

DHCP-SNOOPING配置

目 录

第 1 章 DHCP-snooping配置.....	1
1.1 DHCP-snooping配置任务	1
1.1.1 开启/关闭DHCP-snooping功能.....	1
1.1.2 在VLAN 上启动DHCP-snooping.....	1
1.1.3 配置接口为DHCP信任接口	2
1.1.4 在VLAN 上启动DAI功能	2
1.1.5 配置接口为ARP监测信任接口	2
1.1.6 在VLAN 上启动IP源地址监测功能.....	3
1.1.7 配置接口为IP 源信任接口.....	3
1.1.8 配置接口绑定关系备份的TFTP服务器.....	3
1.1.9 配置接口绑定关系备份的文件名.....	3
1.1.10 配置接口绑定关系备份检查的时间间隔.....	4
1.1.11 手工配置接口绑定	4
1.1.12 DHCP-snooping的监控与维护.....	4
1.1.13 DHCP-snooping配置示例	5

第1章 DHCP-snooping配置

1.1 DHCP-snooping配置任务

DHCP-snooping 的任务就是对 DHCP 报文进行判断，防止伪造的 DHCP 服务器提供 DHCP 服务，维护接口上 MAC 地址与 IP 地址的对应绑定关系。根据 MAC 地址与 IP 地址的对应绑定，可以完成 DAI（动态 ARP 监测）和 IP source guard 功能。DHCP-snooping 功能主要包括侦听 DHCP 报文、动态维护 MAC 地址与 IP 地址的对应绑定表，二层交换机过滤非信任端口的不满足这种对应绑定关系的报文，防止非法用户对网络的攻击。

- [开启/关闭DHCP-snooping功能](#)
- 在 VLAN 上启动 DHCP-snooping
- [配置接口为DHCP信任接口](#)
- [在VLAN上启动DAI功能](#)
- [配置接口为ARP监测信任接口](#)
- [在VLAN上启动IP源地址监测功能](#)
- [配置接口为IP 源地址监测信任接口](#)
- [配置DHCP-snooping绑定备份的TFTP服务器](#)
- 配置 DHCP-snooping 绑定备份的文件名
- 配置 DHCP-snooping 绑定备份的时间间隔
- 手工配置添加绑定关系
- [DHCP-snooping的监控与维护](#)
- [配置DHCP-snooping的示例](#)

1.1.1 开启/关闭DHCP-snooping功能

在全局配置模式下进行下列配置：

命令	目的
ip dhcp-relay snooping	开启DHCP-snooping功能。
no ip dhcp-relay snooping	恢复缺省设置。

该命令是启动 DHCP snooping 功能的全局控制命令。配置该命令，则交换机侦听所有 DHCP 报文，形成相应的绑定关系。

注意：如果客户端是在配置该命令之前通过此交换机获取地址，则交换机不能添加相应的绑定关系。

1.1.2 在VLAN 上启动DHCP-snooping

在 VLAN 上启动 DHCP snooping 功能，则对属于整个 VLAN 的所有非信任物理端口收到的 DHCP 报文进行合法化检查。对于 VLAN 内的非信任物理端口收到的 DHCP 响应报文将丢弃，防止用户非法伪造或者误配的 DHCP 服务器提供地址分

配；对于非信任端口的 DHCP 请求报文，如果报文发送 MAC 地址和报文内的硬件地址字段不匹配，认为是用户故意伪造的用于 DHCP DOS（拒绝服务）的攻击报文，交换机也将丢弃。

在全局配置模式下进行下列配置：

命令	目的
ip dhcp-relay snooping vlan <i>vlan_id</i>	在VLAN上启动DHCP snooping 功能
no ip dhcp-snooping vlan <i>vlan_id</i>	在VLAN上关闭DHCP snooping 功能。

1.1.3 配置接口为DHCP信任接口

配置接口为 DHCP 信任接口，则该接口收到的 DHCP 报文不进行检查。

在物理接口配置模式下进行下列配置：

命令	操作
dhcp snooping trust	配置接口为DHCP信任接口
no dhcp snooping trust	恢复接口为DHCP非信任接口。

缺省情况下接口为非信任接口。

1.1.4 在VLAN 上启动DAI功能

在属于某个 VLAN 的所有物理端口进行 ARP 动态监测，如果该接口收到的 ARP 报文的源 MAC 和源 IP 地址不满足接口上配置的 MAC 和 IP 地址绑定关系，则拒绝处理该报文。接口上配置的绑定关系可以是 DHCP 动态绑定的，也可以是手工配置的。如果物理接口上没有配置任何 MAC 和 IP 地址绑定，则交换机拒绝转发所有 ARP 报文。

命令	操作
ip arp inspection vlan <i>vlanid</i>	对VLAN 内的所有非信任端口启动动态ARP监测
no ip arp inspection vlan <i>vlanid</i>	对VLAN 内的所有非信任端口关闭动态ARP监测

1.1.5 配置接口为ARP监测信任接口

对于 ARP 监测信任接口，不启动 ARP 监测功能。接口默认为非信任接口。

在接口配置模式下进行下列配置：

命令	操作
arp inspection trust	配置接口为ARP监测信任接口
no arp inspection trust	恢复接口为ARP监测非信任接口

1.1.6 在VLAN 上启动IP源地址监测功能

启动 IP 源地址监测的 VLAN,属于该 VLAN 的所有物理端口收到的 IP 报文的源 MAC 和源 IP 地址不满足接口上配置的 MAC 和 IP 地址绑定关系,则该报文被拒绝处理。接口上配置的绑定关系可以是 DHCP 动态绑定的,也可以是手工配置的。如果此物理接口上没有配置任何 MAC 和 IP 地址绑定,则交换机拒绝转发所有该接口收到的 IP 报文。

在全局配置模式下进行下列配置:

命令	操作
ip verify source vlan <i>vlanid</i>	对VLAN内的所有非信任接口启动报文源IP地址检查功能
no ip verify source vlan <i>vlanid</i>	对VLAN内的所有接口关闭报文源IP地址检查功能

注意: 如果收到的是 DHCP 报文(也是 IP 报文),则因为配置了全局 snooping 进行软件转发。

1.1.7 配置接口为IP 源信任接口

对于 IP 源地址信任接口,不启动源地址检查功能。

在接口配置模式下进行下列配置:

命令	操作
ip-source trust	配置接口为IP源地址信任接口。
no ip-source trust	恢复接口为IP源地址非信任接口

1.1.8 配置接口绑定关系备份的TFTP服务器

当交换机配置保存重新启动之后,原来配置的接口绑定关系会丢失,这时,接口上没有绑定关系,启动 IP 源地址监测功能后,交换机拒绝转发所有 IP 报文。配置了接口绑定关系备份的 TFTP 服务器之后,绑定关系会通过 TFTP 协议备份到服务器,在交换机重启后,自动到 TFTP 服务器下载绑定表,以保证网络正常工作。

在全局配置模式下进行下列配置:

命令	操作
ip dhcp-relay snooping database-agent <i>ip-address</i>	配置接口绑定关系备份的TFTP服务器IP地址。
no ip dhcp-relay snooping database-agent	删除接口绑定关系备份的TFTP服务器配置

1.1.9 配置接口绑定关系备份的文件名

配置备份接口绑定关系时,在 TFTP 服务器上保存的文件名。这样,不同的交换机可以将自己的接口绑定关系表备份到同一台 TFTP 服务器。

在全局配置模式下进行下列配置:

命令	操作
ip dhcp-relay snooping db-file <i>name</i>	配置接口绑定关系备份保存的文件名
no ip dhcp-relay snooping db-file	删除接口绑定关系备份保存的文件名

1.1.10 配置接口绑定关系备份检查的时间间隔

接口的 MAC 地址和 IP 地址的绑定关系表是动态变化的，需要在一定的时间间隔之后，检查绑定是否有更新，如果有更新（添加或者删除绑定条目）则进行重新备份。默认时间间隔为 30 分钟。

在全局配置模式下进行下列配置：

命令	操作
ip dhcp-relay snooping write <i>num</i>	配置接口绑定关系备份检查的时间间隔，单位分钟
no ip dhcp-relay snooping write	恢复接口绑定关系备份检查的时间间隔为默认时间间隔

1.1.11 手工配置接口绑定

对于不使用 DHCP 获取地址的主机，在交换机接口上可以手工配置添加绑定条目以是主机正常访问网络。使用该命令的 no 命令可以删除绑定条目。

注意：手工配置的绑定条目比动态配置的绑定条目优先级要高，如果配置条目的 MAC 地址与动态配置条目的 MAC 地址相同，则手工配置的更新动态配置条目。接口绑定条目以 MAC 地址为唯一索引。

在全局配置模式下进行下列配置：

命令	操作
ip source binding <i>MAC IP interface name</i>	手工配置接口绑定。
no ip source binding <i>MAC IP</i>	删除接口绑定条目

1.1.12 DHCP-snooping的监控与维护

请在管理态下进行下列操作：

命令	操作
show ip dhcp-relay snooping	显示DHCP-snooping的配置信息
show ip dhcp-relay snooping binding	显示在接口生效的地址绑定条目
show ip dhcp-relay snooping binding all	显示DHCP snooping生成的所有绑定条目
[no] debug ip dhcp-relay [snooping binding event all]	开启/关闭DHCP relay snooping/绑定/事件开关

显示运行 dhcp snooping 功能的配置信息:

```
switch#show ip dhcp-relay snooping
ip dhcp-relay snooping vlan 3
ip arp inspection vlan 3
DHCP Snooping trust interface:
FastEthernet0/1
ARP Inspect interface:
FastEthernet0/11
```

显示 dhcp-relay snooping 绑定信息:

```
switch#show ip dhcp-relay snooping binding
Hardware Address    IP Address    remainder time Type          VLAN    interface
00-e0-0f-26-23-89  192.2.2.101  86400        DHCP_SN        3        FastEthernet0/3
```

显示 dhcp-relay snooping 所有绑定信息:

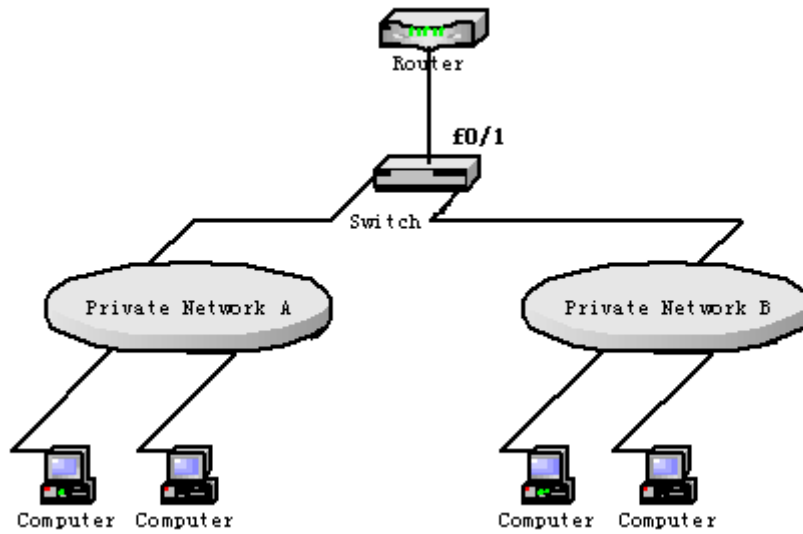
```
switch#show ip dhcp-relay snooping binding all
Hardware Address    IP Address    remainder time Type          VLAN    interface
00-e0-0f-32-1c-59  192.2.2.1    infinite     MANUAL         1        FastEthernet0/2
00-e0-0f-26-23-89  192.2.2.101  86400        DHCP_SN        3        FastEthernet0/3
```

调试 dhcp-relay snooping 信息:

```
switch#debug ip dhcp-relay all
DHCP: receive l2 packet from vlan 3, diID: 3
DHCP: DHCP packet len 277
DHCP: add binding on interface FastEthernet0/3
DHCP: send packet continue
DHCP: receive l2 packet from vlan 3, diID: 1
DHCP: DHCP packet len 300
DHCP: send packet continue
DHCP: receive l2 packet from vlan 3, diID: 3
DHCP: DHCP packet len 289
DHCP: send packet continue
DHCP: receive l2 packet from vlan 3, diID: 1
DHCP: DHCP packet len 300
DHCP: update binding on interface FastEthernet0/3
DHCP: IP address: 192.2.2.101, lease time 86400 seconds
DHCP: send packet continue
```

1.1.13 DHCP-snooping配置示例

示例网络连接如图 1:



配置 Switch:

- (1) 开启连接 Private Network A 的 VLAN 1 的 DHCP-snooping
Switch_config#ip dhcp-relay snooping
Switch_config#ip dhcp-relay snooping vlan 1
- (2) 开启连接 Private Network B 的 VLAN 2 的 DHCP-snooping
Switch_config#ip dhcp-relay snooping
Switch_config#ip dhcp-relay snooping vlan 2
- (3) 配置 DHCP 服务器连接端口为 DHCP 信任端口
Switch_config_f0/1#dhcp snooping trust