

目 录

第 1 章 DHCP配置	1-1
1.1 DHCP介绍	1-1
1.2 DHCP服务器配置	1-2
1.3 DHCP中继配置	1-4
1.4 DHCP配置举例	1-5
1.5 DHCP排错帮助	1-8
第 2 章 DHCPv6 配置	2-1
2.1 DHCPv6 简介	2-1
2.2 DHCPv6 服务器配置.....	2-2
2.3 DHCPv6 中继代理配置	2-3
2.4 DHCPv6 前缀代理服务器端配置.....	2-4
2.5 DHCPv6 前缀代理客户端配置	2-6
2.6 DHCPv6 配置举例	2-6
2.7 DHCPv6 排错帮助	2-10
第 3 章 DHCP option 60 和option 43	3-1
3.1 DHCP option 60 和option 43 介绍	3-1
3.2 DHCP option 60 和option 43 配置任务序列.....	3-1
3.3 DHCP option 60 和option 43 举例	3-2
3.4 DHCP option 60 和option 43 排错帮助	3-2
第 4 章 DHCP option 82 配置.....	4-1
4.1 DHCP option 82 介绍.....	4-1
4.1.1 DHCP option 82 报文结构.....	4-1
4.1.2 option 82 工作机制.....	4-2
4.2 DHCP option 82 的配置任务序列.....	4-2
4.3 DHCP option 82 应用举例	4-5
4.4 DHCP option 82 排错帮助	4-7
第 5 章 DHCP Snooping配置	5-1

5.1 DHCP Snooping介绍	5-1
5.2 DHCP Snooping的配置任务序列	5-2
5.3 DHCP Snooping典型应用	5-7
5.4 DHCP Snooping排错帮助	5-7
5.4.1 监控和调试信息	5-7
5.4.2 DHCP Snooping排错帮助	5-8
第 6 章 DHCPv6 Snooping配置	6-1
6.1 DHCPv6 Snooping介绍	6-1
6.1.1 防止伪装DHCPv6 服务器	6-1
6.1.2 防止伪装IPv6 地址	6-1
6.1.3 防止DHCPv6 地址耗尽攻击	6-1
6.1.4 防止ND欺骗	6-1
6.1.5 应对端口移动需求	6-1
6.2 DHCPv6 Snooping的配置任务序列	6-2
6.3 DHCPv6 Snooping典型应用	6-5
6.4 DHCPv6 Snooping排错帮助	6-5
6.4.1 监控和调试信息	6-5
6.4.2 DHCPv6 Snooping排错帮助	6-6
第 7 章 DHCPv6 option 52	7-1
7.1 DHCPv6 option 52 介绍	7-1
7.2 DHCPv6 option 52 配置任务序列	7-1
7.3 DHCPv6 option 52 配置举例	7-2
7.4 DHCPv6 option 52 排错帮助	7-2

第1章 DHCP配置

说明：

本章所指的路由器代表了一般意义下的路由器或运行了路由协议的无线控制产品。

1.1 DHCP介绍

DHCP[RFC2131]是 Dynamic Host Configuration Protocol 动态主机配置协议的简写，它从地址池中把 IP 地址动态分配给请求的主机，同时也能够提供其它网络配置参数，如缺省网关、DNS 服务器、域名和网络范围内主机映像文件的位置等。DHCP 是 BOOTP 协议功能的增强，与 BOOTP 相比，DHCP 是主流技术，它不仅能为无盘工作站提供引导信息，而且在大型的网络中可以大大减轻网络管理员跟踪记录手工分配 IP 地址的负担，同时也能减轻用户的配置任务和花费。DHCP 的另外一个优点是可以部分缓解 IP 地址紧张的状况，当某一 IP 地址的用户离开使用环境时，该 IP 地址还能再次分配给其他用户使用。

DHCP 是基于 Client—Server 模式的协议，DHCP 客户机向 DHCP 服务器索取网络地址及配置参数；服务器为客户机提供网络地址及配置参数；当 DHCP 客户机和 DHCP 服务器不在同一子网时，需要由 DHCP 中继为 DHCP 客户机和 DHCP 服务器传递 DHCP 报文。协议实现的过程如下：

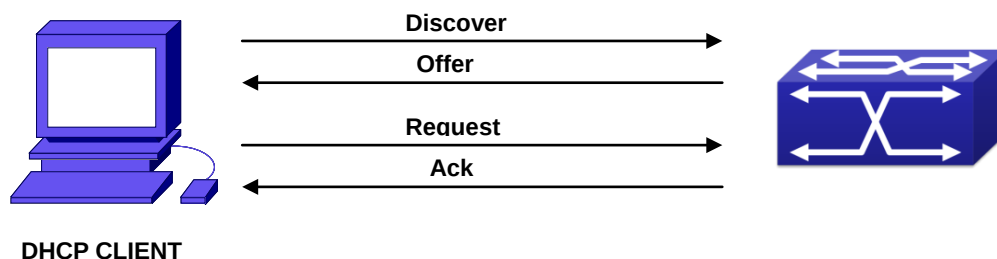


图 1-1 DHCP 协议交互过程

图解：

1. 首先 DHCP 客户机在本子网内广播 DHCPDISCOVER 包；
2. DHCP 服务器收到 DHCPDISCOVER 包后，给该 DHCP 客户机发送带有 IP 地址和其他网络参数的 DHCPOFFER 包；
3. DHCP 客户机对收到的 DHCPOFFER 包进行选择后，广播带有它要选择的 DHCP 服务器的信息的 DHCPREQUEST 包；
4. 被 DHCP 客户机选中的 DHCP 服务器向 DHCP 客户机发送 DHCPACK 包，DHCP 客户机得到 IP 地址和其他网络配置参数。

通过上面四个步骤，完成动态分配主机配置的协议过程。但如果 DHCP 服务器和 DHCP

客户机不在同一网络时，服务器是无法收到客户机发出的 DHCP 广播报文，因此服务器也不会给客户机发送任何 DHCP 报文，这时需要 DHCP 中继来转发这些 DHCP 报文，完成 DHCP 客户机和服务器之间的 DHCP 报文交互过程。

交换机实现了 DHCP 服务器和 DHCP 中继的功能。DHCP 服务器不但支持动态分配 IP 地址，还支持手工绑定 IP 地址（即为指定的硬件地址或者指定设备标识的网络设备分配一个固定的长期的 IP 地址）。动态分配 IP 地址和手工绑定 IP 地址的区别和联系是：1)采用动态方式获得的 IP 地址可以是不固定的；而采用手工绑定方式获得的 IP 地址是固定的；2)采用动态方式获得的 IP 地址租期与其地址池的租期一致，是有时间限制的；而采用手工绑定方式获得的 IP 地址的租期理论上是无限长时间，即没有时间限制；3)已经动态分配出去的地址，不允许再手工绑定；4)手工 DHCP 地址池可以继承相关网段的动态 DHCP 地址池的网络配置参数。

1.2 DHCP服务器配置

DHCP 服务器配置任务序列如下：

- 1. 启动/关闭 DHCP 服务功能
- 2. 配置 DHCP 地址池
 - (1) 创建/删除 DHCP 地址池
 - (2) 配置动态 DHCP 地址池的参数
 - (3) 配置手工 DHCP 地址池的参数
- 3. 启动记录地址冲突的日志功能

1.启动/关闭 DHCP 服务功能

命令	解释
全局配置模式	
service dhcp no service dhcp	启动 DHCP 服务器或中继功能。本命令的 no 操作关闭 DHCP 服务器或中继功能。

2.配置 DHCP 地址池

(1) 创建/删除 DHCP 地址池

命令	解释
全局配置模式	
ip dhcp pool <name> no ip dhcp pool <name>	配置 DHCP 地址池。本命令的 no 操作删除 DHCP 地址池。

(2) 配置动态 DHCP 地址池的参数

命令	解释
DHCP 地址池配置模式	

network-address <network-number> [mask prefix-length] no network-address	配置地址池可分配的地址范围。本命令的 no 操作删除地址池可分配的地址。
default-router [address1[address2[...address8]]] no default-router	为 DHCP 客户机配置缺省网关。本命令的 no 操作删除缺省网关。
dns-server [address1[address2[...address8]]] no dns-server	为 DHCP 客户机配置 DNS 服务器。本命令的 no 操作删除配置的 DNS 服务器。
domain-name <domain> no domain-name	为 DHCP 客户机配置域名；本命令的 no 操作作为删除域名。
netbios-name-server [address1[address2[...address8]]] no netbios-name-server	配置 Wins 服务器的地址。本命令的 no 操作删除服务器的地址。
netbios-node-type {b-node h-node m-node p-node <type -number>} no netbios-node-type	配置 DHCP 客户机的节点类型。本命令的 no 操作删除 DHCP 客户机的节点类型。
bootfile <filename> no bootfile	配置 DHCP 客户机的启动时的导入文件名。本命令的 no 操作删除此操作。
next-server [address1[address2[...address8]]] no next-server [address1[address2[...address8]]]	配置客户机导入文件存放的服务器地址。本命令的 no 操作删除客户机导入文件存放的服务器地址。
option <code> {ascii <string> hex <hex> ipaddress <ipaddress>} no option <code>	配置 option 所指定代码的网络参数的值。本命令的 no 操作删除 option 所指定代码的网络参数值。
lease { days [hours][minutes] infinite } no lease	配置地址池中地址的租用期限。本命令的 no 操作删除地址池中地址的租用期限。
max-lease-time {[<days>] [<hours>] [<minutes>] infinite } no max-lease-time	配置地址池中地址的最大租用期限；本命令的 no 操作作为恢复缺省值。
全局配置模式	
ip dhcp excluded-address <low-address> [<high-address>] no ip dhcp excluded-address <low-address> [<high-address>]	排除地址池中的不用于动态分配的地址。本命令的 no 操作删除此操作。

(3) 配置手工 DHCP 地址池的参数

命令	解释
DHCP 地址池配置模式	
hardware-address <hardware-address> [{Ethernet IEEE802}<type-number>] no hardware-address	在手工分配地址时，指定/删除用户的硬件地址。
host <address> [<mask> <prefix-length>] no host	在手工绑定地址时，配置/删除分配给指定客户机的用户的 IP 地址。
client-identifier <unique-identifier> no client-identifier	在手工绑定地址时，指定/删除用户的唯一标识。

3.启动记录地址冲突的日志功能

命令	解释
全局配置模式	
ip dhcp conflict logging no ip dhcp conflict logging	打开/关闭 DHCP 服务器检测地址冲突的日志功能。
特权用户配置模式	
clear ip dhcp conflict <address all>	删除单条地址冲突的记录或全部地址的冲突记录。

1.3 DHCP中继配置

当 DHCP 客户机和 DHCP 服务器不在同一个网段时，由 DHCP 中继传递 DHCP 报文。增加 DHCP 中继功能的好处是不必为每个网段都设置 DHCP 服务器，同一个 DHCP 服务器可以为很多个子网的客户机提供网络配置参数，既节约了成本又方便了管理。

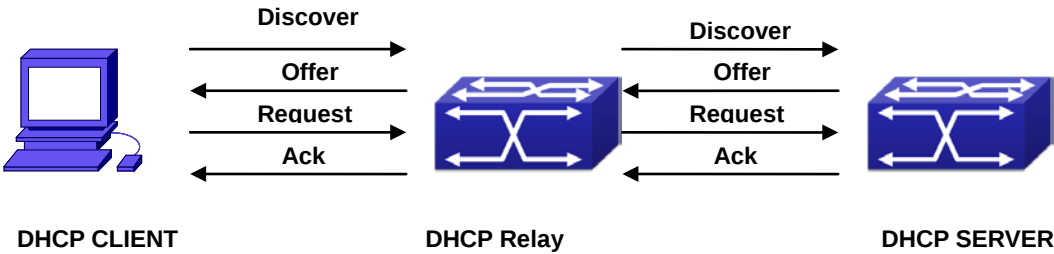


图 1-2 DHCP 中继

如上图所示，DHCP 客户机和 DHCP 服务器不在一个网络内，DHCP 客户机仍然遵循 DHCP 的四个步骤，但增加了 DHCP 中继的转发功能：

1. 首先广播 DHCPDISCOVER 报文，DHCP 中继接收到客户机广播的 DHCPDISCOVER 文后，在该报文的中继代理字段处加入自己的 IP 地址后转发给指定的 DHCP 服务器（有关 DHCP 帧格式可参看 RFC2131）；
2. DHCP 服务器接收到经过 DHCP 中继转发的 DHCPDISCOVER 后，带有网络配置参数的 DHCPOFFER 报文经过 DHCP 中继发送给 DHCP 客户机；
3. DHCP 客户机选中一个 DHCP 服务器，广播 DHCPREQUEST 报文，DHCP 中继处理该报文后转发给 DHCP 服务器；
4. DHCP 服务器收到 DHCPREQUEST 后，回应 DHCPACK 报文经过 DHCP 中继发送给 DHCP 客户机。

DHCP 中继配置任务序列如下：

1. 启动 DHCP 中继
2. 配置 DHCP 中继转发 DHCP 广播报文

1. 启动 DHCP 中继

命令	解释
全局配置模式	
service dhcp no service dhcp	在启动 DHCP 服务器功能的同时也启动了 DHCP 中继功能。

2. 配置 DHCP 中继转发 DHCP 广播报文

命令	解释
全局配置模式	
ip forward-protocol udp bootps no ip forward-protocol udp bootps	中继转发 UDP 端口号为 67 的 DHCP 广播报文。
接口配置模式	
ip helper-address <ipaddress> no ip helper-address <ipaddress>	指定 DHCP 中继转发的目标 IP 地址；本命令的 no 操作为取消该项配置。

1.4 DHCP 配置举例

案例 1:

为减轻网络管理员和用户的配置负担，现有某公司将交换机作为 DHCP 服务器。其 Admin VLAN 的 IP 地址为 10.16.1.2/24。其中公司局域网因为办公地点分成了 A 地、B 地两部分，A 地、B 地的网络配置如下表。

PoolA(network 10.16.1.0)		PoolB(network 10.16.2.0)	
设备	IP 地址	设备	IP 地址

缺省网关	10.16.1.200 10.16.1.201	缺省网关	10.16.2.200 10.16.2.201
DNS 服务器	10.16.1.202	DNS 服务器	10.16.2.202
Wins 服务器	10.16.1.209	WWW 服务器	10.16.2.209
Wins 的节点类型	H-node		
Lease	3 天	Lease	1 天

其中在 A 处，因为工作的需要，特地将一台 MAC 地址为 00-03-22-23-dc-ab 的机器分配固定的 IP 地址 10.16.1.210，命名为 management。

```
Switch(config)#service dhcp
Switch(config)#interface vlan 1
Switch(Config-if-Vlan-1)#ip address 10.16.1.2 255.255.255.0
Switch(Config-if-Vlan-1)#exit
Switch(config)#ip dhcp pool A
Switch(dhcp-A-config)#network 10.16.1.0 24
Switch(dhcp-A-config)#lease 3
Switch(dhcp-A-config)#default-router 10.16.1.200 10.16.1.201
Switch(dhcp-A-config)#dns-server 10.16.1.202
Switch(dhcp-A-config)#netbios-name-server 10.16.1.209
Switch(dhcp-A-config)#netbios-node-type H-node
Switch(dhcp-A-config)#exit
Switch(config)#ip dhcp excluded-address 10.16.1.200 10.16.1.201
Switch(config)#ip dhcp pool B
Switch(dhcp-B-config)#network 10.16.2.0 24
Switch(dhcp-B-config)#lease 1
Switch(dhcp-B-config)#default-router 10.16.2.200 10.16.2.201
Switch(dhcp-B-config)#dns-server 10.16.2.202
Switch(dhcp-B-config)#option 72 ip 10.16.2.209
Switch(dhcp-config)#exit
Switch(config)#ip dhcp excluded-address 10.16.2.200 10.16.2.201
Switch(config)#ip dhcp pool A1
Switch(dhcp-A1-config)#host 10.16.1.210
Switch(dhcp-A1-config)#hardware-address 00-03-22-33-dc-ab
Switch(dhcp-A1-config)#exit
```

使用提示：

当有 DHCP/BOOTP Client 连接在交换机的属于 VLAN1 端口时，该 Client 只能获取属于 10.16.1.0/24 网段的地址而不可能获取 10.16.2.0/24 网段的地址。因为 Client 发出的广播包经过交换机的 VLAN 接口转发后，申请的是与 VLAN 接口在一个网段的 IP 地址，交换机的 VLAN 接口的 IP 地址为 10.16.1.2/24，因此 Client 申请到的 IP 地址是 10.16.1.0/24 网段的。

若 DHCP/BOOTP Client 希望申请到 10.16.2.0/24 网段的地址, 该 Client 发出的广播包经由转发的网关必须是 10.16.2.0/24 网段的。若要从交换机获取 10.16.2.0/24 地址池的 IP 地址, 则首先要保证该 Client 的网关到交换机的可达性。

案例 2:

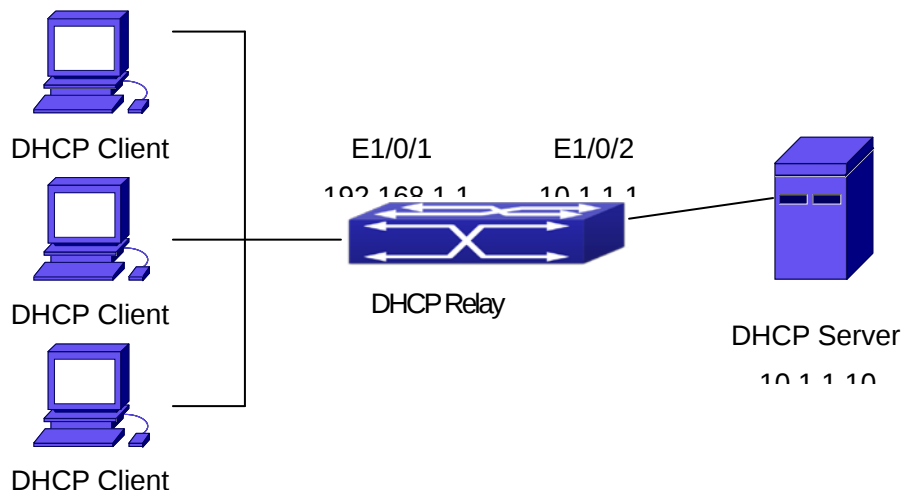


图 1-3 DHCP Relay 配置

如图所示, 配置 Switch 为 DHCP 中继。DHCP 服务器的地址为 10.1.1.10, 则配置如下:

```
Switch(config)#service dhcp
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 192.168.1.1 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#vlan 2
Switch(Config-Vlan2)#exit
Switch(config)#interface Ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#switchport access vlan 2
Switch(Config-If-Ethernet1/0/2)#exit
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ip address 10.1.1.1 255.255.255.0
Switch(Config-if-Vlan2)#exit
Switch(Config)#ip forward-protocol udp bootps
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip helper-address 10.1.1.10
Switch(Config-if-Vlan1)#exit
```

注意: 建议配置命令 **ip forward-protocol udp bootps** 和 **ip helper-address**

<ipaddress> 结合使用。**ip helper-address** 只能在三层端口下配置，不能直接在二层端口下配置。

1.5 DHCP排错帮助

DHCP 客户机无法获得 IP 地址及其它网络参数，在确保 DHCP 客户机硬件、线缆等没有问题的前提下，检查可能存在的情况和建议的解决方法：

- ☞ 首先检查 DHCP 服务器是否已启动，若没有启动，建议启动相关的 DHCP 服务器；若 DHCP 客户机和服务器不在同一个物理网络中，检查中间负责转发 DHCP 报文的路由器是否具备 DHCP 中继功能。若中间路由器不具备 DHCP 中继功能，建议替换掉中间的路由器或更新版本，使其具备 DHCP 中继功能；
- ☞ 用户比较容易遇到的现象是 DHCP 客户机连接在交换机上，却获得不到 IP 地址。遇到这种情况请检测 DHCP Server 内是否有与交换机 VLAN 接口在一个网段的地址池，如没有则请添加该网段的地址池；
- ☞ 在 DHCP 服务中，动态分配 IP 地址与手工分配 IP 地址的地址池是互斥的，即如果在一个地址池执行命令 **network** 和命令 **host** 时，只能有一个生效；并且在手工地址池中一个地址池内只能配置一对 IP-MAC 的绑定，如果需要建立多对绑定，可以建立多个手工地址池，在每个地址池分别配置 IP-MAC 的绑定，否则在同一地址池内配置新的配置会覆盖旧的配置。

第2章 DHCPv6 配置

说明：

本章所指的三层交换机和路由器代表了一般意义下的路由器或运行了路由协议的无线控制产品。

2.1 DHCPv6 简介

DHCPv6 是动态主机配置协议（DHCP）的 IPv6 版本，协议基本规范由 RFC3315 定义。DHCPv6 服务端可以向 DHCPv6 客户端分配 IPv6 地址以及 DNS 地址和域名等配置参数。相对于 IPv6 无状态地址自动配置协议，DHCPv6 属于一种有状态地址自动配置协议。在有状态地址配置过程中，DHCPv6 服务器分配一个完整的 IPv6 地址给主机，并提供 DNS 地址和域名等其他配置信息，这中间可能通过中继代理转交 DHCPv6 报文，而且最终服务器能把分配的 IPv6 地址和客户端的绑定关系记录在案，从而增强了网络的可管理性；DHCPv6 服务器也能提供无状态 DHCPv6 服务，即不分配 IPv6 地址，仅需向主机提供 DNS 地址和域名等其他配置信息，从而补足了 IPv6 无状态地址自动配置的缺陷；DHCPv6 协议还提供了 DHCPv6 前缀代理的扩展功能，上游路由器可以自动为下游路由器分派地址前缀，从而实现了层次化网络环境中 IPv6 地址的自动规划，解决互联网提供商（ISP）的 IPv6 网络部署问题。

DHCPv6 报文用于客户端、中继代理与服务器三者之间的通信，以完成 DHCPv6 的协议行为。DHCPv6 报文承载于 UDP 协议之上。DHCPv6 客户端使用 UDP 端口 547 向 DHCPv6 服务器或中继代理发送请求报文，DHCPv6 服务器和中继代理使用 UDP 端口 546 向 DHCPv6 客户端发送应答报文。DHCPv6 客户端使用所有 DHCP 中继代理和服务器多播地址(FF02::1:2)发送服务器发现(Solicit)或请求(Request)报文。协议实现的过程如下：

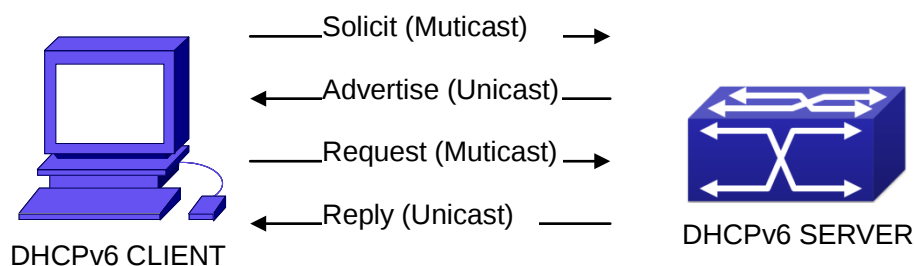


图 2-1 DHCPv6 协议交互过程

当 DHCPv6 客户端向位于同一链路的 DHCPv6 服务器请求分配 IPv6 地址以及其它配置参数时，客户端首先要定位和选择合适的服务器，然后才能向服务器请求分配地址和其它配置参数。

1. 在定位服务器时，客户端向所有 DHCP 中继代理和服务器多播地址 (FF02::1:2) 发出 SOLICIT 消息希望发现合适的 DHCPv6 服务器。
2. 任何能够满足该请求的服务器都会发送一个 ADVERTISE 消息给客户端，其中包

含可分配的配置信息以及服务器的身份标识(DUID)和该服务器的优先值信息。

- 3. 客户端可能接收到多个这样的通告消息，依据某种策略(如选择服务器优先值选项中优先值最高的服务器)选择其中一个服务器，然后向选定服务器发送 REQUEST 消息请求服务器分配通告的 IPv6 地址和其它配置参数。
- 4. 被选择的服务器回应以 REPLY 消息，其中包含确认的 IPv6 地址和其它配置参数，客户端收到 REPLY 消息提取地址和配置参数完成 DHCPv6 配置任务。

通过上面四个步骤，完成动态分配主机配置的协议过程。但如果 DHCPv6 服务器和 DHCPv6 客户机不相邻时，服务器是无法收到客户机发出的 DHCPv6 多播报文，因此服务器也不会给客户机发送任何 DHCPv6 报文，这时需要 DHCPv6 中继代理来转发这些 DHCPv6 报文，完成 DHCPv6 客户机和服务器之间的 DHCPv6 报文交互过程。

交换机实现了 DHCPv6 服务器、DHCPv6 中继的功能和 DHCPv6 前缀代理客户端功能。中继代理节点收到来自客户端的 DHCPv6 消息，重新封装成 Relay-forward 报文转发给 DHCPv6 服务器或下一个中继代理，服务器回应的 DHCPv6 消息被封装成 Relay-reply 报文交给 DHCPv6 中继代理节点，中继代理节点解除最外层中继封装后再转发给 DHCPv6 客户端或下一个中继代理，从而完成客户端与服务器之间的通信。

DHCPv6 前缀代理(Prefix Delegation)机制中，上游网络路由器(PE)启动 DHCPv6 服务器，下游网络路由器(CPE)启动 DHCPv6 前缀代理客户端。此时下游网络路由器不需要再手工指定用户侧链路的 IPv6 地址前缀，它只需要向上游网络路由器提出前缀分配申请，上游网络路由器便可以分配合适的地址前缀给下游路由器。二者之间的报文交互与 DHCPv6 地址分配的过程类似。然后下游路由器把获得的前缀(一般前缀长度小于 64)进一步自动细分成 64 前缀长度的子网网段，把细分的地址前缀再通过路由公告(RA)至与主机直连的用户链路上，实现主机的地址自动配置，从而完成整个系统层次的地址布局。

2.2 DHCPv6 服务器配置

DHCPv6 服务器配置任务序列如下：

- 1. 启动/关闭 DHCPv6 服务
- 2. 配置 DHCPv6 地址池
 - (1) 创建/删除 DHCPv6 地址池
 - (2) 配置 DHCPv6 地址池的参数
- 3. 在接口上启动 DHCPv6 服务器功能

1.启动/关闭 DHCPv6 服务

命令	解释
全局配置模式	
service dhcpv6 no service dhcpv6	启动 DHCPv6 服务。

2. 配置 DHCPv6 地址池

(1) 创建/删除 DHCPv6 地址池

命令	解释
全局配置模式	
ipv6 dhcp pool <poolname> no ipv6 dhcp pool <poolname>	配置 DHCPv6 地址池。

(2) 配置 DHCPv6 地址池的参数

命令	解释
DHCPv6 地址池配置模式	
network-address <ipv6-pool-start-address> {<ipv6-pool-end-address> <prefix-length>} [eui-64] no network-address	配置地址池可分配的 IPv6 地址范围。
dns-server <ipv6-address> no dns-server <ipv6-address>	为 DHCPv6 客户机配置 DNS 服务器地址。
domain-name <domain-name> no domain-name <domain-name>	为 DHCPv6 客户机配置域名。
excluded-address <ipv6-address> no excluded-address <ipv6-address>	排除地址池中不用于动态分配的 IPv6 地址。
lifetime {<valid-time> infinity} {<preferred-time> infinity} no lifetime	配置 DHCPv6 地址池动态分配地址或前缀的生存期。

3. 在接口上启动 DHCPv6 服务器功能

命令	解释
接口配置模式	
ipv6 dhcp server <poolname> [preference<value>] [rapid-commit] [allow-hint] no ipv6 dhcp server <poolname>	在指定接口上启动 DHCPv6 服务器功能，并绑定使用的 DHCPv6 地址池。

2.3 DHCPv6 中继代理配置

DHCPv6 中继代理配置任务序列如下：

1. 启动/关闭 DHCPv6 服务
2. 在接口上配置 DHCPv6 中继代理

1. 启动 DHCPv6 服务

命令	解释
全局配置模式	
service dhcpv6 no service dhcpv6	启动 DHCPv6 服务。

2. 在接口上配置 DHCPv6 中继代理

命令	解释
接口配置模式	
ipv6 dhcp relay destination {[<ipv6-address>] [interface {<interface-name> vlan <1-4096>}]} no ipv6 dhcp relay destination {[<ipv6-address>] [interface {<interface-name> vlan <1-4096>}]}	指定 DHCPv6 中继转发的目的地址；本命令的 no 操作为取消该项配置。

2.4 DHCPv6 前缀代理服务器端配置

DHCPv6 前缀代理服务器端配置任务序列如下：

1. 启动/关闭 DHCPv6 服务
2. 配置代理前缀池
3. 配置 DHCPv6 地址池
 - (1) 创建/删除 DHCPv6 地址池
 - (2) 配置 DHCPv6 地址池使用的代理前缀池
 - (3) 配置静态代理前缀绑定
 - (4) 配置 DHCPv6 地址池其它参数
4. 在接口上启动 DHCPv6 前缀代理服务器功能

1. 启动/关闭 DHCPv6 服务

命令	解释
全局配置模式	
service dhcpv6 no service dhcpv6	启动 DHCPv6 服务。

2. 配置代理前缀池

命令	解释
全局配置模式	

ipv6 local pool <poolname> <prefix/prefix-length> <assigned-length> no ipv6 local pool <poolname>	配置代理前缀池。
--	----------

3. 配置 DHCPv6 地址池

(1) 创建/删除 DHCPv6 地址池

命令	解释
全局配置模式	
ipv6 dhcp pool <poolname> no ipv6 dhcp pool <poolname>	配置 DHCPv6 地址池。

(2) 配置 DHCPv6 地址池使用的代理前缀池

命令	解释
DHCPv6 地址池配置模式	
prefix-delegation pool <poolname> [lifetime {<valid-time> infinity} {<preferred-time> infinity}] no prefix-delegation pool <poolname>	指定 IDHCPv6 地址池使用的代理前缀池，从该前缀池中分配可用的前缀给客户端。

(3) 配置静态代理前缀绑定

命令	解释
DHCPv6 地址池配置模式	
prefix-delegation <ipv6-prefix/prefix-length> <client-DUID> [iaid <iaid>] [lifetime {<valid-time> infinity} {<preferred-time> infinity}] no prefix-delegation <ipv6-prefix/prefix-length> <client-DUID> [iaid <iaid>]	指定 IPv6 前缀与某个前缀请求客户端静态绑定。

(4) 配置 DHCPv6 地址池其他参数

命令	解释
DHCPv6 地址池配置模式	
dns-server <ipv6-address> no dns-server <ipv6-address>	为 DHCPv6 客户机配置 DNS 服务器地址。
domain-name <domain-name> no domain-name <domain-name>	为 DHCPv6 客户机配置域名。

4. 在接口上启动 DHCPv6 服务器功能

命令	解释
接口配置模式	
ipv6 dhcp server <poolname> [preference <value>] [rapid-commit] [allow-hint] no ipv6 dhcp server <poolname>	在指定接口上启动 DHCPv6 服务器功能，并绑定使用的 DHCPv6 地址池。

2.5 DHCPv6 前缀代理客户端配置

DHCPv6 前缀代理客户端配置任务序列如下：

1. 启动/关闭 DHCPv6 服务
2. 在接口上启动 DHCPv6 前缀代理客户端功能

1. 启动/关闭 DHCPv6 服务

命令	解释
全局配置模式	
service dhcpv6 no service dhcpv6	启动 DHCPv6 服务。

2. 在接口上启动 DHCPv6 前缀代理客户端功能

命令	解释
接口配置模式	
ipv6 dhcp client pd <prefix-name> [rapid-commit] no ipv6 dhcp client pd	在指定接口上启动客户端前缀代理请求功能，获取的前缀与设置的通用前缀名关联。

2.6 DHCPv6 配置举例

案例 1:

在部署全 IPv6 校园网时，若使用专门的服务器进行 IPv6 地址的统一分配和管理，则可以使用路由交换设备的 DHCPv6 服务器功能进行 IPv6 地址分派。DHCPv6 服务器同时支持有状态与无状态 DHCPv6。

网络拓扑:

接入层使用二层接入设备 Switch1，连接宿舍楼栋的用户；一级汇聚层使用汇聚设备 Switch2 做 DHCPv6 中继代理；二级汇聚层使用汇聚设备 Switch3 做 DHCPv6 服务器，并与骨干网或更高的汇聚层设备相连；用户 PC 端一般装有 Windows Vista 操作系统，具有

DHCPv6 客户端。

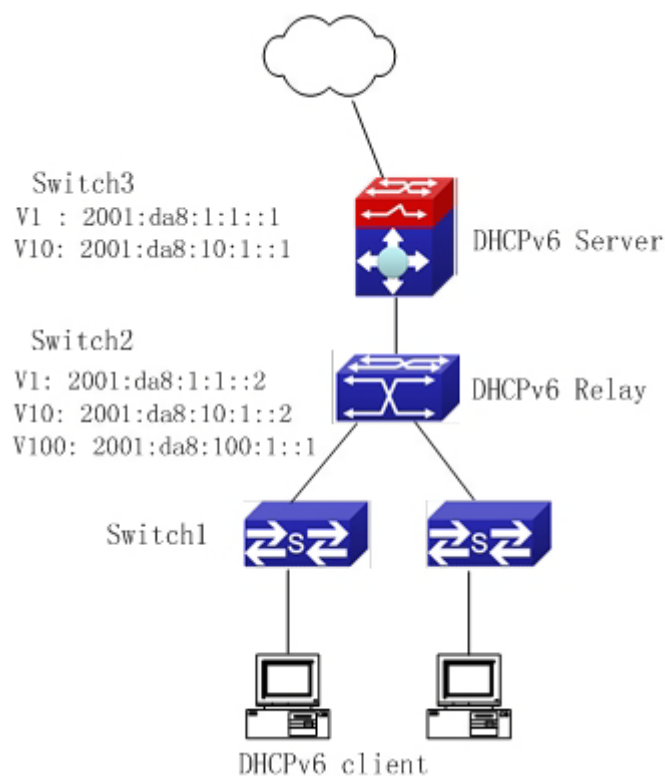


图 2-2 DHCPv6 配置举例示意图 1

使用提示:

Switch3 配置:

Switch3>enable

Switch3#config

Switch3(config)#service dhcpv6

Switch3(config)#ipv6 dhcp pool EastDormPool

Switch3(dhcpv6-EastDormPool-config)#network-address 2001:da8:100:1::1
2001:da8:100:1::100

Switch3(dhcpv6-EastDormPool-config)#excluded-address 2001:da8:100:1::1

Switch3(dhcpv6-EastDormPool-config)#dns-server 2001:da8::20

Switch3(dhcpv6-EastDormPool-config)#dns-server 2001:da8::21

Switch3(dhcpv6-EastDormPool-config)#domain-name dhcpv6.com

Switch3(dhcpv6-EastDormPool-config)#lifetime 1000 600

Switch3(dhcpv6-EastDormPool-config)#exit

Switch3(config)#interface vlan 1

Switch3(Config-if-Vlan1)#ipv6 address 2001:da8:1:1::1/64

Switch3(Config-if-Vlan1)#exit

Switch3(config)#interface vlan 10

```
Switch3(Config-if-Vlan10)#ipv6 address 2001:da8:10:1::1/64
Switch3(Config-if-Vlan10)#ipv6 dhcp server EastDormPool preference 80
Switch3(Config-if-Vlan10)#exit
Switch3(config)#
```

Switch2 配置:

```
Switch2>enable
Switch2#config
Switch2(config)#service dhcpv6
Switch2(config)#interface vlan 1
Switch2(Config-if-Vlan1)#ipv6 address 2001:da8:1:1::2/64
Switch2(Config-if-Vlan1)#exit
Switch2(config)#interface vlan 10
Switch2(Config-if-Vlan10)#ipv6 address 2001:da8:10:1::2/64
Switch2(Config-if-Vlan10)#exit
Switch2(config)#interface vlan 100
Switch2(Config-if-Vlan100)#ipv6 address 2001:da8:100:1::1/64
Switch2(Config-if-Vlan100)#no ipv6 nd suppress-ra
Switch2(Config-if-Vlan100)#ipv6 nd managed-config-flag
Switch2(Config-if-Vlan100)#ipv6 nd other-config-flag
Switch2(Config-if-Vlan100)#ipv6 dhcp relay destination 2001:da8:10:1::1
Switch2(Config-if-Vlan100)#exit
Switch2(config)#
```

案例 2:

运营商在部署层次化的 IPv6 网络时, 不再需要为网络下游的路由交换设备手工配置 IPv6 地址, 可以通过前缀代理机制, 实现层次化 IPv6 网络的自动配置:

1. 配置上游路由交换设备为 DHCPv6 前缀代理服务器, 维护一个保存已分配前缀与下游设备 DUID 关联信息的本地数据库;
2. 配置下游路由交换设备为前缀代理客户端, 通过与前缀代理服务器进行类似 DHCPv6 地址分配相似的交互, 获得长度小于 64 的 IPv6 地址前缀;
3. 获得前缀的下游接入设备与用户 PC 处于同一链路的接口通过路由公告(RA)告知接入用户所在链路的前缀信息, 用户的 PC 机进一步通过无状态地址自动配置获取 IPv6 地址; 同时, 该接口配置无状态 DHCPv6 服务器, 为 DHCPv6 client 提供 DNS、Domain name 信息。

网络拓扑:

下游路由交换设备使用接入设备 Switch1, 与上游路由交换设备相连的接口配置前缀代理客户端, 与用户 PC 处于同一链路的接口配置无状态 DHCPv6 服务器, 为 PC 提供无状态信息 (如 DNS、domain name 等), 并开启无状态地址自动配置的路由公告; 上游路由交换设备使用汇聚设备 Switch2, 配置前缀代理服务器, 开启有状态地址自动配置的路由公

告；用户 PC 端一般装有 Windows Vista 操作系统，具有 DHCPv6 客户端。

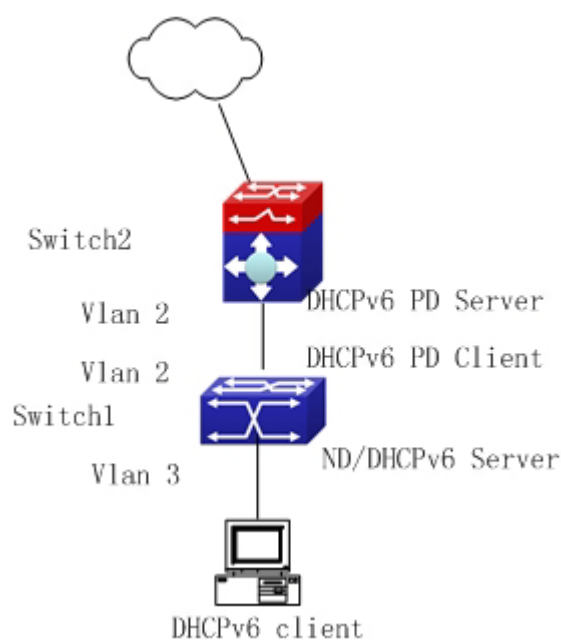


图 2-3 DHCPv6 配置举例示意图 2

使用提示：

Switch2 配置

```
Switch2>enable
```

```
Switch2#config
```

```
Switch2(config)#interface vlan 2
```

```
Switch2(Config-if-Vlan2)#ipv6 address 2001:da8:1100::1/64
```

```
Switch2(Config-if-Vlan2)#exit
```

```
Switch2(config)#service dhcpv6
```

```
Switch2(config)#ipv6 local pool client-prefix-pool 2001:da8:1800::/40 48
```

```
Switch2(config)#ipv6 dhcp pool dhcp-pool
```

```
Switch2(dhcpv6-dhcp-pool-config)#prefix-delegation pool client-prefix-pool 1800 600
```

```
Switch2(dhcpv6-dhcp-pool-config)#exit
```

```
Switch2(config)#interface vlan 2
```

```
Switch2(Config-if-Vlan2)#ipv6 dhcp server dhcp-pool
```

```
Switch2(Config-if-Vlan2)#exit
```

Switch1 配置

```
Switch1>enable
```

```
Switch1#config
```

```
Switch1(config)#service dhcpv6
```

```
Switch1(config)#interface vlan 2
```

```
Switch1(Config-if-Vlan2)#ipv6 dhcp client pd prefix-from-provider
```

```
Switch1(Config-if-Vlan2)#exit
Switch1(config)#interface vlan 3
Switch1(Config-if-Vlan3)#ipv6 address prefix-from-provider 0:0:0:1::1/64
Switch1(Config-if-Vlan3)#exit
Switch1(config)#ipv6 dhcp pool foo
Switch1(dhcpv6-foo-config)#dns-server 2001:4::1
Switch1(dhcpv6-foo-config)#domain-name www.ipv6.org
Switch1(dhcpv6-foo-config)#exit
Switch1(config)#interface vlan 3
Switch1(Config-if-Vlan3)#ipv6 dhcp server foo
Switch1(Config-if-Vlan3)#ipv6 nd other-config-flag
Switch1(Config-if-Vlan3)#no ipv6 nd suppress-ra
Switch1(Config-if-Vlan3)#exit
```

2.7 DHCPv6 排错帮助

DHCPv6 客户机无法获得 IPv6 地址及其它网络参数, 在确保 DHCPv6 客户机硬件、线缆等没有问题的前提下, 检查可能存在的情况和建议的解决方法:

- ☞ 首先检查全局 DHCPv6 服务是否已启动, 若没有启动, 请启动全局 DHCPv6 服务与相关接口上的 DHCPv6 功能;
- ☞ 若 DHCPv6 客户机和服务器不在同一个物理网络中, 检查中间负责转发 DHCPv6 报文的路由器是否具备 DHCPv6 中继功能。若中间路由器不具备 DHCPv6 中继功能, 建议替换掉中间的路由器或更新版本, 使其具备 DHCPv6 中继功能;
- ☞ 用户比较容易遇到的现象是 DHCPv6 客户机连接在启动了 DHCPv6 服务器功能的交换机上, 却获得不到 IPv6 地址。遇到这种情况请首先确定 DHCPv6 客户机是否直连在启动 DHCPv6 服务器的接口上, 若是直连, 则判断该接口 VLAN 的 IPv6 地址是否与本接口上启动的 DHCPv6 服务器地址池在同一个网段, 如没有则请添加该网段至地址池; 若不是直连, 而且通过了其它启动了 DHCPv6 中继代理的三层交换机接入到 DHCPv6 服务器, 则请判断 DHCPv6 客户机所在链路的交换机接口是否配置了 IPv6 地址, 若没有配置 IPv6 地址, 建议配置该接口 IPv6 地址。若该接口配置了地址, 则进一步判断接口的 IPv6 地址是否在 DHCPv6 服务器地址池的网段之内, 如没有则请添加该网段至地址池。

第3章 DHCP option 60 和option 43

3.1 DHCP option 60 和option 43 介绍

DHCP 服务器解析来自 DHCP 客户端的 DHCP 报文，若报文中包含 option 60，则根据该 option 60 的内容以及 DHCP 服务器地址池中对 option 60 和 option 43 的配置来判断返回 option 43 给 DHCP 客户端。

在 DHCP 服务器地址池模式下配置相应的 option 60 和 option 43。

1. 地址池中同时配置了 option 60 和 option 43，若收到来自 DHCP 客户端的 DHCP 报文中可以解析到 option 60，与 DHCP 服务器地址池中的 option 60 比较，若匹配则返回该地址池中配置的 option 43 给 DHCP 客户端，若不匹配则不返回 option43 给 DHCP 客户端
2. 地址池中仅配置了 option 43 选项，则默认匹配任何内容的 option 60，若收到的来自 DHCP 客户端的 DHCP 报文中可以解析到 option 60，直接返回地址池中配置的 option 43 给 DHCP 客户端
3. 地址池中仅配置了 option 60 选项，则不会返回 option 43 给 DHCP 客户端

3.2 DHCP option 60 和option 43 配置任务序列

1. DHCP option 60 和 option 43 基本功能配置

命令	解释
地址池配置模式下	
option 60 ascii LINE	在 ip dhcp pool 模式下以 ascii 格式配置 option 60 字符串。
option 43 ascii LINE	在 ip dhcp pool 模式下以 ascii 格式配置 option 43 字符串。
option 60 hex WORD	在 ip dhcp pool 模式下以 hex 格式配置 option 60 字符串。
option 43 hex WORD	在 ip dhcp pool 模式下以 hex 格式配置 option 43 字符串。
option 60 ip A.B.C.D	在 ip dhcp pool 模式下以 IP 格式配置 option 60 字符串。
option 43 ip A.B.C.D	在 ip dhcp pool 模式下以 IP 格式配置 option 43 字符串。
no option 60	在地址池模式下删除配置的 option 60。
no option 43	在地址池模式下删除配置的

	option 43。
--	------------

3.3 DHCP option 60 和option 43 举例

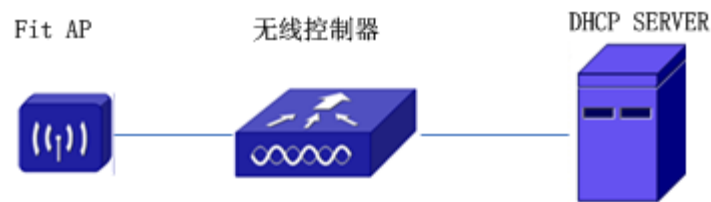


图 3-1 DHCP option 60 和 option 43 功能典型组网图

Fit AP 通过 DHCP server 获取 IP 地址、option 43 属性(此属性中携带无线控制器的 IP 地址信息), 然后向无线控制器发送单播发现请求。DHCP SERVER 通过配置匹配 fit ap 中的 option 60 选项来返回 option 43 属性给 FIT AP。DHCP option 43 携带的无线控制器地址为 192.168.10.5 和 192.168.10.6。

DHCP Server 配置

配置步骤:

```
# 配置 DHCP server
switch(config)#ip dhcp pool a
switch (dhcp-a-config)#option 60 ascii AP1000
switch (dhcp-a-config)#option 43 hex 0104C0A80A050104C0A80A06
```

DCWL-7900 系列 AP 还可以通过 option 43 属性获取无线控制器的域名信息，FIT AP 通过 DNS server 解析域名后，向无线控制器发送单播发现请求。Option 43 字段，第一位若为 01，代表无线控制地址为 IP 地址形式，若为 02 则代表无线控制器地址为域名形式，第二位为相应 IP 地址或者域名的长度。DHCP option 43 携带的无线控制器域名为 www.test.com 和 123.com。DHCP Server 配置配置步骤:

```
# 配置 DHCP server
switch(config)#ipdhcp pool a
switch (dhcp-a-config)#option 60 asciiudhcp 1.18.2
switch (dhcp-a-config)#option 43 hex 020C7777772E746573742E636F6D020731323332E636F6D
```

3.4 DHCP option 60 和option 43 排错帮助

当配置 DHCP option 60 和 option 43 功能出现问题时，请检查是否是如下原因:

- ☞ 是否开启 service dhcp 功能
- ☞ 地址池中若配置了 option 60，是否与报文中的 option 60 匹配

第4章 DHCP option 82 配置

说明：
本章所指的三层交换机代表了一般意义下的路由器或运行了路由协议的无线控制产品。

4.1 DHCP option 82 介绍

DHCP option 82 是 DHCP 报文中的中继代理信息选项（Relay Agent Information Option），其选项编号为 82。DHCP option 82 是为了增强 DHCP 服务器的安全性，改善 IP 地址配置策略而提出的一种机制。通过在网络接入设备上配置 DHCP 中继代理功能，中继代理把从客户端接收到的 DHCP 请求报文添加进 option 82 选项（其中包含了客户端的接入物理端口和接入设备标识等信息），然后再把该报文转发给 DHCP 服务器，支持 option 82 功能的 DHCP 服务器接收到报文后，根据预先配置策略和报文中 option 82 信息分配 IP 地址和其它配置信息给客户端，同时 DHCP 服务器也可以依据 option 82 中的信息识别可能的 DHCP 攻击报文并作出防范。DHCP 中继代理收到服务器应答报文后，剥离其中的 option 82 选项并根据选项中的物理端口信息，把应答报文转交到网络接入设备的指定端口。DHCP option82 的应用对客户端是透明的。

4.1.1 DHCP option 82 报文结构

DHCP 报文可以由多个 option 字段组成，option 82 就是其中的一种 option，它必须在其它选项之后，option255 选项之前。其格式如下图所示：

Code	Len	Agent Information Field					
82	N	i1	i2	i3	i4	...	iN

Code: 表示中继代理信息选项的序号，RFC3046 定义为 82，option 82 即由此得名。
Len: 为代理信息域（Agent Information Field）的字节个数，不包括 Code 和 Len 字段的两个字节。

option 82 可以由多个 sub-option 组成，每个 option 82 选项至少要有一个子选项，RFC3046 定义了以下两个子选项，其格式如下图所示：

SubOpt	Len	Sub-option Value					
1	N	s1	s2	s3	s4	...	sN

SubOpt	Len	Sub-option Value					
2	N	i1	i2	i3	i4	...	iN

SubOpt: 为子选项编号, 其中代理电路 ID (即 Circuit ID) 子选项编号为 1, 代理远程 ID (即 Remote ID) 子选项编号为 2。

Len: 为 Sub-option Value 的字节个数, 不包括 SubOpt 和 Len 字段的两个字节。

4.1.2 option 82 工作机制

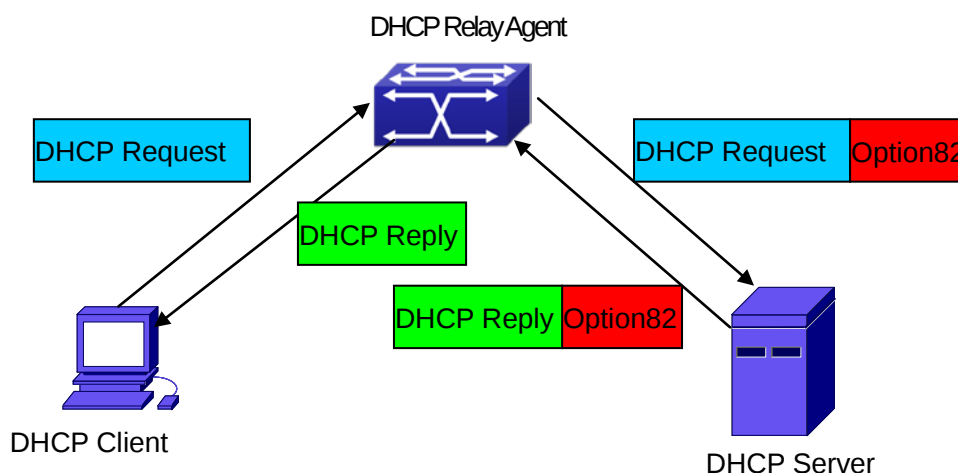


图 4-1 DHCP option 82 流程图

在 DHCP 中继代理支持 option 82 的情况下, DHCP 客户端通过 DHCP 中继从 DHCP 服务器获取 IP 地址同样要经历发现、提供、选择和确认四个阶段。这时 DHCP 协议按如下过程进行:

- 1) DHCP 客户端在初始化时广播发送请求报文, 这时的请求报文并不包含 option 82 选项。
- 2) DHCP 中继代理将 option 82 选项添加到接收到的请求报文尾部后中继转发给 DHCP 服务器。option 82 选项的子选项 1(代理电路 ID)默认是 DHCP 客户端所连接的交换机的接口信息(VLan 名加物理端口名), 也可以由用户自己配置代理电路 ID, option 82 选项的子选项 2(代理远程 ID)是 DHCP 中继设备本身的 MAC 地址。
- 3) DHCP 服务器收到 DHCP 中继设备转发的 DHCP 请求报文后, 根据报文中 option 选项所携带的信息和预定策略分配 IP 地址和其它信息给客户端, 然后将带着 DHCP 配置信息以及 option 82 信息的应答报文发给 DHCP 中继代理。
- 4) DHCP 中继代理收到 DHCP 服务器的应答报文后将剥离报文中的 option 82 信息, 然后将带有 DHCP 配置信息的报文转发给 DHCP 客户端。

4.2 DHCP option 82 的配置任务序列

与 DHCP option 82 相关的配置内容

- 1) 配置中继代理的 DHCP option 82 使能开关
- 2) 配置接口的 DHCP option 82 属性
- 3) 配置服务器的 DHCP option 82 使能开关

- 4) 配置中继代理的 DHCP option 82 默认格式
- 5) 配置分隔符
- 6) 配置 option82 的生成方式
- 7) DHCP option 82 的维护与诊断

1) 配置中继代理的 DHCP option 82 使能开关

命令	解释
全局配置模式	
ip dhcp relay information option no ip dhcp relay information option	设置本命令启用交换机中继代理的 option82 功能，本命令的 no 操作关闭交换机中继代理的 option82 功能。

2) 配置接口的 DHCP option 82 属性

命令	解释
接口配置模式	
ip dhcp relay information policy {drop keep replace} no ip dhcp relay information policy	本命令用于设置系统对于接收到的含有 option82 选项的 DHCP 请求报文的重转发策略，其中 drop 模式表示如果报文中含有 option82 选项，则系统丢弃该 DHCP 报文不作处理；keep 模式表示系统保持现有报文中的 option82 选项不变转发给服务器处理；replace 模式表示系统使用自己的 option82 选项替换现有报文中的 option82 选项，然后转发给服务器处理。本命令的 no 操作设置 option82 选项 DHCP 报文的重转发策略为 replace。
ip dhcp relay information option subscriber-id {standard <circuit-id>} no ip dhcp relay information option subscriber-id	本命令用于设置从接口接收的 DHCP 请求报文添加 option 82 子选项 1(电路 ID 选项)的形式， standard 表示标准的 vlan 名加物理端口名形式，如“Vlan2+Ethernet1/0/12”， <circuit-id> 为用户自己指定的 option 82 的 circuit-id 内容，它是一个长度小于 64 的字符串。本命令的 no 操作把添加 option 82 子选项 1(电路 ID 选项)的形式设置为 standard 形式。
全局配置模式	

ip dhcp relay information option remote-id {standard <remote-id>} no ip dhcp relay information option remote-id	本命令用于设置从接口接收的 DHCP 请求报文添加 option 82 子选项 2(远程 ID 选项)的具体内容。本命令的 no 操作把添加 option 82 子选项 2(远程 ID 选项)的形式设置为 standard。
--	--

3) 配置服务器的 DHCP option 82 使能开关

命令	解释
全局配置模式	
ip dhcp server relay information enable no ip dhcp server relay information enable	本命令用于设置交换机 DHCP 服务器支持对 option82 选项的识别。本命令的 no 操作使服务器忽略处理 option 82 选项。

4) 配置中继代理的 DHCP option 82 默认格式

命令	解释
全局配置模式	
ip dhcp relay information option subscriber-id format {hex acsii vs-hp}	本命令设置交换机中继代理的 option82 功能 subscriber-id 默认格式。
ip dhcp relay information option remote-id format {default vs-hp}	本命令设置交换机中继代理的 option82 功能 remote-id 默认格式。

5) 配置分隔符

命令	解释
全局配置模式	
ip dhcp relay information option delimiter [colon dot slash space] no ip dhcp relay information option delimiter	配置用户在全局定义的用来生成 option82 子选项的各参数的分隔符，该命令的 no 形式恢复分隔符为默认值，即 slash。

6) 配置 option82 的生成方式

命令	解释
全局配置模式	
ip dhcp relay information option self-defined remote-id {hostname mac string WORD} no ip dhcp relay information option self-defined remote-id	配置 option82 的生成方式，用户可以自定义用来生成 option82 子选项 remote-id 的参数（集）。
ip dhcp relay information option self-defined remote-id format [ascii hex]	配置 relay option82 中 remote-id 的生成格式。

<code>ip dhcp relay information option self-defined subscriber-id {vlan port id (switch-id (mac hostname) remote-mac)} string WORD }</code> <code>no ip dhcp relay information option self-defined subscriber-id</code>	配置 option82 的生成方式，用户可以自定义用来生成 option82 子选项 circuit-id 的参数（集）。
<code>ip dhcp relay information option self-defined subscriber-id format [ascii hex]</code>	配置 relay option82 中 circuit-id 的生成格式。

7) DHCP option 82 的维护与诊断

命令	解释
特权配置模式	
<code>show ip dhcp relay information option</code>	本命令显示系统 DHCP option 82 的状态信息，包括 option82 使能开关，接口重转发策略，接口电路 ID 模式，以及交换机 DHCP 服务器 option82 使能开关。
<code>debug ip dhcp relay packet</code>	使用本命令显示 DHCP 中继代理处理数据包的信息，包括 option 82 选项的添加和剥离动作信息。

4.3 DHCP option 82 应用举例

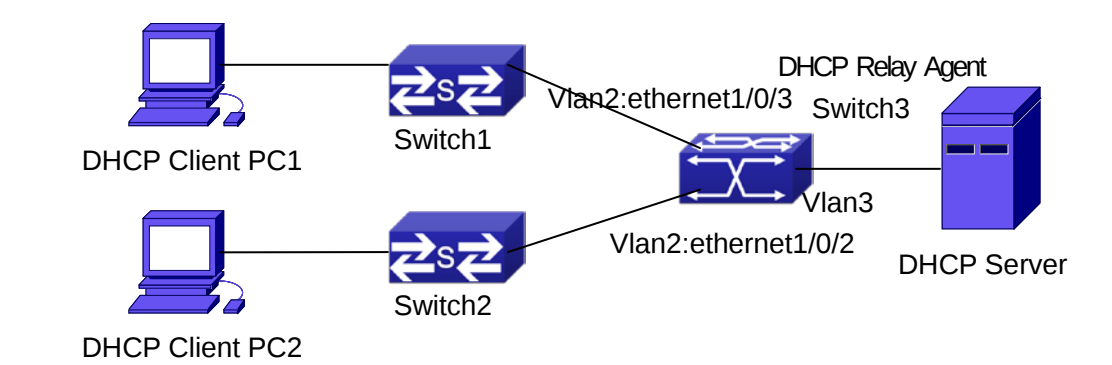


图 4-2 DHCP option 82 典型应用案例

在上面应用案例中，二层交换机 Switch1 和 Switch2 都接在三层交换机 Switch3 上，Switch3 作为 DHCP 中继代理向 DHCP 服务器转交来自 DHCP 客户端的请求报文，并把服务器的应答报文转交给 DHCP 客户端，完成 DHCP 协议过程。在不启用 DHCP option 82 功能时，DHCP 服务器无法区分 DHCP 客户端是来自 Switch1 还是 Switch2 下连的网络，因此 Switch1 和 Switch2 连接的 PC 终端都从 DHCP 服务器中公用地址池中分配地址。启用 DHCP

option 82 功能以后, 由于 Switch3 在来自客户端的请求报文中附加了接入 Switch3 的端口信息, 这时服务器可以区分客户端是来自 Switch1 还是 Switch2 的网络, 因此可以为这两个网络分配互相隔离的地址空间, 便于网络管理。

Switch3(MAC 地址为 00:03:0f:02:33:01)配置如下

```
Switch3(Config)#service dhcp
Switch3(Config)#ip dhcp relay information option
Switch3(Config)#ip forward-protocol udp bootps
Switch3(Config)#interface vlan 3
Switch3(Config-if-vlan3)#ip address 192.168.10.222 255.255.255.0
Switch3(Config-if-vlan2)#ip address 192.168.102.2 255.255.255.0
Switch3(Config-if-vlan2)#ip helper 192.168.10.88
```

Linux 的 ISC DHCP Server 支持 option 82 选项, 其配置文件/etc/dhcpd.conf 为

```
ddns-update-style interim;
ignore client-updates;
```

```
class "Switch3Vlan2Class1" {
match if option agent.circuit-id = "Vlan2+Ethernet1/0/2" and option
agent.remote-id=00:03:0f:02:33:01;
}
```

```
class "Switch3Vlan2Class2" {
match if option agent.circuit-id = "Vlan2+Ethernet1/0/3" and option
agent.remote-id=00:03:0f:02:33:01;
}
```

```
subnet 192.168.102.0 netmask 255.255.255.0 {
option routers 192.168.102.2;
option subnet-mask 255.255.255.0;
option domain-name "example.com.cn";
option domain-name-servers 192.168.10.3;
authoritative;
```

```
pool {
range 192.168.102.21 192.168.102.50;
default-lease-time 86400; #24 Hours
max-lease-time 172800; #48 Hours
```

```
allow members of "Switch3Vlan2Class1";  
}  
pool {  
range 192.168.102.51 192.168.102.80;  
default-lease-time 43200; #12 Hours  
max-lease-time 86400; #24 Hours  
allow members of "Switch3Vlan2Class2";  
}  
}
```

这时 DHCP 服务器会为经 Switch3 中继来自 Switch1 的网络节点分配 192.168.102.21～192.168.102.50 之间的地址，为来自 Switch1 的网络节点分配 192.168.102.51～192.168.102.80 之间的地址。

4.4 DHCP option 82 排错帮助

- ☞ DHCP option 82 是作为 DHCP 中继代理的一个子功能模块实现的，在使用 option 82 功能之前，要确保 DHCP 中继代理正确配置。
- ☞ DHCP option 82 是 DHCP 中继代理和 DHCP 服务器共同配合完成 IP 地址分配任务，DHCP 服务器要针对中继代理的网络拓扑，正确设置分配策略，否则即使中继代理的 option 82 工作正常，地址分配也不会成功进行。在存在多种中继代理情况时，注意设置好接口 DHCP 请求报文的重转发策略。
- ☞ 对于 DHCP 中继代理的 option 82 功能实现，运行过程中可以使用 `debug ip dhcp relay packet` 命令显示中继代理的数据包处理过程，包括添加 option 82 的具体内容，采取的重转发策略，中继代理剥离服务器的 option 82 内容等，这些信息有助于用户排错诊断。
- ☞ 对于 DHCP 服务器的 option 82 功能实现，运行过程中可以使用 `debug ip dhcp server packet` 命令显示服务器的数据包处理过程，包括显示识别出请求包的 option 82 信息，在应答包中返回的 option 82 信息。

第5章 DHCP Snooping配置

5.1 DHCP Snooping介绍

DHCP Snooping 功能指交换机监测 DHCP CLIENT 通过 DHCP 协议获取 IP 的过程。它通过设置信任端口和非信任端口,来防止 DHCP 攻击及私设 DHCP SERVER。从信任端口接收的 DHCP 报文无需校验即可转发。典型的设置是将信任端口连接 DHCP SERVER 或者 DHCP RELAY 代理。非信任端口连接 DHCP CLIENT,交换机将转发从非信任端口接收的 DHCP 请求报文,不转发从非信任端口接收的 DHCP 回应报文。如果从非信任端口接收 DHCP 回应报文,除了发出告警信息外,并可根据设置对该端口执行相应的动作,比如 shutdown, 下发 blackhole。如果启用了 DHCP Snooping 绑定功能,则交换机将会保存非信任端口下的 DHCP CLIENT 的绑定信息,每一条绑定信息包含该 DHCP CLIENT 的 MAC 地址、IP 地址、租期、VLAN 号和端口号,这些绑定信息存放于 DHCP Snooping 的绑定表中。利用绑定信息,DHCP Snooping 可以结合 dot1x, arp 等模块或独立实现用户的接入控制。

防伪装 DHCP Server: 一旦交换机截获了从非信任端口收到的 DHCP Server 回应包(包括 DHCP OFFER, DHCP ACK 和 DHCP NAK),将发出警告,并相应做出反应(shutdown 端口或下发 BlackHole)。

防 DHCP 过载攻击: 要对信任端口和非信任端口做 DHCP 收包限速,防止过多的 DHCP 报文攻击 CPU。

记录 DHCP 绑定数据: DHCP SNOOPING 在转发 DHCP 报文的同时,记录 DHCP SERVER 分配的绑定数据,并可以把绑定数据上载到指定的服务器进行备份。这些绑定数据主要用于配置 dot1x userbased 端口的动态用户。有关 dot1x userbased 模式的用法请参考《dot1x 配置》的章节。

添加绑定 ARP: DHCP SNOOPING 捕获到绑定数据之后,可以根据绑定数据中的参数添加静态绑定 ARP,这样可以防止 ARP 欺骗。

添加信任用户: DHCP SNOOPING 捕获到绑定数据之后,可以根据绑定数据中的参数添加信任用户表项,这样这些用户就可以不经过 DOT1X 认证而访问所有资源。

自动恢复: 交换机 shutdown 端口或者下发 blockhole 一段时间后,交换机应主动恢复该端口或源 Mac 的通讯,同时通过 syslog 发送信息到 Log Server。

LOG 功能: 交换机检测发现异常收包时;或者自动恢复时,应自动发送 syslog 信息到 Log Server。

私有报文的加密: 交换机与内网安全管理系统 TrustView 之间使用私有报文进行通讯,用户允许配置版本 2 的私有报文进行加密处理。

添加认证 option82 功能: 与 dot1x dhcphoption82 认证方式配合使用,根据用户认证状态在 DHCP 报文中添加不同 option 82 内容。

5.2 DHCP Snooping 的配置任务序列

1. 启动 DHCP Snooping
2. 启动 DHCP Snooping 绑定功能
3. 启动 DHCP Snooping 绑定 ARP 功能
4. 启动 DHCP Snooping option82 功能
5. 配置私有报文版本号
6. 配置私有报文 DES 加密密钥
7. 配置 helper server 地址
8. 设置信任端口
9. 启动 DHCP Snooping 绑定 DOT1X 功能
10. 启动 DHCP Snooping 绑定 USER 功能
11. 添加静态表项功能
12. 设置防御动作
13. 打开调试开关
14. 设置 DHCP Snooping option82 属性

1. 启动 DHCP Snooping

命令	解释
全局配置模式	
ip dhcp snooping enable no ip dhcp snooping enable	开启或关闭 DHCP snooping 功能。

2. 启动 DHCP Snooping 绑定功能

命令	解释
全局配置模式	
ip dhcp snooping binding enable no ip dhcp snooping binding enable	开启或关闭 DHCP snooping 绑定功能。

3. 启动 DHCP Snooping option82 功能

命令	解释
全局配置模式	
ip dhcp snooping information enable	开启或关闭 DHCP snooping option82 功能。

no ip dhcp snooping information enable	
---	--

4. 配置私有报文版本号

命令	解释
全局配置模式	
ip user private packet version two no ip user private packet version two	配置或删除私有报文版本号。

5. 配置私有报文 DES 加密密钥

命令	解释
全局配置模式	
enable trustview key 0/7 <password> no enable trustview key	配置或删除私有报文 DES 加密密钥。

6. 配置 helper server 地址

命令	解释
全局配置模式	
ip user helper-address A.B.C.D [port <udpport>] source <ipAddr> (secondary) no ip user helper-address (secondary)	配置或删除 helper address 地址。

7. 启动 DHCP Snooping 绑定 ARP 功能

命令	解释
全局配置模式	
ip dhcp snooping binding arp no ip dhcp snooping binding arp	开启或关闭 DHCP snooping 绑定 ARP 功能。

8. 设置信任端口

命令	解释
端口配置模式	
ip dhcp snooping trust no ip dhcp snooping trust	设置或删除端口的 DHCP snooping 信任属性。

9. 启动 DHCP SNOOPING 绑定 DOT1X 功能

命令	解释
端口配置模式	
ip dhcp snooping binding dot1x no ip dhcp snooping binding dot1x	开启或关闭 DHCP snooping 绑定 dot1x 功能。

10. 启动 DHCP SNOOPING 绑定 USER 功能

命令	解释
端口配置模式	
ip dhcp snooping binding user-control no ip dhcp snooping binding user-control	开启或关闭 DHCP snooping 绑定 user 功能。

11. 添加静态绑定信息

命令	解释
全局配置模式	
ip dhcp snooping binding user <mac> address <ipAddr> vlan <vid> interface (ethernet) <ifname> no ip dhcp snooping binding user <mac> interface (ethernet) <ifname>	添加/删除 DHCP snooping 静态绑定表项。

12. 设置防御动作

命令	解释
端口配置模式	
ip dhcp snooping action {shutdown blackhole} [recovery <second>] no ip dhcp snooping action	设置或删除端口的 DHCP snooping 自动防御动作。

13. 打开调试开关

命令	解释
特权配置模式	
debug ip dhcp snooping packet debug ip dhcp snooping event debug ip dhcp snooping update debug ip dhcp snooping binding	请参照系统排错章节。

14. 设置 DHCP Snooping option82 属性

命令	解释
全局配置模式	
ip dhcp snooping information option subscriber-id format {hex ascii vs-hp}	本命令设置 DHCP snooping option82 功能 subscriber-id 默认格式。
ip dhcp snooping information option remote-id {standard <remote-id>} no ip dhcp snooping information option remote-id	本命令用于设置从端口接收的 DHCP 请求报文添加 option 82 子选项 2(远程 ID 选项)的具体内容。本命令的 no 操作把添加 option 82 子选项 2(远程 ID 选项)的形式设置为 standard。
ip dhcp snooping information option delimiter [colon dot slash space] no ip dhcp snooping information option delimiter	配置用户在全局定义的用来生成 option82 子选项的各参数的分隔符, 该命令的 no 形式恢复分隔符为默认值, 即 slash。
ip dhcp snooping information option self-defined remote-id {hostname mac string WORD} no ip dhcp snooping information option self-defined remote-id	配置 option82 的生成方式, 用户可以自定义用来生成 option82 子选项 remote-id 的参数(集)。
ip dhcp snooping information option self-defined remote-id format [ascii hex]	配置 snooping option82 中 remote-id 的生成格式。

<pre>ip dhcp snooping information option self-defined subscriber-id {vlan port id (switch-id (mac hostname) remote-mac) string WORD} no ip dhcp snooping information option type self-defined subscriber-id</pre>	配置 option82 的生成方式，用户可以自定义用来生成 option82 子选项 circuit-id 的参数（集）。
<pre>ip dhcp snooping information option self-defined subscriber-id format [ascii hex]</pre>	配置 snooping option82 中 circuit-id 的生成格式。
端口配置模式	
<pre>ip dhcp snooping information option subscriber-id {standard <circuit-id>} no ip dhcp snooping information option subscriber-id</pre>	本命令用于设置从端口接收的 DHCP 请求报文添加 option 82 子选项 1(电路 ID 选项)的具体内容。本命令的 no 操作把添加 option 82 子选项 1(电路 ID 选项)的形式设置为 standard。

命令	解释
全局配置模式	
<pre>ip dhcp snooping information option allow-untrusted (replace) no ip dhcp snooping information option allow-untrusted (replace)</pre>	本命令用于设置允许从 DHCP snooping 的非信任端口接收含有 option82 选项的 DHCP 报文，在设置参数 replace 时，允许替换 option82 选项；关闭此命令时，所有非信任端口将丢弃含有 option82 选项的 DHCP 报文。

5.3 DHCP Snooping 典型应用

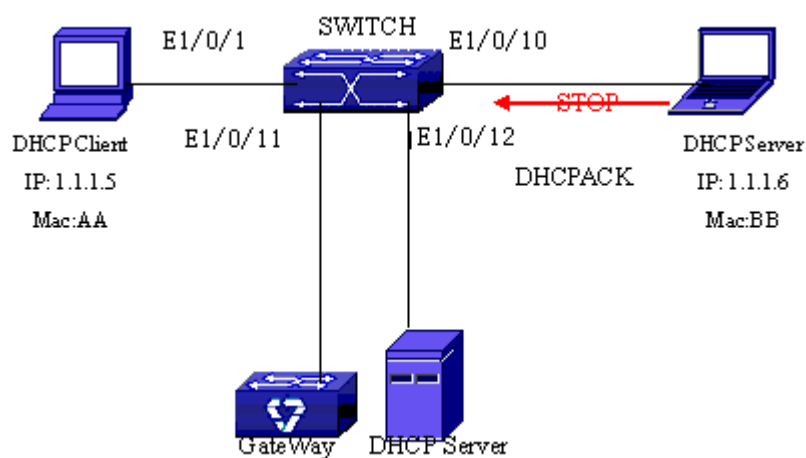


图 5-1 DHCP Snooping 防止非法 dhcp server 示意图

如上图, Mac-AA 设备为正常用户, 连接在交换机非信任端口 1/0/1 上, 其通过 DHCP Client 获得 IP 1.1.1.5; DHCP Server 和 GateWay 分别连接在交换机的信任端口 1/0/11; 1/0/12 上; 恶意用户 Mac-BB 连接在非信任端口 1/0/10 上, 试图伪装 DHCP Server (发送 DHCPACK)。在交换机上设置 DHCP snooping 将能有效发现并阻止这种网络攻击。

配置序列为:

```
switch#
switch#config
switch(config)#ip dhcp snooping enable
switch(config)#interface ethernet 1/0/11
switch(Config-Ethernet1/0/11)#ip dhcp snooping trust
switch(Config-Ethernet1/0/11)#exit
switch(config)#interface ethernet 1/0/12
switch(Config-Ethernet1/0/12)#ip dhcp snooping trust
switch(Config-Ethernet1/0/12)#exit
switch(config)#interface ethernet 1/0/1-10
switch(Config-Port-Range)#ip dhcp snooping action shutdown
switch(Config-Port-Range)#
```

5.4 DHCP Snooping 排错帮助

5.4.1 监控和调试信息

可以使用 `debug ip dhcp snooping` 命令来监控调试信息。

5.4.2 DHCP Snooping排错帮助

当在使用 DHCP Snooping 功能出现问题时，请检查是否是如下原因：

- ☞ 检查全局 DHCP Snooping 开关是否打开；
- ☞ 如果配置 DHCP Snooping, 而 DHCP 客户端没有获取 IP 时，请检查连接 dhcp server/relay 的端口是否已配置成信任端口。

第6章 DHCPv6 Snooping配置

6.1 DHCPv6 Snooping介绍

DHCPv6 Snooping 监听 DHCPv6 客户端和服务端端的报文交互流程,以此来创建用户绑定表,并以此绑定表为基础实施各种安全策略。DHCPv6 Snooping 具有以下主要功能:

6.1.1 防止伪装DHCPv6 服务器

DHCPv6 Snooping 为了防止网络中用户私自配置 DHCPv6 服务器,可以将连接真正 DHCPv6 服务器的端口设置为信任端口,其他端口默认为非信任端口。DHCPv6 Snooping 不转发从非信任口收到的 DHCPv6 回应报文,并根据从非信任端口收到的 DHCPv6 回应报文的源 MAC 实施安全策略,如将该 MAC 在一段时间内设置为黑洞 MAC,或直接将该端口 shutdown 一段时间等。

6.1.2 防止伪装IPv6 地址

DHCPv6 Snooping 功能可以基于端口建立的绑定下发控制表项。端口默认拒绝所有 IPv6 流量,只允许转发来自该端口的以绑定的 IPv6 地址和 MAC 地址为源的 IPv6 报文。这样可以有效的防止恶意用户伪装或私设 IPv6 地址接入网络。

6.1.3 防止DHCPv6 地址耗尽攻击

DHCPv6 Snooping 可以限制端口下的绑定数量,绑定数量超过阈值的端口不转发且丢弃后来的 DHCPv6 地址申请报文,这样可以有效的防止 DHCPv6 地址耗尽攻击。

6.1.4 防止ND欺骗

IPv6 网络中通过 DHCPv6 协议获得的 IPv6 地址相对可信,故 DHCPv6 Snooping 可以将绑定表项转化为静态 ND,有效防止针对网关设备的 ND 欺骗攻击。DHCPv6 Snooping 绑定 ND 的功能需要启用在三层网关设备上。

6.1.5 应对端口移动需求

DHCPv6 Snooping 是通过捕获 DHCPv6 报文的端口来判断 DHCPv6 用户所在的端口的。DHCPv6 Snooping 绑定创建以后,如果 DHCPv6 Snooping 收到从其他端口收到 DHCPv6 客户端的 CONFIRM/REQUEST 报文并收到回应时,需要先使用 DAD NS/NA 检测原端口上存在的绑定是否仍然可用:若仍可用(即收到 DAD NA 响应),则不在新端口创建新绑定,反之(在规定时间内未收到 DAD NA 响应),则在新端口创建绑定,并删除原端口上的绑定。

6.2 DHCPv6 Snooping 的配置任务序列

1. 启动 DHCPv6 Snooping 绑定功能
2. 启动 DHCPv6 Snooping 绑定 ND 功能
3. 删除 DHCPv6 Snooping 动态绑定信息
4. 设置端口绑定限制数目
5. 配置静态绑定表项
6. 设置信任端口
7. 设置防御动作
8. 设置 Blackhole MAC 的最大数目
9. 启动用户接入控制功能
10. 打开调试开关
11. 显示配置情况

1. 启动 DHCPv6 Snooping 绑定功能

命令	解释
全局配置模式	
ipv6 dhcp snooping binding enable no ipv6 dhcp snooping binding enable	开启或关闭 DHCPv6 Snooping 绑定功能。

2. 启动 DHCPv6 Snooping 绑定 ND 功能

命令	解释
全局配置模式	
ipv6 dhcp snooping binding nd no ipv6 dhcp snooping binding nd	开启或关闭 DHCPv6 Snooping 绑定 ND 功能。

3. 删除 DHCPv6 Snooping 动态绑定信息

命令	解释
特权配置模式	
clear ipv6 dhcp snooping binding {<MAC> <ipv6address> interface {ethernet <IFNAME> port-channel <IFNAME> <IFNAME>} all}	删除 DHCPv6 Snooping 动态绑定信息。

4. 设置端口绑定限制数目

命令	解释
端口配置模式	
ipv6 dhcp snooping binding-limit <max-num> no ipv6 dhcp snooping binding-limit	设置或删除端口上允许建立的最大 DHCPv6 Snooping 动态绑定数。

5. 配置静态表项

命令	解释
全局配置模式	
ipv6 dhcp snooping binding user <MAC-address> address <ipv6-address> vlan <vid> interface [ethernet port-channel] <ifname> no ipv6 dhcp snooping binding user <MAC-address>	配置或删除用户设置静态的绑定表项。

6. 设置信任端口

命令	解释
端口配置模式	
ipv6 dhcp snooping trust no ipv6 dhcp snooping trust	设置或删除端口的 DHCPv6 Snooping 信任属性。

7. 设置防御动作

命令	解释
端口配置模式	
ipv6 dhcp snooping action {shutdown blackhole} [recovery <second>] no ipv6 dhcp snooping action	设置或删除端口的 DHCPv6 Snooping 自动防御动作。

8. 设置 Blackhole MAC 的最大数目

命令	解释
全局配置模式	
ipv6 dhcp snooping action {<max-num> default}	设置每个非信任端口 Blackhole MAC 下发的最大数目。

9. 启动用户接入控制功能

命令	解释
端口配置模式	
ipv6 dhcp snooping binding user-control no ipv6 dhcp snooping binding user-control	开启或关闭 DHCPv6 Snooping 绑定用户接入控制功能。

10. 打开调试开关

命令	解释
特权配置模式	
debug ipv6 dhcp snooping packet debug ipv6 dhcp snooping event debug ipv6 dhcp snooping binding	请参照系统排错章节。

11. 显示配置情况

命令	解释
特权配置模式	
show ipv6 dhcp snooping interface [ethernet port-channel] <ifname> show ipv6 dhcp snooping binding {<MAC> <ipv6address> interface [ethernet port-channel] <ifname> all}	请参照命令手册。

6.3 DHCPv6 Snooping 典型应用

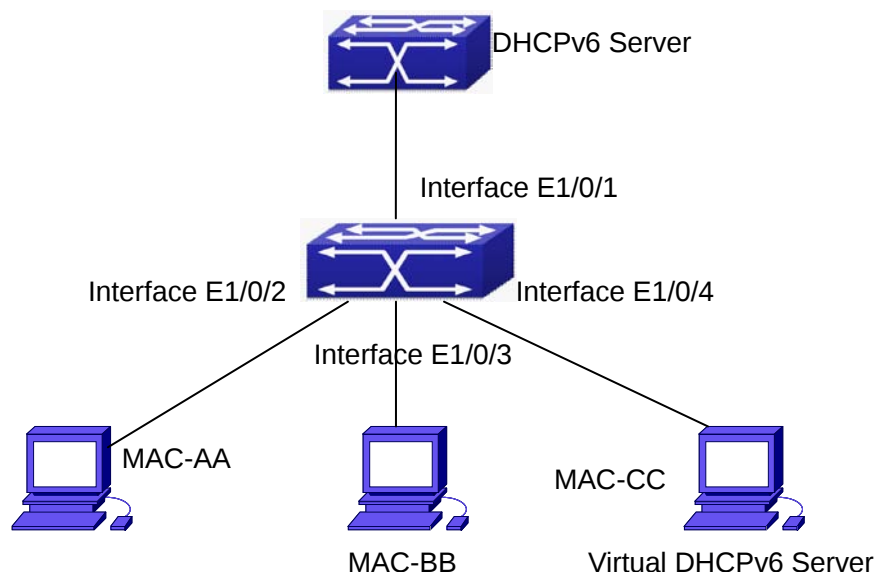


图 6-1 DHCPv6 Snooping 防止非法 DHCPv6 server 示意图

如上图，Mac-AA 和 Mac-BB 设备为正常用户，连接在交换机非信任端口 1/0/2 和 1/0/3 上，其通过 DHCPv6 Client 获得 IP 2010::3 和 2010::4；DHCPv6 Server 连接在交换机的信任端口 1/0/1 上；恶意用户 Mac-CC 连接在非信任端口 1/0/4 上，试图伪装 DHCPv6 Server。在交换机上设置 DHCPv6 Snooping 将能有效发现并阻止这种网络攻击。

配置序列为：

```
switch#
switch#config
switch(config)#ipv6 dhcp snooping enable
switch(config)#ipv6 dhcp snooping binding enable
switch(config)#interface ethernet 1/0/1
switch(Config-Ethernet 1/0/1)#ipv6 dhcp snooping trust
switch(Config-Ethernet1/0/1)#exit
switch(config)#interface ethernet 1/0/4-10
switch(Config-Port-Range)#ipv6 dhcp snooping action shutdown
switch(Config-Port-Range)#
```

6.4 DHCPv6 Snooping 排错帮助

6.4.1 监控和调试信息

可以使用 `debug ipv6 dhcp snooping` 命令来监控调试信息。

6.4.2 DHCPv6 Snooping 排错帮助

当在使用 DHCPv6 Snooping 功能出现问题时，请检查是否是如下原因：

- ☞ 检查全局 DHCPv6 Snooping 开关是否打开
- ☞ 如果配置 DHCPv6 Snooping，而 DHCP 客户端没有获取 IP 时，请检查连接 DHCPv6 server/relay 的端口是否已配置成信任端口
- ☞ DHCPv6 Snooping 与以下功能互斥：
 - ◆ IPv6 flow redirect
 - ◆ IPv6 受控组播/策略组播
 - ◆ IPv6 ACL
 - ◆ 配置 IPv6 ACL 的 QoS

第7章 DHCPv6 option 52

7.1 DHCPv6 option 52 介绍

DHCPv6 Option52 为 CAPWAP_AC_v6 option，用于 DHCPv6 服务器为 AP 下发无线控制器的 ipv6 无线地址列表。AP 作为 DHCPv6 客户端，在 DHCPv6 Solicit 报文的 option 6（该选项表明 DHCPv6 客户端需要请求的 DHCPv6 option）中如果填写了 52（0x34），则表示 AP 请求 option52 选项的内容，即需要通过 DHCPv6 服务器获取无线控制器的 IPv6 地址列表。DHCPv6 服务器在收到 AP 发来的 Solicit 报文以后，会解析里面携带的 option6，如果 option6 指明了客户端需要请求 option52，则会在回复的 Advertise 报文中带上 option52 信息。

7.2 DHCPv6 option 52 配置任务序列

1. DHCPv6 option 52 基本功能配置

命令	解释
地址池配置模式下	
option 52 ascii LINE	在 ipv6 dhcp pool 模式下以 ascii 格式配置 option 52 字符串。
option 52 hex WORD	在 ipv6 dhcp pool 模式下以 hex 格式配置 option 52 字符串。
option52 ipv6 X:X::X:X	在 ipv6 dhcp pool 模式下以 IPv6 格式配置 option 52 字符串。
no option 52	在地址池模式下删除配置的 option 52。

7.3 DHCPv6 option 52 配置举例

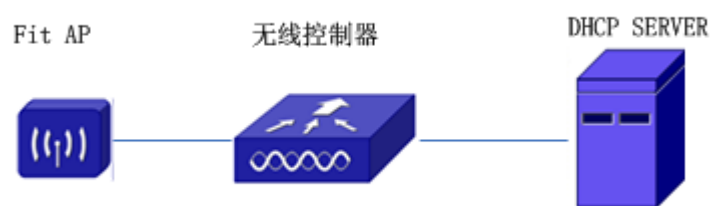


图 7-1 DHCPv6 option52 功能典型组网图

Fit AP 通过 DHCPv6 server 获取 IPv6 地址、option 52 属性(此属性中携带无线控制器的 IPv6 地址信息),然后向无线控制器发送单播发现请求。DHCPv6 SERVER 返回 option 52 属性给 FIT AP。

DHCPv6 Server 配置

配置步骤:

配置 DHCPv6 server

```
switch(config)#ipv6 dhcp pool a
```

```
switch(dhcpv6-a-config)#option 52 ipv6 2001:1::100
```

7.4 DHCPv6 option 52 排错帮助

当配置 DHCPv6 option52 功能出现问题时, 请检查是否是如下原因:

- ☞ 是否开启 service dhcp 功能
- ☞ Option 52 的字符串格式书写是否正确。