HCIE-Security 备考指南

DHCP Snooping(S5700 交换机)

HCIE 只是一个开始….

HCIE 仅是一个证书…懂得做人和处事比证书和技能更重要…

希望大家顺利通过 HCIE，取得更好的职业发展！

目 录

HCIE-Security DHCP Snooping(S5700 交换机)需要掌握的知识点

- 掌握 DHCP Snooping 原理及配置

DHCP Snooping 概述

简要介绍 DHCP Snooping 的原理。

DHCP Snooping 是 DHCP（Dynamic Host Configuration Protocol）的一种安全特性，通过截获 DHCP Client 和 DHCP Server 之间的 DHCP 报文并进行分析处理，可以过滤不信任的 DHCP 报文并建立和维护一个 DHCP Snooping 绑定表。该绑定表包括 MAC 地址、IP 地址、租约时间、绑定类型、VLAN ID、接口等信息。

DHCP Snooping 通过记录 DHCP Client 的 IP 地址与 MAC 地址的对应关系，保证合法用户能访问网络，作用相当于在 DHCP Client 和 DHCP Server 之间建立一道防火墙。

DHCP Snooping 可以解决设备应用 DHCP 时遇到 DHCP DoS（Denial of Service）攻击、DHCP Server 仿冒攻击、DHCP 仿冒续租报文攻击等问题。

S5700 支持的 DHCP Snooping 特性

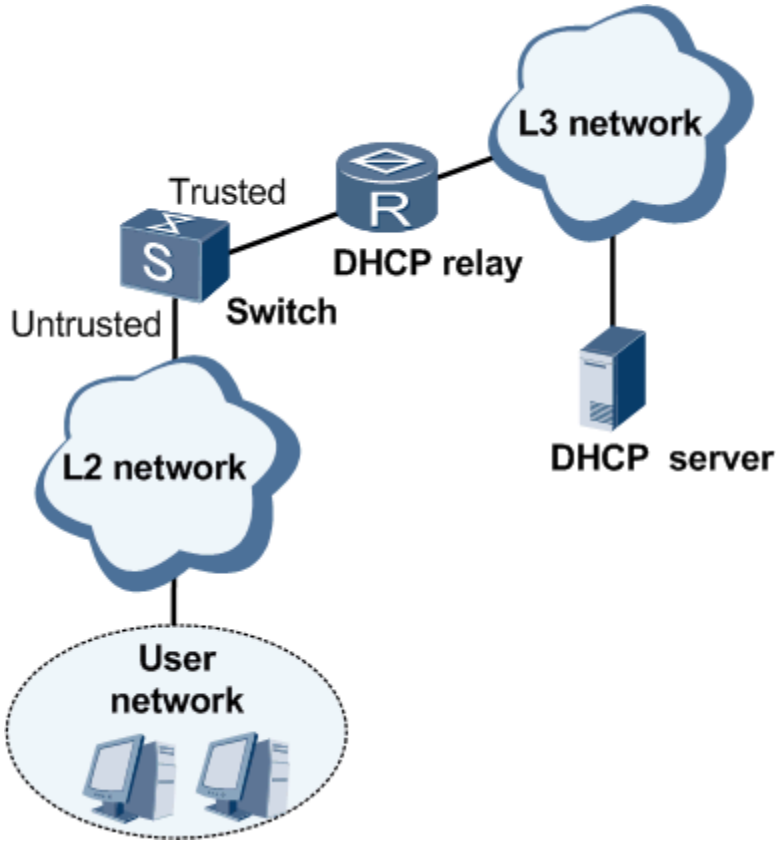
介绍 DHCP Snooping 特性在 S5700 中的支持情况。

S5700 支持 Trusted 接口、DHCP Snooping 安全绑定、IP + MAC + 接口 + VLANID 组合绑定、Option82 字段等安全方面的功能，为 DHCP 功能在网络中的应用提供更高的安全性。

S5700 在二层网络中应用 DHCP Snooping

S5700 部署在二层网络中时，处于 DHCP Relay 和用户网络之间。DHCP Snooping 在 S5700 上的应用如图 1 所示，图中 S5700 使能了 DHCP Snooping 功能。

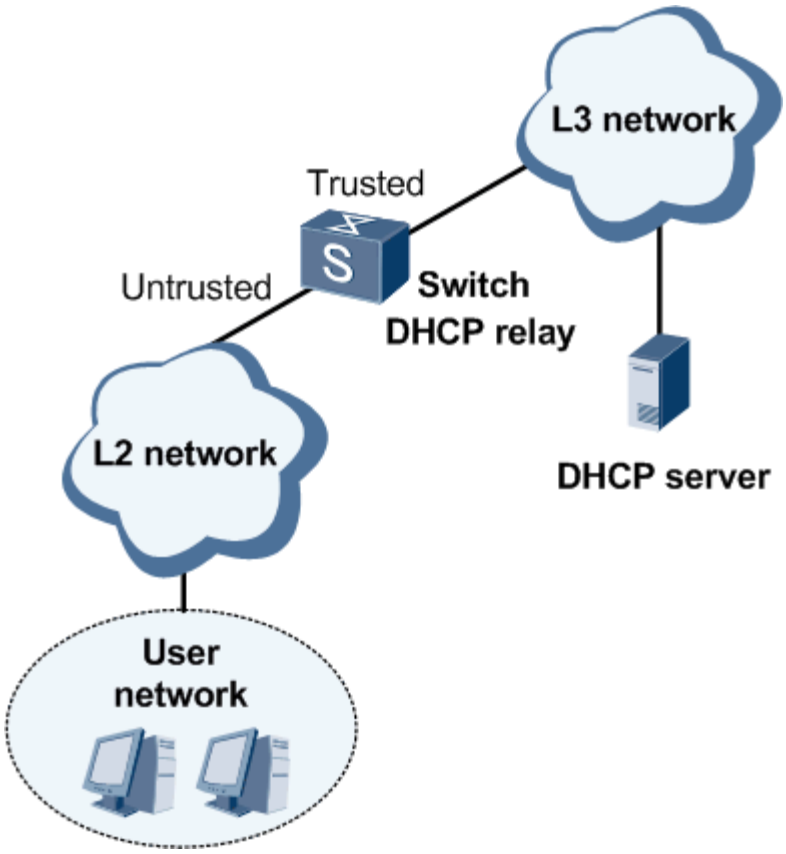
图 1 S5700 在二层网络中应用 DHCP Snooping 典型组网图



S5700 作为 DHCP Relay 应用 DHCP Snooping

S5700 具有三层路由功能，也可以作为 DHCP Relay 应用在组网中。如图 2 所示，S5700 作为 DHCP Relay，使能了 DHCP Snooping 功能。

图 2 S5700 作为 DHCP Relay 应用 DHCP Snooping 典型组网图



说明：

S5700 应用在二层网络中或作为 DHCP Relay 应用时使能 DHCP Snooping，都可以防止如表 1 所示的几种攻击类型。在配置上的区别仅是：作为 DHCP Relay 时支持 ARP 与 DHCP 的联动功能。在二层网络中应用时不支持该功能。

DHCPv6 Snooping

S5700 支持 DHCPv6 Snooping，在使能 DHCP Snooping 功能后，对 IPv6 地址的用户也会生成绑定表。绑定表的内容包括 IPv6 地址、MAC 地址、接口、VLAN 等信息。

DHCP Snooping 能对抗的攻击类型

根据不同的攻击类型，DHCP Snooping 提供不同的工作模式，见表 1。

表 1 攻击类型与 DHCP Snooping 工作模式对应表

攻击类型	DHCP Snooping 工作模式
DHCP Server 仿冒者攻击	配置接口状态为信任（Trusted）/不信任（Untrusted）
改变 CHADDR 值的 DoS 攻击	检查 DHCP 报文的 CHADDR 字段
仿冒 DHCP 续租报文攻击	检查 DHCP Request 报文是否匹配 DHCP Snooping 绑定表

表 1 攻击类型与 DHCP Snooping 工作模式对应表	
攻击类型	**DHCP Snooping 工作模式**
DHCP 报文洪泛攻击	限制 DHCP 报文的上送速率

配置防止 DHCP Server 仿冒者攻击

为防止 DHCP 服务器仿冒者攻击，可使用 DHCP Snooping 的“信任（Trusted）/不信任（Untrusted）”工作模式。

应用环境

当网络中存在 DHCP Server 仿冒者时，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 服务器、错误的 IP 等，从而使 Client 无法访问网络或访问到不正确的网络。

为了避免受到 DHCP Server 仿冒者的攻击，可以在 S5700 上配置 DHCP Snooping 功能，把网络侧的接口配置为 Trusted 模式，把用户侧的接口配置为 Untrusted 模式，凡是从 Untrusted 接口收到的 DHCP Reply 报文全部丢弃。

同时为定位 DHCP Server 仿冒者，可以在 S5700 上配置伪 DHCP Server 探测功能，通过检查 DHCP Reply 报文，获取 DHCP Server 相关信息，记入日志中，便于网络管理员进行网络维护。

前置任务

在配置防止 DHCP Server 仿冒者攻击之前，需要完成以下任务：

- 配置 DHCP Server。

数据准备

在配置防止 DHCP Server 仿冒者攻击之前，需要准备以下数据。

序号	数据
1	需要配置为 Trusted 模式的接口类型和编号

使能 DHCP Snooping 功能

在全局使能 DHCP Snooping 功能之后，必须在接口或 VLAN 下使能，否则不生效。

背景信息

使能 DHCP Snooping 功能的顺序如下所示。

- 全局使能 DHCP 功能。
- 全局使能 DHCP Snooping 功能。
- 在接口或 VLAN 下使能 DHCP Snooping 功能。

操作步骤

- VLAN 视图下使能 DHCP Snooping 功能

  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 [ipv4 | ipv6]**，全局使能 DHCP Snooping 功能。
  4. 执行命令 **vlan** *vlan-id*，进入 VLAN 视图。
  5. 执行命令 **dhcp snooping enable**，使能 VLAN 的 DHCP Snooping 功能。
  6. 执行命令 **quit**，返回到系统视图。
  7. （可选）执行命令 **interface** *interface-type interface-number*，进入接口视图。
  8. （可选）执行命令 **dhcp snooping disable**，去使能 VLAN 下特定接口的 DHCP Snooping 功能。

  如果用户需要去使能 VLAN 下某个特定接口的 DHCP Snooping 功能，需要执行 7、8 步骤。

- 接口视图下使能 DHCP Snooping 功能

  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 [ipv4 | ipv6]**，全局使能 DHCP Snooping 功能。
  4. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  5. 执行命令 **dhcp snooping enable**，使能接口的 DHCP Snooping 功能。

配置接口为信任状态

一般把通向 DHCP Server 的接口设成“信任（Trusted）”，其他接口都设为“不信任（Untrusted）”。

背景信息

使能接口的 DHCP Snooping 功能后，缺省情况下，接口为“不信任”状态。

操作步骤

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。

   该接口为连接 DHCP Server 的网络侧接口。
3. 接口视图下执行命令 **dhcp snooping trusted** ，或者 VLAN 视图下执行命令 **dhcp snooping trusted interface** *interface-type interface-number* ，配置接口为“信任”状态。

   配置接口状态后，从“不信任”接口收到的 DHCP Reply 报文被直接丢弃。

   如果在 VLAN 视图下指定接口为“信任”状态，该接口必须已经加入了该 VLAN。

（可选）使能 DHCP Server 探测功能

使能 DHCP Server 探测功能前，必须使能 S5700 全局和接口下的 DHCP Snooping 功能，否则 DHCP Server 探测功能不生效。

操作步骤

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **dhcp server detect**，使能 DHCP Server 探测功能。

   缺省情况下，S5700 没有使能 DHCP Server 探测功能。

配置防止改变 CHADDR 值的 DoS 攻击

防止攻击者通过改变 CHADDR 值攻击 DHCP Server。

应用环境

如果攻击者改变的不是数据帧头部的源 MAC，而是通过改变 DHCP 报文中的 CHADDR（Client Hardware Address）值来不断申请 IP 地址，而 S5700 仅根据数据帧头部的源 MAC 来判断该报文是否合法，那么 MAC 地址限制不能完全起作用，这样的攻击报文还是可以被正常转发。

为了避免受到攻击者改变 CHADDR 值的攻击，可以在 S5700 上配置 DHCP Snooping 功能，检查 DHCP Request 报文中 CHADDR 字段。如果该字段跟数据帧头部的源 MAC 相匹配，转发报文；否则，丢弃报文。

前置任务

在配置防止改变 CHADDR 值的 DoS 攻击之前，需要完成以下任务：

- 配置 DHCP Server。

数据准备

在配置防止改变 CHADDR 值的 DoS 攻击之前，需要准备以下数据。

序号	数据
1	使能报文检查的接口类型和接口编号

使能对报文的 CHADDR 值检查功能

把 DHCP Request 报文中携带的 CHADDR 字段与以太帧中的源 MAC 值相比较，如果不相同则认为是攻击报文，直接丢弃该报文。

操作步骤

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。

   该接口为用户侧接口。
3. 执行命令 **dhcp snooping check dhcp-chaddr enable**，配置接口或 VLAN 下检查 DHCP 报文的 CHADDR 值与源 MAC 是否一致。

   缺省情况下，S5700 没有使能 CHADDR 值检查功能。

配置防止仿冒 DHCP 续租报文攻击

防止攻击者通过仿冒 DHCP 续租报文攻击 DHCP Server。

应用环境

如果攻击者通过不断发送 DHCP Request 报文来冒充用户续租 IP 地址，会导致一些到期的 IP 地址无法正常回收。

为了避免攻击者仿冒 DHCP 续租报文进行攻击，可以在 S5700 上配置绑定表，检查 DHCP Request 报文的源 IP 地址、源 MAC 地址、VLAN 及接口是否与绑定表中的匹配，如果找到匹配的表项，则 DHCP Request 报文被正常转发。否则，报文被丢弃。

说明：

IP 地址包括 IPv4 地址和 IPv6 地址，S5700 对 DHCP Request 报文的源 IPv4 地址和源 IPv6 地址都会进行检查。

对 DHCP Request 报文的检查规则如下：

1. 首先检查报文中是否携带 request-ip 字段，如果是则认为是第一次上线的 DHCP Request 广播报文，直接通过；如果否则认为是续租报文，根据绑定表进行检查；
2. 检查报文中的 CHADDR 是否命中绑定表，如果没有命中，则认为是第一次上线，直接通过；如果 CHADDR 命中绑定表，则继续检查报文中的 VLAN、IP、接口信息是否均和绑定表匹配，完全匹配通过，否则丢弃。

前置任务

在配置防止仿冒 DHCP 续租报文攻击之前，需要完成以下任务：

- 配置 DHCP Server。
- 配置 DHCP Relay。

数据准备

在配置防止仿冒 DHCP 续租报文攻击之前，需要准备以下数据。

序号	数据
1	使能报文检查的接口类型和接口编号

使能 DHCP Request 报文检查功能

为了防止非法用户不断发送 DHCP Request 报文冒充合法用户续租 IP 地址，可以通过检查 DHCP 续租报文是否匹配绑定表，来决定是否转发该报文。

背景信息

对 DHCP 用户，使能 DHCP Snooping 功能后会自动生成绑定表；对静态分配 IP 地址的用户，需要手工配置静态绑定表。

操作步骤

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。

   该接口应为用户侧接口。
3. 执行命令 **dhcp snooping check dhcp-request enable（接口视图）**，配置接口下的 DHCP Request 报文检查功能。

   缺省情况下，接口下没有使能 DHCP Request 报文检查功能。

> **说明：**
>
> **dhcp snooping check dhcp-request enable（接口视图）**命令还可以检查 Release 报文是否匹配绑定表，以防止非法用户冒充合法用户释放 IP 地址。

配置 DHCP Snooping 用户数限制

防止攻击者通过不断申请 IP 地址造成合法用户无法上线。

应用环境

为了抑制用户恶意申请 IP 地址，可配置限制用户数的功能。

当用户数达到配置的最大用户数限制数量，任何用户将无法成功申请到 IP 地址。

前置任务

在配置用户数限制之前，需要完成以下任务：

- 全局使能 DHCP Snoopin 功能。
- 配置检查 DHCP Snooping 绑定表的功能。

数据准备

在配置用户数限制之前，需要准备以下数据。

序号	数据
1	接口类型和接口编号、VLAN 编号、限制的用户数数量

配置接入用户数限制

为了防止非法用户恶意申请 IP 地址，造成合法用户无法接入，可以配置接入用户数限制。

操作步骤

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **dhcp snooping max-user-number** *max-user-number*，配置全局允许接入的最大用户总数。

   缺省情况下，S5700 所有接口允许接入的最大用户总数为 1024。

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 max-user-number** *max-user-number*，配置接口或 VLAN 下允许接入的最大用户数。

   缺省情况下，S5700 接口或 VLAN 下允许接入的最大用户数为 1024。

   如果同时在接口、VLAN 或全局配置了允许接入用户的最大数，它们共同生效。

（可选）配置接口下 MAC 安全功能

对于 DHCP 用户，用户上线后生成动态绑定表可转化为静态 MAC，报文可以被正常转发。对于静态用户，静态绑定表无法转化为静态 MAC，必须配置静态 MAC，报文才能正常转发。

操作步骤

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。

   该接口为用户侧接口。
3. 执行命令 **dhcp snooping sticky-mac**，配置接口下 DHCP Snooping 功能的 MAC 安全。

   缺省情况下，S5700 未使能 DHCP Snooping 功能的 MAC 安全。

   本命令生效的前提是全局使能 DHCP Snooping 功能。

   执行本命令后，接口接收到的 IP 报文首先被上送到主控板 CPU，在主控板 CPU 生成动态绑定表。生成动态绑定表后，在对应接口上下发静态 MAC，即将动态 MAC 转换成静态 MAC。静态 MAC 表项中包含用户的 MAC、VLAN 信息。后续只有源 MAC 与静态 MAC 匹配的报文才可以通过接口，否则报文会被丢弃。

   对于静态用户，静态绑定表不会下发静态 MAC，必须为静态用户配置静态 MAC。

配置限制 DHCP 报文上送速率

防止攻击者发送大量的 DHCP Request 报文攻击 S5700。

应用环境

如果网络中有攻击者不断地发送 DHCP 报文，会对 S5700 的 DHCP 协议栈造成影响。

为了避免受到攻击者发送大量 DHCP 报文攻击，可以在 S5700 上配置 DHCP Snooping 功能，检查 DHCP 报文，并限制报文的上送速率，在一定的时间内只允许规定数目的报文上送协议栈，多余的报文将被丢弃。

前置任务

在配置限制报文上送速率之前，需要完成以下任务：

- 配置 DHCP Server。

- 配置 DHCP Relay。

数据准备

在配置限制报文上送速率之前，需要准备以下数据。

序号	数据
1	DHCP 报文的上送速率限值

配置限制 DHCP 报文上送速率

用户可以在全局、VLAN 或接口下配置限制 DHCP 报文上送速率，如果在全局、VLAN 或接口下同时配置，有效的顺序为接口优先，VLAN 其次，最后为全局。

操作步骤

- 系统视图下配置限制 DHCP 报文上送速率

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **dhcp snooping check dhcp-rate enable**，全局使能 DHCP 报文的速率检查功能。

   缺省情况下，全局没有使能 DHCP 报文速率检查功能。

3. 执行命令 **dhcp snooping check dhcp-rate** *rate*，全局配置 DHCP 报文的上送速率。

   缺省情况下，上送的 DHCP 报文速率限制在 100pps 以内。超过此速率限制的 DHCP 报文会被丢弃。

4. （可选）执行命令 **dhcp snooping alarm dhcp-rate enable**，全局使能 DHCP 报文的速率检查告警功能。

   缺省情况下，不对 DHCP 报文上送到 DHCP 协议栈的速率检查产生告警。

5. （可选）执行命令 **dhcp snooping alarm dhcp-rate threshold** *threshold*，全局配置 DHCP 报文的速率检查告警阈值。

   缺省情况下，DHCP 报文速率检查告警阈值为 100。当 DHCP 报文超过速率限制被丢弃的数目超过此阈值时，发出告警信息。

- VLAN 视图下配置限制 DHCP 报文上送速率

  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 **dhcp snooping check dhcp-rate enable**，在 VLAN 视图下使能 DHCP 报文的速率检查功能。

     缺省情况下，VLAN 视图下没有使能 DHCP 报文速率检查功能。
  4. 执行命令 **dhcp snooping check dhcp-rate** *rate*，在 VLAN 视图下配置 DHCP 报文的上送速率。

     缺省情况下，上送的 DHCP 报文速率限制在 100pps 以内。超过此速率限制的 DHCP 报文会被丢弃。

- 接口视图下配置限制 DHCP 报文上送速率

  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 **dhcp snooping check dhcp-rate** { **enable** | **enable** *rate* | *rate* } [**alarm dhcp-rate** [**enable**] [**threshold** *threshold-value*]]，可以在接口下同时配置以下功能。
     - 使能 DHCP 报文上送到 DHCP 协议栈的速率检查功能。
     - 配置 DHCP 报文上送到 DHCP 协议栈的检查速率。
     - 使能 DHCP 报文上送到 DHCP 协议栈的速率检查告警功能。
     - 配置 DHCP 报文上送到 DHCP 协议栈的速率检查的告警阈值。

     缺省情况下，在接口下 DHCP 报文上送到 DHCP 协议栈的速率检查功能未使能，检查速率为 100pps；DHCP 报文上送到 DHCP 协议栈的速率检查告警功能未使能，告警阈值为 100。

配置丢弃报文告警功能

丢弃的报文数超过指定阈值时发出告警。

应用环境

配置 DHCP Snooping 功能后，S5700 将丢弃攻击者发送的报文，其中攻击类型和丢弃报文种类的对应关系如表 1 所示：

表 1 攻击类型和丢弃报文种类的对应关系	
攻击类型	**丢弃报文类型**
仿冒者攻击	Untrusted 接口收到的 DHCP Reply 报文
改变 CHADDR 值攻击	CHADDR 字段与源 MAC 地址不一致的 DHCP Request 报文
仿冒 DHCP 续租报文攻击	与绑定表不匹配的 DHCP Request 报文
发送大量 DHCP Request 报文	超出速率限制的报文

使能丢弃报文告警功能后，S5700 丢弃报文的数量达到告警阈值后会产生告警信息。

前置任务

在配置报文相关告警功能之前，需要完成以下任务：

- 配置 DHCP Server。
- 配置 DHCP Relay。
- 配置丢弃用户侧 Untrusted 接口的 DHCP Reply 报文。
- 配置 DHCP Request 报文检查功能。
- 配置检查 DHCP Request 报文中的 CHADDR 字段功能。
- 配置检查 DHCP 报文的上送速率。

数据准备

在配置报文相关告警功能之前，需要准备以下数据。

序号	数据
1	丢弃报文后产生告警的阈值

配置丢弃报文告警

使能告警功能后如果有对应的攻击，并且丢弃的攻击报文超过阈值，会有相应的告警信息出现。

背景信息

丢弃报文告警可以在全局和接口下配置。

- 全局的配置对所有接口都有效。
- 接口的配置只在指定接口下有效。如果接口下没有配置，则继承全局的配置值。

操作步骤

- 配置全局丢弃报文告警

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dhcp snooping alarm threshold** *threshold*，配置全局丢弃报文的告警阈值。

     缺省情况下，全局丢弃报文数量的告警阈值为 100。

- 配置接口丢弃报文告警

  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 **dhcp snooping check dhcp-chaddr enable** ，使能根据 DHCP Request 报文里的 CHADDR 字段检查 DHCP Request 报文的功能和丢弃 DHCP Request 报文的告警功能，配置接口下丢弃 DHCP Request 报文的告警阈值。

     缺省情况下，根据 DHCP Request 报文里的 CHADDR 字段检查 DHCP Request 报文的功能和 DHCP Request 报文丢弃告警功能均未使能。丢弃 DHCP Request 报文告警的阈值为 100。

  4. 执行命令 **dhcp snooping check dhcp-request enable**，使能检查 DHCP Request 报文功能和丢弃 DHCP Request 报文告警功能，配置接口下丢弃 DHCP Request 报文的告警阈值。

     缺省情况下，DHCP Request 报文检查功能和 DHCP Request 报文丢弃告警功能均未使能。丢弃 DHCP Request 报文告警的阈值为 100。

  5. （可选）执行命令 **dhcp snooping alarm** { **dhcp-chaddr** | **dhcp-reply** | **dhcp-request** } { **enable** [**check** { **dhcp-giaddr** | **dhcp-chaddr** | **dhcp-request** } **enable** | **threshold** *threshold*] }，使能从非信任接口接收到 DHCP 报文的丢弃告警功能。

     缺省情况下，从非信任接口丢弃 DHCP 报文的告警功能未使能，丢弃 DHCP 报文告警阈值为 100。

     配置该命令后，S5700 会丢弃以下类型的报文：

     - 与 DHCP Snooping 绑定表不匹配的 DHCP Request 报文

- Untrusted 接口接收到的 DHCP Reply 报文。
- 源 MAC 地址与 CHADDR 字段不匹配的 DHCP Request 报文。

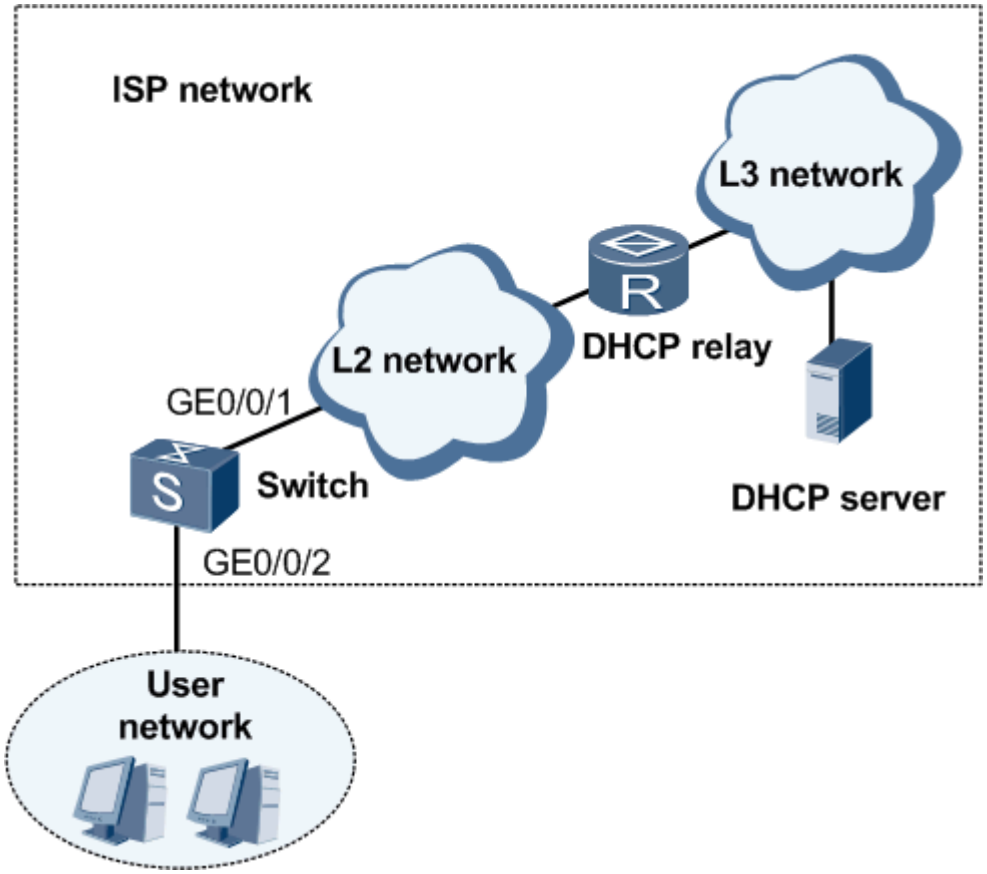
配置防止 DHCP Server 仿冒者攻击示例

介绍防止 DHCP Server 仿冒者攻击的基本配置过程，包括配置信任接口、配置 DHCP Reply 报文丢弃告警功能。

组网需求

如图 1 所示，Switch 应用在用户网络和 ISP 的二层网络之间，为防止 DHCP Server 仿冒者攻击，要求在 Switch 上应用 DHCP Snooping 功能，把用户侧的接口配置为 Untrusted 模式，把运营商网络侧的接口配置为 Trusted 模式。同时配置 DHCP Reply 报文丢弃告警功能。

图 1 配置防止 DHCP Server 仿冒者攻击组网图



配置思路

采用如下的思路配置 DHCP Server 仿冒者攻击（假设 DHCP Server 已经配置完成）：

1. 使能全局和接口下的 DHCP Snooping 功能。
2. 使能伪 DHCP Server 探测功能。
3. 把连接 DHCP Server 的接口设置为“信任（Trusted）”。
4. 配置 DHCP Reply 报文丢弃告警功能。

数据准备

为完成此配置举例，需要准备如下数据：

- 接口的 Trusted/Untrusted 模式：GE0/0/1 接口 Trusted 模式，GE0/0/2 接口 Untrusted 模式。
- 发出告警的阈值：120。

说明：

以下配置步骤中，只列出了和 DHCP Snooping 配置相关的命令。

操作步骤

1. 配置 DHCP Snooping 功能

   # 使能全局 DHCP Snooping 功能。

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] dhcp snooping enable
```

   # 使能伪 DHCP Server 探测功能。

```
[Quidway] dhcp server detect
```

   # 使能用户侧接口的 DHCP Snooping 功能。

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] dhcp snooping enable
[Quidway-GigabitEthernet0/0/2] quit
```

2. 配置接口的 Trusted/Untrusted 模式

配置 DHCP Server 侧的接口为 Trusted 模式。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] dhcp snooping enable
[Quidway-GigabitEthernet0/0/1] dhcp snooping trusted
[Quidway-GigabitEthernet0/0/1] quit
```

配置用户侧的接口为 Untrusted 模式。

GE0/0/2 接口使能了 DHCP Snooping 功能后，接口模式默认为“Untrusted”

3. 配置 DHCP Reply 报文丢弃告警功能

使能对不信任端口收到的 DHCP Reply 报文丢弃告警功能，并配置告警阈值。

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] dhcp snooping alarm dhcp-reply enable
[Quidway-GigabitEthernet0/0/2]  dhcp snooping alarm dhcp-reply threshold 120
[Quidway-GigabitEthernet0/0/2] quit
```

4. 验证配置结果

在 Switch 上执行 **display dhcp snooping configuration** 命令可以看到全局和接口视图下已经使能 DHCP Snooping 功能。

```
<Quidway> display dhcp snooping configuration
 dhcp snooping enable
 dhcp server detect
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
 dhcp snooping trusted
#
interface GigabitEthernet0/0/2
 dhcp snooping enable
```

```
 dhcp snooping alarm dhcp-reply enable
#
```

配置文件

```
#
 dhcp enable
 dhcp snooping enable
 dhcp server detect
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
 dhcp snooping trusted
#
interface GigabitEthernet0/0/2
 dhcp snooping enable
 dhcp snooping alarm dhcp-reply enable
 dhcp snooping alarm dhcp-reply threshold 120
#
return
```

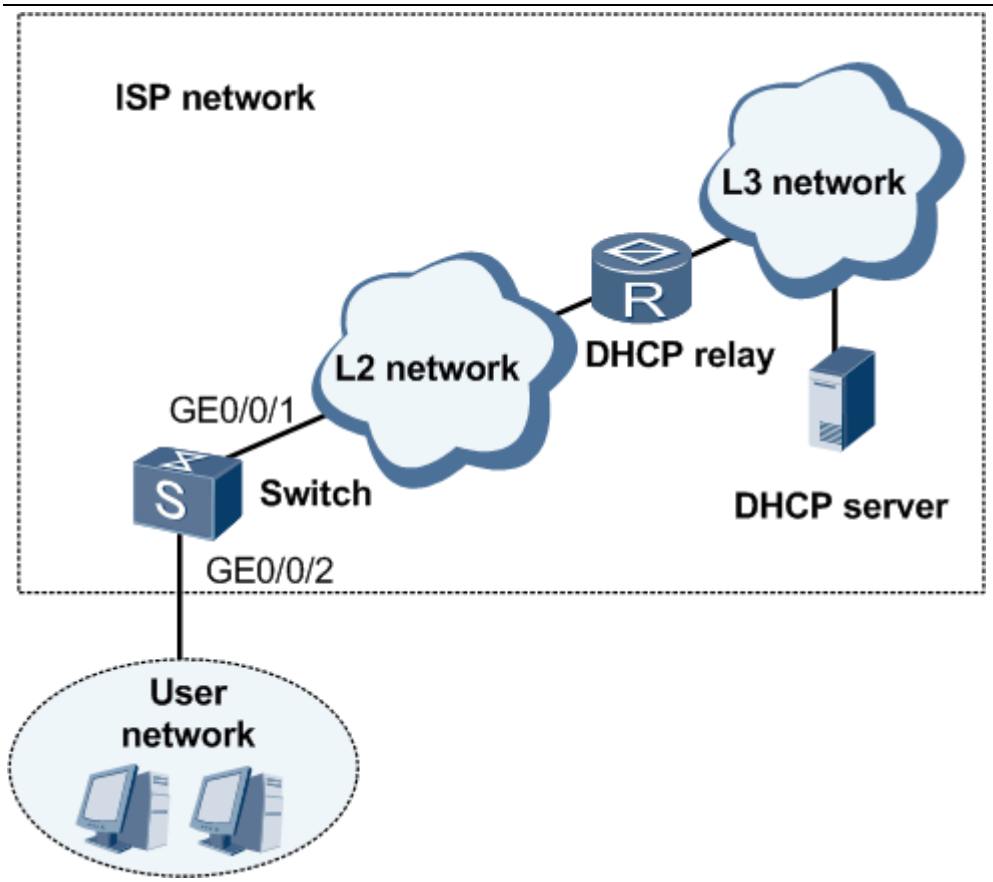
配置防止改变 CHADDR 值的 DoS 攻击示例

介绍防止改变 CHADDR 值的 DoS 攻击的基本配置过程，包括配置用户侧接口的 CHADDR 检查功能和告警功能。

组网需求

如图 1 所示，Switch 应用在用户网络和 ISP 的二层网络之间，为防止攻击者通过改变 CHADDR 值进行 DoS 攻击，要求在 Switch 上应用 DHCP Snooping 功能。检查 DHCP Request 报文中 CHADDR 字段，如果该字段跟数据帧头部的源 MAC 相匹配，便转发报文；否则丢弃报文。同时使能丢弃报文告警功能。

图 1 配置防止改变 CHADDR 值的 DoS 攻击组网图



配置思路

采用如下的思路配置防止攻击者通过改变 CHADDR 值攻击：

1. 使能全局和接口下的 DHCP Snooping 功能。
2. 把连接 DHCP Server 的接口设置为“信任（Trusted）”。
3. 在用户侧接口配置 CHADDR 值检查。
4. 配置告警功能。

数据准备

为完成此配置举例，需要准备如下数据：

- 发出告警的阈值

说明：

以下配置步骤中，只列出了和 DHCP Snooping 配置相关的命令。

操作步骤

1. 配置 DHCP Snooping 功能

   # 使能全局 DHCP Snooping 功能。

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] dhcp snooping enable
```

   # 使能用户侧接口的 DHCP Snooping 功能。

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] dhcp snooping enable
[Quidway-GigabitEthernet0/0/2] quit
```

2. 配置接口的 Trusted/Untrusted 模式

   # 配置 DHCP Server 侧的接口为 Trusted 模式。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] dhcp snooping enable
[Quidway-GigabitEthernet0/0/1] dhcp snooping trusted
[Quidway-GigabitEthernet0/0/1] quit
```

   # 配置用户侧的接口为 Untrusted 模式。

   GE0/0/2 接口使能了 DHCP Snooping 功能后，接口模式默认为“Untrusted”

3. 配置用户侧接口的 CHADDR 检查功能。

4. [Quidway] interface gigabitethernet 0/0/2

```
[Quidway-GigabitEthernet0/0/2] dhcp snooping check dhcp-chaddr enable
```

5. 验证配置结果

   在 Switch 上执行 **display dhcp snooping configuration** 命令可以看到全局和接口视图下已经使能 DHCP Snooping 功能。

```
<Quidway> display dhcp snooping configuration
  dhcp snooping enable
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
 dhcp snooping trusted
#
interface GigabitEthernet0/0/2
 dhcp snooping enable
 dhcp snooping check dhcp-chaddr enable
#
```

配置文件

```
#
 dhcp enable
 dhcp snooping enable
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
 dhcp snooping trusted
#
interface GigabitEthernet0/0/2
 dhcp snooping enable
 dhcp snooping check dhcp-chaddr enable
#
return
```

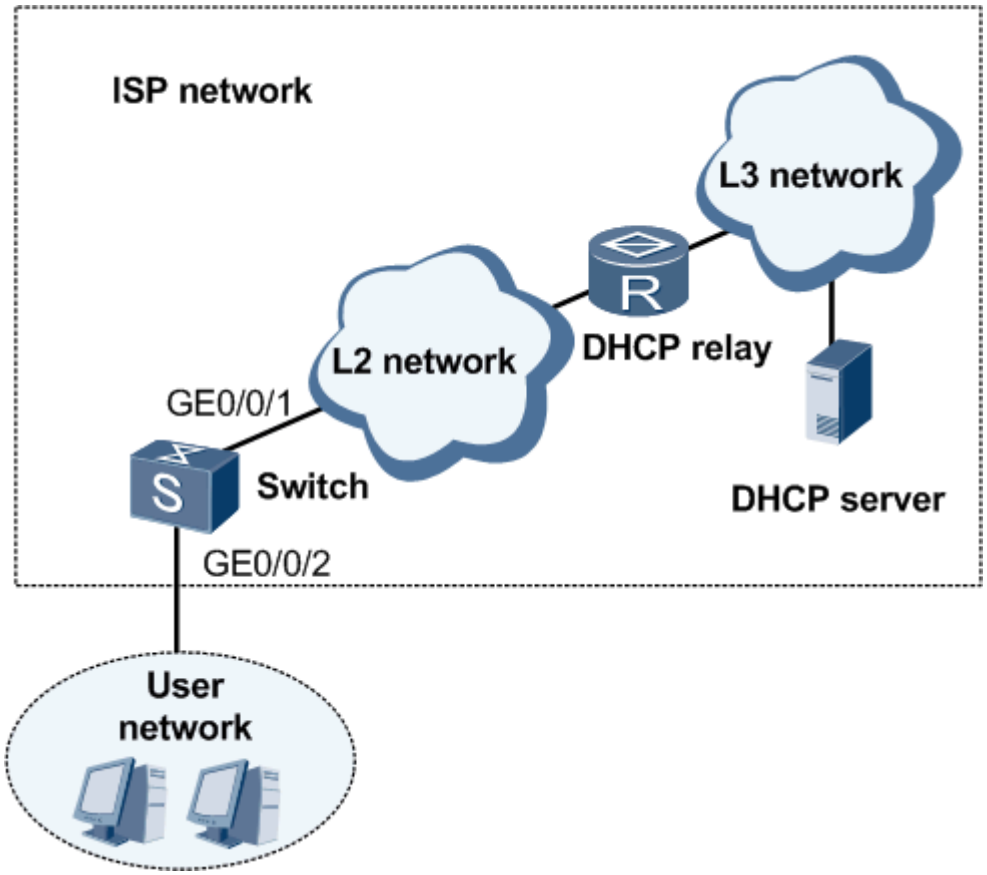
配置防止仿冒 DHCP 续租报文攻击示例

介绍防止仿冒 DHCP 续租报文攻击的基本配置过程，包括配置用户侧接口的 DHCP Request 报文检查功能和告警功能。

组网需求

如图 1 所示，Switch 应用在用户网络和 ISP 的二层网络之间。为防止攻击者仿冒 DHCP 续租报文，要求在 Switch 上应用 DHCP Snooping 功能，建立 DHCP Snooping 绑定表，检查接收到的 DHCP Request 报文，只有和绑定表中的内容一致的报文才被转发，否则将被丢弃。同时使能丢弃报文告警功能。

图 1 配置防止仿冒 DHCP 续租攻击组网图



配置思路

采用如下的思路配置防止攻击者仿冒 DHCP 续租报文攻击的示例：

1. 在全局视图和接口视图下使能 DHCP Snooping。
2. 把连接 DHCP Server 的接口设置为“信任（Trusted）”。
3. 使用 DHCP Snooping 绑定表工作模式，对 DHCP Request 报文进行匹配绑定检查。
4. 配置丢弃报文告警功能。

数据准备

为完成此配置举例，需要准备如下数据：

- 各接口所属的 VLAN。
- 允许转发的静态 IP 地址。
- 发出告警的阈值。

说明：

以下配置步骤中，只列出了和 DHCP Snooping 配置相关的命令。

操作步骤

1. 配置 DHCP Snooping 功能

   # 使能全局 DHCP Snooping 功能。

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] dhcp snooping enable
```

   # 使能用户侧接口的 DHCP Snooping 功能。

```
[Quidway] interface gigabitethernet 0/0/2
[Quidway-GigabitEthernet0/0/2] dhcp snooping enable
[Quidway-GigabitEthernet0/0/2] quit
```

2. 配置接口的 Trusted/Untrusted 模式

   # 配置 DHCP Server 侧的接口为 Trusted 模式。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] dhcp snooping enable
[Quidway-GigabitEthernet0/0/1] dhcp snooping trusted
[Quidway-GigabitEthernet0/0/1] quit
```

   # 配置用户侧的接口为 Untrusted 模式。

   GE0/0/2 接口使能了 DHCP Snooping 功能后，接口模式默认为“Untrusted”

3. 配置报文检查功能。

```
4. [Quidway] interface gigabitethernet 0/0/2
5. [Quidway-GigabitEthernet0/0/2] dhcp snooping alarm dhcp-request enable
   [Quidway-GigabitEthernet0/0/2] quit
```

6. 查看动态绑定表

执行 **display dhcp snooping user-bind all** 命令可以看到所有 DHCP snooping 用户绑定表项。

```
<Quidway> display dhcp snooping user-bind all
DHCP Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - map vlan
IP Address       MAC Address     VSI/VLAN(O/I/P) Interface      Lease
--------------------------------------------------------------------------------
10.1.1.3         0000-005e-008a   3 /--  /--      GE0/0/2        2010.08.14-12:58
--------------------------------------------------------------------------------
print count:           1         total count:           1
```

7. 验证配置结果

在 Switch 上执行 **display dhcp snooping configuration** 命令可以看到全局和接口视图下已经使能 DHCP Snooping 功能。

```
<Quidway> display dhcp snooping configuration
 dhcp snooping enable
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
 dhcp snooping trusted
#
interface GigabitEthernet0/0/2
 dhcp snooping enable
 dhcp snooping alarm dhcp-request enable
#
```

配置文件

```
#
 dhcp enable
 dhcp snooping enable
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
 dhcp snooping trusted
#
interface GigabitEthernet0/0/2
 dhcp snooping enable
 dhcp snooping alarm dhcp-request enable
#
return
```

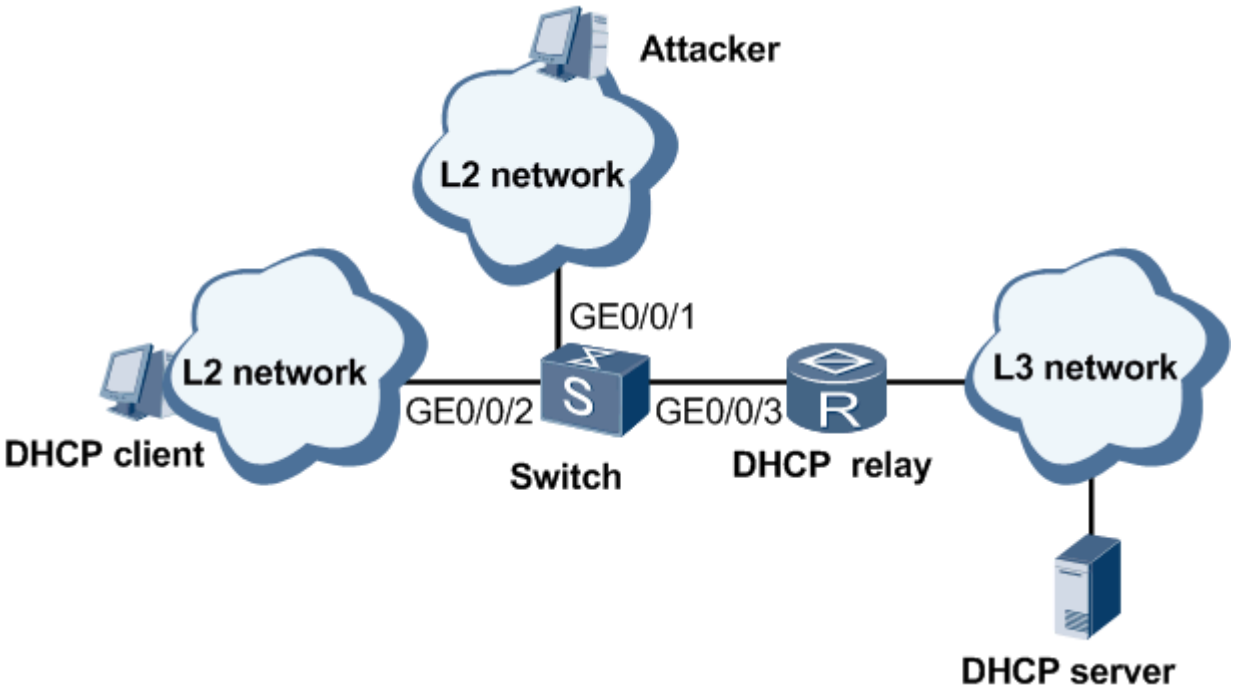
配置限制 DHCP 报文上送速率示例

介绍限制 DHCP 报文上送速率的基本配置过程，包括配置 DHCP 报文上送协议栈的速率和配置报文限速告警功能。

组网需求

当网络中存在攻击者通过大量发送 DHCP Request 或 Reply 报文进行攻击时，会造成 Switch 处理资源紧张，合法用户的请求得不到及时处理。如图 1 所示，为了防止大量发送 DHCP 报文的攻击，需要在 Switch 上配置 DHCP Snooping 功能，控制 DHCP 报文的上送速率，同时使能报文限速告警功能。

图 1 配置限制 DHCP 报文的上送速率组网图



配置思路

采用如下的思路配置防止攻击者发送大量 DHCP 报文攻击的示例：

1. 在全局视图和接口视图下使能 DHCP Snooping。
2. 把连接 DHCP Server 的接口设置为“信任（Trusted）”。
3. 在接口下配置 DHCP 报文上送协议栈的速率。
4. 在接口下配置报文限速告警功能。

数据准备

为完成此配置举例，需要准备如下数据：

- DHCP 报文的上送速率
- 发出告警的阈值

说明：

以下配置步骤中，只列出了和 DHCP Snooping 配置相关的命令。

操作步骤

1. 配置 DHCP Snooping 功能

使能全局 DHCP Snooping 功能。

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] dhcp snooping enable
```

使能用户侧接口的 DHCP Snooping 功能。GE0/0/2、GE0/0/3 和 GE0/0/1 的配置步骤一样，此处省略。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] dhcp snooping enable
```

2. 配置接口的 Trusted/Untrusted 模式

配置 DHCP Server 侧的接口为 Trusted 模式。

```
[Quidway] interface gigabitethernet 0/0/3
[Quidway-GigabitEthernet0/0/3] dhcp snooping enable
[Quidway-GigabitEthernet0/0/3] dhcp snooping trusted
[Quidway-GigabitEthernet0/0/3] quit
```

配置用户侧的接口为 Untrusted 模式。

GE0/0/1 接口和 GE0/0/2 接口使能了 DHCP Snooping 功能后，接口模式默认为“Untrusted”

3. 配置 DHCP 报文上送速率限制以及报文限速告警功能。

配置接口下 DHCP 报文上送速率限制以及报文限速告警功能。GE0/0/2、GE0/0/3 和 GE0/0/1 的配置步骤一样，此处省略。

```
[Quidway-GigabitEthernet0/0/1] dhcp snooping check dhcp-rate enable 50 alarm dhcp-rate enable threshold 50
[Quidway-GigabitEthernet0/0/1] quit
```

4. 验证配置结果

在 Switch 上执行 **display dhcp snooping configuration** 命令，可以看到全局和接口视图下已经使能 DHCP Snooping 功能。

```
[Quidway] display dhcp snooping configuration
#
 dhcp snooping enable
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
 dhcp snooping check dhcp-rate enable
 dhcp snooping check dhcp-rate 50
 dhcp snooping alarm dhcp-rate enable
 dhcp snooping alarm dhcp-rate threshold 50
#
interface GigabitEthernet0/0/2
 dhcp snooping enable
 dhcp snooping check dhcp-rate enable
 dhcp snooping check dhcp-rate 50
 dhcp snooping alarm dhcp-rate enable
 dhcp snooping alarm dhcp-rate threshold 50
#
interface GigabitEthernet0/0/3
 dhcp snooping enable
 dhcp snooping trusted
 dhcp snooping check dhcp-rate enable
 dhcp snooping check dhcp-rate 50
 dhcp snooping alarm dhcp-rate enable
 dhcp snooping alarm dhcp-rate threshold 50
#
```

在 Switch 上执行 **display dhcp snooping interface** 命令，可以看到接口视图下 DHCP Snooping 的配置信息。

```
[Quidway] display dhcp snooping interface GigabitEthernet0/0/3
 DHCP snooping running information for interface GigabitEthernet0/0/3 :
```

```
DHCP snooping                             : Enable
Trusted interface                         : Yes
Dhcp user max number                      : 1024     (default)
Current dhcp user number                  : 0
Check dhcp-giaddr                         : Disable  (default)
Check dhcp-chaddr                         : Disable  (default)
Alarm dhcp-chaddr                         : Disable  (default)
Check dhcp-request                        : Disable  (default)
Alarm dhcp-request                        : Disable  (default)
Check dhcp-rate                           : Enable
Dhcp-rate limit(pps)                      : 50
Alarm dhcp-rate                           : Enable
Alarm dhcp-rate threshold                 : 50
Discarded dhcp packets for rate limit     : 0
Alarm dhcp-reply                          : Disable  (default)
[Quidway] 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                      : 1024     (default)
Current dhcp user number                  : 0
Check dhcp-giaddr                         : Disable  (default)
Check dhcp-chaddr                         : Disable  (default)
Alarm dhcp-chaddr                         : Disable  (default)
Check dhcp-request                        : Disable  (default)
Alarm dhcp-request                        : Disable  (default)
Check dhcp-rate                           : Enable
Dhcp-rate limit(pps)                      : 50
Alarm dhcp-rate                           : Enable
Alarm dhcp-rate threshold                 : 50
Discarded dhcp packets for rate limit     : 0
```

```
Alarm dhcp-reply                          : Disable  (default)
[Quidway] display dhcp snooping interface GigabitEthernet 0/0/2
DHCP snooping                             : Enable
Trusted interface                         : No
Dhcp user max number                      : 1024     (default)
Current dhcp user number                  : 0
Check dhcp-giaddr                         : Disable  (default)
Check dhcp-chaddr                         : Enable
Alarm dhcp-chaddr                         : Disable  (default)
Check dhcp-request                        : Enable
Alarm dhcp-request                        : Disable  (default)
Check dhcp-rate                           : Enable
Dhcp-rate limit(pps)                      : 50
Alarm dhcp-rate                           : Enable
Alarm dhcp-rate threshold                 : 50
Discarded dhcp packets for rate limit     : 0
Alarm dhcp-reply                          : Enable
Alarm dhcp-reply threshold                : 100
Discarded dhcp packets for check reply    : 0
```

配置文件

```
#
 dhcp enable
 dhcp snooping enable
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
 dhcp snooping check dhcp-rate enable
 dhcp snooping check dhcp-rate 50
 dhcp snooping alarm dhcp-rate enable
 dhcp snooping alarm dhcp-rate threshold 50
```

```
#
interface GigabitEthernet0/0/2
 dhcp snooping enable
 dhcp snooping check dhcp-rate enable
 dhcp snooping check dhcp-rate 50
 dhcp snooping alarm dhcp-rate enable
 dhcp snooping alarm dhcp-rate threshold 50
#
interface GigabitEthernet0/0/3
 dhcp snooping enable
 dhcp snooping trusted
dhcp snooping check dhcp-rate enable
 dhcp snooping check dhcp-rate 50
 dhcp snooping alarm dhcp-rate enable
 dhcp snooping alarm dhcp-rate threshold 50
#
return
```

配置在二层网络中应用 DHCP Snooping 示例

介绍二层网络中应用 DHCP Snooping 的基本配置过程，包括配置信任接口、配置对 DHCP 报文的检查功能、配置 DHCP 报文上送速率限制和配置 Option82 功能等。

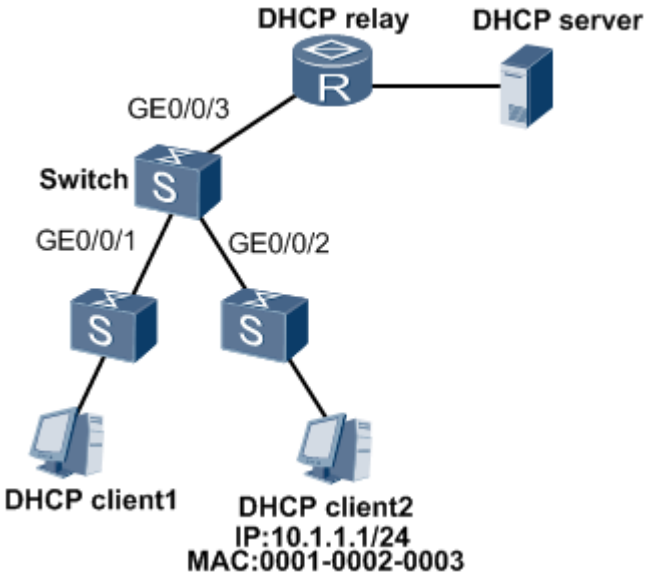
组网需求

如图 1 所示，DHCP Client 通过 VLAN10 接入 Switch。其中 DHCP Client1 使用动态分配的 IP 地址；DHCP Client2 使用静态分配的 IP 地址。要求在 Switch 的用户侧接口 GE0/0/1 和 GE0/0/2 上配置 DHCP Snooping 功能，以防止以下类型的攻击：

- DHCP Server 仿冒者攻击
- 改变 CHADDR 值的 DoS 攻击
- 仿冒 DHCP 续租报文攻击

- 大量发送 DHCP 请求报文

图 1 配置在二层网络中应用 DHCP Snooping 功能组网图



配置思路

采用如下的思路配置 DHCP Snooping 的基本功能：

1. 在全局视图和接口视图下使能 DHCP Snooping。
2. 配置 Trusted/Untrusted 接口，防止 DHCP Server 仿冒者攻击。
3. 配置 DHCP Snooping 绑定表，对 DHCP 请求报文进行匹配绑定检查，防止仿冒 DHCP 续租报文攻击。
4. 配置 CHADDR 值检查，防止改变 CHADDR 值的 DoS 攻击。
5. 配置 DHCP 报文上送协议栈的速率，防止 DHCP Reply 报文攻击。
6. 配置 Option82 功能。
7. 配置丢弃报文告警。

数据准备

为完成此配置举例，需要准备如下数据：

- 接口所属的 VLAN：VLAN 10。
- 接口的 Trusted/Untrusted 模式：GE0/0/2 为 Untrusted 模式，GE0/0/3 为 Trusted 模式。
- 允许转发的静态 IP 地址：10.1.1.1/24，对应的 MAC 地址：0001-0002-0003。

- DHCP 报文上送协议栈的速率：90。
- Option82 功能的模式：**insert**。
- 丢弃报文告警阈值：120。

说明：

以下配置步骤中，只列出了和 DHCP Snooping 配置相关的命令。

操作步骤

1. 使能 DHCP Snooping 功能

   # 使能全局 DHCP Snooping 功能。

```
<Quidway> system-view
[Quidway] dhcp enable
[Quidway] dhcp snooping enable
```

   # 使能用户侧接口的 DHCP Snooping 功能。以 GE0/0/1 接口为例，GE0/0/2 的配置相同，此处省略。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] dhcp snooping enable
[Quidway-GigabitEthernet0/0/1] quit
```

2. 配置 Trusted 接口

   # 将连接 DHCP Server 侧的接口配置为“Trusted”，将连接 DHCP Clinet 侧的所有接口使能 DHCP Snooping（如果用户侧接口没有配置“Trusted”模式，那么使能了接口的 Snooping 特性后，接口模式默认为“Untrusted”），这样可以防止 DHCP Server 仿冒者攻击。

```
[Quidway] interface gigabitethernet 0/0/3
[Quidway-GigabitEthernet0/0/3] dhcp snooping enable
[Quidway-GigabitEthernet0/0/3] dhcp snooping trusted
[Quidway-GigabitEthernet0/0/3] quit
```

3. 配置对 DHCP 报文的检查，并配置告警功能。

在 DHCP Clinet 侧的接口配置进行 DHCP Request 报文检查和告警功能，这样可以防止仿冒 DHCP 续租报文的攻击。以 GE0/0/1 接口为例，GE0/0/2 的配置相同，此处省略。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] dhcp snooping check dhcp-request enable
```

在 DHCP Clinet 侧的接口配置进行 CHADDR 检查和告警功能，这样可以防止改变 CHADDR 值的 DoS 攻击。以 GE0/0/1 接口为例，GE0/0/2 的配置相同，此处省略。

```
[Quidway-GigabitEthernet0/0/1] dhcp snooping check dhcp-chaddr enable
[Quidway-GigabitEthernet0/0/1] quit
```

4. 确认 DHCP 动态绑定表信息

执行 **display dhcp snooping user-bind all** 命令，查看 DHCP 动态绑定表信息。

```
<Quidway> display dhcp snooping user-bind all
DHCP Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - map vlan
IP Address       MAC Address     VSI/VLAN(O/I/P) Interface      Lease
--------------------------------------------------------------------------------
10.1.1.1         0001-0002-0003   10 /--  /--     GE0/0/2        2010.08.14-12:58
--------------------------------------------------------------------------------
print count:           1         total count:           1
```

5. 配置 DHCP 报文上送速率限制

配置 DHCP 上送速率检查，这样可以防止 DHCP Request 报文攻击。

```
[Quidway] dhcp snooping check dhcp-rate enable
[Quidway] dhcp snooping check dhcp-rate 90
```

6. 配置 Option82 功能

在 DHCP Client 侧接口配置 Option82 功能。以 GE0/0/1 接口为例，GE0/0/2 的配置相同，此处省略。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] dhcp option82 insert enable
```

```
[Quidway-GigabitEthernet0/0/1] quit
```

7. 配置告警功能

配置 DHCP Reply 报文丢弃告警功能。以 GE0/0/1 接口为例，GE0/0/2 的配置相同，此处省略。

```
[Quidway] interface gigabitethernet 0/0/1
[Quidway-GigabitEthernet0/0/1] dhcp snooping alarm dhcp-reply enable
[Quidway-GigabitEthernet0/0/1] quit
```

8. 验证配置结果

在 Switch 上执行 **display dhcp snooping configuration** 命令可以看到全局已经使能 DHCP Snooping 功能，并查看告警的统计信息。

```
[Quidway] display dhcp snooping configuration
#
 dhcp snooping enable
 dhcp snooping check dhcp-rate enable
 dhcp snooping check dhcp-rate 90
#
 user-bind static ip-address 10.1.1.1 mac-address 0001-0002-0003 interface
GigabitEthernet 0/0/2 vlan 10
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
 dhcp snooping alarm dhcp-reply enable threshold 120
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping check dhcp-request enable
#
interface GigabitEthernet0/0/2
 dhcp snooping enable
 dhcp snooping alarm dhcp-reply enable threshold 120
 dhcp snooping check dhcp-chaddr enable
```

```
 dhcp snooping check dhcp-request enable
#
interface GigabitEthernet0/0/3
 dhcp snooping enable
 dhcp snooping trusted
#
```

执行 **display dhcp snooping interface** 命令可以看到接口下的 DHCP Snooping 信息。

```
[Quidway] display dhcp snooping interface gigabitethernet 0/0/1
 DHCP snooping                          : Enable
 Trusted interface                      : No
 Dhcp user max number                   : 1024     (default)
 Current dhcp user number               : 0
 Check dhcp-giaddr                      : Disable  (default)
 Check dhcp-chaddr                      : Enable
 Alarm dhcp-chaddr                      : Disable  (default)
 Check dhcp-request                     : Enable
 Alarm dhcp-request                     : Disable  (default)
 Check dhcp-rate                        : Enable
 Dhcp-rate limit(pps)                   : 50
 Alarm dhcp-rate                        : Enable
 Alarm dhcp-rate threshold              : 50
 Discarded dhcp packets for rate limit  : 0
 Alarm dhcp-reply                       : Enable
 Alarm dhcp-reply threshold             : 120
 Discarded dhcp packets for check reply : 0
[Quidway] display dhcp snooping interface gigabitethernet 0/0/3
 DHCP snooping                          : Enable
 Trusted interface                      : Yes
 Dhcp user max number                   : 1024     (default)
 Current dhcp user number               : 0
```

```
Check dhcp-giaddr                          : Disable  (default)
Check dhcp-chaddr                          : Disable  (default)
Alarm dhcp-chaddr                          : Disable  (default)
Check dhcp-request                         : Disable  (default)
Alarm dhcp-request                         : Disable  (default)
Check dhcp-rate                            : Disable  (default)
Alarm dhcp-rate                            : Disable  (default)
Alarm dhcp-rate threshold                  : 50
Discarded dhcp packets for rate limit      : 0
Alarm dhcp-reply                           : Disable  (default)
```

执行 **display dhcp option82 configuration interface** 命令可以查看接口下 Option82 的配置。

```
[Quidway] display dhcp option82 configuration interface gigabitethernet 0/0/1
#
interface GigabitEthernet0/0/1
 dhcp option82 insert enable
#
```

配置文件

```
#
 dhcp enable
 dhcp snooping enable
 dhcp snooping check dhcp-rate enable
 dhcp snooping check dhcp-rate 90
#
 user-bind static ip-address 10.1.1.1 mac-address 0001-0002-0003 interface GigabitEthernet
0/0/2 vlan 10
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
 dhcp snooping alarm dhcp-reply enable threshold 120
 dhcp snooping check dhcp-chaddr enable
```

```
 dhcp snooping check dhcp-request enable
 dhcp option82 insert enable
#
interface GigabitEthernet0/0/2
 dhcp snooping enable
 dhcp snooping alarm dhcp-reply enable threshold 120
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping check dhcp-request enable
 dhcp option82 insert enable
#
interface GigabitEthernet0/0/3
 dhcp snooping enable
 dhcp snooping trusted
#
return
```

HCIE-Security 模拟面试问题及面试建议

1. DHCP Snooping 防范机制是什么？能够防范哪些攻击？