

DHCP-SNOOPING配置命令

目 录

第 1 章 DHCP-SNOOPING 配置命令.....	1
1.1 DHCP-SNOOPING 配置命令.....	1
1.1.1 ip dhcp-relay snooping.....	1
1.1.2 ip dhcp-relay snooping vlan.....	2
1.1.3 ip dhcp-relay snooping vlan <i>vlan_id</i> max-client.....	3
1.1.4 ip dhcp-relay snooping database-agent.....	3
1.1.5 ip dhcp-relay snooping db-file.....	4
1.1.6 ip dhcp-relay snooping write-time.....	5
1.1.7 ip dhcp-relay snooping write-immediately.....	5
1.1.8 ip dhcp-relay snooping log.....	6
1.1.9 ip dhcp-relay snooping rapid-refresh-bind.....	7
1.1.10 dhcp-relay snooping information option.....	7
1.1.11 ip verify source vlan.....	8
1.1.12 ip arp inspection vlan.....	9
1.1.13 ip source binding.....	10
1.1.14 arp inspection trust.....	11
1.1.15 dhcp snooping trust.....	11
1.1.16 dhcp snooping deny.....	12
1.1.17 dhcp snooping information circuit-id.....	12
1.1.18 dhcp snooping information remote-id string.....	13
1.1.19 dhcp snooping information vendor-specific.....	14
1.1.20 dhcp snooping information append.....	15
1.1.21 dhcp snooping information drop.....	16
1.1.22 ip-source trust.....	17
1.1.23 show ip dhcp-relay snooping.....	17
1.1.24 show ip dhcp-relay snooping binding.....	18
1.1.25 debug ip dhcp-relay snooping.....	19
1.1.26 debug ip dhcp-relay event.....	19
1.1.27 debug ip dhcp-relay binding.....	20

第 1 章 DHCP-SNOOPING 配置命令

1.1 DHCP-SNOOPING配置命令

DHCP-SNOOPING 配置命令包括：

- ip dhcp-relay snooping
- ip dhcp-relay snooping vlan
- ip dhcp-relay snooping database-agent
- ip dhcp-relay snooping db-file
- ip verify source vlan
- ip arp inspection vlan
- ip source binding
- arp inspection trust
- dhcp snooping trust
- ip-source trust
- show ip dhcp-relay snooping
- show ip dhcp-relay snooping binding
- debug ip dhcp-relay snooping
- debug ip dhcp-relay event
- debug ip dhcp-relay binding

1.1.1 ip dhcp-relay snooping

命令描述

ip dhcp-relay snooping

no ip dhcp-relay snooping

配置 VLAN 的 Dhcp-relay snooping 功能开启和关闭，no 命令恢复到默认值。

参数

无

缺省

关闭 dhcp-relay snooping 功能。

说明

无。

示例

下面的命令将开启 DHCP snooping 功能：

```
Switch_config#ip dhcp-relay snooping
Switch_config#
```

1.1.2 ip dhcp-relay snooping vlan

命令描述

ip dhcp-relay snooping vlan *vlan_id*

no ip dhcp-relay snooping vlan *vlan_id*

参数

参数	参数说明
<i>vlan_id</i>	VLAN标识。取值范围：1-4094。

缺省

无

说明

配置 DHCP snooping 的 VLAN。

示例

下面的命令将在 VLAN 2 上对 DHCP 报文进行 snooping 检查

```
Switch_config#ip dhcp-relay snooping vlan 2
Switch_config#
```

1.1.3 ip dhcp-relay snooping vlan *vlan_id* max-client

命令描述

ip dhcp-relay snooping vlan *vlan_id* max-client *number*
no ip dhcp-relay snooping vlan *vlan_id* max-client

参数

参数	参数说明
<i>vlan_id</i>	VLAN标识。取值范围：1-4094。
<i>number</i>	允许最大用户数：0~65535

缺省

默认为 65535 个最大用户数。

说明

配置 DHCP snooping 的 VLAN 下的允许最大用户数，执行先到先得的原则，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。

示例

下面的命令将在 VLAN 2 上对 DHCP 报文进行 snooping 检查，允许最大的用户数为 3。

```
Switch_config#ip dhcp-relay snooping vlan 2 max-client 3
Switch_config#
```

1.1.4 ip dhcp-relay snooping database-agent

命令描述

ip dhcp-relay snooping database-agent *A.B.C.D*
no ip dhcp-relay snooping database-agent *A.B.C.D*

配置 DHCP snooping 绑定备份的 TFTP 服务器。

参数

参数	参数说明
A.B.C.D	TFTP 服务器的IP地址

缺省

无备份服务器。

说明

如果没有配置 TFTP 服务器地址，则不进行绑定备份

示例

下面的命令配置 DHCP snooping 绑定备份的服务器地址为 192.168.1.1。

```
Switch_config#ip dhcp-relay snooping database-agent 192.168.1.1
Switch_config#
```

1.1.5 ip dhcp-relay snooping db-file

命令描述

ip dhcp-relay snooping db-file *name* [*timestamp*]

no ip dhcp-relay snooping db-file [*timestamp*]

参数

参数	参数说明
<i>Name</i>	备份DHCP snooping绑定保存的文件名
<i>timestamp</i>	备份的绑定表文件名保存时带时间戳

缺省

文件空

说明

如果没有配置文件名，则不进行绑定备份。

示例

下面的命令配置备份绑定的文件名为 `dhcp_binding.txt`。

```
Switch_config#ip dhcp-relay snooping db-file dhcp_binding.txt
Switch_config#
```

1.1.6 ip dhcp-relay snooping write-time

命令描述

ip dhcp-relay snooping write-time *num*

no ip dhcp-relay snooping write-time

参数

参数	参数说明
<i>Num</i>	备份DHCP snooping绑定的时间间隔（2-1440）

缺省

默认 30 分钟

说明

在配置的时间间隔内检查是否有绑定更新，如果有更新，则备份绑定信息。

示例

下面的命令配置备份绑定的时间间隔为 60 分钟。

```
Switch_config#ip dhcp-relay snooping write-time 60
Switch_config#
```

1.1.7 ip dhcp-relay snooping write-immediately

命令描述

ip dhcp-relay snooping write-immediately

no ip dhcp-relay snooping write-immediately

参数

无

缺省

无

说明

如果有表项更新，将立刻写入绑定表数据库。建议在表项较多时不要打开这个功能，不然可能影响性能。

示例

下面的命令配置表项更新后立即备份绑定表。

```
Switch_config#ip dhcp-relay snooping write-immediately  
Switch_config#
```

1.1.8 ip dhcp-relay snooping log

命令描述

ip dhcp-relay snooping log

no ip dhcp-relay snooping log

参数

无

缺省

无

说明

打开该 log 功能后，如果从非 trust 端口有 dhcp server 的报文，那么会报 syslog，说明哪个端口上有非法的 dhcp server。

示例

下面的命令配置启动 dhcp snooping 的 log 功能。


```
Switch_config#ip dhcp-relay snooping log
Switch_config#
```

1.1.9 ip dhcp-relay snooping rapid-refresh-bind

命令描述

ip dhcp-relay snooping rapid-refresh-bind

no ip dhcp-relay snooping rapid-refresh-bind

开启 dhcp snooping 快速更新表项功能。

参数

无

缺省

无。

说明

此功能开启以后将关闭伪造 mac 的 dhcp 攻击，同时允许客户端更换接入的端口后，无需等待 ip 地址租约到期，就能够直接获取地址。

在此功能关闭以后，如果客户端更换接入的端口，将被开启 snooping 的设备认为是伪造 mac 的 dhcp 报文攻击，会将此 dhcp 报文丢弃。

示例

无

1.1.10 dhcp-relay snooping information option

命令描述

ip dhcp-relay snooping information option [format snmp-ifindex | manual | hn-type [host]]

no ip dhcp-relay snooping information option [format snmp-ifindex | manual | hn-type [host]]

参数

参数	参数说明
format snmp-ifindex	使用SNMP ifindex的方式填写option82（可选）
format manual	使用手动配置填写option82(可选)
format hn-type [host]	使用cisco格式填写option82（可选） Host表示配置设备为主交换机

缺省

默认不会在报文中追加或删除 option82

说明

指定交换机设备在进行 DHCP snooping 时是否进行 DHCP option82 的处理。若指定了 **format snmp-ifindex**，则使用 SNMP ifindex 的方式填写 option82；若指定了 **format manual**，则使用在各个端口利用命令 “**dhcp snooping information circuit-id string**” 配置的字符串填写 option82 的 circuit-id 选项；否则按照 RFC3046 的规定填写 option82。

示例

下面的命令配置使用 SNMP ifindex 的方式填写 option82。

```
Switch_config#ip dhcp-relay snooping
Switch_config#ip dhcp-relay snooping information option format snmp-ifindex
```

下面的命令配置使用 manual 的方式填写 option82。

```
Switch_config#ip dhcp-relay snooping
Switch_config#ip dhcp-relay snooping vlan [WORD] // [WORD]为需要启动 snooping
功能的 vlan 名
Switch_config# ip dhcp-relay snooping information option format manual
```

1.1.11 ip verify source vlan

命令描述

```
ip verify source vlan vlanid
no ip verify source vlan vlanid
```

参数

参数	参数说明
<i>vlan id</i>	VLAN标识。取值范围：1-4094。

缺省

无

说明

配置进行 IP 源地址监测的 VLAN，`no` 命令去掉监测。如果 IP 报文的源 IP 和源 MAC 不是 dhcp snooping 所监听到的 dhcp server 分配的 client 合法地址，那么在启用 IP 源地址监测的 vlan 内将此类报文视为非法报文，并且丢弃此报文。

示例

下面的命令将 VLAN 2 的所有物理端口（信任端口除外）的报文都进行 IP 源地址监测。

```
Switch_config#ip verify source vlan 2
Switch_config#
```

1.1.12 ip arp inspection vlan

命令描述

ip arp inspection vlan *vlanid*

no ip arp inspection vlan *vlanid*

参数

参数	参数说明
<i>vlanid</i>	VLAN标识。取值范围：1-4094。

缺省

无

说明

配置进行 ARP 报文源地址监测的 VLAN，`no` 命令去掉监测。在启用 ARP 报文源地址监测的 vlan 下，会丢弃拥有不符合 dhcp server 分配给 client 的 IP 地址、mac 地址对应的 SIP 和 SMAC 的 ARP 报文。

示例

下面的命令将 VLAN 2 的所有物理端口（信任端口除外）的报文都进行 ARP 报文源地址监测。

```
Switch_config#ip arp inspection vlan 2
Switch_config#
```

1.1.13 ip source binding

命令描述

ip source binding *xx-xx-xx-xx-xx-xx A.B.C.D interface name vlan vlan-id*

no ip source binding *xx-xx-xx-xx-xx-xx A.B.C.D vlan vlan-id*

手工添加或者删除端口的 MAC 地址和 IP 地址绑定。

参数

参数	参数说明
<i>xx-xx-xx-xx-xx-xx</i>	MAC地址
<i>A.B.C.D</i>	IP 地址
<i>Name</i>	接口名称
<i>vlan-id</i>	vlan id号

缺省

无。

说明

无

示例

下面的命令在接口 GigaEthernet0/1 上绑定 08-00-3e-00-00-01 和 192.168.1.2。

```
Switch_config#ip source binding 08-00-3e-00-00-01 192.168.1.2 interface GigaEthernet0/1
Switch_config#
```

1.1.14 arp inspection trust

命令描述

arp inspection trust

no arp inspection trust

参数

无

缺省

默认端口为非信任端口

说明

对于 ARP 信任端口不进行 ARP 监测，no 命令配置端口为默认值。

示例

下面的命令将端口 GigaEthernet0/1 配置为 ARP 信任端口

```
Switch_config_g0/1#arp inspection trust
```

1.1.15 dhcp snooping trust

命令描述

dhcp snooping trust

no dhcp snooping trust

参数

无

缺省

默认端口为非信任端口

说明

对于 DHCP 信任端口不进行 DHCP snooping 监测，no 命令配置端口为默认值。

示例

下面的命令将端口 GigaEthernet0/1 配置为 DHCP 信任端口

```
Switch_config_g0/1#dhcp snooping trust
```

1.1.16 dhcp snooping deny

命令描述

dhcp snooping deny

no dhcp snooping deny

参数

无

缺省

默认端口不禁止 snooping 监测

说明

关闭端口上 DHCP snooping 监测，配置之后自动打开 dhcp snooping trust、ip-source trust、arp inspection trust 。no 命令配置端口为默认值。

示例

下面的命令关闭端口 GigaEthernet0/1 DHCP snooping 监测

```
Switch_config_g0/1#dhcp snooping deny
```

1.1.17 dhcp snooping information circuit-id

命令描述

dhcp snooping information circuit-id {string [STRING] | hex xx-xx-xx-xx-xx-xx}

参数

参数	参数说明
string <i>STRING</i>	Option82 circuit-id子选项所带的字符串
hex <i>xx-xx-xx-xx-xx-xx</i>	Option82 circuit-id子选项所带的十六进制数

缺省

无

说明

此命令可以在每个连接 client 的端口上配置。配置此命令可以配置 dhcp snooping 监听的 dhcp client 发到 dhcp server 的 dhcp 报文 option82 子选项。（需要打开手动方式配置 option82 选项开关，见命令 **ip dhcp-relay snooping information option format manual**）

示例

在端口 g0/3 上手动配置 option82 子选项为 group1，且端口 g0/3 属于 vlan 1。

```
Switch_config#ip dhcp-relay snooping
```

```
Switch_config#ip dhcp-relay snooping vlan 1
```

```
Switch_config#ip dhcp-relay snooping information option format manual
```

```
Switch_config#interface g0/3
```

```
Switch_config_g0/3#dhcp snooping information circuit-id string group1
```

1.1.18 dhcp snooping information remote-id string

命令描述

dhcp snooping information remote-id {string [STRING] | hex *xx-xx-xx-xx-xx-xx*}

参数

参数	参数说明
string <i>STRING</i>	Option82 remote-id 子选项所带的字符串
hex <i>xx-xx-xx-xx-xx-xx</i>	Option82 remote-id 子选项所带的十六进制数

缺省

无

说明

此命令可以在每个连接 client 的端口上配置。配置此命令可以配置 dhcp snooping 监听的 dhcp client 发到 dhcp server 的 dhcp 报文 option82 子选项。（需要打开手动方式配置 option82 选项开关，见命令 **ip dhcp-relay snooping information option format manual**）

示例

在端口 g0/3 上手动配置 option82 子选项为 group1，且端口 g0/3 属于 vlan 1。

```
Switch_config# ip dhcp-relay snooping
```

```
Switch_config# ip dhcp-relay snooping vlan 1
```

```
Switch_config#ip dhcp-relay snooping information option format manual
```

```
Switch_config#interface g0/3
```

```
Switch_config_g0/3# dhcp snooping information remote-id string group1
```

1.1.19 dhcp snooping information vendor-specific**命令描述**

```
dhcp snooping information vendor-specific {string [STRING] | hex  
xx-xx-xx-xx-xx-xx}
```

参数

参数	参数说明
string STRING	Option82 vendor-specific 子选项所带的字符串
hex xx-xx-xx-xx-xx-xx	Option82 vendor-specific 子选项所带的十六进制数

缺省

无

说明

此命令可以在每个连接 client 的端口上配置。配置此命令可以配置 dhcp snooping 监听的 dhcp client 发到 dhcp server 的 dhcp 报文 option82 子选项。（需要打开手动方式配置 option82 选项开关，见命令 **ip dhcp-relay snooping information option format manual**）

示例

在端口 g0/3 上，用十六进制 00-00-00-09-0d-01-0b-78-69-61-6f-6d-69-6e-37-31-31-34 配置 option82 选项 vendor-specific(suboption 9)。

```
Switch_config# ip dhcp-relay snooping
```

```
Switch_config# ip dhcp-relay snooping vlan 1
```

```
Switch_config#ip dhcp-relay snooping information option format manual
```

```
Switch_config#interface g0/3
```

```
Switch_config_g0/3#      dhcp      snooping      information      vendor-specific      hex
00-00-00-09-0d-01-0b-78-69-61-6f-6d-69-6e-37-31-31-34
```

1.1.20 dhcp snooping information append

命令描述

dhcp snooping information append

```
dhcp snooping information append first-subop9-param { hex XX-XX-XX-XX-XX-XX |
hostname | vlanip }
```

```
dhcp snooping information append second-subop9-param { hex XX-XX-XX-XX-XX-XX
| hostname | vlanip }
```

```
no dhcp snooping information append
```

```
no dhcp snooping information append first-subop9-param
```

```
no dhcp snooping information append second-subop9-param
```

参数

参数	参数说明
first-subop9-param hex [xx-xx-xx-xx-xx-xx]	Option82 vendor-specific（suboption9）子选项所带的第一个参数的十六进制
second-subop9-param	Option82 vendor-specific（suboption9）子选项所带的第二个参

hex [XX-XX-XX-XX-XX-XX]	数的十六进制
hostname	Option82 vendor-specific (suboption9) 子选项所带的参数为主机名
vlanip	Option82 vendor-specific (suboption9) 子选项所带的参数为 interface vlan 的 ip 地址

缺省

无

说明

此命令可以在每个连接 client 的端口上配置。配置此命令可以配置 dhcp snooping 监听的 dhcp client 发到 dhcp server 的 dhcp 报文 option82 子选项。

此命令不带参数时为开关命令。当打开 append 后，则在 option82 选项的 suboption9 中追加自己信息。追加信息为 first-subop9-param 和 second-subop9-param。

示例

在端口 g0/3 上扩充带 option82 的 dhcp 报文，用十六进制 61-62-63-61-62-63 配置 suboption9 追加参数一。

```
Switch_config_g0/3# dhcp snooping information append
Switch_config_g0/3# dhcp snooping information append first-subop9-param hex
61-62-63-61-62-63
```

其中 61-62-63-61-62-63 为需要增加的参数的十六进制。

1.1.21 dhcp snooping information drop

命令描述

dhcp snooping information drop

no dhcp snooping information drop

参数

无

缺省

无

说明

此命令可以在每个连接 **client** 的端口上配置。

此命令配置后，将在制定端口上丢弃包含 **option82** 选项的请求包。

示例

在端口 **g0/3** 上配置丢弃带 **option82** 的 **dhcp** 报文。

```
Switch_config_g0/3# dhcp snooping information drop
```

1.1.22 ip-source trust

命令描述

ip-source trust

no ip-source trust

参数

无

缺省

默认端口为非信任端口

说明

对于 **IP** 源地址信任端口不进行 **IP** 源地址监测，**no** 命令配置端口为默认值。

示例

下面的命令将端口 **GigaEthernet0/1** 配置为 **IP** 源地址信任端口

```
Switch_config_g0/1#ip-source trust
```

1.1.23 show ip dhcp-relay snooping

命令描述

show ip dhcp-relay snooping

参数

无

缺省

无

说明

显示 Dhcp-relay snooping 的配置信息。

示例

下面的命令将显示 dhcp-relay snooping 的配置信息。

```
Switch_config#show ip dhcp-relay snooping
```

1.1.24 show ip dhcp-relay snooping binding

命令描述

show ip dhcp-relay snooping binding [all]

参数

无

缺省

无

说明

显示 dhcp-relay snooping 的添加到端口绑定信息。

命令 all 显示 所有 Dhcp-relay snooping 的绑定信息

示例

下面的命令将显示 dhcp-relay snooping 的 binding 信息。

```
Switch_config#show ip dhcp-relay snooping binding
```

1.1.25 debug ip dhcp-relay snooping

命令描述

debug ip dhcp-relay snooping

no debug ip dhcp-relay snooping

参数

无

缺省

无

说明

打开/关闭 Dhcp-relay snooping 的调试开关。

示例

下面的命令将打开 dhcp-relay snooping 的调试开关。

```
Switch#debug ip dhcp-relay snooping  
Switch#
```

1.1.26 debug ip dhcp-relay event

命令描述

debug ip dhcp-relay event

no debug ip dhcp-relay event

参数

无

缺省

无

说明

打开/关闭 Dhcp-relay 的 event 调试开关。

示例

下面的命令将打开 dhcp-relay 的 event 调试开关。

```
Switch#debug ip dhcp-relay event  
Switch#
```

1.1.27 debug ip dhcp-relay binding

命令描述

debug ip dhcp-relay binding

no debug ip dhcp-relay binding

参数

无

缺省

无

说明

打开/关闭 Dhcp-relay snooping 的 binding 调试开关。

示例

下面的命令将打开 dhcp-relay snooping 的 binding 调试开关。

```
Switch#debug ip dhcp-relay binding  
Switch#
```