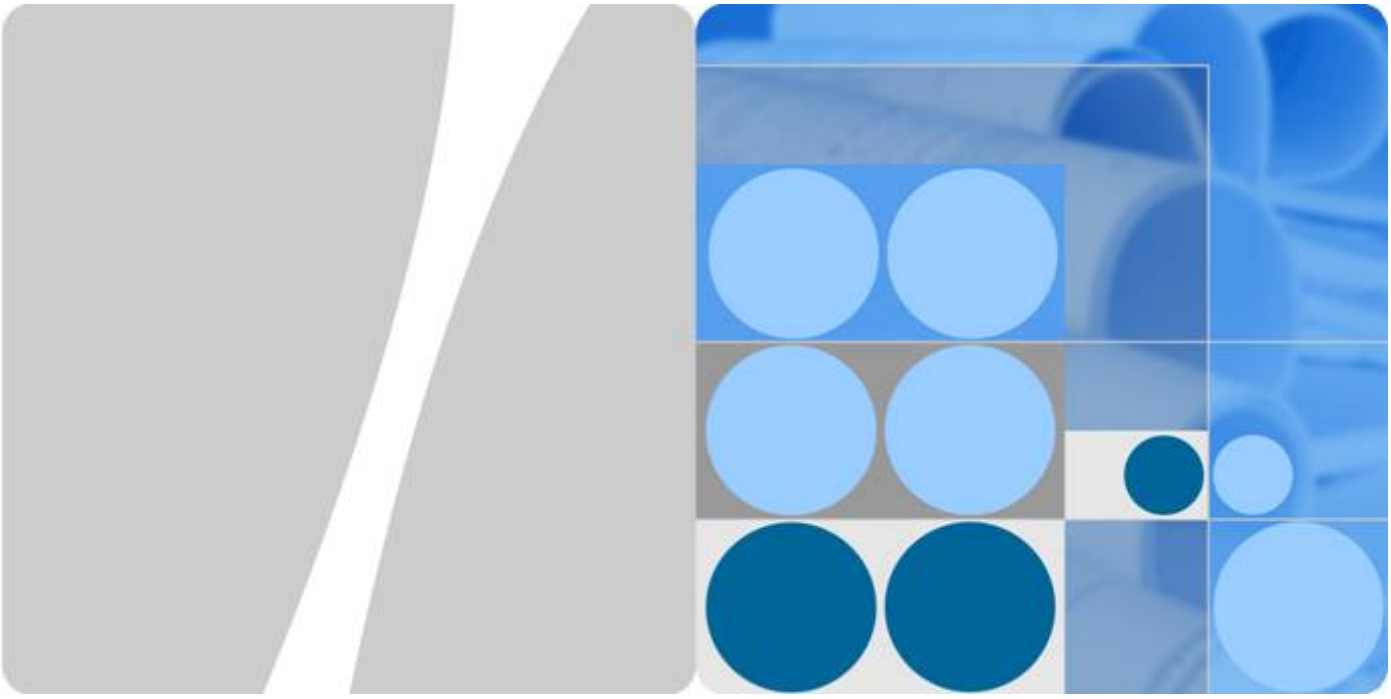


S600-E 系列交换机

V200R021C00

配置指南-安全

文档版本　02

发布日期　2022-06-07

华为技术有限公司

HUAWEI

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://e.huawei.com

前言

读者对象

本文档适用于负责配置和管理交换机的网络工程师。您应该熟悉以太网基础知识，且具有丰富的网络部署与管理经验。

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
须知	用于传递设备或环境安全警示信息。如不避免则可能会导致设备损坏、数据丢失、设备性能降低或其他不可预知的结果。 “须知”不涉及人身伤害。
说明	对正文中重点信息的补充说明。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

命令行格式约定

在本文中可能出现下列命令行格式，它们所代表的含义如下。

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。

格式	意义
{ x | y | ... }*	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...]*	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&的参数可以重复1～n次。
#	由“#”开始的行表示为注释行。

接口编号约定

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

安全约定

- 密码配置约定
  - 配置密码时请尽量选择密文模式(cipher)。为充分保证设备安全，请用户不要关闭密码复杂度检查功能，并定期修改密码。
  - 配置明文模式的密码时，请不要以“%^%#.....%^%#”、“%#%#.....%#%#”、“%@%@.....%@%@”或者“@%@%.....@%@%”作为起始和结束符。因为用这些字符为起始和结束符的是合法密文（本设备可以解密的密文），配置文件会显示与用户配置相同的明文。
  - 配置密文密码时，不同特性的密文密码不能互相使用。例如AAA特性生成的密文密码不能用于配置其他特性的密文密码。
- 加密算法约定

  目前设备采用的加密算法包括3DES、AES、RSA、SHA1、SHA2和MD5。3DES、RSA和AES加密算法是可逆的，SHA1、SHA2和MD5加密算法是不可逆的。DES/3DES/RSA(1024位以下)/MD5(数字签名场景和口令加密)/SHA1(数字签名场景)加密算法安全性低，存在安全风险。在协议支持的加密算法选择范围内，建议使用更安全的加密算法，比如AES/RSA(2048位以上)/SHA2/HMAC-SHA2。具体采用哪种加密算法请根据场景而定：对于管理员类型的密码，必须采用不可逆加密算法，推荐使用安全性更高的SHA2。
- 个人数据约定

  您购买的产品、服务或特性在业务运营或故障定位的过程中将可能获取或使用用户的某些个人数据（如终端用户的MAC地址或IP地址），因此您有义务根据所适用国家的法律制定必要的用户隐私政策并采取足够的措施以确保用户的个人数据受到充分的保护。
- 本文档中出现的“镜像端口、端口镜像、流镜像、镜像”等相关词汇仅限于为了描述该产品进行检测通信传输中的故障和错误的目的而使用，不涉及采集、处理任何个人数据或任何用户通信内容。
- 可靠性设计声明

  对于网络规划和站点设计，必须严格遵守可靠性设计原则，具备设备级和方案级保护。设备级保护包括双网双平面，双机、跨板双链路的规划原则，避免出现单

点，单链路故障。方案级指FRR、VRRP等快速收敛保护机制。在应用方案级保护时，应避免保护方案的主备路径经过相同链路或者传输，以免方案级保护不生效。

参考标准和协议

请登录**华为网站**，搜索“标准协议顺从表”，获取《华为 Sx7系列交换机 标准协议顺从表》。

特别声明

- 本文档仅作为使用指导，其内容（如Web界面、CLI命令格式、命令输出）依据实验室设备信息编写。文档提供的内容具有一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号不同、配置文件不同等原因，可能造成文档中提供的内容与用户使用的设备界面不一致。请以用户设备界面的信息为准，本文档不再针对前述情况造成的差异一一说明。
- 本文档中提供的最大值是设备在实验室特定场景（例如，被测试设备上只有某种类型的单板，或者只配置了某一种协议）达到的最大值。在现实网络中，由于设备硬件配置不同、承载的业务不同等原因会使设备测试出的最大值与文档中提供的数据不一致。
- 出于特性介绍及配置示例的需要，本文档可能会使用公网IP地址，如无特殊说明出现的公网IP地址均为示意，不指代任何实际意义。

目 录

1 安全概述

网络安全威胁

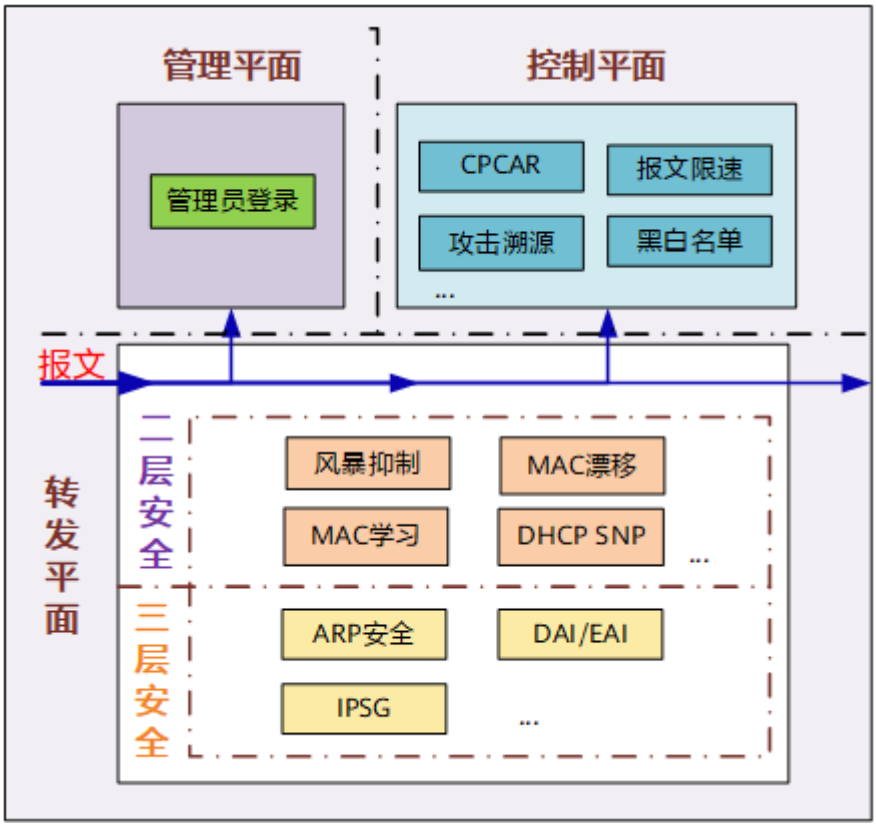
网络安全威胁是指网络系统所面临的，由已经发生的或潜在的安全事件对某一资源的保密性、完整性、可用性或合法使用所造成的威胁。能够在不同程度、不同范围内解决或者缓解网络安全威胁的手段和措施就是网络安全服务。

在网络中占有重要地位的交换机，不可避免的成为黑客攻击的重点对象。交换机的核心在于“交换”，因此交换机安全最重要的任务就是能够正常转发数据，并保证数据在传输过程中不被截获或者篡改。交换机的网络安全主要包括以下三个方面：

- 保密性：交换机存储、处理和传输的信息，不会被泄露到非授权的用户、实体或过程。即信息只为授权用户使用。
- 完整性：信息未经授权不能进行改变的特性。即网络信息在交换机存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等行为破坏和丢失的特性。
- 可用性：在要求的外部资源得到保证的前提下，交换机在规定的条件下和规定的时刻或时间区间内处于可执行规定功能状态的能力。业务持续可用，满足电信级服务质量要求。

为了满足上述要求，交换机从以下三个平面对网络安全进行规划和部署。如**图1-1**所示。

图 1-1 交换机安全规划部署图



管理平面

管理平面的安全重点在于确保设备能够被合法管理，包括哪些用户可以登录设备，登录到设备上的用户又可以进行哪些操作等。如图1-1所示，交换机管理平面的安全主要通过只允许管理员登录设备来实现。管理员登录就是保证管理员安全的管理设备，交换机通过设置用户名和密码、ACL限制用户登录，通过STelnet登录方式保证管理员登录过程安全，通过设置用户的级别控制用户操作权限。详细的原理和配置可以参见《 S600-E V200R021C00, C01 配置指南-基础配置 》登录设备命令行界面和登录设备Web网管界面。

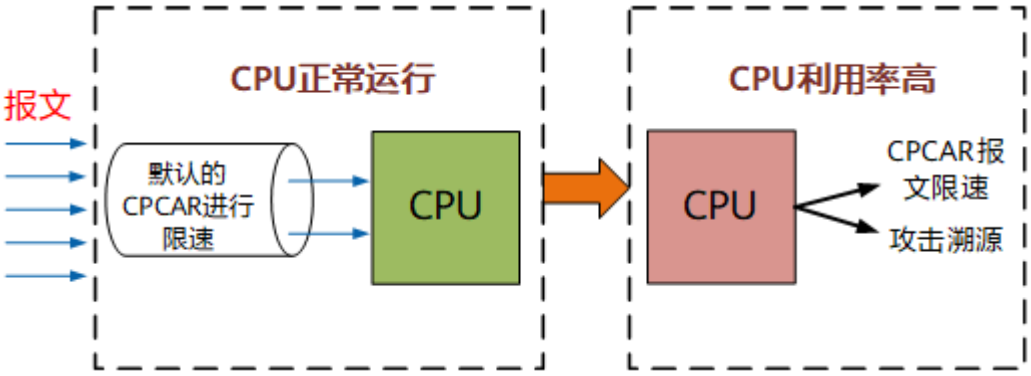
控制平面

控制平面主要通过CPU实现转发控制。CPU就像我们的大脑，指挥着设备各项机能的正常运转。CPU的安全是设备和协议正常运行的前提。如果上送CPU处理的协议报文过多导致CPU繁忙，设备性能就会下降，业务就会中断。因此，作为交换机的核心部件，CPU也就成为非法用户攻击的对象。交换机支持的控制平面的安全配置主要包括**本机防攻击**和**攻击防范**。

如图1-2所示，为了保证CPU的正常运行，交换机使用默认的CPCAR值对上送的协议报文进行限速。如果经过交换机默认的CPCAR限速后，上送CPU的报文依然超过了CPU可以处理的范围，CPU利用率很高，还可以通过以下方式做进一步的处理：

- 调整CPCAR值：缩小CPCAR值，减少上送CPU的协议报文的数量。
- 攻击溯源：对上送CPU的报文进行分析统计，设置检查阈值，对于超过检查阈值的报文执行相应的惩罚措施，如丢弃报文、Shutdown接口、设置黑名单等。

图 1-2 CPU 防攻击处理流程



转发平面

转发平面的作用就是通过查询转发表项指导数据流量正确转发，因此针对转发平面的攻击主要为以下两种：

- 耗尽转发表资源，导致合法用户的转发表无法被学习，合法用户的流量无法被转发。
- 篡改转发表，导致合法用户的流量转发至错误的地方。

基于交换机网络部署位置，主要分为二层网络的防攻击方法和三层网络的防攻击方法。

- 二层网络：二层网络数据转发依赖MAC表，所有数据流量的转发都需要查找MAC表，因此MAC表也就成为非法用户攻击二层网络的主要目标。非法用户通过发送大量的报文，迅速耗尽MAC表资源，使报文因查找不到MAC表项进行广播，从而占用带宽资源，产生广播风暴。交换机支持通过MAC学习控制、**端口安全**、**DHCP Snooping**和**风暴抑制**等方式来保护MAC表的安全。
- 三层网络：三层网络数据转发依赖ARP表和路由表。路由表是通过路由协议协商生成的，因此非法用户很难对此进行攻击。ARP表是通过协议报文生成的，非法用户可以发送大量的协议报文或者伪造协议报文使ARP表项出现异常。因此ARP表是交换机在三层网络中保护的主要对象。交换机支持通过**ARP安全**、**DAI**、EAI、**IPSG**防止此类攻击。

2 ACL 配置

2.1 ACL 简介

定义

访问控制列表ACL（Access Control List）是由一条或多条规则组成的集合。所谓规则，是指描述报文匹配条件的判断语句，这些条件可以是报文的源地址、目的地址、端口号等。

ACL本质上是一种报文过滤器，规则是过滤器的滤芯。设备基于这些规则进行报文匹配，可以过滤出特定的报文，并根据应用ACL的业务模块的处理策略来允许或阻止该报文通过。

ACL配置完成后，必须应用在业务模块中才能生效，其中最基本的ACL应用，就是在简化流策略/流策略中应用ACL，使设备能够基于全局、VLAN或接口下发ACL，实现对转

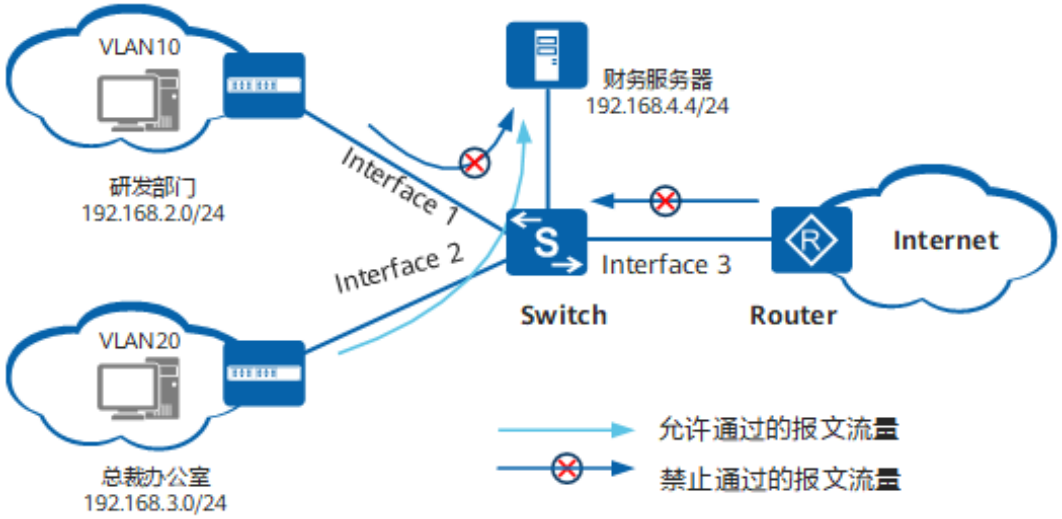
发报文的过滤。此外，ACL还可以应用在Telnet、FTP、路由等模块。业务模块之间的ACL默认处理动作和处理机制有所不同，具体请参见**2.2.7 ACL应用模块的ACL默认动作和处理机制**。

目的

ACL可以实现对网络中报文流的精确识别和控制，达到控制网络访问行为、防止网络攻击和提高网络带宽利用率的目的，从而切实保障网络环境的安全性和网络服务质量的可靠性。

图2-1是一个典型的ACL应用组网场景。

图 2-1 ACL 典型应用场景



某企业为保证财务数据安全，禁止研发部门访问财务服务器，但总裁办公室不受限制。实现方式：在Interface 1的入方向上部署ACL，禁止研发部门访问财务服务器的报文通过。Interface 2上无需部署ACL，总裁办公室访问财务服务器的报文默认允许通过。

保护企业内网环境安全，防止Internet病毒入侵。实现方式：在Interface 3的入方向上部署ACL，防止病毒通过该接口入侵。

2.2 ACL 原理描述

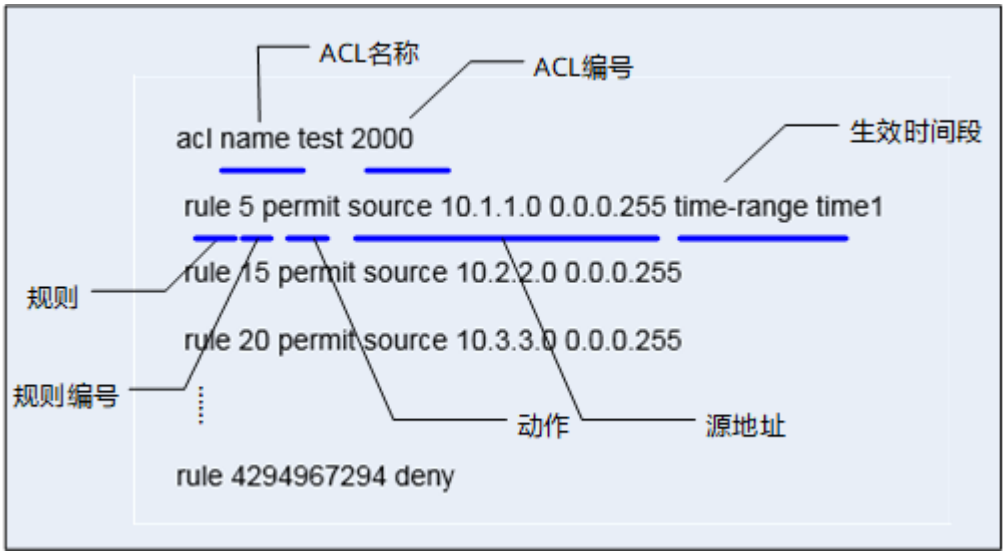
2.2.1 ACL 的基本原理

ACL由一系列规则组成，通过将报文与ACL规则进行匹配，设备可以过滤出特定的报文。设备支持软件ACL和硬件ACL两种实现方式。

ACL 的组成

一条ACL的结构组成，如图2-2所示。

图 2-2 ACL 的结构组成



- **ACL名称**：通过名称来标识ACL，就像用域名代替IP地址一样，更加方便记忆。这种ACL，称为命名型ACL。

  命名型ACL一旦创建成功，便不允许用户再修改其名称。

  仅基本ACL与基本ACL6，以及高级ACL与高级ACL6，可以使用相同的ACL名称；其他类型ACL之间，不能使用相同的ACL名称。

  命名型ACL实际上是“名字+数字”的形式，可以在定义命名型ACL时同时指定ACL编号。如果不指定编号，则由系统自动分配，设备为其分配的编号是该类型ACL可用编号中取值范围内的最大值。
- **ACL编号**：用于标识ACL，也可以单独使用ACL编号，表明该ACL是数字型。

  不同的ACL类型使用不同的ACL编号取值标识。
- **规则**：即描述报文匹配条件的判断语句。
  - **规则编号**：用于标识ACL规则。可以自行配置规则编号，也可以由系统自动分配。

    ACL规则的编号范围是0～4294967294，所有规则均按照规则编号从小到大进行排序。系统按照规则编号从小到大的顺序，将规则依次与报文匹配，一旦匹配上一条规则即停止匹配。
  - **动作**：报文处理动作，包括permit/deny两种，表示允许/拒绝。
  - **匹配项**：ACL定义了极其丰富的匹配项。除了图2-2中的源地址和生效时间段，ACL还支持很多其他规则匹配项。例如，二层以太网帧头信息（如源MAC、目的MAC、以太帧协议类型），三层报文信息（如目的IP地址、协议类型），以及四层报文信息（如TCP/UDP端口号）等。关于每种匹配项的详细介绍，请参见2.2.2 交换机支持的ACL及常用匹配项。

ACL 的实现方式

目前设备支持的ACL，有以下两种实现方式。

- 软件ACL：针对与本机交互的报文（必须上送CPU处理的报文），由软件实现来过滤报文的ACL，比如FTP、TFTP、Telnet、SNMP、HTTP、路由协议、组播协议中引用的ACL。

- 硬件ACL：针对所有报文，通过下发ACL资源到硬件来过滤报文的ACL，比如流策略、基于ACL的简化流策略、用户组以及为接口收到的报文添加外层Tag功能中引用的ACL。

两者主要区别在于：

- 过滤的报文类型不同：软件ACL用来过滤与本机交互的报文，硬件ACL可以用来过滤所有报文。
- 报文过滤方式不同：软件ACL是被上层软件引用来实现报文的过滤，硬件ACL是被下发到硬件来实现报文的过滤。通过软件ACL过滤报文时，会消耗CPU资源，通过硬件ACL过滤报文时，则会占用硬件资源。通过硬件ACL过滤报文的速度更快。
- 对不匹配ACL的报文的处理动作不同：当使用软件ACL时，如果报文未匹配上ACL中的规则，设备对该报文采取的动作为deny，即拒绝报文通过；当使用硬件ACL时，如果报文未匹配上ACL中的规则，设备对该报文采取的动作为permit，即允许报文通过。

2.2.2 交换机支持的 ACL 及常用匹配项

交换机支持的 ACL

如表2-1所示，交换机支持的ACL规则包括过滤IPv4报文的ACL、过滤IPv6报文的ACL6以及既支持过滤IPv4报文又支持过滤IPv6报文的二层ACL和用户自定义ACL。

表 2-1 交换机支持的 ACL

分类	适用的IP版本	规则定义描述	编号范围
基本ACL	IPv4	仅使用报文的**源IP地址**、分片信息和生效时间段信息来定义规则。	2000～2999
高级ACL	IPv4	既可使用IPv4报文的**源IP地址**，也可使用**目的IP地址**、IP协议类型、ICMP类型、TCP源/目的端口、UDP源/目的端口号、生效时间段等来定义规则。	3000～3999
二层ACL	IPv4和IPv6	使用报文的**以太网帧头信息**来定义规则，如根据源MAC（Media Access Control）地址、目的MAC地址、二层协议类型等。	4000～4999
用户自定义ACL	IPv4和IPv6	使用**报文头、偏移位置、字符串掩码和用户自定义字符串**来定义规则，即以报文头为基准，指定从报文的第几个字节开始与字符串掩码进行“与”操作，并将提取出的字符串与用户自定义的字符串进行比较，从而过滤出相匹配的报文。	5000～5999

分类	适用的IP版本	规则定义描述	编号范围
用户ACL	IPv4	既可使用IPv4报文的**源IP地址或源UCL（User Control List）组**，也可使用**目的IP地址或目的UCL组**、IP协议类型、ICMP类型、TCP源端口/目的端口、UDP源端口/目的端口号等来定义规则。	6000～9999
基本ACL6	IPv6	可使用IPv6报文的**源IPv6地址**、分片信息和生效时间段来定义规则。	2000～2999
高级ACL6	IPv6	可以使用IPv6报文的**源IPv6地址**、**目的IPv6地址**、IPv6协议类型、ICMPv6类型、TCP源/目的端口、UDP源/目的端口号、生效时间段等来定义规则。	3000～3999
用户ACL6	IPv6	既可使用IPv6报文的**源IPv6地址或源UCL组**，也可使用**目的IPv6地址**、IPv6协议类型、ICMPv6类型、TCP源端口/目的端口、UDP源端口/目的端口号等来定义规则。	6000～9999

常用匹配项

交换机支持的ACL匹配项种类非常丰富，其中最常用的匹配项包括以下几种。

- **生效时间段**

  所有ACL均支持根据生效时间段**time-range** *time-name*过滤报文。关于生效时间段的详细介绍，请参见**2.2.4 ACL的生效时间段**。

- **IP承载的协议类型**

  格式：*protocol-number* | **icmp** | **tcp** | **udp** | **gre** | **igmp** | **ip** | **ipinip** | **ospf**

  高级ACL支持基于协议类型过滤报文，常用的协议类型如下表所示。

协议类型	协议编号
ICMP	1
TCP	6
UDP	17
GRE	47
IGMP	2
IPinIP	4
OSPF	89

IP表示任何IP层协议。协议号的取值可以是1～255。

例如，当设备某个接口下的用户存在大量的攻击者时，如果希望能够禁止这个接口下的所有用户接入网络，则可以通过指定协议类型为IP来屏蔽这些用户的IP流量来达到目的。配置如下：

```
rule deny ip //表示拒绝IP报文通过
```

- **源/目的IP地址及其通配符掩码**

  源IP地址及其通配符掩码格式：**source** { *source-address source-wildcard* | **any** }

  目的IP地址及其通配符掩码格式：**destination** { *destination-address destination-wildcard* | **any** }

  基本ACL支持根据源IP地址过滤报文，高级ACL不仅支持源IP地址，还支持根据目的IP地址过滤报文。

  将源/目的IP地址定义为规则匹配项时，需要在源/目的IP地址字段后面同时指定通配符掩码，用来与源/目的IP地址字段共同确定一个地址范围。

  IP地址通配符掩码与IP地址的反向子网掩码类似，也是一个32比特位的数字字符串，用于指示IP地址中的哪些位将被检查。各比特位中，“0”表示“检查相应的位”，“1”表示“不检查相应的位”，概括为一句话就是“检查0，忽略1”。但与IP地址子网掩码不同的是，子网掩码中的“0”和“1”要求必须连续，而通配符掩码中的“0”和“1”可以不连续。

  通配符掩码可以为0，相当于0.0.0.0，表示源/目的地址为主机地址；也可以为255.255.255.255，表示任意IP地址，相当于指定**any**参数。

  举一个IP地址通配符掩码的示例，当希望来自192.168.1.0/24网段的所有IP报文都能够通过，可以配置如下规则：

  ```
  rule 5 permit ip source 192.168.1.0 0.0.0.255
  ```

  规则中的通配符掩码为0.0.0.255，表示只需检查IP地址的前三组二进制八位数对应的比特位。因此，如果报文源IP地址的前24个比特位与参照地址的前24个比特位（192.168.1）相同，即报文的源IP地址是192.168.1.0/24网段的地址，则允许该报文通过。**表2-2**展示了该例的地址范围计算过程。

表 2-2 通配符掩码示例

项目	十进制等价值	二进制等价值
参照地址	192.168.1.0	11000000.10101000.00000001.00000000
通配符掩码	0.0.0.255	00000000.00000000.00000000.**11111111**
确定的地址范围	192.168.1.* *表示0～255之间的整数	11000000.10101000.00000001.**xxxxxxxx** x既可以是0，也可以是1

更多的IP地址与通配符掩码共同确定的地址范围示例，详见**表2-3**。

表 2-3 IP 地址与通配符掩码共同确定的地址范围

IP地址	IP地址通配符掩码	确定的地址范围
0.0.0.0	255.255.255.255	任意IP地址
172.18.0.0	0.0.255.255	172.18.0.0/16网段的IP地址
172.18.5.2	0.0.0.0	仅172.18.5.2这一个主机地址
172.18.8.0	0.0.0.7	172.18.8.0/29网段的IP地址
172.18.8.8	0.0.0.7	172.18.8.8/29网段的IP地址
10.1.2.0	0.0.254.255（通配符掩码中的1和0不连续）	10.1.0.0/24～10.1.254.0/24网段之间且第三个字节为偶数的IP地址，如10.1.0.0/24、10.1.2.0/24、10.1.4.0/24、10.1.6.0/24等。

- **源/目的MAC地址及其通配符掩码**

  源MAC地址及其通配符掩码格式：**source-mac** *source-mac-address* [*source-mac-mask*]

  目的地址及其通配符掩码格式：**destination-mac** *dest-mac-address* [*dest-mac-mask*]

  仅二层ACL支持基于源/目的MAC地址过滤报文。

  将源/目的MAC地址定义为规则匹配项时，可以在源/目的MAC地址字段后面同时指定通配符掩码，用来与源/目的MAC地址字段共同确定一个地址范围。

  MAC地址通配符掩码的格式与MAC地址相同，采用十六进制数表示，共六个字节（48位），用于指示MAC地址中的哪些位将被检查。与IP地址通配符掩码不同的是，MAC地址通配符掩码各比特位中，1表示“检查相应的位”，0表示“不检查相应的位”。如果不指定通配符掩码，则默认掩码为ffff-ffff-ffff，表示检查MAC地址的每一位。

  MAC地址与通配符掩码共同确定的地址范围示例，如表2-4所示。

表 2-4 MAC 地址与通配符掩码共同确定的地址范围

MAC地址	MAC地址通配符掩码	确定的地址范围
00e0-fc01-0101	0000-0000-0000	任意MAC地址
00e0-fc01-0101	ffff-ffff-ffff	仅00e0-fc01-0101这一个MAC地址
00e0-fc01-0101	ffff-ffff-0000	00e0-fc01-0000～00e0-fc01-ffff

- **VLAN编号及其掩码**

  外层VLAN及其掩码格式：**vlan-id** *vlan-id* [*vlan-id-mask*]

将VLAN编号定义为规则匹配项时，可以在VLAN编号字段后面同时指定VLAN掩码，用来与VLAN编号字段共同确定一个VLAN范围。

VLAN掩码的格式是十六进制形式，取值范围是0x0～0xFFF。如果不指定VLAN掩码，则默认掩码为0xFFF，表示检查VLAN编号的每一位。

VLAN编号与掩码共同确定的VLAN范围示例，如表2-5所示。

表 2-5 VLAN 编号及其掩码共同确定的 VLAN 范围

VLAN编号	VLAN掩码	确定的VLAN范围
10	0x000	任意VLAN
10	0xFFF	仅VLAN 10
10	0xFF0	VLAN 1～VLAN 15

- **TCP/UDP端口号**

  源端口号格式：**source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }

  目的端口号格式：**destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }

  在高级ACL中，当协议类型指定为TCP或UDP时，设备支持基于TCP/UDP的源/目的端口号过滤报文。

  其中，TCP/UDP端口号的比较符含义如下：

  - **eq** *port*：指定等于源/目的端口。
  - **gt** *port*：指定大于源/目的端口。
  - **lt** *port*：指定小于源/目的端口。
  - **range** *port-start port-end*：指定源/目的端口的范围。*port-start*是端口范围的起始，*port-end*是端口范围的结束。

  TCP/UDP端口号可以使用数字表示，也可以用字符串（助记符）表示。例如，**rule deny tcp destination-port eq 80**，可以用**rule deny tcp destination-port eq www**替代。常见TCP/UDP端口号及对应的字符串参见**rule（高级ACL视图）**中的常用TCP协议源端口号或者目的端口号与*port*的取值对应关系和常用UDP协议源端口号或者目的端口号与*port*的取值对应关系表。

- **TCP标志信息**

  格式：**tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** }*

  在高级ACL中，当协议类型指定为TCP时，设备支持基于TCP标志信息过滤报文。

  TCP报文头有6个标志位：ack (acknowledge)、fin (finish)、psh (push)、rst (reset)、syn (synchronize)和urg (urgent)。

  TCP标志信息中的**established**，表示标志位为ACK(010000)或RST(000100)。

  指定**tcp-flag**的ACL规则可以用来实现单向访问控制。假设，要求192.168.1.0/24网段用户可以主动访问192.168.2.0/24网段用户，但反过来192.168.2.0/24网段用户不能主动访问192.168.1.0/24。可通过在设备上连接192.168.2.0/24网段的接口入方向上，应用ACL规则来实现该需求。

  由TCP建立连接和关闭连接的过程可知，只有在TCP中间连接过程的报文才会ACK=1或者RST=1。根据这个特点，配置如下两种ACL规则，允许TCP中间连接过程的报文通过，拒绝其他TCP报文通过，就可以限制192.168.2.0/24网段主动发起的TCP连接。

- 类型一：配置指定**ack**和**rst**参数的ACL规则

```
rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack  //允许ACK=1的TCP报文通过
rule 10 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag rst  //允许RST=1的TCP报文通过
rule 15 deny tcp source 192.168.2.0 0.0.0.255  //拒绝其他TCP报文通过
```

- 类型二：配置指定**established**参数的ACL规则

```
rule permit tcp source 192.168.2.0 0.0.0.255 tcp-flag established  // established表示ACK=1或者RST=1，表示允许TCP中间连接过程的报文通过
rule deny tcp source 192.168.2.0 0.0.0.255    //拒绝其他TCP报文通过
```

- **IP分片信息**

  格式：**fragment**

  基本ACL和高级ACL支持基于IP分片信息过滤报文。

  IP分片除了首片报文外，还有后续分片报文，又叫做非首片分片报文。仅首片分片报文携带四层信息（如TCP/UDP端口号等），后续分片报文均不携带。网络设备收到分片报文后，会判断其是否是最后一个分片报文。如果不是，则为其分配内存空间，以便于最后一个分片报文到达后完成重组。黑客可以利用这一点，向接收方设备发起分片报文攻击，始终不向接收方发送最后一个分片报文。

  为了解决这个问题，可以配置指定**fragment**匹配项的ACL规则来阻塞非首片分片报文，从而达到防范分片报文攻击的目的。

  针对非分片报文、首片分片报文、非首片分片报文这三类报文，ACL的处理方式如**表2-6**所示。

  表 2-6 ACL 对 IP 分片报文的处理方式

规则包含的匹配项	非分片报文	首片分片报文	非首片分片报文
三层信息（如源/目的IP地址）	三层信息匹配上，则返回匹配结果（permit/deny）；未匹配上，则转下一条规则进行匹配	三层信息匹配上，则返回匹配结果（permit/deny）；未匹配上，则转下一条规则进行匹配	三层信息匹配上，则返回匹配结果（permit/deny）；未匹配上，则转下一条规则进行匹配
三层信息 + 四层信息（如TCP/UDP端口号）	三层和四层信息都匹配上，则返回匹配结果（permit/deny）；未匹配上，则转下一条规则进行匹配	三层和四层信息都匹配上，则返回匹配结果（permit/deny）；未匹配上，则转下一条规则进行匹配	不匹配，转下一条规则进行匹配
三层信息 + **fragment**	不匹配，转下一条规则进行匹配	不匹配，转下一条规则进行匹配	三层信息匹配上，则返回匹配结果（permit/deny）；未匹配上，则转下一条规则进行匹配

  例如，ACL 3012中存在以下规则：

```
#
acl number 3012
 rule 5 deny tcp destination 192.168.2.2 0 fragment
 rule 10 permit tcp destination 192.168.2.2 0 destination-port eq www
 rule 15 deny ip
#
```

对于目的IP地址是192.168.2.2的TCP报文：

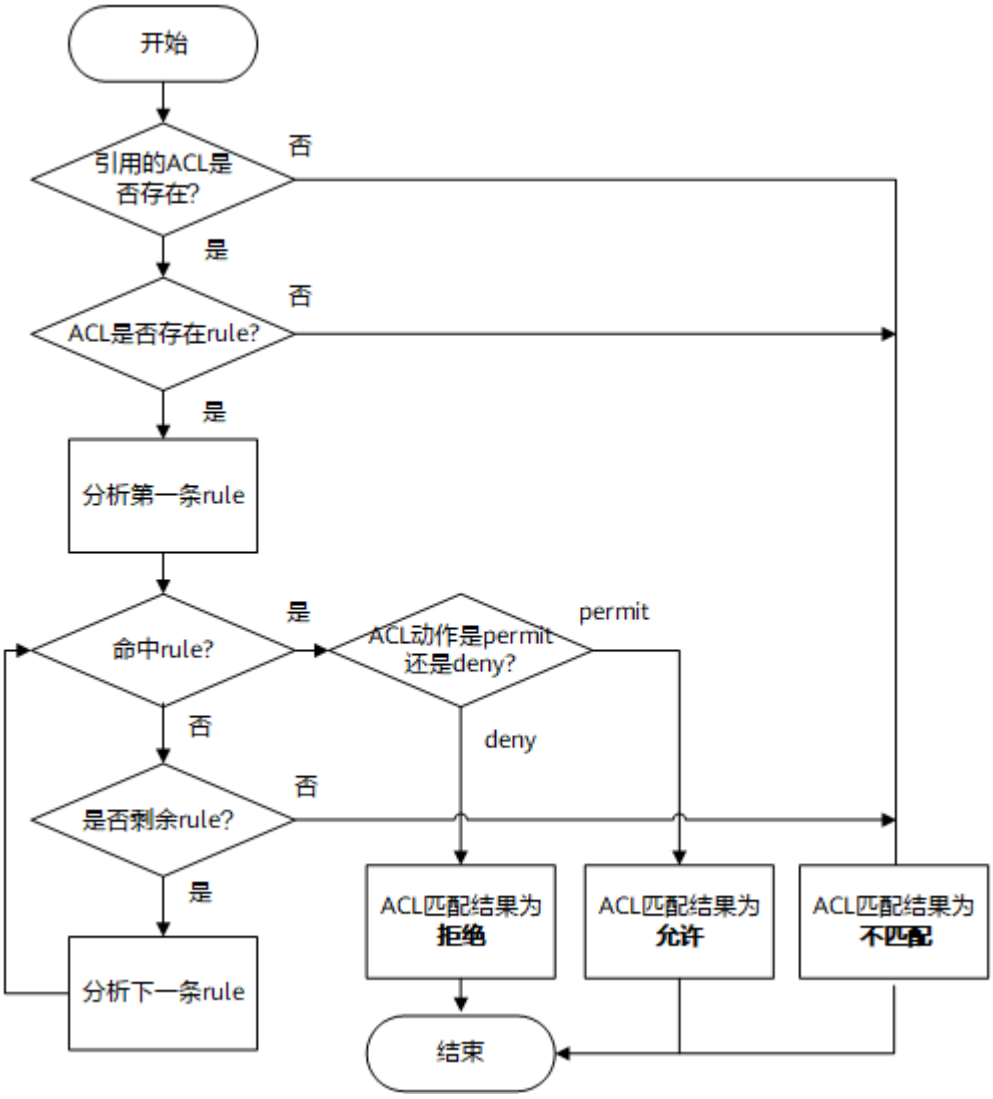
- 该报文是非分片报文或首片分片报文时：如果该报文的目的端口号是80（www对应的端口号是80），则报文与rule 10匹配，报文被允许通过；如果该报文的目的端口号不是80，则报文与rule 15匹配，报文被拒绝通过。
- 该报文是非首片分片报文时：该报文与rule 5匹配，报文被拒绝通过。

2.2.3 ACL 的匹配机制

ACL 的匹配机制

设备将报文与ACL规则进行匹配时，遵循“一旦命中即停止匹配”的机制，如图2-3所示。

图 2-3 ACL 的匹配机制



从上面的ACL匹配流程可以看出，报文与ACL规则匹配后，会产生两种结果：“命中规则”和“未命中规则”。

- 命中规则：指存在ACL，且在ACL中查找到了符合匹配条件的规则。
- 未命中规则：指不存在ACL，或ACL中无规则，再或者在ACL中遍历了所有规则都没有找到符合匹配条件的规则。

报文最终是被允许通过还是拒绝通过，实际是ACL规则中的指定动作和应用ACL的各个业务模块来共同决定。不同的业务模块，对命中和未命中规则报文的处理方式也各不相同。例如，在Telnet模块中应用ACL，只要报文命中了规则且ACL规则动作为permit，就允许通过；而在流策略中应用ACL，如果报文命中了规则且ACL规则动作为permit，但流行为动作配置的是deny，该报文仍会被拒绝通过。关于各个业务模块ACL处理机制的详细介绍，请参见**2.2.7 ACL应用模块的ACL默认动作和处理机制**。

匹配顺序

如上面的流程图所示，一条ACL由多条rule规则组成时，这些规则可能存在重复或矛盾的地方。例如，在一条ACL中先后配置以下两条规则：

```
rule deny ip destination 10.1.0.0 0.0.255.255   //表示拒绝目的IP地址为10.1.0.0/16网段地址的报文通过
rule permit ip destination 10.1.1.0 0.0.0.255   //表示允许目的IP地址为10.1.1.0/24网段地址的报文通过，该网段地址范围小于10.1.0.0/16网段范围
```

对于目的IP=10.1.1.1的报文，如果系统先将deny规则与其匹配，则该报文会被拒绝通过。相反，如果系统先将permit规则与其匹配，则该报文会得到允许通过。

因此，对于规则之间存在重复或矛盾的情形，报文的匹配结果与ACL的匹配顺序是息息相关的。

设备支持两种ACL匹配顺序：配置顺序（**config**模式）和自动排序（**auto**模式）。缺省的ACL匹配顺序是**config**模式。

配置顺序

配置顺序，即系统按照ACL规则编号从小到大的顺序进行报文匹配，规则编号越小越容易被匹配。

- 如果配置规则时指定了规则编号，则规则编号越小，规则插入位置越靠前，该规则越先被匹配。
- 如果配置规则时未指定规则编号，则由系统自动为其分配一个编号。该编号是一个大于当前ACL内最大规则编号且是步长整数倍的最小整数，因此该规则会被最后匹配。

自动排序

自动排序，是指系统使用“深度优先”的原则，将规则按照精确度从高到低进行排序，并按照精确度从高到低的顺序进行报文匹配。规则中定义的匹配项限制越严格，规则的精确度就越高，即优先级越高，系统越先匹配。各类ACL的“深度优先”顺序匹配原则如**表2-7**所示。

表 2-7 “深度优先”匹配原则

ACL类型	匹配顺序（从高到低）
基本ACL&ACL6	1. 源IP地址范围，源IP地址范围小（IP地址通配符掩码中“0”位的数量多）的规则优先。 2. 规则编号，规则编号小的优先。

ACL类型	匹配顺序（从高到低）
高级ACL&ACL6	1. 协议范围，指定了IP协议承载的协议类型的规则优先。 2. 源IP地址范围，源IP地址范围小（IP地址通配符掩码中“0”位的数量多）的规则优先。 3. 目的IP地址范围，目的IP地址范围小（IP地址通配符掩码中“0”位的数量多）的规则优先。 4. 四层端口号（TCP/UDP端口号）范围，四层端口号范围小的规则优先。 5. 规则编号，规则编号小的优先。
二层ACL	1. 二层协议类型通配符掩码，通配符掩码大（协议类型通配符掩码中“1”位的数量多）的规则优先。 2. 源MAC地址范围，源MAC地址范围小（MAC地址通配符掩码中“1”位的数量多）的规则优先。 3. 目的MAC地址范围，目的MAC地址范围小（MAC地址通配符掩码中“1”位的数量多）的规则优先。 4. 规则编号，规则编号小的优先。
用户自定义ACL	用户自定义ACL规则的匹配顺序只支持配置顺序，即规则编号从小到大的顺序进行匹配。
用户ACL&ACL6	1. 协议范围，指定了IP协议承载的协议类型的规则优先。 2. 源IP地址范围。如果规则的源IP地址均为IP网段，则源IP地址范围小（IP地址通配符掩码中“0”位的数量多）的规则优先，否则，源IP地址为IP网段的规则优先于源IP地址为UCL组的规则。 3. 目的IP地址范围。如果规则的目的IP地址均为IP网段，则目的IP地址范围小（IP地址通配符掩码中“0”位的数量多）的规则优先，否则，目的IP地址为IP网段的规则优先于目的IP地址为UCL组的规则。 4. 四层端口号（TCP/UDP端口号）范围，四层端口号范围小的规则优先。 5. 规则编号，规则编号小的优先。

关于**表2-7**中提到的ACL匹配项的详细介绍，请参见**2.2.2 交换机支持的ACL及常用匹配项**。

在自动排序的ACL中配置规则时，不允许自行指定规则编号。系统能自动识别出该规则在这条ACL中对应的优先级，并为其分配一个适当的规则编号。

例如，在**auto**模式的高级ACL 3001中，先后配置以下两条规则：

```
rule deny ip destination 10.1.0.0 0.0.255.255  //表示拒绝目的IP地址为10.1.0.0/16网段地址的报文通过
rule permit ip destination 10.1.1.0 0.0.0.255  //表示允许目的IP地址为10.1.1.0/24网段地址的报文通过，该网段地址范围小于10.1.0.0/16网段范围
```

两条规则协议范围、源IP地址范围相同，所以根据**表2-7**中高级ACL的深度优先匹配原则，接下来需要进一步比较规则的目的IP地址范围。由于permit规则指定的目的地址范围小于deny规则，所以permit规则的精确度更高，系统为其分配的规则编号更小。配置完上述两条规则后，ACL 3001的规则排序如下：

```
#
acl number 3001 match-order auto
```

```
 rule 5 permit ip destination 10.1.1.0 0.0.0.255
 rule 10 deny ip destination 10.1.0.0 0.0.255.255
#
```

此时，如果再插入一条新的规则rule deny ip destination 10.1.1.1 0（目的IP地址范围是主机地址，优先级高于以上两条规则），则系统将按照规则的优先级关系，重新为各规则分配编号。插入新规则后，ACL 3001新的规则排序如下：

```
#
acl number 3001 match-order auto
 rule 5 deny ip destination 10.1.1.1 0
 rule 10 permit ip destination 10.1.1.0 0.0.0.255
 rule 15 deny ip destination 10.1.0.0 0.0.255.255
#
```

相比**config**模式的ACL，**auto**模式ACL的规则匹配顺序更为复杂，但是**auto**模式ACL有其独特的应用场景。例如，在网络部署初始阶段，为了保证网络安全性，管理员定义了较大的ACL匹配范围，用于丢弃不可信网段范围的所有IP报文。随着时间的推移，实际应用中需要允许这个大范围中某些特征的报文通过。此时，如果管理员采用的是**auto**模式，则只需要定义新的ACL规则，无需再考虑如何对这些规则进行排序避免报文被误丢弃。

2.2.4 ACL 的生效时间段

产生背景

ACL的生效时间段可以规定ACL规则在何时生效，比如某个特定时间段或者每周的某个固定时间段。管理员可以根据网络访问行为的要求和网络的拥塞情况，配置一个或多个ACL生效时间段，然后在ACL规则中引用该时间段，从而实现在不同的时间段设置不同的策略，达到网络优化的目的。

生效时间段模式

在ACL规则中引用的生效时间段存在两种模式：

- 第一种模式——周期时间段：以星期为参数来定义时间范围，表示规则以一周为周期（如每周一的8至12点）循环生效。
- 第二种模式——绝对时间段：从某年某月某日的某一时间开始，到某年某月某日的某一时间结束，表示规则在这段时间范围内生效。

可以使用同一名称（*time-name*）配置内容不同的多条时间段，配置的各周期时间段之间以及各绝对时间段之间的交集将成为最终生效的时间范围。

多个周期时间段之间是或的关系，多个绝对时间段之间也是或的关系，周期时间段和绝对时间段之间是与的关系。如果多个周期时间段之间冲突，那就这几个时间段都生效，多个绝对时间段也是一样的。如果周期时间段和绝对时间段之间冲突，配置的时间段不生效。

例如，在ACL 2001中引用了时间段“test”，“test”包含了三个生效时间段：

```
#
time-range test 8:00 to 18:00 working-day
time-range test 14:00 to 18:00 off-day
time-range test from 00:00 2014/01/01 to 23:59 2014/12/31
#
acl number 2001
 rule 5 permit time-range test
```

- 第一个时间段，表示在周一到周五每天8:00到18:00生效，这是一个周期时间段。
- 第二个时间段，表示在周六、周日下午14:00到18:00生效，这是一个周期时间段。

- 第三个时间段，表示从2014年1月1日00:00起到2014年12月31日23:59生效，这是一个绝对时间段。

时间段“test”最终描述的时间范围为：2014年的周一到周五每天8:00到18:00以及周六和周日下午14:00到18:00。

如果第三个时间配置为2014年1月1日19:00起到2014年1月1日21:00，则时间段“test”无效。

2.2.5 ACL 的步长设定

步长的含义

步长，是指系统自动为ACL规则分配编号时，每个相邻规则编号之间的差值。

系统为ACL中首条未手工指定编号的规则分配编号时，使用步长值作为该规则的起始编号；为后续规则分配编号时，则使用大于当前ACL内最大规则编号且是步长整数倍的最小整数作为规则编号。例如ACL中包含规则rule 5和rule 12，ACL的缺省步长为5，大于12且是5的倍数的最小整数是15，所以系统分配给新配置的规则的编号为15。

基本ACL6和高级ACL6不支持步长设定，缺省步长为5。

步长的作用

设置步长的作用，在于方便后续在旧规则之间插入新的规则。

假设，一条ACL中，已包含了三条规则rule 5、rule 10、rule 15，步长是5。

```
rule 5 deny source 10.1.1.1 0  //表示拒绝源IP地址为10.1.1.1的报文通过
rule 10 deny source 10.1.1.2 0 //表示拒绝源IP地址为10.1.1.2的报文通过
rule 15 permit source 10.1.1.0 0.0.0.255 //表示允许源IP地址为10.1.1.0/24网段地址的报文通过
```

如果希望源IP地址为10.1.1.3的报文也被拒绝通过，该如何处理？由于ACL匹配报文时遵循“**一旦命中即停止匹配**”的原则，rule 15规则定义的网段包含10.1.1.3，所以源IP地址为10.1.1.3的报文，会命中rule 15而允许通过。若想让源IP地址为10.1.1.3的报文也被拒绝通过，则必须在rule 15之前插入一条新规则rule 11，这样源IP地址为10.1.1.3的报文，就会因先命中rule 11而被系统拒绝通过。如果这条ACL的规则间隔是1（rule 1、rule 2、rule 3…），这时再想插入新的规则，就只能先删除已有的规则，然后再配置新规则，最后将之前删除的规则重新配置还原。

```
rule 5 deny source 10.1.1.1 0  //表示禁止源IP地址为10.1.1.1的报文通过
rule 10 deny source 10.1.1.2 0 //表示禁止源IP地址为10.1.1.2的报文通过
rule 11 deny source 10.1.1.3 0 //表示拒绝源IP地址为10.1.1.3的报文通过
rule 15 permit source 10.1.1.0 0.0.0.255 //表示允许源IP地址为10.1.1.0网段地址的报文通过
```

2.2.6 ACL 的常用配置原则

配置ACL规则时，可以遵循以下原则：

1. 如果配置的ACL规则存在包含关系，应注意严格条件的规则编号需要排序靠前，宽松条件的规则编号需要排序靠后，避免报文因命中宽松条件的规则而停止往下继续匹配，从而使其无法命中严格条件的规则。
2. 根据各业务模块ACL默认动作（请参见**2.2.7 ACL应用模块的ACL默认动作和处理机制**）的不同，ACL的配置原则也不同。例如，在默认动作为permit的业务模块中，如果只希望deny部分IP地址的报文，只需配置具体IP地址的deny规则，结尾无需添加任意IP地址的permit规则；而默认动作为deny的业务模块恰与其相反。详细的ACL常用配置原则，如**表2-8**所示。

说明

以下rule的表达方式仅是示意形式，实际配置方法请参考各类ACL规则的命令行格式。

- **rule permit/deny a**/**rule permit/deny b**：表示允许或拒绝指定的报文通过，a/b表示指定报文的标识，其中b的范围大于a，即b包含a。

表 2-8 ACL 的常用配置原则

业务模块的ACL默认动作	permit所有报文	deny所有报文	permit少部分报文，deny大部分报文	deny少部分报文，permit大部分报文
permit	无需应用ACL	配置**rule deny**	需先配置**rule permit a**，再配置**rule deny b**或**rule deny** **说明** 以上原则适用于报文过滤的情形。当ACL应用于流策略中进行流量监管或者流量统计时，如果仅希望对指定的报文进行限速或统计，则只需配置**rule permit a**。	只需配置**rule deny a**，无需再配置**rule permit b**或**rule permit** **说明** 如果配置**rule permit**并在流策略中应用ACL，且该流策略的流行为behavior配置为**deny**，则设备会拒绝所有报文通过，导致全部业务中断。
deny	• 路由和组播模块：需配置**rule permit** • 其他模块：无需应用ACL	• 路由和组播模块：无需应用ACL • 其他模块：需配置**rule deny**	只需配置**rule permit a**，无需再配置**rule deny b**或**rule deny**	需先配置**rule deny a**，再配置**rule permit b**或**rule permit**

举例：

- 例1：在流策略中应用ACL，使设备对192.168.1.0/24网段的报文进行过滤，拒绝192.168.1.2和192.168.1.3主机地址的报文通过，允许192.168.1.0/24网段的其他地址的报文通过。

  流策略的ACL默认动作为**permit**，该例属于“deny少部分报文，permit大部分报文”的情况，所以只需配置**rule deny a**。

  ```
  #
  acl number 2000
   rule 5 deny source 192.168.1.2 0
   rule 10 deny source 192.168.1.3 0
  #
  ```

- 例2：在流策略中应用ACL，使设备对192.168.1.0/24网段的报文进行过滤，允许192.168.1.2和192.168.1.3主机地址的报文通过，拒绝192.168.1.0/24网段的其他地址的报文通过。

流策略的ACL默认动作为**permit**，该例属于“permit少部分报文，deny大部分报文”的情况，所以需先配置**rule permit a**，再配置**rule deny b**。

```
#
acl number 2000
 rule 5 permit source 192.168.1.2 0
 rule 10 permit source 192.168.1.3 0
 rule 15 deny source 192.168.1.0 0.0.0.255
#
```

- 例3：在Telnet中应用ACL，仅允许管理员主机（IP地址为172.16.105.2）能够Telnet登录设备，其他用户不允许Telnet登录。

  Telnet的ACL默认动作为**deny**，该例属于“permit少部分报文，deny大部分报文”的情况，所以只需配置**rule permit a**。

  ```
  #
  acl number 2000
   rule 5 permit source 172.16.105.2 0
  #
  ```

- 例4：在Telnet中应用ACL，不允许某两台主机（IP地址为172.16.105.3和172.16.105.4）Telnet登录设备，其他用户均允许Telnet登录。

  Telnet的ACL默认动作为**deny**，该例属于“deny少部分报文，permit大部分报文”的情况，所以需先配置**rule deny a**，再配置**rule permit**。

  ```
  #
  acl number 2000
   rule 5 deny source 172.16.105.3 0
   rule 10 deny source 172.16.105.4 0
   rule 15 permit
  #
  ```

- 例5：在FTP中应用ACL，不允许用户在周六的00:00～8:00期间访问FTP服务器，允许用户在其他任意时间访问FTP服务器。

  FTP的ACL默认动作为**deny**，该例属于“deny少部分报文，permit大部分报文”的情况，所以需先配置**rule deny a**，再配置**rule permit b**。

  ```
  #
  time-range t1 00:00 to 08:00 Sat
  time-range t2 00:00 to 23:59 daily
  #
  acl number 2000
   rule 5 deny time-range t1
   rule 10 permit time-range t2
  #
  ```

2.2.7 ACL 应用模块的 ACL 默认动作和处理机制

ACL 的应用模块

配置完ACL后，必须在具体的业务模块中应用ACL，才能使ACL正常下发和生效。

最基本的ACL应用方式，是在简化流策略或流策略中应用ACL，使设备能够基于全局、VLAN或接口下发ACL，实现对转发报文的过滤。此外，ACL还可以应用在Telnet、FTP、路由等模块。

如表2-9所示，ACL应用的业务模块，主要分为以下几类。

表 2-9 ACL 应用的业务模块

业务分类	应用场景	涉及业务模块
对转发的报文进行过滤	基于全局、接口和VLAN，对转发的报文进行过滤，从而使设备能够进一步对过滤出的报文进行丢弃、修改优先级、重定向等处理。 例如，使用ACL限制不同网段用户互访、禁止特定用户主机在特定时间内上网、利用ACL降低P2P下载、网络视频等消耗大量带宽的数据流的服务等级，在网络拥塞时优先丢弃这类流量，减少它们对其他重要流量的影响。	简化流策略/流策略
对上送CPU处理的报文进行过滤	对上送CPU的报文进行必要的限制，可以避免CPU处理过多的协议报文造成占用率过高、性能下降。 例如，当发现某用户向设备发送大量的ARP攻击报文，造成设备CPU繁忙，引发系统中断时，可以在本机防攻击策略的黑名单中应用ACL，将该用户加入黑名单，使CPU丢弃该用户发送的报文。	黑名单
登录控制	对设备的登录权限进行控制，允许合法用户登录，拒绝非法用户登录，从而有效防止未经授权用户的非法接入，保证网络安全性。 例如，一般情况下设备只允许管理员登录，非管理员用户不允许随意登录。这时就可以在Telnet中应用ACL，并在ACL中定义哪些主机可以登录，哪些主机不能。	Telnet、STelnet、FTP、SFTP、HTTP、SNMP
路由过滤	ACL可以应用在各种动态路由协议中，对路由协议发布、接收的路由信息以及组播组进行过滤。 例如，可以将ACL和路由策略配合使用过滤路由信息，禁止设备将某网段路由发给邻居路由器。	RIP、RIPng、组播协议

应用模块的 ACL 默认动作和处理机制

在各类业务模块中应用ACL时，ACL的默认动作各有不同，所以各业务模块对命中/未命中ACL规则报文的处理机制也各不相同。

例如，流策略中的ACL默认动作是permit，在流策略中应用ACL时，如果ACL中存在规则但报文未匹配上，该报文仍可以正常通过。而Telnet中的ACL默认动作是deny，在Telnet中应用ACL时，如果遇到此种情况，该报文会被拒绝通过。

此外，黑名单模块中的ACL处理机制与其他模块有所不同。在黑名单中应用ACL时，无论ACL规则配置成permit还是deny，只要报文命中了规则，该报文都会被系统丢弃。

各类业务模块中的ACL默认动作及ACL处理机制，如表2-10、表2-11、表2-12所示。

表 2-10 各业务模块的 ACL 默认动作及 ACL 处理机制

ACL默认动作及处理规则	Telnet	STelnet	HTTP	FTP	TFTP
ACL默认动作	deny	deny	deny	deny	deny
命中permit规则	permit（允许登录）	permit（允许登录）	permit（允许登录）	permit（允许登录）	permit（允许登录）
命中deny规则	deny（拒绝登录）	deny（拒绝登录）	deny（拒绝登录）	deny（拒绝登录）	deny（拒绝登录）
ACL中配置了规则，但未命中任何规则	deny（拒绝登录）	deny（拒绝登录）	deny（拒绝登录）	deny（拒绝登录）	deny（拒绝登录）
ACL中未配置规则	permit（允许登录）	permit（允许登录）	permit（允许登录）	permit（允许登录）	permit（允许登录）
ACL未创建	permit（允许登录）	permit（允许登录）	permit（允许登录）	permit（允许登录）	permit（允许登录）

表 2-11 各业务模块的 ACL 默认动作及 ACL 处理机制

ACL默认动作及处理规则	SFTP	SNMP	流策略	简化流策略	本机防攻击策略（黑名单）
ACL默认动作	deny	deny	permit	permit	permit

ACL默认动作及处理规则	SFTP	SNMP	流策略	简化流策略	本机防攻击策略（黑名单）
命中permit规则	permit（允许登录）	permit（允许登录）	• 流行为是permit时:permit（允许通过） • 流行为是deny时:deny（丢弃报文） • 流行为是其他动作时:permit（执行流策略动作）	permit（执行简化流策略动作）	deny(丢弃报文)
命中deny规则	deny（拒绝登录）	deny（拒绝登录）	deny(丢弃报文) **说明** 报文命中deny规则时，只有在流行为是流量统计、MAC地址不学习或流镜像的情况下，设备才会执行流行为动作，否则流行为动作不生效。	• 简化流策略动作为报文过滤（traffic-filter或traffic-secure）时:deny（丢弃报文） • 简化流策略动作为其他动作时:permit（执行简化流策略动作）	deny(丢弃报文)
ACL中配置了规则，但未命中任何规则	deny（拒绝登录）	deny（拒绝登录）	permit（功能不生效，按照原转发方式进行转发）	permit（功能不生效，按照原转发方式进行转发）	permit（功能不生效，正常上送报文）

ACL默认动作及处理规则	SFTP	SNMP	流策略	简化流策略	本机防攻击策略（黑名单）
ACL中未配置规则	permit（允许登录）	permit（允许登录）	permit（功能不生效，按照原转发方式进行转发）	permit（功能不生效，按照原转发方式进行转发）	permit（功能不生效，正常上送报文）
ACL未创建	permit（允许登录）	permit（允许登录）	permit（功能不生效，按照原转发方式进行转发）	permit（功能不生效，按照原转发方式进行转发）	permit（功能不生效，正常上送报文）

表 2-12 各业务模块的 ACL 默认动作及 ACL 处理机制

ACL默认动作及处理规则	Route Policy	Filter Policy	igmp-snooping ssm-policy	igmp-snooping group-policy
ACL默认动作	deny	deny	deny	deny
命中permit规则	• 匹配模式是permit时：permit(允许执行路由策略) • 匹配模式是deny时：deny(不允许执行路由策略)	permit（允许发布或接收该路由）	permit(允许加入SSM组播组范围)	permit(允许加入组播组)
命中deny规则	deny（功能不生效，不允许执行路由策略）	deny（不允许发布或接收该路由）	deny(禁止加入SSM组地址范围)	deny(禁止加入组播组)
ACL中配置了规则，但未命中任何规则	deny（功能不生效，不允许执行路由策略）	deny（不允许发布或接收该路由）	deny(禁止加入SSM组地址范围)	deny（禁止加入组播组）
ACL中未配置规则	permit（对经过的所有路由生效）	deny（不允许发布或接收路由）	deny（禁止加入SSM组地址范围，所有组都不在SSM组地址范围内）	deny（禁止加入组播组）

ACL默认动作及处理规则	Route Policy	Filter Policy	igmp-snooping ssm-policy	igmp-snooping group-policy
ACL未创建	deny（功能不生效，不允许执行路由策略）	permit（允许发布或接收路由）	deny(禁止加入SSM组地址范围，只有临时组地址范围232.0.0.0～232.255.255.255在SSM组地址范围内)	deny（禁止加入组播组）

2.3 ACL 配置注意事项

涉及网元

无需其他网元配合。

License 支持

本特性是交换机的基本特性，无需获得License许可即可应用此功能。

V200R021C00、V200R021C01 版本特性支持情况

S600-E系列交换机中所有款型均支持ACL。

说明

如需了解交换机软件配套详细信息，请点击**Info-Finder**。

特性依赖和限制

配置ACL规则时：

- 如果指定的*rule-id*已存在，且新规则与原规则存在冲突，则冲突的部分新规则代替原规则，相当于编辑一个已经存在的ACL的规则。
- 仅基本ACL与基本ACL6，以及高级ACL与高级ACL6，可以使用相同的ACL名称；其他类型ACL之间，不能使用相同的ACL名称。
- 不同的ACL匹配顺序，可能会造成不同的报文匹配结果，所以配置ACL时需注意ACL匹配顺序。创建ACL时，如果未指定**match-order**参数，则该ACL默认的规则匹配顺序为**config**。
- 当在规则中指定参数**time-range**引入生效时间段时，需保证交换机的系统时间与网络上其他设备的时间一致，否则可能造成ACL不生效。而且需保证*time-name*已存在，否则该规则无法与该时间段绑定。
- 配置的ACL6规则应用为硬件ACL时的约束请参见《S600-E V200R021C00, C01 配置指南-安全配置》ACL配置中的**2.7.7 配置高级ACL6**。
- MPLS L3VPN场景下，仅配置基本ACL或高级ACL就可以匹配报文的IPv4头部、IPv6头部或者四层头部的信息，其他款型需要配置用户自定义ACL才可以匹配。

应用ACL规则时：

- 在接口上应用ACL时，需注意ACL的应用方向。如果在接口的入方向上应用ACL，交换机会对从该接口进入的报文进行ACL匹配处理；如果在接口的出方向上应用ACL，交换机会对从该接口出去的报文进行ACL匹配处理。

删除ACL规则时：

规则即使被引用（简化流策略中引用ACL指定rule的情况除外），使用**undo rule**命令行也可以删除该规则。请谨慎操作，在删除前判断该规则是否已经被引用。

堆叠系统对ACL的支持情况与单机系统完全一致，在堆叠系统的主交换机上配置ACL，配置信息会同步到系统中的备交换机和从交换机。

2.4 ACL 配置任务概览

ACL的配置任务如表2-13所示。各配置任务之间，是并列关系，至少要选择其中的一种ACL进行配置。

表 2-13 ACL 配置任务概览

场景	描述	对应任务（按照顺序依次配置）
配置并应用基本ACL	基本ACL根据源IP地址、分片信息和生效时间段等信息来定义规则，对IPv4报文进行过滤。 如果只需要根据源IP地址对报文进行过滤，可以配置基本ACL。	1. 2.7.1 配置基本ACL 2. 2.8 应用ACL
配置并应用高级ACL	与基本ACL相比，高级ACL提供了更准确、丰富、灵活的规则定义方法。比如根据源IP地址、目的IP地址、IP协议类型、TCP源/目的端口、UDP源/目的端口号、分片信息和生效时间段等信息来定义规则，对IPv4报文进行过滤。	1. 2.7.2 配置高级ACL 2. 2.8 应用ACL
配置并应用二层ACL	二层ACL根据以太网帧头信息来定义规则，如源MAC（Media Access Control）地址、目的MAC地址、VLAN ID、二层协议类型等，对报文进行过滤。	1. 2.7.3 配置二层ACL 2. 2.8 应用ACL

场景	描述	对应任务（按照顺序依次配置）
配置并应用用户自定义ACL	用户自定义ACL根据报文头、偏移位置、字符串掩码和用户自定义字符串来定义规则，即以报文头为基准，指定从报文的第几个字节开始与字符串掩码进行“与”操作，并将提取出的字符串与用户自定义的字符串进行比较，对IPv4和IPv6报文进行过滤。 用户自定义ACL比基本ACL、高级ACL和二层ACL提供了更准确、丰富、灵活的规则定义方法。例如，当希望同时根据源IP地址、ARP报文类型对ARP报文进行过滤时，则可以配置用户自定义ACL。	1. **2.7.4 配置用户自定义ACL** 2. **2.8 应用ACL**
配置并应用用户ACL	用户ACL根据IPv4报文的源IP地址或源UCL（User Control List）组、目的IP地址或目的UCL组、IP协议类型、ICMP类型、TCP源端口/目的端口、UDP源端口/目的端口号、生效时间段等来定义规则，对IPv4报文进行过滤。 如果需要根据UCL组对报文进行过滤，可以配置用户ACL。	1. **2.7.5 配置用户ACL** 2. **2.8 应用ACL**
配置并应用基本ACL6	基本ACL6根据源IPv6地址、分片信息和生效时间段等信息来定义规则，对IPv6报文进行过滤。 如果只需要根据源IPv6地址对报文进行过滤，可以配置基本ACL6。	1. **2.7.6 配置基本ACL6** 2. **2.8 应用ACL**

场景	描述	对应任务（按照顺序依次配置）
配置并应用高级ACL6	高级ACL6根据源IPv6地址、目的IPv6地址、IPv6协议类型、TCP源/目的端口、UDP源/目的端口号、分片信息和生效时间段等信息来定义规则，对IPv6报文进行过滤。 高级ACL6比基本ACL6提供了更准确、丰富、灵活的规则定义方法。例如，希望同时根据源IPv6地址和目的IPv6地址对报文进行过滤时，则需要配置高级ACL6。	1. **2.7.7 配置高级ACL6** 2. **2.8 应用ACL**
配置并应用用户ACL6	用户ACL6根据IPv6报文的源IPv6地址或源UCL（User Control List）组、目的IPv6地址、IPv6协议类型、ICMPv6类型、TCP源端口/目的端口、UDP源端口/目的端口号、生效时间段等来定义规则，对IPv6报文进行过滤。 如果需要根据UCL组对报文进行过滤，可以配置用户ACL6。	1. **2.7.8 配置用户ACL6** 2. **2.8 应用ACL**

2.5 ACL 缺省配置

ACL的缺省配置如**表2-14**所示。

表 2-14 ACL 缺省配置

参数	缺省值
规则步长	ACL4规则默认步长为5，可以通过命令调整步长值。 ACL6规则默认步长为5，不能通过命令调整步长值。
匹配顺序	配置顺序

2.6 （可选）配置 ACL 的生效时间段

背景信息

缺省情况下，ACL一旦被应用到业务模块后是一直生效的。通过定义生效时间段，并将时间段与ACL规则关联，可以使ACL规则在某段时间范围内生效，从而达到使用基于时间的ACL来控制业务的目的。例如，在上班时间禁止员工访问互联网网站，避免影响工作；在网络流量高峰期，限制P2P/下载类业务的带宽，避免网络拥塞等。

在ACL规则中引用的生效时间段存在两种模式：

- 第一种模式——周期时间段：以星期为参数来定义时间范围，表示规则以一周为周期（如每周一的8至12点）循环生效。
- 第二种模式——绝对时间段：从某年某月某日的某一时间开始，到某年某月某日的某一时间结束，表示规则在这段时间范围内生效。

说明

为避免设备的系统时间与网络不同步造成ACL不生效，建议配置NTP（Network Time Protocol），实现系统时钟的自动同步，保证设备与网络中所有设备时钟的一致性。关于NTP的具体配置，请参见《S600-E V200R021C00, C01 配置指南-设备管理》NTP配置 中的“配置NTP基本功能”。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**time-range** *time-name* { *start-time* **to** *end-time* { *days* } &<1-7> | **from** *time1 date1* [**to** *time2 date2*] }，创建一个时间段。

缺省情况下，设备没有配置时间段。

可以使用同一名称（*time-name*）配置内容不同的多条时间段，配置的各周期时间段之间以及各绝对时间段之间的交集将成为最终生效的时间范围。

如果要删除时间段，可参见**删除生效时间段**。

----结束

后续处理

创建生效时间段后，还需创建ACL并配置与生效时间段关联的ACL规则。ACL的配置，请参见**2.7 配置ACL**。

配置小窍门

删除生效时间段

删除生效时间段前，需要先删除关联生效时间段的ACL规则或者整个ACL。

例如，在ACL 2001中配置了rule 5，该规则关联了时间段time1。

```
#
time-range time1 from 00:00 2014/1/1 to 23:59 2014/12/31
#
acl number 2001
 rule 5 permit time-range time1
#
```

如果需要删除时间段time1，则需先删除rule 5或者先删除ACL 2001：

- 先删除rule 5，再删除time1。

```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] undo rule 5
[HUAWEI-acl-basic-2001] quit
[HUAWEI] undo time-range time1
```

- 先删除ACL 2001，再删除time1。

```
<HUAWEI> system-view
[HUAWEI] undo acl 2001
[HUAWEI] undo time-range time1
```

2.7 配置 ACL

2.7.1 配置基本 ACL

前提条件

如果配置基于时间的ACL，则需创建生效时间段，并将其与ACL规则关联起来。具体操作请参见**2.6 （可选）配置ACL的生效时间段**。

背景信息

基本ACL根据源IP地址、分片信息和生效时间段等信息来定义规则，对IPv4报文进行过滤。

如果只需要根据源IP地址对报文进行过滤，可以配置基本ACL。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 创建基本ACL。可使用编号或者名称两种方式创建。

- 执行命令**acl** [**number**] *acl-number* [**match-order** { **auto** | **config** }]，使用编号（2000～2999）创建一个数字型的基本ACL，并进入基本ACL视图。
- 执行命令**acl name** *acl-name* { **basic** | *acl-number* } [**match-order** { **auto** | **config** }]，使用名称创建一个命名型的基本ACL，并进入基本ACL视图。

缺省情况下，未创建ACL。

如果创建ACL时未指定**match-order**参数，则该ACL默认的规则匹配顺序为**config**。关于ACL匹配顺序的详细介绍，请参见**2.2.3 ACL的匹配机制**。

创建ACL后，ACL的缺省步长为5。如果该值不能满足管理员部署ACL规则的需求，则可以对ACL步长值进行调整。关于步长的详细介绍，请参见**2.2.5 ACL的步长设定**；关于步长调整的具体操作，请参见**2.11.1 调整ACL规则的步长**。

步骤3 （可选）执行命令**description** *text*，配置ACL的描述信息。

缺省情况下，未配置ACL的描述信息。

配置ACL时，为ACL添加描述信息可以方便理解和记忆该ACL的功能或具体用途。

步骤4 执行命令**rule** [*rule-id*] { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **fragment** | **logging** | **time-range** *time-name*] *，配置基本ACL的规则。

以上步骤仅是一条permit/deny规则的配置步骤。实际配置ACL规则时，需根据具体的业务需求，决定配置多少条规则以及规则的先后匹配顺序。

关于生效时间段、源IP地址及其通配符掩码和IP分片信息的详细介绍，请参见**2.2.2 交换机支持的ACL及常用匹配项**。详细的规则配置示例，请参见**配置基本ACL规则**。

步骤5 （可选）执行命令**rule** *rule-id* **description** *description*，配置ACL规则的描述信息。

缺省情况下，各规则没有描述信息。

配置ACL规则时，为ACL规则添加描述信息，可以方便理解和记忆该ACL规则的功能或具体用途。

设备仅允许为已存在的规则添加描述信息，不允许先配置规则的描述信息再配置具体的规则内容。

----结束

后续任务

配置完ACL后，必须在具体的业务模块中应用ACL，才能使ACL正常下发和生效。具体支持的应用模块和配置请参见**2.8 应用ACL**。

配置示例

配置基本ACL规则

- **配置基于源IP地址（主机地址）过滤报文的规则**

  在ACL 2001中配置规则，允许源IP地址是192.168.1.3主机地址的报文通过。

  ```
  <HUAWEI> system-view
  [HUAWEI] acl 2001
  [HUAWEI-acl-basic-2001] rule permit source 192.168.1.3 0
  ```

- **配置基于源IP地址（网段地址）过滤报文的规则**

  在ACL 2001中配置规则，仅允许源IP地址是192.168.1.3主机地址的报文通过，拒绝源IP地址是192.168.1.0/24网段其他地址的报文通过，并配置ACL描述信息为Permit only 192.168.1.3 through。

  ```
  <HUAWEI> system-view
  [HUAWEI] acl 2001
  [HUAWEI-acl-basic-2001] rule permit source 192.168.1.3 0
  [HUAWEI-acl-basic-2001] rule deny source 192.168.1.0 0.0.0.255
  [HUAWEI-acl-basic-2001] description permit only 192.168.1.3 through
  ```

- **配置基于时间的ACL规则**

  创建时间段working-time（周一到周五每天8:00到18:00），并在名称为work-acl的ACL中配置规则，在working-time限定的时间范围内，拒绝源IP地址是192.168.1.0/24网段地址的报文通过。

  ```
  <HUAWEI> system-view
  [HUAWEI] time-range working-time 8:00 to 18:00 working-day
  [HUAWEI] acl name work-acl basic
  [HUAWEI-acl-basic-work-acl] rule deny source 192.168.1.0 0.0.0.255 time-range working-time
  ```

- **配置基于IP分片信息、源IP地址（网段地址）过滤报文的规则**

  在ACL 2001中配置规则，拒绝源IP地址是192.168.1.0/24网段地址的非首片分片报文通过。

```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] rule deny source 192.168.1.0 0.0.0.255 fragment
```

2.7.2 配置高级 ACL

前提条件

如果配置基于时间的ACL，则需创建生效时间段，并将其与ACL规则关联起来。具体操作请参见**2.6 （可选）配置ACL的生效时间段**。

背景信息

与基本ACL相比，高级ACL提供了更准确、丰富、灵活的规则定义方法。比如根据源IP地址、目的IP地址、IP协议类型、TCP源/目的端口、UDP源/目的端口号、分片信息和生效时间段等信息来定义规则，对IPv4报文进行过滤。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 创建高级ACL。可使用编号或者名称两种方式创建。

- 执行命令**acl** [**number**] *acl-number* [**match-order** { **auto** | **config** }]，使用编号（3000～3999）创建一个数字型的高级ACL，并进入高级ACL视图。
- 执行命令**acl name** *acl-name* { **advance** | *acl-number* } [**match-order** { **auto** | **config** }]，使用名称创建一个命名型的高级ACL，进入高级ACL视图。

缺省情况下，未创建ACL。

如果创建ACL时未指定**match-order**参数，则该ACL默认的规则匹配顺序为**config**。关于ACL匹配顺序的详细介绍，请参见**2.2.3 ACL的匹配机制**。

创建ACL后，ACL的缺省步长为5。如果该值不能满足管理员部署ACL规则的需求，则可以对ACL步长值进行调整。关于步长的详细介绍，请参见**2.2.5 ACL的步长设定**；关于步长调整的具体操作，请参见**2.11.1 调整ACL规则的步长**。

步骤3 （可选）执行命令**description** *text*，配置ACL的描述信息。

缺省情况下，未配置ACL的描述信息。

配置ACL时，为ACL添加描述信息可以方便理解和记忆该ACL的功能或具体用途。

步骤4 配置高级ACL规则。

根据IP承载的协议类型不同，在设备上配置不同的高级ACL规则。对于不同的协议类型，有不同的参数组合。

- 当参数protocol为ICMP时，高级ACL的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **icmp** } [**destination** { *destination-address destination-wildcard* | **any** } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **fragment** | **logging** | **icmp-type** { *icmp-name* | *icmp-type* [*icmp-code*] } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name*] *

- 当参数protocol为TCP时，高级ACL的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **tcp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port*

| **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name*] *

- 当参数protocol为UDP时，高级ACL的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **udp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name*] *

- 当参数protocol为GRE、IGMP、IP、IPINIP、OSPF时，高级ACL的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ip** | **ipinip** | **ospf** } [**destination** { *destination-address destination-wildcard* | **any** } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name*] *

以上步骤仅是一条permit/deny规则的配置步骤。实际配置ACL规则时，需根据具体的业务需求，决定配置多少条规则以及规则的先后匹配顺序。

关于生效时间段、IP承载的协议类型、源/目的IP地址及其通配符掩码、TCP/UDP端口号、TCP标志信息和IP分片信息的详细介绍，请参见**2.2.2 交换机支持的ACL及常用匹配项**。详细的规则配置示例，请参见**配置高级ACL规则**。

步骤5 （可选）执行命令**rule** *rule-id* **description** *description*，配置ACL规则的描述信息。

缺省情况下，各规则没有描述信息。

配置ACL规则时，为ACL规则添加描述信息，可以方便理解和记忆该ACL规则的功能或具体用途。

设备仅允许为已存在的规则添加描述信息，不允许先配置规则的描述信息再配置具体的规则内容。

----结束

后续任务

配置完ACL后，必须在具体的业务模块中应用ACL，才能使ACL正常下发和生效。具体支持的应用模块和配置请参见**2.8 应用ACL**。

配置示例

配置高级ACL规则

- **配置基于ICMP协议类型、源IP地址（主机地址）和目的IP地址（网段地址）过滤报文的规则**

  在ACL 3001中配置规则，允许源IP地址是192.168.1.3主机地址且目的IP地址是192.168.2.0/24网段地址的ICMP报文通过。

  ```
  <HUAWEI> system-view
  [HUAWEI] acl 3001
  [HUAWEI-acl-adv-3001] rule permit icmp source 192.168.1.3 0 destination 192.168.2.0 0.0.0.255
  ```

- **配置基于TCP协议类型、TCP目的端口号、源IP地址（主机地址）和目的IP地址（网段地址）过滤报文的规则**

在名称为deny-telnet的高级ACL中配置规则，拒绝IP地址是192.168.1.3的主机与192.168.2.0/24网段的主机建立Telnet连接。

```
<HUAWEI> system-view
[HUAWEI] acl name deny-telnet
[HUAWEI-acl-adv-deny-telnet] rule deny tcp destination-port eq telnet source 192.168.1.3 0 destination 192.168.2.0 0.0.0.255
```

在名称为no-web的高级ACL中配置规则，禁止192.168.1.3和192.168.1.4两台主机访问Web网页（HTTP协议用于网页浏览，对应TCP端口号是80），并配置ACL描述信息为Web access restrictions。

```
<HUAWEI> system-view
[HUAWEI] acl name no-web
[HUAWEI-acl-adv-no-web] description Web access restrictions
[HUAWEI-acl-adv-no-web] rule deny tcp destination-port eq 80 source 192.168.1.3 0
[HUAWEI-acl-adv-no-web] rule deny tcp destination-port eq 80 source 192.168.1.4 0
```

- **配置基于TCP协议类型、源IP地址（网段地址）和TCP标志信息过滤报文的规则**

  在ACL 3002中配置规则，拒绝192.168.2.0/24网段的主机主动发起的TCP握手报文通过，允许该网段主机被动响应TCP握手的报文通过，实现192.168.2.0/24网段地址的单向访问控制。同时，配置ACL规则描述信息分别为Allow the ACK TCP packets through、Allow the RST TCP packets through和Do not Allow the other TCP packet through。

  完成以上配置，必须先配置两条permit规则，允许192.168.2.0/24网段的ACK=1或RST=1的报文通过，再配置一条deny规则，拒绝该网段的其他TCP报文通过。

```
<HUAWEI> system-view
[HUAWEI] acl 3002
[HUAWEI-acl-adv-3002] rule permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack
[HUAWEI-acl-adv-3002] display this  //如果配置规则时未指定规则编号，则可以通过此步骤查看到系统为该规则分配的编号，然后根据该编号，为该规则配置描述信息。
#
acl number 3002
 rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack          //系统分配的规则编号是5
#
return
[HUAWEI-acl-adv-3002] rule 5 description Allow the ACK TCP packets through
[HUAWEI-acl-adv-3002] rule permit tcp source 192.168.2.0 0.0.0.255 tcp-flag rst
[HUAWEI-acl-adv-3002] display this
#
acl number 3002
 rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack
 rule 5 description Allow the ACK TCP packets through
 rule 10 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag rst       //系统分配的规则编号是10
#
return
[HUAWEI-acl-adv-3002] rule 10 description Allow the RST TCP packets through
[HUAWEI-acl-adv-3002] rule deny tcp source 192.168.2.0 0.0.0.255
[HUAWEI-acl-adv-3002] display this
#
acl number 3002
 rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack
 rule 5 description Allow the ACK TCP packets through
 rule 10 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag rst
 rule 10 description Allow the RST TCP packets through
 rule 15 deny tcp source 192.168.2.0 0.0.0.255       //系统分配的规则编号是15
#
return
[HUAWEI-acl-adv-3002] rule 15 description Do not Allow the other TCP packet through
```

  也可以通过配置established参数，允许192.168.2.0/24网段的ACK=1或RST=1的报文通过，再配置一条deny规则，拒绝该网段的其他TCP报文通过。

```
<HUAWEI> system-view
[HUAWEI] acl 3002
[HUAWEI-acl-adv-3002] rule permit tcp source 192.168.2.0 0.0.0.255 tcp-flag established
[HUAWEI-acl-adv-3002] rule 5 description Allow the Established TCP packets through
[HUAWEI-acl-adv-3002] rule deny tcp source 192.168.2.0 0.0.0.255
[HUAWEI-acl-adv-3002] rule 10 description Do not Allow the other TCP packet through
```

```
[HUAWEI-acl-adv-3002] display this
#
acl number 3002
 rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag
established
 rule 5 description Allow the Established TCP packets
through
 rule 10 deny tcp source 192.168.2.0
0.0.0.255
 rule 10 description Do not Allow the other TCP packet
through
#
return
```

- **配置基于时间的ACL规则**

  请参见“配置基本ACL”中的**配置基于时间的ACL规则**，不再赘述。

- **配置基于IP分片信息、源IP地址（网段地址）过滤报文的规则**

  请参见“配置基本ACL”中的**配置基于IP分片信息、源IP地址（网段地址）过滤报文的规则**，不再赘述。

2.7.3 配置二层 ACL

前提条件

如果配置基于时间的ACL，则需创建生效时间段，并将其与ACL规则关联起来。具体操作请参见**2.6 （可选）配置ACL的生效时间段**。

背景信息

二层ACL根据以太网帧头信息来定义规则，如源MAC（Media Access Control）地址、目的MAC地址、VLAN ID、二层协议类型等，对报文进行过滤。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 创建二层ACL。可使用编号或者名称两种方式创建。

- 执行命令**acl** [**number**] *acl-number* [**match-order** { **auto** | **config** }]，使用编号（4000～4999）创建一个数字型的二层ACL，并进入二层ACL视图。
- 执行命令**acl name** *acl-name* { **link** | *acl-number* } [**match-order** { **auto** | **config** }]，使用名称创建一个命名型的二层ACL，进入二层ACL视图。

缺省情况下，未创建ACL。

如果创建ACL时未指定**match-order**参数，则该ACL默认的规则匹配顺序为**config**。关于ACL匹配顺序的详细介绍，请参见**2.2.3 ACL的匹配机制**。

创建ACL后，ACL的缺省步长为5。如果该值不能满足管理员部署ACL规则的需求，则可以对ACL步长值进行调整。关于步长的详细介绍，请参见**2.2.5 ACL的步长设定**；关于步长调整的具体操作，请参见**2.11.1 调整ACL规则的步长**。

步骤3 （可选）执行命令**description** *text*，配置ACL的描述信息。

缺省情况下，未配置ACL的描述信息。

配置ACL时，为ACL添加描述信息可以方便理解和记忆该ACL的功能或具体用途。

步骤4 执行命令**rule** [*rule-id*] { **permit** | **deny** } [[**ether-ii** | **802.3** | **snap**] | **l2-protocol** *type-value* [*type-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **source-mac** *source-mac-address* [*source-mac-mask*] | **vlan-id** *vlan-id* [*vlan-id-mask*] | **8021p** *802.1p-value* | **time-range** *time-name*] *，配置二层ACL的规则。

以上步骤仅是一条permit/deny规则的配置步骤。实际配置ACL规则时，需根据具体的业务需求，决定配置多少条规则以及规则的先后匹配顺序。

关于生效时间段、源/目的MAC地址及其通配符掩码、VLAN编号及其掩码的详细介绍，请参见**2.2.2 交换机支持的ACL及常用匹配项**。详细的规则配置示例，请参见**配置二层ACL规则**。

步骤5 （可选）执行命令**rule** *rule-id* **description** *description*，配置ACL规则的描述信息。

缺省情况下，各规则没有描述信息。

配置ACL规则时，为ACL规则添加描述信息，可以方便理解和记忆该ACL规则的功能或具体用途。

设备仅允许为已存在的规则添加描述信息，不允许先配置规则的描述信息再配置具体的规则内容。

----结束

后续任务

配置完ACL后，必须在具体的业务模块中应用ACL，才能使ACL正常下发和生效。具体支持的应用模块和配置请参见**2.8 应用ACL**。

配置示例

配置二层ACL规则

- **配置基于源MAC地址（单个MAC地址）、目的MAC地址（单个MAC地址）和二层协议类型过滤报文的规则**

  在ACL 4001中配置规则，允许目的MAC地址是0000-0000-0001、源MAC地址是0000-0000-0002的ARP报文（二层协议类型值为0x0806）通过。

  ```
  <HUAWEI> system-view
  [HUAWEI] acl 4001
  [HUAWEI-acl-L2-4001] rule permit destination-mac 0000-0000-0001 source-mac 0000-0000-0002 l2-protocol 0x0806
  ```

  在ACL 4001中配置规则，拒绝PPPoE报文（二层协议类型值为0x8863）通过。

  ```
  <HUAWEI> system-view
  [HUAWEI] acl 4001
  [HUAWEI-acl-L2-4001] rule deny l2-protocol 0x8863
  ```

- **配置基于源MAC地址（MAC地址段）和VLAN过滤报文的规则**

  在名称为deny-vlan10-mac的二层ACL中配置规则，拒绝来自VLAN10且源MAC地址在00e0-fc01-0000～00e0-fc01-ffff范围内的报文通过。

  ```
  <HUAWEI> system-view
  [HUAWEI] acl name deny-vlan10-mac link
  [HUAWEI-acl-L2-deny-vlan10-mac] rule deny vlan-id 10 source-mac 00e0-fc01-0000 ffff-ffff-0000
  ```

- **配置基于时间的ACL规则**

  请参见“配置基本ACL”中的**配置基于时间的ACL规则**，不再赘述。

2.7.4 配置用户自定义 ACL

前提条件

如果配置基于时间的ACL，则需创建生效时间段，并将其与ACL规则关联起来。具体操作请参见**2.6 （可选）配置ACL的生效时间段**。

背景信息

用户自定义ACL根据报文头、偏移位置、字符串掩码和用户自定义字符串来定义规则，即以报文头为基准，指定从报文的第几个字节开始与字符串掩码进行“与”操作，并将提取出的字符串与用户自定义的字符串进行比较，对IPv4和IPv6报文进行过滤。

用户自定义ACL比基本ACL、高级ACL和二层ACL提供了更准确、丰富、灵活的规则定义方法。例如，当希望同时根据源IP地址、ARP报文类型对ARP报文进行过滤时，则可以配置用户自定义ACL。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 创建用户自定义ACL。可使用编号或者名称两种方式创建。

- 执行命令**acl** [**number**] *acl-number* [**match-order** { **auto** | **config** }]，使用编号（5000～5999）创建一个数字型的用户自定义ACL，并进入用户自定义ACL视图。
- 执行命令**acl name** *acl-name* { **user** | *acl-number* } [**match-order** { **auto** | **config** }]，使用名称创建一个命名型的用户自定义ACL，进入用户自定义ACL视图。

缺省情况下，未创建ACL。

如果创建ACL时未指定**match-order**参数，则该ACL默认的规则匹配顺序为**config**。关于ACL匹配顺序的详细介绍，请参见**2.2.3 ACL的匹配机制**。

创建ACL后，ACL的缺省步长为5。如果该值不能满足管理员部署ACL规则的需求，则可以对ACL步长值进行调整。关于步长的详细介绍，请参见**2.2.5 ACL的步长设定**；关于步长调整的具体操作，请参见**2.11.1 调整ACL规则的步长**。

步骤3 （可选）执行命令**description** *text*，配置ACL的描述信息。

缺省情况下，未配置ACL的描述信息。

配置ACL时，为ACL添加描述信息可以方便理解和记忆该ACL的功能或具体用途。

步骤4 执行命令**rule** [*rule-id*] { **deny** | **permit** } [[**l2-head** | **ipv4-head** | **l4-head**] { *rule-string rule-mask offset* } | **time-range** *time-name*] *，配置用户自定义ACL规则。

以上步骤仅是一条permit/deny规则的配置步骤。实际配置ACL规则时，需根据具体的业务需求，决定配置多少条规则以及规则的先后匹配顺序。

详细的规则配置示例，请参见**配置用户自定义ACL规则**。

步骤5 （可选）执行命令**rule** *rule-id* **description** *description*，配置ACL规则的描述信息。

缺省情况下，各规则没有描述信息。

配置ACL规则时，为ACL规则添加描述信息，可以方便理解和记忆该ACL规则的功能或具体用途。

设备仅允许为已存在的规则添加描述信息，不允许先配置规则的描述信息再配置具体的规则内容。

----结束

后续任务

配置完ACL后，必须在具体的业务模块中应用ACL，才能使ACL正常下发和生效。具体支持的应用模块和配置请参见**2.8 应用ACL**。

配置示例

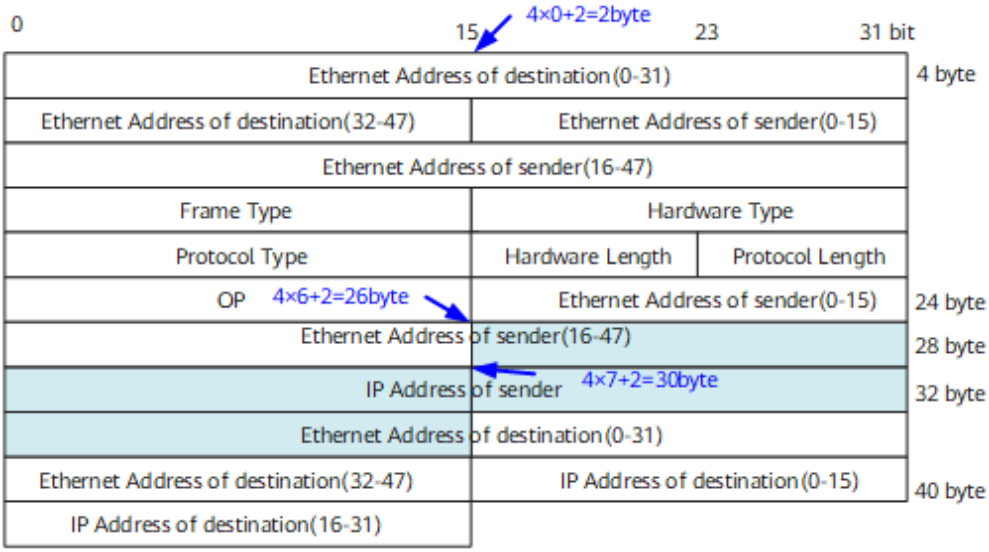
配置用户自定义ACL规则

- **配置基于报文的二层头、偏移位置、字符串掩码和用户自定义字符串过滤报文的规则**

  在ACL 5001中配置规则，拒绝源IP地址为192.168.0.2的ARP报文通过。

  以下规则中的0x00000806是ARP帧类型，0x0000ffff是字符串掩码，10是设备内部处理不含VLAN信息的ARP报文中的协议类型字段的偏移量，c0a80002是192.168.0.2的十六进制形式，26和30分别是设备内部处理不含VLAN信息的ARP报文中源IP地址字段高两个字节和低两个字节的偏移量（ARP报文的源IP地址字段从二层头第28个字节开始占4个字节，受到用户自定义ACL规定二层头偏移位置只能是“4n+2”（n是整数）的限制，因此针对源IP地址，需要拆分成两段进行匹配，即偏移量为4×6+2=26的位置开始往后匹配4个字节的低两个字节以及偏移量为4×7+2=30的位置开始往后匹配4个字节的高两个字节）。如果要对携带VLAN信息的ARP报文进行过滤，则要将以下规则中的三个偏移量值再分别加上4。

  图 2-4 ARP 报文源 IP 地址字段在二层头中的偏移量示意图



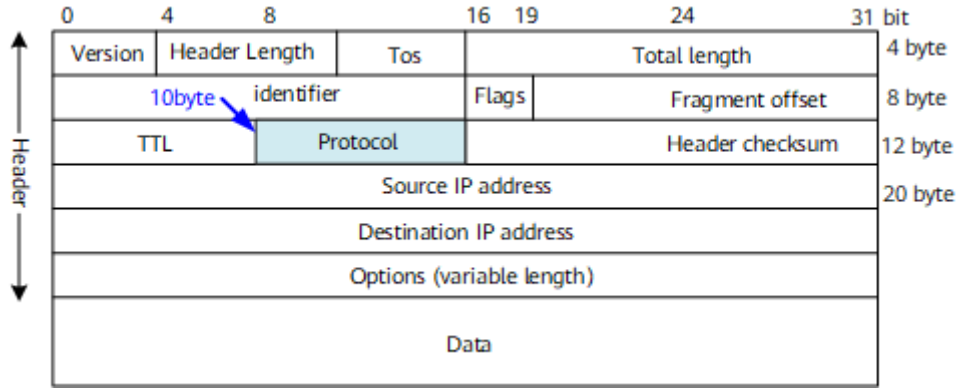

```
<HUAWEI> system-view
[HUAWEI] acl 5001
[HUAWEI-acl-user-5001] rule deny l2-head 0x00000806 0x0000ffff 10
```

在名称为deny-tcp的用户自定义ACL中配置规则，拒绝所有TCP报文通过。

以下规则中的0x00060000是TCP协议号，8是设备内部处理IP报文中协议字段的偏移量（由于IP报文中的协议字段从IPv4头第10个字节开始占1个字节，并且受到用户自定义ACL规定IPv4头偏移位置只能是“4n”（n是整数）的限制，因此针对协议字段，需要从IPv4头偏移量为8的位置开始往后匹配4个字节的第二个高位字节）。

```
<HUAWEI> system-view
[HUAWEI] acl name deny-tcp user
[HUAWEI-acl-user-deny-tcp] rule 5 deny ipv4-head 0x00060000 0x00ff0000 8
```

图 2-5 TCP 协议字段在 IPv4 头中的偏移量示意图



- **配置基于时间的ACL规则**

  请参见“配置基本ACL”中的**配置基于时间的ACL规则**，不再赘述。

2.7.5 配置用户 ACL

前提条件

- 通过命令**authentication unified-mode**将NAC配置模式切换成统一模式，并重启设备使该模式功能生效。
- 通过命令**ucl-group**创建标记用户类别的UCL组。
- 如果配置基于时间的ACL，则需创建生效时间段，并将其与ACL规则关联起来。具体操作请参见**2.6 （可选）配置ACL的生效时间段**。

背景信息

用户ACL根据IPv4报文的源IP地址或源UCL（User Control List）组、目的IP地址或目的UCL组、IP协议类型、ICMP类型、TCP源端口/目的端口、UDP源端口/目的端口号、生效时间段等来定义规则，对IPv4报文进行过滤。

如果需要根据UCL组对报文进行过滤，可以配置用户ACL。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 创建用户ACL。可使用编号或者名称两种方式创建。

- 执行命令**acl** [**number**] *acl-number* [**match-order** { **auto** | **config** }]，使用编号（6000～9999）创建一个数字型的用户ACL，并进入用户ACL视图。
- 执行命令**acl name** *acl-name* { **ucl** | *acl-number* } [**match-order** { **auto** | **config** }]，使用名称创建一个命名型的用户ACL，并进入用户ACL视图。

缺省情况下，未创建ACL。

如果创建ACL时未指定**match-order**参数，则该ACL默认的规则匹配顺序为**config**。关于ACL匹配顺序的详细介绍，请参见**2.2.3 ACL的匹配机制**。

创建ACL后，ACL的缺省步长为5。如果该值不能满足管理员部署ACL规则的需求，则可以对ACL步长值进行调整。关于步长的详细介绍，请参见**2.2.5 ACL的步长设定**；关于步长调整的具体操作，请参见**2.11.1 调整ACL规则的步长**。

步骤3 （可选）执行命令**description** *text*，配置ACL的描述信息。

缺省情况下，未配置ACL的描述信息。

配置ACL时，为ACL添加描述信息可以方便理解和记忆该ACL的功能或具体用途。

步骤4 配置用户ACL规则。

根据IP承载的协议类型不同，在设备上配置不同的用户ACL规则。对于不同的协议类型，有不同的参数组合。

- 当参数protocol为ICMP时，用户ACL的命令格式为：

  rule [*rule-id*] { **permit** | **deny** } { **icmp** | *protocol-number* } [**source** { { *source-address source-wildcard* | **any** } | { **ucl-group** { **name** *source-ucl-group-name* | *source-ucl-group-index* } } } * | **destination** { *destination-address destination-wildcard* | **any** } | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-name* } | **time-range** *time-name*] *
- 当参数protocol为TCP时，用户ACL的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **tcp** } [**source** { { *source-address source-wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { *destination-address destination-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name*] *
- 当参数protocol为UDP时，用户ACL的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **udp** } [**source** { { *source-address source-wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { *destination-address destination-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name*] *
- 当参数protocol为GRE、IGMP、IP、IPINIP、OSPF时，用户ACL的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ip** | **ipinip** | **ospf** } [**source** { { *source-address source-wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { *destination-address destination-wildcard* | **any** } | **time-range** *time-name*] *

以上步骤仅是一条permit/deny规则的配置步骤。实际配置ACL规则时，需根据具体的业务需求，决定配置多少条规则以及规则的先后匹配顺序。

详细的规则配置示例，请参见**配置用户ACL规则**。

步骤5 （可选）执行命令**rule** *rule-id* **description** *description*，配置ACL规则的描述信息。

缺省情况下，各规则没有描述信息。

配置ACL规则时，为ACL规则添加描述信息，可以方便理解和记忆该ACL规则的功能或具体用途。

设备仅允许为已存在的规则添加描述信息，不允许先配置规则的描述信息再配置具体的规则内容。

----结束

后续任务

配置完ACL后，必须在具体的业务模块中应用ACL，才能使ACL正常下发和生效。具体支持的应用模块和配置请参见**2.8 应用ACL**。

配置示例

配置用户ACL规则

- **配置基于源UCL组、目的IP地址过滤报文的ACL规则**

  在ACL 6000中配置规则，拒绝从源UCL组group1的主机向192.168.1.0/24网段的主机发送的所有IP报文通过。

```
<HUAWEI> system-view
[HUAWEI] ucl-group 1 name group1
[HUAWEI] acl 6000
[HUAWEI-acl-ucl-6000] rule deny ip source ucl-group name group1 destination 192.168.1.0 0.0.0.255
```

- **配置基于时间的ACL规则**

  请参见“配置基本ACL”中的**配置基于时间的ACL规则**，不再赘述。

2.7.6 配置基本 ACL6

前提条件

如果配置基于时间的ACL6，则需创建生效时间段，并将其与ACL6规则关联起来。具体操作请参见**2.6 （可选）配置ACL的生效时间段**。

背景信息

基本ACL6根据源IPv6地址、分片信息和生效时间段等信息来定义规则，对IPv6报文进行过滤。

如果只需要根据源IPv6地址对报文进行过滤，可以配置基本ACL6。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 创建基本ACL6。可使用编号或者名称两种方式创建。

- 执行命令**acl ipv6** [**number**] *acl6-number* [**match-order** { **auto** | **config** }]，使用编号（2000～2999）创建一个数字型的基本ACL6，并进入基本ACL6视图。
- 执行命令**acl ipv6 name** *acl6-name* { **basic** | *acl6-number* } [**match-order** { **auto** | **config** }]，使用名称创建一个命名型的基本ACL6，并进入基本ACL6视图。

缺省情况下，未创建ACL6。

如果创建ACL6时未指定**match-order**参数，则该ACL6默认的规则匹配顺序为**config**。ACL6的规则匹配顺序同ACL匹配顺序，详细介绍请参见**2.2.3 ACL的匹配机制**。

步骤3 （可选）执行命令**description** *text*，配置ACL6的描述信息。

缺省情况下，未配置ACL6的描述信息。

配置ACL6时，为ACL6添加描述信息可以方便理解和记忆该ACL6的功能或具体用途。

步骤4 执行命令**rule** [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | **time-range** *time-name*] *，配置基本ACL6规则。

以上步骤仅是一条permit/deny规则的配置步骤。实际配置ACL规则时，需根据具体的业务需求，决定配置多少条规则以及规则的先后匹配顺序。

详细的规则配置示例，请参见**配置基本ACL6规则**。

步骤5 （可选）执行命令**rule** *rule-id* **description** *description*，配置ACL规则的描述信息。

缺省情况下，各规则没有描述信息。

配置ACL规则时，为ACL规则添加描述信息，可以方便理解和记忆该ACL规则的功能或具体用途。

设备仅允许为已存在的规则添加描述信息，不允许先配置规则的描述信息再配置具体的规则内容。

----结束

后续任务

配置完ACL后，必须在具体的业务模块中应用ACL，才能使ACL正常下发和生效。具体支持的应用模块和配置请参见**2.8 应用ACL**。

配置示例

配置基本ACL6规则

- **配置基于源IPv6地址（主机地址）过滤报文的规则**

  在ACL6 2001中配置规则，允许源IPv6地址是fc00:1::1/128主机地址的报文通过。

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 2001
[HUAWEI-acl6-basic-2001] rule permit source fc00:1::1 128
```

- **配置基于源IPv6地址（网段地址）过滤报文的规则**

  在ACL6 2001中配置规则，仅允许源IPv6地址是fc00:1::1/128主机地址的报文通过，拒绝源IPv6地址是fc00:1::/64网段其他地址的报文通过。

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 2001
```



```
[HUAWEI-acl6-basic-2001] rule permit source fc00:1::1 128
[HUAWEI-acl6-basic-2001] rule deny source fc00:1:: 64
```

- **配置基于时间的ACL6规则**

  请参见“配置基本ACL”中的**配置基于时间的ACL规则**，不再赘述。

- **配置基于IP分片信息、源IP地址（网段地址）过滤报文的规则**

  请参见“配置基本ACL”中的**配置基于IP分片信息、源IP地址（网段地址）过滤报文的规则**，不再赘述。

2.7.7 配置高级 ACL6

前提条件

如果配置基于时间的ACL6，则需创建生效时间段，并将其与ACL6规则关联起来。具体操作请参见**2.6 （可选）配置ACL的生效时间段**。

背景信息

高级ACL6根据源IPv6地址、目的IPv6地址、IPv6协议类型、TCP源/目的端口、UDP源/目的端口号、分片信息和生效时间段等信息来定义规则，对IPv6报文进行过滤。

高级ACL6比基本ACL6提供了更准确、丰富、灵活的规则定义方法。例如，希望同时根据源IPv6地址和目的IPv6地址对报文进行过滤时，则需要配置高级ACL6。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 创建高级ACL。可使用编号或者名称两种方式创建。

- 执行命令**acl ipv6** [**number**] *acl6-number* [**match-order** { **auto** | **config** }]，使用编号（3000～3999）创建一个数字型的高级ACL6，并进入高级ACL6视图。
- 执行命令**acl ipv6 name** *acl6-name* { **advance** | *acl6-number* } [**match-order** { **auto** | **config** }]，使用名称创建一个命名型的高级ACL6，进入高级ACL6视图。

缺省情况下，未创建ACL6。

如果创建ACL6时未指定**match-order**参数，则该ACL6默认的规则匹配顺序为**config**。ACL6的规则匹配顺序同ACL匹配顺序，详细介绍请参见**2.2.3 ACL的匹配机制**。

步骤3 （可选）执行命令**description** *text*，配置ACL6的描述信息。

缺省情况下，未配置ACL6的描述信息。

配置ACL6时，为ACL6添加描述信息可以方便理解和记忆该ACL6的功能或具体用途。

步骤4 配置高级ACL6规则。

根据IP承载的协议类型不同，在设备上配置不同的高级ACL6规则。对于不同的协议类型，有不同的参数组合。

- 当参数protocol为TCP时，高级ACL6的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { **tcp** | *protocol-number* } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-*

length | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **fragment** | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name*] *

- 当参数protocol为UDP时，高级ACL6的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { **udp** | *protocol-number* } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **fragment** | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name*] *

- 当参数protocol为ICMPv6时，高级ACL6的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { **icmpv6** | *protocol-number* } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **fragment** | **icmp6-type** { *icmp6-name* | *icmp6-type* [*icmp6-code*] } | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | **time-range** *time-name*] *

- 当参数protocol为其他协议时，高级ACL6的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **ipv6** | **ospf** } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **fragment** | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | **time-range** *time-name*] *

表 2-15 配置的 ACL 规则应用为硬件 ACL 时，各协议的参数支持情况

参数	TCP	UDP	ICMPv6	其他协议
destination	支持	支持	支持	支持
source	支持	支持	支持	支持
destination-port	支持	支持	不支持	不支持
source-port	支持	支持	不支持	不支持
icmp6-type	不涉及	不涉及	支持	不涉及

参数	TCP	UDP	ICMPv6	其他协议
precedence	不支持	不支持	不支持	支持
tos	不支持	不支持	不支持	支持
dscp	不支持	不支持	不支持	支持
tcp-flag	不支持	不支持	不支持	不支持
routing	不支持	不支持	不支持	不支持
fragment | **first-fragment**	不支持	不支持	不支持	不支持
time-range	支持	支持	支持	支持
logging	支持	支持	支持	支持
vpn-instance *vpn-instance-name* | **public**	不支持	不支持	不支持	不支持

以上步骤仅是一条permit/deny规则的配置步骤。实际配置ACL规则时，需根据具体的业务需求，决定配置多少条规则以及规则的先后匹配顺序。

详细的规则配置示例，请参见**配置高级ACL6规则**。

步骤5 （可选）执行命令**rule** *rule-id* **description** *description*，配置ACL规则的描述信息。

缺省情况下，各规则没有描述信息。

配置ACL规则时，为ACL规则添加描述信息，可以方便理解和记忆该ACL规则的功能或具体用途。

设备仅允许为已存在的规则添加描述信息，不允许先配置规则的描述信息再配置具体的规则内容。

----结束

后续任务

配置完ACL后，必须在具体的业务模块中应用ACL，才能使ACL正常下发和生效。具体支持的应用模块和配置请参见**2.8 应用ACL**。

配置示例

配置高级ACL6规则

- **配置基于ICMPv6协议类型、源IPv6地址（主机地址）和目的IPv6地址（网段地址）过滤报文的规则**

  在ACL6 3001中配置规则，允许源IPv6地址是fc00:1::1主机地址且目的IPv6地址是fc00:2::/64网段的ICMPv6报文通过。

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 3001
[HUAWEI-acl6-adv-3001] rule permit icmpv6 source fc00:1::1 128 destination fc00:2:: 64
```

- **配置基于TCP协议类型、TCP目的端口号、源IPv6地址（主机地址）和目的IPv6地址（网段地址）过滤报文的规则**

  在名称为deny-telnet的高级ACL6中配置规则，拒绝源IPv6地址是fc00:1::3的主机与目的IP地址是fc00:2::/64网段的主机建立Telnet连接。

  ```
  <HUAWEI> system-view
  [HUAWEI] acl ipv6 name deny-telnet
  [HUAWEI-acl6-adv-deny-telnet] rule deny tcp destination-port eq telnet source fc00:1::3 128 destination fc00:2:: 64
  ```

  在名称为no-web的高级ACL6中配置规则，禁止fc00:1::3和fc00:1::4两台主机访问Web网页（HTTP协议用于网页浏览，对应TCP端口号是80）。

  ```
  <HUAWEI> system-view
  [HUAWEI] acl ipv6 name no-web
  [HUAWEI-acl6-adv-no-web] rule deny tcp destination-port eq 80 source fc00:1::3 128
  [HUAWEI-acl6-adv-no-web] rule deny tcp destination-port eq 80 source fc00:1::4 128
  ```

- **配置基于时间的ACL6规则**

  请参见“配置基本ACL”中的**配置基于时间的ACL规则**，不再赘述。

- **配置基于IP分片信息、源IP地址（网段地址）过滤报文的规则**

  请参见“配置基本ACL”中的**配置基于IP分片信息、源IP地址（网段地址）过滤报文的规则**，不再赘述。

2.7.8 配置用户 ACL6

前提条件

- 通过命令**authentication unified-mode**将NAC配置模式切换成统一模式，需重启设备后生效。缺省情况下，NAC配置模式为统一模式。
- 通过命令**assign resource-template acl-mode**将ACL规格的资源分配模式配置为NAC模式，需重启设备后生效。缺省情况下，ACL规格的资源分配模式为Normal模式。
- 通过命令**ucl-group**创建标记用户类别的UCL组。
- 如果配置基于时间的ACL6，则需创建生效时间段，并将其与ACL6规则关联起来。具体操作请参见**2.6 （可选）配置ACL的生效时间段**。

背景信息

用户ACL6根据IPv6报文的源IPv6地址或源UCL（User Control List）组、目的IPv6地址、IPv6协议类型、ICMPv6类型、TCP源端口/目的端口、UDP源端口/目的端口号、生效时间段等来定义规则，对IPv6报文进行过滤。

如果需要根据UCL组对报文进行过滤，可以配置用户ACL6。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 创建用户ACL6。可使用编号或者名称两种方式创建。

- 执行命令**acl ipv6** [**number**] *acl6-number* [**match-order** { **auto** | **config** }]，使用编号（6000～6999）创建一个数字型的用户ACL6，并进入用户ACL6视图。

- 执行命令**acl ipv6 name** *acl6-name* { **ucl** | *acl6-number* } [**match-order** { **auto** | **config** }]，使用名称创建一个命名型的用户ACL6，进入用户ACL6视图。

缺省情况下，未创建ACL6。

如果创建ACL6时未指定**match-order**参数，则该ACL6默认的规则匹配顺序为**config**。ACL6的规则匹配顺序同ACL匹配顺序，详细介绍请参见**2.2.3 ACL的匹配机制**。

步骤3 （可选）执行命令**description** *text*，配置ACL6的描述信息。

缺省情况下，未配置ACL6的描述信息。

配置ACL6时，为ACL6添加描述信息可以方便理解和记忆该ACL6的功能或具体用途。

步骤4 配置用户ACL6规则。

根据IPv6承载的协议类型不同，在设备上配置不同的用户ACL6规则。对于不同的协议类型，有不同的参数组合。

- 当参数protocol为ICMPv6时，用户ACL6的命令格式为：

  rule [*rule-id*] { **permit** | **deny** } { **icmpv6** | *protocol-number* } [**source** { { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | { **ucl-group** { **name** *source-ucl-group-name* | *source-ucl-group-index* } } } * | **destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | **icmp6-type** { *icmp6-type* [*icmp6-code*] | *icmp6-name* } | **time-range** *time-name*] *

- 当参数protocol为TCP时，用户ACL6的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { **tcp** | *protocol-number* } [**source** { { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name*] *

- 当参数protocol为UDP时，用户ACL6的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { **udp** | *protocol-number* } [**source** { { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name*] *

- 当参数protocol为GRE、IPv6、OSPF时，用户ACL6的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { **gre** | **ipv6** | **ospf** | *protocol-number* } [**source** { { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-*

length | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | **time-range** *time-name*] *

以上步骤仅是一条permit/deny规则的配置步骤。实际配置ACL规则时，需根据具体的业务需求，决定配置多少条规则以及规则的先后匹配顺序。

详细的规则配置示例，请参见**配置用户ACL6规则**。

步骤5 （可选）执行命令**rule** *rule-id* **description** *description*，配置ACL规则的描述信息。

缺省情况下，各规则没有描述信息。

配置ACL规则时，为ACL规则添加描述信息，可以方便理解和记忆该ACL规则的功能或具体用途。

设备仅允许为已存在的规则添加描述信息，不允许先配置规则的描述信息再配置具体的规则内容。

----结束

后续任务

配置完ACL后，必须在具体的业务模块中应用ACL，才能使ACL正常下发和生效。具体支持的应用模块和配置请参见**2.8 应用ACL**。

配置示例

配置用户ACL6规则

- **配置基于源UCL组、目的IPv6地址过滤报文的ACL6规则**

  在ACL6 6000中配置规则，拒绝从源UCL组group1的主机向fc00:1::/64网段的主机发送的所有IPv6报文通过。

```
<HUAWEI> system-view
[HUAWEI] ucl-group 1 name group1
[HUAWEI] acl ipv6 6000
[HUAWEI-acl6-ucl-6000] rule deny ipv6 source ucl-group name group1 destination fc00:1:: 64
```

- **配置基于时间的ACL规则**

  请参见“配置基本ACL”中的**配置基于时间的ACL规则**，不再赘述。

2.7.9 检查 ACL 配置结果

操作步骤

- 执行命令**display acl** { *acl-number* | **name** *acl-name* | **all** }，查看ACL的配置信息。
- 执行命令**display acl ipv6** { *acl6-number* | **name** *acl6-name* | **all** }，查看ACL6的配置信息。
- 执行命令**display time-range** { **all** | *time-name* }，查看时间段信息。

----结束

2.8 应用 ACL

背景信息

配置完ACL后，必须在具体的业务模块中应用ACL，才能使ACL正常下发和生效。

最基本的ACL应用方式，是在简化流策略或流策略中应用ACL，使设备能够基于全局、VLAN或接口下发ACL，实现对转发报文的过滤。此外，ACL还可以应用在Telnet、FTP、路由等模块。

业务分类	应用场景	各业务模块的ACL应用方式	支持的ACL类型
对转发的报文进行过滤	基于全局、接口和VLAN，对转发的报文进行过滤，从而使设备能够进一步对过滤出的报文进行丢弃、修改优先级、重定向等处理。 例如，使用ACL限制不同网段用户互访、禁止特定用户主机在特定时间内上网、利用ACL降低P2P下载、网络视频等消耗大量带宽的数据流的服务等级，在网络拥塞时优先丢弃这类流量，减少它们对其他重要流量的影响。	• 简化流策略：请参见《 S600-E V200R021C00, C01 配置指南-QoS 》基于ACL的简化流策略配置 • 流策略：请参见《 S600-E V200R021C00, C01 配置指南-QoS 》MQC配置	• 基本ACL • 高级ACL • 二层ACL • 用户自定义ACL • 用户ACL • 基本ACL6 • 高级ACL6 • 用户ACL6

业务分类	应用场景	各业务模块的ACL应用方式	支持的ACL类型
对上送CPU处理的报文进行过滤	对上送CPU的报文进行必要的限制，可以避免CPU处理过多的协议报文造成占用率过高、性能下降。 例如，当发现某用户向设备发送大量的ARP攻击报文，造成设备CPU繁忙，引发系统中断时，可以在本机防攻击策略的黑名单中应用ACL，将该用户加入黑名单，使CPU丢弃该用户发送的报文。	黑名单：请参见“本机防攻击配置”中的“**3.5.2 配置黑名单**”。	• 基本ACL • 高级ACL • 二层ACL • 高级ACL

业务分类	应用场景	各业务模块的ACL应用方式	支持的ACL类型
登录控制	对设备的登录权限进行控制，允许合法用户登录，拒绝非法用户登录，从而有效防止未经授权用户的非法接入，保证网络安全性。	• Telnet：请参见《S600-E V200R021C00, C01 配置指南-基础配置》通过CLI登录设备配置 中的“配置通过Telnet登录设备” • FTP：请参见《S600-E V200R021C00, C01 配置指南-基础配置》文件管理 中的“通过FTP进行文件操作” • SFTP：请参见《S600-E V200R021C00, C01 配置指南-基础配置》文件管理 中的“通过SFTP进行文件操作” • HTTP：请参见《S600-E V200R021C00, C01 配置指南-基础配置》通过Web网管登录设备配置 中的“配置通过Web网管登录设备” • SNMP：请参见《S600-E V200R021C00, C01 配置指南-网络管理与监控》SNMP配置中的“（可选）限制网管对设备的管理权限”（SNMPv1、SNMPv2c）和“（可选）限制网管对设备的管	• 基本ACL • 高级ACL • 基本ACL6 • 高级ACL6

业务分类	应用场景	各业务模块的ACL应用方式	支持的ACL类型
		理权限”（SNMPv3）	
路由过滤	ACL可以应用在各种动态路由协议中，对路由协议发布、接收的路由信息以及组播组进行过滤。 例如，可以将ACL和路由策略配合使用过滤路由信息，禁止设备将某网段路由发给邻居路由器。	• RIP：请参见《S600-E V200R021C00,C01 配置指南-IP单播路由》RIP配置 中的“配置RIP引入外部路由信息”和“配置RIP对接收的路由进行过滤” • 组播：请参见《S600-E V200R021C00,C01 配置指南-IP组播》IGMP Snooping配置 中的“配置组播组过滤策略”和“（可选）配置SSM组策略”	• 基本ACL • 高级ACL • 基本ACL6 • 高级ACL6

2.9 修改 ACL

背景信息

当用户需要对已经配置的ACL规则进行调整时，可以通过删除已有rule规则，添加新的rule规则方式修改ACL规则。不建议修改已经存在的rule规则，如果修改时新规则与原规则存在冲突，则冲突的部分新规则代替原规则，可能会导致用户配置无法达到预期效果。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**acl** *acl-number*或者执行命令**acl name** *acl-name*，进入需要修改的ACL视图。

步骤3 根据实际需要修改的ACL类型，配置新的rule规则，并删除不用的rule规则。

说明

更新ACL规则时，设备会先把旧的rule规则和新的rule规则一起下发，然后再将ACL下面的旧的rule规则删除，因此需要保证设备当前还有足够的ACL资源才能更新成功。例如，ACL 3001下面配置了三条规则，用户需要增加一条新规则时，需要保证有四条ACL资源可用才能更新成功。

----结束

2.10 删除 ACL

背景信息

当设备上面的ACL资源使用已经达到满规格，用户需要部署新的ACL业务时，需要删除之前的无用ACL配置以释放资源。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 根据设备上的实际配置，选择下面的配置步骤

- 执行命令**undo acl** { [**number**] *acl-number* | **all** }或**undo acl name** *acl-name*，删除ACL。
- 执行命令**undo acl ipv6** { **all** | [**number**] *acl6-number* }或**undo acl ipv6 name** *acl6-name*，删除ACL6。

说明

设备删除ACL或ACL6，不受引用ACL或ACL6的业务模块影响（简化流策略中引用ACL或ACL6指定rule的情况除外），因此删除时需要保证业务模块不再需要引用该ACL或ACL6规则。

----结束

2.11 维护 ACL

2.11.1 调整 ACL 规则的步长

背景信息

在网络日常维护过程中，已部署的ACL可能无法满足新的业务需求，需要管理员为原ACL添加新的规则。由于ACL的缺省步长是5（即系统自动为ACL规则分配编号时的相邻规则编号之间的差值是5，例如rule 5、rule 10...），所以管理员在系统分配的相邻编号的规则之间，最多只能插入4条规则（rule 6、rule 7、rule 8、rule 9）。如果新业务要求在这两个规则之间插入4条以上的规则，则可以将ACL规则的步长调大到6以上，使系统按照新步长重新调整规则编号（rule 6、rule 12...），从而可以方便的插入4条以上的新规则（rule 7、rule 8、rule 9、rule 10、rule 11）。

关于步长的详细介绍，请参见**2.2.5 ACL的步长设定**。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 创建ACL，可使用编号或者名称两种方式创建。

- 执行命令**acl** [**number**] *acl-number* [**match-order** { **auto** | **config** }]，使用编号创建一个数字型的ACL，并进入ACL视图。
- 执行命令**acl name** *acl-name* [**advance** | **basic** | **link** | **ucl** | **user** | *acl-number*] [**match-order** { **auto** | **config** }]，使用名称创建一个命名型的ACL，并进入ACL视图。

缺省情况下，未创建ACL。

步骤3 执行命令**step** *step*，配置ACL步长。

缺省情况下，步长值为5。

----结束

2.11.2 查看 ACL 的资源信息

背景信息

当用户发现应用ACL时设备提示失败，原因之一可能是设备上的ACL资源已分配完毕。

为了确认设备ACL资源的分配情况，可以查看ACL的资源信息。

操作步骤

- 在任意视图下执行命令**display acl resource** [**slot** *slot-id*]，查看ACL的资源信息。

  显示信息中的“Rule Free”计数非零，表示设备仍存在空余的ACL资源。

----结束

2.11.3 优化 ACL 资源

背景信息

很多业务都会使用ACL，ACL通过ACL规则实现对报文的控制，这些ACL规则都会占用一定的ACL资源。由于设备的ACL资源是有限的，ACL资源超限会导致新的业务无法下发，但对设备的正常运行以及已下发ACL的相关业务不会产生影响。

优化ACL资源需要了解ACL规则是如何占用ACL资源的，通常来说，ACL资源占用数目的计算方式如下：

ACL资源占用数目=ACL规则数目×ACL的应用范围（接口数目/VLAN数目/应用到全局时数目为1）×ACL的应用方向（入方向或出方向各为1，双向为2）

例如，使用命令**if-match acl** { *acl-number* | *acl-name* }配置了1K条规则，并且将引用ACL的流策略应用在8个接口的**outbound**方向上，该配置实际需要占用的ACL资源为8K（1K×8×1）。

实际上，用户在设备上配置的ACL规则数目和实际占用的ACL资源是不一样的，具体的计算方式还因硬件芯片和应用ACL的业务类型等因素而异。

操作步骤

在上述流策略的举例中，如果设备支持的下行ACL资源规格7K，此时该业务无法配置成功。通过以下几种方式，可以减少该业务占用的ACL资源，从而可以顺利配置成功。

- **方式一：删除非必需配置的业务**
  - 执行命令**display traffic-policy applied-record**命令来查看流策略的应用记录，删除已配置的冗余流策略。
  - 排查流策略以外使用到ACL的业务，删除已配置的冗余业务或冗余ACL。
- **方式二：调整ACL应用范围**

  如果应用流策略的接口均在同一个VLAN，或者部分接口在同一个VLAN，并且未应用流策略的接口均不属于这些VLAN，则可以将ACL应用在各接口所属的VLAN下（假设为VLAN 10和VLAN 20）。调整应用范围后，上例占用的ACL资源为1K（规则数）×2（VLAN数）=2K条，满足设备ACL资源规格的限制。
- **方式三：合并ACL规则，减少ACL规则数量**

  分析各ACL规则公用的匹配项，找出各规则之间的联系。

  假设，1K条ACL规则中包含以下内容：

```
#
acl number 3009
 rule 1 permit ip source 10.1.1.1 0 destination 10.10.1.1 0
 rule 2 permit ip source 10.1.1.2 0 destination 10.10.1.1 0
 rule 3 permit ip source 10.1.1.3 0 destination 10.10.1.1 0
 rule 4 permit ip source 10.1.1.4 0 destination 10.10.1.1 0
 ...
 rule 255 permit ip source 10.1.1.255 0 destination 10.10.1.1 0
 rule 256 permit ip source 10.1.2.1 0 destination 10.10.1.1 0
 ...
 rule 510 permit ip source 10.1.2.255 0 destination 10.10.1.1 0
 ...
 rule 801 deny tcp destination-port eq www   //80端口
 rule 802 deny tcp destination-port eq 81
 rule 803 deny tcp destination-port eq 82
 ...
 rule 830 deny tcp destination-port eq pop2  //109端口
 rule 831 deny tcp destination-port eq pop3  //110端口
 ...
 rule 1000 xxx
#
```

  由于rule 1～rule 510均用到了匹配项源IP地址和目的IP地址，且源IP地址覆盖了10.1.1.0/24和10.1.2.0/24两个网段的所有地址，因此可以利用IP地址通配符掩码，将rule 1～rule 510合并成以下两条规则：

```
#
acl number 3009
 rule 1 permit ip source 10.1.1.0 0.0.0.255 destination 10.10.1.1 0
 rule 2 permit ip source 10.1.2.0 0.0.0.255 destination 10.10.1.1 0
 ...
#
```

  合并规则后，上例中的规则减少到492条，占用ACL资源数降低到492（规则数）×8（接口数）=3936条，满足设备ACL资源规格的限制。

  此外，由于前rule 801～rule 831均用到了匹配项TCP目的端口号，且端口号范围覆盖了80～110整个号段，因此可以利用TCP目的端口号的**range**比较符，将rule 801～rule 831合并成以下一条规则：

```
#
acl number 3009
 ...
 rule 801 deny tcp destination-port range 80 110
 ...
#
```


合并规则后，上例中的规则再次减少到462条，占用ACL资源数降低到462（规则数）×8（接口数）=3696条，满足设备ACL资源规格的限制。

2.11.4 配置 ACL 的资源告警阈值百分比

背景信息

设备的ACL或者ACL6业务会占用ACL资源，流量限速业务会占用Meter资源，流量统计业务会占用Counter资源，此时可以配置ACL、Meter或Counter资源的告警阈值百分比。

当ACL、Meter或Counter资源的使用率等于或高于上限告警阈值百分比时，设备将会发出超限告警。之后，如果该比例又等于或小于下限告警阈值百分比，设备会再次发出告警，表明之前的超限告警情况已经恢复正常。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**acl** [**meter** | **counter**] **threshold-alarm** { **upper-limit** *upper-limit* | **lower-limit** *lower-limit* } *，配置ACL、Meter或Counter资源的告警阈值百分比。

缺省情况下，下限告警阈值百分比为70，上限告警阈值百分比为80。

----结束

2.11.5 配置 ACL 规格的资源分配模式

背景信息

当前设备缺省的资源分配模式为Normal模式，在该模式下，ACL不支持匹配目的IPv6地址。如果需要匹配目的IPv6地址，可以将资源分配模式切换至NAC模式。

操作步骤

步骤1 （可选）执行命令**display system resource-template** [**slot** *slot-id*]，查看系统的资源模板信息。

步骤2 执行命令**system-view**，进入系统视图。

步骤3 执行命令**assign resource-template acl-mode** { **nac** | **normal** } [**slot** *slot-id*]，配置ACL规格的资源分配模式。

缺省情况下，ACL规格的资源分配模式为Normal模式。

说明

配置ACL规格的资源分配模式后，需要保存配置重启设备才能生效。

----结束

2.11.6 清除 ACL 或 ACL6 的统计信息

背景信息

须知

清除统计信息后，以前的统计信息将无法恢复，请务必仔细确认。

操作步骤

- 在确认需要清除ACL的运行信息后，请在用户视图下执行**reset acl counter** { **name** *acl-name* | *acl-number* | **all** }命令，清除ACL统计信息。
- 在确认需要清除ACL6的运行信息后，请在用户视图下执行**reset acl ipv6 counter** { **name** *acl6-name* | *acl6-number* | **all** }命令，清除ACL6统计信息。

----结束

2.12 ACL 配置举例

2.12.1 使用基本 ACL 限制 FTP 访问权限示例

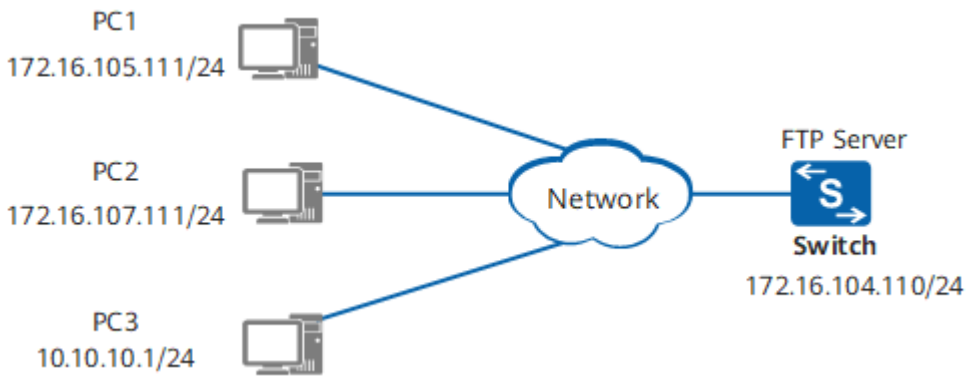
组网需求

如图2-6所示，Switch作为FTP服务器，对网络中的不同用户开放不同的访问权限：

- 子网1（172.16.105.0/24）的所有用户在任意时间都可以访问FTP服务器。
- 子网2（172.16.107.0/24）的所有用户只能在某一个时间范围内访问FTP服务器。
- 其他用户不可以访问FTP服务器。

已知Switch与各个子网之间路由可达，要求在Switch上进行配置，实现FTP服务器对客户端访问权限的设置。

图 2-6 使用基本 ACL 限制 FTP 访问权限组网图



配置思路

采用如下的思路在Switch上进行配置：

1. 配置时间段和ACL，使设备可以基于时间的ACL，对网络中不同用户的报文进行过滤，从而控制不同用户的FTP访问权限。
2. 配置FTP基本功能。
3. 在FTP模块中应用ACL，使ACL生效。

操作步骤

步骤1 配置时间段

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] time-range ftp-access from 0:0 2014/1/1 to 23:59 2014/12/31
[Switch] time-range ftp-access 14:00 to 18:00 off-day
```

步骤2 配置基本ACL

```
[Switch] acl number 2001
[Switch-acl-basic-2001] rule permit source 172.16.105.0 0.0.0.255
[Switch-acl-basic-2001] rule permit source 172.16.107.0 0.0.0.255 time-range ftp-access
[Switch-acl-basic-2001] rule deny source any
[Switch-acl-basic-2001] quit
```

步骤3 配置FTP基本功能

```
[Switch] ftp server-source -i Vlanif 10    //假设客户端使用IP地址172.16.104.110接服务器，该地址对应的接口为Vlanif 10
[Switch] ftp server enable
[Switch] aaa
[Switch-aaa] local-user test password irreversible-cipher SetUserPasswd@123
[Switch-aaa] local-user test privilege level 15
[Switch-aaa] local-user test service-type ftp
[Switch-aaa] local-user test ftp-directory flash:
[Switch-aaa] quit
```

步骤4 配置FTP服务器访问权限

```
[Switch] ftp acl 2001
```

步骤5 验证配置结果

在子网1的PC1（172.16.105.111/24）上执行**ftp 172.16.104.110**命令，可以连接FTP服务器。

2014年某个周一在子网2的PC2（172.16.107.111/24）上执行**ftp 172.16.104.110**命令，不能连接FTP服务器；2014年某个周六下午15:00在子网2的PC2（172.16.107.111/24）上执行**ftp 172.16.104.110**命令，可以连接FTP服务器。

在PC3（10.10.10.1/24）上执行**ftp 172.16.104.110**命令，不能连接FTP服务器。

----结束

配置文件

Switch的配置文件

```
#
sysname Switch
#
FTP server enable
FTP server-source -i vlanif10
FTP acl 2001
```

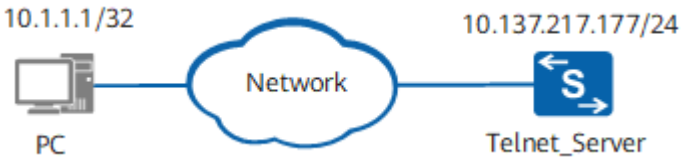
```
#
time-range ftp-access 14:00 to 18:00 off-day
time-range ftp-access from 00:00 2014/1/1 to 23:59 2014/12/31
#
acl number 2001
 rule 5 permit source 172.16.105.0 0.0.0.255
 rule 10 permit source 172.16.107.0 0.0.0.255 time-range ftp-access
 rule 15 deny
#
aaa
 local-user test password irreversible-cipher $1a$a/sUWg/.p1*))=~SWzIRS0N",`&aS%'7X).m=o[PkQcv"!!
TTQOI~Z)C'1<9$
 local-user test privilege level 15
 local-user test ftp-directory flash:
 local-user test service-type ftp
#
return
```

2.12.2 使用基本 ACL 限制 Telnet 登录权限示例

组网需求

如图2-7所示，PC与设备之间路由可达，用户希望简单方便的配置和管理远程设备，可以在服务器端配置Telnet用户使用AAA验证登录，并配置安全策略，保证只有符合安全策略的用户才能登录设备。

图 2-7 配置通过 Telnet 登录设备组网图



配置思路

采用如下的思路配置通过Telnet登录设备：

1. 配置Telnet方式登录设备，以实现远程维护网络设备。
2. 配置管理员的用户名和密码，并配置AAA认证策略，保证只有认证通过的用户才能登录设备。
3. 配置安全策略，保证只有符合安全策略的用户才能登录设备。

操作步骤

步骤1 使能服务器功能

```
<HUAWEI> system-view
[HUAWEI] sysname Telnet_Server
[Telnet_Server] telnet server-source -i Vlanif 10  //假设客户端使用IP地址10.137.217.177接服务器，该地址对应的接口为Vlanif 10
[Telnet_Server] telnet server enable
```

步骤2 配置VTY用户界面的相关参数

配置VTY用户界面的最大个数。

```
[Telnet_Server] user-interface maximum-vty 15
```

配置允许用户登录设备的主机地址。

```
[Telnet_Server] acl 2001
[Telnet_Server-acl-basic-2001] rule permit source 10.1.1.1 0
[Telnet_Server-acl-basic-2001] quit
[Telnet_Server] user-interface vty 0 14
[Telnet_Server-ui-vty0-14] protocol inbound telnet
[Telnet_Server-ui-vty0-14] acl 2001 inbound
```

配置VTY用户界面的终端属性。

```
[Telnet_Server-ui-vty0-14] shell
[Telnet_Server-ui-vty0-14] idle-timeout 20
[Telnet_Server-ui-vty0-14] screen-length 0
[Telnet_Server-ui-vty0-14] history-command max-size 20
```

配置VTY用户界面的用户验证方式。

```
[Telnet_Server-ui-vty0-14] authentication-mode aaa
[Telnet_Server-ui-vty0-14] quit
```

步骤3 配置登录用户的相关信息

配置登录验证方式。

```
[Telnet_Server] aaa
[Telnet_Server-aaa] local-user admin1234 password irreversible-cipher Helloworld@6789
[Telnet_Server-aaa] local-user admin1234 service-type telnet
[Telnet_Server-aaa] local-user admin1234 privilege level 3
[Telnet_Server-aaa] quit
```

步骤4 客户端登录

进入管理员PC的Windows的命令行提示符，执行相关命令，通过Telnet方式登录设备。

```
C:\Documents and Settings\Administrator> telnet 10.137.217.177
```

输入Enter键后，在登录窗口输入AAA验证方式配置的登录用户名和密码，验证通过后，出现用户视图的命令行提示符，至此用户成功登录设备。（以下显示信息仅为示意）

```
Login authentication


Username:admin1234
Password:
Info: The max number of VTY users is 8, and the number
      of current VTY users on line is 2.
      The current login time is 2012-08-06 18:33:18+00:00.
<Telnet_Server>
```

----结束

配置文件

Telnet_Server的配置文件

```
#
sysname Telnet_Server
#
telnet server enable
telnet server-source -i Vlanif 10
#
acl number 2001
```

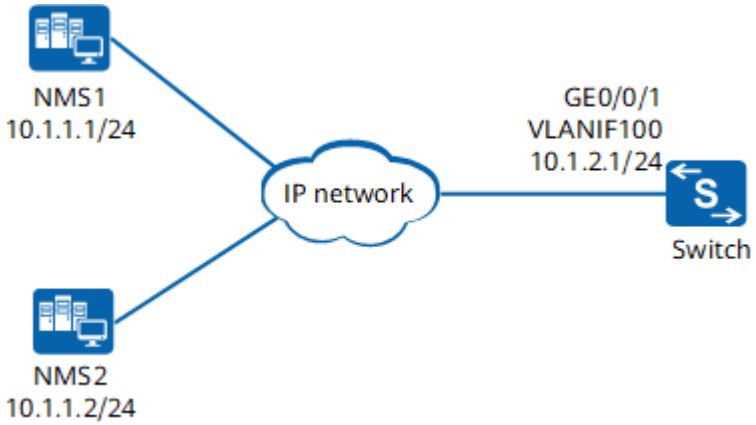
```
 rule 5 permit source 10.1.1.1 0
#
aaa
 local-user admin1234 password irreversible-cipher $1a$aVW8S=aP=B<OWi1Bu'^R[=_!~oR*85r_nNY+kA(I}
[TiLiVGR-i/'DFGAI-O$
 local-user admin1234 privilege level 3
 local-user admin1234 service-type telnet
#
user-interface maximum-vty 15
user-interface vty 0 14
 acl 2001 inbound
 authentication-mode aaa
 history-command max-size 20
 idle-timeout 20 0
 screen-length 0
 protocol inbound telnet
#
return
```

2.12.3 SNMP 中应用基本 ACL 过滤非法网管示例

组网需求

如图2-8所示，网络中存在两个网管可以对网络中的设备进行监管。由于网络规模较小、安全性较高，管理员希望Switch使用SNMPv1版本与网管进行通信，并且只有可信任的网管（NMS2）才能管理Switch，禁止非法网管管理Switch。此外，根据业务需要，管理员希望网管站只对交换机的除RMON的之外的节点进行管理，并且通过网管站的管理，可以让管理员能够快速的进行故障定位和排除。

图 2-8 SNMP 中应用基本 ACL 过滤非法网管组网图



配置思路

采用如下的配置思路：

1. 配置Switch的SNMP版本为SNMPv1。
2. 配置ACL、MIB视图和团体名，控制网管站的访问权限，使NMS2可以管理Switch上RMON之外的节点，NMS1不能管理Switch。
3. 配置告警主机，使Switch产生的告警能够发送至NMS2。为了方便对告警信息进行定位，避免过多的无用告警对处理问题造成干扰，仅允许缺省打开的模块可以发送告警。

4. 配置网管NMS2。

操作步骤

步骤1 配置Switch的接口IP地址，使其和网管站之间路由可达

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type hybrid
[Switch-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[Switch-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface vlanif 100
[Switch-Vlanif100] ip address 10.1.2.1 24
[Switch-Vlanif100] quit
```

步骤2 配置Switch可以接收和响应网管请求报文的接口。

```
[Switch] snmp-agent protocol source-interface vlanif 100
```

步骤3 配置Switch的SNMP版本为SNMPv1

```
[Switch] snmp-agent sys-info version v1
```

步骤4 配置访问权限

配置ACL，使NMS2可以管理Switch，NMS1不允许管理Switch。

```
[Switch] acl 2001
[Switch-acl-basic-2001] rule 5 permit source 10.1.1.2 0.0.0.0
[Switch-acl-basic-2001] rule 6 deny source 10.1.1.1 0.0.0.0
[Switch-acl-basic-2001] quit
```

配置MIB视图，限制NMS2可以管理Switch上除RMON之外的节点。

```
[Switch] snmp-agent mib-view excluded allextrmon 1.3.6.1.2.1.16
```

配置团体名并引用ACL和MIB视图。

```
[Switch] snmp-agent community write adminnms2 mib-view allextrmon acl 2001
```

步骤5 配置告警主机

```
[Switch] snmp-agent target-host trap address udp-domain 10.1.1.2 params securityname adminnms2
```

步骤6 配置网管站（NMS2）

网管系统的认证参数配置必须和设备上保持一致，否则网管系统无法管理设备。如果设备上只配置了write团体名，那么网管端读和写团体名都用设备上配置的write团体名。

说明

网管系统的认证参数配置必须和设备上保持一致，否则网管系统无法管理设备。

步骤7 验证配置结果

配置完成后，可以执行下面的命令，检查配置内容是否生效。

查看SNMP版本。

```
[Switch] display snmp-agent sys-info version
  SNMP version running in the system:
        Polling: SNMPv1:enable,  SNMPv2c:disable,
SNMPv3:disable
        Trap   : SNMPv1:enable,  SNMPv2c:disable,
```

```
SNMPv3:disable
```

查看告警的目标主机。

```
[Switch] display snmp-agent target-host
Target-host NO. 1
------------------------------------------------------------
  IP-address    : 10.1.1.2
  Domain        : -
  Source interface : -
  VPN instance  : -
  Security name : %^%#uq/!YZfvW4*vf[~C|.:Cl}UqS(vXd#wwqR~5M(rU%%^%#
  Port          : 162
  Type          : trap
  Version       : v1
  Level         : No authentication and privacy
  NMS type      : NMS
  With ext-vb   : No
------------------------------------------------------------
```

----结束

配置文件

Switch的配置文件

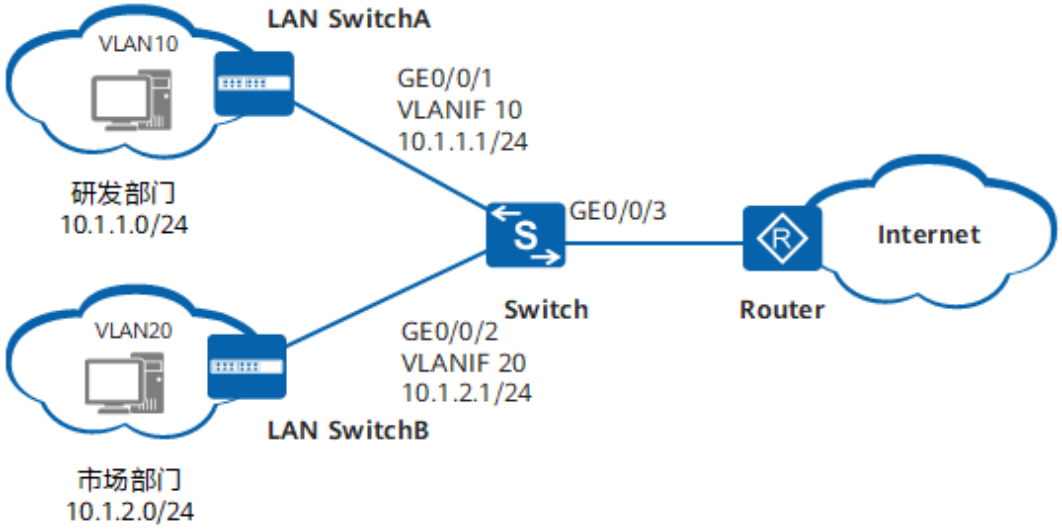
```
#
sysname Switch
#
vlan batch 100
#
acl number 2001
 rule 5 permit source 10.1.1.2 0
 rule 6 deny source 10.1.1.1 0
#
interface Vlanif100
 ip address 10.1.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type hybrid
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
snmp-agent
snmp-agent local-engineid 800007DB03360102101100
snmp-agent community write cipher %^%#.T|&Whvyf$<Gd"I,wXi5SP_6~Nakk6<<+3H:N-h@aJ6d,l0md
%HCeAY8~>X=>xV\JKNAL=124r839v<*%^%# mib-view allextrmon acl 2001
snmp-agent sys-info version v1 v3
snmp-agent target-host trap address udp-domain 10.1.1.2 params securityname cipher %^%#uq/!
YZfvW4*vf[~C|.:Cl}UqS(vXd#wwqR~5M(rU%%^%#
snmp-agent mib-view excluded allextrmon rmon
snmp-agent protocol source-interface Vlanif100
#
return
```

2.12.4 使用高级 ACL 限制不同网段的用户互访示例

组网需求

如图2-9所示，某公司通过Switch实现各部门之间的互连。为方便管理网络，管理员为公司的研发部和市场部规划了两个网段的IP地址。同时为了隔离广播域，又将两个部门划分在不同VLAN之中。现要求Switch能够限制两个网段之间互访，防止公司机密泄露。

图 2-9 使用高级 ACL 限制不同网段的用户互访示例



配置思路

采用如下的思路在Switch上进行配置：

1. 配置高级ACL和基于ACL的流分类，使设备可以对研发部与市场部互访的报文进行过滤。
2. 配置流行为，拒绝匹配上ACL的报文通过。
3. 配置并应用流策略，使ACL和流行为生效。

操作步骤

步骤1 配置接口所属的VLAN以及接口的IP地址

创建VLAN10和VLAN20。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 10 20
```

配置Switch的接口GE0/0/1和GE0/0/2为trunk类型接口，并分别加入VLAN10和VLAN20。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type trunk
[Switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] port link-type trunk
[Switch-GigabitEthernet0/0/2] port trunk allow-pass vlan 20
[Switch-GigabitEthernet0/0/2] quit
```

创建VLANIF10和VLANIF20，并配置各VLANIF接口的IP地址。

```
[Switch] interface vlanif 10
[Switch-Vlanif10] ip address 10.1.1.1 24
[Switch-Vlanif10] quit
[Switch] interface vlanif 20
```

```
[Switch-Vlanif20] ip address 10.1.2.1 24
[Switch-Vlanif20] quit
```

步骤2 配置ACL

创建高级ACL 3001并配置ACL规则，拒绝任一部门访问另一部门的报文通过，这里以拒绝研发部访问市场部的报文通过为例。

```
[Switch] acl 3001
[Switch-acl-adv-3001] rule deny ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[Switch-acl-adv-3001] quit
```

步骤3 配置基于高级ACL的流分类

配置流分类tc1，对匹配ACL 3001的报文进行分类。

```
[Switch] traffic classifier tc1
[Switch-classifier-tc1] if-match acl 3001
[Switch-classifier-tc1] quit
```

步骤4 配置流行为

配置流行为tb1，动作为拒绝报文通过。

```
[Switch] traffic behavior tb1
[Switch-behavior-tb1] deny
[Switch-behavior-tb1] quit
```

步骤5 配置流策略

定义流策略，将流分类与流行为关联。

```
[Switch] traffic policy tp1
[Switch-trafficpolicy-tp1] classifier tc1 behavior tb1
[Switch-trafficpolicy-tp1] quit
```

步骤6 在接口下应用流策略

由于研发部访问市场部的流量从接口GE0/0/1进入Switch，所以在接口GE0/0/1的入方向应用流策略。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] traffic-policy tp1 inbound
[Switch-GigabitEthernet0/0/1] quit
```

步骤7 验证配置结果

查看ACL规则的配置信息。

```
[Switch] display acl 3001
Advanced ACL 3001, 1 rule
Acl's step is 5
 rule 5 deny ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
```

查看流分类的配置信息。

```
[Switch] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: tc1
    Operator: OR
    Rule(s) : if-match acl 3001

Total classifier number is 1
```

查看流策略的配置信息。

```
[Switch] display traffic policy user-defined tp1
  User Defined Traffic Policy Information:
  Policy: tp1
```

```
  Classifier: tc1
   Operator: OR
    Behavior: tb1
     Deny
```

研发部和市场部所在的两个网段之间不能互访。

----结束

配置文件

Switch的配置文件

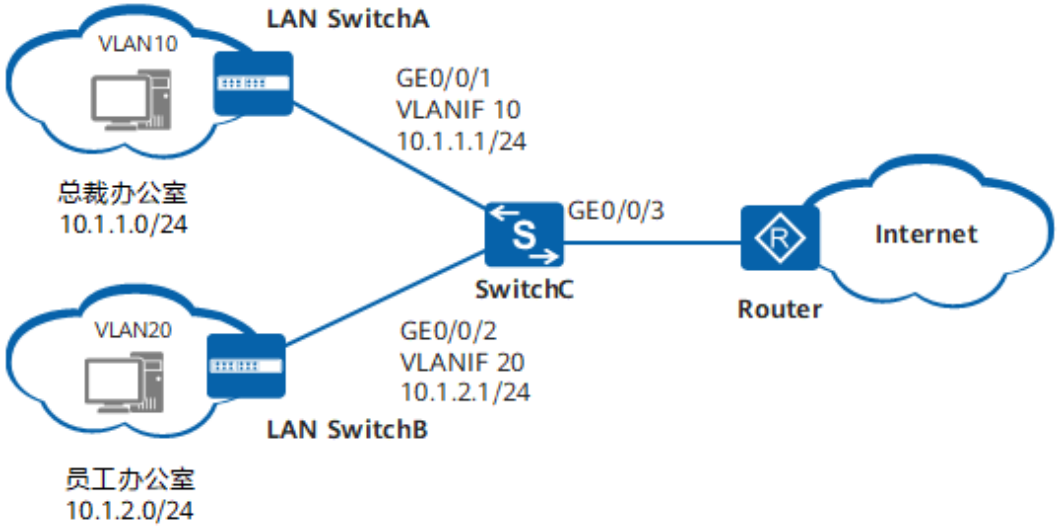
```
#
sysname Switch
#
vlan batch 10 20
#
acl number 3001
 rule 5 deny ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
traffic classifier tc1 operator or
 if-match acl 3001
#
traffic behavior tb1
 deny
#
traffic policy tp1
 classifier tc1 behavior tb1
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface Vlanif20
 ip address 10.1.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 traffic-policy tp1 inbound
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
return
```

2.12.5 使用高级 ACL 实现单向访问控制示例

组网需求

如图2-10所示，某公司通过SwitchC实现各部门之间的互连。为方便管理网络，管理员为公司的总裁办公室和员工办公室规划了两个网段的IP地址。同时为了隔离广播域，又将两个部门划分在不同VLAN之中。现要求总裁办公室能够访问员工办公室，但员工办公室不能访问总裁办公室，防止公司机密泄露。

图 2-10 使用高级 ACL 实现单向访问控制示例



配置思路

1. 配置高级ACL和基于ACL的流分类，通过限制ICMP和TCP业务的方式实现总裁办公室到员工办公室的单向访问：
   - TCP业务：允许员工办公室到总裁办公室的syn+ack报文通过，即允许对总裁办公室发起的TCP连接进行回应；拒绝员工办公室到总裁办公室的syn请求报文通过，防止员工办公室主动发起TCP连接。
   - ICMP业务：拒绝员工办公室到总裁办公室的echo请求报文通过，防止员工办公室主动发起ping连通性测试。

   说明

   UDP业无法实现单向访问。
2. 配置流行为，对匹配上ACL的报文不作任何动作，按原来策略转发。
3. 配置并应用流策略，使ACL和流行为生效。

操作步骤

步骤1 配置接口所属的VLAN以及接口的IP地址

创建VLAN10和VLAN20。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchC
[SwitchC] vlan batch 10 20
```

配置SwitchC的接口GE0/0/1和GE0/0/2为trunk类型接口，并分别加入VLAN10和VLAN20。

```
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] port link-type trunk
[SwitchC-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[SwitchC-GigabitEthernet0/0/1] quit
[SwitchC] interface gigabitethernet 0/0/2
[SwitchC-GigabitEthernet0/0/2] port link-type trunk
[SwitchC-GigabitEthernet0/0/2] port trunk allow-pass vlan 20
[SwitchC-GigabitEthernet0/0/2] quit
```

创建VLANIF10和VLANIF20，并配置各VLANIF接口的IP地址。

```
[SwitchC] interface vlanif 10
[SwitchC-Vlanif10] ip address 10.1.1.1 24
[SwitchC-Vlanif10] quit
[SwitchC] interface vlanif 20
[SwitchC-Vlanif20] ip address 10.1.2.1 24
[SwitchC-Vlanif20] quit
```

步骤2 配置ACL

创建高级ACL 3001并配置ACL规则。

```
[SwitchC] acl 3001
[SwitchC-acl-adv-3001] rule permit tcp source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255 tcp-flag syn ack
[SwitchC-acl-adv-3001] rule deny tcp source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255 tcp-flag syn
[SwitchC-acl-adv-3001] rule deny icmp source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255 icmp-type echo
[SwitchC-acl-adv-3001] quit
```

步骤3 配置基于高级ACL的流分类

配置流分类tc1，对匹配ACL 3001进行分类。

```
[SwitchC] traffic classifier tc1
[SwitchC-classifier-tc1] if-match acl 3001
[SwitchC-classifier-tc1] quit
```

步骤4 配置流行为

配置流行为tb1。

```
[SwitchC] traffic behavior tb1
[SwitchC-behavior-tb1] permit
[SwitchC-behavior-tb1] quit
```

步骤5 配置流策略

定义流策略，将流分类与流行为关联。

```
[SwitchC] traffic policy tp1
[SwitchC-trafficpolicy-tp1] classifier tc1 behavior tb1
[SwitchC-trafficpolicy-tp1] quit
```

步骤6 在接口下应用流策略

在接口GE0/0/2的入方向应用流策略。

```
[SwitchC] interface gigabitethernet 0/0/2
[SwitchC-GigabitEthernet0/0/2] traffic-policy tp1 inbound
[SwitchC-GigabitEthernet0/0/2] quit
```

步骤7 验证配置结果

查看ACL规则的配置信息。

```
[SwitchC] display acl 3001
Advanced ACL 3001, 3 rules
Acl's step is 5
 rule 5 permit tcp source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255 tcp-flag ack syn
 rule 10 deny tcp source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255 tcp-flag syn
 rule 15 deny icmp source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255 icmp-type echo
```

查看流分类的配置信息。

```
[SwitchC] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: tc1
    Operator: OR
    Rule(s) : if-match acl 3001
```



```
Total classifier number is 1
```

查看流策略的配置信息。

```
[SwitchC] display traffic policy user-defined tp1
  User Defined Traffic Policy Information:
  Policy: tp1
   Classifier: tc1
    Operator: OR
     Behavior: tb1
      Permit
```

总裁办公室访问员工办公室，但员工办公室不能访问总裁办公室。

----结束

配置文件

SwitchC的配置文件

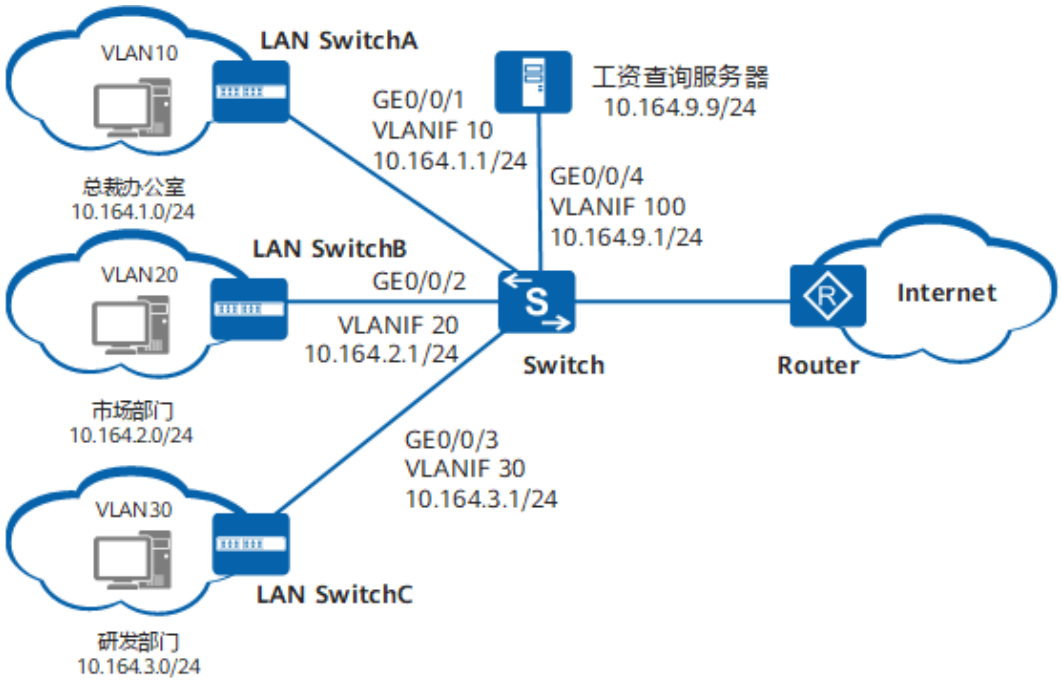
```
#
sysname SwitchC
#
vlan batch 10 20
#
acl number 3001
 rule 5 permit tcp source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255 tcp-flag ack syn
 rule 10 deny tcp source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255 tcp-flag syn
 rule 15 deny icmp source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255 icmp-type echo
#
traffic classifier tc1 operator or
 if-match acl 3001
#
traffic behavior tb1
 permit
#
traffic policy tp1 match-order config
 classifier tc1 behavior tb1
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface Vlanif20
 ip address 10.1.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
 traffic-policy tp1 inbound
#
return
```

2.12.6 使用高级 ACL 限制用户在特定时间访问特定服务器的权限示例

组网需求

如图2-11所示，某公司通过Switch实现各部门之间的互连。公司要求禁止研发部门和市场部门在上班时间（8:00至17:30）访问工资查询服务器（IP地址为10.164.9.9），总裁办公室不受限制，可以随时访问。

图 2-11 使用高级 ACL 限制用户在特定时间访问特定服务器的权限组网图



配置思路

采用如下的思路在Switch上进行配置：

1. 配置时间段、高级ACL和基于ACL的流分类，使设备可以基于时间的ACL，对用户访问服务器的报文进行过滤，从而限制不同用户在特定时间访问特定服务器的权限。
2. 配置流行为，拒绝匹配上ACL的报文通过。
3. 配置并应用流策略，使ACL和流行为生效。

操作步骤

步骤1 配置接口加入VLAN，并配置VLANIF接口的IP地址

将GE0/0/1～GE0/0/3分别加入VLAN10、20、30，GE0/0/4加入VLAN100，并配置各VLANIF接口的IP地址。下面配置以GE0/0/1和VLANIF 10接口为例，接口GE0/0/2、GE0/0/3和GE0/0/4的配置与GE0/0/1接口类似，接口VLANIF 20、VLANIF 30和VLANIF 100的配置与VLANIF 10接口类似，不再赘述。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 10 20 30 100
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type trunk
[Switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface vlanif 10
[Switch-Vlanif10] ip address 10.164.1.1 255.255.255.0
[Switch-Vlanif10] quit
```

步骤2 配置时间段

配置8:00至17:30的周期时间段。

```
[Switch] time-range satime 8:00 to 17:30 working-day
```

步骤3 配置ACL

配置市场部门到工资查询服务器的访问规则。

```
[Switch] acl 3002
[Switch-acl-adv-3002] rule deny ip source 10.164.2.0 0.0.0.255 destination 10.164.9.9 0.0.0.0 time-range satime
[Switch-acl-adv-3002] quit
```

配置研发部门到工资查询服务器的访问规则。

```
[Switch] acl 3003
[Switch-acl-adv-3003] rule deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0.0.0.0 time-range satime
[Switch-acl-adv-3003] quit
```

步骤4 配置基于ACL的流分类

配置流分类c_market，对匹配ACL 3002的报文进行分类。

```
[Switch] traffic classifier c_market
[Switch-classifier-c_market] if-match acl 3002
[Switch-classifier-c_market] quit
```

配置流分类c_rd，对匹配ACL 3003的报文进行分类。

```
[Switch] traffic classifier c_rd
[Switch-classifier-c_rd] if-match acl 3003
[Switch-classifier-c_rd] quit
```

步骤5 配置流行为

配置流行为b_market，动作为拒绝报文通过。

```
[Switch] traffic behavior b_market
[Switch-behavior-b_market] deny
[Switch-behavior-b_market] quit
```

配置流行为b_rd，动作为拒绝报文通过。

```
[Switch] traffic behavior b_rd
[Switch-behavior-b_rd] deny
[Switch-behavior-b_rd] quit
```

步骤6 配置流策略

配置流策略p_market，将流分类c_market与流行为b_market关联。

```
[Switch] traffic policy p_market
[Switch-trafficpolicy-p_market] classifier c_market behavior b_market
[Switch-trafficpolicy-p_market] quit
```

配置流策略p_rd，将流分类c_rd与流行为b_rd关联。

```
[Switch] traffic policy p_rd
[Switch-trafficpolicy-p_rd] classifier c_rd behavior b_rd
[Switch-trafficpolicy-p_rd] quit
```

步骤7 应用流策略

由于市场部访问服务器的流量从接口GE0/0/2进入Switch，所以可以在GE0/0/2接口的入方向应用流策略p_market。


```
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] traffic-policy p_market inbound
[Switch-GigabitEthernet0/0/2] quit
```

由于研发部访问服务器的流量从接口GE0/0/3进入Switch，所以可以在GE0/0/3接口的入方向应用流策略p_rd。

```
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] traffic-policy p_rd inbound
[Switch-GigabitEthernet0/0/3] quit
```

步骤8 验证配置结果

查看ACL规则的配置信息。

```
[Switch] display acl all
 Total nonempty ACL number is 2

Advanced ACL 3002, 1 rule
Acl's step is 5
 rule 5 deny ip source 10.164.2.0 0.0.0.255 destination 10.164.9.9 0 time-range satime (Active)

Advanced ACL 3003, 1 rule
Acl's step is 5
 rule 5 deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0 time-range satime (Active)
```

查看流分类的配置信息。

```
[Switch] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c_market
    Operator: OR
    Rule(s) : if-match acl 3002

   Classifier: c_rd
    Operator: OR
    Rule(s) : if-match acl 3003

Total classifier number is 2
```

查看流策略的配置信息。

```
[Switch] display traffic policy user-defined
  User Defined Traffic Policy Information:
  Policy: p_market
   Classifier: c_market
    Operator: OR
     Behavior: b_market
      Deny

  Policy: p_rd
   Classifier: c_rd
    Operator: OR
     Behavior: b_rd
      Deny

Total policy number is 2
```

查看流策略的应用信息。

```
[Switch] display traffic-policy applied-record
#
----------------------------------------------------
  Policy Name:   p_market
  Policy Index:  0
     Classifier:c_market      Behavior:b_market
----------------------------------------------------
 *interface GigabitEthernet0/0/2
    traffic-policy p_market inbound
      slot 0    :  success
```

```
-----------------------------------------------
  Policy total applied times: 1.
#
-----------------------------------------------
  Policy Name:   p_rd
  Policy Index:  1
    Classifier:c_rd      Behavior:b_rd
-----------------------------------------------
 *interface GigabitEthernet0/0/3
    traffic-policy p_rd inbound
      slot 0    :  success
-----------------------------------------------
  Policy total applied times: 1.
#
```

研发部门和市场部门在上班时间（8:00至17:30）无法访问工资查询服务器。

----结束

配置文件

Switch的配置文件

```
#
sysname Switch
#
vlan batch 10 20 30 100
#
time-range satime 08:00 to 17:30 working-day
#
acl number 3002
 rule 5 deny ip source 10.164.2.0 0.0.0.255 destination 10.164.9.9 0 time-range satime
acl number 3003
 rule 5 deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0 time-range satime
#
traffic classifier c_market operator or
 if-match acl 3002
traffic classifier c_rd operator or
 if-match acl 3003
#
traffic behavior b_market
 deny
traffic behavior b_rd
 deny
#
traffic policy p_market
 classifier c_market behavior b_market
traffic policy p_rd
 classifier c_rd behavior b_rd
#
interface Vlanif10
 ip address 10.164.1.1 255.255.255.0
#
interface Vlanif20
 ip address 10.164.2.1 255.255.255.0
#
interface Vlanif30
 ip address 10.164.3.1 255.255.255.0
#
interface Vlanif100
 ip address 10.164.9.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
```

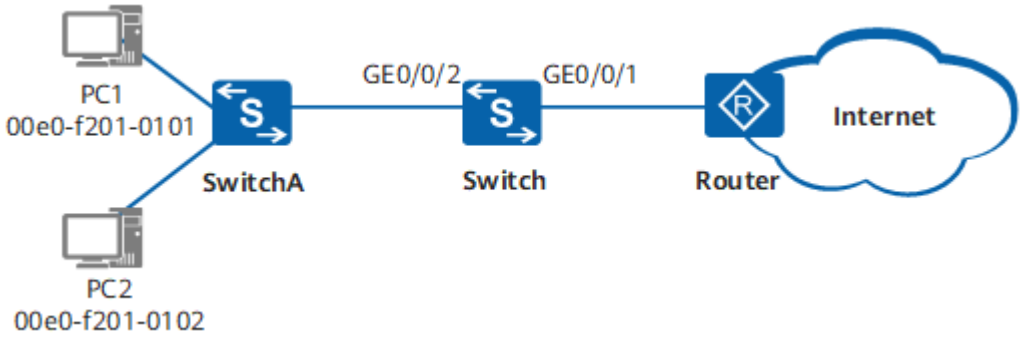
```
 port trunk allow-pass vlan 20
 traffic-policy p_market inbound
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 30
 traffic-policy p_rd inbound
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 100
#
return
```

2.12.7 使用二层 ACL 禁止特定用户上网示例

组网需求

如图2-12所示，Switch作为网关设备，下挂用户PC。管理员发现PC1（MAC地址为00e0-f201-0101）用户是非法用户，要求禁止该用户上网。

图 2-12 使用二层 ACL 禁止特定用户上网示例组网图



配置思路

采用如下的思路在Switch上进行配置：

1. 配置二层ACL和基于ACL的流分类，使设备对MAC地址为00e0-f201-0101的报文进行过滤，从而禁止该地址对应的用户上网。
2. 配置流行为，拒绝匹配上ACL的报文通过。
3. 配置并应用流策略，使ACL和流行为生效。

操作步骤

步骤1 配置ACL

配置符合要求的二层ACL。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] acl 4000
[Switch-acl-L2-4000] rule deny source-mac 00e0-f201-0101 ffff-ffff-ffff
[Switch-acl-L2-4000] quit
```

步骤2 配置基于ACL的流分类

配置流分类tc1，对匹配ACL 4000的报文进行分类。

```
[Switch] traffic classifier tc1
[Switch-classifier-tc1] if-match acl 4000
[Switch-classifier-tc1] quit
```

步骤3 配置流行为

配置流行为tb1，动作为拒绝报文通过。

```
[Switch] traffic behavior tb1
[Switch-behavior-tb1] deny
[Switch-behavior-tb1] quit
```

步骤4 配置流策略

配置流策略tp1，将流分类tc1与流行为tb1关联。

```
[Switch] traffic policy tp1
[Switch-trafficpolicy-tp1] classifier tc1 behavior tb1
[Switch-trafficpolicy-tp1] quit
```

步骤5 应用流策略

由于PC1的报文从接口GE0/0/2进入Switch并流向Internet，所以可以在接口GE0/0/2的入方向应用流策略tp1。

```
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] traffic-policy tp1 inbound
[Switch-GigabitEthernet0/0/2] quit
```

步骤6 验证配置结果

查看ACL规则的配置信息。

```
[Switch] display acl 4000
L2 ACL 4000, 1 rule
Acl's step is 5
 rule 5 deny source-mac 00e0-f201-0101
```

查看流分类的配置信息。

```
[Switch] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: tc1
    Operator: OR
    Rule(s) : if-match acl 4000

Total classifier number is 1
```

查看流策略的配置信息。

```
[Switch] display traffic policy user-defined tp1
 User Defined Traffic Policy Information:
 Policy: tp1
  Classifier: tc1
   Operator: OR
    Behavior: tb1
     Deny
```

查看流策略的应用信息。

```
[Switch] display traffic-policy applied-record
#
----------------------------------------------------
 Policy Name:   tp1
 Policy Index:  0
```



```
    Classifier:tc1      Behavior:tb1
-------------------------------------------------
 *interface GigabitEthernet0/0/2
   traffic-policy tp1 inbound
     slot 0    :  success
-------------------------------------------------
  Policy total applied times: 1.
#
```

源MAC地址是00e0-f201-0101的用户无法上网。

----结束

配置文件

Switch的配置文件

```
#
sysname Switch
#
acl number 4000
 rule 5 deny source-mac 00e0-f201-0101
#
traffic classifier tc1 operator or
 if-match acl 4000
#
traffic behavior tb1
 deny
#
traffic policy tp1
 classifier tc1 behavior tb1
#
interface GigabitEthernet0/0/2
 traffic-policy tp1 inbound
#
return
```

2.12.8 在 QoS 中使用二层 ACL 实施流量监管示例

组网需求

网络中的语音业务对应的VLAN ID为120，视频业务对应的VLAN ID为110，数据业务对应的VLAN ID为100。

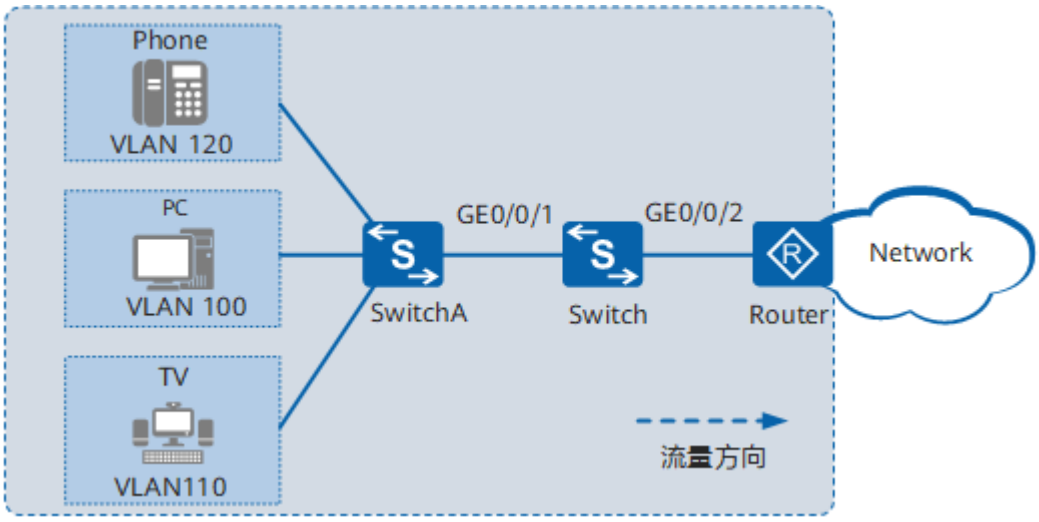
在Switch上需要对不同业务的报文分别进行流量监管，以将流量限制在一个合理的范围之内，并保证各业务的带宽需求。

具体配置需求如表2-16所示。

表 2-16 Switch 为上行流量提供的 QoS 保障

流量类型	CIR(kbps)	PIR(kbps)
语音	2000	10000
视频	4000	10000
数据	4000	10000

图 2-13 流量监管配置组网图



配置思路

采用如下的思路配置基于ACL的简化流策略实现流量监管：

1. 创建VLAN，并配置各接口，使用户能够通过Switch访问网络。
2. 在Switch上配置ACL匹配不同的VLAN ID以区分不同的业务。
3. 在Switch上配置基于ACL的流量监管，对报文分别限速。

操作步骤

步骤1 创建VLAN并配置各接口

在Switch上创建VLAN 100、110、120。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 100 110 120
```

将接口GE0/0/1、GE0/0/2的接入类型分别配置为trunk，并分别将接口GE0/0/1和GE0/0/2加入VLAN 100、VLAN 110、VLAN 120。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type trunk
[Switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 110 120
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] port link-type trunk
[Switch-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 110 120
[Switch-GigabitEthernet0/0/2] quit
```

步骤2 配置ACL

在Switch上创建二层ACL，对不同业务流按照其VLAN ID进行分类。

```
[Switch] acl 4001
[Switch-acl-L2-4001] rule 1 permit vlan-id 120
[Switch-acl-L2-4001] quit
[Switch] acl 4002
[Switch-acl-L2-4002] rule 1 permit vlan-id 110
```

```
[Switch-acl-L2-4002] quit
[Switch] acl 4003
[Switch-acl-L2-4003] rule 1 permit vlan-id 100
[Switch-acl-L2-4003] quit
```

步骤3 配置流量监管

在Switch的接口GE0/0/1入方向上配置流量监管，对报文进行限速。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] traffic-limit inbound acl 4001 cir 2000 pir 10000
[Switch-GigabitEthernet0/0/1] traffic-limit inbound acl 4002 cir 4000 pir 10000
[Switch-GigabitEthernet0/0/1] traffic-limit inbound acl 4003 cir 4000 pir 10000
[Switch-GigabitEthernet0/0/1] quit
```

步骤4 验证配置结果

查看设备接口入方向上应用的ACL规则和流动作信息。

```
[Switch] display traffic-applied interface gigabitethernet 0/0/1 inbound
-------------------------------------------------------------
ACL applied inbound interface GigabitEthernet0/0/1

ACL 4001
 rule 1 permit vlan-id 120
ACTIONS:
 limit cir 2000 ,cbs 250000
       pir 10000 ,pbs 1250000
       green : pass
       yellow : pass
       red : drop
-------------------------------------------------------------

ACL 4002
 rule 1 permit vlan-id 110
ACTIONS:
 limit cir 4000 ,cbs 500000
       pir 10000 ,pbs 1250000
       green : pass
       yellow : pass
       red : drop
-------------------------------------------------------------

ACL 4003
 rule 1 permit vlan-id 100
ACTIONS:
 limit cir 4000 ,cbs 500000
       pir 10000 ,pbs 1250000
       green : pass
       yellow : pass
       red : drop
-------------------------------------------------------------
```

----结束

配置文件

Switch的配置文件

```
#
sysname Switch
#
vlan batch 100 110 120
#
acl number 4001
 rule 1 permit vlan-id 120
acl number 4002
 rule 1 permit vlan-id 110
```

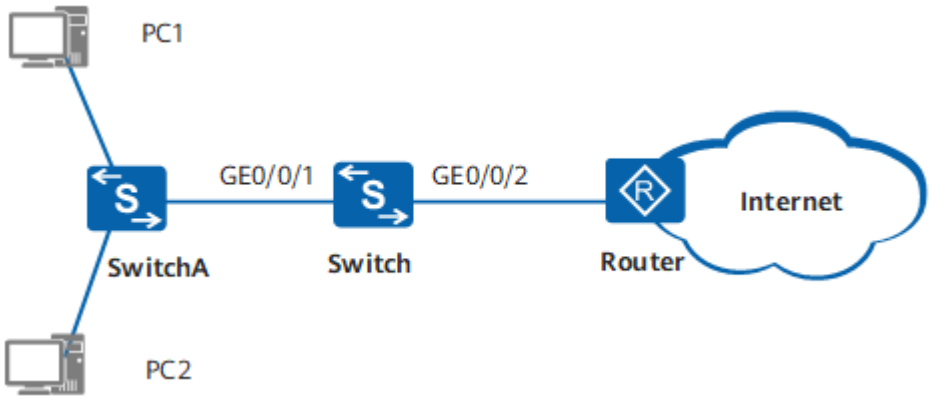
```
acl number 4003
 rule 1 permit vlan-id 100
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 110 120
 traffic-limit inbound acl 4001 cir 2000 pir 10000 cbs 250000 pbs 1250000
 traffic-limit inbound acl 4002 cir 4000 pir 10000 cbs 500000 pbs 1250000
 traffic-limit inbound acl 4003 cir 4000 pir 10000 cbs 500000 pbs 1250000
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 100 110 120
#
return
```

2.12.9 使用用户自定义 ACL 过滤特定报文流示例

组网需求

如图2-14所示，Switch通过GE0/0/1接口连接用户。要求Switch能对来自用户的特定报文（从二层报文头偏移14个字节开始匹配的字符串内容为0x0180C200的报文）进行过滤，并拒绝该报文通过。

图 2-14 使用用户自定义 ACL 过滤特定报文流示例组网图



配置思路

采用如下的思路在Switch上进行配置：

1. 配置用户自定义ACL和基于ACL的流分类，使设备可以对特定报文（从二层报文头偏移14个字节开始匹配的字符串是0x0180C200的报文）进行过滤。
2. 配置流行为，拒绝匹配上ACL的报文通过。
3. 配置并应用流策略，使ACL和流行为生效。

操作步骤

步骤1 配置ACL

配置符合要求的用户自定义ACL。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
```

```
[Switch] acl 5000
[Switch-acl-user-5000] rule deny l2-head 0x0180C200 0xFFFFFFFF 14
[Switch-acl-user-5000] quit
```

步骤2 配置基于用户自定义ACL的流分类

配置流分类tc1，对匹配ACL 5000的报文进行分类。

```
[Switch] traffic classifier tc1
[Switch-classifier-tc1] if-match acl 5000
[Switch-classifier-tc1] quit
```

步骤3 配置流行为

配置流行为tb1，动作为拒绝报文通过。

```
[Switch] traffic behavior tb1
[Switch-behavior-tb1] deny
[Switch-behavior-tb1] quit
```

步骤4 配置流策略

定义流策略，将流分类与流行为关联。

```
[Switch] traffic policy tp1
[Switch-trafficpolicy-tp1] classifier tc1 behavior tb1
[Switch-trafficpolicy-tp1] quit
```

步骤5 在接口下应用流策略

在接口GE0/0/1的入方向应用流策略。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] traffic-policy tp1 inbound
[Switch-GigabitEthernet0/0/1] quit
```

步骤6 验证配置结果

查看ACL规则的配置信息。

```
[Switch] display acl 5000
User ACL 5000, 1 rule
Acl's step is 5
 rule 5 deny 0x0180c200 0xffffffff 14
```

查看流分类的配置信息。

```
[Switch] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: tc1
    Operator: OR
    Rule(s) : if-match acl 5000

Total classifier number is 1
```

查看流策略的配置信息。

```
[Switch] display traffic policy user-defined tp1
  User Defined Traffic Policy Information:
  Policy: tp1
   Classifier: tc1
    Operator: OR
     Behavior: tb1
      Deny
```

----结束

配置文件

Switch的配置文件

```
#
sysname Switch
#
acl number 5000
 rule 5 deny 0x0180c200 0xffffffff 14
#
traffic classifier tc1 operator or
 if-match acl 5000
#
traffic behavior tb1
 deny
#
traffic policy tp1
 classifier tc1 behavior tb1
#
interface GigabitEthernet0/0/1
 traffic-policy tp1 inbound
#
return
```

2.12.10 使用用户 ACL 对企业内用户的访问权限进行分组控制示例

组网需求

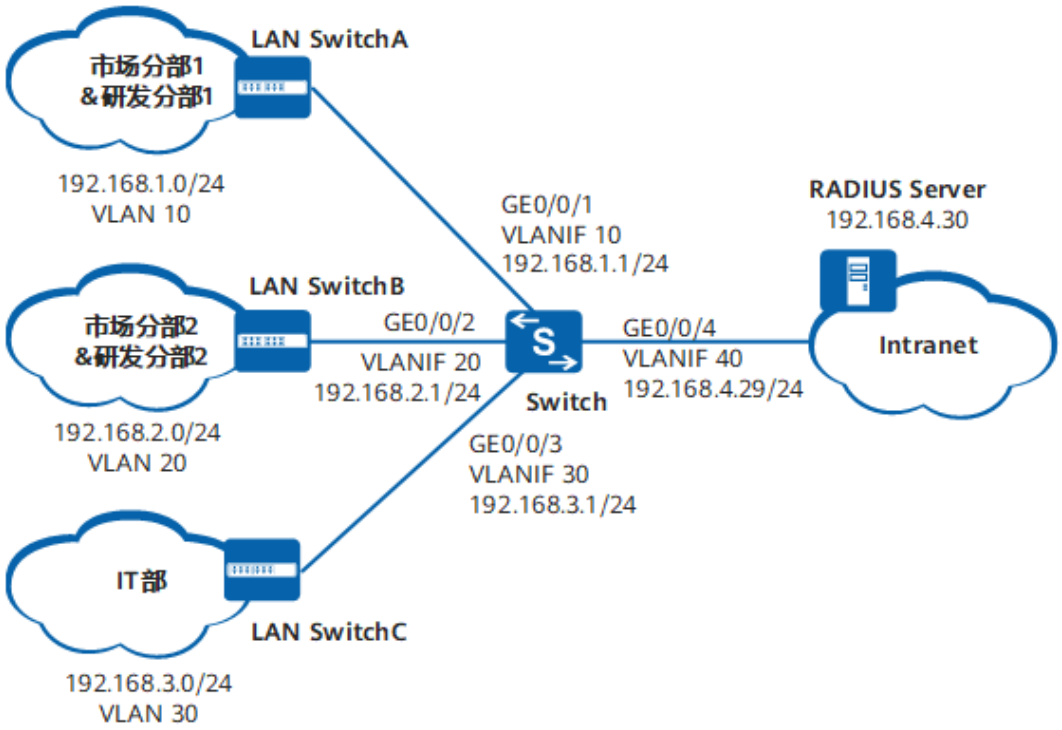
如图2-15所示，某公司办公区内大量用户终端通过Switch接入公司内部网络。由于部分部门有多个分部，各分部人员办公位置分布较散，所以同一部门的用户终端未共用同一网段的IP地址。

管理员希望Switch能对各部门接入的用户终端（包括主机和打印机）进行认证，防止非法用户接入破坏公司内网环境。同时，由于各部门人员的工作性质不同，管理员还希望Switch能为不同部门的人员授予不同的网络访问权限，避免各部门之间相互访问造成公司机密的泄露。

具体要求如下：

- 禁止市场部人员访问IT部。
- 禁止研发部人员访问IT部。

图 2-15 使用用户 ACL 对企业内用户的访问权限进行分组控制示例组网图



配置思路

采用如下思路在Switch上进行配置：

1. 创建并配置RADIUS服务器模板、AAA方案以及认证域，并在认证域下绑定RADIUS服务器模板与AAA方案，保证Switch与RADIUS Server之间能够信息交互，使用户终端可以通过RADIUS服务器进行认证。
2. 由于各部门的用户终端类型包括用户主机和无法安装802.1X客户端的打印机，因此可以同时配置MAC认证和802.1X认证功能并使MAC认证优先，保证所有类型的用户终端均能够通过认证访问网络资源。
3. 由于各部门用户终端数量较多且部分部门内的终端分布在不同网段，为每台终端单独部署网络访问权限的控制策略工作量巨大，因此可以配置UCL组对用户终端进行分类，并配置用户ACL关联UCL组使每个组内的终端可以复用一组ACL规则，以减小管理员的工作量，也可以节约设备的ACL资源。
4. 创建业务方案，并在业务方案中应用UCL组，以实现对各部门的网络访问权限进行分组控制。

说明

本举例只包括Switch上的配置，LAN Switch和RADIUS服务器的配置这里不做相关说明。

操作步骤

步骤1 配置接口所属的VLAN以及接口的IP地址，保证网络通畅。

创建VLAN10、VLAN20、VLAN30和VLAN40。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 10 20 30 40
```

配置Switch的接口GE0/0/1、GE0/0/2、GE0/0/3和GE0/0/4为trunk类型接口，并分别加入VLAN10、VLAN20、VLAN30和VLAN40。以接口GE0/0/1为例，接口GE0/0/2、GE0/0/3和GE0/0/4的配置与GE0/0/1类似，不再赘述。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type trunk
[Switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Switch-GigabitEthernet0/0/1] quit
```

创建VLANIF10、VLANIF20、VLANIF30和VLANIF40，并配置各VLANIF接口的IP地址，使用户终端、Switch、企业内网资源之间能够建立起路由。

```
[Switch] interface vlanif 10
[Switch-Vlanif10] ip address 192.168.1.1 24
[Switch-Vlanif10] quit
[Switch] interface vlanif 20
[Switch-Vlanif20] ip address 192.168.2.1 24
[Switch-Vlanif20] quit
[Switch] interface vlanif 30
[Switch-Vlanif30] ip address 192.168.3.1 24
[Switch-Vlanif30] quit
[Switch] interface vlanif 40
[Switch-Vlanif40] ip address 192.168.4.29 24
[Switch-Vlanif40] quit
```

步骤2 创建并配置RADIUS服务器模板、AAA方案以及认证域。

创建并配置RADIUS服务器模板“rd1”。

```
[Switch] radius-server template rd1
[Switch-radius-rd1] radius-server authentication 192.168.4.30 1812
[Switch-radius-rd1] radius-server shared-key cipher test@123
[Switch-radius-rd1] radius-server retransmit 2
[Switch-radius-rd1] quit
```

创建AAA方案“abc”并配置认证方式为RADIUS。

```
[Switch] aaa
[Switch-aaa] authentication-scheme abc
[Switch-aaa-authen-abc] authentication-mode radius
[Switch-aaa-authen-abc] quit
```

创建认证域“abc11”，并在认证域其上绑定AAA方案“abc”与RADIUS服务器模板“rd1”。

```
[Switch-aaa] domain abc11
[Switch-aaa-domain-abc11] authentication-scheme abc
[Switch-aaa-domain-abc11] radius-server rd1
[Switch-aaa-domain-abc11] quit
[Switch-aaa] quit
```

步骤3 配置MAC认证和802.1X认证。

将NAC模式切换为统一模式。

说明

缺省情况下，NAC配置模式为统一模式，无需执行此步骤。

传统模式与统一模式相互切换后，必须重启设备，新配置模式的各项功能才能生效。

```
[Switch] authentication unified-mode
```

配置MAC接入模板。

```
[Switch] mac-access-profile name m1
[Switch-mac-access-profile-m1] mac-authen username fixed A-123 password cipher test123
[Switch-mac-access-profile-m1] quit
```

配置802.1X接入模板。

说明

802.1X接入模板默认采用EAP认证方式。请确保RADIUS服务器支持EAP协议，否则无法处理802.1X认证请求。

```
[Switch] dot1x-access-profile name d1
[Switch-dot1x-access-profile-d1] quit
```

配置认证模板。

```
[Switch] authentication-profile name p1
[Switch-authen-profile-p1] mac-access-profile m1
[Switch-authen-profile-p1] dot1x-access-profile d1
[Switch-authen-profile-p1] authentication dot1x-mac-bypass
[Switch-authen-profile-p1] quit
```

在接口GE0/0/1、GE0/0/2、GE0/0/3下使能MAC认证和802.1X认证。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] authentication-profile p1
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] authentication-profile p1
[Switch-GigabitEthernet0/0/2] quit
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] authentication-profile p1
[Switch-GigabitEthernet0/0/3] quit
```

步骤4 创建UCL组，并配置关联UCL组的用户ACL，最后应用用户ACL对报文进行过滤。

创建UCL组group_m和group_r。将市场部规划到group_m中，研发部规划到group_r中。

```
[Switch] ucl-group 1 name group_m
[Switch] ucl-group 2 name group_r
```

说明

RADIUS服务器上必须同时存在市场、研发部门用户对应的用户组信息。

创建用户ACL 6001并配置ACL规则。配置rule 5，禁止市场部人员访问IT部；配置rule 10，禁止研发部人员访问IT部。

```
[Switch] acl 6001
[Switch-acl-ucl-6001] rule 5 deny ip source ucl-group name group_m destination 192.168.3.0 0.0.0.255
[Switch-acl-ucl-6001] rule 10 deny ip source ucl-group name group_r destination 192.168.3.0 0.0.0.255
[Switch-acl-ucl-6001] quit
```

配置基于用户ACL对报文进行过滤，使用户ACL生效。

```
[Switch] traffic-filter inbound acl 6001
```

步骤5 创建业务方案“service-scheme1”、“service-scheme2”，并在业务方案中分别应用UCL组group_m、group_r，实现各部门网络权限的分组控制。

```
[Switch] aaa
[Switch-aaa] service-scheme service-scheme1
[Switch-aaa-service-service-scheme1] ucl-group name group_m
[Switch-aaa-service-service-scheme1] quit
[Switch-aaa] service-scheme service-scheme2
[Switch-aaa-service-service-scheme2] ucl-group name group_r
[Switch-aaa-service-service-scheme2] quit
[Switch-aaa] quit
[Switch] quit
```

说明

执行以上步骤后，还需对RADIUS服务器进行配置，将service-scheme与用户关联。

步骤6 验证配置结果。

执行命令**display acl all**，查看用户ACL规则的配置信息。

```
<Switch> display acl all
 Total nonempty ACL number is 1

Ucl-group ACL 6001, 2 rules
Acl's step is 5
 rule 5 deny ip source ucl-group name group_m destination 192.168.3.0 0.0.0.255
 rule 10 deny ip source ucl-group name group_r destination 192.168.3.0 0.0.0.255
```

执行命令**display ucl-group all**，检查创建的所有ucl-group信息。

执行命令**display dot1x**，查看802.1X认证的配置信息。从显示信息中能够看到接口GE0/0/1、GE0/0/2、GE0/0/3下已使能了802.1X认证（**802.1x protocol is Enabled**）。

执行命令**display mac-authen**，查看MAC认证的配置信息。从显示信息中能够看到接口GE0/0/1、GE0/0/2、GE0/0/3下已使能了MAC认证（**MAC address authentication is enabled**）。

市场部人员不能访问IT部，研发部人员不能访问IT部。

----结束

配置文件

Switch的配置文件

```
#
sysname Switch
#
vlan batch 10 20 30 40
#
authentication-profile name p1
 dot1x-access-profile d1
 mac-access-profile m1
 authentication dot1x-mac-bypass
ucl-group 1 name group_m
ucl-group 2 name group_r
#
radius-server template rd1
 radius-server shared-key cipher %^%#zH_B2{mN=177WZ2z+G|5)c'OKD[VaPNYP4>&6uC~%^%#
 radius-server authentication 192.168.4.30 1812 weight 80
 radius-server retransmit 2
#
acl number 6001
 rule 5 deny ip source ucl-group name group_m destination 192.168.3.0 0.0.0.255                    rule
10 deny ip source ucl-group name group_r destination 192.168.3.0 0.0.0.255
#
aaa
 authentication-scheme abc
  authentication-mode radius
 service-scheme service-scheme1
  ucl-group name group_m
 service-scheme service-scheme2
  ucl-group name group_r
 domain abc11
  authentication-scheme abc
  radius-server rd1
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
#
interface Vlanif20
```



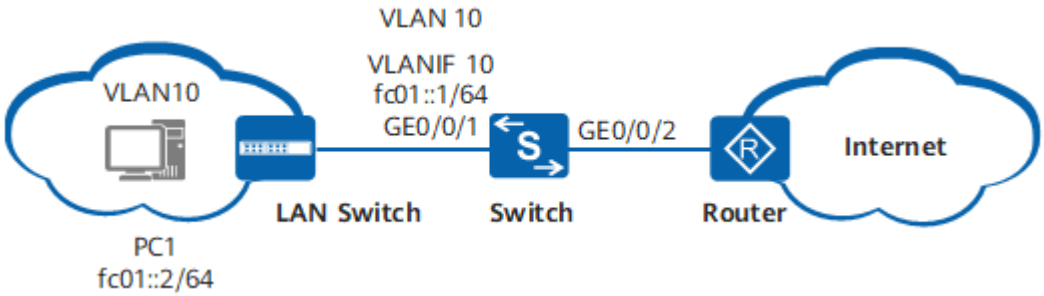
```
 ip address 192.168.2.1 255.255.255.0
#
interface Vlanif30
 ip address 192.168.3.1 255.255.255.0
#
interface Vlanif40
 ip address 192.168.4.29 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 authentication-profile p1
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
 authentication-profile p1
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 30
 authentication-profile p1
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 40
#
traffic-filter inbound acl 6001
#
dot1x-access-profile name d1
#
mac-access-profile name m1
 mac-authen username fixed A-123 password cipher %^%#(!XnF'#X^Sc=[&,fH38!
OKNNEjez>NO`Z*NJK*s4%^%#
#
return
```

2.12.11 使用高级 ACL6 过滤特定 IPv6 报文示例

组网需求

如图2-16所示，Switch通过GE0/0/1接口连接用户。要求Switch能对来自用户的特定IPv6报文（源IPv6地址为fc01::2/64、目的IPv6地址为fc01::1/64的IPv6报文）进行过滤，并拒绝该报文通过。

图 2-16 使用高级 ACL6 过滤特定 IPv6 报文示例组网图



配置思路

采用如下思路在Switch上进行配置：

1. 配置高级ACL6和基于ACL6的流分类，使设备可以对特定IPv6报文（源IPv6地址为fc01::2/64、目的IPv6地址为fc01::1/64的IPv6报文）进行过滤。
2. 配置流行为，拒绝匹配上ACL6的报文通过。
3. 配置并应用流策略，使ACL6和流行为生效。

操作步骤

步骤1 使能IPv6转发能力，并配置接口加入VLAN以及VLANIF接口的IPv6地址。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] ipv6
[Switch] vlan batch 10
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type trunk
[Switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface vlanif 10
[Switch-Vlanif10] ipv6 enable
[Switch-Vlanif10] ipv6 address fc01::1 64
[Switch-Vlanif10] quit
```

步骤2 配置高级ACL6和基于ACL6的流分类，并配置流行为和流策略，再在接口GE0/0/1的入方向应用流策略，用于拒绝源IPv6地址为fc01::2/64、目的IPv6地址为fc01::1/64的IPv6报文通过。

```
[Switch] acl ipv6 number 3001
[Switch-acl6-adv-3001] rule deny ipv6 source fc01::2/64 destination fc01::1/64
[Switch-acl6-adv-3001] quit
[Switch] traffic classifier class1
[Switch-classifier-class1] if-match ipv6 acl 3001
[Switch-classifier-class1] quit
[Switch] traffic behavior behav1
[Switch-behavior-behav1] deny
[Switch-behavior-behav1] statistic enable
[Switch-behavior-behav1] quit
[Switch] traffic policy policy1
[Switch-trafficpolicy-policy1] classifier class1 behavior behav1
[Switch-trafficpolicy-policy1] quit
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] traffic-policy policy1 inbound
[Switch-GigabitEthernet0/0/1] quit
```

步骤3 验证配置结果

查看ACL6的配置信息。

```
[Switch] display acl ipv6 3001

Advanced IPv6 ACL 3001, 1 rule
 rule 0 deny ipv6 source FC01::/64 destination FC01::/64
```

查看流分类的配置信息。

```
[Switch] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: class1
    Operator: OR
    Rule(s) : if-match ipv6 acl 3001

Total classifier number is 1
```

查看流策略的配置信息。

```
[Switch] display traffic policy user-defined
  User Defined Traffic Policy Information:
  Policy: policy1
   Classifier: class1
    Operator: OR
     Behavior: behav1
      Deny
      Statistic: enable

Total policy number is 1
```

PC1无法访问网络，在Switch上执行命令**display traffic policy statistics interface gigabitethernet 0/0/1 inbound**可以看到匹配的报文与丢弃的报文数一样多，匹配ACL3001的报文全部被丢弃。

----结束

配置文件

Switch的配置文件

```
#
sysname Switch
#
ipv6
#
vlan batch 10
#
acl ipv6 number 3001
 rule 0 deny ipv6 source FC01::/64 destination FC01::/64
#
traffic classifier class1 operator or
 if-match ipv6 acl 3001
#
traffic behavior behav1
 deny
 statistic enable
#
traffic policy policy1
 classifier class1 behavior behav1
#
interface Vlanif10
 ipv6 enable
 ipv6 address FC01::1/64
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 traffic-policy policy1 inbound
#
return
```

2.13 ACL 常见配置错误

2.13.1 误屏蔽 DNS 服务器地址导致用户无法上网

故障现象

配置ACL限制用户可访问的地址时，误将DNS服务器地址加入到了限制的地址范围内，导致用户访问网站时向DNS服务器发送的查询报文被屏蔽，网站域名得不到解析，从而造成用户无法上网。

操作步骤

步骤1 在系统视图下，执行命令**display acl**，查看ACL规则的配置。

发现设备上配置了如下一条规则：

```
rule 100 deny ip destination 10.102.192.0 0.0.0.255  //禁止访问10.102.192.0/24网段的报文通过
```

由于用户PC上设置的DNS服务器地址是10.102.192.68，属于10.102.192.0/24网段，因此用户向DNS服务器发送的报文也被禁止通过，导致其访问网站的域名得不到解析，从而无法上网。

步骤2 在上述规则对应的ACL视图下，执行命令**rule（高级ACL视图）**，在原规则前增加一条放行DNS服务器地址的规则。

```
rule 99 permit ip destination 10.102.192.68 0.0.0.0  //允许访问DNS服务器地址的报文通过
rule 100 deny ip destination 10.102.192.0 0.0.0.255  //禁止访问10.102.192.0/24网段的报文通过
```

添加新规则rule 99后，用户发送给DNS服务器地址的报文会先命中rule 99而得到允许通过，从而使用户访问网站的域名能够被DNS服务器正常解析，用户可以正常上网。

----结束

2.13.2 系统时间不正确导致基于时间的 ACL 不生效

故障现象

由于设备的系统时间与现实时间不一致，导致设备上配置的基于时间的ACL不生效。

操作步骤

步骤1 在系统视图下，执行命令**display acl**，查看ACL规则的配置。

发现设备上配置了一条基于时间的ACL规则：

```
rule 10 deny ip source 10.1.1.1 0 time-range time1 //在time1设定的时间范围内，禁止源地址是10.1.1.1的报文通过
```

步骤2 在系统视图下，执行命令**display time-range** { **all** | *time-name* }，查看生效时间段**time1**的配置。

显示信息如下：

```
Current time is 14:53:17 8-16-2013 Friday

Time-range: time1 ( Inactive )
from 00:00 2014/1/1 to 23:59 2014/12/31
Total time-range number is 1
```

可以看到，时间段**time1**设定的范围是2014年1月1日零点开始到2014年12月31日23：59分结束，并且设备上的系统时间是2013年的8月16日14:53:17秒。由于当前的实际日期是2014年8月16日，并且设备上设置的系统时间不在时间段**time1**设定的时间范围内，因此引用**time1**的ACL不生效，源地址是10.1.1.1的报文不会被设备禁止通过。

步骤3 调整系统日期和时间。

- 重新配置设备的当前日期和时间，保证设备时间与现实时间的一致。

  在用户视图下，执行命令**clock datetime**。

  ```
  clock datetime 14:53:17 2014-08-16 //将日期调整为2014-08-16
  ```

- 配置NTP，实现系统时钟的自动同步，使设备与时间可信任的设备（该设备通过网络和权威时钟同步过时钟）上的时间保持一致。

a. 在时间可信任的设备上，配置使用本地设备时钟作为NTP主时钟以及NTP主时钟所处的层数。

在系统视图下，执行命令**ntp-service refclock-master**。

```
ntp-service refclock-master 2 //层数值越小表示时钟准确度越高
```

b. 在本设备（需同步其他设备时钟的设备）上，配置NTP工作模式，具体配置请参见《S600-E V200R021C00, C01 配置指南-设备管理》NTP配置 中的“配置NTP工作模式”。

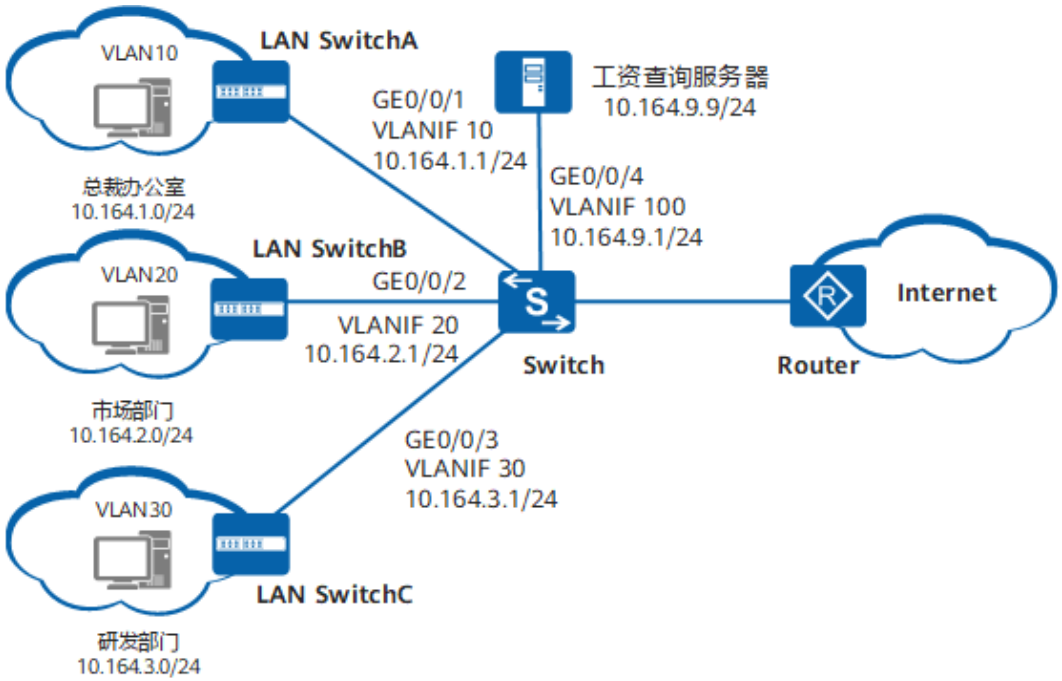
----结束

2.13.3 流策略应用方向错误导致访问控制不生效

故障现象

如图2-17所示，某公司通过Switch实现各部门之间的互连。Switch的GE0/0/4连接工资查询服务器。公司要求禁止研发和市场等部门访问工资查询服务器，仅允许总裁办公室可以访问。因此，管理员在Switch上配置了ACL以及引用ACL的流策略，并在接口GE0/0/4的入方向上应用了流策略。由于应用方向错误，导致访问控制不生效。

图 2-17 在接口上应用流策略组网图



操作步骤

步骤1 在任意视图下，执行命令**display traffic policy interface** [*interface-type interface-number*]，查看接口下已配置的流策略信息。

发现接口GE0/0/4的入方向上应用了流策略p1：

```
Interface: GigabitEthernet0/0/4
```

```
Direction: Inbound
Policy: p1
......
```

步骤2 在任意视图下，执行命令**display traffic-applied interface** [*interface-type interface-number*] **inbound verbose**，查看接口下应用的流策略中引用的ACL以及流策略应用的接口方向。

发现流策略p1引用的ACL编号是3001，并且流策略应用的接口方向是入方向。

```
-------------------------------------------------------------
Policy applied inbound interface GigabitEthernet0/0/4

  Interface: GigabitEthernet0/0/4

  Direction: Inbound

  Policy: p1
    Classifier: c1
      Operator: OR
      Rule(s) :
        if-match acl 3001
    Behavior: b1
      Deny
-------------------------------------------------------------
```

步骤3 在ACL 3001对应的高级ACL视图下，执行命令**display this**，查看ACL规则的配置。

发现ACL 3001里配置了如下规则：

```
acl number 3001
 rule 5 permit ip source 10.164.1.0 0.0.0.255 destination 10.164.9.9 0          //允许总裁办公室访问服务器
 rule 10 deny ip destination 10.164.9.9 0          //禁止其他部门访问服务器
```

可以看到，规则中的源IP地址是总裁办公室所在的网段，目的IP地址是服务器的IP地址，符合各部门访问服务器的报文特征，说明ACL规则配置是正确的。

步骤4 分析流策略应用的接口方向

由**步骤2**可知，流策略应用的接口方向是入方向。进一步分析，各部门访问服务器的报文并不是从连接服务器的接口GE0/0/4进入Switch，而是从其他接口进入Switch并从接口GE0/0/4被转发出去（Switch收到这些报文后经过路由查询，将报文发送至出接口GE0/0/4）。

因此将引用该ACL的流策略应用在接口GE0/0/4的入方向，访问控制不会生效。若要访问控制生效，则需将调整应用方向为出方向，或者调整流策略的应用位置（在全局、各部门对应的VLAN或Switch连接各部门的接口的入方向应用）。

步骤5 调整流策略应用方向

在接口视图（GE0/0/4）下，执行命令**traffic-policy** *policy-name* **outbound**，调整流策略在接口上的应用方向为出方向。

----结束

2.14 ACL FAQ

2.14.1 ACL 中的 permit/deny 与 traffic policy 中 behavior 的 permit/deny 之间是什么关系?

ACL与traffic policy（流策略）经常组合使用。traffic policy定义符合ACL的流分类，然后再定义符合流分类的行为，即behavior，例如允许通过，拒绝通过等等。

ACL中的permit/deny与traffic policy中behavior的permit/deny组合有如下四种情况：

表 2-17 ACL 中的 permit/deny 与 traffic policy 中 behavior 的 permit/deny 组合情况

ACL	traffic policy中的behavior	匹配报文的最终处理结果
permit	permit	permit
permit	deny	deny
deny	permit	deny
deny	deny	deny

说明

在流策略模块中，设备默认报文都是permit的，如果只是要求网段之间不能访问，则只需在ACL里配置想要deny的报文的规则即可。如果最后多添加一条**rule permit**规则，则未命中该规则之前规则的所有报文都会命中此条规则，并且如果流行为behavior被配置为deny，则设备将拒绝所有命中该规则的报文通过，导致全部业务中断。

2.14.2 如何在 VLAN 下应用 ACL?

可以通过以下两种方式，将ACL与业务模块（流策略或简化流策略）绑定起来，再在VLAN下应用。

说明

以下命令行表达方式仅是示意形式，实际配置方法请参考各版本的命令行格式。

- 方式一：在VLAN下应用流策略
  a. 配置流分类
     i. 在系统视图下，执行命令**traffic classifier** *classifier-name* [**operator** { **and** | **or** }] [**precedence** *precedence-value*]，进入流分类视图。
     ii. 执行命令**if-match acl** { *acl-number* | *acl-name* }，配置ACL应用于流分类。
  b. 配置流行为
     在系统视图下，执行命令**traffic behavior** *behavior-name*，定义流行为并进入流行为视图。
  c. 配置流动作。
     报文过滤有两种流动作：**deny**或**permit**。其他流动作，请参见相应版本“配置指南-QoS”中的介绍。
  d. 配置流策略

i. 在系统视图下，执行命令**traffic policy** *policy-name*，定义流策略并进入流策略视图。

ii. 执行命令**classifier** *classifier-name* **behavior** *behavior-name*，在流策略中为指定的流分类配置所需流行为，即绑定流分类和流行为。

e. 应用流策略

在VLAN视图下，执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，应用流策略。

- 方式二：在全局下应用指定VLAN编号的简化流策略

可以在系统视图下，执行以下命令：

- 基于ACL的报文过滤
  - **traffic-filter vlan** *vlan-id* **inbound acl xxx**
  - **traffic-filter vlan** *vlan-id* **outbound acl xxx**
  - **traffic-secure vlan** *vlan-id* **inbound acl xxx**
- 基于ACL的流量监管
  - **traffic-limit vlan** *vlan-id* **inbound acl xxx**
  - **traffic-limit vlan** *vlan-id* **outbound acl xxx**
- 基于ACL的重定向

  traffic-redirect vlan *vlan-id* **inbound acl xxx**
- 基于ACL的重标记
  - **traffic-remark vlan** *vlan-id* **inbound acl xxx**
  - **traffic-remark vlan** *vlan-id* **outbound acl xxx**
- 基于ACL的流量统计
  - **traffic-statistic vlan** *vlan-id* **inbound acl xxx**
  - **traffic-statistic vlan** *vlan-id* **outbound acl xxx**
- 基于ACL的流镜像

  traffic-mirror vlan *vlan-id* **inbound acl xxx**

2.14.3 如何在接口上应用 ACL?

ACL无法直接在接口上应用，但可以通过以下两种方式，将ACL与业务模块（流策略或简化流策略）绑定起来，再在接口上应用。

说明

以下命令行表达方式仅是示意形式，实际配置方法请参考各版本的命令行格式。

- 方式一：在接口上应用流策略

a. 配置流分类

i. 在系统视图下，执行命令**traffic classifier** *classifier-name* [**operator** { **and** | **or** }] [**precedence** *precedence-value*]，进入流分类视图。

ii. 执行命令**if-match acl** { *acl-number* | *acl-name* }，配置ACL应用于流分类。

b. 配置流行为

在系统视图下，执行命令**traffic behavior** *behavior-name*，定义流行为并进入流行为视图。

c. 配置流动作。

报文过滤有两种流动作：**deny**或**permit**。其他流动作，请参见相应版本“配置指南-QoS”中的介绍。

d. 配置流策略

i. 在系统视图下，执行命令**traffic policy** *policy-name*，定义流策略并进入流策略视图。

ii. 执行命令**classifier** *classifier-name* **behavior** *behavior-name*，在流策略中为指定的流分类配置所需流行为，即绑定流分类和流行为。

e. 应用流策略

在接口视图下，执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，应用流策略。

- 方式二：在接口下应用简化流策略

可以在接口视图下，执行以下命令：

– 基于ACL的报文过滤

▪ **traffic-filter inbound acl xxx**

▪ **traffic-filter outbound acl xxx**

▪ **traffic-secure inbound acl xxx**

– 基于ACL的流量监管

▪ **traffic-limit inbound acl xxx**

▪ **traffic-limit outbound acl xxx**

– 基于ACL的重定向

traffic-redirect inbound acl xxx

– 基于ACL的重标记

▪ **traffic-remark inbound acl xxx**

▪ **traffic-remark outbound acl xxx**

– 基于ACL的流量统计

▪ **traffic-statistic inbound acl xxx**

▪ **traffic-statistic outbound acl xxx**

– 基于ACL的流镜像

traffic-mirror inbound acl xxx

2.14.4 如何查看 ACL 的生效顺序?

在任意视图下执行命令**display acl** { *acl-number* | **name** *acl-name* | **all** }、**display acl ipv6** { *acl6-number* | **name** *acl6-name* | **all** }或在ACL视图下执行命令**display this**，可以查看ACL规则的生效顺序，如**表2-18**所示。

表 2-18 ACL 的生效顺序

ACL类型	ACL的生效顺序
config模式的ACL	编号小的规则优先生效
auto模式的ACL	编号小的规则优先生效
config模式的ACL6	编号小的规则优先生效
auto模式的ACL6	排序靠前的规则优先生效，规则不一定按照编号从小到大的顺序进行排序

说明

当在流策略中引用ACL并且设备上应用了多个流策略时，如果报文同时匹配上了多个流策略中的ACL规则，则ACL的生效顺序与流策略模块的处理机制相关，具体请参见相应版本“配置指南-QoS”中的介绍。

2.14.5 应用在流策略中的 ACL 不支持对哪些报文进行过滤?

应用在流策略中的ACL不支持对上送CPU处理的协议报文进行过滤，例如：

- VRRP使用的协议报文是目的IP地址为224.0.0.18的组播报文，该报文到达设备后会被上送CPU处理，因此流策略中的ACL对该报文不生效，VRRP组内的成员交换机仍能够协商出主备关系。
- DHCP客户端为了获取合法的动态IP地址，会与服务器之间交互DHCP报文，该报文到达设备后会被上送CPU处理，因此流策略中的ACL对该报文不生效，设备无法阻止一个接口下的用户通过DHCP自动获取IP地址。
- 用户主机Ping本设备时，ICMP报文到达设备后会被上送CPU处理，因此流策略中的ACL对该报文不生效，设备无法阻止用户主机Ping本设备。

对于上送CPU处理的协议报文，可以通过在本机防攻击中的黑名单中应用ACL进行过滤，步骤如下：

1. 在系统视图下，执行命令**cpu-defend policy** *policy-name*，进入防攻击策略视图。
2. 执行命令**blacklist** *blacklist-id* **acl** *acl-number*，创建黑名单。
3. 在系统视图下，执行命令**cpu-defend-policy** *policy-name* [**global**]，应用防攻击策略；或者在槽位视图下，执行命令**cpu-defend-policy** *policy-name*，应用防攻击策略。

2.14.6 为什么配置一条流策略后，通过 display acl resource 命令查看到的 ACL 资源显示多占用两条资源

交换机为了正常运转，系统中存在一些需要上送CPU处理的报文以及用于单板间通信的报文。为了防止流策略对该两类报文产生影响，交换机会在下发流策略ACL规则前先下发两条ACL规则。

2.14.7 ACL 的 rule 中的 deny/permit 在各个业务模块里的场景是怎样的

ACL的rule中的deny/permit在各个业务模块里的场景不同，具体如下：

- 流策略
  a. 当ACL的rule配置为**permit**时，系统匹配该规则才执行流行为中的动作，流行为中的动作为**deny**则禁止匹配规则的流量通过，动作为**permit**则允许匹配规则的流量通过。
  b. 当ACL的rule配置为**deny**时，只要匹配该规则就执行丢弃报文动作，并且流行为中的具体动作不生效（流量统计和流镜像除外）。
  c. 当ACL里未配置rule时，则应用该ACL的流策略功能不生效。
- 简化流策略
  a. 当ACL的rule配置为**permit**时，设备执行简化流策略功能中的动作，如允许匹配该规则的报文通过、对匹配ACL规则的报文进行限速等。
  b. 当ACL的rule配置为**deny**时，如果将ACL应用在简化流策略的报文过滤功能中，设备会拒绝匹配该规则的报文通过；如果应用在其他简化流策略功能中，设备仍会执行简化流策略功能中的动作。
  c. 当ACL里未配置rule时，则应用该ACL的简化流策略功能不生效。
- IPSec
  a. 仅当ACL的rule配置为**permit**时，设备会对匹配该规则的报文进行IPSec保护后再发送该报文。
  b. 当ACL的rule配置为**deny**时，设备对匹配ACL规则的报文将不做IPSec保护，即不做任何处理直接转发。
  c. 当ACL未配置rule时，应用该ACL的IPSec功能不生效，即设备直接发送通过接口的报文。
- 防火墙
  a. 当ACL的rule配置为**permit**时：
     - 如果该ACL应用在**inbound**方向，则允许从优先级低到优先级高的安全区域并且匹配该规则的报文通过。
     - 如果该ACL应用在**outbound**方向，则允许从优先级高到优先级低的安全区域并且匹配该规则的报文通过。
  b. 当ACL的rule配置为**deny**时：
     - 如果该ACL应用在**inbound**方向，则拒绝从优先级低到优先级高的安全区域且匹配该规则的报文通过。
     - 如果该ACL应用在**outbound**方向，则拒绝从优先级高到优先级低的安全区域且匹配该规则的报文通过。
  c. 当ACL里未配置rule时：
     - 如果该ACL应用在**inbound**方向，则该ACL不生效，设备会拒绝从优先级低到优先级高的安全区域的所有报文通过。
     - 如果该ACL应用在**outbound**方向，则该ACL不生效，设备会允许从优先级高到优先级低的安全区域的所有报文通过。

- NAT
  a. 仅当ACL的rule配置为**permit**时，设备允许匹配该规则中指定的源IP地址使用地址池进行地址转换。
  b. 当ACL的rule配置为**deny**或ACL未配置rule时，应用该ACL的NAT功能不生效，即不允许使用地址池进行地址转换，设备根据目的地址查找路由表转发报文。
- Telnet
  a. 当ACL的rule配置为**permit**时：
     - 如果该ACL应用在**inbound**方向，则允许匹配该rule规则的其他设备访问本设备。
     - 如果该ACL应用在**outbound**方向，则允许本设备访问匹配该rule规则的其他设备。
  b. 当ACL的rule配置为**deny**时：
     - 如果该ACL应用在**inbound**方向，则拒绝匹配该rule规则的其他设备访问本设备。
     - 如果该ACL应用在**outbound**方向，则拒绝本设备访问匹配该rule规则的其他设备。
  c. 当ACL配置了rule，但来自其他设备的报文没有匹配该rule规则时：
     - 如果该ACL应用在**inbound**方向，则拒绝其他设备访问本设备。
     - 如果该ACL应用在**outbound**方向，则拒绝本设备访问其他设备。
  d. 当ACL未配置rule时：
     - 如果该ACL应用在**inbound**方向，则允许任何其他设备访问本设备。
     - 如果该ACL应用在**outbound**方向，则允许本设备访问任何其他设备。
- HTTP
  a. 当ACL的rule配置为**permit**时，则允许指定源IP地址的其他设备与本设备建立HTTP连接。
  b. 当ACL的rule配置为**deny**时，则拒绝其他设备与本设备建立HTTP连接。
  c. 当ACL配置了rule，但来自其他设备的报文没有匹配该rule规则时，则拒绝其他设备与本设备建立HTTP连接。
  d. 当ACL未配置rule时，则允许任何其他设备与本设备建立HTTP连接。
- FTP
  a. 当ACL的rule配置为**permit**时，则允许指定源IP地址的其他设备与本设备建立FTP连接。
  b. 当ACL的rule配置为**deny**时，则拒绝任何其他设备与本设备建立FTP连接。
  c. 当ACL配置了rule，但来自其他设备的报文没有匹配该rule规则时，则拒绝其他设备与本设备建立FTP连接。
  d. 当ACL未配置rule时，则允许任何其他设备与本设备建立FTP连接。
- TFTP
  a. 当ACL的rule配置为**permit**时，则允许本设备与指定源IP地址的设备建立TFTP连接。

b. 当ACL的rule配置为**deny**时，则拒绝本设备与任何其他设备建立TFTP连接。
c. 当ACL配置了rule，但来自其他设备的报文没有匹配该rule规则时，则拒绝其他设备与本设备建立TFTP连接。
d. 当ACL未配置rule时，则允许本设备与任何其他设备建立TFTP连接。

- SNMP
  a. 当ACL的rule配置为**permit**时，则允许指定源IP地址的网管访问本设备。
  b. 当ACL的rule配置为**deny**时，则拒绝其他网管访问本设备。
  c. 当ACL未配置rule时，则允许任何其他网管访问本设备。
- NTP
  a. 当ACL的rule配置为**permit**时，则使用**ntp-service access**命令配置的访问控制权限才能生效。
  b. 当ACL的rule配置为**deny**，则使用**ntp-service access**命令配置的访问控制权限不生效。
  c. 当ACL未配置rule时，则使用**ntp-service access**命令配置的访问控制权限不生效。

3 本机防攻击配置

3.1 本机防攻击简介

定义

在网络中，存在着大量针对CPU（Central Processing Unit）的恶意攻击报文以及需要正常上送CPU的各类报文。针对CPU的恶意攻击报文会导致CPU长时间繁忙的处理攻击报文，从而引发其他业务的中断甚至系统的中断；大量正常的报文也会导致CPU占用率过高，性能下降，从而影响正常的业务。

为了保护CPU，保证CPU对正常业务的处理和响应，设备提供了本机防攻击功能。本机防攻击针对的是上送CPU的报文，主要用于保护设备自身安全，保证已有业务在发生攻击时的正常运转，避免设备遭受攻击时各业务的相互影响。

功能简介

本机防攻击包括CPU防攻击、攻击溯源和端口防攻击三部分功能。各个功能从不同维度，通过不同方式实现对CPU的保护，如表3-1所示。

表 3-1 本机防攻击功能简介

功能名称	定义
CPU防攻击	CPU防攻击可以针对上送CPU的报文进行限制和约束，使单位时间内上送CPU报文的数量限制在一定的范围之内，从而保证CPU对业务的正常处理。
攻击溯源	攻击溯源能够防御DoS（Denial of Service）攻击。设备通过对上送CPU的报文进行统计分析，然后对统计的报文设置一定的阈值，将超过阈值的报文判定为攻击报文，再根据攻击报文信息找出攻击源用户或者攻击源接口，最后通过日志、告警等方式提醒管理员，以便管理员采用一定的措施来保护设备，或者直接丢弃攻击报文以对攻击源进行惩罚。
端口防攻击	端口防攻击是针对DoS攻击的另一种防御方式。它基于端口维度进行防御，可以避免攻击端口的协议报文挤占带宽，其他端口的协议报文无法正常上送CPU处理而造成业务中断。

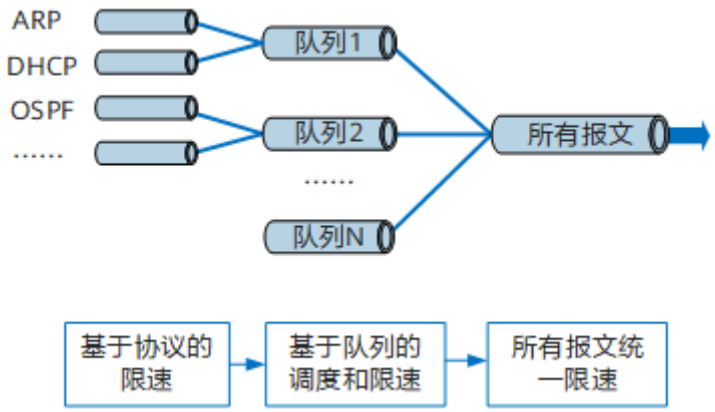
CPU 防攻击

CPU防攻击的核心部分是CPCAR（Control Plane Committed Access Rate）功能。此外，CPU防攻击还提供了动态链路保护功能、黑名单功能。

- **CPCAR**

  CPCAR通过对上送控制平面的不同业务的协议报文分别进行限速，来保护控制平面的安全。报文限速主要分为如下几类：基于每个协议的限速、基于队列的调度和限速和所有报文统一限速。如图3-1所示。

  图 3-1 上送 CPU 的报文限速分类



- **基于协议报文的限速**：是指CPCAR中可以针对每种协议单独设置承诺信息速率CIR（Committed Information Rate）和承诺突发尺寸CBS（Committed Burst Size），对于超过该速率值的协议报文，设备直接予以丢弃，从而可以保证每种协议对应的业务能够得到正常处理，同时可以保证协议之间不会相互影响，避免因为某种协议的流量过大导致其它协议报文得不到处理的情况发生。
- **基于队列的调度和限速**：协议限速之后，设备可对一类协议再分配一个队列，比如Telnet、SSH等管理类协议分为一个队列，路由协议分为一个队列，各个队列之间按照权重或优先级方式调度，保证各类业务的优先级，优先级高的业务被CPU调度的几率更大，在有冲突的情况下保证高优先级业务优先处理。同时，可以针对每个队列进行限速，限制各个队列向CPU上送报文的最大速率。对于超过最大速率的协议报文，设备会直接丢弃。
- **所有报文统一限速**：所有报文统一限速是为了限制CPU处理的报文总数，保证CPU在其正常处理能力范围内尽可能多的处理报文，而不会造成CPU异常，保证了设备CPU的正常运行。

说明

- 当三种限速方式同时生效时，设备以最小限速值进行限速。
- 以上所有CPU防攻击功能对设备的管理网口不起作用。针对设备管理网口下的网络存在的攻击，一旦攻击较为严重，可能会导致用户无法从管理网口登录并管理设备，此时建议用户对该网络上的PC（Personal Computer）进行杀毒或者重新规划组网。
- 多协议并行时，上送CPU的协议报文可能会由于超出CIR/CBS、队列上送CPU报文的最大速率、或者CPU处理的报文总数被丢弃，出现协议震荡。

- **动态链路保护功能**

  动态链路保护功能，是指设备针对基于会话的应用层数据的保护，它可以保证已有业务受到攻击时仍能够正常运行。当协议连接建立后，基于协议的限速就不再起作用，设备以动态链路保护功能设定的限速值对匹配相应Session的报文进行限速，由此保证此Session相关业务运行的可靠性和稳定性。

- **黑名单功能**

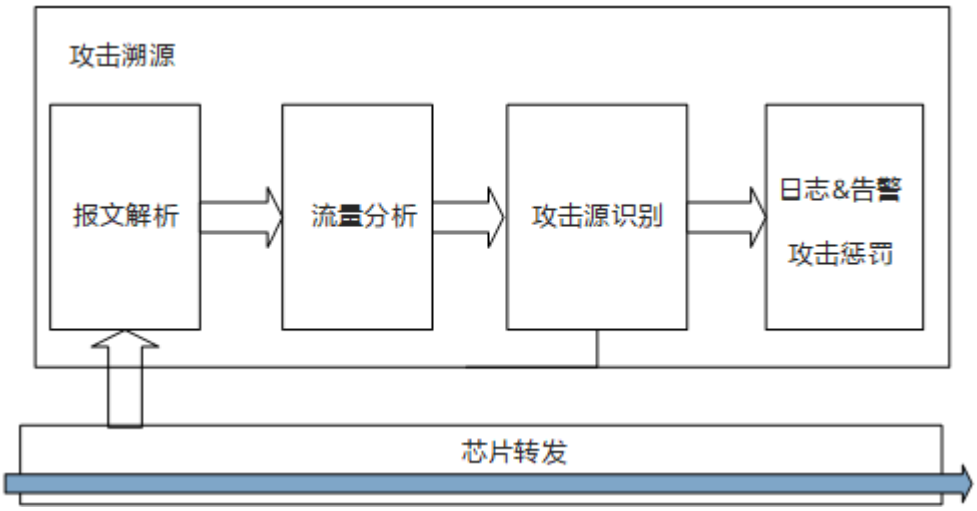
  CPU防攻击提供的黑名单功能，是指通过定义ACL来设置黑名单，设备会将后续匹配黑名单特征的报文全部丢弃，因此可以将已确定为攻击者的非法用户设置到黑名单中。

攻击溯源

如图3-2所示，攻击溯源包括报文解析、流量分析、攻击源识别和发送日志告警通知管理员以及实施惩罚四个过程。

1. 从IP地址、MAC地址以及端口三个维度进行报文解析，其中端口通过“物理端口+VLAN”标识。
2. 根据IP地址、MAC地址或者端口信息统计接收到的满足攻击溯源防范报文类型的协议报文数量。
3. 当单位时间上送CPU的报文数量超过了阈值时，就认为是攻击。
4. 当检测到攻击后，会发送日志、告警通知管理员或者直接实施惩罚，如丢弃攻击报文。

图 3-2 攻击溯源原理



此外，攻击溯源还提供了白名单功能。通过定义ACL或者直接将端口设置为攻击溯源白名单，使设备不对白名单用户的报文进行溯源，从而可以保证确定为合法用户的报文能够正常上送CPU处理。因此可以将已确定的合法用户或者端口设置到白名单中。

端口防攻击

端口防攻击的处理流程如下：

1. 基于端口维度进行报文解析，并统计收到的端口防攻击所防范的协议报文的数量。
2. 当单位时间上送CPU的报文数量超过了端口防攻击检查阈值时，就认为该端口存在攻击。
3. 检测到攻击后，设备会发送日志，并将产生攻击端口的未超出协议限速值数量的报文移入低优先级队列后再上送CPU处理，超出限速值数量的报文，则直接丢弃。关于“协议限速”和“优先级队列”的概念，请参见“**CPU防攻击**”中的说明。

   端口防攻击的限速处理方式，相比较攻击溯源的惩罚措施，对设备正常业务造成的影响更小。

此外，端口防攻击还提供了白名单功能。通过定义ACL或者直接将端口设置为端口防攻击白名单，使设备不对白名单用户的报文进行溯源和限速处理，从而可以保证确定为合法用户的报文能够正常上送CPU处理。因此可以将已确定的合法用户或者端口设置到白名单中。

3.2 本机防攻击配置注意事项

涉及网元

无需其他网元配合。

License 支持

本特性是交换机的基本特性，无需获得License许可即可应用此功能。

V200R021C00、V200R021C01 版本特性支持情况

S600-E系列交换机中所有款型均支持本机防攻击。

说明

如需了解交换机软件配套详细信息，请点击**Info-Finder**。

特性依赖和限制

- V200R011C10及之前版本，攻击溯源功能对IPv6报文不生效。
- 同时匹配用户级限速规则和用户自定义流规则的报文，设备按照较小的限速值对报文进行限速。
- 目的IP是本机的报文会上送CPU，另外一些协议报文对应的功能使能后也会上送CPU，比如OSPF、LACP使能后也会上送CPU处理。上送CPU的报文同时匹配流策略中的流分类规则，如果CPCAR和流策略动作冲突，流策略生效。

3.3 本机防攻击缺省配置

CPU防攻击缺省配置请参见**表3-2**、攻击溯源缺省配置请参见**表3-3**、端口防攻击缺省配置请参见**表3-4**。

表 3-2 CPU 防攻击缺省配置

参数	缺省值
防攻击策略	名称为**default**的防攻击策略。
黑名单	没有配置黑名单。
CAR速率抑制值	缺省情况下，设备对上送CPU的报文按照**default**策略缺省的限速值进行限速，可通过命令**display cpu-defend configuration**查看。
建立协议连接时OSPF、FTP、HTTP、IKE、IP-CLOUD、IPSEC-ESP、SSH、TELNET和TFTP协议报文的CPCAR值	缺省情况下，FTP、IPv6 FTP、HTTP、IKE、IPSEC-ESP、SSH、TELNET和TFTP协议建立连接时的承诺信息速率是1024kbit/s，承诺突发尺寸是128000bytes；OSPF协议建立连接时的承诺信息速率是512kbit/s，承诺突发尺寸是96256bytes；IP-CLOUD协议建立连接时的承诺信息速率是2048kbit/s，承诺突发尺寸是385024bytes。
动态链路保护功能	缺省情况下，FTP、IPv6 FTP、HTTP、HTTPS、IKE、IP-CLOUD、IPSEC-ESP、SSH、TELNET和TFTP协议的动态链路保护功能已使能，OSPF协议的动态链路保护功能未使能。

表 3-3 攻击溯源缺省配置

参数	缺省值
防攻击策略	名称为**default**的防攻击策略。
攻击溯源功能	已使能
攻击溯源检查阈值	60pps
攻击溯源的采样比	5
攻击溯源模式	基于源IP地址和基于源MAC地址。
攻击溯源防范的报文类型	缺省情况下，攻击溯源防范的报文类型为8021X、ARP、DHCP、DHCPv6、ICMP、ICMPv6、IGMP、MLD、ND、TCP、TCPv6、Telnet。
攻击溯源白名单	缺省情况下，没有攻击溯源的白名单。但是如果符合下面三种条件之一，无论攻击溯源功能有没有使能，设备都会自动将相应条件作为白名单的匹配规则。在使能了攻击溯源功能后，设备不会对匹配这些规则的报文作溯源处理。 ● 某个业务使用TCP协议，并且与设备成功建立TCP连接，设备不会对匹配相应源IP地址的TCP报文进行溯源处理。但是如果在1小时内，都没有相应源IP地址的TCP报文匹配，对应规则就会老化失效。 ● 通过**dhcp snooping trusted**将设备某接口配置成了DHCP信任接口，设备不会对该接口收到的DHCP报文进行溯源处理。 ● 通过**mac-forced-forwarding network-port**将设备某接口配置成了MFF的网络侧接口，设备不会对该接口收到的ARP报文进行溯源处理。
攻击溯源告警功能	未使能
攻击溯源告警阈值	60pps
攻击溯源的惩罚功能	未使能

表 3-4 端口防攻击缺省配置

参数	缺省值
防攻击策略	名称为**default**的防攻击策略。
端口防攻击功能	已使能
端口防攻击防范的报文类型	缺省情况下，端口防攻击支持防范的报文类型为ARP Request、ARP Reply、DHCP、IGMP和ND报文。

参数	缺省值
端口防攻击的检查阈值	各协议报文基于端口防攻击的检查阈值均不同，详见**3.7.4 配置端口防攻击的检查阈值**中的说明。
端口防攻击的采样比	5
端口防攻击的老化探测周期	300秒
端口防攻击的告警功能	未使能
端口防攻击白名单	缺省情况下，没有配置端口防攻击的白名单。但是如果符合下面两种条件之一，无论端口防攻击有没有使能，设备都会自动将相应条件作为白名单的匹配规则。在使能了端口防攻击后，设备不会对匹配这些规则的报文作端口防攻击处理。 • 通过**dhcp snooping trusted**将设备某接口配置成了DHCP信任接口，设备不会对该接口收到的DHCP报文进行端口防攻击处理。 • 通过**mac-forced-forwarding network-port**将设备某接口配置成了MFF的网络侧接口，设备不会对该接口收到的ARP报文进行端口防攻击处理。

3.4 本机防攻击配置任务概览

本机防攻击的配置任务如**表3-5**所示。

表 3-5 本机防攻击配置任务概览

场景	对应任务
3.5 配置CPU防攻击	在配置CPU防攻击任务中，必须首先创建防攻击策略，其余步骤是并列关系，无严格配置顺序，用户根据需要选择配置即可。防攻击策略在创建之后必须应用才能生效，但应用时机无严格限制。 **3.5.1 创建防攻击策略** **3.5.2 配置黑名单** **3.5.4 配置上送CPU报文的限速规则** **3.5.5 应用防攻击策略**

场景	对应任务
3.6 配置攻击溯源	在配置攻击溯源任务中，必须首先创建防攻击策略，并使能攻击溯源功能（默认使能）。其余步骤是并列关系，无严格配置顺序，用户根据需要选择配置即可。防攻击策略在创建之后必须应用才能生效，但应用时机无严格限制。 3.6.1 创建防攻击策略 3.6.2 使能攻击溯源功能 3.6.3 配置攻击溯源检查阈值 3.6.4 配置攻击溯源的采样比 3.6.5 配置攻击溯源的溯源模式 3.6.6 配置攻击溯源防范的报文类型 3.6.7 配置攻击溯源的白名单 3.6.8 配置攻击溯源事件上报功能 3.6.9 配置攻击溯源惩罚功能 3.6.10 应用防攻击策略
3.7 配置端口防攻击	在配置端口防攻击任务中，必须首先创建防攻击策略，并使能端口防攻击功能（默认使能）。其余步骤是并列关系，无严格配置顺序，用户根据需要选择配置即可。防攻击策略在创建之后必须应用才能生效，但应用时机无严格限制。 3.7.1 创建防攻击策略 3.7.2 使能端口防攻击功能 3.7.3 配置端口防攻击防范的报文类型 3.7.4 配置端口防攻击的检查阈值 3.7.5 配置端口防攻击的采样比 3.7.6 配置端口防攻击的老化探测周期 3.7.7 配置端口防攻击的白名单 3.7.8 配置端口防攻击事件上报功能 3.7.9 应用防攻击策略

3.5 配置 CPU 防攻击

3.5.1 创建防攻击策略

背景信息

用户需要先创建防攻击策略，然后在创建的防攻击策略中配置本机防攻击功能。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-defend policy** *policy-name*，创建防攻击策略并进入防攻击策略视图。

设备最多支持13个防攻击策略。其中名称为**default**的策略为系统自动生成的缺省策略，**default**策略默认应用到设备上，不允许删除，也不允许修改参数；其余12个允许用户创建、修改和删除。

步骤3 （可选）执行命令**description** *text*，配置防攻击策略的描述信息。

缺省情况下，防攻击策略没有配置描述信息。

----结束

3.5.2 配置黑名单

背景信息

通过创建黑名单，把符合特定特征的用户纳入到黑名单中，设备将直接丢弃黑名单用户上送的报文。设备支持通过ACL灵活设置黑名单。此外，IPv4黑名单都是报文上送到CPU再丢弃，为了进一步减小CPU的占用率，还可以在设备上配置直接在转发芯片上丢弃报文的黑名单。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤3 创建黑名单

- 执行命令**blacklist** *blacklist-id* **acl** *acl-number1*，创建IPv4黑名单。

  IPv4黑名单应用的ACL可以是基本ACL、高级ACL或二层ACL。ACL的配置方法，请参见**2 ACL配置**。

  缺省情况下，设备中没有配置IPv4黑名单。

- 执行命令**blacklist** *blacklist-id* **acl** *acl-number3* **hard-drop**，创建直接在转发芯片中丢弃匹配ACL规则报文的黑名单。

  直接在转发芯片中丢弃报文的黑名单应用的ACL只能为高级ACL，且仅对IPv4报文生效。ACL的配置方法，请参见**2 ACL配置**。

  缺省情况下，设备中没有配置直接在转发芯片中丢弃匹配ACL规则报文的黑名单。

说明

- 设备的一个防攻击策略最多可以配置8条黑名单（包括IPv4黑名单和直接在转发芯片中丢弃匹配ACL规则报文的黑名单）。
- 黑名单中应用的ACL，无论其rule配置为**permit**还是**deny**，命中该ACL的报文均会被丢弃。
- 如果ACL的rule为空，则应用该ACL的黑名单功能不生效。

----结束

3.5.3 配置白名单

背景信息

通过创建白名单，把符合特定特征的用户纳入到白名单中，设备将优先处理匹配白名单特征的报文。设备支持通过ACL灵活设置白名单。

说明

当同时配置了黑名单和白名单并应用了相同的ACL，则黑名单生效。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤3 执行命令**whitelist** *whitelist-id* **acl** *acl-number*，创建自定义白名单。

白名单应用的ACL可以是基本ACL、高级ACL或二层ACL。ACL的配置方法，请参见。

缺省情况下，设备中没有配置白名单。

说明

- 设备的一个防攻击策略最多可以配置8条白名单。
- 如果白名单中应用的ACL，其rule配置为**deny**，则命中该ACL的报文会被丢弃。
- 当白名单中应用的ACL，其rule配置为**permit**，且设备上同时配置了用户自定义流时，如果报文同时匹配白名单和用户自定义流中应用的ACL，此时用户自定义流不生效。
- 如果ACL的rule为空，则应用该ACL的白名单功能不生效。

----结束

3.5.4 配置上送 CPU 报文的限速规则

背景信息

为了减少上送CPU的报文数量，降低不同类型报文的相互影响，交换机支持对上送CPU的报文进行限速，主要分为协议报文限速、动态链路保护功能的报文速率限制。其中，动态链路保护功能的报文速率限制优先级最高。

说明

- 建议在交换机上使用默认CPCAR值。
- OSPF协议在交换机初始化时是关闭的，当协议启动未建立连接时交换机使用命令**car**设置的CPCAR值上送报文；当协议已建立连接，且使能了动态链路保护功能时，交换机则使用命令**linkup-car**设置的CPCAR值上送报文。
- 配置上送CPU报文的速率限制时速率单位是kbps，但是交换机实际按照pps进行限速。kbps转换为pps的计算公式为pps=（kbps*1024/（packet_length+20）/8）。其中packet_length表示报文长度。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 配置上送CPU报文的限速规则

在防攻击策略视图下配置协议报文限速和动态链路保护功能的报文速率限制。执行命令**cpu-defend policy** *policy-name*，进入防攻击策略视图。

- 配置协议报文限速。

  协议报文上送CPU的上送规则包括**car**和**deny**两种。当先后配置同一报文类型的**car**命令和**deny**命令时，最后配置的命令生效。

  - 执行命令**car packet-type** *packet-type* **cir** *cir-value* [**cbs** *cbs-value*]，配置对上送CPU的报文进行CPCAR限速。

    缺省情况下，协议报文的CAR速率可以通过命令**display cpu-defend configuration**查看。

  - 执行命令**deny packet-type** *packet-type*，配置对上送CPU的报文动作为丢弃。

    缺省情况下，交换机不会丢弃上送CPU的报文，而是按照**default**策略缺省的限速值对上送CPU的报文进行限速，可通过命令**display cpu-defend configuration**查看各种报文的限速值。

- 配置动态链路保护功能的报文速率限制。

  a. 执行命令**linkup-car packet-type** { **ftp** | **ftpv6** | **http** | **ike** | **ip-cloud** | **ipsec-esp** | **ospf** | **ssh** | **telnet** | **tftp** } **cir** *cir-value* [**cbs** *cbs-value*]，配置协议连接建立时协议报文的CPCAR值，包括配置承诺信息速率和承诺突发尺寸。

  缺省情况下，FTP、IPv6 FTP、HTTP、IKE、IPSEC-ESP、SSH、TELNET和TFTP协议建立连接时的承诺信息速率是1024kbit/s，承诺突发尺寸是128000bytes；OSPF协议建立连接时的承诺信息速率是512kbit/s，承诺突发尺寸是96256bytes；IP-CLOUD协议建立连接时的承诺信息速率是2048kbit/s，承诺突发尺寸是385024bytes。

  说明

  建立FTP、TFTP和SSH连接时的FTP、TFTP和SSH报文CPCAR值共用，即执行命令**linkup-car packet-type ftp cir** *cir-value* [**cbs** *cbs-value*]时，既指定了建立FTP连接时FTP报文的CPCAR值，又指定了建立TFTP和SSH连接时TFTP和SSH报文的CPCAR值。

  b. 执行命令**quit**，返回系统视图。

  c. 执行命令**cpu-defend application-apperceive enable**，使能全局动态链路保护功能。

  缺省情况下，全局动态链路保护功能已使能。

  d. 执行命令**cpu-defend application-apperceive** { **ftp** | **ftpv6** | **http** | **https** | **ike** | **ip-cloud** | **ipsec-esp** | **ospf** | **ssh** | **telnet** | **tftp** } **enable**，使能协议报文的动态链路保护功能。

  缺省情况下，FTP、IPv6 FTP、HTTP、HTTPS、IKE、IP-CLOUD、IPSEC-ESP、SSH、TELNET和TFTP协议的动态链路保护功能已使能，OSPF协议的动态链路保护功能未使能。

  说明

  使能HTTPS动态链路联动功能，能够自动增大car值（增大传输速率），保证Web网管能够和交换机高速率传输文件。

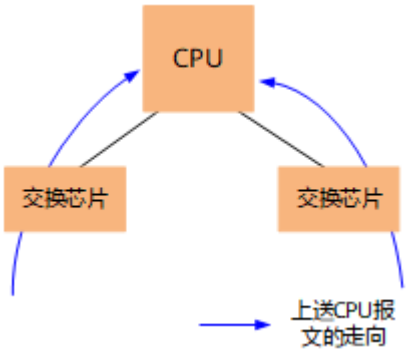
----结束

3.5.5 应用防攻击策略

背景信息

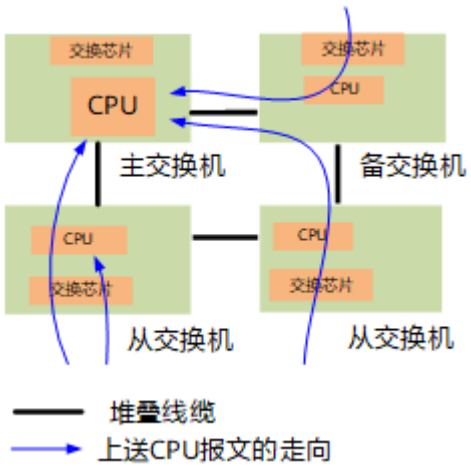
设备将报文上送CPU的过程如图3-3所示，报文先经过交换芯片，然后再上送到CPU。一般情况下，设备通过携带“global”参数，在交换芯片上应用防攻击策略。

图 3-3 上送 CPU 报文的走向



在对上送CPU的报文进行限速时，支持堆叠的设备还可以通过不携带“global”参数，在CPU上应用此防攻击策略。这个功能最主要应用于如图3-4所示的堆叠系统。如果仅在成员交换机的交换芯片进行限速，主交换机的CPU仍容易受到大量协议报文上送攻击。因为大部分协议报文经备交换机和从交换机CPU处理过后，还需要上送到主交换机的CPU。因此需要在主交换机的CPU上应用防攻击策略，对上送CPU的报文进行限速。

图 3-4 堆叠系统上送 CPU 报文的走向



操作步骤

- 在CPU上应用防攻击策略
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**cpu-defend-policy** *policy-name1*，应用防攻击策略。

说明

仅支持堆叠的设备支持该命令。

在堆叠系统中，某些协议报文不会上送到主交换机的CPU。对于此类协议报文，在CPU上应用防攻击策略时，系统会提示不支持。

仅支持CPU防攻击策略（对上送CPU的报文进行限速）应用在CPU上。其他防攻击策略不支持应用在CPU上，即配置此步骤无意义。

- 在交换芯片上应用防攻击策略
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**cpu-defend-policy** *policy-name2* **global**，应用防攻击策略。

----结束

3.5.6 检查 CPU 防攻击的配置结果

操作步骤

- 执行命令**display cpu-defend policy** [*policy-name*]，查看防攻击策略信息。
- 执行命令**display cpu-defend statistics** [**packet-type** *packet-type*] [**all** | **slot** *slot-id*]，查看上送CPU报文的统计信息。
- 执行命令**display cpu-defend applied** [**packet-type** *packet-type*] { **mcu** | **slot** *slot-id* | **all** }，查看协议报文下发到芯片后的实际CAR参数值。
- 执行命令**display cpu-defend configuration** [**packet-type** *packet-type*] { **all** | **slot** *slot-id* | **mcu** }，查看上送CPU报文的CAR的配置信息。

----结束

3.6 配置攻击溯源

3.6.1 创建防攻击策略

背景信息

用户需要先创建防攻击策略，然后在创建的防攻击策略中配置本机防攻击功能。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-defend policy** *policy-name*，创建防攻击策略并进入防攻击策略视图。

设备最多支持13个防攻击策略。其中名称为**default**的策略为系统自动生成的缺省策略，**default**策略默认应用到设备上，不允许删除，也不允许修改参数；其余12个允许用户创建、修改和删除。

步骤3 （可选）执行命令**description** *text*，配置防攻击策略的描述信息。

缺省情况下，防攻击策略没有配置描述信息。

----结束

3.6.2 使能攻击溯源功能

背景信息

网络上可能会出现大量攻击报文攻击设备的CPU，如果使能攻击溯源功能，通过分析上送CPU的报文是否会对CPU造成攻击，设备能够追溯到攻击源并以日志或告警的方式通知网络管理员，以便网络管理员采取措施对攻击源进行防御部署。缺省情况下，攻击溯源功能以日志的方式通知网络管理员。

该功能默认已使能。只有攻击溯源能在已使能的情况下，才允许配置攻击溯源的其他相关功能。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤3 执行命令**auto-defend enable**，使能攻击溯源功能。

缺省情况下，攻击溯源功能已使能。

----结束

3.6.3 配置攻击溯源检查阈值

背景信息

网络上可能会出现大量攻击报文攻击设备的CPU。通过使能攻击溯源功能并配置攻击溯源检查阈值，设备可以分析上送CPU的报文是否会对CPU造成攻击。当可能的攻击源在单位时间内发送某种协议类型的报文超过检查阈值时，设备会将可能造成攻击的报文以日志方式通知网络管理员，以便网络管理员采取措施对攻击源进行防御部署。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤3 执行命令**auto-defend threshold** *threshold*，配置攻击溯源检查阈值。

缺省情况下，攻击溯源检查阈值为60pps。

----结束

3.6.4 配置攻击溯源的采样比

背景信息

攻击溯源的实现采用抽样采取报文来辨别攻击。在辨别是否为攻击报文或者计算攻击报文速率上存在一定误差，精度为采样比。采样比的大小会影响攻击溯源的精度，采样比越小，攻击溯源的精度越高，但是相对CPU占用率就越高。

当攻击溯源采样比很低时，譬如为1，则每一个报文都能被解析到，这样设备可以很精准的辨别出攻击报文，但是因为对每个报文都进行解析和计算，会增加CPU的利用

率。所以配置合适的采样比可以在满足精度要求的同时又可以保证不过多增加CPU的占用率，用户可以根据对攻击溯源精度的要求和CPU使用率的现状合理配置采样比的值。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤3 执行命令**auto-defend attack-packet sample** *sample-value*，配置攻击溯源的采样比。

缺省情况下，攻击溯源的采样比为5。

----结束

3.6.5 配置攻击溯源的溯源模式

背景信息

当攻击溯源启动后，设备将根据配置的溯源模式进行溯源。目前，设备支持三种溯源模式，分别适用于以下场景：

- 针对三层报文的攻击，则配置基于源IP地址进行溯源。
- 针对固定源MAC地址报文的攻击，则配置基于源MAC地址进行溯源。
- 针对变换源MAC地址报文的攻击，则配置基于接口和VLAN进行溯源。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤3 执行命令**auto-defend trace-type** { **source-ip** | **source-mac** | **source-portvlan** } *，配置攻击溯源的溯源模式。

缺省情况下，攻击溯源默认开启的溯源模式为基于源IP地址和基于源MAC地址。

说明

对于攻击溯源的溯源模式为**source-ip**且惩罚措施为**error-down**的情况，如果多个接口同时接收到**source-ip**相同的攻击报文，当此报文数量超过检查阈值时，设备不会将所有接口都shutdown掉，而是先shutdown其中一个接口，然后继续进行检测。如果报文数量还是超过检查阈值，设备会再shutdown掉其中一个接口，以此类推，直到报文数量在阈值范围内。

----结束

3.6.6 配置攻击溯源防范的报文类型

背景信息

当攻击发生时，由于设备同时对多种类型的报文进行溯源，网络管理员无法区分攻击报文的具体类型。通过灵活配置攻击溯源防范的报文类型，设备将针对所配置的报文类型进行溯源。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤3 执行命令**auto-defend protocol** { **all** | { **8021x** | **arp** | **dhcp** | **dhcpv6** | **icmp** | **icmpv6** | **igmp** | **mld** | **nd** | **tcp** | **tcpv6** | **telnet** | **ttl-expired** | **udp** | **udpv6** }* }，配置攻击溯源防范的报文类型。

缺省情况下，攻击溯源防范的报文类型为8021X、ARP、DHCP、DHCPv6、ICMP、ICMPv6、IGMP、MLD、ND、TCP、TCPv6、Telnet。

说明

配置攻击溯源防范的报文类型为ICMPv6时，仅支持对目的IP是本接口IPv6地址的ICMPv6报文进行攻击溯源。

----结束

3.6.7 配置攻击溯源的白名单

背景信息

攻击溯源功能可以帮助定位攻击源，并对攻击源进行惩罚。当希望某些用户无论其是否存在攻击都不对其进行攻击溯源分析和攻击溯源惩罚时，则可以配置攻击溯源的白名单。

说明

- 如果使用ACL定义攻击溯源白名单，需要配置ACL和对应的规则。
- 如果定义了某些协议的ACL白名单，需要保证攻击溯源支持该协议，可以通过**display auto-defend configuration**命令查看攻击溯源支持的协议类型。如果定义的协议不支持，则可以使用**auto-defend protocol**命令进行配置。
- 设备ACL资源不足，可能导致白名单应用失败。
- 攻击溯源白名单中应用的ACL，无论其rule配置为**permit**还是**deny**，命中该ACL的报文均会被当作白名单合法报文，不对其进行溯源。

  如果ACL的rule为空，则应用该ACL的端口防攻击白名单功能不生效。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤3 执行命令**auto-defend whitelist** *whitelist-number* { **acl** *acl-number* | **interface** *interface-type interface-number* }，配置攻击溯源的白名单。

缺省情况下，没有攻击溯源的白名单。但是如果符合下面三种条件之一，无论攻击溯源功能有没有使能，设备都会自动将相应条件作为白名单的匹配规则。在使能了攻击溯源功能后，设备不会对匹配这些规则的报文作溯源处理。

- 某个业务使用TCP协议，并且与设备成功建立TCP连接，设备不会对匹配相应源IP地址的TCP报文进行溯源处理。但是如果在1小时内，都没有相应源IP地址的TCP报文匹配，对应规则就会老化失效。

- 通过**dhcp snooping trusted**将设备某接口配置成了DHCP信任接口，设备不会对该端口收到的DHCP报文进行溯源处理。
- 通过**mac-forced-forwarding network-port**将设备某接口配置成了MFF的网络侧接口，设备不会对该端口收到的ARP报文进行溯源处理。

上述的自动下发白名单的规则有数量限制，基于源IP地址、接口的规则总数最多能够下发16条，其中对基于源IP地址的TCP报文不进行溯源的规则最多能够下发8条。

----结束

3.6.8 配置攻击溯源事件上报功能

背景信息

当可能的攻击源在单位时间内发送某种协议类型的报文超过一定阈值时，如果希望设备能以事件上报的方式提醒网络管理员，以便管理员采取一定的措施来保护设备，则可以使能攻击溯源事件上报功能并配置攻击溯源事件上报阈值。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤3 配置攻击溯源事件上报功能

1. 执行命令**auto-defend alarm enable**，使能攻击溯源事件上报功能。

   缺省情况下，攻击溯源事件上报功能未使能。

2. 执行命令**auto-defend threshold** *threshold*，配置攻击溯源事件上报阈值。

   缺省情况下，攻击溯源事件上报阈值为60pps。

----结束

3.6.9 配置攻击溯源惩罚功能

背景信息

配置攻击溯源惩罚功能，可以使设备在识别出攻击源后，对攻击源进行一定的惩罚，丢弃与攻击源相关的报文或者将攻击报文进入的接口shutdown，从而避免攻击源继续攻击设备。

须知

如果配置攻击溯源的惩罚措施是将攻击报文进入的接口shutdown，则会造成设备业务的中断，接口下合法的用户会受牵连，请谨慎使用。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤3 执行命令**auto-defend action** { **deny** [**timer** *time-length*] | **error-down** }，使能攻击溯源的惩罚功能，并指定惩罚措施。

缺省情况下，未使能攻击溯源的惩罚功能。

说明

设备不对攻击溯源的白名单用户进行攻击溯源的惩罚。

----结束

3.6.10 应用防攻击策略

背景信息

创建防攻击策略之后，必须将策略在系统视图下应用，否则防攻击策略不会生效。

操作步骤

- 应用防攻击策略
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**cpu-defend-policy** *policy-name* **global**，应用防攻击策略。

----结束

3.6.11 检查攻击溯源的配置结果

操作步骤

- 执行命令**display auto-defend attack-source** [**history** [**begin** *begin-date begin-time*] [**slot** *slot-id*] | [**slot** *slot-id*] [**detail**]]，查看攻击源信息。
- 执行命令**display auto-defend configuration** [**cpu-defend policy** *policy-name*]，查看防攻击策略的攻击溯源配置信息。
- 执行命令**display cpu-defend policy** [*policy-name*]，查看防攻击策略的信息。
- 执行命令**display auto-defend whitelist** [**slot** *slot-id*]，查看攻击溯源的白名单信息。

----结束

3.7 配置端口防攻击

3.7.1 创建防攻击策略

背景信息

用户需要先创建防攻击策略，然后在创建的防攻击策略中配置本机防攻击功能。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-defend policy** *policy-name*，创建防攻击策略并进入防攻击策略视图。

设备最多支持13个防攻击策略。其中名称为**default**的策略为系统自动生成的缺省策略，**default**策略默认应用到设备上，不允许删除，也不允许修改参数；其余12个允许用户创建、修改和删除。

步骤3 （可选）执行命令**description** *text*，配置防攻击策略的描述信息。

缺省情况下，防攻击策略没有配置描述信息。

----结束

3.7.2 使能端口防攻击功能

背景信息

如果某个端口下存在攻击者发起DoS攻击，从该端口上送CPU处理的大量恶意攻击报文会挤占带宽，导致其他端口的协议报文无法正常上送CPU处理，从而造成业务中断。

通过部署基于端口的防攻击功能，可以有效控制从端口上送CPU处理的报文数量，以防御针对CPU的DoS攻击。

该功能默认已使能。只有端口防攻击功能在已使能的情况下，才允许配置端口防攻击的其他相关功能。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤3 执行命令**auto-port-defend enable**，使能基于端口的防攻击功能。

缺省情况下，已使能基于端口的防攻击功能。

----结束

3.7.3 配置端口防攻击防范的报文类型

背景信息

缺省情况下，设备会对端口收到的所有可防范的协议报文的速率进行计算，并对该端口的攻击报文进行溯源和限速处理。如果管理员发现设备检测出的多种攻击报文类型中，仅有少部分才是真正的攻击报文，则可以删除不必要的防范报文类型，避免设备因对过多的协议报文进行限速而影响正常业务。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤3 执行命令**auto-port-defend protocol** { **all** | { **arp-request** | **arp-reply** | **dhcp** | **igmp** | **nd** } * }，配置端口防攻击可以防范的报文类型。

缺省情况下，端口防攻击支持防范的报文类型为ARP Request、ARP Reply、DHCP、IGMP和ND报文。

----结束

3.7.4 配置端口防攻击的检查阈值

背景信息

基于端口的防攻击功能在已使能的情况下，设备会对端口收到的可防范协议报文的速率进行计算。如果该值超过了端口防攻击检查阈值，就认为该端口存在攻击，设备将对该端口的攻击报文进行溯源和限速处理，并通过日志的方式通知网络管理员。设备的限速处理方式为：对于未超出限速值（该值等同于防攻击策略里协议报文的CPCAR值。关于CPCAR值的概念，请参见**配置上送CPU报文的分类限速上送规则**中的说明）的报文，设备将其移入低优先级队列后再上送CPU处理；对于超出限速值的报文，设备直接丢弃。

网络管理员可以根据设备上的业务运行情况，配置合理的端口防攻击检查阈值。如果因为端口防攻击导致过多的协议报文未被CPU及时处理而影响了该协议对应的正常业务，则可以适当放大该协议报文的端口防攻击检查阈值；如果因为CPU处理过多个别协议报文而影响了其他协议报文对应的业务，则可以适当调小该协议报文的端口防攻击检查阈值。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤3 执行命令**auto-port-defend protocol** { **all** | **arp-request** | **arp-reply** | **dhcp** | **igmp** | **nd** } **threshold** *threshold*，配置基于端口防攻击的协议报文检查阈值。

缺省情况下，各协议报文基于端口防攻击的检查阈值分别为：

报文类型	基于端口防攻击的检查阈值
arp-request	30pps
arp-reply	30pps
dhcp	30pps
igmp	60pps
nd	30pps

----结束

3.7.5 配置端口防攻击的采样比

背景信息

在基于端口的防攻击实现中，设备通过抽样采取报文来辨别攻击。在辨别报文是否为攻击报文，或者计算攻击报文速率时，存在一定的误差。通过配置采样比，可以有效控制防攻击的精度，避免因误差太大而达不到防攻击的效果。

采样比越小，防攻击的精度越高，同时CPU使用率也相对越高。当端口防攻击采样比很低时，例如为1，则设备会对每一个报文都进行解析，从而可以很精准的辨别出攻击报文。但是因为对每个报文都进行解析和计算，会导致CPU的使用率大幅度提高，影响正常业务。因此请根据对端口防攻击的精度要求和CPU使用率的现状，合理配置采样比的值。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤3 执行命令**auto-port-defend sample** *sample-value*，配置基于端口防攻击的协议报文采样比。

缺省情况下，基于端口防攻击的协议报文采样比为5，即每5个报文采样1个报文。

----结束

3.7.6 配置端口防攻击的老化探测周期

背景信息

基于端口的防攻击功能在已使能的情况下，设备一旦检测到存在攻击的端口，就会在老化探测周期内（假设为T秒）对该端口的攻击报文持续进行溯源和限速处理。达到T秒之后，设备会再次计算该端口收到协议报文的速率，如果该值超过了检查阈值（即存在攻击），则继续对其进行溯源和限速处理；反之，则停止溯源和限速。

老化探测周期过短，设备频繁启动端口报文速率的检测，会消耗CPU资源；反之，老化探测周期过长，设备长时间进行端口防攻击限速，可能会导致过多的协议报文未被CPU及时处理而影响该协议对应的正常业务。因此，网络管理员可以根据设备CPU使用率的现状和业务运行情况，配置合理的端口防攻击老化探测周期。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤3 执行命令**auto-port-defend aging-time** *time*，配置端口防攻击的老化探测周期。

缺省情况下，端口防攻击的老化探测周期为300秒。

----结束

3.7.7 配置端口防攻击的白名单

背景信息

基于端口的防攻击功能默认已使能，因此设备会计算所有端口的可防范协议报文的速率，并对所有端口被检测出的攻击报文进行溯源和限速处理。如果有特殊业务需求，例如网络侧的端口通常会收到大量协议报文，然而这些协议报文一般为合法报文，此时通过将该端口或者该端口连接的其他网络节点加入端口防攻击白名单，使设备不对其溯源和限速，可以避免因网络侧大量协议报文得不到CPU及时处理而影响正常业务。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤3 执行命令**auto-port-defend whitelist** *whitelist-number* { **acl** *acl-number* | **interface** *interface-type interface-number* }，配置端口防攻击的白名单。

设备上最多可以配置16条白名单。

白名单应用的ACL可以是基本ACL、高级ACL或二层ACL。ACL的配置方法，请参见**2 ACL配置**。

缺省情况下，没有配置端口防攻击的白名单。但是如果符合下面两种条件之一，无论端口防攻击有没有使能，设备都会自动将相应条件作为白名单的匹配规则。在使能了端口防攻击后，设备不会对匹配这些规则的报文作端口防攻击处理。

- 通过**dhcp snooping trusted**将设备某接口配置成了DHCP信任接口，设备不会对该接口收到的DHCP报文进行端口防攻击处理。
- 通过**mac-forced-forwarding network-port**将设备某接口配置成了MFF的网络侧接口，设备不会对该接口收到的ARP报文进行端口防攻击处理。

上述的自动下发白名单的规则有数量限制，基于源IP地址、接口的规则总数最多能够下发16条。

说明

端口防攻击白名单中应用的ACL，无论其rule配置为**permit**还是**deny**，命中该ACL的报文均会被当作白名单合法报文，不对其进行溯源和限速。

如果ACL的rule为空，则应用该ACL的端口防攻击白名单功能不生效。

----结束

3.7.8 配置端口防攻击事件上报功能

背景信息

如果某个端口下存在DoS攻击，从该端口上送CPU处理的大量恶意攻击报文会挤占带宽，导致其他端口的协议报文无法正常上送CPU处理，从而造成业务中断。此时可以配置端口防攻击事件上报功能，当端口下协议报文数量超过检查阈值时，设备以事件（event）上报的方式提醒网络管理员，以便管理员采取一定的措施来保护设备。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤3 配置端口防攻击事件上报功能

1. 执行命令**auto-port-defend alarm enable**，使能端口防攻击事件上报功能。

   缺省情况下，端口防攻击事件上报功能未使能。

2. 执行命令**auto-port-defend protocol** { **all** | **arp-request** | **arp-reply** | **dhcp** | **igmp** | **nd** } **threshold** *threshold*，配置基于端口防攻击的协议报文检查阈值。

   缺省情况下，各协议报文基于端口防攻击的检查阈值分别为：

报文类型	基于端口防攻击的检查阈值
arp-request	30pps
arp-reply	30pps
dhcp	30pps
igmp	60pps
nd	30pps

----结束

3.7.9 应用防攻击策略

背景信息

创建防攻击策略之后，必须将策略在系统视图下应用，否则防攻击策略不会生效。

操作步骤

- 应用防攻击策略
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**cpu-defend-policy** *policy-name* **global**，应用防攻击策略。

----结束

3.7.10 检查端口防攻击的配置结果

操作步骤

- 执行命令**display auto-port-defend attack-source** [**slot** *slot-id*]，查看端口防攻击的溯源信息。
- 执行命令**display auto-port-defend configuration**，查看端口防攻击的配置信息。

- 执行命令**display auto-port-defend whitelist** [**slot** *slot-id*]，查看端口防攻击的白名单信息。

----结束

3.8 维护本机防攻击

3.8.1 清除上送 CPU 报文统计信息

背景信息

当需要对上送CPU的报文重新进行统计时，可以在用户视图下执行以下命令，清除之前的统计信息。

须知

清除上送CPU报文统计信息后，以前的统计信息将无法恢复，请于清除之前仔细确认。

操作步骤

步骤1 执行命令**reset cpu-defend statistics** [**packet-type** *packet-type*] { **all** | **slot** *slot-id* }，清除上送CPU报文统计信息。

----结束

3.8.2 清除攻击溯源信息

背景信息

当需要对攻击溯源信息重新进行统计时，可以在系统视图下执行以下命令，清除之前的统计信息。

须知

清除攻击溯源信息后，以前的统计信息将无法恢复，请于清除之前仔细确认。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**reset auto-defend attack-source** [**history**] [**slot** *slot-id*]，清除攻击溯源信息。

步骤3 执行命令**reset auto-defend attack-source trace-type** { **source-mac** [*mac-address*] | **source-ip** [*ipv4-address* | **ipv6** *ipv6-address*] | **source-portvlan** [**interface** *interface-type interface-number* **vlan-id** *vlan-id* [**cvlan-id** *cvlan-*

id]] } [**slot** *slot-id*]，清除基于源MAC地址、基于源IP地址或基于源端口+VLAN三种方式的攻击溯源计数。

----结束

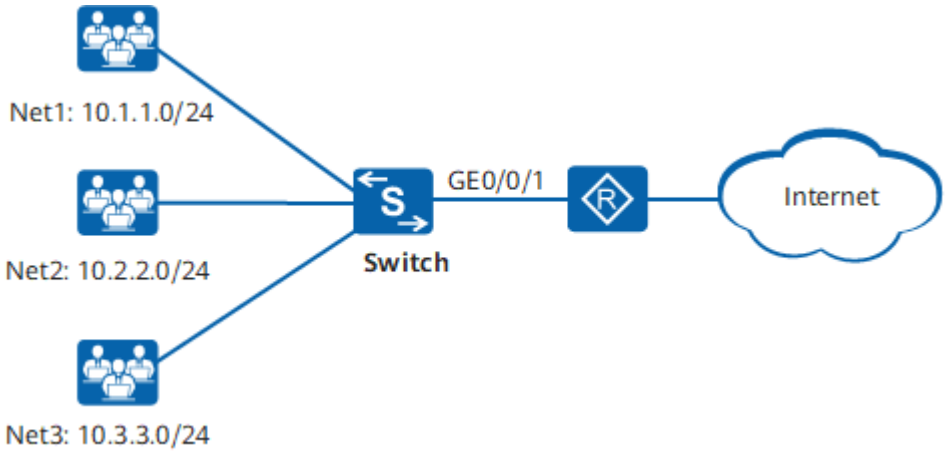
3.9 配置本机防攻击示例

组网需求

如图3-5所示，位于不同网段的用户通过Switch接入Internet。由于接入了大量用户，因此Switch的CPU会处理大量收到的协议报文。如果存在恶意用户发送大量攻击报文，会导致CPU使用率过高，影响正常业务。

- 管理员希望能够实时了解CPU的安全状态。当确定CPU受到攻击时，Switch能够及时通知管理员，并采取一定的安全措施来保护CPU。
- 管理员发现Switch收到了大量的ARP Request报文，因处理这些ARP Request报文导致CPU使用率大幅度提高，希望能够降低CPU使用率，防止影响正常业务。
- 管理员发现Net1网段中的用户经常会发生攻击行为，希望能够阻止该网段用户接入网络。Net2网段的用户为固定合法用户。
- 管理员发现Net2网段的用户为固定合法用户，希望该网段用户的报文能够优先上送CPU处理。
- 管理员需要以FTP方式上传文件到Switch，希望管理员主机与Switch之间FTP数据能够可靠、稳定地传输。

图 3-5 配置本机防攻击示例组网图



配置思路

采用如下的思路在Switch上配置本机防攻击：

1. 配置攻击溯源检查、告警和惩罚功能，使设备在检测到攻击源时通过告警方式通知管理员，并能够对攻击源自动实施惩罚。
2. 将Net2网段中的用户列入攻击溯源白名单，不对其进行攻击溯源分析和攻击溯源惩罚。

3. 配置ARP Request报文的CPCAR值，将ARP Request报文上送CPU处理的速率限制在更小的范围内，减少CPU处理ARP Request报文对正常业务的影响。
4. 将Net1网段中的攻击者列入黑名单，禁止Net1网段用户接入网络。
5. 将Net2网段中的用户列入CPU防攻击白名单，实现Net2网段用户报文的优先处理。
6. 配置FTP协议建立连接时FTP报文上送CPU的速率限制（FTP协议的动态链路保护功能缺省情况下已使能，这里无需再次使能），实现管理员主机与Switch之间文件数据传输的可靠性和稳定性。

操作步骤

步骤1 配置上送CPU报文的过滤规则

定义ACL规则。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] acl number 2001
[Switch-acl-basic-2001] rule permit source 10.1.1.0 0.0.0.255
[Switch-acl-basic-2001] quit
[Switch] acl number 2002
[Switch-acl-basic-2002] rule permit source 10.2.2.0 0.0.0.255
[Switch-acl-basic-2002] quit
```

步骤2 配置防攻击策略

创建防攻击策略。

```
[Switch] cpu-defend policy policy1
```

配置攻击溯源检查功能。

```
[Switch-cpu-defend-policy-policy1] auto-defend enable
```

使能攻击溯源告警功能。

```
[Switch-cpu-defend-policy-policy1] auto-defend alarm enable
```

配置攻击溯源白名单。

说明

建议将周边合法服务器地址、网络互连端口、网络管理设备等加入白名单。

```
[Switch-cpu-defend-policy-policy1] auto-defend whitelist 1 acl 2002
```

配置攻击溯源惩罚措施为丢弃攻击报文。

说明

在配置攻击溯源惩罚措施之前，请确保设备受到了非法攻击，避免因误丢弃大量正常协议报文而影响正常业务。

```
[Switch-cpu-defend-policy-policy1] auto-defend action deny
```

配置ARP Request报文的CPCAR值为120kbit/s。

```
[Switch-cpu-defend-policy-policy1] car packet-type arp-request cir 120
Warning: Improper parameter settings may affect stable operating of the system. Use this command under assistance of Huawei engineers. Continue? [Y/N]:y
```

配置CPU防攻击黑名单。

```
[Switch-cpu-defend-policy-policy1] blacklist 1 acl 2001
```


配置CPU防攻击白名单。
```
[Switch-cpu-defend-policy-policy1] whitelist 1 acl 2002
```

配置FTP协议建立连接时FTP报文上送CPU的速率限制为5000kbit/s。
```
[Switch-cpu-defend-policy-policy1] linkup-car packet-type ftp cir 5000
[Switch-cpu-defend-policy-policy1] quit
```

步骤3 全局应用防攻击策略
```
[Switch] cpu-defend-policy policy1 global
[Switch] quit
```

步骤4 验证配置结果

查看攻击溯源的配置信息。
```
<Switch> display auto-defend configuration
 ------------------------------------------------------------------------------
 Name  : policy1
 Related slot : <0>
 auto-defend                    : enable
 auto-defend attack-packet sample : 5
 auto-defend threshold            : 60 (pps)
 auto-defend alarm                : enable
 auto-defend trace-type           : source-mac source-ip
 auto-defend protocol             : arp icmp dhcp igmp tcp telnet 8021x
 auto-defend action               : deny (Expired time : 300 s)
 auto-defend whitelist 1          : acl number 2002
 ------------------------------------------------------------------------------
```

查看配置的防攻击策略的信息。
```
<Switch> display cpu-defend policy policy1
 Related slot : <0>
 Configuration :
   Whitelist 1 ACL number : 2002
   Blacklist 1 ACL number : 2001
   Car packet-type arp-request : CIR(120)  CBS(22560)
   Linkup-car packet-type  ftp : CIR(5000)  CBS(940000)
```

----结束

配置文件

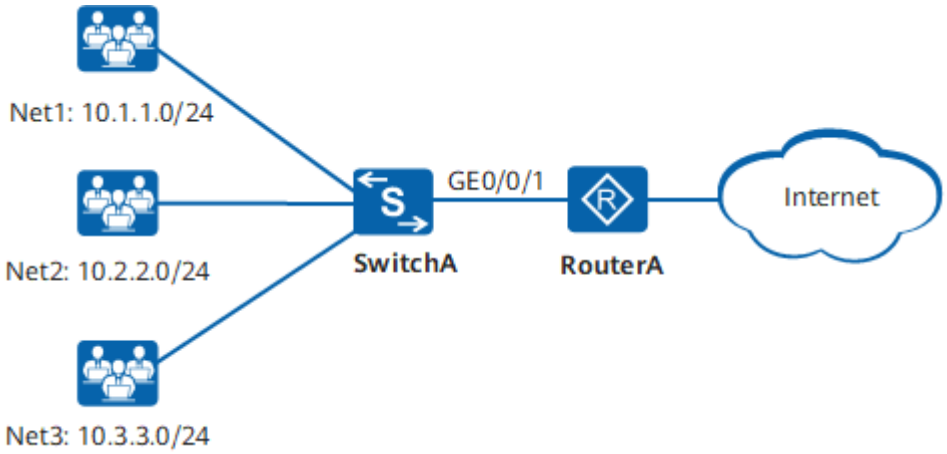
Switch的配置文件
```
#
sysname Switch
#
acl number 2001
 rule 5 permit source 10.1.1.0 0.0.0.255
acl number 2002
 rule 5 permit source 10.2.2.0 0.0.0.255
#
cpu-defend policy policy1
 whitelist 1 acl 2002
 blacklist 1 acl 2001
 car packet-type arp-request cir 120 cbs 22560
 linkup-car packet-type ftp cir 5000 cbs 940000
 auto-defend alarm enable
 auto-defend action deny
 auto-defend whitelist 1 acl 2002
#
cpu-defend-policy policy1 global
#
return
```


3.10 配置攻击溯源示例

组网需求

如图3-6所示，位于不同网段的用户通过SwitchA接入Internet。由于接入的用户数量较多，SwitchA经常因为处理大量的ARP报文导致CPU使用率过高，影响正常业务。管理员希望设备能够对上送CPU的ARP报文进行分析，将超过阈值的报文判定为攻击报文，并找出攻击源用户或者源接口，通过日志、告警的方式通知管理员，以便管理员采取一定的安全措施来保护CPU。此外，Net2网段的用户为固定合法用户，需要确保该网段用户的ARP报文能够正常上送CPU。

图 3-6 配置攻击溯源示例组网图



配置思路

1. 配置攻击溯源检查功能、检查阈值和防范的报文类型，对超过一定阈值的ARP报文进行攻击溯源分析。
2. 配置基于源IP地址和源MAC地址的攻击溯源模式。
3. 配置攻击溯源告警和惩罚功能，使设备在检测到攻击源时通过告警方式通知管理员，并且指定攻击溯源的惩罚措施为丢弃攻击报文。
4. 将Net2网段中的用户列入攻击溯源白名单，不对其进行攻击溯源分析和攻击溯源惩罚。

操作步骤

步骤1 配置防攻击策略。

创建防攻击策略。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] cpu-defend policy policy1
```

配置攻击溯源检查功能。

```
[SwitchA-cpu-defend-policy-policy1] auto-defend enable
```

配置攻击溯源检查阈值。

```
[SwitchA-cpu-defend-policy-policy1] auto-defend threshold 60
```

配置攻击溯源防范的报文类型。

```
[SwitchA-cpu-defend-policy-policy1] auto-defend protocol arp
```

配置攻击溯源的溯源模式。

```
[SwitchA-cpu-defend-policy-policy1] auto-defend trace-type source-ip source-mac
```

使能攻击溯源告警功能。

```
[SwitchA-cpu-defend-policy-policy1] auto-defend alarm enable
```

使能攻击溯源惩罚功能。

说明

在配置攻击溯源惩罚措施之前，请确保设备受到了非法攻击，避免因误丢弃大量正常协议报文而影响正常业务。

```
[SwitchA-cpu-defend-policy-policy1] auto-defend action deny timer 300
[SwitchA-cpu-defend-policy-policy1] quit
```

配置攻击溯源白名单。

说明

建议将周边合法服务器地址、网络互连端口、网络管理设备等加入白名单。

```
[SwitchA] acl number 2001
[SwitchA-acl-basic-2001] rule permit source 10.2.2.0 0.0.0.255
[SwitchA-acl-basic-2001] quit
[SwitchA] cpu-defend policy policy1
[SwitchA-cpu-defend-policy-policy1] auto-defend whitelist 1 acl 2001
[SwitchA-cpu-defend-policy-policy1] quit
```

步骤2 全局应用防攻击策略。

```
[SwitchA] cpu-defend-policy policy1 global
[SwitchA] quit
```

步骤3 验证配置结果。

查看攻击溯源的配置信息。

```
<SwitchA> display auto-defend configuration
-------------------------------------------------------------------------------
Name  : policy1
Related slot : <0>
auto-defend                    : enable
auto-defend attack-packet sample : 5
auto-defend threshold            : 60 (pps)
auto-defend alarm                : enable
auto-defend trace-type           : source-mac source-ip
auto-defend protocol             : arp
auto-defend action               : deny (Expired time : 300 s)
auto-defend whitelist 1          : acl number 2001
-------------------------------------------------------------------------------
```

等待一段时间后，查看攻击源信息。

```
<SwitchA> display auto-defend attack-source
 Attack Source User Table (slot 0):
 -------------------------------------------------------------------------------
 MacAddress       InterfaceName              Vlan:Outer/Inner    TotalPackets
 -------------------------------------------------------------------------------
 00e0-fc12-3456   GigabitEthernet0/0/1       10                  1395
 -------------------------------------------------------------------------------
 Total: 1
```



```
Attack Source Port Table (slot 0):
------------------------------------------------------------
InterfaceName              Vlan:Outer/Inner    TotalPackets
------------------------------------------------------------
GigabitEthernet0/0/1       10                  605
------------------------------------------------------------
Total: 1
```

----结束

配置文件

SwitchA的配置文件

```
#
sysname SwitchA
#
acl number 2001
 rule 5 permit source 10.2.2.0 0.0.0.255
#
cpu-defend policy policy1
 auto-defend alarm enable
 auto-defend protocol arp
 auto-defend action deny
 auto-defend whitelist 1 acl 2001
#
cpu-defend-policy policy1 global
#
return
```

3.11 本机防攻击常见配置错误

3.11.1 攻击溯源功能不生效

故障现象

配置了攻击溯源功能后，攻击溯源功能不生效。

常见原因

本类故障的常见原因主要包括：

- 配置攻击溯源的防攻击策略没有被应用
- 攻击溯源的检测阈值过大造成设备不认为该报文为攻击报文

操作步骤

步骤1 确定配置攻击溯源的防攻击策略是否被应用

1. 在系统视图下执行命令**display this**，检查是否配置了**cpu-defend-policy**命令。
2. 或者执行命令**display auto-defend configuration**查看“Name”字段取值（防攻击策略名）和“Related slot”取值（应用位置）。
3. 如果没有配置，则在系统视图下执行命令**cpu-defend-policy**进行配置，否则继续执行以下检查。

步骤2 检查攻击溯源检测阈值是否过大

执行命令**display auto-defend configuration**查看“auto-defend threshold”字段取值。如果攻击溯源的检查阈值较大，则在防攻击策略视图下执行命令**auto-defend threshold**命令减小攻击溯源的检查阈值。

----结束

3.11.2 黑名单功能不生效

故障现象

配置了黑名单功能后，黑名单功能不生效。

常见原因

本类故障的常见原因主要包括：

- 黑名单的规则与报文不匹配
- ACL资源不足造成黑名单应用失败

操作步骤

步骤1 执行命令**display cpu-defend policy** *policy-name*，查看防攻击策略相关信息。

步骤2 从防攻击策略显示信息中可查看到黑名单对应的ACL，然后执行命令**display acl** *acl-number*，检查ACL中的规则是否与业务需求一致。

步骤3 如果不一致，请在对应ACL视图下执行命令**rule**，修改规则，使之与业务需求一致。如果一致，可能是设备ACL资源不足造成黑名单应用失败。

----结束

3.12 本机防攻击 FAQ

3.12.1 如何定位常见的攻击，解决办法包括哪些

常见的攻击，可以通过以下步骤进行定位：

1. 清除上送CPU的报文统计计数。
2. 等待1分钟后，查看这段时间内上送CPU和丢弃的协议报文数量，如ICMP、TTL Expired、SSH、FTP等。如果上送或丢弃的报文数量较大，则可认为是攻击，如ICMP攻击、TTL Expired攻击、SSH流量攻击、FTP攻击等。
3. 通过攻击溯源来确认攻击源。

对于这些攻击，可以在确认攻击源之后，通过在**cpu-defend policy**中配置黑名单功能来禁止该源的攻击上送控制平面，也可以通过配置**auto-defend**的自动惩罚功能来丢弃攻击报文。

另外，对于ICMP攻击，还可以针对该攻击源设备的ICMP报文速率进行抑制；对于SSH、FTP攻击，还可以通过配置流策略以丢弃攻击报文。

3.13 防攻击报文类型汇总

当前防攻击报文类型仅作为参考，请以设备实际显示为准。设备支持的防攻击报文类型查看，请执行命令**display cpu-defend configuration slot** *slot-id*。

S600-E 系列

报文类型	报文解释
8021x	802.1X报文
arp-reply	ARP响应报文
arp-request	ARP请求报文
bpdu	BPDU报文
bpdu-tunnel	BPDU Tunnel报文
capwap-ctrl	CAPWAP控制报文
dhcp-client	DHCP客户端报文
dhcp-server	DHCP服务器报文
eth-ring	环网协议报文
fib-hit	命中路由报文
ftp	FTP报文
https	HTTPS报文
icmp	ICMP报文
igmp	IGMP报文
ip-cloud	NETCONF报文
kerberos	Kerberos报文
lacp	LACP报文
ldt	LDT报文
lnp	LNP报文
nd	IPv6邻居发现协议报文
ospf	OSPF报文
pppoe	PPPOE报文
rip	RIP报文
sip	SIP协议报文
telnet	Telnet报文

报文类型	报文解释
vbst	VBST协议报文
vbst-trunk	VBST Eth-trunk协议报文

4 MFF 配置

4.1 MFF 简介

定义

MFF（MAC-Forced Forwarding）是实现同一广播域内的用户之间二层隔离和三层互通的一种解决方案。

MFF通过ARP代答机制，截获用户发送的ARP请求报文，回复包含网关MAC地址的ARP应答报文。设备通过这种方式将用户流量强制引向网关，达到二层隔离和三层互通的作用。

目的

在以太网中，由于用户之间的业务不同，需要对用户之间进行二层隔离。在不同业务的用户之间有时又需要进行通信，所以需要实现用户之间的三层互通。在传统的以太网组网方案中，为了实现不同用户之间的二层隔离和三层互通，通常采用在设备上划分VLAN的方法。但是存在以下几种不足：

- 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；
- 为实现用户之间三层互通，需要为每个VLAN规划不同的IP网段，并配置VLANIF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。

而MFF作为实现同一广播域内的用户之间二层隔离和三层互通的一种解决方案，既可以充分利用以太网的广播域优势，又没有IP地址浪费和规模限制。MFF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。

说明

设备上部署了MFF功能时，为了避免MFF模块处理过多的过路ARP报文（即ARP报文的目的IP地址不是本设备的IP地址）导致CPU负荷过重，则可以在设备上部署基于全局、VLAN和接口的ARP报文限速功能。具体配置参见**配置ARP报文限速（针对全局、VLAN和接口）**。

受益

- 实现不同业务用户之间的二层隔离，不用担心用户之间的恶意攻击。
- 通过网关转发实现三层互通，达到网关实施计费的功能。
- 更安全的网络环境，更稳定的网络服务。

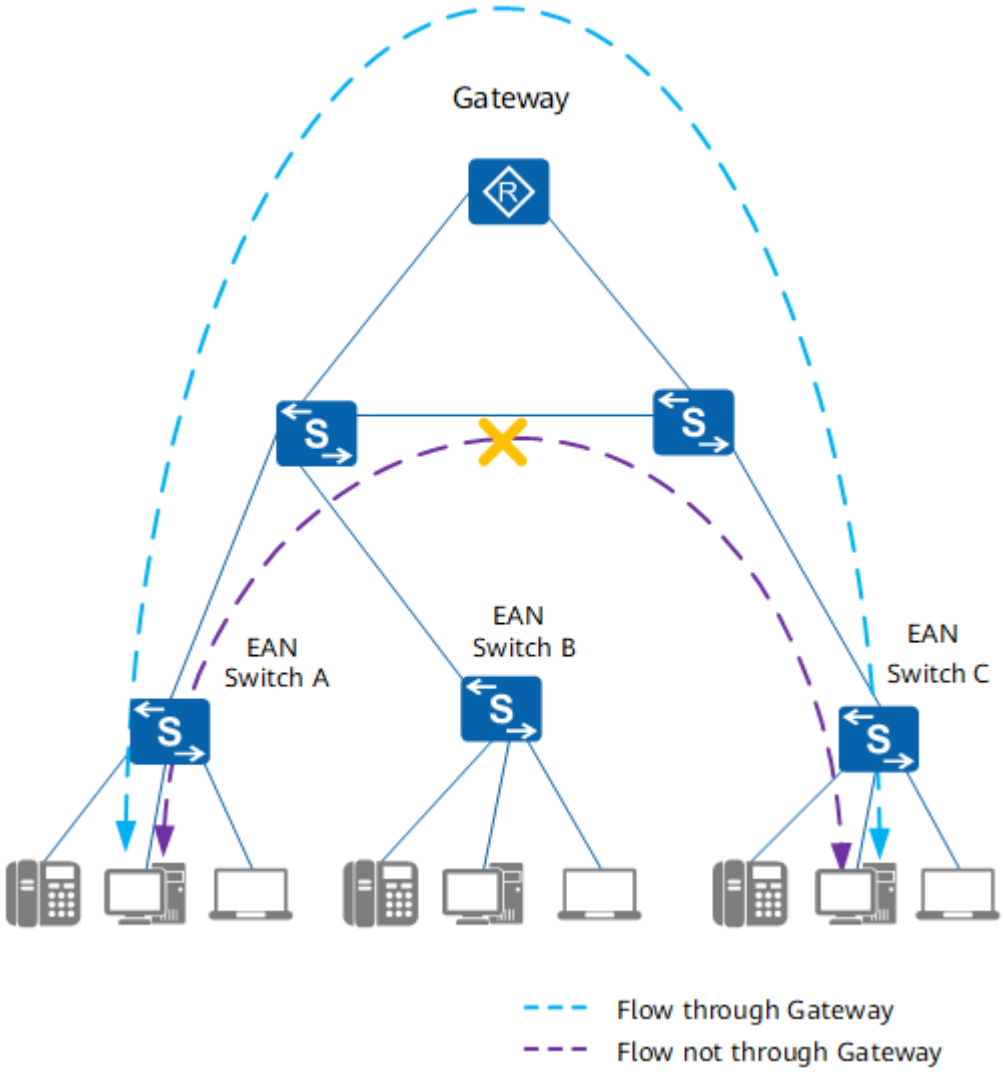
4.2 MFF 原理描述

工作机制

如**图4-1**所示为以太接入网MFF方案的应用场景，这些应用场景中往往需要网关统一管理和计费客户端的数据流量。在EAN（Ethernet Access Nodes）上部署MFF，可以使客户端的数据流量首先经过网关再通过三层转发至其它用户，实现了二层流量的隔离，同时达到监控和计费的目的。

MFF环境下用户的二层隔离和三层互通是通过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。关于**ARP代答机制**，具体请参见实现功能中的介绍。

图 4-1 MFF 方案的应用场景



接口角色

在部署MFF的设备（后续简称MFF设备）上存在两种接口角色：用户接口和网络接口。

用户接口是指连接终端用户的接口。

用户接口对于不同报文的处理方式如下：

- 丢弃IGMP Query报文，允许其他IGMP协议报文通过；允许DHCP报文通过。
- ARP报文上送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，其他报文将被丢弃；若没有学习到网关MAC地址，目的MAC地址作为网关MAC地址的单播报文也将被丢弃。
- 组播数据报文和广播数据报文都不允许通过。

网络接口是指连接其他网络设备如接入交换机、汇聚交换机或者网关的接口。

网络接口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。

实现功能

MFF解决方案主要包括以下几个方面的内容：获取网关和用户信息、ARP代答、网关探测和用户在线探测。

- **获取网关和用户信息**

  用户获取IP地址的方式有两种：静态配置IP地址和通过DHCP协议动态获取IP地址，对应这两种方式，MFF设备获取的网关信息也分为两种情况：手动配置网关IP地址和DHCP Snooping动态定制网关。

  - 手动配置网关IP地址

    如果用户的IP地址是静态配置的，MFF设备则无法通过DHCP报文来获取网关IP地址，因此需要在MFF设备上手动配置该IP。配置静态网关（即静态用户的网关）的IP地址后，MFF设备通过捕获用户侧在线用户的ARP请求报文，进而触发生成或者更新包含用户信息的MFF表项。如果在未学习到网关MAC地址的情况下收到用户的ARP请求，MFF设备将不会转发该ARP请求，而以用户的IP地址和MAC地址为源信息构造ARP请求报文发给网关，并从网关回应的ARP应答报文中学习网关MAC地址。

  - DHCP Snooping动态定制网关

    如果用户的IP地址是通过DHCP协议动态获取的，MFF设备将从DHCP Snooping表中获取用户的IP地址和MAC地址信息，并解析来自网络端口的DHCP ACK报文中的OPTION121或OPTION3字段，从中获取网关IP。之后，MFF设备再以用户的IP地址和MAC地址为源信息构造ARP请求报文发给网关，并从网关回应的ARP应答报文中学习网关MAC地址。

    若用户被授权访问多个网关，则当MFF设备收到来自该用户的非网关的ARP请求后，会使用第一个网关的MAC地址代答。而MFF设备收到对网关的ARP请求时则会用该网关的MAC地址代答。

- **ARP代答**

  MFF设备捕获用户发出的ARP请求报文，并以网关的MAC地址作为源MAC构造ARP应答报文发送给用户，使用户的ARP表记录的IP地址都与网关的MAC对应，由此强制用户发出的所有数据报文在二层转发中都以网关为目的地，从而使数据流量监控、计费得以实施，提高网络的安全性。

  对于网关请求用户的ARP报文，MFF设备则会以用户的MAC地址进行代答。

  对于网络侧非网关设备（如网络中部署的DHCP Server、组播服务器等应用服务器）请求用户的ARP报文，默认情况下，MFF设备直接以用户的MAC地址进行代答，此时非网关设备发送给用户的报文无需经过网关转发。如果MFF设备使能了网关探测用户状态的ARP报文透传功能，MFF设备则使用网关的MAC地址进行代答，此时非网关设备发送给用户的报文需要经过网关转发。关于网关探测用户状态的ARP报文透传功能，具体请参见“用户在线探测”中的介绍。

- **网关探测**

  为了及时感知网关MAC地址的变化，MFF支持网关定时探测功能。当网关探测功能开启后（该功能默认已开启），MFF设备每隔30秒会扫描已记录的网关信息，并使用某一个用户的信息构造ARP请求报文发向网络端，再从网关的ARP应答中获取网关的MAC地址。如果MAC地址发生变化，MFF设备将立即更新网关信息，同时广播免费ARP报文到用户端，用于及时刷新用户的网关地址映射关系。

说明

若VLAN中没有记录任何用户，那么MFF设备将不会向网关发送ARP请求报文，直到有一个用户上线为止。

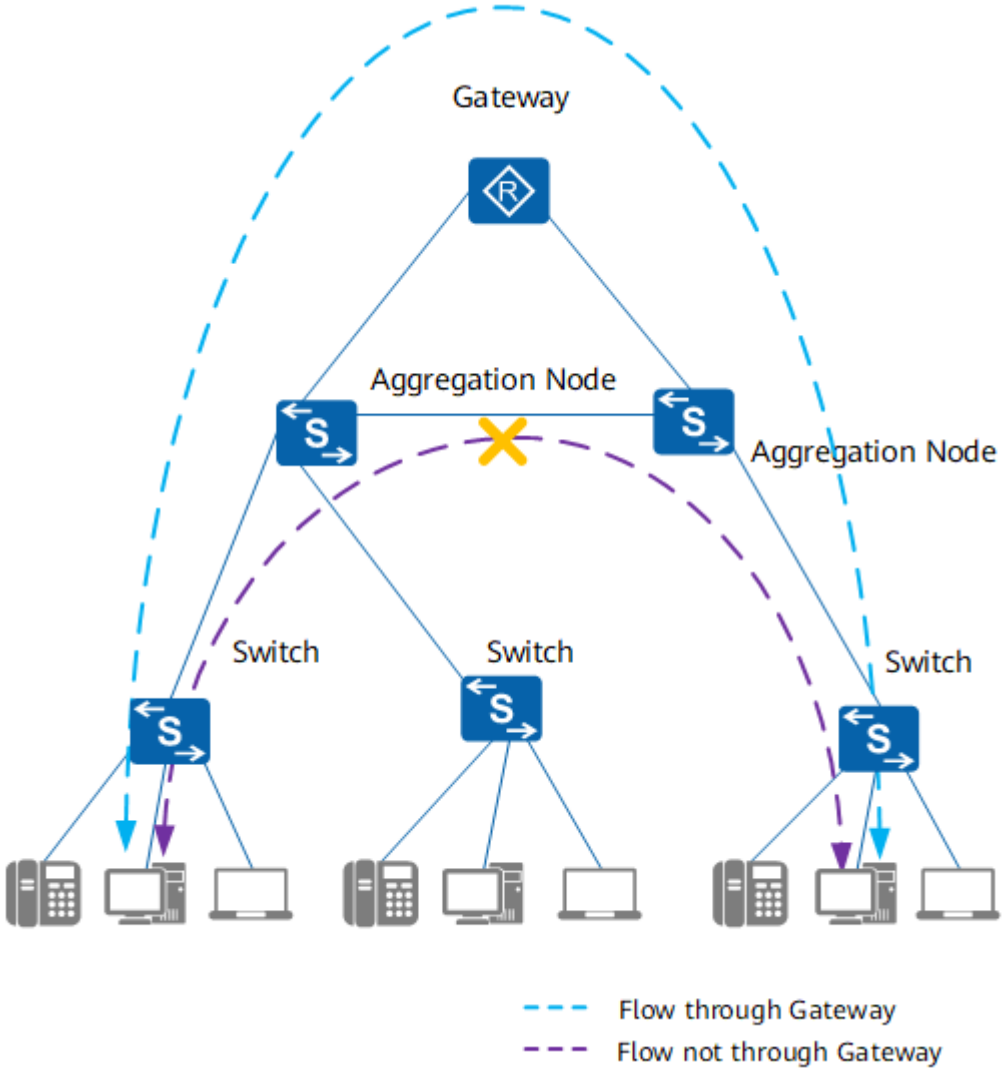
- **用户在线探测**

  当网关用来计费时，如果按照时间计费，网关需要通过ARP请求来感知用户某个时刻是否在线。MFF默认的处理方式是：网关对于用户的请求会被配置MFF特性的MFF设备直接代答，只要MFF表项未老化，MFF设备始终能代答网关的请求，网关获得的信息是用户始终在线，但实际上用户可能已经下线。为了避免这种情况，可以配置网关探测用户状态的ARP报文透传功能，使MFF设备透传网关发给用户的ARP请求报文，不再进行ARP代答。如果网关收不到用户发出的ARP应答报文，则可以判断该用户已下线。

4.3 MFF 应用场景

MFF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，构造源MAC为网关MAC地址的ARP应答报文发给用户。通过这种方式，强制用户将所有流量发送到网关，使网关可以监控数据流量，防止用户之间的恶意攻击，更好地保障网络部署的安全性。

图 4-2 通过 MFF 实现二层网络隔离



如图4-2所示，用户流量不能从二层汇聚节点直接通过，而是从网关通过，实现了二层隔离。

4.4 MFF 配置注意事项

涉及网元

无需其他网元配合。

License 支持

本特性是交换机的基本特性，无需获得License许可即可应用此功能。

V200R021C00、V200R021C01 版本特性支持情况

S600-E系列交换机中所有款型均支持MFF。

说明

如需了解交换机软件配套详细信息，请点击**Info-Finder**。

特性依赖和限制

- 使能MFF的VLAN数量规格为32。
- 当使能MFF的VLAN数量达到规格数时，如果设备仍存在可用的ACL资源，可以继续在其他VLAN下使能VLAN内的MFF功能。
- 交换机使能MFF功能时，如果网关设备开启了VRRP，交换机下连接的用户只能看到网关的VRRP虚MAC和虚IP。在VLAN视图下执行命令**mac-forced-forwarding server** *server-ip* **&<1-10>**时，*server-ip*配置为网关的实IP地址。

4.5 配置 MFF

前置任务

在配置MFF的基本功能之前，如果存在动态分配IP的用户，需要完成以下任务：

- 使能DHCP Snooping功能。
- 配置DHCP Snooping信任接口。

4.5.1 使能全局 MFF 功能

背景信息

只有使能了全局MFF功能，才能进行MFF其他功能的配置。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**mac-forced-forwarding enable**，使能全局MFF功能。缺省情况下，未使能全局MFF功能。

----结束

4.5.2 配置 MFF 的网络接口

背景信息

VLAN内的MFF功能生效的前提是，至少存在一个网络接口属于该VLAN，因此需要配置MFF的网络接口。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入连接网络设备侧的接口视图。

步骤3 执行命令**mac-forced-forwarding network-port**，配置当前接口为网络接口。

缺省情况下，接口为用户接口。

----结束

4.5.3 使能 VLAN 内的 MFF 功能

背景信息

在MFF组网中，只有使能VLAN内的MFF功能，才能对VLAN内的其他MFF特性进行配置。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**vlan** *vlan-id*，进入VLAN视图。

步骤3 执行命令**mac-forced-forwarding enable**，使能VLAN内的MFF功能。

缺省情况下，未使能VLAN内的MFF功能。

说明

由于MFF和VLANIF互斥，如果配置了以上特性，则不能使能VLAN内的MFF功能。

设备支持MFF和1:1映射方式的Vlan Mapping结合，可以配置在Mapping后的VLAN下。

当使能MFF的VLAN数量达到规格数时，如果设备仍存在可用的ACL资源，可以继续在其他VLAN下使能VLAN内的MFF功能。

----结束

4.5.4 （可选）配置静态网关地址

背景信息

应用于存在静态配置IP地址用户的场景中。对于静态配置IP地址的用户，MFF设备无法通过DHCP报文来动态获取网关信息，在此情况下，可以通过配置MFF静态网关IP地址来访问网关。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**vlan** *vlan-id*，进入VLAN视图。

步骤3 执行命令**mac-forced-forwarding static-gateway** *ip-address* &<1-16>，配置静态网关IP地址。

缺省情况下，未配置VLAN中的静态网关。

----结束

4.5.5 （可选）使能网关定时探测功能

背景信息

在实际网络场景中，如果网关MAC地址发生了变化，MFF设备未能及时感知，会导致业务长时间不通。为了避免上述问题的出现，可以使能网关定时探测功能。使能该功能后（该功能默认已开启），MFF设备每隔*interval-time*秒会扫描已记录的网关信息，并使用某一个用户的信息构造ARP请求报文发向网络端，再从网关的ARP应答中获取网关的MAC地址。如果MAC地址发生变化，MFF设备将立即更新网关信息，同时广播免费ARP报文到用户端，用于及时刷新用户的网关地址映射关系。

说明

为了防止网关失效导致用户间流量阻塞，在使能网关定时探测功能后，如果连续5次探测都没有收到回应，设备会认为该网关已经失效，并将该网关的MAC地址清空。在探测期间，如果修改了网关探测时间间隔，探测次数累加不清零。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**vlan** *vlan-id*，进入VLAN视图。

步骤3 执行命令**mac-forced-forwarding gateway-detect** [**interval** *interval-time*]，使能网关定时探测功能及配置网关探测时间间隔。

缺省情况下，已使能网关定时探测功能，网关探测时间间隔为30秒。

----结束

4.5.6 （可选）配置网络中部署的服务器 IP 地址

背景信息

在网络中除了网关外可能还部署了应用服务器，比如DHCP Server、组播服务器、其他业务服务器等。此时可以在部署MFF特性的设备上指定应用服务器的IP地址，设置用户可以访问的应用服务器列表。

说明

通常在应用服务器与用户在同一个VLAN内时才需要配置此功能。

- 当MFF设备的网络侧接口收到指定应用服务器的ARP请求时，默认情况下，MFF设备会以用户MAC地址进行代答，这样服务器发送给用户的报文无需经过网关转发；
- 如果MFF设备上同时配置了透传网关探测用户状态的报文功能，MFF设备则会以网关MAC地址进行代答，此时服务器发送给用户的报文需要经过网关转发。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**vlan** *vlan-id*，进入VLAN视图。
3. 执行命令**mac-forced-forwarding server** *server-ip* & <1–10>，配置网络中部署的服务器IP地址。

缺省情况下，未配置服务器IP地址。

4.5.7 （可选）配置透传网关探测用户状态的 ARP 报文

背景信息

在MFF组网中，网关可能用来计费，如果按照时间计费，网关需要感知用户某个时刻是否在线。MFF默认的处理方式是：网关对于用户的请求会被配置MFF特性的MFF设备直接代答，只要MFF表项未老化，MFF设备始终能代答网关的请求，网关获得的信息是用户始终在线，但实际上用户可能已经下线。

为了避免这种情况，可以配置网关探测用户状态的ARP报文透传功能，使MFF设备透传网关发给用户的ARP请求报文，不再进行ARP代答。如果网关收不到用户发出的ARP应答报文，则可以判断该用户已下线，从而达到时刻关注用户在线状态并准确计费的目的。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**vlan** *vlan-id*，进入VLAN视图。
3. 执行命令**mac-forced-forwarding user-detect transparent**，使能透传网关探测用户状态的ARP报文功能。

   缺省情况下，未使能透传网关探测用户状态的ARP报文功能。

4.5.8 （可选）配置转发网关发送的 ARP 报文到哑终端功能

背景信息

对于MFF设备连接哑终端（哑终端不主动发送ARP请求报文，或者发送ARP请求报文的时间间隔较长）的场景，当设备上MFF表项老化后，需要将网关的ARP报文透传给哑终端，否则可能导致网关上哑终端用户的ARP表项老化，影响用户业务。因此对于MFF设备连接哑终端的场景，需要在MFF设备上配置转发网关发送的ARP报文到哑终端的功能。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**vlan** *vlan-id*，进入VLAN视图。

步骤3 执行命令**mac-forced-forwarding dumb-terminal-compatible**，配置设备转发网关发送的ARP报文到哑终端功能。

缺省情况下，未配置设备转发网关发送的ARP报文到哑终端功能。

说明

配置设备发送ARP报文到哑终端功能后，需要执行**mac-forced-forwarding static-gateway** *ip-address* &<1-16>命令配置静态网关IP地址，否则功能不生效。

----结束

4.5.9 （可选）配置 IPv6 报文隔离功能

背景信息

IPv4的网络环境中用户发送IPv6报文时，IPv6报文会在VLAN下广播，引起用户之间互相学习到对方的MAC，导致MFF的用户隔离功能失效。

此时配置IPv6报文隔离功能，可以在端口丢弃用户发送的IPv6报文，防止上述情况的发生。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**vlan** *vlan-id*，进入VLAN视图。

步骤3 执行命令**mac-forced-forwarding ipv6-isolate**，配置在连接用户的MFF设备的入端口上丢弃用户的IPv6报文，防止IPv6报文在VLAN内广播。

缺省情况下，在连接用户的MFF设备的入端口上不丢弃用户的IPv6报文。

----结束

4.5.10 （可选）配置 ARP 触发 MFF 功能

背景信息

在数据中心场景中，用户与虚拟机服务器通过MFF在EAN设备上进行二层隔离。当虚拟机在不同的服务器之间进行了迁移，并且迁移前后连接在不同EAN设备的情况下，可能出现虚拟机迁移后连接的EAN设备上存在备份的绑定关系表以及迁移前连接的EAN设备没有能够及时删除MFF表项，从而使用户与服务器之间的二层隔离、三层互通的安全性无法得到保障。此时可以通过配置ARP触发MFF功能解决该问题。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**vlan** *vlan-id*，进入VLAN视图。

步骤3 执行命令**mac-forced-forwarding arp-trigger**，使能从用户侧收到ARP报文后添加或更新MFF表项功能。

缺省情况下，未使能从用户侧收到ARP报文后添加或更新MFF表项功能。

步骤4 执行命令**mac-forced-forwarding network-port-arp-trigger**，使能从网络侧收到用户的ARP报文后删除MFF表项功能。

缺省情况下，未使能从网络侧收到用户的ARP报文后删除MFF表项功能。

----结束

4.5.11 （可选）配置丢弃用户侧的 IGMP query 报文

背景信息

缺省情况下，VLAN内使能MFF后设备会丢弃用户侧发送的IGMP query报文。但是在同时使能了IGMP snooping的情况下，由于IGMP snooping的优先级较高，设备会处理用户侧接收到的IGMP query报文，这样会造成IGMP query在VLAN内广播。IGMP query报文被转发到网络侧后，会影响设备上游的IGMP查询器的选举，进而导致组播功能出现异常。

在此场景中，配置丢弃用户侧的IGMP query报文功能，可以防止上述情况的发生。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**vlan** *vlan-id*，进入VLAN视图。

步骤3 执行命令**mac-forced-forwarding igmp-query discard**，配置丢弃用户侧的IGMP query报文。

缺省情况下，在VLAN内同时使能MFF和IGMP snooping的情况下，未使能丢弃用户侧发送的IGMP query报文的功能。

----结束

4.5.12 检查 MFF 的配置结果

操作步骤

- 执行**display mac-forced-forwarding network-port**命令，查看MFF网络接口。
- 执行**display mac-forced-forwarding vlan** *vlan-id*命令，查看VLAN下MFF功能的相关配置信息。

----结束

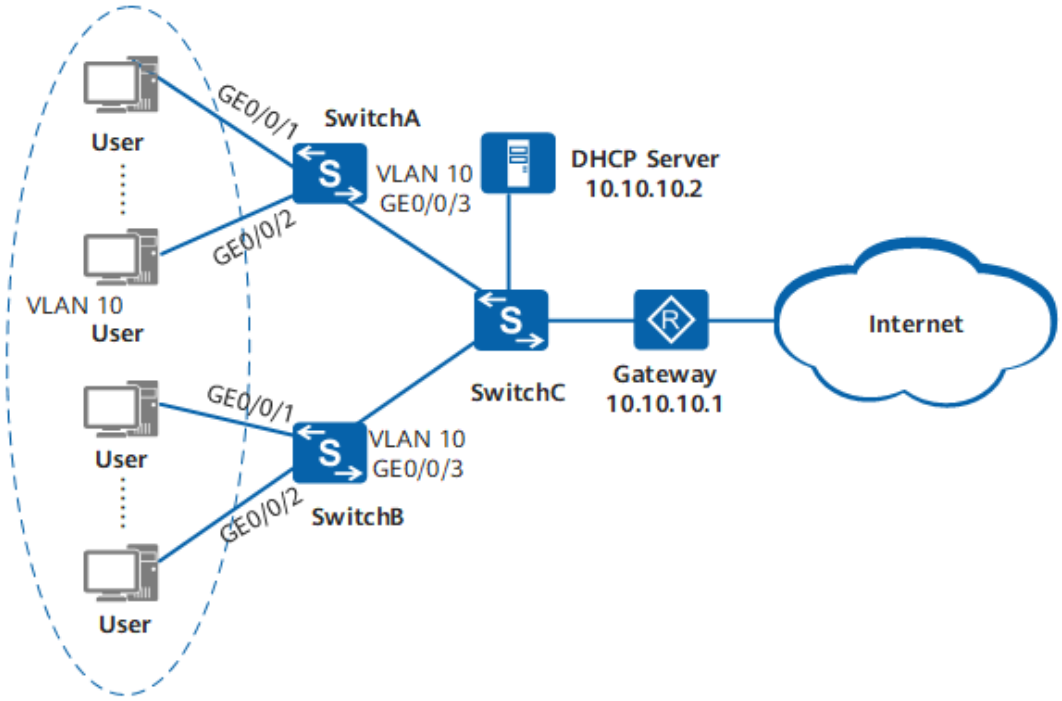
4.6 MFF 配置举例

4.6.1 配置 MFF 功能实现用户的二层隔离和三层互通示例

组网需求

如图4-3所示，企业某部门使用SwitchA和SwitchB作为用户主机的接入设备，SwitchC作为汇聚设备。管理员希望位于VLAN10内的用户主机在接入设备上二层隔离，并且只能通过网关进行三层通信，从而达到网关对用户流量进行监控的目的。由于主机数量较多，为了便于统一管理IP地址，该部门的用户主机均通过DHCP方式获取IP地址，管理员希望应用服务器（DHCP Server）访问用户的流量可以二层透传给用户，避免网关因转发过多应用服务器的流量而影响网关性能。

图 4-3 配置 MFF 功能组网图



配置思路

采用如下的思路进行配置：

1. 在SwitchA和SwitchB上配置DHCP Snooping功能，为二层隔离和三层互通功能的实现提供包含IP地址、MAC地址、VLAN等动态用户的信息。
2. 在SwitchA和SwitchB上配置MFF功能，强制用户流量由网关进行转发，实现用户主机之间的二层隔离和三层互通，同时达到网关对用户流量进行监控的目的。
3. 在SwitchA和SwitchB上配置DHCP Server的IP地址，使DHCP Server访问用户的流量可以二层透传给用户，从而减轻网关的负担。

说明

本举例仅包括SwitchA和SwitchB上的配置，SwitchC（只需配置二层透传即可）、DHCP Server和网关Gateway的配置这里不做相关说明。

操作步骤

步骤1 创建VLAN并配置各接口加入VLAN

在SwitchA上创建VLAN10，并将接口GE0/0/1、GE0/0/2、GE0/0/3加入到VLAN10中。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 10
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type access
[SwitchA-GigabitEthernet0/0/1] port default vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
```

```
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type access
[SwitchA-GigabitEthernet0/0/2] port default vlan 10
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 10
[SwitchA-GigabitEthernet0/0/3] quit
```

在SwitchB上创建VLAN10，并将接口GE0/0/1、GE0/0/2、GE0/0/3加入到VLAN10中。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchB
[SwitchB] vlan batch 10
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type access
[SwitchB-GigabitEthernet0/0/1] port default vlan 10
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] interface gigabitethernet 0/0/2
[SwitchB-GigabitEthernet0/0/2] port link-type access
[SwitchB-GigabitEthernet0/0/2] port default vlan 10
[SwitchB-GigabitEthernet0/0/2] quit
[SwitchB] interface gigabitethernet 0/0/3
[SwitchB-GigabitEthernet0/0/3] port link-type trunk
[SwitchB-GigabitEthernet0/0/3] port trunk allow-pass vlan 10
[SwitchB-GigabitEthernet0/0/3] quit
```

步骤2 配置DHCP Snooping功能

在SwitchA上全局使能DHCP Snooping功能。

```
[SwitchA] dhcp enable
[SwitchA] dhcp snooping enable
```

因所有用户主机均位于VLAN10，所以在SwitchA上使能VLAN10的DHCP Snooping功能。

```
[SwitchA] vlan 10
[SwitchA-vlan10] dhcp snooping enable
[SwitchA-vlan10] quit
```

在SwitchA上配置接口GE0/0/3为DHCP Snooping信任接口。

```
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] dhcp snooping trusted
[SwitchA-GigabitEthernet0/0/3] quit
```

在SwitchB上全局使能DHCP Snooping功能。

```
[SwitchB] dhcp enable
[SwitchB] dhcp snooping enable
```

因所有用户主机均位于VLAN10，所以在SwitchB上使能VLAN10的DHCP Snooping功能。

```
[SwitchB] vlan 10
[SwitchB-vlan10] dhcp snooping enable
[SwitchB-vlan10] quit
```

在SwitchB上配置接口GE0/0/3为DHCP Snooping信任接口。

```
[SwitchB] interface gigabitethernet 0/0/3
[SwitchB-GigabitEthernet0/0/3] dhcp snooping trusted
[SwitchB-GigabitEthernet0/0/3] quit
```

步骤3 配置MFF功能

在SwitchA上全局使能MFF功能。


```
[SwitchA] mac-forced-forwarding enable
```

配置SwitchA的接口GE0/0/3为MFF的网络接口。

```
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] mac-forced-forwarding network-port
[SwitchA-GigabitEthernet0/0/3] quit
```

在SwitchA上使能VLAN10的MFF功能。

```
[SwitchA] vlan 10
[SwitchA-vlan10] mac-forced-forwarding enable
```

在SwitchB上全局使能MFF功能。

```
[SwitchB] mac-forced-forwarding enable
```

配置SwitchB的接口GE0/0/3为MFF的网络接口。

```
[SwitchB] interface gigabitethernet 0/0/3
[SwitchB-GigabitEthernet0/0/3] mac-forced-forwarding network-port
[SwitchB-GigabitEthernet0/0/3] quit
```

在SwitchB上使能VLAN10的MFF功能。

```
[SwitchB] vlan 10
[SwitchB-vlan10] mac-forced-forwarding enable
```

步骤4 配置DHCP Server的IP地址

在SwitchA上配置DHCP Server的IP地址。

```
[SwitchA-vlan10] mac-forced-forwarding server 10.10.10.2
[SwitchA-vlan10] quit
```

在SwitchB上配置DHCP Server的IP地址。

```
[SwitchB-vlan10] mac-forced-forwarding server 10.10.10.2
[SwitchB-vlan10] quit
```

步骤5 验证配置结果

以SwitchB为例，执行命令**display mac-forced-forwarding vlan 10**查看VLAN10下的MFF配置情况。

```
[SwitchB] display mac-forced-forwarding vlan 10
[Vlan 10] MFF host total count = 1
--------------------------------------------------------------------------------
Servers        10.10.10.2
--------------------------------------------------------------------------------
User IP        User MAC              Gateway IP      Gateway MAC
--------------------------------------------------------------------------------
10.10.10.11    0001-0001-0001        10.10.10.1      0002-0002-0001
--------------------------------------------------------------------------------
```

以SwitchB为例，执行命令**display mac-forced-forwarding network-port**查看MFF的网络接口信息。

```
[SwitchB] display mac-forced-forwarding network-port
--------------------------------------------------------------------------------
VLAN ID                Network-ports
--------------------------------------------------------------------------------
VLAN 10                GigabitEthernet0/0/3
--------------------------------------------------------------------------------
```

此时如果将网关连接SwitchC的接口**shut down**，则VLAN10内的任意两个用户主机之间不能Ping通，而将该接口恢复为正常状态后，用户就能相互Ping通，即表明已实现用户的二层隔离和三层互通，MFF功能已生效。

----结束

配置文件

- SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 10
#
mac-forced-forwarding enable
#
dhcp enable
#
dhcp snooping enable
#
vlan 10
 dhcp snooping enable
 mac-forced-forwarding enable
 mac-forced-forwarding server 10.10.10.2
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
 mac-forced-forwarding network-port
 dhcp snooping trusted
#
return
```

- SwitchB的配置文件

```
#
sysname SwitchB
#
vlan batch 10
#
mac-forced-forwarding enable
#
dhcp enable
#
dhcp snooping enable
#
vlan 10
 dhcp snooping enable
 mac-forced-forwarding enable
 mac-forced-forwarding server 10.10.10.2
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/3
```



```
 port link-type trunk
 port trunk allow-pass vlan 10
 mac-forced-forwarding network-port
 dhcp snooping trusted
#
return
```

4.7 MFF 常见配置错误

4.7.1 配置 MFF 功能后用户不能上网

故障现象

设备配置完MFF功能后，下接的用户不能上网。

操作步骤

步骤1 执行命令**display mac-forced-forwarding vlan** *vlan-id*，检查MFF生成信息。

- 如果输出信息中User IP和User MAC字段的显示内容为空，表示主机信息未生成，请执行步骤2。
- 如果输出信息中Gateway MAC字段的显示内容为空，表示没有学习到网关MAC，请执行步骤3。

步骤2 MFF主机信息未生成排查过程

1. 检查用户绑定表项是否生成

用户类型	使用命令	输出处理
动态用户	**display dhcp snooping user-bind vlan** *vlan-id*	– 如果输出信息中没有用户IP对应的绑定表项，请执行步骤b。 – 如果输出信息中有用户IP对应的绑定表项，说明用户已成功上线，请执行步骤c。
静态用户	**display dhcp static user-bind vlan** *vlan-id*	– 如果输出信息中没有对应用户IP的绑定表项，执行步骤b。 – 如果输出信息中有对应用户IP的绑定表项，说明用户已成功上线，请执行步骤c。

2. 检查用户相关配置是否正确

用户类型	检查项	检查方法	输出处理
动态用户	用户接口是否使能DHCP Snooping功能	进入用户接口视图，执行命令**display this**，检查是否有**dhcp snooping enable**命令。	如果没有，请在接口视图下执行命令**dhcp snooping enable**配置。此命令也可以在VLAN视图下执行，需保证用户接口加入到该VLAN中。
	网络接口是否为“信任”状态	进入网络接口视图，执行命令**display this**，检查是否有**dhcp snooping trusted**命令。	如果没有，请在接口视图下执行命令**dhcp snooping trusted**配置。也可以在VLAN视图下执行命令**dhcp snooping trusted**配置。需保证接口已加入该VLAN。
	用户是否成功上线	在确保用户接口使能DHCP Snooping功能、网络接口为“信任”状态后，执行命令**display dhcp snooping user-bind vlan** *vlan-id*，查看DHCP Snooping表项。	如果不存在用户IP对应的DHCP Snooping表项，说明用户没有成功上线，请参考**9.13.1 开启DHCP Snooping功能后部分用户无法正常获取IP地址**或**9.13.2 开启DHCP Snooping功能后所有用户无法正常获取IP地址**解决用户不能成功上线问题。

用户类型	检查项	检查方法	输出处理
静态用户	静态网关地址是否正确配置	进入配置MFF的VLAN视图，执行命令**display this**，检查是否有**mac-forced-forwarding static-gateway** *ip-address* &<1-16>命令，并检查静态网关IP地址是否与静态用户IP地址属于同一网段。	如果没有或者静态用户IP地址与静态网关IP地址不在同一网段，请执行命令**mac-forced-forwarding static-gateway** *ip-address* &<1-16>配置与静态用户在同一网段的静态网关。
	静态用户是否正确配置	进入系统视图，执行命令**display dhcp static user-bind vlan** *vlan-id*，检查是否有指定IP的静态用户绑定表项。	如果没有，请执行命令**user-bind static**配置。

如果表中检查项均正确或者修改配置后问题仍然存在，请执行下一步。

3. 检查MFF相关配置是否正确
   - 进入用户接口视图，执行命令**display this**，查看接口是否加入配置MFF的VLAN。如果没有加入，请执行相应命令加入。
   - 进入网络接口视图，执行命令**display this**，查看该接口上是否配置有**mac-forced-forwarding network-port**命令，如果没有，请执行该命令配置。

步骤3 MFF未学习到网关MAC排查过程

1. 检查设备是否接收到网关的ARP应答报文

   用户视图下执行命令**debugging ethernet packet arp interface** *interface-type interface-number*，查看设备是否接收到来自网关的ARP应答报文：
   - 如果没有接收到ARP应答报文，静态用户请执行步骤b，动态用户请执行步骤c。
2. 检查设备到网关的链路是否有问题

   从设备Ping网关以检查路由是否可达：
   - 如果Ping不通，请先根据排除路由故障。
   - 如果能Ping通，请执行步骤c。
3. 检查ARP应答报文是否被丢弃
   - 系统视图、VLAN视图或接口视图下执行命令**display this**查看是否配置了ARP报文限速。

     如果配置了ARP报文限速“arp anti-attack rate-limit”，配置的阈值过小，则有可能ARP应答报文被丢弃。使用命令**arp anti-attack rate-limit**可以修改速率抑制大小。

- 进入使能MFF功能的VLAN视图，执行命令**mac-forced-forwarding gateway-detect** [**interval** *interval-time*]启动MFF网关定时探测功能，以重新发送ARP请求获取网关的MAC地址。

----结束

4.8 MFF FAQ

4.8.1 VLAN 内使能 MFF 功能并配置网关定时探测功能后，原来已经学到网关 MAC 地址后，为何会出现网关 MAC 地址为空的现象

为了防止网关失效导致用户间流量互通，在使能网关定时探测功能后，如果连续5次探测都没有回应，设备会认为网关已经失效，并将当前的网关MAC地址清空，删除下发的网关MAC地址的ACL规则。

4.8.2 在交换机使能了 MFF 功能且配置了静态网关地址的场景下，静态用户间 ping 不通的原因有哪些

在交换机使能了MFF功能且配置了静态网关地址的场景下，要求非DHCP的静态用户必须通过ARP请求报文或者发送免费ARP报文来触发交换机建立MFF的用户表项，才能保证用户之间可以ping通。如果是用测试仪模拟静态用户，请务必确保测试仪能够发送ARP请求报文和免费ARP报文，否则交换机上没有用户对应的MFF表项，就会出现静态用户之间ping不通的现象。

4.8.3 配置 ARP 速率抑制功能且 VLAN 内使能 MFF 功能时，ARP 速率抑制功能对 MFF 模块处理的 ARP 报文生效吗

设备会检查报文携带的VLAN编号，进而判断该VLAN是否使能了MFF功能。如果该VLAN内已使能了MFF功能，设备则先对ARP报文进行速率抑制，再由MFF模块处理ARP报文。

5 攻击防范配置

5.1 攻击防范简介

定义

攻击防范是一种重要的网络安全特性。它通过分析上送CPU处理的报文的内容和行为，判断报文是否具有攻击特性，并配置对具有攻击特性的报文执行一定的防范措施。

攻击防范主要分为畸形报文攻击防范、分片报文攻击防范和泛洪攻击防范。

目的

目前，网络的攻击日益增多，而通信协议本身的缺陷以及网络部署问题，导致网络攻击造成的影响越来越大。特别是对网络设备的攻击，将会导致设备或者网络瘫痪等严重后果。

攻击防范针对上送CPU的不同类型攻击报文，采用丢弃或者限速的手段，以保障设备不受攻击的影响，使业务正常运行。

5.2 攻击防范原理描述

5.2.1 畸形报文攻击防范

畸形报文攻击是通过向目标设备发送有缺陷的IP报文，使得目标设备在处理这样的IP报文时出错和崩溃，给目标设备带来损失。畸形报文攻击防范是指设备实时检测出畸形报文并予以丢弃，实现对本设备的保护。

畸形报文攻击主要分为以下几类：

没有 IP 载荷的泛洪

如果IP报文只有20字节的IP报文头，没有数据部分，就认为是没有IP载荷的报文。攻击者经常构造只有IP头部，没有携带任何高层数据的IP报文，目标设备在处理这些没有IP载荷的报文时会出错和崩溃，给设备带来损失。

启用畸形报文攻击防范后，设备在接收到没有载荷的IP报文时，直接将其丢弃。

IGMP 空报文

IGMP报文是20字节的IP头加上8字节的IGMP报文体，总长度小于28字节的IGMP报文称为IGMP空报文。设备在处理IGMP空报文时会出错和崩溃，给目标设备带来损失。

启用畸形报文攻击防范后，设备在接收到IGMP空报文时，直接将其丢弃。

LAND 攻击

LAND攻击是攻击者利用TCP连接三次握手机制中的缺陷，向目标主机发送一个源地址和目的地址均为目标主机、源端口和目的端口相同的SYN报文，目标主机接收到该报文后，将创建一个源地址和目的地址均为自己的TCP空连接，直至连接超时。在这种攻击方式下，目标主机将会创建大量无用的TCP空连接，耗费大量资源，直至设备瘫痪。

启用畸形报文攻击防范后，设备采用检测TCP SYN报文的源地址和目的地址的方法来避免LAND攻击。如果TCP SYN报文中的源地址和目的地址一致，则认为是畸形报文攻击，丢弃该报文。

Smurf 攻击

Smurf攻击是指攻击者向目标网络发送源地址为目标主机地址、目的地址为目标网络广播地址的ICMP请求报文，目标网络中的所有主机接收到该报文后，都会向目标主机发送ICMP响应报文，导致目标主机收到过多报文而消耗大量资源，甚至导致设备瘫痪或网络阻塞。

启用畸形报文攻击防范后，设备通过检测ICMP请求报文的目标地址是否是广播地址或子网广播地址来避免Smurf攻击。如果检测到此类报文，直接将其丢弃。

TCP 标志位非法攻击

TCP报文包含6个标志位：URG、ACK、PSH、RST、SYN、FIN，不同的系统对这些标志位组合的应答是不同的：

- 6个标志位全部为1，就是圣诞树攻击。设备在受到圣诞树攻击时，会造成系统崩溃。

- SYN和FIN同时为1，如果端口是关闭的，会使接收方应答一个RST | ACK消息；如果端口是打开的，会使接收方应答一个SYN | ACK消息，这可用于主机探测(主机在线或者下线)和端口探测（端口打开或者关闭）。
- 6个标志位全部为0，如果端口是关闭的，会使接收方应答一个RST | ACK消息，这可以用于探测主机；如果端口是开放的，Linux和UNIX系统不会应答，而Windows系统将回答RST | ACK消息，这可以探测操作系统类型（Windows系统，Linux和UNIX系统等）。

启用畸形报文攻击防范后，设备采用检查TCP的各个标志位避免TCP标志位非法攻击，如果符合下面条件之一，则将该TCP报文丢弃：

- 6个标志位全部为1；
- SYN和FIN位同时为1；
- 6个标志位全部为0。

5.2.2 分片报文攻击防范

分片报文攻击是通过向目标设备发送分片出错的报文，使得目标设备在处理分片错误的报文时崩溃、重启或消耗大量的CPU资源，给目标设备带来损失。分片报文攻击防范是指设备实时检测出分片报文并予以丢弃或者限速处理，实现对本设备的保护。

分片报文攻击主要分为以下几类：

分片数量巨大攻击

IP报文中的偏移量是以8字节为单位的。正常情况下，IP报文的头部有20个字节，IP报文的最大载荷为65515。对这些数据进行分片，分片个数最大可以达到8189片，对于超过8189的分片报文，设备在重组这些分片报文时会消耗大量的CPU资源。

启用分片报文攻击防范后，针对分片数量巨大攻击，如果同一报文的分片数目超过8189个，则设备认为是恶意报文，丢弃该报文的所有分片。

巨大 Offset 攻击

攻击者向目标设备发送一个Offset值超大的分片报文，从而导致目标设备分配巨大的内存空间来存放所有分片报文，消耗大量资源。

Offset字段的最大取值为65528，但是在正常情况下，Offset值不会超过8190（如果offset=8189*8，IP头部长度为20，最后一片报文最多只有3个字节IP载荷，所以正常Offset的最大值是8189），所以如果Offset值超过8190，则这种报文即为恶意攻击报文，设备直接丢弃。

启用分片报文攻击防范后，设备在收到分片报文时判断Offset*8是否大于65528，如果大于就当作恶意分片报文直接丢弃。

重复分片攻击

重复分片攻击就是把同样的分片报文多次向目标主机发送，存在两种情况：

- 多次发送的分片完全相同，这样会造成目标主机的CPU和内存使用不正常；
- 多次发送的分片报文不相同，但Offset相同，目标主机就会处于无法处理的状态：哪一个分片应该保留，哪一个分片应该丢弃，还是都丢弃。这样就会造成目标主机的CPU和内存使用不正常。

启用分片报文攻击防范后，对于重复分片类报文的攻击，设备实现对分片报文进行CAR（Committed Access Rate）限速，保留首片，丢弃其余所有相同的重复分片，保证不对CPU造成攻击。

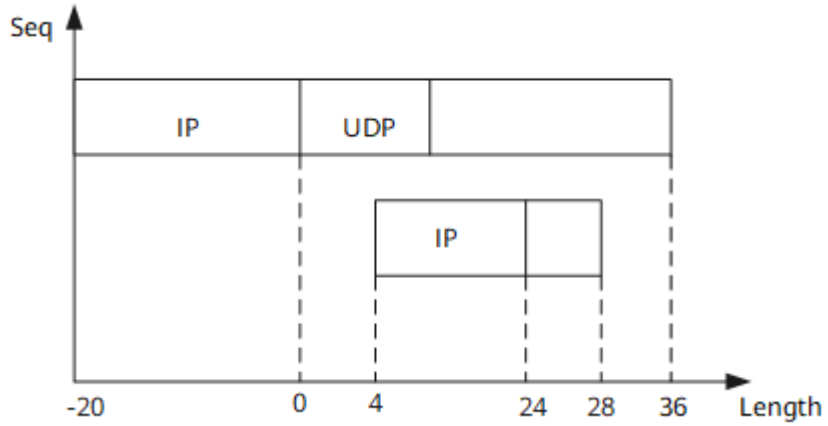
Tear Drop 攻击

Tear Drop攻击是最著名的IP分片攻击，原理是IP分片错误，第二片包含在第一片之中。即数据包中第二片IP包的偏移量小于第一片结束的位移，而且算上第二片IP包的Data，也未超过第一片的尾部。

如图5-1所示：

- 第一个分片IP载荷为36字节，总长度为56字节，protocol为UDP，UDP检验和为0（没有检验）；
- 第二片IP载荷为4字节，总长度为24字节，protocol为UDP，Offset=24（错误，正确应该为36）。

图 5-1 Tear Drop 攻击分片示意图



Tear Drop攻击会导致系统崩溃或重启。启用分片报文攻击防范后，对于Tear Drop攻击，设备会直接丢弃所有分片报文。

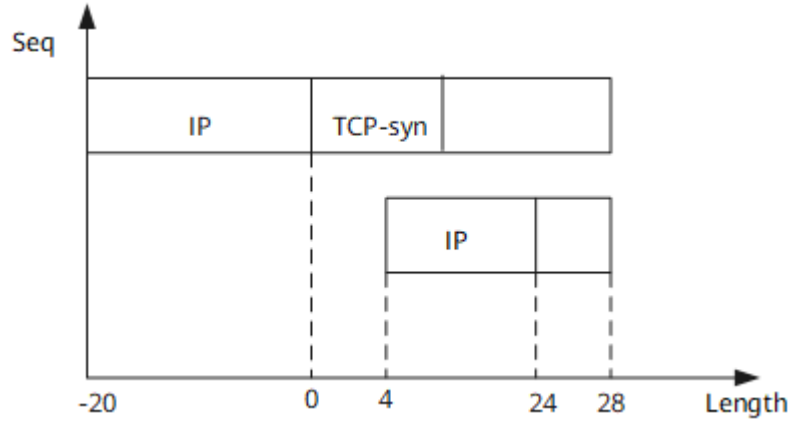
Syndrop 攻击

Syndrop攻击原理和Tear Drop原理一致，区别在于Syndrop攻击使用了TCP协议，Flag为SYN，而且带有载荷。

如图5-2所示：

- 第一片IP载荷为28字节，IP头部20字节；
- 第二片IP载荷为4字节，IP头部20字节，Offset=24（错误，正确应该是28）。

图 5-2 Syndrop 攻击分片示意图



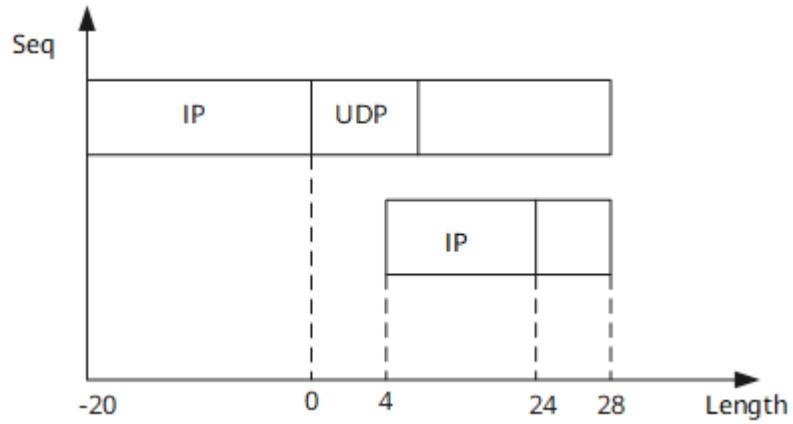
Syndrop攻击会导致系统崩溃或重启。启用分片报文攻击防范后，对于Syndrop攻击，设备会直接丢弃所有分片报文。

NewTear 攻击

NewTear攻击是分片错误的攻击。如图5-3所示，protocol使用UDP。

- 第一片IP载荷28字节（包含UDP头部，UDP检验和为0）；
- 第二片IP载荷4字节，offset=24（错误，正确应该是28）。

图 5-3 NewTear 攻击分片示意图



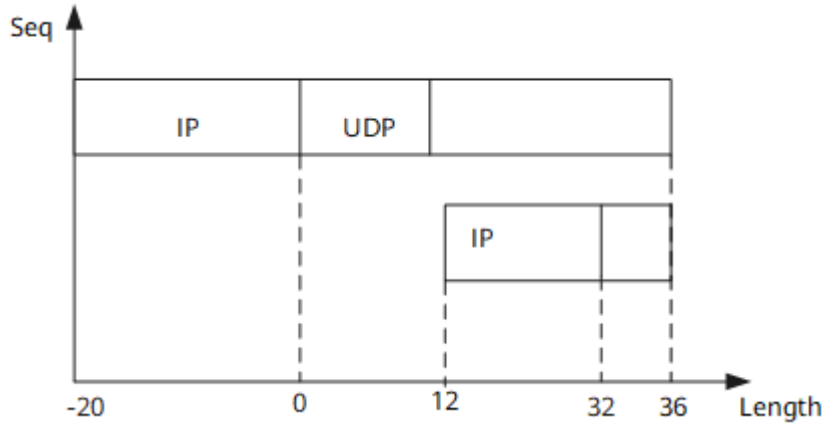
NewTear攻击会导致系统崩溃或重启。启用分片报文攻击防范后，对于NewTear攻击，设备会直接丢弃所有分片报文。

Bonk 攻击

Bonk攻击是分片错误的攻击。如图5-4所示，protocol使用UDP。

- 第一片IP载荷为36字节（包含UDP头部，UDP检验和为0）；
- 第二片IP载荷为4字节，offset=32（错误，正确应该是36）。

图 5-4 Bonk 攻击分片示意图



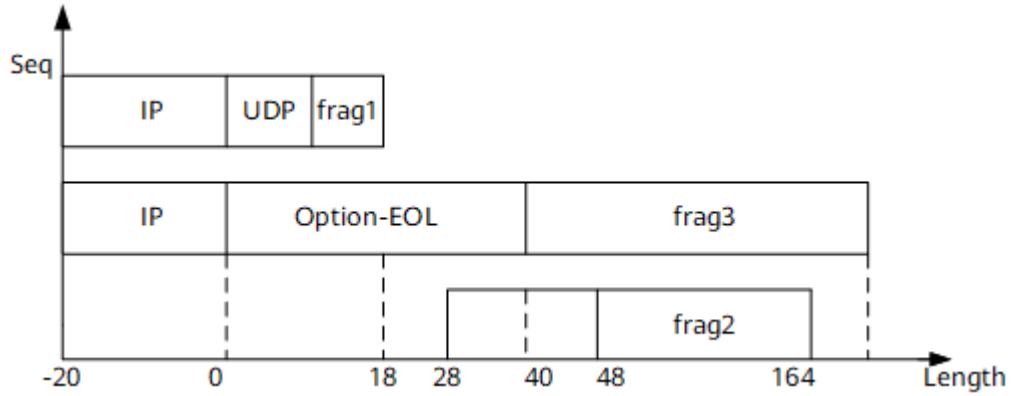
Bonk攻击会导致系统崩溃或重启。启用分片报文攻击防范后，对于Bonk攻击，设备会直接丢弃所有分片报文。

Nesta 攻击

Nesta攻击是分片错误的攻击。如图5-5所示：

- 第一片IP载荷为18，protocol为UDP，检验和为0；
- 第二片offset为48，IP载荷为116字节；
- 第三片offset为0，more frag为1，也就是还有分片，40字节的IP option，都是EOL，IP载荷为224字节。

图 5-5 Nesta 攻击分片示意图



Nesta攻击会导致系统崩溃或重启。启用分片报文攻击防范后，对于Nesta攻击，设备会直接丢弃所有分片报文。

Rose 攻击

IP protocol可以是UDP或TCP，可以选择。

如图5-6所示：

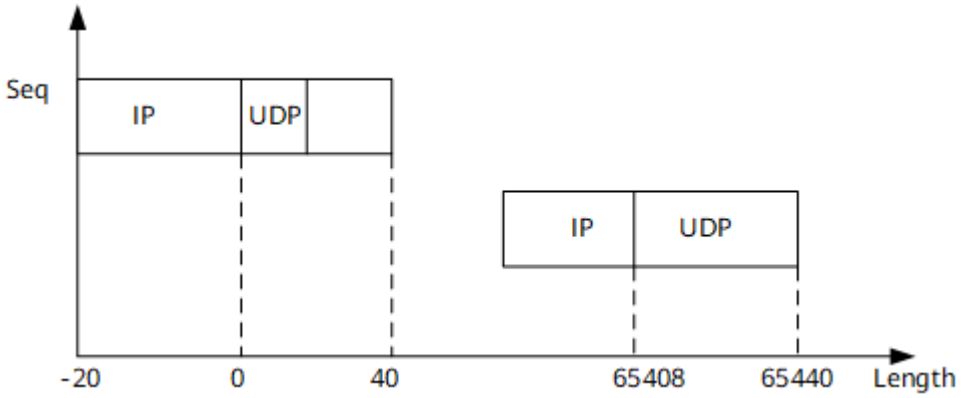
如果IP protocol是TCP：

- 第一片IP载荷为48字节（包含TCP头部），IP头部20字节；
- 第二片IP报文的载荷为32字节，但是offset=65408，more frag=0，即最后一片。

如果IP protocol是UDP：

- 第一片载荷长度40字节（包含UDP头部，UDP校验和为0），IP头部20字节；
- 第二片IP报文的载荷为32字节，但是offset＝65408，more frag＝0，即最后一片。

图 5-6 Rose 攻击分片示意图

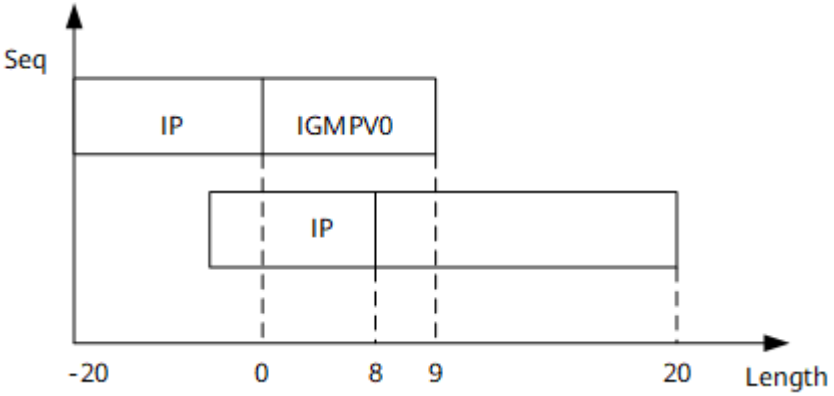


Rose攻击会导致系统崩溃或重启。启用分片报文攻击防范后，对于Rose攻击，设备会直接丢弃所有分片报文。

Fawx 攻击

Fawx攻击是一种分片错误的IGMP报文。如图5-7，Fawx攻击的特征是：发送IGMP报文分片，一共两片，第一片9个字节，第二个分片offset＝8，载荷长度为16字节，没有结束分片。

图 5-7 Fawx 攻击分片示意图



Fawx攻击会导致系统崩溃或重启。启用分片报文攻击防范后，对于Fawx攻击，设备会直接丢弃所有分片报文。

Ping of Death 攻击

Ping of Death攻击原理是攻击者发送一些尺寸较大（数据部分长度超过65507字节）的ICMP报文对设备进行攻击。设备在收到这样一个尺寸较大的ICMP报文后，如果处理不当，会造成协议栈崩溃。

启用分片报文攻击防范后，设备在收到这种攻击报文后，直接丢弃该报文。

Jolt 攻击

Jolt攻击是攻击者发送总长度大于65535字节的报文对设备进行攻击。Jolt攻击报文一共173个分片，每个分片报文的IP载荷为380字节，因此总长度为：173*380+20 = 65760，远远超过65535。设备在收到这样的报文时，如果处理不当，会造成设备崩溃、死机或重启。

启用分片报文攻击防范后，设备在收到Jolt攻击报文后，直接丢弃该报文。

5.2.3 泛洪攻击防范

泛洪攻击是指攻击者在短时间内向目标设备发送大量的虚假报文，导致目标设备忙于应付无用报文，而无法为用户提供正常服务。

泛洪攻击防范是指设备实时检测出泛洪报文并予以丢弃或者限速处理，实现对本设备的保护。

泛洪攻击主要分为TCP SYN泛洪攻击、UDP泛洪攻击和ICMP泛洪攻击。

TCP SYN 泛洪攻击

TCP SYN攻击利用了TCP三次握手的漏洞。在TCP的3次握手期间，当接收端收到来自发送端的初始SYN报文时，向发送端返回一个SYN+ACK报文。接收端在等待发送端的最终ACK报文时，该连接一直处于半连接状态。如果接收端最终没有收到ACK报文包，则重新发送一个SYN+ACK到发送端。如果经过多次重试，发送端始终没有返回ACK报文，则接收端关闭会话并从内存中刷新会话，从传输第一个SYN+ACK到会话关闭大约需要30秒。

在这段时间内，攻击者可能将数十万个SYN报文发送到开放的端口，并且不回应接收端的SYN+ACK报文。接收端内存很快就会超过负荷，且无法再接受任何新的连接，并将现有的连接断开。

设备对TCP SYN攻击处理的方法是在使能了TCP SYN泛洪攻击防范后对TCP SYN报文进行速率限制，保证受到攻击时设备资源不被耗尽。

UDP 泛洪攻击

UDP泛洪攻击是指攻击者在短时间内向目标设备发送大量的UDP报文，导致目标设备负担过重而不能处理正常的业务。UDP泛洪攻击分为以下两类：

- Fraggle攻击

  Fraggle攻击的原理是攻击者发送源地址为目标主机地址，目的地址为广播地址，目的端口号为7的UDP报文。如果该广播网络中有很多主机都起用了UDP响应请求服务，目的主机将收到很多回复报文，造成系统繁忙，达到攻击效果。

  使能泛洪攻击防范功能后，设备默认UDP端口号为7的报文是攻击报文，直接将其丢弃。

- UDP诊断端口攻击

  攻击者对UDP诊断端口（7-echo，13-daytime，19-Chargen等UDP端口）发送报文，如果同时发送的数据包数量很大，造成泛洪，影响网络设备的正常工作。

  使能泛洪攻击防范功能后，设备将UDP端口为7、13和19的报文认为是攻击报文，直接丢弃。

ICMP 泛洪攻击

通常情况下，网络管理员会用Ping程序对网络进行监控和故障排除，大概过程如下：

1. 源设备向接收设备发出ICMP响应请求报文；
2. 接收设备接收到ICMP响应请求报文后，会向源设备回应一个ICMP应答报文。

如果攻击者向目标设备发送大量的ICMP响应请求报文，则目标设备会忙于处理这些请求，而无法继续处理其他的数据报文，造成对正常业务的冲击。

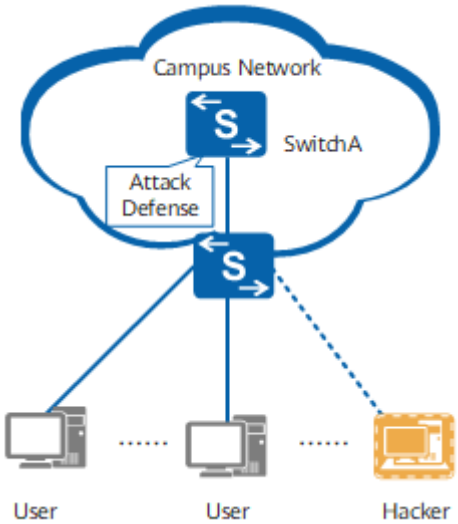
设备针对ICMP泛洪攻击进行CAR（Committed Access Rate）限速，保证CPU不被攻击，保证网络的正常运行。

5.3 攻击防范应用场景

如图5-8所示，SwitchA经常会受到不同类型的网络攻击，这样会导致设备资源使用率过高，影响网络服务。为保障给用户提供安全的网络服务，在SwitchA上部署攻击防范功能，主要防范的攻击类型包括：

- 畸形报文攻击防范，防止畸形报文攻击。
- 分片报文攻击防范，限制分片报文的速率，防止分片报文对CPU造成攻击，占用过多CPU和设备资源。
- 泛洪攻击防范，包括以下三种：
  - TCP SYN泛洪攻击防范，限制TCP SYN报文的速率，防止CPU处理TCP SYN报文占用过多资源；
  - UDP泛洪攻击防范，对特定端口发送的UDP报文直接丢弃；
  - ICMP泛洪攻击防范，限制ICMP泛洪攻击报文的上送速率，防止CPU处理ICMP泛洪攻击报文占用过多资源。

图 5-8 攻击防范应用组网图



5.4 攻击防范配置注意事项

涉及网元

无需其他网元配合。

License 支持

本特性是交换机的基本特性，无需获得License许可即可应用此功能。

V200R021C00、V200R021C01 版本特性支持情况

S600-E系列交换机中所有款型均支持攻击防范。

说明

如需了解交换机软件配套详细信息，请点击**Info-Finder**。

特性依赖和限制

目前防范攻击只支持分析IPv4报文。

5.5 攻击防范缺省配置

攻击防范的缺省配置如**表5-1**所示。

表 5-1 攻击防范缺省配置

参数	缺省值
畸形报文攻击防范功能	已使能
分片报文攻击防范功能	已使能
分片报文发送速率	155000000bit/s
TCP Syn攻击防范功能	已使能
TCP Syn泛洪报文发送速率	155000000bit/s
UDP泛洪攻击防范功能	已使能
ICMP泛洪攻击防范功能	已使能
ICMP泛洪报文发送速率	155000000bit/s

5.6 配置畸形报文攻击防范

背景信息

攻击者通过向目标设备发送畸形报文，使得目标设备在处理畸形报文时出错、崩溃，给目标设备带来损失，或者通过发送大量无用报文占用网络带宽等行为来造成攻击。

为了避免设备被畸形报文攻击的情况下瘫痪，保证正常的网络服务，可以配置畸形报文攻击防范。设备对畸形报文攻击防范的主要措施是判断是否是几种畸形报文攻击报文类型之一，若是，则直接丢弃畸形报文。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**anti-attack abnormal enable**，使能畸形报文攻击防范功能。

缺省情况下，畸形报文攻击防范功能处于使能状态。

说明

在系统视图下，执行命令**anti-attack enable**可以使能所有的攻击防范功能（包括畸形报文攻击防范、分片报文攻击防范和TCP SYN/UDP/ICMP泛洪攻击防范）。

----结束

检查配置结果

- 执行命令**display anti-attack statistics abnormal**，查看设备上畸形报文防攻击的统计数据。

5.7 配置分片报文攻击防范

背景信息

攻击者通过向目标设备发送分片出错的报文，使得目标设备在处理分片错误的报文时消耗大量的CPU资源，给目标设备带来损失。

为了避免设备被分片报文攻击的情况下瘫痪，保证正常的网络服务，可以配置分片报文攻击防范。对分片报文攻击防范的主要措施是进行速率限制，防止大量的分片报文造成CPU繁忙，保证CPU在造成攻击的情况下正常运行。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**anti-attack fragment enable**，使能分片报文攻击防范功能。

缺省情况下，分片报文攻击防范功能处于使能状态。

说明

在系统视图下，执行命令**anti-attack enable**可以使能所有的攻击防范功能（包括畸形报文攻击防范、分片报文攻击防范和TCP SYN/UDP/ICMP泛洪攻击防范）。

步骤3 执行命令**anti-attack fragment car cir** *cir*，限制分片报文接收的速率。

缺省情况下，分片报文的接收速率为155000000bit/s。

----结束

检查配置结果

- 执行命令**display anti-attack statistics fragment**，查看设备上分片报文防攻击的统计数据。

5.8 配置泛洪攻击防范

5.8.1 配置 TCP SYN 泛洪攻击防范

背景信息

攻击者向目标设备发送SYN报文，然后对于目标返回的SYN+ACK报文不作回应。目标设备如果没有收到攻击者的ACK回应，就会一直等待，形成半连接。攻击者利用这种方式，让目标设备上生成大量的半连接，迫使其大量资源浪费在这些半连接上。

为了避免TCP SYN泛洪攻击，可以在设备上配置TCP SYN泛洪攻击防范功能，通过限制TCP SYN报文的发送速率来防范TCP SYN泛洪攻击。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**anti-attack tcp-syn enable**，使能TCP SYN泛洪攻击防范功能。

缺省情况下，TCP SYN泛洪攻击防范功能处于使能状态。

说明

在系统视图下，执行命令**anti-attack enable**可以使能所有的攻击防范功能（包括畸形报文攻击防范、分片报文攻击防范和TCP SYN/UDP/ICMP泛洪攻击防范）。

步骤3 执行命令**anti-attack tcp-syn car cir** *cir*，限制TCP SYN报文接收的速率。

缺省情况下，TCP SYN报文接收的速率为155000000bit/s。

----结束

5.8.2 配置 UDP 泛洪攻击防范

背景信息

如果攻击者在短时间内向特定目标发送特定目的端口号的UDP报文，会造成目标设备负担过重而不能处理正常的业务。为了避免UDP泛洪攻击，可以在设备上配置UDP泛洪攻击防范功能。

设备上配置UDP泛洪攻击防范功能，对于端口号为7、13和19的报文，直接丢弃。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**anti-attack udp-flood enable**，使能UDP泛洪攻击防范功能。

缺省情况下，UDP泛洪攻击防范功能处于使能状态。

说明

在系统视图下，执行命令**anti-attack enable**可以使能所有的攻击防范功能（包括畸形报文攻击防范、分片报文攻击防范和TCP SYN/UDP/ICMP泛洪攻击防范）。

----结束

5.8.3 配置 ICMP 泛洪攻击防范

背景信息

如果攻击者在短时间内向目标设备发送大量的ICMP响应请求报文，使目标设备忙于回复这些请求，会造成目标设备负担过重而不能处理正常的业务。为了避免ICMP泛洪攻击，可以在设备上配置ICMP泛洪攻击防范功能。

设备上配置ICMP泛洪攻击防范功能，通过限制ICMP报文的速率来防范ICMP泛洪攻击。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**anti-attack icmp-flood enable**，使能ICMP泛洪攻击防范功能。

缺省情况下，ICMP泛洪攻击防范功能处于使能状态。

说明

在系统视图下，执行命令**anti-attack enable**可以使能所有的攻击防范功能（包括畸形报文攻击防范、分片报文攻击防范和TCP SYN/UDP/ICMP泛洪攻击防范）。

步骤3 执行命令**anti-attack icmp-flood car cir** *cir*，限制ICMP泛洪攻击报文接收的速率。

缺省情况下，ICMP泛洪攻击报文接收的速率为155000000bit/s。

----结束

5.8.4 检查泛洪攻击防范的配置结果

操作步骤

- 执行**display anti-attack statistics** [**tcp-syn** | **udp-flood** | **icmp-flood**]命令，查看泛洪防攻击的统计数据。

----结束

5.9 清除攻击防范统计信息

背景信息

须知

清除信息后，以前的信息将无法恢复，务必仔细确认。

在确认需要清除攻击防范的统计信息时，请执行以下命令清除攻击防范的统计信息。

操作步骤

- 执行**reset anti-attack statistics** [**abnormal** | **fragment** | **tcp-syn** | **udp-flood** | **icmp-flood**]命令，清除攻击防范的报文统计信息。

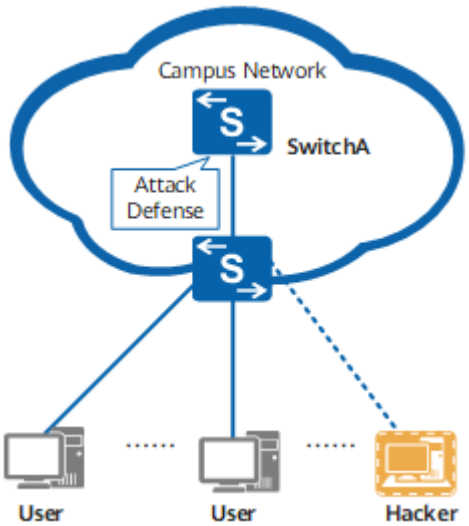
----结束

5.10 配置攻击防范示例

组网需求

如图5-9所示，如果局域网内存在Hacker向SwitchA发起畸形报文攻击、分片报文攻击和泛洪攻击，将会造成SwitchA瘫痪。为了预防这种情况，管理员希望通过在SwitchA上部署各种攻击防范措施来为用户提供安全的网络环境，保障正常的网络服务。

图 5-9 配置攻击防范组网图



配置思路

采用如下思路在SwitchA上配置攻击防范：

1. 使能畸形报文攻击防范功能，避免畸形报文攻击。
2. 使能分片报文攻击防范功能，避免分片报文攻击。
3. 使能泛洪攻击防范功能，避免泛洪攻击。

操作步骤

步骤1 使能畸形报文攻击防范

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] anti-attack abnormal enable
```

步骤2 使能分片报文攻击防范，并限制分片报文接收的速率为15000bit/s

```
[SwitchA] anti-attack fragment enable
[SwitchA] anti-attack fragment car cir 15000
```

步骤3 使能泛洪攻击防范

使能TCP SYN攻击防范，并限制TCP SYN报文接收的速率为15000bit/s。

```
[SwitchA] anti-attack tcp-syn enable
[SwitchA] anti-attack tcp-syn car cir 15000
```

使能UDP泛洪攻击防范，对特定端口发送的UDP报文直接丢弃。

```
[SwitchA] anti-attack udp-flood enable
```

使能ICMP泛洪攻击防范，并限制ICMP泛洪报文接收的速率为15000bit/s。

```
[SwitchA] anti-attack icmp-flood enable
[SwitchA] anti-attack icmp-flood car cir 15000
```

步骤4 检查配置结果

配置完成后，可以通过执行命令**display anti-attack statistics**查看报文攻击防范的统计数据。

```
[SwitchA] display anti-attack statistics
Packets Statistic Information:
-------------------------------------------------------------------------------
AntiAtkType  TotalPacketNum       DropPacketNum        PassPacketNum
             (H)       (L)       (H)       (L)       (H)       (L)
-------------------------------------------------------------------------------
URPF         0         0         0         0         0         0
Abnormal     0         0         0         0         0         0
Fragment     0         0         0         0         0         0
Tcp-syn      0         34        0         28        0         6
Udp-flood    0         0         0         0         0         0
Icmp-flood   0         0         0         0         0         0
-------------------------------------------------------------------------------
```

由显示信息可知，SwitchA上产生了TCP SYN报文的丢弃计数，表明攻击防范功能已经生效。

----结束

配置文件

SwitchA的配置文件

```
#
sysname SwitchA
#
anti-attack fragment car cir 15000
```



```
anti-attack tcp-syn car cir 15000
anti-attack icmp-flood car cir 15000
#
return
```

6 流量抑制及风暴控制配置

6.1 流量抑制及风暴控制简介

定义

流量抑制可以通过配置阈值来限制广播、未知组播、未知单播、已知组播和已知单播报文的速率，防止广播、未知组播报文和未知单播报文产生广播风暴，防止已知组播报文和已知单播报文的大流量冲击。

风暴控制可以通过阻塞报文来阻断广播、未知组播和未知单播报文的流量。

目的

当设备某个二层以太接口收到广播、未知组播或未知单播报文时，如果根据报文的目的MAC地址设备不能明确报文的出接口，设备会向同一VLAN内的其他二层以太接口转发这些报文，这样可能导致广播风暴，降低设备转发性能。

当设备某个以太接口收到已知组播或已知单播报文时，某种报文流量过大可能会对设备造成冲击，影响其他业务的正常处理。

引入流量抑制和风暴控制特性，可以有效地控制这几类报文流量。

6.2 流量抑制原理描述

流量抑制特性按以下三种形式来限制广播、组播和单播报文。

- 在接口视图下，入方向上，设备支持对广播、未知组播、未知单播、已知组播和已知单播报文按百分比、包速率和比特速率进行流量抑制。

  设备监控接口下的各类报文速率并和配置的阈值相比较，当入口流量超过配置的阈值时，设备会丢弃超额的流量。
- 在接口视图下，出方向上，设备支持对广播、未知组播和未知单播报文的阻塞（Block）。
- 在VLAN视图下，设备支持对广播报文按比特速率进行流量抑制。

  设备监控同一VLAN内广播报文的速率并和配置的阈值相比较，当VLAN内流量超过配置的阈值时，设备会丢弃超额的流量。

流量抑制还可以通过配置阈值的方式对ICMP报文进行限速，防止大量ICMP报文上送CPU处理，导致其他业务功能异常。

缺省情况下，设备支持MAC漂移触发流量抑制功能。在设备开启MAC漂移检测功能时，若检测到MAC地址发生漂移，将触发对漂移端口的流量抑制功能，表现为对未知单播以50%的百分比进行流量抑制。

说明

如果端口通过命令**unicast-suppression**配置了对未知单播的流量抑制功能且流量抑制百分比配置为非100，或者通过命令**storm-control**配置了对未知单播的风暴控制功能，该端口MAC漂移将不会触发流量抑制功能。

6.3 风暴控制原理描述

风暴控制可以用来防止广播、未知组播以及未知单播报文产生广播风暴。

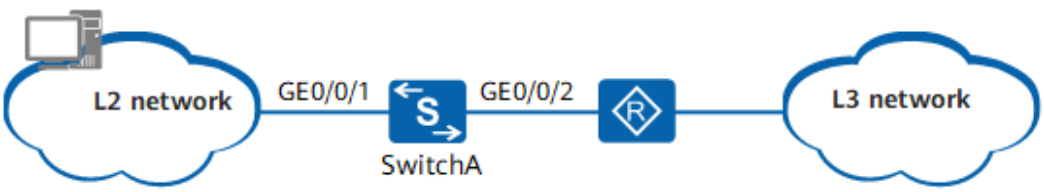
设备支持对接口下的这三类报文分别按包速率、字节速率、百分比进行风暴控制。

在一个检测时间间隔内，设备监控接口下接收的三类报文的平均速率并和配置的最大阈值相比较，当报文速率大于配置的最大阈值时，设备会对该接口进行风暴控制，执行配置好的风暴控制动作。

风暴控制的动作为阻塞报文，当接口上接收报文的平均速率小于指定的最小阈值时，风暴控制会放开在接口上对该报文的阻塞。

6.4 流量抑制应用场景

图 6-1 流量抑制典型应用组网图

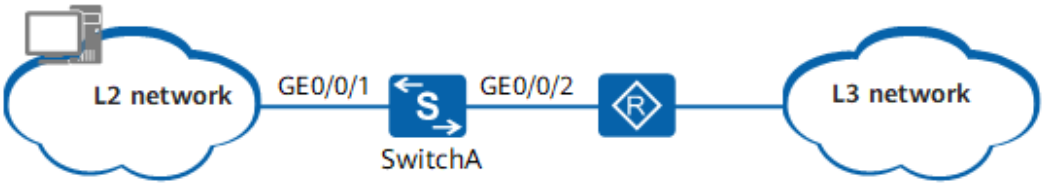


如图6-1所示，

- 在二层网络内的设备上，可以配置VLAN内的流量抑制来限制VLAN内的广播报文。
- SwitchA作为二层网络到路由器的衔接点，当需要限制二层网络转发的来自用户的广播、未知组播和未知单播报文时，可以通过在SwitchA的二层以太接口GE0/0/1上配置流量抑制功能来实现；当需要限制二三层网络转发已知组播和已知单播报文时，可以通过在SwitchA的以太接口GE0/0/1和GE0/0/2上配置流量抑制功能来实现。
- 在接口GE0/0/1出方向上，可以采取阻塞广播、未知组播和未知单播报文的方式，保证二层网络内用户和其他网络设备的安全性。

6.5 风暴控制应用场景

图 6-2 风暴控制典型应用组网图



如图6-2所示，SwitchA作为二层网络到路由器的衔接点，当需要限制二层网络转发的来自用户的广播、未知组播和未知单播报文时，可以通过在SwitchA的二层以太接口GE0/0/1上配置风暴控制功能来实现。

6.6 流量抑制及风暴控制配置注意事项

涉及网元

无需其他网元配合。

License 支持

本特性是交换机的基本特性，无需获得License许可即可应用此功能。

V200R021C00、V200R021C01 版本特性支持情况

S600-E系列交换机中所有款型均支持流量抑制及风暴控制。

说明

如需了解交换机软件配套详细信息，请点击Info-Finder。

特性依赖和限制

不同视图支持情况

接口视图和VLAN视图支持的流量抑制及风暴控制特性如表6-1所示。

表 6-1 不同视图支持情况

视图	交换机支持的流量抑制及风暴控制特性
接口视图	• 对广播、未知组播、未知单播、已知组播和已知单播报文配置流量抑制。 • 对广播、未知组播和未知单播报文配置风暴控制。 • 对ICMP报文配置流量抑制。
VLAN视图	对广播报文配置流量抑制。

流量抑制和风暴控制的区别

- 从原理来看，两者对流量控制的形式不一样：
  - 流量抑制中，可以为接口入方向的报文流量配置阈值，当流量超过阈值时，系统将丢弃多余的流量，阈值范围内的报文可以正常通过，从而将流量限制在合理的范围内。此外，流量抑制还支持对接口出方向的流量进行阻塞。
  - 风暴控制中，只可以为接口入方向的报文流量配置阈值。当流量超过阈值时，系统会阻塞该接口收到的该类型报文流量。
- 对于同一个接口下同种报文的入方向流量，交换机仅允许同时配置流量抑制或风暴控制两种功能中的一种。

其他特性依赖和限制

- 同一接口下最多支持广播、已知组播、未知组播、已知单播、未知单播、MAC漂移触发流量抑制中的三种流量抑制或风暴控制功能。例如，接口下已配置广播流量抑制、广播风暴控制和已知单播流量抑制，当接口发生MAC地址漂移时不会触发对漂移接口的流量抑制功能。
- 对于，流量抑制按照每秒包速率进行配置时，配置值小于24则按照24进行流量抑制，配置值大于等于24则按照实际配置值进行流量抑制。

6.7 流量抑制及风暴控制缺省配置

流量抑制及风暴控制缺省值如表6-2和表6-3所示。

表 6-2 流量抑制缺省值

参数	缺省值
接口的流量抑制	• 广播报文的流量抑制：使能 • 未知组播、未知单播、已知组播和已知单播报文的流量抑制：未使能
接口的流量抑制方式	百分比方式

参数	缺省值
百分比抑制比例值	广播报文流量的百分比抑制比例值为10%，其他报文流量的百分比抑制比例值为100%
接口出方向阻塞报文	未使能
VLAN的流量抑制	未使能
ICMP（Internet Control Message Protocol）报文流量抑制	未使能
ICMP报文接口限速阈值	缺省情况下，全局和接口下的ICMP报文限速阈值为190pps。

表 6-3 风暴控制缺省值

参数	缺省值
风暴控制	未使能
记录日志和上报告警	未使能
检测时间间隔	5秒

6.8 配置流量抑制

6.8.1 配置接口的流量抑制

背景信息

为了限制接口的广播、未知组播、未知单播、已知组播和已知单播报文的速率，防止广播风暴或大流量冲击，可以在该接口上配置对应报文类型的流量抑制功能。

说明

设备支持在接口上同时配置对广播、未知组播、未知单播、已知组播和已知单播报文的流量抑制功能。

前置任务

在配置接口的流量抑制之前，需完成以下任务：

- 配置接口的链路层协议参数，使接口的链路协议状态为Up。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 （可选）执行命令**suppression mode** { **by-packets** | **by-bits** }，在全局下配置流量抑制模式。

说明

如果在全局下配置流量抑制模式为**packets**，则在接口下配置允许通过的最大流量时，不能配置**cir**参数。

如果在全局下配置流量抑制模式为**bits**，则在接口下配置允许通过的最大流量时，不能配置**packets**参数。

步骤3 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤4 执行命令{ **broadcast-suppression** | **multicast-suppression** | **unicast-suppression** | **known-multicast-suppression** | **known-unicast-suppression** } { *percent-value* | **cir** *cir-value* [**cbs** *cbs-value*] | **packets** *packets-per-second* }，配置流量抑制。

的接口下配置流量抑制时，抑制模式需与全局的流量抑制模式保持一致，否则设备会提示错误信息。

步骤5 执行命令{ **broadcast-suppression** | **multicast-suppression** | **unicast-suppression** } **block outbound**，配置在接口出方向上阻塞报文。

----结束

6.8.2 配置 VLAN 的流量抑制

背景信息

为了限制进入VLAN的广播类型报文的速率，防止广播风暴，可以在该VLAN内配置对应报文类型的流量抑制功能。

说明

配置VLAN下的流量抑制时，设备允许VLAN下每秒通过的报文数与报文长度计算方式有关。默认情况下，设备会计算20字节的帧间隙和前导码，即按照报文实际长度加20字节帧间隙和前导码进行计算。

当同时配置了接口入方向的流量监管、VLAN的广播流量抑制以及入方向的基于流的流量监管时，如果报文同时符合上述两种或两种以上限速的条件，限速生效的优先级由高到低依次是接口入方向的流量监管、VLAN的广播流量抑制、入方向的基于流的流量监管。例如，同时匹配了接口入方向的流量监管和VLAN的广播流量抑制，则接口入方向的流量监管生效。关于接口入方向的流量监管、入方向的基于流的流量监管的具体配置，请参考《 S600-E V200R021C00, C01 配置指南-QoS 》流量监管、流量整形和接口限速配置 中的“配置入方向的接口限速”和“配置MQC实现流量监管”。

前置任务

在配置VLAN的流量抑制之前，需完成以下任务：

- 配置VLAN内接口的链路层协议参数，使VLAN内接口的链路协议状态为Up。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**vlan** *vlan-id*，进入VLAN视图。

步骤3 执行命令**broadcast-suppression** *threshold-value*，配置VLAN的广播抑制速率。

----结束

6.8.3 配置 ICMP 报文流量抑制

背景信息

网络中经常存在攻击者发送大量ICMP报文进行攻击，如果设备全部将这些ICMP报文上送CPU处理，会消耗大量CPU资源，导致其他业务功能异常。此时在设备上配置ICMP报文流量抑制功能，可以有效防范ICMP报文攻击。

配置ICMP报文流量抑制功能后，当接口每秒钟上送的ICMP报文超出配置的阈值时，设备会将ICMP报文丢弃。

ICMP报文流量抑制功能生效需要使用命令**undo icmp-reply fast**去使能ICMP-Reply fast功能。

前置任务

在配置ICMP报文流量抑制之前，需完成以下任务：

- 配置接口的链路层协议参数，使接口的链路协议状态为Up。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**icmp rate-limit enable**，使能ICMP流量抑制功能。

缺省情况下，ICMP流量抑制功能未使能。

步骤3 执行命令**icmp rate-limit** { **total** | **interface** *interface-type interface-number* [**to** *interface-number*] } **threshold** *threshold-value*，配置接口和全局的ICMP报文限速阈值。

缺省情况下，全局和接口下的ICMP报文限速阈值为190pps。

----结束

6.8.4 检查流量抑制的配置结果

操作步骤

- 使用命令**display flow-suppression interface** *interface-type interface-number* 查看流量抑制配置信息。

----结束

6.9 配置风暴控制

背景信息

为了限制进入接口的广播、未知组播或未知单播类型报文的速率，防止广播风暴，可以在该接口上配置对应报文类型的风暴控制功能。

说明

当进入接口的报文为JUMBO帧时，建议配置风暴控制模式为字节模式。

设备在检测单播报文时，不区分未知单播报文和已知单播报文，统计的报文速率是未知单播报文和已知单播报文共同的速率。但当风暴控制动作为阻塞报文时，设备仅对未知单播报文进行阻塞。组播报文的原理同单播报文。

设备在检测组播报文时，不区分未知组播报文和已知组播报文，统计的报文速率是未知组播报文和已知组播报文共同的速率。当风暴控制动作为阻塞报文时，设备对未知组播和已知组播报文都进行阻塞。

前置任务

在配置风暴控制之前，需完成以下任务：

- 配置接口的链路层协议参数，使接口的链路协议状态为Up。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**storm-control** { **broadcast** | **multicast** | **unicast** } **min-rate** *min-rate-value* **max-rate** *max-rate-value*，对接口上的广播、未知组播或未知单播报文进行风暴控制。

步骤4 执行命令**storm-control action block**，配置风暴控制的动作。

步骤5 （可选）执行命令**storm-control enable** { **log** | **trap** }，使能风暴控制时记录日志或者上报告警。

步骤6 （可选）执行命令**storm-control interval** *interval-value*，配置风暴控制的检测时间间隔。

----结束

检查配置结果

使用命令**display storm-control** [**interface** *interface-type interface-number*]，查看接口的风暴控制信息。

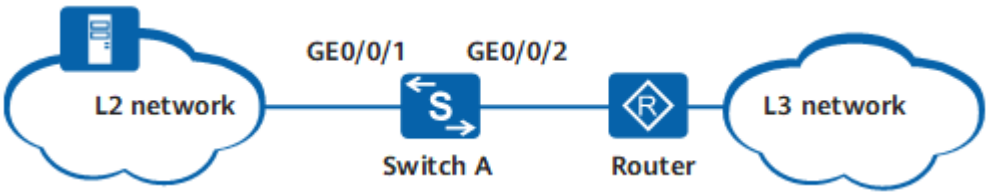
6.10 流量抑制及风暴控制配置举例

6.10.1 配置流量抑制示例

组网需求

如图6-3所示，SwitchA作为二层网络到三层路由器的衔接点，需要限制二层网络转发的广播、未知组播和未知单播报文，防止产生广播风暴，同时限制二三层网络转发的已知组播和已知单播报文，防止大流量冲击。

图 6-3 配置流量抑制组网图



配置思路

用如下的思路配置流量抑制。

1. 通过在GE0/0/1接口视图下配置流量抑制功能，限制二层网络转发的广播、未知组播和未知单播报文。
2. 通过GE0/0/1和GE0/0/2接口视图下配置流量抑制功能，限制二三层网络转发的已知组播和已知单播报文。

操作步骤

步骤1 进入接口GE0/0/1视图

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] interface gigabitethernet 0/0/1
```

步骤2 配置广播流量抑制，按百分比抑制，百分比值为80%。

```
[SwitchA-GigabitEthernet0/0/1] broadcast-suppression 80
```

步骤3 配置未知组播流量抑制，按百分比抑制，百分比值为80%。

```
[SwitchA-GigabitEthernet0/0/1] multicast-suppression 80
```

步骤4 配置未知单播流量抑制，按百分比抑制，百分比值为80%。

```
[SwitchA-GigabitEthernet0/0/1] unicast-suppression 80
```

步骤5 配置已知组播流量抑制，按百分比抑制，百分比值为80%。

```
[SwitchA-GigabitEthernet0/0/1] known-multicast-suppression 80
```

步骤6 配置已知单播流量抑制，按百分比抑制，百分比值为80%。

```
[SwitchA-GigabitEthernet0/0/1] known-unicast-suppression 80
[SwitchA-GigabitEthernet0/0/1] quit
```

步骤7 进入接口GE0/0/2视图

```
[SwitchA] interface gigabitethernet 0/0/2
```

步骤8 配置已知组播流量抑制，按百分比抑制，百分比值为80%。

```
[SwitchA-GigabitEthernet0/0/2] known-multicast-suppression 80
```

步骤9 配置已知单播流量抑制，按百分比抑制，百分比值为80%。

```
[SwitchA-GigabitEthernet0/0/2] known-unicast-suppression 80
[SwitchA-GigabitEthernet0/0/2] quit
```

步骤10 验证配置结果

执行命令**display flow-suppression interface**查看GE0/0/1接口下的流量抑制配置情况。

```
[SwitchA] display flow-suppression interface gigabitethernet 0/0/1
 storm type        rate mode   set rate value
```

```
--------------------------------------------------------------------------------
 unknown-unicast    percent     percent: 80%
 multicast          percent     percent: 80%
 broadcast          percent     percent: 80%
 known-unicast      percent     percent: 80%
 known-multicas     percent     percent: 80%
--------------------------------------------------------------------------------
```

执行命令**display flow-suppression interface**查看GE0/0/2接口下的流量抑制配置情况。

```
[SwitchA] display flow-suppression interface gigabitethernet 0/0/2
 storm type         rate mode   set rate value
--------------------------------------------------------------------------------
 unknown-unicast    percent     percent: 100%
 multicast          percent     percent: 100%
 broadcast          percent     percent: 10%
 known-unicast      percent     percent: 80%
 known-multicas     percent     percent: 80%
--------------------------------------------------------------------------------
```

----结束

配置文件

SwitchA的配置文件

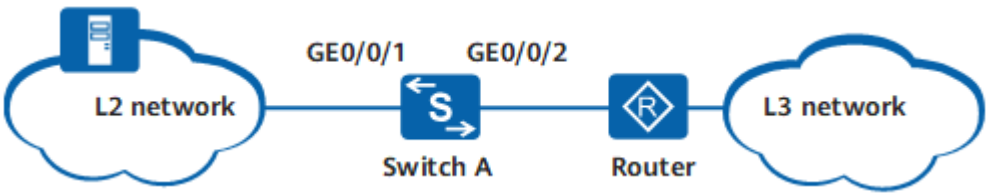
```
#
sysname SwitchA
#
interface GigabitEthernet0/0/1
 unicast-suppression 80
 multicast-suppression 80
 broadcast-suppression 80
 known-unicast-suppression 80
 known-multicast-suppression 80
#
#
interface GigabitEthernet0/0/2
 known-unicast-suppression 80
 known-multicast-suppression 80
#
return
```

6.10.2 配置风暴控制示例

组网需求

如图6-4所示，SwitchA作为二层网络到三层路由器的衔接点，需要防止二层网络转发的广播、未知组播或未知单播报文产生广播风暴。

图 6-4 配置风暴控制组网图



配置思路

用如下的思路配置风暴控制。

1. 通过在GE0/0/1接口视图下配置风暴控制功能，实现防止二层网络转发的广播、未知组播或未知单播报文产生广播风暴。

操作步骤

步骤1 进入接口视图

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] interface gigabitethernet0/0/1
```

步骤2 配置广播风暴控制

```
[SwitchA-GigabitEthernet0/0/1] storm-control broadcast min-rate 1000 max-rate 2000
```

步骤3 配置未知组播风暴控制

```
[SwitchA-GigabitEthernet0/0/1] storm-control multicast min-rate 1000 max-rate 2000
```

步骤4 配置未知单播风暴控制

```
[SwitchA-GigabitEthernet0/0/1] storm-control unicast min-rate 1000 max-rate 2000
```

步骤5 配置风暴控制的动作为阻塞报文

```
[SwitchA-GigabitEthernet0/0/1] storm-control action block
```

步骤6 配置打开风暴控制时记录日志的功能

```
[SwitchA-GigabitEthernet0/0/1] storm-control enable log
```

步骤7 配置风暴控制的检测时间间隔

```
[SwitchA-GigabitEthernet0/0/1] storm-control interval 90
[SwitchA-GigabitEthernet0/0/1] quit
```

步骤8 验证配置结果

执行命令**display storm-control interface**查看GE0/0/1接口下的风暴控制配置情况。

```
[SwitchA] display storm-control interface gigabitethernet 0/0/1
-------------------------------------------------------------------------------
PortName     Type      Rate      Mode Action   Punish-  Trap Log Int Last-
                         (Min/Max)             Status              Punish-Time
-------------------------------------------------------------------------------
GE0/0/1      Broadcast 1000      Pps  Block    Normal   Off  On  90  -
                         /2000
GE0/0/1      Multicast 1000      Pps  Block    Normal   Off  On  90  -
                         /2000
GE0/0/1      Unicast   1000      Pps  Block    Normal   Off  On  90  -
                         /2000
-------------------------------------------------------------------------------
```

----结束

配置文件

SwitchA的配置文件

```
#
sysname SwitchA
#
interface GigabitEthernet0/0/1
 storm-control broadcast min-rate 1000 max-rate 2000
 storm-control multicast min-rate 1000 max-rate 2000
 storm-control unicast min-rate 1000 max-rate 2000
```

```
 storm-control interval 90
 storm-control action block
 storm-control enable log
#
return
```

6.11 流量抑制及风暴控制常见配置错误

6.11.1 广播流量抑制无效

故障现象

接口配置了广播流量抑制功能后，仍然出现了广播报文引起的广播风暴，导致正常流量中断。

常见原因

本类故障的常见原因主要包括：

- 接口下没有配置广播流量抑制或者配置的广播流量抑制值过大。
- 广播风暴报文在入接口没有丢弃。

说明

- 请保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。
- 本文以广播流量抑制故障处理为例，未知组播和未知单播流量抑制的故障处理步骤与此类似。

操作步骤

步骤1 检查接口下的流量抑制配置。

用户视图下执行命令**display flow-suppression interface** *interface-type interface-number*，查看输出信息中**broadcast**字段对应的**rate mode**和**set rate value**值，看其是否合适：

- 如果不合适，请在接口视图下执行命令**broadcast-suppression** { *percent-value* | **packets** *packets-per-second* }修改广播流量抑制参数。
- 如果合适，执行步骤2。

步骤2 检查广播报文在接口入方向是否被丢弃。

有两种方法：

- 用户视图下执行命令**display interface** *interface-type interface-number*，查看输出信息中**Input bandwidth utilization**是否在抑制前后有较大变化。正常情况下，在配置流量抑制之后，接口丢弃超过阈值限制的报文，接口带宽利用率会降低。如果没有变化或变化很小，请执行步骤3。
- 准备另外一个接口B，将要检查的接口A（即配置流量抑制的接口）和接口B加入相同VLAN，查看接口B的出方向流量是否为接口A上配置的抑制后的流量。如果不是，说明报文没有在接口A的入方向被丢弃。请执行步骤3。

步骤3 请收集如下信息，并联系技术支持人员。

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

----结束

7 ARP 安全配置

7.1 ARP 安全简介

定义

ARP（Address Resolution Protocol）安全是针对ARP攻击的一种安全特性，它通过一系列对ARP表项学习和ARP报文处理的限制、检查等措施来保证网络设备的安全性。ARP安全特性不仅能够防范针对ARP协议的攻击，还可以防范网段扫描攻击等基于ARP协议的攻击。

目的

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，容易被攻击者利用。在网络中，常见的ARP攻击方式主要包括：

- ARP泛洪攻击，也叫拒绝服务攻击DoS（Denial of Service），主要存在这样两种场景：
  - 设备处理ARP报文和维护ARP表项都需要消耗系统资源，同时为了满足ARP表项查询效率的要求，一般设备都会对ARP表项规模有规格限制。攻击者就利

用这一点，通过伪造大量源IP地址变化的ARP报文，使得设备ARP表资源被无效的ARP条目耗尽，合法用户的ARP报文不能继续生成ARP条目，导致正常通信中断。

- 攻击者利用工具扫描本网段主机或者进行跨网段扫描时，会向设备发送大量目标IP地址不能解析的IP报文，导致设备触发大量ARP Miss消息，生成并下发大量临时ARP表项，并广播大量ARP请求报文以对目标IP地址进行解析，从而造成CPU（Central Processing Unit）负荷过重。

- ARP欺骗攻击，是指攻击者通过发送伪造的ARP报文，恶意修改设备或网络内其他用户主机的ARP表项，造成用户或网络的报文通信异常。

ARP攻击行为存在以下危害：

- 会造成网络连接不稳定，引发用户通信中断。
- 利用ARP欺骗截取用户报文，进而非法获取游戏、网银、文件服务等系统的帐号和口令，造成被攻击者重大利益损失。

为了避免上述ARP攻击行为造成的各种危害，可以部署ARP安全特性。

受益

- 可以有效降低用户为保证网络正常运行和网络信息安全而产生的维护成本。
- 可以为用户提供更安全的网络环境和更稳定的网络服务。

7.2 ARP 安全原理描述

7.2.1 ARP 报文限速

如果设备对收到的大量ARP报文全部进行处理，可能导致CPU负荷过重而无法处理其他业务。因此，在处理之前，设备需要对ARP报文进行限速，以保护CPU资源。

设备提供了如下几类针对ARP报文的限速功能：

- 根据源IP地址进行ARP报文限速

  当设备检测到某一个用户在短时间内发送大量的ARP报文，可以针对该用户配置基于源IP地址的ARP报文限速。在1秒时间内，如果该用户的ARP报文数目超过设定阈值（ARP报文限速值），则丢弃超出阈值部分的ARP报文。

  根据源IP地址进行ARP报文限速：如果指定IP地址，则针对指定源IP地址的ARP报文根据限速值进行限速；如果不指定IP地址，则针对每一个源IP地址的ARP报文根据限速值进行限速。

- 针对全局、VLAN和接口的ARP报文限速

  设备支持在全局、VLAN和接口下配置ARP报文的限速值和限速时间，当同时在全局、VLAN和接口下配置ARP报文的限速值和限速时间时，设备会先按照接口进行限速，再按照VLAN进行限速，最后按照全局进行限速。

  另外，在接口下还可以指定阻塞ARP报文的时间段。如果设备的某个接口在ARP报文限速时间内接收到的ARP报文数目超过了设定阈值（ARP报文限速值），则丢弃超出阈值部分的ARP报文，并在接下来的一段时间内（即阻塞ARP报文时间段）持续丢弃该接口下收到的所有ARP报文。

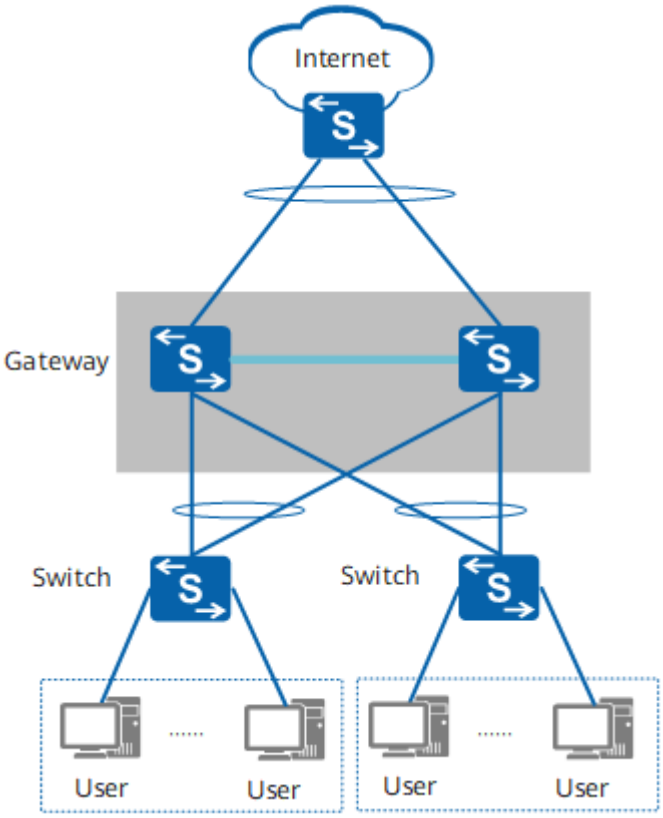
  - 针对全局的ARP报文限速：在设备出现ARP攻击时，限制全局处理的ARP报文数量。

- 针对VLAN的ARP报文限速：在某个VLAN内的所有接口出现ARP攻击时，限制处理收到的该VLAN内的ARP报文数量，配置本功能可以保证不影响其他VLAN内所有接口的ARP学习。
- 针对接口的ARP报文限速：在某个接口出现ARP攻击时，限制处理该接口收到的ARP报文数量，配置本功能可以保证不影响其他接口的ARP学习。

7.2.2 ARP 优化应答

如图7-1所示，如果多台设备组建的堆叠系统作为接入网关时，会收到大量请求本系统接口MAC地址的ARP请求报文。如果全部将这些ARP报文上送主交换机处理，将会导致主交换机CPU使用率过高，影响CPU对正常业务的处理。

图 7-1 ARP 优化应答典型组网应用



为了避免上述危害，可以使能ARP优化应答功能，提高设备防御ARP泛洪攻击的能力。使能该功能后，堆叠系统会进行如下判断：

- 对于目的IP是本系统接口IP地址的ARP请求报文，该接口所在的交换机直接回复ARP应答报文。
- 对于目的IP不是本系统接口IP地址的ARP请求报文，如果主交换机上配置了VLAN内Proxy ARP功能，接口所在的交换机会判断ARP请求报文是否满足代理条件，如果满足，则该接口所在的交换机直接回复ARP应答报文；如果不满足，堆叠系统会丢弃该报文。

说明

盒式交换机在非堆叠环境下，可以配置ARP优化应答功能，但是没有优化效果。

缺省情况下，ARP优化应答功能处于使能状态。因此在收到ARP请求报文后，堆叠系统首先查看是否有该ARP请求报文中源IP对应的ARP表项。

- 如果对应的ARP表项存在，堆叠系统对该ARP请求报文进行优化应答。
- 如果对应的ARP表项不存在，堆叠系统不对ARP请求报文的应答进行优化。

7.2.3 ARP 表项严格学习

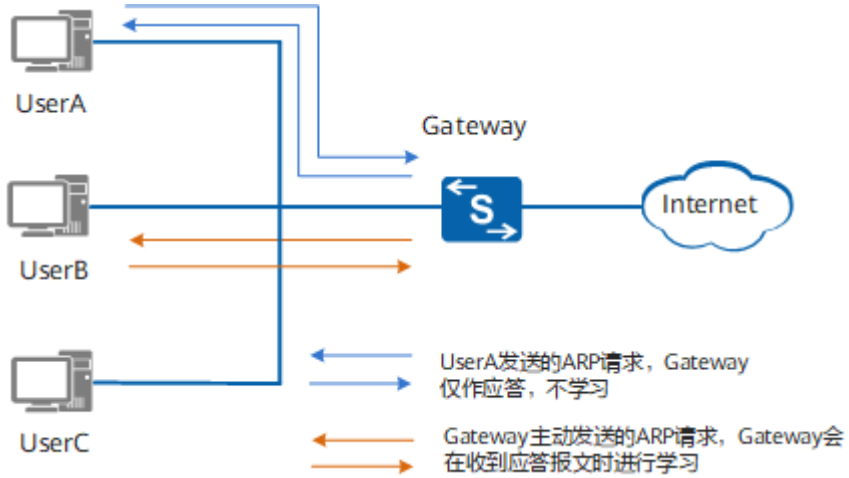
如果大量用户在同一时间段内向设备发送大量ARP报文，或者攻击者伪造正常用户的ARP报文发送给设备，则会造成下面的危害：

- 设备因处理大量ARP报文而导致CPU负荷过重，同时设备学习大量的ARP报文可能导致设备ARP表项资源被无效的ARP条目耗尽，造成合法用户的ARP报文不能继续生成ARP条目，进而导致用户无法正常通信。
- 伪造的ARP报文将错误地更新设备的ARP表项，导致用户无法正常通信。

为避免上述危害，可以在网关设备上部署ARP表项严格学习功能。

ARP表项严格学习是指只有本设备主动发送的ARP请求报文的应答报文才能触发本设备学习ARP，其他设备主动向本设备发送的ARP报文不能触发本设备学习ARP，这样，可以拒绝大部分的ARP报文攻击。

图 7-2 ARP 表项严格学习



如图7-2所示。通常情况下，当UserA向Gateway发送ARP请求报文后，Gateway会向UserA回应ARP应答报文，并且添加或更新UserA对应的ARP表项。当Gateway配置ARP表项严格学习功能以后：

- 对于Gateway收到UserA发送来的ARP请求报文，Gateway不添加也不更新UserA对应的ARP表项。如果该请求报文请求的是Gateway的MAC地址，那么Gateway会向UserA回应ARP应答报文。
- 如果Gateway向UserB发送ARP请求报文，待收到与该请求对应的ARP应答报文后，Gateway会添加或更新UserB对应的ARP表项。

7.2.4 ARP 表项限制

ARP表项限制功能应用在网关设备上，可以限制设备的某个接口学习动态ARP表项的数目。默认状态下，接口可以学习的动态ARP表项数目规格与全局的ARP表项规格保持一

致。当部署完ARP表项限制功能后，如果指定接口下的动态ARP表项达到了允许学习的最大数目，将不再允许该接口继续学习动态ARP表项，以保证当一个接口所接入的某一用户主机发起ARP攻击时不会导致整个设备的ARP表资源都被耗尽。

7.2.5 禁止接口学习 ARP 表项

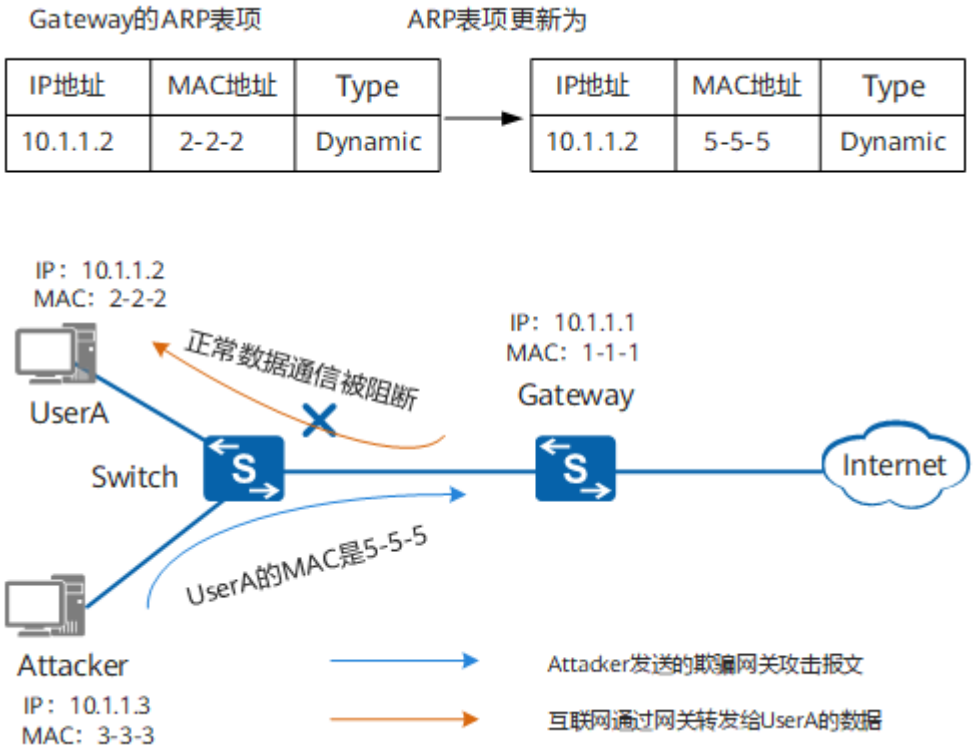
当某接口下学习了大量动态ARP表项时，出于安全考虑可以配置禁止该接口的动态ARP表项学习功能，以防止该接口下所接入的用户主机发起ARP攻击使整个设备的ARP表资源都被耗尽。

禁止接口学习ARP表项功能和ARP表项严格学习功能配合起来使用，可以使设备对接口下动态ARP的学习进行更加细致的控制。

7.2.6 ARP 表项固化

如图7-3所示，Attacker仿冒UserA向Gateway发送伪造的ARP报文，导致Gateway的ARP表中记录了错误的UserA地址映射关系，造成UserA接收不到正常的数据报文。

图 7-3 欺骗网关攻击示意图



为了防御这种欺骗网关攻击，可以在网关设备上部署ARP表项固化功能。网关设备在第一次学习到ARP以后，不再允许用户更新此ARP表项或只能允许更新此ARP表项的部分信息，或者通过发送单播ARP请求报文的方式对更新ARP条目的报文进行合法性确认。

设备提供的三种ARP表项固化模式，如表7-1所示。

表 7-1 ARP 表项固化模式介绍

固化模式	功能
fixed-all模式	如果设备收到的ARP报文中的MAC地址、接口或VLAN信息和ARP表中的信息不匹配，则直接丢弃该ARP报文。此模式适用于用户MAC地址固定，并且用户接入位置相对固定的场景。
fixed-mac模式	如果设备收到的ARP报文中的MAC地址与ARP表中对应条目的MAC地址不匹配，则直接丢弃该ARP报文；如果匹配，但是收到报文的接口或VLAN信息与ARP表中对应条目不匹配，则可以更新对应ARP条目中的接口和VLAN信息。此模式适用于用户MAC地址固定，但用户接入位置频繁变动的场景。
send-ack模式	如果设备收到的ARP报文A涉及ARP表项MAC地址、接口或VLAN信息的修改，设备不会立即更新ARP表项，而是先向待更新的ARP表项现有MAC地址对应的用户发送一个单播的ARP请求报文进行确认。 • 如果在随后的3秒内设备收到ARP应答报文B，且当前ARP条目中的IP地址、MAC地址、接口和VLAN信息与ARP应答报文B的一致，则认为ARP报文A为攻击报文，不更新该ARP条目。 • 如果在随后的3秒内设备未收到ARP应答报文，或者收到ARP应答报文B与当前ARP条目中的IP地址、MAC地址、接口和VLAN信息不一致，设备会再向刚才收到的ARP报文A对应的源MAC发送一个单播ARP请求报文。 – 如果在随后的3秒内收到ARP应答报文C，且ARP报文A与ARP应答报文C的源IP地址、源MAC地址、接口和VLAN信息一致，则认为现有ARP条目已经无效且ARP报文A是可以更新该ARP条目的合法报文，并根据ARP报文A来更新该ARP条目。 – 如果在随后的3秒内未收到ARP应答报文，或者ARP报文A与收到的ARP应答报文C的源IP地址、源MAC地址、接口和VLAN信息不一致，则认为ARP报文A为攻击报文，设备会忽略收到的ARP报文A，ARP条目不会更新。 此模式适用于用户的MAC地址和接入位置均频繁变动的场景。

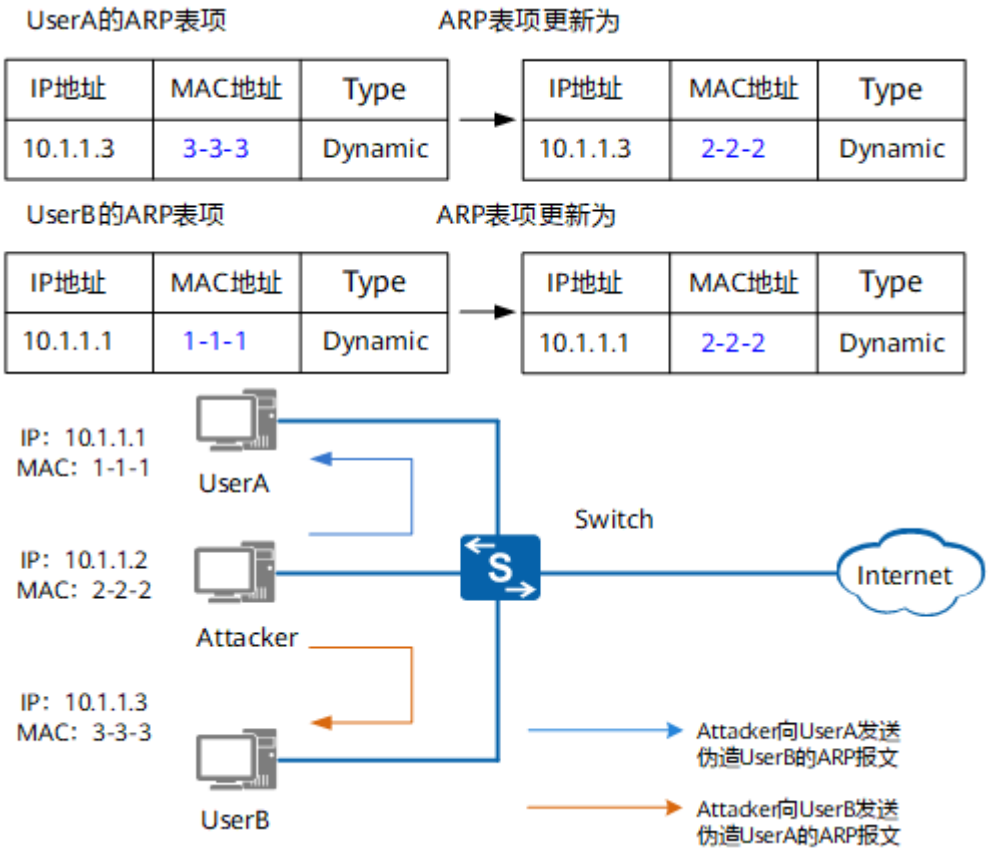
7.2.7 动态 ARP 检测（DAI）

网络中针对ARP的攻击层出不穷，中间人攻击是常见的ARP欺骗攻击方式之一。

中间人攻击（Man-in-the-middle attack）是指攻击者与通讯的两端分别创建独立的联系，并交换其所收到的数据，使通讯的两端认为与对方直接对话，但事实上整个会话都被攻击者完全控制。在中间人攻击中，攻击者可以拦截通讯双方的通话并插入新的内容。

如图7-4所示，是中间人攻击的一个场景。攻击者主动向UserA发送伪造UserB的ARP报文，导致UserA的ARP表中记录了错误的UserB地址映射关系，攻击者可以轻易获取到UserA原本要发往UserB的数据；同样，攻击者也可以轻易获取到UserB原本要发往UserA的数据。这样，UserA与UserB间的信息安全无法得到保障。

图 7-4 中间人攻击



为了防御中间人攻击，可以在Switch上部署动态ARP检测DAI（Dynamic ARP Inspection）功能。

动态ARP检测是利用绑定表来防御中间人攻击的。当设备收到ARP报文时，将此ARP报文对应的源IP、源MAC、VLAN以及接口信息和绑定表的信息进行比较，如果信息匹配，说明发送该ARP报文的用户是合法用户，允许此用户的ARP报文通过，否则就认为是攻击，丢弃该ARP报文。

说明

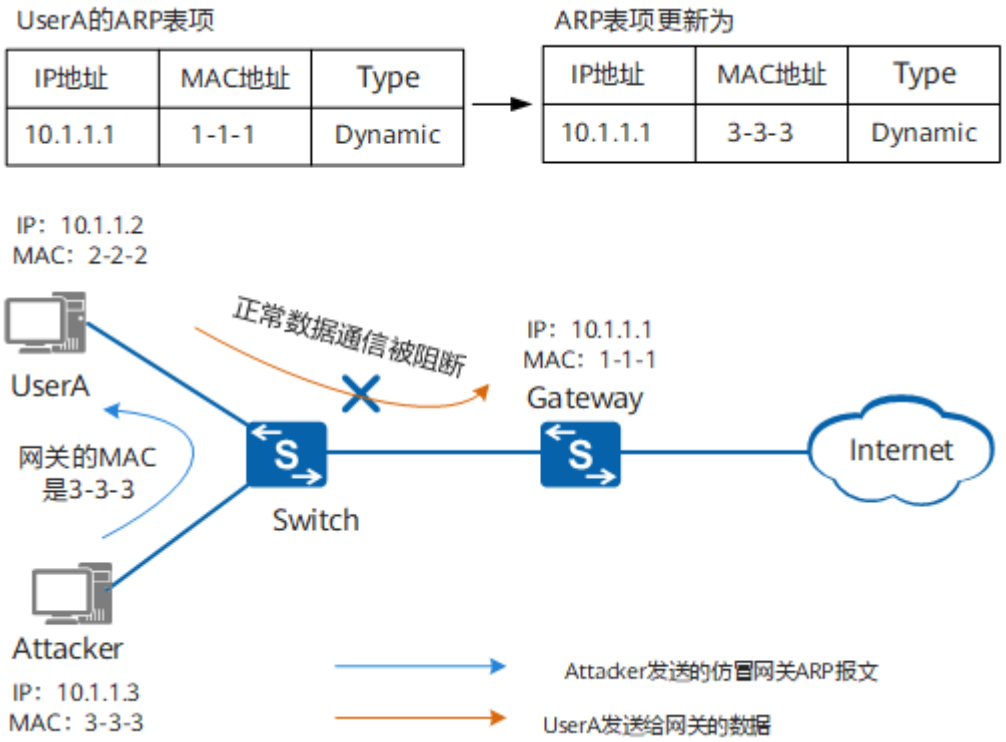
动态ARP检测功能仅适用于DHCP Snooping场景。设备使能DHCP Snooping功能后，当DHCP用户上线时，设备会自动生成DHCP Snooping绑定表；对于静态配置IP地址的用户，设备不会生成DHCP Snooping绑定表，所以需要手动添加静态绑定表。关于DHCP Snooping的详细介绍，请参见**DHCP Snooping的基本原理**中的描述。

当Switch上部署动态ARP检测功能后，如果攻击者连接到Switch并试图发送伪造的ARP报文，Switch会根据绑定表检测到这种攻击行为，对该ARP报文进行丢弃处理。如果Switch上同时使能了动态ARP检测丢弃报文告警功能，则当ARP报文因不匹配绑定表而被丢弃的数量超过了告警阈值时，Switch会发出告警通知管理员。

7.2.8 发送免费 ARP 报文

如**图7-5**所示，Attacker仿冒网关向UserA发送了伪造的ARP报文，导致UserA的ARP表中记录了错误的网关地址映射关系，从而正常的数据不能被网关接收。

图 7-5 仿冒网关攻击



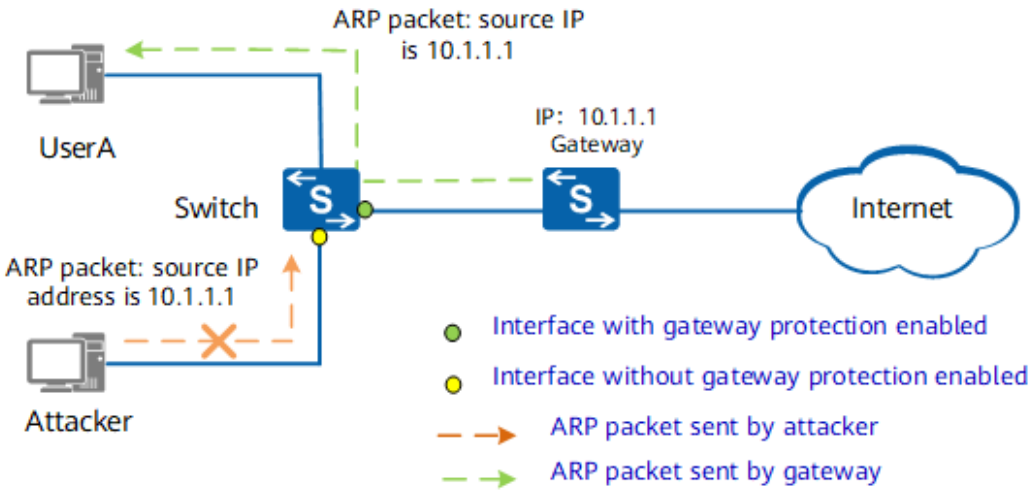
为了避免上述危害，可以在网关设备上部署发送免费ARP报文功能，定期更新用户的ARP表项，使得用户ARP表项中记录的是正确的网关MAC地址。

7.2.9 ARP 网关保护

如图7-6所示，当网络中存在攻击者Attacker仿冒网关或用户误配主机IP地址为网关地址时，其发送的ARP报文会使得网络中其他用户误以为Attacker即网关，造成正常用户跟网关的数据通信中断。在设备与网关相连的接口上配置ARP网关保护功能，可以防止伪造网关攻击。当源IP地址为网关地址10.1.1.1的ARP报文到达设备时：

- 开启对网关IP地址10.1.1.1保护功能的接口：正常接收转发该ARP报文。
- 未开启对网关IP地址10.1.1.1保护功能的接口：丢弃该ARP报文。

图 7-6 ARP 网关保护



7.2.10 ARP 报文内 MAC 地址一致性检查

ARP报文内MAC地址一致性检查功能主要应用于网关设备上，可以防御以太网数据帧首部中的源/目的MAC地址和ARP报文中的源/目的MAC地址不同的ARP攻击。

部署本功能后，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/目的MAC地址和ARP报文中的源/目的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。

7.2.11 ARP 报文合法性检查

ARP报文合法性检查功能可以部署在接入设备或网关设备上，用来对MAC地址和IP地址不合法的报文进行过滤。设备支持以下三种可以任意组合的检查。

- 源MAC地址检查：设备会检查ARP报文中的源MAC地址和以太网数据帧首部中的源MAC地址是否一致，一致则认为合法，否则丢弃报文；
- 目的MAC地址检查：设备会检查ARP应答报文中的目的MAC地址是否和以太网数据帧首部中的目的MAC地址一致，一致则认为合法，否则丢弃报文；
- IP地址检查：设备会检查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。

7.2.12 DHCP 触发 ARP 学习

在DHCP用户场景下，当DHCP用户数目很多时，设备进行大规模ARP表项的学习和老化会对设备性能和网络环境形成冲击。

为了避免此问题， 可以在网关设备上部署DHCP触发ARP学习功能。当DHCP服务器给用户分配了IP地址，网关设备会根据VLANIF接口上收到的DHCP ACK报文直接生成该用户的ARP表项。该功能生效的前提是使能DHCP Snooping功能。

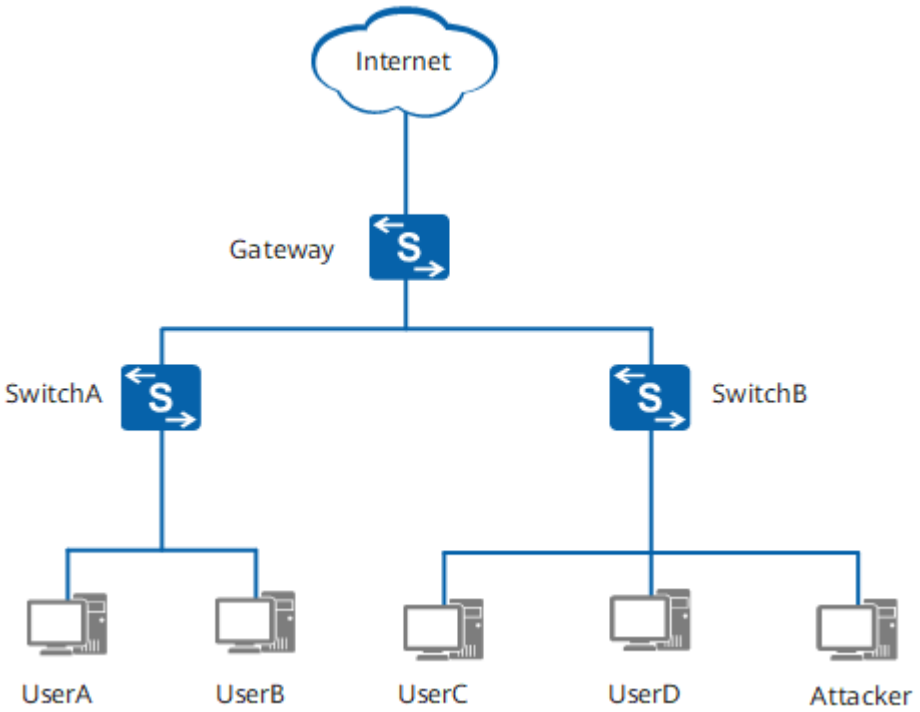
网关设备上还可同时部署动态ARP检测功能，防止DHCP用户的ARP表项被伪造的ARP报文恶意修改。

7.3 ARP 安全应用场景

7.3.1 防 ARP 泛洪攻击

如图7-7所示，局域网中用户通过SwitchA和SwitchB接入连接到Gateway访问Internet。当网络中出现过多的ARP报文时，会导致网关设备CPU负载加重，影响设备正常处理用户的其它业务。另一方面，网络中过多的ARP报文会占用大量的网络带宽，引起网络堵塞，从而影响整个网络通信的正常运行。

图 7-7 防 ARP 泛洪攻击组网



为了避免上述危害，可以在网关设备上部署防ARP泛洪攻击功能，包括ARP报文限速功能、ARP表项严格学习功能以及ARP表项限制功能。

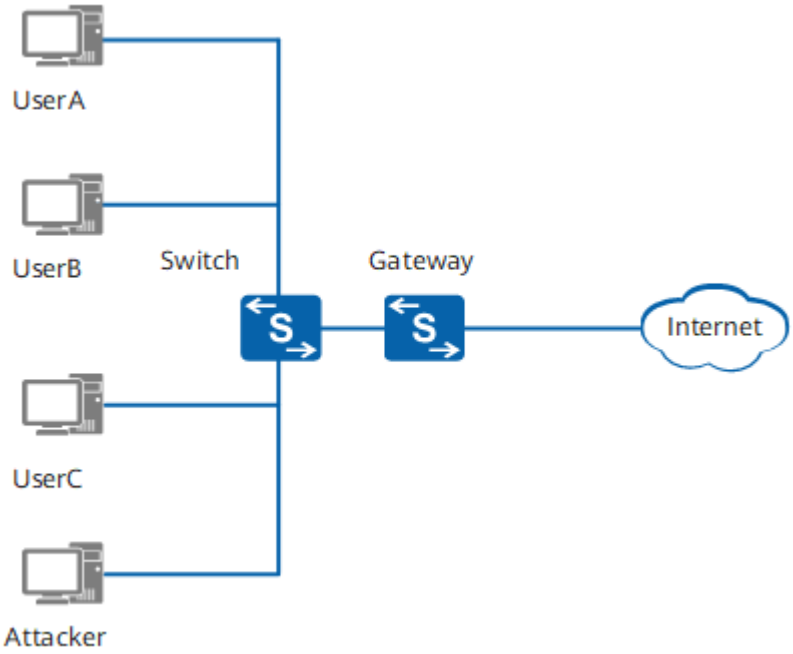
- 部署**ARP报文限速**功能后，Gateway会对收到的ARP报文进行数量统计，如果在一定时间内，ARP报文的数量超出了配置的阈值（ARP报文限速值），则丢弃超出阈值部分的ARP报文，这样可以防止设备因处理大量ARP报文造成CPU负荷过重。
- 部署**ARP表项严格学习**功能后，Gateway仅仅学习自己发送的ARP请求报文的应答报文，并不学习其它设备主动向Gateway发送的ARP报文，这样可以防止Gateway因学习大量ARP报文而导致ARP表项资源被无效的ARP条目耗尽。
- 部署**ARP表项限制**功能后，Gateway会对各个接口学习动态ARP表项的数目进行限制。当指定接口下的动态ARP表项达到允许学习的最大数目后，将不允许新增动态ARP表项，这样可以防止一个接口所接入的某一用户主机发起ARP攻击而导致整个设备的ARP表资源都被耗尽。

7.3.2 防 ARP 欺骗攻击

如图7-8所示，局域网中UserA、UserB、UserC等用户通过Switch接入连接到Gateway访问Internet。

正常情况下，UserA、UserB、UserC上线之后，通过相互之间交互ARP报文，UserA、UserB、UserC和Gateway上都会创建相应的ARP表项。此时，如果有攻击者通过在广播域内发送伪造的ARP报文，篡改Gateway或者UserA、UserB、UserC上的ARP表项，攻击者可以轻而易举地窃取UserA、UserB、UserC的信息或者阻碍UserA、UserB、UserC正常访问网络。

图 7-8 防 ARP 欺骗攻击组网



为了避免上述危害，可以在网关设备上部署防ARP欺骗攻击功能，包括ARP表项固化功能、ARP表项严格学习功能、发送免费ARP报文等功能。如果局域网中的用户大多是DHCP用户，还可以在接入设备上部署动态ARP检测功能。

- 部署**ARP表项固化**功能后，Gateway在第一次学习到ARP之后，不再允许用户更新此ARP表项或只能更新此ARP表项的部分信息，或者通过发送单播ARP请求报文的方式对更新ARP条目的报文进行合法性确认，这样可以防止攻击者伪造ARP报文修改网关上其他用户的ARP表项。
- 部署**ARP表项严格学习**功能后，Gateway仅仅学习自己向UserA、UserB或UserC发送的ARP请求报文的应答报文，不学习攻击者主动向Gateway发送的ARP报文，并且不允许攻击者主动发送的ARP报文更新Gateway上现有的ARP条目，这样可以防止攻击者冒充其他用户修改网关上对应的ARP表项。
- 部署**发送免费ARP报文**功能后，Gateway主动向用户发送以自己IP地址为目标IP地址的ARP请求报文，定时更新用户ARP表项的网关MAC地址，这样可以防止用户的报文不能正常的转发到网关或者被恶意攻击者窃听。
- 部署**动态ARP检测**功能后，当Switch收到ARP报文时，将此ARP报文中的源IP、源MAC、收到ARP报文的接口及VLAN信息和绑定表的信息进行比较，如果信息匹

配，则认为是合法用户，允许此用户的ARP报文通过，否则认为是攻击，丢弃该ARP报文，这样可以有效防止中间人攻击。

7.4 ARP 安全配置注意事项

涉及网元

无需其他网元配合。

License 支持

本特性是交换机的基本特性，无需获得License许可即可应用此功能。

V200R021C00、V200R021C01 版本特性支持情况

S600-E系列交换机中所有款型均支持ARP安全。

说明

如需了解交换机软件配套详细信息，请点击**Info-Finder**。

特性依赖和限制

- 当针对全局、VLAN、接口的ARP报文限速以及根据源IP地址进行ARP报文限速中的多个限速功能同时配置时，设备对同时满足这些限速条件的ARP报文以其中最小的限速值进行限速。
- 在系统资源充足的情况下，设备最多支持在10个VLAN下使能DAI功能。
- 在同一接口下同时配置用户认证和使能ARP Snooping功能时，用户上线时的首个ARP报文不会触发ARP Snooping学习和ARP Snooping表项的生成，后续的ARP报文才会触发ARP Snooping学习并生成ARP Snooping表项。

7.5 ARP 安全缺省配置

ARP安全的缺省配置如**表7-2**所示。

表 7-2 ARP 安全缺省配置

参数	缺省值
ARP报文限速（根据源IP地址）	设备允许1秒内最多只能有30个同一个源IP地址的ARP报文通过
ARP报文限速（针对全局、VLAN和接口）	未使能
ARP报文的限速值、限速时间（针对全局、VLAN和接口）	在1秒内设备最多允许100个ARP报文通过
持续丢弃超过限速值的接口下所有ARP报文的功能	未使能

参数	缺省值
ARP报文限速丢弃告警功能（针对全局、VLAN和接口）	未使能
ARP报文限速丢弃告警阈值（针对全局、VLAN和接口）	100
临时ARP表项的老化时间	3秒
ARP优化应答功能	已使能
ARP表项严格学习功能	未使能
基于接口的ARP表项限制	在规格范围内，设备对接口能够学习到的最大动态ARP表项数目没有限制
ARP表项固化功能	未使能
动态ARP检测功能	未使能
发送ARP免费报文功能	未使能
发送免费ARP报文的时间间隔	60秒
ARP报文内MAC地址一致性检查功能	未使能
ARP报文合法性检查功能	未使能
DHCP触发ARP学习功能	未使能

7.6 配置防 ARP 泛洪攻击

前置任务

在配置防ARP泛洪攻击之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为Up。

配置流程

在配置防ARP泛洪攻击任务中，各配置步骤均是并列关系，无严格配置顺序，用户根据需要选择配置即可。

7.6.1 配置 ARP 报文限速（根据源 IP 地址）

背景信息

设备处理大量源IP地址相对固定的ARP报文（例如同一个源IP地址的ARP报文对应的MAC地址或出接口信息不断发生跳变），会造成CPU繁忙，影响到正常业务的处理。

为了避免此问题，可以在网关设备上配置设备根据源IP地址进行ARP报文限速。设备会对上送CPU的ARP报文根据源IP地址进行统计，如果在1秒内收到的同一个源IP地址的ARP报文超过设定阈值（ARP报文限速值），设备则丢弃超出阈值部分的ARP报文。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 配置根据源IP地址进行ARP报文限速

- 执行命令**arp speed-limit source-ip maximum** *maximum*，配置根据任意源IP地址进行ARP报文限速的限速值。
- 执行命令**arp speed-limit source-ip** *ip-address* **maximum** *maximum*，配置对指定IP地址用户的ARP报文进行限速的限速值。

两种配置同时存在的情况下，当ARP报文源IP地址匹配限速指定的IP地址时，对该源IP地址的ARP报文限速值为后一步骤中配置的*maximum*值；否则为前一步骤中配置的*maximum*值。

缺省情况下，设备允许1秒内最多只能有同一个源IP地址的30个ARP报文通过。

设备使能ARP优化应答功能后（通过**undo arp optimized-reply disable**命令配置，缺省情况下，ARP优化应答功能处于使能状态），根据源IP地址进行ARP报文限速不生效。

----结束

7.6.2 配置 ARP 报文限速（针对全局、VLAN 和接口）

背景信息

如果设备对收到的大量ARP报文全部进行处理，可能导致CPU负荷过重而无法处理其他业务。因此，在处理之前，设备需要对ARP报文进行限速，以保护CPU资源。

使能ARP报文限速功能后，可以在全局、VLAN或接口下配置ARP报文的限速值和限速时间。在ARP报文限速时间内，如果收到的ARP报文数目超过ARP报文限速值，设备会丢弃超出限速值的ARP报文。

- 针对全局的ARP报文限速：在设备出现ARP攻击时，限制全局处理的ARP报文数量。
- 针对VLAN的ARP报文限速：在某个VLAN内的所有接口出现ARP攻击时，限制处理收到的该VLAN内的ARP报文数量，配置本功能可以保证不影响其他VLAN内所有接口的ARP学习。
- 针对接口的ARP报文限速：在某个接口出现ARP攻击时，限制处理该接口收到的ARP报文数量，配置本功能可以保证不影响其他接口的ARP学习。

当同时在全局、VLAN和接口下配置ARP报文的限速值和限速时间时，设备会先按照接口进行限速，再按照VLAN进行限速，最后按照全局进行限速。

当设备丢弃的ARP报文数量较多时，如果希望设备能够以告警的方式提醒网络管理员，则可以使能ARP报文限速丢弃告警功能。当丢弃的ARP报文数超过告警阈值时，设备将产生告警。

建议在网关设备上进行如下配置。

说明

当接入设备上部署了**MFF**功能时，为了避免MFF模块处理过多的过路ARP报文（即ARP报文的目的IP地址不是该报文接收接口的IP地址）导致CPU负荷过重，则可以在接入设备上部署针对全局、VLAN和接口的ARP报文限速功能。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 （可选）执行命令**interface** *interface-type interface-number*，进入接口视图；或执行命令**vlan** *vlan-id*，进入VLAN视图。

在系统视图下配置ARP报文限速功能无需执行此步骤。

步骤3 执行命令**arp anti-attack rate-limit enable**，使能ARP报文限速功能。

缺省情况下，未使能ARP报文限速功能。

设备使能ARP优化应答功能后（通过**undo arp optimized-reply disable**命令配置，缺省情况下，ARP优化应答功能处于使能状态），根据全局、VLAN和接口进行ARP报文限速不生效。

步骤4 执行命令**arp anti-attack rate-limit packet** *packet-number* [**interval** *interval-value* | **block-timer** *timer*] *，配置ARP报文的限速值、限速时间，以及当某个接口的ARP报文超过限速值时，在后续一段时间内持续丢弃该接口下收到的所有ARP报文的功能（即开启**block**模式）。

系统视图和VLAN视图下不支持**block timer** *timer*参数。

缺省情况下，在1秒内设备最多允许100个ARP报文通过，且未配置当某个接口的ARP报文超过限速值时，在后续一段时间内持续丢弃该接口下收到的所有ARP报文的功能。

说明

该命令在非**block**模式下只对上送CPU的ARP报文进行限速，对芯片转发的报文不会产生影响；在**block**模式下，仅在接口下上送CPU的ARP报文超过限速值时会触发**block**，触发后设备会持续丢弃该接口下的所有ARP报文。

步骤5 （可选）执行命令**arp anti-attack rate-limit alarm enable**，使能ARP报文限速丢弃告警功能。

缺省情况下，未使能ARP报文限速丢弃告警功能。

步骤6 （可选）执行命令**arp anti-attack rate-limit alarm threshold** *threshold*，配置ARP报文限速丢弃告警阈值。

缺省情况下，ARP报文限速丢弃告警阈值为100。

----结束

7.6.3 配置临时 ARP 表项的老化时间

背景信息

当IP报文触发ARP Miss消息时，设备会根据ARP Miss消息生成临时ARP表项，并且向目的网段发送ARP请求报文。

- 在临时ARP表项老化时间范围内：
  - 设备收到ARP应答报文前，匹配临时ARP表项的IP报文将被丢弃并且不会触发ARP Miss消息。
  - 设备收到ARP应答报文后，则生成正确的ARP表项来替换临时ARP表项。

- 当老化时间超时后，设备会清除临时ARP表项。此时如果设备转发IP报文匹配不到对应的ARP表项，则会重新触发ARP Miss消息并生成临时ARP表项，如此循环重复。

故可以通过配置临时ARP表项的老化时间来控制ARP Miss消息的触发频率。当判断设备受到攻击时，可以调大该时间，减小设备ARP Miss消息的触发频率，从而减小攻击对设备的影响。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**arp-fake expire-time** *expire-time*，配置临时ARP表项的老化时间。

缺省情况下，临时ARP表项的老化时间是3秒。

----结束

7.6.4 配置 ARP 优化应答

背景信息

如果多台设备组建的堆叠系统作为接入网关时，会收到大量请求本系统接口MAC地址的ARP请求报文。如果全部将这些ARP报文上送主交换机处理，将会导致主交换机CPU使用率过高，影响CPU对正常业务的处理。

为了避免上述危害，可以使能ARP优化应答功能，提高设备防御ARP泛洪攻击的能力。使能该功能后，堆叠系统会进行如下判断：

- 对于目的IP是本系统接口IP地址的ARP请求报文，该接口所在的交换机直接回复ARP应答报文。
- 对于目的IP不是本系统接口IP地址的ARP请求报文，如果主交换机上配置了VLAN内Proxy ARP功能，接口所在的交换机会判断ARP请求报文是否满足代理条件，如果满足，则该接口所在的交换机直接回复ARP应答报文；如果不满足，堆叠系统会丢弃该报文。

说明

盒式交换机在非堆叠环境下，可以配置ARP优化应答功能，但是没有优化效果。

缺省情况下，ARP优化应答功能处于使能状态。因此在收到ARP请求报文后，堆叠系统首先查看是否有该ARP请求报文中源IP对应的ARP表项。

- 如果对应的ARP表项存在，堆叠系统对该ARP请求报文进行优化应答。
- 如果对应的ARP表项不存在，堆叠系统不对ARP请求报文的应答进行优化。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**undo arp optimized-reply disable**，使能ARP优化应答功能。

   缺省情况下，ARP优化应答功能处于使能状态。
   - 设备不支持对携带双层VLAN tag的ARP请求报文进行ARP优化代答。
   - 设备仅支持对VLANIF接口接收到的ARP请求报文进行ARP优化应答。

- 以下配置会导致全局或相应接口的ARP优化应答功能不生效：
  - 执行命令**ip address** *ip-address* { *mask* | *mask-length* } **sub**，接口上配置了从IP地址。
  - 执行命令**arp ip-conflict-detect enable**，使能了设备的IP地址冲突检测功能。
  - 执行命令**arp anti-attack check user-bind enable**，使能了动态ARP检测功能。

    说明

    物理接口视图下使能了动态ARP检测功能，仅使能动态ARP检测功能的物理接口所在设备ARP优化应答功能不生效。Eth-trunk接口视图或者VLAN视图下使能动态ARP检测功能，全局ARP优化应答功能不生效。
  - 执行命令**dhcp snooping arp security enable**，使能了出口ARP检测功能。
  - 执行命令**arp-proxy enable**，使能了路由式ARP代理功能。
  - 执行命令**arp-proxy inter-sub-vlan-proxy enable**，使能VLAN间ARP代理功能。
- 设备使能ARP优化应答功能后，以下功能不生效：
  - 根据源IP地址进行ARP报文限速功能（通过**arp speed-limit source-ip**命令配置）
  - 针对全局、VLAN和接口进行ARP报文限速（通过**arp anti-attack rate-limit enable**等命令配置）

7.6.5 配置 ARP 表项严格学习

背景信息

如果大量用户在同一时间段内向设备发送大量ARP报文，或者攻击者伪造正常用户的ARP报文发送给设备，则会造成如下危害：

- 设备因处理大量ARP报文而导致CPU负荷过重，同时设备学习大量的ARP报文可能导致设备ARP表项资源被无效的ARP条目耗尽，造成合法用户的ARP报文不能继续生成ARP条目，导致用户无法正常通信。
- 伪造的ARP报文将错误地更新设备ARP表项，导致合法用户无法正常通信。

为避免上述危害，可以在网关设备上配置ARP表项严格学习功能。配置该功能后，只有本设备主动发送的ARP请求报文的应答报文才能触发本设备学习ARP，其他设备主动向本设备发送的ARP报文不能触发本设备学习ARP，这样，可以拒绝大部分的ARP报文攻击。

ARP表项严格学习功能可在全局和接口视图下进行配置。

- 全局使能该功能，则设备的所有接口均进行ARP表项严格学习。
- 接口视图下使能该功能，则只有该接口进行ARP表项严格学习。

当同时在全局和接口视图下进行配置时，接口下配置的优先级高于全局配置的优先级。

说明

在全局使能ARP表项严格学习功能的前提下：

- 如果在指定接口下执行命令**arp learning strict force-disable**，则该接口将会被强制执行去使能ARP表项严格学习的功能。
- 如果在指定接口下执行命令**arp learning strict trust**时，则该接口的ARP表项严格学习功能和全局的配置保持一致。

由于有些用户主机上安装的防火墙会阻止其收到ARP请求时发送ARP应答或网卡无法回复ARP应答，所以使能ARP表项严格学习功能后，如果设备上触发了ARP Miss消息，则设备主动发出的ARP请求将无法得到该用户的ARP应答，从而使设备无法学习到该用户的ARP。在这种场景下，如果仅是个别用户出现该问题，则可以为其配置静态ARP，具体配置请参见《S600-E V200R021C00, C01 配置指南-IP业务》ARP配置 中的“配置静态ARP”；如果该问题在用户中非常普遍，则建议去使能ARP表项严格学习功能。

操作步骤

- 配置全局ARP表项严格学习功能
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**arp learning strict**，配置全局ARP表项严格学习功能。

     缺省情况下，未使能ARP表项严格学习功能。
- 配置接口的ARP表项严格学习功能
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**arp learning strict** { **force-enable** | **force-disable** | **trust** }，配置接口的ARP表项严格学习功能。

     缺省情况下，未使能ARP表项严格学习功能。

----结束

7.6.6 配置基于接口的 ARP 表项限制

背景信息

为了防止当一个接口所接入的某一用户主机发起ARP攻击时导致整个设备的ARP表资源都被耗尽，可以在指定接口下配置接口能够学习到的最大动态ARP表项数目。当指定接口下的动态ARP表项达到允许学习的最大数目后，将不允许新增动态ARP表项。

建议在网关设备上进行如下配置。

操作步骤

- 配置二层接口的ARP表项限制
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**arp-limit vlan** *vlan-id1* [**to** *vlan-id2*] **maximum** *maximum*，配置基于二层接口的ARP表项限制。

     缺省情况下，在规格范围内，设备对接口能够学习到的最大动态ARP表项数目没有限制。

- 配置VLANIF接口的ARP表项限制
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface vlanif** *vlan-id*，进入VLANIF接口视图。
  c. 执行命令**arp-limit maximum** *maximum*，配置基于VLANIF接口的ARP表项限制。

     缺省情况下，在规格范围内，设备对接口能够学习到的最大动态ARP表项数目没有限制。

----结束

7.6.7 配置禁止接口学习 ARP 表项

背景信息

当某接口下出现大量动态ARP表项时，出于安全考虑建议在网关设备上配置禁止该接口学习ARP表项的功能，以防止该接口下所接入的用户主机发起ARP攻击使整个设备的ARP表资源都被耗尽。

禁止ARP学习前，如果接口上已经有动态学习到的ARP表项，系统并不会自动删除这些表项。用户可以根据需要，手动删除或保留这些已经学习到的动态ARP表项。

须知

禁止接口下的动态ARP学习能力，可能会造成转发不通，用户配置时需要注意。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface vlanif** *interface-number*，进入VLANIF接口视图。

步骤3 执行命令**arp learning disable**，禁止接口学习动态ARP表项。

缺省情况下，接口下的动态ARP表项学习功能处于使能状态。

----结束

7.6.8 检查防 ARP 泛洪攻击的配置结果

操作步骤

- 使用命令**display arp anti-attack configuration** { **arp-rate-limit** | **arp-speed-limit** | **entry-check** | **log-trap-timer** | **packet-check** | **all** }，查看ARP防攻击配置。
- 使用命令**display arp-limit** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*]，查看接口可以学习到的动态ARP表项数目的最大值。
- 使用命令**display arp learning strict**，查看全局和所有VLANIF接口上的ARP表项严格学习情况。

----结束

7.7 配置防 ARP 欺骗攻击

前置任务

在配置防ARP欺骗攻击之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为Up。

配置流程

在配置防ARP欺骗攻击任务中，各配置步骤均是并列关系，无严格配置顺序，用户根据需要选择配置即可。

7.7.1 配置 ARP 表项固化

背景信息

为了防止ARP地址欺骗攻击，可以在网关设备上配置ARP表项固化功能。三种ARP表项固化模式适用于不同的应用场景，且是互斥关系。

- **fixed-mac**方式：设备收到的ARP报文中的MAC地址与ARP表中对应条目的MAC地址不匹配，则直接丢弃该ARP报文；如果匹配，但是收到报文的接口或VLAN信息与ARP表中对应条目不匹配，则可以更新对应ARP条目中的接口和VLAN信息。此方式适用于用户MAC地址固定，但用户接入位置频繁变动的场景。当用户从不同接口接入设备时，设备上该用户对应的ARP表项中的接口信息可以及时更新。
- **fixed-all**方式：只有当ARP报文对应的MAC地址、接口、VLAN信息和ARP表项中的信息完全匹配时，设备才可以更新ARP表项的其他内容。此方式适用于用户MAC地址固定，并且用户接入位置相对固定的场景。
- **send-ack**方式：设备收到一个涉及MAC地址、VLAN、接口修改的ARP报文时，不会立即更新ARP表项，而是先向待更新的ARP表项现有MAC地址对应的用户发送一个单播的ARP请求报文进行确认，根据确认结果再决定是否更新ARP表项中的MAC地址、VLAN和接口信息。此方式适用于用户的MAC地址和接入位置均频繁变动的场景。

可在全局和VLANIF接口下配置ARP表项固化功能。

- 全局配置该功能后，默认设备上所有接口的ARP表项固化功能均已使能。
- 当全局和VLANIF接口下同时配置了该功能时，VLANIF接口下的配置优先生效。

操作步骤

- 全局使能ARP表项固化功能
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**arp anti-attack entry-check** { **fixed-mac** | **fixed-all** | **send-ack** } **enable**，配置ARP表项固化功能。

     缺省情况下，未配置ARP表项固化功能。
- 接口使能ARP表项固化功能
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface vlanif** *vlan-id*，进入VLANIF接口视图。

c. 执行命令**arp anti-attack entry-check** { **fixed-mac** | **fixed-all** | **send-ack** } **enable**，配置ARP表项固化功能。

缺省情况下，未配置ARP表项固化功能。

----结束

7.7.2 配置动态 ARP 检测（DAI）

背景信息

为了防御中间人攻击，避免合法用户的数据被中间人窃取，可以执行本命令使能动态ARP检测功能。设备会将ARP报文对应的源IP、源MAC、接口和VLAN信息与绑定表中的信息进行比较，如果信息匹配，说明发送该ARP报文的用户是合法用户，允许此用户的ARP报文通过，否则就认为是攻击，丢弃该ARP报文。

可在接口视图或VLAN视图下使能动态ARP检测功能。在接口视图下使能时，则对该接口收到的所有ARP报文进行绑定表匹配检查；在VLAN视图下使能时，则对加入该VLAN的接口收到的属于该VLAN的ARP报文进行绑定表匹配检查。

当设备丢弃的不匹配绑定表的ARP报文数量较多时，如果希望设备能够以告警的方式提醒网络管理员，则可以使能动态ARP检测丢弃报文告警功能。当丢弃的ARP报文数超过告警阈值时，设备将产生告警。

说明

当网关设备上部署了DHCP触发ARP学习功能时，则可以在网关设备上部署本功能。

本功能仅适用于DHCP Snooping场景。设备使能DHCP Snooping功能后，当DHCP用户上线时，设备会自动生成DHCP Snooping绑定表；对于静态配置IP地址的用户，设备不会生成DHCP Snooping绑定表，所以需要手动添加静态绑定表。DHCP Snooping的配置，请参见**9 DHCP Snooping配置**。静态绑定表的配置，请参见**13.7.1 配置基于静态绑定表的IPSG**。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图；或者执行命令**vlan** *vlan-id*，进入VLAN视图。

步骤3 执行命令**arp anti-attack check user-bind enable**，使能动态ARP检测功能（即对ARP报文进行绑定表匹配检查功能）。

缺省情况下，未使能动态ARP检测功能。

在系统资源充足的情况下，设备最多支持在400个VLAN下使能DAI功能。

步骤4 （可选）接口视图下执行命令**arp anti-attack check user-bind check-item** { **ip-address** | **mac-address** | **vlan** } *，或者在VLAN视图下执行命令**arp anti-attack check user-bind check-item** { **ip-address** | **mac-address** | **interface** } *，配置对ARP报文进行绑定表匹配检查的检查项。

缺省情况下，对ARP报文的IP地址、MAC地址、VLAN和接口信息都进行检查。

如果希望仅匹配绑定表某一项或某两项内容的特殊ARP报文也能够通过，则可以配置对ARP报文进行绑定表匹配检查时只检查某一项或某两项内容。

说明

IP地址包括IPv4地址和IPv6地址，即配置ARP报文绑定表匹配检查的检查项为IP地址时，设备将对ARP报文的IPv4地址和IPv6地址都进行绑定表匹配检查。

指定ARP报文绑定表匹配检查项对配置了静态绑定表的用户不起作用，即设备仍然按照静态绑定表的内容对ARP报文进行绑定表匹配检查。

当同时在VLAN和加入该VLAN的接口下配置了动态ARP检测功能，设备会先按照接口下配置的检查选项对ARP报文进行绑定表匹配检查，如果ARP报文检查通过，设备再根据VLAN下配置的检查选项进行检查。

步骤5 （可选）执行命令**arp anti-attack check user-bind alarm enable**，使能动态ARP检测丢弃报文告警功能。

缺省情况下，未使能动态ARP检测丢弃报文告警功能。

步骤6 （可选）**arp anti-attack check user-bind alarm threshold** *threshold*，配置动态ARP检测丢弃报文告警阈值。

缺省情况下，动态ARP检测丢弃报文告警阈值为系统视图下**arp anti-attack check user-bind alarm threshold** *threshold*命令配置的值。如果系统视图下没有配置该值，则接口、VLAN下缺省的告警阈值为100。

步骤7 配置信任接口

将与合法DHCP服务器直接或间接连接的接口配置为信任接口，否则回程报文会因匹配不到绑定表而被丢弃，导致业务不通。配置为信任接口后，从信任接口收到的报文不做匹配检查直接允许通过。

1. 在系统视图下执行命令**dhcp enable**，全局使能DHCP功能。

   缺省情况下，没有全局使能DHCP功能。
2. 执行命令**dhcp snooping enable**，全局使能DHCP Snooping功能。

   缺省情况下，没有全局使能DHCP Snooping功能。
3. 执行命令**interface** *interface-type interface-number*，进入接口视图；或者执行命令**vlan** *vlan-id*，进入VLAN视图。
4. 执行命令**dhcp snooping enable**，使能接口或VLAN下的DHCP Snooping功能。

   缺省情况下，接口和VLAN未使能DHCP Snooping功能。
5. 在接口视图下执行命令**dhcp snooping trusted**，或在VLAN视图中执行**dhcp snooping trusted interface** *interface-type interface-number*，配置接口为信任状态。

   缺省情况下，接口为非信任状态。

----结束

7.7.3 配置发送 ARP 免费报文

背景信息

如果有攻击者向其他用户发送仿冒网关的ARP报文，会导致其他用户的ARP表中记录错误的网关地址映射关系，造成其他用户的正常数据不能被网关接收。此时可以在网关设备上配置发送免费ARP报文的功能，用来定期更新合法用户的ARP表项，使得合法用户ARP表项中记录的是正确的网关地址映射关系。

可在全局或VLANIF接口下配置发送免费ARP报文功能。

- 全局配置该功能后，则默认设备上所有接口的发送ARP免费报文功能均已使能。
- 当全局和VLANIF接口下同时配置了该功能时，VLANIF接口下的配置优先生效。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 （可选）执行命令**interface vlanif** *interface-number*，进入VLANIF接口视图。

说明

在系统视图下配置发送ARP免费报文功能无需执行此步骤。

步骤3 执行命令**arp gratuitous-arp send enable**，使能发送免费ARP报文的功能。

缺省情况下，未使能发送免费ARP报文的功能。

步骤4 （可选）执行命令**arp gratuitous-arp send interval** *interval-time*，配置发送免费ARP报文的时间间隔。

缺省情况下，发送免费ARP报文的时间间隔为60秒。

----结束

7.7.4 配置 ARP 网关保护功能

背景信息

当网络中存在攻击者Attacker仿冒网关或用户误配主机IP地址为网关地址时，其发送的ARP报文会使得网络中其他用户误以为Attacker即网关，造成正常用户跟网关的数据通信中断。在设备与网关相连的接口上配置ARP网关保护功能，可以防止伪造网关攻击。当来自网关的ARP报文到达设备时：

- 开启对网关地址保护功能的接口：正常接收转发该ARP报文。
- 未开启对网关地址保护功能的接口：丢弃该ARP报文。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**arp trust source** *ip-address*，开启ARP网关保护功能，并配置被保护的网关IP地址。

缺省情况下，ARP网关保护功能处于关闭状态。

每个接口下最多可以指定8个被保护的网关IP地址，全局最多支持指定32个被保护的网关IP地址。全局在不同的接口下指定相同的网关IP地址，这种情况认为指定了多个被保护的网关IP地址。

----结束

7.7.5 配置 ARP 报文内 MAC 地址一致性检查

背景信息

ARP报文内MAC地址一致性检查功能主要应用于网关设备上，可以防御以太网数据帧首部中的源/目的MAC地址和ARP报文数据区中的源/目的MAC地址不同的ARP攻击。

配置ARP报文内MAC地址一致性检查后，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/目的MAC地址和ARP报文数据区中的源/目的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。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**arp validate** { **source-mac** | **destination-mac** } *，使能ARP报文内MAC地址一致性检查功能，即设备对以太网数据帧首部中的源/目的MAC地址和ARP报文数据区中的源/目的MAC地址进行一致性检查的功能。

缺省情况下，设备不对以太网数据帧首部中的源/目的MAC地址和ARP报文数据区中的源/目的MAC地址进行一致性检查。

说明

本命令不支持在VLANIF接口上配置。当VLANIF接口收到ARP报文时，ARP报文内MAC地址一致性检查遵循成员口下的检查规则。

----结束

7.7.6 配置 ARP 报文合法性检查

背景信息

为了防止非法ARP报文的攻击，可以在接入设备或网关设备上配置ARP报文合法性检查功能，用来对MAC地址和IP地址不合法的ARP报文进行过滤。设备提供以下三种可以任意组合的检查项配置：

- IP地址检查：设备会检查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。
- 源MAC地址检查：设备会检查ARP报文中的源MAC地址和以太网数据帧首部中的源MAC地址是否一致，一致则认为合法，否则丢弃报文。
- 目的MAC地址检查：设备会检查ARP应答报文中的目的MAC地址是否和以太网数据帧首部中的目的MAC地址一致，一致则认为合法，否则丢弃报文。

说明

通常，ARP报文中源MAC地址和以太网数据帧首部中的源MAC地址不一致的ARP报文，以及目的MAC地址和以太网数据帧首部中的目的MAC地址不一致的ARP应答报文均是ARP协议允许的ARP报文。因此，只有在网络管理员发现攻击产生后，通过报文头获取方式定位，确定是由于对应项不一致的ARP报文导致的攻击，才能指定ARP报文合法性检查时需要检查源MAC地址和检查目的MAC地址。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**arp anti-attack packet-check** { **ip** | **dst-mac** | **sender-mac** } *，使能ARP报文合法性检查功能，并指定ARP报文合法性检查项。

缺省情况下，未使能ARP报文合法性检查功能。

本命令为累积式命令。

----结束

7.7.7 配置 ARP 表项严格学习

背景信息

如果大量用户在同一时间段内向设备发送大量ARP报文，或者攻击者伪造正常用户的ARP报文发送给设备，则会造成如下危害：

- 设备因处理大量ARP报文而导致CPU负荷过重，同时设备学习大量的ARP报文可能导致设备ARP表项资源被无效的ARP条目耗尽，造成合法用户的ARP报文不能继续生成ARP条目，导致用户无法正常通信。
- 伪造的ARP报文将错误地更新设备ARP表项，导致合法用户无法正常通信。

为避免上述危害，可以在网关设备上配置ARP表项严格学习功能。配置该功能后，只有本设备主动发送的ARP请求报文的应答报文才能触发本设备学习ARP，其他设备主动向本设备发送的ARP报文不能触发本设备学习ARP，这样，可以拒绝大部分的ARP报文攻击。

ARP表项严格学习功能可在全局和接口视图下进行配置。

- 全局使能该功能，则设备的所有接口均进行ARP表项严格学习。
- 接口视图下使能该功能，则只有该接口进行ARP表项严格学习。

当同时在全局和接口视图下进行配置时，接口下配置的优先级高于全局配置的优先级。

说明

在全局使能ARP表项严格学习功能的前提下：

- 如果在指定接口下执行命令**arp learning strict force-disable**，则该接口将会被强制执行去使能ARP表项严格学习的功能。
- 如果在指定接口下执行命令**arp learning strict trust**时，则该接口的ARP表项严格学习功能和全局的配置保持一致。

由于有些用户主机上安装的防火墙会阻止其收到ARP请求时发送ARP应答或网卡无法回复ARP应答，所以使能ARP表项严格学习功能后，如果设备上触发了ARP Miss消息，则设备主动发出的ARP请求将无法得到该用户的ARP应答，从而使设备无法学习到该用户的ARP。在这种场景下，如果仅是个别用户出现该问题，则可以为其配置静态ARP，具体配置请参见《S600-E V200R021C00, C01 配置指南-IP业务》ARP配置 中的“配置静态ARP”；如果该问题在用户中非常普遍，则建议去使能ARP表项严格学习功能。

操作步骤

- 配置全局ARP表项严格学习功能
  a. 执行命令**system-view**，进入系统视图。

b. 执行命令**arp learning strict**，配置全局ARP表项严格学习功能。

缺省情况下，未使能ARP表项严格学习功能。

- 配置接口的ARP表项严格学习功能
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**arp learning strict** { **force-enable** | **force-disable** | **trust** }，配置接口的ARP表项严格学习功能。

  缺省情况下，未使能ARP表项严格学习功能。

----结束

7.7.8 配置 DHCP 触发 ARP 学习

背景信息

在DHCP用户场景下，当DHCP用户数目很多时，设备进行大规模ARP表项的学习和老化会对设备性能和网络环境形成冲击。

为了避免此问题，可以在网关设备上使能DHCP触发ARP学习功能。当DHCP服务器给用户分配了IP地址，网关设备会根据VLANIF接口上收到的DHCP ACK报文直接生成该用户的ARP表项。

说明

DHCP触发ARP学习功能生效的前提是通过命令**dhcp enable**使能DHCP功能。

网关设备上还可同时部署**动态ARP检测功能**，防止DHCP用户的ARP表项被伪造的ARP报文恶意修改。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface vlanif** *vlan-id*，进入VLANIF接口视图。

步骤3 执行命令**arp learning dhcp-trigger**，使能DHCP触发ARP学习功能。

缺省情况下，未使能DHCP触发ARP学习功能。

----结束

7.7.9 检查防 ARP 欺骗攻击的配置结果

操作步骤

- 使用命令**display arp anti-attack configuration** { **arp-rate-limit** | **arp-speed-limit** | **entry-check** | **log-trap-timer** | **packet-check** | **all** }，查看ARP防攻击配置。
- 使用命令**display arp anti-attack configuration check user-bind** [**vlan** [*vlan-id*] | **interface** [*interface-type interface-number*]]，查看VLAN或接口下动态ARP检测的相关配置。

- 使用命令**display arp learning strict**，查看全局和所有VLANIF接口上的ARP表项严格学习情况。

----结束

7.8 配置 ARP Snooping 功能

7.8.1 使能 ARP Snooping 功能

背景信息

在视频大联网运维方案中，网管需要获取网元的IP地址和MAC地址绘制拓扑，方便后期运维。对于不支持LLDP等协议的网元设备，可以在接入交换机上配置ARP Snooping功能。通过ARP报文触发学习ARP Snooping表，进而获取网元的IP地址和MAC地址等信息。

使能ARP Snooping功能后，设备将收到的ARP报文上送CPU处理。CPU对上送的ARP报文进行分析，获取ARP报文的源IP地址、源MAC地址、VLAN和入接口信息，建立记录用户信息的ARP Snooping表。

ARP Snooping表项创建后，老化时间默认为900秒。ARP Snooping表项基于ARP报文的源IP地址和VLAN信息创建，当收到源IP地址和VLAN信息与已存在的ARP Snooping表项中的IP地址和VLAN信息不一致的ARP报文时，新建ARP Snooping表项；当收到源IP地址和VLAN信息与已存在的ARP Snooping表项中的IP地址和VLAN信息一致的ARP报文时，则更新对应条目的MAC地址和接口信息，并重置老化计时器。

此外，设备会对即将老化的表项会做ARP探测，发送源IP地址为全零的probe ARP报文，目的IP地址为即将老化表项的IP地址。此时，如果对端为网关设备，则会识别收到的ARP报文为本机发送的免费ARP报文，并进行IP地址冲突检测，频繁生成冲突告警和日志。为了避免以上问题，可以对指定IP地址的ARP Snooping表项不进行ARP探测。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**arp snooping enable**，全局使能ARP Snooping功能。

缺省情况下，设备全局未使能ARP Snooping功能。

步骤3 在VLAN或接口下使能ARP Snooping功能。

1. 执行命令**vlan** *vlan-id*，进入VLAN视图；或执行命令**interface** *interface-type interface-number*，进入接口视图。
2. 执行命令**arp snooping enable**，使能VLAN或接口下的ARP Snooping功能。

   缺省情况下，VLAN或接口下未使能ARP Snooping功能。

在VLAN视图下执行此命令，则对该VLAN收到的所有ARP报文生效；在接口下执行该命令，则对该接口收到的所有ARP报文生效。

步骤4 （可选）执行命令**quit**，进行系统视图。

步骤5 （可选）执行命令**arp snooping detect ignored-ip**，配置对指定IP地址的ARP Snooping表项不进行ARP探测。

缺省情况下，设备对所有IP地址的ARP Snooping表项均进行ARP探测。

----结束

7.8.2 （可选）配置 ARP Snooping 表项固化功能

背景信息

为防止攻击者伪造ARP报文，导致设备的ARP Snooping表项学习到错误的用户地址映射关系，造成用户无法正常接收数据报文，可以在设备上使能ARP Snooping表项固化功能。使能ARP Snooping表项固化功能之后，一旦设备学习到某一ARP Snooping表项，便不再允许用户更新此ARP Snooping表项或只允许更新此ARP Snooping表项的部分信息，或者通过发送单播ARP请求报文的方式对更新ARP Snooping条目的报文进行合法性确认。设备提供三种ARP Snooping表项固化模式，适用于不同的应用场景，且是互斥关系。

- **fixed-mac**模式：该模式适用于用户MAC地址固定，但用户接入位置频繁变动的场景。当用户从设备的不同接口接入时，设备上该用户对应的ARP Snooping表项中的接口信息可以及时更新。
- **fixed-all**模式：该模式适用于用户MAC地址固定，并且用户接入位置相对固定的场景。
- **send-ack**模式：该模式适用于用户的MAC地址和接入位置均频繁变动的场景。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**arp snooping anti-attack entry-check** { **fixed-mac** | **fixed-all** | **send-ack** } **enable**，使能ARP Snooping表项固化功能。

缺省情况下，ARP Snooping表项固化功能处于未使能状态。

----结束

7.8.3 （可选）配置 ARP Snooping 检测功能

背景信息

为了防止中间人伪造ARP报文，导致通信双方学习到了对方错误的地址映射关系，造成合法用户的数据被中间人窃取，可以在设备上使能ARP Snooping检测功能。使能ARP Snooping检测功能之后，设备会将接收的ARP报文的源IP、源MAC、接口、VLAN信息和ARP Snooping表项中的信息进行比较。如果不存在和ARP报文的源IP地址和VLAN信息一致的ARP Snooping表项，则进行创建；如果存在和ARP报文的源IP地址和VLAN信息一致的ARP Snooping表项且所有信息匹配，说明发送该ARP报文的用户是合法用户，允许此用户的ARP报文通过，否则就丢弃该ARP报文。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**arp snooping anti-attack check enable**，使能接口下的ARP Snooping检测功能。

缺省情况下，接口下的ARP Snooping检测功能处于未使能状态。

----结束

7.9 维护 ARP 安全

7.9.1 监控 ARP 安全运行情况

操作步骤

- 执行命令**display arp packet statistics**，查看ARP处理的报文统计数据。
- 执行命令**display arp anti-attack statistics check user-bind interface** *interface-type interface-number*，查看接口下进行ARP报文绑定表匹配检查的ARP报文丢弃计数。
- 执行命令**display arp anti-attack packet-check statistics**，查看ARP报文合法性检查过程中被过滤的非法ARP报文统计数据。
- 执行命令**display arp optimized-reply status**，查看设备ARP优化应答功能的状态。
- 执行命令**display arp optimized-reply statistics** [**slot** *slot-id*]，查看ARP优化应答报文统计信息。
- 执行命令**display arp snooping** { **all** | **interface** *interface-type interface-number* | **vlan** *vlan-id* | **ip-address** *ip-address* | **mac-address** *mac-address* }，查看ARP Snooping绑定表信息。

----结束

7.9.2 清除 ARP 安全统计信息

背景信息

须知

清除统计信息后，以前的统计信息将无法恢复，务必仔细确认。

在确认需要清除运行信息后，请在用户视图下执行下列命令。

操作步骤

- 执行命令**reset arp packet statistics**，清除ARP报文的统计信息。
- 执行命令**reset arp anti-attack statistics check user-bind interface** *interface-type interface-number*，清除由于不匹配绑定表而丢弃的ARP报文计数。
- 执行命令**reset arp anti-attack statistics rate-limit**，清除由于ARP报文超过速率限制阈值而被丢弃的计数。
- 执行命令**reset arp optimized-reply statistics** [**slot** *slot-id*]，清除ARP优化应答报文统计信息。

- 执行命令**reset arp snooping** { **all** | **interface** *interface-type interface-number* | **vlan** *vlan-id* | **ip-address** *ip-address* | **mac-address** *mac-address* }，清除ARP Snooping表信息。

----结束

7.9.3 配置对潜在的 ARP 攻击行为发送告警

背景信息

在使能了根据源IP地址进行ARP报文限速功能后，在1秒内如果设备收到的ARP报文超过了设定的阈值，超出部分的ARP报文将被丢弃。此时设备认为这是一种潜在的攻击行为，会针对这种攻击行为向网管系统发送ARP告警，实时记录ARP运行的异常情况。通过配置发送告警的时间间隔，可以减少告警发送的数量，以避免ARP攻击时造成海量告警信息。

说明

该配置仅对**arp speed-limit source-ip**命令对应的根据源IP地址进行ARP报文限速功能的告警有效，对ARP安全特性的其他告警无效，其他告警均是固定每5分钟发送一次。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**arp anti-attack log-trap-timer** *time*，配置对潜在的ARP攻击行为发送告警的时间间隔。

缺省情况下，发送ARP告警时间间隔为0，即设备不发送ARP告警信息。

----结束

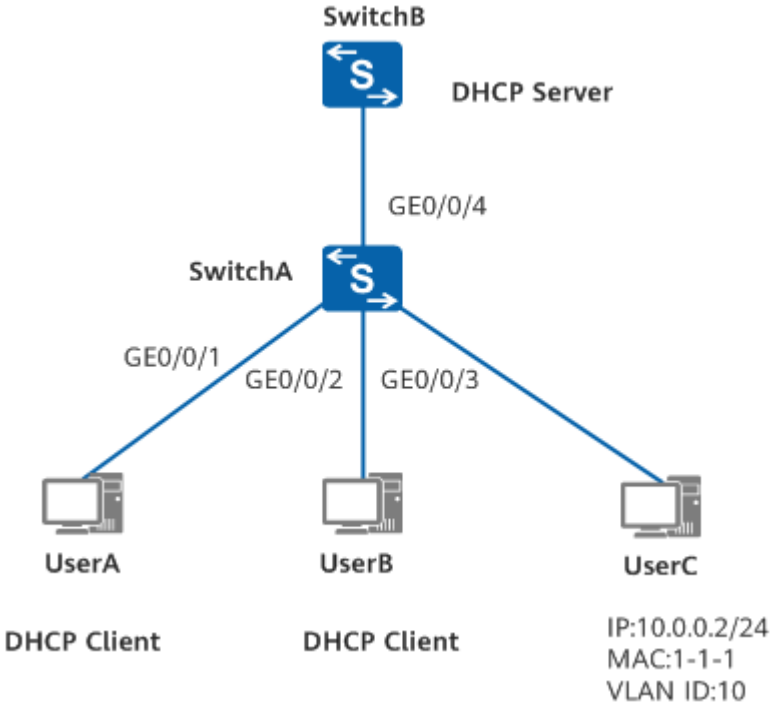
7.10 ARP 安全配置举例

7.10.1 配置防止 ARP 中间人攻击示例

组网需求

如图7-9所示，SwitchA通过接口GE0/0/4连接DHCP Server，通过接口GE0/0/1、GE0/0/2连接DHCP客户端UserA和UserB，通过接口GE0/0/3连接静态配置IP地址的用户UserC。SwitchA的接口GE0/0/1、GE0/0/2、GE0/0/3、GE0/0/4都属于VLAN10。管理员希望能够防止ARP中间人攻击，避免合法用户的数据被中间人窃取，同时希望能够了解当前ARP中间人攻击的频率和范围。

图 7-9 配置防止 ARP 中间人攻击组网图



配置思路

采用如下思路在SwitchA上进行配置：

1. 使能动态ARP检测功能，使SwitchA对收到的ARP报文对应的源IP、源MAC、VLAN以及接口信息进行DHCP Snooping绑定表匹配检查，实现防止ARP中间人攻击。
2. 使能动态ARP检测丢弃报文告警功能，使SwitchA开始统计丢弃的不匹配DHCP Snooping绑定表的ARP报文数量，并在丢弃数量超过告警阈值时能以告警的方式提醒管理员，这样可以使管理员根据告警信息以及报文丢弃计数来了解当前ARP中间人攻击的频率和范围。
3. 配置DHCP Snooping功能，并配置静态绑定表，使动态ARP检测功能生效。

操作步骤

步骤1 创建VLAN，将接口加入到VLAN中

创建VLAN10，并将接口GE0/0/1、GE0/0/2、GE0/0/3、GE0/0/4加入VLAN10中。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 10
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type access
[SwitchA-GigabitEthernet0/0/1] port default vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type access
[SwitchA-GigabitEthernet0/0/2] port default vlan 10
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type access
[SwitchA-GigabitEthernet0/0/3] port default vlan 10
```

```
[SwitchA-GigabitEthernet0/0/3] quit
[SwitchA] interface gigabitethernet 0/0/4
[SwitchA-GigabitEthernet0/0/4] port link-type trunk
[SwitchA-GigabitEthernet0/0/4] port trunk allow-pass vlan 10
[SwitchA-GigabitEthernet0/0/4] quit
```

步骤2 使能动态ARP检测功能和动态ARP检测丢弃报文告警功能

在接口GE0/0/1、GE0/0/2、GE0/0/3下使能动态ARP检测功能和动态ARP检测丢弃报文告警功能。以GE0/0/1为例，GE0/0/2、GE0/0/3的配置与GE0/0/1接口类似，不再赘述。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] arp anti-attack check user-bind enable
[SwitchA-GigabitEthernet0/0/1] arp anti-attack check user-bind alarm enable
[SwitchA-GigabitEthernet0/0/1] quit
```

步骤3 配置DHCP Snooping功能

全局使能DHCP Snooping功能。

```
[SwitchA] dhcp enable
[SwitchA] dhcp snooping enable
```

在VLAN10内使能DHCP Snooping功能。

```
[SwitchA] vlan 10
[SwitchA-vlan10] dhcp snooping enable
[SwitchA-vlan10] quit
```

配置接口GE0/0/4为DHCP Snooping信任接口。

```
[SwitchA] interface gigabitethernet 0/0/4
[SwitchA-GigabitEthernet0/0/4] dhcp snooping trusted
[SwitchA-GigabitEthernet0/0/4] quit
```

配置静态绑定表。

```
[SwitchA] user-bind static ip-address 10.0.0.2 mac-address 0001-0001-0001 interface gigabitethernet 0/0/3 vlan 10
```

步骤4 验证配置结果

执行命令**display arp anti-attack configuration check user-bind interface**，查看各接口下动态ARP检测的配置信息，以GE0/0/1为例。

```
[SwitchA] display arp anti-attack configuration check user-bind interface gigabitethernet 0/0/1
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
```

执行命令**display arp anti-attack statistics check user-bind interface**，查看各接口下动态ARP检测的ARP报文丢弃计数，以GE0/0/1为例。

```
[SwitchA] display arp anti-attack statistics check user-bind interface gigabitethernet 0/0/1
 Dropped ARP packet number is 966
 Dropped ARP packet number since the latest warning is 605
```

由显示信息可知，接口GE0/0/1下产生了ARP报文丢弃计数，表明防ARP中间人攻击功能已经生效。

当在各接口下多次执行命令**display arp anti-attack statistics check user-bind interface**时，管理员可根据显示信息中“Dropped ARP packet number is”字段值的变化来了解ARP中间人攻击频率和范围。

----结束

配置文件

SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 10
#
dhcp enable
#
dhcp snooping enable
user-bind static ip-address 10.0.0.2 mac-address 0001-0001-0001 interface GigabitEthernet0/0/3 vlan 10
#
vlan 10
 dhcp snooping enable
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 10
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 10
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 10
 dhcp snooping trusted
#
return
```

7.11 ARP 安全 FAQ

7.11.1 为什么交换机上 ARP 无法动态迁移

如果发现设备上存在ARP表项的VLAN、MAC地址、接口信息无法迁移的情况，请重点检查设备上是否配置了ARP防攻击相关策略，如**arp anti-attack entry-check** { **fixed-mac** | **fixed-all** | **send-ack** } **enable**。此策略会导致ARP表项的相关信息无法动态迁移。

7.11.2 使能 ARP 严格学习功能后，有时候用户已经学到了交换机的 ARP，为什么交换机主动 Ping 用户也无法学习到用户的 ARP?

使能ARP严格学习功能后，交换机只会根据自己发出的ARP请求报文的应答报文来学习ARP。

有些用户计算机上安装的防火墙会阻止计算机在收到ARP请求时发送ARP应答或有些用户计算机的网卡无法回复ARP应答。这时，不管是交换机主动Ping还是用户发送数据报文到交换机触发ARP-Miss消息，交换机主动发出的ARP请求都无法得到该用户的ARP应答，故无法主动学习到用户的ARP。

在这种场景下，如果是个别用户出现此类问题，可以为其配置静态ARP；如果问题在用户中比较普遍，则建议去使能交换机的ARP严格学习功能。

7.11.3 使能 DAI 功能后，合法的 ARP 报文为什么不再线速转发了

DAI功能的实现是通过软件对报文进行合法性检查，合法报文是软转发出去的，转发速率跟ARP报文的CPCAR值以及CPU负载等因素相关。

7.11.4 使能 DAI 功能的 VLAN 下配置 VLANIF 接口后，客户端能否 Ping 通对应 VLANIF 接口下配置的 IP 地址

当VLAN或VLAN所在的端口使能了DAI功能，并且对应的VLAN配置了VLANIF接口时，如果要从该VLAN或者端口Ping通VLANIF接口的IP地址，则需要Ping报文的源IP地址匹配DHCP Snooping静态绑定表时才可Ping通。

7.11.5 如何针对静态用户进行 ARP 攻击防范?

静态用户是指配置静态IP地址的用户，比如打印机和服务器等哑终端，一般都是为其分配静态IP地址。攻击者通常利用认证用户IP地址连接网络，进行ARP攻击，导致网络通信异常。

为了防范ARP攻击，对于静态用户，可以配置静态用户绑定表和动态ARP检测DAI（即对ARP报文进行绑定表匹配检查）功能。

静态用户绑定表可以通过**user-bind static**命令来配置。动态ARP检测功能可以通过**arp anti-attack check user-bind enable**命令来使能。

配置后，当设备收到ARP报文时，将此ARP报文对应的源IP、源MAC、VLAN以及接口信息和静态绑定表的信息进行比较，如果信息匹配，说明发送该ARP报文的用户是合法用户，允许此用户的ARP报文通过，否则就认为是攻击，丢弃该ARP报文。

8 端口安全配置

8.1 端口安全简介

端口安全（Port Security）通过将接口学习到的动态MAC地址转换为安全MAC地址（包括安全动态MAC、安全静态MAC和Sticky MAC），阻止非法用户通过本接口和交换机通信，从而增强设备的安全性。

8.2 端口安全原理描述

安全 MAC 地址的分类

安全MAC地址分为：安全动态MAC、安全静态MAC与Sticky MAC。

表 8-1 安全 MAC 地址的说明

类型	定义	特点
安全动态MAC地址	使能端口安全而未使能Sticky MAC功能时转换的MAC地址。	设备重启后表项会丢失，需要重新学习。 缺省情况下不会被老化，只有在配置安全MAC的老化时间后才可以被老化。 安全动态MAC地址的老化类型分为：绝对时间老化和相对时间老化。 ● 如设置绝对老化时间为5分钟：系统每隔1分钟计算一次每个MAC的存在时间，若大于等于5分钟，则立即将该安全动态MAC地址老化。否则，等待下1分钟再检测计算。 ● 如设置相对老化时间为5分钟：系统每隔1分钟检测一次是否有该MAC的流量。若没有流量，则经过5分钟后将该安全动态MAC地址老化。
安全静态MAC地址	使能端口安全时手工配置的静态MAC地址。	不会被老化，手动保存配置后重启设备不会丢失。
Sticky MAC地址	使能端口安全后又同时使能Sticky MAC功能后转换到的MAC地址。	不会被老化，手动保存配置后重启设备不会丢失。

MAC 地址变化情况

当端口安全功能或者Sticky MAC功能使能/去使能时，接口上的MAC地址会变化或者被删除，详细情况请参见下表。

功能	使能	去使能
端口安全功能	接口上之前学习到的动态MAC地址表项将被删除，之后学习到的MAC地址将变为安全动态MAC地址。	接口上的安全动态MAC地址将被删除，重新学习动态MAC地址。
Sticky MAC功能	接口上的安全动态MAC地址表项将转化为Sticky MAC地址，之后学习到的MAC地址也变为Sticky MAC地址。	接口上的Sticky MAC地址，会转换为安全动态MAC地址。

超过安全 MAC 地址限制数后的动作

接口上安全MAC地址数达到限制后，如果收到源MAC地址不存在的报文，无论目的MAC地址是否存在，交换机即认为有非法用户攻击，就会根据配置的动作对接口做保护处理。缺省情况下，保护动作是丢弃该报文并上报告警。

表 8-2 端口安全的保护动作

动作	说明
restrict	丢弃源MAC地址不存在的报文并上报告警。推荐使用restrict动作。
protect	只丢弃源MAC地址不存在的报文，不上报告警。
shutdown	接口状态被置为error-down，并上报告警。 默认情况下，接口关闭后不会自动恢复，只能由网络管理人员在接口视图下使用**restart**命令重启接口进行恢复。 如果用户希望被关闭的接口可以自动恢复，则可在接口error-down前通过在系统视图下执行**error-down auto-recovery cause port-security interval** *interval-value*命令使能接口状态自动恢复为Up的功能，并设置接口自动恢复为Up的延时时间，使被关闭的接口经过延时时间后能够自动恢复。

告警信息可以通过执行**display trapbuffer**命令查看，也可以直接上报网管，通过网管查看。

配置静态 MAC 地址漂移检测功能后出现静态 MAC 地址漂移时的动作

安全MAC地址也属于静态MAC地址，接口上配置静态MAC地址漂移检测功能后，如果收到报文的源MAC地址已经存在在其他接口的静态MAC表中，交换机则认为存在静态MAC地址漂移，就会根据配置的动作对接口做保护处理。端口安全保护动作有restrict、protect和shutdown三种。

表 8-3 端口安全的保护动作

动作	说明
restrict	丢弃触发静态MAC地址漂移的报文并上报告警。推荐使用restrict动作。
protect	只丢弃触发静态MAC地址漂移的报文，不上报告警。
shutdown	接口状态被置为error-down，并上报告警。 默认情况下，接口关闭后不会自动恢复，只能由网络管理人员在接口视图下使用**restart**命令重启接口进行恢复。 如果用户希望被关闭的接口可以自动恢复，则可在接口error-down前通过在系统视图下执行**error-down auto-recovery cause port-security interval** *interval-value*命令使能接口状态自动恢复为Up的功能，并设置接口自动恢复为Up的延时时间，使被关闭的接口经过延时时间后能够自动恢复。

告警信息可以通过执行**display trapbuffer**命令查看，也可以直接上报网管，通过网管查看。

8.3 端口安全应用场景

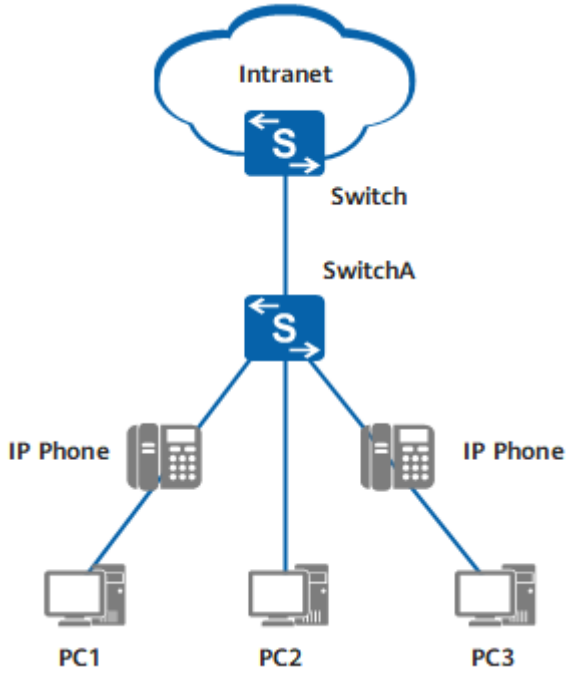
端口安全经常使用在以下几种场景：

- 应用在接入层设备，通过配置端口安全可以防止仿冒用户从其他端口攻击。
- 应用在汇聚层设备，通过配置端口安全可以控制接入用户的数量。

接入层使用场景

如图8-1，用户PC1和PC3通过IP Phone接入SwitchA设备，用户PC2直接接入设备SwitchA，为了保证接入设备安全性，防止非法用户攻击，可以在接入设备SwitchA的接口上配置端口安全功能。

图 8-1 端口安全使用在接入设备的组网场景

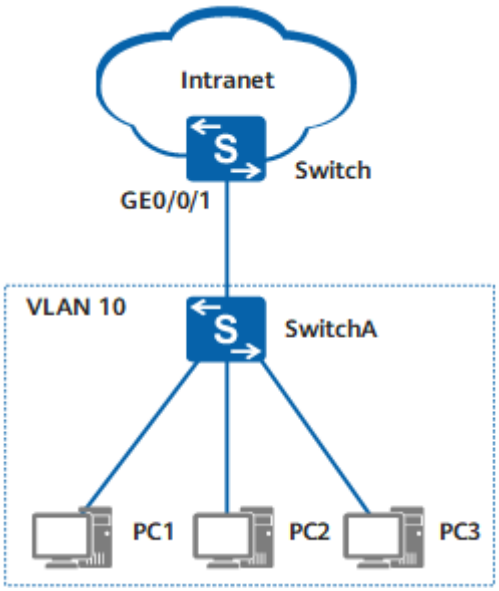


- 如果接入用户变动比较频繁，可以通过端口安全把动态MAC地址转换为安全动态MAC地址。这样可以在用户变动时，及时清除绑定的MAC地址表项。
- 如果接入用户变动较少，可以通过端口安全把动态MAC地址转换为Sticky MAC地址。这样在保存配置重启后，绑定的MAC地址表项不会丢失。
- 如果接入用户变动较少，且数量较少的情况下，可以通过配置为安全静态MAC地址，实现MAC地址表项的绑定。

汇聚层使用场景

如图8-2，树状组网中，多个用户通过SwitchA和汇聚层设备Switch进行通信。为了保证汇聚设备的安全性，控制接入用户的数量，可以在汇聚设备配置端口安全功能，同时指定安全MAC地址的限制数。

图 8-2 端口安全使用在汇聚层设备的组网场景



8.4 端口安全配置注意事项

涉及网元

无需其他网元配合。

License 支持

本特性是交换机的基本特性，无需获得License许可即可应用此功能。

V200R021C00、V200R021C01 版本特性支持情况

S600-E系列交换机中所有款型均支持端口安全。

说明

如需了解交换机软件配套详细信息，请点击**Info-Finder**。

特性依赖和限制

- 端口安全的默认安全MAC地址的限制数是1个，即只能学习一个MAC地址表项，请根据组网需求正确配置安全MAC地址的限制数。
- 端口安全和RRPP、Smart Link、SEP、ERPS不能配置在同一端口上，否则会导致RRPP、Smart Link、SEP、ERPS无法破环。

8.5 端口安全缺省配置

表 8-4 端口安全的缺省配置

参数	缺省值
端口安全功能	未使能
端口学习的安全MAC地址数	1个
达到安全MAC地址数后的保护动作	restrict：丢弃源MAC地址不存在的报文并上报告警
安全MAC老化时间	不老化

8.6 配置端口安全

前置任务

在配置端口安全之前，需完成以下任务：

- 关闭基于接口的MAC地址学习限制功能。
- 关闭配置的MUX VLAN功能。
- 关闭DHCP Snooping的MAC安全功能。

8.6.1 配置安全 MAC 功能

背景信息

在对接入用户的安全性要求较高的网络中，可以配置端口安全功能及端口安全动态MAC学习的限制数量。此时接口学习到的MAC地址会被转换为安全MAC地址，接口学习的最大MAC数量达到上限后不再学习新的MAC地址，仅允许这些MAC地址和交换机通信。而且接口上安全MAC地址数达到限制后，如果收到源MAC地址不存在的报文，无论目的MAC地址是否存在，交换机即认为有非法用户攻击，就会根据配置的动作对接口做保护处理。这样可以阻止其他非信任用户通过本接口和交换机通信，提高交换机与网络的安全性。端口安全的保护动作如下表所示。

表 8-5 端口安全的保护动作

动作	说明
restrict	丢弃源MAC地址不存在的报文并上报告警。推荐使用restrict动作。
protect	只丢弃源MAC地址不存在的报文，不上报告警。

动作	说明
shutdown	接口状态被置为error-down，并上报告警。 默认情况下，接口关闭后不会自动恢复，只能由网络管理人员在接口视图下使用**restart**命令重启接口进行恢复。 如果用户希望被关闭的接口可以自动恢复，则可在接口error-down前通过在系统视图下执行**error-down auto-recovery cause port-security interval** *interval-value*命令使能接口状态自动恢复为Up的功能，并设置接口自动恢复为Up的延时时间，使被关闭的接口经过延时时间后能够自动恢复。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**port-security enable**，使能端口安全功能。

缺省情况下，未使能端口安全功能。

步骤4 执行命令**port-security max-mac-num** *max-number*，配置端口安全动态MAC学习限制数量。

缺省情况下，接口学习的安全MAC地址限制数量为1。

说明

- 如果用户PC使用IP Phone连接交换机，MAC地址学习限制数请配置为3个。因为IP Phone需要占用两个MAC地址表项，PC需要占用一个MAC地址表项。其中IP Phone占用的两个MAC地址表项的VLAN不同，一个VLAN用来传输语音报文，一个VLAN用来传输数据报文。
- 当接口下有多个NAC用户在线时，如需配置端口安全功能，需要先执行**port-security max-mac-num**命令配置该接口学习的安全MAC地址限制数量，然后再执行**port-security enable**命令使能端口安全功能，否则会导致通过该接口接入的用户下线，仅保留1个用户。

步骤5 （可选）执行命令**port-security mac-address** *mac-address* **vlan** *vlan-id*，手工配置安全静态MAC地址表项。

步骤6 （可选）执行命令**port-security protect-action** { **protect** | **restrict** | **shutdown** }，配置端口安全保护动作。

缺省情况下，端口安全保护动作为**restrict**。

步骤7 （可选）执行命令**port-security aging-time** *time* [**type** { **absolute** | **inactivity** }]，配置接口学习到的安全动态MAC地址的老化时间。如果需要配置老化时间时，请合理配置MAC表项老化时间，设置时间过短（比如一分钟）会导致MAC表项老化过快而流量转发失败。

缺省情况下，接口学习的安全动态MAC地址不老化。

----结束

检查配置结果

- 查看安全MAC地址。

  - 执行命令**display mac-address security** [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]，查看安全动态MAC表项。
  - 执行命令**display mac-address sec-config** [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]，查看配置的安全静态MAC表项。
- 告警信息可以通过执行**display trapbuffer**命令查看，也可以直接上报网管，通过网管查看。

8.6.2 配置 Sticky MAC 功能

背景信息

配置端口安全功能后，接口学习到的MAC地址会转换为安全MAC地址，接口学习的最大MAC数量达到上限后不再学习新的MAC地址，仅允许这些MAC地址和交换机通信。如果接入用户发生变动，可以通过设备重启或者配置安全MAC老化时间刷新MAC地址表项。对于相对比较稳定的接入用户，如果不希望后续发生变化，可以进一步使能接口Sticky MAC功能，这样在保存配置之后，MAC地址表项不会刷新或者丢失。

使能接口Sticky MAC功能之后的保护动作与端口安全保护动作一致，如下表所示。

表 8-6 端口安全的保护动作

动作	说明
restrict	丢弃源MAC地址不存在的报文并上报告警。推荐使用restrict动作。
protect	只丢弃源MAC地址不存在的报文，不上报告警。
shutdown	接口状态被置为error-down，并上报告警。 默认情况下，接口关闭后不会自动恢复，只能由网络管理人员在接口视图下使用**restart**命令重启接口进行恢复。 如果用户希望被关闭的接口可以自动恢复，则可在接口error-down前通过在系统视图下执行**error-down auto-recovery cause port-security interval** *interval-value*命令使能接口状态自动恢复为Up的功能，并设置接口自动恢复为Up的延时时间，使被关闭的接口经过延时时间后能够自动恢复。

Sticky MAC功能一般使用在终端用户变更较少的网络中。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**port-security enable**，使能端口安全功能。

缺省情况下，未使能端口安全功能。

步骤4 执行命令**port-security mac-address sticky**，使能接口Sticky MAC功能。

缺省情况下，接口未使能Sticky MAC功能。

步骤5 执行命令**port-security max-mac-num** *max-number*，配置接口Sticky MAC学习限制数量。

使能接口Sticky MAC功能后，缺省情况下，接口学习的MAC地址限制数量为1。

说明

- 如果用户PC使用IP Phone连接交换机，MAC地址学习限制数请配置为3个。因为IP Phone需要占用两个MAC地址表项，PC需要占用一个MAC地址表项。其中IP Phone占用的两个MAC地址表项的VLAN不同，一个VLAN用来传输语音报文，一个VLAN用来传输数据报文。
- 当接口下有多个NAC用户在线时，如需配置端口安全功能，需要先执行**port-security max-mac-num**命令配置该接口学习的安全MAC地址限制数量，然后再执行**port-security enable**命令使能端口安全功能，否则会导致通过该接口接入的用户下线，仅保留1个用户。

步骤6 （可选）执行命令**port-security protect-action** { **protect** | **restrict** | **shutdown** }，配置端口安全保护动作。

缺省情况下，端口安全保护动作为**restrict**。

步骤7 （可选）执行命令**port-security mac-address sticky** *mac-address* **vlan** *vlan-id*，手动配置一条**sticky-mac**表项。

说明

- 接口使能Sticky MAC功能，安全动态MAC地址表项将转化为Sticky MAC地址，之后学习到的MAC地址也变为Sticky MAC地址。
- 接口使能Sticky MAC功能，即使配置了**port-security aging-time**，Sticky MAC也不会被老化。
- 使用命令**port-security mac-address sticky** *mac-address* **vlan** *vlan-id*手动配置的Sticky MAC表项不会显示在当前配置信息中。
- 手动配置的Sticky MAC表项和自动生成的Sticky MAC表项每10分钟自动保存或者通过命令**save**保存在后缀是ztbl或者ctbl的文件中。保存后的文件重启设备不丢弃。该文件名称必须与系统配置文件名称保持一致，比如系统配置文件是test.cfg，则Sticky MAC表项文件必须是test.ctbl，否则会导致设备重启后Sticky MAC表项恢复失败。

----结束

检查配置结果

- 执行命令**display mac-address sticky** [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]，查看Sticky MAC表项。
- 告警信息可以通过执行**display trapbuffer**命令查看，也可以直接上报网管，通过网管查看。

8.7 配置静态 MAC 地址漂移检测功能

背景信息

安全MAC地址也属于静态MAC地址，如果接口接收到报文的源MAC地址已经存在在其他接口的静态MAC地址表中，那么此接口会将这个报文直接丢弃，对用户的业务带来影响。例如，接口GE0/0/1上使能了Sticky MAC功能后，PC1通过GE0/0/1与设备相连，GE0/0/1的静态MAC表项中保存了PC1的MAC地址。如果将PC1从接口GE0/0/1拔出，再通过GE0/0/2接入设备，此时GE0/0/2将会丢弃从PC1发过来的报文。此时，可以执行本命令使能静态MAC漂移的检测功能，设备会根据配置的动作对接口GE0/0/2做保护处理。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**port-security static-flapping protect**，使能静态MAC地址漂移的检测功能。

步骤3 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤4 执行命令**port-security enable**，使能端口安全功能。

缺省情况下，未使能端口安全功能。

步骤5 （可选）执行命令**port-security protect-action** { **protect** | **restrict** | **shutdown** }，配置端口安全保护动作。

缺省情况下，端口安全保护动作为**restrict**。

----结束

后续处理

接口上配置静态MAC地址漂移检测功能后，如果收到报文的源MAC地址已经存在在其他接口的静态MAC表中，端口安全则认为存在静态MAC地址漂移，就会根据配置的动作对接口做保护处理。端口安全保护动作有以下三种：restrict、protect和shutdown。

表 8-7 端口安全的保护动作

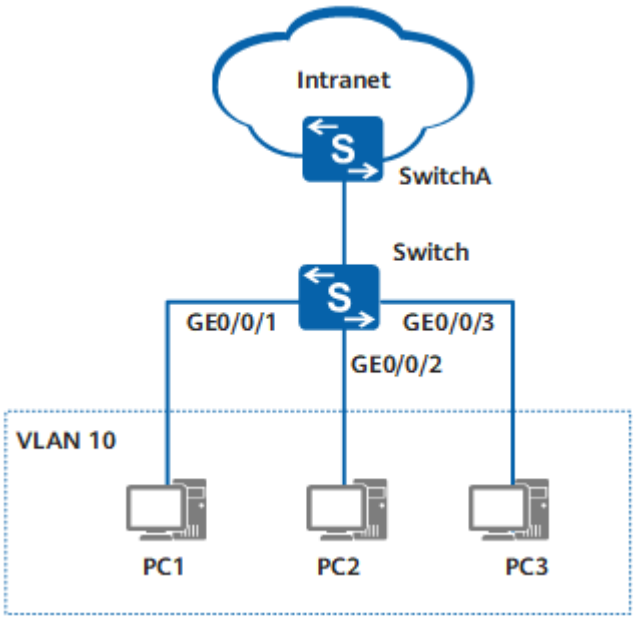
动作	说明
restrict	丢弃触发静态MAC地址漂移的报文并上报告警。推荐使用restrict动作。
protect	只丢弃触发静态MAC地址漂移的报文，不上报告警。
shutdown	接口状态被置为error-down，并上报告警。 默认情况下，接口关闭后不会自动恢复，只能由网络管理人员在接口视图下使用**restart**命令重启接口进行恢复。 如果用户希望被关闭的接口可以自动恢复，则可在接口error-down前通过在系统视图下执行**error-down auto-recovery cause port-security interval** *interval-value*命令使能接口状态自动恢复为Up的功能，并设置接口自动恢复为Up的延时时间，使被关闭的接口经过延时时间后能够自动恢复。

8.8 配置端口安全示例

组网需求

如图8-3所示，用户PC1、PC2、PC3通过接入设备连接公司网络。为了提高用户接入的安全性，将接入设备Switch的接口使能端口安全功能，并且设置接口学习MAC地址数的上限为接入用户数，这样其他外来人员使用自己带来的PC无法访问公司的网络。

图 8-3 配置端口安全示例组网图



配置思路

采用如下的思路配置端口安全：

1. 配置VLAN，实现二层转发功能。
2. 配置端口安全功能，实现学习到的MAC地址表项不老化。

操作步骤

步骤1 在Switch上创建VLAN，并把接口加入VLAN

#创建VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan 10
[Switch-vlan10] quit
```

#接口GE0/0/1加入VLAN10。接口GE0/0/2和GE0/0/3的配置与接口GE0/0/1相同，不再赘述。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type access
[Switch-GigabitEthernet0/0/1] port default vlan 10
[Switch-GigabitEthernet0/0/1] quit
```

步骤2 配置GE0/0/1接口的端口安全功能。

使能接口Sticky MAC功能，同时配置MAC地址限制数。接口GE0/0/2和GE0/0/3的配置与接口GE0/0/1相同，不再赘述。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port-security enable
[Switch-GigabitEthernet0/0/1] port-security mac-address sticky
[Switch-GigabitEthernet0/0/1] port-security max-mac-num 1
```

步骤3 验证配置结果

将PC1、PC2、PC3换成其他设备，无法访问公司网络。

----结束

配置文件

Switch的配置文件

```
#
sysname Switch
#
vlan batch 10
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
 port-security enable
 port-security mac-address sticky
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 10
 port-security enable
 port-security mac-address sticky
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 10
 port-security enable
 port-security mac-address sticky
#
return
```


9 DHCP Snooping 配置

9.1 DHCP Snooping 简介

定义

DHCP Snooping是DHCP（Dynamic Host Configuration Protocol）的一种安全特性，用于保证DHCP客户端从合法的DHCP服务器获取IP地址，并记录DHCP客户端IP地址与MAC地址等参数的对应关系，防止网络上针对DHCP攻击。

目的

目前DHCP协议（RFC2131）在应用的过程中遇到很多安全方面的问题，网络中存在一些针对DHCP的攻击，如DHCP Server仿冒者攻击、DHCP Server的拒绝服务攻击、仿冒DHCP报文攻击等。

为了保证网络通信业务的安全性，可引入DHCP Snooping技术，在DHCP Client和DHCP Server之间建立一道防火墙，以抵御网络中针对DHCP的各种攻击。

受益

- 设备具有防御网络上DHCP攻击的能力，增强了设备的可靠性，保障通信网络的正常运行。
- 为用户提供更安全的网络环境，更稳定的网络服务。

9.2 DHCP Snooping 原理描述

9.2.1 DHCP Snooping 的基本原理

DHCP Snooping分为DHCPv4 Snooping和DHCPv6 Snooping，两者实现原理相似，以下以DHCPv4 Snooping为例进行描述。

使能了DHCP Snooping的设备将用户（DHCP客户端）的DHCP请求报文通过信任接口发送给合法的DHCP服务器。之后设备根据DHCP服务器回应的DHCP ACK报文信息生成DHCP Snooping绑定表。后续设备再从使能了DHCP Snooping的接口接收用户发来的DHCP报文时，会进行匹配检查，能够有效防范非法用户的攻击。

DHCP Snooping 信任功能

DHCP Snooping的信任功能，能够保证客户端从合法的服务器获取IP（Internet Protocol）地址。

如图9-1所示，网络中如果存在私自架设的DHCP Server仿冒者，则可能导致DHCP客户端获取错误的IP地址和网络配置参数，无法正常通信。DHCP Snooping信任功能可以控制DHCP服务器应答报文的来源，以防止网络中可能存在的DHCP Server仿冒者为DHCP客户端分配IP地址及其他配置信息。

DHCP Snooping信任功能将接口分为信任接口和非信任接口：

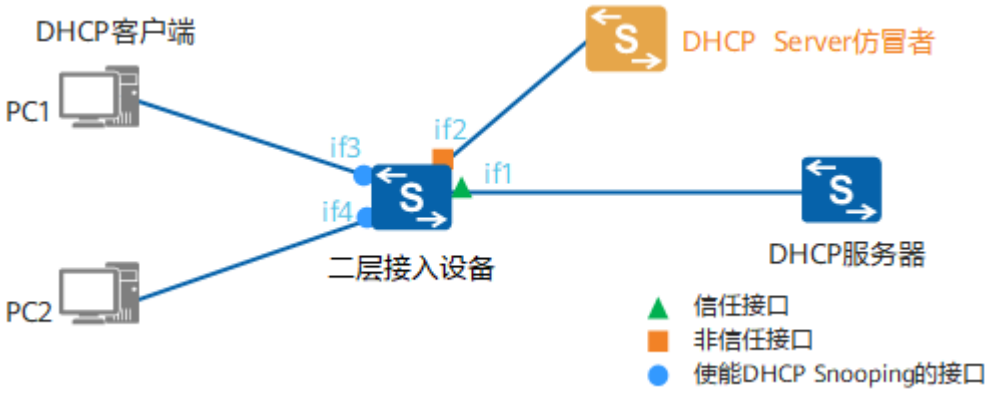
- 信任接口正常接收DHCP服务器响应的DHCP ACK、DHCP NAK和DHCP Offer报文。
- 非信任接口在接收到DHCP服务器响应的DHCP ACK、DHCP NAK和DHCP Offer报文后，丢弃该报文。

说明

- 配置**dhcp snooping enable**命令的接口，收到DHCP请求报文后，转发给所有的信任接口；收到DHCP响应报文后丢弃。
- 配置**dhcp snooping trusted**命令的接口，收到DHCP请求报文后，转发给所有的信任接口，如果没有其他信任接口，则丢弃该DHCP请求报文；收到DHCP响应报文后，只转发给连接对应客户端的并且配置命令**dhcp snooping enable**的接口，如果查不到上述接口，则丢弃该DHCP响应报文。

在二层网络接入设备使能DHCP Snooping场景中，一般将与合法DHCP服务器直接或间接连接的接口设置为信任接口（如图9-1中的if1接口），其他接口设置为非信任接口（如图9-1中的if2接口），使DHCP客户端的DHCP请求报文仅能从信任接口转发出去，从而保证DHCP客户端只能从合法的DHCP服务器获取IP地址，私自架设的DHCP Server仿冒者无法为DHCP客户端分配IP地址。

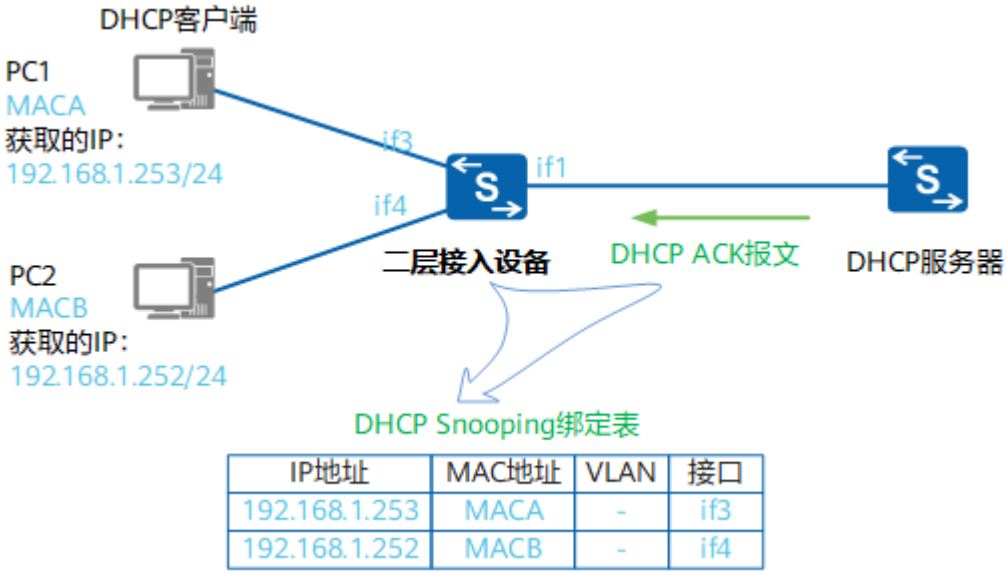
图 9-1 DHCP Snooping 信任功能示意图



DHCP Snooping 绑定表

如图9-2所示的DHCP场景中，连接在二层接入设备上的PC配置为自动获取IP地址。PC作为DHCP客户端通过广播形式发送DHCP请求报文，使能了DHCP Snooping功能的二层接入设备将其通过信任接口转发给DHCP服务器。最后DHCP服务器将含有IP地址信息的DHCP ACK报文通过单播的方式发送给PC。在这个过程中，二层接入设备收到DHCP ACK报文后，会从该报文中提取关键信息（包括PC的MAC地址以及获取到的IP地址、地址租期），并获取与PC连接的使能了DHCP Snooping功能的接口信息（包括接口编号及该接口所属的VLAN），根据这些信息生成DHCP Snooping绑定表。以PC1为例，图9-2中二层接入设备会从DHCP ACK报文提取到IP地址信息为192.168.1.253，MAC地址信息为MACA。再获取与PC连接的接口信息为if3，根据这些信息生成一条DHCP Snooping绑定表项。

图 9-2 DHCP Snooping 绑定表功能示意图



DHCP Snooping绑定表根据DHCP租期进行老化或根据用户释放IP地址时发出的DHCP Release报文自动删除对应表项。

由于DHCP Snooping绑定表记录了DHCP客户端IP地址与MAC地址等参数的对应关系，故通过对报文与DHCP Snooping绑定表进行匹配检查，能够有效防范非法用户的攻击。

为了保证设备在生成DHCP Snooping绑定表时能够获取到用户MAC等参数，DHCP Snooping功能需应用于二层网络中的接入设备或第一个DHCP Relay上。

在DHCP中继使能DHCP Snooping场景中，DHCP Relay设备不需要设置信任接口。因为DHCP Relay收到DHCP请求报文后进行源目的IP、MAC转换处理，然后以单播形式发送给指定的合法DHCP服务器，所以DHCP Relay收到的DHCP ACK报文都是合法的，生成的DHCP Snooping绑定表也是正确的。

9.2.2 DHCP Snooping 支持的 Option82 功能

概述

在传统的DHCP动态分配IP地址过程中，DHCP Server不能够根据DHCP请求报文感知到用户的具体物理位置，以致同一VLAN的用户得到的IP地址所拥有的权限是完全相同的。由于网络管理者不能对同一VLAN中特定的用户进行有效的控制，即不能够控制客户端对网络资源的访问，这将给网络的安全控制提出了严峻的挑战。

RFC 3046定义了DHCP Relay Agent Information Option（Option 82），该选项记录了DHCP Client的位置信息。DHCP Snooping设备或DHCP Relay通过在DHCP请求报文中添加Option82选项，将DHCP Client的精确物理位置信息传递给DHCP Server，从而使得DHCP Server能够为主机分配合适的IP地址和其他配置信息，实现对客户端的安全控制。

Option82包含两个常用子选项Circuit ID和Remote ID。其中Circuit ID子选项主要用来标识客户端所在的VLAN、接口等信息，Remote ID子选项主要用来标识客户端接入的设备，一般为设备的MAC地址。

设备作为DHCP Relay时，使能或未使能DHCP Snooping功能都可支持Option82选项功能，但若设备在二层网络作为接入设备，则必须使能DHCP Snooping功能方可支持Option82功能。

Option82选项仅记录了DHCP用户的精确物理位置信息并通过DHCP请求报文中将该信息发送给DHCP Server。而如果需要对不同的用户部署不同的地址分配或安全策略，则需DHCP Server支持Option82功能并在其上已配置了IP地址分配或安全策略。

Option82选项携带的用户位置信息与DHCP Snooping绑定表记录的用户参数是两个相互独立的概念，没有任何关联。Option82选项携带的用户位置信息是在DHCP用户申请IP地址时（此时用户还未分配到IP地址），由设备添加到DHCP请求报文中。DHCP Snooping绑定表是在设备收到DHCP Server回应的DHCP Ack报文时（此时已为用户分配了IP地址），设备根据DHCP Ack报文信息自动生成。

实现

设备作为DHCP Relay或设备在二层网络作为接入设备并使能DHCP Snooping功能时均可支持Option82功能。使能设备的Option82功能有Insert和Rebuild两种方式，使能方式不同设备对DHCP请求报文的处理也不同。

- Insert方式：当设备收到DHCP请求报文时，若该报文中没有Option82选项，则插入Option82选项；若该报文中含有Option82选项，则判断Option82选项中是否包含remote-id，如果包含，则保持Option82选项不变，如果不包含，则插入remote-id。
- Rebuild方式：当设备收到DHCP请求报文时，若该报文中没有Option82选项，则插入Option82选项；若该报文中含有Option82选项，则删除该Option82选项并插入管理员自己在设备上配置的Option82选项。

对于Insert和Rebuild两种方式，当设备接收到DHCP服务器的响应报文时，处理方式一致。

- DHCP响应报文中有Option82选项：
  - 如果设备收到的DHCP请求报文中没有Option82选项，则设备将删除DHCP响应报文中的Option82选项，之后转发给DHCP Client。
  - 如果设备收到的DHCP请求报文中有Option82选项，则设备将DHCP响应报文中的Option82选项格式还原为DHCP请求报文中的Option82选项，之后转发给DHCP Client。
- DHCP响应报文不含有Option82选项：直接转发。

9.2.3 DHCPv6 Snooping 支持的 LDRA 功能

概述

RFC 6221定义了轻量级DHCPv6中继代理LDRA（Lightweight DHCPv6 Relay Agent），它是一种在DHCPv6交互报文中插入中继代理选项信息以标示用户位置的规范。

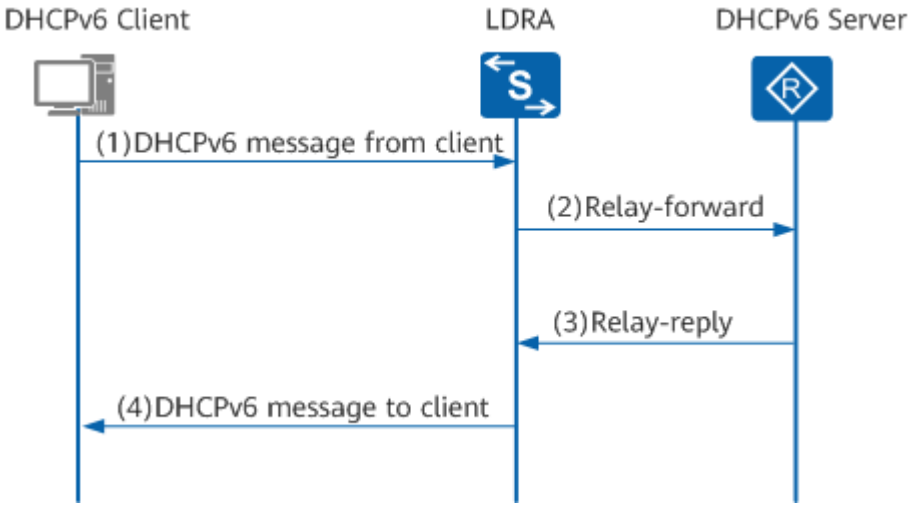
类似于DHCPv4网络中使用的Option82选项，在DHCPv6网络中可以使用LDRA获取用户详细的位置信息。LDRA一般部署在靠近用户的接入设备上。

实现

LDRA工作流程与DHCPv6中继工作流程相似。当接收到用户的DHCPv6请求报文时，部署LDRA功能的设备即会构建Relay-Forward报文并在其中封装用户的位置信息（如用户与设备连接的接口信息等）然后转发给DHCPv6 Server，从而使得DHCPv6 Server能够获取到DHCPv6 Client的物理位置信息进而为用户部署诸如IP地址分配、QoS、接入控制等策略。

如图9-3所示，LDRA详细工作交互过程如下。

图 9-3 LDRA 工作流程图



1. DHCPv6客户端向LDRA设备发送DHCPv6报文。

2. LDRA设备收到客户端的DHCPv6报文后，将其封装在Relay-Forward报文的中继消息选项中，同时将用户的位置信息封装在Relay-Forward报文中的interface-id或remote-id中，之后将Relay-Forward报文发送给DHCPv6服务器。
3. DHCPv6服务器从Relay-Forward报文中解析出DHCPv6客户端的请求以及用户位置信息，之后根据用户位置信息为DHCPv6客户端选取IPv6地址和其他配置参数，构造应答消息，将应答消息封装在Relay-Reply报文中，并发送给LDRA设备。
4. LDRA设备从Relay-Reply报文中解析出DHCPv6服务器的应答，转发给DHCPv6客户端。DHCPv6客户端根据应答报文获取到DHCPv6服务器地址，后续从该服务器获取IPv6地址和其他网络配置参数。

Relay-Forward报文与Relay-Reply报文相关介绍请参见《S600-E V200R021C00, C01 配置指南-IP业务》DHCPv6配置 中的“DHCPv6报文介绍”。

9.2.4 DHCPv6 Snooping 支持的 option18 与 option37 功能

Option18与Option37选项功能类似于Option82。Option82用于插入DHCPv4报文中，而对于DHCPv6报文则需插入Option18与Option37选项用于记录DHCPv6 Client的位置信息。

说明

设备必须使能DHCPv6 snooping功能方可支持Option18与Option37选项功能，详见**9.10 配置在DHCPv6报文中添加Option18或Option37字段**。

9.3 DHCP Snooping 应用场景

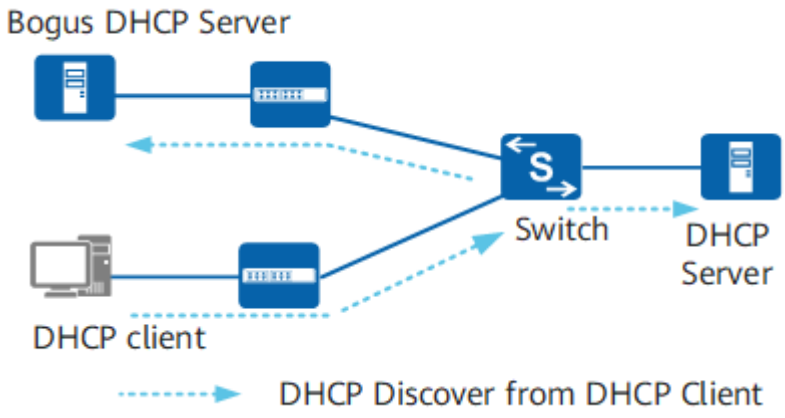
9.3.1 防止 DHCP Server 仿冒者攻击导致用户获取到错误的 IP 地址和网络参数

攻击原理

由于DHCP Server和DHCP Client之间没有认证机制，所以如果在网络上随意添加一台DHCP服务器，它就可以为客户端分配IP地址以及其他网络参数。如果该DHCP服务器为用户分配错误的IP地址和其他网络参数，将会对网络造成非常大的危害。

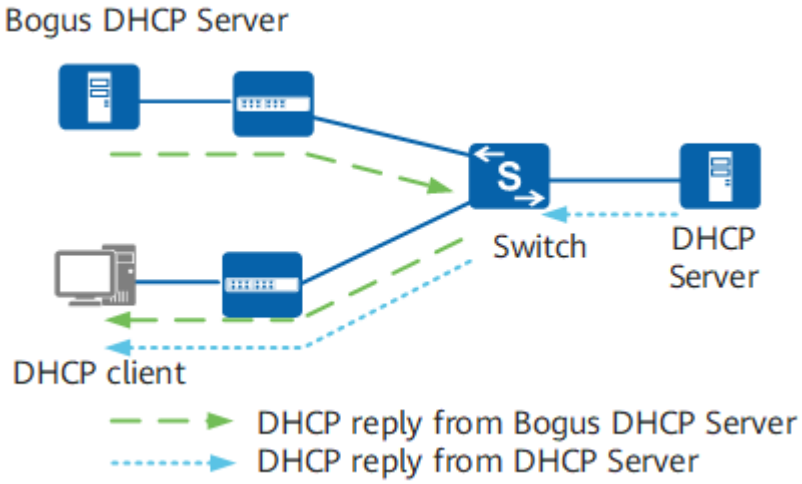
如**图9-4**所示，DHCP Discover报文是以广播形式发送，无论是合法的DHCP Server，还是非法的DHCP Server都可以接收到DHCP Client发送的DHCP Discover报文。

图 9-4 DHCP Client 发送 DHCP Discover 报文示意图



如果此时DHCP Server仿冒者回应给DHCP Client仿冒信息，如错误的网关地址、错误的DNS（Domain Name System）服务器、错误的IP等信息，如图9-5所示。DHCP Client将无法获取正确的IP地址和相关信息，导致合法客户无法正常访问网络或信息安全受到严重威胁。

图 9-5 DHCP Server 仿冒者攻击示意图

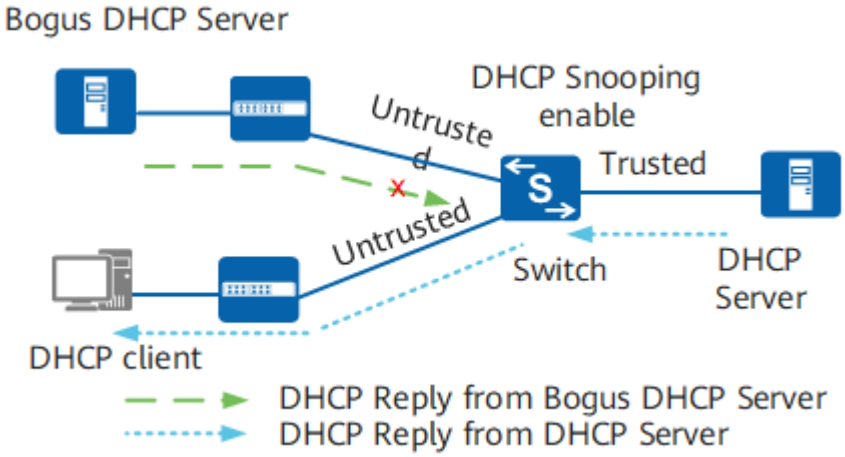


解决方法

为了防止DHCP Server仿冒者攻击，可配置设备接口的“信任（Trusted）/非信任（Untrusted）”工作模式。

将与合法DHCP服务器直接或间接连接的接口设置为信任接口，其他接口设置为非信任接口。此后，从“非信任（Untrusted）”接口上收到的DHCP回应报文将被直接丢弃，这样可以有效防止DHCP Server仿冒者的攻击。如图9-6所示。

图 9-6 Trusted/Untrusted 工作模式示意图



9.3.2 防止非 DHCP 用户攻击导致合法用户无法正常使用网络

攻击原理

在DHCP网络中，静态获取IP地址的用户（非DHCP用户）对网络可能存在多种攻击，譬如仿冒DHCP Server、构造虚假DHCP Request报文等。这将为合法DHCP用户正常使用网络带来了一定的安全隐患。

解决方法

为了有效的防止非DHCP用户攻击，可开启设备根据DHCP Snooping绑定表生成接口的静态MAC表项功能。

之后，设备将根据接口下所有的DHCP用户对应的DHCP Snooping绑定表项自动执行命令生成这些用户的静态MAC表项，并同时关闭接口学习动态MAC表项的能力。此时，只有源MAC与静态MAC表项匹配的报文才能够通过该接口，否则报文会被丢弃。因此对于该接口下的非DHCP用户，只有管理员手动配置了此类用户的静态MAC表项其报文才能通过，否则报文将被丢弃。

动态MAC表项是设备自动学习并生成的，静态MAC表项则是根据命令配置而成的。MAC表项中包含用户的MAC、所属VLAN、连接的接口号等信息，设备可根据MAC表项对报文进行二层转发。

9.3.3 防止 DHCP 报文泛洪攻击导致设备无法正常工作

攻击原理

在DHCP网络环境中，若攻击者短时间内向设备发送大量的DHCP报文，将会对设备的性能造成巨大的冲击以致可能会导致设备无法正常工作。

解决方法

为了有效的防止DHCP报文泛洪攻击，在使能设备的DHCP Snooping功能时，可同时使能设备对DHCP报文上送DHCP报文处理单元的速率进行检测的功能。此后，设备将会检测DHCP报文的上送速率，并仅允许在规定速率内的报文上送至DHCP报文处理单元，而超过规定速率的报文将会被丢弃。

9.3.4 防止仿冒 DHCP 报文攻击导致合法用户无法获得 IP 地址或异常下线

攻击原理

已获取到IP地址的合法用户通过向服务器发送DHCP Request或DHCP Release报文用以续租或释放IP地址。如果攻击者冒充合法用户不断向DHCP Server发送DHCP Request报文来续租IP地址，会导致这些到期的IP地址无法正常回收，以致一些合法用户不能获得IP地址；而若攻击者仿冒合法用户的DHCP Release报文发往DHCP Server，将会导致用户异常下线。

解决方法

为了有效的防止仿冒DHCP报文攻击，可利用DHCP Snooping绑定表的功能。设备通过将DHCP Request续租报文和DHCP Release报文与绑定表进行匹配操作能够有效的判别报文是否合法（主要是检查报文中的VLAN、IP、MAC、接口信息是否匹配动态绑定表），若匹配成功则转发该报文，匹配不成功则丢弃。

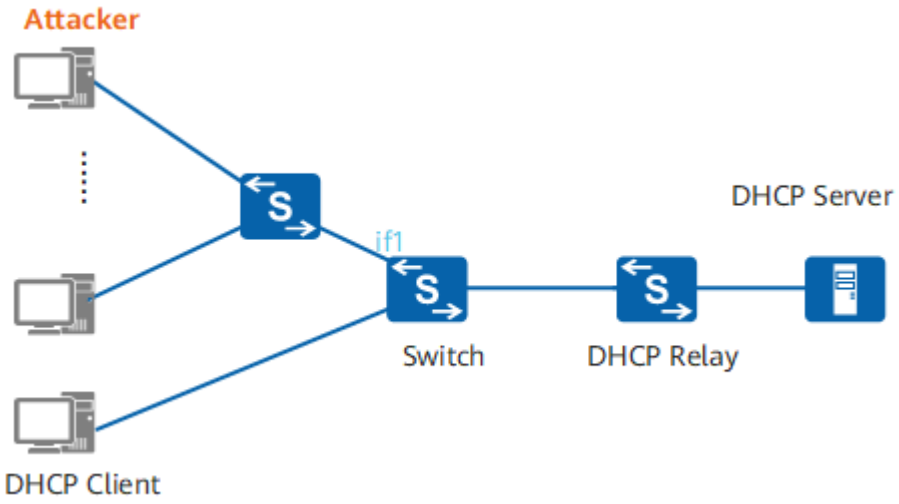
9.3.5 防止 DHCP Server 服务拒绝攻击导致部分用户无法上线

攻击原理

如图9-7所示，若设备接口if1下存在大量攻击者恶意申请IP地址，会导致DHCP Server中IP地址快速耗尽而不能为其他合法用户提供IP地址分配服务。

另一方面，DHCP Server通常仅根据DHCP Request报文中的CHADDR（Client Hardware Address）字段来确认客户端的MAC地址。如果某一攻击者通过不断改变CHADDR字段向DHCP Server申请IP地址，同样将会导致DHCP Server上的地址池被耗尽，从而无法为其他正常用户提供IP地址。

图 9-7 DHCP Server 服务拒绝攻击示意图



解决方法

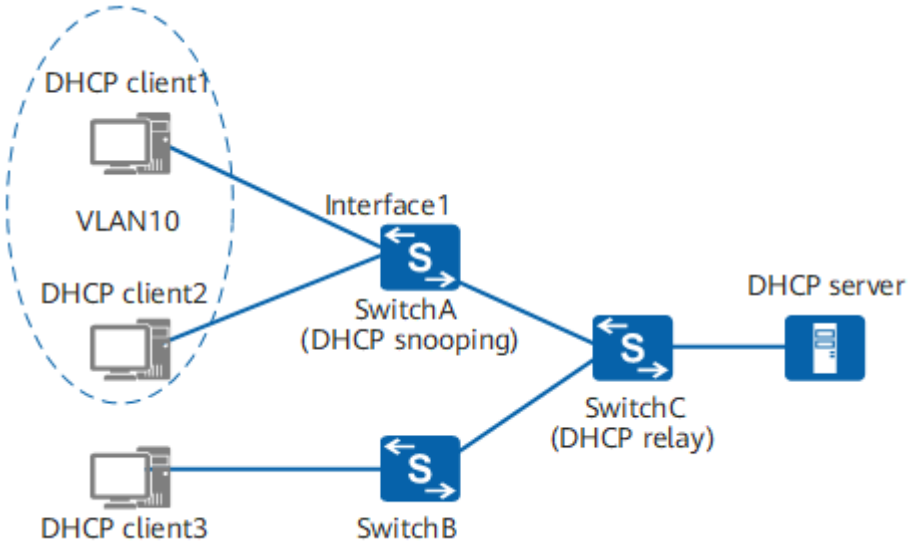
为了抑制大量DHCP用户恶意申请IP地址，在使能设备的DHCP Snooping功能后，可配置设备或接口允许接入的最大DHCP用户数，当接入的用户数达到该值时，则不再允许任何用户通过此设备或接口成功申请到IP地址。

而对通过改变DHCP Request报文中的CHADDR字段方式的攻击，可使能设备检测DHCP Request报文帧头MAC与DHCP数据区中CHADDR字段是否一致功能，此后设备将检查上送的DHCP Request报文中的帧头MAC地址是否与CHADDR值相等，相等则转发，否则丢弃。

9.3.6 Option82 的典型应用

Option 82（DHCP Relay Agent Information Option）称为中继代理信息选项，该选项记录了DHCP Client的位置信息。DHCP Snooping设备或DHCP Relay通过在DHCP请求报文中添加Option82选项，将DHCP Client的位置信息传递给DHCP Server，从而使得DHCP Server能够为主机分配合适的IP地址和其他配置信息，并实现对客户端的安全控制。

图 9-8 Option82 应用组网图



如图9-8所示，用户通过DHCP方式获取IP地址。在管理员组建该网络时需要控制接口interface1下用户对网络资源的访问以提高网络的安全性。

在传统的DHCP动态分配IP地址过程中，DHCP Server是无法区分同一VLAN内的不同用户的，以致同一VLAN内的用户得到的IP地址所拥有的权限是完全相同的。

为实现上述目的，管理员在使能SwitchA的DHCP Snooping功能之后可使能其Option82功能。之后SwitchA在接收到用户申请IP地址发送的DHCP请求报文时，将会在报文中插入Option82选项，以标注用户的精确位置信息，譬如MAC地址、所属VLAN、所连接的接口号等参数。DHCP Server在接收到携带有Option82选项的DHCP请求报文后，即可通过Option82选项的内容获悉到用户的精确物理位置进而根据其上已部署的IP地址分配策略或其他安全策略为用户分配合适的IP地址和其他配置信息。

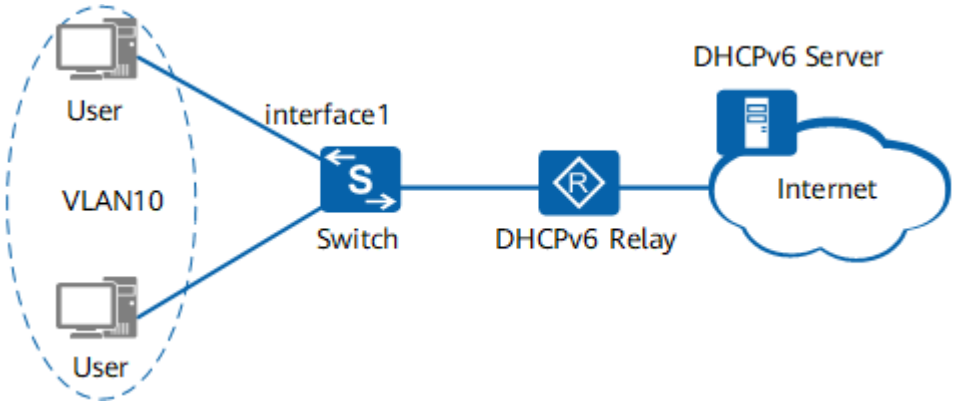
Option82选项仅记录了DHCP用户的精确物理位置信息并通过DHCP请求报文中将该信息发送给DHCP Server。而如果需要对不同的用户部署不同的地址分配或安全策略，则需DHCP Server支持Option82功能并在其上已配置了IP地址分配或安全策略。

9.3.7 通过 LDRA 功能感知用户位置信息

LDRA称为轻量级DHCPv6中继代理，该中继代理能够记录用户位置信息并将其发送到DHCPv6 Server，从而使得DHCPv6 Server能够获取到用户详细的物理位置信息，以实现对用户客户端部署诸如地址分配、计费、接入控制等策略。

如图9-9所示，用户通过DHCPv6方式获取IPv6地址。在管理员部署该网络时需要限制接口interface1下的用户对网络资源的访问以提高网络的安全性。

图 9-9 LDRA 应用组网图



在传统的DHCPv6动态分配IPv6地址过程中，DHCPv6 Server无法获取到用户详细的物理位置信息，以致不能为interface1接口下的用户部署地址分配、接入控制等策略。

为解决上述问题，管理员在使能Switch的DHCP Snooping功能之后，可使能其LDRA功能。这样，Switch既能够获取用户详细的位置信息并将其发送到DHCPv6 Server。DHCPv6 Server即可根据用户的详细位置信息为其部署地址分配策略或其他安全策略。

LDRA功能仅是记录了DHCPv6用户的详细位置信息并通过RELAY-FORW报文将该信息发送给DHCPv6 Server，对不同的用户部署诸如地址分配、计费、接入控制等策略，由DHCPv6 Server实现。

9.4 DHCP Snooping 配置注意事项

涉及网元

无需其他网元配合。

License 支持

本特性是交换机的基本特性，无需获得License许可即可应用此功能。

V200R021C00、V200R021C01 版本特性支持情况

S600-E系列交换机中所有款型均支持DHCP Snooping。

说明

如需了解交换机软件配套详细信息，请点击**Info-Finder**。

特性依赖和限制

- 如果需要上线的用户数目超过了设备支持的DHCP Snooping绑定表规格，超出的用户将无法上线。
- DHCP Snooping功能不支持在接口的三层模式下配置。
- DHCP触发ARP学习功能仅适用于有线用户、无线用户不支持。

- IPv4 DHCP Snooping功能可以配置在二层接入设备和第一跳DHCPv4 Relay设备上；IPv6 DHCP Snooping功能可以配置在二层接入设备、从V200R012C00版本开始支持配置在第一跳DHCPv6 Relay设备上。
- VRRP场景下，备设备不能同步主设备上的DHCP Snooping绑定表。故VRRP场景下不能配置DHCP Snooping功能，否则会导致主备倒换后原有业务失效。
- DHCP Snooping最多支持处理带有双层VLAN Tag的DHCP报文。对于带有更多层VLAN Tag的报文建议不要配置DHCP Snooping功能，否则会导致丢包，影响用户的使用体验。
- 在已配置DHCP Snooping功能情况下，如果用户涉及认证授权VLAN，由于用户授权VLAN前后的VLAN和IP地址信息变化，会导致设备上一个用户可能生成两条DHCP Snooping绑定表。此时，如果设备是三层设备可以通过配置ARP与DHCP Snooping的联动功能来删除老的DHCP Snooping绑定表。
- 如果设备使能了DHCP Snooping功能，不能配置2 to 2的VLAN Mapping功能，否则会导致DHCP用户无法上线。

9.5 DHCP Snooping 缺省配置

DHCP Snooping的缺省配置如表9-1所示：

表 9-1 DHCP Snooping 的缺省配置

参数	缺省值
DHCP Snooping功能	未使能
接口的信任状态	非信任
DHCP Snooping用户位置迁移功能	已使能
ARP与DHCP Snooping的联动功能	未使能
DHCP Snooping支持的Option82功能	未使能
根据DHCP Snooping绑定表生成接口的静态MAC表项功能	未使能
DHCP报文上送DHCP报文处理单元的最大允许速率	100pps
对DHCP报文进行绑定表匹配检查的功能	未使能
检测DHCP Request报文帧头MAC与DHCP数据区中CHADDR字段是否一致功能	未使能
检测DHCP Request报文中GIADDR字段是否非零的功能	未使能

9.6 配置 DHCP Snooping 的基本功能

前置任务

在配置DHCP Snooping的基本功能之前，需要完成以下任务：

- 网络中已完成DHCP功能的部署。有关DHCP的详细配置，请参见《S600-E V200R021C00, C01 配置指南-IP业务配置》中的“DHCP配置”。

配置流程

配置DHCP Snooping的基本功能需要在设备上进行以下配置。

9.6.1 使能 DHCP Snooping 功能

背景信息

DHCP Snooping是一种DHCP安全特性，在配置DHCP Snooping各安全功能之前需首先使能DHCP Snooping功能。

使能DHCP Snooping功能的顺序是先使能全局下的DHCP Snooping功能，再使能接口或VLAN下的DHCP Snooping功能。

如图9-10所示，Switch_1是二层接入设备，将用户PC的DHCP请求转发给DHCP服务器。以Switch_1为例，在使能DHCP Snooping功能时需要注意：

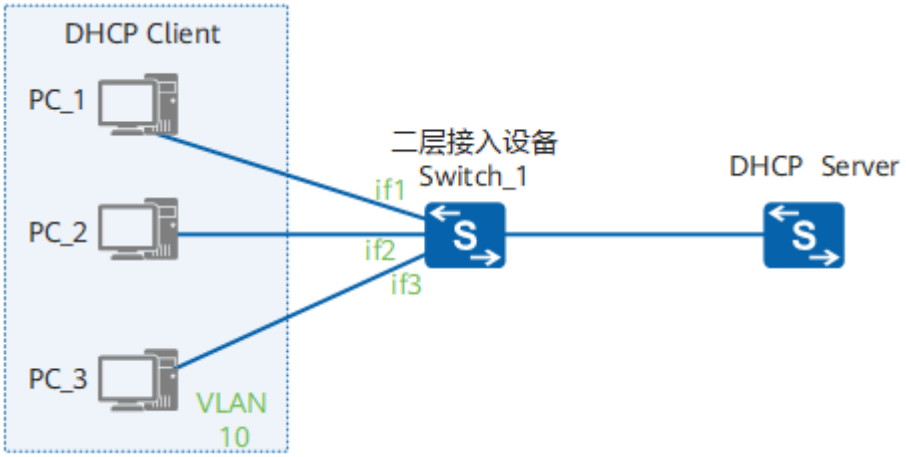
- 使能DHCP Snooping功能之前，必须已使用命令**dhcp enable**使能了设备的DHCP功能。
- 全局使能DHCP Snooping功能后，还需要在连接用户的接口（如图中的接口if1、if2和if3）或其所属VLAN（如图中的VLAN 10）使能DHCP Snooping功能。

  当存在多个用户PC属于同一个VLAN时，为了简化配置，可以在这个VLAN使能DHCP Snooping功能。

说明

DHCP Snooping不支持BOOTP协议，而无盘工作站使用BOOTP协议，所以无盘工作站不能通过DHCP Snooping生成动态绑定表。由于IPSG功能和DAI功能是基于绑定表实现的，如果无盘工作站要使用以上功能，需要执行命令**user-bind static**配置静态绑定表。

图 9-10 配置 DHCP Snooping 基本功能组网图



请在二层网络中的接入设备或第一个DHCP Relay上执行以下步骤。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**dhcp snooping enable** [**ipv4** | **ipv6**]，全局使能DHCP Snooping功能。

缺省情况下，设备全局未使能DHCP Snooping功能。

说明

系统视图下，**dhcp snooping enable**命令是DHCP Snooping相关功能的总开关。执行**undo dhcp snooping enable**命令后，设备上所有DHCP Snooping相关的配置会被删除；再次执行**dhcp snooping enable**命令使能DHCP Snooping功能后，设备上所有DHCP Snooping相关配置将被恢复为缺省配置。

步骤3 使能DHCP Snooping功能，可在系统视图、VLAN视图或接口视图下进行配置。

- 系统视图下：

1. 执行命令**dhcp snooping enable vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，使能DHCP Snooping功能。

   缺省情况下，设备未使能DHCP Snooping功能。

- VLAN视图或接口视图下：

1. 执行命令**vlan** *vlan-id*，进入VLAN视图；或执行命令**interface** *interface-type interface-number*，进入连接用户的接口视图。
2. 执行命令**dhcp snooping enable**，使能接口或VLAN下的DHCP Snooping功能。

   缺省情况下，设备未使能DHCP Snooping功能。

   在VLAN视图下执行此命令，则对设备所有接口接收到的属于该VLAN的DHCP报文命令功能生效；在接口下执行该命令，则对该接口下的所有DHCP报文命令功能生效。

----结束

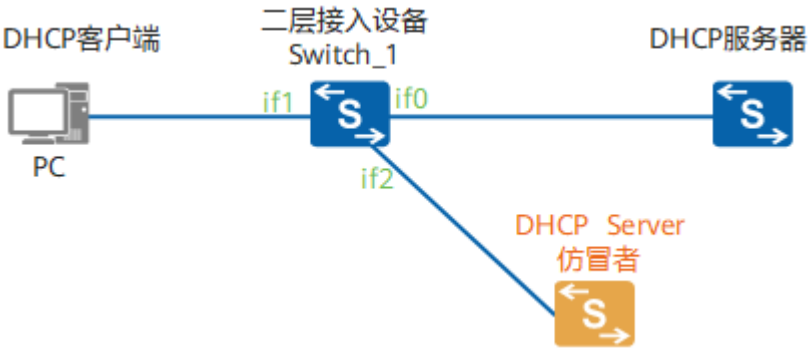
9.6.2 配置接口信任状态

背景信息

如图9-11所示场景中，为使DHCP客户端能通过合法的DHCP服务器获取IP地址，需将与管理员信任的DHCP服务器直接或间接连接的设备接口设置为信任接口（如图中的if0），其他接口设置为非信任接口（如图中的if2）。从而保证DHCP客户端只能从合法的DHCP服务器获取IP地址，私自架设的DHCP Server仿冒者无法为DHCP客户端分配IP地址。

在连接用户的接口或VLAN下使能DHCP Snooping功能之后，需将连接DHCP服务器的接口配置为“信任”模式，两者同时生效设备即能够生成DHCP Snooping动态绑定表。

图 9-11 配置 DHCP Snooping 基本功能组网图



请在二层网络中的接入设备上执行以下步骤。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 配置接口为“信任”状态，可在接口视图、VLAN视图下执行。

- 接口视图下：

1. 执行命令**interface** *interface-type interface-number*，进入接口视图。
2. 执行命令**dhcp snooping trusted**，配置接口为“信任”接口。

   缺省情况下，接口的状态为“非信任”状态。

- VLAN视图下：

1. 执行命令**vlan** *vlan-id*，进入VLAN视图。
2. 执行命令**dhcp snooping trusted interface** *interface-type interface-number*，配置接口为“信任”接口。

   缺省情况下，接口的状态为“非信任”状态。

   在VLAN视图下执行此命令，则命令功能仅对加入该VLAN的接口收到的属于此VLAN的DHCP报文生效；在接口下执行该命令，则命令功能对该接口接收到的所有DHCP报文生效。

----结束

9.6.3 （可选）去使能 DHCP Snooping 用户位置迁移功能

背景信息

在移动应用场景中，若某一用户由接口A上线后，切换到接口B重新上线，用户将发送DHCP Discover报文申请IP地址。缺省情况下设备使能DHCP Snooping功能之后将允许该用户上线，并刷新DHCP Snooping绑定表。但是在某些场景中，这样的处理方式存在安全风险，比如网络中存在攻击者仿冒合法用户发送DHCP Discover报文，最终导致DHCP Snooping绑定表被刷新，合法用户网络访问中断。此时需要去使能DHCP Snooping用户位置迁移功能，丢弃DHCP Snooping绑定表中已存在的用户（用户MAC信息存在于DHCP Snooping绑定表中）从其他接口发送来的DHCP Discover报文。

说明

接口A和接口B必须属于同一VLAN。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**undo dhcp snooping user-transfer enable**，去使能DHCP Snooping用户位置迁移功能。

缺省情况下，已使能DHCP Snooping用户位置迁移功能。

----结束

9.6.4 （可选）配置 ARP 与 DHCP Snooping 的联动功能

背景信息

DHCP Snooping设备在收到DHCP用户发出的DHCP Release报文时将会删除该用户对应的绑定表项，但若用户发生了异常下线而无法发出DHCP Release报文时，DHCP Snooping设备将不能够及时的删除该DHCP用户对应的绑定表。

使能ARP与DHCP Snooping的联动功能，如果DHCP Snooping表项中的IP地址对应的ARP表项达到老化时间，则DHCP Snooping设备会对该IP地址进行ARP探测，如果在规定的探测次数内探测不到用户，设备将删除用户对应的ARP表项。之后，设备将会再次按规定的探测次数对该IP地址进行ARP探测，如果最后仍不能够探测到用户，则设备将会删除该用户对应的绑定表项。

说明

使用ARP与DHCP Snooping的联动功能之前，需要保证设备上具有与客户端同网段的IP地址用于ARP探测。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**arp dhcp-snooping-detect enable**，使能ARP与DHCP Snooping的联动功能。

缺省情况下，未使能ARP与DHCP Snooping的联动功能。

----结束

9.6.5 （可选）配置用户下线后及时清除对应 MAC 表项功能

背景信息

当某一DHCP用户下线时，设备上其对应的动态MAC表项还未达到老化时间，则设备在接收到来自网络侧以该用户IP地址为目的地址的报文时，将继续根据动态MAC表项转发此报文。这种无效的报文处理在一定程度上将会降低设备的性能。

设备在接收到DHCP用户下线时发送DHCP Release报文后，将会立刻删除用户对应的DHCP Snooping绑定表项。利用这种特性，使能当DHCP Snooping动态表项清除时移

除对应用户的MAC表项功能，则当用户下线时，设备将会及时的移除用户的MAC表项。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**dhcp snooping user-offline remove mac-address**，使能当DHCP Snooping动态表项清除时移除对应用户的MAC表项功能。

缺省情况下，未使能当DHCP Snooping动态表项清除时移除对应用户的MAC表项功能。

----结束

9.6.6 （可选）配置丢弃 GIADDR 字段非零的 DHCP 报文

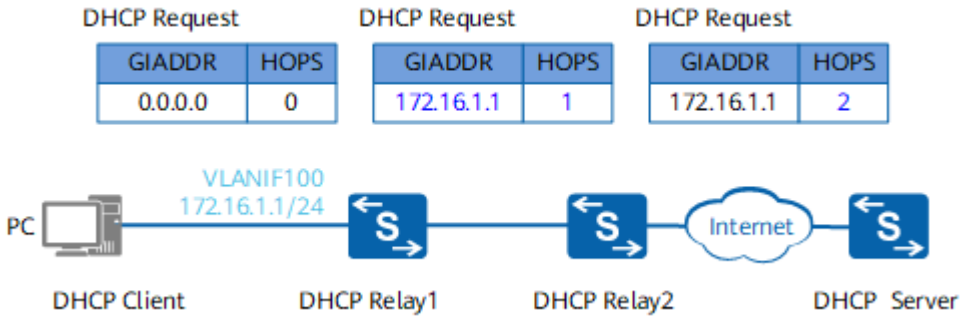
背景信息

DHCP报文中的GIADDR（Gateway Ip Address）字段记录了DHCP报文经过的第一个DHCP Relay的IP地址，当客户端发出DHCP请求时，如果服务器和客户端不在同一个网段，那么第一个DHCP Relay在将DHCP请求报文转发给DHCP服务器时，会把自己的IP地址填入此字段，DHCP服务器会根据此字段来判断出客户端所在的网段地址，从而选择合适的地址池，为客户端分配该网段的IP地址。

如图9-12所示，在为了保证设备在生成DHCP Snooping绑定表时能够获取到用户MAC等参数，DHCP Snooping功能需应用于二层网络中的接入设备或第一个DHCP Relay上（如图中的DHCP Relay1设备）。故DHCP Snooping设备接收到的DHCP报文中GIADDR字段必然为零，若不为零则该报文为非法报文，设备需丢弃此类报文。在DHCP中继使能DHCP Snooping场景中，建议配置该功能。

通常情况下，PC发出的DHCP报文中GIADDR字段为零。在某些情况下，PC发出的DHCP报文中GIADDR字段不为零，可能导致DHCP服务器分配错误的IP地址。为了防止PC用户伪造GIADDR字段不为零的DHCP报文申请IP地址，建议配置该功能。

图 9-12 多 DHCP 中继场景下 DHCP 报文处理流程（以 DHCP Request 报文为例）



操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 使能检测DHCP Request报文中GIADDR字段是否非零的功能，可在系统视图、VLAN视图或接口视图下进行配置。

- 系统视图下：

1. 执行命令**dhcp snooping check dhcp-giaddr enable vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，使能检测DHCP Request报文中GIADDR字段是否非零的功能。

   缺省情况下，未使能检测DHCP Request报文中GIADDR字段是否非零的功能。

- VLAN视图或接口视图下：

1. 执行命令**vlan** *vlan-id*，进入VLAN视图；或执行命令**interface** *interface-type interface-number*，进入接口视图。
2. 执行命令**dhcp snooping check dhcp-giaddr enable**，使能检测DHCP Request报文中GIADDR字段是否非零的功能。

   缺省情况下，未使能检测DHCP Request报文中GIADDR字段是否非零的功能。

在VLAN视图下执行此命令，则对设备所有接口接收到的属于该VLAN的DHCP报文命令功能生效；在接口下执行该命令，则对该接口下的所有DHCP报文命令功能生效。

----结束

9.6.7 （可选）配置丢弃 DHCPv6 Relay-Forward 报文

背景信息

DHCPv6 Snooping功能需应用于二层网络中的接入设备或第一个DHCPv6中继设备上，所以，配置DHCPv6 Snooping功能的设备不应该收到中继转发的报文（DHCPv6 Relay-Forward报文），如果收到，则该报文为非法报文，设备需丢弃此类报文。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 使能丢弃DHCPv6 Relay-Forward报文的功能，可在系统视图、VLAN视图或接口视图下进行配置。

- 系统视图下：

1. 执行命令**dhcpv6 snooping check relay-forward enable vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，使能丢弃DHCPv6 Relay-Forward报文的功能。

   缺省情况下，未使能丢弃DHCPv6 Relay-Forward报文功能。

- VLAN视图或接口视图下：

1. 执行命令**vlan** *vlan-id*，进入VLAN视图；或执行命令**interface** *interface-type interface-number*，进入接口视图。
2. 执行命令**dhcpv6 snooping check relay-forward enable**，使能丢弃DHCPv6 Relay-Forward报文的功能。

   缺省情况下，未使能丢弃DHCPv6 Relay-Forward报文功能。

在VLAN视图下执行此命令，则对设备所有接口接收到的属于该VLAN的DHCP报文命令功能生效；在接口下执行该命令，则对该接口下的所有DHCP报文命令功能生效。

----结束

9.6.8 （可选）配置 DHCP 报文交互时记录日志的功能

背景信息

打开DHCP报文交互时记录日志的功能后，设备每次收到DHCP报文都会记录日志**DHCP/6/SNP_RCV_MSG**。该日志可以用在智能运维等场景中，网络分析器通过该日志对用户IP地址获取问题进行智能分析。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**dhcp snooping packet-flow log enable**，打开DHCP报文交互时记录日志的功能。

缺省情况下，DHCP报文交互时记录日志的功能处于关闭状态。

----结束

检查配置结果

执行命令**display dhcp snooping**，查看DHCP报文交互时记录日志的功能是否开启。

9.6.9 （可选）配置 DHCPv6 Snooping 探测 confirm-client 是否在线功能

背景信息

confirm-client指通过DHCPv6 Confirm报文生成绑定表的客户端，当客户端重新上线时，会发送DHCPv6 Confirm报文。

DHCPv6 Snooping在用户侧端口收到DHCPv6 Confirm报文会生成DHCPv6 Snooping绑定表。由于DHCPv6 Confirm报文没有携带有效租期，当confirm-client离线时，绑定表无法及时老化删除，占用了表项规格，可能导致新用户无法正常上线。

开启探测confirm-client是否在线功能后，DHCPv6 Snooping会周期性发送DAD类型的NS报文探测用户是否在线，及时删除下线的confirm-client的DHCPv6 Snooping表项。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**dhcpv6 snooping user-bind detect confirm-client enable**，开启DHCPv6 Snooping探测confirm-client是否在线功能。

缺省情况下，DHCPv6 Snooping探测confirm-client是否在线功能处于开启状态。

步骤3 执行命令**dhcpv6 snooping user-bind detect retransmit** *times* **interval** *interval*，配置DHCPv6 Snooping探测用户是否在线的DAD NS报文的发送次数和发送时间间隔。

缺省情况下，DHCPv6 Snooping探测用户是否在线的DAD NS报文发送次数为3次，发送时间间隔为180秒。

----结束

9.6.10 （可选）去使能接口 DHCP Snooping 功能

背景信息

若使能了某一VLAN的DHCP Snooping功能，则VLAN内所有的接口均使能了DHCP Snooping功能。此时如果需要去使能一特定接口的DHCP Snooping功能，可使用命令**dhcp snooping disable**去使能特定接口的DHCP Snooping功能。此后该接口下的用户将能正常上线，但是并不会生成DHCP动态绑定表。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入指定的接口视图。

步骤3 执行命令**dhcp snooping disable**，去使能接口的DHCP Snooping功能。

缺省情况下，接口的DHCP Snooping功能是否使能依赖于是否在该接口或者该接口所在的VLAN下使用**dhcp snooping enable**命令使能DHCP Snooping功能。

----结束

9.6.11 检查 DHCP Snooping 基本功能的配置结果

前提条件

已经完成DHCP Snooping基本功能的所有配置。

操作步骤

- 查看DHCP Snooping的配置和运行相关信息。
  - 执行命令**display dhcp snooping configuration** [**vlan** *vlan-id* | **interface** *interface-type interface-number*]，查看DHCP Snooping的配置信息
  - 执行命令**display dhcp snooping** [**interface** *interface-type interface-number* | **vlan** *vlan-id*]，查看DHCP Snooping的运行信息。
- 查看DHCP Snooping绑定表相关信息。
  - 执行命令**display dhcp snooping user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**]，查看DHCP Snooping绑定表信息。
  - 执行命令**display dhcpv6 snooping user-bind** { { **interface** *interface-type interface-number* | **ipv6-address** { *ipv6-address* | **all** } | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**]，查看DHCPv6 Snooping绑定表信息。
  - 执行命令**display dhcpv6 snooping user-bind ipv6-prefix** { *prefix*| *prefix-length* | **all** } [**verbose**]，查看IPv6前缀绑定表信息。

- 执行命令**display dhcp snooping statistics** { **global** | **vlan** *vlan-id* | **interface** *interface-type interface-number* }，查看设备接收到的各类型DHCP报文的统计信息。
- 执行命令**display dhcpv6 snooping statistics**，查看DHCPv6 Snooping统计信息。

----结束

9.7 配置 DHCP Snooping 的攻击防范功能

本章节中，**配置防止仿冒DHCP报文攻击**功能、**配置防止DHCP Server服务拒绝攻击**中的“步骤2”相关功能同样适用于DHCPv6 Snooping。

前提条件

配置DHCP Snooping的攻击防范功能之前，务必确保已完成DHCP Snooping的基本功能配置。

9.7.1 使能 DHCP Server 探测功能

背景信息

在使能DHCP Snooping功能并配置了接口的信任状态之后，设备将能够保证客户端从合法的服务器获取IP地址，这将能够有效的防止DHCP Server仿冒者攻击。但是此时却不能够定位DHCP Server仿冒者的位置，使得网络中仍然存在着安全隐患。

通过配置DHCP Server探测功能，DHCP Snooping设备将会检查并在日志中记录所有DHCP回应报文中携带的DHCP Server地址与接口等信息，此后网络管理员可根据日志来判定网络中是否存在伪DHCP Server进而对网络进行维护。

DHCP Snooping设备缺省只根据MAC地址检查DHCP回应报文识别设备，仅通过MAC地址无法正确识别设备时，执行**dhcp snooping check server-vlan enable**命令后，DHCP Snooping设备根据MAC地址和VLAN信息检查DHCP回应报文识别设备。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**dhcp snooping enable**，使能了设备的DHCP Snooping功能。

步骤3 执行命令**dhcp server detect**，使能DHCP Server探测功能。

缺省情况下，未使能DHCP Server探测功能。

步骤4 （可选）执行命令**dhcp snooping check server-vlan enable**，使能DHCP Snooping设备检查DHCP回应报文携带VLAN信息功能。

缺省情况下，未使能DHCP Snooping设备检查DHCP回应报文携带VLAN信息功能。

----结束

9.7.2 配置防止 DHCP 报文泛洪攻击

背景信息

在DHCP网络环境中，若存在DHCP用户短时间内向设备发送大量的DHCP报文，将会对设备的性能造成巨大的冲击以致可能会导致设备无法正常工作。通过使能对DHCP报文上送DHCP报文处理单元的速率进行检测功能将能够有效防止DHCP报文泛洪攻击。

说明

- 配置以下功能前，需确保已使用命令**dhcp snooping enable**使能了设备的DHCP Snooping功能。
- 配置限制DHCP报文的上送速率时：
  - 在系统视图配置时，则对设备所有的接口有效；在接口视图配置时，则仅针对该接口有效；在VLAN视图配置时，则对属于该VLAN的所有接口有效。
  - 在系统视图、VLAN视图、接口视图同时配置最大允许的上送速率时，则以三者中的最小值为准。
- 配置告警功能时：
  - 在系统视图配置时，则对设备所有的接口有效；在接口视图配置时，则仅针对该接口有效。
  - 在系统视图、接口视图下同时配置告警阈值时，则以两者最小值为准。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 配置限制DHCPv4报文的上送速率和告警功能。

配置限制DHCPv4报文的上送速率：

- 系统视图下：
  a. 执行命令**dhcp snooping check dhcp-rate enable**，使能对DHCP报文上送DHCP报文处理单元的速率进行检测功能。

     缺省情况下，未使能对DHCP报文上送DHCP报文处理单元的速率进行检测功能。

     在系统视图下执行命令**dhcp snooping check dhcp-rate enable vlan** { *vlan-id1* [**to** *vlan-id2*] }&<1-10>，功能与在VLAN视图下执行命令**dhcp snooping check dhcp-rate enable**相同。
  b. 执行命令**dhcp snooping check dhcp-rate** *rate*，配置DHCP报文上送DHCP报文处理单元的最大允许速率。

     缺省情况下，全局DHCP报文上送DHCP报文处理单元的最大允许速率为100pps，接口下DHCP报文上送DHCP报文处理单元的最大允许速率为在系统视图下配置的值。
- VLAN视图下：
  a. 执行命令**vlan** *vlan-id*，进入VLAN视图。
  b. 执行命令**dhcp snooping check dhcp-rate enable**，使能对DHCP报文上送DHCP报文处理单元的速率进行检测功能。

     缺省情况下，未使能对DHCP报文上送DHCP报文处理单元的速率进行检测功能。

     在VLAN视图下执行此命令，则对设备所有接口接收到的属于该VLAN的DHCP报文命令功能生效。

在系统视图下执行命令**dhcp snooping check dhcp-rate vlan** { *vlan-id1* [**to** *vlan-id2*] }&<1-10>，功能与在VLAN视图下执行命令**dhcp snooping check dhcp-rate enable**相同。

c. 执行命令**dhcp snooping check dhcp-rate** *rate*，配置DHCP报文上送DHCP报文处理单元的最大允许速率。

缺省情况下，全局DHCP报文上送DHCP报文处理单元的最大允许速率为100pps，接口下DHCP报文上送DHCP报文处理单元的最大允许速率为在系统视图下配置的值。

d. 执行命令**quit**，返回到系统视图。

- 接口视图下：

a. 执行命令**interface** *interface-type interface-number*，进入接口视图。

b. 执行命令**dhcp snooping check dhcp-rate**，使能对DHCP报文上送DHCP报文处理单元的速率进行检测功能。

缺省情况下，未使能对DHCP报文上送DHCP报文处理单元的速率进行检测功能。

c. 执行命令**dhcp snooping check dhcp-rate** *rate*，配置DHCP报文上送DHCP报文处理单元的最大允许速率。

缺省情况下，全局DHCP报文上送DHCP报文处理单元的最大允许速率为100pps，接口下DHCP报文上送DHCP报文处理单元的最大允许速率为在系统视图下配置的值。

d. 执行命令**quit**，返回到系统视图。

告警功能：

- 系统视图下：

a. 执行命令**dhcp snooping alarm dhcp-rate enable**，使能当丢弃的DHCP报文数达到告警阈值时的告警功能。

若在系统视图下执行该命令，则对设备所有的接口该命令功能生效。

缺省情况下，未使能当丢弃的DHCP报文数达到告警阈值时的告警功能。

b. 执行命令**dhcp snooping alarm dhcp-rate enable** *threshold*，配置接口下被丢弃的DHCP报文的告警阈值。

缺省情况下，全局被丢弃的DHCP报文的告警阈值为100packets，接口下被丢弃的DHCP报文的告警阈值为在系统视图下配置的值。

- 接口视图下：

a. 执行命令**interface** *interface-type interface-number*，进入接口视图。

b. 执行命令**dhcp snooping alarm dhcp-rate enable**，使能当丢弃的DHCP报文数达到告警阈值时的告警功能。

若在系统视图下执行该命令，则对设备所有的接口该命令功能生效。

缺省情况下，未使能当丢弃的DHCP报文数达到告警阈值时的告警功能。

c. 执行命令**dhcp snooping alarm dhcp-rate enable** *threshold*，配置接口下被丢弃的DHCP报文的告警阈值。

缺省情况下，全局被丢弃的DHCP报文的告警阈值为100packets，接口下被丢弃的DHCP报文的告警阈值为在系统视图下配置的值。

d. 执行命令**quit**，返回到系统视图。

步骤3 配置限制DHCPv6报文的上送速率和告警功能。

配置限制DHCPv6报文的上送速率：

- 系统视图下：
  a. 执行命令**dhcp snooping check dhcpv6-rate enable**，使能对DHCPv6报文上送DHCPv6报文处理单元的速率进行检测功能。

     缺省情况下，未使能对DHCPv6报文上送DHCPv6报文处理单元的速率进行检测功能。
  b. 执行命令**dhcp snooping check dhcpv6-rate** *rate*，配置DHCPv6报文上送DHCPv6报文处理单元的最大允许速率。

     缺省情况下，DHCPv6报文上送DHCPv6报文处理单元的最大允许速率为100pps。
- VLAN视图下：
  a. 执行命令**vlan** *vlan-id*，进入VLAN视图。
  b. 执行命令**dhcp snooping check dhcpv6-rate enable**，使能对DHCPv6报文上送DHCPv6报文处理单元的速率进行检测功能。

     缺省情况下，未使能对DHCPv6报文上送DHCPv6报文处理单元的速率进行检测功能。
  c. 执行命令**dhcp snooping check dhcpv6-rate** *rate*，配置DHCPv6报文上送DHCPv6报文处理单元的最大允许速率。

     缺省情况下，DHCPv6报文上送DHCPv6报文处理单元的最大允许速率为100pps。
  d. 执行命令**quit**，返回到系统视图。
- 接口视图下：
  a. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  b. 执行命令**dhcp snooping check dhcpv6-rate enable**，使能对DHCPv6报文上送DHCPv6报文处理单元的速率进行检测功能。

     缺省情况下，未使能对DHCPv6报文上送DHCPv6报文处理单元的速率进行检测功能。
  c. 执行命令**dhcp snooping check dhcpv6-rate** *rate*，配置DHCPv6报文上送DHCPv6报文处理单元的最大允许速率。

     缺省情况下，DHCPv6报文上送DHCPv6报文处理单元的最大允许速率为100pps。
  d. 执行命令**quit**，返回到系统视图。

告警功能：

- 系统视图下：
  a. 执行命令**dhcp snooping alarm dhcpv6-rate enable**，使能当丢弃的DHCPv6报文数达到告警阈值时的告警功能。

     缺省情况下，未使能当丢弃的DHCPv6报文数达到告警阈值时的告警功能。
  b. 执行命令**dhcp snooping alarm dhcpv6-rate threshold** *threshold*，配置被丢弃的DHCPv6报文的告警阈值。

     缺省情况下，全局被丢弃的DHCPv6报文的告警阈值为100packets。
- 接口视图下：
  a. 执行命令**interface** *interface-type interface-number*，进入接口视图。

b. 执行命令**dhcp snooping alarm dhcpv6-rate enable**，使能当丢弃的DHCPv6报文数达到告警阈值时的告警功能。

缺省情况下，未使能当丢弃的DHCPv6报文数达到告警阈值时的告警功能。

c. 执行命令**dhcp snooping alarm dhcpv6-rate threshold** *threshold*，配置被丢弃的DHCPv6报文的告警阈值。

缺省情况下，接口下被丢弃的DHCPv6报文的告警阈值为在系统视图下配置的值。

d. 执行命令**quit**，返回到系统视图。

----结束

9.7.3 配置防止仿冒 DHCP 报文攻击

背景信息

在DHCP网络环境中，若攻击者仿冒合法用户的DHCP报文发往DHCP服务器，会导致合法用户无法使用该IP地址或异常下线。在生成DHCP Snooping绑定表后，设备可根据绑定表项，对DHCP报文进行匹配检查，只有匹配成功的报文设备才将其转发，否则将丢弃。这将能有效的防止非法用户通过发送伪造DHCP报文冒充合法用户进行续租或释放IP地址。

操作步骤

步骤1 开启对DHCP报文进行绑定表匹配检查的功能

在VLAN视图下执行以下命令，对属于该VLAN的所有接口都生效；在接口下执行该命令，仅对该接口生效。

- 系统视图下：

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**dhcp snooping check dhcp-request enable vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，开启对从指定VLAN内上送的DHCP报文进行绑定表匹配检查的功能。

   缺省情况下，未开启对DHCP请求报文进行绑定表匹配检查的功能。
3. 执行命令**dhcp snooping check dhcp-chaddr enable vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，开启检测DHCP Request报文帧头源MAC地址与CHADDR字段是否相同的功能。

   缺省情况下，未开启检测DHCP Request报文帧头源MAC地址与CHADDR字段是否相同的功能。

- VLAN视图或接口视图下：

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**vlan** *vlan-id*，进入VLAN视图；或执行命令**interface** *interface-type interface-number*，进入接口视图。
3. 执行命令**dhcp snooping check dhcp-request enable**，开启对DHCP报文进行绑定表匹配检查的功能。

   缺省情况下，未开启对DHCP报文进行绑定表匹配检查的功能。
4. 执行命令**dhcp snooping check dhcp-chaddr enable**，开启检测DHCP Request报文帧头源MAC地址与CHADDR字段是否相同的功能。

缺省情况下，未开启检测DHCP Request报文帧头源MAC地址与CHADDR字段是否相同的功能。

步骤2 （可选）开启DHCP Snooping告警功能

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**vlan** *vlan-id*，进入VLAN视图；或执行命令**interface** *interface-type interface-number*，进入接口视图。
3. 执行命令**dhcp snooping alarm** { **dhcp-request** | **dhcp-chaddr** | **dhcp-reply** | **dhcpv6-request** } **enable**，开启DHCP Snooping告警功能。

   缺省情况下，未开启DHCP Snooping告警功能。

步骤3 （可选）配置告警阈值

若在系统视图、接口视图下同时进行了配置，则接口下DHCP Snooping丢弃报文数量的告警阈值以两者最小值为准。

- 系统视图下：

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**dhcp snooping alarm threshold** *threshold*，配置DHCP Snooping丢弃报文数量的告警阈值。

   在系统视图下执行该命令，则对设备所有的接口该命令功能生效。

   缺省情况下，DHCP Snooping丢弃报文数量的告警阈值为100packets。

- 接口视图、VLAN视图下：

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**vlan** *vlan-id*，进入VLAN视图；或执行命令**interface** *interface-type interface-number*，进入接口视图。
3. 执行命令**dhcp snooping alarm** { **dhcp-request** | **dhcp-chaddr** | **dhcp-reply** | **dhcpv6-request** } **threshold** *threshold*，配置DHCP Snooping丢弃报文数量的告警阈值。

   缺省情况下，全局DHCP Snooping丢弃报文数量的告警阈值为100packets，接口下DHCP Snooping丢弃报文数量的告警阈值为在系统视图下使用命令**dhcp snooping alarm threshold**配置的值。

----结束

9.7.4 配置防止 DHCP Server 服务拒绝攻击

背景信息

若在网络中存在DHCP用户恶意申请IP地址，将会导致IP地址池中的IP地址快速耗尽以致DHCP Server无法为其他合法用户分配IP地址。另一方面，DHCP Server通常仅根据CHADDR（client hardware address）字段来确认客户端的MAC地址。如果攻击者通过不断改变DHCP Request报文中的CHADDR字段向DHCP Server申请IP地址，将会导致DHCP Server上的地址池被耗尽，从而无法为其他正常用户提供IP地址。

为了防止某些端口的DHCP用户恶意申请IP地址，可配置接口允许学习的DHCP Snooping绑定表项的最大个数来控制上线用户的个数，当用户数达到该值时，则任何用户将无法通过此接口成功申请到IP地址。为了防止攻击者不断改变DHCP Request报文中的CHADDR字段进行攻击，可使能检测DHCP Request报文帧头MAC地址与DHCP数据区中CHADDR字段是否相同的功能，相同则转发报文，否则丢弃。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 配置接口允许学习的DHCP Snooping绑定表项的最大个数，可在系统视图、VLAN视图或接口视图下配置。

- 系统视图下：

1. 执行命令**dhcp snooping max-user-number** *max-user-number* **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，配置设备允许学习的DHCP Snooping绑定表项的最大个数。

   执行该命令后，设备所有的接口允许学习的DHCP Snooping绑定表项之和为该命令所配置的值。

   缺省情况下，接口允许学习的DHCP Snooping绑定表项的最大个数为512。

2. （可选）执行命令**dhcp snooping user-alarm percentage** *percent-lower-value percent-upper-value*，配置DHCP Snooping绑定表的告警阈值百分比。

   缺省情况下，DHCP Snooping绑定表的下限告警阈值百分比为50，上限告警阈值百分比为100。

- VLAN视图或接口视图下：

1. 执行命令**vlan** *vlan-id*，进入VLAN视图；或执行命令**interface** *interface-type interface-number*，进入接口视图。
2. 执行命令**dhcp snooping max-user-number** *max-user-number* ，配置接口允许学习的DHCP Snooping绑定表项的最大个数。

   若在VLAN视图下执行该命令，则VLAN内所有的接口接入的用户最大数为该命令所配置的值。

   缺省情况下，接口允许学习的DHCP Snooping绑定表项的最大个数为512。

   在VLAN视图下执行此命令，则对设备所有接口接收到的属于该VLAN的DHCP报文命令功能生效；在接口下执行该命令，则对该接口下的所有DHCP报文命令功能生效。

   若在系统视图、VLAN视图、接口视图下同时进行了配置，则接口下允许接入的最大用户数以三者最小值为准。

步骤3 使能对报文的CHADDR字段进行检查功能，可在系统视图、VLAN视图或接口视图下进行配置。

- 系统视图下：

1. 执行命令**dhcp snooping check dhcp-chaddr enable vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，使能检测DHCP Request报文帧头MAC与DHCP数据区中CHADDR字段是否一致功能。

   缺省情况下，未使能检测DHCP Request报文帧头MAC与DHCP数据区中CHADDR字段是否一致功能。

2. （可选）执行命令**dhcp snooping alarm threshold** *threshold*，配置全局DHCP Snooping丢弃报文数量的告警阈值。

   在系统视图下执行该命令，则设备所有的接口该命令功能生效。

   缺省情况下，全局DHCP Snooping丢弃报文数量的告警阈值为100packets。

- VLAN视图或接口视图下：

1. 执行命令**vlan** *vlan-id*，进入VLAN视图；或执行命令**interface** *interface-type interface-number*，进入接口视图。
2. 执行命令**dhcp snooping check dhcp-chaddr enable**，使能检测DHCP Request报文帧头MAC与DHCP数据区中CHADDR字段是否一致功能。

   缺省情况下，未使能检测DHCP Request报文帧头MAC与DHCP数据区中CHADDR字段是否一致功能。

   在VLAN视图下执行此命令，则对设备所有接口接收到的属于该VLAN的DHCP报文命令功能生效；在接口下执行该命令，则仅对该接口接收到的所有DHCP报文命令功能生效。
3. （可选）执行命令**dhcp snooping alarm dhcp-chaddr enable**，使能数据帧头MAC地址与DHCP报文中的CHADDR字段不一致被丢弃的报文达到阈值时的DHCP Snooping告警功能。

   缺省情况下，未使能DHCP Snooping告警功能。

   说明

   该命令仅能在接口视图下执行。
4. （可选）执行命令**dhcp snooping alarm dhcp-chaddr threshold** *threshold*，配置帧头MAC地址与DHCP数据区中CHADDR字段不匹配而被丢弃的DHCP报文的告警阈值。

   缺省情况下，全局DHCP Snooping丢弃报文数量的告警阈值为100packets，接口下DHCP Snooping丢弃报文数量的告警阈值为在系统视图下使用命令**dhcp snooping alarm threshold**配置的值。

   若在系统视图、接口视图下同时进行了配置，则接口下DHCP Snooping丢弃报文数量的告警阈值以两者最小值为准。

   说明

   该命令仅能在接口视图下执行。

----结束

9.7.5 检查 DHCP Snooping 攻击防范功能的配置结果

背景信息

DHCP Snooping的攻击防范功能配置完成后，可使用命令查看已配置的参数信息。

操作步骤

- 执行命令**display dhcp snooping** [**interface** *interface-type interface-number* | **vlan** *vlan-id*]，查看DHCP Snooping的运行信息。
- 执行命令**display dhcp snooping configuration** [**vlan** *vlan-id* | **interface** *interface-type interface-number*]，查看DHCP Snooping的配置信息。
- 执行命令**display dhcp snooping statistics** { **global** | **vlan** *vlan-id* | **interface** *interface-type interface-number* }，查看设备接收到的各类型DHCP报文的统计信息。

----结束

9.7.6 配置防止仿冒 DHCPv6 报文攻击

背景信息

在DHCPv6网络环境中，若攻击者仿冒合法用户的DHCPv6报文发往DHCPv6服务器，会导致合法用户无法使用该IP地址或异常下线。在生成DHCPv6 Snooping绑定表后，设备可根据MAC表项作为key值查找绑定表项，对DHCPv6 Request报文和DHCPv6 Release报文进行匹配检查，只有匹配成功的报文设备才将其转发，否则将丢弃。这将能有效的防止非法用户通过发送伪造的DHCPv6报文冒充合法用户续租或释放IP地址。当判断DHCPv6报文非法时，丢弃报文。此时开启探测用户是否在线功能，DHCPv6 Snooping会以探测3次、每次3秒的周期发送DAD类型的NS报文，探测DHCPv6用户是否在线。如果在周期内未收到DHCPv6用户的回应报文，则认为该用户已下线，及时删除下线用户的DHCPv6 Snooping表项。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**dhcp enable**，开启DHCP功能。

步骤3 执行命令**dhcp snooping enable** [**ipv4** | **ipv6**]，全局使能DHCP Snooping功能。

缺省情况下，设备全局未使能DHCP Snooping功能。

说明

系统视图下，**dhcp snooping enable**命令是DHCP Snooping相关功能的总开关。执行**undo dhcp snooping enable**命令后，设备上所有DHCP Snooping相关的配置会被删除；再次执行**dhcp snooping enable**命令使能DHCP Snooping功能后，设备上所有DHCP Snooping相关配置将被恢复为缺省配置。

步骤4 使能依据MAC检查DHCPv6报文合法性功能

缺省情况下，未使能依据MAC检查DHCPv6报文合法性功能。

在VLAN视图下执行此命令，将仅对属于该VLAN的DHCPv6报文命令功能生效；在接口下执行该命令，则将对该接口下的所有DHCPv6报文命令功能生效。

在系统视图下执行该命令，则对设备所有的接口该命令功能生效。

- 系统视图下：

1. 执行命令**dhcp snooping check dhcpv6-request mac**，使能依据MAC检查DHCPv6报文合法性功能。

- VLAN视图下：

1. 执行命令**vlan** *vlan-id*，进入VLAN视图；
2. 执行命令**dhcp snooping check dhcpv6-request mac**，使能依据MAC检查DHCPv6报文合法性功能。
3. 执行命令**quit**，返回系统视图

- 接口视图下：

1. 执行命令**interface** *interface-type interface-number*，进入接口视图。
2. 执行命令**dhcp snooping check dhcpv6-request mac**，使能依据MAC检查DHCPv6报文合法性功能。
3. 执行命令**quit**，返回系统视图

步骤5 使能DHCPv6 Snooping探测用户是否在线功能

缺省情况下，未使能DHCPv6 Snooping探测用户是否在线功能。

1. 执行命令**dhcpv6 snooping user-bind mac-conflict detect enable**，使能DHCPv6 Snooping探测用户是否在线功能。

----结束

9.8 配置在 DHCP 报文中添加 Option82 字段

背景信息

Option82选项记录了DHCP Client的位置信息。设备通过在DHCP请求报文中添加Option82选项，可将DHCP Client的位置信息发送给DHCP Server，从而使得DHCP Server能够根据Option82选项的内容为DHCP Client分配合适的IP地址和其他配置信息，并可以实现对客户端的安全控制。

说明

- DHCP Option82必须配置在设备的用户侧，否则设备向DHCP Server发出的DHCP报文不会携带Option82选项内容。
- 所有Option82选项共用1～255个字节长度，因此，所有Option82选项长度之和不能超过255个字节，否则会导致部分Option82选项信息丢失。
- 设备不限制配置多少个Option82选项，但是大量配置会占用很多内存，并延长设备处理时间。为保证设备性能，建议用户根据自身需要和设备内存大小来配置Option82选项。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 使能在DHCP报文中添加Option82选项功能，可在VLAN视图或接口视图下进行配置。

视图	操作步骤
VLAN视图	1. 执行命令**vlan** *vlan-id*，进入VLAN视图。 2. 执行命令**dhcp option82** { **insert** | **rebuild** } **enable interface** *interface-type interface-number1* [**to** *interface-number2*]，使能在DHCP报文中添加Option82选项功能。缺省情况下，未使能在DHCP报文中添加Option82选项功能。 3. 执行命令**quit**，返回到系统视图。
接口视图	1. 执行命令**interface** *interface-type interface-number*，进入接口视图。 2. 执行命令**dhcp option82** { **insert** | **rebuild** } **enable**，使能在DHCP报文中添加Option82选项功能。 缺省情况下，未使能在DHCP报文中添加Option82选项功能。 3. 执行命令**quit**，返回到系统视图。

步骤3 （可选）配置Option82选项的格式，可在系统视图或接口视图下进行配置。在系统视图下进行配置，对设备所有的接口功能生效；在接口下进行配置，仅对指定的接口功能生效。

视图	操作步骤
系统视图	1. 执行命令**dhcp option82** [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] [**circuit-id** | **remote-id**] **format** { **default** | **common** | **extend** | **user-defined** *text* }，配置在DHCP报文中添加的Option82选项的格式。 缺省情况下，在DHCP报文中添加的Option82选项的格式为**default**格式。
接口视图	1. 执行命令**interface** *interface-type interface-number*，进入接口视图。 2. 执行命令**dhcp option82** [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] [**circuit-id** | **remote-id**] **format** { **default** | **common** | **extend** | **user-defined** *text* }，配置在DHCP报文中添加的Option82选项的格式。 缺省情况下，在DHCP报文中添加的Option82选项的格式为**default**格式。 3. 执行命令**quit**，返回到系统视图。

步骤4 （可选）执行命令**dhcp option82 subscriber-id format** { **ascii** *ascii-text* | **hex** *hex-text* }，配置在DHCP报文的Option82选项中插入Sub6子选项。

缺省情况下，未配置在DHCP报文的Option82选项中插入Sub6子选项。

步骤5 （可选）配置在DHCP报文的Option82选项中插入Sub9子选项。

Option82选项的Sub9子选项分为新旧两种格式，旧格式携带hwid或其他公司的ID，新格式不携带。

- 执行命令**dhcp option82 vendor-specific format vendor-sub-option** *sub-option-num* { **ascii** *ascii-text* | **hex** *hex-text* | **ip-address** *ip-address* &<1-8> | **sysname** }，配置在DHCP报文的Option82选项中插入旧格式的Sub9子选项。
- 配置在DHCP报文的Option82选项中插入新格式的Sub9子选项。

视图	操作步骤
VLAN视图	1. 执行命令**vlan** *vlan-id*，进入VLAN视图。 2. 执行命令**dhcp option82 append vendor-specific**，配置在DHCP报文的Option82选项中插入新格式的Sub9子选项。 3. 执行命令**quit**，返回到系统视图。
接口视图	1. 执行命令**interface** *interface-type interface-number*，进入接口视图。 2. 执行命令**dhcp option82 append vendor-specific**，配置在DHCP报文的Option82选项中插入新格式的Sub9子选项。 3. 执行命令**quit**，返回到系统视图。

缺省情况下，未配置在DHCP报文的Option82选项中插入Sub9子选项。

说明

- 命令**dhcp option82 append vendor-specific**和命令**dhcp option82 vendor-specific format**同时配置时，前者生效。
- 只有设备上配置的Sub9子选项格式与接收到的DHCP报文中的格式一致时，Sub9子选项才能插入到Option82选项中。如果格式不一致：
  - 当配置命令**dhcp option82 vendor-specific format**时，新格式的Sub9子选项不能插入到Option82选项中。
  - 当配置命令**dhcp option82 append vendor-specific**时，旧格式的Sub9子选项信息能否插入到Option82选项中，还取决于Option82选项的添加方式（通过命令**dhcp option82 enable**配置）：

    Insert方式时，不会被插入到Option82选项。

    Rebuild方式时，旧格式的Sub9子选项信息被重构，然后被插入到Option82选项。

步骤6 （可选）配置插入DHCP Option82选项中的子选项，可在系统视图、VLAN视图或接口视图下进行配置。在系统视图下进行配置，对设备所有的接口功能生效；在VLAN视图下进行配置，对设备所有接口接收到的属于该VLAN的DHCP报文功能生效；在接口下进行配置，仅对指定的接口功能生效。

视图	操作步骤
系统视图	1. 执行命令**dhcp option82 encapsulation** { **circuit-id** | **remote-id** | **subscriber-id** | **vendor-specific-id** } *，配置插入DHCP Option82选项中的子选项。 缺省情况下，插入DHCP Option82选项中的子选项为circuit-id（CID）子选项和remote-id（RID）子选项。
VLAN视图	1. 执行命令**vlan** *vlan-id*，进入VLAN视图。 2. 执行命令**dhcp option82 encapsulation** { **circuit-id** | **remote-id** | **subscriber-id** | **vendor-specific-id** } *，配置插入DHCP Option82选项中的子选项。 缺省情况下，插入DHCP Option82选项中的子选项为circuit-id（CID）子选项和remote-id（RID）子选项。 3. 执行命令**quit**，返回到系统视图。
接口视图	1. 执行命令**interface** *interface-type interface-number*，进入接口视图。 2. 执行命令**dhcp option82 encapsulation** { **circuit-id** | **remote-id** | **subscriber-id** | **vendor-specific-id** } *，配置插入DHCP Option82选项中的子选项。 缺省情况下，插入DHCP Option82选项中的子选项为circuit-id（CID）子选项和remote-id（RID）子选项。 3. 执行命令**quit**，返回到系统视图。

----结束

检查配置结果

- 执行命令**display dhcp option82 configuration** [**vlan** *vlan-id* | **interface** *interface-type interface-number*]，查看DHCP Option82的配置信息。

9.9 配置通过 LDRA 功能感知用户位置

背景信息

在DHCPv6网络中，为获取用户详细的位置信息，可在靠近用户的接入设备上部署LDRA功能。

在使能LDRA功能之后，如果管理员信任DHCPv6网络中的用户，并且用户较多时，可取消DHCP Snooping记录用户绑定表项功能，否则一旦设备上的绑定表项数目达到最大值，新用户将无法上线。另一方面，设备通过在Relay-Forward报文中插入interface-id与remote-id选项以记录用户的位置信息，管理员可根据用户实际位置情况配置interface-id与remote-id选项的格式。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**vlan** *vlan-id*，进入VLAN视图。

步骤3 执行命令**dhcpv6 snooping relay-information enable** [**trust**]，使能DHCPv6 Snooping支持的LDRA功能。

缺省情况下，未使能DHCPv6 Snooping支持的LDRA功能。

步骤4 执行命令**quit**，返回到系统视图。

步骤5 （可选）执行命令**dhcpv6 interface-id format** { **default** | **user-defined** *text* }，配置在DHCPv6报文中添加的interface-id的格式。

缺省情况下，DHCPv6报文中添加的interface-id的格式为**default**。

步骤6 （可选）执行命令**dhcpv6 remote-id format** { **default** | **user-defined** *text* }，配置在DHCPv6报文中添加的remote-id的格式。

缺省情况下，DHCPv6报文中添加的remote-id的格式为**default**。

步骤7 （可选）配置在使能DHCP Snooping功能后，接口不生成用户绑定表。

基于VLAN进行配置，表示对设备所有接口下连接的属于该VLAN的DHCP用户，命令功能生效；基于接口进行配置，表示对设备该接口下连接的所有DHCP用户，命令功能生效。

缺省情况下，在使能DHCP Snooping功能后，接口生成用户绑定表。

配置维度	操作步骤
基于VLAN配置	在系统视图下针对多个VLAN批量配置 • 执行命令**dhcp snooping enable no-user-binding vlan** { *vlan-id1* [**to** *vlan-id2*] }&<1-10>，配置在使能DHCP Snooping功能后，接口不生成用户绑定表。 在VLAN视图下针对单个VLAN配置 1. 执行命令**vlan** *vlan-id*，进入VLAN视图。 2. 执行命令**dhcp snooping enable no-user-binding**，配置在使能DHCP Snooping功能后，接口不生成用户绑定表。 3. 执行命令**quit**，返回到系统视图。
基于接口配置	1. 执行命令**interface** *interface-type interface-number*，进入接口视图。 2. 执行命令**dhcp snooping enable no-user-binding**，配置在使能DHCP Snooping功能后，接口不生成用户绑定表。 3. 执行命令**quit**，返回到系统视图。

----结束

9.10 配置在 DHCPv6 报文中添加 Option18 或 Option37 字段

背景信息

DHCPv6报文中的Option18与Option37选项功能与DHCPv4报文中的Option82选项功能类似，其中Option18选项记录了客户端的接口信息，Option37选项记录了客户端的MAC地址信息。设备通过在DHCPv6请求报文中添加Option18或Option37选项，可将DHCPv6 Client的位置信息发送给DHCP Server，从而使得DHCP Server能够根据Option18或Option37选项的内容为DHCPv6 Client分配合适的IP地址和其他配置信息，并实现对客户端的安全控制。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**dhcpv6** { **option18** | **option37** } { **insert** | **rebuild** } **enable**，使能在DHCPv6 Request报文中添加Option18或Option37选项的功能。

缺省情况下，未使能在DHCPv6报文中添加Option18或Option37选项的功能。

说明

在VLAN视图下执行此命令，则对设备所有接口接收到的属于该VLAN的DHCPv6报文命令功能生效；在接口下执行该命令，则仅对该接口接收到的所有DHCPv6报文命令功能生效。

步骤4 执行命令**quit**，返回到系统视图。

步骤5 （可选）配置在DHCPv6报文中添加的Option18选项的格式，可在系统视图、VLAN视图或接口视图下执行。

- 系统视图下：
  a. 执行命令（可选）执行命令**dhcpv6 option18** [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] **format user-defined** *text*，配置在DHCPv6报文中添加的Option18选项的格式。

     缺省情况下，未配置在DHCPv6报文中添加的Option18选项的格式。
- VLAN视图下：
  a. 执行命令**vlan** *vlan-id*，进入VLAN视图。
  b. （可选）执行命令**dhcpv6 option18 format user-defined** *text*，配置在DHCPv6报文中添加的Option18选项的格式。

     缺省情况下，未配置在DHCPv6报文中添加的Option18选项的格式。
- 接口视图下：
  a. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  b. （可选）执行命令**dhcpv6 option18** [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] **format user-defined** *text*，配置在DHCPv6报文中添加的Option18选项的格式。

     缺省情况下，未配置在DHCPv6报文中添加的Option18选项的格式。

说明

在系统视图下执行此命令，则对所有DHCPv6报文的Option18选项生效；在VLAN视图下执行此命令，则对设备所有接口接收到的属于该VLAN的DHCPv6报文的Option18选项生效；在接口下执行该命令，则仅对该接口接收到的所有DHCPv6报文的Option18选项生效。

步骤6 （可选）配置在DHCPv6报文中添加的Option37选项的格式，可在系统视图、VLAN视图或接口视图下执行。

- 系统视图下：
  a. 执行命令**dhcpv6 option37** [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] **format user-defined** *text*，配置在DHCPv6报文中添加的Option37选项的格式。

     缺省情况下，未配置在DHCPv6报文中添加的Option37选项的格式。
- VLAN视图下：
  a. 执行命令**vlan** *vlan-id*，进入VLAN视图。
  b. 执行命令**dhcpv6 option37 format user-defined** *text*，配置在DHCPv6报文中添加的Option37选项的格式。

     缺省情况下，未配置在DHCPv6报文中添加的Option37选项的格式。
- 接口视图下：
  a. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  b. 执行命令**dhcpv6 option37** [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] **format user-defined** *text*，配置在DHCPv6报文中添加的Option37选项的格式。

     缺省情况下，未配置在DHCPv6报文中添加的Option37选项的格式。

说明

在系统视图下执行此命令，则对所有DHCPv6报文的Option37选项生效；在VLAN视图下执行此命令，则对设备所有接口接收到的属于该VLAN的DHCPv6报文的Option37选项生效；在接口下执行该命令，则仅对该接口接收到的所有DHCPv6报文的Option37选项生效。

----结束

9.11 维护 DHCP Snooping

9.11.1 清除 DHCP Snooping 的统计信息

背景信息

须知

清除统计信息后，以前的统计信息将无法恢复，请慎重操作。

操作步骤

- 在用户视图下执行命令**reset dhcp snooping statistics global**，清除全局的报文丢弃统计计数。
- 在用户视图下执行命令**reset dhcp snooping statistics interface** *interface-type interface-number* [**vlan** *vlan-id*]，清除接口下的报文丢弃统计计数。
- 在用户视图下执行命令**reset dhcp snooping statistics vlan** *vlan-id* [**interface** *interface-type interface-number*]，清除VLAN下的报文丢弃统计计数。

----结束

9.11.2 清除 DHCP Snooping 绑定表

背景信息

由于在组网环境变化之后，DHCP Snooping绑定表不会立即老化，而DHCP Snooping绑定表匹配的如下信息可能会发生变化，导致报文转发错误。

- 用户所属VLAN信息。
- 用户所连接的接口信息。

所以，请在变更组网环境之前手动清除所有DHCP Snooping绑定表项，使得设备根据新的网络环境生成新的DHCP Snooping绑定表。

须知

清除DHCP Snooping绑定表后，设备下所连接的所有DHCP用户均需重新上线生成绑定表后方可恢复正常网络通信，请慎重操作。

操作步骤

- 用户视图下，执行如下命令清除DHCP Snooping绑定表：
  - **reset dhcp snooping user-bind** [**vlan** *vlan-id* | **interface** *interface-type interface-number*] * [**ipv4** | **ipv6**]
  - **reset dhcp snooping user-bind** [**ip-address** [*ip-address*] | **ipv6-address** [*ipv6-address*]]
  - **reset dhcp snooping user-bind** [**ipv6-prefix** [*prefix*/*prefix-length*]]

----结束

9.11.3 备份 DHCP Snooping 绑定表

背景信息

如果没有备份绑定表，设备重启后DHCP Snooping绑定表将丢失，这将导致DHCP用户必须重新进行上线以生成DHCP Snooping绑定表项才能正常通信。在备份DHCP Snooping绑定表后，设备重启后恢复DHCP Snooping绑定表，即可避免上述问题。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 使能DHCP Snooping绑定表的自动备份功能，可分为本地备份和远端FTP、HTTP、HTTPS、SFTP和TFTP服务器备份。

- 执行命令**dhcp snooping user-bind autosave** *file-name* [**write-delay** *delay-time*]，使能DHCP Snooping绑定表的本地自动备份功能。

  缺省情况下，未使能DHCP Snooping绑定表的本地自动备份功能。
- 执行命令**dhcp snooping user-bind ftp remotefilename** *filename* **host-ip** *ip-address* **username** *username* **password** *password* [**write-delay** *delay-time*]，使能DHCP Snooping绑定表在远端FTP服务器上的自动备份功能。

  缺省情况下，未使能DHCP Snooping绑定表在远端FTP服务器上的自动备份功能。
- 执行命令**dhcp snooping user-bind sftp remotefilename** *filename* **host-ip** *ip-address* **username** *username* **password** *password* [**write-delay** *delay-time*]，使能DHCP Snooping绑定表在远端SFTP服务器上的自动备份功能。

  缺省情况下，未使能DHCP Snooping绑定表在远端SFTP服务器上的自动备份功能。
- 执行命令**dhcp snooping user-bind tftp remotefilename** *filename* **host-ip** *ip-address* [**write-delay** *delay-time*]，使能DHCP Snooping绑定表在远端TFTP服务器上的自动备份功能。

  缺省情况下，未使能DHCP Snooping绑定表在远端TFTP服务器上的自动备份功能。
- 执行命令**dhcp snooping user-bind http** { **remotefilename** *filename* **host-ip** *ip-address* [**port** *port-number*] | **url** *url-string* } [**username** *username* **password** *password*] [**write-delay** *delay-time*]，使能DHCP Snooping绑定表在远端HTTP服务器上的自动备份功能。

  缺省情况下，未使能DHCP Snooping绑定表在远端HTTP服务器上的自动备份功能。

- 执行命令**dhcp snooping user-bind https ssl-policy** *ssl-policy-name* { **remotefilename** *filename* **host-ip** *ip-address* [**port** *port-number*] | **url** *url-string* } [**username** *username* **password** *password*] [**write-delay** *delay-time*]，使能DHCP Snooping绑定表在远端HTTPS服务器上的自动备份功能。

  缺省情况下，未使能DHCP Snooping绑定表在远端HTTPS服务器上的自动备份功能。

说明

设备不支持多种DHCP Snooping绑定表的自动备份方式同时生效，即以上方式只能选择一种。

使用FTP、HTTP和TFTP协议存在安全风险，建议采用SFTP或HTTPS方式进行文件操作。

步骤3 （可选）执行命令**dhcp snooping user-bind upload format ascii**，使能DHCP Snooping绑定表在远端服务器上的自动备份功能时，备份DHCP Snooping绑定表同时有ASCII格式和二进制格式。

缺省情况下，使能DHCP Snooping绑定表在远端服务器上的自动备份功能时，备份DHCP Snooping绑定表仅有二进制格式。

----结束

9.11.4 恢复 DHCP Snooping 绑定表

背景信息

在远端FTP、HTTP、HTTPS、TFTP或者SFTP服务器上备份DHCP Snooping绑定表后，即可对备份的绑定表项进行恢复。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 从远端FTP、HTTP、HTTPS、TFTP或者SFTP服务器上获取并恢复DHCP Snooping绑定表。

- 执行命令**dhcp snooping user-bind ftp load remotefilename** *filename* **host-ip** *ip-address* **username** *username* **password** *password*，配置从远端FTP服务器上获取并恢复已备份的DHCP Snooping绑定表项。
- 执行命令**dhcp snooping user-bind sftp load remotefilename** *filename* **host-ip** *ip-address* **username** *username* **password** *password*，配置从远端SFTP服务器上获取并恢复已备份的DHCP Snooping绑定表项。
- 执行命令**dhcp snooping user-bind tftp load remotefilename** *filename* **host-ip** *ip-address*，配置从远端TFTP服务器上获取并恢复已备份的DHCP Snooping绑定表项。
- 执行命令**dhcp snooping user-bind http load** { **remotefilename** *filename* **host-ip** *ip-address* [**port** *port-number*] | **url** *url-string* } [**username** *username* **password** *password*]，配置从远端HTTP服务器上获取并恢复已备份的DHCP Snooping绑定表项。
- 执行命令**dhcp snooping user-bind https ssl-policy** *ssl-policy-name* **load** { **remotefilename** *filename* **host-ip** *ip-address* [**port** *port-number*] | **url** *url-string* } [**username** *username* **password** *password*]，配置从远端HTTPS服务器上获取并恢复已备份的DHCP Snooping绑定表项。

说明

使用FTP、HTTP和TFTP协议存在安全风险，建议采用SFTP或HTTPS方式进行文件操作。

----结束

9.12 DHCP Snooping 配置举例

9.12.1 配置 DHCP Snooping 的攻击防范功能示例

组网需求

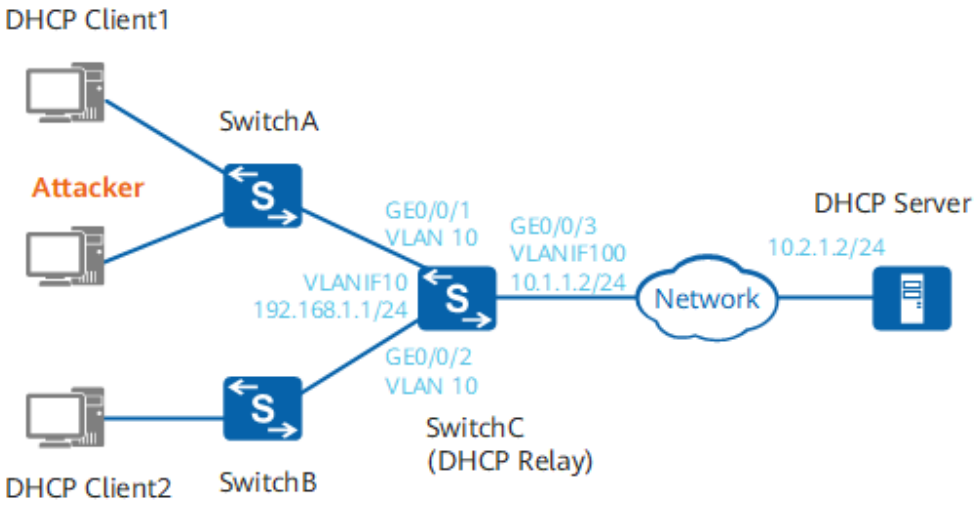
如图9-13所示，SwitchA与SwitchB是二层交换机，SwitchC是用户网关，作为DHCP Relay向DHCP服务器转发DHCP报文，使得DHCP客户端可以从DHCP服务器上申请到IP地址等相关配置信息。

然而网络中可能会存在针对DHCP的攻击，例如：

- DHCP Server仿冒者攻击：在网络上随意添加一台DHCP服务器，它可以为客户端分配IP地址以及其他网络参数。如果该DHCP服务器为用户分配错误的IP地址和其他网络参数，将会对网络造成非常大的危害。
- DHCP报文泛洪攻击：若攻击者短时间内向设备发送大量的DHCP报文，将会对设备的性能造成巨大的冲击以致可能会导致设备无法正常工作。
- 仿冒DHCP报文攻击：如果攻击者冒充合法用户不断向DHCP Server发送DHCP Request报文来续租IP地址，会导致这些到期的IP地址无法正常回收，以致一些合法用户不能获得IP地址；而若攻击者仿冒合法用户的DHCP Release报文发往DHCP Server，将会导致用户异常下线。
- DHCP Server服务拒绝攻击：当存在大量攻击者恶意申请IP地址或者某一攻击者通过不断改变CHADDR字段向DHCP Server申请IP地址，会导致DHCP Server中IP地址快速耗尽而不能为其他合法用户提供IP地址分配服务。

为了为DHCP用户提供更优质的服务，网络管理员可以通过配置DHCP Snooping功能，实现DHCP攻击防范。

图 9-13 配置 DHCP Snooping 的攻击防范功能组网图



配置思路

通过在DHCP Relay配置DHCP Snooping进行攻击防范：

1. 配置DHCP功能，实现SwitchC转发不同网段的DHCP报文给DHCP服务器。
2. 配置DHCP Snooping的基本功能，防止DHCP Server仿冒者攻击。同时可以使能ARP与DHCP Snooping的联动功能，保证DHCP用户在异常下线时实时更新绑定表。还可以配置丢弃GIADDR字段非零的DHCP报文，防止非法用户攻击。
3. 配置DHCP报文上送DHCP报文处理单元的最大允许速率，防止DHCP报文泛洪攻击。同时可以使能丢弃报文告警功能，当丢弃的DHCP报文数达到告警阈值时产生告警信息。
4. 使能对DHCP报文进行绑定表匹配检查的功能，防止仿冒DHCP报文攻击。同时可以使能与绑定表不匹配而被丢弃的DHCP报文数达到阈值时产生告警信息功能。
5. 配置允许接入的最大用户数以及使能检测DHCP Request报文帧头MAC与DHCP数据区中CHADDR字段是否一致功能，防止DHCP Server服务拒绝攻击。同时可以使能数据帧头MAC地址与DHCP报文中的CHADDR字段不一致被丢弃的报文达到阈值时产生告警信息功能。

本例仅涉及交换机SwitchC的配置。关于DHCP服务器的配置，本例中不予以详细介绍，只给出需要的步骤描述。

操作步骤

步骤1 配置DHCP功能。

在DHCP Relay设备上配置DHCP功能。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchC
[SwitchC] dhcp server group dhcpgroup1
[SwitchC-dhcp-server-group-dhcpgroup1] dhcp-server 10.2.1.2
[SwitchC-dhcp-server-group-dhcpgroup1] quit
[SwitchC] vlan batch 10 100
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] port link-type access
[SwitchC-GigabitEthernet0/0/1] port default vlan 10
[SwitchC-GigabitEthernet0/0/1] quit
[SwitchC] interface gigabitethernet 0/0/2
[SwitchC-GigabitEthernet0/0/2] port link-type access
[SwitchC-GigabitEthernet0/0/2] port default vlan 10
[SwitchC-GigabitEthernet0/0/2] quit
[SwitchC] interface gigabitethernet 0/0/3
[SwitchC-GigabitEthernet0/0/3] port link-type access
[SwitchC-GigabitEthernet0/0/3] port default vlan 100
[SwitchC-GigabitEthernet0/0/3] quit
[SwitchC] dhcp enable
[SwitchC] interface vlanif 10
[SwitchC-Vlanif10] ip address 192.168.1.1 255.255.255.0
[SwitchC-Vlanif10] dhcp select relay
[SwitchC-Vlanif10] dhcp relay server-select dhcpgroup1
[SwitchC-Vlanif10] quit
[SwitchC] interface vlanif 100
[SwitchC-Vlanif100] ip address 10.1.1.2 255.255.255.0
[SwitchC-Vlanif100] quit
[SwitchC] ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
```

DHCP服务器IP地址配置为10.2.1.2/24，同时配置一个IP地址范围为192.168.1.0/24的地址池，地址池中网关配置为192.168.1.1。

步骤2 使能DHCP Snooping基本功能。

使能全局DHCP Snooping功能并配置设备仅处理DHCPv4报文。

```
[SwitchC] dhcp snooping enable ipv4
```

使能用户侧接口的DHCP Snooping功能。以GE0/0/1接口为例，GE0/0/2的配置与GE0/0/1接口相同，不再赘述。

```
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] dhcp snooping enable
[SwitchC-GigabitEthernet0/0/1] quit
```

使能ARP与DHCP Snooping的联动功能。

```
[SwitchC] arp dhcp-snooping-detect enable
```

使能检测DHCP Request报文中GIADDR字段是否非零的功能。以GE0/0/1接口为例，GE0/0/2的配置与GE0/0/1接口相同，不再赘述。

```
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] dhcp snooping check dhcp-giaddr enable
[SwitchC-GigabitEthernet0/0/1] quit
```

步骤3 配置DHCP报文上送DHCP报文处理单元的最大允许速率并使能丢弃报文告警功能。

配置DHCP报文上送DHCP报文处理单元的最大允许速率为90pps。

```
[SwitchC] dhcp snooping check dhcp-rate enable
[SwitchC] dhcp snooping check dhcp-rate 90
```

使能丢弃报文告警功能，并配置报文限速告警阈值。

```
[SwitchC] dhcp snooping alarm dhcp-rate enable
[SwitchC] dhcp snooping alarm dhcp-rate threshold 500
```

步骤4 使能对DHCP报文进行绑定表匹配检查的功能并使能与绑定表不匹配而被丢弃的DHCP报文数达到阈值时产生告警信息功能。

在用户侧接口进行配置。以GE0/0/1接口为例，GE0/0/2的配置与GE0/0/1接口相同，不再赘述。

```
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] dhcp snooping check dhcp-request enable
[SwitchC-GigabitEthernet0/0/1] dhcp snooping alarm dhcp-request enable
[SwitchC-GigabitEthernet0/0/1] dhcp snooping alarm dhcp-request threshold 120
[SwitchC-GigabitEthernet0/0/1] quit
```

步骤5 配置接口允许接入的最大用户数并使能对CHADDR字段检查功能，同时使能数据帧头MAC地址与DHCP报文中的CHADDR字段不一致被丢弃的报文达到阈值时产生告警信息功能。

在用户侧接口进行配置。以GE0/0/1接口为例，GE0/0/2的配置与GE0/0/1接口相同，不再赘述。

```
[SwitchC] interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1] dhcp snooping max-user-number 20
[SwitchC-GigabitEthernet0/0/1] dhcp snooping check dhcp-chaddr enable
[SwitchC-GigabitEthernet0/0/1] dhcp snooping alarm dhcp-chaddr enable
[SwitchC-GigabitEthernet0/0/1] dhcp snooping alarm dhcp-chaddr threshold 120
[SwitchC-GigabitEthernet0/0/1] quit
```

步骤6 验证配置结果

执行命令**display dhcp snooping configuration**，查看DHCP Snooping的配置信息。


```
[SwitchC] display dhcp snooping configuration
#
dhcp snooping enable ipv4
dhcp snooping check dhcp-rate enable
dhcp snooping check dhcp-rate 90
dhcp snooping alarm dhcp-rate enable
dhcp snooping alarm dhcp-rate threshold 500
arp dhcp-snooping-detect enable
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check dhcp-request enable
 dhcp snooping alarm dhcp-request enable
 dhcp snooping alarm dhcp-request threshold 120
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr threshold 120
 dhcp snooping max-user-number 20
#
interface GigabitEthernet0/0/2
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check dhcp-request enable
 dhcp snooping alarm dhcp-request enable
 dhcp snooping alarm dhcp-request threshold 120
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr threshold 120
 dhcp snooping max-user-number 20
#
```

执行命令**display dhcp snooping interface**，查看接口下的DHCP Snooping运行信息。可以看到**Check dhcp-giaddr**、**Check dhcp-chaddr**和**Check dhcp-request**字段都为**Enable**。以接口GE0/0/1的回显为例：

```
[SwitchC] display dhcp snooping interface gigabitethernet 0/0/1
 DHCP snooping running information for interface GigabitEthernet0/0/1 :
 DHCP snooping                          : Enable
 Trusted interface                      : No
 Dhcp user max number                   : 20
 Current dhcp and nd user number        : 0
 Check dhcp-giaddr                      : Enable
 Check dhcp-chaddr                      : Enable
 Alarm dhcp-chaddr                      : Enable
 Alarm dhcp-chaddr threshold            : 120
 Discarded dhcp packets for check chaddr  : 0
 Check dhcp-request                     : Enable
 Alarm dhcp-request                     : Enable
 Alarm dhcp-request threshold           : 120
 Discarded dhcp packets for check request : 0
 Check dhcp-rate                        : Disable  (default)
 Alarm dhcp-rate                        : Disable  (default)
 Alarm dhcp-rate threshold              : 500
 Discarded dhcp packets for rate limit    : 0
 Alarm dhcp-reply                       : Disable  (default)
 Check dhcpv6-rate                      : Disable  (default)
 Alarm dhcpv6-rate                      : Disable  (default)
 Discarded dhcpv6 packets for rate limit  : 0
 Alarm dhcpv6-request                   : Disable  (default)
 DHCPv6 snooping check relay-forward    : Disable  (default)
```

----结束

配置文件

SwitchC的配置文件

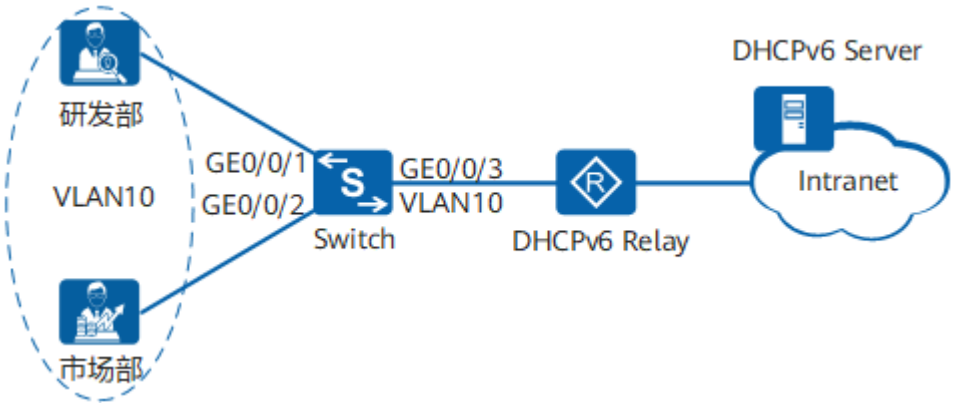
```
#
sysname SwitchC
#
vlan batch 10 100
#
dhcp enable
#
dhcp snooping enable ipv4
dhcp snooping check dhcp-rate enable
dhcp snooping check dhcp-rate 90
dhcp snooping alarm dhcp-rate enable
dhcp snooping alarm dhcp-rate threshold 500
arp dhcp-snooping-detect enable
#
dhcp server group dhcpgroup1
 dhcp-server 10.2.1.2 0
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select dhcpgroup1
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check dhcp-request enable
 dhcp snooping alarm dhcp-request enable
 dhcp snooping alarm dhcp-request threshold 120
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr threshold 120
 dhcp snooping max-user-number 20
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 10
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check dhcp-request enable
 dhcp snooping alarm dhcp-request enable
 dhcp snooping alarm dhcp-request threshold 120
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr threshold 120
 dhcp snooping max-user-number 20
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 100
#
ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
#
return
```

9.12.2 配置通过 LDRA 功能感知用户位置示例

组网需求

如图9-14所示，某公司研发部与市场部通过Switch接入网络并通过DHCPv6方式获取IPv6地址。由于研发部与市场部工作性质不同，所以该公司希望DHCPv6服务器能够判别出研发与市场部不同的客户端，进而为这两个部门部署不同的地址分配、接入控制、QOS等策略。

图 9-14 配置 LDRA 功能组网图



配置思路

采用如下的思路在Switch上进行配置。

1. 使能DHCP Snooping功能，为使能LDRA功能做准备。
2. 使能LDRA功能。通过在靠近用户的接入设备Switch上部署LDRA功能，能够将用户详细的位置信息上送至DHCPv6 Server，满足DHCPv6 Server根据用户详细位置信息为用户部署各种策略的需求。

操作步骤

步骤1 创建VLAN并配置各接口

在Switch上创建VLAN10。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 10
```

将接口GE0/0/1、GE0/0/2、GE0/0/3加入到VLAN10中。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type access
[Switch-GigabitEthernet0/0/1] port default vlan 10
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] port link-type access
[Switch-GigabitEthernet0/0/2] port default vlan 10
[Switch-GigabitEthernet0/0/2] quit
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] port link-type trunk
[Switch-GigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Switch-GigabitEthernet0/0/3] quit
```

步骤2 使能DHCP Snooping功能

使能全局DHCP Snooping功能。

```
[Switch] dhcp enable
[Switch] dhcp snooping enable
```

使能用户侧接口的DHCP Snooping功能。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] dhcp snooping enable
```



```
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] dhcp snooping enable
[Switch-GigabitEthernet0/0/2] quit
```

配置接口的信任状态，将连接DHCPv6 Server的接口状态配置为“Trusted”。

```
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] dhcp snooping trusted
[Switch-GigabitEthernet0/0/3] quit
```

步骤3 使能LDRA功能

在VLAN10下使能LDRA功能。

```
[Switch] vlan 10
[Switch-vlan10] dhcpv6 snooping relay-information enable
```

在VLAN10下配置在使能DHCP Snooping功能后，接口不生成用户绑定表，以使设备不会对上线用户数目进行限制。

```
[Switch-vlan10] dhcp snooping enable no-user-binding
Warning: To execute no-user-binding will delete all dynamic binding table with the same vlan. Continue? [Y/N]y
[Switch-vlan10] quit
```

步骤4 验证配置结果

执行命令**display dhcp snooping configuration**查看LDRA的相关配置信息。

```
[Switch] display dhcp snooping configuration
#
dhcp snooping enable
#
vlan 10
 dhcp snooping enable no-user-binding
 dhcpv6 snooping relay-information enable
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
#
interface GigabitEthernet0/0/2
 dhcp snooping enable
#
interface GigabitEthernet0/0/3
 dhcp snooping trusted
#
```

----结束

配置文件

Switch的配置文件

```
#
sysname Switch
#
vlan batch 10
#
dhcp enable
#
dhcp snooping enable
#
vlan 10
 dhcp snooping enable no-user-binding
 dhcpv6 snooping relay-information enable
#
interface GigabitEthernet0/0/1
```

```
 port link-type access
 port default vlan 10
 dhcp snooping enable
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 10
 dhcp snooping enable
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
 dhcp snooping trusted
#
return
```

9.12.3 基本 QinQ 场景下配置 DHCP Snooping 功能示例

组网需求

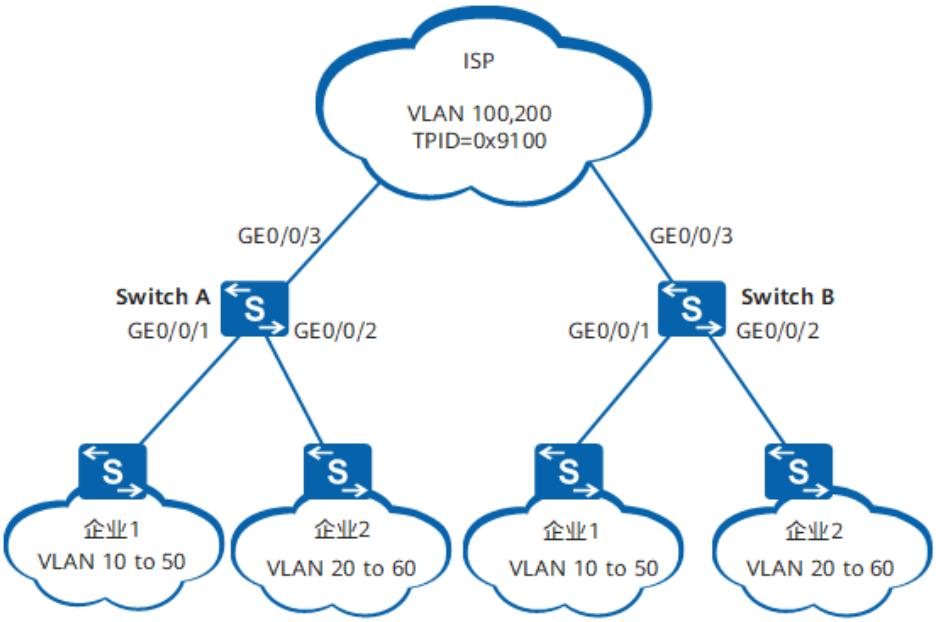
如图9-15所示，网络中有两个企业通过DHCP方式获取IPv4地址，企业1有两个分支，企业2有两个分支。这两个企业的各办公地的企业网都分别和运营商网络中的SwitchA和SwitchB相连，且公网中存在其它厂商设备，其外层VLAN Tag的TPID值为0x9100。

现需要实现：

- 企业1和企业2独立划分VLAN，两者互不影响。
- 各企业两分支之间流量通过公网透明传输，相同业务之间互通，不同业务之间互相隔离。
- 防止网络中针对DHCP的攻击，为DHCP用户提供更优质的服务。

可通过配置QinQ与DHCP Snooping功能来实现以上需求。利用公网提供的VLAN100使企业1互通，利用公网提供的VLAN200使企业2互通，不同企业之间互相隔离。并通过在连接其它厂商设备的接口上配置修改QinQ外层VLAN Tag的TPID值，来实现与其它厂商设备的互通。在DHCP Relay上配置DHCP Snooping功能，实现DHCP攻击防范。

图 9-15 配置基本 QinQ 示例组网图



配置思路

采用如下的思路在SwitchA和SwitchB上进行配置。

1. 在SwitchA和SwitchB上均创建VLAN100和VLAN200，配置连接业务的接口为QinQ类型，并分别加入VLAN。实现不同业务添加不同的外层VLAN Tag。
2. 配置SwitchA和SwitchB上连接公网的接口加入相应VLAN，实现允许VLAN100和200的报文通过。
3. 在SwitchA和SwitchB连接公网的接口上配置外层VLAN tag的TPID值，实现与其它厂商设备的互通。
4. 在SwitchA和SwitchB上配置DHCP Snooping功能，实现DHCP攻击防范。

说明

DHCP Snooping最多支持处理带有双层VLAN Tag的DHCP报文。对于带有更多层VLAN Tag的报文建议不要配置DHCP Snooping功能，否则会导致丢包，影响用户的使用体验。

操作步骤

步骤1 创建VLAN

在SwitchA上创建VLAN100和VLAN200。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 100 200
```

在SwitchB上创建VLAN100和VLAN200。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchB
[SwitchB] vlan batch 100 200
```

步骤2 配置接口类型为QinQ

在SwitchA上配置接口GE0/0/1、GE0/0/2的类型为QinQ，GE0/0/1的外层tag为VLAN100，GE0/0/2的外层tag为VLAN200。SwitchB的配置与SwitchA类似，不再赘述。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type dot1q-tunnel
[SwitchA-GigabitEthernet0/0/1] port default vlan 100
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type dot1q-tunnel
[SwitchA-GigabitEthernet0/0/2] port default vlan 200
[SwitchA-GigabitEthernet0/0/2] quit
```

步骤3 配置Switch连接公网侧的接口

在SwitchA上配置接口GE0/0/3加入VLAN100和VLAN200。SwitchB的配置与SwitchA类似，不再赘述。

```
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 100 200
[SwitchA-GigabitEthernet0/0/3] quit
```

步骤4 配置外层VLAN tag的TPID值

在SwitchA上配置外层VLAN tag的TPID值为0x9100。


```
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] qinq protocol 9100
```

在SwitchB上配置外层VLAN tag的TPID值为0x9100。

```
[SwitchB] interface gigabitethernet 0/0/3
[SwitchB-GigabitEthernet0/0/3] qinq protocol 9100
```

步骤5 配置DHCP Snooping功能

在SwitchA上使能全局DHCP Snooping功能并配置设备仅处理DHCPv4报文。SwitchB的配置与SwitchA类似，不再赘述。

```
[SwitchA] dhcp enable
[SwitchA] dhcp snooping enable ipv4
```

步骤6 使能接口下的DHCP Snooping功能

在SwitchA上使能用户侧接口的DHCP Snooping功能。SwitchB的配置与SwitchA类似，不再赘述。

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] dhcp snooping enable
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] dhcp snooping enable
[SwitchA-GigabitEthernet0/0/2] quit
```

步骤7 配置接口的信任状态

将连接DHCP Server的接口状态配置为“Trusted”。SwitchB的配置与SwitchA类似，不再赘述。

```
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] dhcp snooping trust
[SwitchA-GigabitEthernet0/0/3] quit
```

步骤8 验证配置结果

在SwitchA上执行命令**display dhcp snooping configuration**查看DHCP Snooping的配置信息。SwitchB的配置与SwitchA类似，不再赘述。

```
[SwitchA] display dhcp snooping configuration
#
dhcp snooping enable ipv4
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
#
interface GigabitEthernet0/0/2
 dhcp snooping enable
#
interface GigabitEthernet0/0/3
 dhcp snooping trusted
#
```

在SwitchA上执行命令**display dhcp snooping user-bind all**查看用户的DHCP Snooping绑定表信息。SwitchB的配置与SwitchA类似，不再赘述。

```
DHCP Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address      MAC Address     VSI/VLAN(O/I/P)/ Interface        Lease
-------------------------------------------------------------------------------------------------
10.1.1.141      xxxx-xxxx-xxx1  100 /50  /--           GE0/0/1      2021.12.27-07:31
10.1.1.137      xxxx-xxxx-xxx2  200 /50  /--           GE0/0/2      2021.11.27-07:31
-------------------------------------------------------------------------------------------------
Print count:          2         Total count:          2
```


从企业1一处分支内任意VLAN的一台PC ping企业1另外一处分支同一VLAN内的PC，如果可以ping通则表示企业1内部可以互相通信。

从企业2一处分支内任意VLAN的一台PC ping企业2另外一处分支同一VLAN内的PC，如果可以ping通则表示企业2内部可以互相通信。

从企业1一处分支内任意VLAN的一台PC ping企业2任意一处分支同一VLAN内的PC，如果不能ping通则表示企业1和企业2之间相互隔离。

----结束

配置文件

- SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 100 200
#
dhcp enable
#
dhcp snooping enable
#
interface GigabitEthernet0/0/1
 port link-type dot1q-tunnel
 port default vlan 100
 dhcp snooping enable
#
interface GigabitEthernet0/0/2
 port link-type dot1q-tunnel
 port default vlan 200
 dhcp snooping enable
#
interface GigabitEthernet0/0/3
 qinq protocol 9100
 port link-type trunk
 port trunk allow-pass vlan 100 200
 dhcp snooping trusted
#
```

- SwitchB的配置文件

```
#
sysname SwitchA
#
vlan batch 100 200
#
dhcp enable
#
dhcp snooping enable
#
interface GigabitEthernet0/0/1
 port link-type dot1q-tunnel
 port default vlan 100
 dhcp snooping enable
#
interface GigabitEthernet0/0/2
 port link-type dot1q-tunnel
 port default vlan 200
 dhcp snooping enable
#
interface GigabitEthernet0/0/3
 qinq protocol 9100
 port link-type trunk
 port trunk allow-pass vlan 100 200
 dhcp snooping trusted
#
```


9.13 DHCP Snooping 常见配置错误

9.13.1 开启 DHCP Snooping 功能后部分用户无法正常获取 IP 地址

故障现象

开启DHCP Snooping功能后部分用户无法正常获取IP地址可能由以下原因造成：

- 用户侧接口下DHCP用户数达到配置的最大值
- DHCP报文过多，超过限速，导致新用户的DHCP报文被丢弃

操作步骤

步骤1 查看DHCP上线用户数是否达到配置的最大值。

1. 执行命令**display dhcp snooping** [**interface** *interface-type interface-number* | **vlan** *vlan-id*]，查看全局、VLAN、以及用户侧接口下是否有“Dhcp user max number: XX”信息。

   缺省情况下，接口允许学习的DHCP Snooping绑定表项的最大个数为512。

2. 执行命令**display dhcp snooping user-bind all**，查看当前设备使能DHCP Snooping功能的接口上一共生成多少DHCP用户动态绑定表项。如果表项数已经达到配置的限制值，后续用户无法接入是正常现象。

   如果需要增加DHCP上线用户数的限制值，可以执行命令**dhcp snooping max-user-number** *max-number*进行修改。

步骤2 如果DHCP上线用户数未达到配置的限制值，则查看是否DHCP报文过多，超过限速值而被丢弃。

1. 执行命令**display dhcp snooping** [**interface** *interface-type interface-number* | **vlan** *vlan-id*]，查看全局、VLAN、以及用户侧接口下是否有“Dhcp-rate limit(pps): xx”信息。

   若没有“Dhcp-rate limit(pps): xx”信息，则限速值取默认值100pps。若配置了该信息则以配置值为准。

2. 如果DHCP报文的限速值较小，可在系统视图、接口视图、VLAN视图下执行命令**dhcp snooping check dhcp-rate** *rate*，适当增大限速值。

----结束

9.13.2 开启 DHCP Snooping 功能后所有用户无法正常获取 IP 地址

故障现象

DHCP Snooping导致用户无法上线可能由以下原因造成：

- 连接DHCP Server的接口未配置为“信任”状态
- 全局使能DHCP Snooping功能后，连接用户的接口或其所属VLAN没有使能DHCP Snooping功能

操作步骤

步骤1 查看连接DHCP Server的接口状态是否配置错误。

1. 执行命令**display dhcp snooping configuration**和**display dhcp snooping** [**interface** *interface-type interface-number* | **vlan** *vlan-id*]，查看在哪些VLAN下、哪些接口下使能了DHCP Snooping功能并查看**连接DHCP Server的接口**下是否有“Trusted interface: Yes”信息。

   “Trusted”是接口信任状态的标识，接口默认为“非信任”状态。对网络侧报文，设备只处理信任接口收到的DHCP Reply报文，非信任接口收到DHCP Reply报文会丢弃；对用户侧报文，设备收到用户的请求报文时，只会向信任接口转发。

2. 连接DHCP Server的接口应该配置为“Trusted”。如果该接口不是信任接口，可在VLAN视图或接口视图下执行命令**dhcp snooping trusted**，配置接口为信任状态。

   在DHCP中继使能DHCP Snooping场景中，DHCP Relay设备不需要设置信任接口。因为DHCP Relay收到DHCP请求报文后进行源目的IP、MAC转换处理，然后以单播形式发送给指定的合法DHCP服务器，所以DHCP Relay收到的DHCP ACK报文都是合法的，生成的DHCP Snooping绑定表也是正确的。

步骤2 如果接口信任状态配置正确，则检查连接用户的接口或其所属VLAN是否使能了DHCP Snooping功能。

1. 执行命令**display dhcp snooping configuration**和**display dhcp snooping** [**interface** *interface-type interface-number* | **vlan** *vlan-id*]，查看连接用户的接口或其所属VLAN是否使能了DHCP Snooping功能。
2. 连接用户的接口或其所属VLAN应该使能DHCP Snooping功能。如果没有使能，可在VLAN视图或接口视图下执行命令**dhcp snooping enable**，使能接口或VLAN下的DHCP Snooping功能。

----结束

9.14 DHCP Snooping FAQ

9.14.1 为什么配置了 DHCP Snooping 之后，设备下挂用户无法获取 IP 地址?

在使能DHCP Snooping之后，设备所有接口状态缺省都是非信任状态。这时要使用命令**dhcp snooping trusted**将与DHCP Server相连的接口配置成信任状态，否则DHCP Server回应的DHCP Reply报文都会被丢弃，导致设备下挂用户无法获取DHCP Server分配的IP地址。

9.14.2 为什么 PC 通过 DHCP 获取到 IP 地址之后不能访问 Internet?

通常情况下，PC通过DHCP获取到IP之后，可以正常访问Internet。但是当网络中存在DHCP Server仿冒者攻击时，会导致PC申请到的IP地址错误，不能访问Internet。建议用户发现此问题之后，在二层网络中的接入设备或第一个DHCP Relay上部署DHCP Snooping功能，保障PC获取到正确的IP地址。

- 对于二层接入设备来说，1、2和3都是必选步骤，请按照以下顺序配置。

- 对于DHCP中继设备来说，仅需配置步骤1和2。

1. 全局下的配置。

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
```

2. 连接DHCP客户端侧接口的配置。所有连接DHCP客户端的接口都需要配置，以接口GE0/0/1为例。

```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable
[HUAWEI-GigabitEthernet0/0/1] quit
```

3. 连接DHCP服务器侧接口的配置，以接口GE0/0/2为例。

```
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] dhcp snooping trusted
[HUAWEI-GigabitEthernet0/0/2] quit
```


10 ND Snooping 配置

10.1 ND Snooping 简介

定义

ND Snooping是针对IPv6 ND（Neighbor Discovery，邻居发现）的一种安全特性，用于二层交换网络环境。通过侦听用户重复地址检测DAD（Duplicate Address Detection）过程的邻居请求报文NS（Neighbor Solicitation）来建立ND Snooping动态绑定表，从而记录下报文的源IPv6地址、源MAC地址、所属VLAN、入端口等信息，以防止后续仿冒用户、仿冒网关的ND报文攻击。

关于ND协议的详细介绍，请参见《S600-E V200R021C00, C01 配置指南-IP业务》IPv6基础配置 中的“邻居发现”。

目的

ND协议是IPv6的一个关键协议，它功能强大，但是因为其没有任何安全机制，所以容易被攻击者利用。在网络中，常见的ND攻击有如下两种情况。

- 地址欺骗攻击：攻击者仿冒其他用户的IP地址发送邻居请求报文NS（Neighbor Solicitation）/邻居通告报文NA（Neighbor Advertisement）/路由器请求报文RS（Router Solicitation），会改写网关上或者其他用户的ND表项，导致被仿冒用户无法正常接收报文，从而无法正常通信。同时攻击者通过截获被仿冒用户的报文，可以非法获取用户的游戏、网银等帐号口令，会造成这些用户的重大利益损失。

- RA攻击：攻击者仿冒网关向其他用户发送路由器通告报文RA（Router Advertisement），会改写其他用户的ND表项或导致其它用户记录错误的IPv6配置参数，造成这些用户无法正常通信。

为了避免上述ND攻击带来的危害，设备提供了ND Snooping功能以对ND攻击进行防范。

受益

- 可以有效降低用户为保证网络正常运行和网络信息安全而产生的维护成本。
- 可以为用户提供更安全的网络环境和更稳定的网络服务。

10.2 ND Snooping 原理描述

ND Snooping是通过侦听**基于ICMPv6实现的ND报文**来建立**前缀管理表**和**ND Snooping动态绑定表**，使设备可以根据前缀管理表来管理接入用户的IPv6地址，并根据ND Snooping动态绑定表来过滤从**非信任接口**接收到的非法ND报文，从而可以防止ND攻击的一种安全技术。

基于 ICMPv6 实现的 ND 报文

ND协议定义的报文使用ICMP承载，其类型包括以下五种。

- 邻居请求报文NS（Neighbor Solicitation）：IPv6节点（使用IPv6协议的主机或网络设备）通过NS报文可以得到邻居的链路层地址，检查邻居是否可达，也可以进行重复地址检测DAD（Duplicate Address Detect）。
- 邻居通告报文NA（Neighbor Advertisement）：NA报文是IPv6节点对NS报文的响应，同时IPv6节点在链路层变化时也可以主动发送NA报文。
- 路由器请求报文RS（Router Solicitation）：IPv6节点启动后，向路由器发出RS报文，以请求网络前缀和其他配置信息，用于IPv6节点地址的自动配置。路由器则会以RA报文进行响应。
- 路由器通告报文RA（Router Advertisement）：路由器周期性的发布RA报文，其中包括网络前缀等网络配置的关键信息，或者路由器以RA报文响应RS报文。
- 重定向报文RR（Redirect）：路由器发现报文的入接口和出接口相同时，可以通过重定向报文通知主机选择另外一个更好的下一跳地址进行后续报文的发送。

ND Snooping 信任接口/非信任接口

为了区分可信任和不可信任的IPv6节点，ND Snooping将设备连接IPv6节点的接口区分为以下两种角色。

- ND Snooping信任接口：该类型接口用于连接可信任的IPv6节点，对于从该类型接口接收到的ND报文，设备正常转发，同时设备会根据接收到的RA报文建立前缀管理表。
- ND Snooping非信任接口：该类型接口用于连接不可信任的IPv6节点，对于从该类型接口接收到的RA报文，设备认为是非法报文直接丢弃；对于收到的NA/NS/RS报文，如果该接口或接口所在的VLAN使能了ND报文合法性检查功能，设备会根据ND Snooping动态绑定表对NA/NS/RS报文进行绑定表匹配检查，当报文不符合绑定表关系时，则认为该报文是非法用户报文直接丢弃；对于收到的其他类型ND报文，设备正常转发。

前缀管理表

通过无状态地址自动配置方式获取IPv6地址的用户，其IPv6地址是根据路由器发送的RA报文中的网络前缀等配置信息来自动生成的。配置ND Snooping功能后，设备通过侦听从ND Snooping信任接口接收到的RA报文，可以生成前缀管理表（表项内容包括前缀、前缀长度、前缀老化租期等信息）供管理员查看，以方便灵活管理这些用户的IPv6地址。

ND Snooping 动态绑定表

ND Snooping动态绑定表的表项内容包括报文的源IPv6地址、源MAC地址、所属VLAN和入接口等信息，可用于设备对从非信任接口接收到的NA/NS/RS报文进行绑定表匹配检查，从而可以过滤非法的NA/NS/RS报文。

ND Snooping动态绑定表的新建、更新机制

配置ND Snooping功能后，设备通过检查DAD NS报文来建立ND Snooping动态绑定表；通过检查NS（包括DAD NS报文和普通NS报文）/NA报文来更新ND Snooping动态绑定表。

ND Snooping动态绑定表的新建、更新机制如下：

第一种情况：设备收到DAD NS报文

首先根据报文中的Target Address查找是否有对应的前缀管理表表项。

说明

Target Address表示请求目标的IP地址。不能是组播地址，可以是本地链路、本地站点、全局地址。

如果没有，则直接丢弃该报文。

如果有，则继续根据Target Address查找是否有对应ND Snooping动态绑定表表项。

- 如果没有，则新建ND Snooping动态绑定表表项，并且转发该报文。
- 如果有，则判断DAD NS报文的MAC地址、入端口、VLAN信息与现有该表项的MAC地址、入端口、VLAN信息是否一致。
  - 一致，则更新对应表项中用户的地址租期；
  - MAC地址一致、其他信息不一致，则删除原有表项，重新建立表项，并且转发该报文。
  - MAC地址不一致，则表项不变，并且转发该报文。

第二种情况：设备收到普通NS报文

首先根据报文中的Source Address查找是否有对应的ND Snooping动态绑定表表项。

如果没有，则检查是否开启ND协议报文合法性检查功能，如果有，则丢弃该报文，如果没有则转发该报文。

如果有，则判断NS报文的MAC地址、入端口、VLAN信息与现有该表项的MAC地址、入端口、VLAN信息是否一致。

- 一致，则更新对应表项中用户的地址租期；
- 不一致，则检查是否开启ND协议报文合法性检查功能，如果有，则丢弃该报文，如果没有则转发该报文。

第三种情况：设备收到NA报文

首先判断收到NA报文的接口是否为以下任一接口：配置了命令**dhcp snooping disable**的接口、配置了命令**dhcp snooping trust**或**nd snooping trust**的接口、未配置命令**nd snooping check na enable**的接口。

如果是以上任一接口，则直接转发该NA报文。

如果不是以上列举的接口，则继续根据NA报文的源IP地址和目的IP地址判断是否有对应的ND Snooping动态绑定表表项。

- 如果没有，则直接丢弃该NA报文。
- 如果有，则判断NA报文的端口信息与现有表项的是否一致。
  - 一致，则更新对应绑定表表项中用户地址租期；
  - 不一致，说明该NA报文与现有表项冲突，此时会触发设备发送NS报文探测用户是否在线。如果在表项生存时间内，设备从表项对应的端口上收到NA报文，说明该用户仍然在线，更新对应表项中用户的地址租期。如果在表项生存时间内，设备没有从表项对应的端口上收到NA报文，说明该用户已经下线，更新对应表项中用户的地址租期并将表项的端口更新为新端口。

    说明

    设备收到与绑定表冲突的NA报文后，触发用户在线状态探测功能时，用户在线状态的定时探测功能暂停。

ND Snooping动态绑定表的删除老化机制

ND Snooping动态绑定表的删除老化机制如下：

ND Snooping动态绑定表项的自动老化时间是由ND用户的地址租期决定的。

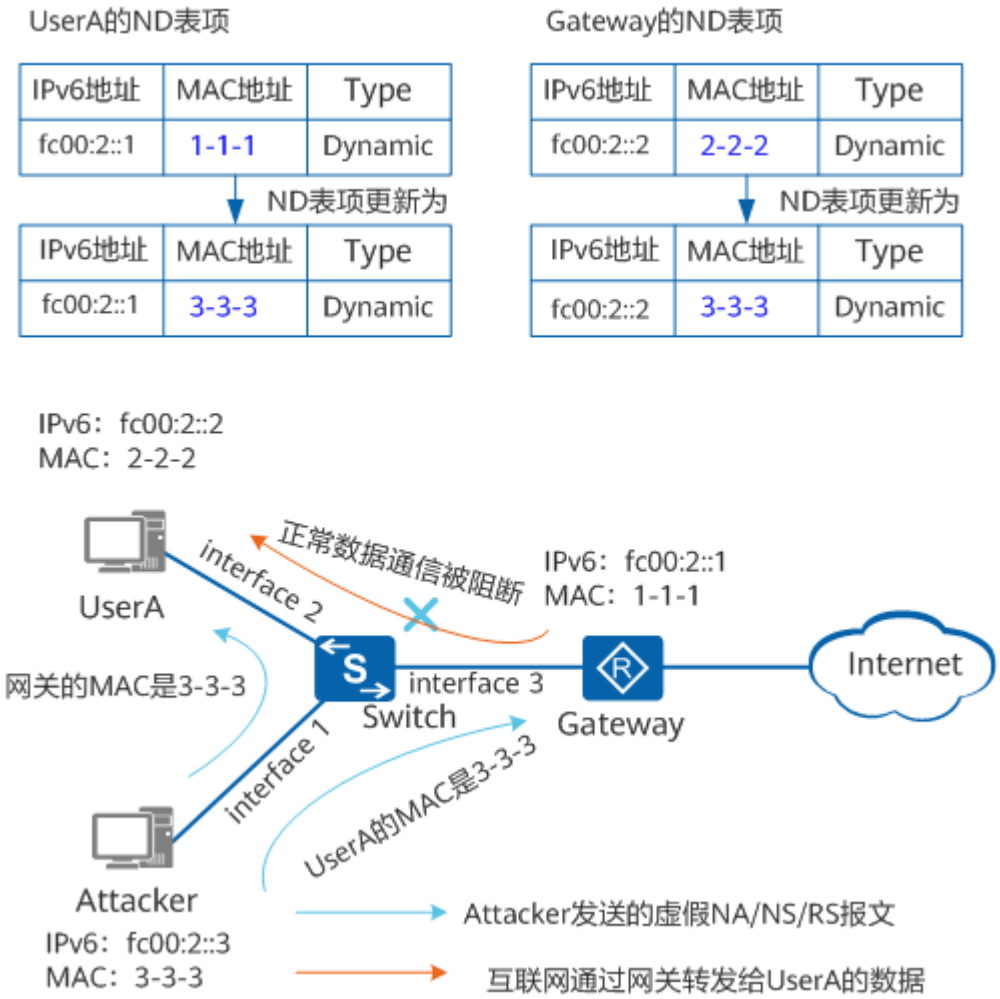
- 如果用户地址租期时间已到期，则ND Snooping动态绑定表项会自动老化。
- 在用户的地址租期未到期的情况下，存在以下两种删除ND Snooping动态绑定表项的情形：
  - 当设备收到用户的NS报文新建或更新ND Snooping动态绑定表项后，如果又收到了其他用户回应的通知该用户地址已被使用的NA报文，则设备会删除该ND Snooping动态绑定表项。
  - 当用户实际已经下线，该用户对应的ND Snooping动态绑定表项不会被及时删除。如果设备上使能了自动探测ND Snooping动态绑定表项对应用户的在线状态功能，则设备会根据配置的探测次数和探测时间间隔向对应用户发送NS探测报文。在发出探测次数的NS探测报文后，用户仍然没有回应NA报文，设备则认为该用户不在线，删除该用户对应的ND Snooping动态绑定表项。

10.3 ND Snooping 应用场景

10.3.1 防地址欺骗攻击

如图10-1所示，Attacker仿冒UserA向网关发送伪造的NA/NS/RS报文，导致网关的ND表项中记录了错误的UserA地址映射关系，Attacker可以轻易获取到网关原来要发往UserA的数据；同时Attacker又仿冒网关向UserA发送伪造的NA/NS/RS报文，导致UserA的ND表中记录了错误的网关地址映射关系，Attacker可以轻易获取到UserA原来要发往网关的数据。这样不仅会造成UserA无法接收到正常的数据报文，还会使UserA的信息安全无法得到保障。

图 10-1 防地址欺骗攻击



为了防止上述地址欺骗攻击，建议在接入设备Switch的**interface 1**和**interface 3**上部署ND Snooping功能，将Switch与网关相连的接口**interface 3**配置为信任接口，并在用户侧接口**interface 1**上使能ND协议报文合法性检查功能。对于从**interface 1**接收到的NA/NS/RS报文，Switch会根据生成的ND Snooping动态绑定表进行绑定表匹配检查，对于非法报文将直接丢弃，从而可以避免伪造的NA/NS/RS报文带来的危害。

10.3.2 防 RA 攻击

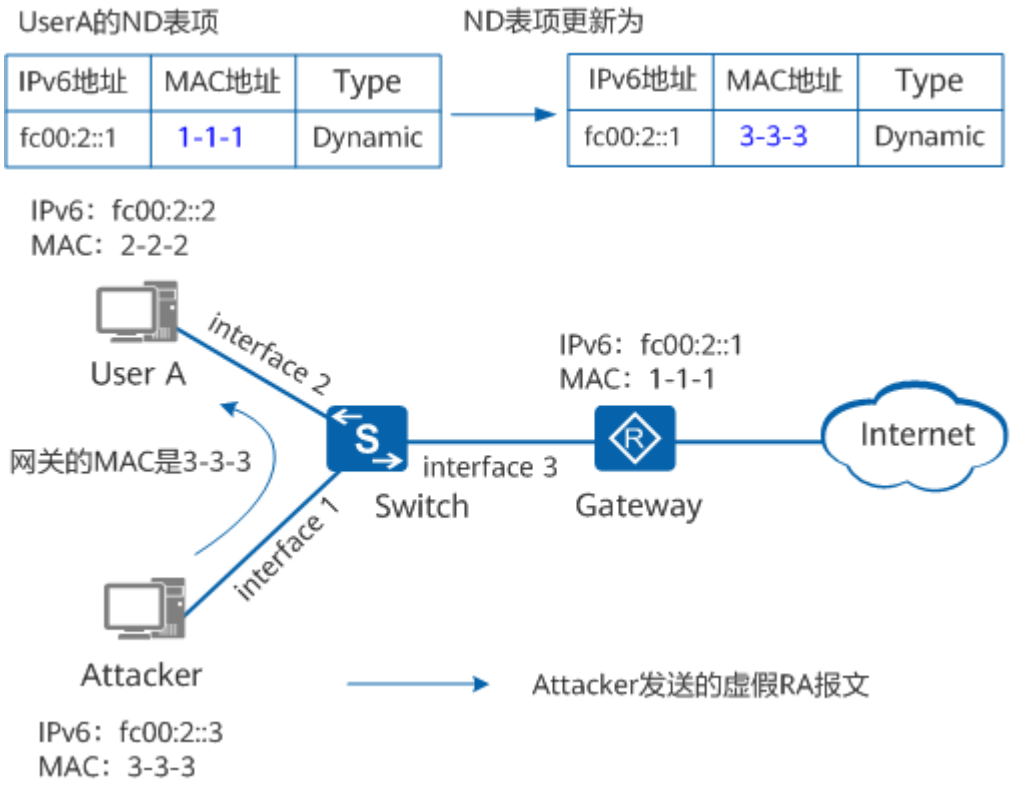
RA报文能够携带很多网络配置信息，包括默认路由器、网络前缀列表以及是否使用DHCPv6服务器进行有状态地址分配等网络配置的关键信息。如图10-2所示，攻击者通过发送伪造的RA报文，修改用户主机的网络配置，使合法用户无法进行正常通信。常见的RA报文攻击包括：

- 伪造不存在的前缀，修改合法用户主机的路由表。
- 伪造网关MAC地址，造成合法用户主机记录错误的网关地址映射关系；或者伪造RA报文中的Router Lifetime字段，造成合法用户主机的默认网关变为其他网关设备。
- 伪造DHCPv6服务器，同时伪造RA报文中的M标识位，造成合法用户主机使用DHCPv6服务器分配到的虚假地址。

Router Lifetime表示发送该RA报文的路由器使用该字段的值作为缺省路由器的生命周期。如果该字段为0，表示该路由器不能作为缺省路由器，但RA报文的其他信息仍然有效。

M表示管理地址配置标识（Managed address configuration），取值包括0和1。0表示无状态地址分配，客户端通过无状态协议（如ND）获得IPv6地址；1表示有状态地址分配，客户端通过有状态协议（如DHCPv6）获得IPv6地址。

图 10-2 防 RA 攻击



为了防止上述RA攻击，建议在接入设备Switch的**interface 1**和**interface 3**上部署ND Snooping功能，并将Switch与网关相连的接口**interface 3**配置为信任接口。这样Switch就会直接丢弃用户侧接口**interface 1**（默认为非信任接口）收到的RA报文，仅处理信任接口收到的RA报文，从而可以避免伪造的RA报文带来的各种危害。

说明

如果管理员希望更加精细的过滤RA报文，可以配置IPv6 RA Guard功能，具体配置请参见11 IPv6 RA Guard配置。

10.4 ND Snooping 配置注意事项

涉及网元

无需其他网元配合。

License 支持

本特性是交换机的基本特性，无需获得License许可即可应用此功能。

V200R021C00、V200R021C01 版本特性支持情况

S600-E系列交换机中所有款型均支持ND Snooping。

说明

如需了解交换机软件配套详细信息，请点击**Info-Finder**。

特性依赖和限制

- 设备支持同时配置ND snooping和对Untagged报文添加双层Tag的功能。
- ND Snooping绑定表是在收到用户DAD NS报文时生成的，用户终端添加单播IPv6地址时发送DAD NS报文进行IPv6地址冲突检测，添加地址成功后不会再次发送DAD NS报文。当用户终端重启网卡或者插拔网线时，与终端相连的设备端口默认延时UP并进行STP检测。在此期间，终端发送的DAD NS报文设备端口还不能转发，DAD NS报文会被设备丢弃，最终导致设备无法生成ND Snooping绑定表。为避免该问题，需要配置命令**carrier up-hold-time 0**关闭端口UP延时，配置命令**stp disable**关闭端口STP功能。

10.5 ND Snooping 缺省配置

ND Snooping的缺省配置如**表10-1**所示。

表 10-1 ND Snooping 缺省配置

参数	缺省值
ND Snooping功能	未使能。
ND Snooping信任接口	所有接口为非信任接口。
ND协议报文合法性检查功能	未使能。
自动探测ND Snooping动态绑定表项对应用户在线状态功能	未使能。
发送NS探测报文的探测次数和探测时间间隔	探测次数为2次，探测时间间隔为1000毫秒。
接口允许学习ND Snooping动态绑定表项的最大个数	在规格范围内，设备对接口能够学习到的最大ND Snooping动态绑定表项数目没有限制。
ND Snooping动态绑定表的告警阈值百分比	下限告警阈值百分比为50，上限告警阈值百分比为100。

10.6 配置 ND Snooping

前置任务

在配置ND Snooping之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为Up。

10.6.1 使能 ND Snooping 功能

背景信息

配置ND Snooping功能前必须先使能ND Snooping功能。

使能ND Snooping功能时，必须先全局使能ND Snooping功能，再在接口、VLAN下使能ND Snooping功能。

在接口视图下使能时，则对特定接口生效；在VLAN视图下使能时，则对加入该VLAN的所有接口生效。

如果配置了接口为**ND Snooping信任接口**，则该接口会自动使能ND Snooping功能，无需再在该接口、VLAN下使能ND Snooping功能。

操作步骤

- 在接口视图下使能
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**nd snooping enable**，全局使能ND Snooping功能。

     缺省情况下，全局未使能ND Snooping功能。
  c. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  d. 执行命令**nd snooping enable**，使能接口下的ND Snooping功能。

     缺省情况下，接口下未使能ND Snooping功能。
- 在接口视图下使能(DHCPv6 Only场景)
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**nd snooping enable**，全局使能ND Snooping功能。

     缺省情况下，全局未使能ND Snooping功能。
  c. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  d. 执行命令**nd snooping enable dhcpv6 only**，使能接口下的ND Snooping功能。

     缺省情况下，接口下未使能ND Snooping功能。
- 在VLAN视图下使能
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**nd snooping enable**，全局使能ND Snooping功能。

     缺省情况下，全局未使能ND Snooping功能。
  c. 执行命令**vlan** *vlan-id*，进入VLAN视图。
  d. 执行命令**nd snooping enable**，使能VLAN下的ND Snooping功能。

     缺省情况下，VLAN下未使能ND Snooping功能。
- 在VLAN视图下使能(DHCPv6 Only场景)
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**nd snooping enable**，全局使能ND Snooping功能。

     缺省情况下，全局未使能ND Snooping功能。

c. 执行命令**vlan** *vlan-id*，进入VLAN视图。

d. 执行命令**nd snooping enable dhcpv6 only**，使能VLAN下的ND Snooping功能。

缺省情况下，VLAN下未使能ND Snooping功能。

----结束

10.6.2 配置 ND Snooping 信任接口

背景信息

为了区分可信任和不可信任的IPv6节点，ND Snooping将设备连接IPv6节点的接口区分为信任接口和非信任接口两种角色。缺省情况下，设备的所有接口均为非信任接口。

- 对于可信任的IPv6节点，必须将连接此节点的接口配置为信任接口，使设备能够正常转发从该接口接收到的ND报文，同时能使设备根据接收到的RA报文建立前缀管理表，以方便管理员管理用户的IPv6地址。
- 对于不可信任的IPv6节点，连接此节点的接口必须为非信任接口。设备会直接丢弃从该接口接收到的RA报文，以防止攻击者发送伪造的RA报文进行RA攻击。

可在接口、VLAN视图下配置ND Snooping信任接口。在接口视图下配置时，对该接口收到的所有ND报文均生效；在VLAN视图下配置时，指定的接口必须属于此VLAN，此时仅对该接口收到的属于此VLAN的ND报文生效，故VLAN视图下的配置精度相对更高。

说明

一般将设备连接网关的接口配置成信任接口，其他接口均为非信任接口。

操作步骤

- 在接口视图下配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**nd snooping trusted**，配置接口为ND Snooping信任接口。

  缺省情况下，所有接口为非信任接口。
- 在接口视图下配置(DHCPv6 Only场景)
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**nd snooping trusted dhcpv6 only**，配置接口为ND Snooping信任接口。

  缺省情况下，所有接口为非信任接口。
- 在VLAN视图下配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**vlan** *vlan-id*，进入VLAN视图。
  c. 执行命令**nd snooping trusted interface** *interface-type interface-number*，配置加入该VLAN的接口为ND Snooping信任接口。

缺省情况下，所有接口为非信任接口。

- 在VLAN视图下配置(DHCPv6 Only场景)
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**vlan** *vlan-id*，进入VLAN视图。
  c. 执行命令**nd snooping trusted interface** *interface-type interface-number* **dhcpv6 only**，配置加入该VLAN的接口为ND Snooping信任接口。

     缺省情况下，所有接口为非信任接口。

----结束

10.6.3 配置 ND 协议报文合法性检查

背景信息

为了防止攻击者发送伪造的NA/NS/RS报文进行地址欺骗攻击，可以开启ND协议报文合法性检查功能。

开启该功能后，设备将根据ND Snooping动态绑定表、DHCPv6动态绑定表或者IPv6静态绑定表，对从非信任接口接收到的NA/NS/RS报文进行绑定表匹配检查，检查该用户是否是报文收到端口所属VLAN上的合法用户。对于合法用户的NA/NS/RS报文进行正常转发，否则直接丢弃。

配置注意事项

配置ND协议报文合法性检查功能后，建议在系统视图下，通过命令**savi enable**，使能SAVI功能，使链路本地地址（前缀地址为FE80::/10的IPv6地址）能够自动生成ND Snooping绑定表。这是由于IPv6主机在邻居发现过程中，NA/NS/RS报文的源IPv6地址可能是链路本地地址，如果链路本地地址没有生成对应的ND Snooping绑定表，合法的NA/NS/RS报文会被丢弃，导致IPv6主机之间无法通信。

操作步骤

步骤1 开启ND协议报文合法性检查功能

可在接口、VLAN视图下配置ND协议报文合法性检查。在接口视图下配置时，则对该非信任接口收到的所有NA/NS/RS报文生效；在VLAN视图下配置时，则对加入该VLAN的所有非信任接口收到的属于此VLAN的NA/NS/RS报文生效。

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**interface** *interface-type interface-number*，进入接口视图。

   或者，执行命令**vlan** *vlan-id*，进入VLAN视图。
3. 执行命令**nd snooping check** { **na** | **ns** | **rs** } **enable**，开启ND协议报文合法性检查功能。

   缺省情况下，未开启ND协议报文合法性检查功能。

步骤2 （可选）开启ND Snooping绑定表检查告警功能

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**interface** *interface-type interface-number*，进入接口视图。

   或者，执行命令**vlan** *vlan-id*，进入VLAN视图。

3. 执行命令**nd snooping alarm binding-table check enable**，开启ND Snooping绑定表检查告警功能。

   缺省情况下，未开启ND Snooping绑定表检查告警功能。

步骤3 （可选）配置告警阈值

- 在系统视图下配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**nd snooping alarm binding-table check threshold** *threshold*，配置ND Snooping丢弃报文数量的告警阈值。

     缺省情况下，全局ND Snooping丢弃报文数量的告警阈值为100packets。
- 在其他视图下配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。

     或者，执行命令**vlan** *vlan-id*，进入VLAN视图。
  c. 执行命令**nd snooping alarm binding-table check threshold** *threshold*，配置ND Snooping丢弃报文数量的告警阈值。

     缺省情况下，接口下ND Snooping丢弃报文数量的告警阈值为在系统视图下配置的值。

----结束

10.6.4 （可选）配置用户在线状态探测功能

背景信息

设备在使能ND Snooping功能后通过检查NS报文来建立ND Snooping动态绑定表；通过检查NS/NA报文来更新ND Snooping动态绑定表。该表表项的自动老化时间是由用户的IPv6地址租期决定的。如果用户的租期未到期，但是实际该用户已经下线，此时该用户对应的ND Snooping动态绑定表项不能被及时删除，一方面会占用设备的绑定表资源，另一方面会造成新的表项信息无法更新。

为了解决该问题，可以配置用户在线状态探测功能。探测方式分为两种：定时探测和由与现有表项IP地址相同、端口号不同的NA报文触发探测。

- 定时探测：

  设备根据**nd user-bind detect**命令配置的探测次数（n）和探测时间间隔向对应的用户发送NS探测报文。在发出n次NS探测报文后，如果该用户仍然没有回应NA报文，设备则认为该用户不在线，删除该用户对应的ND Snooping动态绑定表项。

  如果网络小且质量好，用户可以很快回应NA报文，此时可以将发送探测报文的时间间隔适当调小；如果网络大且质量不好，用户的回应NA报文较慢，为了避免在还没收到回应的NA报文时就开始发送下一个NS探测报文，可以将时间间隔适当调大。请根据实际网络环境进行调整。
- 由冲突的NA报文触发探测：

  设备收到与现有表项的IP地址相同、入端口不同的NA报文时，说明该NA报文与现有表项冲突，此时会触发设备发送NS报文来探测对应表项的用户在否在线。
  - 如果在表项生存时间内，设备从表项对应的端口上收到NA报文，说明该用户仍然在线，更新对应表项中用户的地址租期。

- 如果在表项生存时间内，设备没有从表项对应的端口上收到NA报文，说明该用户已经下线，更新对应表项中用户的地址租期并将表项的端口更新为新端口。

说明

设备收到与绑定表冲突的NA报文后，触发用户在线状态探测功能时，用户在线状态的定时探测功能暂停。

操作步骤

- 定时探测：
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**nd user-bind detect enable**，使能定时探测ND Snooping动态绑定表项对应用户的在线状态功能。
     缺省情况下，未使能定时探测ND Snooping动态绑定表项对应用户的在线状态功能。
  c. 执行命令**nd user-bind detect retransmit** *retransmit-times* **interval** *retransmit-interval*，配置发送NS探测报文的探测次数和探测时间间隔。
     缺省情况下，探测次数为2次，探测时间间隔为1000毫秒。
- 冲突的NA报文触发探测：
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**nd snooping wait-time** *wait-time* **life-time** *life-time*，配置设备发送NS探测报文的等待时间和探测期间ND Snooping绑定表表项的生存时间。
     缺省情况下，设备发送NS探测报文的等待时间为250毫秒、探测期间ND Snooping绑定表表项的生存时间为500毫秒。

----结束

10.6.5 （可选）配置接口允许学习 ND Snooping 动态绑定表项的最大个数

背景信息

为了防止当一个接口下有大量用户上线，设备处理这些用户发送的大量NS报文会导致整个设备的ND Snooping动态绑定表资源都被耗尽，可以配置接口允许学习ND Snooping动态绑定表项的最大个数。如果指定接口下学习到的绑定表项数目达到了允许学习的最大个数，则不再新增与该接口相关的绑定表项。

可在系统视图或接口视图下配置接口允许学习ND Snooping动态绑定表项的最大个数，系统视图下的配置对所有接口都生效，接口视图下的配置仅对特定接口生效。如果同时在两个视图下进行了配置，则该接口允许学习的绑定表项最大个数以两个视图下配置的较小值为准。

操作步骤

- 在系统视图下配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**nd snooping max-user-number** *max-user-number*，配置接口允许学习ND Snooping动态绑定表项的最大个数。

缺省情况下，在规格范围内，设备对接口能够学习到的最大ND Snooping动态绑定表项数目没有限制。

- 在接口视图下配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**nd snooping max-user-number** *max-user-number*，配置接口允许学习ND Snooping动态绑定表项的最大个数。

     缺省情况下，在规格范围内，设备对接口能够学习到的最大ND Snooping动态绑定表项数目没有限制。

----结束

10.6.6 （可选）配置 ND Snooping 动态绑定表的告警阈值百分比

背景信息

配置接口允许学习ND Snooping动态绑定表项的最大个数后，可以配置ND Snooping动态绑定表的告警阈值百分比。

当设备实际学习到的ND Snooping动态绑定表项数占设备允许学习的最大表项数的比例等于或高于上限告警阈值百分比时，设备将会发出超限告警。之后，如果该比例又等于或小于下限告警阈值百分比，设备会再次发出告警，表明之前的超限告警情况已经恢复正常。管理员通过这些告警信息，可实时掌握ND Snooping动态绑定表资源的使用状况。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**nd snooping user-alarm percentage** *percent-lower-value percent-upper-value*，配置ND Snooping动态绑定表的告警阈值百分比。

缺省情况下，下限告警阈值百分比为50，上限告警阈值百分比为100。

----结束

10.6.7 （可选）配置静态前缀管理表项

背景信息

设备根据收到的NS报文新建ND Snooping动态绑定表项之前，首先要求报文中的Target Address字段能够匹配用户的前缀管理表项。设备会截获从ND Snooping信任接口收到的RA报文，并根据RA报文自动生成前缀管理表项。但是，在网关设备不发送RA报文的情况下，前缀管理表项无法自动生成，进而无法新建对应的ND Snooping动态绑定表项，对业务造成影响。此时，可以通过以下步骤，手动配置前缀管理表项。

通过命令**display nd snooping prefix**可以查看设备上所有的前缀管理表项，包括静态配置的和动态生成的。静态配置的和动态生成的共享规格，超规格则无法配置。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**nd snooping static-prefix** *ipv6-address/prefix-length* [**vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]]，配置静态前缀管理表项。

缺省情况下，设备上没有配置静态前缀管理表项。

----结束

10.6.8 （可选）配置 DAD NS 报文重传速率检查功能

背景信息

设备非信任接口收到DAD NS报文时，会进行转发，用于重复地址检查和用户仿冒检查。在ND Snooping绑定表未建立的情况下，为避免因丢包等原因造成对端设备接收不到设备转发的报文，设备的非信任接口收到DAD NS报文时会进行重传。默认情况下，设备不对重传速率进行控制。在报文过多时，重传可能会影响网络业务正常运行。为解决该问题，可以配置DAD NS报文重传速率检查功能。配置该功能后，设备对重传报文进行限速，每秒钟重传的报文超过设置值时，超出部分直接丢弃，不会转发。

操作步骤

- 在系统视图下配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**nd snooping check dad-ns retransmit-rate enable**，使能DAD NS报文重传速率检查功能。

     缺省情况下，未使能DAD NS报文重传速率检查功能。
  c. 执行命令**nd snooping check dad-ns retransmit-rate rate** *rate-value*，配置DAD NS报文重传速率的最大值。

     缺省情况下，DAD NS报文重传速率的最大值50包/秒。
- 在VLAN视图下配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**vlan** *vlan-id*，进入VLAN视图。
  c. 执行命令**nd snooping check dad-ns retransmit-rate enable**，使能DAD NS报文重传速率检查功能。

     缺省情况下，未使能DAD NS报文重传速率检查功能。
  d. 执行命令**nd snooping check dad-ns retransmit-rate rate** *rate-value*，配置DAD NS报文重传速率的最大值。

     缺省情况下，DAD NS报文重传速率的最大值50包/秒。
- 在接口视图下配置
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**nd snooping check dad-ns retransmit-rate enable**，使能DAD NS报文重传速率检查功能。

     缺省情况下，未使能DAD NS报文重传速率检查功能。
  d. 执行命令**nd snooping check dad-ns retransmit-rate rate** *rate-value*，配置DAD NS报文重传速率的最大值。

缺省情况下，DAD NS报文重传速率的最大值50包/秒。

----结束

10.6.9 检查 ND Snooping 的配置结果

操作步骤

- 执行命令**display nd snooping** [**static** | **dynamic**] **prefix** [**verbose**]，查看ND用户的前缀管理表项。
- 执行命令**display nd snooping user-bind all** [**verbose**]或**display nd snooping user-bind** { **ipv6-address** *ipv6-address* | **mac-address** *mac-address* | **interface** *interface-type interface-number* | **vlan** *vlan-id* } * [**verbose**]，查看ND Snooping动态绑定表项。
- 执行命令**display nd snooping statistics**，查看设备接收与丢弃的ND Snooping用户报文统计信息。
- 执行命令**display nd snooping configuration**，查看ND Snooping的配置信息。

----结束

10.7 维护 ND Snooping

10.7.1 清除前缀管理表

背景信息

网关路由器会定时发送RA报文，通知用户更新网络前缀信息。交换机作为用户的接入设备会根据RA报文建立前缀管理表项，用来维护和管理用户的前缀信息。

一般情况下，不建议手工清除用户的前缀管理表项。当同时具备以下两种情况时，才需要手动进行清除：

- 用户的租期未到期，该用户的前缀管理表项不能自动老化。
- 确定该用户不再需要连接网络。

在确认需要手动清除前缀管理表项后，请在用户视图下执行以下命令。

操作步骤

- 使用命令**reset nd snooping prefix** [*ipv6-address*|*prefix-length*]，清除用户的前缀管理表项。

----结束

10.7.2 清除 ND Snooping 动态绑定表

背景信息

当同时具备以下几种情况时需要手动清除ND Snooping动态绑定表项:

- 因未到老化周期，ND Snooping动态绑定表项暂不能自动老化。

- 确认用户不再连接网络。
- 用户的VLAN或接口信息发生变化。

须知

由于组网环境变化之后，用户的VLAN或接口信息可能已经发生变化，然而用户对应的ND Snooping动态绑定表项却没有立即老化更新，此时会造成设备误将不匹配ND Snooping动态绑定表的合法ND报文丢弃。所以，请在变更组网环境之前手动清除所有ND Snooping动态绑定表项，使得设备根据新的网络环境生成新的ND Snooping动态绑定表。

在确认需要手动清除ND Snooping动态绑定表项后，请在用户视图下执行以下命令。

操作步骤

- 使用命令**reset nd snooping user-bind** [**interface** *interface-type interface-number* | **ipv6-address** *ipv6-address* | **mac-address** *mac-address* | **vlan** *vlan-id*]，清除ND Snooping动态绑定表项。

----结束

10.7.3 清除 ND Snooping 报文统计信息

背景信息

须知

清除统计信息后，以前的统计信息将无法恢复，请慎重操作。

操作步骤

- 在用户视图下执行命令**reset nd snooping statistics**，清除ND Snooping用户报文统计信息。

----结束

10.8 ND Snooping 配置举例

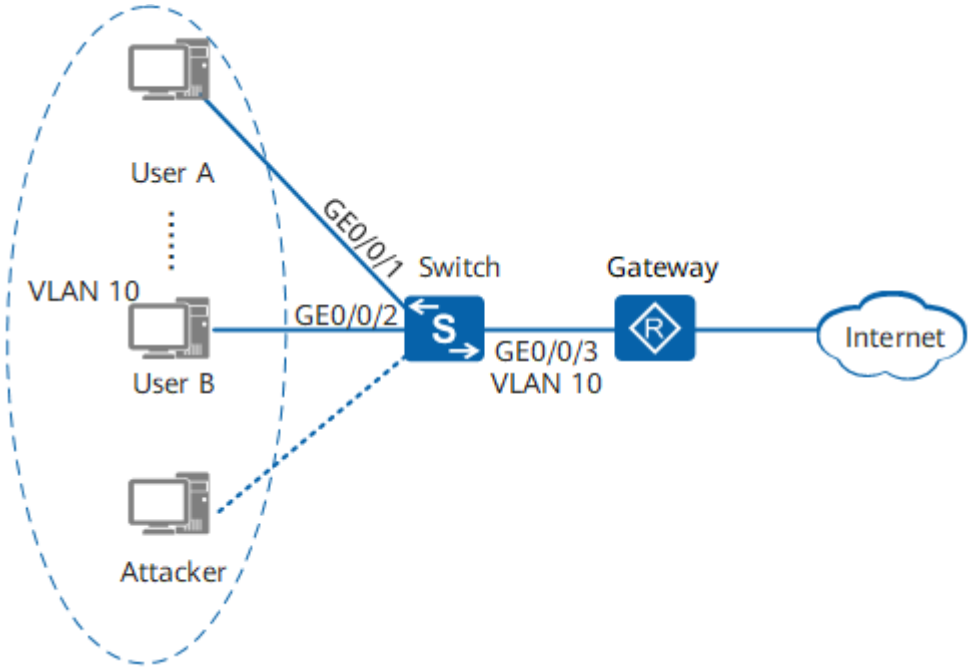
10.8.1 配置 ND Snooping 功能示例

组网需求

如图10-3所示，企业某部门使用Switch作为用户主机连接网关的设备。网络中未部署DHCPv6服务器，该部门主机只能通过无状态地址自动配置方式获取IPv6地址。如果有攻击者发送非法的NA/NS/RS/RA报文，将会存在合法用户主机无法获取IPv6地址、通信过程中断、用户帐号口令被盗用等一系列安全隐患。

为了预防这种情况，管理员希望通过在Switch上进行配置，对非法的NA/NS/RS/RA进行有效防范，为合法用户提供更安全的网络环境和更稳定的网络服务，并且希望能够掌握网关分配给用户的网络前缀信息，从而可以灵活管理接入用户的IPv6地址。

图 10-3 配置 ND Snooping 功能示例组网图



配置思路

采用如下的思路在Switch上进行配置：

1. 使能ND Snooping功能，以便生成地址、VLAN和接口的绑定关系表，用于后续的ND报文合法性检查。
2. 将连接网关的接口配置为ND Snooping信任接口，以便Switch可以根据从信任接口收到的RA报文生成前缀管理表，实现对接入用户地址的灵活管理。

   连接用户侧的接口缺省为ND Snooping非信任接口，Switch会自动过滤非信任接口收到的RA报文。
3. 使能ND协议报文合法性检查功能，使Switch根据绑定关系表对NA/NS/RS报文进行合法性检查，过滤非法NA/NS/RS报文。
4. 配置自动探测ND Snooping动态绑定表项对应用户的在线状态功能，保证ND用户下线时对应的ND Snooping动态绑定表项能够及时被删除，避免占用绑定表资源。
5. 配置接口允许学习ND Snooping动态绑定表项的最大个数，防止在配置ND Snooping功能后，由于某一接口下有大量用户上线，Switch处理大量的NS报文会导致绑定表资源被耗尽，造成其他用户无法正常通信。

操作步骤

步骤1 创建VLAN并配置各接口

在Switch上创建VLAN10。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 10
```

将接口GE0/0/1、GE0/0/2、GE0/0/3加入到VLAN10中。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type access
[Switch-GigabitEthernet0/0/1] port default vlan 10
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] port link-type access
[Switch-GigabitEthernet0/0/2] port default vlan 10
[Switch-GigabitEthernet0/0/2] quit
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] port link-type trunk
[Switch-GigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Switch-GigabitEthernet0/0/3] quit
```

步骤2 使能ND Snooping功能

全局使能ND Snooping功能。

```
[Switch] nd snooping enable
```

在VLAN10内使能ND Snooping功能。

```
[Switch] vlan 10
[Switch-vlan10] nd snooping enable
[Switch-vlan10] quit
```

步骤3 配置接口GE0/0/3为ND Snooping信任接口

```
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] nd snooping trusted
[Switch-GigabitEthernet0/0/3] quit
```

步骤4 使能ND协议报文合法性检查功能

```
[Switch] vlan 10
[Switch-vlan10] nd snooping check ns enable
[Switch-vlan10] nd snooping check na enable
[Switch-vlan10] nd snooping check rs enable
[Switch-vlan10] quit
```

步骤5 配置自动探测ND Snooping动态绑定表项对应用户的在线状态功能

使能自动探测ND Snooping动态绑定表项对应用户的在线状态功能，并配置发送NS探测报文的探测次数和探测时间间隔。

```
[Switch] nd user-bind detect enable
[Switch] nd user-bind detect retransmit 5 interval 600
```

步骤6 配置接口允许学习ND Snooping动态绑定表项的最大个数

```
[Switch] nd snooping max-user-number 200
```

步骤7 验证配置结果

在系统视图下执行命令**display this**可以看到全局下已经使能了ND Snooping功能和自动探测ND Snooping动态绑定表项对应用户的在线状态功能，并配置了接口允许学习ND Snooping动态绑定表项的最大个数。

```
[Switch] display this
......
 nd snooping enable
 nd user-bind detect enable
 nd user-bind detect retransmit 5 interval 600
```

```
 nd snooping max-user-number 200
......
```

在VLAN视图下执行命令**display this**可以看到VLAN10下已经使能了ND Snooping功能和ND协议报文合法性检查功能。

```
[Switch] vlan 10
[Switch-vlan10] display this
#
vlan 10
 nd snooping enable
 nd snooping check ns enable
 nd snooping check na enable
 nd snooping check rs enable
#
return
[Switch-vlan10] quit
```

在接口视图下执行命令**display this**可以看到接口GE0/0/3已经配置为信任接口。

```
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] display this
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
 nd snooping trusted
#
return
[Switch-GigabitEthernet0/0/3] quit
[Switch] quit
```

执行命令**display nd snooping prefix**可以查看ND用户的前缀管理表。

```
<Switch> display nd snooping prefix
prefix-table:
Prefix                          Length   Valid-Time  Preferred-Time
-------------------------------------------------------------------------------
FC00:1::                         64       100000      100000
-------------------------------------------------------------------------------
Prefix table total count:      1
```

执行命令**display nd snooping user-bind all**可以查看ND Snooping动态绑定表。

```
<Switch> display nd snooping user-bind all
ND Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping                          IP Address                  MAC
Address     VSI/VLAN(O/I/P) Lease
-------------------------------------------------------------------------------
FC00:1::E58C:A2E7:AA4C:8E59     000e0-fc12-3456 10  /--  /--    2011.05.06-20:09
-------------------------------------------------------------------------------
print count:          1          total count:          1
```

如果Switch上生成了前缀管理表和ND Snooping动态绑定表，则说明ND Snooping功能已配置成功。

----结束

配置文件

Switch的配置文件

```
#
sysname Switch
#
vlan batch 10
#
nd snooping enable
```

```
nd user-bind detect enable
nd user-bind detect retransmit 5 interval 600
nd snooping max-user-number 200
#
vlan 10
 nd snooping enable
 nd snooping check ns enable
 nd snooping check na enable
 nd snooping check rs enable
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
 nd snooping trusted
#
return
```

11 IPv6 RA Guard 配置

11.1 IPv6 RA Guard 概述

IPv6 ND（IPv6 Neighbor Discovery，IPv6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和重定向。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）

关于ND协议的详细介绍，请参见《S600-E V200R021C00, C01配置指南-IP业务》IPv6基础配置 中的“邻居发现”。

ND协议是IPv6的一个关键协议，它功能强大，但是因为其没有任何安全机制，所以容易被攻击者利用。其中的RA报文攻击，攻击者仿冒网关向其他用户发送路由器通告报文RA（Router Advertisement），会改写其他用户的ND表项或导致其它用户记录错误的IPv6配置参数，造成这些用户无法正常通信。

根据RA报文攻击的特点，IPv6 RA Guard功能采用以下两种方式在二层接入设备上阻止恶意的RA报文攻击：

说明

两种配置方式互斥，同一个二层接口上只能配置其中一种。

- 为接收RA报文的接口配置接口角色，系统根据接口角色选择转发还是丢弃该RA报文：
  - 若接口角色为路由器，则直接转发RA报文；
  - 若接口角色为用户，则直接丢弃RA报文。
- 为接收RA报文的接口配置IPv6 RA Guard策略，按照策略内配置的匹配规则对RA报文进行过滤：
  - 若IPv6 RA Guard策略中未配置任何匹配规则，则应用该策略的接口直接转发RA报文；
  - 若IPv6 RA Guard策略中配置了匹配规则，则RA报文需成功匹配策略下所有规则后才会被转发；否则，该报文被丢弃。

11.2 IPv6 RA Guard 配置注意事项

涉及网元

需要其他网元支持IPv6 RA Guard。

License 支持

本特性是交换机的基本特性，无需获得License许可即可应用此功能。

V200R021C00、V200R021C01 版本特性支持情况

S600-E系列交换机中所有款型均支持IPv6 RA Guard。

说明

如需了解交换机软件配套详细信息，请点击**Info-Finder**。

特性依赖和限制

无

11.3 配置 IPv6 RA Guard

11.3.1 配置接口角色

背景信息

管理员可根据接口在组网中的位置来配置接口的角色。如果确定接口连接的是用户主机，则配置接口角色为用户（host）；如果确定接口连接的是路由器，则配置接口角色为路由器（router）。

- 若接口角色为路由器，则直接转发RA报文；
- 若接口角色为用户，则直接丢弃RA报文。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入二层接口视图。

步骤3 执行命令**nd raguard role** { **host** | **router** }，配置IPv6 RA Guard功能的接口角色。

缺省情况下，未配置IPv6 RA Guard功能的接口角色。

----结束

11.3.2 配置 IPv6 RA Guard 策略

背景信息

以下两种情况，可以通过配置IPv6 RA Guard策略来过滤RA报文：

- 不能判断接口连接的设备或终端的类型，即不能通过配置接口角色来选择丢弃还是转发RA报文；
- 能够确定接口连接的是路由器，但用户不希望直接转发RA报文，希望按条件进行过滤。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**nd raguard policy** *policy-name*，创建IPv6 RA Guard策略。

步骤3 配置IPv6 RA Guard策略内的匹配规则。

说明

- RA报文必须匹配策略内配置的所有规则才能转发。
- 当ACL作为匹配规则时，如果指定的ACL未创建、ACL中未配置规则或者ACL中配置的规则不是源MAC地址、源IPv6地址或前缀，则RA报文不检查该匹配项目。RA报文检查时不关注ACL内配置的动作（permit/deny），只关注匹配项（源MAC地址、源IPv6地址或前缀），命中匹配项则转发。

- 执行命令**if-match source-mac-address acl** *acl-number*，配置RA报文源MAC地址的匹配规则。

  缺省情况下，未配置RA报文源MAC地址的匹配规则。

  匹配规则通过二层ACL指定，二层ACL的配置方法请参见“ACL配置”中的“**2.7.3 配置二层ACL**”。
- 执行命令**if-match ipv6-source-address acl** *acl-number*，配置RA报文源IPv6地址的匹配规则。

  缺省情况下，未配置RA报文源IPv6地址的匹配规则。

  匹配规则通过基本ACL6指定，基本ACL6的配置方法请参见“ACL配置”中的“**2.7.6 配置基本ACL6**”。
- 执行命令**if-match prefix acl** *acl-number*，配置RA报文携带的IPv6前缀的匹配规则。

  缺省情况下，未配置RA报文携带的IPv6前缀的匹配规则。

  匹配规则通过基本ACL6指定，基本ACL6的配置方法请参见“ACL配置”中的“**2.7.6 配置基本ACL6**”。

- 执行命令**hop-limit** { **maximum** *max-value* | **minimum** *min-value* }，配置RA报文中跳数限制的最大值和最小值匹配规则。

  缺省情况下，RA报文中跳数限制最大值为255和最小值为1。
- 执行命令**managed-address-flag** { **on** | **off** }，配置RA报文中M标志位的匹配规则。

  缺省情况下，未配置RA报文中M标志位的匹配规则。
- 执行命令**other-config-flag** { **on** | **off** }，配置RA报文中O标志位的匹配规则。

  缺省情况下，未配置RA报文中O标志位的匹配规则。
- 执行命令**router-preference maximum** { **high** | **medium** | **low** }，配置RA报文中路由最高优先级的匹配规则。

  缺省情况下，未配置RA报文中路由最高优先级匹配规则。

步骤4 执行命令**quit**，退回到系统视图。

步骤5 执行命令**interface** *interface-type interface-number*，进入二层接口视图。

步骤6 执行命令**nd raguard attach-policy** *policy-name*，在接口下绑定IPv6 RA Guard策略。

缺省情况下，接口下没有绑定IPv6 RA Guard策略。

----结束

操作结果

执行命令**display nd raguard policy** [*policy-name*]，查看IPv6 RA Guard策略的配置信息。

11.4（可选）配置 IPv6 RA Guard 日志功能

背景信息

IPv6 RA Guard日志是为了满足管理员审计的需要，对处理RA报文的信息进行的记录。开启IPv6 RA Guard 日志功能后，设备在检测到非法RA报文时将生成日志**ND_RAGUARD/3/ND_RAGUARD_DROP**，日志内容包括：受到攻击的接口名称、RA报文的源IP地址、源MAC地址和接口下丢弃的RA报文总数。

设备生成的IPv6 RA Guard日志信息会上送到信息中心模块处理，信息中心模块的配置将决定日志信息的输出规则和输出方向。关于信息中心的详细描述请参见《 S600-E V200R021C00, C01配置指南-设备管理 》中的“信息中心配置”。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**nd raguard log enable**，打开IPv6 RA Guard记录日志的功能。

----结束

11.5 查询和清除 IPv6 RA Guard 报文统计信息

背景信息

接口角色为用户（host）时或者接口应用IPv6 RA Guard策略后不满足匹配规则时会丢弃RA报文。设备支持基于接口查看丢弃的RA报文计数。

操作步骤

- 执行命令**display nd raguard statistic** [**interface** *interface-type interface-number*]，查看接口丢弃RA报文的统计信息。
- 执行命令**reset nd raguard statistic** [**interface** *interface-type interface-number*]，清除接口丢弃RA报文的统计信息。

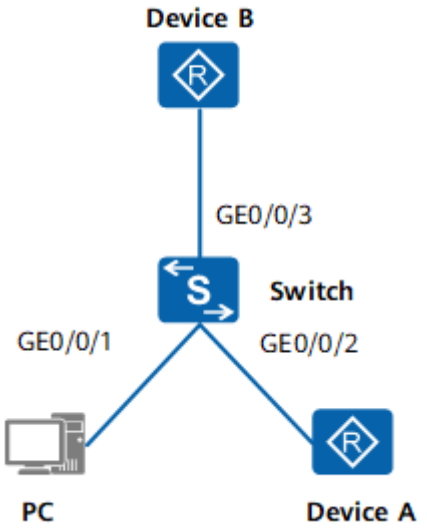
11.6 配置 IPv6 RA Guard 示例

组网需求

如图11-1所示，在Switch上接口GE0/0/1、GE0/0/2和GE0/0/3分别PC、Device A和Device B。为防止RA报文攻击，在Switch的接口上配置IPv6 RA Guard功能：

- 接口GE0/0/1连接的是PC，该接口收到的RA报文可以直接丢弃；
- 接口GE0/0/2连接的Device A是路由器，该接口收到的RA报文可以直接转发；
- 接口GE0/0/3连接的Device B是未知设备，通过在该接口上配置IPv6 RA Guard策略，对收到的RA报文进行过滤。

图 11-1 IPv6 RA Guard 功能组网图



配置过程

1. 配置接口GE0/0/1的接口角色为用户。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] nd raguard role host
[Switch-GigabitEthernet0/0/1] quit
```

2. 配置接口GE0/0/2的接口角色为路由器。

```
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] nd raguard role router
[Switch-GigabitEthernet0/0/2] quit
```

3. 配置接口GE0/0/3应用IPv6 RA Guard策略“p1”，仅允许转发IPv6前缀地址为fc00:1::/64、M标志位和O标志位都为1的RA报文。

```
[Switch] acl ipv6 2000
[Switch-acl6-basic-2000] rule 1 permit source fc00:1:: 64
[Switch-acl6-basic-2000] quit
[Switch] nd raguard policy p1
[Switch-nd-raguard-policy-p1] if-match prefix acl 2000
[Switch-nd-raguard-policy-p1] managed-address-flag on
[Switch-nd-raguard-policy-p1] other-config-flag on
[Switch-nd-raguard-policy-p1] quit
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] nd raguard attach-policy p1
[Switch-GigabitEthernet0/0/3] quit
```

12 PPPoE+配置

12.1 PPPoE+概述

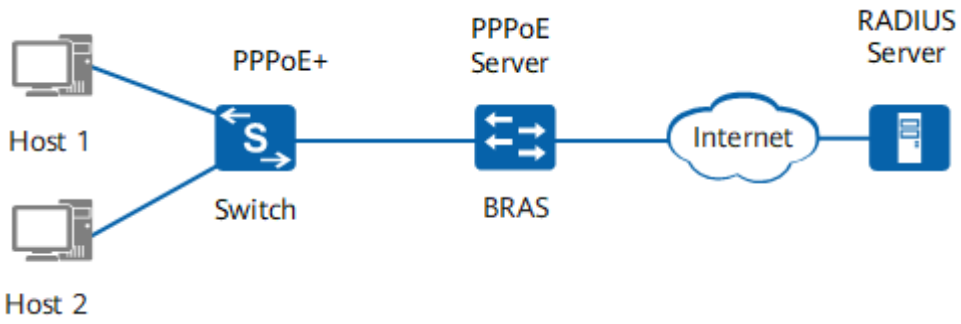
PPPoE+产生背景

PPPoE是一种通过一个远端接入设备为以太网上的主机提供接入服务，并可以对接入的每个主机实现控制和计费的技术。PPPoE使用Client/Server模型，PPPoE Client向PPPoE Server发起连接请求，在两者会话协商过程中，PPPoE Server向PPPoE Client提供接入控制、认证等功能。

目前所使用的PPPoE具有较好的认证和安全机制，但仍然存在一些缺陷。比如PPPoE Server仅通过用户名和密码对接入用户进行认证，如果账号被盗，盗用者可以很容易的在其他地方通过该账号接入网络。为了解决上述问题，引入了PPPoE+特性。

PPPoE+，又称PPPoE Intermediate Agent，部署在终端用户主机和宽带远程接入服务器BRAS（Broadband Remote Access Server）之间的接入设备Switch上，如**图12-1**所示。Switch将终端用户主机接入的端口信息（如槽位号/子卡号/接口号、VLAN、MAC地址等）通过PAD（PPPoE Active Discovery ）报文上送给PPPoE Server，由PPPoE Server根据报文信息实现终端用户的用户账号与接入端口的绑定认证，避免用户账号被盗用。

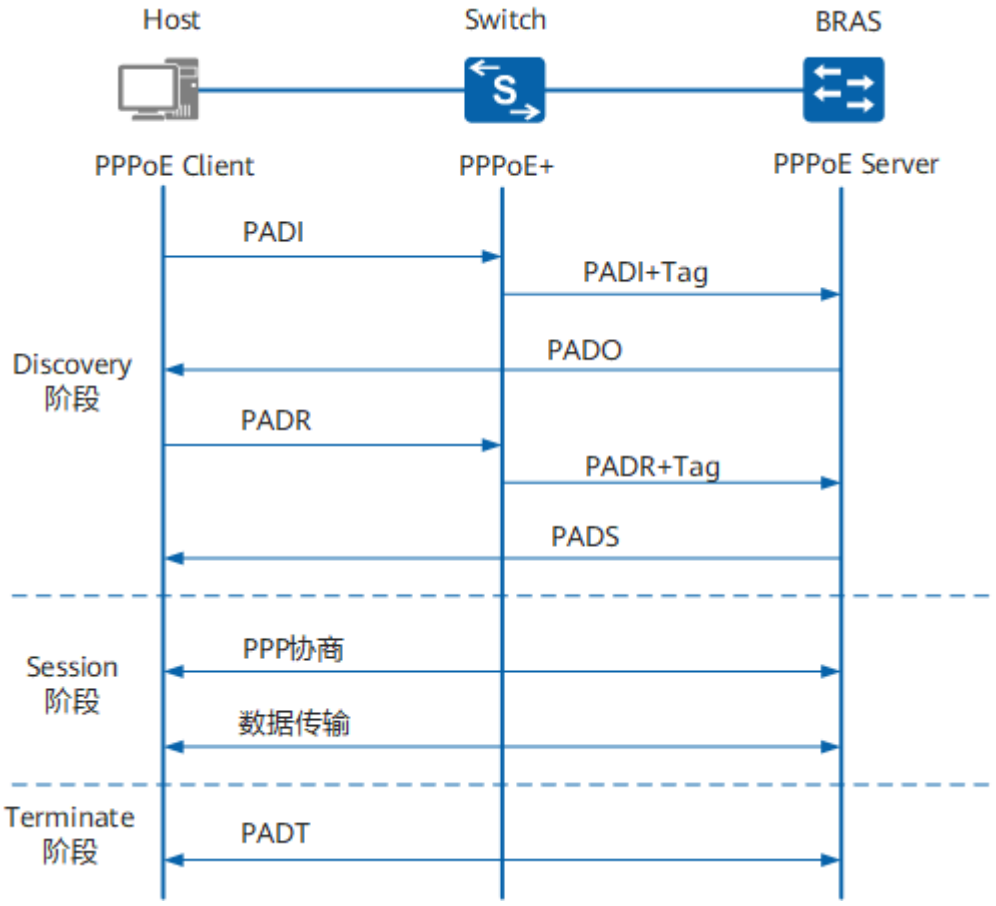
图 12-1 PPPoE+组网示意图



PPPoE+工作流程

PPPoE可分为三个阶段，即Discovery阶段、Session阶段和Terminate阶段。PPPoE+主要作用于Discovery阶段和Session阶段。PPPoE+的具体流程如图12-2所示：

图 12-2 PPPoE+工作流程示意图



1. 终端用户主机（PPPoE Client）发起PPPoE请求，发送PADI（PPPoE Active Discovery Initial）报文。

2. Switch截获PADI报文后把终端用户主机接入的端口信息（如槽位号/子卡号/接口号、VLAN、MAC地址等）以PPPoE+ Tag形式插入PADI报文里，再转发给BRAS（PPPoE Server）。
3. BRAS收到PADI+Tag以后，向终端用户主机回应PADO（PPPoE Active Discovery Offer）报文。
4. 终端用户主机收到PADO报文后，发送PADR（PPPoE Active Discovery Request）报文。
5. Switch截获PADR报文后把PPPoE+ Tag插入到PADR报文里，再转发给BRAS。
6. BRAS收到PADR+Tag以后，将产生一个唯一的会话ID（PPP Session ID），标识和终端用户主机的这个会话，并向终端用户主机回应PADS（PPPoE Active Discovery Session-confirmation）报文。如果没有发生错误，双方进入Session阶段。
7. Session阶段内，终端用户主机和BRAS之间进行PPP协商和PPP报文传输。PPP协商完成后，BRAS将PPPoE+ Tag封装在RADIUS报文的Radius NAS-Port-ID属性里发送给RADIUS Server，RADIUS Server将根据该属性值对终端用户主机进行用户账号与接入端口的绑定认证。
8. PPPoE会话建立后，PPPoE Client和PPPoE Server随时可以通过发送PADT（PPPoE Active Discovery Terminate）报文的方式来结束PPPoE会话。

12.2 PPPoE+配置注意事项

涉及网元

无需其他网元配合。

License 支持

本特性是交换机的基本特性，无需获得License许可即可应用此功能。

V200R021C00、V200R021C01 版本特性支持情况

S600-E系列交换机中所有款型均支持PPPoE+。

说明

如需了解交换机软件配套详细信息，请点击**Info-Finder**。

特性依赖和限制

无

12.3 PPPoE+缺省配置

PPPoE+的缺省配置如**表12-1**所示。

表 12-1 PPPoE+缺省配置

参数	缺省值
全局PPPoE+功能	关闭
信任接口	所有接口为非信任接口
对用户侧PPPoE报文原有信息字段的处理方式	**replace**
在PPPoE报文中添加的信息字段格式和内容	**common**格式的**circuit-id**和**remote-id**
在PPPoE报文中添加的VENDOR ID值	2011
对服务器侧PPPoE回应报文原有信息字段的处理方式	不处理

12.4 配置 PPPoE+

前置任务

在配置PPPoE+之前，需完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为Up。

12.4.1 开启 PPPoE+功能

背景信息

为了防止用户账号盗用现象，可以配置PPPoE+功能。开启全局PPPoE+功能是配置PPPoE+具体功能的前提条件。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**pppoe intermediate-agent information enable**，开启全局PPPoE+功能。

在系统视图下执行该命令后，所有接口都将开启PPPoE+功能。

缺省情况下，全局未开启PPPoE+功能。

----结束

12.4.2 配置 PPPoE+信任接口

背景信息

设备与PPPoE Server相连的接口必须是信任接口，才可以防止PPPoE Server欺骗，并且防止PPPoE报文被转发至非PPPoE业务端口而遭到非法用户的获取。配置信任接口

后，从PPPoE Client到PPPoE Server方向的PPPoE报文将只会由信任接口进行转发，同时也只有从信任接口收到的PPPoE报文才会被转发至PPPoE Client。

说明

信任接口只对PPPoE Discovery阶段的协议报文进行控制，对于PPPoE Session阶段的业务报文不进行控制。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入以太网接口视图。

步骤3 执行命令**pppoe uplink-port trusted**，配置接口为信任接口。

缺省情况下，所有接口为非信任接口。

----结束

12.4.3 配置对用户侧 PPPoE 报文的处理方式

背景信息

通过配置对用户侧PPPoE报文的处理方式，设备可以将终端用户主机接入的端口信息加入PPPoE报文中，实现终端用户的用户账号与接入端口的绑定认证，避免用户账号被盗用。

可在系统视图或接口视图下配置对用户侧PPPoE报文原有信息字段的处理方式，系统视图下的配置对所有接口都生效。如果希望在某个接口上采用其他处理方式，则可以在指定接口下进行配置，此时该接口对PPPoE报文的处理方式将以在该接口上所做的配置为准。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 配置对用户侧PPPoE报文原有信息字段的处理方式。

- 系统视图下配置对用户侧PPPoE报文原有信息字段的处理方式

  执行命令**pppoe intermediate-agent information policy** { **drop** | **keep** | **replace** }，配置所有接口对PPPoE报文中原有信息字段的处理方式。

  缺省情况下，设备接口对收到的用户侧PPPoE报文中的信息字段采取**replace**方式。

- 接口视图下配置对用户侧PPPoE报文原有信息字段的处理方式

  a. 执行命令**interface** *interface-type interface-number*，进入以太网接口视图。

  b. 执行命令**pppoe intermediate-agent information policy** { **drop** | **keep** | **replace** }，用来配置指定接口对PPPoE报文中原有信息字段的处理方式。

  c. （可选）执行命令**pppoe intermediate-agent information** [**vlan** *vlan-id*] [**ce-vlan** *cevlan-id*] **format** { **circuit-id** | **remote-id** } { **common** | **extend** | **user-defined** *text* }，配置在PPPoE报文中添加的信息字段格式。

  缺省情况下，设备在PPPoE报文中添加的信息字段是格式为**common**的**circuit-id**和**remote-id**。

接口视图和系统视图下同时配置该命令时，接口视图下的配置优先生效。

d. 执行命令**quit**，返回系统视图。

缺省情况下，设备接口对收到的用户侧PPPoE报文中的信息字段采取**replace**方式。

步骤3 （可选）当设备对用户侧PPPoE报文原有信息字段的处理方式为**replace**时，可配置用于替换原有PPPoE报文信息字段的字段格式和内容。

1. 执行命令**pppoe intermediate-agent information encapsulation** { **circuit-id** | **remote-id** }*，配置在PPPoE报文中添加的信息字段内容。
2. 执行命令**pppoe intermediate-agent information format** { **circuit-id** | **remote-id** } { **common** | **extend** | **user-defined** *text* }，配置在PPPoE报文中添加的信息字段格式。

   缺省情况下，设备在PPPoE报文中添加的信息字段是格式为**common**的**circuit-id**和**remote-id**。

   接口视图和系统视图下同时配置该命令时，接口视图下的配置优先生效。

步骤4 （可选）执行命令**pppoe intermediate-agent information vendor-id** *vendor-id*，配置设备在PPPoE报文中添加的VENDOR ID值。

缺省情况下，设备在PPPoE报文中添加的VENDOR ID值为2011。

说明

VENDOR ID用于标识厂商，使能PPPoE+功能后，设备必须通过含有VENDOR ID的PPPoE报文才能与PPPoE Server进行PPP协商。设备默认在PPPoE报文中添加值为2011的VENDOR ID。如果设备对接其他厂商的PPPoE Server，要求的VENDOR ID值是其他值时（例如3561），则可以通过命令**pppoe intermediate-agent information vendor-id** *vendor-id*进行修改。

----结束

12.4.4 （可选）配置对服务器侧 PPPoE 报文的处理方式

背景信息

通常情况下，设备不需要对服务器侧回应的PPPoE报文进行处理，直接透传报文给PPPoE Client即可。只有在PPPoE Client无法识别设备直接透传的PPPoE报文时，为了保证PPPoE Client和PPPoE Server之间PPPoE会话的正常建立，设备才需要对服务器侧回应的PPPoE报文进行处理。具体处理方式如下：

- 当设备上配置的对PPPoE报文原有信息字段的处理方式为**replace**或**keep**时，
  - 如果服务器侧回应的PPPoE报文不含信息字段，则设备直接透传PPPoE报文；
  - 如果服务器侧回应的PPPoE报文中含有信息字段，且格式和内容与设备在用户侧PPPoE报文中添加的信息字段格式和内容一致，设备会将该PPPoE报文中的信息字段剥掉再进行转发，如果不一致，则设备直接透传PPPoE报文。
- 当设备上配置的对PPPoE报文原有信息字段的处理方式为**drop**时，设备直接透传PPPoE报文。

说明

如果配置设备需要处理服务器侧的PPPoE回应报文，会使大量PPPoE用户并发上线的速度受到影响。

只有在全局使能了PPPoE+功能之后，对服务器侧PPPoE报文的处理方式配置才生效，而且如需修改此配置，必须先去使能PPPoE+功能才可以进行配置更改。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**pppoe intermediate-agent information ignore-reply** { **disable** | **enable** }，配置设备是否不处理服务器侧发送的PPPoE回应报文，直接对其进行透传。

缺省情况下，设备不处理服务器侧发送的PPPoE回应报文。

----结束

12.4.5 检查配置结果

操作步骤

步骤1 使用命令**display pppoe intermediate-agent information format**，查看全局配置的circuit-id和remote-id格式信息。

步骤2 使用命令**display pppoe intermediate-agent information encapsulation**，查看在PPPoE报文中添加的信息字段内容以及VENDOR ID值。

步骤3 使用命令**display pppoe intermediate-agent information policy**，查看全局配置的对用户侧和服务器侧PPPoE报文中原有信息字段的处理方式。

----结束

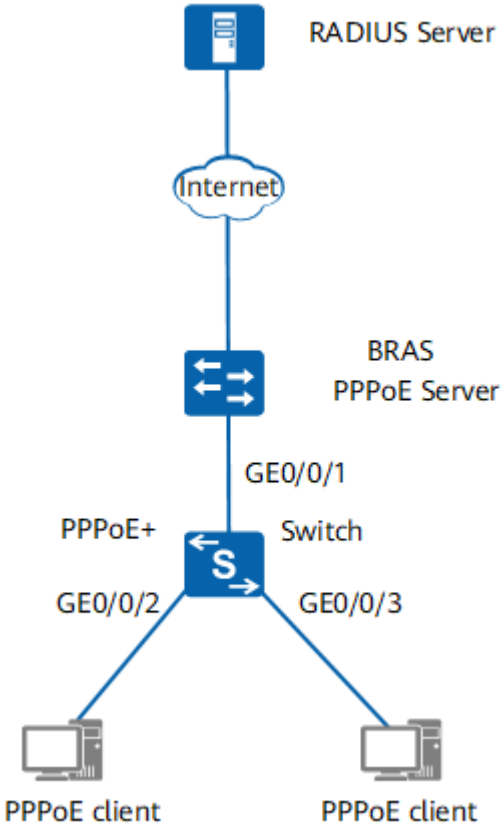
12.5 配置举例

12.5.1 配置 PPPoE+功能示例

组网需求

如图12-3所示，Switch上行连接BRAS设备，下行连接终端用户主机，BRAS内置PPPoE Server功能。网络中存在非法用户获取合法用户的PPPoE报文、盗用合法用户账号的现象，管理员希望能够为合法用户提供账号安全保障，避免用户账号被盗用。

图 12-3 配置 PPPoE+功能示例组网图



配置思路

采用如下思路在Switch上配置PPPoE+功能：

1. 全局使能PPPoE+功能，实现终端用户的用户账号与接入端口的绑定认证，防止用户账号被盗用。
2. 配置Switch与PPPoE Server连接的接口为信任接口，防止PPPoE报文被转发至非PPPoE业务端口而遭到非法用户的获取。
3. 根据PPPoE Server对PPPoE报文信息字段格式的要求，配置Switch对用户侧PPPoE报文中原有信息字段的处理方式，使Switch能够与PPPoE Server正常通信。

操作步骤

步骤1 使能PPPoE+功能

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] pppoe intermediate-agent information enable
```

说明

全局使能后，所有接口都将使能PPPoE+功能。

步骤2 配置GE0/0/1接口为信任接口

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] pppoe uplink-port trusted
[Switch-GigabitEthernet0/0/1] quit
```

步骤3 配置所有接口对用户侧PPPoE报文中原有信息字段的处理方式为**replace**，使用Switch的**circuit-id**和**remote-id**替换原有PPPoE报文中的信息字段

```
[Switch] pppoe intermediate-agent information policy replace
```

步骤4 配置用于替换原有PPPoE报文信息字段的**circuit-id**的格式为**extend**

```
[Switch] pppoe intermediate-agent information format circuit-id extend
```

步骤5 验证配置结果

执行命令**display pppoe intermediate-agent information policy**，查看对用户侧PPPoE报文中原有信息字段的处理方式是否配置正确。

```
[Switch] display pppoe intermediate-agent information policy
 The current information Policy :REPLACE
 The current ignore-reply Policy:ENABLE
```

执行命令**display pppoe intermediate-agent information format**，查看**circuit-id**格式信息是否配置正确。

```
[Switch] display pppoe intermediate-agent information format
 The current information format :
  Circuit ID : EXTEND
  Remote  ID : COMMON
 For example:
  interface GigabitEthernet0/0/1 SVLAN:200 CVLAN:100
  The PPPOE Intermediate Agent information follow:
  Circuit ID:00 04 00 c8 00 00
  Remote  ID:0025-9efb-494a
```

----结束

配置文件

Switch的配置文件

```
#
sysname Switch
#
pppoe intermediate-agent information enable
pppoe intermediate-agent information format circuit-id extend
#
interface GigabitEthernet0/0/1
 pppoe uplink-port trusted
#
return
```

12.6 常见配置错误

12.6.1 PPPoE 用户无法上线

故障现象

配置了PPPoE+功能后，PPPoE用户无法上线。

常见原因

本类故障的常见原因主要包括：

- 配置网络侧接口为非信任接口
- 配置对用户侧PPPoE报文原有信息字段的处理方式与业务需求不相符
- 配置在PPPoE报文中添加的信息字段格式与PPPoE服务器要求的格式不一致

操作步骤

步骤1 检查与PPPoE服务器连接的网络侧接口是否为信任接口

如果网络侧接口不是信任接口，设备将会丢弃PPPoE报文，从而使合法PPPoE用户无法上线。

进入网络侧接口视图，执行命令**display this**，检查接口上是否配置了**pppoe uplink-port trusted**命令：

- 如果没有配置，则网络侧接口是非信任接口，请执行命令**pppoe uplink-port trusted**配置。
- 如果已经配置，则网络侧接口是信任接口，请继续执行以下检查。

步骤2 检查针对用户侧PPPoE报文原有信息字段的处理方式是否与业务需求相符

在系统视图以及PPPoE用户侧接口视图下分别执行命令**display this**，查看全局和接口上是否配置了**pppoe intermediate-agent information policy**命令。

- 如果接口和全局均配置了针对用户侧PPPoE报文原有信息字段的处理方式，则以接口下配置为准。
- 如果均没有配置，则设备缺省采用**replace**方式。

检查处理方式是否与业务需求相符：

- 如果不相符，请执行命令**pppoe intermediate-agent information policy** { **drop** | **keep** | **replace** }配置合适的处理方式。
- 如果相符，请继续执行以下检查。

步骤3 检查在PPPoE报文中添加的信息字段格式与PPPoE服务器要求的格式是否一致

执行命令**display pppoe intermediate-agent information format**查看在PPPoE报文中添加的信息字段格式是否与PPPoE服务器要求的格式一致：

如果不一致，请执行命令**pppoe intermediate-agent information** [**vlan** *vlan-id*] [**ce-vlan** *cevlan-id*] **format** { **circuit-id** | **remote-id** } { **common** | **extend** | **user-defined** *text* }配置合适的信息字段格式。

----结束

13 IPSG 配置

13.1 IPSG 简介

定义

IP源防攻击IPSG（IP Source Guard）是一种基于二层接口的源IP地址过滤技术，它能够防止恶意主机伪造合法主机的IP地址来仿冒合法主机，还能确保非授权主机不能通过自己指定IP地址的方式来访问网络或攻击网络。

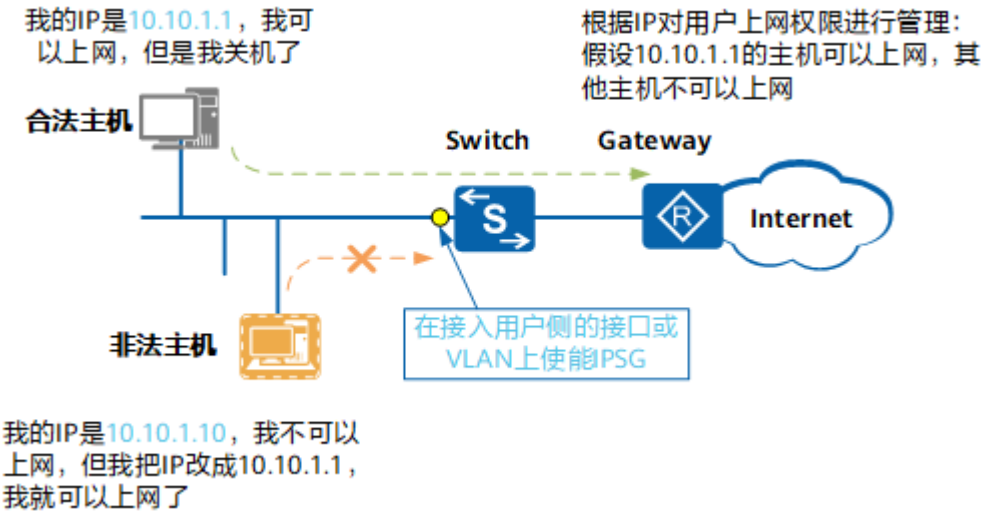
目的

随着网络规模越来越大，通过伪造源IP地址实施的网络攻击（简称IP地址欺骗攻击）也逐渐增多。一些攻击者通过伪造合法用户的IP地址获取网络访问权限，非法访问网络，甚至造成合法用户无法访问网络，或者信息泄露。IPSG针对IP地址欺骗攻击提供了一种防御机制，可以有效阻止此类网络攻击行为。

一个典型的利用IPSG防攻击的示例如**图13-1**所示，非法主机伪造合法主机的IP地址获取上网权限。此时，通过在Switch的接入用户侧的接口或VLAN上部署IPSG功能，

Switch可以对进入接口的IP报文进行检查，丢弃非法主机的报文，从而阻止此类攻击。

图 13-1 IPSG 典型防攻击示例图



13.2 IPSG 原理描述

13.2.1 IPSG 基本原理

IPSG利用绑定表（源IP地址、源MAC地址、所属VLAN、入接口的绑定关系）去匹配检查二层接口上收到的IP报文，只有匹配绑定表的报文才允许通过，其他报文将被丢弃。

绑定表如表13-1所示，包括静态和动态两种。

表 13-1 绑定表

绑定表类型	生成过程	适用场景
静态绑定表	使用**user-bind**命令手工配置。	针对IPv4和IPv6主机，适用于主机数较少且主机使用静态IP地址的场景。
DHCP Snooping动态绑定表（1）	配置DHCP Snooping功能后，DHCP主机动态获取IP地址时，设备根据DHCP服务器发送的DHCP回复报文动态生成。	针对IPv4和IPv6主机，适用于主机数较多且主机从DHCP服务器获取IP地址的场景。
DHCP Snooping动态绑定表（2）	802.1X用户认证过程中，设备根据认证用户的信息生成。	针对IPv4和IPv6主机，适用于主机数较多、主机使用静态IP地址、并且网络中部署了802.1X认证的场景。 该方式生成的表项不可靠，建议配置静态绑定表。

绑定表类型	生成过程	适用场景
ND Snooping动态绑定表	配置ND Snooping功能后，设备通过侦听用户用于重复地址检测的NS（Neighbor Solicitation）报文来建立。	仅针对IPv6主机，适用于主机数较多的场景。

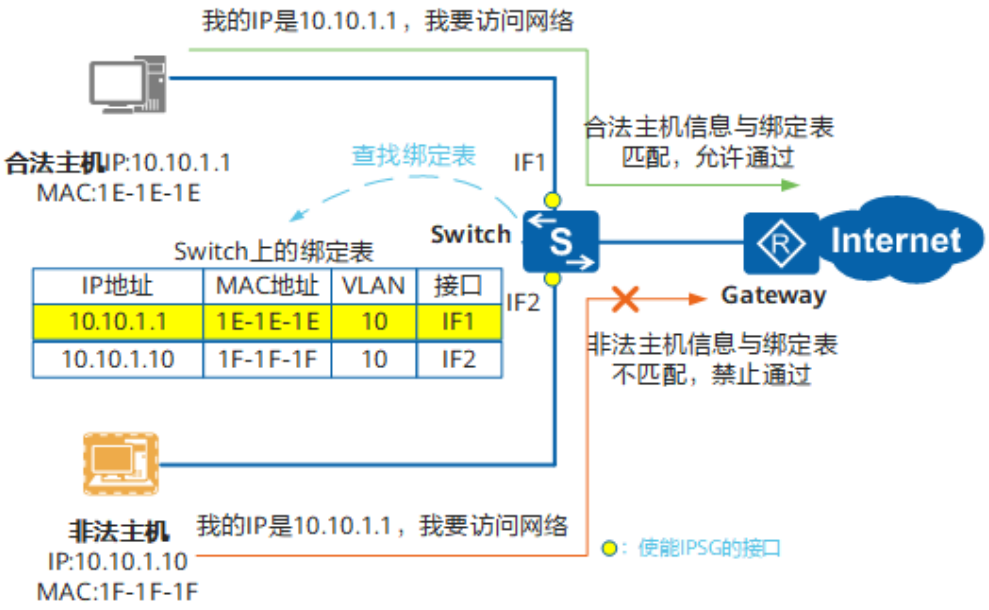
绑定表生成后，IPSG基于绑定表向指定的接口或者指定的VLAN下发ACL，由该ACL来匹配检查所有IP报文。主机发送的报文，只有匹配绑定表才会允许通过，不匹配绑定表的报文都将被丢弃。当绑定表信息变化时，设备会重新下发ACL。缺省情况下，如果在没有绑定表的情况下使能了IPSG，设备会允许IP协议报文通过，但是会拒绝所有的数据报文。

说明

IPSG只匹配检查主机发送的IP报文，包括IPv4和IPv6报文，对于ARP等非IP报文，IPSG不做匹配检查。

IPSG原理图如图13-2所示，非法主机仿冒合法主机的IP地址发送报文到达Switch后，因报文和绑定表不匹配被Switch丢弃。

图 13-2 IPSG 实现原理图



IPSG 中的接口角色

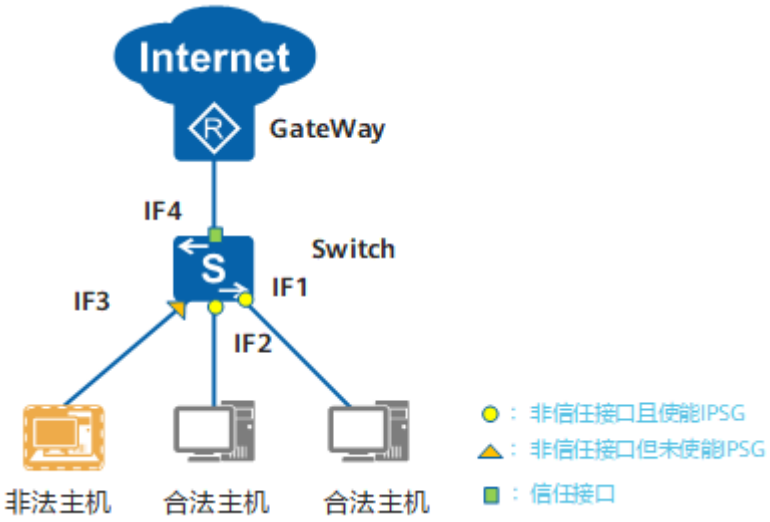
IPSG仅支持在二层物理接口或者VLAN上应用，且只对使能了IPSG功能的非信任接口进行检查。对于IPSG来说，缺省所有的接口均为非信任接口，信任接口由用户指定。IPSG的信任接口/非信任接口也就是DHCP Snooping或ND Snooping中的信任接口/非信任接口，信任接口/非信任接口同样适用于基于静态绑定表方式的IPSG。

IPSG中各接口角色如图13-3所示。其中：

- IF1和IF2接口为非信任接口且使能IPSG功能，从IF1和IF2接口收到的报文会执行IPSG检查。

- IF3接口为非信任接口但未使能IPSG功能，从IF3接口收到的报文不会执行IPSG检查，可能存在攻击。
- IF4接口为用户指定的信任接口，从IF4接口收到的报文也不会执行IPSG检查，但此接口一般不存在攻击。在DHCP Snooping的场景下，通常把与合法DHCP服务器直接或间接连接的接口设置为信任接口。

图 13-3 IPSG 中的接口角色示意图



IPSG 的过滤方式

静态绑定表项包含：MAC地址、IP地址、VLAN ID、入接口。静态绑定表项中指定的信息均用于IPSG过滤接口收到的报文。

动态绑定表项包含：MAC地址、IP地址、VLAN ID、入接口。IPSG依据该表项中的哪些信息过滤接口收到的报文，由用户设置的检查项决定，缺省是四项都进行匹配检查。常见的几种检查项如表13-2所示，其他组合类似，不一一列举。

表 13-2 IPSG 过滤方式

设置的检查项	含义
基于源IP地址过滤	根据源IP地址对报文进行过滤，只有源IP地址和绑定表匹配，才允许报文通过。
基于源MAC地址过滤	根据源MAC地址对报文进行过滤，只有源MAC地址和绑定表匹配，才允许报文通过。
基于源IP地址+源MAC地址过滤	根据源IP和源MAC地址对报文进行过滤，只有源IP和源MAC地址都和绑定表匹配，才允许报文通过。
基于源IP地址+源MAC地址+接口过滤	根据源IP地址、源MAC地址和接口对报文进行过滤，只有源IP、源MAC地址和接口都和绑定表匹配，才允许报文通过。

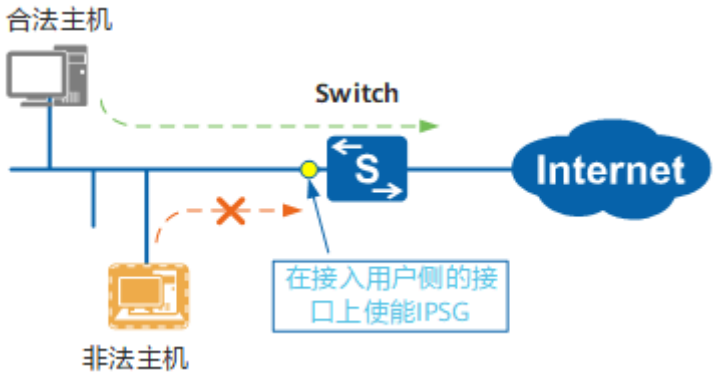
设置的检查项	含义
基于源IP地址+源MAC地址+接口+VLAN过滤	根据源IP地址、源MAC地址、接口和VLAN对报文进行过滤，只有源IP地址、源MAC地址、接口和VLAN都和绑定表匹配，才允许报文通过。

13.2.2 IPSG 应用在网络中的位置

IPSG一般应用在与用户直连的接入设备上，可以基于接口或者基于VLAN应用。

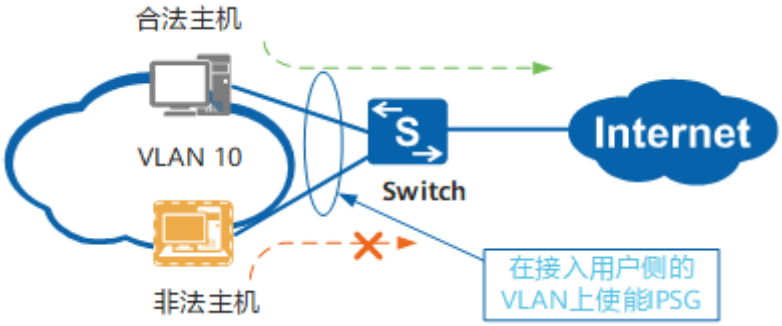
- 如图13-4所示，在接入用户侧的接口上应用IPSG，该接口接收的所有IP报文均进行IPSG检查。

  图 13-4 基于接口使能 IPSG

- 如图13-5所示，在接入用户侧的VLAN上应用IPSG，属于该VLAN的所有接口接收到IP报文均进行IPSG检查。

  图 13-5 基于 VLAN 使能 IPSG

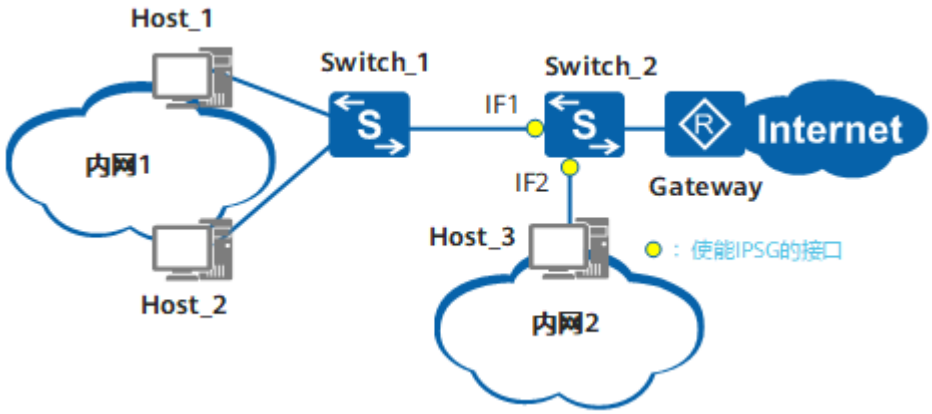
如果与用户直连的接入设备不支持IPSG功能，也可以在汇聚设备或核心设备上应用IPSG，如图13-6所示。

- 假设接入内网1的Switch_1不支持IPSG功能，可以在Switch_2上的IF1接口应用IPSG（需要在Switch_2上创建内网1内主机的绑定表）。但是由于Switch_1没有

IPSG功能，所以从Switch_1发送过来的报文是有可能存在IP欺骗攻击的，在Switch_2的IF1接口上应用IPSG可以把攻击隔绝在这里，使受攻击的范围减小到最小。

- 接入内网2的Switch_2的IF2接口上也需要应用IPSG功能，如果不应用，内网2内也可能存在IP地址欺骗攻击。

图 13-6 多交换机环境



13.2.3 IPSG 与其他相关特性的比较

IPSG、动态ARP检测DAI（Dynamic ARP Inspection）、静态ARP、端口安全都是提高网络安全的技术，以下分别介绍**IPSG与DAI**、**IPSG与静态ARP**、**IPSG与端口安全**的主要区别。

IPSG 与 DAI

IPSG和DAI都是利用绑定表（静态绑定表或者DHCP Snooping绑定表）实现对报文过滤的技术。它们的主要区别如**表13-3**所示。

表 13-3 IPSG 与 DAI 的区别

特性	功能介绍	应用场景
IPSG	利用绑定表对IP报文进行过滤。设备会匹配检查接口上接收到的IP报文，只有匹配绑定表的IP报文才允许通过。	防止IP地址欺骗攻击。如防止非法主机盗用合法主机的IP地址，非法获取上网权限或者攻击网络。
DAI	利用绑定表对ARP报文进行过滤。设备会匹配检查接口上接收到的ARP报文，只有匹配绑定表的ARP报文才允许通过。	防御中间人攻击。中间人通过ARP欺骗，引导流量从自己这里经过，从而可以截获他人信息。

另外，IPSG无法避免地址冲突。例如，当非法主机在合法主机在线时盗用其IP地址，非法主机发送的ARP请求会广播到合法主机，从而产生地址冲突。所以，为了避免IP地址冲突，可以在部署IPSG的同时配置DAI。

有关DAI的详细介绍，请参见**ARP安全配置**。

IPSG 与静态 ARP

IPSG（指基于静态绑定表的IPSG）和静态ARP都可以实现IP和MAC的绑定，它们的主要区别如**表13-4**所示。

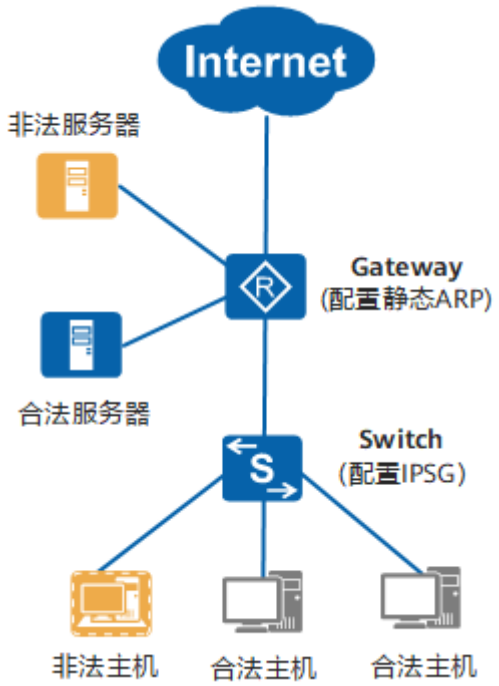
表 13-4 IPSG 和静态 ARP 的区别

特性	功能介绍	应用场景
IPSG	通过静态绑定表固定IP地址和MAC地址之间映射关系，设备会匹配检查接口上接收到的报文，只有匹配绑定表报文才允许通过。	一般部署在与用户直连的接入设备（也可以是汇聚或者核心设备）上，防止内网中的IP地址欺骗攻击，如非法主机仿冒合法主机的IP地址获取上网权限。
静态ARP	通过静态ARP表固定IP地址和MAC地址之间映射关系，静态ARP表项不会被动态刷新，设备根据静态ARP表转发接收到的报文。	一般部署在网关上，配置重要服务器的静态ARP表项，防止ARP欺骗攻击，保证主机和服务器之间的正常通信。

举例说明IPSG和静态ARP的应用，如**图13-7**所示。

- 通过在Switch上配置IPSG，防止非法主机随意更改IP地址、仿冒合法主机取得上网权限。
- 通过在Gateway上配置服务器的静态ARP表项，防止非法服务器的ARP攻击、错误刷新ARP表项，导致主机无法和合法服务器通信。

图 13-7 IPSG 和静态 ARP 的应用组网图



IPSG和静态ARP的功能区别如下：

- **静态ARP防止不了IP地址欺骗攻击**

  假设Switch上未配置IPSG，而是在网关上配置了主机的静态ARP。当非法主机仿冒合法主机的IP地址访问Internet，报文转发过程如下：

  a. 非法主机发送的报文到达Switch。
  b. Switch将报文转发到Gateway。
  c. Gateway将报文发往Internet。
  d. Internet回程报文到达Gateway。
  e. Gateway根据目的IP地址（即仿冒的合法主机的IP地址）查找静态ARP表项，这个IP对应的MAC为合法主机的MAC，Gateway将封装后的报文发送给Switch。
  f. Switch根据目的MAC地址将报文转发到合法主机。

  从过程来看，如果伪造的是合法主机的IP地址，配置静态ARP也能防止非法主机更改IP地址上网，但是会导致合法主机收到大量非法回应报文。如果合法主机在线时，非法主机不断构造并发送这种报文，则会对合法主机造成攻击。

  如果非法主机仿冒的IP地址是一个未使用的IP地址，并且这个IP地址没有被添加到静态ARP表中，则会仿冒成功，回程报文可以到达非法主机。如果是希望通过配置静态ARP来防止主机仿冒IP，那就需要把所有的IP（包括未使用的IP）都添加到静态ARP表项中，这样配置工作量会很大。

  另外，因为是在网关上配置的静态ARP，所以Switch所连接的网络内是存在IP欺骗攻击的，这个无法避免。

  所以，如果是为了防止内网中的IP地址欺骗的攻击行为，建议在Switch上配置IPSG更为合适。

- **IPSG防止不了ARP欺骗攻击**

  假设Switch上配置了IPSG，而网关上未配置主机的静态ARP。

  a. 非法主机伪造了合法主机的IP地址发送了虚假的ARP请求报文到达Switch。
  b. Switch会转发到Gateway，导致Gateway将合法主机的ARP表项刷新成错误的表项（IP为合法主机的IP，MAC为非法主机的MAC）。
  c. 当合法主机访问Internet，Internet回程报文将被转发到非法主机，导致合法主机也上不了网。

     而且，从Internet主动发给合法主机的报文也会被非法主机截获，无法正常发送到合法主机。

  为了解决这个问题，一种方法是在网关上同时配置主机的静态ARP，但是对于主机规模较大的场景下配置和维护会非常复杂。另一种方法是在Switch上同时配置DAI功能，Switch对于接口上收到的ARP报文也会匹配绑定表，对于非法的ARP报文同样会因与绑定表不匹配而被Switch丢弃。非法ARP报文到达不了网关，也就更改不了ARP表项。

有关静态ARP的详细介绍，请参见《S600-E V200R021C00, C01 配置指南-IP业务》ARP配置。

IPSG 与端口安全

IPSG（指基于静态绑定表的IPSG）和端口安全都可以实现MAC地址和接口的绑定，它们的主要区别如**表13-5**所示。

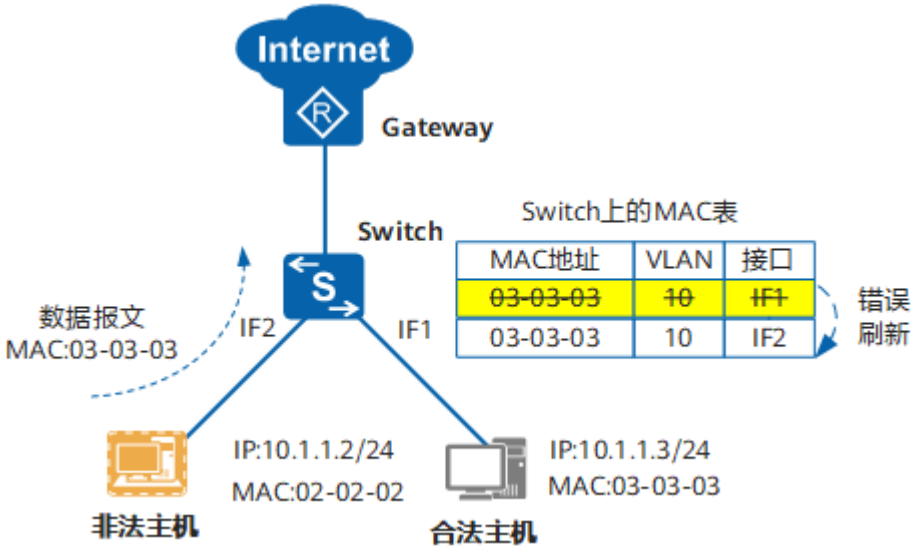
表 13-5 IPSG 与端口安全的区别

特性	功能介绍	应用场景
IPSG	通过在绑定表中固定MAC和接口的绑定关系，实现固定主机只能从固定接口上线，并且绑定表以外的非法MAC主机无法通过设备通信。 绑定表项需要手工配置，如果主机较多，配置工作量比较大。	绑定MAC和接口只是IPSG的一部分功能，IPSG能实现IP地址、MAC地址、VLAN和接口之间的任意绑定。它主要用来防止IP地址欺骗攻击，如防止非法主机盗用合法主机的IP地址，非法获取上网权限或者攻击网络。
端口安全	通过将接口学习到的指定数量的动态MAC地址转换为安全MAC地址，以固定MAC表项，实现固定主机只能从固定接口上线，并且MAC表以外的非法MAC主机无法通过设备通信。 安全MAC地址是动态生成的，无需手工配置。	防止非法主机接入，还可以控制接入主机的数量，比较适合于主机较多的场景。

因此，如果只是希望阻止非法MAC通过设备通信，并且在主机较多的环境下，配置端口安全更合适。

另外，IPSG不会固定MAC表项，无法防止MAC表被错误刷新而产生MAC漂移问题。如图13-8所示，非法主机伪造合法主机的MAC地址发送数据（例如发送伪造的ARP报文）到达Switch，会错误刷新MAC表，导致非法主机截获发往合法主机的报文。

图 13-8 MAC 表错误刷新示意图



此时，可设置根据绑定表生成Snooping类型的MAC表项（也是一种安全MAC），解决上述问题。

有关端口安全的详细介绍，请参见**端口安全配置**。

由此可见，IPSG、DAI、静态ARP、端口安全是针对不同需求的，它们都有自己独特的价值。为了网络更加安全，建议综合考虑，灵活应用。

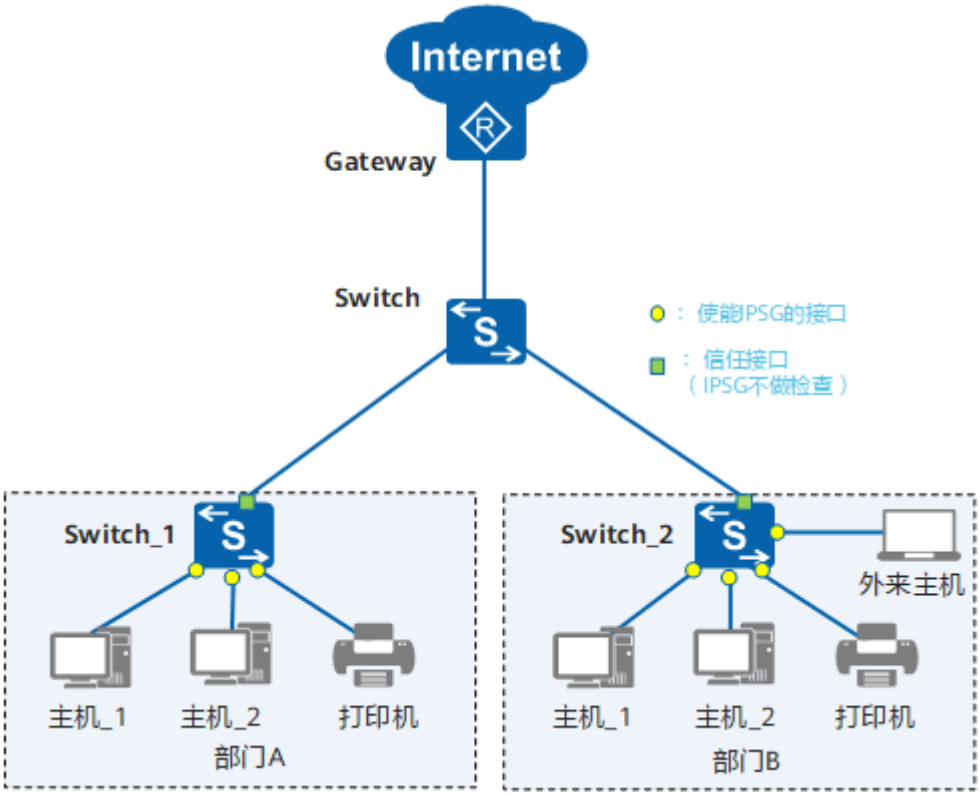
13.3 IPSG 应用场景

某园区网如图13-9所示，针对不同的园区，可能会有不同地址规划。一般情况下：

- 在园区规模较小时，园区内主机和打印机会使用静态的IP地址；
- 在园区规模稍大时，园区内主机会通过DHCP方式获取IP地址，而部分打印机等使用静态的IP地址。

在园区网接入用户的交换机（图中的Switch_1、Switch_2）上部署IPSG，实现如下场景应用。

图 13-9 IPSG 典型应用组网图



场景 1：通过 IPSG 防止主机私自更改 IP 地址

- 主机只能使用DHCP Server分配的IP地址或者管理员配置的静态地址，随意更改IP地址后无法访问网络，防止主机非法取得上网权限。
- 打印机配置的静态IP地址只供打印机使用，防止主机通过仿冒打印机的IP地址访问网络。

场景 2：通过 IPSG 限制非法主机接入（针对 IP 地址是静态分配的环境）

- 固定的主机只能从固定的接口接入，不能随意更换接入位置，满足基于接口限速的目的。
- 外来人员自带电脑不能随意接入内网，防止内网资源泄露。

对于IP地址是DHCP动态分配的环境，一般是通过NAC认证（比如Portal认证或802.1X认证等）功能实现限制非法主机接入。

13.4 IPSG 配置任务概览

IPSG的配置任务如表13-6所示。各任务之间相互独立，请根据需要选择其一或进行组合配置。

表 13-6 IPSG 配置任务简介

场景	描述	对应任务
配置基于静态绑定表的IPSG	对于局域网络中主机数较少且主机使用静态配置IP地址的网络环境，通过配置基于静态绑定表的IPSG，对非信任接口上接收的IP报文进行过滤控制，可以有效防止恶意主机盗用合法主机的IP地址来仿冒合法主机，获取网络资源的使用权限。	13.7.1 配置基于静态绑定表的IPSG
配置基于动态绑定表的IPSG	对于局域网络中主机较多，或者主机使用DHCP动态获取IP地址的网络环境，通过配置基于动态绑定表的IPSG，对非信任接口上接收的IP报文进行过滤控制，可以有效防止恶意主机盗用合法主机的IP地址来仿冒合法主机，获取网络资源的使用权限。	13.7.2 配置基于动态绑定表的IPSG
配置根据绑定表生成Snooping类型的MAC表项	配置基于静态绑定表或者动态绑定表的IPSG功能后，能有效防止非法MAC的主机访问网络，但无法防止MAC表被错误学习及刷新，产生MAC漂移等问题。 通过配置此功能关闭接口的MAC学习，由绑定表生成Snooping类型MAC表项，有效避免上述问题。	13.7.3 配置根据绑定表生成Snooping类型的MAC表项

13.5 IPSG 配置注意事项

涉及网元

无需其他网元配合。

License 支持

本特性是交换机的基本特性，无需获得License许可即可应用此功能。

V200R021C00、V200R021C01 版本特性支持情况

S600-E系列交换机中所有款型均支持IPSG。

说明

如需了解交换机软件配套详细信息，请点击**Info-Finder**。

特性依赖和限制

无

13.6 IPSG 缺省配置

IPSG的缺省配置如**表13-7**所示。

表 13-7 IPSG 缺省配置

参数	缺省值
IP报文检查功能	未使能
IP报文检查选项	• 基于静态绑定表：根据配置的绑定表项进行完全匹配，即绑定表项有几项，就检查几项。 • 基于动态绑定表：源IP地址、源MAC地址、接口和VLAN。
IP报文检查告警功能	未使能
IP报文检查告警阈值	100

13.7 配置 IPSG

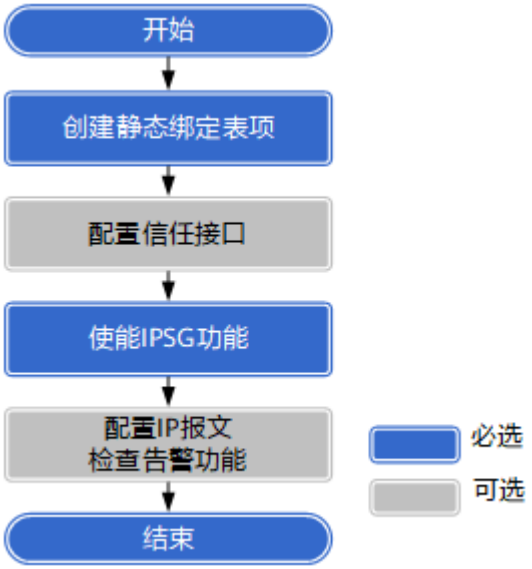
13.7.1 配置基于静态绑定表的 IPSG

背景信息

该方式适用于局域网络中主机数较少且主机使用静态配置IP地址的情况。

配置流程

图 13-10 基于静态绑定表的 IPSG 配置流程图



请在接入用户的设备上进行如下配置。

操作步骤

步骤1 创建静态绑定表项

静态绑定表项包括IPv4和IPv6两种绑定表项，请根据网络环境选择配置。

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**user-bind static** { { { **ip-address** | **ipv6-address** } { *start-ip* [**to** *end-ip*] } &<1-10> | **ipv6-prefix** *prefix/prefix-length* } | **mac-address** *mac-address* } * [**interface** *interface-type interface-number*] [**vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]]，配置静态用户绑定表项。

   缺省情况下，不存在静态绑定表。

   说明

   IPSG按照静态绑定表项进行完全匹配，即静态绑定表项包含几项就检查几项。请确保所创建的绑定表是正确且完整的，主机发送的报文只有匹配绑定表才会允许通过，不匹配绑定表的报文都将被丢弃。

   设备支持将多个IP地址（段）做批量绑定，例如多个IP批量绑定到同一个接口或同一个MAC。

   - 如果这些IP地址不是连续的，可以重复输入1～10个*start-ip*地址。例如执行命令**user-bind static ip-address 192.168.1.2 192.168.1.5 192.168.1.12 interface gigabitethernet 0/0/1**，将多个IP地址绑定到同一个接口。
   - 如果这些IP地址是连续的，可以重复输入1～10个*start-ip* **to** *end-ip*的地址段。需要注意的是，采用关键字to输入的区间不能有交叉。例如执行命令**user-bind static ip-address 172.16.1.1 to 172.16.1.4 mac-address xxxx-xxxx-xxx1**，将多个IP地址绑定到同一个MAC地址。

如果绑定表创建错误或者已绑定主机的网络权限变更，需要删除某些静态表项，请执行命令**undo user-bind static** [{ **ip-address** { *start-ip* [**to** *end-ip*] } &<1-10> | **ipv6-address** [*start-ip* [**to** *end-ip*]] &<1-10> | **ipv6-prefix** [*prefix/prefix-length*] } | **mac-address** *mac-address* | **interface** *interface-type interface-number* | **vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]] *。

步骤2 （可选）配置信任接口

主机是静态地址分配的环境，一般不需要配置信任接口。但当上行接口同时在使能IPSG功能的VLAN内，则需要将上行口配置成信任接口，否则回程报文会因匹配不到绑定表而被丢弃，导致业务不通。故障详述请参见**13.10.3 IPSG中未配置上行信任接口导致业务不通**。配置为信任接口后，从信任接口收到的报文不做匹配检查直接允许通过，可以避免上述问题的发生。

1. 执行命令**dhcp enable**，全局使能DHCP功能。

   缺省情况下，没有全局使能DHCP功能。

2. 执行命令**dhcp snooping enable**，全局使能DHCP Snooping功能。

   缺省情况下，没有全局使能DHCP Snooping功能。

3. 在接口视图下执行命令**dhcp snooping trusted**，或在VLAN视图中执行**dhcp snooping trusted interface** *interface-type interface-number*，配置接口为信任状态。

   缺省情况下，接口为未信任状态。

步骤3 使能IPSG功能

绑定表创建后，IPSG并未生效，只有在指定接口（接入用户侧的接口）或在指定VLAN上使能IPSG后才生效。以下两种方式二选一。

- 基于接口使能IPSG：该接口接收的所有的报文均进行IPSG检查。如果用户只希望在某些不信任的接口上进行IPSG检查，而信任其他接口，可以选择此方式。并且，当接口属于多个VLAN时，基于接口使能IPSG更方便，无需在每个VLAN上使能。
- 基于VLAN使能IPSG：属于该VLAN的所有接口接收的报文均进行IPSG检查。如果用户只希望在某些不信任VLAN上进行IPSG检查，而信任其他VLAN，可以选择此方式。并且，当多个接口属于相同的VLAN时，基于VLAN使能IPSG更方便，无需在每个接口上使能。

说明

- 接口上使能仅对该接口生效，其它接口不会执行IPSG检查。
- VLAN上使能仅对该VLAN生效，其它VLAN不会执行IPSG检查。
- 设备ACL资源不足时可能会导致绑定表下发失败，但是设备可以查看到IPSG相关配置，此时需要通过命令行**display dhcp static user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } **verbose**回显中的IPSG Status字段确认IPSG功能是否生效。

1. 进入接口或VLAN视图。
   - 执行命令**interface** *interface-type interface-number*，进入接口视图。
   - 执行命令**vlan** *vlan-id*，进入VLAN视图。
2. 执行命令**ip source check user-bind enable**、**ipv4 source check user-bind enable**或者**ipv6 source check user-bind enable**，使能接口或者VLAN的IP报文检查功能。

   缺省情况下，接口和VLAN上未使能IP报文检查功能。

步骤4 （可选）配置IP报文检查告警功能

仅当**步骤3**中基于接口或VLAN使能IPSG，本步骤才生效。配置了IP报文检查告警功能后，当丢弃的IP报文超过告警阈值时，会产生告警提醒用户。

1. 执行命令**system-view**，进入系统视图。
2. 进入接口或VLAN视图
   - 执行命令**interface** *interface-type interface-number*，进入接口视图。
   - 执行命令**vlan** *vlan-id*，进入VLAN视图。
3. 执行命令**ip source check user-bind alarm enable**，使能IP报文检查告警功能。

   缺省情况下，未使能IP报文检查告警功能。
4. 执行命令**ip source check user-bind alarm threshold** *threshold*，配置IP报文检查告警阈值。

   缺省情况下，IP报文检查告警阈值为100。

----结束

检查配置结果

- 查看指定接口的IPSG配置

  执行命令**display ip source check user-bind interface** *interface-type interface-number*，查看接口下IPSG的配置信息。
- 查看生成的静态绑定表项及状态

  执行命令**display dhcp static user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**]，查看IPv4静态绑定表信息。

  执行命令**display dhcpv6 static user-bind** { { **interface** *interface-type interface-number* | **ipv6-address** { *ipv6-address* | **all** } | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**]，查看IPv6静态绑定表信息。

  带**verbose**参数可以查看到IPSG的状态。
  - 如果IPSG Status显示为“IPv4 effective”或者“IPv6 effective”，表示该条表项的IPSG已生效。
  - 如果IPSG Status显示为“ineffective”，表示该条表项的IPSG未生效，这可能因硬件ACL资源不足导致。

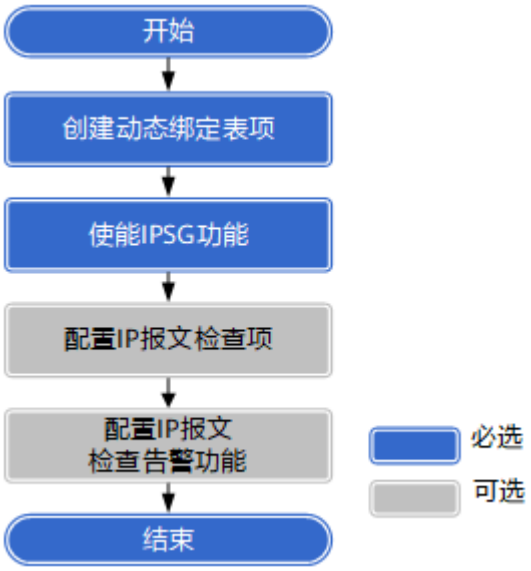
13.7.2 配置基于动态绑定表的 IPSG

背景信息

该方式适用于局域网络中主机较多，或者主机使用DHCP动态获取IP地址的情况。

配置流程

图 13-11 基于动态绑定表的 IPSG 配置流程图



请在接入用户的设备上进行如下配置。

操作步骤

步骤1 创建动态绑定表项

动态绑定表项包括IPv4和IPv6两种绑定表项，请根据网络环境选择配置。

- 通过DHCP方式获取IP地址的IPv4或者IPv6主机，可以配置DHCP Snooping生成DHCP Snooping动态绑定表项
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**dhcp enable**，使能DHCP功能。
     缺省情况下，未使能DHCP功能。
  c. 执行命令**dhcp snooping enable**，全局使能DHCP Snooping功能。
     缺省情况下，全局未使能DHCP Snooping功能。
  d. 进入VLAN或者接口视图。
     - 执行命令**vlan** *vlan-id*，进入VLAN视图。
     - 执行命令**interface** *interface-type interface-number*，进入接口视图。
  e. 执行命令**dhcp snooping enable**，使能VLAN或者接口的DHCP Snooping功能。
     缺省情况下，VLAN和接口下未使能DHCP Snooping功能。
  f. 配置信任接口，以下任务二选一。
     - 在VLAN视图下执行命令**dhcp snooping trusted interface** *interface-type interface-number*，配置加入该VLAN的接口为信任状态。

- 在接口视图下执行命令**dhcp snooping trusted**，配置该接口为信任状态。

缺省情况下，使能DHCP Snooping功能后，接口为非信任状态。

说明

一般将与DHCP服务器直接或间接相连的接口配置为信任接口，IPSG对于从信任接口收到的报文不做匹配检查，直接允许通过。

有关DHCP Snooping的详细配置，请参见**9 DHCP Snooping配置**。

- 通过静态方式获取IP地址的IPv4或者IPv6主机，如果网络中部署了802.1X认证功能，可以配置生成静态主机的DHCP Snooping动态绑定表项

  该方式生成的表项可能不可靠，建议配置静态绑定表。

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**dhcp enable**，使能DHCP功能。

     缺省情况下，未使能DHCP功能。
  c. 执行命令**dhcp snooping enable**，全局使能DHCP Snooping功能。

     缺省情况下，全局未使能DHCP Snooping功能。
  d. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  e. 执行命令**dhcp snooping enable**，使能接口的DHCP Snooping功能。

     缺省情况下，接口下未使能DHCP Snooping功能。
  f. 执行命令**dot1x trigger dhcp-binding**（传统模式）或者**dot1x trigger dhcp-binding**（统一模式），配置静态主机802.1X认证成功后，设备自动生成对应的DHCP Snooping绑定表。

     传统模式下配置该功能前，必须已经通过命令**dot1x enable**使能了全局和接口的802.1X认证功能。

     缺省情况下，静态主机802.1X认证成功后，设备不会自动生成对应的DHCP Snooping绑定表。

  有关802.1X认证的相关配置，请参见《S600-E V200R021C00, C01 配置指南-用户接入与认证》 NAC配置（传统模式） 或 NAC配置（统一模式）。

- 对于IPv6主机，也可以配置ND Snooping功能生成ND Snooping动态绑定表项

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**nd snooping enable**，全局使能ND Snooping功能。

     缺省情况下，全局未使能ND Snooping功能。
  c. 进入VLAN或者接口视图。
     i. 执行命令**vlan** *vlan-id*，进入VLAN视图。
     ii. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  d. 执行命令**nd snooping enable**，使能VLAN或者接口的ND Snooping功能。

     缺省情况下，VLAN和接口下未使能ND Snooping功能。
  e. 配置信任接口，以下任务二选一。
     i. 在VLAN视图下执行命令**nd snooping trusted interface** *interface-type interface-number*，配置加入该VLAN的接口为ND Snooping信任接口。
     ii. 在接口视图下执行命令**nd snooping trusted**，配置接口为ND Snooping信任接口。

     缺省情况下，使能ND Snooping功能后，所有接口为非信任状态。

有关ND Snooping的详细配置，请参见**10 ND Snooping配置**。

步骤2 使能IPSG功能

绑定表创建后，IPSG并未生效，只有在指定接口（接入用户侧的接口）或在指定VLAN上使能IPSG后才生效。以下两种方式二选一。

- 基于接口使能IPSG：该接口接收的所有的报文均进行IPSG检查。如果用户只希望在某些不信任的接口上进行IPSG检查，而信任其他接口，可以选择此方式。并且，当接口属于多个VLAN时，基于接口使能IPSG更方便，无需在每个VLAN上使能。
- 基于VLAN使能IPSG：属于该VLAN的所有接口接收的报文均进行IPSG检查。如果用户只希望在某些不信任VLAN上进行IPSG检查，而信任其他VLAN，可以选择此方式。并且，当多个接口属于相同的VLAN时，基于VLAN使能IPSG更方便，无需在每个接口上使能。

说明

- 接口上使能仅对该接口生效，其它接口不会执行IPSG检查。
- VLAN上使能仅对该VLAN生效，其它VLAN不会执行IPSG检查。
- 设备ACL资源不足时可能会导致绑定表下发失败，但是设备可以查看到IPSG相关配置，此时需要通过命令行**display dhcp snooping user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } **verbose**回显中的IPSG Status字段确认IPSG功能是否生效。

1. 进入接口或VLAN视图。
   - 执行命令**interface** *interface-type interface-number*，进入接口视图。
   - 执行命令**vlan** *vlan-id*，进入VLAN视图。
2. 执行命令**ip source check user-bind enable**、**ipv4 source check user-bind enable**或者**ipv6 source check user-bind enable**，使能接口或者VLAN的IP报文检查功能。

   缺省情况下，接口和VLAN上未使能IP报文检查功能。

步骤3 （可选）配置IP报文检查项

- 如果基于VLAN使能IPSG，在VLAN视图下执行命令**ip source check user-bind check-item** { **ip-address** | **mac-address** | **interface** } *，配置IP报文检查项。
- 如果基于接口使能IPSG，在接口视图下执行命令**ip source check user-bind check-item** { **ip-address** | **mac-address** | **vlan** } *，配置IP报文检查项。

缺省情况下，IP报文检查项包括IP地址、MAC地址、VLAN和接口。如果用户信任某些检查项，或者某些项目不固定（例如客户端的流量可能从不同的接口进入设备），可以选择配置此步骤。一般采用缺省值。

步骤4 （可选）配置IP报文检查告警功能

仅当**步骤2**中基于接口使能IPSG，本步骤才生效。配置此功能后，当丢弃的IP报文超过告警阈值时，会产生告警提醒用户。

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**interface** *interface-type interface-number*，进入接口视图。
3. 执行命令**ip source check user-bind alarm enable**，使能IP报文检查告警功能。

   缺省情况下，没有使能IP报文检查告警功能。
4. 执行命令**ip source check user-bind alarm threshold** *threshold*，配置IP报文检查告警阈值。

缺省情况下，IP报文检查告警阈值为100。

----结束

检查配置结果

- 查看指定接口的IPSG配置

  执行命令**display ip source check user-bind interface** *interface-type interface-number*，查看接口下IPSG的配置信息。

- 查看生成的动态绑定表项及状态
  - 执行命令**display dhcp snooping user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**]，查看DHCP Snooping动态绑定表信息。
  - 执行命令**display dhcpv6 snooping user-bind** { { **interface** *interface-type interface-number* | **ipv6-address** { *ipv6-address* | **all** } | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**]，查看DHCPv6 Snooping动态绑定表信息。
  - 执行命令**display nd snooping user-bind all** [**verbose**]或**display nd snooping user-bind** { **ipv6-address** *ipv6-address* | **mac-address** *mac-address* | **interface** *interface-type interface-number* | **vlan** *vlan-id* } * [**verbose**]，查看ND Snooping动态绑定表信息。

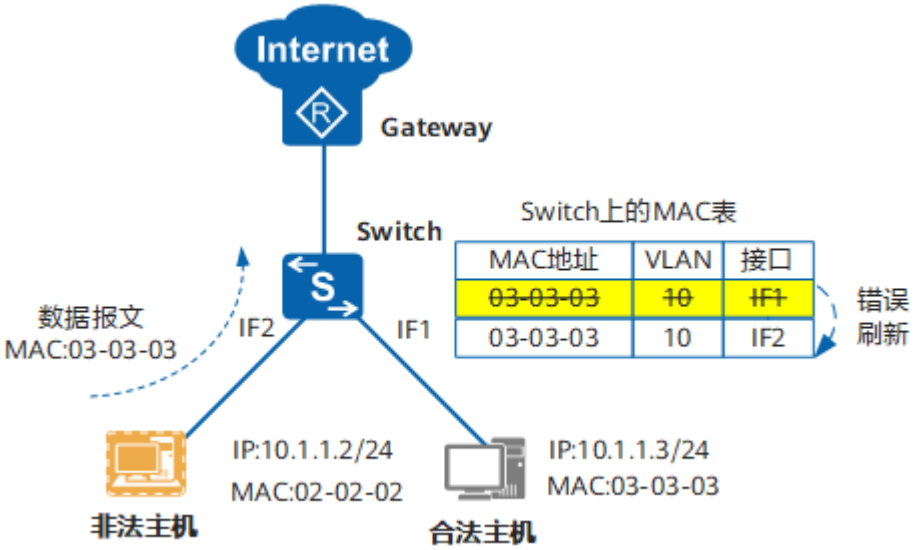
  带**verbose**参数可以查看到IPSG的状态。
  - 如果IPSG Status显示为“IPv4 effective”或者“IPv6 effective”，表示该条表项的IPSG已生效。
  - 如果IPSG Status显示为“ineffective”，表示该条表项的IPSG未生效，这可能因硬件ACL资源不足导致。

13.7.3 配置根据绑定表生成 Snooping 类型的 MAC 表项

背景信息

配置基于绑定表的IPSG能防止非法MAC的主机访问网络，但无法防止MAC表被错误刷新而产生的MAC漂移问题。如图13-12所示，非法主机伪造合法主机的MAC地址发送数据（例如发送伪造的ARP报文）到达交换机，会错误刷新MAC表，导致非法主机截获发往合法主机的报文。

图 13-12 MAC 表错误刷新示意图



通过配置此功能关闭该接口动态学习MAC表项的能力，并使设备可根据绑定表生成Snooping类型MAC表项，可以解决以上问题。

该功能与以下功能点冲突，请不要同时配置。

功能描述	命令
使能接口802.1X功能	**dot1x enable**
使能接口MAC地址认证功能	**mac-authen**
配置MAC地址学习功能	**mac-address learning disable**
配置MAC地址学习最大数量	**mac-limit**
配置VLAN Mapping功能	**port vlan-mapping vlan map-vlan**
配置接口安全功能	**port-security enable**

前置任务

在配置此功能之前，需要完成以下任务：

- 创建静态绑定表或动态绑定表。

  说明

  创建静态绑定表时，必须至少同时指定MAC地址、VLAN和接口三个参数且指定的VLAN必须已经创建，设备才能根据静态绑定表生成Snooping类型的MAC表项。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**user-bind ip sticky-mac**，使能根据绑定表生成Snooping类型MAC表项功能。

缺省情况下，未使能根据绑定表生成Snooping类型MAC表项功能。

----结束

检查配置结果

执行命令**display mac-address snooping** [*interface-type interface-number* | **vlan** *vlan-id*] * [**verbose**]，查看根据绑定表生成的Snooping类型MAC表项。

13.8 维护 IPSG

维护IPSG的相关操作如**表13-8**所示。

表 13-8 维护 IPSG

操作	命令
查看静态绑定表信息	**display dhcp static user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**] 指定**verbose**参数，可以查看绑定表项对应的IPSG的生效状态。
查看DHCP Snooping动态绑定表信息	**display dhcp snooping user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* }* | **all** } [**verbose**] 指定**verbose**参数，可以查看绑定表项对应的IPSG的生效状态。
查看ND Snooping动态绑定表信息	**display nd snooping user-bind all** [**verbose**]或**display nd snooping user-bind** { **ipv6-address** *ipv6-address* | **mac-address** *mac-address* | **interface** *interface-type interface-number* | **vlan** *vlan-id* }* [**verbose**] 指定**verbose**参数，可以查看绑定表项对应的IPSG的生效状态。

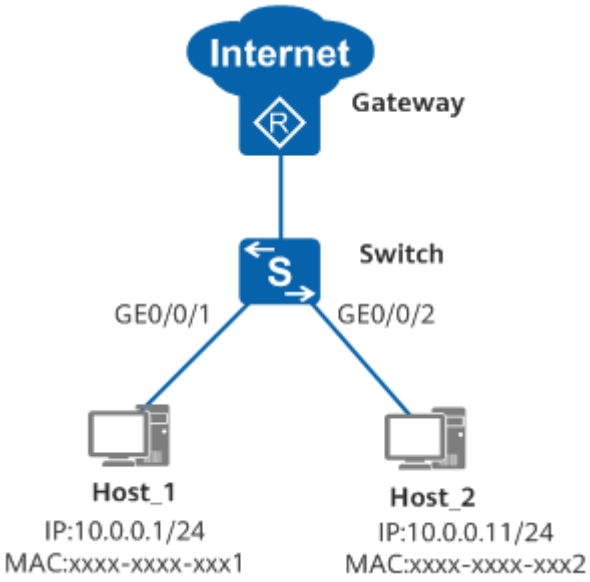
13.9 IPSG 配置举例

13.9.1 配置 IPSG 防止主机私自更改 IP 地址示例（静态绑定）

组网需求

如图13-13所示，Host通过Switch接入网络，Gateway为企业出口网关，各Host均使用静态配置的IP地址。管理员希望Host使用管理员分配的固定IP地址上网，不允许私自更改IP地址非法获取网络访问权限。

图 13-13 配置 IPSG 防止主机私自更改 IP 地址（静态绑定）组网图



配置思路

采用如下的思路在Switch上配置IPSG功能，实现上述需求。

1. 在Switch上配置Host_1和Host_2的静态绑定表，固定IP和MAC的绑定关系。
2. 在Switch连接用户主机的接口使能IPSG，实现Host只能使用管理员分配的固定IP地址上网。同时，在接口开启IP报文检查告警功能，当交换机丢弃非法上网用户的报文达到阈值后上报告警。

操作步骤

步骤1 创建Host_1和Host_2的静态绑定表项

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] user-bind static ip-address 10.0.0.1 mac-address xxxx-xxxx-xxx1
[Switch] user-bind static ip-address 10.0.0.11 mac-address xxxx-xxxx-xxx2
```

步骤2 使能IPSG并设置丢弃报文上报告警功能

在连接Host_1的GE0/0/1接口使能IPSG和IP报文检查告警功能，当丢弃报文阈值到达200将上报告警。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] ip source check user-bind enable
[Switch-GigabitEthernet0/0/1] ip source check user-bind alarm enable
[Switch-GigabitEthernet0/0/1] ip source check user-bind alarm threshold 200
[Switch-GigabitEthernet0/0/1] quit
```

在连接Host_2的GE0/0/2接口使能IPSG和IP报文检查告警功能，当丢弃报文阈值到达200将上报告警。

```
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] ip source check user-bind enable
[Switch-GigabitEthernet0/0/2] ip source check user-bind alarm enable
[Switch-GigabitEthernet0/0/2] ip source check user-bind alarm threshold 200
[Switch-GigabitEthernet0/0/2] quit
```

步骤3 验证配置结果

在Switch上执行**display dhcp static user-bind all**命令，可以查看静态绑定表信息。

```
[Switch] display dhcp static user-bind all
DHCP static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address                MAC Address     VSI/VLAN(O/I/P) Interface
--------------------------------------------------------------------------------
10.0.0.1                  xxxx-xxxx-xxx1  --  /--  /--    --
10.0.0.11                 xxxx-xxxx-xxx2  --  /--  /--    --
--------------------------------------------------------------------------------
Print count:          2         Total count:          2
```

Host_1和Host_2使用管理员分配的固定IP地址可以正常访问网络，更改IP地址后无法访问网络。

----结束

配置文件

Switch的配置文件

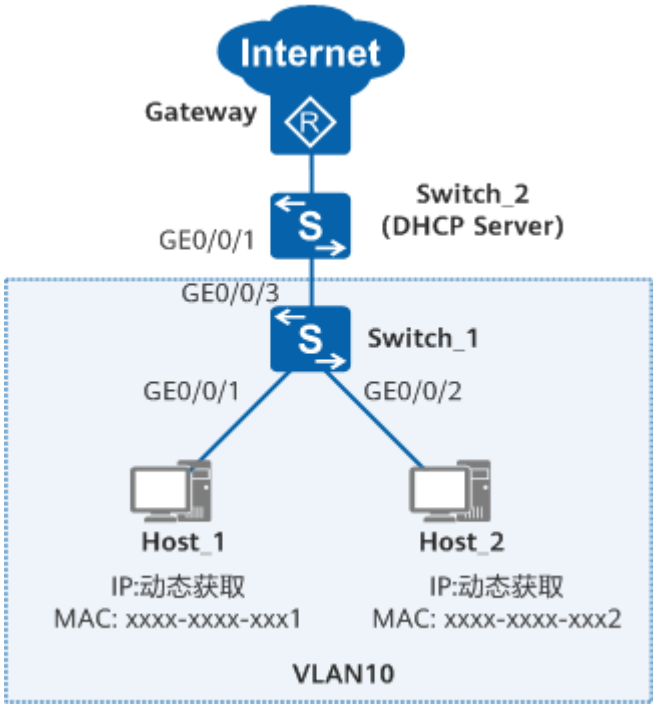
```
#
sysname Switch
#
user-bind static ip-address 10.0.0.1 mac-address xxxx-xxxx-xxx1
user-bind static ip-address 10.0.0.11 mac-address xxxx-xxxx-xxx2
#
interface GigabitEthernet0/0/1
 ipv4 source check user-bind enable
 ipv6 source check user-bind enable
 ip source check user-bind alarm enable
 ip source check user-bind alarm threshold 200
#
interface GigabitEthernet0/0/2
 ipv4 source check user-bind enable
 ipv6 source check user-bind enable
 ip source check user-bind alarm enable
 ip source check user-bind alarm threshold 200
#
return
```

13.9.2 配置 IPSG 防止主机私自更改 IP 地址示例（DHCP Snooping 动态绑定）

组网需求

如图13-14所示，Host通过Switch_1接入网络，Switch_2作为DHCP Server为Host动态分配IP地址，Gateway为企业出口网关。管理员希望Host使用动态分配的地址，不允许私自配置静态IP地址，如果私自指定IP地址将无法访问网络。

图 13-14 配置 IPSG 防止主机私自更改 IP 地址（DHCP Snooping 动态绑定）组网图



配置思路

采用如下的思路配置IPSG功能，实现上述需求。

1. 在Switch_2上配置DHCP Server功能（假设地址池为10.1.1.0/24），为Host动态分配IP地址。
2. 在Switch_1上配置DHCP Snooping功能，保证Host从合法的DHCP Server获取IP地址，同时生成DHCP Snooping动态绑定表，记录Host的IP地址、MAC地址、VLAN、接口的绑定关系。
3. 在Switch_1连接Host的VLAN上使能IPSG功能，防止Host通过私自配置IP地址的方式访问网络。

操作步骤

步骤1 在Switch_2上配置DHCP Server功能

```
<HUAWEI> system-view
[HUAWEI] sysname Switch_2
[Switch_2] vlan batch 10
[Switch_2] interface gigabitethernet 0/0/1
[Switch_2-GigabitEthernet0/0/1] port link-type trunk
[Switch_2-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[Switch_2-GigabitEthernet0/0/1] quit
[Switch_2] dhcp enable
[Switch_2] ip pool 10
[Switch_2-ip-pool-10] network 10.1.1.0 mask 24
[Switch_2-ip-pool-10] gateway-list 10.1.1.1
[Switch_2-ip-pool-10] quit
[Switch_2] interface vlanif 10
[Switch_2-Vlanif10] ip address 10.1.1.1 255.255.255.0
[Switch_2-Vlanif10] dhcp select global
[Switch_2-Vlanif10] quit
```

步骤2 在Switch_1上配置DHCP Snooping功能

配置各接口所属VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch_1
[Switch_1] vlan batch 10
[Switch_1] interface gigabitethernet 0/0/1
[Switch_1-GigabitEthernet0/0/1] port link-type access
[Switch_1-GigabitEthernet0/0/1] port default vlan 10
[Switch_1-GigabitEthernet0/0/1] quit
[Switch_1] interface gigabitethernet 0/0/2
[Switch_1-GigabitEthernet0/0/2] port link-type access
[Switch_1-GigabitEthernet0/0/2] port default vlan 10
[Switch_1-GigabitEthernet0/0/2] quit
[Switch_1] interface gigabitethernet 0/0/3
[Switch_1-GigabitEthernet0/0/3] port link-type trunk
[Switch_1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10
[Switch_1-GigabitEthernet0/0/3] quit
```

使能DHCP Snooping功能，并将连接DHCP Server的GE0/0/3接口配置为信任接口。

```
[Switch_1] dhcp enable
[Switch_1] dhcp snooping enable
[Switch_1] vlan 10
[Switch_1-vlan10] dhcp snooping enable
[Switch_1-vlan10] dhcp snooping trusted interface gigabitethernet 0/0/3
```

步骤3 在Switch_1的VLAN10上使能IPSG功能

```
[Switch_1-vlan10] ip source check user-bind enable
[Switch_1-vlan10] quit
```

步骤4 验证配置结果

Host上线后，在Switch_1上执行**display dhcp snooping user-bind all**命令，可以查看Host的动态绑定表信息。

```
[Switch_1] display dhcp snooping user-bind all
DHCP Dynamic Bind-table:Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address       MAC Address     VSI/VLAN(O/I/P) Interface      Lease
--------------------------------------------------------------------------------
10.1.1.254       xxxx-xxxx-xxx1 --  /10  /--    GE0/0/1        2014.08.17-07:3110.1.1.253       0xxxx-xxxx-xxx2
--  /10  /--    GE0/0/2        2014.08.17-07:34
--------------------------------------------------------------------------------
print count:      2     total count:      2
```

Host使用DHCP服务器动态分配的IP地址可以正常访问网络，将Host更改为与动态获得的IP地址不一样的静态IP地址后无法访问网络。

----结束

配置文件

- Switch_1的配置文件

```
#
sysname Switch_1
#
vlan batch 10
#
dhcp enable
#
dhcp snooping enable
#
vlan 10
 dhcp snooping enable
 dhcp snooping trusted interface GigabitEthernet0/0/3
 ipv4 source check user-bind enable
 ipv6 source check user-bind enable
#
```



```
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

- Switch_2的配置文件

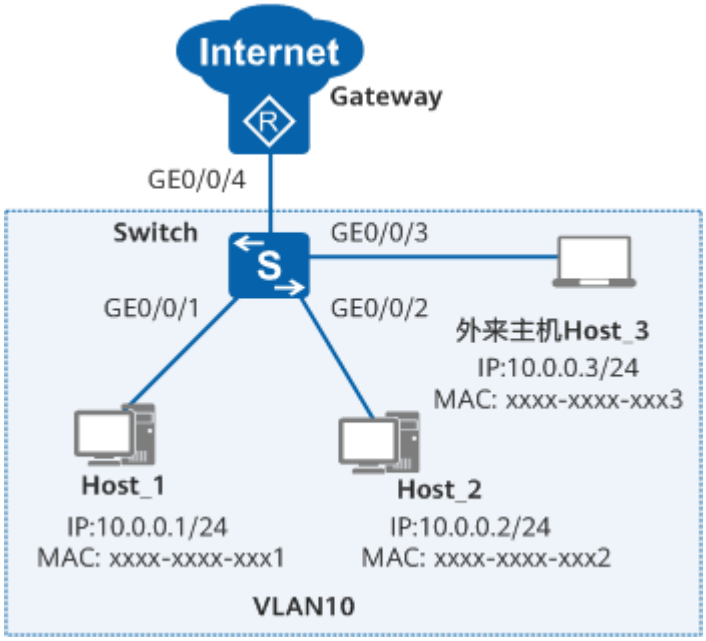
```
#
sysname Switch_2
#
vlan batch 10
#
dhcp enable
#
ip pool 10
 gateway-list 10.1.1.1
 network 10.1.1.0 mask 255.255.255.0
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

13.9.3 配置 IPSG 限制非法主机访问内网示例（静态绑定）

组网需求

如图13-15所示，Host通过Switch接入网络，Gateway为企业出口网关，各Host均使用静态配置的IP地址。管理员在Switch上做了接口限制，希望Host使用管理员分配的固定IP地址、从固定的接口上线。同时为了安全考虑，不允许外来人员的电脑随意接入内网。

图 13-15 配置 IPSG 限制非法主机访问内网（静态绑定）组网图



配置思路

采用如下的思路在Switch上配置IPSG功能，实现上述需求。

1. 在Switch上配置各接口所属VLAN。
2. 在Switch上创建Host_1和Host_2的静态绑定表项，固定IP地址、MAC地址、接口的绑定关系。
3. 在Switch上配置GE0/0/4为信任接口，从该接口收到的报文不执行IPSG检查，防止从Gateway回程报文被丢弃。
4. 在Switch连接用户主机的VLAN上使能IPSG功能，实现Host_1、Host_2使用固定的IP地址、从固定的接口上线，并且外来主机Host_3无法随意接入内网。

操作步骤

步骤1 配置各接口所属VLAN

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 10
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type access
[Switch-GigabitEthernet0/0/1] port default vlan 10
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] port link-type access
[Switch-GigabitEthernet0/0/2] port default vlan 10
[Switch-GigabitEthernet0/0/2] quit
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] port link-type access
[Switch-GigabitEthernet0/0/3] port default vlan 10
[Switch-GigabitEthernet0/0/3] quit
[Switch] interface gigabitethernet 0/0/4
[Switch-GigabitEthernet0/0/4] port link-type trunk
[Switch-GigabitEthernet0/0/4] port trunk allow-pass vlan 10
[Switch-GigabitEthernet0/0/4] quit
```

步骤2 创建Host_1和Host_2的静态绑定表项

```
[Switch] user-bind static ip-address 10.0.0.1 mac-address xxxx-xxxx-xxx1 interface gigabitethernet 0/0/1
[Switch] user-bind static ip-address 10.0.0.2 mac-address xxxx-xxxx-xxx2 interface gigabitethernet 0/0/2
```

步骤3 配置上行口GE0/0/4为信任接口

```
[Switch] dhcp enable
[Switch] dhcp snooping enable
[Switch] interface gigabitethernet 0/0/4
[Switch-GigabitEthernet0/0/4] dhcp snooping trusted
[Switch-GigabitEthernet0/0/4] quit
```

步骤4 在连接Host的VLAN10上使能IPSG功能

```
[Switch] vlan 10
[Switch-vlan10] ip source check user-bind enable
[Switch-vlan10] quit
```

步骤5 验证配置结果

在Switch上执行**display dhcp static user-bind all**命令，可以查看Host_1和Host_2的绑定表信息。

```
[Switch] display dhcp static user-bind all
DHCP static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address                MAC Address     VSI/VLAN(O/I/P) Interface
--------------------------------------------------------------------------------
10.0.0.1                  xxxx-xxxx-xxx1  --  /--  /--    GE0/0/1
10.0.0.2                  xxxx-xxxx-xxx2  --  /--  /--    GE0/0/2
--------------------------------------------------------------------------------
Print count:          2         Total count:          2
```

Host_1和Host_2可以正常访问网络，更换IP地址或者从其他接口接入后将无法访问网络。

将一台外来主机Host_3配置10.0.0.3的IP地址并接入接口GE0/0/3后，Host_3仍无法访问网络，说明外来主机不能通过随意设置IP地址访问内网。如果Host_3需要访问内网资源，需要管理员在静态绑定表中添加Host_3的表项。

----结束

配置文件

Switch的配置文件

```
#
sysname Switch
#
vlan batch 10
#
dhcp enable
#
dhcp snooping enable
user-bind static ip-address 10.0.0.1 mac-address xxxx-xxxx-xxx1 interface GigabitEthernet0/0/1
user-bind static ip-address 10.0.0.2 mac-address xxxx-xxxx-xxx2 interface GigabitEthernet0/0/2
#
vlan 10
 ipv4 source check user-bind enable
 ipv6 source check user-bind enable
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
#
```



```
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 10
 dhcp snooping trusted
#
return
```

13.10 IPSG 常见配置错误

13.10.1 接口或 VLAN 上未使能导致 IPSG 功能不生效

故障现象

已创建并生成了绑定表，但IPSG功能未能生效。

操作步骤

步骤1 检查IPSG功能是否在指定接口或者指定VLAN上使能

绑定表创建后，IPSG并未生效，只有在指定接口或在指定VLAN上使能IPSG后功能才生效。

1. 执行命令**display ip source check user-bind interface** *interface-type interface-number*，查看接入用户的接口上是否使能了IPSG。
2. 如果接口未使能IPSG，继续在VLAN视图下执行命令**display this**，查看接入用户的VLAN上是否使能了IPSG。
3. 如果接口和VLAN上均未使能IPSG功能（显示信息中无“ipv4 source check user-bind enable”或“ipv6 source check user-bind enable”），请在接口视图或者VLAN视图下执行命令**ip source check user-bind enable**，使能IPSG功能。

接口或VLAN方式只选择其一即可，两者的区别在于：

- 基于接口使能IPSG：该接口接收的所有的报文均进行IPSG检查。如果用户只希望在某些不信任的接口上进行IPSG检查，而信任其他接口，可以选择此方式。并且，当接口属于多个VLAN时，基于接口使能IPSG更方便，无需在每个VLAN上使能。
- 基于VLAN使能IPSG：属于该VLAN的所有接口接收的报文均进行IPSG检查。如果用户只希望在某些不信任VLAN上进行IPSG检查，而信任其他VLAN，可以选择此方式。并且，当多个接口属于相同的VLAN时，基于VLAN使能IPSG更方便，无需在每个接口上使能。

另外，需要注意的是，IPSG仅在使能的接口或使能的VLAN上生效，未使能的接口和VLAN上不会执行IPSG检查。所以如果是部分的接口或VLAN上IPSG不生效，很可能是这部分接口或VLAN上未使能IPSG导致的。

----结束

13.10.2 静态绑定表项错误导致合法主机上不了网

故障现象

已创建静态绑定表且使能了IPSG功能，但合法主机却上不了网。

操作步骤

步骤1 检查绑定表信息是否正确

执行命令**display dhcp static user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** }，查看静态绑定表信息。

需要上网的合法主机却上不了网，可能因为绑定表信息不正确导致。

- 如果合法主机信息不在绑定表中，请添加该主机的绑定表项。只有绑定表中存在该主机的表项，设备才允许主机的报文通过。
- 如果需要合法主机信息在绑定表中，请查看该条表项的MAC地址是否正确，是否因主机更换了网卡未及时刷新绑定表导致。如果是，请删除该条绑定表项并重新添加。
- 如果合法主机信息在绑定表中，请查看该条表项是否包含VLAN信息。如果包含VLAN信息，请执行命令**display vlan**查看主机接入的接口是否加入该VLAN中。只有该接口加入了这个VLAN，设备才允许主机的报文通过。

添加绑定表的命令为：**user-bind static** { { { **ip-address** | **ipv6-address** } { *start-ip* [**to** *end-ip*] } &<1-10> | **ipv6-prefix** *prefix/prefix-length* } | **mac-address** *mac-address* } * [**interface** *interface-type interface-number*] [**vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]]

删除绑定表的命令为：**undo user-bind static** [{ { **ip-address** | **ipv6-address** } { *start-ip* [**to** *end-ip*] } &<1-10> | **ipv6-prefix** *prefix/prefix-length* } | **mac-address** *mac-address* | **interface** *interface-type interface-number* | **vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]] *

----结束

13.10.3 IPSG 中未配置上行信任接口导致业务不通

故障现象

VLAN内使能IPSG后所有主机访问不了外网，业务不通。

操作步骤

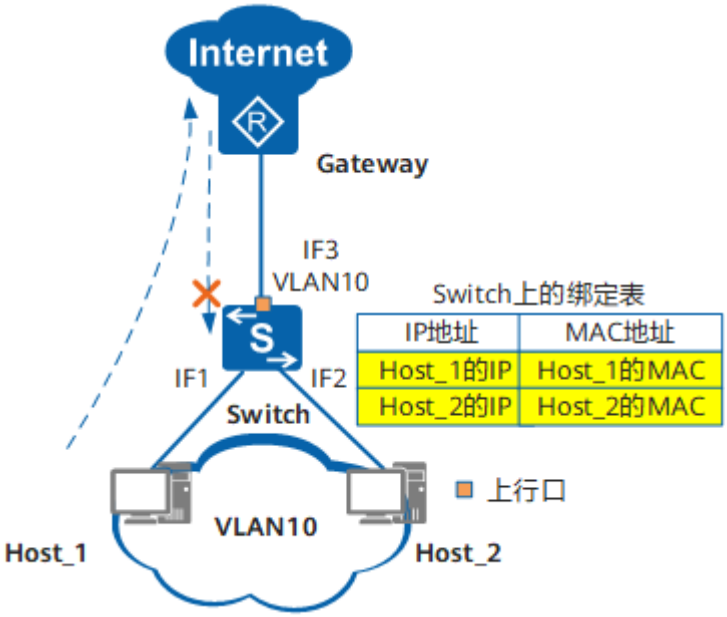
步骤1 检查上行口是否在使能IPSG功能的VLAN内

如果上行接口同时在使能IPSG功能的VLAN内，则需要将上行口配置成信任接口，否则回程报文会因匹配不到绑定表而被丢弃，导致业务不通。

如图13-16所示，Host_1和Host_2同属于VLAN10，IF3允许VLAN10报文通过。在Switch上创建了Host_1和Host_2的静态绑定表项，并且基于VLAN10使能了IPSG功能。Host无法访问Internet（Host之间可以通信）。以Host_1为例说明。

- Host_1发往Internet的报文：当报文到达Switch的IF1接口时，Switch检查报文和绑定表匹配，允许报文通过。
- 从Internet发往Host_1的回程报文：当报文到达Switch的IF3接口时，因为IF3接口在VLAN10内，Switch会检查报文是否和绑定表匹配，因匹配失败（绑定表中无对应的绑定表项）而丢弃报文。

图 13-16 IPSG 中未配置上行信任接口导致业务不通



步骤2 解决办法

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**dhcp enable**，全局使能DHCP功能。
3. 执行命令**dhcp snooping enable**，全局使能DHCP Snooping功能。
4. 执行命令**interface** *interface-type interface-number*，进入IF3接口视图。
5. 执行命令**dhcp snooping trusted**，配置IF3接口为信任状态。

----结束

13.10.4 上行接口使能 IPSG 导致业务不通

故障现象

接口上使能IPSG后所有主机访问不了外网，业务不通。

操作步骤

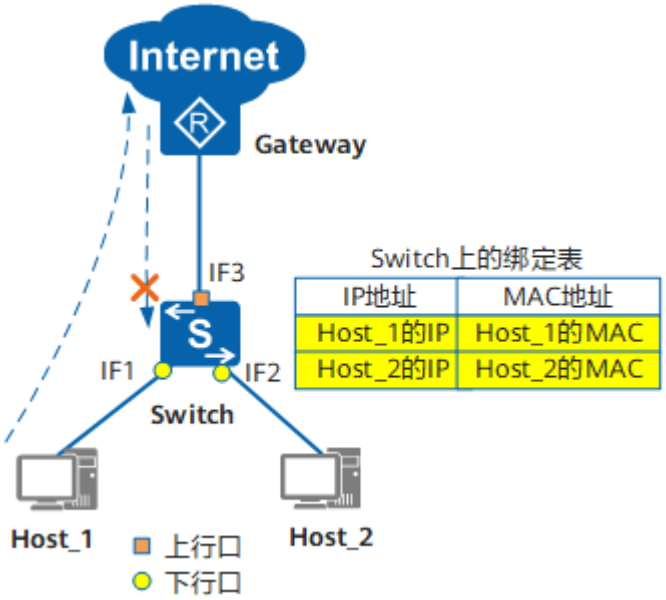
步骤1 检查使能IPSG的接口是否是上行口

正常情况下，IPSG使能在用户侧的接口（即下行口）。如果同时在上行口使能了IPSG，回程报文可能会被丢弃，导致用户业务不通。

如图13-17所示，在Switch上创建了Host_1和Host_2的静态绑定表项，IF1、IF2和IF3上同时使能了IPSG功能后，Host无法访问Internet（Host之间可以互通）。以Host_1为例说明。

- Host_1发往Internet的报文：当报文到达Switch的IF1接口时，Switch检查报文和绑定表匹配，允许报文通过。
- 从Internet发往Host_1的回程报文：当报文到达Switch的IF3接口时，因IF3使能了IPSG功能，Switch检查报文是否和绑定表匹配，因匹配失败（绑定表中无对应的绑定表项）而丢弃报文。

图 13-17 上行接口使能 IPSG 导致业务不通



步骤2 解决办法

1. 执行命令**display ip source check user-bind interface** *interface-type interface-number*，查看上行口IF3是否使能了IPSG功能。
2. 如果显示“ipv4 source check user-bind enable”或“ipv6 source check user-bind enable”表示接口使能了IPSG，请在接口视图下执行命令**undo ip source check user-bind enable**，去使能上行口IF3的IPSG功能。

----结束

13.10.5 配置 IP 和 MAC 绑定后，未绑定的主机仍可以上网

故障现象

配置IP和MAC绑定后，未绑定的主机仍可以上网。

操作步骤

步骤1 检查是否生成了静态绑定表

执行命令**display dhcp static user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** }，查看静态绑定表信息。

如果没有静态绑定表项，可能IP和MAC的绑定方式不对。请检查是否是通过执行命令**arp static** *ip-address mac-address*进行的IP和MAC绑定，这是静态ARP而不是IPSG，静态ARP无法实现未绑定的主机不能上网。

步骤2 创建静态绑定表

请执行命令**user-bind static** { { { **ip-address** | **ipv6-address** } { *start-ip* [**to** *end-ip*] } &<1-10> | **ipv6-prefix** *prefix/prefix-length* } | **mac-address** *mac-address* } * [**interface** *interface-type interface-number*] [**vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]]，创建静态绑定表。

绑定表正确创建后，还需要在指定的接口或指定的VLAN下执行命令**ip source check user-bind enable**使能IPSG，这样配置后可以实现未绑定的主机不能上网。

----结束

13.10.6 动态环境下未配置 DHCP Snooping 导致 IPSG 功能不生效

故障现象

主机通过DHCP服务器可以动态获取到IP地址，使能IPSG后功能不生效。

操作步骤

步骤1 检查DHCP Snooping绑定表是否存在

在主机通过DHCP方式获取IP地址的环境下，IPSG借助DHCP Snooping动态绑定表，对接口上接收的报文进行匹配检查。只有配置了DHCP Snooping功能，设备才会在主机上线时自动生成的DHCP Snooping绑定表。

执行命令**display dhcp snooping user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* }* | **all** }，查看DHCP Snooping绑定表信息。

如果没有动态绑定表项，请参见**13.7.2 配置基于动态绑定表的IPSG**中的步骤，完成DHCP Snooping的配置。主要过程如下：

1. 全局使能DHCP Snooping
2. 接口或VLAN下使能DHCP Snooping
3. 配置信任接口

DHCP Snooping配置完成后，主机重新上线后，设备会生成DHCP Snooping绑定表，IPSG才能生效。并且，如果设备在没有生成DHCP Snooping动态绑定表的情况下使能了IPSG，设备会拒绝所有除DHCP请求报文外的其他IP报文，DHCP主机的通信都会受到影响。所以，使能IPSG功能之前请先配置DHCP Snooping生成动态绑定表。

----结束

13.11 IPSG FAQ

13.11.1 交换机是否支持一个接口绑定多个 IP 地址

交换机支持一个接口绑定多个IP地址：

- 如果这些IP地址不是连续的，可以重复输入1～10个地址。例如，将IP地址10.1.1.2、10.1.1.5和10.1.1.12绑定到接口GE0/0/1。

  ```
  <HUAWEI> system-view
  [HUAWEI] user-bind static ip-address 10.1.1.2 10.1.1.5 10.1.1.12 interface gigabitethernet 0/0/1
  ```

- 如果这些IP地址是连续的，可以重复输入1～10个IP地址段。需要注意的是，IP地址段之间不能有交叉。例如，将10.2.1.1～10.2.1.10，10.2.1.20～10.2.1.30范围内的IP地址绑定到接口GE0/0/1。

  ```
  <HUAWEI> system-view
  [HUAWEI] user-bind static ip-address 10.2.1.1 to 10.2.1.10 10.2.1.20 to 10.2.1.30 interface gigabitethernet 0/0/1
  ```

13.11.2 交换机是否支持一个 MAC 地址绑定多个 IP 地址

交换机支持一个MAC地址绑定多个IP地址：

- 如果这些IP地址不是连续的，可以重复输入1～10个地址。例如，将IP地址10.1.1.2、10.1.1.5和10.1.1.12绑定到MAC地址xxxx-xxxx-xxx1。

  ```
  <HUAWEI> system-view
  [HUAWEI] user-bind static ip-address 10.1.1.2 10.1.1.5 10.1.1.12 mac-address xxxx-xxxx-xxx1
  ```

- 如果这些IP地址是连续的，可以重复输入1～10个IP地址段。需要注意的是，IP地址段之间不能有交叉。例如，将10.2.1.1～10.2.1.10，10.2.1.20～10.2.1.30范围内的IP地址绑定到MAC地址xxxx-xxxx-xxx2。

  ```
  <HUAWEI> system-view
  [HUAWEI] user-bind static ip-address 10.2.1.1 to 10.2.1.10 10.2.1.20 to 10.2.1.30 mac-address xxxx-xxxx-xxx2
  ```

13.11.3 如何删除静态绑定表项

当绑定表创建错误或者已绑定主机的网络权限变更时，需要执行命令**undo user-bind static** [{ { **ip-address** | **ipv6-address** } { *start-ip* [**to** *end-ip*] } &<1-10> | **ipv6-prefix** *prefix/prefix-length* } | **mac-address** *mac-address* | **interface** *interface-type interface-number* | **vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]] *，删除静态绑定表项。

- 删除单条绑定表时，**undo**命令指定的参数必须和绑定表中表项完全匹配，才能删除成功。
- 支持批量删除绑定表项。例如：
  - 执行命令**undo user-bind static**，删除所有绑定表信息。
  - 执行命令**undo user-bind static interface gigabitethernet 0/0/1**，删除指定接口**GE0/0/1**的所有表项。
  - 执行命令**undo user-bind static vlan 10**，删除指定**VLAN10**的所有表项。

以下通过示例介绍如何删除静态绑定表项。

首先，通过命令**display dhcp static user-bind all**查看已存在的静态绑定表项。

```
<HUAWEI> display dhcp static user-bind all
DHCP static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address                MAC Address     VSI/VLAN(O/I/P) Interface
------------------------------------------------------------------------------
192.168.1.1               xxxx-xxxx-xxx1  --  /--  /--    --
192.168.1.2               xxxx-xxxx-xxx2  --  /--  /--    GE1/0/2
192.168.2.1               --              --  /--  /--    GE0/0/1
```



```
192.168.2.2                --            --  /--  /--    GE0/0/1
192.168.2.3                --            --  /--  /--    GE0/0/1
192.168.3.1                xxxx-xxxx-xxx4  10  /--  /--    --
192.168.3.2                xxxx-xxxx-xxx5  10  /--  /--    --
------------------------------------------------------------------------------
Print count:          7        Total count:          7
```

删除IP地址为192.168.1.1的静态绑定表项。

```
<HUAWEI> system-view
[HUAWEI] undo user-bind static ip-address 192.168.1.1 mac-address xxxx-xxxx-xxx1
```

删除IP地址为192.168.1.2的静态绑定表项。

```
<HUAWEI> system-view
[HUAWEI] undo user-bind static ip-address 192.168.1.2 mac-address xxxx-xxxx-xxx2 interface gigabitethernet 0/0/2
```

删除GE0/0/1接口的所有静态绑定表项。

```
<HUAWEI> system-view
[HUAWEI] undo user-bind static interface gigabitethernet 0/0/1
```

删除VLAN10的所有静态绑定表项。

```
<HUAWEI> system-view
[HUAWEI] undo user-bind static vlan 10
```

以上步骤顺序执行完后，所有绑定表项均被删除。

14 SAVI 配置

14.1 SAVI 概述

设备通过侦听（Snooping）各种地址分配方式的控制报文建立地址和端口的绑定关系表，对于从相应端口接收到的ND协议报文、DHCPv6协议报文和IPv6数据报文，根据其源地址是否能匹配绑定关系表来确定报文是否合法，合法报文则正常转发，非法报文则丢弃，从而防止非法报文形成攻击。

SAVI功能可以在下列地址分配场景下使用：

- DHCPv6-Only：和配置SAVI功能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功能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功能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。

14.2 SAVI 配置注意事项

涉及网元

无需其他网元配合。

License 支持

本特性是交换机的基本特性，无需获得License许可即可应用此功能。

V200R021C00、V200R021C01 版本特性支持情况

S600-E系列交换机中所有款型均支持SAVI。

说明

如需了解交换机软件配套详细信息，请点击**Info-Finder**。

特性依赖和限制

设备支持同时配置SAVI和对Untagged报文添加双层Tag的功能。

- 如果希望过滤非法IPv6数据报文，请使能ND Snooping、DHCPv6 Snooping和IPSG功能。
- 如果希望过滤非法ND协议报文，还需执行**nd snooping check enable**命令使能ND协议报文合法性检查功能。
- 如果希望过滤非法DHCPv6协议报文，还需配置防止仿冒DHCP报文攻击。详细内容请参见相应版本“配置指南 — 安全” DHCP Snooping配置 中的“配置防止仿冒DHCP报文攻击”。

14.3 SAVI 缺省配置

SAVI的缺省配置如**表14-1**所示。

表 14-1 SAVI 缺省配置

参数	缺省值
SAVI功能	未使能
侦听响应地址冲突的NA报文的时间	2秒
侦听DHCPv6客户端对获取地址作冲突检测的时间	2秒

14.4 配置 SAVI

前置任务

在配置SAVI功能之前，请使能ND Snooping和DHCPv6 snooping功能。

- 如果希望过滤非法IPv6数据报文，还需配置**IPSG**功能。
- 如果希望过滤非法ND协议报文，还需配置**ND协议报文合法性检查**功能。
- 如果希望过滤非法DHCPv6协议报文，还需**配置防止仿冒DHCP报文攻击**功能。

14.4.1 使能 SAVI 功能

背景信息

为了防止源地址非法的ND协议报文、DHCPv6协议报文和IPv6数据报文形成攻击，可以配置SAVI功能，设备将根据通过ND Snooping功能、DHCPv6 Snooping功能建立起

的地址和端口的绑定关系表对ND协议报文、DHCPv6协议报文和IPv6数据报文的源地址进行合法性的过滤检查。

配置SAVI功能前必须先使能SAVI功能。

说明

使能SAVI功能后，前缀地址为FE80::/10的IPv6地址才能自动生成绑定表，但不会生成前缀表。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**savi enable**，使能SAVI功能。

缺省情况下，未使能SAVI功能。

----结束

14.4.2 （可选）配置接口允许学习 SAVI 绑定表项的最大个数

背景信息

SAVI绑定表是ND Snooping绑定表和DHCPv6 Snooping绑定表的集合，当接口下ND Snooping绑定表项和DHCPv6 Snooping绑定表项之和达到所配置的SAVI绑定表项最大数时，后续用户将无法接入。此功能可以有效避免设备处理用户发送的大量源地址非法的ND协议报文和DHCPv6协议报文，防止对设备造成攻击。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**savi max-binding-table** *max-number*，配置接口允许学习SAVI绑定表项的最大个数。

缺省情况下，在规格范围内，设备对接口能够学习到的最大SAVI绑定表项数目没有限制。

----结束

14.4.3 （可选）配置侦听响应地址冲突的 NA 报文的时间

背景信息

配置侦听响应地址冲突的NA报文的时间仅适用于SLAAC-Only场景或DHCPv6与SLAAC混合场景。

- SLAAC-Only场景下：

  客户端以无状态地址自动配置方式获取地址，客户端通过RA报文获取地址前缀并自动生成IPv6地址。生成地址后，客户端会发送DAD NS报文来检测网络中是否存在重复地址。当设备侦听到客户端的DAD NS报文后，会生成ND Snooping表项并将其置为detection状态，同时开始侦听相应的NA报文。

  – 如果在配置的侦听时间内侦听到NA报文，则说明该IPv6地址存在冲突，设备删除该ND Snooping表项。

  - 如果在配置的侦听时间内未侦听到NA报文，设备则将该ND Snooping表项置为bound状态，表明该IPv6地址不存在冲突，客户端可以使用该IPv6地址。直至ND Snooping表项老化时间到期，设备才将该ND Snooping表项删除；或者当设备配置了自动探测ND Snooping表项对应用户的在线状态功能（通过命令**nd user-bind detect enable**配置），在设备发出配置的探测次数（通过命令**nd user-bind detect retransmit** *retransmit-times* **interval** *retransmit-interval*配置）的NS探测报文之后，仍未收到用户回应的NA报文，使设备认为该用户已经下线，设备才将该ND Snooping表项删除。
- DHCPv6与SLAAC混合场景下：
  - 如果客户端以无状态地址自动配置方式获取地址，情况同SLAAC-Only场景。
  - 如果客户端通过DHCPv6方式获取地址，客户端在获取地址后，有可能会发送DAD NS报文来检测网络中是否存在重复地址。当设备侦听到客户端的DAD NS报文后，会将对应的DHCPv6 snooping表项置为detection状态，同时开始侦听相应的NA报文。
    - 如果在配置的侦听时间内侦听到NA报文，则说明该IPv6地址存在冲突，设备删除该DHCPv6 Snooping表项。
    - 如果在配置的侦听时间内未侦听到NA报文，设备则将该DHCPv6 Snooping表项置为bound状态，表明该IPv6地址不存在冲突，客户端可以使用该IPv6地址。直至侦听到DHCPv6客户端发送的DHCPv6 Decline或DHCPv6 Release报文，设备才将该DHCPv6 Snooping表项删除。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**savi max dad-delay** *value*，配置侦听响应地址冲突的NA报文的时间。

缺省情况下，侦听响应地址冲突的NA报文的时间为2秒。

----结束

14.4.4 （可选）配置侦听 DHCPv6 客户端对获取地址作冲突检测的时间

背景信息

配置侦听DHCPv6客户端对获取地址作冲突检测的时间仅适用于DHCPv6-Only场景或DHCPv6与SLAAC混合场景。

设备在侦听到DHCPv6客户端获取到IPv6地址后，还会侦听DHCPv6客户端是否会发送DAD NS报文对获取到的地址作冲突检测。

- DHCPv6-Only场景下：
  - 如果在配置的侦听时间内未侦听到DAD NS报文，设备则将对应的DHCPv6 Snooping表项置为bound状态，表明DHCPv6客户端未对获取到的地址作冲突检测，或者该IPv6地址不存在冲突，DHCPv6客户端可以使用该IPv6地址。
  - 如果在配置的侦听时间内侦听到DAD NS报文，设备不会改变对应的DHCPv6 Snooping表项状态。直至侦听时间到期，设备才会将该DHCPv6 Snooping表项置为bound状态。

  在DHCPv6-Only场景下，设备侦听到DHCPv6客户端发送的DHCPv6 Decline或DHCPv6 Release报文，会将对应的DHCPv6 Snooping表项删除。

- DHCPv6与SLAAC混合场景下：
  - 如果在配置的侦听时间内未侦听到DAD NS报文，设备则将对应的DHCPv6 Snooping或ND Snooping表项置为bound状态，表明客户端未对获取到的地址作冲突检测，或者该IPv6地址不存在冲突，客户端可以使用该IPv6地址。
  - 如果在配置的侦听时间内侦听到DAD NS报文，设备则将对应的DHCPv6 Snooping或ND Snooping表项置为detection状态，并继续侦听相应的NA报文。侦听方式请参见**（可选）配置侦听响应地址冲突的NA报文的时间**。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**savi max dad-prepare-delay** *value*，配置侦听DHCPv6客户端对获取地址作冲突检测的时间。

缺省情况下，侦听DHCPv6客户端对获取地址作冲突检测的时间为2秒。

----结束

14.4.5 检查 SAVI 的配置结果

操作步骤

- 系统视图和接口视图下执行命令**display this**，查看SAVI功能的配置信息。

----结束

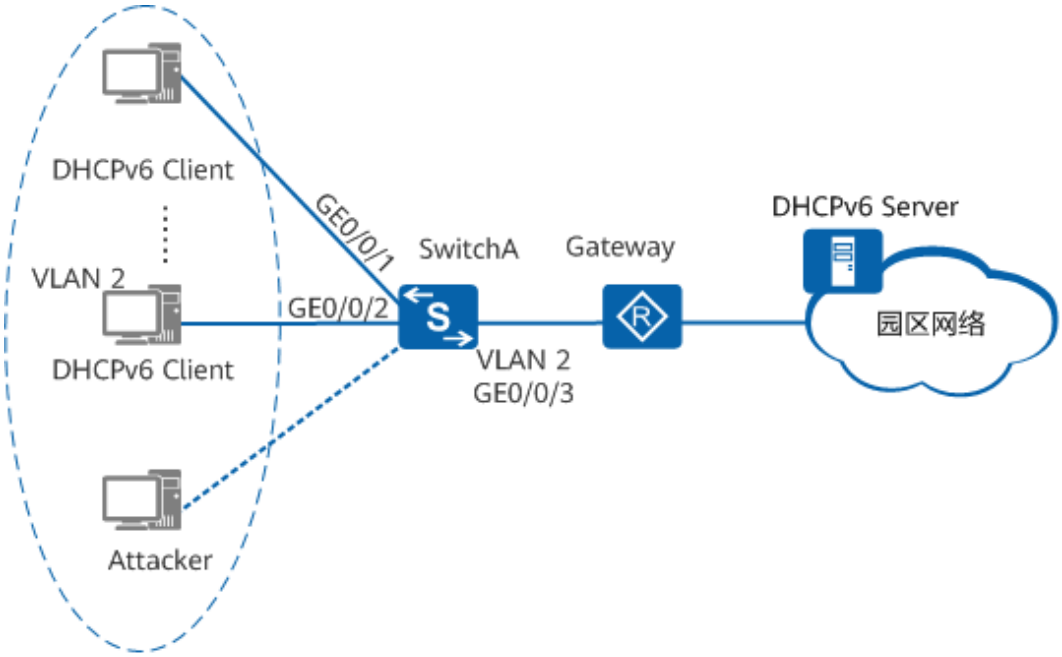
14.5 SAVI 配置举例

14.5.1 DHCPv6-Only 场景下配置 SAVI 功能示例

组网需求

如图14-1所示，企业某部门使用SwitchA作为直接连接用户的设备。该部门主机数量较多，为了便于统一管理IPv6地址，该部门的主机均通过DHCPv6方式获取IPv6地址。如果存在攻击者发送大量非法DHCPv6协议报文或非法IPv6数据报文，将会存在合法用户通信中断、用户帐号口令被盗用等一系列安全隐患。为了预防这种情况，管理员希望通过在SwitchA上进行配置，对非法的DHCPv6协议报文和IPv6数据报文（源地址非法）进行有效防范，为合法用户提供更安全的网络环境和更稳定的网络服务。

图 14-1 DHCPv6-Only 场景下配置 SAVI 功能示例组网图



配置思路

在用户主机上线之前，采用如下思路在SwitchA上进行配置：

1. 配置DHCPv6 Snooping功能，以便生成地址和端口的绑定关系表，用于后续的DHCPv6协议报文和IPv6数据报文源地址合法性检查。
2. 使能SAVI功能，使设备根据绑定关系表对DHCPv6协议报文进行源地址合法性检查，过滤非法DHCPv6协议报文。
3. 使能IP Source Guard功能，使设备根据绑定关系表对IPv6数据报文进行源地址合法性检查，过滤非法IPv6数据报文。

操作步骤

步骤1 使能SAVI功能

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] savi enable
```

步骤2 创建VLAN2

```
[SwitchA] vlan batch 2
```

步骤3 将接口GE0/0/1、GE0/0/2、GE0/0/3加入到VLAN2中

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type access
[SwitchA-GigabitEthernet0/0/1] port default vlan 2
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type access
[SwitchA-GigabitEthernet0/0/2] port default vlan 2
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 2
[SwitchA-GigabitEthernet0/0/3] quit
```

步骤4 配置DHCPv6 Snooping功能

全局使能DHCPv6 Snooping功能。

```
[SwitchA] dhcp enable
[SwitchA] dhcp snooping enable
```

在VLAN2内使能DHCPv6 Snooping功能。

```
[SwitchA] vlan 2
[SwitchA-vlan2] dhcp snooping enable
```

在VLAN2内使能DHCPv6协议报文的绑定表匹配检查功能。

```
[SwitchA-vlan2] dhcp snooping check dhcp-request enable
[SwitchA-vlan2] quit
```

配置接口GE0/0/3为DHCP Snooping信任接口。

```
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] dhcp snooping trusted
[SwitchA-GigabitEthernet0/0/3] quit
```

步骤5 在VLAN2内使能IP Source Guard功能

```
[SwitchA] vlan 2
[SwitchA-vlan2] ip source check user-bind enable
[SwitchA-vlan2] quit
```

步骤6 验证配置结果

在系统视图下执行**display this**命令可以看到全局已经使能SAVI功能和DHCPv6 Snooping功能。

```
[SwitchA] display this
...
#
dhcp enable
#
dhcp snooping enable
#
savi enable
#
...
```

在VLAN视图下执行**display this**命令可以看到VLAN2下已经使能DHCPv6 Snooping功能、DHCPv6协议报文绑定表匹配检查功能和IP Source Guard功能。

```
[SwitchA] vlan 2
[SwitchA-vlan2] display this
#
vlan 2
 dhcp snooping enable
 dhcp snooping check dhcp-request enable
#
return
[SwitchA-vlan2] quit
```

在接口视图下执行**display this**命令可以看到接口GE0/0/3已经配置为DHCP Snooping信任接口。

```
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] display this
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2
 dhcp snooping trusted
#
return
```

----结束

配置文件

SwitchA的配置文件

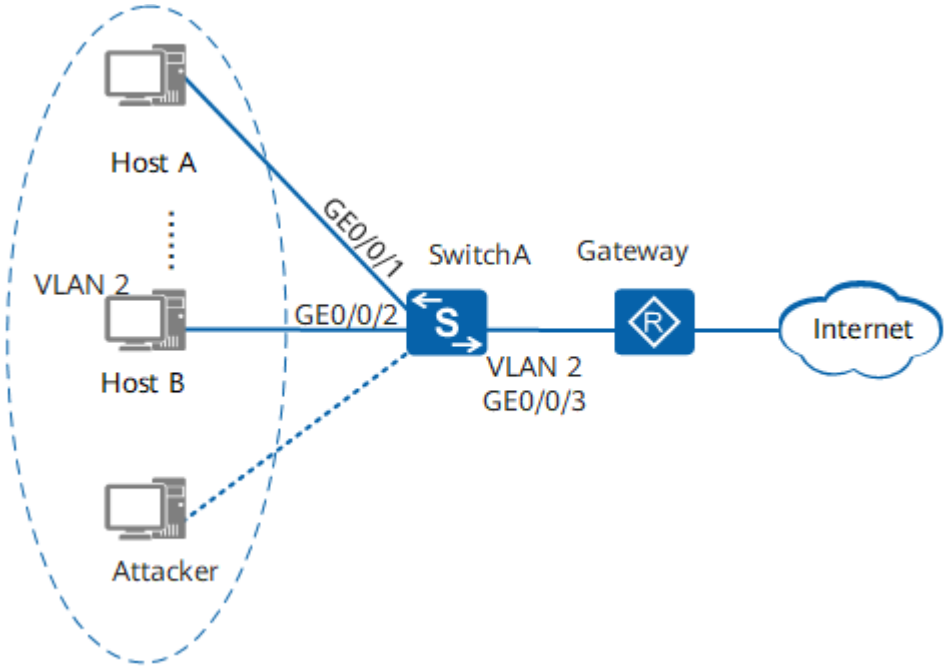
```
#
sysname SwitchA
#
vlan batch 2
#
dhcp enable
#
dhcp snooping enable
#
savi enable
#
vlan 2
 dhcp snooping enable
 dhcp snooping check dhcp-request enable
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 2
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 2
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2
 dhcp snooping trusted
#
return
```

14.5.2 SLAAC-Only 场景下配置 SAVI 功能示例

组网需求

如图14-2所示，企业某部门使用SwitchA作为直接连接用户主机的设备。网络中未部署DHCPv6服务器，该部门主机只能通过无状态地址自动配置方式获取IPv6地址。如果存在攻击者发送大量非法ND协议报文或非法IPv6数据报文，将会存在合法用户主机通信中断、用户帐号口令被盗用等一系列安全隐患。为了预防这种情况，管理员希望通过在SwitchA上进行配置，对非法的ND协议报文和IPv6数据报文（源地址非法）进行有效防范，为合法用户提供更安全的网络环境和更稳定的网络服务。

图 14-2 SLAAC-Only 场景下配置 SAVI 功能示例组网图



配置思路

在用户主机上线之前，采用如下思路在SwitchA上进行配置：

1. 配置ND Snooping功能，以便生成地址和端口的绑定关系表，用于后续的ND协议报文和IPv6数据报文源地址合法性检查。
2. 使能SAVI功能，使设备根据绑定关系表对ND协议报文进行源地址合法性检查，过滤非法ND协议报文。
3. 使能IP Source Guard功能，使设备根据绑定关系表对IPv6数据报文进行源地址合法性检查，过滤非法IPv6数据报文。

操作步骤

步骤1 使能SAVI功能

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] savi enable
```

步骤2 创建VLAN2

```
[SwitchA] vlan batch 2
```

步骤3 将接口GE0/0/1、GE0/0/2、GE0/0/3加入到VLAN2中

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type access
[SwitchA-GigabitEthernet0/0/1] port default vlan 2
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type access
[SwitchA-GigabitEthernet0/0/2] port default vlan 2
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
```

```
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 2
[SwitchA-GigabitEthernet0/0/3] quit
```

步骤4 配置ND Snooping功能

全局使能ND Snooping功能。

```
[SwitchA] nd snooping enable
```

在VLAN2内使能ND Snooping功能。

```
[SwitchA] vlan 2
[SwitchA-vlan2] nd snooping enable
```

在VLAN2内使能对NA报文和NS报文进行合法性检查功能。

```
[SwitchA-vlan2] nd snooping check na enable
[SwitchA-vlan2] nd snooping check ns enable
[SwitchA-vlan2] quit
```

配置接口GE0/0/3为ND Snooping信任接口。

```
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] nd snooping trusted
[SwitchA-GigabitEthernet0/0/3] quit
```

步骤5 在VLAN2内使能IP Source Guard功能

```
[SwitchA] vlan 2
[SwitchA-vlan2] ip source check user-bind enable
[SwitchA-vlan2] quit
```

步骤6 验证配置结果

在系统视图下执行**display this**命令可以看到全局已经使能SAVI功能和ND Snooping功能。

```
[SwitchA] display this
...
#
nd snooping enable
savi enable
#
...
```

在VLAN视图下执行**display this**命令可以看到VLAN2下已经使能ND Snooping功能、ND协议报文合法性检查功能和IP Source Guard功能。

```
[SwitchA] vlan 2
[SwitchA-vlan2] display this
#
vlan 2
 nd snooping enable
 nd snooping check ns enable
 nd snooping check na enable
#
return
[SwitchA-vlan2] quit
```

在接口视图下执行**display this**命令可以看到接口GE0/0/3已经配置为ND Snooping信任接口。

```
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] display this
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2
 nd snooping trusted
```



```
#
return
```

----结束

配置文件

SwitchA的配置文件

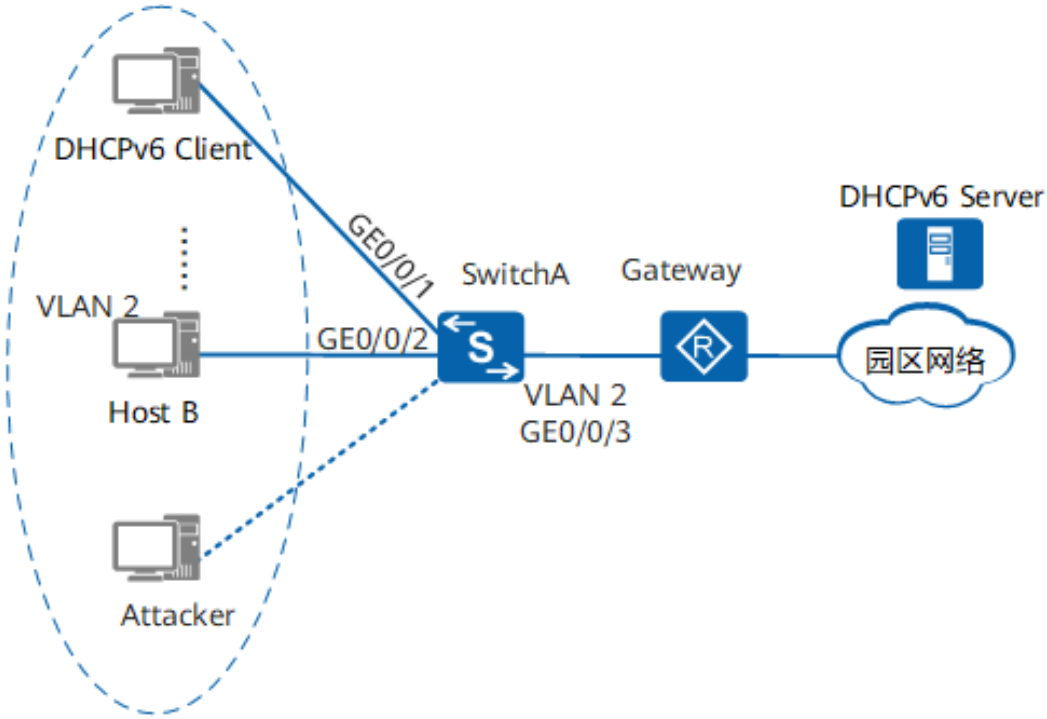
```
#
sysname SwitchA
#
vlan batch 2
#
nd snooping enable
savi enable
#
vlan 2
 nd snooping enable
 nd snooping check ns enable
 nd snooping check na enable
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 2
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 2
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2
 nd snooping trusted
#
return
```

14.5.3 DHCPv6 与 SLAAC 混合场景下配置 SAVI 功能示例

组网需求

如图14-3所示，企业某部门使用SwitchA作为直接连接用户主机的设备。该部门部分主机通过无状态地址自动配置方式获取IPv6地址，部分主机通过DHCPv6方式获取IPv6地址。如果存在攻击者发送大量非法的ND协议报文、DHCPv6协议报文或IPv6数据报文，将会存在合法用户主机通信中断、用户帐号口令被盗用等一系列安全隐患。为了预防这种情况，管理员希望通过在SwitchA上进行配置，对非法的ND协议报文、DHCPv6协议报文和IPv6数据报文（源地址非法）进行有效防范，为合法用户提供更安全的网络环境和更稳定的网络服务。

图 14-3 DHCPv6 与 SLAAC 混合场景下配置 SAVI 功能示例组网图



配置思路

在用户主机上线之前，采用如下思路在SwitchA上进行配置：

1. 配置DHCPv6 Snooping功能，以便生成地址和端口的绑定关系表，用于后续的DHCPv6报文和IPv6数据报文源地址合法性检查。
2. 配置ND Snooping功能，以便生成地址和端口的绑定关系表，用于后续的ND协议报文和IPv6数据报文源地址合法性检查。
3. 使能SAVI功能，使设备根据绑定关系表对DHCPv6协议报文和ND协议报文进行源地址合法性检查，过滤非法协议报文。
4. 使能IP Source Guard功能，使设备根据绑定关系表对IPv6数据报文进行源地址合法性检查，过滤非法IPv6数据报文。

操作步骤

步骤1 使能SAVI功能

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] savi enable
```

步骤2 创建VLAN2

```
[SwitchA] vlan batch 2
```

步骤3 将接口GE0/0/1、GE0/0/2、GE0/0/3加入到VLAN2中

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type access
[SwitchA-GigabitEthernet0/0/1] port default vlan 2
[SwitchA-GigabitEthernet0/0/1] quit
```

```
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type access
[SwitchA-GigabitEthernet0/0/2] port default vlan 2
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 2
[SwitchA-GigabitEthernet0/0/3] quit
```

步骤4 配置DHCPv6 Snooping功能

全局使能DHCPv6 Snooping功能。

```
[SwitchA] dhcp enable
[SwitchA] dhcp snooping enable
```

在VLAN2内使能DHCPv6 Snooping功能。

```
[SwitchA] vlan 2
[SwitchA-vlan2] dhcp snooping enable
```

在VLAN2内使能DHCPv6协议报文的绑定表匹配检查功能。

```
[SwitchA-vlan2] dhcp snooping check dhcp-request enable
[SwitchA-vlan2] quit
```

配置接口GE0/0/3为DHCP Snooping信任接口。

```
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] dhcp snooping trusted
[SwitchA-GigabitEthernet0/0/3] quit
```

步骤5 配置ND Snooping功能

全局使能ND Snooping功能。

```
[SwitchA] nd snooping enable
```

在VLAN2内使能ND Snooping功能。

```
[SwitchA] vlan 2
[SwitchA-vlan2] nd snooping enable
```

在VLAN2内使能对NA报文和NS报文进行合法性检查功能。

```
[SwitchA-vlan2] nd snooping check na enable
[SwitchA-vlan2] nd snooping check ns enable
[SwitchA-vlan2] quit
```

配置接口GE0/0/3为ND Snooping信任接口。

```
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] nd snooping trusted
[SwitchA-GigabitEthernet0/0/3] quit
```

步骤6 在VLAN2内使能IP Source Guard功能

```
[SwitchA] vlan 2
[SwitchA-vlan2] ip source check user-bind enable
[SwitchA-vlan2] quit
```

步骤7 验证配置结果

在系统视图下执行**display this**命令可以看到全局已经使能SAVI功能、DHCPv6 Snooping功能和ND Snooping功能。

```
[SwitchA] display this
...
#
dhcp enable
#
```



```
dhcp snooping enable
#
nd snooping enable
savi enable
#
...
```

在VLAN视图下执行**display this**命令可以看到VLAN2下已经使能DHCPv6 Snooping功能、DHCPv6协议报文绑定表匹配检查功能、ND Snooping功能、ND协议报文合法性检查功能以及IP Source Guard功能。

```
[SwitchA] vlan 2
[SwitchA-vlan2] display this
#
vlan 2
 dhcp snooping enable
 dhcp snooping check dhcp-request enable
 nd snooping enable
 nd snooping check ns enable
 nd snooping check na enable
#
return
[SwitchA-vlan2] quit
```

在接口视图下执行**display this**命令可以看到接口GE0/0/3已经配置为DHCP Snooping信任接口和ND Snooping信任接口。

```
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] display this
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2
 dhcp snooping trusted
 nd snooping trusted
#
return
```

----结束

配置文件

SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 2
#
dhcp enable
#
dhcp snooping enable
#
nd snooping enable
savi enable
#
vlan 2
 dhcp snooping enable
 dhcp snooping check dhcp-request enable
 nd snooping enable
 nd snooping check ns enable
 nd snooping check na enable
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 2
#
interface GigabitEthernet0/0/2
 port link-type access
```



```
 port default vlan 2
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 2
 dhcp snooping trusted
 nd snooping trusted
#
return
```


15 PKI 配置

15.1 PKI 简介

定义

公钥基础设施PKI（Public Key Infrastructure），是一种遵循既定标准的证书管理平台，它利用公钥技术能够为所有网络应用提供安全服务。PKI技术是信息安全技术的核心，也是电子商务的关键和基础技术。

目的

随着网络技术和信息技术的发展，电子商务已逐步被人们所接受，并得到不断普及。但通过网络进行电子商务交易时，存在如下问题：

- 交易双方并不现场交易，无法确认双方的合法身份。
- 通过网络传输时信息易被窃取和篡改，无法保证信息的安全性。
- 交易双方发生纠纷时没有凭证可依，无法提供仲裁。

为了解决上述问题，PKI技术应运而生，其利用公钥技术保证在交易过程中能够实现身份认证、保密、数据完整性和不可否认性。因而在网络通信和网络交易中，特别是电子政务和电子商务业务，PKI技术得到了广泛的应用。

受益

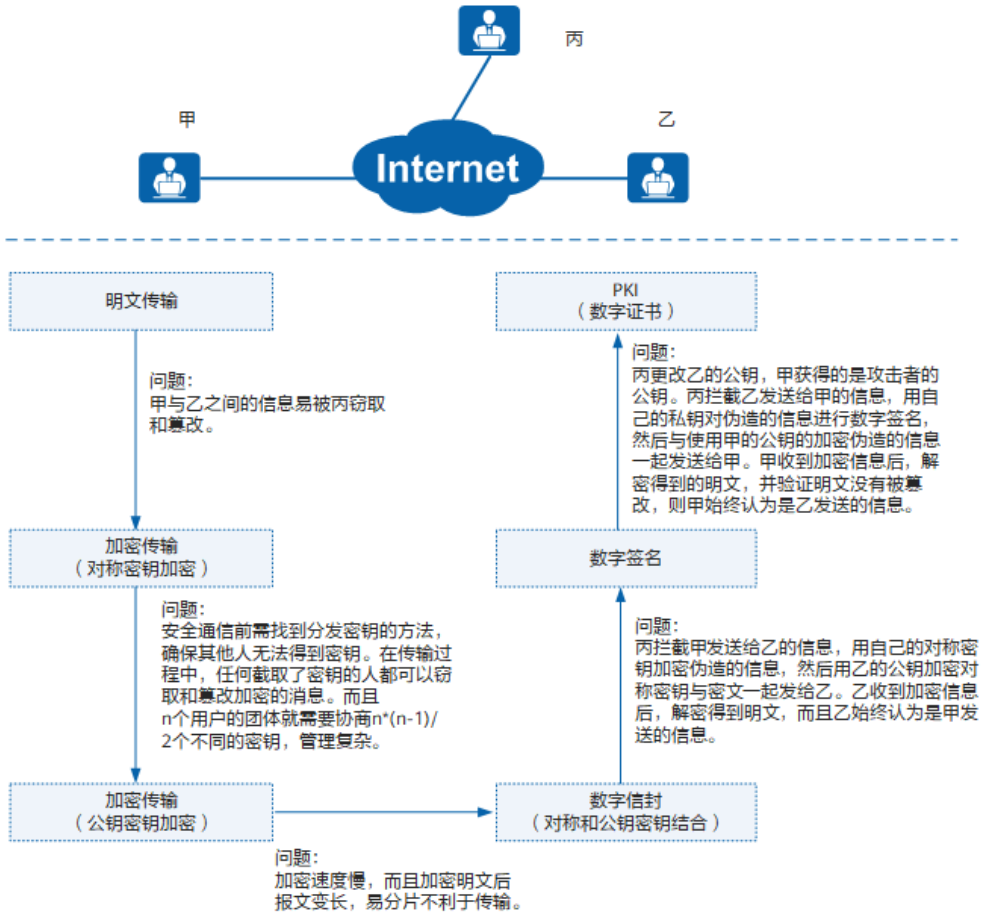
- 用户受益
  - 通过PKI证书认证技术，用户可以验证接入设备的合法性，从而可以保证用户接入安全、合法的网络中。
  - 通过PKI加密技术，可以保证网络中传输的数据的私密性，数据不会被篡改和窥探。
  - 通过PKI签名技术，可以保证数据的安全性，未授权的设备和用户无法查看该数据。
- 企业受益
  - 企业可以防止非法用户接入企业网络中。
  - 企业分支之间可以建立安全通道，保证企业数据的安全性。

15.2 PKI 原理描述

15.2.1 PKI 基本概念

PKI的核心技术就围绕着数字证书的申请、颁发和使用等整个生命周期进行展开，而在这整个生命周期过程中，PKI会使用到对称密钥加密、公钥加密、数字信封和数字签名技术。下面以图15-1为例介绍这些技术间的演进过程。甲和乙通过Internet进行通信，丙为攻击者专门破坏甲和乙间的通信。

图 15-1 演进示意图



对于这些概念的详细介绍请参见相应的章节。

15.2.1.1 加密

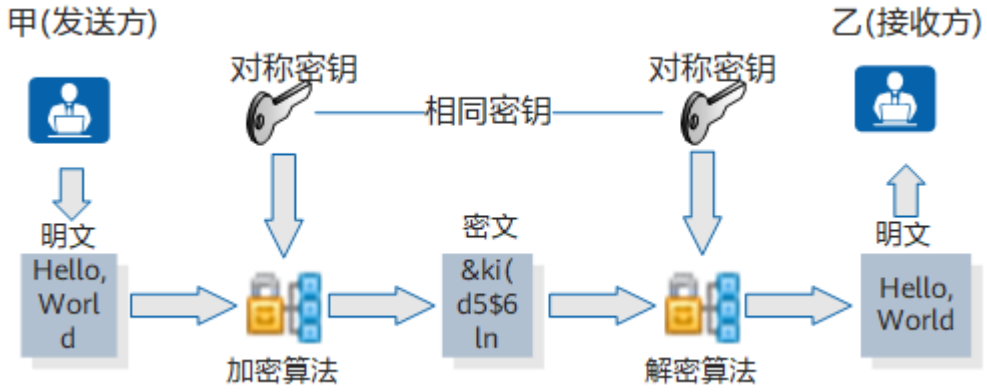
加密是通过网络传输信息的基础。通俗地讲，加密就是利用数学方法将明文(需要被隐蔽的数据)转换为密文（不可读的数据）从而达到保护数据的目的。

对称密钥加密

对称密钥加密又称为共享密钥加密，它使用同一个密钥对数据进行加密和解密。

对称密钥的加解密过程如图15-2所示。

图 15-2 对称密钥加解密过程示意图



甲与乙事先协商好对称密钥，具体加解密过程如下：

1. 甲使用对称密钥对明文加密，并将密文发送给乙。
2. 乙接收到密文后，使用对称密钥对密文解密，得到最初的明文。

对称密钥加密的优点是效率高，算法简单，系统开销小，适合加密大量数据。缺点是实现困难，扩展性差。实现困难原因在于进行安全通信前需要以安全方式进行密钥交换；扩展性差表现在每对通信用户之间都需要协商密钥，n个用户的团体就需要协商n*(n-1)/2个不同的密钥。

目前比较常用的对称密钥加密算法，主要包含DES（Data Encryption Standard）、3DES(Triple Data Encryption Standard)、AES（Advance Encrypt Standard）算法。其中，DES和3DES算法安全性低，存在安全风险，不推荐使用。

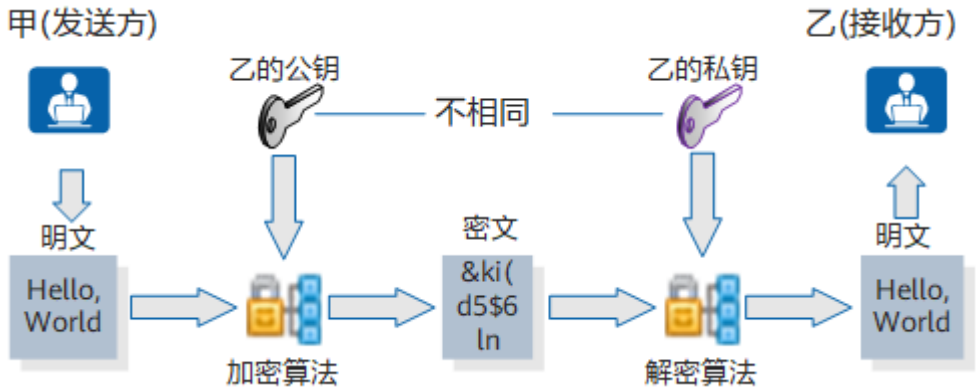
公钥加密

公钥加密又称为非对称密钥加密，它使用了两个不同的密钥：一个可对外界公开，称为“公钥”；一个只有所有者知道，称为“私钥”。

公钥加密解决了对称密钥的发布和管理问题，一个用于加密信息，另一个则用于解密信息，通信双方无需事先交换密钥就可进行保密通信。通常以公钥作为加密密钥，以私钥作为解密密钥。因为其他人没有对应的私钥，发送的加密信息仅该用户可以解读，从而实现通信的加密传输。

公钥加解密的过程如图15-3所示。

图 15-3 公钥加解密过程示意图



甲事先获得乙的公钥，具体加解密过程如下：

1. 甲使用乙的公钥对明文加密，并将密文发送给乙。
2. 乙收到密文后，使用自己的私钥对密文解密，得到最初的明文。

公钥加密的优点是无法从一个密钥推导出另一个密钥；公钥加密的信息只能用私钥进行解密。缺点是算法非常复杂，导致加密大量数据所用的时间较长，而且加密后的报文较长，不利于网络传输。

基于公钥加密的优缺点，公钥加密适合对密钥或身份信息等敏感信息加密，从而在安全性上满足用户的需求。

目前比较常用的公钥加密算法，主要包含DH（Diffie-Hellman）、RSA（Ron Rivest、Adi Shamir、Leonard Adleman）和DSA（Digital Signature Algorithm）算法。

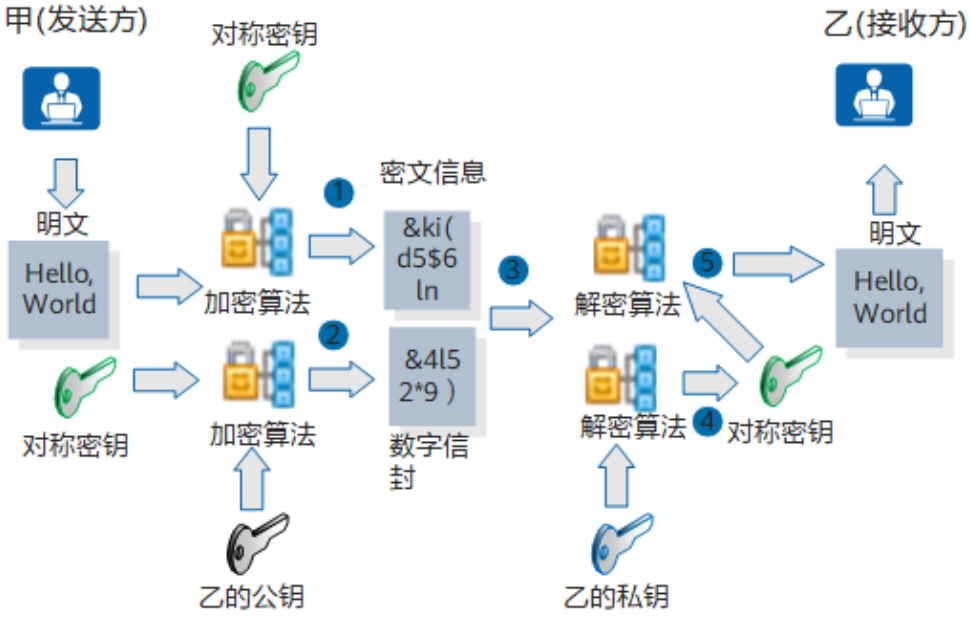
15.2.1.2 数字信封和数字签名

数字信封

数字信封是指发送方采用接收方的公钥来加密对称密钥后所得的数据。采用数字信封时，接收方需要使用自己的私钥才能打开数字信封得到对称密钥。

数字信封的加解密过程如图15-4所示。

图 15-4 数字信封的加解密过程示意图



甲事先获得乙的公钥，具体加解密过程如下：

1. 甲使用对称密钥对明文进行加密，生成密文信息。
2. 甲使用乙的公钥加密对称密钥，生成数字信封。

3. 甲将数字信封和密文信息一起发送给乙。
4. 乙接收到甲的加密信息后，使用自己的私钥打开数字信封，得到对称密钥。
5. 乙使用对称密钥对密文信息进行解密，得到最初的明文。

从加解密过程中，可以看出，数字信封技术结合了对称密钥加密和公钥加密的优点，解决了对称密钥的发布和公钥加密速度慢等问题，提高了安全性、扩展性和效率等。

但是，数字信封技术还有个问题，如果攻击者拦截甲的信息，用自己的对称密钥加密伪造的信息，并用乙的公钥加密自己的对称密钥，然后发送给乙。乙收到加密信息后，解密得到的明文，而且乙始终认为是甲发送的信息。此时，需要一种方法确保接收方收到的信息就是指定的发送方发送的。

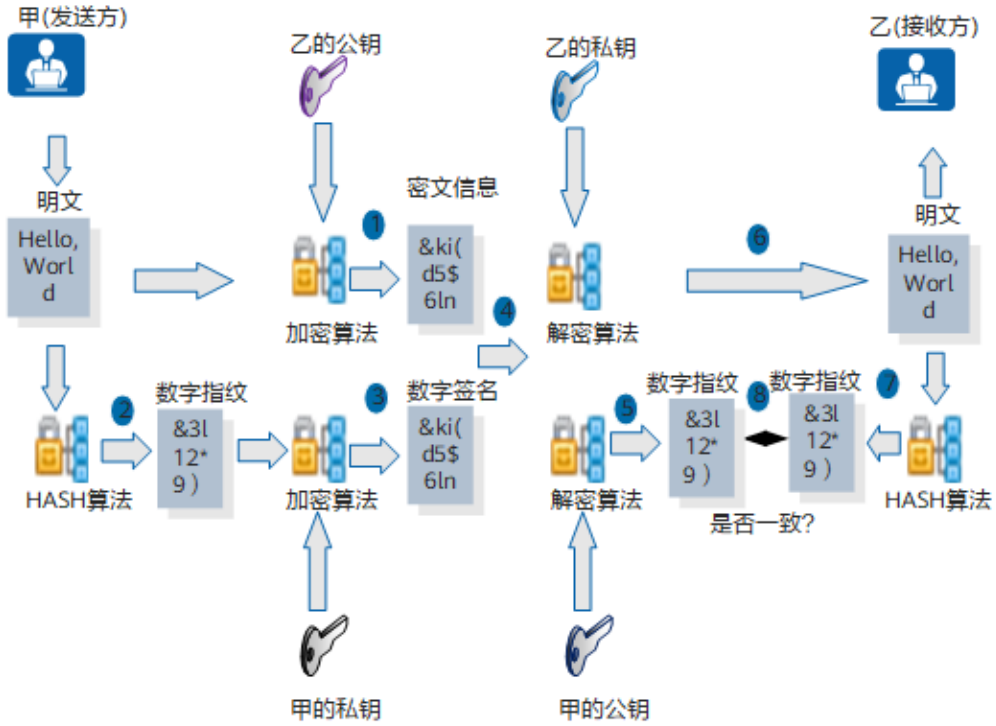
数字签名

数字签名是指发送方用自己的私钥对数字指纹进行加密后所得的数据。采用数字签名时，接收方需要使用发送方的公钥才能解开数字签名得到数字指纹。

数字指纹又称为信息摘要，它是指发送方通过HASH算法对明文信息计算后得出的数据。采用数字指纹时，发送方会将数字指纹和明文一起发送给接收方，接收方用同样的HASH算法对明文计算生成的数据指纹，与收到的数字指纹进行匹配，如果一致，便可确定明文信息没有被篡改。

数字签名的加解密过程如图15-5所示。

图 15-5 数字签名的加解密过程示意图



甲事先获得乙的公钥，具体加解密过程如下：

1. 甲使用乙的公钥对明文进行加密，生成密文信息。

2. 甲使用HASH算法对明文进行HASH运算，生成数字指纹。
3. 甲使用自己的私钥对数字指纹进行加密，生成数字签名。
4. 甲将密文信息和数字签名一起发送给乙。
5. 乙使用甲的公钥对数字签名进行解密，得到数字指纹。
6. 乙接收到甲的加密信息后，使用自己的私钥对密文信息进行解密，得到最初的明文。
7. 乙使用HASH算法对明文进行HASH运算，生成数字指纹。
8. 乙将生成的数字指纹与得到的数字指纹进行比较，如果一致，乙接受明文；如果不一致，乙丢弃明文。

从加解密过程中，可以看出，数字签名技术不但证明了信息未被篡改，还证明了发送方的身份。数字签名和数字信封技术也可以组合使用。

但是，数字签名技术还有个问题，如果攻击者更改乙的公钥，甲获得的是攻击者的公钥，攻击者拦截乙发送给甲的信息，用自己的私钥对伪造的信息进行数字签名，然后与使用甲的公钥的加密伪造的信息一起发送给甲。甲收到加密信息后，解密得到的明文，并验证明文没有被篡改，则甲始终认为是乙发送的信息。此时，需要一种方法确保一个特定的公钥属于一个特定的拥有者。

15.2.1.3 数字证书

数字证书简称证书，它是一个经证书授权中心（即在PKI中的**证书认证机构CA**）数字签名的文件，包含拥有者的公钥及相关身份信息。

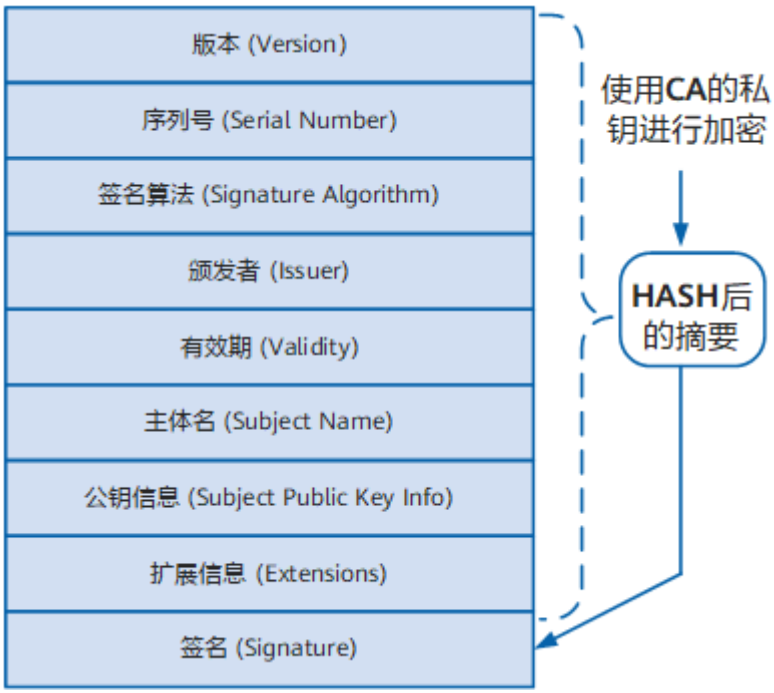
数字证书可以说是Internet上的安全护照或身份证。当人们到其他国家旅行时，用护照可以证实其身份，并被获准进入这个国家。数字证书提供的是网络上的身份证明。

数字证书技术解决了数字签名技术中无法确定公钥是指定拥有者的问题。

证书结构

最简单的证书包含一个公钥、名称以及证书授权中心的数字签名。一般情况下证书中还包括密钥的有效期，颁发者（证书授权中心）的名称，该证书的序列号等信息，证书的结构遵循X.509 v3版本的规范。**图15-6**展示了一个常见的证书结构。

图 15-6 证书结构示意图



证书的各字段解释：

- 版本：即使用X.509的版本，目前普遍使用的是v3版本（0x2）。
- 序列号：颁发者分配给证书的一个正整数，同一颁发者颁发的证书序列号各不相同，可用与颁发者名称一起作为证书唯一标识。
- 签名算法：颁发者颁发证书使用的签名算法。
- 颁发者：颁发该证书的设备名称，必须与颁发者证书中的主体名一致。通常为CA服务器的名称。
- 有效期：包含有效的起、止日期，不在有效期范围的证书为无效证书。
- 主体名：证书拥有者的名称，如果与颁发者相同则说明该证书是一个自签名证书。
- 公钥信息：用户对外公开的公钥以及公钥算法信息。
- 扩展信息：通常包含了证书的用法、CRL的发布地址等可选字段。
- 签名：颁发者用私钥对证书信息的签名。

证书分类

证书有四种类型，如表15-1所示。

表 15-1 证书类型

类型	描述	说明
自签名证书	自签名证书又称为根证书，是自己颁发给自己的证书，即证书中的颁发者和主体名相同。	申请者无法向CA申请本地证书时，可以通过设备生成自签名证书，可以实现简单证书颁发功能。 设备不支持对其生成的自签名证书进行生命周期管理（如证书更新、证书撤销等），为了确保设备和证书的安全，建议用户替换为自己的本地证书。
CA证书	CA自身的证书。如果PKI系统中没有多层级CA，CA证书就是自签名证书；如果有多层级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。	申请者通过验证CA的数字签名从而信任CA，任何申请者都可以得到CA的证书（含公钥），用以验证它所颁发的本地证书。
本地证书	CA颁发给申请者的证书。	-
设备本地证书	设备根据CA证书给自己颁发的证书，证书中的颁发者名称是CA服务器的名称。	申请者无法向CA申请本地证书时，可以通过设备生成设备本地证书，可以实现简单证书颁发功能。

证书格式

设备支持三种文件格式保存证书，如表15-2所示。

表 15-2 证书格式

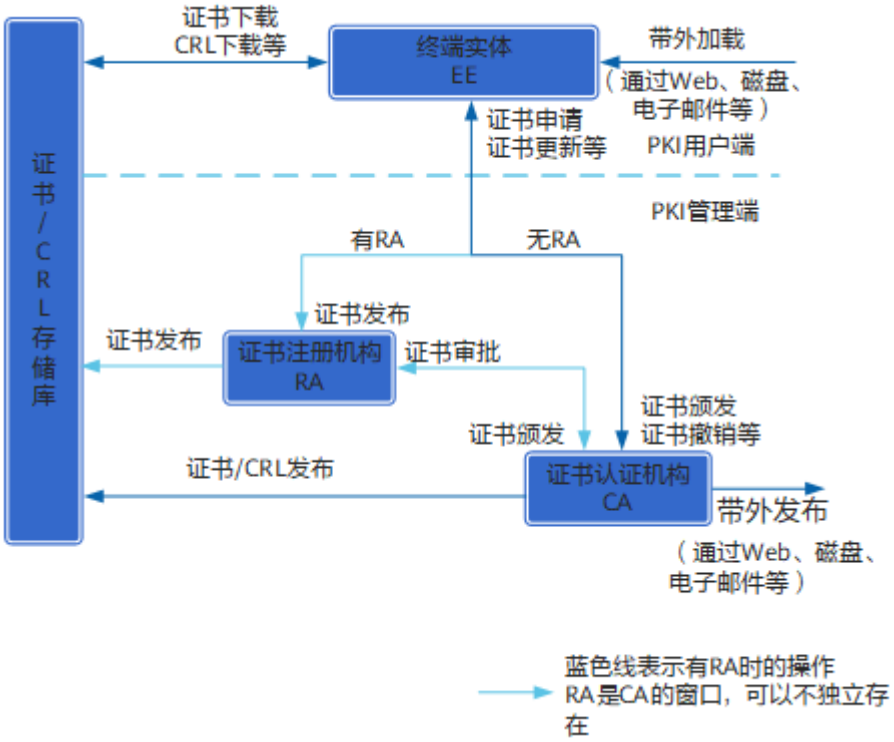
格式	描述	说明
PKCS#12	以二进制格式保存证书，可以包含私钥，也可以不包含私钥。常用的后缀有：.P12和.PFX。	对于证书后缀为.CER或.CRT，可以用记事本打开证书，查看证书内容来区分证书格式。 • 如果有类似 " -----BEGIN CERTIFICATE----- " 和 " -----END CERTIFICATE----- " 的头尾标记，则证书格式为PEM。 • 如果是乱码，则证书格式为DER。
DER	以二进制格式保存证书，不包含私钥。常用的后缀有：.DER、.CER和.CRT。	

格式	描述	说明
PEM	以ASCII码格式保存证书，可以包含私钥，也可以不包含私钥。常用的后缀有：.PEM、.CER和.CRT。	

15.2.2 PKI 体系架构

如图15-7所示，一个PKI体系由终端实体、证书认证机构、证书注册机构和证书/CRL存储库四部分共同组成。

图 15-7 PKI 体系架构



- 终端实体EE（End Entity）

  终端实体也称为PKI实体，它是PKI产品或服务的最终使用者，可以是个人、组织、设备（如路由器、防火墙）或计算机中运行的进程。

- 证书认证机构CA（Certificate Authority）

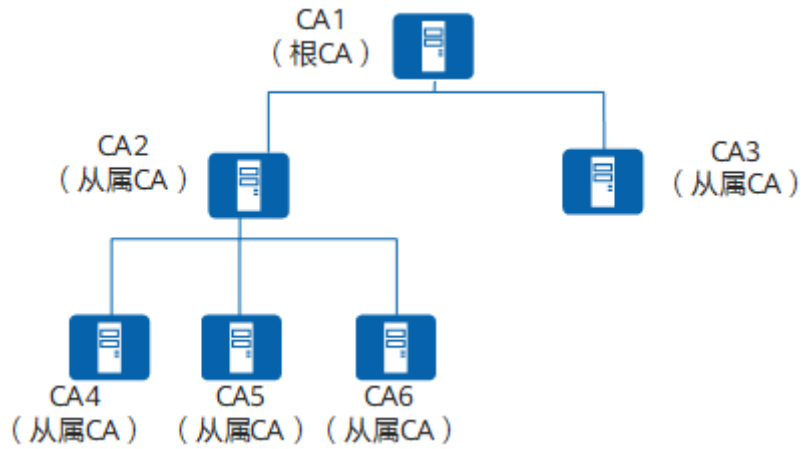
  CA是PKI的信任基础，是一个用于颁发并管理数字证书的可信实体。它是一种权威性、可信任性和公正性的第三方机构，通常由服务器充当，例如Windows Server 2008。

如图15-8所示，CA通常采用多层次的分级结构，根据证书颁发机构的层次，可以划分为根CA和从属CA。

- 根CA是公钥体系中第一个证书颁发机构，它是信任的起源。根CA可以为其它CA颁发证书，也可以为其它计算机、用户、服务颁发证书。对大多数基于证书的应用程序来说，使用证书的认证都可以通过证书链追溯到根CA。根CA通常持有一个自签名证书。
- 从属CA必须从上级CA处获取证书。上级CA可以是根CA或者是一个已由根CA授权可颁发从属CA证书的从属CA。上级CA负责签发和管理下级CA的证书，最下一级的CA直接面向用户。例如，CA2和CA3是从属CA，持有CA1发行的CA证书；CA4、CA5和CA6是从属CA，持有CA2发行的CA证书。

当某个PKI实体信任一个CA，则可以通过证书链来传递信任，证书链就是从用户的证书到根证书所经过的一系列证书的集合。当通信的PKI实体收到待验证的证书时，会沿着证书链依次验证其颁发者的合法性。

图 15-8 CA 层次示意图



CA的核心功能就是发放和管理数字证书，包括：证书的颁发、证书的更新、证书的撤销、证书的查询、证书的归档、证书废除列表CRL（Certificate Revocation List）的发布等。

- 证书注册机构RA（Registration Authority）

  RA是数字证书注册审批机构，RA是CA面对用户的窗口，是CA的证书发放、管理功能的延伸，它负责接受用户的证书注册和撤销申请，对用户的身份信息进行审查，并决定是否向CA提交签发或撤销数字证书的申请。

  RA作为CA功能的一部分，实际应用中，通常RA并不一定独立存在，而是和CA合并在一起。RA也可以独立出来，分担CA的一部分功能，减轻CA的压力，增强CA系统的安全性。

- 证书/CRL存储库

  由于用户名称的改变、私钥泄露或业务中止等原因，需要存在一种方法将现行的证书吊销，即撤销公钥及相关的PKI实体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CRL。

  任何一个证书被撤销以后，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。因此，CRL提供了一种检验证书有效性的方式。

证书/CRL存储库用于对证书和CRL等信息进行存储和管理，并提供查询功能。构建证书/CRL存储库可以采用FTP（File Transfer Protocol）服务器、HTTP（Hypertext Transfer Protocol）服务器或者数据库等等。

PKI的核心技术就围绕着本地证书的申请、颁发、存储、下载、安装、验证、更新和撤销的整个生命周期进行展开。

证书申请

证书申请即证书注册，就是一个PKI实体向CA自我介绍并获取证书的过程。通常情况下PKI实体会生成一对公私钥，公钥和自己的身份信息（包含在证书注册请求消息中）被发送给CA用来生成本地证书，私钥PKI实体自己保存用来数字签名和解密对端实体发送过来的密文。

PKI实体向CA申请本地证书有以下两种方式：

- 在线申请

  PKI实体支持通过SCEP（Simple Certificate Enrollment Protocol）或CMPv2（Certificate Management Protocol version 2）协议向CA发送证书注册请求消息来申请本地证书。
- 离线申请（PKCS#10方式）

  离线申请是指PKI实体使用PKCS#10格式打印出本地的证书注册请求消息并保存到文件中，然后通过带外方式（如Web、磁盘、电子邮件等）将文件发送给CA进行证书申请。

还有种方式，PKI实体可以为自己颁发一个自签名证书或本地证书，实现简单的证书颁发功能。

证书颁发

PKI实体向CA申请本地证书时，如果有RA，则先由RA审核PKI实体的身份信息，审核通过后，RA将申请信息发送给CA。CA再根据PKI实体的公钥和身份信息生成本地证书，并将本地证书信息发送给RA。如果没有RA，则直接由CA审核PKI实体身份信息。

证书存储

CA生成本地证书后，CA/RA会将本地证书发布到证书/CRL存储库中，为用户提供下载服务和目录浏览服务。

证书下载

PKI实体通过SCEP或CMPv2协议向CA服务器下载已颁发的证书，或者通过HTTP或者带外方式，下载已颁发的证书。该证书可以是自己的本地证书，也可以是CA/RA证书或者其他PKI实体的本地证书。

证书安装

PKI实体下载证书后，还需安装证书，即将证书导入到设备的内存中，否则证书不生效。该证书可以是自己的本地证书，也可以是CA/RA证书，或其他PKI实体的本地证书。

证书验证

PKI实体获取对端实体的证书后，当需要使用对端实体的证书时，例如与对端建立安全隧道或安全连接，通常需要验证对端实体的本地证书和CA的合法性（证书是否有效或

者是否属于同一个CA颁发等）。如果证书颁发者的证书无效，则由该CA颁发的所有证书都不再有效。但在CA证书过期前，设备会自动更新CA证书，异常情况下才会出现CA证书过期现象。

PKI实体可以使用CRL或者OCSP（Online Certificate Status Protocol）方式检查证书是否有效。使用CRL方式时，PKI实体先查找本地内存的CRL，如果本地内存没有CRL，则需下载CRL并安装到本地内存中，如果证书在CRL中，表示此证书已被撤销。使用OCSP方式时，PKI实体向OCSP服务器发送一个对于证书状态信息的请求，OCSP服务器会回复一个“有效”（证书没有被撤销）、“过期”（证书已被撤销）或“未知”（OCSP服务器不能判断请求的证书状态）的响应。

证书更新

当证书过期、密钥泄露时，PKI实体必须更换证书，可以通过重新申请来达到更新的目的，也可以使用SCEP或CMPv2协议自动进行更新。

设备在证书即将过期前，先申请一个证书作为“影子证书”，在当前证书过期后，影子证书成为当前证书，完成证书更新功能。

申请“影子证书”的过程，实质上是一个新的证书注册的过程。

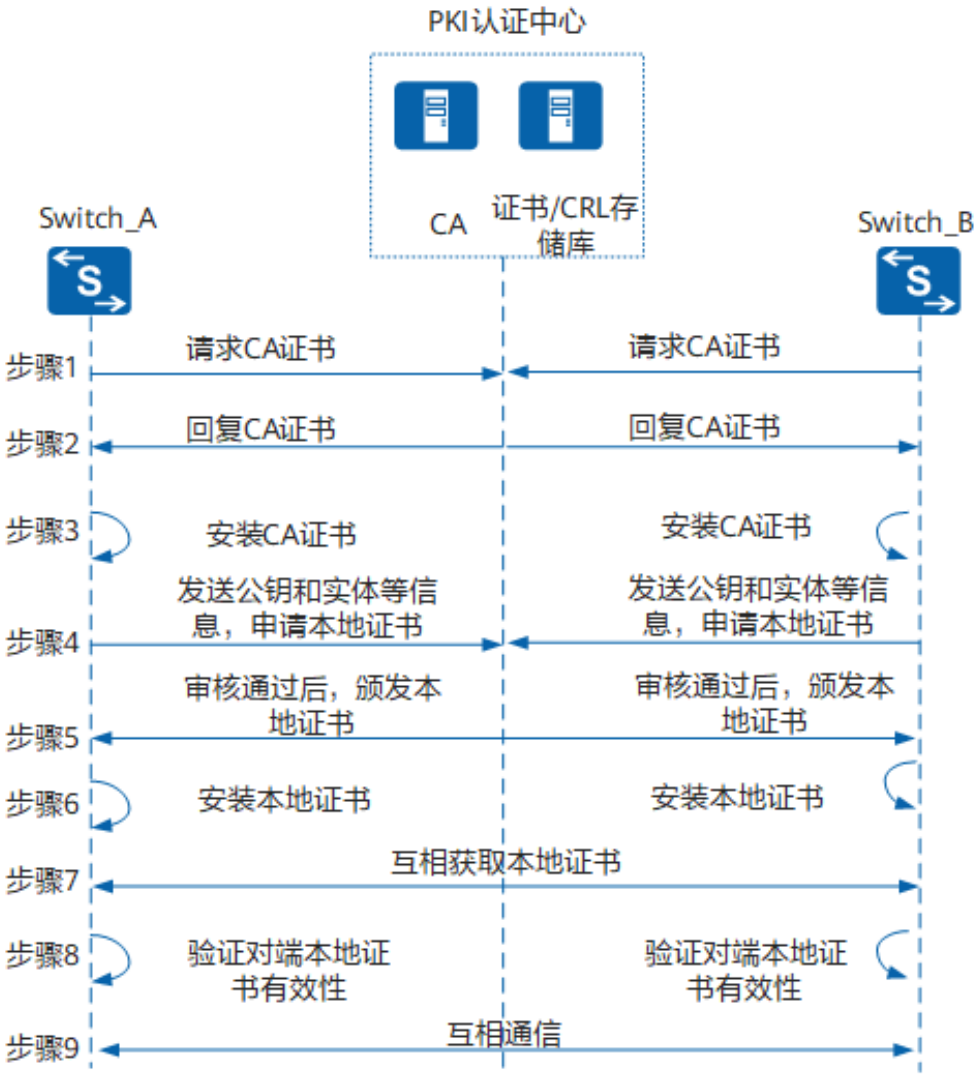
证书撤销

由于用户身份、用户信息或者用户公钥的改变、用户业务中止等原因，用户需要将自己的数字证书撤销，即撤销公钥与用户身份信息的绑定关系。在PKI中，CA主要采用CRL或OCSP协议撤销证书，而PKI实体撤销自己的证书是通过带外方式申请。

15.2.3 PKI 工作机制

针对一个使用PKI的网络，配置PKI的目的就是为指定的PKI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。PKI具体工作过程如**图15-9**所示。

图 15-9 PKI 工作过程示意图



1. PKI实体向CA请求CA证书，即CA服务器证书。
2. CA收到PKI实体的CA证书请求时，将自己的CA证书回复给PKI实体。
3. PKI实体收到CA证书后，安装CA证书。

   当PKI实体通过SCEP协议申请本地证书时，PKI实体会用配置的HASH算法对CA证书进行运算得到数字指纹，与提前配置的CA服务器的数字指纹进行比较，如果一致，则PKI实体接受CA证书，否则PKI实体丢弃CA证书。
4. PKI实体向CA发送证书注册请求消息（包括配置的密钥对中的公钥和PKI实体信息）。

   当PKI实体通过SCEP协议申请本地证书时，PKI实体对证书注册请求消息使用CA证书的公钥进行加密和自己的私钥进行数字签名。如果CA要求验证挑战密码，则证书注册请求消息必须携带挑战密码（与CA的挑战密码一致）。

   当PKI实体通过CMPv2协议申请本地证书时，PKI实体可以使用额外证书（其他CA颁发的本地证书）或者消息认证码方式进行身份认证。

   - 额外证书方式

PKI实体对证书注册请求消息使用CA证书的公钥进行加密和PKI实体的额外证书相对应的私钥进行数字签名。

- 消息认证码方式

  PKI实体对证书注册请求消息使用CA证书的公钥进行加密，而且证书注册请求消息必须包含消息认证码的参考值和秘密值（与CA的消息认证码的参考值和秘密值一致）。

5. CA收到PKI实体的证书注册请求消息。

   当PKI实体通过SCEP协议申请本地证书时，CA使用自己的私钥解密和PKI实体的公钥解密数字签名并验证数字指纹。数字指纹一致时，CA才会审核PKI实体身份等信息，审核通过后，同意PKI实体的申请，颁发本地证书。然后CA使用PKI实体的公钥进行加密和自己的私钥进行数字签名，将证书发送给PKI实体，也会发送到证书/CRL存储库。

   当PKI实体通过CMPv2协议申请本地证书时：

   - 额外证书方式

     CA使用自己的私钥解密和PKI实体的额外证书中的公钥解密数字签名并验证数字指纹。数字指纹一致时，CA才会审核PKI实体身份等信息，审核通过后，同意PKI实体的申请，颁发本地证书。然后CA使用PKI实体的额外证书中的公钥进行加密和自己的私钥进行数字签名，将证书发送给PKI实体，也会发送到证书/CRL存储库。

   - 消息认证码方式

     CA使用自己的私钥解密后，并验证消息认证码的参考值和秘密值。参考值和秘密值一致时，CA才会审核PKI实体身份等信息，审核通过后，同意PKI实体的申请，颁发本地证书。然后CA使用PKI实体的公钥进行加密，将证书发送给PKI实体，也会发送到证书/CRL存储库。

6. PKI实体收到CA发送的证书信息。

   当PKI实体通过SCEP协议申请本地证书时，PKI实体使用自己的私钥解密，并使用CA的公钥解密数字签名并验证数字指纹。数字指纹一致时，PKI实体接受证书信息，然后安装本地证书。

   当PKI实体通过CMPv2协议申请本地证书时：

   - 额外证书方式

     PKI实体使用额外证书相对应的私钥解密，并使用CA的公钥解密数字签名并验证数字指纹。数字指纹一致时，PKI实体接受证书信息，然后安装本地证书。

   - 消息认证码方式

     PKI实体使用自己的私钥解密，并验证消息认证码的参考值和秘密值。参考值和秘密值一致时，PKI实体接受证书信息，然后安装本地证书。

7. PKI实体间互相通信时，需各自获取并安装对端实体的本地证书。PKI实体可以通过HTTP等方式下载对端的本地证书。在一些特殊的场景中，例如IPSec，PKI实体会把各自的本地证书发送给对端。
8. PKI实体安装对端实体的本地证书后，通过CRL或OCSP方式验证对端实体的本地证书的有效性。
9. 对端实体的本地证书有效时，PKI实体间才可以使用对端证书的公钥进行加密通信。

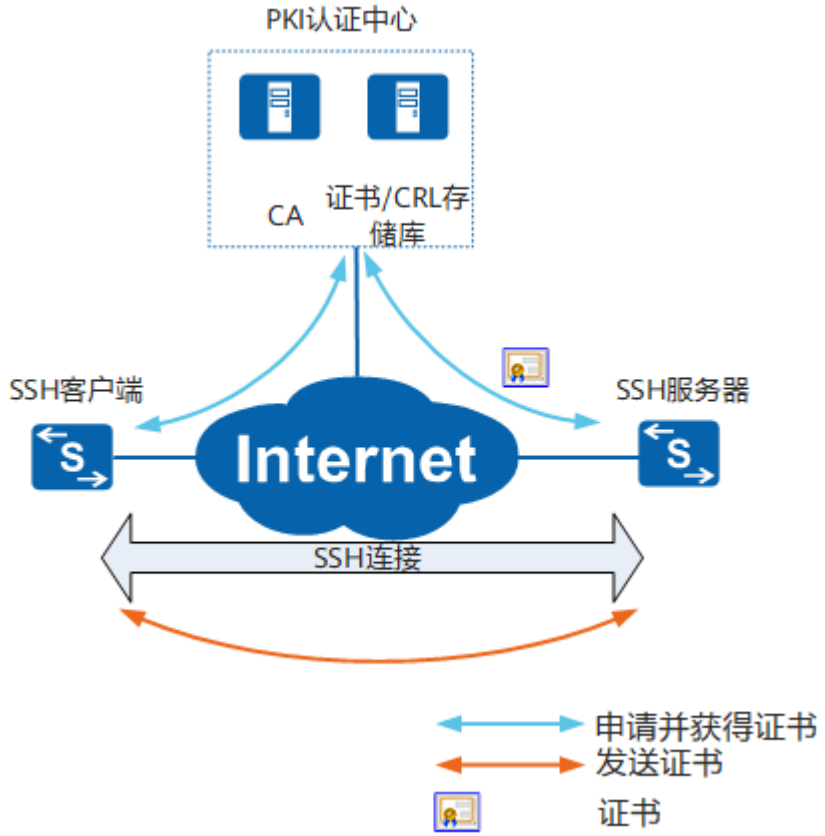
如果PKI认证中心有RA，则PKI实体也会下载RA证书。由RA审核PKI实体的本地证书申请，审核通过后将申请信息发送给CA来颁发本地证书。

15.3 PKI 应用场景

15.3.1 在 SSH 中的应用

如图15-10所示，SSH客户端可以通过SSH方式安全地访问SSH服务器的Web界面，并通过Web界面对设备进行管理。为了提高双方建立SSH连接时的安全性，在设备上为SSH客户端和服务器指定CA颁发的本地证书。这样，双方进行SSH连接时先验证双方的证书，证书验证通过后，双方才可以建立SSH连接，避免了可能存在的主动攻击。

图 15-10 在 SSH 中的应用组网图



在SSH连接建立的过程中，SSH客户端和SSH服务器之间的主要交互流程如下：

1. SSH客户端和服务器向PKI认证中心申请本地证书。
2. PKI认证中心向SSH客户端和服务器颁发本地证书。
3. SSH客户端向SSH服务器发起SSH连接请求，并将携带自己的本地证书发送给SSH服务器。
4. SSH服务器验证SSH客户端的本地证书合法后，向SSH客户端发起反向SSH连接请求，并将自己的本地证书发送给SSH客户端。
5. SSH客户端验证SSH服务器的本地证书合法后，将认证结果发送给SSH服务器。双方的SSH连接建立成功。

15.4 PKI 配置注意事项

涉及网元

在智简园区网络解决方案中，应用PKI特性涉及以下网元：

- PKI认证中心（包含CA服务器、证书/CRL存储服务器等）
- SSH客户端（比如交换机）
- SSH服务器（支持NETCONF over SSH模式的第三方网管或iMaster NCE-Campus）

License 支持

PKI是交换机的基本特性，无需获得License许可即可应用此功能。

V200R021C00、V200R021C01 版本特性支持情况

S600-E系列交换机中所有款型均支持PKI。

说明

如需了解交换机软件配套详细信息，请点击**Info-Finder**。

特性依赖和限制

对于V200R013C00及之后版本，在堆叠场景中，备设备不支持自动备份主设备的RSA密钥对，当主备切换时，备设备将无法备份主设备PKI域下的**rsa local-key-pair** *key-name*命令，因此需要用户先在备/从设备上手工创建相应的RSA密钥对。

15.5 PKI 缺省配置

表 15-3 PKI 的缺省配置

参数	缺省值
PKI实体	无
PKI域	default
RSA密钥对	default
设备保存证书请求、证书和CRL时的文件格式	PEM
证书状态检查方式	CRL方式

15.6 PKI 配置任务概览

PKI配置任务如**表15-4**所示。

表 15-4 PKI 配置任务概览

场景	描述	对应任务
在线申请本地证书	用户可以使用SCEP或CMPv2协议在线申请本地证书。使用SCEP或CMPv2协议都可以自动更新证书，SCEP比CMPv2协议维护更方便，但使用CMPv2协议可以为其他设备申请本地证书。	使用SCEP协议申请本地证书时，请按照如下顺序依次配置： 1. **15.7 申请本地证书的预配置** 2. **15.8 申请和更新本地证书**中的**15.8.1 配置通过SCEP协议为PKI实体申请和更新本地证书** 3. **15.11 验证CA证书和本地证书** 使用CMPv2协议申请本地证书时，请按照如下顺序依次配置： 1. **15.7 申请本地证书的预配置** 2. **15.8 申请和更新本地证书**中的**15.8.2 配置通过CMPv2协议为PKI实体申请和更新本地证书** 3. **15.10 （可选）安装本地证书** 4. **15.11 验证CA证书和本地证书**

场景	描述	对应任务
离线申请本地证书	如果受网络环境限制，设备无法访问CA服务器，可选择离线申请本地证书。 用户可以通过设备生成证书申请文件，然后通过带外方式（Web、磁盘、电子邮件等）将证书申请文件发送给CA申请本地证书;也可以无需通过设备生成证书申请文件，直接通过Web方式将申请证书信息发送给CA申请本地证书。	通过设备生成证书申请文件时，请按照如下顺序依次配置： 1. **15.7 申请本地证书的预配置** 2. **15.8 申请和更新本地证书**中的**15.8.3 配置为PKI实体离线申请本地证书** 3. **15.9 （可选）下载本地证书** 4. **15.10 （可选）安装本地证书** 5. **15.11 验证CA证书和本地证书** 未通过设备生成证书申请文件时，请按照如下顺序依次配置： 1. 直接通过Web方式将申请证书信息发送给CA申请本地证书 2. 下载CA提供的CA证书、本地证书和密钥对并上传至设备的存储介质中 3. 安装密钥对，请参考**15.7 申请本地证书的预配置**中的**15.7.2 配置RSA密钥对** 4. 安装CA证书，请参考**15.7 申请本地证书的预配置**中的**15.7.3.2 （可选）配置为PKI实体安装CA证书** 5. 安装本地证书，请参考**15.10 （可选）安装本地证书** 6. 验证证书，请参考**15.11 验证CA证书和本地证书**

15.7 申请本地证书的预配置

15.7.1 配置 PKI 实体信息

背景信息

本地证书是由CA进行数字签名并颁发的。它是公钥与PKI实体身份信息的绑定。PKI实体信息就是PKI实体的身份信息，CA根据PKI实体提供的身份信息来唯一标识证书申请者。因此，申请本地证书时，PKI实体必须将包含PKI实体信息的证书注册请求消息发送给CA。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**pki entity** *entity-name*，创建PKI实体并进入PKI实体视图，或者直接进入PKI实体视图。

缺省情况下，系统未配置PKI实体。

说明

由于Windows Server 2003服务器处理能力有限，与该型号服务器对接时，设备上不能配置过多实体信息或携带密钥对位数过大的密钥对，否则可能导致设备与服务器对接失败。

步骤3 执行命令**common-name** *common-name*，配置PKI实体的通用名称。

缺省情况下，系统未配置PKI实体的通用名称。

为了更好的标识证书申请者的唯一身份，还需配置以下可选步骤的参数，作为PKI实体的一种别名。否则，当PKI实体间的通用名称相同时，会导致某PKI实体申请证书失败。

步骤4 （可选）执行命令**ip-address** { *ipv4-address* | *interface-type interface-number* }，配置PKI实体的IP地址。

缺省情况下，系统未配置PKI实体的IP地址。

步骤5 （可选）执行命令**fqdn** *fqdn-name*，配置PKI实体的FQDN名称。

缺省情况下，系统未配置PKI实体的FQDN名称。

步骤6 （可选）执行命令**email** *email-address*，配置PKI实体的电子邮箱地址。

缺省情况下，系统未配置PKI实体的电子邮箱地址。

步骤7 （可选）执行命令**country** *country-code*，配置PKI实体所属的国家代码。

缺省情况下，系统未配置PKI实体的国家代码。

步骤8 （可选）执行命令**locality** *locality-name*，配置PKI实体所在的地理区域名称。

缺省情况下，系统未配置PKI实体的地理区域名称。

步骤9 （可选）执行命令**state** *state-name*，配置PKI实体所属的州或省。

缺省情况下，系统未配置PKI实体所属的州或者省。

步骤10 （可选）执行命令**organization** *organization-name*，配置PKI实体所属的组织名称。

缺省情况下，系统未配置PKI实体的组织名称。

步骤11 （可选）执行命令**organization-unit** *organization-unit-name*，配置PKI实体所属的部门名称。

缺省情况下，系统未配置PKI实体所在的部门名称。

----结束

15.7.2 配置 RSA 密钥对

背景信息

本地证书是由CA进行数字签名并颁发的。它是公钥与PKI实体身份信息的绑定。因此，申请本地证书时，需先配置RSA密钥对生成公钥和私钥。公钥由PKI实体发送给CA，可以被对端用来加密明文；私钥由PKI实体保留，可以被用来数字签名和解密对端发送过来的密文。

配置RSA密钥对有以下两种方式：

- 创建RSA密钥对

  设备上可以直接创建密钥对，无需再导入密钥对到设备的内存中。
- 导入RSA密钥对

  当需要使用其他PKI实体产生的密钥对时，可以通过FTP/SFTP传到设备上，然后导入密钥对到设备的内存中，否则密钥对不生效。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 请根据实际情况选择配置。

- 创建RSA密钥对

  执行命令**pki rsa local-key-pair create** *key-name* [**modulus** *modulus-size*] [**exportable**]，创建证书申请时使用的RSA密钥对。
- 导入RSA密钥对

  执行命令**pki import rsa-key-pair** *key-name* [**include-cert realm** *realm-name*] { **pem** | **pkcs12** } *file-name* [**exportable**] [**password** *password*]或执行命令**pki import rsa-key-pair** *key-name* **der** *file-name* [**exportable**]，将RSA密钥对和证书导入设备的内存中。

  说明

  仅当配置**exportable**参数时，创建的RSA密钥对才可以被导出。

  由于Windows Server 2003服务器处理能力有限，与该型号服务器对接时，设备上不能配置过多实体信息或携带密钥对位数过大的密钥对，否则可能导致设备与服务器对接失败。

----结束

后续处理

- 当需要备份RSA密钥对或者RSA密钥对给其他设备使用时，可以执行命令**pki export rsa-key-pair** *key-name* [**and-certificate** *certificate-name*] { **pem** *file-name* **aes** | **pkcs12** *file-name* } **password** *password*，将RSA密钥对导出到设备的存储介质中，同时支持导出与其关联的证书。然后用户可以通过FTP/SFTP获取RSA密钥对。
- RSA密钥对泄露、损坏、不用或丢失时，可以执行命令**pki rsa local-key-pair destroy** *key-name*，销毁指定的RSA密钥对。

  配置后，系统会销毁设备中对应名称的RSA密钥对，以及备设备中对应名称的RSA密钥对。
- 用户不知道证书所对应的RSA密钥对时，可以执行命令**pki match-rsa-key certificate-filename** *file-name*，查找证书所对应的RSA密钥对。

15.7.3 配置为 PKI 实体获取 CA 证书

背景信息

申请本地证书时，PKI实体会将证书注册请求消息发送给CA。为了提高传输过程中的安全性，PKI实体必须使用CA的公钥对证书注册请求消息进行加密保护。因此，PKI实体必须先获取到CA证书，并从CA证书中获取CA的公钥。

说明

设备出厂时已经在**default**域预置了CA和本地证书，可以执行命令**display pki certificate ca realm** *default*查看CA证书信息。

配置流程

PKI实体获取CA证书需要先下载CA证书，然后再安装CA证书。

15.7.3.1 配置为 PKI 实体下载 CA 证书

背景信息

下载CA证书有如下几种方式，请根据CA提供的服务方式选择。

- 通过SCEP协议从CA服务器下载CA证书，将CA证书下载到设备的存储介质中。
- 通过HTTP协议从Web服务器上下载CA证书，将CA证书下载到设备的存储介质中。
- 通过CMPv2协议从CMPv2服务器下载CA证书，将CA证书下载到设备的存储介质中。
- 通过带外方式（Web、磁盘、电子邮件等）获得CA证书后，上传到设备的存储介质中。

如果通过CMPv2协议申请本地证书时，这里下载的CA证书为CA服务器的根证书。

操作步骤

- 通过SCEP协议下载CA证书。

  通过SCEP协议下载CA证书的具体配置请参见**15.8.1 配置通过SCEP协议为PKI实体申请和更新本地证书**。
- 通过HTTP方式下载CA证书。
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pki http** [**esc**] *url-address save-name*，配置通过HTTP方式下载CA证书。

     *url-address*必须包含完整的证书文件及扩展名，例如http://10.1.1.1:8080/cert.cer。如果设置为域名方式，必须保证该域名可以正常解析。
- 通过CMPv2协议下载CA证书。

  通过CMPv2协议下载CA证书的具体配置请参见**15.8.2 配置通过CMPv2协议为PKI实体申请和更新本地证书**。
- 通过带外方式下载CA证书。

用户通过Web、磁盘、电子邮件等方式获得CA证书后，需要手工上传到设备的存储介质中。也可以选择通过管理PC下载证书后，使用FTP/SFTP或Web方式上传到设备的存储介质中。

----结束

15.7.3.2 （可选）配置为 PKI 实体安装 CA 证书

背景信息

下载的CA证书只有导入到设备的内存中才可以正常生效，并且设备会将导入内存证书文件保存到缺省目录下的**ca_config.ini**文件中，在重启后可以自动加载文件中记录的证书文件。

说明

请确保CA证书文件不超过1M，避免安装失败。

配置通过SCEP协议申请本地证书时，设备会自动安装CA证书，无需手动安装CA证书。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**pki import-certificate ca realm** *realm-name* { **der** | **pkcs12** | **pem** } [**filename** *filename*] [**replace**] [**no-check-validate**] [**no-check-hash-alg**]或执行命令**pki import-certificate ca realm** *realm-name* **pkcs12 filename** *filename* [**no-check-validate**] [**no-check-hash-alg**] **password** *password*，将CA证书导入到设备的内存中。

步骤3 （可选）执行命令**pki set-certificate expire-prewarning** *day*，配置内存中的CA证书的过期预告警时间。

缺省情况下，内存中的CA证书的过期预告警时间为7天。

----结束

后续处理

- 如果需要把CA证书拷贝到其他设备上使用，可以执行命令**pki export-certificate ca realm** *realm-name* { **pem** | **pkcs12** } [**filename** *filename*]，将CA证书导出到设备存储介质中。然后，用户可以通过FTP/SFTP取出CA证书。
- 如果CA证书过期或者不用，可以执行命令**pki delete-certificate ca realm** *realm-name*，从内存中删除CA证书。

15.7.4 检查申请本地证书的预配置的配置结果

前提条件

已经完成配置PKI实体信息、RSA密钥对或者CA证书。

操作步骤

- 执行命令**display pki entity** [*entity-name*]，查看PKI实体信息。

- 执行命令**display pki rsa local-key-pair** { **pem** | **pkcs12** } *filename* [**password** *password*]，查看RSA密钥对信息。
- 执行命令**display pki rsa local-key-pair** [**name** *key-name*] **public** [**temporary**]，查看RSA公钥信息。
- 执行命令**display pki realm** [*realm-name*]，查看PKI域的信息。
- 执行命令**display pki certificate ca realm** *realm-name*，查看设备上已加载的CA证书的内容。
- 执行命令**display pki credential-storage-path**，查看证书的缺省保存路径。
- 执行命令**display pki ca-capability realm** *realm-name*，查看PKI域相对应的CA能力。

----结束

15.8 申请和更新本地证书

背景信息

说明

设备出厂时已经在**default**域预置了CA和本地证书，可以执行命令**display pki certificate local realm** *default*查看本地证书信息。

前置任务

在申请和更新本地证书之前，需完成**15.7 申请本地证书的预配置**。

配置流程

请根据CA提供的服务方式选择配置申请和更新本地证书的方式。

15.8.1 配置通过 SCEP 协议为 PKI 实体申请和更新本地证书

背景信息

配置通过SCEP协议为PKI实体申请本地证书，有两种方式：

- 自动触发申请和更新本地证书

  如果本地证书需要的配置信息齐全并且设备没有本地证书时，将自动触发设备通过SCEP协议申请本地证书；或者当证书即将过期、已经过期、已到达指定百分比时，自动触发设备通过SCEP协议申请并更新证书。
- 手动触发申请本地证书

  如果本地证书需要的配置信息齐全并且设备没有本地证书时，将手动触发设备通过SCEP协议申请本地证书，当证书即将过期、已经过期、已到达指定百分比时，不会自动触发设备通过SCEP协议申请并更新证书。

这两种方式申请本地证书时，设备都会先向CA获取CA证书保存到存储介质中并将CA证书自动导入设备的内存中，然后使用CA证书的公钥加密证书注册请求消息并发送给CA来申请本地证书，获取本地证书保存到存储介质中并将本地证书自动导入设备的内存中。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**pki file-format** { **der** | **pem** }，配置设备保存证书时的文件格式。

缺省情况下，设备保存证书时的文件格式为PEM。

步骤3 执行命令**pki realm** *realm-name*，创建PKI域并进入PKI域视图，或者直接进入PKI域视图。

缺省情况下，设备存在名称为**default**的PKI域，且该域只能修改不能删除。

PKI域是一个本地概念，一个设备上配置的PKI域对CA和其他设备是不可见的，每一个PKI域有单独的参数配置信息。

步骤4 执行命令**ca id** *ca-name*，配置PKI域信任的CA。

缺省情况下，系统未配置PKI域信任的CA。

*ca-name*通常指的是CA服务器的名称。

步骤5 执行命令**entity** *entity-name*，指定申请证书的PKI实体。

缺省情况下，系统未指定申请证书的PKI实体。

*entity-name*是一个已经通过**pki entity**命令创建的PKI实体。

步骤6 执行命令**rsa local-key-pair** *key-name*，配置使用SCEP方式申请证书时使用的RSA密钥对。

缺省情况下，系统未配置使用SCEP方式申请证书时使用的RSA密钥对。

*key-name*是一个已经通过**pki rsa local-key-pair create**命令创建的RSA密钥对。

步骤7 （可选）执行命令**key-usage** { **ike** | **ssl-client** | **ssl-server** } *，配置证书公钥用途属性。

缺省情况下，系统未配置证书公钥用途属性。

步骤8 （可选）执行命令**source** { **interface** *interface-type interface-number* | *ip-address* }，配置建立TCP连接使用的源地址。

缺省情况下，设备使用出接口的IP地址作为建立TCP连接的源地址。

如果指定接口，请确保该接口为三层接口，且接口下已经配置了IP地址。

步骤9 执行命令**enrollment-url** [**esc**] *url* [**interval** *minutes*] [**times** *count*] [**ra**]，配置CA服务器的URL。

缺省情况下，系统未配置CA服务器的URL。

配置时，需注意：

- 未配置**esc**参数时，URL地址格式为**http://*server_location*/*ca_script_location***。
  其中，*server_location*目前支持IP地址和域名解析的表示方式。*ca_script_location*是在CA服务器主机上的应用程序脚本的路径。比如：服务器版本的Windows系统作为CA服务器时，URL的格式为**http://*host*:*port*/certsrv/mscep/mscep.dll**，其中*host*为CA服务器的IP地址，*port*为CA服务器的端口号。服务器的IP为10.137.145.158，端口为8080时，URL为**http://10.137.145.158:8080/certsrv/mscep/mscep.dll**。

- 配置**esc**参数时，支持以ASCII码形式输入包含“?”的URL地址。

  关键字**esc**作用是支持以ASCII码形式输入包含“?”的URL地址，格式必须为“\x3f”，3f为字符“?”的16进制ASCII码。例如，如果用户想输入“http://***.com?page1”，则对应的URL为“http://***.com\x3fpage1”；如果用户想同时输入“?”和“\x3f”（http://www.***.com?page1\x3f），则对应的URL为“http://www.***.com\x3fpage1\\x3f”。

- 如果在CA服务器使用手工方式处理证书请求，证书发布可能需要较长时间。申请证书的PKI实体需要周期性发送查询，以便在证书颁发后能够及时获取到证书。此时，可以增大**interval**和**times**参数来调整注册证书状态查询的时间间隔和最大查询次数。
- 配置**ra**参数时，指定RA审核PKI实体申请本地证书时的身份信息。缺省情况下，CA审核PKI实体申请本地证书时的身份信息。

步骤10 执行命令**enrollment-request signature message-digest-method** { **md5** | **sha-256** | **sha-384** | **sha-512** }，配置签名证书注册请求消息使用的摘要算法。

缺省情况下，签名证书注册请求消息使用的摘要算法为**sha-256**。

md5算法为不安全算法，建议使用SHA2算法。

PKI实体使用的摘要算法必须与CA服务器上的摘要算法一致。

步骤11 执行命令**password cipher** *password*，配置SCEP证书申请时使用的挑战密码，也是证书撤销密码。

缺省情况下，系统未配置SCEP证书申请时使用的挑战密码。

PKI实体使用的挑战密码必须与CA服务器上设置的密码一致。如果CA服务器不要求使用挑战密码，则不用配置挑战密码。

步骤12 执行命令**fingerprint** { **md5** | **sha1** | **sha256** } *fingerprint*，配置对CA证书进行验证时使用的CA证书数字指纹。

缺省情况下，系统未配置对CA证书进行验证时使用的CA证书数字指纹。

*fingerprint*参数需要通过离线的方式从CA服务器上获取。例如，当Windows Server 2008作为CA服务器时，可以通过登录网页http://host:port/certsrv/mscep_admin/获得CA证书指纹信息，其中host为CA服务器的IP地址，port为CA服务器的端口号。

步骤13 配置申请和更新本地证书的方式，请根据情况选择配置。

- 配置自动触发申请和更新本地证书。

  执行命令**auto-enroll** [*percent*] [**regenerate** [*key-bit*]] [**updated-effective**]，开启证书自动注册和更新功能。

  缺省情况下，证书自动注册和更新功能处于关闭状态。

- 配置手动触发申请本地证书。

  a. 执行命令**quit**，返回至系统视图。

  b. 执行命令**pki enroll-certificate realm** *realm-name* [**password** *password*]，配置手工触发设备申请证书。

  如果配置了**password**命令，这里的**password**参数可以不用。如果都配置，这里配置的**password**优先级高。

----结束

15.8.2 配置通过 CMPv2 协议为 PKI 实体申请和更新本地证书

背景信息

当设备可以访问CA，并且CA支持CMPv2协议时，可选择此方式申请和更新本地证书。

通过CMPv2协议申请本地证书有两种情况：

- 首次申请本地证书IR（Initialization Request）

  首次证书申请适用于设备第一次向CA申请证书的情况。在这种情况下，设备提供以下两种向CMPv2服务器进行身份认证的方式。

  - 消息认证码方式：设备和CMPv2服务器共享一对消息认证码的参考值和秘密值。在进行首次证书申请的时候，设备会将这对参考值和秘密值加入到请求报文当中发送到CMPv2服务器，CMPv2服务器通过验证参考值和秘密值来鉴定设备的身份。
  - 签名方式：通过CMPv2协议的IR请求，向CA发起证书请求时，设备使用其他CA颁发的证书相对应的私钥来签名保护。

- 为其他设备申请本地证书CR（Certification Request）

  证书申请适用于当设备已经有了CA所颁发的本地证书，而需要申请额外的证书的情况。在这种情况下，设备会使用已经有的证书作为身份认证的手段。

通过CMPv2协议更新本地证书有两种方式：

- 手工更新证书，即密钥更新请求KUR（Key Update Request）

  密钥更新请求又称为证书更新请求，是对设备已有的证书（尚未过期且没有被吊销）进行更新操作。在更新过程中，使用现有的证书作为身份认证的手段。更新操作可以使用新的公钥，也可以使用原来的公钥。

  通过IR方式申请本地证书，安全性较低，建议通过KUR方式更新本地证书及密钥对。

- 自动更新证书

  为了避免业务的中断，在有效期截止前必须申请新的证书，而使用手工更新证书的方式容易出现忘记更新证书的情况。设备支持证书的自动更新功能，当系统检测到时间超过了设置的证书自动更新时间之后，会自动向CMPv2服务器发起证书的更新请求。申请的新证书会同时替换存储介质中的证书文件和内存中对应的证书，业务不会中断。

  此方式可以对IR方式申请的本地证书或KUR方式更新的本地证书进行自动更新。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**pki file-format** { **der** | **pem** }，配置设备保存证书时的文件格式。

缺省情况下，设备保存证书时的文件格式为PEM。

步骤3 执行命令**pki realm** *realm-name*，创建PKI域并进入PKI域视图，或者直接进入PKI域视图。

缺省情况下，系统未创建PKI域。

步骤4 执行命令**quit**，返回至系统视图。

步骤5 执行命令**pki cmp session** *session-name*，创建CMP会话并进入CMP会话视图，或者直接进入CMP会话视图。

缺省情况下，系统未创建CMP会话。

CMP会话是一个本地概念，一个设备上配置的CMP会话对CA和其他设备是不可见的。

步骤6 执行命令**cmp-request entity** *entity-name*，配置设备使用CMPv2方式申请证书时使用的PKI实体名称。

缺省情况下，系统未配置CMPv2方式申请证书时使用的PKI实体名称。

步骤7 执行命令**cmp-request ca-name** *ca-name*，为CMP会话配置CA的名称。

缺省情况下，系统未配置CMP会话下的CA名称。

配置的CA名称中各个字段的顺序必须要和实际CA证书中的顺序保持一致，否则CMPv2服务器会认为是错误的。

步骤8 执行命令**cmp-request server url** [**esc**] *url-addr*，配置CMPv2服务器的URL。

缺省情况下，系统未配置CMPv2服务器的URL。

*url-addr*可以设置为IP地址形式或域名形式，如果设置为域名形式，必须在PKI实体上正确配置DNS，使PKI实体可以通过DNS服务器解析域名。

步骤9 执行命令**cmp-request rsa local-key-pair** *key-name* [**regenerate** [*key-bit*]]，配置CMPv2方式申请证书时使用的RSA密钥对。

缺省情况下，系统未配置CMPv2方式申请证书时使用的RSA密钥对。

如果配置了**regenerate**参数，则证书自动更新时，系统会生成新的RSA密钥对去申请新证书，并且用新的证书和RSA密钥对替换原有的证书和RSA密钥对。否则证书自动更新时，系统会继续使用原来的RSA密钥对。

步骤10 执行命令**cmp-request realm** *realm-name*，配置使用CMPv2方式申请证书时使用的域名称。

缺省情况下，系统未配置CMPv2方式申请证书时使用的PKI域。

步骤11 （可选）执行命令**cmp-request verification-cert** *cert-file-name*，配置验证CA响应签名的证书文件。

缺省情况下，系统未配置验证CA响应签名的证书文件。

- 如果配置了此命令，并且服务器的响应报文是签名的方式时，则设备使用该命令行配置的证书来验证服务器的响应签名。此处配置的证书为CA证书，即CA自身的证书。
- 如果未配置此命令，并且服务器的响应报文是签名的方式时，则依据设备以及服务器响应中的证书构建证书链，验证服务器的响应签名；如果服务器使用消息认证码方式做保护时，则设备使用配置的消息认证码来验证服务器的响应报文，不受该命令配置影响。

步骤12 请根据实际情况选择配置来申请本地证书。

- 首次申请本地证书（IR）
  a. 执行命令**cmp-request origin-authentication-method** { **message-authentication-code** | **signature** }，配置使用CMPv2协议进行首次证书申请（IR）的认证方式。

缺省情况下，使用CMPv2协议进行首次证书申请（IR）的认证方式为消息认证码方式。

- **message-authentication-code**表示消息认证码方式。选择此方式时请执行**步骤12.b**。
- **signature**表示签名方式。选择此方式时请执行**步骤12.c**。

b. 执行命令**cmp-request message-authentication-code** *reference-value secret-value*，配置消息认证码的参考值和秘密值。

缺省情况下，系统未配置消息认证码的参考值和秘密值。

消息认证码的参考值和秘密值，需要用户以带外方式从CMPv2服务器上获取。

c. 执行命令**cmp-request authentication-cert** *cert-name*，配置CMPv2请求中用于证明身份的证书。

缺省情况下，系统未配置CMPv2请求中用于证明身份的证书。

此证书是额外证书，并且必须由受CA信任的证书申请机构为设备颁发。

d. 执行命令**quit**，返回至系统视图。

e. 执行命令**pki cmp initial-request session** *session-name*，根据CMP会话的配置信息向CMPv2服务器进行首次证书申请（IR）。

配置后，系统首先会检查CMP会话中的配置是否可以进行证书申请。如果条件不满足，会给出错误的提示信息。如果条件满足，会依据配置内容发起首次证书请求。申请下来的证书将以文件的形式保存到存储介质中，不会执行导入内存的操作。同时，若服务器端在响应中给出CA证书，则CA证书也会以文件形式保存起来。

- 为其他设备申请本地证书（CR）

a. 执行命令**cmp-request authentication-cert** *cert-name*，配置CMPv2请求中用于证明身份的证书。

缺省情况下，系统未配置CMPv2请求中用于证明身份的证书。

此证书是CA已经颁发给设备的本地证书。

b. 执行命令**quit**，返回至系统视图。

c. 执行命令**pki cmp certificate-request session** *session-name*，根据CMP会话的配置信息向CMPv2服务器进行证书申请（CR）。

配置后，系统首先会检查CMP会话中的配置是否可以进行证书更新申请。如果条件不满足，会给出错误的提示信息。如果条件满足，会依据配置内容发起证书更新请求。申请下来的证书将以文件的形式保存到存储介质中，不会执行导入内存的操作。

步骤13 请根据实际情况选择配置来更新本地证书。

- 手工更新本地证书（KUR）

a. 执行命令**pki cmp session** *session-name*，直接进入CMP会话视图。

b. 执行命令**cmp-request authentication-cert** *cert-name*，配置CMPv2请求中用于证明身份的证书。

缺省情况下，系统未配置CMPv2请求中用于证明身份的证书。

此证书是CA已经颁发给设备的本地证书，同时也是将要被更新的本地证书。

c. 执行命令**quit**，返回至系统视图。

d. 执行命令**pki cmp keyupdate-request session** *session-name*，根据CMP会话的配置信息向CMPv2服务器进行密钥更新请求（KUR）。

向CMPv2服务器进行密钥更新请求时，同时也会重新申请本地证书。

配置后，系统首先会检查CMP会话中的配置是否可以进行证书更新申请。如果条件不满足，会给出错误的提示信息。如果条件满足，会依据配置内容发起证书更新请求。申请下来的证书将以文件的形式保存到存储介质中，不会执行导入内存的操作。

- 自动更新证书
  a. 执行命令**pki cmp session** *session-name*，直接进入CMP会话视图。
  b. 执行命令**cmp-request authentication-cert** *cert-name*，配置CMPv2请求中用于证明身份的证书。

     缺省情况下，系统未配置CMPv2请求中用于证明身份的证书。

     此证书是CA已经颁发给设备的本地证书，同时也是将要被更新的本地证书。
  c. 执行命令**certificate auto-update enable**，开启使用CMPv2方式自动更新证书功能。

     缺省情况下，使用CMPv2方式自动更新证书功能处于关闭状态。
  d. 执行命令**certificate update expire-time** *valid-percent*，配置证书自动更新的时间，以当前使用证书有效期的百分比形式体现。

     缺省情况下，证书更新时间的默认百分比是50%。

     配置后，当系统检测到时间达到*valid-percent*时，会自动发起证书更新请求，并依据**cmp-request rsa local-key-pair**命令的配置决定是否创建新的RSA密钥对。申请到新的证书后，系统会使用新的证书和RSA密钥对替换原有的证书和RSA密钥对。
  e. 执行命令**quit**，返回至系统视图。

步骤14 （可选）执行命令**undo pki cmp poll-request session** *session-name*，取消正在进行的CMP轮询请求。

当客户端发起证书相关的请求时，如果服务器不能够马上给出结果，服务器会让客户端每隔一段时间发起一次轮询请求，直到给出最终的结果为止。如果用户不想继续等待，可以取消正在进行的CMP轮询请求，从而取消本次的证书申请操作。

----结束

15.8.3 配置为 PKI 实体离线申请本地证书

背景信息

如果CA服务器不支持SCEP和CMPv2协议，可以配置离线申请本地证书。用户在设备上生成证书请求文件，然后通过Web、磁盘、电子邮件等带外方式将证书申请文件发送给CA，向CA申请本地证书。完成申请后，还需从存放本地证书的服务器上下载证书，保存到设备的存储介质中。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**pki realm** *realm-name*，创建PKI域并进入PKI域视图，或者直接进入PKI域视图。

缺省情况下，设备存在名称为**default**的PKI域，且该域只能修改不能删除。

PKI域是一个本地概念，一个设备上配置的PKI域对CA和其他设备是不可见的，每一个PKI域有单独的参数配置信息。

步骤3 执行命令**entity** *entity-name*，指定申请证书的PKI实体。

缺省情况下，系统未指定申请证书的PKI实体。

*entity-name*是一个已经通过**pki entity**命令创建的PKI实体。

步骤4 执行命令**rsa local-key-pair** *key-name*，配置使用离线方式申请证书时使用的RSA密钥对。

缺省情况下，系统未配置使用离线方式申请证书时使用的RSA密钥对。

步骤5 执行命令**enrollment-request signature message-digest-method** { **md5** | **sha-256** | **sha-384** | **sha-512** }，配置签名证书注册请求消息使用的摘要算法。

缺省情况下，签名证书注册请求消息使用的摘要算法为**sha-256**。

md5算法为不安全算法，建议使用SHA2算法。

PKI实体使用的摘要算法必须与CA服务器上的摘要算法一致。

步骤6 （可选）执行命令**key-usage** { **ike** | **ssl-client** | **ssl-server** } *，配置证书公钥用途属性。

缺省情况下，系统未配置证书公钥用途属性。

步骤7 执行命令**quit**，返回至系统视图。

步骤8 执行命令**pki file-format** { **der** | **pem** }，配置设备保存证书和证书请求时的文件格式。

缺省情况下，设备保存证书和证书请求时的文件格式为PEM。

步骤9 执行命令**pki enroll-certificate realm** *realm-name* **pkcs10** [**filename** *filename*] [**password** *password*]，配置以PKCS#10格式保存证书申请信息到文件中。

PKI实体使用的挑战密码必须与CA服务器上设置的密码一致。如果CA服务器不要求使用挑战密码，则不用配置挑战密码。

步骤10 通过Web、磁盘、电子邮件等带外方式将证书申请文件发送给CA，向CA申请本地证书。

----结束

15.8.4 检查申请和更新本地证书的配置结果

前提条件

已经完成申请和更新本地证书的所有配置。

操作步骤

- 执行命令**display pki realm** [*realm-name*]，查看PKI域的信息。
- 执行命令**display pki credential-storage-path**，查看证书的缺省保存路径。
- 执行命令**display pki certificate enroll-status** [**realm** *realm-name*]，查看证书的注册状态。

- 执行命令**display pki cert-req filename** *file-name*，查看证书请求文件的内容。
- 执行命令**display pki cmp statistics** [**session** *session-name*]，查看CMP会话的统计信息。
- 执行命令**display pki certificate** { **ca** | **local** } **realm** *realm-name*，查看设备上已加载的CA证书和本地证书的内容。

----结束

15.9 （可选）下载本地证书

背景信息

通过SCEP或CMPv2协议申请本地证书时，设备会自动下载本地证书。仅当离线申请本地证书时，才需要下载本地证书。

通常采用以下方式获得本地证书，设备采用哪种方式下载证书，取决于CA服务器提供的服务方式：

- 通过HTTP协议从Web服务器上下载本地证书，将本地证书下载到设备的存储介质中。
- 通过带外方式（Web、磁盘、电子邮件等）获得本地证书后，上传到设备的存储介质中。

前置任务

已经完成本地证书的离线申请，本地证书已经在CA上注册成功。

操作步骤

- 通过HTTP方式下载本地证书。
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pki http** [**esc**] *url-address save-name*，配置通过HTTP方式下载本地证书。

     *url-address*必须包含完整的证书文件及扩展名，例如http://10.1.1.1:8080/cert.cer。如果设置为域名方式，必须保证该域名可以正常解析。
- 通过带外方式下载本地证书。

  用户通过Web、磁盘、电子邮件等方式获得本地证书后，需要手工上传到设备的存储介质中。也可以选择通过管理PC下载证书后，使用FTP/SFTP或Web方式上传到设备的存储介质中。

----结束

检查配置结果

- 执行命令**display pki credential-storage-path**，查看证书的缺省保存路径。
- 执行命令**dir（用户视图）**，查看存储器中的本地证书文件。

15.10 （可选）安装本地证书

背景信息

下载的本地证书只有导入到设备的内存中才可以正常生效，并且设备会将导入内存证书文件保存到缺省目录下的**ca_config.ini**文件中，在重启后可以自动加载文件中记录的证书文件。

前置任务

已经完成本地证书的下载，证书文件已经保存到设备的存储介质中。

说明

请确保本地证书文件不超过1M，避免安装失败。

当通过CMPv2协议或离线申请本地证书时，需要手动安装本地证书。设备通过SCEP协议申请本地证书会自动安装本地证书。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**pki import-certificate local realm** *realm-name* { **der** | **pkcs12** | **pem** } [**filename** *filename*] [**replace**] [**no-check-validate**] [**no-check-hash-alg**]或执行命令**pki import-certificate local realm** *realm-name* **pkcs12 filename** *filename* [**no-check-validate**] [**no-check-hash-alg**] **password** *password*，将本地证书导入到设备的内存中。

证书及其密钥对有两种存在形式，一种是证书文件中包含密钥对文件，两者以一个文件的形式存在；另一种是证书和密钥对相互独立以两个文件形式存在。不同形式下，将其导入内存所使用的方法不同。

- 证书文件中包含密钥对文件。

  执行命令**pki import rsa-key-pair**一次导入证书文件和密钥对文件。

  说明

  证书文件中包含密钥对文件时，执行命令**pki import-certificate**只能导入证书文件，密钥对文件不会被导入。如果需要导入密钥对文件，可执行命令**pki import rsa-key-pair**将密钥对继续导入。

- 证书文件和密钥对文件独立存在。

  a. 导入证书文件。

     执行命令**pki import-certificate**导入证书文件。

  b. 导入密钥对文件。

     执行命令**pki import rsa-key-pair**导入密钥对文件。

说明

若用户无法辨别待导入证书的格式，可依次配置不同格式并检查是否成功导入证书。若不指定待导入证书的格式，系统将自行识别导入。

步骤3 （可选）执行命令**pki set-certificate expire-prewarning** *day*，配置内存中的本地证书的过期预告警时间。

缺省情况下，内存中的本地证书的过期预告警时间为90天。

----结束

后续处理

如果需要把本地证书拷贝到其他设备上使用，可以执行命令**pki export-certificate local realm** *realm-name* { **pem** | **pkcs12** }，将本地证书导出到设备的存储介质中。然后，用户可以通过FTP/SFTP取出本地证书。

检查配置结果

执行命令**display pki certificate local realm** *realm-name*，查看设备上已加载的本地证书的内容。

15.11 验证 CA 证书和本地证书

前置任务

在验证证书之前，需完成**15.10 （可选）安装本地证书**。

配置流程

请按照以下顺序进行配置。对于可选步骤，请根据情况选择配置。

15.11.1 配置检查本地证书状态

背景信息

当验证对端实体的本地证书时，经常需要检查对端实体的本地证书是否有效，例如对端实体的本地证书是否过期、是否被加入CRL。通常检查证书状态的方式有三种：CRL方式、OCSP方式、None方式。

- CRL方式

  如果CA支持作为CRL发布点CDP（CRL Distribution Point），则当CA颁发证书时，在证书中会包含CDP信息，用以描述获取该证书CRL的途径和方式。PKI实体利用CDP中指定的机制（HTTP方式）和地址来下载CRL。

  如果PKI实体配置了CDP的URL地址，该地址将覆盖证书中携带的CDP信息，PKI实体使用配置的URL来获取CRL。如果CA不支持作为CDP，则PKI实体可以使用SCEP方式下载CRL。

  当PKI实体验证本地证书时，先查找本地内存的CRL，如果本地内存没有CRL，则需下载CRL并安装到本地内存中，如果对端实体的本地证书在CRL中，表示此证书已被撤销。

- OCSP方式

  在IPSec场景中，PKI实体间使用证书方式进行IPSec协商时，可以通过OCSP方式实时检查对端实体的证书状态。

  OCSP克服了CRL的主要缺陷：PKI实体必须经常下载CRL以确保列表的更新。当PKI实体访问OCSP服务器时，会发送一个对于证书状态信息的请求。OCSP服务器会回复一个“有效”、“过期”或“未知”的响应。

- 有效表示证书没有被撤销。
- 过期表示证书已被撤销。
- 未知表示OCSP服务器不能判断请求的证书状态。

- None方式

  如果PKI实体没有可用的CRL和OCSP服务器，或者不需要检查PKI实体的本地证书状态，可以采用None方式，即不检查证书是否被撤销。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**pki realm** *realm-name*，创建PKI域并进入PKI域视图，或者直接进入PKI域视图。

   缺省情况下，设备存在名称为**default**的PKI域，且该域只能修改不能删除。
3. 执行命令**certificate-check** { { **crl** | **ocsp** } * [**none**] | **none** }，配置PKI域中证书吊销状态的检查方式。

   缺省情况下，PKI域中证书吊销状态的检查方式为CRL。

   如果配置了多种吊销状态的检查方式，会按照配置的先后顺序执行，当前一种方式不可用（如服务器连接不上）时才会使用后边的方式。如果选用了不检查（none），当前面配置的方式均不可用时，认为证书有效。以配置了**certificate-check crl none**命令为例，先使用CRL方式检查证书是否有效，如果CRL方式不可用，则认为证书是有效的。
4. 请根据CA提供的服务方式选择配置检查对端实体本地证书状态的方式。
   - **自动更新CRL方式**
   - **手动更新CRL方式**
   - **OCSP方式**

自动更新 CRL 方式

1. 执行命令**quit**，返回至系统视图。
2. （可选）执行命令**pki file-format** { **der** | **pem** }，配置设备保存CRL时的文件格式。

   缺省情况下，设备保存CRL时的文件格式为PEM。
3. 执行命令**pki realm** *realm-name*，直接进入PKI域视图。
4. 执行命令**crl auto-update enable**，开启CRL自动更新功能。

   缺省情况下，CRL自动更新功能处于开启状态。
5. 执行命令**crl update-period** *interval*，配置CRL自动更新的时间间隔。

   缺省情况下，CRL自动更新的时间间隔为8小时。
6. 请根据CA提供的服务方式选择配置自动更新CRL方式。
   - 通过SCEP方式自动更新CRL。
     i. 执行命令**crl scep**，配置使用SCEP方式自动更新CRL。

        缺省情况下，使用HTTP方式自动更新CRL。

     ii. 执行命令**cdp-url** [**esc**] *url-addr*，配置CRL发布点的URL。

         缺省情况下，系统未配置CRL发布点的URL。
   - 通过HTTP方式自动更新CRL。

i. 执行命令**crl http**，配置使用HTTP方式自动更新CRL。

缺省情况下，使用HTTP方式自动更新CRL。

ii. 执行命令**cdp-url** [**esc**] *url-addr*，配置CRL发布点的URL。或者执行命令**cdp-url from-ca**，配置从CA证书中获取CDP URL。

缺省情况下，系统未配置CRL发布点的URL。

7. 执行命令**crl cache**，配置允许PKI域使用缓存中的CRL。

缺省情况下，系统允许PKI域使用缓存中的CRL。

8. （可选）立即更新CRL。

a. 执行命令**quit**，返回至系统视图。

b. 执行命令**pki get-crl realm** *realm-name*，立即更新CRL。

立即更新CRL后，新的CRL会替换设备存储介质中原来的CRL，同时新的CRL也会被自动导入设备内存中替换原来的CRL。

手动更新 CRL 方式

1. 执行命令**quit**，返回至系统视图。
2. （可选）执行命令**pki file-format** { **der** | **pem** }，配置设备保存CRL时的文件格式。

缺省情况下，设备保存CRL时的文件格式为PEM。

3. 执行命令**pki http** [**esc**] *url-address save-name*，配置通过HTTP方式下载CRL。

*url-address*必须包含完整的证书文件及扩展名，例如http://10.1.1.1:8080/cert.cer。如果设置为域名方式，必须保证该域名可以正常解析。

4. 执行命令**pki import-crl realm** *realm-name* **filename** *file-name*，将CRL导入设备的内存中。

OCSP 方式

1. （可选）执行命令**source interface** { **interface** *interface-type interface-number* | *ip-address* }，配置建立TCP连接使用的源接口。

缺省情况下，设备使用出接口作为TCP连接的源接口。

请确保该接口为三层接口，且接口下已经配置了IP地址。

2. 执行命令**ocsp url** [**esc**] *url-address*，配置OCSP服务器的URL。或者执行命令**ocsp-url from-ca**，配置从CA证书的AIA选项中获取OCSP服务器的URL。

缺省情况下，系统未配置OCSP服务器的URL。

3. （可选）执行命令**ocsp nonce enable**，配置PKI实体发送OCSP请求时带有Nonce扩展。

缺省情况下，PKI实体发送OCSP请求时带有Nonce扩展。

通过该功能可以增强PKI实体与OCSP服务器通信时的安全性和可靠性。配置后，PKI实体与OCSP服务器通信时发送的OCSP请求中带有Nonce扩展，内容为随机数。对于OCSP服务器发出的响应报文，可以不包含Nonce扩展，但是如果包含了Nonce扩展，则必须与OCSP请求中的Nonce扩展一致。

4. （可选）执行命令**ocsp signature enable**，开启OCSP请求消息签名功能。

缺省情况下，OCSP请求消息签名功能处于关闭状态。

如果OCSP服务器要求对OCSP请求消息进行签名验证，设备需要配置本命令。

5. 执行命令**quit**，返回至系统视图。
6. 执行命令**pki import-certificate ocsp realm** *realm-name* { **der** | **pkcs12** | **pem** } [**filename** *filename*] 或执行命令**pki import-certificate ocsp realm** *realm-name* **pkcs12 filename** *filename* **password** *password*，将OCSP服务器证书导入到设备的存中。
7. 执行命令**pki validate ocsp-server-certificate enable**，开启OCSP证书校验OCSP服务器报文的功能。

   缺省情况下，OCSP证书校验OCSP服务器报文的功能处于开启状态。
8. 执行命令**pki ocsp response cache enable**，开启PKI实体缓存OCSP响应的功能。

   缺省情况下，PKI实体缓存OCSP响应的功能处于关闭状态。

   开启缓存OCSP响应功能后，PKI实体在使用OCSP检查证书的吊销状态时，会先查找缓存，如果查找失败则再向OCSP服务器发起请求。同时，PKI实体会将有效的OCSP响应缓存起来，以便下次查找。

   OCSP响应是有生效期限的，开启缓存OCSP响应功能后，PKI实体会每隔1分钟刷新缓存的OCSP响应，清除其中过期的OCSP响应。
9. （可选）执行命令**pki ocsp response cache number** *number*，配置PKI实体可以缓存的OCSP响应的最大数量。

   缺省情况下，PKI实体可以缓存的OCSP响应的最大数量是2。
10. （可选）执行命令**pki ocsp response cache refresh interval** *interval*，配置PKI实体刷新OCSP响应缓存的周期。

    缺省情况下，PKI实体刷新OCSP响应缓存的周期为5分钟。

后续处理

- 如果需要把OCSP服务器证书拷贝到其他设备上使用时，可以执行命令**pki export-certificate ocsp realm** *realm-name* { **pem** | **pkcs12** }，将OCSP服务器证书导出到设备的存储介质中。然后，可以通过文件传输协议取出证书。
- 如果OCSP服务器证书过期或者不使用时，可以执行命令**pki delete-certificate ocsp realm** *realm-name*，从内存中删除OCSP服务器证书。
- 如果CRL过期或者不使用时，可以执行命令**pki delete-crl realm** *realm-name*，从内存中删除CRL。

15.11.2 配置检查 CA 证书和本地证书有效性

背景信息

在使用每一个证书之前，必须对证书进行验证以确保证书的合法性。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，而且未被撤销。

为完成证书验证，除了需要对端实体的本地证书外，本地设备需要下面的信息：CA证书、CRL、本地证书及其私钥及证书认证相关配置信息。

本地证书验证的主要过程如下：

1. 使用CA证书的公钥验证CA的签名是否正确。

   为验证一个证书的合法性，首先需要获得颁发这个证书的CA的公钥（即获得CA证书），以便检查该证书上CA的签名。一个CA可以让另一个更高层次的CA来证明

其证书的合法性，这样顺着证书链，验证证书就变成了一个迭代过程，最终这个链必须在某个“信任点”（一般是持有自签名证书的根CA或者是PKI实体信任的中间CA）处结束。

任何PKI实体，如果它们共享相同的根CA或子CA，并且已获取CA证书，都可以验证对端证书。一般情况下，当验证对端证书链时，验证过程在碰到第一个可信任的证书或CA机构时结束。

证书链的验证过程是一个从目标证书（待验证的PKI实体证书）到信任点证书逐层验证的过程。

2. 根据证书的有效期，验证证书是否过期。
3. 检查证书的状态，即通过CRL和None方式检查证书是否被撤销。

当用户需要验证本地设备的CA证书和本地证书的有效性时，可以执行以下步骤。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**pki validate-certificate** { **ca** | **local** } **realm** *realm-name*，检查CA证书或本地证书的有效性。

pki validate-certificate ca命令只能验证根CA的CA证书有效性，不能验证从属CA的CA证书有效性。在多级CA的环境中，当设备上导入了多个CA证书时，只能使用**pki validate-certificate local**命令来验证从属CA的CA证书有效性。

----结束

15.11.3 检查验证 CA 证书和本地证书的配置结果

前提条件

已经完成验证CA证书和本地证书的所有配置。

操作步骤

- 执行命令**display pki realm** [*realm-name*]，查看PKI域的信息。
- 执行命令**display pki crl** { **realm** *realm-name* | **filename** *filename* }，查看设备中的CRL内容。
- 执行命令**display pki certificate ocsp realm** *realm-name*，查看设备上已加载的OCSP服务器证书的内容。
- 执行命令**display pki ocsp cache statistics**，查看OCSP响应缓存的统计信息。
- 执行命令**display pki ocsp server down-information**，查看设备上记录的OCSP服务器DOWN状态信息。

----结束

15.12 删除本地证书

背景信息

本地证书过期或者重新申请新的证书时，可以删除本地证书。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**pki delete-certificate local realm** *realm-name*，从内存中删除本地证书。

----结束

15.13 配置 PKI 扩展功能

15.13.1 配置获取证书

背景信息

获取CA证书时，设备会自动将CA证书导入到设备内存中。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**pki get-certificate ca realm** *realm-name*，获取证书至设备的存储介质中。

如果设备中存在相同的证书，则需要删除设备中的证书，否则会导致获取证书失败。

----结束

15.13.2 配置导入和释放对端实体的证书

背景信息

当采用数字信封认证方式时，如果设备作为数据发送者，设备上需要配置数据接收者的公钥。导入对端实体的证书即为获取对端实体的公钥的一种方法，该方法建立了用户身份信息与用户公钥的关联，安全性高，适合在大规模网络时部署。

当导入的对端实体的证书不需要使用时，可以将对端实体的证书释放。

操作步骤

- 导入对端实体的证书
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pki import-certificate peer** *peer-name* { **der** | **pem** | **pkcs12** } **filename** [*filename*]或执行命令**pki import-certificate peer** *peer-name* **pkcs12 filename** *filename* **password** *password*，导入对端实体的证书到设备的内存中。
- 释放对端实体的证书
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**pki release-certificate peer** { **name** *peer-name* | **all** }，释放对端实体的证书。

----结束

检查配置结果

执行命令**display pki peer-certificate** { **name** *peer-name* | **all** }，查看已导入的对端实体证书。

15.13.3 配置自签名证书

背景信息

如果设备无法向CA申请本地证书，可以通过设备生成自签名证书后，生成的证书以文件形式保存在存储器中，实现简单的证书颁发功能。用户可以将证书导出供其他设备使用。

说明

设备不支持对其生成的自签名证书进行生命周期管理（如证书更新、证书撤销等），为了确保设备和证书的安全，建议用户替换为自己的本地证书。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**pki create-certificate self-signed filename** *file-name*，创建自签名证书。

配置时，会提示用户输入证书的一些信息，比如PKI实体属性、证书文件名称、证书有效期和RSA密钥长度等。

创建的自签名证书的文件格式为PEM。

----结束

15.13.4 配置 PKI 加入到指定的 VPN 内

背景信息

当CA等服务器位于某个VPN内时，为了让设备可以与这些服务器进行通信以实现证书的获取或有效性校验等功能，此时需配置PKI域加入到指定的VPN内。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**pki realm** *realm-name*，创建PKI域并进入PKI域视图，或者直接进入PKI域视图。

   缺省情况下，设备存在名称为**default**的PKI域，且该域只能修改不能删除。

   PKI域是一个本地概念，一个设备上配置的PKI域对CA和其他设备是不可见的，每一个PKI域有单独的参数配置信息。
3. 执行命令**vpn-instance** *vpn-instance-name*，将PKI加入到指定的VPN内。

   缺省情况下，系统未将PKI加入到任何VPN内。

   *vpn-instance-name*参数可通过命令**ip vpn-instance**配置。

15.13.5 配置被覆盖的文件删除到回收站功能

背景信息

覆盖文件时，被覆盖的文件默认彻底删除，无法恢复。如果用户希望被覆盖的文件能够恢复，以防止新文件不可用，此时可以配置被覆盖的文件删除到回收站功能。

该功能仅适用于以下场景：

- 执行命令**pki get-certificate**覆盖已有的证书。
- 执行命令**pki http**覆盖已有的证书、CRL。
- 执行命令**pki cmp initial-request session**覆盖已有的证书。
- 执行命令**pki cmp certificate-request session**覆盖已有的证书。
- 执行命令**pki cmp keyupdate-request session**覆盖已有的证书。
- 执行命令**pki get-crl**覆盖已有的CRL。
- 执行命令**pki enroll-certificate**覆盖已有的证书。
- 执行命令**pki create-certificate**覆盖已有的证书。
- 执行命令**pki export-certificate**覆盖已有的证书。
- 执行命令**pki export rsa-key-pair**覆盖已有的RSA密钥对。
- 执行命令**pki import-certificate peer**覆盖已有的证书。
- 执行命令**pki import-crl**覆盖已有的CRL。
- 执行命令**pki import rsa-key-pair**覆盖已有的RSA密钥对、证书。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**pki delete replaced-file to recycle-bin enable**，开启被覆盖的文件删除到回收站功能。

缺省情况下，被覆盖的文件被彻底删除。

----结束

15.14 维护 PKI

15.14.1 查看 PKI 信息

背景信息

在日常维护工作中，了解PKI相关信息时，可以在对应视图下选择执行以下命令查看证书等信息。

操作步骤

- 执行命令**display pki certificate enroll-status** [**realm** *realm-name*]，查看证书的注册状态。

- 执行命令**display pki cmp statistics** [**session** *session-name*]，查看CMP会话的统计信息。
- 执行命令**display pki ocsp cache statistics**，查看OCSP响应缓存的统计信息。
- 执行命令**display pki ocsp server down-information**，查看设备上记录的OCSP服务器DOWN状态信息。
- 执行命令**display pki certificate** { **ca** | **local** | **ocsp** } **realm** *realm-name*，查看设备上已加载的CA证书、本地证书或者OCSP服务器证书的内容。
- 执行命令**display pki peer-certificate** { **name** *peer-name* | **all** }，查看已导入的对端实体证书。
- 执行命令**display pki ocsp cache detail**，查看OCSP响应缓存的详细信息。

----结束

15.14.2 清除 PKI 信息

背景信息

清空PKI信息后，以前的信息将无法恢复，务必仔细确认。请在用户视图下执行以下命令。

操作步骤

- 执行命令**reset pki cmp statistics** [**session** *session-name*]，清除CMP会话的统计信息。
- 执行命令**reset pki ocsp response cache**，清除OCSP响应缓存。
- 执行命令**reset pki ocsp server down-information** [**url** [**esc**] *url-addr*]，清除设备上记录的OCSP服务器DOWN状态信息。

----结束

15.15 PKI 配置举例

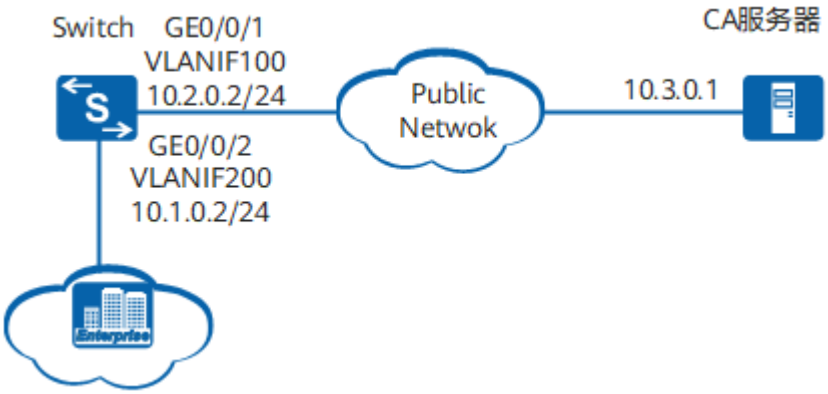
15.15.1 配置通过 SCEP 协议自动为 PKI 实体申请本地证书示例

组网需求

如图15-11所示，某企业在网络边界处部署了Switch作为出口网关，Switch向公网上的CA服务器在线申请本地证书。

用户希望通过简单快捷的方式为PKI实体申请本地证书，申请成功后能自动将证书导入到设备内存中，而且证书过期时，能自动更新证书。此时，可以配置通过SCEP协议自动为PKI实体申请本地证书实现上述需求。

图 15-11 配置通过 SCEP 协议自动为 PKI 实体申请本地证书组网图



说明

本举例只列出了申请证书时Switch侧的相关配置，CA服务器的部署和配置请参见相关产品手册。这里的CA服务器以Windows Server 2008自带的“证书服务”，并安装了SCEP插件为例进行说明。

配置思路

采用如下思路配置通过SCEP协议自动为PKI实体申请本地证书：

1. 配置接口的IP地址及到CA服务器的静态路由，实现Switch和CA服务器之间路由互通。
2. 创建RSA密钥对，实现申请本地证书时携带公钥。
3. 配置PKI实体，实现申请本地证书时携带PKI实体信息用来标识PKI实体的身份。
4. 通过SCEP协议申请和自动更新证书，实现自动安装证书，并且证书过期时，能自动更新证书。

数据准备

申请证书前需要以离线方式从CA服务器上获取数字指纹和挑战密码。这里假设数字指纹为“e71add0744360e91186b828412d279e06dcc15a4ab4bb3d13842820396b526a0”和挑战密码为“6AE73F21E6D3571D”。

本文以Windows Server 2008作为CA服务器为例，可以通过登录网页http://*host*:*port*/certsrv/mscep_admin/获得CA证书指纹信息和挑战密码，其中*host*为CA服务器的IP地址，*port*为CA服务器的端口号。

操作步骤

步骤1 配置接口的IP地址及到CA服务器的静态路由。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 100 200
[Switch] interface vlanif 100
[Switch-Vlanif100] ip address 10.2.0.2 255.255.255.0
[Switch-Vlanif100] quit
[Switch] interface vlanif 200
[Switch-Vlanif200] ip address 10.1.0.2 255.255.255.0
```



```
[Switch-Vlanif200] quit
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type trunk
[Switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] port link-type trunk
[Switch-GigabitEthernet0/0/2] port trunk allow-pass vlan 200
[Switch-GigabitEthernet0/0/2] quit
[Switch] ip route-static 10.3.0.0 255.255.255.0 10.2.0.1
```

步骤2 创建RSA密钥对。

创建一个2048位的RSA密钥对rsa_scep，并设置为可以从设备上导出。

```
[Switch] pki rsa local-key-pair create rsa_scep exportable
 Info: The name of the new key-pair will be: rsa_scep
 The size of the public key ranges from 2048 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...        ..................+++
.......................+++
```

步骤3 配置PKI实体，标识申请证书PKI实体的身份信息。

配置PKI实体为user01。

```
[Switch] pki entity user01
[Switch-pki-entity-user01] common-name hello
[Switch-pki-entity-user01] country cn
[Switch-pki-entity-user01] email user@test.abc.com
[Switch-pki-entity-user01] fqdn test.abc.com
[Switch-pki-entity-user01] ip-address 10.2.0.2
[Switch-pki-entity-user01] state jiangsu
[Switch-pki-entity-user01] organization huawei
[Switch-pki-entity-user01] organization-unit info
[Switch-pki-entity-user01] quit
```

步骤4 通过SCEP协议申请和更新证书。

```
[Switch] pki realm abc
[Switch-pki-realm-abc] ca id ca_root
[Switch-pki-realm-abc] entity user01
[Switch-pki-realm-abc] fingerprint sha256
e71add0744360e91186b828412d279e06dcc15a4ab4bb3d13842820396b526a0
[Switch-pki-realm-abc] enrollment-url http://10.3.0.1:80/certsrv/mscep/mscep.dll ra
[Switch-pki-realm-abc] rsa local-key-pair rsa_scep
[Switch-pki-realm-abc] enrollment-request signature message-digest-method sha-384
[Switch-pki-realm-abc] password cipher 6AE73F21E6D3571D
```

步骤5 开启证书自动注册和更新功能，指定证书有效期到60%时自动更新并同时更新RSA密钥。

```
[Switch-pki-realm-abc] auto-enroll 60 regenerate 2048
[Switch-pki-realm-abc] quit
```

申请本地证书时，设备会先获取CA证书并自动安装CA证书，然后再获取本地证书并自动安装本地证书。获取的CA证书和本地证书名称分别为abc_ca.cer和abc_local.cer。

步骤6 验证配置结果。

1. 证书申请成功后，可执行命令**display pki certificate local**查看已经导入内存的本地证书的内容。

```
[Switch] display  pki certificate local realm abc
 The x509 object type is certificate:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            48:65:aa:2a:00:00:00:00:3f:c6
    Signature Algorithm: sha1WithRSAEncryption
```



```
        Issuer: CN=ca_root
        Validity
            Not Before: Dec 21 11:46:10 2015 GMT
            Not After : Dec 21 11:56:10 2016 GMT
        Subject: C=CN, ST=jiangsu, O=huawei, OU=info, CN=hello
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:94:6f:49:bd:6a:f3:d5:07:ee:10:ee:4f:d3:06:
                    80:59:15:cb:a8:0a:b2:ba:c2:db:52:ec:e9:d1:a7:
                    72:de:ac:35:df:bb:e0:72:62:08:3e:c5:54:c1:ba:
                    4a:bb:1b:a9:d9:dc:e4:b6:4d:ca:b3:54:90:b6:8e:
                    15:a3:6e:2d:b2:9e:9e:7a:33:b0:56:3f:ec:bc:67:
                    1c:4c:59:c6:67:0f:a7:03:52:44:8c:53:72:42:bd:
                    6e:0c:90:5b:88:9b:2c:95:f7:b8:89:d1:c2:37:3e:
                    93:78:fa:cb:2c:20:22:5f:e5:9c:61:23:7b:c0:e9:
                    fe:b7:e6:9c:a1:49:0b:99:ef:16:23:e9:44:40:6d:
                    94:79:20:58:d7:e1:51:a1:a6:4b:67:44:f7:07:71:
                    54:93:4e:32:ff:98:b4:2b:fa:5d:b2:3c:5b:df:3e:
                    23:b2:8a:1a:75:7e:8f:82:58:66:be:b3:3c:4a:1c:
                    2c:64:d0:3f:47:13:d0:5a:29:94:e2:97:dc:f2:d1:
                    06:c9:7e:54:b3:42:2e:15:b8:40:f3:94:d3:76:a1:
                    91:66:dd:40:29:c3:69:70:6d:5a:b7:6b:91:87:e8:
                    bb:cb:a5:7e:ec:a5:31:11:f3:04:ab:1a:ef:10:e6:
                    f1:bd:d9:76:42:6c:2e:bf:d9:91:39:1d:08:d7:b4:
                    18:53
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage:
                Digital Signature, Key Encipherment
            X509v3 Subject Alternative Name:
                IP Address:10.2.0.2, DNS:test.abc.com, email:user@test.abc.com
            X509v3 Subject Key Identifier:
                15:D1:F6:24:EB:6B:C0:26:19:58:88:91:8B:60:42:CE:BA:D5:4D:F3
            X509v3 Authority Key Identifier:
                keyid:B8:63:72:A4:5E:19:F3:B1:1D:71:E1:37:26:E1:46:39:01:B6:82:C
5

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:file://\\vasp-e6000-127.china.organization.com\CertEnroll\ca_roo
t.crl
                  URI:http://10.3.0.1:8080/certenroll/ca_root.crl

            Authority Information Access:
                CA Issuers - URI:http://vasp-e6000-127.china.huawei.com/CertEnro
ll/vasp-e6000-127.china.huawei.com_ca_root.crt
                OCSP - URI:file://\\vasp-e6000-127.china.huawei.com\CertEnroll\v asp-
e6000-127.china.huawei.com_ca_root.crt

            1.3.6.1.4.1.311.20.2:
                .0.I.P.S.E.C.I.n.t.e.r.m.e.d.i.a.t.e.O.f.f.l.i.n.e
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Extended Key Usage:
                1.3.6.1.5.5.8.2.2
    Signature Algorithm: sha1WithRSAEncryption
        d2:be:a8:52:6b:03:ce:89:f1:5b:49:d4:eb:2b:9f:fd:59:17:
        d4:3c:f1:db:4f:1b:d1:12:ac:bf:ae:59:b4:13:1b:8a:20:d0:
        52:6a:f8:a6:03:a6:72:06:41:d2:a7:7d:3f:51:64:9b:84:64:
        cf:ec:4c:23:0a:f1:57:41:53:eb:f6:3a:44:92:f3:ec:bd:09:
        75:db:02:42:ab:89:fa:c4:cd:cb:09:bf:83:1d:de:d5:4b:68:
        8a:a6:5f:7a:e8:b3:34:d3:e8:ec:24:37:2b:bd:3d:09:ed:88:
        d8:ed:a7:f8:66:aa:6f:b0:fe:44:92:d4:c9:29:21:1c:b3:7a:
        65:51:32:50:5a:90:fa:ae:e1:19:5f:c8:63:8d:a8:e7:c6:89:
        2e:6d:c8:5b:2c:0c:cd:41:48:bd:79:74:0e:b8:2f:48:69:df:
        02:89:bb:b3:59:91:7f:6b:46:29:7e:22:05:8c:bb:6a:7e:f3:
```

```
        11:5a:5f:fb:65:51:7d:35:ff:49:9e:ec:d1:2d:7e:73:e5:99:
        c6:41:84:0c:50:11:ed:97:ed:15:de:11:22:73:a1:78:11:2e:
        34:e6:f5:de:66:0c:ba:d5:32:af:b8:54:26:4f:5b:9e:89:89:
        2a:3f:b8:96:27:00:c3:08:3a:e9:e8:a6:ce:4b:5a:e3:97:9e:
        6b:dd:f0:72

Pki realm name: abc
Certificate file name: abc_local.cer
Certificate peer name: -
```

2. 证书申请成功后，可执行命令**display pki certificate ca**查看已经导入内存的CA证书的内容。

```
[Switch] display  pki certificate ca realm abc
 The x509 object type is certificate:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0c:f0:1a:f3:67:21:44:9a:4a:eb:ec:63:75:5d:d7:5f
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=ca_root
        Validity
            Not Before: Jun  4 14:58:17 2015 GMT
            Not After : Jun  4 15:07:10 2020 GMT
        Subject: CN=ca_root
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d9:5f:2a:93:cb:66:18:59:8c:26:80:db:cd:73:
                    d5:68:92:1b:04:9d:cf:33:a2:73:64:3e:5f:fe:1a:
                    53:78:0e:3d:e1:99:14:aa:86:9b:c3:b8:33:ab:bb:
                    76:e9:82:f6:8f:05:cf:f6:83:8e:76:ca:ff:7d:f1:
                    bc:22:74:5e:8f:4c:22:05:78:d5:d6:48:8d:82:a7:
                    5d:e1:4c:a4:a9:98:ec:26:a1:21:07:42:e4:32:43:
                    ff:b6:a4:bd:5e:4d:df:8d:02:49:5d:aa:cc:62:6c:
                    34:ab:14:b0:f1:58:4a:40:20:ce:be:a5:7b:77:ce:
                    a4:1d:52:14:11:fe:2a:d0:ac:ac:16:95:78:34:34:
                    21:36:f2:c7:66:2a:14:31:28:dc:7f:7e:10:12:e5:
                    6b:29:9a:e8:fb:73:b1:62:aa:7e:bd:05:e5:c6:78:
                    6d:3c:08:4c:9c:3f:3b:e0:e9:f2:fd:cb:9a:d1:b7:
                    de:1e:84:f4:4a:7d:e2:ac:08:15:09:cb:ee:82:4b:
                    6b:bd:c6:68:da:7e:c8:29:78:13:26:e0:3c:6c:72:
                    39:c5:f8:ad:99:e4:c3:dd:16:b5:2d:7f:17:e4:fd:
                    e4:51:7a:e6:86:f0:e7:82:2f:55:d1:6f:08:cb:de:
                    84:da:ce:ef:b3:b1:d6:b3:c0:56:50:d5:76:4d:c7:
                    fb:75
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.20.2:
                ...C.A
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                B8:63:72:A4:5E:19:F3:B1:1D:71:E1:37:26:E1:46:39:01:B6:82:C5
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://vasp-e6000-127.china.huawei.com/CertEnroll/ca_root.
crl
                  URI:file://\\vasp-e6000-127.china.huawei.com\CertEnroll\ca_roo
t.crl

            1.3.6.1.4.1.311.21.1:
                ...
    Signature Algorithm: sha1WithRSAEncryption
        52:21:46:b8:67:c8:c3:4a:e7:f8:cd:e1:02:d4:24:a7:ce:50:
```



```
      be:33:af:8a:49:47:67:43:f9:7f:79:88:9c:99:f5:87:c9:ff:
      08:0f:f3:3b:de:f9:19:48:e5:43:0e:73:c7:0f:ef:96:ef:5a:
      5f:44:76:02:43:83:95:c4:4e:06:5e:11:27:69:65:97:90:4f:
      04:4a:1e:12:37:30:95:24:75:c6:a4:73:ee:9d:c2:de:ea:e9:
      05:c0:a4:fb:39:ec:5c:13:29:69:78:33:ed:d0:18:37:6e:99:
      bc:45:0e:a3:95:e9:2c:d8:50:fd:ca:c2:b3:5a:d8:45:82:6e:
      ec:cc:12:a2:35:f2:43:a5:ca:48:61:93:b9:6e:fe:7c:ac:41:
      bf:88:70:57:fc:bb:66:29:ae:73:9c:95:b9:bb:1d:16:f7:b4:
      6a:da:03:df:56:cf:c7:c7:8c:a9:19:23:61:5b:66:22:6f:7e:
      1d:26:92:69:53:c8:c6:0e:b3:00:ff:54:77:5e:8a:b5:07:54:
      fd:18:39:0a:03:ac:1d:9f:1f:a1:eb:b9:f8:0d:21:25:36:d5:
      06:de:33:fa:7b:c8:e9:60:f3:76:83:bf:63:c6:dc:c1:2c:e4:
      58:b9:cb:48:15:d2:a8:fa:42:72:15:43:ef:55:63:39:58:77:
      e8:ae:0f:34

Pki realm name: abc
Certificate file name: abc_ca.cer
Certificate peer name: -
```

3. 配置证书自动更新功能后，当系统检测到时间已经超过了配置的当前证书有效期的60%之后，就会向SCEP服务器发起证书的更新请求。

   由于配置命令**auto-enroll**时选择了**regenerate**参数，更新时系统会生成新的RSA密钥对去申请新证书。

----结束

配置文件

Switch的配置文件

```
#
sysname Switch
#
vlan batch 100 200
#
interface Vlanif100
 ip address 10.2.0.2 255.255.255.0
#
interface Vlanif200
 ip address 10.1.0.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 200
#
ip route-static 10.3.0.0 255.255.255.0 10.2.0.1
#
pki realm abc
 ca id ca_root
 enrollment-url http://10.3.0.1:80/certsrv/mscep/mscep.dll ra
 entity user01
 fingerprint sha256 e71add0744360e91186b828412d279e06dcc15a4ab4bb3d13842820396b526a0
 rsa local-key-pair rsa_scep
 password cipher %^%#\1HN-bn(k;^|O85OAtYF3(M4%^%#
 auto-enroll 60 regenerate
 enrollment-request signature message-digest-method sha-384
#
pki entity user01
 country CN
 state jiangsu
 organization huawei
 organization-unit info
 common-name hello
```



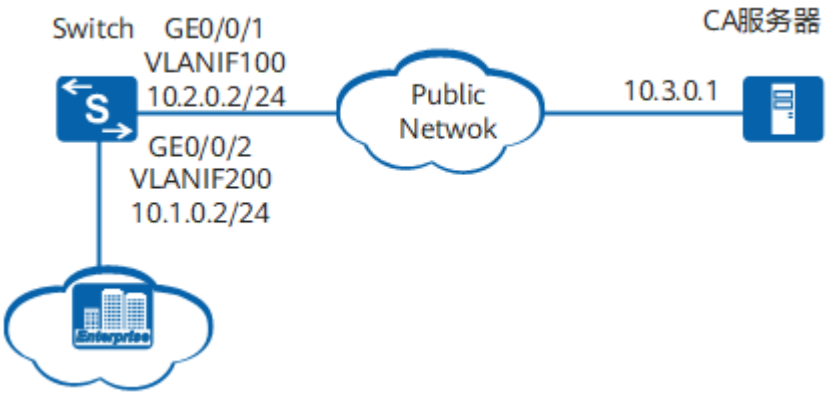
```
 fqdn test.abc.com
 ip-address 10.2.0.2
 email user@test.abc.com
#
return
```

15.15.2 配置通过 CMPv2 协议为 PKI 实体首次申请本地证书示例

组网需求

如图15-12所示，某企业在网络边界处部署了Switch作为出口网关，Switch使用CMPv2协议向公网上的CA服务器在线首次申请证书，申请成功后自动将本地证书下载到设备存储介质中。

图 15-12 配置通过 CMPv2 协议为 PKI 实体首次申请本地证书组网图



说明

本举例只列出了申请证书时Switch侧的相关配置，CA服务器的部署和配置请参见相关产品手册。

配置前请确保各设备之间路由可达。

配置思路

采用如下思路配置通过CMPv2协议为PKI实体首次申请本地证书：

1. 创建RSA密钥对，实现申请本地证书时携带公钥。
2. 配置PKI实体，实现申请本地证书时携带PKI实体信息用来标识PKI实体的身份。
3. 通过CMPv2协议申请和自动更新证书，并使用消息认证码来验证消息，实现自动下载CA和本地证书。
4. 安装CA和本地证书，实现证书生效，即设备可以使用证书来保护通信。

数据准备

为完成此配置示例，需准备如下的数据：

- CA名称
  为CA证书的主题字段。

- 消息认证码的参考值和秘密值
  需要以带外方式从CMPv2服务器上获取消息认证码的参考值和秘密值。

操作步骤

步骤1 创建RSA密钥对。

创建一个2048位的RSA密钥对rsa_cmp，并设置为可以从设备上导出。

```
[Switch] pki rsa local-key-pair create rsa_cmp exportable
 Info: The name of the new key-pair will be: rsa_cmp
 The size of the public key ranges from 2048 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
.....+++
.....+++
```

步骤2 配置PKI实体，标识申请证书PKI实体的身份信息。

配置PKI实体为user01。

```
[Switch] pki entity user01
[Switch-pki-entity-user01] common-name hello
[Switch-pki-entity-user01] country cn
[Switch-pki-entity-user01] email user@test.abc.com
[Switch-pki-entity-user01] fqdn test.abc.com
[Switch-pki-entity-user01] ip-address 10.2.0.2
[Switch-pki-entity-user01] state jiangsu
[Switch-pki-entity-user01] organization huawei
[Switch-pki-entity-user01] organization-unit info
[Switch-pki-entity-user01] quit
```

步骤3 创建PKI域。

```
[Switch] pki realm abc
[Switch-pki-realm-abc] quit
```

步骤4 配置CMP会话。

创建CMP会话cmp。

```
[Switch] pki cmp session cmp
```

指定CMP会话引用的PKI实体名称。

```
[Switch-pki-cmp-session-cmp] cmp-request entity user01
```

配置CA的名称，举例中假设为“C=cn,ST=beijing,L=SD,O=BB,OU=BB,CN=BB”。

说明

配置的CA名称中各个字段的顺序必须要和实际CA证书中的顺序保持一致，否则服务器端会认为是错误的。

```
[Switch-pki-cmp-session-cmp] cmp-request ca-name "C=cn,ST=beijing,L=SD,O=BB,OU=BB,CN=BB"
```

配置申请证书的URL。

```
[Switch-pki-cmp-session-cmp] cmp-request server url http://10.3.0.1:8080
```

指定申请证书时使用的RSA密钥对，并设置为证书自动更新时同时更新RSA密钥对。

```
[Switch-pki-cmp-session-cmp] cmp-request rsa local-key-pair rsa_cmp regenerate
```

指定CMP服务器证书所属的PKI域，并设置CMP服务器证书所属的域名称为abc。

```
[Switch-pki-cmp-session-cmp] cmp-request realm abc
```


首次申请证书时，使用消息认证码认证。配置消息认证码的参考值和秘密值，举例中假设分别为“1234”和“123456”。

```
[Switch-pki-cmp-session-cmp] cmp-request message-authentication-code 1234 123456
[Switch-pki-cmp-session-cmp] quit
[Switch] pki cmp initial-request session cmp
[Switch]
 Info: Initializing configuration.
 Info: Creatting initial request packet.
 Info: Connectting to CMPv2 server.
 Info: Sending initial request packet.
 Info: Waitting for initial response packet.
 Info: Creatting confirm packet.
 Info: Connectting to CMPv2 server.
 Info: Sending confirm packet.
 Info: Waitting for confirm packet from server.
 Info: CMPv2 operation finish.
```

获取到的CA、本地证书将会分别被命名为cmp_ca1.cer和cmp_ir.cer保存在设备存储介质中。

步骤5 安装证书。

导入CA证书到PKI域。

```
[Switch] pki import-certificate ca realm abc pem filename cmp_ca1.cer
 The CA's Subject is /C=cn/ST=beijing/L=BB/O=BB/OU=BB/CN=BB
 The CA's fingerprint is:
   MD5  fingerprint:3AC7 54FD E272 09BE 9008 84EE D1FC 118E
   SHA1 fingerprint:492A 8E0B BED2 BE10 C097 9039 99FE F7E1 9AA5 B658
 Is the fingerprint correct?(Y/N):y
 Info: Succeeded in importing file.
```

导入本地证书到PKI域。

```
[Switch] pki import-certificate local realm abc pem filename cmp_ir.cer
 Info: Succeeded in importing file.
```

步骤6 配置证书自动更新功能。

配置设备用于证明自己身份的证书，也是待更新的证书cmp_ir.cer。

```
[Switch] pki cmp session cmp
[Switch-pki-cmp-session-cmp] cmp-request authentication-cert cmp_ir.cer
```

开启证书自动更新的功能。

```
[Switch-pki-cmp-session-cmp] certificate auto-update enable
```

配置当前系统时间超过证书有效期的60%时开始更新证书。

```
[Switch-pki-cmp-session-cmp] certificate update expire-time 60
[Switch-pki-cmp-session-cmp] quit
```

步骤7 验证配置结果。

1. 证书申请成功后，可执行命令**display pki certificate**查看已经导入内存的本地证书的内容。

```
[Switch] display pki certificate filename cmp_ir.cer
 The  x509_obj type is Cert:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1144733510 (0x443b3f46)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=cn, ST=beijing, L=BB, O=BB, OU=BB, CN=BB
        Validity
            Not Before: Jun 12 09:33:10 2012 GMT
            Not After : Aug 13 02:38:27 2016 GMT
        Subject: C=CN, ST=jiangsu, O=huawei, OU=info, CN=hello
```



```
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:d3:12:fe:57:48:c6:a5:10:12:e9:2f:f9:2a:ff:
                7b:2a:d8:45:69:11:c4:85:30:c4:9a:4d:0f:ad:58:
                e7:56:cd:5c:f0:18:e1:c3:6d:44:c2:c3:5e:64:22:
                d1:28:c9:c3:37:3c:34:ed:28:04:7f:62:9e:8b:94:
                af:bc:72:de:f6:72:7f:e4:d8:45:31:fd:f9:ac:ce:
                5a:b9:c7:1b:23:53:00:28:a6:3b:f5:61:69:5d:ab:
                67:cb:bb:e8:96:2f:ce:ab:2c:6b:91:5b:26:91:86:
                8f:80:a9:b0:66:c1:16:3d:31:55:a2:d4:b5:5a:af:
                85:88:6e:99:f8:f8:53:58:77:26:91:ed:0e:94:ad:
                c5:8d:53:67:67:55:08:8d:90:38:e0:5e:96:37:b9:
                64:0e:36:e7:cf:9a:d2:77:e4:b0:24:05:a6:eb:03:
                6e:ff:f7:ab:be:93:9e:8c:66:7d:31:66:be:6d:c8:
                f3:17:9d:86:19:88:21:2d:d9:69:86:5f:b2:55:a4:
                db:bc:d7:d0:6b:ac:66:ac:e4:63:9c:66:79:9c:42:
                5c:83:b8:9e:4b:6e:67:85:a2:47:19:f1:5c:c0:3c:
                c9:a3:47:02:a8:53:69:59:9e:d9:c7:5e:90:83:8d:
                ac:cd:21:3c:d5:31:39:49:84:e6:f8:f4:e0:44:dd:
                5d:7b
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Alternative Name:
            IP Address:10.2.0.2, DNS:test.abc.com, email:user@test.abc.com
Signature Algorithm: sha1WithRSAEncryption
    53:d5:79:31:7b:40:52:aa:ec:a9:35:ed:07:62:32:c4:ce:22:
    d3:37:0e:83:0c:4c:fa:61:dd:8c:db:a8:d3:fd:6a:ca:0e:3c:
    91:2c:91:ab:92:31:34:b5:87:1e:30:a4:ff:94:9c:d2:71:3c:
    6b:1f:4f:be:a7:20:f2:e1:c2:ad:71:8b:c2:79:0f:50:1f:3c:
    f9:87:df:1d:ee:3d:38:8c:f3:30:b7:3b:00:9b:72:38:b0:68:
    e1:c0:08:f4:02:91:81:a8:fa:51:9e:53:0d:03:b3:6b:0e:e2:
    62:80:ef:2a:a0:cb:9b:9b:91:21:7c:df:fe:6a:38:cc:03:36:
    9c:fc

Pki realm name: abc
Certificate file name: cmp_ir.cer
Certificate peer name: -
```

2. 证书申请成功后，可执行命令**display pki certificate**查看已经导入内存的CA证书的内容。

```
[Switch] display pki certificate filename cmp_ca1.cer
 The x509 object  type is certificate:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=cn, ST=beijing, L=BB, O=BB, OU=BB, CN=BB
        Validity
            Not Before: Aug 15 02:38:27 2011 GMT
            Not After : Aug 13 02:38:27 2016 GMT
        Subject: C=CN, ST=jiangsu, O=huawei, OU=info, CN=hello
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b7:3e:65:7f:3b:3c:18:b8:87:34:39:76:3c:87:
                    39:f7:a9:b3:35:9b:e0:e0:5b:c7:4f:3c:bb:fa:dd:
                    da:93:0b:55:6e:eb:ba:52:c8:86:d1:cf:14:1e:1c:
                    35:c6:53:68:f3:51:e7:2c:d4:b8:fa:0f:b3:04:ef:
                    3f:a0:b3:4d:78:c1:26:88:26:15:41:3d:14:7f:67:
                    3e:2f:35:32:ce:c7:73:73:43:5c:12:d3:0f:a0:ec:
                    96:ae:55:61:27:32:39:a4:f8:32:a1:68:50:e6:3d:
                    2b:39:6d:42:e8:09:5d:4f:98:46:6e:fc:80:87:0e:
                    36:ca:09:7a:ca:2f:dd:ad:d3
                Exponent: 65537 (0x10001)
        X509v3 extensions:
```



```
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                4F:67:F4:CB:F4:C3:F7:61:2C:BD:FF:1D:D1:29:FD:39:28:9F:3B:8B
            X509v3 Key Usage:
                Certificate Sign, CRL Sign
            Netscape Cert Type:
                SSL CA, S/MIME CA, Object Signing CA
            Netscape Comment:
                xca certificate
    Signature Algorithm: sha1WithRSAEncryption
        75:43:24:eb:db:ee:7d:05:30:88:b8:1b:d5:32:ca:51:49:74:
        04:94:fe:d0:31:29:6f:72:c7:4a:86:ac:2a:4c:45:24:9d:3c:
        b4:30:b5:d1:43:88:29:f7:b4:88:b8:37:dc:dd:f4:fa:42:34:
        1c:e6:a5:bc:bb:0b:37:ef:db:8c:b2:b0:bd:97:7f:15:ae:6c:
        71:1b:ff:f1:90:13:74:a4:1f:7c:f7:4e:80:5b:42:aa:6b:22:
        2a:cf:04:48:29:20:c0:b2:95:38:11:06:be:76:f0:cb:8d:4a:
        c6:1a:50:af:31:81:58:ac:14:fe:89:f2:e0:bb:95:3c:94:d0:
        54:96

Pki realm name: abc
Certificate file name: cmp_ca1.cer
Certificate peer name: -
```

3. 配置证书自动更新功能后，当系统检测到时间已经超过了配置的当前证书有效期的60%之后，就会向CMPv2服务器发起证书的更新请求。

   由于配置命令**cmp-request rsa local-key-pair**时选择了**regenerate**参数，更新时系统会生成新的RSA密钥对去申请新证书，申请下来的新证书会同时替换设备存储介质中的证书文件和内存中对应的证书。

----结束

配置文件

Switch的配置文件

```
#
sysname Switch
#
pki entity user01
 country CN
 state jiangsu
 organization huawei
 organization-unit info
 common-name hello
 fqdn user@test.abc.com
 ip-address 10.2.0.2
 email user@user@test.abc.com
#
pki realm abc
#
pki cmp session cmp
 cmp-request ca-name "C=cn,ST=beijing,L=SD,O=BB,OU=BB,CN=BB"
 cmp-request authentication-cert cmp_ir.cer
 cmp-request entity user01
 cmp-request server url http://10.3.0.1:8080
 cmp-request rsa local-key-pair rsa_cmp regenerate
 cmp-request realm abc
 cmp-request message-authentication-code 1234 %^%#ZodFBGH[^BkU2(~>[NRBv|#b>se|@I7"'A,llG_B%^
%#
 certificate auto-update enable
 certificate update expire-time 60
#
ip route-static 10.3.0.0 255.255.255.0 10.2.0.1
#
return
```

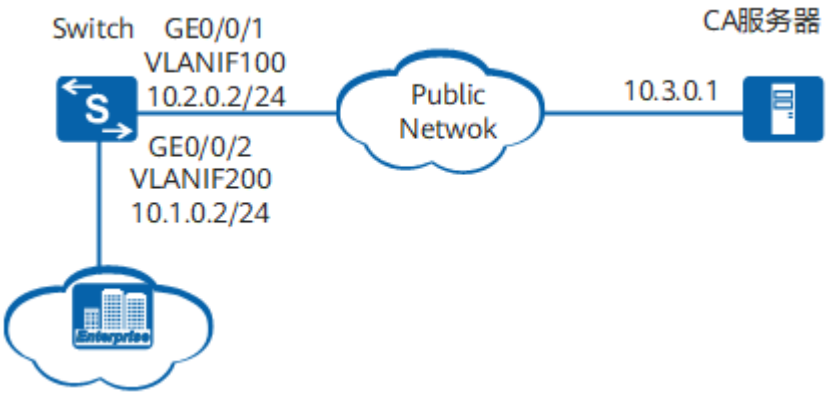
15.15.3 配置为 PKI 实体离线申请本地证书示例

组网需求

如图15-13所示，某企业在网络边界处部署了Switch作为出口网关，Switch向公网上的CA服务器申请本地证书。

用户无法通过SCEP协议在线向CA申请本地证书时，可以通过带外方式为PKI实体离线申请本地证书。

图 15-13 配置为 PKI 实体离线申请本地证书组网图



说明

本举例只列出了申请证书时Switch侧的相关配置，CA服务器的部署和配置请参见相关产品手册。这里的CA服务器以Windows Server 2008自带的“证书服务”，并安装了SCEP插件为例进行说明。

配置思路

采用如下思路配置为PKI实体离线申请本地证书：

1. 创建RSA密钥对，实现申请本地证书时携带公钥。
2. 配置PKI实体，实现申请本地证书时携带PKI实体信息用来标识PKI实体的身份。
3. 配置为PKI实体离线申请本地证书，生成本地证书请求文件。
4. 通过带外方式发送本地证书请求文件来申请本地证书，并通过带外方式下载本地证书。
5. 安装本地证书，使得设备可以使用证书来保护通信。

操作步骤

步骤1 配置接口的IP地址及到CA服务器的静态路由。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 100 200
[Switch] interface vlanif 100
[Switch-Vlanif100] ip address 10.2.0.2 255.255.255.0
[Switch-Vlanif100] quit
[Switch] interface vlanif 200
[Switch-Vlanif200] ip address 10.1.0.2 255.255.255.0
```

```
[Switch-Vlanif200] quit
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type trunk
[Switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] port link-type trunk
[Switch-GigabitEthernet0/0/2] port trunk allow-pass vlan 200
[Switch-GigabitEthernet0/0/2] quit
[Switch] ip route-static 10.3.0.0 255.255.255.0 10.2.0.1
```

步骤2 创建RSA密钥对。

创建一个2048位的RSA密钥对rsa，并设置为可以从设备上导出。

```
[Switch] pki rsa local-key-pair create rsakey exportable
 Info: The name of the new key-pair will be: rsakey
 The size of the public key ranges from 2048 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...        ..................+++
.....................+++
```

步骤3 配置PKI实体，标识申请证书PKI实体的身份信息。

配置PKI实体为user01。

```
[Switch] pki entity user01
[Switch-pki-entity-user01] common-name hello
[Switch-pki-entity-user01] country cn
[Switch-pki-entity-user01] email user@test.abc.com
[Switch-pki-entity-user01] fqdn test.abc.com
[Switch-pki-entity-user01] ip-address 10.2.0.2
[Switch-pki-entity-user01] state jiangsu
[Switch-pki-entity-user01] organization huawei
[Switch-pki-entity-user01] organization-unit info
[Switch-pki-entity-user01] quit
```

步骤4 配置为PKI实体离线申请本地证书。

```
[Switch] pki realm abc
[Switch-pki-realm-abc] entity user01
[Switch-pki-realm-abc] rsa local-key-pair rsakey
[Switch-pki-realm-abc] quit
[Switch] pki enroll-certificate realm abc pkcs10 filename cer_req
 Info: Creating certificate request file...
 Info: Create certificate request file successfully.
```

已完成配置后，可执行命令**display pki cert-req**查看证书请求文件的内容。

```
[Switch] display pki cert-req filename cer_req
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=CN, ST=jiangsu, O=huawei, OU=info, CN=hello
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a2:db:e3:30:17:8e:f6:2d:2e:64:15:46:51:ad:
                    70:86:dd:32:c4:bb:6b:58:3a:8c:5f:a0:06:a1:e1:
                    56:2e:a4:eb:7e:12:06:05:04:28:b2:6d:64:7a:9c:
                    4f:85:24:c1:aa:b8:99:dc:e9:bb:c4:1e:e2:9d:a0:
                    18:51:1f:ad:b5:2f:60:18:06:8b:c1:cc:6f:32:58:
                    f2:21:2c:16:e8:29:c2:a8:c5:aa:9d:6c:1e:ca:14:
                    fc:7a:e9:bc:07:91:ce:ed:a0:c0:52:d9:0c:e9:ba:
                    9b:64:43:e0:9a:3f:c5:d1:2c:86:36:96:6b:4b:4f:
                    d4:df:05:d0:4b:41:2c:ec:0a:d7:0e:45:83:ed:cd:
                    07:78:40:ed:d5:3d:7f:fe:0f:08:90:04:2e:ac:e5:
                    42:b9:81:ea:ec:77:e2:cc:04:6e:e4:63:9f:69:ed:
                    60:06:5e:c7:e8:bf:30:57:6a:5d:e0:46:68:d3:ee:
```



```
                b0:da:47:24:e3:b6:a5:f3:20:d8:5a:75:92:70:c2:
                a9:a6:97:07:07:0d:1c:94:9a:03:6f:f7:8c:db:6f:
                b7:06:de:51:50:9e:71:fd:86:f3:b5:c9:99:05:bf:
                f1:10:20:28:d3:a6:29:3d:e0:f4:a7:ba:1e:27:85:
                a9:66:fc:a9:90:49:f0:35:f7:d9:6d:06:a2:43:3f:
                18:87
            Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment, Data Encip
herment
            X509v3 Subject Alternative Name:
                IP Address:10.2.0.2, DNS:test.abc.com, email:user@test.abc.com
    Signature Algorithm: sha256WithRSAEncryption
        0e:0a:a5:b7:d5:54:11:10:c4:ea:ff:77:da:f9:24:4b:a9:98:
        a1:75:36:08:10:59:60:fa:1a:30:70:2c:b7:f6:5f:5e:31:b7:
        55:a5:7a:26:e5:af:4a:cd:83:c5:f3:90:f3:b9:d5:f9:0a:6d:
        6e:8f:25:b4:ed:95:9c:75:a5:d7:b6:25:fc:8d:39:89:fb:af:
        37:fc:01:7b:09:07:9c:96:7c:fa:28:6d:e2:11:49:a7:95:94:
        ed:26:5b:ca:f8:98:b0:e7:64:7e:dd:2d:75:ff:89:03:b7:0a:
        92:53:25:d4:a1:23:b9:5c:eb:5b:29:1d:8a:92:8f:36:68:7b:
        77:32:bc:48:92:48:84:fa:87:5a:d7:2e:3e:be:d5:6b:e4:df:
        b1:f2:02:35:91:6a:eb:cd:fc:5a:ea:37:85:6c:12:74:5f:a5:
        5c:c0:05:09:cd:34:59:0d:c6:c8:75:ca:1c:18:d6:48:e5:4b:
        e7:8e:e3:ff:25:99:0f:2e:a8:b4:c5:8e:4d:8f:dd:64:c5:1f:
        61:3c:58:21:4f:d5:35:ba:c8:8e:5f:76:41:9f:27:41:0a:94:
        59:2c:59:25:2d:de:60:5c:92:07:ac:8a:a5:7a:ba:75:af:2c:
        82:5f:bb:55:a8:48:49:54:0f:99:54:af:8d:12:4d:4b:7d:8b:
        95:28:ce:dc
```

步骤5 通过Web、磁盘、电子邮件等带外方式将证书申请文件发送给CA服务器，向CA服务器申请本地证书。

本地证书注册成功后，可以通过带外方式下载本地证书abc_local.cer。下载后，可以通过文件传输协议导入到设备的存储介质中。

步骤6 安装本地证书。

```
[Switch] pki import-certificate local realm abc pem filename abc_local.cer
 Info: Succeeded in importing file.
```

安装本地证书后，设备就可以使用证书来保护通信。

步骤7 验证配置结果。

执行命令**display pki certificate local**查看已经导入内存的本地证书的内容。

```
[Switch] display  pki certificate local realm abc
 The x509 object type is certificate:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            48:65:aa:2a:00:00:00:00:3f:c6
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=ca_root
        Validity
            Not Before: Dec 21 11:46:10 2015 GMT
            Not After : Dec 21 11:56:10 2016 GMT
        Subject: C=CN, ST=jiangsu, O=huawei, OU=info, CN=hello
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:94:6f:49:bd:6a:f3:d5:07:ee:10:ee:4f:d3:06:
                    80:59:15:cb:a8:0a:b2:ba:c2:db:52:ec:e9:d1:a7:
                    72:de:ac:35:df:bb:e0:72:62:08:3e:c5:54:c1:ba:
                    4a:bb:1b:a9:d9:dc:e4:b6:4d:ca:b3:54:90:b6:8e:
```



```
                15:a3:6e:2d:b2:9e:9e:7a:33:b0:56:3f:ec:bc:67:
                1c:4c:59:c6:67:0f:a7:03:52:44:8c:53:72:42:bd:
                6e:0c:90:5b:88:9b:2c:95:f7:b8:89:d1:c2:37:3e:
                93:78:fa:cb:2c:20:22:5f:e5:9c:61:23:7b:c0:e9:
                fe:b7:e6:9c:a1:49:0b:99:ef:16:23:e9:44:40:6d:
                94:79:20:58:d7:e1:51:a1:a6:4b:67:44:f7:07:71:
                54:93:4e:32:ff:98:b4:2b:fa:5d:b2:3c:5b:df:3e:
                23:b2:8a:1a:75:7e:8f:82:58:66:be:b3:3c:4a:1c:
                2c:64:d0:3f:47:13:d0:5a:29:94:e2:97:dc:f2:d1:
                06:c9:7e:54:b3:42:2e:15:b8:40:f3:94:d3:76:a1:
                91:66:dd:40:29:c3:69:70:6d:5a:b7:6b:91:87:e8:
                bb:cb:a5:7e:ec:a5:31:11:f3:04:ab:1a:ef:10:e6:
                f1:bd:d9:76:42:6c:2e:bf:d9:91:39:1d:08:d7:b4:
                18:53
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                IP Address:10.2.0.2, DNS:test.abc.com, email:user@test.abc.com
            X509v3 Subject Key Identifier:
                15:D1:F6:24:EB:6B:C0:26:19:58:88:91:8B:60:42:CE:BA:D5:4D:F3
            X509v3 Authority Key Identifier:
                keyid:B8:63:72:A4:5E:19:F3:B1:1D:71:E1:37:26:E1:46:39:01:B6:82:C
5

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:file://\\vasp-e6000-127.china.huawei.com\CertEnroll\ca_roo
t.crl
                  URI:http://10.3.0.1:8080/certenroll/ca_root.crl

            Authority Information Access:
                CA Issuers - URI:http://vasp-e6000-127.china.huawei.com/CertEnro
ll/vasp-e6000-127.china.huawei.com_ca_root.crt
                OCSP - URI:file://\\vasp-e6000-127.china.huawei.com\CertEnroll\v asp-
e6000-127.china.huawei.com_ca_root.crt

            1.3.6.1.4.1.311.20.2:
                .0.I.P.S.E.C.I.n.t.e.r.m.e.d.i.a.t.e.O.f.f.l.i.n.e
    Signature Algorithm: sha1WithRSAEncryption
         d2:be:a8:52:6b:03:ce:89:f1:5b:49:d4:eb:2b:9f:fd:59:17:
         d4:3c:f1:db:4f:1b:d1:12:ac:bf:ae:59:b4:13:1b:8a:20:d0:
         52:6a:f8:a6:03:a6:72:06:41:d2:a7:7d:3f:51:64:9b:84:64:
         cf:ec:4c:23:0a:f1:57:41:53:eb:f6:3a:44:92:f3:ec:bd:09:
         75:db:02:42:ab:89:fa:c4:cd:cb:09:bf:83:1d:de:d5:4b:68:
         8a:a6:5f:7a:e8:b3:34:d3:e8:ec:24:37:2b:bd:3d:09:ed:88:
         d8:ed:a7:f8:66:aa:6f:b0:fe:44:92:d4:c9:29:21:1c:b3:7a:
         65:51:32:50:5a:90:fa:ae:e1:19:5f:c8:63:8d:a8:e7:c6:89:
         2e:6d:c8:5b:2c:0c:cd:41:48:bd:79:74:0e:b8:2f:48:69:df:
         02:89:bb:b3:59:91:7f:6b:46:29:7e:22:05:8c:bb:6a:7e:f3:
         11:5a:5f:fb:65:51:7d:35:ff:49:9e:ec:d1:2d:7e:73:e5:99:
         c6:41:84:0c:50:11:ed:97:ed:15:de:11:22:73:a1:78:11:2e:
         34:e6:f5:de:66:0c:ba:d5:32:af:b8:54:26:4f:5b:9e:89:89:
         2a:3f:b8:96:27:00:c3:08:3a:e9:e8:a6:ce:4b:5a:e3:97:9e:
         6b:dd:f0:72

Pki realm name: abc
Certificate file name: abc_local.cer
Certificate peer name: -
```

----结束

配置文件

Switch的配置文件

```
#
sysname Switch
#
```



```
vlan batch 100 200
#
interface Vlanif100
 ip address 10.2.0.2 255.255.255.0
#
interface Vlanif200
 ip address 10.1.0.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 200
#
ip route-static 10.3.0.0 255.255.255.0 10.2.0.1
#
pki realm abc
 entity user01
 rsa local-key-pair rsakey
#
pki entity user01
 country CN
 state jiangsu
 organization huawei
 organization-unit info
 common-name hello
 fqdn test.abc.com
 ip-address 10.2.0.2
 email user@test.abc.com
#
return
```

15.16 PKI 常见配置错误

15.16.1 获取 CA 证书失败

故障现象

- 通过手工方式获取CA证书，查看设备存储介质中没有下载到CA证书，其失败的原因为通过HTTP方式下载CA证书时配置的不正确。
- 通过SCEP协议获取CA证书，查看设备存储介质中没有下载到CA证书，其失败的原因如下：
  - 获取CA证书的命令未配置。
  - 信任的CA名称配置的不正确或未配置。
  - 证书注册服务器的URL配置的不正确或未配置。
  - 指定的PKI实体未配置。
  - 指纹信息配置的不正确或未配置。
  - 使用的RSA密钥对未配置。
  - TCP连接使用的源接口配置的不正确。

操作步骤

- 通过手工方式获取CA证书

  检查HTTP方式下载CA证书的配置是否正确。如果不正确，请修改相应的内容。详情请参见命令**pki http**。

- 通过SCEP协议获取CA证书
  a. 检查在系统视图下是否已执行命令**pki get-certificate**申请CA证书。
     如果没有，请执行本命令。当申请CA证书相关配置不全时，会提示您配置相应的内容。
  b. 检查PKI域下配置的申请CA证书的相关配置是否正确。
     可以在任意视图下执行命令**display pki realm**或者在PKI域下执行**display this**查看。
     如下所示，这里例举申请CA证书所需的配置。

```
pki realm test
 ca id ca_server   //配置PKI域信任的CA
 enrollment-url http://10.13.14.15:8080/certsrv/mscep/mscep.dll   //配置证书注册服务器的URL
 entity zzz   //指定使用的PKI实体
 fingerprint sha1 7a34d94624b1c1bcbf6d763c4a67035d5b578eaf   //配置对CA证书进行认证时使用的CA证书指纹，从CA服务器上获取
 rsa local-key-pair 8   //指定使用的RSA密钥对
 source interface GigabitEthernet0/0/2   //指定TCP连接使用的源接口（确保该接口为三层接口，且接口下已经配置了IP地址），缺省情况下设备使用出接口作为TCP连接的源接口
```

     如果相关配置不正确，请修改相应的内容。详情请参见**15.8.1 配置通过SCEP协议为PKI实体申请和更新本地证书**。

----结束

15.16.2 获取本地证书失败

故障现象

- 通过手工方式离线获取本地证书，查看设备存储介质中没有下载到本地证书，其失败的原因如下：
  - 指定的PKI实体配置的不正确。
  - 挑战密码配置的不正确或未配置。
  - 通过HTTP方式下载本地证书时配置的不正确。
- 通过SCEP或CMPv2协议获取本地证书，查看设备存储介质中没有下载到本地证书，其失败的原因如下：
  - 执行获取操作之前PKI域中没有CA证书。
  - 指定的PKI实体配置的不正确或未配置。
  - 信任的CA名称配置的不正确或未配置。
  - 证书注册服务器的URL配置的不正确或未配置。
  - 使用的RSA密钥对未配置。
  - TCP连接使用的源接口配置的不正确。
  - 签名证书注册请求消息使用的摘要算法配置的不正确。
  - 挑战密码配置的不正确或未配置。
  - 消息认证码的参考值和秘密值配置的不正确或未配置。
  - 消息认证码的参考值和秘密值配置的不正确或未配置。
  - 用于证明身份的证书配置不正确。
  - 用于证明身份的证书配置不正确。

操作步骤

- 通过手工方式获取本地证书
  a. 检查配置的PKI实体配置是否正确。

     在PKI域下指定的PKI实体，可以执行命令**display pki entity**查看配置的PKI实体信息。

     如果某些内容配置错误，例如PKI实体所属的国家代码配置错误，请修改相应的内容。详情请参见**15.7.1 配置PKI实体信息**。
  b. 检查挑战密码配置是否正确。

     请先确定CA服务器是否要验证挑战密码，如果是，请配置CA服务器的挑战密码，两者要一致。详情请参见命令**pki enroll-certificate**。
  c. 检查HTTP方式下载本地证书的配置是否正确。

     如果不正确，请修改相应的内容。详情请参见命令**pki http**。
- 通过SCEP或CMPv2协议获取本地证书
  a. 检查CA证书是否已导入设备的内存中。

     可以执行命令**display pki certificate**查看设备内存中的CA证书。

     如果没有请获取CA证书并执行命令**pki import-certificate**将CA证书导入设备的内存中。
  b. 检查配置的PKI实体配置是否正确。

     在PKI域下指定的PKI实体，可以执行命令**display pki entity**查看配置的PKI实体信息。

     如果某些内容配置错误，例如PKI实体所属的国家代码配置错误，请修改相应的内容。详情请参见**15.7.1 配置PKI实体信息**。
  c. 检查PKI域或者CMP会话下配置的申请CA证书的相关配置是否正确。

     - PKI域下

       可以在任意视图下执行命令**display pki realm**或者在PKI域下执行命令**display this**查看。

       如下所示，这里例举申请本地证书所需的配置。

       ```
       pki realm test
        ca id ca_server   //配置PKI域信任的CA
        enrollment-url http://10.13.14.15:8080/certsrv/mscep/mscep.dll   //配置证书注册服务器的URL
        entity zzz   //指定使用的PKI实体
        rsa local-key-pair 8   //指定使用的RSA密钥对
        password cipher %^%#\1HN-bn(k;^|O85OAtYF3(M4%^%#   //配置SCEP证书申请时使用的挑战密码，与CA服务器一致
        source interface Vlanif100   //指定TCP连接使用的源接口（确保该接口为三层接口，且接口下已经配置了IP地址），缺省情况下设备使用出接口作为TCP连接的源接口
        enrollment-request signature message-digest-method sha256   //配置签名证书注册请求消息使用的摘要算法，与CA服务器一致
       ```

       如果相关配置不正确，请修改相应的内容。详情请参见**15.8.1 配置通过SCEP协议为PKI实体申请和更新本地证书**。

     - CMP会话下

       可以在CMP会话下执行命令**display this**查看。

       如下所示，这里例举申请CA证书所需的配置。

       ```
       pki cmp session cmp
        cmp-request ca-name "C=cn,ST=beijing,L=SD,O=BB,OU=BB,CN=BB"   //配置CA的名称，CA
       ```

```
名称中各个字段的顺序必须要和实际CA证书中的顺序保持一致
 cmp-request authentication-cert local.cer  //配置CMPv2请求中用于证明身份的证书，用于更新证书或为其他设备申请证书等
 cmp-request entity user01  //指定使用的PKI实体
 cmp-request server url http://10.3.0.1:8080  //配置CMPv2服务器的URL
 cmp-request rsa local-key-pair rsa  regenerate  //指定使用的RSA密钥对
 cmp-request message-authentication-code 1234 %^%#ZodFBGH[^BkU2(~>[NRBv|#b>se|@I7"'A,llG_B%^%#  //配置消息认证码的参考值和秘密值，与CA服务器一致
```

如果相关配置不正确，请修改相应的内容。详情请参见**15.8.2 配置通过CMPv2协议为PKI实体申请和更新本地证书**。

----结束

15.17 PKI FAQ

15.17.1 CA 证书、本地证书和自签名证书的区别?

CA证书、本地证书和自签名证书的区别如**表15-5**所示。

表 15-5 证书类型

类型	描述	说明
自签名证书	自签名证书又称为根证书，是自己颁发给自己的证书，即证书中的颁发者和主体名相同。	申请者无法向CA申请本地证书时，可以通过设备生成自签名证书，可以实现简单证书颁发功能。 设备不支持对其生成的自签名证书进行生命周期管理（如证书更新、证书撤销等），为了确保设备和证书的安全，建议用户替换为自己的本地证书。
CA证书	CA自身的证书。如果PKI系统中没有多层级CA，CA证书就是自签名证书；如果有多层级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。	申请者通过验证CA的数字签名从而信任CA，任何申请者都可以得到CA的证书（含公钥），用以验证它所颁发的本地证书。
本地证书	CA颁发给申请者的证书。	-
设备本地证书	设备根据CA证书给自己颁发的证书，证书中的颁发者名称是CA服务器的名称。	申请者无法向CA申请本地证书时，可以通过设备生成设备本地证书，可以实现简单证书颁发功能。

15.17.2 证书支持哪几种格式?

设备支持三种文件格式保存证书，如下表所示。

表 15-6 证书格式

格式	描述	说明
PKCS#12	以二进制格式保存证书，可以包含私钥，也可以不包含私钥。常用的后缀有：.P12和.PFX。	对于证书后缀为.CER或.CRT，可以用记事本打开证书，查看证书内容来区分证书格式。 ● 如果有类似 " -----BEGIN CERTIFICATE----- " 和 " -----END CERTIFICATE----- " 的头尾标记，则证书格式为PEM。 ● 如果是乱码，则证书格式为DER。
DER	以二进制格式保存证书，不包含私钥。常用的后缀有：.DER、.CER和.CRT。	
PEM	以ASCII码格式保存证书，可以包含私钥，也可以不包含私钥。常用的后缀有：.PEM、.CER和.CRT。	

15.17.3 如何手工导入证书和 RSA 密钥对?

说明

用户通过设备生成证书请求文件（RSA密钥对已经在设备上生成），并将证书请求文件提供给证书颁发机构（CA），CA只颁发本地证书。用户只需将CA提供的CA和本地证书导入设备内存中，无需导入RSA密钥对。

手工替换CA和本地证书时，请先确保证CA和本地证书未被业务使用，然后再执行命令**pki delete-certificate**删除CA和本地证书。例如删除本地证书：

```
[HUAWEI] pki delete-certificate local realm abc
```

手工导入证书和RSA密钥对的步骤如下所示：

1. 用户已通过Web、磁盘、电子邮件等带外方式将申请证书信息发送给CA申请本地证书。
2. 下载CA提供的CA证书、本地证书和RSA密钥对文件，并通过TFTP等方式上传至设备的存储介质中。

   一般情况下，DER和PEM格式的证书和密钥对文件是分开的，PKCS#12格式的证书和密钥对在同一个文件中。
3. 导入CA证书，如果有多个CA证书，则需导入全部CA证书。

   例如，获取到的CA证书文件名为rootca.pem。

   ```
   <HUAWEI> system-view
   [HUAWEI] pki realm abc
   [HUAWEI-pki-realm-abc] quit
   [HUAWEI] pki import-certificate ca realm abc pem filename rootca.pem
   ```


导入成功后，查看CA证书的信息。

```
[HUAWEI] display pki certificate ca realm abc
```

4. 导入本地证书。

   例如，获取到的本地证书文件名为localcert.pem。

   ```
   [HUAWEI] pki import-certificate local realm abc pem filename localcert.pem
   ```

   导入成功后，查看本地证书的信息。

   ```
   [HUAWEI] display pki certificate local realm abc
   ```

5. 导入RSA密钥对。对于PEM和PKCS#12格式的文件还需要CA提供的RSA密钥对相应的密码。

   例如，获取到的RSA密钥对文件名为local_privatekey.pem，密码为test@123。

   ```
   [HUAWEI] pki import rsa-key-pair abc pem local_privatekey.pem password test@123
   ```

   导入成功后，查看RSA密钥对的信息。

   ```
   [HUAWEI] display pki rsa local-key-pair name abc public
   ```

6. 检查导入的本地证书和RSA密钥对是否匹配，如果没有找到匹配的密钥对，请检查导入的文件是否正确。

   ```
   [HUAWEI] pki match-rsa-key certificate-filename localcert.pem
   Info: The file localcert.pem contains certificates 1.
   Info: Certificate 1 from file localcert.pem matches RSA key test.
   ```


16 OLC 配置

16.1 OLC 简介

定义

CPU过载控制OLC（Overload Control）是一种CPU过载调控机制。当CPU过载时，OLC能够对受监控协议报文和任务进行调控，通过不同优先级业务的合理规划和限制报文通过等方式，降低对CPU资源的消耗，并确保设备不会因为某种受监控协议或任务冲击CPU导致的CPU过载而影响对其他业务的正常处理。

目的

由于现网组网的复杂性，上送CPU的业务量过大或发生非法业务恶意冲击CPU等问题，都可能会导致CPU过载。CPU过载会造成设备性能下降和业务处理异常等问题。

OLC采用多级漏桶算法，通过令牌桶和多级漏桶的方式对上送CPU处理的受监控协议报文和任务进行调控，能够解决如下问题：

- 避免CPU资源被长时间过度消耗，保证设备资源的可用性。
- 避免设备受到非法业务的恶意攻击，保证设备的安全性。
- 避免某种业务冲击影响对其他业务的正常处理，保证业务处理的公平性。

16.2 OLC 原理描述

OLC和CPU占用率相关联，当CPU占用率达到OLC启动门限阈值时，OLC功能启动。OLC采用多级漏桶算法实现对受监控协议报文和任务的调控，其中令牌桶决定其是否允许通过，多级漏桶则决定其通过的速率，通过后的报文才能被上送到CPU。

当前受OLC监控的任务包括ACL任务和ARP广播任务，受OLC监控的协议报文和白名单协议报文，请参见**16.8 受OLC监控的协议报文和白名单协议报文汇总**。

令牌桶

令牌桶用于存放令牌，可存放的令牌总数相当于CPU占用率100%时的报文处理能力。当报文进入漏桶时，必须获得一个令牌才允许通过。令牌桶令牌数的恢复周期为1秒，系统每秒为令牌桶分配一定的令牌数，OLC根据CPU占用率变化自动调整给令牌桶分配的令牌数以控制报文通过的数量。当CPU占用率超过一定阈值后，系统会减少分配的令牌数。当令牌桶的令牌用完之后，进入漏桶的报文将申请不到令牌，则无法被上送到CPU，从而减少CPU的负荷。

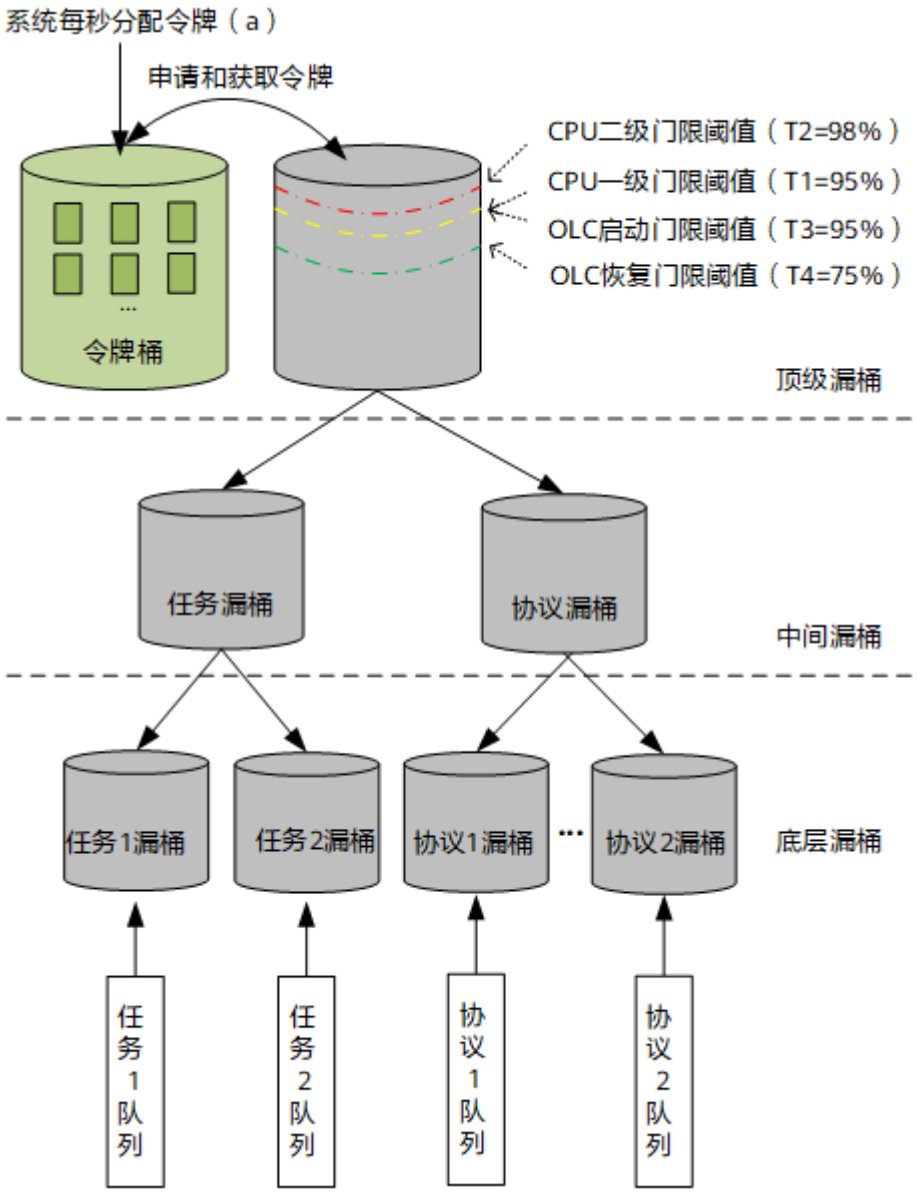
多级漏桶

漏桶相当于一个计数器，每当报文进入漏桶时，首先向令牌桶申请令牌，令牌申请成功后，漏桶计数值加1，该计数值累计达到设定的阈值时，后续到达的报文可能会被丢弃。报文通过后，漏桶计数值减1，该数值按照一定的漏出速率减少，漏桶据此控制报文按照一定的速率通过。

OLC采用的多级漏桶包括顶级漏桶、中间漏桶和底层漏桶，由顶级漏桶对整个系统的漏桶进行控制。中间漏桶分为任务中间漏桶和协议中间漏桶，不同受监控协议和任务关联不同的底层漏桶。OLC根据不同业务的优先级，给各个漏桶赋予了不同的权重值，并按照权重值给各漏桶分配资源（可申请的令牌数），保证了不同业务之间的公平性。

多级漏桶基本原理如**图16-1**所示。顶级漏桶相当于CPU占用率100%时的处理能力，当CPU占用率达到OLC启动门限阈值时OLC才能启动调控。各受监控协议和任务上送CPU前，分别进入对应的底层漏桶，逐级向上向令牌桶申请令牌，令牌申请成功后才被允许通过。同时，多级漏桶通过调整漏出速率控制报文通过的速率。

图 16-1 多级漏桶基本原理



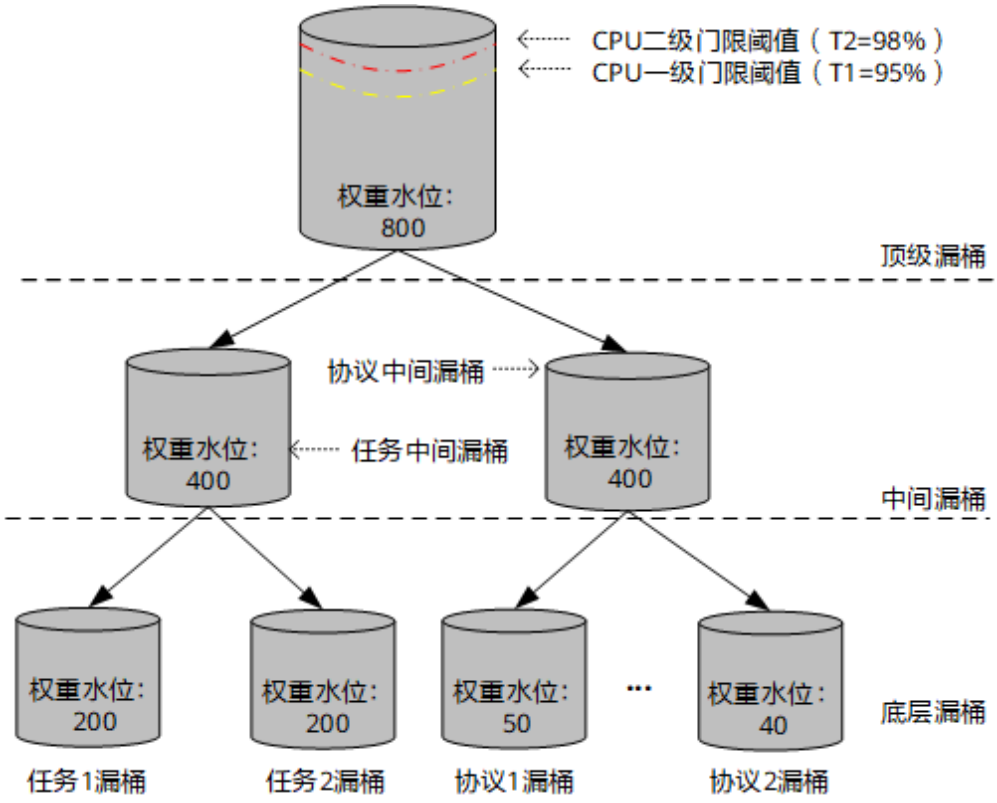
- 多级漏桶的控制参数
  - 漏出速率（a）：该参数数值与系统每秒为令牌桶分配的令牌数相同，表示每秒处理的报文数量。
  - 顶级漏桶容量（N）：该参数默认值相当于CPU占用率100%时的报文处理能力。
  - CPU一级门限阈值（T1）：该参数默认值为95%，表示CPU占用率为95%。当CPU占用率达到该门限阈值时，开始调低漏出速率。
  - CPU二级门限阈值（T2）：该参数默认值为98%，表示CPU占用率为98%。当CPU占用率达到该门限阈值时，加倍调低漏出速率。
  - OLC启动门限阈值（T3）：该参数与CPU一级门限阈值相同。当CPU占用率达到OLC启动门限阈值时，启动OLC启动门限定时器（10秒），在该定时器超时前，如果CPU占用率没有低于OLC启动门限阈值，启动OLC功能。

- OLC恢复门限阈值（T4）：该参数默认值为75%，表示CPU占用率为75%，该数值等于CPU一级门限阈值减去20%。当CPU占用率低于OLC恢复门限阈值时，启动OLC恢复门限定时器（20秒），在该定时器超时前，如果CPU不再次达到OLC启动门限阈值，则停止OLC功能。
- 调整因子（S）：该参数用于设置漏出速率的调整速度，调整因子越小，调整速度越快，调整因子越大，调整速度越慢。调整因子过小可以让漏出速率能够根据业务变化得到快速调整，但是可能会导致漏出速率出现反复抖动。

- 多级漏桶的权重水位

  OLC按照权重值给各漏桶分配资源，各漏桶被分配的资源决定了其权重水位，即各漏桶可申请的令牌数。如图16-2所示（仅为示例），顶级漏桶的初始权重水位相当于CPU占用率95%时可申请的令牌数，随后由顶级漏桶按权重值逐级向下分配给所有子漏桶，每一层级所有漏桶的权重水位之和相同。

  图 16-2 多级漏桶权重水位分配



- 多级漏桶水位更新

  漏桶的水位是指该漏桶需要申请令牌的报文数量，各级漏桶的水位根据令牌申请情况和权重水位进行更新，具体流程如下：

  a. 受监控协议报文或任务进入底层漏桶后，需要申请令牌，漏桶的水位增长，同时上级漏桶即中间漏桶和顶级漏桶的水位也增长同样的水位。
  b. 底层漏桶判断自身当前水位是否超过权重水位，如果没有超过，申请令牌成功，允许报文通过；如果底层漏桶水位超过权重水位，则向上级漏桶申请资源，如果上级漏桶没有超过权重水位，申请令牌成功，允许报文通过。
  c. 报文通过后，底层漏桶减少的水位，在上级漏桶减少同样的水位。

- 多级漏桶债务分摊

如果顶级漏桶的水位超过了权重水位，表明整个系统产生了负债。系统需要每秒对漏桶水位进行刷新，计算各级漏桶的债务，没有产生负债的漏桶可以共享出空闲资源，对产生债务的漏桶的债务资源进行分摊。

说明

空闲协议漏桶只能分摊负债协议漏桶的负债资源，空闲任务漏桶只能分摊负债任务漏桶的负债资源。

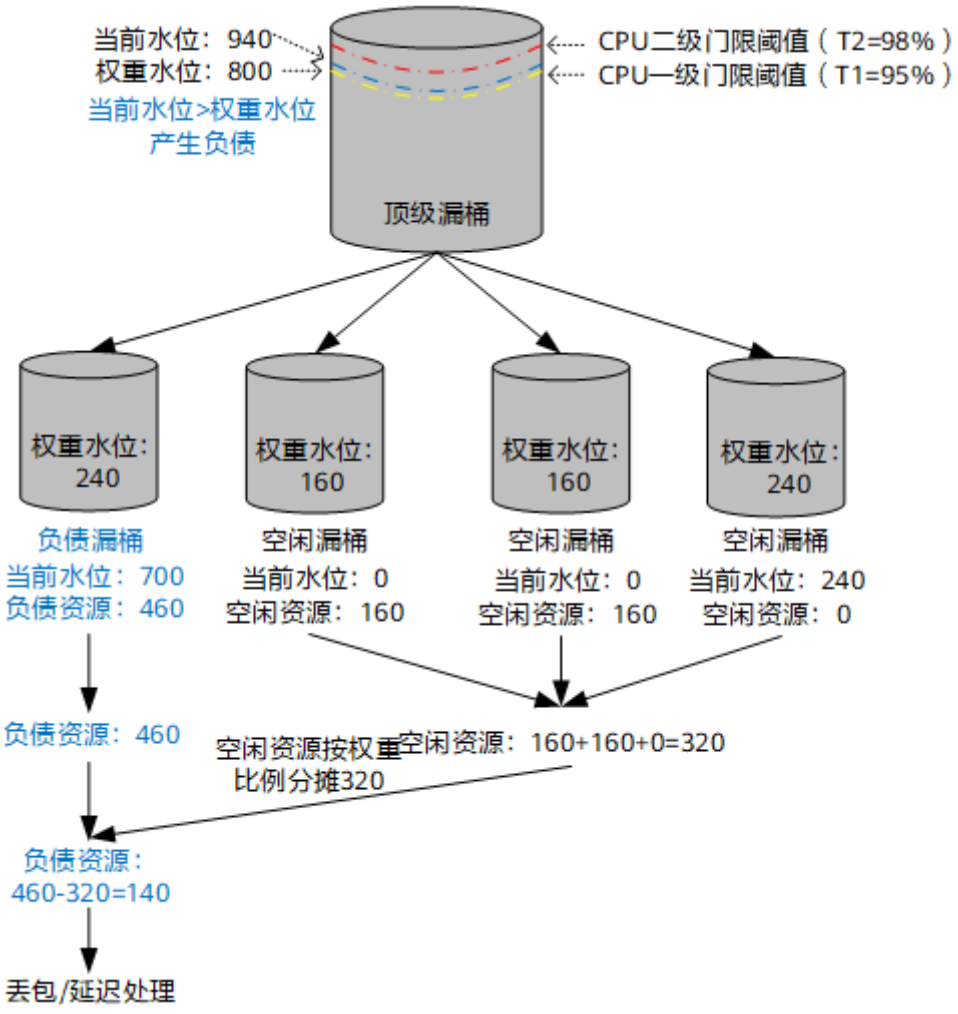
如图16-3所示（仅为示例），顶级漏桶的当前水位超过了权重水位，系统产生负债，具体债务分摊流程如下：

a. 计算负债资源和空闲资源：负债漏桶和空闲漏桶分别计算当前水位和权重水位的差值得出负债资源和空闲资源。

b. 自顶向下，逐级分摊：各负债漏桶按照权重比例，分摊其他空闲漏桶的空闲资源。

c. 丢包或延迟处理：如果负债漏桶仍有负债资源，对于协议报文进行丢包处理，对于任务进行延迟处理。

图 16-3 多级漏桶债务分摊



- 漏桶水位阈值设置

  为防止某种受监控协议或任务漏桶独占顶级漏桶的资源，出现资源分配不公平，在顶级漏桶产生负债时，根据每一层级漏桶的空闲资源和负债资源情况，对负债

较大的漏桶计算漏桶水位阈值。在设置漏桶水位阈值后，该漏桶申请令牌时，如果当前水位大于漏桶权重水位且大于漏桶水位阈值，则不允许向上级漏桶申请资源。

16.3 OLC 配置注意事项

涉及网元

无需其他网元配合。

License 支持

OLC是交换机的基本特性，无需获得License许可即可应用此功能。

V200R021C00、V200R021C01 版本特性支持情况

S600-E系列交换机中所有款型均支持OLC。

说明

如需了解交换机软件配套详细信息，请点击**Info-Finder**。

特性依赖和限制

- 对于非受监控任务导致的CPU过载，OLC无法调控此类任务，因此受监控任务的正常处理会受到CPU过载的影响。

16.4 OLC 缺省配置

参数	缺省值
OLC功能	已使能
所有受监控协议的OLC功能	已使能
所有受监控任务的OLC功能	未使能
OLC告警功能	已使能
CPU门限阈值和调整因子	• CPU一级门限阈值：95% • CPU二级门限阈值：98% • 调整因子：10

16.5 配置 OLC

16.5.1 使能 OLC 功能

背景信息

为了在CPU过载时能够及时对受监控协议和任务进行调控，设备默认使能OLC功能，用户可以选择使能指定受监控协议或任务的OLC功能。同时，设备默认使能OLC告警功能，当CPU占用率达到OLC启动门限阈值或低于OLC恢复门限阈值时发出告警。

操作步骤

- 使能OLC功能
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**undo cpu-overload-control disable slot** *slot-id*，使能OLC功能。

     缺省情况下，OLC功能处于使能状态。
  c. （可选）执行命令**undo cpu-overload-control packet-type** *packet-type* &<1-20> **disable slot** *slot-id*，使能指定受监控协议的OLC功能。

     缺省情况下，所有受监控协议的OLC功能均处于使能状态。
  d. （可选）执行命令**cpu-overload-control task** *task-name* &<1-2> **enable slot** *slot-id*，使能指定受监控任务的OLC功能。

     缺省情况下，所有受监控任务的OLC功能均处于未使能状态。

  说明

  使能OLC功能后，所使能的受监控协议和任务的OLC功能才能生效。
- （可选）使能OLC告警功能
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**undo cpu-overload-control alarm disable**，使能OLC告警功能。

     缺省情况下，OLC告警功能处于使能状态。

----结束

16.5.2 配置 CPU 门限阈值和调整因子

背景信息

OLC功能只有当CPU占用率达到OLC启动门限阈值（CPU一级门限阈值）时会启动调控，通过调低漏出速率降低报文通过速度，达到CPU二级门限阈值时加倍调低漏出速率，当CPU占用率低于OLC恢复门限阈值（CPU一级门限阈值减去20%）时停止调控。调整因子用于设置漏出速率的调整速度，调整因子越小，调整速度越快，调整因子越大，调整速度越慢。漏出速率的调整速度不宜过快或过慢，否则会导致漏出速率出现反复抖动，建议保持系统默认值。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-overload-control** { **threshold1** *threshold1-value* | **threshold2** *threshold2-value* | **adjustfactor** *adjustfactor-value* } * **slot** *slot-id*，设置CPU门限阈值和调整因子。

缺省情况下，CPU一级门限阈值为95%、CPU二级门限阈值为98%、调整因子为10。

----结束

16.5.3 配置漏桶权重值

背景信息

各个使能OLC功能的受监控协议和任务分别关联一个底层漏桶，设备默认根据各受监控协议和任务的优先级为对应漏桶分配了不同的权重值，系统根据各漏桶的权重值为其分配不同的权重水位（可申请的令牌数）。因此用户可以结合实际业务量的需求，为各受监控协议和漏桶设置合理的权重值。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**cpu-overload-control** { **packet-type** *packet-type* | **task** *task-name* } **bucket-weight** *bucket-weight-value* **slot** *slot-id* ，设置指定受监控协议或任务漏桶的权重值。

缺省情况下，各受监控协议和任务的权重值如下：8021x-1st为90，8021x-other 为200，arp-request、arp-reply、icmp、dhcp、arp-miss、igmp、ttl-expired、ip-frag、fib-hit、icmpv6、dhcpv6、mld和nd为290，cos-4为250，cos-3为240，cos-2为200，cos-1为150，cos-0为100，acl和arpa为2500。

----结束

16.5.4 检查 OLC 功能配置结果

操作步骤

- 执行命令**display cpu-overload-control configuration** [**packet-type** *packet-type* | **task** *task-name*] **slot** *slot-id*，查看OLC功能的配置信息。

----结束

16.6 维护 OLC

背景信息

执行如下命令可以查看或清除OLC功能的统计信息。

操作步骤

- 执行命令**display cpu-overload-control statistics** [**packet-type** *packet-type* | **task** *task-name*] **slot** *slot-id*，查看OLC功能的统计信息。
- 执行命令**reset cpu-overload-control statistics** [**packet-type** *packet-type* | **task** *task-name*] **slot** *slot-id*，清除OLC功能的统计信息。

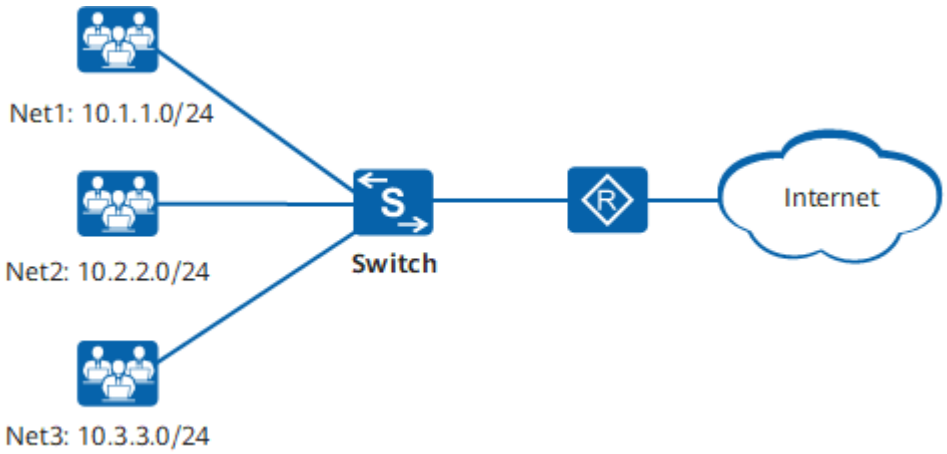
----结束

16.7 配置 OLC 示例

组网需求

如图16-4所示，位于不同网段的用户通过Switch接入Internet。由于接入了大量用户，Switch的CPU会处理大量的协议报文和任务。其中，用户发现Switch经常收到大量的ARP Request、ARP Reply和ARP Miss协议报文，并经常处理ARP广播任务，常因此导致CPU占用率大幅升高，造成业务处理异常。用户希望设备能够在CPU占用率超过90%时发出告警并对以上协议报文和任务进行调控，使得CPU负载时不会因为以上协议和任务的冲击而影响其他业务的正常处理，同时希望能够降低CPU的占用率，使其维持在一个稳定水平。

图 16-4 配置 OLC 示例组网图



配置思路

采用如下思路在Switch上配置OLC功能：

1. 使能OLC功能。
2. 使能ARP Request、ARP Reply、ARP Miss协议报文的OLC功能。
3. 使能ARP广播任务的OLC功能。
4. 使能OLC告警功能。
5. 设置OLC启动门限阈值为90%。

操作步骤

步骤1 使能OLC功能。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] undo cpu-overload-control disable slot 0
```

步骤2 使能ARP Request、ARP Reply、ARP Miss协议报文的OLC功能。

```
[Switch] undo cpu-overload-control packet-type arp-request arp-reply arp-miss disable slot 0
```

步骤3 使能ARP广播任务的OLC功能。

```
[Switch] cpu-overload-control task arpa enable slot 0
```

步骤4 使能OLC告警功能。

```
[Switch] undo cpu-overload-control alarm disable
```

步骤5 设置OLC启动门限阈值为90%。

```
[Switch] cpu-overload-control threshold1 90 slot 0
Warning: The value of threshold 1 affects the service processing capability when the CPU is overloaded.
Continue? [Y/N]:y
[Switch] quit
```

步骤6 验证配置结果

查看OLC功能的配置信息。

```
<Switch> display cpu-overload-control configuration slot 0
CPU OLC Status: enable.
Alarm Status  : enable.
Low  Threshold: 90%.
High Threshold: 98%.
Ajustfactor   : 10.
Total Weight  : 10000.
----------------------------------
Task            Weight   Enable
----------------------------------
arpa             2500     Y
acl              2500     N
----------------------------------
----------------------------------
Protocol        Weight   Enable
----------------------------------
8021x             290     Y
  8021x-1st        90     Y
  8021x-other     200     Y
arp-request       290     Y
arp-reply         290     Y
icmp              290     Y
dhcp              290     Y
arp-miss          290     Y
igmp              290     Y
ttl-expired       290     Y
ip-frag           290     Y
fib-hit           290     Y
icmpv6            290     Y
dhcpv6            290     Y
nd                290     Y
mld               290     Y
cos-4             250     Y
cos-3             240     Y
cos-2             200     Y
cos-1             150     Y
cos-0             100     Y
----------------------------------
```

查看OLC功能的统计信息。

```
<Switch> display cpu-overload-control  statistics slot 0
-------------------------------------------------------------------------------
Task        Total Runtime  Total Delaytime  Average Runtime  Average Delaytime
              (ms)           (ms)             (ms)             (ms)
-------------------------------------------------------------------------------
arpa        0              0                0                0
acl         0              0                0                0
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Protocol     Total Pass     Total Drop      Average Pass     Average Drop
             (packet)       (packet)        (packet)         (packet)
-------------------------------------------------------------------------------
8021x-1st    0              0               0                0
8021x-other  0              0               0                0
arp-request  0              0               0                0
```

```
arp-reply    0            0            0            0
icmp         0            0            0            0
dhcp         0            0            0            0
arp-miss     0            0            0            0
igmp         0            0            0            0
ttl-expired  0            0            0            0
ip-frag      0            0            0            0
fib-hit      0            0            0            0
icmpv6       0            0            0            0
dhcpv6       0            0            0            0
nd           0            0            0            0
mld          0            0            0            0
cos-4        0            0            0            0
cos-3        0            0            0            0
cos-2        0            0            0            0
cos-1        0            0            0            0
cos-0        0            0            0            0
------------------------------------------------------------------------------
```

----结束

16.8 受 OLC 监控的协议报文和白名单协议报文汇总

OLC功能启动后，会对受监控的协议报文进行调控。对于不受监控协议报文，即白名单协议报文，OLC功能不会对其进行调控。

受 OLC 监控的协议报文汇总

报文类型	报文解释
8021x-1st	802.1X首片报文
8021x-other	802.1X非首片报文
arp-request	ARP Request报文
arp-reply	ARP Reply报文
icmp	ICMP报文
dhcp	DHCP报文
igmp	IGMP报文
ttl-expired	IPv4 TTL终结的报文
ip-frag	IP分片报文
fib-hit	命中路由报文
icmpv6	ICMPv6报文
dhcpv6	DHCPv6报文
mld	MLD报文
nd	IPv6邻居发现协议报文
cos-4	优先级为大于等于4的报文（白名单协议报文除外）

报文类型	报文解释
cos-3	优先级为3的报文（白名单协议报文除外）
cos-2	优先级为2的报文（白名单协议报文除外）
cos-1	优先级为1的报文（白名单协议报文除外）
cos-0	优先级为0的报文（白名单协议报文除外）

OLC 白名单协议报文汇总

以下列出的为所有OLC白名单协议报文类型，具体协议报文以的设备支持情况为准。

报文类型	报文解释
asdp	ASDP报文
bfd	BFD报文
bgp	BGP报文
bgp4plus	BGP4PLUS报文
bpdu	BPDU报文
bpdu-tunnel	BPDU隧道报文
capwap-ac-auth	AC间心跳报文
capwap-ap-auth	分布式AP通过中心AP注册时发送的AP认证报文
capwap-ap-update	CAPWAP AP升级报文
capwap-echo	CAPWAP回应报文
capwap-keepalive	CAPWAP心跳报文
capwap-license-mng	CAPWAP License管理报文
dldp	DLDP报文
ecm	ECM报文
eoam-1ag	以太OAM 1ag报文
eoam-3ah	以太OAM 3ah报文
esp	ESP报文
ftp	FTP报文

报文类型	报文解释
gre-keepalive	GRE隧道保活报文
http	HTTP报文
https	HTTPS报文
ip-cloud	NETCONF报文
ipfpm	IPFPM协议报文
ipmc-invalid	IPMC无效报文
ipsec-ah	IPSec报文头认证报文
ipsec-esp	IPSec封装安全载荷协议报文
isis	ISIS报文
lacp	LACP报文
lldp	LLDP报文
macsec-mka	MACsec MKA报文
mpls-ldp	MPLS LDP报文
mpls-oam	MPLS OAM报文
mpls-rsvp	MPLS RSVP报文
ospf	OSPF报文
ospf-hello	OSPF Hello报文
ospfv3	OSPFv3报文
pim	PIM报文
pimv6	PIMv6报文
rip	RIP报文
ripng	RIPng报文
rrpp	RRPP报文
sftp	SFTP报文
snmp	SNMP报文
ssh	SSH报文
stp	STP报文
telnet	Telnet报文
tftp	TFTP报文
vbst	VBST报文

报文类型	报文解释
vbst-trunk	VBST Eth-trunk报文
vcmp	VCMP报文
vrrp	VRRP报文
vrrp6	VRRP6报文

17 业务与管理隔离配置

背景信息

为提高网络安全性，防止非法用户的攻击，系统默认将业务与管理进行隔离。

- **management-port isolate enable**命令用来使能管理口隔离功能，防止非法用户对转发报文进行攻击。设备将禁止管理口和业务口之间转发报文，即从管理口收到的报文不会从业务口转发出去，同样，从业务口收到的报文也不会从管理口转发出去。
- **management-plane isolate enable**命令用来使能管理面隔离功能，防止非法用户通过业务网络对管理网络造成攻击。设备将禁止非法用户通过业务口访问管理口，即业务口接收到目的地址是管理口地址的报文不能访问设备，反之，从管理口到业务口的访问则不做限制。

说明

以上提到的报文是指IP报文。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**management-port isolate enable**，使能管理口隔离功能。

缺省情况下，系统已使能管理口隔离功能。

步骤3 执行命令**management-plane isolate enable**，使能管理面隔离功能。

缺省情况下，系统已使能管理面隔离功能。

----结束

18 安全风险查询

背景信息

由于协议自身的安全性能不同，用户配置时使用的某些协议可能存在安全风险。通过**display security risk**命令可查看系统中存在的安全风险，并根据给出的修复建议解除风险。例如，用户配置了SNMPv1功能，该功能存在安全风险，系统会提示并建议使用SNMPv3协议。

操作步骤

在用户视图下，执行命令**display security risk** [**feature** *feature-name*] [**level** { **high** | **medium** | **low** }]，查询当前系统中存在的安全风险信息及风险的修复建议。

说明

不同级别的用户查看到的安全风险信息也不相同。管理级用户能够查看到系统中所有风险信息，其他级别用户只能看到低于或等于自己级别的风险信息。