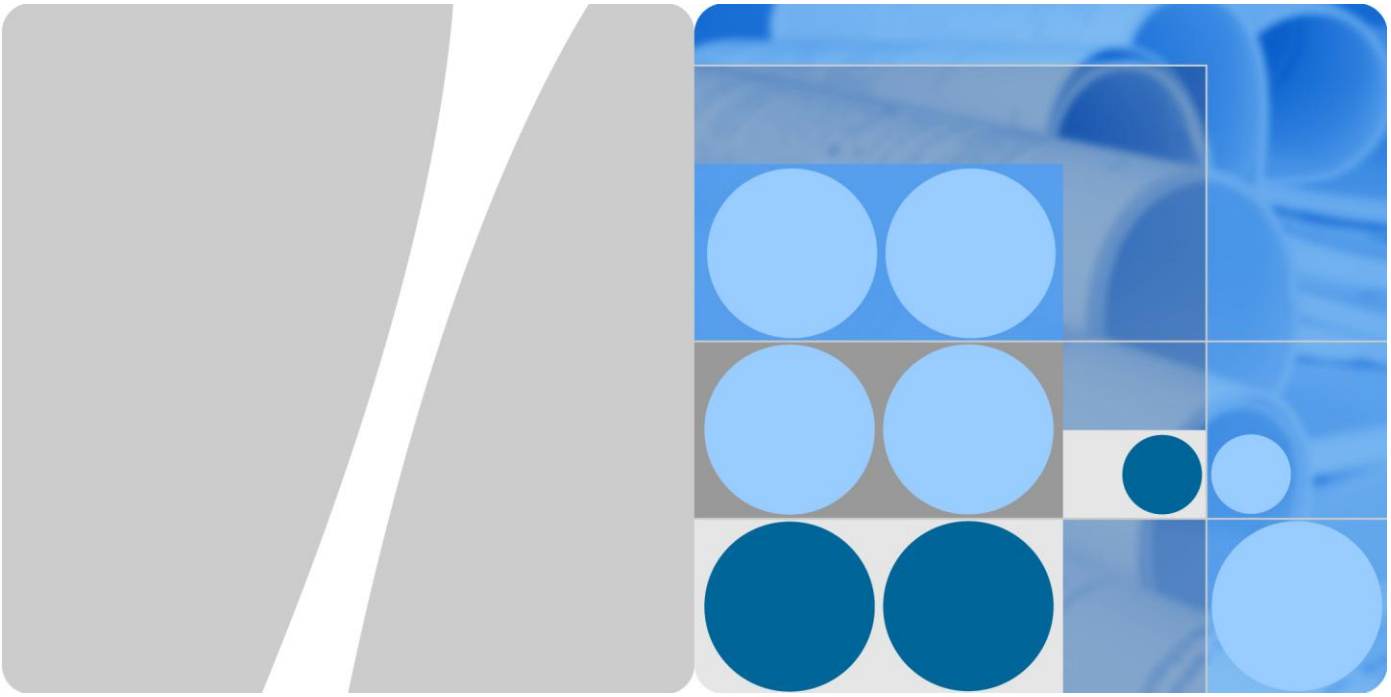


DHCP Snooping 技术白皮书

文档版本 01

发布日期 2012-09-10

华为技术有限公司

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默示的声明或保证。

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： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

1 DHCP Snooping

关于本章

1.1 介绍

定义

DHCP Snooping 是 DHCP 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、防止仿冒 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。

1.2 参考标准和协议

本特性的参考资料清单如下：

文档	描述	备注
RFC2132	DHCP Options and BOOTP Vendor Extensions	-
RFC3046	DHCP Relay Agent Information Option	-

1.3 原理描述

1.3.1 DHCP Snooping 基本功能

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 地址。

网络中如果存在私自架设的伪 DHCP 服务器，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伪造或非法 DHCP 服务器为其他主机分配 IP 地址及其他配置信息。

DHCP Snooping 信任功能允许将端口分为信任端口和非信任端口：

1. 配置 DHCP Snooping 信任端口：

```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] dhcp snooping enable
[Quidway-GigabitEthernet1/0/1] dhcp snooping trusted
```

DHCP Snooping 基本监听功能

DHCP Snooping 的基本监听功能，能够记录 DHCP 客户端 IP 地址与 MAC 地址等参数的对应关系。

开启 DHCP Snooping 功能后，设备能够通过监听 DHCP 请求报文和回应报文，生成 DHCP Snooping 绑定表，绑定表项包括客户端的 MAC 地址、获取到的 IP 地址、与 DHCP 客户端连接的端口及该端口所属的 VLAN 等信息。

DHCP Snooping 用户位置迁移功能

在绑定表生成后，此时若某一合法用户位置变动，则需要及时更新设备上其对应的绑定表项。使能 DHCP Snooping 用户位置迁移功能后，设备将在检查到用户位置变动时立刻更新其对应的 DHCP Snooping 动态绑定表项以保证表项的正确性。

2. 使能 DHCP Snooping 用户位置迁移功能

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

ARP 与 DHCP Snooping 的联动功能

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，若在规定的探测次数内探测不到用户，设备将会删除该用户对应的绑定表项。

说明

只有设备作为 DHCP Relay 时，才支持 ARP 与 DHCP Snooping 的联动功能

3. 使能 ARP 与 DHCP Snooping 的联动功能

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

用户下线后及时清除对应用户的 MAC 表项功能

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，则当用户下线对应的绑定表项被清除时，设备将会及时的移除用户的 MAC 表项。

4. 使能 DHCP Snooping 动态表项清除时移除对应用户的 MAC 表现功能

```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] dhcp snooping user-offline remove mac-address
```

丢弃 GIADDR 字段非零的 DHCP Request 报文功能

DHCP Request 报文中的 GIADDR（Gateway Ip Address）字段记录了 DHCP Request 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。

在通过 DHCP Snooping 的基本监听功能生成绑定表的过程中，为了保证设备能够获取到用户 MAC 等参数，DHCP Snooping 功能需应用于二层接入设备或第一个 DHCP Relay 上。故 DHCP Snooping 设备接收到的 DHCP Request 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。

5. 使能 VLAN 10 丢弃 GIADDR 字段非零的 DHCP Request 报文功能

```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] vlan 10
[Quidway-vlan10] dhcp snooping enable
[Quidway-vlan10] dhcp snooping check dhcp-giaddr enable
```

1.3.2 DHCP Snooping 的攻击防范功能

在配置完成 DHCP Snooping 的基本功能后，设备能够保证客户端从合法的服务器获取 IP 地址，这有效防止了网络中 DHCP Server 仿冒者攻击。但是在 DHCP 网络环境中，攻击者仍有多种攻击手段可对网络进行攻击。此时根据需要，管理员可配置 DHCP Snooping 的攻击防范功能。

DHCP Server 探测功能

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 地址与端口等信息，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。

6. 开启 DHCP Server 探测功能

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

防止非 DHCP 用户攻击功能

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。

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、连接的端口号等信息，设备可根据 MAC 表项对报文进行二层转发。

配置接口的静态 MAC 表项功能后，设备将根据该接口下所有 DHCP 用户对应的 DHCP Snooping 动态绑定表项自动执行命令生成这些用户的静态 MAC 表，并同时关闭该接口学习动态 MAC 表的能力。之后，则只有源 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。这样能够有效的防止非 DHCP 用户对网络的攻击。

7. 开启根据 DHCP Snooping 绑定表生成接口的静态 MAC 表项功能

```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] dhcp snooping enable
[Quidway-GigabitEthernet1/0/1] dhcp snooping sticky-mac
```

防止 DHCP 报文泛洪攻击

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。

8. 配置允许上送 DHCP 报文处理单元的 DHCP 报文速率最大值为 50pps

```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] dhcp snooping check dhcp-rate enable
[Quidway] dhcp snooping check dhcp-rate 50
```

防止仿冒 DHCP 报文攻击

在 DHCP 网络环境中，若攻击者仿冒合法用户的 DHCP Request 报文发往 DHCP Server，将会导致用户的 IP 地址租约到期之后不能够及时释放，以致合法用户无法使用该 IP 地址；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。

在生成 DHCP Snooping 绑定表后，设备可根据绑定表项，对 DHCP Request 报文或 DHCP 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 DHCP Request 或 DHCP Release 报文冒充合法用户续租或释放 IP 地址。

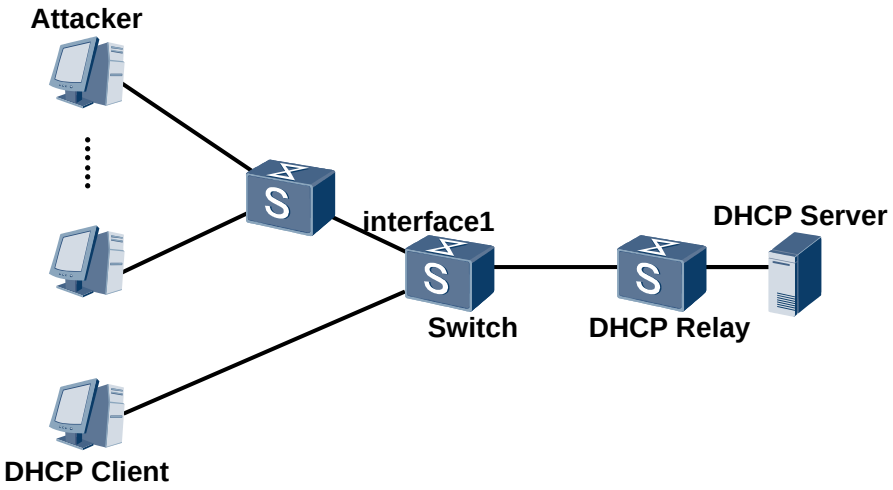
9. 使能 VLAN 10 的 DHCP 报文绑定表匹配检查功能

```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] vlan 10
[Quidway-vlan10] dhcp snooping enable
[Quidway-vlan10] dhcp snooping check dhcp-request enable
```

防止 DHCP Server 服务拒绝攻击

如图 1-1 所示，若设备接口 interface1 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 CHADDR 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。

图1-1 DHCP Server 服务拒绝攻击示意图



为了抑制 DHCP 用户恶意申请 IP 地址，可配置连接恶意 DHCP 用户的设备或接口允许接入的最大用户数，当用户数达到该值时，则任何用户将无法通过此设备或接口成功申请到 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，相等则转发报文，否则丢弃。

10. 配置防止 DHCP Server 服务拒绝攻击

1）. 配置GE1/0/1接口最多接入200个DHCP用户。

```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] dhcp snooping enable
[Quidway-GigabitEthernet1/0/1] dhcp snooping max-user-number 200
```

2）. 使能 GE1/0/1 的 dhcp-chaddr 检查功能。

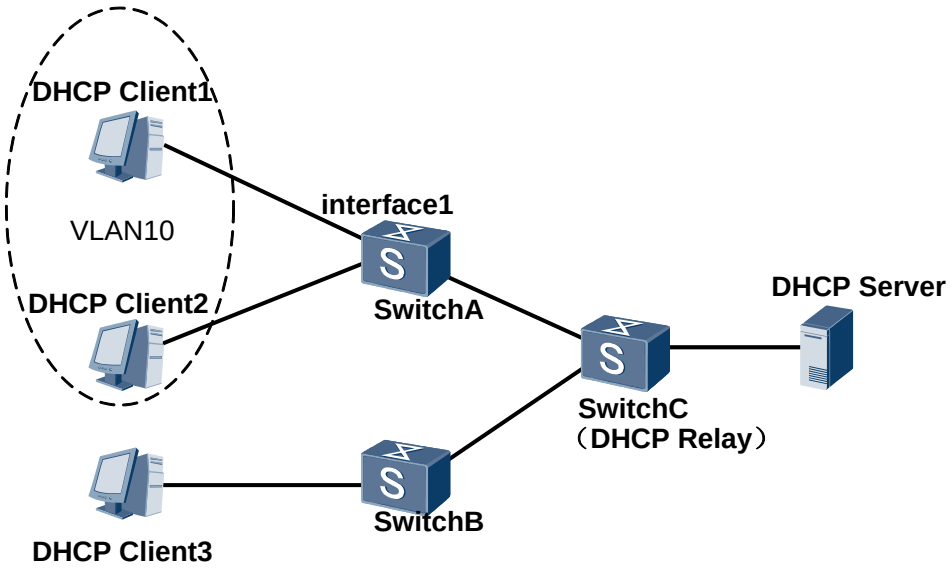
```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] dhcp snooping enable
[Quidway-GigabitEthernet1/0/1] dhcp snooping check dhcp-chaddr enable
```

1.3.3 DHCP Snooping 支持的 Option82 功能

概述

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 Option 82 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1-2 Option82 应用组网图



如图 1-2 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。Option82 包含两个子选项 Circuit ID（Sub-option 1）和 Remote ID（Sub-option 2）。其中 Circuit ID 子选项主要用来标识客户端所在的 VLAN、端口等信息，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。DHCP Server 在接收到携带有 Option82 选项的 DHCP 请求报文后，即可通过 Opion82 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。

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 DHCPv4 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：若该报文中含有 Option82 选项，则删除之，并转发给 DHCP Client；若报文中不含有 Option82 选项，则直接转发。

11. 在 GE1/0/1 接口上使能在 DHCP 报文中插入 Option82 选项功能

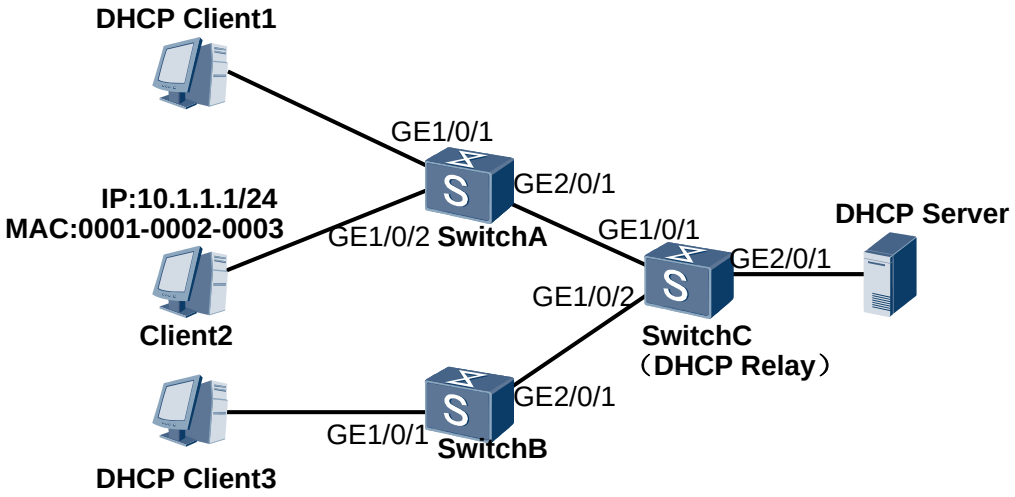
```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] dhcp snooping enable
[Quidway-GigabitEthernet1/0/1] dhcp option82 insert enable
```

1.4 应用

1.4.1 DHCP Snooping 的攻击防范功能典型组网应用

如图 1-3 所示，SwitchA 与 SwitchB 为接入设备，SwitchC 为 DHCP Relay。Client1 与 Client2 分别通过 GE1/0/1 与 GE1/0/2 接入 SwitchA，Client3 通过 GE1/0/1 接入 SwitchB，其中 Client1 与 Client3 通过 DHCP 方式获取 IPv4 地址，而 Client2 使用静态配置的 IPv4 地址。网络中存在非法用户的攻击导致合法用户不能正常获取 IP 地址，管理员希望能够防止网络中针对 DHCP 的攻击，为 DHCP 用户提供更优质的服务。

图1-3 配置 DHCP Snooping 的攻击防范功能组网图



Switch C 的配置文件

```
#
sysname SwitchC
#
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 80
arp dhcp-snooping-detect enable
#
interface GigabitEthernet1/0/1
 dhcp snooping sticky-mac
 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 alarm dhcp-reply enable
 dhcp snooping alarm dhcp-reply threshold 120
 dhcp snooping max-user-number 20
#
interface GigabitEthernet1/0/2
 dhcp snooping sticky-mac
 dhcp snooping 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 alarm dhcp-reply enable
 dhcp snooping alarm dhcp-reply threshold 120
 dhcp snooping max-user-number 20
#
interface GigabitEthernet2/0/1
 dhcp snooping trusted
#
return
```

1.5 术语与缩略语

缩略语

缩略语	英文全称	中文全称
DHCP	Dynamic Host Configure Protocol	动态主机配置协议