DHCP 技术白皮书

Copyright © 2021 紫光恒越技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除紫光恒越技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。本文中的内容为通用性技术信息，某些信息可能不适用于您所购买的产品。

目 录

1 概述 1
1.1 产生背景 1
1.2 技术优势 1
2 DHCP 技术实现 1
2.1 概念介绍 1
2.2 DHCP 报文格式 2
2.3 DHCP 服务器运行机制 3
2.3.1 地址分配策略 3
2.3.2 动态获取 IP 地址 3
2.3.3 重用曾经分配的 IP 地址 5
2.3.4 更新租约 5
2.3.5 DHCP 客户端主动释放 IP 地址 6
2.3.6 获取除 IP 地址外的配置信息 6
2.3.7 转控分离组网地址池支持动态分配子网段 6
2.3.8 ODAP 组网按需分配地址池 7
2.3.9 IP 地址池组 9
2.3.10 应用限制 9
2.4 DHCP 中继运行机制 10
2.5 DHCP Snooping 运行机制 11
2.5.1 DHCP Snooping 基本监听功能 11
2.5.2 DHCP Snooping 信任功能 11
3 DHCP 扩展功能 11
3.1 DHCP 安全功能 11
3.2 DHCP Option 82 功能 13
3.3 自动配置功能 14
4 典型组网应用 14
4.1 在本网段内申请地址组网 14
1.2 跨网段申请地址组网 15
1.3 DHCP Snooping 应用组网 15
1.4 自动配置应用组网 16
1.5 DHCP 应用综合组网 16

5 参考文献 ·····17

1 概述

1.1 产生背景

连接到 Internet 的计算机需要在发送或接收数据报前知道其 IP 地址和其他信息，如网关地址、使用的子网掩码和域名服务器的地址。计算机可以通过 BOOTP 协议获取这些信息。

BOOTP 协议（Bootstrap Protocol）是一种较早出现的远程启动的协议，通过与远程服务器通信以获取通信所需的必要信息，主要用于无磁盘的客户端从服务器得到自己的 IP 地址、服务器的 IP 地址、启动映像文件名、网关 IP 地址等等。

BOOTP 设计用于相对静态的环境，每台主机都有一个永久的网络连接。管理人员创建一个 BOOTP 配置文件，该文件定义了每台主机的一组 BOOTP 参数。由于配置通常保持不变，该文件不会经常改变。一般情况下，配置将保持数星期不变。

随着网络规模的不断扩大、网络复杂度的不断提高，网络配置也变得越来越复杂，在计算机经常移动（如便携机或无线网络）和计算机的数量超过可分配的 IP 地址等情况下，原有针对静态主机配置的 BOOTP 协议已经越来越不能满足实际需求。为方便用户快速地接入和退出网络、提高 IP 地址资源的利用率，需要在 BOOTP 基础上制定一种自动机制来进行 IP 地址的分配。为此，IETF 设计了一个新的协议，即 DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）。

1.2 技术优势

DHCP 是 BOOTP 的增强版本。它采用客户端/服务器的通信模式。所有的 IP 网络配置参数都由 DHCP 服务器集中管理，并负责处理客户端的 DHCP 请求；而客户端则会使用服务器分配的 IP 网络参数进行通信。

随着网络规模的扩大化和网络环境的复杂化，DHCP 服务被应用到越来越多的网络环境中，UNIS 公司的DHCP 特性解决方案具有完整的产品系列，可以为客户提供完善、灵活、便捷的组网配置方案，其主要优势有以下几点：

- 功能完备，可以为客户提供 DHCP 客户端、中继到服务器的全面功能实现；
- 具有出色的业务支持能力及灵活的组网方案；
- 良好的易用性和可配置性；
- 可以与业界其它主流厂商设备及 Windows、Linux 服务器实现良好的互通；
- 方便管理、部署经济、设备开销低。

2 DHCP 技术实现

2.1 概念介绍

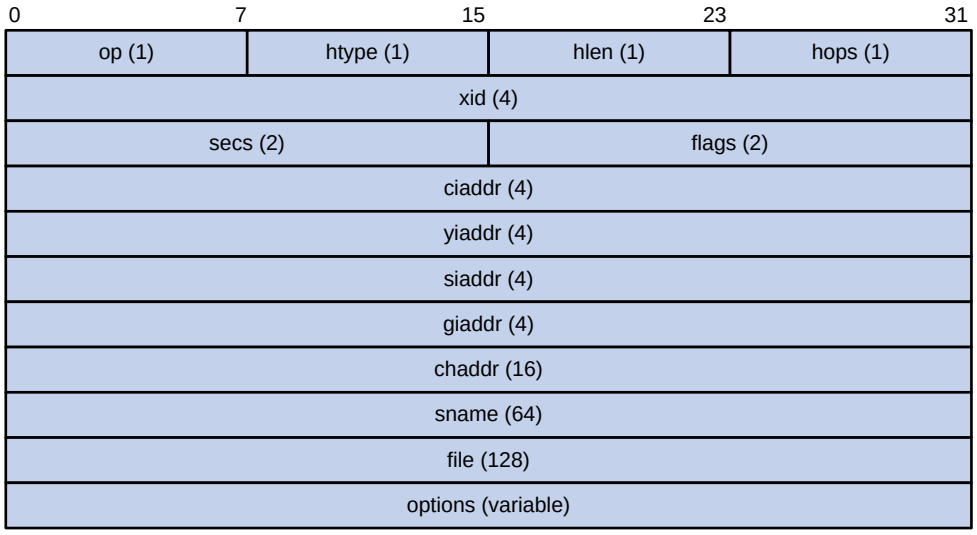
- DHCP 服务器：DHCP 服务的提供者，通过 DHCP 报文与 DHCP 客户端交互，为各种类型的客户端分配合适的 IP 地址，并可以根据需要为客户端分配其它网络参数。
- DHCP 客户端：是整个 DHCP 过程的触发者和驱动者，通过 DHCP 报文和 DHCP 服务器交互，得到 IP 地址和其他网络参数。

- DHCP 中继：DHCP 报文的中继转发者。它在处于不同网段间的 DHCP 客户端和服务器之间承担中继服务，解决了 DHCP 客户端和 DHCP 服务器必须位于同一网段的问题。
- DHCP Snooping：DHCP 服务的二层监听功能。利用该功能可以从接收到的 DHCP-ACK 和 DHCP-REQUEST 报文中提取并记录 IP 地址和 MAC 地址信息。

2.2 DHCP报文格式

DHCP 报文格式如图 1 所示。

图1 DHCP 报文格式



DHCP 报文的各个字段的具体说明如下：

- op：报文的操作类型，1 为请求报文，2 为响应报文。具体的报文类型在 option 字段中标识。
- htype：硬件地址类型。
- hlen：硬件地址长度。系统目前只支持以太网，硬件地址长度固定为 6。
- hops：DHCP 报文经过的 DHCP 中继的数目。DHCP 请求报文每经过一个 DHCP 中继，该字段就会增加 1。
- xid：由客户端软件产生的随机数，用于匹配请求和应答报文。
- secs：客户端进入 IP 地址申请进程的时间或者更新 IP 地址进程的时间；由客户端软件根据情况设定。目前没有使用，固定为 0。
- flags：标志字段。第一个比特为广播响应标识位，用来标识 DHCP 服务器响应报文是采用单播还是广播方式发送，0 表示采用单播方式，1 表示采用广播方式。其余比特保留不用。
- ciaddr：DHCP 客户端的 IP 地址。
- yiaddr：DHCP 服务器分配给客户端的 IP 地址。
- siaddr：DHCP 客户端获取 IP 地址等信息的服务器 IP 地址。
- giaddr：DHCP 客户端发出请求报文后经过的第一个 DHCP 中继的 IP 地址。
- chaddr：DHCP 客户端的硬件地址。
- sname：DHCP 客户端获取 IP 地址等信息的服务器名称。

- file：DHCP 服务器为 DHCP 客户端指定的启动配置文件名称及路径信息。
- options：可选变长选项字段，包含报文的类型、有效租期、DNS 服务器的 IP 地址、WINS 服务器的 IP 地址等配置信息。

2.3 DHCP服务器运行机制

由于在 IP 地址动态获取过程中采用广播方式发送报文，因此要求 DHCP 客户端和服务器位于同一个网段内。如果 DHCP 客户端和 DHCP 服务器位于不同的网段，则需要通过 DHCP 中继来转发 DHCP 报文。

通过 DHCP 中继完成动态配置的过程中，客户端与服务器的处理方式与不通过 DHCP 中继时的处理方式基本相同。下面仅以 DHCP 客户端与 DHCP 服务器在同一网段的情况为例，说明 DHCP 协议的工作过程。

2.3.1 地址分配策略

针对客户端的不同需求，DHCP 提供三种 IP 地址分配策略：

- 手工分配地址：由管理员为少数特定客户端（如 WWW 服务器等）静态绑定固定的 IP 地址，通过 DHCP 将配置的固定 IP 地址发给客户端；
- 自动分配地址：DHCP 为客户端分配租期为无限长的 IP 地址；
- 动态分配地址：DHCP 为客户端分配有有效期限的 IP 地址，到达使用期限后，客户端需要重新申请地址。

管理员可以选择 DHCP 采用哪种策略响应每个网络或每台主机。

2.3.2 动态获取IP地址

为了动态获取并使用一个合法的 IP 地址，需要经历以下几个阶段：

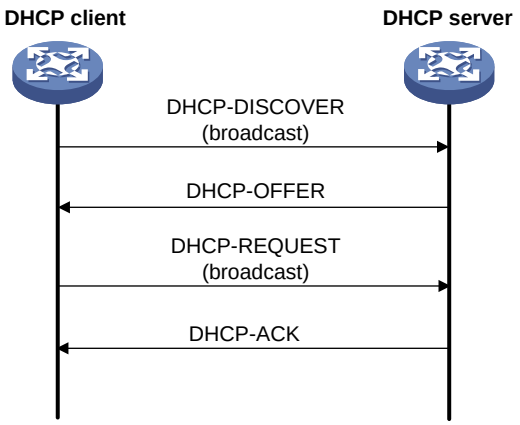
(1) 发现阶段：即 DHCP 客户端寻找 DHCP 服务器的阶段。

(2) 提供阶段：即 DHCP 服务器提供 IP 地址的阶段。

(3) 选择阶段：即 DHCP 客户端选择某台 DHCP 服务器提供的 IP 地址的阶段。

(4) 确认阶段：即 DHCP 服务器确认所提供的 IP 地址的阶段。

图2 IP 地址动态获取过程



IP 地址的动态获取过程如图 2 所示，下面将详细介绍每个阶段的工作过程。

1. 发现阶段

在发现阶段，DHCP 客户端通过发送 DHCP-DISCOVER 报文来寻找 DHCP 服务器。

由于 DHCP 服务器的 IP 地址对于客户端来说是未知的，所以 DHCP 客户端以广播方式发送 DHCP-DISCOVER 报文。所有收到 DHCP-DISCOVER 报文的 DHCP 服务器都会发送回应报文，DHCP 客户端据此可以知道网络中存在的 DHCP 服务器的位置。

2. 提供阶段

网络中接收到 DHCP-DISCOVER 报文的 DHCP 服务器，会选择一个合适的 IP 地址，连同 IP 地址租约期限和其他配置信息（如网关地址，域名服务器地址等）一同通过 DHCP-OFFER 报文发送给 DHCP 客户端。

DHCP 服务器通过地址池保存可供分配的 IP 地址和其他配置信息。当 DHCP 服务器接收到 DHCP 请求报文后，将从 IP 地址池中选取空闲的 IP 地址及其他的参数，发送给 DHCP 客户端。

DHCP 服务器为客户端分配 IP 地址的优先次序如下：

(1) 与客户端 MAC 地址或客户端 ID 静态绑定的 IP 地址；

(2) DHCP 服务器记录的曾经分配给客户端的 IP 地址；

(3) 客户端发送的 DHCP-DISCOVER 报文中 Option 50 字段指定的 IP 地址；

(4) 在 DHCP 地址池中，顺序查找可供分配的 IP 地址，最先找到的 IP 地址；

(5) 如果未找到可用的 IP 地址，则依次查询租约过期、曾经发生过冲突的 IP 地址，如果找到则进行分配，否则将不予处理。

DHCP 服务器为客户端分配 IP 地址时，服务器首先需要确认所分配的 IP 没有被网络上的其他设备所使用。DHCP 服务器通过发送 ICMP Echo Request（ping）报文对分配的 IP 进行探测。如果在规定的时间内没有收到应答，那么服务器就会再次发送 ping 报文。到达指定的次数后，如果仍没有收到应答，则所分配的 IP 地址可用。否则将探测的 IP 地址记录为冲突地址，并重新选择 IP 地址进行分配。

3. 选择阶段

如果有多台 DHCP 服务器向 DHCP 客户端回应 DHCP-OFFER 报文，则 DHCP 客户端只接受第一个收到的 DHCP-OFFER 报文。然后以广播方式发送 DHCP-REQUEST 请求报文，该报文中包含 Option 54（服务器标识选项），即它选择的 DHCP 服务器的 IP 地址信息。

以广播方式发送 DHCP-REQUEST 请求报文，是为了通知所有的 DHCP 服务器，它将选择 Option 54 中标识的 DHCP 服务器提供的 IP 地址，其他 DHCP 服务器可以重新使用曾提供的 IP 地址。

4. 确认阶段

收到 DHCP 客户端发送的 DHCP-REQUEST 请求报文后，DHCP 服务器根据 DHCP-REQUEST 报文中携带的 MAC 地址来查找有没有相应的租约记录。如果有，则发送 DHCP-ACK 报文作为应答，通知 DHCP 客户端可以使用分配的 IP 地址。

DHCP 客户端收到 DHCP 服务器返回的 DHCP-ACK 确认报文后，会以广播的方式发送免费 ARP（Address Resolution Protocol，地址解析协议）报文，探测是否有主机使用服务器分配的 IP 地址，如果在规定的时间内没有收到回应，客户端才使用此地址。否则，客户端会发送 DHCP-DECLINE 报文给 DHCP 服务器，通知 DHCP 服务器该地址不可用，并重新申请 IP 地址。

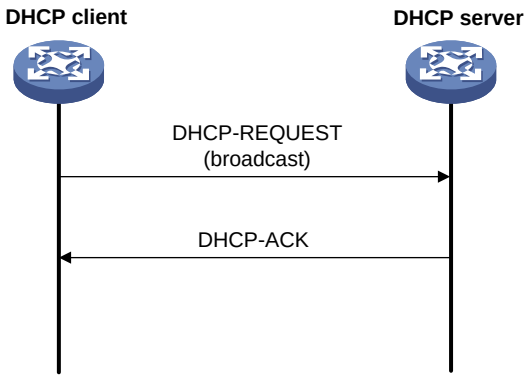
如果 DHCP 服务器收到 DHCP-REQUEST 报文后，没有找到相应的租约记录，或者由于某些原因无法正常分配 IP 地址，则发送 DHCP-NAK 报文作为应答，通知 DHCP 客户端无法分配合适 IP 地址。DHCP 客户端需要重新发送 DHCP-DISCOVER 报文来请求新的 IP 地址。

2.3.3 重用曾经分配的IP地址

DHCP 客户端每次重新登录网络时，不需要再发送 DHCP-DISCOVER 报文，而是直接广播发送包含前一次分配的 IP 地址的 DHCP-REQUEST 请求报文，即报文中的 Option 50（请求的 IP 地址选项）字段填入曾经使用过的 IP 地址。DHCP 服务器收到这一报文后，判断 DHCP 客户端是否可以使用请求的地址：

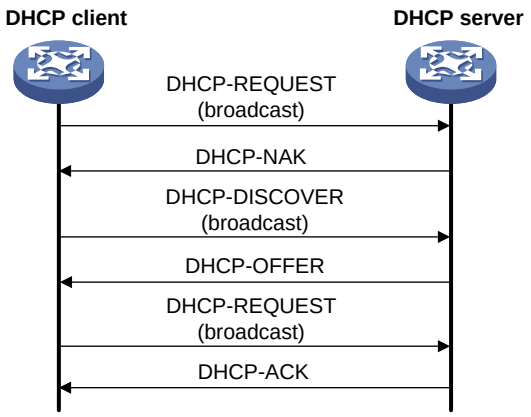
- 如果可以使用请求的地址，DHCP 服务器将回复 DHCP-ACK 确认报文。收到 DHCP-ACK 报文后，DHCP 客户端可以继续使用该地址进行通信。如图 3 所示。

  图3 DHCP 客户端可以重新使用曾分配的 IP 地址



- 如果请求的 IP 地址已无法再分配给 DHCP 客户端（例如，此 IP 地址已分配给其它 DHCP 客户端使用），则 DHCP 服务器将回复 DHCP-NAK 否认报文。DHCP 客户端收到此报文后，必须重新发送 DHCP-DISCOVER 报文来请求新的 IP 地址。如图 4 所示。

  图4 DHCP 客户端不能重新使用曾分配的 IP 地址



2.3.4 更新租约

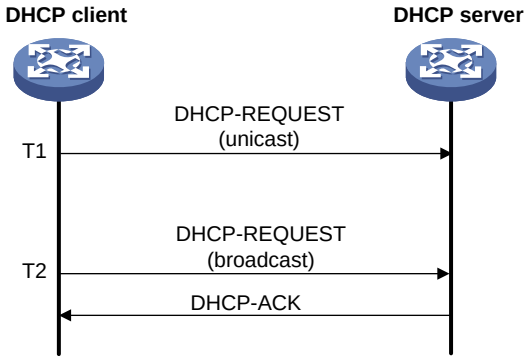
DHCP 服务器分配给 DHCP 客户端的 IP 地址一般都有一个租借期限，期满后 DHCP 服务器便会收回分配的 IP 地址。如果 DHCP 客户端要延长其 IP 租约，则必须更新其 IP 租约。

(1) IP 租约期限达到一半（T1）时，DHCP 客户端会自动以单播的方式，向 DHCP 服务器发送 DHCP-REQUEST 报文，请求更新 IP 地址租约。如果收到 DHCP-ACK 报文，则租约更新成功；如果收到 DHCP-NAK 报文，则重新发起申请过程。

(2) 到达租约期限的 87.5%（T2）时，如果仍未收到 DHCP 服务器的应答，DHCP 客户端会自动向 DHCP 服务器发送更新其 IP 租约的广播报文。如果收到 DHCP-ACK 报文，则租约更新成功；如果收到 DHCP-NAK 报文，则重新发起申请过程。

如图 5 所示，租约达到 87.5%，广播发送 DHCP-REQUEST 报文后，收到 DHCP 服务器回应的 DHCP-ACK 报文，租约更新成功。

图5 更新 IP 地址租约



2.3.5 DHCP客户端主动释放IP地址

DHCP 客户端不再使用分配的 IP 地址时，会主动向 DHCP 服务器发送 DHCP-RELEASE 报文，通知 DHCP 服务器释放 IP 地址的租约。DHCP 服务器会保留这个 DHCP 客户端的配置信息，以便该客户端重新申请地址时，重用这些参数。

2.3.6 获取除IP地址外的配置信息

DHCP 客户端获取 IP 地址后，如果需要从 DHCP 服务器获取更为详细的配置信息，则发送 DHCP-INFORM 报文向 DHCP 服务器进行请求。DHCP 客户端通过 Option 55（请求参数列表选项），指明需要从服务器获取哪些网络配置参数。

DHCP 服务器收到该报文后，将通过 DHCP-ACK 报文为客户端分配它所需要的网络参数。

2.3.7 转控分离组网地址池支持动态分配子网段

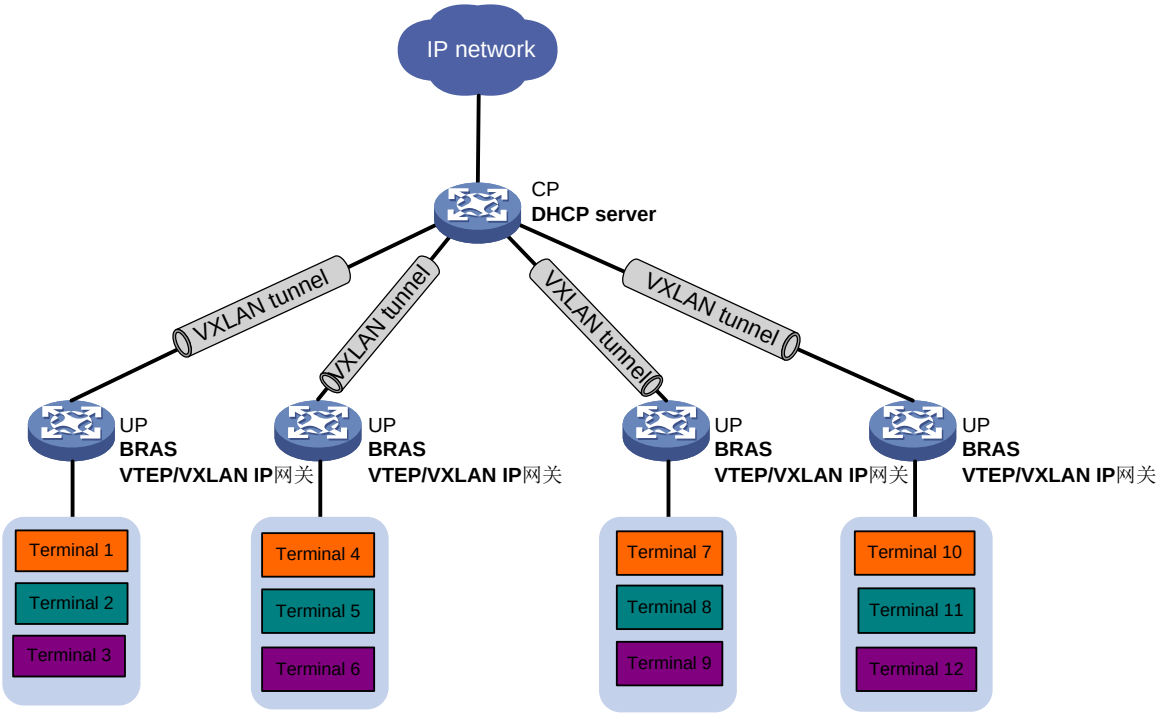
本功能适用于转发控制分离组网，此类组网主要包括 CP（Control Plane，控制平面）和 UP（User Plane，用户平面）两类设备：

- CP 设备：负责所有终端用户的认证、授权等工作。
- UP 设备：负责将连接的终端用户按照不同业务划分到不同的 VXLAN 组网、转发终端用户报文等工作。

CP 设备和 UP 设备之间通过建立 OpenFlow 和 VXLAN 两条传输通道：

- OpenFlow 作为 CP 设备和 UP 设备之间的表项下发通道。
- VXLAN 隧道作为 CP 设备和 UP 设备之间的协议报文通道。

图6 IP 地址池支持动态分配子网段功能原理图



如图 6 所示，CP 设备通过 VXLAN 隧道连接多台 UP 设备，CP 设备上开启了 DHCP 服务器功能，CP 设备根据配置的子网段掩码长度将 IP 地址池中的地址空间分成多个子网段。

动态地址池组网的工作过程为：

(1) CP 设备收到 DHCP 客户端发送的 DHCP-DISCOVER 报文时，根据动态地址池下配置的分配模式（up-id、interface 或 up-backup-group），查看是否有子网段可以为这个 DHCP 客户端分配租约。如果存在，直接使用该子网段为 DHCP 客户端分配租约；如果不存在，则进入下一步骤。

(2) CP 设备按照用户上线时携带的 up-id、interface 或 up-backup-group 信息及动态地址池下配置的分配模式来给 UP 设备动态分配一个子网段，并从该子网段中选择地址分配给上线用户。同时，CP 设备会将该子网段对应的网段路由下发给 UP 设备，当路由收敛结束后，外部网络可以访问到此 UP 设备下联的用户。

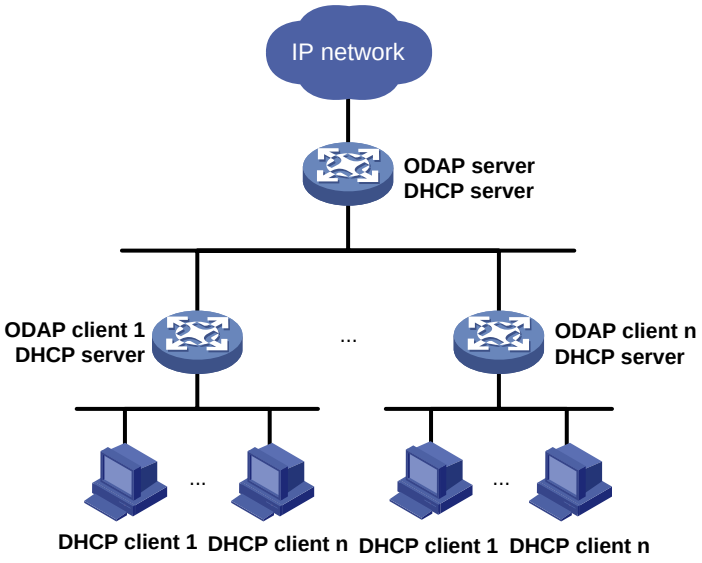
(3) 当某个子网段的用户全部下线后，CP 设备会回收该子网段。

本功能实现了 DHCP 服务器对 IP 地址空间的灵活分配和回收，使地址空间分配更合理，并大幅节约了人力维护成本。

2.3.8 ODAP 组网按需分配地址池

ODAP（On-Demand Address Pool，按需地址池）根据实际需求动态分配和回收子网段，可以充分利用地址资源。ODAP 适用于大量用户上线的组网环境。ODAP 组网主要包括服务器子网管理设备（ODAP 服务器）和本地子网管理设备（ODAP 客户端）。

图7 ODAP 按需地址池分配子网段功能原理图



如图 7 所示，一台 ODAP 服务器可以连接多台 ODAP 客户端，ODAP 服务器和 ODAP 客户端均作为 DHCP 服务器。ODAP 服务器上的 IP 地址池中创建了含有大量地址的网段地址空间，ODAP 服务器根据配置的子网掩码长度将这些地址空间分成多个子网段。ODAP 客户端上的 IP 地址池不创建网段地址空间，ODAP 客户端需要先从 ODAP 服务器申请子网段，再从该子网段中选择地址分配给 DHCP 客户端。

ODAP 组网的工作过程为：

(1) ODAP 客户端收到 DHCP 客户端发送的 DHCP-DISCOVER 报文时，根据 ODAP 客户端地址池下配置的分配模式（up-id、interface 或 up-backup-group），查看是否有子网段可以给这个 DHCP 客户端分配。如果存在，则直接使用该子网段给 DHCP 客户端分配租约；如果不存在，则进入下一步骤。

(2) ODAP 客户端向 ODAP 服务器申请子网段。子网段申请过程与 IP 地址申请过程基本相同，不同之处在于子网段申请过程中，ODAP 客户端和 ODAP 服务器发送的报文中均携带 Option 220 和 Option 221 选项。其中，ODAP 客户端发送的请求报文中的 Option 220 携带请求子网段信息，Option 221 携带 ODAP 客户端地址池所在 VPN 信息；ODAP 服务器发送的应答报文中的 Option 220 携带分配的子网段信息，Option 221 携带 ODAP 服务器地址池所在 VPN 信息。

(3) ODAP 客户端使用申请到的子网段为 DHCP 客户端分配租约。

相比于动态分配子网段功能，ODAP 功能降低了 ODAP 服务器工作负担，使 ODAP 组网适用于更大规模的动态网段分配组网环境。

当 ODAP 客户端发生故障或者与 ODAP 服务器之间连接中断时，ODAP 服务器感知不到此类事件，导致 ODAP 服务器无法回收该 ODAP 客户端的子网段。此时，可以强制 ODAP 服务器更新子网，该过程为：

(1) 触发一次 ODAP 服务器的子网强制更新操作后，ODAP 服务器会主动向所有 ODAP 客户端发送 DHCP-FORCERENEW 报文请求申请到的子网段信息。

(2) ODAP 客户端收到该报文后，通过 DHCP-REQUEST 报文将自己申请到的子网段信息发送给 ODAP 服务器。

(3) ODAP 服务器统计 DHCP-REQUEST 报文中记录的所有子网段信息，未统计到的子网段都会被 ODAP 服务器直接回收。

本功能保证了子网段资源不会被浪费。

2.3.9 IP 地址池组

在 AAA 组网中，终端用户经过 AAA 认证后，DHCP 设备根据 AAA 服务器的授权信息从本地配置的 IP 地址池中选择 IP 地址。如果只配置 AAA 关联某个独立的 IP 地址池，则无法满足如下需求：

- 为不同位置的接入用户选择不同的 DHCP 服务器。
- AAA 设备既需要作为 DHCP 服务器也需要作为 DHCP 中继，作为 DHCP 服务器可以直接为客户端分配地址；作为 DHCP 中继可以将用户的请求报文转发给 DHCP 服务器，并将 DHCP 服务器的应答报文转发给终端用户。
- 普通组网和转控分离组网混合环境，AAA 需要同时添加普通地址池和可动态分配子网段的地址池。

AAA 关联 IP 地址池组功能可以满足上述需求。使用 IP 地址池组功能，管理员可以将多个 IP 地址池添加到同一个 IP 地址池组中。IP 地址池包括普通地址池、本地 BAS IP 地址池和远端 BAS IP 地址池。配置 AAA 关联 IP 地址池组后，AAA 按照匹配顺序选择 IP 地址池组中的地址池为终端用户分配 IP 地址。

DHCP 客户端通过 IP 地址池组获取地址的工作过程为：

(1) 设备收到 DHCP 客户端发送的 DHCP-DISCOVER 报文时，如果设备发现该用户已经成功上线，则还会使用同样的地址分配给用户；如果用户未上线，但在某个地址池下存在对应的静态绑定关系，则使用静态绑定关系对应的地址分配给用户，如果不存在以上情况，则继续执行如下步骤。

(2) 根据该用户上线时的 UP 设备地址或远端接口信息，查看是否存在 UP 地址或远端接口绑定的可用的普通地址池和本地 BAS IP 地址池。如果存在，则选择该地址池为用户分配地址；如果不存在，则继续执行如下步骤。

(3) 设备查看是否存在未绑定 UP 地址和远端接口的可用普通地址池和本地 BAS IP 地址池。如果存在，则按照 Buildrun 显示的顺序选取地址池为用户分配租约；如果不存在，则继续执行如下步骤。

(4) 根据该用户上线时的 UP 地址或远端接口信息，查看是否存在 UP 地址或远端接口绑定的可用远端 BAS IP 地址池。如果存在，则将报文转发给该地址池对应的 DHCP 服务器；如果不存在，则继续执行如下步骤。

(5) 设备查看是否存在未绑定 UP 地址和远端接口的可用远端 BAS IP 地址池。如果存在，则按照 Buildrun 显示的顺序选择远端 BAS IP 地址池，并将报文转发给地址池对应的 DHCP 服务器；如果不存在，则用户无法获取到 IP 地址。

当用户匹配到 IP 地址池组中的最后一个地址池，仍无法为用户分配地址，则地址分配过程失败。

2.3.10 应用限制

DHCP 具有如下缺点：

- 当网络上存在多个 DHCP 服务器时，一个 DHCP 服务器不能查出已被其它服务器分配出去的 IP 地址；

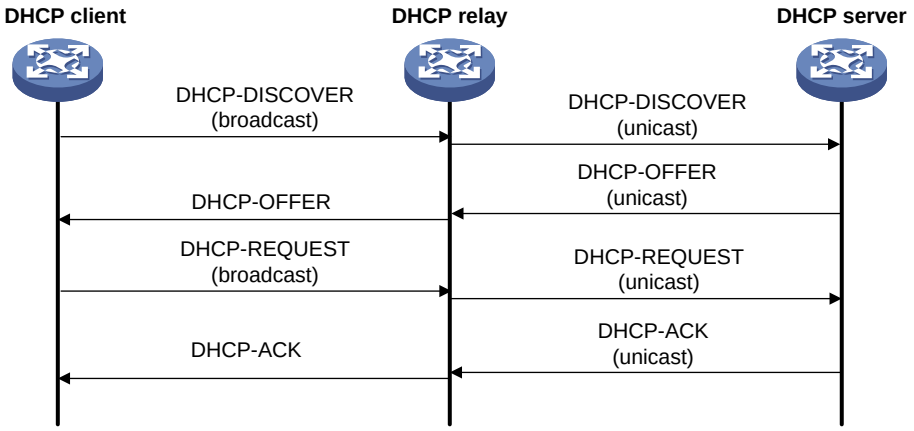
- DHCP 服务器不能跨网段与客户端通信，除非通过 DHCP 中继转发报文。

2.4 DHCP中继运行机制

原始的 DHCP 协议要求客户端和服务器只能在同一个子网内，不可以跨网段工作。因此，为进行动态主机配置需要在所有网段上都设置一个 DHCP 服务器，这显然是不经济的。

DHCP 中继的引入解决了这一问题，它在处于不同网段间的 DHCP 客户端和服务器之间承担中继服务，将 DHCP 协议报文跨网段中继到目的 DHCP 服务器，于是不同网络上的 DHCP 客户端可以共同使用一个 DHCP 服务器。

图8 DHCP 中继工作过程示意图



DHCP 中继的工作过程如图 8 所示。DHCP 客户端发送请求报文给 DHCP 服务器，DHCP 中继收到该报文并适当处理后，发送给指定的位于其它网段上的 DHCP 服务器。服务器根据请求报文中提供的必要信息，通过 DHCP 中继将配置信息返回给客户端，完成对客户端的动态配置。

(1) DHCP 中继接收到 DHCP-DISCOVER 或 DHCP-REQUEST 报文后，将进行如下处理：
   - 为防止 DHCP 报文形成环路，抛弃报文头中 hops 字段的值大于限定跳数的 DHCP 请求报文。如果收到的请求报文的报文头中 hops 字段的值小于或等于限定跳数，则继续进行下面的操作。
   - 检查 giaddr 字段。如果是 0，需要将 giaddr 字段设置为接收请求报文的接口 IP 地址。如果接口有多个 IP 地址，则选择接口的主 IP 地址。以后从该接口接收的所有请求报文都使用该 IP 地址。如果 giaddr 字段不是 0，则不修改该字段。
   - 将 hops 字段增加 1，表明又经过一次 DHCP 中继。
   - 将请求报文的 TTL 设置为 DHCP 中继设备的 TTL 缺省值，而不是原来请求报文的 TTL 减 1。中继报文的环路问题和跳数限制问题都可以通过 hops 字段来解决。
   - DHCP 请求报文的目的地址修改为 DHCP 服务器或下一个 DHCP 中继的 IP 地址。从而，将 DHCP 请求报文中继转发给 DHCP 服务器或下一个 DHCP 中继。

(2) DHCP 服务器根据 giaddr 字段为客户端分配 IP 地址等参数，并将 DHCP 应答报文发送给 giaddr 字段标识的 DHCP 中继。DHCP 中继接收到 DHCP 应答报文后，会进行如下处理：
   - DHCP 中继假设所有的应答报文都是发给直连的 DHCP 客户端。giaddr 字段用来识别与客户端直连的接口。如果 giaddr 不是本地接口的地址，DHCP 中继将丢弃应答报文。

- DHCP 中继检查报文的广播标志位。如果广播标志位为 1，则将 DHCP 应答报文广播发送给 DHCP 客户端；否则将 DHCP 应答报文单播发送给 DHCP 客户端，其目的地址为 yiaddr，链路层地址为 chaddr。

2.5 DHCP Snooping运行机制

2.5.1 DHCP Snooping基本监听功能

DHCP Snooping 即 DHCP 服务的二层监听功能。出于安全性的考虑，安全部门需要记录用户上网时所用的 IP 地址，确认用户申请的 IP 地址和用户使用的主机的 MAC 地址的对应关系。此时，可以通过 DHCP Snooping 功能监听接收到的 DHCP-REQUEST 报文和 DHCP-ACK 报文，从中提取并记录用户获取的 IP 地址信息。

2.5.2 DHCP Snooping信任功能

DHCP Snooping 的信任功能，可以为用户提供进一步的安全性保证

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 信任功能将端口分为信任端口和不信任端口：

- 信任端口是与合法的 DHCP 服务器直接或间接连接的端口。信任端口对接收到的 DHCP 报文正常转发，从而保证了 DHCP 客户端获取正确的 IP 地址。
- 不信任端口是不与合法的 DHCP 服务器连接的端口。从不信任端口接收到 DHCP 服务器响应的 DHCP-ACK、DHCP-NAK 和 DHCP-OFFER 报文会被丢弃，从而防止了 DHCP 客户端获得错误的 IP 地址。

3 DHCP 扩展功能

3.1 DHCP安全功能

DHCP 安全功能可以防止非法用户发起的地址申请攻击。在 DHCP 服务器或 DHCP 中继设备上配置 DHCP 安全功能后，就可以有效地进行地址规划和分配，实现对用户的控制。

DHCP 安全实现的基本功能如下：

(1) 合法用户 IP 地址表项管理

确保所有合法用户都记录在 DHCP 中继的用户地址表项中。

当客户端通过 DHCP 中继从 DHCP 服务器获取到 IP 地址时，DHCP 中继可以自动记录客户端 IP 地址与 MAC 地址的绑定关系，生成 DHCP 中继的动态用户地址表项。DHCP 中继还支持用户表项的手工删除和查询功能。

(2) 用户地址表项老化功能

DHCP 客户端释放动态获取的 IP 地址时，会向 DHCP 服务器单播发送 DHCP-RELEASE 报文，DHCP 中继不会处理该报文的内容。如果此时 DHCP 中继上记录了该 IP 地址与 MAC 地址的绑定关系，则会造成 DHCP 中继的用户地址表项无法实时刷新。为了解决这个问题，DHCP 中继支持动态用户地址表项的定时刷新功能。

DHCP 中继动态用户地址表项定时刷新功能开启时，DHCP 中继每隔指定时间间隔采用客户端获取到的 IP 地址和 DHCP 中继接口的 MAC 地址向 DHCP 服务器发送 DHCP-REQUEST 报文：

- 如果 DHCP 中继接收到 DHCP 服务器响应的 DHCP-ACK 报文或在指定时间内未接收到 DHCP 服务器的响应报文，则表明这个 IP 地址已经可以进行分配，DHCP 中继会删除对应的动态用户地址表项。为了避免地址浪费，DHCP 中继收到 DHCP-ACK 报文后，会发送 DHCP-RELEASE 报文释放申请到的 IP 地址。
- 如果 DHCP 中继接收到 DHCP 服务器响应的 DHCP-NAK 报文，则表示该 IP 地址的租约仍然存在，DHCP 中继不会删除该 IP 地址对应的表项。

(3) DHCP Flood 攻击防范功能

DHCP Flood 攻击防范功能用于防止源 MAC 地址固定的 DHCP 泛洪类攻击，本功能支持在 DHCP 服务器和 DHCP 中继上配置。

配置 DHCP Flood 攻击防范功能后，DHCP 设备会根据 DHCP 报文中的源 MAC 地址统计收到的 DHCP 报文数，并创建一个 check 状态的 DHCP 防 Flood 攻击表项。当收到某个 MAC 地址对应 DHCP 客户端发送的报文数在指定的时间内达到配置的最大报文数时，DHCP 设备认为受到了该 DHCP 客户端的攻击，DHCP 防 Flood 攻击表项状态从 check 状态变成 restrain 状态，且 DHCP 设备丢弃该 DHCP 客户端发送的 DHCP 报文。DHCP 设备在 DHCP Flood 攻击表项老化时间到达后会检查表项对应报文的抑制速率。如果速率小于 DHCP Flood 攻击报文速率阈值，设备会删除此表项，设备再次收到源 MAC 地址为此 MAC 地址的 DHCP 请求报文时，会重新统计接收到的报文数目；如果速率大于等于 DHCP Flood 攻击报文速率阈值，设备不会删除此表项，老化时间重新刷新。

(4) DHCP 接口攻击抑制功能

DHCP 接口攻击抑制功能用于防止对某个指定接口的 DHCP 泛洪类攻击，本功能支持在 DHCP 服务器和 DHCP 中继上配置。

在某接口开启 DHCP 接口攻击抑制功能后，该接口收到 DHCP 报文后，会统计收到的 DHCP 报文数，同时创建一个 check 状态的 DHCP 接口攻击抑制表项。当接口收到的 DHCP 报文数在指定的时间内达到配置的最大报文数时，则认为该接口受到了 DHCP 报文攻击，DHCP 接口攻击抑制表项状态从 check 状态变成 restrain 状态。在 DHCP 接口攻击抑制表项的老化时间到期之前，设备会限制被攻击的接口每秒钟接收 DHCP 报文的速率，防止 DHCP 攻击报文持续冲击 CPU。当某个接口对应的 DHCP 接口攻击抑制表项老化时间到达后，接口会检查当前接口收到报文的速率。如果速率达不到攻击标准，设备会删除此表项，接口再次收到 DHCP 报文时，会重新统计接收到的报文数目；如果速率超过攻击标准，则 DHCP 接口攻击抑制表项老化时间重新刷新。

(5) DHCP 防饿死功能

DHCP 饿死攻击是指攻击者伪造 chaddr 字段各不相同的 DHCP 请求报文，向 DHCP 服务器申请大量的 IP 地址，导致 DHCP 服务器地址池中的地址耗尽，无法为合法的 DHCP 客户端分配 IP 地址，或导致 DHCP 服务器消耗过多的系统资源，无法处理正常业务。

如果封装 DHCP 请求报文的数据帧的源 MAC 地址各不相同，则通过 **`mac-address max-mac-count`** 命令限制端口可以学习到的 MAC 地址数，并配置学习到的 MAC 地址数达到最大值时，丢弃源 MAC 地址不在 MAC 地址表里的报文，能够避免攻击者申请过多的 IP 地址，在一定程度上阻止了 DHCP 饿死攻击。此时，不存在 DHCP 饿死攻击的端口下的 DHCP

客户端可以正常获取 IP 地址，但存在 DHCP 饿死攻击的端口下的 DHCP 客户端仍可能无法获取 IP 地址。如果封装 DHCP 请求报文的数据帧的 MAC 地址都相同，则通过 **mac-address max-mac-count** 命令无法防止 DHCP 饿死攻击。

DHCP 服务器的 MAC 地址检查功能可以很好地解决饿死攻击问题。开启该功能后，DHCP 服务器检查接收到的 DHCP 请求报文中的 chaddr 字段和数据帧的源 MAC 地址字段是否一致。如果一致，则认为该报文合法，进行后续处理；如果不一致，则丢弃该报文。

(6) DHCP 中继代理功能

设备可以通过配置 DHCP 中继支持代理功能，来防止非法用户攻击 DHCP 服务器。

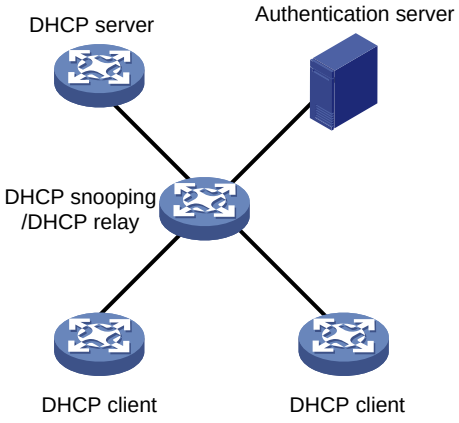
开启该功能后，DHCP 中继收到 DHCP 服务器的应答报文，会把报文中的 DHCP 服务器地址修改为中继的接口地址，并转发给 DHCP 客户端。当 DHCP 客户端通过 DHCP 中继从 DHCP 服务器获取到 IP 地址等网络参数后，DHCP 客户端会把 DHCP 中继当作自己的服务器，来进行后续的 DHCP 功能的报文交互。从而达到了把真正的 DHCP 服务器和 DHCP 客户端隔离开，保护 DHCP 服务器的目的。

3.2 DHCP Option 82功能

在传统的 DHCP 动态分配 IP 地址方式中，同一 VLAN 的用户得到的 IP 地址所拥有的权限是完全相同的。网络管理者不能对同一 VLAN 中特定的用户进行有效的控制。普通的 DHCP 中继代理不支持 Option 82（DHCP Relay Agent Information Option，DHCP 中继代理信息选项），也不能够区分不同的客户端，从而无法结合 DHCP 动态分配 IP 地址的应用来控制客户端对网络资源的访问，给网络的安全控制提出了严峻的挑战。

RFC 3046 定义了 DHCP Relay Agent Information Option（Option 82），在 DHCP 请求报文中附加一些选项信息，使 DHCP 服务器能够更精确地确定用户的位置，从而对不同的用户采取不同的地址分配策略。Option 82 包含两个子选项 Circuit ID（Sub-option 1）和 Remote ID（Sub-option 2）。

图9 Option82 原理示意图



如图 9 所示，Option 82 的工作过程为：

(1) 用户未获得动态 IP 地址前，只有 DHCP 报文可以通过 DHCP Snooping/DHCP 中继设备。

(2) 客户端发出的 DHCP-DISCOVER 报文到达 DHCP Snooping/DHCP 中继设备后，DHCP Snooping/DHCP 中继设备将客户端的位置信息携带到 Option 82 中，将 DHCP-DISCOVER 报文转发给服务器。

(3) 支持 DHCP Option 82 地址分配策略的 DHCP 服务器根据 Option 82 为用户分配相应的 IP 地址，回应 DHCP-OFFER 报文，在该报文中携带原来的 Option 82 信息。

(4) DHCP Snooping/DHCP 中继设备将回应报文中的 Option 82 剥离后，将回应报文发给客户端。

(5) 客户端发出的 DHCP-REQUEST 报文到达 DHCP Snooping/DHCP 中继设备后，DHCP Snooping/DHCP 中继设备将客户端的位置信息携带到 Option 82 中，将 DHCP-REQUEST 报文转发给服务器。

(6) 支持 DHCP Option 82 地址分配策略的 DHCP 服务器回应 DHCP-ACK，在该报文中携带原来的 Option 82 信息。

(7) DHCP Snooping/DHCP 中继设备将 DHCP-ACK 报文中的 Option 82 剥离后，将 DHCP-ACK 报文发给客户端。

通过将 Option 82 与支持 Option 82 地址分配策略的 DHCP 服务器结合，可以实现使用 Option 82 的 Circuit ID 和 Remote ID 子选项按不同的用户权限为用户分配不同的 IP 地址。一方面能更精确地进行 IP 地址管理，另一方面可以让设备进行“源 IP 地址”的策略路由，从而达到不同 IP 地址的用户有不同的路由规则的目的。

3.3 自动配置功能

自动配置功能是设备在空配置启动时自动获取并执行配置文件的功能。

当设备在空配置启动时，系统会自动将设备的指定接口（如 VLAN 接口 1 或第一个以太网接口）设置为 DHCP 客户端，并向 DHCP 服务器获取 IP 地址及后续获取配置文件所需要的信息（例如：TFTP（Trivial File Transfer Protocol，简单文件传输协议）服务器的 IP 地址、TFTP 服务器名、启动文件名等）。如果获取到相关信息，则 DHCP 客户端就可发起 TFTP 请求，从指定的 TFTP 服务器获取配置文件，之后设备使用获取到的配置文件进行设备初始化工作。如果没有获取到相关信息，设备使用空配置文件进行设备初始化工作。

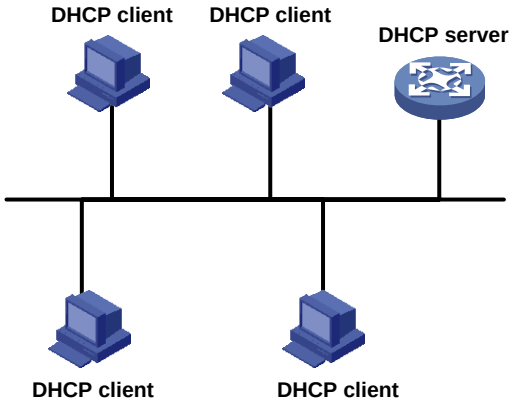
4 典型组网应用

4.1 在本网段内申请地址组网

如图 10 所示，DHCP 客户端与 DHCP 服务器处于同一个网段内，以 DHCP 的方式动态获取 IP 地址和其他网络参数。

组网时需要保证 DHCP 服务器上的地址池网段与 DHCP 服务器的接口 IP 地址网段相匹配。

图10 DHCP 客户端和 DHCP 服务器在同一个网段内

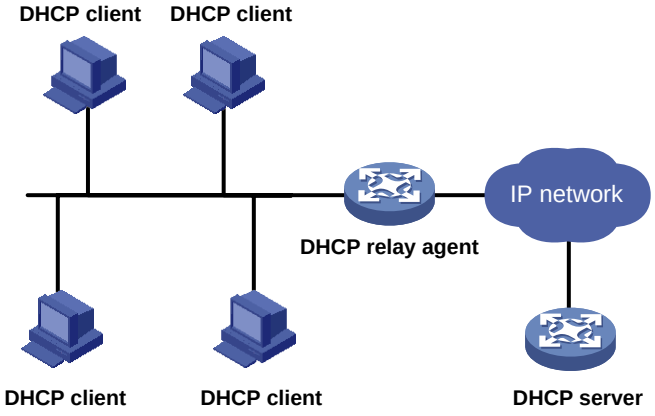


1.2 跨网段申请地址组网

如图 11 所示，用户跨网段申请地址，DHCP 服务器与 DHCP 客户端不在同一个局域网中，客户端通过 DHCP 中继，以 DHCP 的方式动态获取 IP 地址和其他网络参数。

组网时需要把 DHCP 中继的接口网段与 DHCP 服务器的地址池网段配置为一致，否则可能会导致 DHCP 客户端申请的地址不在网关的网段内，致使 DHCP 客户端无法进行通信。同时，DHCP 服务器上需要配置好路由，以保证 DHCP 中继与 DHCP 服务器能够单播通信。

图11 DHCP 客户端和 DHCP 服务器不在同一个网段内

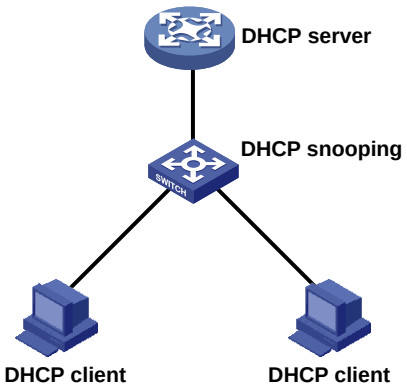


1.3 DHCP Snooping应用组网

如图 12 所示，DHCP 客户端与 DHCP 服务器在同一网段内，二者通过 DHCP Snooping 通信，以保证 DHCP 客户端从合法的 DHCP 服务器获取 IP 地址。还可以通过 DHCP Snooping 在 DHCP 请求报文中添加 Option 82，以便 DHCP 服务器根据 DHCP 客户端的位置信息为其分配 IP 地址。

组网时需要注意的是，DHCP Snooping 设备所有端口默认为非信任端口，需要配置连接服务器的端口为信任端口，否则会导致 DHCP 服务器的应答报文无法传递给 DHCP 客户端。

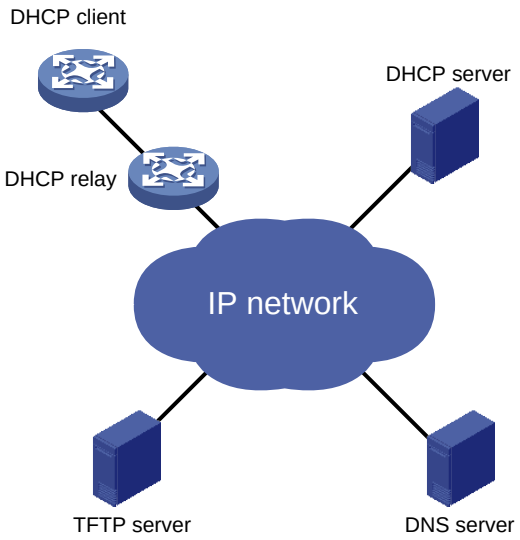
图12 Option 82 典型组网应用



1.4 自动配置应用组网

如图 13 所示，DHCP 客户端在空配置启动时，通过 DHCP 服务器获取 IP 地址、TFTP 服务器地址等信息后，从 TFTP 服务器获取配置文件并执行。

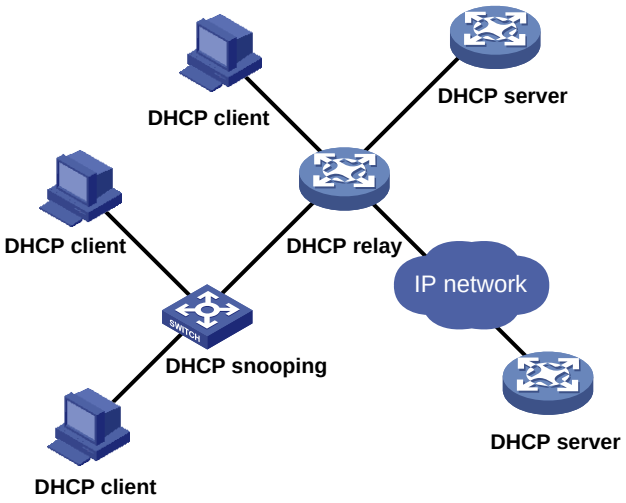
图13 自动配置典型组网应用



1.5 DHCP应用综合组网

如所示，用户跨网段以 DHCP 的方式动态获取 IP 地址，并在二层通过 DHCP Snooping 提高安全性。

图14 DHCP 应用综合组网



5 参考文献

- RFC 951：BOOTSTRAP PROTOCOL(BOOTP)
- RFC 1497：BOOTP Vendor Information Extensions
- RFC 2131：Dynamic Host Configuration Protocol(DHCP)
- RFC 2132：DHCP Options and BOOTP Vendor Extensions
- RFC 3046：DHCP Relay Agent Information Option