DHCP技术白皮书

华为技术有限公司

Huawei Technologies Co., Ltd.

目　录

DHCP 技术白皮书

摘要

本文介绍了DHCP的基本技术和典型应用.

关键词

DHCP，DHCP SERVER，DHCP RELAY， DHCP CLIENT，DHCP SNOOPING，DHCP SECURITY，BOOTP CLIENT。

一 概述

1.1 DHCP 产生的背景

连接到Internet的每台计算机需要在发送或接收数据报前知道其IP地址。另外，计算机还需要其他信息，如路由器的地址、使用的子网掩码和名字服务器的地址。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机从服务器得到自己的IP地址、服务器的IP地址、启动映象文件名、网关IP等等。BOOTP协议使用TCP/IP网络协议UDP的67/68通讯端口。

BOOTP设计用于相对静态的环境，其中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。典型情况下，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地址资源的利用率以及支持无盘网络工作站等应用，需要在BOOTP基础上制定一种自动机制来进行IP地址的分配。

为处理自动地址分配，IETF设计了一个新协议，即动态主机配置协议DHCP（Dynamic Host Configuration Protocol）。此协议从两种方式上扩充了BOOTP。首先，DHCP可使计算机通过一个报文获取所需的全部配置信息。例如：DHCP报文除能获取IP地址外，还能获取子网掩码。第二，DHCP允许计算机快速、动态的获取IP地址。为使用DHCP的动态地址分配机制，管理员必须配置DHCP服务器，使其能提供一组IP地址，称之为地址池。任何时候一旦有新的计算机连接到网络上，该计算机就与服务器联系，并申请一个IP地址。服务器从配置的地址池

中选择一个地址，并将它分配给该计算机。

为做到通用，DHCP允许分配三种类型的地址，管理员可以选择DHCP如何响应每个网络或每台主机。首先，DHCP允许手工配置，管理人员可以为特定的某台计算机配置特定的地址；其次，DHCP也允许自动配置，管理人员允许DHCP服务器为第一次上网的机器分配一个永久地址；同时，DHCP允许完全动态分配，服务器可以使计算机在一段有限时间内“租用”一个地址。

1.2 DHCP 协议简介

DHCP是Dynamic Host Configuration Protocol的缩写，它的前身是BOOTP。

DHCP可以说是BOOTP的增强版本，它分为两个部分：一个是服务器端，而另一个是客户端。所有的IP网路设定资料都由DHCP服务器集中管理，并负责处理客户端的DHCP要求，而客户端则会使用从服务器分配下来的IP环境资料。

DHCP共有八种报文，分别为DHCPDISCOVER，DHCPOFFER，DHCPREQUEST，DHCPACK，DHCPNAK，DHCPRELEASE，DHCPDECLINE，DHCPINFORM。

报文类型分析如下：

- **DHCPDISCOVER报文：**DHCP CLIENT请求地址时，并不知道DHCP SERVER的位置，因此CLIENT会在本地网络内以广播的方式发送请求报文，这个报文称为DISCOVER，目的是发现网络中的DHCP SERVER，因为所有收到DISCOVER报文的SERVER都会发送回应报文，CLIENT据此可以知道网络中存在的SERVER的位置。
- **DHCPOFFER报文：**DHCP SERVER收到DISCOVER报文后，就会在所配置的地址池中查找一个合适的IP地址，加上相应的租约期限和其他配置信息（如GATEWAY，DNS SERVER等），构造一个OFFER报文，发送给用户，告知用户本SERVER可以为其提供IP地址的分配。
- **DHCPREQUEST报文：**DHCP CLIENT可能会收到很多OFFER，所以必须在这些回应中选择一个，也就是选择一个SERVER作为自己的目标SERVER。CLIENT通常选择第一个回应OFFER报文的SERVER作为自己的目标SERVER，并回应一个REQUEST报文，通知SERVER它已经被选中。
- **DHCPACK报文：**DHCP SERVER收到REQUEST报文后，根据REQUEST报文中携带的用户MAC来查找有没有相应的租约记录，如果有则发送ACK报文作为回应，通知用户可以使用分配的IP地址。

- **DHCPNAK报文：**如果DHCP SERVER收到REQUEST报文后，没有发现有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NAK报文作为回应，通知用户无法分配合适IP地址。
- **DHCPRELEASE报文：**当用户不再需要使用分配的IP地址时，就会主动向DHCP SERVER发送DHCPRELEASE报文，告知SERVER用户不再需要分配的IP地址，SERVER会释放被绑定的租约。
- **DHCPDECLINE报文：**DHCP CLIENT收到SERVER回应的ACK报文后，通过地址冲突检测发现SERVER分配的地址冲突或由于其它原因导致不能使用，则发送DHCPDECLINE报文，通知SERVER所分配的IP地址不可用。
- **DHCPINFORM报文：**DHCP CLIENT如果需要从SERVER端获取更为详细的配置信息，则发送DHCPINFORM报文向SERVER进行请求，SERVER收到该报文后，将根据租约进行查找，找到相应的配置信息后，发送DHCPACK报文回应CLIENT。

1.3 DHCP 报文格式

DHCP报文格式如下表所示：

<table>
<tr><td>0 字节</td><td>1 字节</td><td>2 字节</td><td>3 字节</td></tr>
<tr><td>op(1)</td><td>htype(1)</td><td>hlen(1)</td><td>hops(1)</td></tr>
<tr><td colspan="4">xid(4)</td></tr>
<tr><td colspan="2">secs(2)</td><td colspan="2">flags(2)</td></tr>
<tr><td colspan="4">ciaddr(4)</td></tr>
<tr><td colspan="4">yiaddr(4)</td></tr>
<tr><td colspan="4">siaddr(4)</td></tr>
<tr><td colspan="4">giaddr(4)</td></tr>
<tr><td colspan="4">chaddr(16)</td></tr>
<tr><td colspan="4">sname(64)</td></tr>
<tr><td colspan="4">file(128)</td></tr>
<tr><td colspan="4">options(variable)</td></tr>
</table>

表1-1 DHCP 报文格式

DHCP报文的各个字段的具体说明如下：

op ：和BOOTP兼容，只有BOOTREQUEST ＝ 1和BOOTREPLY ＝ 2两个取值，具体的消息类别在数据包的尾部的OPTIONS中。

htype ： 硬件类型代码。

hlen ： 硬件地址长度。[系统目前只对10mb以太网支持，硬件地址长度应该固定为6]

hops ： 客户端清0。DHCP中继服务器在提供中继服务的时候使用。

xid ： 一个由客户端软件产生的随机数，用于识别请求和应答消息匹配。

secs ： 客户进入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。

flags ： 标志字段。这个16 比特的字段，目前只有最左边一个BIT有用。

ciaddr ： 客户的IP地址。只有在客户端处于BOUND，RENEW，REBINDING 的状态下发送消息的时候才设置。可以用来响应ARP协议。

yiaddr ： 由DHCP服务器分配给客户端的IP地址。

siaddr ： 表明DHCP协议流程的下一个阶段要使用的服务器的地址。

giaddr ： DHCP中继器的IP地址。

chaddr ： 客户端的硬件地址。

sname ： 服务器的主机名。

file ： 启动文件名字。

options ： 除IP地址之外的所有其他的子选项都放在这里。

1.4 DHCP 相关概念

DHCP SERVER ： DHCP服务器，为用户提供可用的IP地址。

DHCP CLIENT ： DHCP客户端，通过DHCP动态申请IP地址的用户。

DHCP RELAY ： DHCP中继，用户跨网段申请IP地址时，实现报文的中继转发功能。

DCHP SECURITY ： DHCP安全特性，实现合法用户IP地址表的管理功能。

DHCP SNOOPING ： DHCP监听，记录通过二层设备申请到IP地址的用户信息。

二 DHCP 实现原理

DHCP客户端实际上是一个接口级的概念，一台主机若包含多个以太网接口，则该主机的每一个以太网接口都可以配置成一个独立的DHCP客户端。

交换机上实现的DHCP客户端特性，比主机上实现的DHCP客户端特性要简单一些。

为了获取并使用一个合法的动态IP地址，在不同的阶段，DHCP客户端需要与服务器之间交互不同的信息，两者的交互包括以下几个过程：

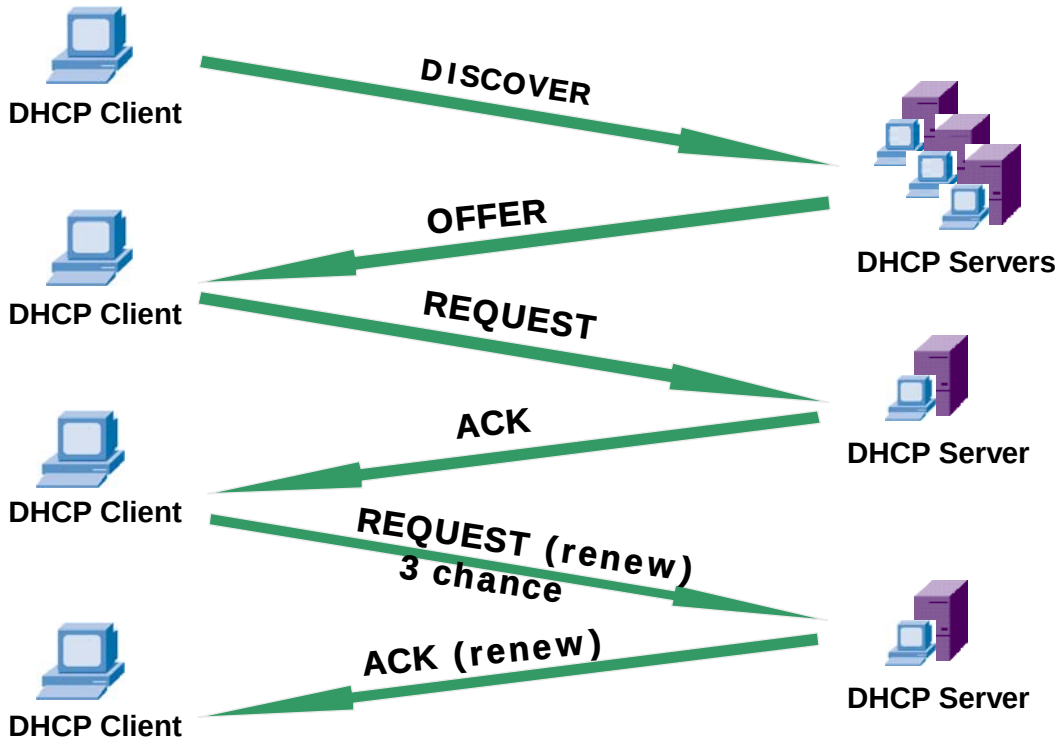

图2-1 DHCP交互过程

1、发现阶段，即DHCP客户机寻找DHCP服务器的阶段。因为DHCP服务器的IP地址对于客户机来说是未知的，所以DHCP客户机以广播方式发送DHCP DISCOVER发现信息来寻找DHCP服务器，即向地址255.255.255.255发送特定的广播信息。网络上每一台安装了TCP/IP协议的主机都会接收到这种广播信息，但只有DHCP服务器才会做出响应。

2、提供阶段，即DHCP服务器提供IP地址的阶段。在网络中接收到DHCP DISCOVER发现信息的DHCP服务器都会做出响应，它从尚未出租的IP地址中挑选一个分配给DHCP客户机，向DHCP客户机发送一个包含出租的IP地址和其他设置的DHCP OFFER提供信息。

3、选择阶段，即DHCP客户机选择某台DHCP服务器提供的IP地址的阶段。如果有多台DHCP服务器向DHCP客户机发来的DHCP OFFER提供信息，则DHCP客户机只接收第一个收到的DHCP OFFER提供信息，然后它就以广播方式回答一个DHCP REQUEST请求信息，该信息中包含向它所选定的DHCP服务器请求IP地址的内容。之所以要以广播方式回答，是为了通知所有的DHCP服务器，他将选择某台DHCP服务器所提供的IP地址。

4、确认阶段，即DHCP服务器确认所提供的IP地址的阶段。当DHCP服务器收到DHCP客户机回答的DHCP REQUEST请求信息之后，它便向DHCP客户机发送一个包含它所提供的IP地址和其他设置的DHCP ACK确认信息，告诉DHCP客户机可以使用它所提供的IP地址。然后DHCP客户机便将获取到的IP地址与网卡绑定，另外，除DHCP客户机选中的服务器外，其他的DHCP服务器都将收回曾提供的IP地址。

5、重新登录。以后DHCP客户机每次重新登录网络时，就不需要再发送DHCP DISCOVER发现信息了，而是直接发送包含前一次所分配的IP地址的DHCP REQUEST请求信息。当DHCP服务器收到这一信息后，它会尝试让DHCP客户机继续使用原来的IP地址，并回答一个DHCP ACK确认信息。如果此IP地址已无法再分配给原来的DHCP客户机使用时（比如此IP地址已分配给其它DHCP客户机使用），则DHCP服务器给DHCP客户机回答一个DHCP NAK否认信息。当原来的DHCP客户机收到此DHCP NAK否认信息后，它就必须重新发送DHCP DISCOVER发现信息来请求新的IP地址。

6、更新租约。DHCP服务器向DHCP客户机出租的IP地址一般都有一个租借期限，期满后DHCP服务器便会收回出租的IP地址。如果DHCP客户机要延长其IP租约，则必须更新其IP租约。DHCP客户机启动时和IP租约期限过一半时，DHCP客户机都会自动向DHCP服务器发送更新其IP租约的信息。

3 DHCP 状态机

DHCP中定义了八种状态，分别为INIT状态，SELECTING状态，REQUESTING状态，BOUND状态，RENEWING状态，REBINDING状态，REBOOT状态和HALT状态。

其中前七种为RFC2131中定义的，HALT状态是我司实现DHCP协议时加入的一个状态，表示DHCP CLIENT处于停用状态。

状态迁移图如下所示：

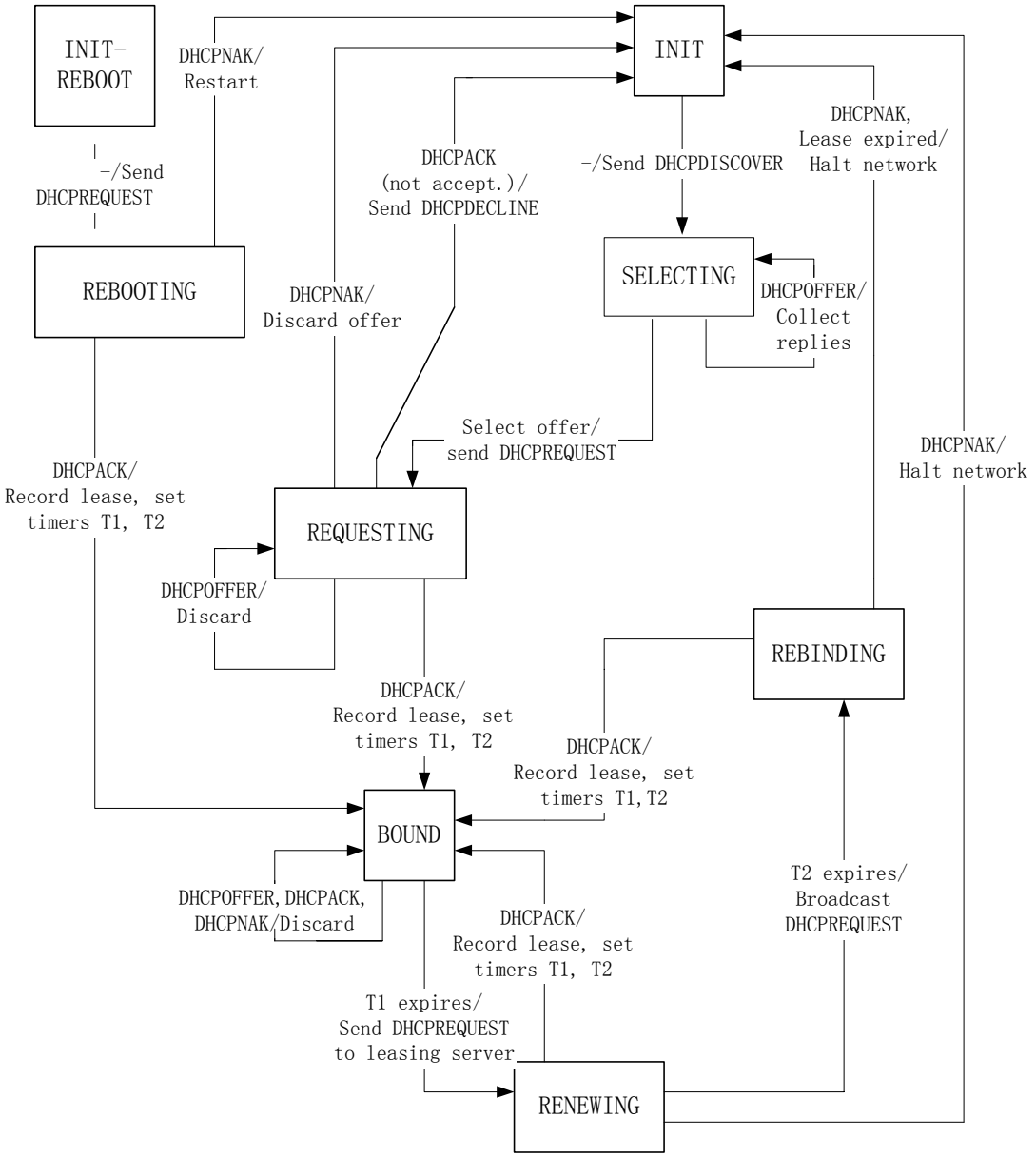

图3-1 DHCP状态迁移图

下面对这八种状态进行详细分析：

- **INIT状态：**当用户第一次启动时，进入初始化状态，为了获取一个IP地址，用户首先要与本地网络上所有的DHCP服务器联系。为此，用户广播一个DHCPDISCOVER报文，并转换到SELECTING状态。
- **SELECTING状态：**当用户处于SELECTING状态时，用户从DHCP服务器收集DHCPOFFER响应。每个响应提供了用户的配置信息，还有服务器给用户提供可以租用的一个IP地址。用户必须选择其中一个响应（一般为最先到达的响应），并与服务器协商租用。为此，用户给服务器发送一个DHCPREQUEST报文，并转换到REQUESTING状态。

- **REQUESTING状态：**为了确认已经接收请求并开始租用，服务器在收到用户的DHCPREQUEST报文后，发送一个DHCPACK报文进行响应。用户收到确认后转换到BOUND状态。
- **BOUND状态：**用户收到SERVER的确认报文后，将分配的IP地址与网卡绑定，开始使用该IP地址。
- **RENEWING状态：**当租约定时器到期时，用户发送DHCPREQUEST报文到分配该IP地址的服务器进行续约，然后用户转换到RENEWING状态等待。
- **REBINDING状态：**用户在进行续约时，如果重绑定定时器到期时用户还是没有收到DHCP SERVER的ACK回应报文，则在本地网络内广播DHCPREQUEST报文，并转换到REBINDING状态等待回应。若在原服务器分配的IP地址到期之前用户收到了原服务器的回应报文，则重新转换到BOUND状态，使用原IP地址。若在原服务器分配的IP地址到期之前用户没有收到原服务器的回应报文，则重新转换到初始化状态重新申请IP地址。
- **REBOOT状态：**为用户的重启动状态，此时用户直接发送DHCPREQUEST报文，申请上一次使用的IP地址，并等待DHCP SERVER的回应报文。
- **HALT状态：**停止状态。用户不再需要使用分配的IP地址时，会主动向DHCP SERVER发送DHCP RELEASE报文，通知SERVER释放被绑定的租约，并转换到停止状态。

4 DHCP 功能特点

DHCP的主要功能是

1、DHCP允许计算机快速、动态的获取IP地址。

2、DHCP报文除能获取IP地址之外，还能获取例如子网掩码等租用地址的详细信息。

DHCP服务的优点：

1、 网络管理员可以验证IP地址和其它配置参数，而不用去检查每个主机；

2、 DHCP不会同时租借相同的IP地址给两台主机；

3、 DHCP管理员可以约束特定的计算机使用特定的IP地址；

4、 可以为每个DHCP作用域设置很多选项；

5、 客户机在不同子网间移动时不需要重新设置IP地址。

DHCP服务的缺点：

1、 DHCP不能发现网络上非DHCP客户机已经在使用的IP地址；

2、 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租出去

的IP地址；

3、 DHCP服务器不能跨路由器与客户机通信，除非路由器允许DHCP转发。

5 华为支持的 DHCP 基本功能

华为公司支持的DHCP基本功能包括BOOTP CLIENT、DHCP CLIENT、DHCP SERVER、DHCP RELAY四个部分。

这里主要介绍DHCP基本功能的功能特点、工作过程以及基本的实现原理，具体操作和命令的使用请参考操作手册和命令手册。

5.1 BOOTP CLIENT 功能

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机从服务器得到自己的IP地址、服务器的IP地址、启动映象文件名、网关IP等等。BOOTP协议使用TCP/IP网络协议UDP的67/68通讯端口。

BOOTP协议的工作过程为：

第1步，由BOOTROM芯片中的BOOTP启动代码启动客户机，此时客户机还没有IP地址，它就用广播形式以IP地址0.0.0.0向网络中发出IP地址查询的请求，这个请求帧中包含了客户机的网卡MAC地址。

第2步，网络中的运行BOOTP服务的服务器接收到的这个请求帧，根据这帧中的MAC地址在BOOTP启动数据库中查找这个MAC的记录，如果没有此MAC的记录则不响应这个请求，如果有就将FOUND帧发送回客户机。FOUND帧中包含的主要信息有客户机的IP地址、服务器的IP地址、硬件类型、网关IP地址、客户机MAC地址和启动映象文件名等。

第3步，客户机根据FOUND帧中的信息通过TFTP服务器下载启动映象文件，并将此文件模拟成磁盘，从这个模拟磁盘启动。

目前我们所使用的BOOTP CLIENT已经做了扩展（包括我司的交换机和2000系统的实现），实现与DHCP CLIENT类似，但较为简单，没有状态机。

BOOTP协议工作过程示意图如下所示：

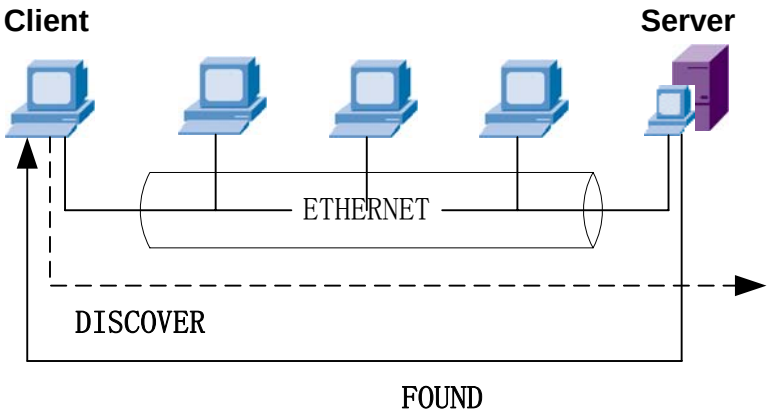

图5-1 BOOTP服务工作过程示意图

BOOTP服务存在的缺陷：

- BOOTP设计用于相对静态的环境，其中每台主机都有一个永久的网络连接。管理员创建一个BOOTP配置文件，该文件定义了每台主机的一组BOOTP参数。
- 如果计算机保持位置不便，而且管理者有足够的IP地址为每台机器分配唯一的地址，静态参数分配将工作的很好。但随着无线联网和移动便携技术的发展，BOOTP已经变得不再合适了。
- 若DHCP SERVER分配的IP地址不可用（例如IP地址冲突），不能自动重新申请一个新的IP地址，而需要管理员来处理。

5.2 DHCP CLIENT 功能

DHCP CLIENT是DHCP服务的客户端，是整个DHCP活动的触发者和驱动者，通过DHCP报文和SERVER进行交互，得到IP地址和相关配置信息。

DHCP CLIENT的工作过程为：

- DHCP CLIENT开始申请IP地址时，发出广播的DISCOVER报文，收到回应的OFFER，然后发出广播的REQUEST报文，收到回应的ACK，这样就得到地址。
- 对SERVER分配的IP地址进行有效性检测，若分配的IP地址不可用（例如地址冲突等），则自动迁移到初始状态重新申请地址。
- 到达续约时间后（租约的一半），发出单播的REQUEST报文进行续约，如收到ACK后更新租约，如收到NAK后，则重新发起申请过程。
- 如果单播的续约报文没有回应，到达重新绑定时间后（租约的7/8）会发送广播的

续约报文。

- CLIENT重启后不进行DISCOVER的申请，而是直接发送REQUEST报文给SERVER。
- CLIENT在进行申请地址时，报文中的Requested IP address字段会填入之前使用过的IP地址，如果这时SERVER认为可以使用那么就进行分配，如果该地址有人使用了，SERVER回应NAK，CLIENT收到后重新进行申请，该字段置空。

DHCP CLIENT工作过程示意图如下所示：

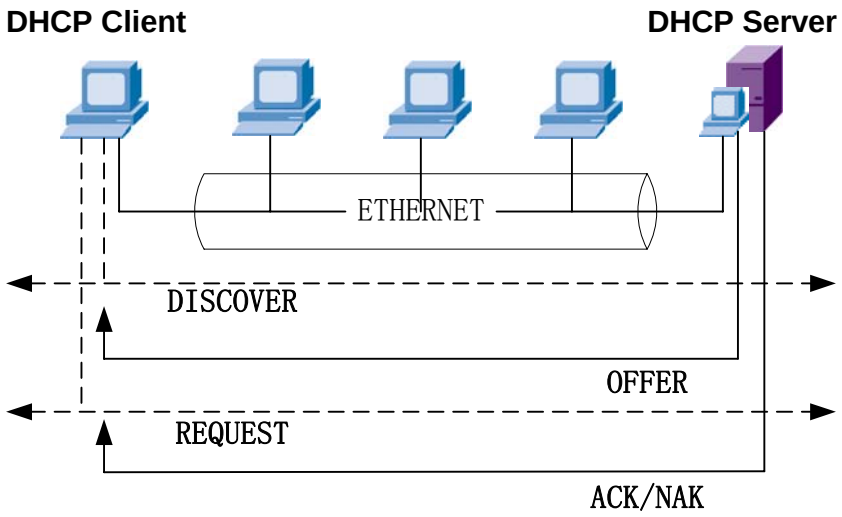

图5-2 DHCP CLIENT工作过程示意图

DHCP服务解决了BOOTP服务存在的缺陷，相对于BOOTP，动态地址分配是DHCP最重要、最新颖的功能。第一，与BOOTP所用的静态地址分配不同，动态地址分配不是一对一的映射，而且服务器不需要预先知道客户的身份。第二，而且，DHCP服务器可以配置成任一个机器都可以获取IP地址并开始通信。

因此，DHCP使得设计自动配置的系统成为可能。一台计算机上网后，它使用DHCP获取一个IP地址，然后配置其TCP/IP软件使用此地址。总之，由于DHCP允许一台主机无人干预即可获得通信所需的全部参数，所以DHCP是允许自动配置的。这些都是DHCP优于BOOTP的方面。

5.3 DHCP SERVER 功能

DHCP SERVER是DHCP服务的提供者，它通过DHCP报文与DHCP CLIENT进行交互，为各种类型的用户分配合适的IP地址，并可以根据需要进行地址池和其它网络参数的相关配置。

DHCP SERVER实现的主要功能为：

1、 创建和删除地址池

网络管理员在DHCP SERVER上创建地址池。当CLIENT向SERVER提出DHCP请求的时候，SERVER将从IP地址池中取得空闲的IP地址以及其他的参数给CLIENT。一个SERVER可能有一个或多个地址池。创建地址池后还需要把这个地址池的其他必要参数都配置上才是可用的地址池。

DHCP SERVER可以配置网络地址池和主机地址池两种类型的地址池。网络地址池用于为用户提供动态分配的IP地址，主机地址池用于为用户提供管理员静态绑定的IP地址。

网络地址池又可以分为全局地址池和接口地址池，全局地址池可以为所有用户提供IP地址分配，接口地址池只为本虚接口下直连用户提供IP地址的分配。

2、 配置地址池的相关参数

系统可以对地址池配置DNS、Domain Name、WINS、netbios-node-type等参数，用于CLIENT的网络配置。具体操作和配置请参考操作手册和命令手册中的网络协议操作第六章。

3、 处理CLIENT发送来的DHCP报文

DHCP SERVER共接收以下五种DHCP报文：

- DHCPDISCOVER
- DHCPREQUEST
- DHCPDECLINE
- DHCPRELEASE
- DHCPINFORM

对每一种报文的处理如下：

1、 DHCPDISCOVER

（1）检查地址池是否有可分配地址，如果没有，则向系统管理员报告；如果有，按照如下的优先顺序进行选择：

- 当前绑定中的当前地址；
- CLIENT的以前地址(现在已经expire或是release了,并且是available的)；
- 在Requested IP Address option中并且valid and available.；
- 从地址池中分配一个可用地址，根据消息所接收到的子网字段（subnet，giaddr=0）或是根据中继代理（relay agent）的地址(giaddr<>0)进行分配。

（2）选定租约：根据选定IP地址来决定用户的绑定租约。

（3）处理CLIENT请求的其它网络参数。

（4）发送回应的OFFER报文。

2、 DHCPREQUEST

DHCPREQUEST的三个来源：

- CLIENT响应SERVER的DHCPOFFER；
- CLIENT确认一个先前分配的IP地址；
- CLIENT请求延长某个网络地址的LEASE；

如果DHCPREQUEST包括一个SERVER IDENTIFIER OPTION，则是情形1，否则是情形2或者3。

如果REQUEST包中有CLIENT IDENTIFIER或是LIST OF REQUESTED PARAMETERS，那么CLIENT必须在以后的报文中都包含它们（或其中的某一个）。

DHCP SERVER根据收到的REQUEST报文的类型进行不同的处理，若可以分配合法的IP地址，则回应CLIENT一个DHCPACK报文。

3、 DHCPDECLINE

若CLIENT发现SERVER分配的IP地址不可用（例如IP地址冲突），则向SERVER发送一个DHCPDECLINE报文，SERVER将该网络地址标记为NOT AVAILABLE。

4、 DHCPRELEASE

SERVER将CLIENT回应的非法网络地址标记为NOT ALLOCATED。它同时应该保持这个CLIENT的初始化参数，以便将来的REUSE。

5、 DHCPINFORM

CLIENT向SERVER发送DHCPINFORM报文用于请求SERVER分配给CLIENT租约的详细信息，包括所属地址池的详细配置等信息。

4、 给CLIENT分配一个可用的IP地址

SERVER按照以下优先级为CLIENT分配IP地址

- 按照SERVER数据库中与CLIENT绑定的地址（已经分配给该CLIENT并且还没有过期的）；
- CLIENT以前曾经使用过的地址（以前分配给过该CLIENT，但已经过期；当该地址链为空时，自动从出租地址链中重新获得过期地址）；
- DHCPDISCOVER包中请求IP地址选项（requested ip addr option）中的地址（用户上次释放过的IP地址）；
- 地址池中可用的地址顺序进行查找，将最先找到的并且没有冲突的地址返回；

- 检测冲突地址链中的冲突地址，如果可以使用，则重新分给用户；
- 从正常分配出去的地址中为CLIENT的DISCOVER请求分配地址（用于DHCP SERVER收到非法攻击导致IP地址耗尽的情况）；
- 如果未找到可用地址，向管理员报告错误。

5、 为CLIENT处理延长租期的请求

CLIENT在分配租约使用一半时间后，会主动向SERVER申请继续使用该IP地址，SERVER对CLILENT的续约请求进行处理，若发现请求的IP地址可用，则回应ACK报文给CLIENT，告知可以继续使用该IP地址，并更新相应的租约和定时器信息。

6、 设定或释放保留地址

保留地址是DHCP协议的IP地址池中不分配的地址段。一旦设定为保留地址后，这个区间的IP地址就不再参加整个IP地址池的分配而保留起来，将保留地址的起始地址和结束地址记录到该IP地址池的参数中。

7、 探测分配IP地址的活动情况

在DHCP SERVER向客户端分配IP地址时，SERVER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，这就需要SERVER发送ICMP（ping）的数据包来对所分配的IP进行探测。

SERVER对需要探测的IP地址发送ping数据包，如果在规定的时间内没有应答（默认情况下是500 ms），那么SERVER就会再次发送ping数据包。到达规定的次数（默认情况下是2次）后，如果仍没有应答，则所分配的IP地址可用。否则系统将向管理员报告出错信息。探测IP地址不影响SERVER对其它CLIENT的响应。

如果IP地址可用，SERVER将继续完成IP地址的配置。否则报告出错信息。

8、 配置相关网络参数以告知CLIENT

DHCP SERVER可以配置以下网络参数并通过交互报文告知CLIENT：

- 配置CLIENT网关地址；
- 配置CLIENT使用的DNS服务器；
- 配置CLIENT网络使用的域名；
- 配置CLIENT的NETBIOS服务器IP地址；
- 配置CLIENT所对应的NETBIOS节点类型。

5.4 DHCP RELAY 功能

使用DHCP协议，客户机可以向DHCP服务器动态的请求配置信息，包括分配的IP地址，子网掩码，缺省网关等信息。

然而，原始的DHCP协议要求客户机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客户机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，于是许多网络上的DHCP客户机可以共同使用一个DHCP服务器。

DHCP协议是以客户/服务器模式工作的，当DHCP客户启动时，发送配置请求报文，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络上的DHCP服务器。服务器根据客户提供的必要信息，再次通过DHCP中继发送配置信息给客户机，完成对主机的动态配置。

DHCP RELAY功能示意图如下所示：

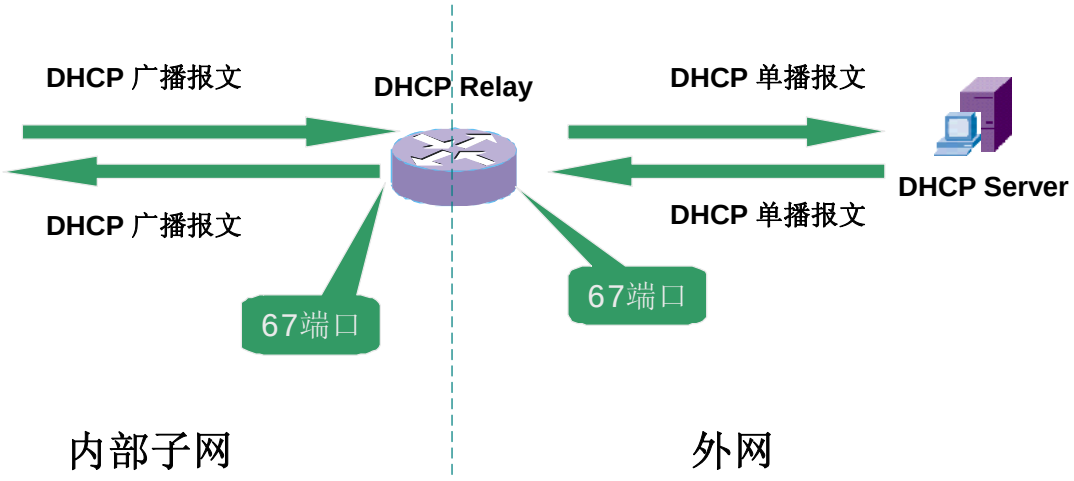

图5-3 DHCP RELAY功能示意图

DHCP RELAY实现的主要功能为：

1、 配置IP辅助地址

用户通过命令行界面，在接口配置模式下，为接口配置IP辅助地址，即指明DHCP SERVER的IP地址。在接口控制块中维护辅助地址信息，供DHCP中继时使用。

各接口可以配置多个IP辅助地址（每个接口可配置的的IP辅助地址最大个数为20，可以根据具体产品需要调整该值），IP辅助地址将被保存在接口控制块中。

2、 处理DHCP中继报文

DHCP中继代理不是对所有收到的DHCP报文都作中继处理，在中继前需要识别需要处理的DHCP报文。需要强调的是在服务器端如回应报文发送给DHCP中继，则回应报文目的端口设为67。

DHCP中继模块通过Socket收发DHCP中继报文。从各接口接收的DHCP协议报文，都是由Socket接收。

对DHCP报文识别后，交由中继模块处理。通常DHCP请求报文的源地址是0， DHCP中继代理必须可以接收IP源地址为0的报文。只接收UDP目的端口号为67的 DHCP报文。

（1）处理请求报文

已识别的DHCP报文，UDP目的端口号为67（BOOTPS），且BOOTP报文头中的op域是BOOTREQUEST（1），即DHCP客户机发给服务器的请求报文。将已识别的DHCP报文发送到指定的DHCP服务器。

DHCP客户机发出的请求报文，一般目的地址为广播地址，目的端口号为67，DHCP中继代理需要将报文发送至DHCP服务器处理，DHCP服务器由报文接收接口所配置的IP辅助地址来指定。

- 为防止DHCP报文中继形成环路，抛弃报文头hops域大于限定跳数的DHCP请求报文，限定跳数定义可以调整，缺省为4，最大不超过16。
- DHCP中继代理在中继DHCP请求报文前，必须检查giaddr域，如果是0，需要将giaddr域设置为接收请求报文的接口的IP地址，如果接口有多个IP地址，可选择其一，并在以后从该接口中继的所有请求报文都使用该IP地址。如果giaddr域不是0，则不修改giaddr域。
- DHCP中继代理中继DHCP报文时将hops域增加1跳，表明已经过一次DHCP中继。
- BOOTP报文头所有其它域在发送前不能被DHCP中继代理修改。
- DHCP请求报文被中继到新的目的地，该目的地就是报文接收接口的IP辅助地址，可以是DHCP服务器地址或另一个中继代理的地址。
- 如果接收接口有多个IP辅助地址，可以选择其一作为中继的新目的地址，对于来自同一个DHCP客户机的DHCP请求报文必须使用同一个辅助地址作为目的地址。具体实现是通过chaddr域识别DHCP客户机。
- 对于同一个接口收到的来自不同DHCP客户机的请求报文，中继采用轮循方式选择一个

IP辅助地址作为报文新的目的地址。

- 对于某个接口接收到的来自不同DHCP客户机的请求报文，中继采用轮循选择一个IP辅助地址作为其新的目的地址。
- 中继的请求报文的TTL采用新缺省值，而不是原来请求报文的TTL减1。对中继报文的环路问题可以通过hops域来避免。

（2）处理回应报文

从各接口收到的已识别的DHCP报文，UDP目的端口号为67，且BOOTP报文头中的op域是BOOTREPLY（2），即DHCP服务器希望通过中继代理发给DHCP客户机的回应报文。将已识别的DHCP报文发送到指定的DHCP客户机。

DHCP服务器发给中继的BOOTREPLY报文，一般目的地址为中继代理在处理请求报文时设置的giaddr，目的端口号为67，DHCP中继代理需要将报文发送至DHCP客户机处理，DHCP客户机与报文的giaddr所属的接口直连，通过该接口采用广播或单播方式发送至DHCP客户机。

- 中继代理假设所有的BOOTREPLY报文是发给直连的DHCP客户机。giaddr域用来识别与客户机直连的接口。如果giaddr不是本地接口的地址，BOOTREPLY报文被丢弃。
- 中继代理检查报文的BROADCAST标志，如果置为1，则发广播报文给DHCP客户机，否则发送单播报文，其目的地址为yiaddr，链路层地址为chaddr。
- 中继代理不能修改 BOOTREPLY 报文的任何域。

6 华为支持的 DHCP 扩展功能

华为支持的DHCP扩展功能包括DHCP SECURITY、DHCP SECURITY增强和DHCP SNOOPING三个特性。这里的扩展功能指的是对DHCP基本的CLIENT、SERVER和RELAY功能的扩展。

这里主要介绍DHCP扩展功能的功能特点、工作过程以及基本的实现原理，具体操作和命令的使用请参考操作手册和命令手册。

6.1 DHCP SECURITY 功能

DHCP SECURITY的主要功能是负责对DHCP RELAY用户地址表的管理，实现合法用户IP地址表的管理功能：包括动态添加、手工添加、手工删除以及查询功能，并通过与ARP模块配合实现禁止非正常获取IP地址的用户上网的功能。这样就可以有效的进行地址规划和分配，实现对用户控制的功能，保护同一子网下其他VLAN的地址资源不被抢占。

DHCP SECURITY示意图如下所示：

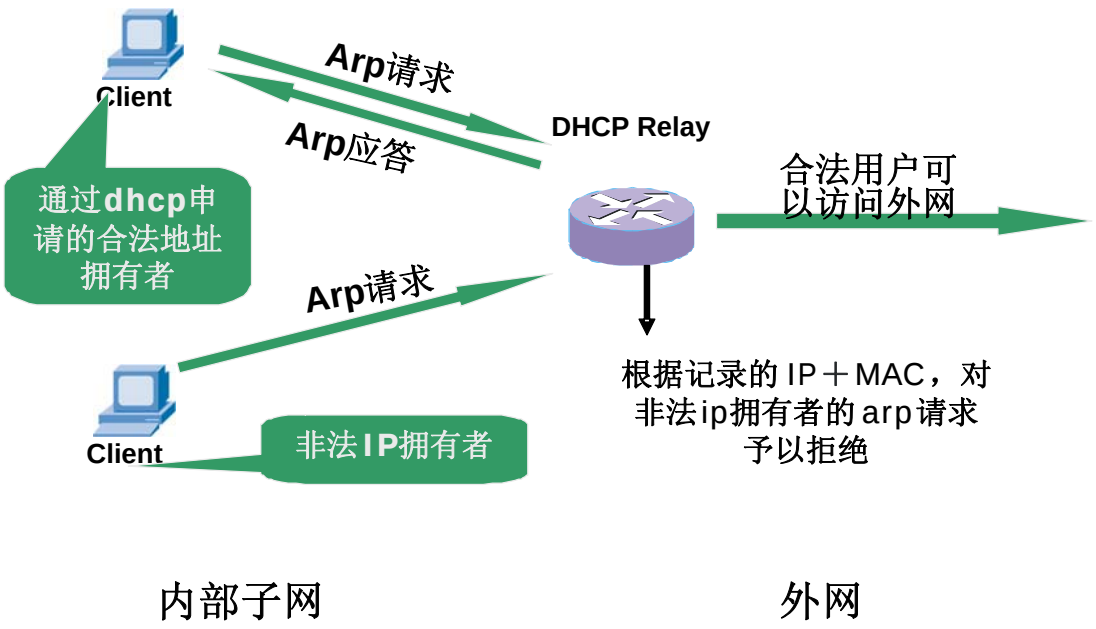

图6-1 DHCP SECURITY示意图

1、DHCP SECURITY实现的基本功能如下：

（1）合法用户IP地址表的管理

确保所有合法用户都在DHCP SECURITY的表项中记录地址信息。通过DHCP中继获取的地址可以动态添加，合法使用固定IP地址的用户可以手工添加，提供手工删除以及查询的功能。

（2）禁止非正常获取IP地址的用户上网的功能

该功能需要ARP模块配合，对于与用户地址表中MAC地址与IP地址不匹配的ARP请求不返回ARP应答。

（3）表项老化功能

由于某些三层设备无法处理DHCP CIENT发出的DHCPRELEASE报文（单播报文不上CPU），因此造成DHCP SECURITY的表项在CLIENT主动释放IP地址后，依然保留用户的绑定信息，使DHCP SECURITY的表项无法老化，为了解决这个问题，我司目前提供握手功能来实现DHCP SECURITY的表项老化。

握手功能即DHCP RELAY模拟CLIENT定期向SERVER发送REQUEST报文，报文的内容根据SECURITY的表项的内容来构建，但源MAC使用交换机的桥MAC，以和正常发送的REQUEST报文进行区分。SERVER收到REQUEST报文后，检测申请的IP地址是否可以分配，若可以分配则回应一个ACK报文，若不可以分配则回应一个NAK报文。RELAY收到SERVER回应的报文后，进行

判断，若收到了ACK报文则证明用户表项中的该IP地址已经被释放（因为已经可以被再次分配了），可以将其老化掉了，就将该表项进行删除操作；若收到了NAK报文则证明用户表项中的该IP地址还没有被用户释放，继续保留该表项。DHCP RELAY可以通过这种定期的和SERVER的握手来对DHCP SECURITY的表项进行老化。

6.2 DHCP SECURITY 增强功能

DHCP SECURITY增强特性实现主要功能如下：

- 仅以一条命令就实现一条MAC和IP的双向唯一绑定。
- 必须可以实现“绑定和不绑定的同时存在”，例如若干台微机接入本交换机，其中10台实现MAC和IP的双向唯一绑定，其他的微机则可以自由的不受限的进行连接。
- 随意的增加或减少自由连接的机器并不需要再对交换机进行设置，以最大限度的实现管理高效。

6.3 DHCP SNOOPING 功能

DHCP SNOOPING即DHCP服务的二层监听功能，开启DHCP SNOOPING功能后，以太网交换机就可以从接收到DHCPACK或DHCPREQUEST报文中提取并记录IP地址和MAC地址信息。

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。我司的二层交换机采取监听DHCP广播报文的方法来记录用户获取的IP地址信息。

DHCP SNOOPING主要通过过滤不信任DHCP报文和创建、维护DHCP SNOOPING绑定表实现下面两方面的功能：

1、过滤不信任端口上的DHCP SERVER的响应消息；

2、记录用户的IP地址和MAC地址的绑定关系。

DHCP SNOOPING功能通过设置信任端口来实现对不信任DHCP报文的过滤功能，来过滤通过该端口的DHCP OFFER/ACK/NAK报文。目前我司实现的DHCP TRUST功能是需要和DHCP SNOOPING功能配合使用的。启动DHCP SNOOPING功能后，必须启动TRUST功能，否则端口的DHCP OFFER/ACK/NAK报文被过滤，用户不能正常申请到IP地址。

DHCP SNOOPING功能目前我司的三层交换机也支持，是根据特定用户的需求提供的，但是由于某些三层交换机不能处理单播报文，因此三层交换机上的DHCP SNOOPING用户地址表

是根据收到的DHCP REQUEST广播报文来记录的，目前不能实现老化，也不能对RENEW报文进行处理。

7 DHCP 的典型组网应用

7.1 在本网段内申请地址

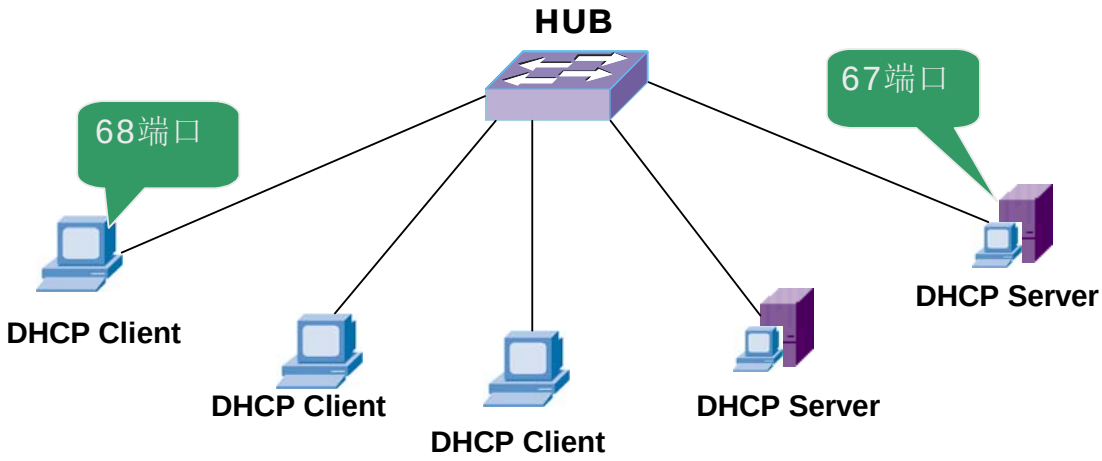

图7－1 DHCP CLIENT和 DHCP SERVER在同一个网段内

用户与DHCP SERVER处于同一个网段内，以DHCP的方式动态获取IP地址。

配置步骤如下：

配置server1

```
[server1] dhcp enable
[server1] interface vlan 1
[server1- Vlan-interface1] ip address 1.1.1.5 255.255.0.0
[server1] dhcp server ip-pool 1
[server1-dhcp1] network 1.1.1.0 mask 255.255.0.0
```

配置server2

```
[server2] dhcp enable
[server2] interface vlan 1
[server2- Vlan-interface1] ip address 1.1.2.5 255.255.0.0
[server2] dhcp server ip-pool 1
```

[server2-dhcp1] network 1.1.2.0 mask 255.255.0.0

配置用户

[client] interface vlan 1

[client- Vlan-interface1] ip address dhcp-alloc

7.2 跨网段申请地址

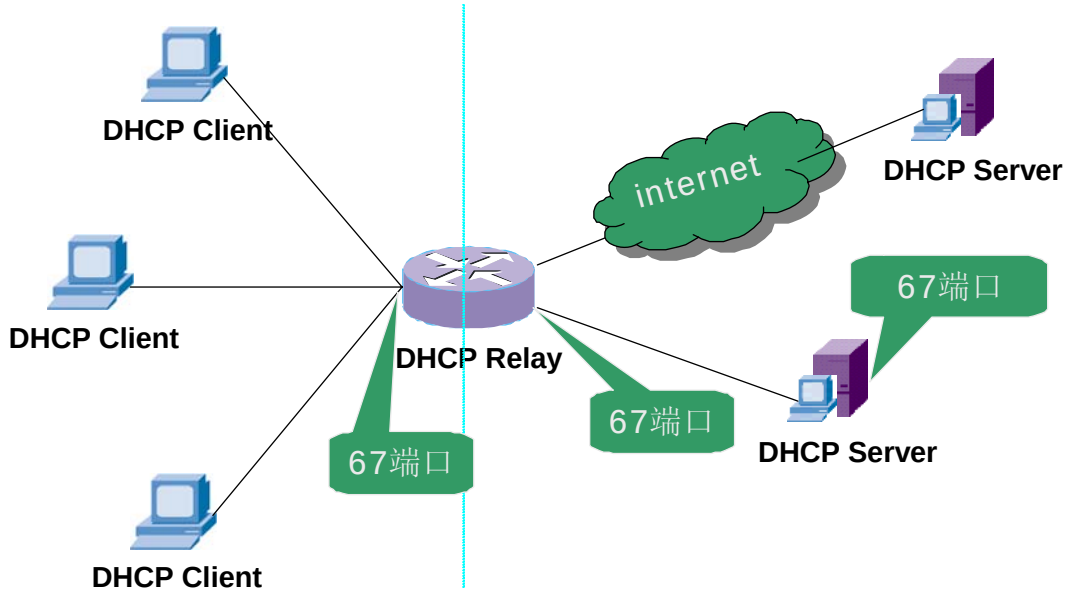

图7－2 DHCP CLIENT和DHCP SERVER不在同一个网段内

用户跨网段申请地址，以DHCP的方式动态获取IP地址。

配置步骤如下：

配置server1

[server1] dhcp enable

[server1] interface vlan 1

[server1- Vlan-interface1] ip address 1.1.1.5 255.255.0.0

[server1] dhcp server ip-pool 1

[server1-dhcp1] network 1.50.1.0 mask 255.255.0.0

配置server2

[server2] dhcp enable

[server2] interface vlan 1

```
[server2- Vlan-interface1] ip address 1.2.2.5 255.255.0.0
[server2] dhcp server ip-pool 1
[server2-dhcp1] network 1.60.1.0 mask 255.255.0.0
```

配置relay

```
[relay] interface vlan 1
[relay- Vlan-interface1] ip address 1.50.1.5 255.255.0.0
[relay- Vlan-interface1] ip relay address 1.1.1.5
[relay- Vlan-interface1] dhcp select relay

[relay] vlan 2
[relay- Vlan2] port e0/1
[relay- Vlan2] interface vlan 2
[relay- Vlan-interface2] ip address 1.60.1.5 255.255.0.0
[relay- Vlan-interface1] ip relay address 1.2.2.5
[relay- Vlan-interface1] dhcp select relay

[relay] vlan 3
[relay- Vlan3] port e0/2
[relay- Vlan3] interface vlan 3
[relay- Vlan-interface3] ip address 1.1.5.5 255.255.0.0

[relay] vlan 4
[relay- Vlan4] port e0/3
[relay- Vlan4] interface vlan 4
[relay- Vlan-interface4] ip address 1.2.5.5 255.255.0.0
```

配置用户

```
[client] interface vlan 1
[client- Vlan-interface1] ip address dhcp-alloc
```

VLAN 1内的用户可以申请到1.50.0.0网段的地址，VLAN 2内的用户可以申请到1.60.0.0网段的地址。

7.3 DHCP 应用综合组网图

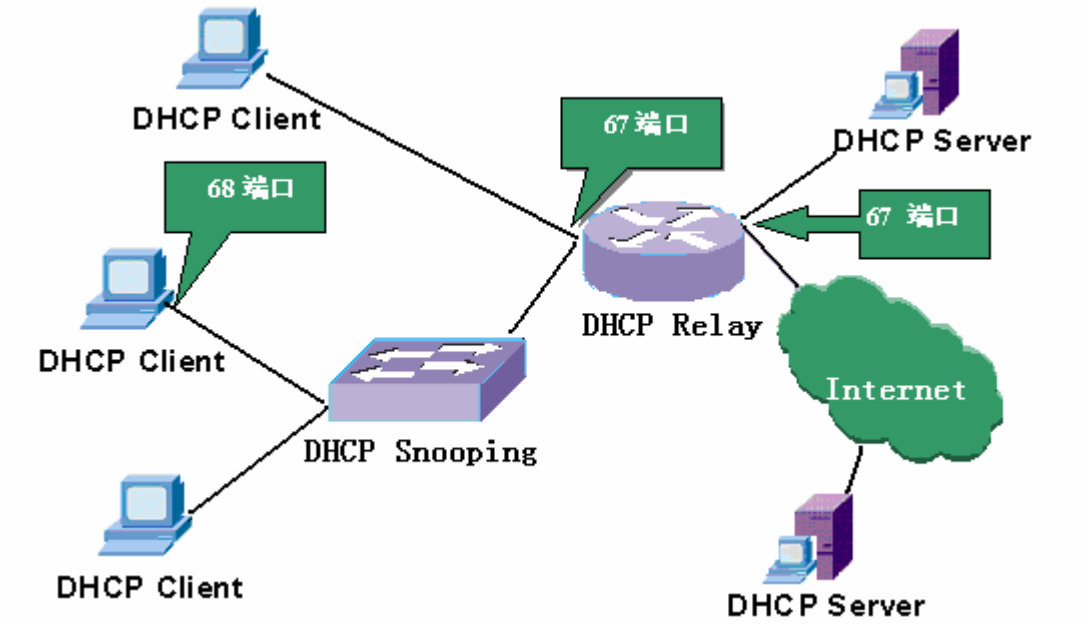

图 7－3 DHCP 应用综合组网图

用户跨网段申请地址，以DHCP的方式动态获取IP地址,该综合应用中包括DHCP SNOOPING、DHCP RELAY等。

配置步骤如下：

配置server1

```
[server1] dhcp enable
[server1] interface vlan 1
[server1- Vlan-interface1] ip address 1.1.1.5 255.255.0.0
[server1] dhcp server ip-pool 1
[server1-dhcp1] network 1.50.1.0 mask 255.255.0.0
```

配置server2

```
[server2] dhcp enable
[server2] interface vlan 1
[server2- Vlan-interface1] ip address 1.2.2.5 255.255.0.0
[server2] dhcp server ip-pool 1
```

```
[server2-dhcp1] network 1.60.1.0 mask 255.255.0.0
```

配置relay

```
[relay] interface vlan 1
[relay- Vlan-interface1] ip address 1.50.1.5 255.255.0.0
[relay- Vlan-interface1] ip relay address 1.1.1.5
[relay- Vlan-interface1] dhcp select relay

[relay] vlan 2
[relay- Vlan2] port e0/1
[relay- Vlan2] interface vlan 2
[relay- Vlan-interface2] ip address 1.60.1.5 255.255.0.0
[relay- Vlan-interface1] ip relay address 1.2.2.5
[relay- Vlan-interface1] dhcp select relay

[relay] vlan 3
[relay- Vlan3] port e0/2
[relay- Vlan3] interface vlan 3
[relay- Vlan-interface3] ip address 1.1.5.5 255.255.0.0

[relay] vlan 4
[relay- Vlan4] port e0/3
[relay- Vlan4] interface vlan 4
[relay- Vlan-interface4] ip address 1.2.5.5 255.255.0.0
```

配置snooping

```
[snooping]dhcp-snooping
[snooping]int Ethernet 0/1
[snooping-Ethernet0/1]dhcp-snooping trust
```

注意：DHCP SNOOPING 必须和端口TRUST功能配合使用，并且将设备的上行端口设置为信任端口。

配置用户

[client] **interface vlan 1**

[client- Vlan-interface1] **ip address dhcp-alloc**

VLAN 1内的用户可以申请到1.50.0.0网段的地址，VLAN 2内的用户可以申请到1.60.0.0网段的地址。

8 与其它功能配合使用情况

8.1 与 Portal 配合使用

PORTAL业务是Lanswitch平台软件的一个特性，它利用硬件提供的流过滤功能实现基于PORTAL业务的认证、计费。

PORTAL认证的原理是：用户通过DHCP动态获取IP地址后，只能访问PORTAL网站，并且任何其它访问都被无条件地重定向到PORTAL服务器，用户只有主动地登录PORTAL服务器通过认证后，才能获得Internet的网络访问权限。

PORTAL特性只涉及到与DHCP RELAY模块的配合使用，与其它DHCP模块没有交互。对于PORTAL的两种认证方式分别简述一下：

1、直接认证方式

要求认证设备与认证用户在同一个网段内，DHCP中继只是处理正常的DHCP报文转发，与认证本身没有任何交互。认证成功后，认证设备会记录用户的认证状态，不需要对DHCP RELAY用户地址表项做任何操作。

2、二次地址认证方式

要求认证设备与认证用户在同一个网段内，这种认证方式需要两次通过DHCP方式获得IP地址。且认证通过后也要基于DHCP RELAY用户地址表及DHCP SECURITY地址检查功能来实现对用户的限制。主要过程如下：

- 首先通过DHCP获得一个私网IP地址，此时DHCP RELAY会判断用户的状态，若为非连接状态则取虚接口从地址，转发报文，同时会记录这个私网IP地址及认证状态。
- PORTAL获得私网IP地址后，进行认证。
- 认证成功后，释放私网IP地址，重新获取公网IP地址。
- 获取公网IP时，DHCP RELAY会进行判断，若为正常连接状态且为公网IP地址则正常

转发报文，同时记录这个公网IP地址及认证状态，否则丢弃该报文。

- 用户以二次地址认证方式进行PORTAL认证必须要启动DHCP SECURITY地址检查功能。当认证通过且正常获取到公网IP地址后，用户访问网络资源时，认证设备会搜索DHCP RELAY用户地址表，若表项中记录了该用户的IP和MAC绑定关系，则允许其上网，否则不允许。

8.2 与 802.1X 配合使用

802.1X协议解决了无线局域网用户的接入认证问题，定义了基于端口的网络接入控制协议，基本思想是通过某种认证机制控制端口的授权状态。

802.1X认证过程本身与DHCP模块并没有关系，只在以下两种情况下会与DHCP模块有交互：

- 当用户认证通过后，发实时计费报文时，读取DHCP RELAY/ DHCP SNOOPING用户地址表，获得用户通过DHCP动态获取的IP地址，填入计费报文的free ip address字段中，并将该属性上传，用于实时计费。
- 当用户下线时，会删除DHCP RELAY/ DHCP SNOOPING表项，但不会对DHCP RELAY/ DHCP SNOOPING表项进行写操作。

9 我司 DHCP 特性解决方案综合分析

我司的DHCP特性是遵循标准的RFC2131和RFC2132实现的，目前可以全面支持RFC中所述的BOOTP和DHCP基本及扩展功能，包括：DHCP CLIENT/BOOTP CLIENT，DHCP RELAY，DHCP SERVER，DHCP SECURITY，DHCP SNOOPING。

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，华为公司的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：

（1）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；

（2）具有出色的业务支持能力及灵活的组网方案；

（3）良好的易用性和可配置性；

（4）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；

（5）方便管理、部署经济、设备开销低。

10 附录

10.1 DHCP 的相关标准

rfc951： BOOTP

rfc2131： DHCP

rfc2132： DHCP OPTION

rfc1497： BOOTP VENDOR

10.2 DHCP 各个模块缺省配置

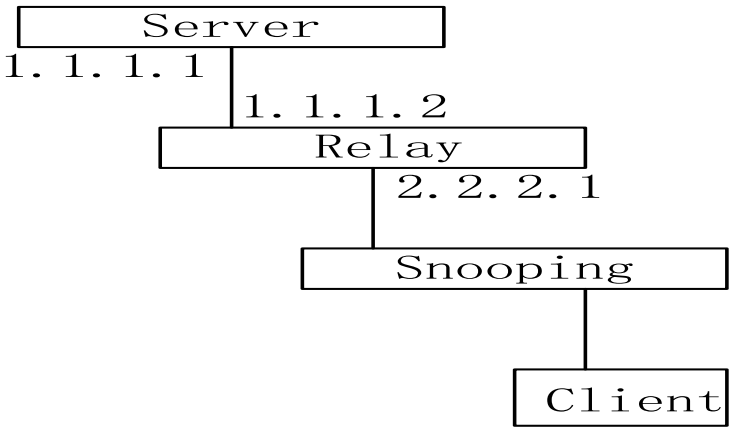

图10-1 DHCP综合组网配置图

Server的配置 ：

```
[Server] dhcp server ip-pool 2.2.2.0
[Server -dhcp-2.2.2.0] network 2.2.2.0 mask 255.255.255.0
[Server -dhcp-2.2.2.0] gateway-list 2.2.2.1
[Server -dhcp-2.2.2.0] expired day 0 hour 0 minute 3
```

Relay的配置：

```
[Relay -Vlan-interface2] ip address 2.2.2.1 255.255.255.0
[Relay -Vlan-interface2] dhcp select relay
[Relay -Vlan-interface2] ip relay address 1.1.1.1
```

Snooping配置：

[Snooping] dhcp-snooping

[Snooping] interface Ethernet0/1

[Snooping -Ethernet0/1] dhcp-snooping trust

Client配置：

[Client] interface vlan-interface 1

[Client -Vlan-interface1] ip address dhcp-alloc

同时保证路由的畅通，可以通过配置静态路由或动态路由协议来完成。

10.3 DHCP 特性综合配置注意事项

1、三层交换机DHCP RELAY和DHCP SNOOPING特性不允许同时配置，二者为互斥的；

2、三层交换机的DHCP SNOOPING功能不提供端口信任功能，因此不能配置端口TRUST；

3、二层交换机的DHCP SNOOPING功能必须与端口信任功能配合使用，否则用户无法正常获取IP地址，配置时需要将设备连接DHCP SERVER的上行端口设置为TRUST；

4、若采用DHCP RELAY中继跨网段申请IP地址，则DHCP SERVER上配置的地址池必须为全局地址池，否则用户无法正常获取到IP地址；

5、若设备使用DHCP动态申请到的IP地址，则不能在该虚接口上配置从地址；

6、配置DHCP SERVER地址池时，网络地址池和主机地址池为互斥关系，若该地址池已经配置为网络地址池，则不能在该地址池上静态绑定IP地址；

7、DHCP RELAY直接连接CLIENT的下行接口的IP地址必须与DHCP SERVER地址池的地址在同一网段，多个RELAY叠加使用时尤其要注意这一点。

10.4 DHCP OPTION 说明

我司目前支持的option如下：

Tag	Name	Description
0	Pad	The pad option can be used to cause subsequent fields to align on word boundaries.

Tag	Name	Description
1	Subnet mask	Specifies da subnet mask for the client
3	Gateways	A list of routers, in preferential order, for the client to use.
6	Domain Name servers	A list of Domain Name servers in preferential order. A Domain Name server enables the client to locate other computers on the network by name.
12	Host name	The host name of the client.
15	Domain name	The domain name the client should use when resolving hostnames via the Domain Name System.
22	Max Datagram Reassembly Size	The maximum size datagram that the client should be prepared to reassemble.
28	Broadcast Address	The broadcast address in use on the client's subnet.
36	Ethernet Encapsulation	A boolean value indicating whether or not the client should use Ethernet Version 2 or IEEE 802.3 encapsulation if the interface is an Ethernet.
43	Vendor Specific Information	Used by clients and servers to exchange vendor-specific information.
44	NBT Name servers	A list of IP addresses, in preferential order, specifying RFC 1001/1002 NetBIOS name servers (NBNS).
46	NBT Node Type	Allows NetBIOS over TCP/IP clients which are configurable to be configured as described in RFC 1001/1002. The value is specified as a single octet which identifies the client type as follows: 1 = B-node, 2 = P-node, 4 = M-node, 8 =
50	Requested IP Address	This option is used in a client request (DHCPDISCOVER) to allow the client to request that a particular IP address be assigned.
51	DHCP Address Lease Time	Used in a client request (DHCPDISCOVER or DHCPREQUEST) to allow the client to request a lease time for the IP address. In a server reply (DHCPOFFER), a DHCP server uses this option to specify the lease time it is willing to offer.

Tag	Name	Description
52	Option Overload	This option is used to indicate that the DHCP 'sname' or 'file' fields are being overloaded by using them to carry DHCP options.
53	DHCP Message Type	Used to convey the type of the DHCP message.
54	Server Identifier	Used in DHCPOFFER and DHCPREQUEST messages, and may optionally be included in the DHCPACK and DHCPNAK messages.
55	Parameter Request List	Used by a DHCP client to request values for specified configuration parameters.
56	Message	This option is used by a DHCP server to provide an error message to a DHCP client in a DHCPNAK message in the event of a failure.
57	Maximum DHCP Message Size	This option specifies the maximum length DHCP message that it is willing to accept.
58	DHCP Renewal Time	The time interval from address assignment until the client transitions to the RENEWING state.
59	DHCP Rebinding Time	The time interval from address assignment until the client transitions to the REBINDING state.
60	Class Identifier	Used by DHCP clients to optionally identify the type and configuration of DHCP client.
61	Client Identifier	This option is used by DHCP clients to specify their unique identifier.
81	Client FQDN	Used to convey the client's Fully Qualified Domain Name (FQDN), as well as information regarding DNS updates.
255	End	Signifies the end of vendor options in a bootp or dhcp packet.

10.5 缩略语

缩略语	英文全名	中文解释
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议

BOOTP	Bootstrap Protocol	自举协议
ARP	Address Resolution Protocol	地址解析协议