，ARP主动确认功能处于关闭状态

1.8 配置ARP Detection功能

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 报文强制转发和 ARP Detection 日志功能。

1. 用户合法性检查

对于 ARP 信任端口，不进行用户合法性检查；对于 ARP 非信任端口，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 所在端口上的合法用户，包括基于配置规则的检查、基于 IP Source Guard 静态绑定表项的检查、基于 DHCP Snooping 安全表项的检查、基于 802.1X 安全表项的检查和 OUI MAC 地址的检查。

- (1) 首先进行基于配置规则的检查。如果在配置的规则中找到与报文匹配的规则，则按照规则对 ARP 报文进行处理。如果在配置的规则中没有找到与报文匹配的规则，继续进行基于 IP Source Guard 静态绑定表项的检查、基于 DHCP Snooping 安全表项的检查、基于 802.1X 安全表项的检查和 OUI MAC 地址的检查。
- (2) 在基于配置规则的检查之后，如果未匹配，则进行基于 IP Source Guard 静态绑定表项检查。如果找到了对应源 IP 地址和源 MAC 地址的静态绑定表项，认为该 ARP 报文合法，进行转发。如果找到了对应源 IP 地址的静态绑定表项但源 MAC 地址不符，认为该 ARP 报文非法，进行丢弃。如果没有找到对应源 IP 地址的静态绑定表项，继续进行 DHCP Snooping 安全表项、802.1X 安全表项和 OUI MAC 地址检查。

- (3) 在基于 IP Source Guard 静态绑定表项检查之后, 如果未匹配, 则进行基于 DHCP Snooping 安全表项、802.1X 安全表项和 OUI MAC 地址检查, 只要符合三者中任何一个, 就认为该 ARP 报文合法, 进行转发。其中, OUI MAC 地址检查指的是, 只要 ARP 报文的源 MAC 地址为 OUI MAC 地址, 并且使能了 Voice VLAN 功能, 就认为是合法报文, 检查通过。
- (4) 如果所有检查都没有找到匹配项, 则认为是非法报文, 直接丢弃。
-



说明

- 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”。
 - 802.1X 安全表项通过 802.1X 功能产生, 802.1X 用户需要使用可以将 IP 地址上传的客户端, 用户通过了 802.1X 认证并且将 IP 地址上传至使能 ARP Detection 的设备后, 设备自动生成可用于 ARP Detection 的用户合法性检查的 802.1X 安全表项。802.1X 的详细介绍请参见“安全配置指导”中的“802.1X”。
 - 关于 Voice VLAN 和 OUI MAC 地址的详细介绍请参见“二层技术-以太网交换配置指导”中的“Voice VLAN”。
-

2. ARP 报文有效性检查

对于 ARP 信任端口, 不进行报文有效性检查; 对于 ARP 非信任端口, 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。

- 对于源 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;
- 对于目的 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, 无效的报文需要被丢弃;
- 对于 IP 地址检查模式, 会检查 ARP 报文中的源 IP 和目的 IP 地址, 全 0、全 1、或者组播 IP 地址都是不合法的, 需要丢弃。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 信任端口接收到的 ARP 报文不受此功能影响, 按照正常流程进行转发; 对于从 ARP 非信任端口接收到的、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, 通过信任端口进行转发;
- 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 应答报文通过信任端口进行转发。

4. ARP Detection日志功能



说明

仅 R5206 及以上版本支持此特性。

在开启 ARP Detection 日志功能后，设备在检测到非法 ARP 报文时将生成检测日志，日志内容包括：

- 受到攻击的端口编号
- 用于攻击的 ARP 报文中源 IP 地址
- 丢弃的攻击 ARP 报文数量

例如 “Detected an inspection occurred on interface GigabitEthernet1/0/1 with IP address 172.18.48.55 (Totally 10 packets dropped).”

1.8.2 配置ARP Detection功能



说明

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. 配置用户合法性检查功能

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	-
配置用户合法性检查的规则	arp detection id-number { permit deny } ip { any ip-address [ip-address-mask] } mac { any mac-address [mac-address-mask] } [vlan vlan-id]	可选 缺省情况下，没有配置用户合法性检查的规则
进入VLAN视图	vlan vlan-id	-
使能ARP Detection功能	arp detection enable	必选 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	-
进入二层以太网端口或者二层聚合接口视图	interface interface-type interface-number	-
将不需要进行用户合法性检查的端口配置为ARP信任端口	arp detection trust	可选 缺省情况下，端口为ARP非信任端口



说明

- 配置用户合法性检查功能时，必须至少配置用户合法性检查的规则、IP Source Guard 静态绑定表项、DHCP Snooping 功能、802.1X 功能四者之一，否则所有从 ARP 非信任端口收到的 ARP 报文都将被丢弃（使能了 Voice VLAN 功能的情况下，源 MAC 地址为 OUI MAC 地址的 ARP 报文不会被丢弃）。
- 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。

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 <i>vlan-id</i>	-
使能ARP Detection功能	arp detection enable	必选 缺省情况下，ARP Detection功能处于关闭状态
退回系统视图	quit	-
使能ARP报文有效性检查功能	arp detection validate { <i>dst-mac</i> <i>ip</i> <i>src-mac</i> } *	必选 缺省情况下，ARP报文有效性检查功能处于关闭状态
进入二层以太网端口或者二层聚合接口视图	interface <i>interface-type</i> <i>interface-number</i>	-
将不需要进行ARP报文有效性检查的端口配置为ARP信任端口	arp detection trust	可选 缺省情况下，端口为ARP非信任端口

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 <i>vlan-id</i>	-
使能ARP报文强制转发功能	arp restricted-forwarding enable	必选 缺省情况下，ARP报文强制转发功能处于关闭状态

4. 配置ARP Detection日志功能

表1-13 配置 ARP Detection 日志功能

操作	命令	说明
进入系统视图	system-view	-
开启ARP Detection日志功能	arp detection log enable	可选 缺省情况下，ARP Detection日志功能处于开启状态

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1-14 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 [{ begin exclude include } <i>regular-expression</i>]
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 <i>interface-type interface-number</i>] [{ begin exclude include } <i>regular-expression</i>]
清除ARP Detection的统计信息	reset arp detection statistics [interface <i>interface-type interface-number</i>]

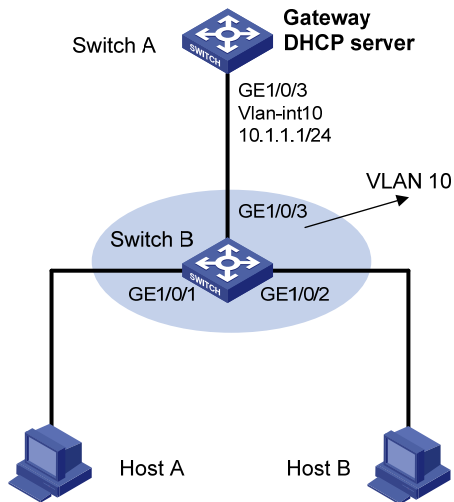
1.8.4 用户合法性检查配置举例

1. 组网需求

- Switch A 是 DHCP 服务器；Switch B 是支持 802.1X 的设备，在 VLAN 10 内启用 ARP Detection 功能，对认证客户端进行保护，保证合法用户可以正常转发报文，否则丢弃。
- Host A 和 Host B 是本地 802.1X 接入用户。

2. 组网图

图1-3 配置用户合法性检查组网图



3. 配置步骤

(1) 配置组网图中所有端口属于 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) 配置客户端 Host A 和 Host B（略），必须使用上传 IP 地址方式。

(4) 配置设备 Switch B

配置 802.1X 功能。

```
<SwitchB> system-view
[SwitchB] dot1x
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] dot1x
[SwitchB-GigabitEthernet1/0/1] quit
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] dot1x
[SwitchB-GigabitEthernet1/0/2] quit
```

添加本地接入用户。

```
[SwitchB] local-user test
[SwitchB-luser-test] service-type lan-access
[SwitchB-luser-test] password simple test
[SwitchB-luser-test] 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
```


端口状态缺省为非信任状态，上行端口配置为信任状态，下行端口按缺省配置。

```
[SwitchB-vlan10] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] arp detection trust
[SwitchB-GigabitEthernet1/0/3] quit
```

完成上述配置后，对于端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 收到的 ARP 报文，需基于 802.1X 安全表项进行用户合法性检查。

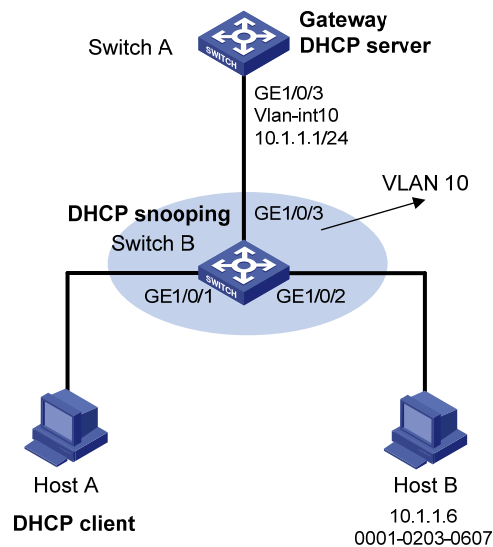
1.8.5 用户合法性检查和报文有效性检查配置举例

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 客户端和用户进行保护，保证合法用户可以正常转发报文，否则丢弃。

2. 组网图

图1-4 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) 配置组网图中所有端口属于 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
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] dhcp-snooping trust
[SwitchB-GigabitEthernet1/0/3] 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
# 端口状态缺省为非信任状态，上行端口配置为信任状态，下行端口按缺省配置。
[SwitchB-vlan10] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] arp detection trust
[SwitchB-GigabitEthernet1/0/3] quit
# 在端口 GigabitEthernet1/0/2 上配置 IP Source Guard 静态绑定表项。
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] ip source binding ip-address 10.1.1.6 mac-address
0001-0203-0607 vlan 10
[SwitchB-GigabitEthernet1/0/2] 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，对于端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 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。

1.8.6 ARP报文强制转发配置举例

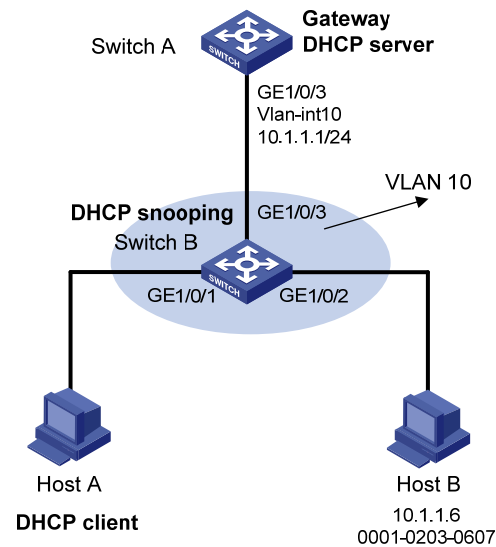
1. 组网需求

- 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，GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 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1-5 配置 ARP 报文强制转发组网图



3. 配置步骤

(1) 配置组网图中所有端口属于 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
[SwitchB] interface gigabitEthernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] dhcp-snooping trust
[SwitchB-GigabitEthernet1/0/3] 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
# 端口状态缺省为非信任状态，上行端口配置为信任状态，下行端口按缺省配置。
[SwitchB-vlan10] interface gigabitEthernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] arp detection trust
[SwitchB-GigabitEthernet1/0/3] quit
```

在端口 GigabitEthernet1/0/2 上配置 IP Source Guard 静态绑定表项。

```
[SwitchB] interface gigabitEthernet 1/0/2
```

```
[SwitchB-GigabitEthernet1/0/2] ip source binding ip-address 10.1.1.6 mac-address 0001-0203-0607 vlan 10
[SwitchB-GigabitEthernet1/0/2] 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] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port-isolate enable
[SwitchB-GigabitEthernet1/0/1] quit
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port-isolate enable
[SwitchB-GigabitEthernet1/0/2] quit
```

完成上述配置后，对于端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 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端口 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，可以有效的防止攻击者修改 ARP 表项。

 说明

推荐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

表1-15 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 <i>interface-type</i> <i>interface-number</i>	-

操作	命令	说明
启动ARP自动扫描功能	arp scan [<i>start-ip-address to end-ip-address</i>]	必选
退回系统视图	quit	-
配置ARP固化功能	arp fixup	必选

说明

- 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。
- 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。
- 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。
- 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

1.10.1 ARP网关保护功能简介

在设备上不与网关相连的端口上配置此功能，可以防止伪造网关攻击。

在端口配置此功能后，当端口收到 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

表1-16 配置 ARP 网关保护功能

操作	命令	说明
进入系统视图	system-view	-
进入二层以太网端口视图/二层聚合接口视图	interface <i>interface-type interface-number</i>	-
开启ARP网关保护功能，配置被保护的网关IP地址	arp filter source <i>ip-address</i>	必选 缺省情况下，ARP网关保护功能处于关闭状态



说明

- 每个端口最多支持配置 8 个被保护的网关 IP 地址。
- 不能在同一个端口下同时配置命令 **arp filter source** 和 **arp filter binding**。
- 本功能与 ARP Detection 和 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进行其他配合功能的处理。

1.10.3 ARP网关保护功能配置举例

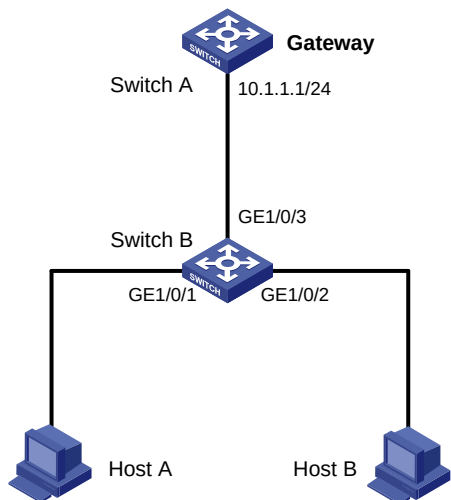
1. 组网需求

与 Switch B 相连的 Host B 进行了伪造网关 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：通过配置防止这种伪造网关攻击。

2. 组网图

图1-6 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 1/0/1
[SwitchB-GigabitEthernet1/0/1] arp filter source 10.1.1.1
[SwitchB-GigabitEthernet1/0/1] quit
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] 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

1.11.1 ARP过滤保护功能简介

本功能用来限制端口下允许通过的 ARP 报文，可以防止仿冒网关和仿冒用户的攻击。

在端口配置此功能后，当端口收到 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

表1-17 配置 ARP 过滤保护功能

操作	命令	说明
进入系统视图	system-view	-
进入二层以太网端口视图/二层聚合接口视图	interface <i>interface-type</i> <i>interface-number</i>	-
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 <i>ip-address</i> <i>mac-address</i>	必选 缺省情况下，ARP过滤保护功能处于关闭状态



说明

- 每个端口最多支持配置 8 组允许通过的 ARP 报文的源 IP 地址和源 MAC 地址。
- 不能在同一端口下同时配置命令 **arp filter source** 和 **arp filter binding**。
- 本功能与 ARP Detection 和 ARP Snooping 功能配合使用时，先进行本功能检查，本功能检查通过后会进行其他配合功能的处理。

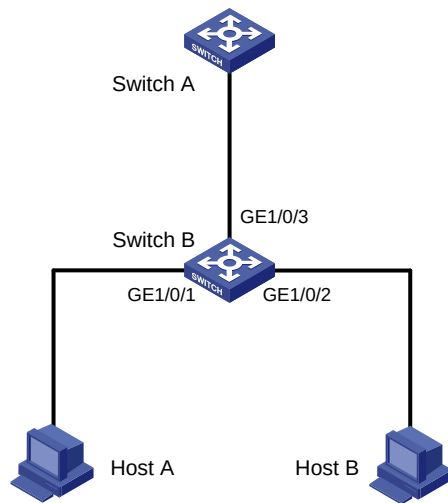
1.11.3 ARP过滤保护功能配置举例

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 GigabitEthernet1/0/1、GigabitEthernet1/0/2 端口只允许指定用户接入，不允许其他用户接入。

2. 组网图

图1-7 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 1/0/1
[SwitchB-GigabitEthernet1/0/1] arp filter binding 10.1.1.2 000f-e349-1233
[SwitchB-GigabitEthernet1/0/1] quit
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] arp filter binding 10.1.1.3 000f-e349-1234
```

完成上述配置后，端口 GigabitEthernet1/0/1 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；端口 GigabitEthernet1/0/2 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 ND攻击防御配置	1-1
1.1 ND攻击防御简介	1-1
1.2 配置ND协议报文源MAC地址一致性检查功能	1-2
1.3 配置ND Detection功能	1-3
1.3.1 ND Detection功能简介	1-3
1.3.2 配置ND Detection功能	1-4
1.3.3 ND Detection功能显示和维护	1-4
1.3.4 ND Detection功能配置举例	1-5

1 ND攻击防御配置

1.1 ND攻击防御简介

IPv6 ND（Neighbor Discovery，邻居发现）协议使用五种类型的 ICMPv6 消息，实现下面五种功能：地址解析、验证邻居是否可达、重复地址检测、路由器发现/前缀发现及地址自动配置、重定向。

ND 协议使用的五种 ICMPv6 消息如下：

- 邻居请求消息 NS（Neighbor Solicitation）
- 邻居通告消息 NA（Neighbor Advertisement）
- 路由器请求消息 RS（Router Solicitation）
- 路由器通告消息 RA（Router Advertisement）
- 重定向消息 RR（Redirect）



说明

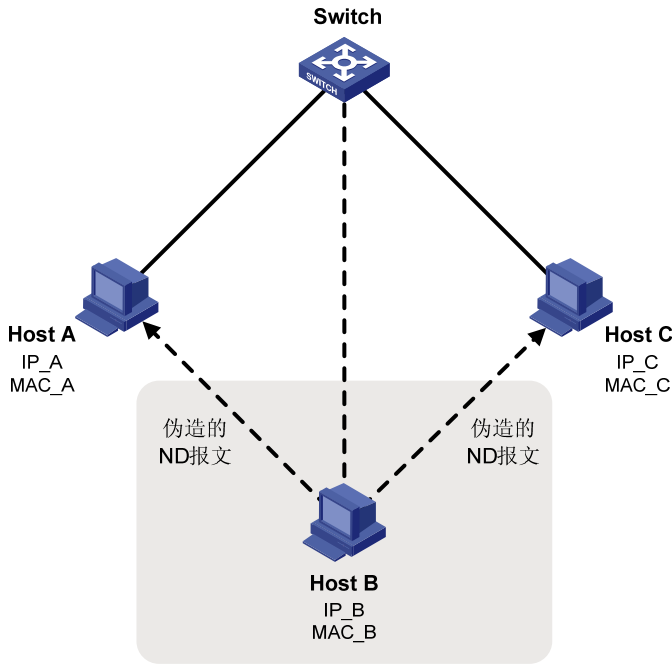
关于 ND 协议五种功能的详细介绍，请参见“三层技术-IP 业务配置指导”中的“IPv6 基础”。

ND 协议功能强大，但是却没有任何安全机制，容易被攻击发起者利用。

如 [图 1-1](#) 所示，当设备 Switch 作为二层接入设备时，攻击者 Host B 可以仿冒其他用户、仿冒网关发送伪造的 ND 报文，对网络进行攻击：

- 如果攻击者仿冒其他用户的 IP 发送 NS/NA/RS 报文，将会改写网关或者其他用户的 ND 表项，导致被仿冒用户的报文错误的发送到攻击者的 PC 上。
- 如果攻击者仿冒网关发送 RA 报文，会导致其它用户的 IPv6 配置参数错误和 ND 表项被改写。

图1-1 ND 攻击示意图



伪造的 ND 报文具有如下特点：

- 伪造的 ND 报文中源 MAC 地址和源链路层选项地址中的 MAC 地址不一致。
- 伪造的 ND 报文中源 IPv6 地址和源 MAC 地址的映射关系不是合法用户真实的映射关系。

根据上述攻击报文的特点，设备开发了多种功能对 ND 攻击进行检测，可以有效地防范 ND 攻击带来的危害。

1.2 配置ND协议报文源MAC地址一致性检查功能

ND 协议报文源 MAC 地址一致性检查功能主要应用于网关设备上，防御 ND 协议报文中的源 MAC 地址和源链路层选项地址中的 MAC 地址不同的 ND 攻击。

配置本特性后，网关设备会对接收的 ND 协议报文进行检查。如果 ND 协议报文中的源 MAC 地址和源链路层选项地址中的 MAC 地址不同，则认为是攻击报文，将其丢弃。

表1-1 配置 ND 协议报文源 MAC 地址一致性检查功能

操作	命令	说明
进入系统视图	system-view	-
使能ND协议报文源MAC地址一致性检查功能	ipv6 nd mac-check enable	可选 缺省情况下，ND协议报文源MAC地址一致性检查功能处于关闭状态



注意

- 对于 VRRP 组网，目前 NA 回复报文的源 MAC 地址和源链路层选项地址中的 MAC 地址都是不一致的，因此对于 VRRP 组网不要使能 ND 协议报文源 MAC 地址一致性检查功能。
-

1.3 配置ND Detection功能

1.3.1 ND Detection功能简介

ND Detection 功能主要应用于接入设备上，检查用户的合法性。对于合法用户的 ND 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。

ND Detection 功能将接入设备上的端口分为两种：ND 信任端口、ND 非信任端口。

- 对于 ND 信任端口，不进行用户合法性检查；
- 对于 ND 非信任端口，如果收到 RA 和 RR 消息，则认为是非法报文直接丢弃，如果收到其它类型的 ND 报文，则需要对用户合法性检查，以防止仿冒用户的攻击。

用户合法性检查是根据 ND 报文中源 IPv6 地址和源 MAC 地址，检查用户是否是报文收到端口所属 VLAN 上的合法用户，包括基于 IP Source Guard 的 IPv6 静态绑定表项的检查、基于 ND Snooping 表项的检查和基于 DHCPv6 Snooping 安全表项的检查。在这三种表项都存在的情况下，检查过程如下：

- 首先进行基于 IP Source Guard 的 IPv6 静态绑定表项检查。如果找到了对应源 IPv6 地址和源 MAC 地址的静态绑定表项，认为该 ND 报文合法，进行转发。如果找到了对应源 IPv6 地址的静态绑定表项但源 MAC 地址不符，认为该 ND 报文非法，进行丢弃。如果没有找到对应源 IPv6 地址的静态绑定表项，继续进行 DHCPv6 Snooping 安全表项、ND Snooping 安全表项检查。
 - 在基于 IP Source Guard 的 IPv6 静态绑定表项检查之后，如果未匹配，则进行基于 DHCPv6 Snooping 安全表项、ND Snooping 安全表项检查，只要符合两者中任何一个，就认为该 ND 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。
-



说明

- IP Source Guard 的 IPv6 静态绑定表项通过 **ipv6 source binding** 命令生成，详细介绍请参见“安全配置指导”中的“IP Source Guard”。
 - DHCPv6 Snooping 安全表项通过 DHCPv6 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“DHCPv6 Snooping”。
 - ND Snooping 安全表项通过 ND 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“IPv6 基础”。
-

1.3.2 配置ND Detection功能

表1-2 配置 ND Detection 功能

操作	命令	说明
进入系统视图	system-view	-
进入VLAN视图	vlan <i>vlan-id</i>	-
使能ND Detection功能	ipv6 nd detection enable	必选 缺省情况下，ND 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	-
进入二层以太网端口视图或二层聚合接口视图	interface <i>interface-type</i> <i>interface-number</i>	-
将不需要进行用户合法性检查的端口配置为ND信任端口	ipv6 nd detection trust	可选 缺省情况下，端口为ND非信任端口



说明

- 配置 ND Detection 功能时，必须至少配置 IP Source Guard 的 IPv6 静态绑定表项、DHCPv6 Snooping 功能、ND Snooping 功能三者之一，否则所有从 ND 非信任端口收到的 ND 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 ND 报文将无法通过基于 IP Source Guard 静态绑定表项的检查。



注意

目前在设备上开启 ND Detection 功能后，不会对链路本地地址类型的 ND 报文进行用户合法性检查。

1.3.3 ND Detection功能显示和维护

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 ND 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 ND Detection 的统计信息。

表1-3 ND Detection 功能显示和维护

操作	命令
显示ND Detection的配置信息	display ipv6 nd detection [<i>{ begin exclude include } regular-expression</i>]
显示ND Detection进行用户合法性检查时丢弃报文的统计信息	display ipv6 nd detection statistics [<i>interface interface-type interface-number</i>] [<i>{ begin exclude include } regular-expression</i>]

操作	命令
清除ND Detection的统计信息	reset ipv6 nd detection statistics [interface <i>interface-type</i> <i>interface-number</i>]

1.3.4 ND Detection功能配置举例

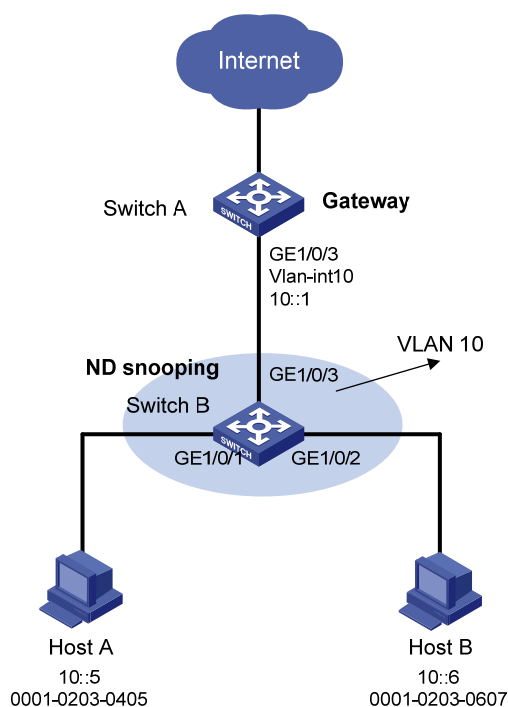
1. 组网需求

用户 Host A 和 Host B 通过 Switch B 接入网关 Switch A。用户 Host A 的 IPv6 地址是 10::5，MAC 地址是 0001-0203-0405。用户 Host B 的 IPv6 地址是 10::6，MAC 地址是 0001-0203-0607。

要求：在 Switch B 上启用 ND Detection 功能对用户的合法性进行检查，保证合法用户的报文可以被正常转发，非法用户的报文被丢弃。

2. 组网图

图1-2 配置 ND Detection 组网图



3. 配置步骤

(1) 配置 Switch A

使能 IPv6 转发功能。

```
<SwitchA> system-view
```

```
[SwitchA] ipv6
```

创建 VLAN 10。

```
[SwitchA] vlan 10
```

```
[SwitchA-vlan10] quit
```

配置端口 GigabitEthernet1/0/3 允许 VLAN 10 的报文通过。

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 10
[SwitchA-GigabitEthernet1/0/3] quit
```

配置 VLAN 接口 10 的 IPv6 地址。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ipv6 address 10::1/64
[SwitchA-Vlan-interface10] quit
```

(2) 配置 Switch B

使能 IPv6 转发功能。

```
<SwitchB> system-view
```

```
[SwitchB] ipv6
```

创建 VLAN 10。

```
[SwitchB] vlan 10
[SwitchB-vlan10] quit
```

配置端口 GigabitEthernet1/0/1~GigabitEthernet1/0/3 允许 VLAN 10 的报文通过。

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port access vlan 10
[SwitchB-GigabitEthernet1/0/1] quit
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port access vlan 10
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port link-type trunk
[SwitchB-GigabitEthernet1/0/3] port trunk permit vlan 10
[SwitchB-GigabitEthernet1/0/3] quit
```

使能全球单播类型地址和链路本地类型地址的 ND Snooping 功能。

```
[SwitchB] ipv6 nd snooping enable link-local
[SwitchB] ipv6 nd snooping enable global
[SwitchB] vlan 10
[SwitchB-vlan10] ipv6 nd snooping enable
```

使能 ND Detection 功能。

```
[SwitchB-vlan10] ipv6 nd detection enable
[SwitchB-vlan10] quit
```

将上行端口 GigabitEthernet1/0/3 配置为 ND 信任端口，下行端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 采用缺省配置，即为 ND 非信任端口。

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] ipv6 nd detection trust
```

完成上述配置后，对于端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 收到的 ND 报文，基于 ND Snooping 安全表项进行检查。

目 录

1 配置URPF.....	1-1
1.1 URPF简介	1-1
1.1.1 URPF概述	1-1
1.1.2 URPF检查方式	1-1
1.1.3 URPF处理流程	1-2
1.1.4 典型组网应用	1-4
1.2 配置URPF	1-5
1.3 URPF典型配置举例	1-5

1 配置URPF



说明

在以下的介绍中所指的路由器，代表了一般意义下的路由器以及运行了路由协议的以太网交换机。为提高可读性，在手册的描述中将不另行说明。

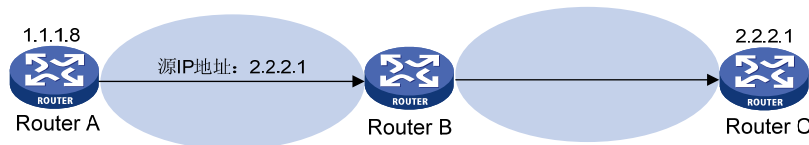
1.1 URPF简介

1.1.1 URPF概述

URPF（Unicast Reverse Path Forwarding，单播反向路径转发）的主要功能是用于防止基于源地址欺骗的网络攻击行为，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。

源地址欺骗攻击为入侵者构造出一系列带有伪造源地址的报文来产生攻击，对于使用基于 IP 地址验证的应用来说，此攻击方法可以导致未被授权用户以他人身份获得访问系统的权限，甚至是以管理员权限来访问。即使响应报文不能达到攻击者，同样也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，在Router A上伪造源地址为 2.2.2.1 的报文，以非常高的速率向服务器Router B发起请求，Router B响应请求时将向真正的“2.2.2.1”发送报文。这种非法报文对Router B和Router C都造成了攻击。

URPF 技术可以应用在上述环境中，对报文的源地址进行反查，并依据其合法性对报文进行过滤，阻止基于源地址欺骗的攻击。

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

不仅检查报文的源地址是否在 FIB 表中存在，而且检查报文的入接口与 FIB 表是否匹配。

在一些特殊情况下（如非对称路由），严格型检查会错误的丢弃非攻击报文。

一般将严格型检查布置在 ISP 的用户端和 ISP 端之间。

2. 松散型URPF

仅检查报文的源地址是否在 FIB 表中存在，而不再检查报文的入接口与 FIB 表是否匹配。

松散型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，可以使用松散型检查。

1.1.3 URPF处理流程

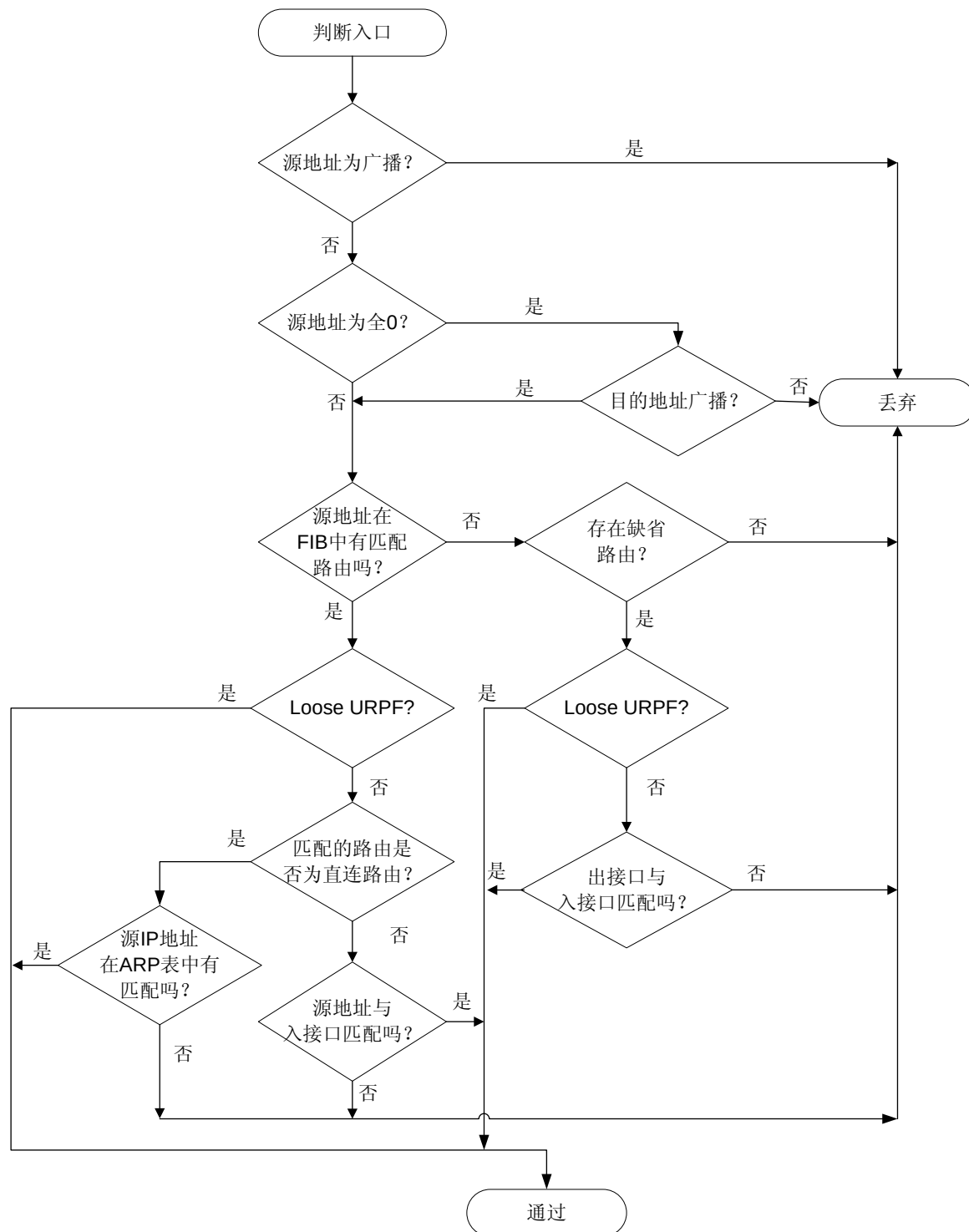


说明

组播报文不进行 URPF 检查。

URPF的处理流程如 [图 1-2](#) 所示。

图1-2 URPF 处理流程图



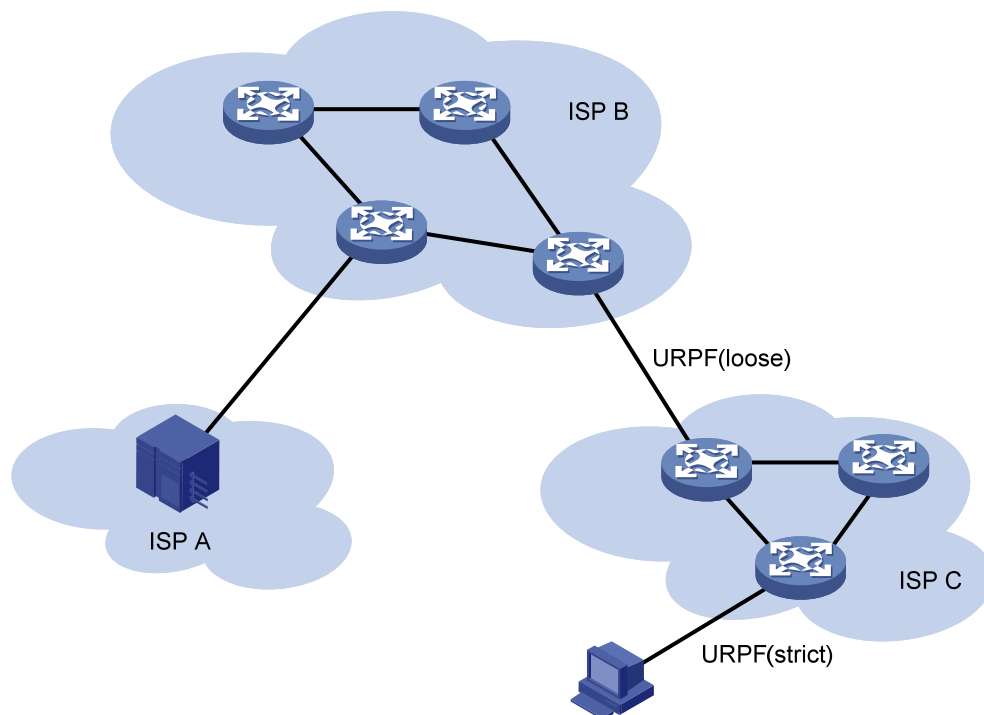
(1) 首先检查源地址合法性：

- 对于全网广播地址，直接予以丢弃。
- 对于全零地址，如果目的地址不是广播，则丢弃。（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。）
- 否则，进入步骤（2）。

- (2) 然后检查报文的源地址在 FIB 表中是否存在匹配的路由。如果在 FIB 表中查找失败，则进入步骤（6），否则进入步骤（3）；
- (3) 查看是否是 loose 型检查，如果是，则进入步骤（8）；否则查看报文的源地址在 FIB 表中匹配的路由是否是直连路由。如果是直连路由，则进入步骤（5），否则进入步骤（4）；
- (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 IP 地址为目的 IP 地址的报文的出接口），若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（8）；如果不匹配，进入步骤（9）；
- (5) 检查报文的源 IP 地址在 ARP 表中是否存在匹配的 ARP 表项。如果在 ARP 表中查找失败，则进入步骤（9）；否则进入步骤（8）；
- (6) 检查 FIB 中是否存在缺省路由，如果没有存在缺省路由，则进入步骤（9）；否则进入步骤（7）；
- (7) 查看是否是 loose 型检查，如果是，则进入步骤（8）；否则检查缺省路由的出接口是否与报文的入接口一致，如果一致，则进入步骤（8），如果不一致，则进入步骤（9）；
- (8) 报文通过检查，进行正常转发。
- (9) 交换机丢弃该报文。

1.1.4 典型组网应用

图1-3 URPF 典型组网应用



在 ISP 与用户端，配置严格 URPF，在 ISP 与 ISP 端，配置松散 URPF。

1.2 配置URPF

表1-1 配置全局 URPF

配置步骤	命令	说明
进入系统视图	system-view	-
在全局使能URPF检查	ip urpf { loose strict }	必选 缺省情况下，全局禁止URPF检查

说明

- 当本系列以太网交换机开启 URPF 功能时，会出现路由规格减半情况（路由规格减半情况为：交换机支持的最大可容纳的路由数，在开启 URPF 功能后变为开启前的一半）。
- 当交换机的路由数超过该交换机可最大容纳的路由数一半时，URPF 功能将不能开启，避免了路由表项丢失以及由其引起的数据包丢失。

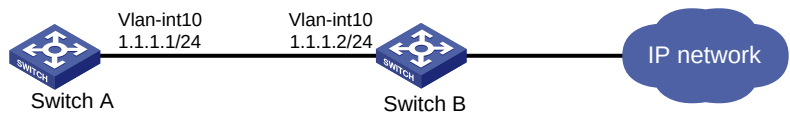
1.3 URPF典型配置举例

1. 组网需求

客户交换机 Switch A 与 ISP 交换机 Switch B 直连，在 Switch B 和 Switch A 上启动严格型 URPF 检查，防止基于源地址欺骗的网络攻击行为。

2. 组网图

图1-4 URPF 配置举例组网图



3. 配置步骤

(1) 配置 Switch A

配置严格型 URPF 检查。

```
<SwitchA> system-view
[SwitchA] ip urpf strict
```

(2) 配置 Switch B

配置严格型 URPF 检查。

```
<SwitchB> system-view
[SwitchB] ip urpf strict
```

目 录

1 MFF配置	1-1
1.1 MFF简介	1-1
1.1.1 MFF作用	1-1
1.1.2 MFF端口角色	1-2
1.1.3 MFF运行模式	1-3
1.1.4 MFF工作机制	1-4
1.1.5 协议规范	1-4
1.2 配置MFF	1-4
1.2.1 配置准备	1-4
1.2.2 使能MFF功能	1-4
1.2.3 配置端口为网络端口	1-4
1.2.4 配置对MFF维护的网关进行定时探测	1-5
1.2.5 配置网络中部署的服务器的IP地址	1-5
1.3 MFF显示和维护	1-6
1.4 MFF典型配置举例	1-6
1.4.1 自动方式树型组网典型配置举例	1-6
1.4.2 自动方式环型组网典型配置举例	1-7
1.4.3 手工方式下树型组网典型配置举例	1-9
1.4.4 手工方式环型组网典型配置举例	1-11

1 MFF配置

1.1 MFF简介

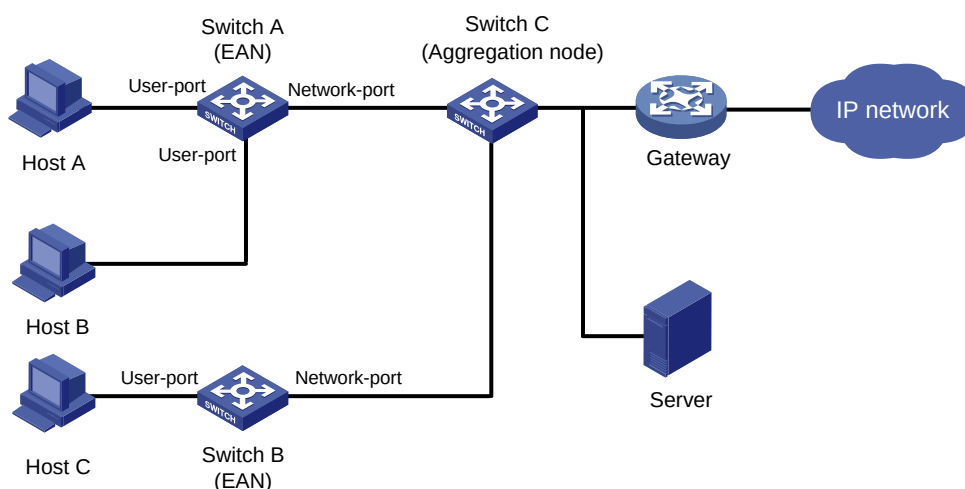
1.1.1 MFF作用

在传统的以太网组网方案中，为了实现不同客户端主机之间的二层隔离和三层互通，通常采用在交换机上划分 VLAN 的方法。但是当彼此间需要二层隔离的用户较多时，这种方式会占用大量的 VLAN 资源；同时，为实现客户端之间三层互通，需要为每个 VLAN 规划不同的 IP 网段，并配置 VLAN 接口的 IP 地址，因此划分过多的 VLAN 会降低 IP 地址的分配效率。

为了改善这种现状，MFF（MAC-Forced Forwarding，MAC 强制转发）为同一广播域内实现客户端主机间的二层隔离和三层互通，提供了一种解决方案。

MFF 截获用户的 ARP 请求报文，通过 ARP 代答机制，回复网关 MAC 地址的 ARP 应答报文。通过这种方式，可以强制用户将所有流量（包括同一子网内的流量）发送到网关，使网关可以监控数据流量，防止用户之间的恶意攻击，能更好的保障网络部署的安全性。

图1-1 应用组网图



如 图 1-1 所示，Switch A和Switch B作为以太网接入节点（Ethernet Access Nodes，EAN），提供了客户端主机与汇聚节点（Switch C）之间的连接。在以太网接入节点上配置MFF功能，可以使客户端的数据报文交互全部通过网关转发，实现了客户端之间的三层互通，又保证了二层数据的隔离，即：客户端主机不会了解相互的MAC地址。

MFF 通常与 DHCP Snooping、ARP Snooping、IP Source Guard、ARP Detection、VLAN 映射等功能配合使用，在接入层交换机上实现客户端的流量过滤、二层隔离和三层互通，提高接入层网络的安全性。



说明

- 关于 DHCP Snooping 功能的介绍，请参见“三层技术-IP 业务配置指导”中的“DHCP Snooping”。
 - 关于 ARP Snooping 功能的介绍，请参见“三层技术-IP 业务配置指导”中的“ARP Snooping”。
 - 关于 IP Source Guard 功能的介绍，请参见“安全配置指导”中的“IP Source Guard”。
 - 关于 ARP Detection 功能的介绍，请参见“安全配置指导”中的“ARP 攻击防御”。
 - 关于 VLAN 映射功能的介绍，请参见“二层技术-以太网交换配置指导”中的“VLAN 映射”。
 - 客户端与配置了 MFF 功能的设备之间是隔离的，即不能 ping 通。
-

1.1.2 MFF端口角色

使能 MFF 功能的设备上存在两种端口角色：用户端口及网络端口。

1. 用户端口

MFF 的用户端口是指直接接入网络终端用户的端口。

用户端口上对于不同的报文处理如下：

- 允许组播报文和 DHCP 报文通过；
- 对于 ARP 报文则上送 CPU 进行处理；
- 若已经学习到网关 MAC 地址，则仅允许目的 MAC 地址为网关 MAC 地址的单播报文通过，其他报文都将被丢弃；若没有学习到网关 MAC 地址，目的 MAC 地址为网关 MAC 地址的单播报文也被丢弃。

2. 网络端口

MFF 的网络端口是指连接其他网络设备如接入交换机、汇聚交换机或网关的端口。

网络端口上对于不同的报文处理如下：

- 允许组播报文和 DHCP 报文通过；
- 对于 ARP 报文则上送 CPU 进行处理；
- 拒绝其他广播报文通过。



- 上行连接网关的端口，级联组网（多个 MFF 设备连接在一起的组网）时连接下游其他 MFF 设备的端口，或者环型组网时设备之间的端口，都应该配置为网络端口。
 - 网络端口只是一种端口角色，它和该端口在网络拓扑中的位置没有关系；换句话说，网络端口不一定总是上行端口。
 - 在使能 MFF 的 VLAN 中，所有端口不是网络端口就是用户端口，不存在二者之外的端口角色。
 - 在使能 MFF 的 VLAN 中包含的所有端口中，只有网络端口支持链路聚合，用户端口不支持链路聚合。即，网络端口可以加入链路聚合组，而用户端口不能加入链路聚合组。关于链路聚合的介绍请参见“二层技术-以太网交换配置指导”中的“以太网链路聚合”。
-

1.1.3 MFF运行模式

MFF 有两种运行模式：手工方式和自动方式。

1. 手工方式

手工方式应用于用户静态配置 IP 地址的场景中，这是因为在用户静态配置 IP 地址时，MFF 无法通过 DHCP 报文来获取网关信息。另外，在用户静态配置 IP 时，由于没有依据进行用户与网关的映射，因此仅维护缺省网关的 MAC 地址，即，一个 VLAN 下仅维护一个缺省网关 MAC 地址。

使能了手工方式后，MFF 代答网关对用户的 ARP 请求，以及伪造 ARP 请求探测网关 MAC 的依据都是 ARP Snooping 表项。

若在 MFF 学习到缺省网关 MAC 地址后，收到来自网关的、携带了与记录的缺省网关 MAC 地址不同的源 MAC 地址的 ARP 报文，则需要更新记录的网关 MAC 地址。

2. 自动方式

自动方式应用于用户通过 DHCP 协议动态获取 IP 地址的场景中。DHCP Snooping 功能通过侦听 DHCP ACK 报文，并解析其中的 Option 3 字段（Router IP）来获取网关 IP 地址。

在使能 MFF 自动方式时，每一个 DHCP Snooping 用户绑定表项都应该有相对应的唯一网关 IP 地址。若 DHCP ACK 报文携带多个网关 IP 地址，则只记录第一个。若学习到的用户绑定表项不包含网关 IP 地址，或者没有记录在用户绑定表项中，则自动方式会根据当前 VLAN 记录的第一个网关作为用户网关应答该用户的 ARP 请求，除非其请求的是一个已知的网关地址。

同时，针对每一个网关 IP 地址，从第一个与其对应的用户绑定表项中获取用户 IP 地址及 MAC 地址，封装并伪造 ARP 请求，去探测网关的 MAC 地址。



- 自动方式下，一个 VLAN 内最多可以学习并维护 20 个网关信息，超过此限制的网关不再学习及处理。网关 IP 获取之后不会进行更新，即网关信息一旦生成就不会老化，除非去使能 MFF。
 - 若在 MFF 学习到网关 MAC 地址后，收到来自网关的 ARP 报文，如果该 ARP 报文中携带的源 MAC 地址与记录的网关 MAC 地址不同，则需要更新记录的网关 MAC 地址。
-

1.1.4 MFF工作机制

MFF 环境下的用户之间的三层互通是通过 ARP 代答机制实现的，这种代答机制在一定程度上减少了网络侧和用户侧之间的广播报文数量。

MFF 设备对 ARP 报文进行如下处理：

- 代答用户 ARP 请求。替代网关给用户主机回应 ARP 报文，使用户之间的报文交互都通过网关进行三层转发。这里，用户主机的 ARP 请求，既包括对于网关的请求，也包括对于其他用户 IP 的 ARP 请求。
- 代答网关 ARP 请求。替代用户主机给网关回应 ARP 报文。如果网关请求的表项在 MFF 设备上存在，就根据表项进行代答。如果表项还没有建立，则转发请求。以便达到减少广播的目的。
- 转发用户主机和网关发来的 ARP 应答。
- 监听网络中的 ARP 报文。更新网关 IP 地址和 MAC 地址对应表并广播。

1.1.5 协议规范

- RFC 4562: MAC-Forced Forwarding

1.2 配置MFF

1.2.1 配置准备

- 自动方式下要求设备使能 DHCP Snooping 功能并配置相应的 DHCP Snooping 信任端口；
- 手动方式下要求设备使能 ARP Snooping 功能。

1.2.2 使能MFF功能

表1-1 使能 MFF 功能

操作	命令	说明
进入系统视图	system-view	-
进入VLAN视图	vlan <i>vlan-id</i>	-
使能MFF功能，同时配置MFF的工作方式	mac-forced-forwarding { auto default-gateway gateway-ip }	必选 缺省情况下，MFF功能处于关闭状态

1.2.3 配置端口为网络端口

表1-2 配置以太网端口为网络端口

操作	命令	说明
进入系统视图	system-view	-
进入端口视图	interface <i>interface-type interface-number</i>	-

操作	命令	说明
配置端口为网络端口	mac-forced-forwarding network-port	必选 缺省情况下，端口为用户端口

1.2.4 配置对MFF维护的网关进行定时探测

对 MFF 维护的网关进行定时探测，可以感知网关 MAC 地址的变化。手工方式和自动方式都支持对网关的定时探测功能。

对网关进行定时探测的时间间隔为 30 秒。探测使用伪造 ARP 报文，在自动方式下其源 IP 地址和源 MAC 地址来自于 DHCP Snooping 表，在手工方式下其源 IP 地址和源 MAC 地址来自于 ARP Snooping 表。其原则是选择对应于探测网关的第一个用户绑定表项。这个伪造报文的源 IP 地址和源 MAC 地址一经选择，就会被记录并持续使用，若该用户表项被删除，则需要重新选择伪造侦听报文的用户信息。若用户表项删除之后网关没有对应用户，则清空网关探测信息。

表1-3 配置对 MFF 维护的网关进行定时探测

操作	命令	说明
进入系统视图	system-view	-
进入VLAN视图	vlan vlan-id	-
配置对MFF维护的网关进行定时探测	mac-forced-forwarding gateway probe	必选 缺省情况下，定时探测功能处于关闭状态

1.2.5 配置网络中部署的服务器的IP地址

如果网络中部署了服务器，就需要在使能 MFF 功能的设备的服务器列表中添加此服务器的 IP 地址，否则，客户端与服务器之间不能进行通信。

在手工方式和自动方式下都可以配置本功能。这里的服务器 IP 地址可以是 DHCP Server 的 IP 地址，也可以是其他业务的服务器的 IP 地址或者是 VRRP 的实 IP 地址。

如果网络侧收到了源 IP 地址为服务器 IP 地址的 ARP 请求，则查询本设备记录的用户信息，利用查询到的用户信息代替用户应答给服务器。即，用户发送给服务器的报文，都会通过网关进行转发，而服务器发送给用户的报文，则不需经过网关转发。

表1-4 配置网络中部署的服务器的 IP 地址

操作	命令	说明
进入系统视图	system-view	-
进入VLAN视图	vlan vlan-id	-
配置网络中部署的服务器的 IP 地址	mac-forced-forwarding server server-ip&<1-10>	必选 缺省情况下，没有配置网络中部署的服务器的 IP 地址

1.3 MFF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 MFF 的运行情况，通过查看显示信息验证配置的效果。

表1-5 MFF 显示和维护

操作	命令
显示MFF端口配置信息	display mac-forced-forwarding interface [{ begin exclude include } <i>regular-expression</i>]
显示指定VLAN的MFF信息	display mac-forced-forwarding vlan <i>vlan-id</i> [{ begin exclude include } <i>regular-expression</i>]

1.4 MFF典型配置举例

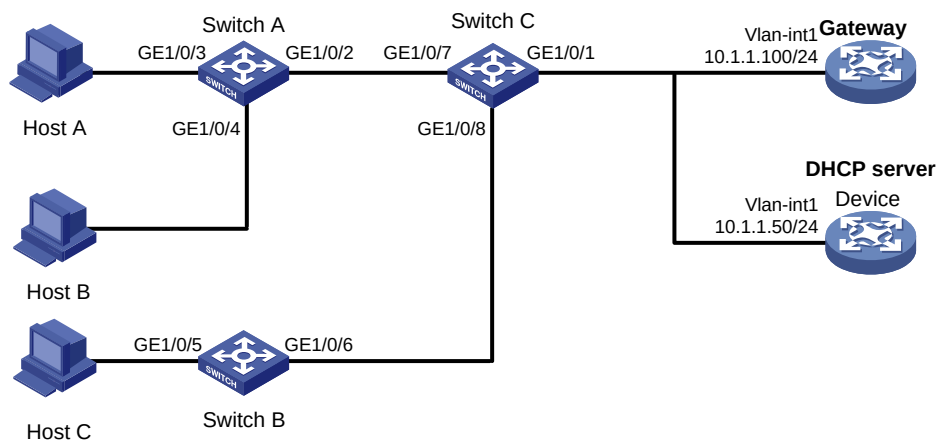
1.4.1 自动方式树型组网典型配置举例

1. 组网需求

如 图 1-2 所示，Host A、Host B和Host C通过DHCP服务器动态获取IP地址，所有设备都在VLAN 100 内。为了实现主机之间二层隔离，同时又可以通过Gateway进行三层互通，在Switch A和Switch B 上启用自动方式MFF功能。

2. 组网图

图1-2 自动方式树型组网图



3. 配置步骤

(1) 配置 Gateway

配置接口的 IP 地址。

```
<Gateway> system-view
[Gateway] interface Vlan-interface 1
[Gateway-Vlan-interface1] ip address 10.1.1.100 24
```

(2) 配置 DHCP 服务器

```
# 使能 DHCP 服务并创建 DHCP 地址池。
<Device> system-view
[Device] dhcp enable
[Device] dhcp server ip-pool 1
[Device-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.0
# 配置 DHCP 地址池为 DHCP 客户端分配的网关地址。
[Device-dhcp-pool-1] gateway-list 10.1.1.100
[Device-dhcp-pool-1] quit
# 配置接口的 IP 地址。
[Device] interface Vlan-interface 1
[Device-Vlan-interface1] ip address 10.1.1.50 24
```

(3) 配置 Switch A

```
# 使能 DHCP Snooping 功能。
<SwitchA> system-view
[SwitchA] dhcp-snooping
# 使能自动方式 MFF 功能。
[SwitchA] vlan 100
[SwitchA-vlan-100] mac-forced-forwarding auto
[SwitchA-vlan-100] quit
# 配置网络端口。
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] mac-forced-forwarding network-port
# 配置 DHCP Snooping 信任端口。
[SwitchA-GigabitEthernet1/0/2] dhcp-snooping trust
```

(4) 配置 Switch B

```
# 使能 DHCP Snooping 功能。
<SwitchB> system-view
[SwitchB] dhcp-snooping
# 使能自动方式 MFF 功能。
[SwitchB] vlan 100
[SwitchB-vlan-100] mac-forced-forwarding auto
[SwitchB-vlan-100] quit
# 配置网络端口。
[SwitchB] interface gigabitethernet 1/0/6
[SwitchB-GigabitEthernet1/0/6] mac-forced-forwarding network-port
# 配置 DHCP Snooping 信任端口。
[SwitchB-GigabitEthernet1/0/6] dhcp-snooping trust
```

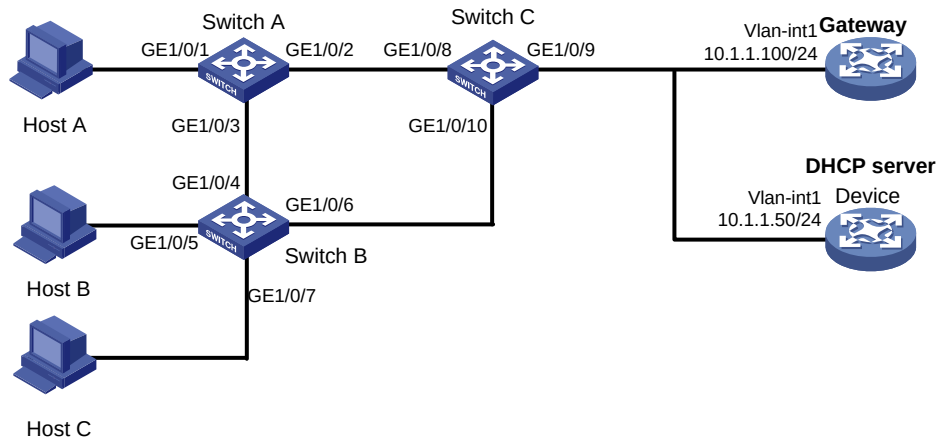
1.4.2 自动方式环型组网典型配置举例

1. 组网需求

如 [图 1-3](#) 所示，Host A、Host B 和 Host C 通过 DHCP 服务器动态获取 IP 地址，网络中存在环路，所有设备都在 VLAN 100 内。为了实现主机之间二层隔离，同时又可以通过 Gateway 进行三层互通，在 Switch A 和 Switch B 上启用自动方式 MFF 功能。

2. 组网图

图1-3 自动方式环型组网图



3. 配置步骤

(1) 配置 Gateway

配置接口的 IP 地址。

```
<Gateway> system-view
[Gateway] interface Vlan-interface 1
[Gateway-Vlan-interface1] ip address 10.1.1.100 24
```

(2) 配置 DHCP 服务器

使能 DHCP 服务并创建 DHCP 地址池。

```
<Device> system-view
[Device] dhcp enable
[Device] dhcp server ip-pool 1
[Device-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.0
```

配置 DHCP 地址池为 DHCP 客户端分配的网关地址。

```
[Device-dhcp-pool-1] gateway-list 10.1.1.100
[Device-dhcp-pool-1] quit
```

配置接口的 IP 地址。

```
[Device] interface Vlan-interface 1
[Device-Vlan-interface1] ip address 10.1.1.50 24
```

(3) 配置 Switch A

使能 DHCP Snooping 功能。

```
<SwitchA> system-view
[SwitchA] dhcp-snooping
```

启动 STP 协议。

```
[SwitchA] stp enable
```

使能自动方式 MFF 功能。

```
[SwitchA] vlan 100
[SwitchA-vlan-100] mac-forced-forwarding auto
[SwitchA-vlan-100] quit
```

```

# 配置网络端口。
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] mac-forced-forwarding network-port
# 配置 DHCP Snooping 信任端口。
[SwitchA-GigabitEthernet1/0/2] dhcp-snooping trust
[SwitchA-GigabitEthernet1/0/2] quit
# 配置网络端口。
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mac-forced-forwarding network-port
# 配置 DHCP Snooping 信任端口。
[SwitchA-GigabitEthernet1/0/3] dhcp-snooping trust no-user-binding
(4) 配置 Switch B
# 使能 DHCP Snooping 功能。
<SwitchB> system-view
[SwitchB] dhcp-snooping
# 启动 STP 协议。
[SwitchB] stp enable
# 使能自动方式 MFF 功能。
[SwitchB] vlan 100
[SwitchB-vlan-100] mac-forced-forwarding auto
[SwitchB-vlan-100] quit
# 配置网络端口。
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] mac-forced-forwarding network-port
# 配置 DHCP Snooping 信任端口。
[SwitchB-GigabitEthernet1/0/4] dhcp-snooping trust no-user-binding
[SwitchB-GigabitEthernet1/0/4] quit
# 配置网络端口。
[SwitchB] interface gigabitethernet 1/0/6
[SwitchB-GigabitEthernet1/0/6] mac-forced-forwarding network-port
# 配置 DHCP Snooping 信任端口。
[SwitchB-GigabitEthernet1/0/6] dhcp-snooping trust
(5) 配置 Switch C
# 启动 STP 协议。
<SwitchC> system-view
[SwitchC] stp enable

```

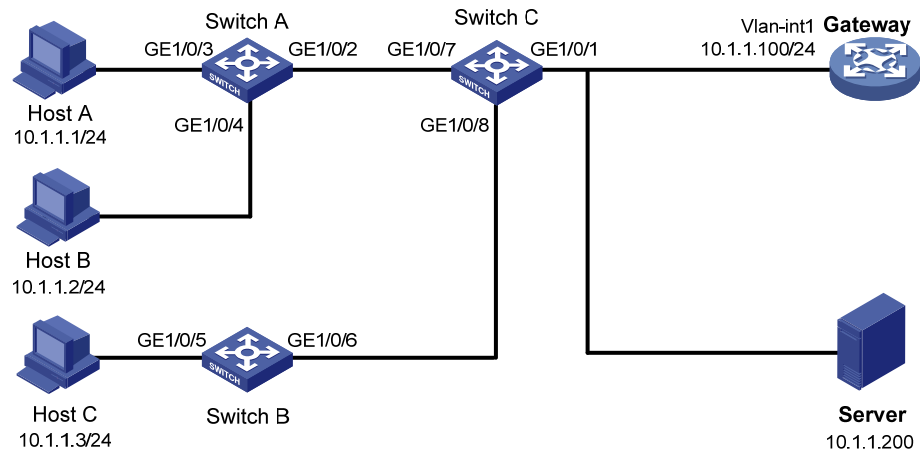
1.4.3 手工方式下树型组网典型配置举例

1. 组网需求

如 [图 1-4](#) 所示，Host A、Host B 和 Host C 配置静态 IP 地址，所有设备都在 VLAN 100 内。为了实现主机之间二层隔离，同时又可以通过 Gateway 进行三层互通，在 Switch A 和 Switch B 上启用手工方式 MFF 功能。为了实现主机与 Server 互通，需要手工配置网络中部署服务器的 IP 地址。

2. 组网图

图1-4 手工方式树型组网图



3. 配置步骤

(1) 如上图在客户端配置静态 IP 地址

(2) 配置 Gateway

配置接口的 IP 地址。

```
<Gateway> system-view
[Gateway] interface Vlan-interface 1
[Gateway-Vlan-interface1] ip address 10.1.1.100 24
```

(3) 配置 Switch A

使能手工方式 MFF 功能。

```
[SwitchA] vlan 100
[SwitchA-vlan-100] mac-forced-forwarding default-gateway 10.1.1.100
# 配置网络中部署的服务器的 IP 地址为 10.1.1.200。
```

```
[SwitchA-vlan-100] mac-forced-forwarding server 10.1.1.200
```

使能 ARP Snooping 功能。

```
[SwitchA-vlan-100] arp-snooping enable
[SwitchA-vlan-100] quit
```

配置网络端口。

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] mac-forced-forwarding network-port
```

(4) 配置 Switch B

使能手工方式 MFF 功能。

```
[SwitchB] vlan 100
[SwitchB-vlan-100] mac-forced-forwarding default-gateway 10.1.1.100
# 配置网络中部署的服务器的 IP 地址为 10.1.1.200。
```

```
[SwitchB-vlan-100] mac-forced-forwarding server 10.1.1.200
```

使能 ARP Snooping 功能。

```
[SwitchB-vlan-100] arp-snooping enable
[SwitchB-vlan-100] quit
```


配置网络端口。

```
[SwitchB] interface gigabitethernet 1/0/6
```

```
[SwitchB-GigabitEthernet1/0/6] mac-forced-forwarding network-port
```

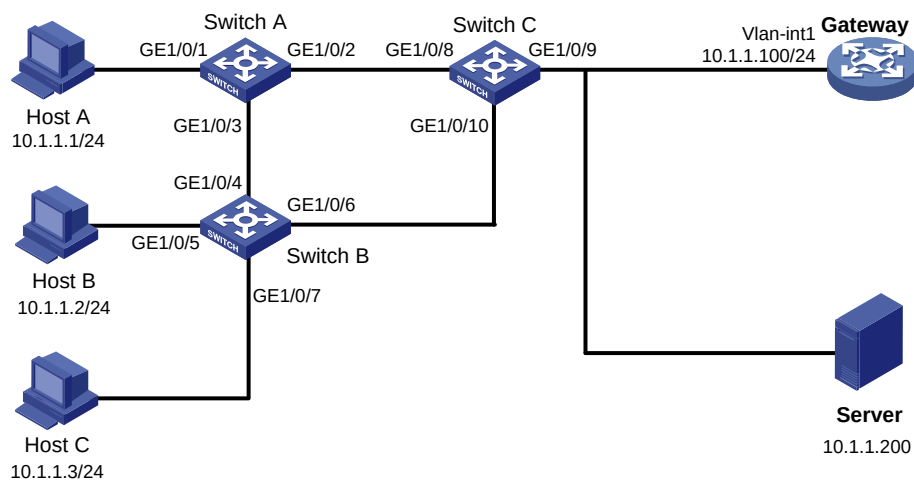
1.4.4 手工方式环型组网典型配置举例

1. 组网需求

如 图 1-5 所示, Host A、Host B和Host C配置静态IP地址, 网络中存在环路, 所有设备都在VLAN 100内。为了实现主机之间二层隔离, 同时又可以通过Gateway进行三层互通, 在Switch A和Switch B上启用手工方式MFF功能。为了实现主机与Server互通, 需要手工配置网络中部署服务器的IP地址。

2. 组网图

图1-5 手工方式环型组网图



3. 配置步骤

(1) 如上图在客户端配置静态 IP 地址

(2) 配置 Gateway

配置接口的 IP 地址。

```
<Gateway> system-view
```

```
[Gateway] interface Vlan-interface 1
```

```
[Gateway-Vlan-interface1] ip address 10.1.1.100 24
```

(3) 配置 Switch A

启动 STP 协议。

```
[SwitchA] stp enable
```

使能手工方式 MFF 功能。

```
[SwitchA] vlan 100
```

```
[SwitchA-vlan-100] mac-forced-forwarding default-gateway 10.1.1.100
```

配置网络中部署的服务器的 IP 地址为 10.1.1.200。

```
[SwitchA-vlan-100] mac-forced-forwarding server 10.1.1.200
```

使能 ARP Snooping 功能。

```
[SwitchA-vlan-100] arp-snooping enable
```

```
[SwitchA-vlan-100] quit
# 配置网络端口。
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] mac-forced-forwarding network-port
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mac-forced-forwarding network-port
(4) 配置 Switch B
# 启动 STP 协议。
[SwitchB] stp enable
# 使能手工方式 MFF 功能。
[SwitchB] vlan 100
[SwitchB-vlan-100] mac-forced-forwarding default-gateway 10.1.1.100
# 配置网络中部署的服务器的 IP 地址为 10.1.1.200。
[SwitchB-vlan-100] mac-forced-forwarding server 10.1.1.200
# 使能 ARP Snooping 功能。
[SwitchB-vlan-100] arp-snooping enable
[SwitchB-vlan-100] quit
# 配置网络端口。
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] mac-forced-forwarding network-port
[SwitchB-GigabitEthernet1/0/4] quit
[SwitchB] interface gigabitethernet 1/0/6
[SwitchB-GigabitEthernet1/0/6] mac-forced-forwarding network-port
(5) 配置 Switch C
# 启动 STP 协议。
<SwitchC> system-view
[SwitchC] stp enable
```

目 录

1 SAVI配置	1-1
1.1 SAVI简介	1-1
1.2 SAVI的全局配置	1-1
1.3 DHCPv6-Only场景中的SAVI配置	1-2
1.4 SLAAC-Only场景中的SAVI配置	1-4
1.5 DHCPv6 与SLAAC混合场景中的SAVI配置	1-6

1 SAVI配置

1.1 SAVI简介

SAVI (Source Address Validation, 源地址有效性验证) 特性应用在接入设备上, 通过 ND Snooping 特性、DHCPv6 Snooping 特性及 IP Source Guard 特性建立起地址和端口的绑定关系表, 并且以绑定关系为依据对 DHCPv6 协议报文、ND 协议报文和 IPv6 数据报文的源地址进行合法性的过滤检查。

SAVI 特性可以在下列地址分配场景下使用:

- **DHCPv6-Only:** 和配置 SAVI 特性的设备连接的主机只能通过 DHCPv6 方式获取地址。
- **SLAAC-Only (Stateless Address Autoconfiguration, 无状态地址自动配置):** 和配置 SAVI 特性的设备连接的主机只能通过自动地址分配方式获取地址。
- **DHCPv6 与 SLAAC 混合:** 和配置 SAVI 特性的设备连接的主机可以通过 DHCPv6 方式和自动地址分配方式获取地址。

不同地址分配场景中的 SAVI 配置不同, 下面将依次介绍 SAVI 的全局配置以及不同场景下的 SAVI 配置。

开启 SAVI 功能后, 当接入交换机的端口 down, 该端口下对应用户的 DHCPv6 Snooping 和 ND Snooping 动态绑定表项不会立刻清除, 而是等待一段时间后才被清除, 这个时间称为 SAVI 绑定表项延迟时间, 可以通过命令行进行配置。这样可以防止端口短暂的 down/up 过程被设备忽略而导致的合法 IPv6 地址无法正常上网的问题。

1.2 SAVI的全局配置

表1-1 SAVI 的全局配置

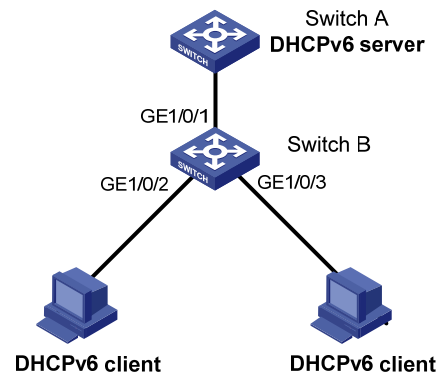
操作	命令	说明
进入系统视图	system-view	-
开启SAVI功能	ipv6 savi strict	必选 缺省情况下, SAVI功能处于关闭状态
配置SAVI绑定表项延迟时间	ipv6 savi down-delay time	可选 缺省情况下, SAVI绑定表项延迟时间为30秒
配置等待通告地址冲突的NA报文的时间	ipv6 savi dad-delay value	可选 缺省情况下, 等待通告地址冲突的NA报文的时间为1秒 ND Snooping表项在detect状态下, 如果超过配置的等待时间没有收到NA消息, 则说明节点可以使用此IPv6地址, 此时记录的ND Snooping表项可以进入bound状态

操作	命令	说明
配置等待DHCPv6客户端对获取地址作冲突检测的时间	ipv6 savi dad-preparedelay value	可选 缺省情况下，等待DHCPv6客户端对获取地址作冲突检测的时间为1秒 本命令配合DHCPv6 Snooping功能使用。DHCPv6 Snooping模块在侦听到客户端获取到地址后，还会侦听客户端是否对获取到的地址作冲突检测，如果超过配置的等待时间没有侦听到客户端发送的DAD NS报文，则设备会主动替客户端发送DAD NS报文

1.3 DHCPv6-Only场景中的SAVI配置

1. 场景描述

图1-1 DHCPv6-Only 场景示意图



在 [图 1-1](#) 所示的DHCPv6-Only场景下，Switch B通过以太网端口GigabitEthernet1/0/1 连接到DHCPv6 服务器，通过以太网端口GigabitEthernet1/0/2、GigabitEthernet1/0/3 连接到主机，GigabitEthernet1/0/1、GigabitEthernet1/0/2 和GigabitEthernet1/0/3 都属于VLAN 2。主机只能通过DHCPv6 方式获取IPv6 地址，不能通过自动地址配置方式获取IPv6 地址。在设备Switch B上配置SAVI特性后，设备Switch B只允许使用已绑定的DHCPv6 方式分配的地址和链路本地地址发送的报文通过。

2. 配置思路

本场景需要在 Switch B 上进行下列配置：

- 开启 SAVI 功能。
- 使能 DHCPv6 Snooping 功能。DHCPv6 Snooping 的详细介绍请参见“三层技术-IP 业务配置指导”中的“DHCPv6 Snooping”。
- 使能链路本地类型地址的 ND Snooping 功能。ND Snooping 的详细介绍请参见“三层技术-IP 业务配置指导”中的“IPv6 基础”。
- 为了检查端口上的 ND 协议报文，需要在 VLAN 下使能 ND Detection 功能。ND Detection 的详细介绍请参见“安全配置指导”中的“ND 攻击防御”。

- 在连接主机的端口上配置 IP Source Guard 的 IPv6 静态绑定表项（本配置可选，如果不配置，检查时将不检查静态绑定表项）。IPv6 静态绑定表项的详细介绍请参见“安全配置指导”中的“IP Source Guard”。
- 在连接主机的端口上配置 IP Source Guard 的 IPv6 动态绑定功能。IPv6 动态绑定功能的详细介绍请参见“安全配置指导”中的“IP Source Guard”。

3. 报文检查原则

接入设备 Switch B 会对 DHCPv6 client 发送的 DHCPv6 协议报文基于链路本地类型的 ND Snooping 表项检查，对 ND 协议报文基于链路本地类型的 ND Snooping 表项、DHCPv6 Snooping 表项和静态绑定表项检查，对连接主机的端口上收到的 IPv6 数据报文基于下发到端口的动态绑定表项（包括链路本地类型的 ND Snooping 表项、DHCPv6 Snooping 表项）和静态绑定表项检查。检查的内容包括 MAC 地址、IPv6 地址、VLAN 信息、入端口信息。

4. 配置步骤

开启 SAVI 功能。

```
<SwitchB> system-view
```

```
[SwitchB] ipv6 savi strict
```

使能 IPv6 转发功能。

```
[SwitchB] ipv6
```

全局使能 DHCPv6 Snooping 功能。

```
[SwitchB] ipv6 dhcp snooping enable
```

将端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 加入 VLAN 2。

```
[SwitchB] vlan 2
```

```
[SwitchB-vlan2] port gigabitethernet 1/0/1 gigabitethernet 1/0/2 gigabitethernet 1/0/3
```

在 VLAN 2 内使能 DHCPv6 Snooping 功能。

```
[SwitchB-vlan2] ipv6 dhcp snooping vlan enable
```

```
[SwitchB] quit
```

配置 GigabitEthernet1/0/1 端口为信任端口。

```
[SwitchB] interface gigabitethernet 1/0/1
```

```
[SwitchB-GigabitEthernet1/0/1] ipv6 dhcp snooping trust
```

```
[SwitchB-GigabitEthernet1/0/1] quit
```

使能本地链路类型的 ND Snooping 功能和 ND Detection 功能。

```
[SwitchB] ipv6 nd snooping enable link-local
```

```
[SwitchB] vlan 2
```

```
[SwitchB-vlan2] ipv6 nd snooping enable
```

```
[SwitchB-vlan2] ipv6 nd detection enable
```

```
[SwitchB-vlan2] quit
```

下行端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 上启用 IP Source Guard 的 IPv6 动态绑定功能。

```
[SwitchB] interface gigabitethernet 1/0/2
```

```
[SwitchB-GigabitEthernet1/0/2] ipv6 verify source ipv6-address mac-address
```

```
[SwitchB-GigabitEthernet1/0/2] quit
```

```
[SwitchB] interface gigabitethernet 1/0/3
```

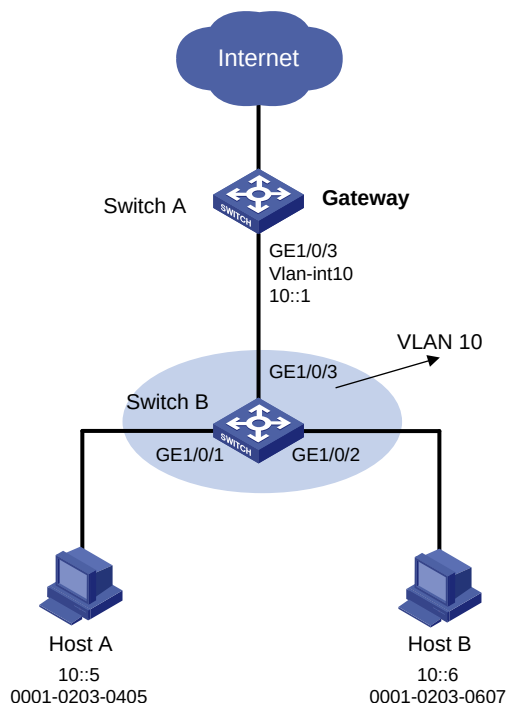
```
[SwitchB-GigabitEthernet1/0/3] ipv6 verify source ipv6-address mac-address
```

```
[SwitchB-GigabitEthernet1/0/3] quit
```

1.4 SLAAC-Only场景中的SAVI配置

1. 场景描述

图1-2 SLAAC-Only 场景组网图



在图 1-2 所示的SLAAC-Only场景下，用户Host A和Host B通过Switch B接入网关Switch A。主机只能通过自动地址分配方式获取IPv6 地址。在设备Switch B上配置SAVI特性后，设备Switch B只允许已绑定的无状态地址自动配置方式分配的地址发送的报文通过，不允许DHCPv6 方式分配的地址发送的报文通过。

2. 配置思路

本场景需要在 Switch B 上进行下列配置：

- 开启 SAVI 功能。
- 使能全球单播类型地址和链路本地类型地址的 ND Snooping 功能。ND Snooping 的详细介绍请参见“三层技术-IP 业务配置指导”中的“IPv6 基础”。
- 为了检查端口上的 ND 协议报文，需要在 VLAN 下使能 ND Detection 功能。ND Detection 的详细介绍请参见“安全配置指导”中的“ND 攻击防御”。
- 在连接主机的端口上配置 IP Source Guard 的 IPv6 静态绑定表项（本配置可选，如果不配置，检查时将不检查静态绑定表项）。IPv6 静态绑定表项的详细介绍请参见“安全配置指导”中的“IP Source Guard”。
- 在连接主机的端口上配置 IP Source Guard 的 IPv6 动态绑定功能。IPv6 动态绑定功能的详细介绍请参见“安全配置指导”中的“IP Source Guard”。
- 需要使能 DHCPv6 Snooping 功能，并且连接 Gateway 的端口保持默认的非 trust 状态，来保证主机不能通过 DHCPv6 方式获取到地址。DHCPv6 Snooping 的详细介绍请参见“三层技术-IP 业务配置指导”中的“DHCPv6 Snooping”。

3. 报文检查原则

接入设备 Switch B 会对 ND 协议报文基于 ND Snooping 表项、静态绑定表项检查，对连接主机的端口上收到的 IPv6 数据报文基于下发到端口的动态绑定表项（包括 ND Snooping 表项）和静态绑定表项检查。检查的内容包括 MAC 地址、IPv6 地址、VLAN 信息、入端口信息。

4. 配置步骤

开启 SAVI 功能。

```
<SwitchB> system-view
```

```
[SwitchB] ipv6 savi strict
```

使能 IPv6 转发功能。

```
[SwitchB] ipv6
```

将端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 加入 VLAN 10。

```
[SwitchB] vlan 10
```

```
[SwitchB-vlan10] port gigabitethernet 1/0/1 gigabitethernet 1/0/2 gigabitethernet 1/0/3
```

```
[SwitchB-vlan10] quit
```

使能全球单播类型地址和链路本地类型地址的 ND Snooping 功能。

```
[SwitchB] ipv6 nd snooping enable link-local
```

```
[SwitchB] ipv6 nd snooping enable global
```

```
[SwitchB] vlan 10
```

```
[SwitchB-vlan10] ipv6 nd snooping enable
```

使能 ND Detection 功能。

```
[SwitchB-vlan10] ipv6 nd detection enable
```

```
[SwitchB-vlan10] quit
```

使能 DHCPv6 Snooping 功能来禁止 DHCPv6 协议报文转发。

```
[SwitchB] ipv6 dhcp snooping enable
```

将上行端口 GigabitEthernet1/0/3 配置为 ND 信任端口。

```
[SwitchB] interface gigabitethernet 1/0/3
```

```
[SwitchB-GigabitEthernet1/0/3] ipv6 nd detection trust
```

```
[SwitchB-GigabitEthernet1/0/3] quit
```

在下行端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上配置 IPv6 动态绑定功能。

```
[SwitchB] interface gigabitethernet 1/0/1
```

```
[SwitchB-GigabitEthernet1/0/1] ipv6 verify source ipv6-address mac-address
```

```
[SwitchB-GigabitEthernet1/0/1] quit
```

```
[SwitchB] interface gigabitethernet 1/0/2
```

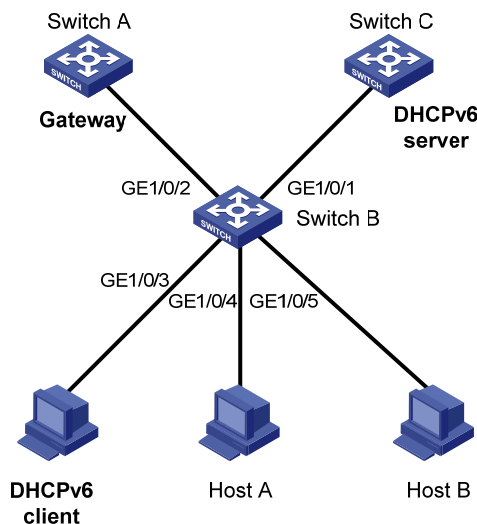
```
[SwitchB-GigabitEthernet1/0/2] ipv6 verify source ipv6-address mac-address
```

```
[SwitchB-GigabitEthernet1/0/2] quit
```


1.5 DHCPv6与SLAAC混合场景中的SAVI配置

1. 场景描述

图1-3 DHCPv6 与 SLAAC 混合场景组网图



在图 1-3 所示的在混合场景下，Switch B 通过以太网端口 GigabitEthernet1/0/1 连接到 DHCPv6 服务器，通过以太网端口 GigabitEthernet1/0/3 连接到 DHCPv6 客户端。用户 Host A 和 Host B 通过 Switch B 接入网关 Switch A。Switch B 上 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3、GigabitEthernet1/0/4 和 GigabitEthernet1/0/5 都属于 VLAN 2。主机可以通过 DHCPv6 方式和自动地址分配方式获取地址。在设备 Switch B 上配置 SAVI 特性后，设备 Switch B 将允许 DHCPv6 方式分配的地址和已绑定的无状态地址自动配置方式分配的地址发送的报文通过。

2. 配置思路

本场景需要在 Switch B 上进行下列配置：

- 开启 SAVI 功能。
- 使能 DHCPv6 Snooping 功能。DHCPv6 Snooping 的详细介绍请参见“三层技术-IP 业务配置指导”中的“DHCPv6 Snooping”。
- 使能全球单播类型地址和链路本地类型地址的 ND Snooping 功能。ND Snooping 的详细介绍请参见“三层技术-IP 业务配置指导”中的“IPv6 基础”。
- 为了检查端口上的 ND 协议报文，需要在 VLAN 下使能 ND Detection 功能。ND Detection 的详细介绍请参见“安全配置指导”中的“ND 攻击防御”。
- 在连接主机的端口上配置 IP Source Guard 的 IPv6 静态绑定表项（本配置可选，如果不配置，检查时将不检查静态绑定表项）。IPv6 静态绑定表项的详细介绍请参见“安全配置指导”中的“IP Source Guard”。
- 在连接主机的端口上配置 IP Source Guard 的 IPv6 动态绑定功能。IPv6 动态绑定功能的详细介绍请参见“安全配置指导”中的“IP Source Guard”。

3. 报文检查原则

接入设备 Switch B 会对 DHCPv6 client 发送的 DHCPv6 协议报文基于链路本地类型的 ND Snooping 表项检查, 对 ND 协议报文基于 ND Snooping 表项、DHCPv6 Snooping 表项和静态绑定表项检查, 对连接主机的端口上收到的 IPv6 数据报文基于下发到端口的动态绑定表项 (包括 ND Snooping 表项、DHCPv6 Snooping 表项) 和静态绑定表项检查。检查的内容包括 MAC 地址、IPv6 地址、VLAN 信息、入端口信息。

4. 配置步骤

开启 SAVI 功能。

```
<SwitchB> system-view
```

```
[SwitchB] ipv6 savi strict
```

使能 IPv6 转发功能。

```
[SwitchB] ipv6
```

使能 DHCPv6 Snooping 功能。

```
[SwitchB] ipv6 dhcp snooping enable
```

将端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3、GigabitEthernet1/0/4 和 GigabitEthernet1/0/5 加入 VLAN 2。

```
[SwitchB] vlan 2
```

```
[SwitchB-vlan2] port gigabitethernet 1/0/1 gigabitethernet 1/0/2 gigabitethernet 1/0/3  
gigabitethernet 1/0/4 gigabitethernet 1/0/5
```

在 VLAN 2 内使能 DHCPv6 Snooping 功能。

```
[SwitchB-vlan2] ipv6 dhcp snooping vlan enable
```

```
[SwitchB] quit
```

配置 GigabitEthernet1/0/1 端口为 DHCPv6 Snooping 信任端口。

```
[SwitchB] interface gigabitethernet 1/0/1
```

```
[SwitchB-GigabitEthernet1/0/1] ipv6 dhcp snooping trust
```

```
[SwitchB-GigabitEthernet1/0/1] quit
```

使能 ND Snooping 功能和 ND Detection 功能。

```
[SwitchB] ipv6 nd snooping enable link-local
```

```
[SwitchB] ipv6 nd snooping enable global
```

```
[SwitchB] vlan 2
```

```
[SwitchB-vlan2] ipv6 nd snooping enable
```

```
[SwitchB-vlan2] ipv6 nd detection enable
```

```
[SwitchB-vlan2] quit
```

配置 GigabitEthernet1/0/2 端口为 ND detection 信任端口。

```
[SwitchB] interface gigabitethernet 1/0/2
```

```
[SwitchB-GigabitEthernet1/0/2] ipv6 nd detection trust
```

```
[SwitchB-GigabitEthernet1/0/2] quit
```

在下行端口 GigabitEthernet1/0/3、GigabitEthernet1/0/4 和 GigabitEthernet1/0/5 上配置 IPv6 动态绑定功能。

```
[SwitchB] interface gigabitethernet 1/0/3
```

```
[SwitchB-GigabitEthernet1/0/3] ipv6 verify source ipv6-address mac-address
```

```
[SwitchB-GigabitEthernet1/0/3] quit
```

```
[SwitchB] interface gigabitethernet 1/0/4
```

```
[SwitchB-GigabitEthernet1/0/4] ipv6 verify source ipv6-address mac-address
```

```
[SwitchB-GigabitEthernet1/0/4] quit
```

```
[SwitchB] interface gigabitethernet 1/0/5  
[SwitchB-GigabitEthernet1/0/5] ipv6 verify source ipv6-address mac-address
```

目 录

1 黑名单配置.....	1-1
1.1 黑名单功能简介简介.....	1-1
1.2 配置黑名单	1-1
1.3 黑名单显示和维护	1-1
1.4 黑名单功能配置举例.....	1-2
1.4.1 组网需求	1-2
1.4.2 组网图.....	1-2
1.4.3 配置步骤	1-2
1.4.4 验证配置结果	1-2

1 黑名单配置

1.1 黑名单功能简介简介

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, 从而有效地将特定 IP 地址发送来的报文屏蔽掉。

黑名单可以由设备动态地进行添加或删除, 这种动态添加是与用户登录设备的认证功能配合实现的, 动态生成的黑名单表项会在一定的时间之后老化。具体实现是:

当设备检测到某用户通过 FTP、Telnet、SSH、SSL 或 Web 方式尝试登录设备的失败次数达到指定阈值之后, 便判定其为恶意攻击用户, 并将其源 IP 地址自动加入黑名单, 之后来自该 IP 地址且访问本设备的报文将被设备过滤掉。此处所指的认证失败情况包括: 用户名错误、密码错误、验证码错误 (针对 Web 登录用户)。该功能可以有效防范恶意用户通过不断尝试登录认证, 尝试破解登录密码的攻击行为。目前, 用户登录失败次数的阈值为 6, 黑名单的老化时间为 10 分钟, 且均不可配。

除上面所说的动态方式之外, 设备还支持手动方式添加或删除黑名单。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, 黑名单表项对应的 IP 地址发送的报文即可正常通过。

1.2 配置黑名单

黑名单的配置包括使能黑名单功能和添加黑名单表项。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。

表1-1 配置黑名单

配置步骤	命令	说明
进入系统视图	system-view	-
使能黑名单功能	blacklist enable	必选 缺省情况下, 黑名单功能处于未使能状态
添加黑名单表项	blacklist ip source-ip-address [timeout minutes]	可选

1.3 黑名单显示和维护

在完成上述配置后, 在任意视图下执行 **display** 命令可以查看黑名单配置的效果。

表1-2 黑名单的显示和维护

操作	命令
显示黑名单信息	display blacklist { all ip source-ip-address [slot slot-number] slot slot-number } [{ begin exclude include } <i>regular-expression</i>]

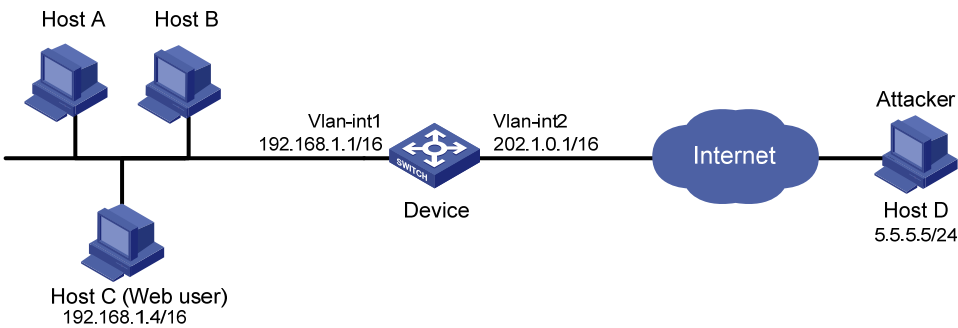
1.4 黑名单功能配置举例

1.4.1 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 Device 上永远过滤掉。另外，网络管理员为了控制内部网络的 Web 认证用户 Host C 的访问行为，当该用户登录失败次数超过 6 次，需要将 Device 上收到的 Host C 的报文阻止 10 分钟。

1.4.2 组网图

图1-1 黑名单配置典型组网图



1.4.3 配置步骤

```
# 配置各接口的 IP 地址，略。
# 使能黑名单功能。
<Device> system-view
[Device] blacklist enable
# 将 Host D 的 IP 地址 5.5.5.5 添加到黑名单中，缺省永不老化。
[Device] blacklist ip 5.5.5.5
```

1.4.4 验证配置结果

完成以上配置后，可以通过 **display blacklist all** 命令查看已添加的黑名单信息。

```
[Device] display blacklist all
Blacklist information
-----
Blacklist                               : enabled
Blacklist items                         : 2
-----
```

IP	Type	Aging started	Aging finished	Dropped packets
		YYYY/MM/DD hh:mm:ss	YYYY/MM/DD hh:mm:ss	
5.5.5.5	manual	2011/04/09 16:02:20	Never	0
192.168.1.4	manual	2011/04/09 16:02:26	2011/04/09 16:12:26	0

配置生效后，Device 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 Device 接收到来自 Host C 的报文，Web 认证失败次数超过 6 次，则在 10 分钟之内，对其进行丢弃处理，10 分钟之后，才进行正常转发。

目 录

1 FIPS.....	1-1
1.1 简介	1-1
1.2 FIPS的自检处理	1-1
1.2.1 启动自检（Power-up Self-tests）	1-1
1.2.2 条件自检（Conditional Self-tests）	1-1
1.2.3 手工触发密码算法自检	1-1
1.3 配置FIPS	1-2
1.3.1 使能FIPS模式	1-2
1.3.2 配置手工触发密码算法自检	1-3
1.4 FIPS的显示和维护.....	1-3
1.5 FIPS典型配置举例.....	1-3

1 FIPS

1.1 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, 它们安全级别依次递增, 可广泛适应于密码模块的各种应用环境。目前, 设备支持 Level 2。

若无特殊说明, 文中的 FIPS 即表示 FIPS 140-2。

1.2 FIPS的自检处理

FIPS 模式处于使能状态之后, 为确保密码模块的功能正常运行, 系统会进行一定的自检处理, 具体包括启动自检和条件自检。启动自检或条件自检失败后, 设备均会自动重启。



注意

如果出现反复自检失败重启的状况, 有可能是设备内部的软件或者设备本身硬件损坏, 需要更新软件或对设备硬件进行维修, 请联系用服工程师解决。

1.2.1 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。

1.2.2 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。该自检过程在 FIPS 模式下任何调用随机数的情况下进行。

1.2.3 手工触发密码算法自检

设备运行过程当中, 当用户或管理员需要确认当前系统中的密码模块是否正常工作时, 可以通过执行命令行来手工触发系统进行密码算法自检工作。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。

1.3 配置FIPS

配置 FIPS 的基本配置思路如下：

- (1) 需要手工删除原有的密钥对，证书等。
- (2) 使能 FIPS 功能；
- (3) 使能 Password-control 功能；
- (4) 配置设备的本地用户相关属性（包括本地用户名，服务类型和密码等）
- (5) 保存配置

完成上述配置并重新启动设备以后，设备进入 FIPS 模式，设备运行于支持 FIPS 140-2 标准的工作模式下。在 CC 认证中，进入 FIPS 模式后，同时相当于设备运行于支持 CC 标准的工作模式下。



注意

设备不支持从非 FIPS 版本升级到 FIPS 版本。

1.3.1 使能FIPS模式

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	必选 缺省情况下，FIPS模式处于关闭状态



注意

- 设备 FIPS 模式的切换，除执行相应命令（**fips mode enable** 或 **undo fips mode enable**），还需要重启设备才能生效。如果在 IRF 环境下切换 FIPS 模式，需要重启整个 IRF 后才能生效。
- 切换到 FIPS 模式后，原非 FIPS 模式下 Telnet 类型的本地用户将无法登录设备。
- FIPS 模式下，为保证用户正常登录，请不要执行 **undo password-control enable** 命令。

进入 FIPS 模式后，设备上的以下功能将发生变化

- FTP/TFTP 功能被禁用。
- Telnet 功能被禁用。
- HTTP 服务器功能被禁用。
- 集群功能被禁用。
- SNMP v1 和 SNMP v2c 版本的 SNMP 功能被禁用，只允许使用 SNMP v3 版本。
- SSL 服务器只支持 TLS1.0 协议。
- SSH 服务器不兼容 SSHv1 客户端。

- SSH 只支持 RSA。
- RSA 只支持 2048 位的密钥对，DSA 支持至少 1024 位的密钥对。
- SSH、SNMPv3、IPsec 和 SSL 不支持 DES、3DES、RC4、MD5 算法。

1.3.2 配置手工触发密码算法自检

表1-2 手工触发密码算法自检配置

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	必选

1.4 FIPS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 FIPS 模式的状态，通过查看显示信息验证配置的效果。

表1-3 FIPS 的显示和维护

操作	命令
显示FIPS模式的状态	display fips status

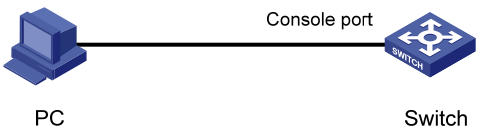
1.5 FIPS典型配置举例

1. 组网需求

- PC 通过 Console 口与 Switch 相连。
- 通过配置 Switch，使终端 PC 成功登录交换机，并进入设备的 FIPS 模式。

2. 组网图

图1-1 进入设备 FIPS 模式登录组网图



3. 配置步骤

配置 FIPS 模式。

```
<Sysname> system-view
```

```
[Sysname] fips mode enable
```

```
FIPS mode change requires a device reboot. Continue?[Y/N]:y
```

Change the configuration to meet FIPS mode requirements, save the configuration to the next-startup configuration file, and then reboot to enter FIPS mode.

开启密码管理功能。

```
[Sysname] password-control enable
# 在设备上添加一个本地用户 test，服务类型为终端用户类型，用户级别为 3 级，并设置其认证密码为 AAbbcc1234%（密码要包含大小写字母，数字和特殊符号组成，并且默认最短为 10 位）。
[Sysname] local-user test
[Sysname-luser-test] service-type terminal
[Sysname-luser-test] authorization-attribute level 3
[Sysname-luser-test] password
Password:*****
Confirm :*****
Updating user(s) information, please wait.....
[Sysname-luser-test] quit
```



注意

设置本地用户的密码时，请采用交互式方式进行设置，即本地用户视图下输入“password”回车后，在提示信息下输入相应密码。

```
# 保存配置。
[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 mainboard device successfully.
Configuration is saved to device successfully.
[Sysname] quit
# 重启设备。
<Sysname> reboot
```

4. 验证结果

重启设备后，输入用户名（test）密码（AAbbcc1234%），提示首次登录成功，请用户输入新密码（新密码和老密码必须至少四个字符不同）并确认后，成功登录设备。

User interface aux0 is available.

Please press ENTER.

Login authentication

```
Username:test
Password:
Info: First logged in. For security reasons you will need to change your password.
Please enter your new password.
Password:*****
Confirm :*****
Updating user(s) information, please wait.....
<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
```



注意

如果配置 FIPS 模式之前未配置本地用户名或密码，只能通过忽略配置文件重启或删除配置文件后重新启动设备，设备恢复到非 FIPS 模式启动。
