DHCP-SNOOPING配置

目 录

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
- 在 VLAN 上启动 DHCP 防攻击功能
- 配置接口为 DHCP 信任接口
- 开启/关闭绑定表快速更新功能
- 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 Option82 选项格式
- 配置 DHCP-snooping Option82 报文策略
- 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 *vlan_id*	在VLAN上启动DHCP snooping 功能
no ip dhcp-relay snooping vlan *vlan_id*	在VLAN上关闭DHCP snooping 功能。

1.1.3 在 VLAN 上启动 DHCP 防攻击功能

在 VLAN 上启动 DHCP 防攻击功能，配置了 DHCP snooping 特定 VLAN 下的允许最大 dhcp client 用户数，执行先到先分配的原则，当 vlan 内的用户数达到配置的允许最大值后，就不允许新的 client 进行分配。

在全局配置模式下进行下列配置：

命令	目的
ip dhcp-relay snooping vlan *vlan_id* **max-client** *number*	在VLAN上启动DHCP防攻击功能
no ip dhcp-relay snooping vlan *vlan_id* **max-client**	在VLAN上关闭DHCP防攻击。

1.1.4 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。

1.1.5 开启/关闭绑定表快速更新功能

默认情况下此功能关闭。没有开启此功能时，如果在一个端口下已经绑定了客户端 A，相同的 mac 地址在其他端口的 dhcp 请求会被认为是伪造 mac 攻击，即使客户端 A 已经下线（没有 release 地址）。

开启此功能后，同一个客户端 A，在其他端口上如果在发送 dhcp 请求报文，dhcp snooping 会将原来端口上的 A 的绑定信息删除，不认为此行为是攻击行为。

建议在客户端会频繁更换端口的环境下，且 dhcp server 分配的地址租约无法改动为较短时间的时候才考虑使用此功能。

命令	操作
ip dhcp-relay snooping rapid-refresh-bind	开启绑定表快速更新功能
no ip dhcp-relay snooping rapid-refresh-bind	关闭绑定表快速更新功能

1.1.6 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 *vlanid*	对VLAN 内的所有非信任端口启动动态ARP监测
no ip arp inspection vlan *vlanid*	对VLAN 内的所有非信任端口关闭动态ARP监测

1.1.7 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

1.1.8 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 *vlanid*	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 *vlanid*	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。

1.1.9 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

1.1.10 配置 DHCP-snooping Option82 选项格式

Option82 选项将可以携带本地信息给服务器，帮助服务器来分配给客户端地址。

在全局模式下进行下列配置：

命令	操作
ip dhcp-relay snooping information option	配置DHCP-snooping转发DHCP报文将携带option82选项，选项为默认格式。
no ip dhcp-relay snooping information option	配置DHCP-snooping转发DHCP报文不携带option82选项。

如果想要指定 option82 格式，则在全局模式下进行下列配置：

命令	操作
ip dhcp-relay snooping information option format {snmp-ifindex/manual/hn-type [host]}	配置DHCP-snooping转发DHCP报文将携带option82选项，选项为SNMP-IFINDEX格式、手动配置格式或者cisco格式。
no ip dhcp-relay snooping information option format {snmp-ifindex/manual/hn-type [host]}	配置DHCP-snooping转发DHCP报文不携带option82选项。

如果配置了手动模式填写 option82，在接口配置模式下进行下列配置 circuit-id 子选项：

命令	操作
dhcp snooping information circuit-id string [STRING]	如果配置了option82为手动格式，则配置DHCP-snooping转发DHCP报文将携带option82选项，选项内容为STRING所写的字符串。此命令在连接client的端口上配置。
dhcp snooping information circuit-id **hex [***xx-xx-xx-xx-xx-xx***]**	如果配置了option82为手动格式，则配置DHCP-snooping转发DHCP报文将携带option82选项，选项内容为所写十六进制。此命令在连接client的端口上配置。
no dhcp snooping information circuit-id	删除手动配置的option82 circuit-id字符串。

如果配置了手动模式填写 option82，在接口配置模式下进行下列配置 remote-id 子选项：

命令	操作
dhcp snooping information remote-id string [STRING]	如果配置了option82为手动格式，则配置DHCP-snooping转发DHCP报文将携带option82选项，选项内容为STRING所写的字符串。此命令在连接client的端口上配置。
dhcp snooping information remote-id **hex [***xx-xx-xx-xx-xx-xx***]**	如果配置了option82为手动格式，则配置DHCP-snooping转发DHCP报文将携带option82选项，选项内容为所写十六进制。此命令在连接client的端口上配置。
no dhcp snooping information remote-id	删除手动配置的option82 remote-id字符串。

如果配置了手动模式填写 option82，在接口配置模式下进行下列配置 vendor-specific 子选项：

命令	操作
dhcp snooping information vendor-specific string STRING	如果配置了 option82 为手动格式，则配置 DHCP-snooping 转发 DHCP 报文将携带 option82 选项，选项内容为 STRING 所写的字符串。此命令在连接 client 的端口上配置。
dhcp snooping information vendor-specific hex [*xx-xx-xx-xx-xx-xx***]**	如果配置了option82为手动格式，则配置DHCP-snooping转发DHCP报文将携带option82选项，选项内容为所写十六进制。此命令在连接client的端口上配置。
no **dhcp snooping information vendor-specific**	删除手动配置的option82 **vendor-specific。**

1.1.11 配置 DHCP-snooping Option82 报文策略

可以配置收到已经携带 option82 选项的 dhcp 请求包后采取的策略。

Drop 策略：在端口模式下输入下列命令，配置丢弃包含 option82 选项的请求包：

命令	操作
dhcp snooping information drop	此命令配置后，将丢弃包含option82选项的请求包。

Append 策略：在端口模式下输入下列命令，配置追加包含 option82 选项的请求包：

命令	操作
dhcp snooping information append	端口开启追加 option82 选项
dhcp snooping information append first-subop9-param { hex *xx-xx-xx-xx-xx-xx* **| vlanip | hostname }**	Option82 vendor-specific（suboption9）子选项所带的第一个参数
dhcp snooping information append second-subop9-param { hex *xx-xx-xx-xx-xx-xx* **| vlanip | hostname }**	Option82 vendor-specific（suboption9）子选项所带的第二个参数

1.1.12 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 *ip-address*	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 *ip-address*	删除接口绑定关系备份的TFTP服务器配置

1.1.13 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 *name*	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

1.1.14 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-immediately	配置 DHCP Snooping 在绑定信息发生变化时即时备份 no ip dhcp-relay snooping {write-time | write-immediately} 恢复接口绑定关系备份检查的时间间隔为默认时间间隔
ip dhcp-relay snooping write-time *num*	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-time	恢复接口绑定关系备份检查的时间间隔为默认时间间隔

1.1.15 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 *MAC IP* interface *name vlan-id*	手工配置接口绑定。
no ip source binding *MAC IP vlan-id*	删除接口绑定条目

1.1.16 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:
   GigaEthernet0/1
ARP Inspect interface:
   GigaEthernet0/11
```

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          GigaEthernet0/3
```

显示 dhcp-relay snooping 所有绑定信息：

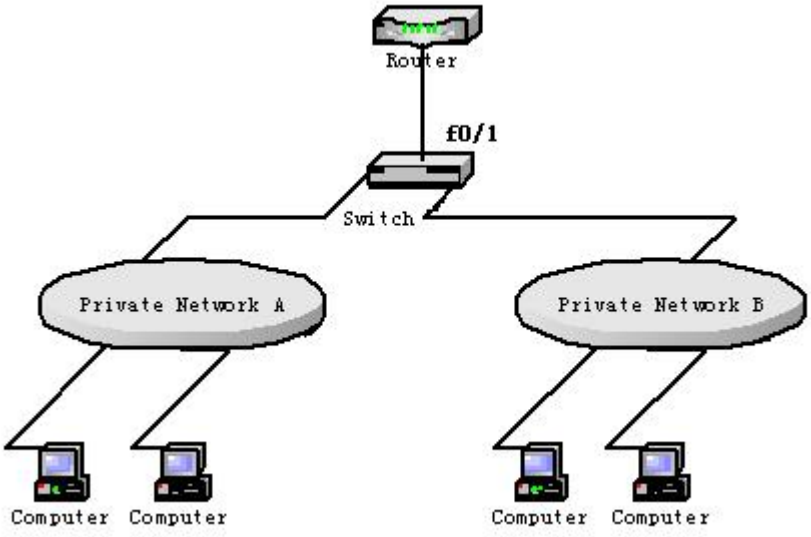
```
switch#show ip dhcp-relay snooping binding all
Hardware Address      IP Address        remainder time Type              VLAN      interface

00-e0-0f-32-1c-59     192.2.2.1         infinite       MANUAL            1          GigaEthernet0/2
00-e0-0f-26-23-89     192.2.2.101       86400       DHCP_SN          3          GigaEthernet0/3
```

调试 dhcp-relay snooping 信息：

```
switch#debug ip dhcp-relay all
DHCPR: receive l2 packet from vlan 3, diID: 3
DHCPR: DHCP packet len 277
DHCPR: add binding on interface GigaEthernet0/3
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, diID: 1
DHCPR: DHCP packet len 300
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, diID: 3
DHCPR: DHCP packet len 289
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, diID: 1
DHCPR: DHCP packet len 300
DHCPR: update binding on interface GigaEthernet0/3
DHCPR:    IP address: 192.2.2.101, lease time 86400 seconds
DHCPR: send packet continue
```

1.1.17 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_g0/1#dhcp snooping trust

(4) 手动配置 option82 选项实例：

interface GigaEthernet0/1

dhcp snooping information circuit-id hex 00-01-00-05

dhcp snooping information remote-id hex 00-e0-0f-13-1a-50

dhcp snooping information vendor-specific hex 00-00-0c-f8-0d-01-0b-78-69-61-6f-6d-69-6e-37-31-31-34

dhcp snooping information append

dhcp snooping information append first-subop9-param hex 61-62-63-61-62-63

!

interface GigaEthernet0/2

dhcp snooping trust

arp inspection trust

ip-source trust

!

!

!

ip dhcp-relay snooping

```
ip dhcp-relay snooping vlan  1-100
ip arp inspection vlan  1
ip verify source vlan  1
ip dhcp-relay snooping information option format manual
```