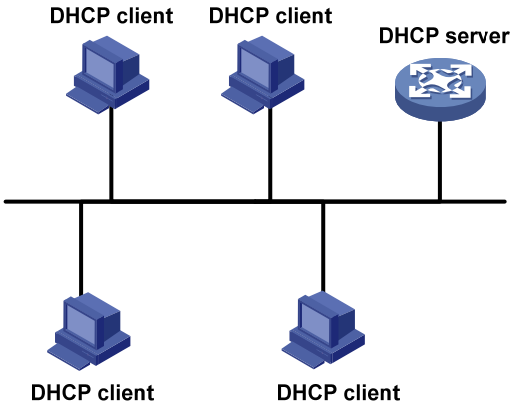
目 录

1 DHCP概述

1.1 DHCP组网模型

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）采用客户端/服务器模式，由服务器为网络设备动态地分配IP地址等网络配置参数。DHCP客户端和DHCP服务器处于不同物理网段时，客户端可以通过DHCP中继与服务器通信，获取IP地址及其他配置信息。DHCP中继的详细介绍，请参见“3.1 DHCP中继简介”。

图1-1 同网段 DHCP 组网应用



1.2 DHCP的IP地址分配

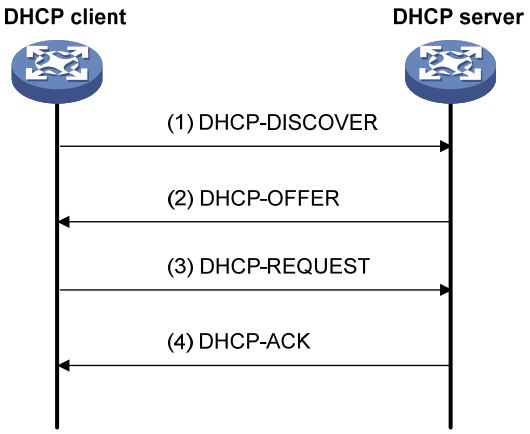
1.2.1 IP地址分配策略

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 地址分配给客户端。
- 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 为客户端分配具有一定有效期限的 IP 地址，到达使用期限后，客户端需要重新申请地址。绝大多数客户端得到的都是这种动态分配的地址。

1.2.2 IP地址获取过程

图1-2 IP 地址动态获取过程



如 图 1-2 所示，DHCP客户端从DHCP服务器获取IP地址，主要通过四个阶段进行：

(1) 发现阶段，即 DHCP 客户端寻找 DHCP 服务器的阶段。客户端以广播方式发送 DHCP-DISCOVER 报文。

(2) 提供阶段，即 DHCP 服务器提供 IP 地址的阶段。DHCP 服务器接收到客户端的 DHCP-DISCOVER 报文后，根据 IP 地址分配的优先次序选出一个 IP 地址，与其他参数一起通过 DHCP-OFFER 报文发送给客户端。

(3) 选择阶段，即 DHCP 客户端选择 IP 地址的阶段。如果有多台 DHCP 服务器向该客户端发来 DHCP-OFFER 报文，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 报文，该报文中包含 DHCP 服务器在 DHCP-OFFER 报文中分配的 IP 地址。

(4) 确认阶段，即 DHCP 服务器确认 IP 地址的阶段。DHCP 服务器收到 DHCP 客户端发来的 DHCP-REQUEST 报文后，只有 DHCP 客户端选择的服务器会进行如下操作：如果确认将地址分配给该客户端，则返回 DHCP-ACK 报文；否则返回 DHCP-NAK 报文，表明地址不能分配给该客户端。

客户端收到服务器返回的 DHCP-ACK 确认报文后，会以广播的方式发送免费 ARP 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未收到回应，并且客户端上不存在与该地址同网段的其他地址时，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，并重新申请 IP 地址。

如果网络中存在多个 DHCP 服务器，除 DHCP 客户端选中的服务器外，其它 DHCP 服务器中本次未分配出的 IP 地址仍可分配给其他客户端。

1.2.3 IP地址的租约更新

DHCP 服务器分配给客户端的 IP 地址具有一定的租借期限（除自动分配的 IP 地址），该租借期限称为租约。当租借期满后服务器会收回该 IP 地址。如果 DHCP 客户端希望继续使用该地址，则 DHCP 客户端需要申请延长 IP 地址租约。

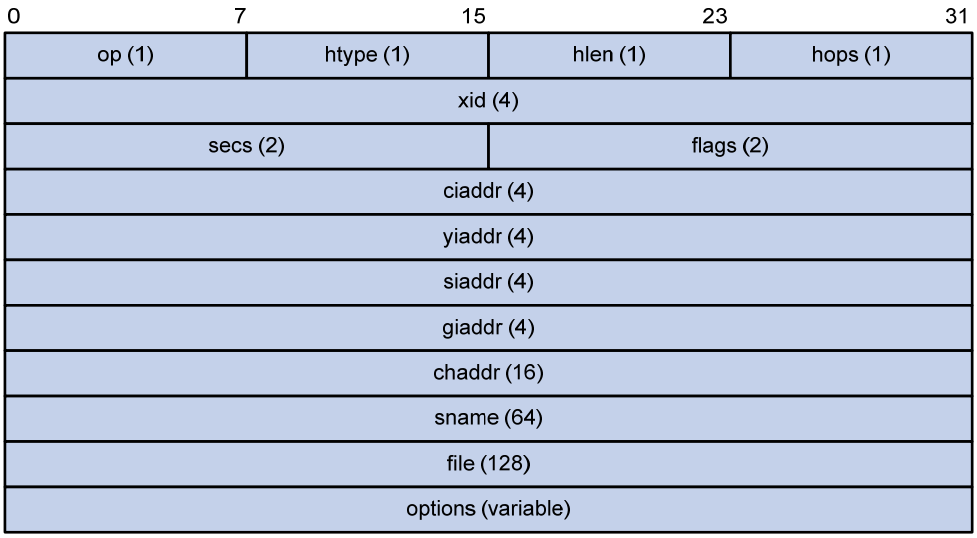
在 DHCP 客户端的 IP 地址租约期限达到一半左右时间时，DHCP 客户端会向为它分配 IP 地址的 DHCP 服务器单播发送 DHCP-REQUEST 报文，以进行 IP 租约的更新。如果客户端可以继续使用此 IP 地址，则 DHCP 服务器回应 DHCP-ACK 报文，通知 DHCP 客户端已经获得新 IP 租约；如果此 IP 地址不可以再分配给该客户端，则 DHCP 服务器回应 DHCP-NAK 报文，通知 DHCP 客户端不能获得新的租约。

如果在租约的一半左右时间进行的续约操作失败，DHCP 客户端会在租约期限达到 7/8 时，广播发送 DHCP-REQUEST 报文进行续约。DHCP 服务器的处理方式同上，不再赘述。

1.3 DHCP报文格式

DHCP有 8 种类型的报文，每种报文的格式都相同，只是某些字段的取值不同。DHCP的报文格式如 图 1-3 所示，括号中的数字表示该字段所占的字节。

图1-3 DHCP 报文格式



各字段的解释如下：

- op：报文的操作类型，分为请求报文和响应报文，1 为请求报文；2 为响应报文。具体的报文类型在 options 字段中标识。
- htype、hlen：DHCP 客户端的硬件地址类型及长度。
- 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：客户端发起一次请求时选择的随机数，用来标识一次地址请求过程。
- secs：DHCP 客户端开始 DHCP 请求后所经过的时间。目前没有使用，固定为 0。
- flags：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。如果客户端有合法和可用的 IP 地址，则将其添加到此字段，否则字段设置为 0。此字段不用于客户端申请某个特定的 IP 地址。
- yiaddr：DHCP 服务器分配给客户端的 IP 地址。
- siaddr：DHCP 客户端获取启动配置信息的服务器 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 客户端获取启动配置信息的服务器名称。
- 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。

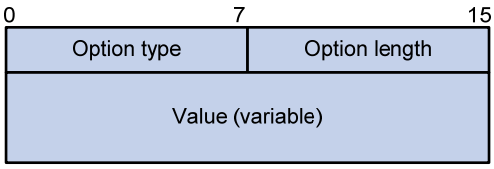
1.4 DHCP选项介绍

为了与 BOOTP（Bootstrap Protocol，自举协议）兼容，DHCP 保留了 BOOTP 的消息格式。DHCP 和 BOOTP 消息的不同主要体现在选项（Options）字段。DHCP 在 BOOTP 基础上增加的功能，通过 Options 字段来实现。

DHCP 利用 Options 字段传递控制信息和网络配置参数，实现地址动态分配的同时，为客户端提供更加丰富的网络配置信息。

DHCP选项的格式如 图 1-4 所示。

图1-4 DHCP 选项格式



1.5 DHCP常用选项

常见的 DHCP 选项有：

- Option 3：路由器选项，用来指定为客户端分配的网关地址。
- Option 6：DNS 服务器选项，用来指定为客户端分配的 DNS 服务器地址。
- Option 33：静态路由选项。该选项中包含一组有分类静态路由（即目的网络地址的掩码固定为自然掩码，不能划分子网），客户端收到该选项后，将在路由表中添加这些静态路由。如果 Option 33 和 Option 121 同时存在，则忽略 Option 33。
- Option 51：IP 地址租约选项。
- Option 53：DHCP 消息类型选项，标识 DHCP 消息的类型。
- Option 55：请求参数列表选项。客户端利用该选项指明需要从服务器获取哪些网络配置参数。该选项内容为客户端请求的参数对应的选项值。
- Option 60：厂商标识选项。客户端利用该选项标识自己所属的厂商；DHCP 服务器可以根据该选项区分客户端所属的厂商，并为其分配特定范围的 IP 地址。
- Option 66：TFTP 服务器名选项，用来指定为客户端分配的 TFTP 服务器的域名。
- Option 67：启动文件名选项，用来指定为客户端分配的启动文件名。

- Option 121：无分类路由选项。该选项中包含一组无分类静态路由（即目的网络地址的掩码为任意值，可以通过掩码来划分子网），客户端收到该选项后，将在路由表中添加这些静态路由。如果 Option 33 和 Option 121 同时存在，则忽略 Option 33。
- Option 150：TFTP 服务器地址选项，用来指定为客户端分配的 TFTP 服务器的地址。

更多 DHCP 选项的介绍，请参见 RFC 2132 和 RFC 3442。

1.6 自定义DHCP选项

有些选项的内容，RFC 2132 中没有统一规定，例如 Option 43、Option 82 和 Option 184。下面将介绍设备上定义的几种选项。

1.6.1 厂商特定信息选项（Option 43）

1. Option 43 的作用

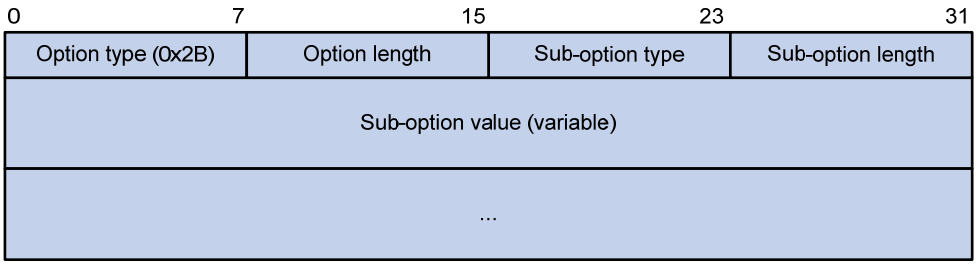
Option 43 称为厂商特定信息选项。DHCP 服务器和 DHCP 客户端通过 Option 43 交换厂商特定的信息。

设备作为 DHCP 客户端时，可以通过 Option 43 获取：

- ACS（Auto-Configuration Server，自动配置服务器）的参数，包括 URL 地址、用户名和密码。
- 服务提供商标识，CPE（Customer Premises Equipment，用户侧设备）从 DHCP 服务器获取该信息后，将该信息通告给 ACS，以便 ACS 选择服务提供商特有的配置和参数等。CPE 和 ACS 的详细介绍，请参见“网络管理和监控配置指导”中的“CWMP（TR-069）”。
- PXE（Preboot eXecution Environment，预启动执行环境）引导服务器地址，以便客户端从 PXE 引导服务器获取启动文件或其他控制信息。
- 在无线网络中，AP（Access Point，接入点）作为 DHCP 客户端，可以通过 Option 43 获取 AC（Access Controller，接入控制器）地址，以便 AP 从 AC 获取启动文件或其他控制信息。

2. Option 43 格式

图1-5 Option 43 格式



为了提供可扩展性，通过Option 43 为客户端分配更多的信息，Option 43 采用子选项的形式，通过不同的子选项为用户分配不同的网络配置参数。如 图 1-5 所示。子选项中各字段的含义为：

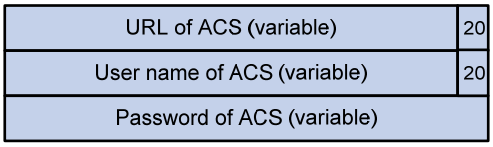
- Sub-option type：子选项类型。目前，子选项类型值可以为 0x01 表示 ACS 参数子选项，0x02 表示服务提供商标识子选项，0x80 表示 PXE 引导服务器地址子选项。
- Sub-option length：子选项的长度，不包括子选项类型和子选项长度字段。

- Sub-option value：子选项的取值。不同类型的子选项，取值格式有所不同。

3. Option 43 子选项取值字段的格式

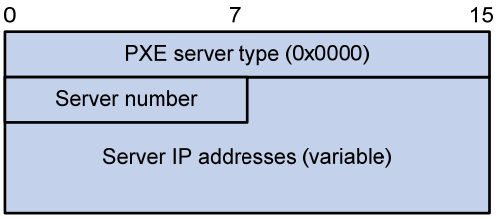
- ACS参数子选项的取值字段格式如 图 1-6 所示。ACS的URL地址、用户名和密码长度可变，每个参数之间用空格（十六进制数为 20）隔开。

图1-6 ACS 参数子选项取值字段的格式



- 服务提供商标识子选项的取值字段内容为服务提供商的标识。
- PXE引导服务器地址子选项的取值字段格式如 图 1-7 所示。其中，PXE服务器类型目前取值只能为 0；Server number为子选项中包含的PXE服务器地址的数目；Server IP addresses为PXE服务器的IP地址。

图1-7 PXE 引导服务器地址子选项取值字段的格式



1.6.2 中继代理信息选项（Option 82）

Option 82 称为中继代理信息选项，该选项记录了 DHCP 客户端的位置信息。DHCP 中继或 DHCP Snooping 设备接收到DHCP 客户端发送给DHCP 服务器的请求报文后，在该报文中添加Option 82，并转发给 DHCP 服务器。

管理员可以从 Option 82 中获得 DHCP 客户端的位置信息，以便定位 DHCP 客户端，实现对客户端的安全和计费等控制。支持 Option 82 的服务器还可以根据该选项的信息制定 IP 地址和其他参数的分配策略，提供更加灵活的地址分配方案。

Option 82 最多可以包含 255 个子选项。若定义了 Option 82，则至少要定义一个子选项。目前设备只支持两个子选项：sub-option 1（Circuit ID，电路 ID 子选项）、sub-option 2（Remote ID，远程 ID 子选项）。

由于 Option 82 的内容没有统一规定，不同厂商通常根据需要进行填充。

设备上，Circuit ID 的填充模式有以下几种：

- 采用 string 模式填充：sub-option 1 的内容是用户配置的字符串。
- 采用 normal 模式填充：sub-option 1 的内容是接收到 DHCP 客户端请求报文的接口所属的 VLAN ID 以及接口编号。

- 采用 verbose 模式填充：sub-option 1 的内容包括用户配置的接入节点标识，接收到 DHCP 客户端请求报文的接口类型、接口编号和接口所属的 VLAN ID。

Remote ID 的填充模式有以下几种：

- 采用 string 模式填充：sub-option 2 的内容是用户配置的字符串。
- 采用 normal 模式填充：sub-option 2 的内容是接收到 DHCP 客户端请求报文的接口 MAC 地址（DHCP 中继）或设备的桥 MAC 地址（DHCP Snooping）。
- 采用 sysname 模式填充：sub-option 2 的内容是设备的系统名称。设备的系统名称可以通过系统视图下的 **sysname** 命令配置。

1.6.3 Option 184

Option 184 是 RFC 中规定的保留选项，用户可以自定义该选项中携带的信息。设备上，Option 184 携带了语音呼叫所需的信息。通过 Option 184，可以实现在为具有语音功能的 DHCP 客户端提供语音呼叫相关信息。

目前 Option 184 支持四个子选项，承载的内容如下：

- sub-option 1：网络呼叫处理器的 IP 地址，用来标识作为网络呼叫控制源及应用程序下载的服务器。只有定义了 sub-option 1（网络呼叫处理器的 IP 地址子选项），其他子选项才能生效。
- sub-option 2：备用服务器的 IP 地址，当 sub-option 1 中携带的网络呼叫处理器不可达或不合法时，DHCP 客户端使用该选项指定的备用服务器作为网络呼叫处理器。
- sub-option 3：语音 VLAN 信息，指定语音 VLAN 的 ID 及 DHCP 客户端是否会将所指定的 VLAN 作为语音 VLAN。
- sub-option 4：自动故障转移呼叫路由，指定故障转移呼叫路由的 IP 地址及其关联的拨号串，即 SIP（Session Initiation Protocol，会话初始协议）用户之间互相通信时对端的 IP 地址和呼叫号码。当网络呼叫处理器和备用服务器均不可达时，SIP 用户可以使用对端 IP 地址及呼叫号码直接与对端 SIP 用户建立连接并通信。

1.7 协议规范

与 DHCP 相关的协议规范有：

- RFC 2131：Dynamic Host Configuration Protocol
- RFC 2132：DHCP Options and BOOTP Vendor Extensions
- RFC 1542：Clarifications and Extensions for the Bootstrap Protocol
- RFC 3046：DHCP Relay Agent Information Option
- RFC 3442：The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4

2 DHCP服务器

2.1 DHCP服务器简介

DHCP 服务器通过地址池保存 IP 地址和网络参数，从地址池中选择 IP 地址和网络参数分配给客户端。

2.1.1 地址池的地址管理方式

地址池的地址管理方式有以下几种：静态绑定 IP 地址，即通过将客户端的 MAC 地址或客户端 ID 与 IP 地址绑定的方式，实现为特定的客户端分配特定的 IP 地址；动态选择 IP 地址，即在地址池中指定可供分配的 IP 地址范围，当收到客户端的 IP 地址申请时，从该地址范围中动态选择 IP 地址，分配给该客户端。

在地址池中指定可供分配的 IP 地址范围，有以下几种方法：

1. 为地址池指定一个主网段，并将该网段划分为多个地址范围。

多个地址范围是指一个地址池动态分配的 IP 地址范围（公共地址范围）和多个为 DHCP 用户类分配的 IP 地址范围。

DHCP 服务器通过定义 DHCP 用户类，实现为满足特定条件的客户端分配特定地址范围的 IP 地址。DHCP 服务器根据客户端发送的请求报文，判断 DHCP 客户端所属的用户类。每个用户类可以配置多个匹配条件，只要客户端发送的 DHCP 请求报文满足任意一个匹配条件，就认为该客户端属于该用户类。在地址池下，可以为不同的用户类指定不同的地址范围。如果 DHCP 客户端属于某个用户类，则从该用户类的地址范围内选择地址分配给该客户端。

采用这种地址管理方式时，地址选择过程为：

(1) 按照地址池下用户类地址范围的配置顺序，将 DHCP 客户端和用户类进行匹配。

(2) 如果 DHCP 客户端属于某个用户类，则从该用户类的地址范围中选择地址分配给客户端。

(3) 如果该用户类中没有可供分配的地址，则继续匹配下一个用户类。如果所有匹配上的用户类地址范围都没有可供分配的地址，则从公共地址范围中选择地址分配给客户端。

(4) 如果 DHCP 客户端不属于任何一个 DHCP 用户类，则会从地址池动态分配的 IP 地址范围（通过 **address range** 命令配置）中选择地址分配给 DHCP 客户端。

(5) 如果动态分配的 IP 地址范围内也没有空闲地址，或者未配置动态分配的 IP 地址范围，则地址分配失败，即 DHCP 服务器无法为 DHCP 客户端分配地址。

说明

每个地址范围内的地址都必须属于指定的主网段，否则无法分配该范围内的地址。

---

2. 为地址池指定一个主网段，并指定多个从网段。

采用此种地址分配方式时，地址选择的过程是：首先从地址池主网段中查找可供分配的 IP 地址。如果主网段中没有可供分配的 IP 地址，则按照该地址池下从网段的配置顺序，依次查找可供分配的 IP 地址。

2.1.2 地址池的选取原则

DHCP 服务器为客户端分配 IP 地址时，按照如下顺序选择地址池：

(1) 如果存在将客户端 MAC 地址或客户端 ID 与 IP 地址静态绑定的地址池，则选择该地址池，并将静态绑定的 IP 地址和其他网络参数分配给客户端。

(2) 如果接收到 DHCP 请求报文的接口引用了某个地址池，则选择该地址池，从该地址池中选取 IP 地址和其他网络参数分配给客户端。

(3) 如果配置了 DHCP 策略，则 DHCP 客户端匹配某个 DHCP 用户类时，DHCP 服务器选择与该 DHCP 用户类关联的 DHCP 地址池；DHCP 客户端未匹配到 DHCP 用户类时，若配置了默认 DHCP 地址池，则选择该 DHCP 地址池；若未配置默认 DHCP 地址池或 DHCP 默认地址池不存在可供分配的 IP 地址时，IP 地址或其他参数分配失败。

(4) 如果上述条件均不满足，则使用以下方法选择 DHCP 地址池：

- 如果客户端与服务器在同一网段，则将 DHCP 请求报文接收接口的 IP 地址与所有地址池配置的主网段进行匹配，并选择最长匹配的主网段所对应的地址池。如果未匹配到主网段，则将 DHCP 请求报文接收接口的 IP 地址与所有地址池配置的从网段进行匹配，并选择最长匹配的网段所对应的地址池。
- 如果客户端与服务器不在同一网段，即客户端通过 DHCP 中继获取 IP 地址，则将 DHCP 请求报文中 giaddr 字段指定的 IP 地址与所有地址池配置的主网段进行匹配，并选择最长匹配的网段所对应的地址池。如果未匹配到主网段，则将 DHCP 请求报文中 giaddr 字段指定的 IP 地址与所有地址池配置的从网段进行匹配，并选择最长匹配的网段所对应的地址池。

例如，DHCP 服务器上配置了两个地址池，动态分配的网段分别是 1.1.1.0/24 和 1.1.1.0/25，如果接收 DHCP 请求报文的接口 IP 地址为 1.1.1.1/25，且未引用地址池，服务器将从 1.1.1.0/25 地址池中选择 IP 地址分配给客户端，1.1.1.0/25 地址池中如果没有可供分配的 IP 地址，则服务器无法为客户端分配地址；如果接收 DHCP 请求报文的接口 IP 地址为 1.1.1.130/25，服务器将从 1.1.1.0/24 地址池中选择 IP 地址分配给客户端。

说明

- 配置地址池动态分配的网段和 IP 地址范围时，请尽量保证其与 DHCP 服务器接口或 DHCP 中继接口地址的网段一致，以免分配错误的 IP 地址。
- 建议合理规划 DHCP 服务器上各地址池中主网段的配置，尽量避免客户端匹配不到主网段、直接匹配从网段的情况发生。

2.1.3 DHCP服务器分配IP地址的优先次序

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。Option 50 为客户端请求的 IP 地址选项（Requested IP Address），客户端通过在 DHCP-DISCOVER 报文中添加该选项来指明客户端希望获取的 IP 地址。该选项的内容由客户端决定。

(4) 按照“2.1.1 地址池的地址管理方式”和“2.1.2 地址池的选取原则”中所述的动态分配地址选择原则，顺序查找可供分配的IP地址，选择最先找到的IP地址。

(5) 如果未找到可用的 IP 地址，则从当前匹配地址池中依次查询租约过期、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。

说明

- 如果客户端所在的网段发生变化，服务器不会为客户端分配曾经分配给它的 IP 地址，而是从匹配新网段的地址池中重新选择 IP 地址。
- 使用曾经发生过冲突的 IP 地址时，只有冲突状态超过一小时的 IP 地址才能够被服务器分配给新的 DHCP 客户端。

2.2 DHCP服务器配置任务简介

DHCP 服务器配置任务如下：

(1) （可选）创建DHCP用户类

(2) 配置DHCP服务器的地址池

(3) （可选）修改 DHCP 服务器的地址池选择方式
   - 配置接口引用地址池
   - 配置DHCP策略动态分配地址和其他参数

(4) 开启DHCP服务

(5) 配置接口工作在DHCP服务器模式

(6) （可选）配置高级功能
   - 配置IP地址冲突检测功能
   - 配置Option 82 的处理方式
   - 配置DHCP服务器兼容性
   - 配置DHCP服务器发送DHCP报文的DSCP优先级
   - 配置DHCP服务器租约固化功能
   - 开启DHCP服务器的用户下线探测功能

(7) （可选）配置告警及日志功能
   - 配置DHCP告警功能
   - 开启DHCP服务器日志信息功能

2.3 创建DHCP用户类

1. 功能简介

DHCP 用户类通过 DHCP 请求报文中的硬件地址、Option 信息或 Giaddr 字段来匹配一组特定的 DHCP 客户端，以实现为特定的 DHCP 客户端分配特定的 IP 地址和其他参数。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 DHCP 用户类，并进入 DHCP 用户类视图。

dhcp class *class-name*

(3) 配置 DHCP 用户类的匹配规则。

if-match rule *rule-number* { **hardware-address** *hardware-address* **mask** *hardware-address-mask* | **option** *option-code* [**ascii** *ascii-string* [**offset** *offset* | **partial**] | **hex** *hex-string* [**mask** *mask* | **offset** *offset* **length** *length* | **partial**]] | **relay-agent** *gateway-address* }

缺省情况下，未配置 DHCP 用户类的匹配规则。

2.4 配置DHCP服务器的地址池

2.4.1 DHCP服务器地址池配置任务简介

DHCP 服务器地址池配置任务如下：

(1) 创建DHCP地址池

(2) 配置为 DHCP 客户端分配地址

同一个地址池中不能同时配置两种动态地址管理方式，但可以同时配置动态地址管理方式和静态地址绑定。

- 配置一个主网段多个地址范围的动态地址管理方式
- 配置一个主网段多个从网段的动态地址管理方式
- 配置静态地址绑定

(3) 配置为 DHCP 客户端分配其他参数

- 配置DHCP客户端使用的网关地址
- 配置DHCP客户端使用的域名后缀
- 配置DHCP客户端使用的DNS服务器地址
- 配置DHCP客户端使用的WINS服务器地址和NetBIOS节点类型
- 配置DHCP客户端使用的BIMS服务器信息
- 配置DHCP客户端使用的远程启动文件信息
- 配置DHCP客户端使用的下一个提供服务的服务器IP地址
- 配置DHCP客户端使用的Option 184 参数
- 自定义DHCP选项

(4) （可选）为DHCP服务器上的地址池绑定VPN实例

(5) （可选）配置DHCP用户类白名单功能

(6) （可选）配置DHCP服务器辅助网关信息

(7) （可选）配置DHCP服务器辅助路由信息

2.4.2 创建DHCP地址池

(1) 进入系统视图。

system-view

(2) 创建 DHCP 地址池，并进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

2.4.3 配置一个主网段多个地址范围的动态地址管理方式

1. 功能简介

在某些组网应用中，需要将一个网段下的不同客户端，按照一定的规则划分到不同的地址范围中。此时，可以按照客户端划分规则创建对应的 DHCP 用户类，并在地址池内为不同的用户类配置不同的地址范围，从而实现为特定的客户端分配特定范围的地址。在这种情况下，还可以配置一个公共地址范围，为不匹配任何用户类的客户端分配给该范围的地址。如果不配置公共地址范围，则不匹配任何用户类的客户端将无法获取到 IP 地址。

如果不需要对客户端进行分类，而仅需要限制网段内可分配的动态地址范围，则可以只配置公共地址范围，而不配置用户类的地址范围。

2. 配置限制和指导

配置为客户端分配的 IP 地址时，需要注意：

- 在同一个 DHCP 地址池中，如果多次执行 **network** 或 **address range** 命令，新的配置会覆盖已有配置；如果多次执行 **class** 命令，则可以为多个用户类指定不同的地址范围；多次执行 **forbidden-ip** 命令，可以配置多个不参与自动分配的 IP 地址。
- 在 DHCP 地址池视图下通过 **forbidden-ip** 命令配置不参与自动分配的 IP 地址后，只有当前的地址池不能分配这些 IP 地址，其他地址池仍然可以分配这些 IP 地址；通过 **dhcp server forbidden-ip** 命令指定不参与自动分配的 IP 地址后，所有地址池都不能分配这些 IP 地址。
- 当用户配置 **class range** 命令修改已存在的为 DHCP 用户类动态分配的 IP 地址范围，且新的 IP 地址范围包括之前 IP 地址范围中已分配的地址租约时，如果 DHCP 服务器收到该地址租约的续约需求，DHCP 服务器会给该 DHCP 客户端分配新的 IP 地址租约，已分配的地址租约会继续老化等待超期释放。如果需要已分配的地址租约立即释放，则需配置 **reset dhcp server ip-in-use** 命令进行清除地址租约操作。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

(3) 配置 DHCP 地址池动态分配的主网段。

network *network-address* [*mask-length* | **mask** *mask*]

缺省情况下，未配置主网段。

(4) （可选）配置地址池动态分配的 IP 地址范围，即公共地址范围。

address range *start-ip-address end-ip-address*

缺省情况下，未配置动态分配的 IP 地址范围。

(5) （可选）配置 DHCP 地址池为指定 DHCP 用户类动态分配的 IP 地址范围。

class *class-name* **range** *start-ip-address end-ip-address*

缺省情况下，未配置为指定 DHCP 用户类动态分配的 IP 地址范围。

class 命令中指定的 DHCP 用户类，必须通过 **dhcp class** 命令创建。否则，无法为该用户类分配指定范围的地址。

(6) （可选）配置动态分配的 IP 地址的租约有效期限。

expired { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }

缺省情况下，IP 地址租约有效期限为 1 天。

(7) （可选）配置 DHCP 地址池中不参与自动分配的 IP 地址。

forbidden-ip *ip-address*&<1-8>

缺省情况下，DHCP 地址池中的所有 IP 地址都参与自动分配。

(8) （可选）在系统视图配置全局不参与自动分配的 IP 地址。

a. 退回系统视图。

quit

b. 配置全局不参与自动分配的 IP 地址。

dhcp server forbidden-ip *start-ip-address* [*end-ip-address*] [**vpn-instance** *vpn-instance-name*]

缺省情况下，除 DHCP 服务器接口的 IP 地址外，DHCP 地址池中的所有 IP 地址都参与自动分配。

2.4.4 配置一个主网段多个从网段的动态地址管理方式

1. 功能简介

在配置了一个主网段和多个从网段的地址池中，从网段的作用是对主网段地址空间的补充。当主网段中没有空闲地址分配给客户端时，服务器会从该地址池中的从网段获取地址分配给客户端。

2. 配置限制和指导

在 DHCP 地址池视图下通过 **forbidden-ip** 命令配置不参与自动分配的 IP 地址后，只有当前的地址池不能分配这些 IP 地址，其他地址池仍然可以分配这些 IP 地址；通过 **dhcp server forbidden-ip** 命令指定不参与自动分配的 IP 地址后，所有地址池都不能分配这些 IP 地址。

3. 在地址池中配置一个主网段和多个从网段

(1) 进入系统视图。

system-view

(2) 进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

(3) 配置 DHCP 地址池动态分配的主网段。

network *network-address* [*mask-length* | **mask** *mask*]

缺省情况下，未配置主网段。

每个 DHCP 地址池中只能配置一个主网段，如果多次执行 **network** 命令配置主网段，则新的配置会覆盖已有配置。

(4) （可选）配置 DHCP 地址池动态分配的从网段。

network *network-address* [*mask-length* | **mask** *mask*] **secondary**

缺省情况下，未配置从网段。

每个 DHCP 地址池中，最多可以配置 32 个从网段。

(5) （可选）退回地址池视图。

quit

4. 在地址池中配置动态分配的IP地址的租约有效期限

(1) 进入系统视图。

system-view

(2) 进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

(3) 配置动态分配的 IP 地址的租约有效期限。

expired { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }

缺省情况下，IP 地址租约有效期限为 1 天。

5. 配置不参与自动分配的地址

(1) 进入系统视图。

system-view

(2) 进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

(3) 配置 DHCP 地址池中不参与自动分配的 IP 地址。

forbidden-ip *ip-address*&<1-8>

缺省情况下，DHCP 地址池中的所有 IP 地址都参与自动分配。

多次执行 **forbidden-ip** 命令，可以配置多个不参与自动分配的 IP 地址段。

(4) （可选）在系统视图下配置全局不参与自动分配的 IP 地址。

a. 退回系统视图。

quit

b. 配置全局不参与自动分配的 IP 地址。

dhcp server forbidden-ip *start-ip-address* [*end-ip-address*] [**vpn-instance** *vpn-instance-name*]

缺省情况下，除 DHCP 服务器接口的 IP 地址外，DHCP 地址池中的所有 IP 地址都参与自动分配。

多次执行 **dhcp server forbidden-ip** 命令，可以配置多个不参与自动分配的 IP 地址段。

2.4.5 配置静态地址绑定

1. 功能简介

某些客户端（如 Web 服务器等）需要固定的 IP 地址，通过以下几种方式可以实现为特定的客户端分配特定的 IP 地址：

- 将客户端的硬件地址与 IP 地址绑定：当具有此 MAC 地址的客户端申请 IP 地址时，DHCP 服务器将根据客户端的 MAC 地址查找到对应的 IP 地址，并分配给客户端。
- 将客户端 ID 与 IP 地址绑定：某些客户端在向 DHCP 服务器发送 DHCP-DISCOVER 报文申请 IP 地址时，会构建客户端 ID 并添加到报文中一起发送。如果在 DHCP 服务器上将客户端 ID 与 IP 地址绑定，则当该客户端申请 IP 地址时，DHCP 服务器将根据客户端 ID 查找到对应的 IP 地址并分配给客户端。

2. 配置限制和指导

- 静态绑定的 IP 地址不能是 DHCP 服务器的接口 IP 地址，否则会导致 IP 地址冲突，被绑定的客户端将无法正常获取到 IP 地址。
- 如果作为 DHCP 客户端的设备，接口的 MAC 地址相同，则为了区分不同接口，采用静态绑定方式进行地址分配时，需要在服务器上配置静态绑定的客户端 ID，而不能配置静态绑定的客户端 MAC 地址，否则可能导致客户端无法成功获取 IP 地址。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

(3) 配置静态地址绑定。

static-bind ip-address *ip-address* [*mask-length* | **mask** *mask*] { **client-identifier** *client-identifier* | **hardware-address** *hardware-address* [**ethernet** | **token-ring**] }

缺省情况下，未配置静态地址绑定。

同一地址只能绑定给一个客户端。不允许通过重复执行 **static-bind ip-address** 命令的方式修改 IP 地址与客户端的绑定关系。只有删除了某个地址的绑定关系，才能将该地址与其他客户端绑定。

(4) （可选）配置静态绑定 IP 地址的租约有效期限。

expired { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }

缺省情况下，IP 地址租约有效期限为 1 天。

2.4.6 配置DHCP客户端使用的网关地址

1. 功能简介

DHCP 客户端访问本网段以外的服务器或主机时，数据必须通过网关进行转发。DHCP 服务器可以为客户端指定网关的地址。

2. 配置限制和指导

- 在 DHCP 服务器上，可以为每个地址池分别指定客户端对应的网关地址。目前，每个 DHCP 地址池视图下、每个从网段视图下最多可以配置 64 个网关地址。
- DHCP 地址池视图下执行 **gateway-list** 命令，配置的是为地址池中所有 DHCP 客户端分配的网关地址。如果用户需要为地址池下某个从网段的 DHCP 客户端分配其它的网关地址，可以在地址池的从网段视图下执行 **gateway-list** 命令。如果在地址池视图和从网段视图下都配置了网关地址，则优先将从网段视图下配置的网关地址分配给从网段的 DHCP 客户端。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

(3) 配置为 DHCP 客户端分配的网关地址。

gateway-list *ip-address*&<1-64>

缺省情况下，未配置为 DHCP 客户端分配的网关地址。

(4) （可选）在从网段视图中配置为 DHCP 客户端分配的网关地址。

a. 进入从网段视图。

network *network-address* [*mask-length* | **mask** *mask*] **secondary**

b. 配置为 DHCP 客户端分配的网关地址。

gateway-list *ip-address*&<1-64>

缺省情况下，未配置为 DHCP 客户端分配的网关地址。

2.4.7 配置DHCP客户端使用的域名后缀

1. 功能简介

在 DHCP 服务器上，可以为每个地址池指定客户端使用的域名后缀。

在客户端进行域名解析时，用户只需要输入域名的部分字段，客户端会自动将输入的域名加上从 DHCP 服务器获得的域名后缀进行解析。有关域名后缀的详细介绍，请参见“三层技术-IP 业务配置指导”中的“域名解析”。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

(3) 配置为 DHCP 客户端分配的域名后缀。

domain-name *domain-name*

缺省情况下，未配置为 DHCP 客户端分配的域名后缀。

2.4.8 配置DHCP客户端使用的DNS服务器地址

1. 功能简介

为了使 DHCP 客户端能够通过域名访问 Internet 上的主机，DHCP 服务器应在为客户端指定 DNS（Domain Name System，域名系统）服务器地址。目前，每个 DHCP 地址池视图下最多可以配置 8 个 DNS 服务器地址。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

(3) 配置为 DHCP 客户端分配的 DNS 服务器地址。

dns-list *ip-address*&<1-8>

缺省情况下，未配置为 DHCP 客户端分配的 DNS 服务器地址。

2.4.9 配置DHCP客户端使用的WINS服务器地址和NetBIOS节点类型

1. 功能简介

对于使用 Microsoft Windows 操作系统的客户端，由 WINS（Windows Internet Naming Service，Windows Internet 名称服务）服务器为通过 NetBIOS 协议通信的主机提供主机名到 IP 地址的解析。所以，大部分 Windows 网络客户端需要进行 WINS 的设置。

为了使 DHCP 客户端实现主机名到 IP 地址的解析，DHCP 服务器应该为客户端指定 WINS 服务器地址。

DHCP 客户端在网络上使用 NetBIOS 协议通信时，需要在主机名和 IP 地址之间建立映射关系。根据获取映射关系方式的不同，NetBIOS 节点分为四种：

- b 类节点（b-node）：“b”代表广播（broadcast），即此类节点采用广播方式获取映射关系。源节点通过发送带有目的节点主机名的广播报文来获取目的节点的 IP 地址，目的节点收到广播报文后，就将自己的 IP 地址返回给源节点。
- p 类节点（p-node）：“p”代表端到端（peer-to-peer），即此类节点采用发送单播报文与 WINS 服务器通信的方式获取映射关系。源节点给 WINS 服务器发送单播报文，WINS 服务器收到单播报文后，返回源节点请求的目的节点名所对应的 IP 地址。
- m 类节点（m-node）：“m”代表混合（mixed），是具有部分广播特性的 p 类节点。即此类节点首先发送广播报文来获取映射关系，如果没有获取到，则再发送单播报文与 WINS 服务器通信来获取映射关系。
- h 类节点（h-node）：“h”代表混合（hybrid），是具备“端到端”通信机制的 b 类节点。即此类节点首先发送单播报文与 WINS 服务器通信来获取映射关系，如果没有获取到，再发送广播报文来获取映射关系。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

(3) 配置为 DHCP 客户端分配的 WINS 服务器地址。

nbns-list *ip-address*&<1-8>

缺省情况下，未配置为 DHCP 客户端分配的 WINS 服务器地址。

对于 b 类节点，为可选；其他情况下，为必选。每个 DHCP 地址池视图下最多可以配置 8 个 WINS 服务器地址。

(4) 配置为 DHCP 客户端分配的 NetBIOS 节点类型。

netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

缺省情况下，未配置为 DHCP 客户端分配的 NetBIOS 节点类型。

2.4.10 配置DHCP客户端使用的BIMS服务器信息

1. 功能简介

为了使 DHCP 客户端通过 BIMS（Branch Intelligent Management System，分支网点智能管理系统）服务器进行软件的备份和升级等操作，DHCP 服务器需要将 BIMS 服务器的 IP 地址、端口号以及加密的共享密钥等信息发给 DHCP 客户端。之后，DHCP 客户端就可以定期向 BIMS 服务器发送连接请求，从 BIMS 服务器上获取配置文件，进行软件的备份和升级等操作。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

(3) 配置为 DHCP 客户端分配的 BIMS 服务器的 IP 地址、端口及共享密钥信息。

bims-server ip *ip-address* [**port** *port-number*] **sharekey** { **cipher** | **simple** } *string*

缺省情况下，未配置为 DHCP 客户端分配的 BIMS 服务器信息。

2.4.11 配置DHCP客户端使用的远程启动文件信息

1. 功能简介

服务器自动配置功能在空配置启动的设备上不需要进行任何配置，但需要在 DHCP 服务器上配置一些必需的参数，包括 TFTP 服务器地址、TFTP 服务器名和启动文件名或远程启动文件的 HTTP 形式 URL 等。

2. 配置DHCP客户端使用的TFTP服务器地址及启动文件名

(1) 进入系统视图。

system-view

(2) 进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

(3) 配置 DHCP 客户端使用的 TFTP 服务器信息。请选择其中至少一项进行配置。

- 配置 DHCP 客户端使用的 TFTP 服务器地址。

  tftp-server ip-address *ip-address*

  缺省情况下，未配置 DHCP 客户端使用的 TFTP 服务器地址。

- 配置 DHCP 客户端使用的 TFTP 服务器名。

  tftp-server domain-name *domain-name*

  缺省情况下，未配置 DHCP 客户端使用的 TFTP 服务器名。

(4) 配置 DHCP 客户端使用的启动文件名。

bootfile-name *bootfile-name*

缺省情况下，未配置 DHCP 客户端使用的启动文件名。

3. 配置DHCP客户端使用的远程启动文件的HTTP形式URL

(1) 进入系统视图。

system-view

(2) 进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

(3) 配置 DHCP 客户端使用的远程启动文件的 HTTP 形式 URL。

bootfile-name *url*

缺省情况下，未配置 DHCP 客户端使用的远程启动文件的 HTTP 形式 URL。

2.4.12 配置DHCP客户端使用的下一个提供服务的服务器IP地址

1. 功能简介

设备在启动后，可能需要访问某些服务器获取设备运行需要的信息，例如从 TFTP 服务器上获取配置文件。通过本配置可以指定 DHCP 服务器为 DHCP 客户端分配的下一个提供服务的服务器 IP 地址，以便客户端启动后访问该服务器，获取必要的信息。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

(3) 配置 DHCP 地址池为 DHCP 客户端分配的下一个提供服务的服务器 IP 地址。

next-server *ip-address*

缺省情况下，未配置 DHCP 地址池为 DHCP 客户端分配的下一个提供服务的服务器 IP 地址。

2.4.13 配置DHCP客户端使用的Option 184 参数

1. 功能简介

为了使具有语音功能的DHCP客户端能够在通过DHCP获取IP地址的同时，获取到语音呼叫所需的相关信息，需要在DHCP服务器上配置Option 184。Option 184 内容的详细介绍，请参见“1.6.3 Option 184”。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

(3) 配置网络呼叫处理器的地址。

voice-config ncp-ip *ip-address*

缺省情况下，未配置网络呼叫处理器的地址。

只有配置了网络呼叫处理器的地址，其他配置才能生效。

(4) （可选）配置备用服务器的地址。

voice-config as-ip *ip-address*

缺省情况下，未配置备用服务器的地址。

(5) （可选）配置语音 VLAN。

voice-config voice-vlan *vlan-id* { **disable** | **enable** }

缺省情况下，未配置语音 VLAN。

(6) （可选）配置自动故障转移呼叫路由。

voice-config fail-over *ip-address dialer-string*

缺省情况下，未配置自动故障转移呼叫路由。

2.4.14 自定义DHCP选项

1. 自定义DHCP选项应用场景

本配置为 DHCP 服务器提供了灵活的选项配置方式，使得 DHCP 服务器可以为 DHCP 客户端提供更加丰富的选项内容。在以下情况下，可以使用本命令自定义 DHCP 选项：

- 随着 DHCP 的不断发展，新的 DHCP 选项会陆续出现。通过自定义 DHCP 选项，可以方便地添加新的 DHCP 选项。
- 有些选项的内容，RFC 中没有统一规定。厂商可以根据需要定义选项的内容，如 Option 43。通过自定义 DHCP 选项，可以为 DHCP 客户端提供厂商指定的信息。
- 设备上只提供了有限的选项配置命令（如 **gateway-list**、**dns-list** 命令），对于没有专门命令来配置的 DHCP 选项，可以通过 **option** 命令配置选项内容。例如，可以通过 **option 4 ip-address** 1.1.1.1 命令指定为 DHCP 客户端分配的时间服务器地址为 1.1.1.1。
- 扩展已有的 DHCP 选项。当前已提供的方式无法满足用户需求时（比如通过 **dns-list** 命令最多只能配置 8 个 DNS 服务器地址，如果用户需要配置的 DNS 服务器地址数目大于 8，则该命令无法满足需求），可以通过自定义 DHCP 选项的方式进行扩展。

2. 常用Option选项

表 2-1 中列出了常用的DHCP选项名称、对应的配置命令和推荐的Option命令参数信息。

表2-1 常用 Option 选项信息

选项编号	选项名称	对应的配置命令	推荐的 **option** 命令参数
3	Router Option	**gateway-list**	**ip-address**
6	Domain Name Server Option	**dns-list**	**ip-address**
15	Domain Name	**domain-name**	**ascii**
44	NetBIOS over TCP/IP Name Server Option	**nbns-list**	**ip-address**
46	NetBIOS over TCP/IP Node Type Option	**netbios-type**	**hex**
66	TFTP server name	**tftp-server**	**ascii**
67	Bootfile name	**bootfile-name**	**ascii**
43	Vendor Specific Information	-	**hex**

3. 配置限制和指导

- 自定义 DHCP 选项时，取值的获取比较复杂，配置错误可能会对 DHCP 的工作过程造成影响，请谨慎使用该功能。
- 用户可在 DHCP 地址池中自定义选项信息。
- 用户可在 DHCP 选项组中自定义选项信息，并在 DHCP 地址池中配置 DHCP 用户类和 DHCP 选项组关联，为 DHCP 客户端分配选项信息。

4. 自定义DHCP地址池选项

(1) 进入系统视图。

system-view

(2) 进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

(3) 自定义 DHCP 地址池选项。

option *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address*&<1-8> }

缺省情况下，未自定义 DHCP 地址池选项。

DHCP 服务器在应答 DHCP 客户端报文时，如果 DHCP 选项组的选项编号和 DHCP 地址池选项编号相同且匹配用户类时，以 DHCP 选项组的选项为准。

5. 自定义DHCP选项组选项

(1) 进入系统视图。

system-view

(2) 创建 DHCP 选项组，并进入 DHCP 选项组视图。

dhcp option-group *option-group-number*

(3) 自定义 DHCP 选项组选项。

option *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address*&<1-8> }

缺省情况下，未定义 DHCP 选项组的选项。

DHCP 服务器在应答客户端报文时，如果多个 DHCP 选项组的选项编号相同时，以最先匹配的 DHCP 用户类对应的 DHCP 选项组的选项为准。

(4) 返回系统视图。

quit

(5) 进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

(6) 配置 DHCP 用户类与 DHCP 选项组的关联。

class *class-name* **option-group** *option-group-number*

缺省情况下，未配置指定 DHCP 用户类与 DHCP 选项组的关联。

2.4.15 为DHCP服务器上的地址池绑定VPN实例

1. 功能简介

当地址池绑定了 VPN 实例后，DHCP 服务器可以将网络划分成公网和 VPN 私网。未配置 VPN 属性的地址池被划分到公网，配置了 VPN 属性的地址池被划分到相应的 VPN 私网，这样，对于处于公网或 VPN 私网中的客户端，服务器都能够选择合适的地址池来为客户端分配租约并且记录该客户端的状态信息。

DHCP 服务器可以通过如下方式判断 DHCP 客户端所属的 VPN 实例：

- 认证模块，用户接入时在 AAA 服务器处授权获得 VPN 实例信息；
- DHCP 服务器接收报文的接口绑定的 VPN 实例即为该客户端所属的 VPN 实例。

如果以上两种方式都可获取到 DHCP 客户端所属的 VPN 实例，则以认证模块为准。

设备作为 MCE（Multi-VPN-instance Customer Edge，多 VPN 实例用户网络边界设备）时，在设备上配置 DHCP 服务器功能，不仅可以为公网上的 DHCP 客户端分配 IP 地址，还可以实现为私网内的 DHCP 客户端分配 IP 地址，但是公网和私网之间、不同私网之间的 IP 地址空间不能重叠。MCE 的详细介绍，请参见“MPLS 配置指导”中的“MCE”。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

(3) 为 DHCP 服务器上的地址池绑定 VPN 实例。

vpn-instance *vpn-instance-name*

缺省情况下，DHCP 服务器上的地址池未绑定 VPN 实例。

2.4.16 配置DHCP用户类白名单功能

1. 功能简介

配置 DHCP 用户类白名单功能，DHCP 服务器只有收到属于用户类白名单的 DHCP 客户端发送的请求报文，才会进行处理。

2. 配置限制和指导

如果 DHCP 客户端请求的是静态绑定租约，则 DHCP 服务器不进行白名单检查直接进行处理。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

(3) 开启 DHCP 用户类白名单功能。

verify class

缺省情况下，DHCP 用户类白名单功能处于关闭状态。

(4) 配置 DHCP 用户类白名单包括的用户类名。

valid class *class-name*&<1-8>

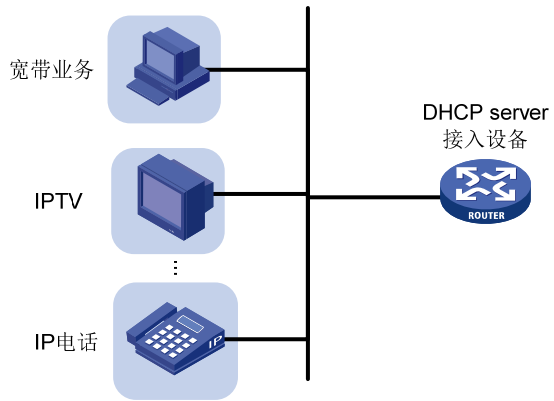
缺省情况下，未配置 DHCP 用户类白名单包括的用户类名。

2.4.17 配置DHCP服务器辅助网关信息

1. 功能简介

在某些接入组网类型（如PPPoE）中，如 图 2-1 所示，接入设备上除了配置接入特性还需要配置DHCP服务器功能。由于接入设备需要接入多种业务的客户端（如IPTV、IP电话和宽带业务等），而不同业务的设备需要获取不同网段的IP地址，所以接入设备的下行口一般不能配置IP地址。此时可以通过在接入设备的DHCP地址池中配置辅助网关功能使不同类型的业务流量能够正常转发。本特性使用辅助网关的IP地址和MAC地址信息应答客户端的ARP请求，即可实现对不同类型的业务流量的引导。

图2-1 DHCP 服务器辅助网关组网图



2. 配置限制和指导

如果地址池绑定了多机备份实例，需保证该地址池所在的接入设备为主用设备；如果地址池绑定了VPN 实例，需保证该 VPN 实例存在。满足了以上两个条件，该接入设备的辅助网关功能才能生效。

3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入 DHCP 地址池视图。

```
dhcp server ip-pool pool-name
```

(3) 配置 DHCP 服务器辅助网关信息。

```
gateway-list ip-address&<1-64> export-route
```

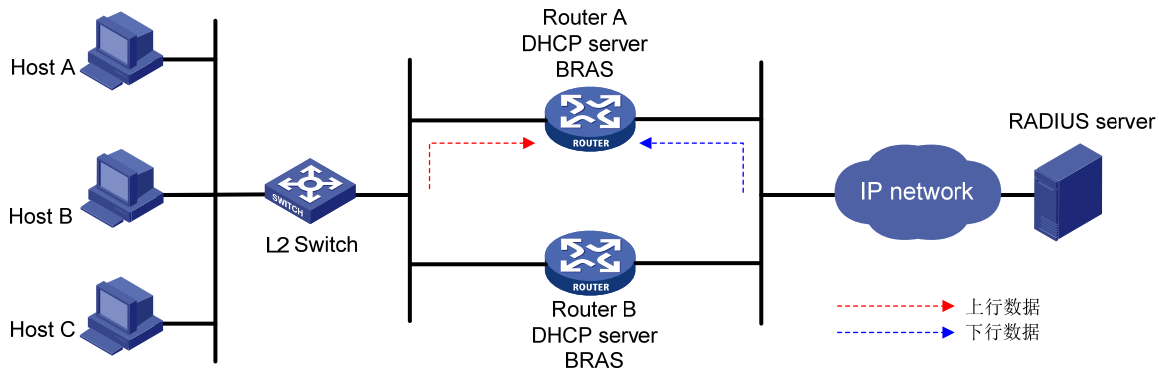
缺省情况下，未配置 DHCP 服务器辅助网关信息。

2.4.18 配置DHCP服务器辅助路由信息

1. 功能简介

在某些特定的业务模型（如 BRAS 组网）下，BRAS 设备需要实时监测网络流量，并将统计数据发送到 RADIUS 服务器。该统计数据为用户上线以来产生的所有上下行流量数据，而不能是设备在某个时间段内发生的上下行流量数据。由于 RADIUS 服务器刷新计数的方法是覆盖以前数据而不是进行累加，所以当一台设备的上下行流量分别从两台 BRAS 设备上通过时，在 RADIUS 服务器上记录的数据就会相互覆盖，这时 RADIUS 服务器得到的统计数据是不准确的。为了提高准确性，需保证一台设备的上下行流量经过同一台 BRAS 设备。通过配置辅助路由信息，并对外发布此网段路由，引导指定网段的下行数据流量来保证上下行流量从一台 BRAS 设备经过。

图2-2 DHCP 服务器辅助路由组网图



2. 配置限制和指导

如果地址池绑定了多机备份实例，需保证该地址池所在的接入设备为主用设备；如果地址池绑定了VPN 实例，需保证该 VPN 实例存在。满足了以上两个条件，该接入设备的辅助路由功能才能生效。

3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

(3) 配置 DHCP 服务器辅助路由信息。

network *network-address* [*mask-length* | **mask** *mask*] [**secondary**]

export-route

缺省情况下，未配置 DHCP 服务器辅助路由信息。

2.5 配置接口引用地址池

1. 功能简介

创建地址池，并在接口引用该地址池后，接口接收到 DHCP 请求，将优先为客户端分配静态绑定的 IP 地址；如果不存在静态绑定的 IP 地址，则从引用的地址池中选择 IP 地址分配给客户端。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置接口引用地址池。

dhcp server apply ip-pool *pool-name*

缺省情况下，接口未引用地址池。

如果接口引用的地址池不存在，将导致无法动态分配地址。

2.6 配置DHCP策略动态分配地址和其他参数

1. 功能简介

创建 DHCP 策略，并在接口引用该策略后，该接口接收到 DHCP 请求报文时，则根据配置顺序逐个匹配 DHCP 策略中通过 **class ip-pool** 命令指定的 DHCP 用户类。匹配情况如下：

- 若匹配 DHCP 用户类成功，当该 DHCP 用户类关联的 DHCP 地址池中存在可供分配的地址信息时，则从该 DHCP 地址池中分配 IP 地址和其他参数；当该 DHCP 用户类关联的 DHCP 地址池中不存在可供分配的地址信息时，IP 地址和其他参数分配失败。
- 若匹配 DHCP 策略中的所有 DHCP 用户类失败，当配置了默认 DHCP 地址池时，则从该地址池中分配 IP 地址和其他参数；当未配置默认 DHCP 地址池或默认 DHCP 地址池中不存在可供分配的地址信息时，IP 地址和其他参数分配失败。

若接收 DHCP 请求报文的接口引用的 DHCP 策略不存在或匹配的 DHCP 用户类关联的 DHCP 地址池不存在时，IP 地址和其他参数分配失败。

2. 配置限制和指导

DHCP 策略需要在接口上引用才生效。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 DHCP 策略，并进入 DHCP 策略视图。

dhcp policy *policy-name*

(3) 指定 DHCP 用户类关联的 DHCP 地址池。

class *class-name* **ip-pool** *pool-name*

缺省情况下，未指定 DHCP 用户类关联的 DHCP 地址池。

(4) 指定默认 DHCP 地址池。

default ip-pool *pool-name*

缺省情况下，未指定默认 DHCP 地址池。

(5) 退回系统视图。

quit

(6) 进入接口视图。

interface *interface-type interface-number*

(7) 指定接口引用的 DHCP 策略。

dhcp apply-policy *policy-name*

缺省情况下，接口未引用 DHCP 策略。

2.7 开启DHCP服务

1. 配置限制和指导

只有开启 DHCP 服务后，其它相关的 DHCP 服务器配置才能生效。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启 DHCP 服务。

dhcp enable

缺省情况下，DHCP 服务处于关闭状态。

2.8 配置接口工作在DHCP服务器模式

1. 功能简介

配置接口工作在 DHCP 服务器模式后，当接口收到 DHCP 客户端发来的 DHCP 报文时，将从 DHCP 服务器的地址池中分配地址等参数。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置接口工作在 DHCP 服务器模式。

dhcp select server

缺省情况下，接口工作在 DHCP 服务器模式。

2.9 配置IP地址冲突检测功能

1. 功能简介

为防止 IP 地址重复分配导致地址冲突，DHCP 服务器为客户端分配地址前，需要先对该地址进行探测。

DHCP 服务器的地址探测是通过 ping 功能实现的，通过检测是否能在指定时间内得到 ping 响应来判断是否存在地址冲突。DHCP 服务器发送目的地址为待分配地址的 ICMP 回显请求报文。如果在指定时间内收到 ICMP 回显响应报文，则认为存在地址冲突。DHCP 服务器从地址池中选择新的 IP 地址，并重复上述操作。如果在指定时间内未收到 ICMP 回显响应报文，则继续发送 ICMP 回显请求报文，直到发送的 ICMP 回显显示报文数目达到最大值。如果仍然未收到 ICMP 回显响应报文，则将地址分配给客户端，从而确保客户端获得的 IP 地址唯一。

DHCP 服务器通过 ping 操作来检测是否发生地址冲突，而 DHCP 客户端则通过发送免费 ARP 报文检测是否发生地址冲突。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) （可选）配置 DHCP 服务器发送 ICMP 回显请求报文的最大数目。

dhcp server ping packets *number*

缺省情况下，DHCP 服务器发送 ICMP 回显请求报文的最大数目为 1。

0 表示 DHCP 服务器将 IP 地址分配给 DHCP 客户端之前，不会通过 ping 操作探测该地址是否冲突。

(3) （可选）配置 DHCP 服务器等待 ICMP 回显响应报文的超时时间。

dhcp server ping timeout *milliseconds*

缺省情况下，DHCP 服务器等待 ICMP 回显响应报文的超时时间为 500 毫秒。

0 表示 DHCP 服务器将 IP 地址分配给 DHCP 客户端之前，不会通过 ping 操作探测该地址是否冲突。

2.10 配置Option 82的处理方式

1. 功能简介

如果配置 DHCP 服务器处理 Option 82，则当 DHCP 服务器收到带有 Option 82 的报文后，会在响应报文中携带 Option 82，并为客户端分配 IP 地址等信息。

如果配置 DHCP 服务器忽略 Option 82，则当 DHCP 服务器收到带有 Option 82 的报文后，不会在响应报文中携带 Option 82，只为客户端分配 IP 地址等信息。

为使Option 82 功能正常使用，需要在DHCP服务器和DHCP中继上都进行相应配置。DHCP中继支持Option 82 功能的相关配置请参见“3.9 配置DHCP中继支持Option 82 功能”。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 DHCP 服务器处理 Option 82。

dhcp server relay information enable

缺省情况下，DHCP 服务器处理 Option 82。

2.11 配置DHCP服务器兼容性

当 DHCP 客户端的行为不符合 RFC 协议规定时，为了与之兼容，需要配置 DHCP 服务器兼容性功能。

2.11.1 配置DHCP服务器始终以广播方式回复请求报文

1. 功能简介

一般情况下，只有 DHCP 请求报文的广播标志位为 1 的时候，DHCP 服务器才会以广播的方式发送应答报文。如果 DHCP 客户端发送的请求报文中广播标志位为 0，且该客户端不支持接收单播的应答报文，则可以配置 DHCP 服务器忽略请求报文的广播标志位，始终以广播方式发送应答报文。

当已经存在 IP 地址的客户端发出请求报文（即报文中 ciaddr 字段不为 0)时，无论是否开启 DHCP 服务器的广播回应报文功能，DHCP 服务器都会以单播形式将回应报文发送给 DHCP 客户端（即目的地址为 ciaddr）。

当请求报文通过 DHCP 中继转发到 DHCP 服务器（即报文中 giaddr 字段不为 0）时，无论是否开启 DHCP 服务器的广播回应报文功能，DHCP 服务器都会以单播形式将回应报文发送给 DHCP 中继（即目的地址为 giaddr）。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启 DHCP 服务器的广播回应报文功能。

dhcp server always-broadcast

缺省情况下，DHCP 服务器的广播回应报文功能处于关闭状态。DHCP 服务器根据请求报文中的广播标志位来决定以广播还是单播的形式发送应答报文。

2.11.2 配置DHCP服务器忽略BOOTP请求报文

1. 功能简介

BOOTP 客户端申请到的地址租约是无限期的。在某些组网环境中，可能不希望出现无限期的地址租约。此时，可以通过配置 DHCP 服务器忽略 BOOTP 请求报文，避免分配无限期的地址租约。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 DHCP 服务器忽略 BOOTP 请求报文。

dhcp server bootp ignore

缺省情况下，DHCP 服务器不会忽略 BOOTP 请求报文。

2.11.3 配置DHCP服务器以RFC 1048 规定的格式发送BOOTP应答报文

1. 功能简介

有些BOOTP客户端发送的请求报文中，vend字段的格式不符合RFC 1048的要求。对于这种报文，DHCP 服务器的缺省处理方法是不解析 vend 字段内容，将报文中 vend 字段的内容拷贝到回复报文中的 vend 字段回应给 BOOTP 客户端。

开启 DHCP 服务器的回应 RFC 1048 格式报文功能后，对于这种格式不符合 RFC 1048 要求的报文，DHCP 服务器会将需要回应的选项以符合 RFC 1048 要求的格式，封装到回复报文的 vend 字段，并回应给 BOOTP 客户端。

2. 配置限制和指导

本配置只在客户端通过 BOOTP 报文申请静态绑定地址时有效。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启 DHCP 服务器回应 RFC 1048 格式报文功能。

dhcp server bootp reply-rfc-1048

缺省情况下，DHCP 服务器回应 RFC 1048 格式报文功能处于关闭状态。

2.11.4 配置DHCP服务器发送DHCP应答报文不携带Option 60 选项

1. 功能简介

如果网络中存在不支持解析 Option 60 的 DHCP 客户端，DHCP 服务器需要配置 DHCP 服务器发送 DHCP 应答报文时不携带 Option 60 选项功能。配置该功能后，DHCP 服务器无论收到的 DHCP 报文中是否携带 Option 60 选项，也无论 DHCP 地址池中是否已经配置了 Option 60 选项内容，DHCP 服务器应答的 DHCP 报文中都不携带 Option 60 选项。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 DHCP 服务器发送 DHCP 应答报文不携带 Option 60 选项。

dhcp server reply-exclude-option60

缺省情况下，DHCP 服务器发送 DHCP 应答报文时可以携带 Option 60 选项。

2.12 配置DHCP服务器发送DHCP报文的DSCP优先级

1. 功能简介

DSCP优先级用来体现报文自身的优先等级，决定报文传输的优先程度。通过本配置可以指定DHCP服务器发送的 DHCP 报文的 DSCP 优先级。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 DHCP 服务器发送 DHCP 报文的 DSCP 优先级。

dhcp dscp *dscp-value*

缺省情况下，DHCP 服务器发送 DHCP 报文的 DSCP 优先级为 56。

2.13 配置DHCP服务器租约固化功能

1. 功能简介

DHCP 服务器重启后，设备上记录的租约信息将丢失，会影响 DHCP 服务器的正常业务。

DHCP 服务器租约固化功能将 DHCP 服务器的在用地址租约和冲突表项保存到指定的文件中，DHCP 服务器设备重启后，自动根据该文件恢复 DHCP 服务器的租约信息，从而保证 DHCP 服务器的租约信息不会丢失。

当 DHCP 服务器设备重启后，自动根据该文件恢复 DHCP 服务器的租约信息，租约恢复的过程中，DHCP 服务器不能提供 DHCP 业务。所以当恢复过程出现问题导致恢复过程无法结束时，用户可配置 **dhcp server database update stop** 命令终止当前的 DHCP 服务器表项恢复操作，以便 DHCP 服务器能及时提供 DHCP 服务。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 指定存储 DHCP 服务器表项的文件名称。

dhcp server database filename { *filename* | **url** *url* [**username** *username* [**password** { **cipher** | **simple** } *string*]] }

缺省情况下，未指定存储 DHCP 服务器表项的文件名称。

执行本命令后，会立即触发一次表项备份。

(3) （可选）将当前的 DHCP 服务器表项保存到用户指定的文件中。

dhcp server database update now

本命令只用来触发一次 DHCP 服务器表项的备份。

(4) （可选）配置刷新 DHCP 服务器表项存储文件的延迟时间。

dhcp server database update interval *interval*

缺省情况下，若 DHCP 服务器表项不变化，则不刷新存储文件；若 DHCP 服务器表项发生变化，默认在 300 秒之后刷新存储文件。

(5) （可选）终止当前的 DHCP 服务器表项恢复操作。

dhcp server database update stop

本命令只用来触发一次终止 DHCP 服务器表项信息的恢复。

2.14 开启DHCP服务器的用户下线探测功能

1. 功能简介

DHCP 服务器的用户下线探测功能以 ARP 表项老化功能为基础，当 ARP 表项老化时认为该表项对应的用户已下线。

如果在接口上开启了 DHCP 服务器的用户下线探测功能，则当 ARP 表项老化时，系统会删除该表项对应用户的地址绑定信息。

2. 配置限制和指导

手工删除 ARP 表项，不会触发 DHCP 服务器删除对应用户的地址绑定信息。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 开启 DHCP 服务器的用户下线探测功能。

dhcp client-detect

缺省情况下，DHCP 服务器的用户下线探测功能处于关闭状态。

2.15 配置DHCP告警功能

1. 功能简介

为了避免地址池地址耗尽，导致用户无法上线，用户可以设置地址池使用率的告警阀值，当地址池中地址使用率超过阀值时，系统发送告警信息到设备的信息中心，通过设置信息中心的告警信息的发送参数，最终决定日志报文的输出规则（即是否允许输出以及输出方向），提醒管理员进行地址池合理规划。有关信息中心参数的配置，请参见“网络管理和监控配置指导”中的“信息中心”。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 DHCP 地址池视图。

dhcp server ip-pool *pool-name*

(3) （可选）设置地址池使用率告警门限阈值。

ip-in-use threshold *threshold-value*

缺省情况下，地址池使用率告警门限阈值为 100%。

2.16 开启DHCP服务器日志信息功能

1. 功能简介

DHCP 服务器日志可以方便管理员定位问题和解决问题。设备生成 DHCP 日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

2. 配置限制和指导

比如大量 DHCP 客户端发生上下线操作时，DHCP 服务器会输出大量日志信息，这可能会降低设备性能，影响 DHCP 服务器分配 IP 地址的速度。为了避免该情况的发生，用户可以关闭 DHCP 服务器日志信息功能，使得 DHCP 服务器不再输出日志信息。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启 DHCP 服务器日志信息功能。

dhcp log enable

缺省情况下，DHCP 服务器日志信息功能处于关闭状态。

2.17 DHCP服务器显示和维护

提示

DHCP 服务器重启或使用 **reset dhcp server ip-in-use** 命令清除租约后，DHCP 服务器上不存在租约信息。此时客户端如果发出续约请求将会被拒绝，客户端需要重新申请 IP 地址。

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 DHCP 服务器的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令清除 DHCP 服务器的相关信息。

表2-2 DHCP 服务器显示和维护

操作	命令
显示DHCP的地址冲突信息	**display dhcp server conflict** [**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*]
显示DHCP服务器的表项备份信息	**display dhcp server database**
显示租约过期的地址绑定信息	**display dhcp server expired** [[**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*] | **pool** *pool-name*]
显示DHCP地址池的空闲地址信息	**display dhcp server free-ip** [**pool** *pool-name* | **vpn-instance** *vpn-instance-name*]
显示DHCP地址绑定信息	**display dhcp server ip-in-use** [[**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*] | **pool** *pool-name*]
显示DHCP地址池的信息	**display dhcp server pool** [*pool-name* | **vpn-instance** *vpn-instance-name*]
显示DHCP服务器的统计信息	**display dhcp server statistics** [**pool** *pool-name* | **vpn-instance** *vpn-instance-name*]
清除DHCP的地址冲突信息	**reset dhcp server conflict** [**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*]
清除租约过期的地址绑定信息	**reset dhcp server expired** [[**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*] | **pool** *pool-name*]
清除DHCP的正式绑定和临时绑定信息	**reset dhcp server ip-in-use** [[**ip** *ip-address*] [**vpn-instance** *vpn-instance-name*] | **pool** *pool-name*]
清除DHCP服务器的统计信息	**reset dhcp server statistics** [**vpn-instance**

操作	命令
	vpn-instance-name]

2.18 DHCP服务器典型配置举例

2.18.1 静态绑定地址配置举例

1. 组网需求

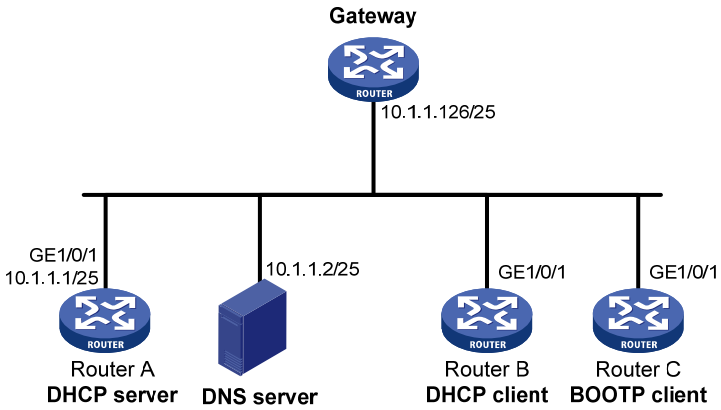
Router B 和 Router C 分别作为 DHCP 客户端和 BOOTP 客户端，从 DHCP 服务器 Router A 获取静态绑定的 IP 地址、域名服务器、网关地址。

其中：

- Router B 的接口 GigabitEthernet1/0/1 的客户端 ID 为：0030-3030-662e-6532-3030-2e30-3030-322d-4574-6865-726e-6574；
- Router C 的接口 GigabitEthernet1/0/1 的 MAC 地址为：000f-e200-01c0。

2. 组网图

图2-3 静态绑定地址组网图



3. 配置步骤

(1) 配置接口的 IP 地址

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ip address 10.1.1.1 25
[RouterA-GigabitEthernet1/0/1] quit
```

(2) 配置 DHCP 服务

创建 DHCP 地址池 0。

```
[RouterA] dhcp server ip-pool 0
```

配置采用静态绑定方式为 Router B 分配 IP 地址。

```
[RouterA-dhcp-pool-0] static-bind ip-address 10.1.1.5 25 client-identifier
0030-3030-662e-6532-3030-2e30-3030-322d-4574-6865-726e-6574
```

配置采用静态绑定方式为 Router C 分配 IP 地址。

```
[RouterA-dhcp-pool-0] static-bind ip-address 10.1.1.6 25 hardware-address
000f-e200-01c0
```

配置域名服务器、网关地址。

```
[RouterA-dhcp-pool-0] dns-list 10.1.1.2
[RouterA-dhcp-pool-0] gateway-list 10.1.1.126
[RouterA-dhcp-pool-0] quit
```

开启 DHCP 服务。

```
[RouterA] dhcp enable
```

配置接口 GigabitEthernet1/0/1 工作在 DHCP 服务器模式。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] dhcp select server
[RouterA-GigabitEthernet1/0/1] quit
```

4. 验证配置

配置完成后，Router B 和 Router C 可以从 DHCP 服务器 Router A 分别申请到 IP 地址 10.1.1.5 和 10.1.1.6，并获取相关网络配置参数。通过 **`display dhcp server ip-in-use`** 命令可以查看 DHCP 服务器为客户端分配的 IP 地址。

```
[RouterA] display dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
10.1.1.5         0030-3030-662e-6532-  Jan 21 14:27:27 2014  Static(C)
                 3030-2e30-3030-322d-
                 4574-6865-726e-6574
10.1.1.6         000f-e200-01c0        Unlimited             Static(C)
```

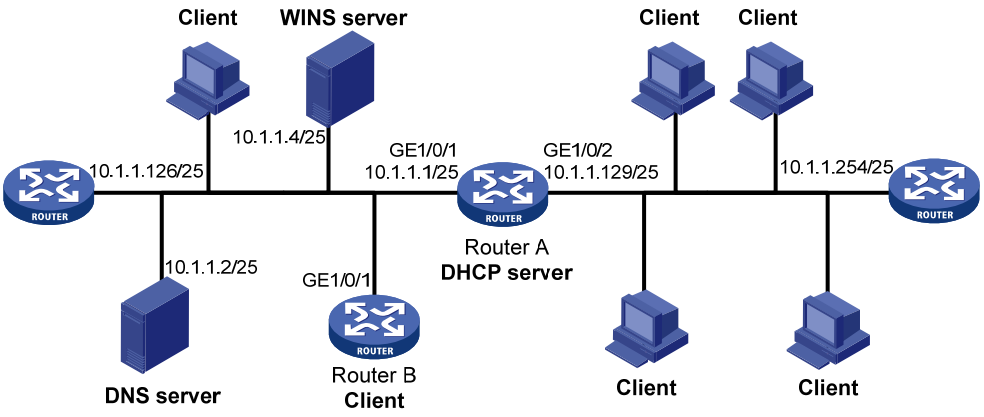
2.18.2 动态分配地址配置举例

1. 组网需求

- 作为 DHCP 服务器的 Router A 为网段 10.1.1.0/24 中的客户端动态分配 IP 地址，该地址池网段分为两个子网网段：10.1.1.0/25 和 10.1.1.128/25；
- Router A 的两个以太网接口，GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 的地址分别为 10.1.1.1/25 和 10.1.1.129/25；
- 10.1.1.0/25 网段内的地址租用期限为 10 天 12 小时，域名后缀为 aabbcc.com，DNS 服务器地址为 10.1.1.2/25，WINS 服务器地址为 10.1.1.4/25，网关的地址为 10.1.1.126/25；
- 10.1.1.128/25 网段内的地址租用期限为 5 天，域名后缀为 aabbcc.com，DNS 服务器地址为 10.1.1.2/25，无 WINS 服务器地址，网关的地址为 10.1.1.254/25。

2. 组网图

图2-4 DHCP 组网图



3. 配置步骤

(1) 配置 DHCP server 各接口的 IP 地址（略）

(2) 配置 DHCP 服务

配置不参与自动分配的 IP 地址（DNS 服务器、WINS 服务器和网关地址）。

```
<RouterA> system-view
[RouterA] dhcp server forbidden-ip 10.1.1.2
[RouterA] dhcp server forbidden-ip 10.1.1.4
[RouterA] dhcp server forbidden-ip 10.1.1.126
[RouterA] dhcp server forbidden-ip 10.1.1.254
```

配置 DHCP 地址池 1，用来为 10.1.1.0/25 网段内的客户端分配 IP 地址和网络配置参数。

```
[RouterA] dhcp server ip-pool 1
[RouterA-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.128
[RouterA-dhcp-pool-1] expired day 10 hour 12
[RouterA-dhcp-pool-1] domain-name aabbcc.com
[RouterA-dhcp-pool-1] dns-list 10.1.1.2
[RouterA-dhcp-pool-1] gateway-list 10.1.1.126
[RouterA-dhcp-pool-1] nbns-list 10.1.1.4
[RouterA-dhcp-pool-1] quit
```

配置 DHCP 地址池 2，用来为 10.1.1.128/25 网段内的客户端分配 IP 地址和网络配置参数。

```
[RouterA] dhcp server ip-pool 2
[RouterA-dhcp-pool-2] network 10.1.1.128 mask 255.255.255.128
[RouterA-dhcp-pool-2] expired day 5
[RouterA-dhcp-pool-2] domain-name aabbcc.com
[RouterA-dhcp-pool-2] dns-list 10.1.1.2
[RouterA-dhcp-pool-2] gateway-list 10.1.1.254
[RouterA-dhcp-pool-2] quit
```

开启 DHCP 服务。

```
[RouterA] dhcp enable
```

配置接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 工作在 DHCP 服务器模式。

```
[RouterA] interface gigabitethernet 1/0/1
```

```
[RouterA-GigabitEthernet1/0/1] dhcp select server
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] dhcp select server
[RouterA-GigabitEthernet1/0/2] quit
```

4. 验证配置

配置完成后，10.1.1.0/25 和 10.1.1.128/25 网段的客户端可以从 DHCP 服务器 Router A 申请到相应网段的 IP 地址和网络配置参数。通过 **display dhcp server ip-in-use** 命令可以查看 DHCP 服务器为客户端分配的 IP 地址。

```
[RouterA] display dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
10.1.1.3         0100-3138-6539-2e62-  Jan 14 22:25:03 2015  Auto(C)
                 6233-632e-3032-3035-
                 2d47-4530-2f30
10.1.1.5         0100-31fe-6542-037e-  Jan 14 22:25:03 2015  Auto(C)
                 0230-635b-3032-3047-
                 0262-0e71-2f5e
10.1.1.130       0130-3030-302e-3030-  Jan 9 10:45:11 2015   Auto(C)
                 3066-2e30-3030-332d-
                 4575-6865-721e
10.1.1.131       0130-3000-20fe-0230-  Jan 9 10:45:11 2015   Auto(C)
                 2070-5202-0120-131e-
                 0202-0190-6823
10.1.1.132       0120-2012-2011-0230-  Jan 9 10:45:11 2015   Auto(C)
                 217e-5202-1120-2534-
                 0202-0190-689a
10.1.1.133       0120-21d0-1202-0242-  Jan 9 10:45:11 2015   Auto(C)
                 2188-5202-0320-2255-
                 e039-2101-0431
```

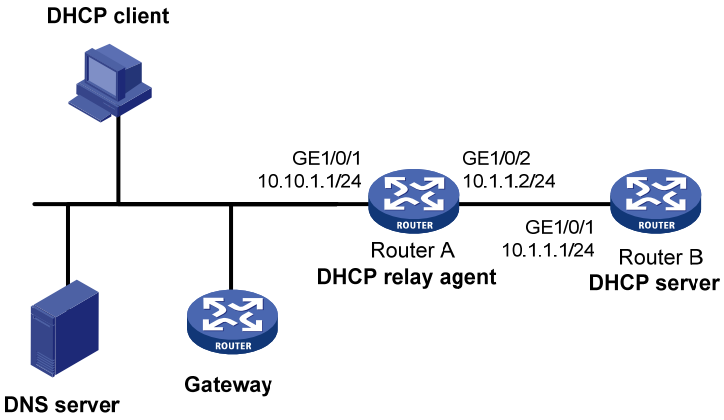
2.18.3 按用户类分配地址配置举例

1. 组网需求

- Router A 作为 DHCP 中继转发 DHCP 报文。在 Router A 上配置 DHCP 中继支持 Option 82 功能，使得 Router A 能够为 DHCP 客户端发送的请求报文添加 Option 82。
- Router B 作为 DHCP 服务器为客户端分配 IP 地址和其他网络配置参数。如果 Router B 接收到的请求报文中带有 Option 82，则为该客户端分配地址范围 10.10.1.2 到 10.10.1.10 内的 IP 地址。如果 Router B 接收到的请求报文匹配硬件地址 aabb-aabb-aab0，硬件地址掩码为 ffff-ffff-fff0，则为该客户端分配地址围 10.10.1.11 到 10.10.1.26 内的 IP 地址。
- Router B 为 10.10.1.0/24 网段内的客户端分配的 DNS 服务器地址为 10.10.1.20/24，网关的地址为 10.10.1.254/24。

2. 组网图

图2-5 按 DHCP 用户类分配地址组网图



3. 配置步骤

(1) 配置 DHCP server 各个接口的 IP 地址（略）

(2) 配置 DHCP 服务

创建 DHCP 用户类 tt，设置匹配规则编号 1，匹配请求报文中带有 Option 82 的客户端。

```
<RouterB> system-view
[RouterB] dhcp class tt
[RouterB-dhcp-class-tt] if-match rule 1 option 82
[RouterB-dhcp-class-tt] quit
```

创建 DHCP 用户类 ss，设置匹配规则编号 1，匹配硬件地址 aabb-aabb-aab0，硬件地址掩码 ffff-ffff-fff0 的请求报文。

```
[RouterB] dhcp class ss
[RouterB-dhcp-class-ss] if-match rule 1 hardware-address aabb-aabb-aab0 mask
ffff-ffff-fff0
[RouterB-dhcp-class-ss] quit
```

创建 DHCP 地址池 aa，配置地址范围和用户类的地址范围，配置网关和 DNS 服务器的地址。

```
[RouterB] dhcp server ip-pool aa
[RouterB-dhcp-pool-aa] network 10.10.1.0 mask 255.255.255.0
[RouterB-dhcp-pool-aa] address range 10.10.1.2 10.10.1.100
[RouterB-dhcp-pool-aa] class tt range 10.10.1.2 10.10.1.10
[RouterB-dhcp-pool-aa] class ss range 10.10.1.11 10.10.1.26
[RouterB-dhcp-pool-aa] gateway-list 10.10.1.254
[RouterB-dhcp-pool-aa] dns-list 10.10.1.20
[RouterB-dhcp-pool-aa] quit
```

开启 DHCP 服务，且配置 DHCP 服务器处理 Option 82 信息。

```
[RouterB] dhcp enable
[RouterB] dhcp server relay information enable
```

配置接口 GigabitEthernet1/0/1 工作在 DHCP 服务器模式。

```
[RouterB] interface gigabitethernet 1/0/1
```

```
[RouterB-GigabitEthernet1/0/1] dhcp select server
[RouterB-GigabitEthernet1/0/1] quit
```

4. 验证配置

配置完成后，10.10.1.0/24 网段的客户端通过用户类分配方式可以从 DHCP 服务器 Router B 申请到相应地址范围的 IP 地址和网络配置参数。通过 **display dhcp server ip-in-use** 命令可以查看 DHCP 服务器为它分配的 IP 地址。

```
[RouterB] display dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
10.10.1.2        0100-3138-6539-2e62-  Jan 14 22:25:03 2015  Auto(C)
                 6233-632e-3032-3035-
                 2d47-4530-2f30
10.10.1.11       aabb-aabb-aab1        Jan 14 22:25:03 2015  Auto(C)
```

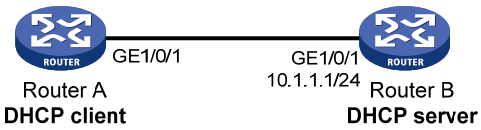
2.18.4 用户类白名单功能配置举例

1. 组网需求

Router B 作为 DHCP 服务器只为局域网中匹配硬件地址 aabb-aabb-0000，硬件地址掩码为 ffff-ffff-0000 的 DHCP 客户端动态分配网段为 10.1.1.0/24 的 IP 地址。

2. 组网图

图2-6 用户类白名单功能典型组网图



3. 配置步骤

(1) 配置 DHCP 服务器接口的 IP 地址（略）

(2) 配置 DHCP 服务

创建 DHCP 用户类 ss，设置匹配规则编号 1，匹配硬件地址为 aabb-aabb-0000，硬件地址掩码为 ffff-ffff-0000

```
<RouterB> system-view
[RouterB] dhcp class ss
[RouterB-dhcp-class-ss] if-match rule 1 hardware-address aabb-aabb-0000 mask
ffff-ffff-0000
[RouterB-dhcp-class-ss] quit
```

创建 DHCP 地址池 aa，配置可分配的地址范围为 10.1.1.0/24，开启用户类白名单功能，配置白名单中包括的用户类为 ss

```
[RouterB] dhcp server ip-pool aa
[RouterB-dhcp-pool-aa] network 10.1.1.0 mask 255.255.255.0
[RouterB-dhcp-pool-aa] verify class
[RouterB-dhcp-pool-aa] valid class ss
[RouterB-dhcp-pool-aa] quit
```

开启 DHCP 服务

```
[RouterB] dhcp enable
```

配置接口 GigabitEthernet1/0/1 工作在 DHCP 服务器模式

```
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] dhcp select server
[RouterB-GigabitEthernet1/0/1] quit
```

4. 验证配置

配置完成后，匹配硬件地址 aabb-aabb-0000，硬件地址掩码 ffff-ffff-0000 的客户端可以从 DHCP 服务器 Router B 申请到地址范围为 10.1.1.0/24 网段的 IP 地址。通过 **display dhcp server ip-in-use** 命令可以查看 DHCP 服务器分配的 IP 地址。

```
[RouterB] display dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
10.1.1.2         aabb-aabb-ab01        Jan 14 22:25:03 2015  Auto(C)
```

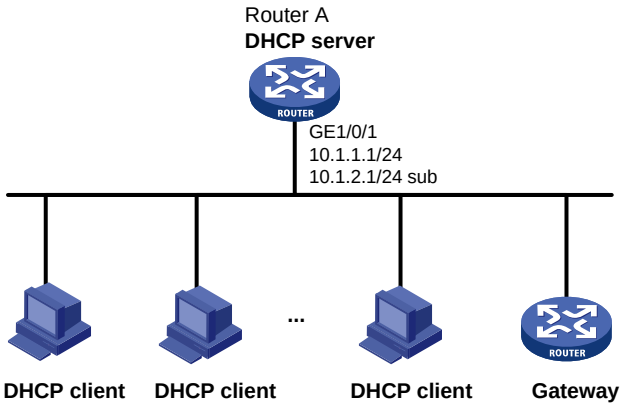
2.18.5 主从网段配置举例

1. 组网需求

- 作为 DHCP 服务器的 Router A 为局域网中的客户端动态分配 IP 地址。
- DHCP 服务器地址池中有两个网段的地址：10.1.1.0/24 和 10.1.2.0/24。当 10.1.1.0/24 网段没有空闲地址后，DHCP 服务器继续从 10.1.2.0/24 网段中选择 IP 地址分配给客户端。
- Router A 为网段 10.1.1.0/24 内的客户端分配的网关地址为 10.1.1.254/24；为网段 10.1.2.0/24 内的客户端分配的网关地址为和 10.1.2.254/24。

2. 组网图

图2-7 主从网段组网图



3. 配置步骤

创建 DHCP 地址池 aa，配置主网段地址范围和从网段地址范围，配置网关地址。

```
<RouterA> system-view
[RouterA] dhcp server ip-pool aa
[RouterA-dhcp-pool-aa] network 10.1.1.0 mask 255.255.255.0
[RouterA-dhcp-pool-aa] gateway-list 10.1.1.254
```

```
[RouterA-dhcp-pool-aa] network 10.1.2.0 mask 255.255.255.0 secondary
[RouterA-dhcp-pool-aa-secondary] gateway-list 10.1.2.254
[RouterA-dhcp-pool-aa-secondary] quit
[RouterA-dhcp-pool-aa] quit
```

开启 DHCP 服务。

```
[RouterA] dhcp enable
```

配置接口 GigabitEthernet1/0/1 的主从 IP 地址，并配置该接口工作在 DHCP 服务器模式。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ip address 10.1.1.1 24
[RouterA-GigabitEthernet1/0/1] ip address 10.1.2.1 24 sub
[RouterA-GigabitEthernet1/0/1] dhcp select server
[RouterA-GigabitEthernet1/0/1] quit
```

4. 验证配置

配置完成后，当 DHCP 服务器地址池主网段中没有空闲地址分配给客户端时，服务器会从该地址池中的从网段获取地址分配给客户端 IP 地址和网络配置参数。通过 **display dhcp server ip-in-use** 命令可以查看 DHCP 服务器已分配的主从网段 IP 地址。（此处只截取部分显示信息）

```
[RouterA] display dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
10.1.1.2         0100-3138-6539-2e62-  Jan 14 22:25:03 2015  Auto(C)
                 6233-632e-3032-3035-
                 2d47-4530-2f30
10.1.2.2         0130-3030-302e-3030-  Jan 14 22:25:03 2015  Auto(C)
                 3066-2e30-3030-332d-
                 4575-6865-721e
```

2.18.6 自定义DHCP选项配置举例

1. 组网需求

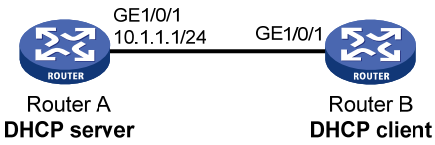
DHCP 客户端 Router B 从 DHCP 服务器 Router A 获取 IP 地址和 PXE 引导服务器地址信息：

- 客户端 IP 地址所在网段为 10.1.1.0/24；
- 匹配硬件地址 aabb-aabb-0000，硬件地址掩码 ffff-ffff-0000 的客户端的 PXE 引导服务器地址为 2.3.4.5 和 3.3.3.3，其他客户端的 PXE 引导服务器地址为 1.2.3.4 和 2.2.2.2。

DHCP服务器需要通过自定义DHCP选项的方式配置Option 43 的内容，从而实现为客户端分配PXE引导服务器地址。Option 43 和PXE服务器地址列表的格式分别如 图 1-5 和 图 1-7。DHCP服务器上地址池中配置的Option 43 选项内容为 80 0B 00 00 02 01 02 03 04 02 02 02 02，其中 80 为子选项类型（Sub-option type），0B为子选项长度（Sub-option length），00 00 为PXE服务器类型（PXE server type），02 为服务器数目（Server number），01 02 03 04 02 02 02 02 为服务器的IP地址 1.2.3.4 和 2.2.2.2。

2. 组网图

图2-8 自定义 DHCP 选项典型配置举例



3. 配置步骤

(1) 配置接口 GigabitEthernet1/0/1 的 IP 地址（略）

(2) 配置 DHCP 服务

创建 DHCP 用户类 ss，设置匹配规则编号 1，匹配硬件地址 aabb-aabb-0000，硬件地址掩码为 ffff-ffff-0000。

```
<RouterA> system-view
[RouterA] dhcp class ss
[RouterA-dhcp-class-ss] if-match rule 1 hardware-address aabb-aabb-0000 mask
ffff-ffff-0000
[RouterA-dhcp-class-ss] quit
```

创建 DHCP 选项组 1，配置选项信息。

```
[RouterA] dhcp option-group 1
[RouterA-dhcp-option-group-1] option 43 hex 800B0000020203040503030303
```

配置 DHCP 地址池 0。

```
[RouterA] dhcp server ip-pool 0
[RouterA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
[RouterA-dhcp-pool-0] option 43 hex 800B000002010203040202020 2
[RouterA-dhcp-pool-0] class ss option-group 1
[RouterA-dhcp-pool-0] quit
```

开启 DHCP 服务。

```
[RouterA] dhcp enable
```

配置接口 GigabitEthernet1/0/1 工作在 DHCP 服务器模式。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] dhcp select server
[RouterA-GigabitEthernet1/0/1] quit
```

4. 验证配置

配置完成后，Router B 可以从 DHCP 服务器 Router A 获取到 10.1.1.0/24 网段的 IP 地址和 PXE 引导服务器地址。通过 **display dhcp server ip-in-use** 命令可以查看 DHCP 服务器为客户端分配的 IP 地址。

```
[RouterA] display dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
10.1.1.2         aabb-aabb-ab01        Jan 14 22:25:03 2015  Auto(C)
```

2.19 DHCP服务器常见故障处理

2.19.1 DHCP客户端获取到冲突的IP地址

1. 故障现象

客户端从 DHCP 服务器动态获得的 IP 地址与其他主机 IP 地址冲突。

2. 故障分析

可能是网络上有主机私自配置了 IP 地址，导致冲突。

3. 故障处理

(1) 禁用客户端的网卡或断开其网线，从另外一台主机执行 ping 操作，检查网络中是否已经存在该 IP 地址的主机。

(2) 如果能够收到 ping 操作的响应消息，则说明该 IP 地址已由用户静态配置。在 DHCP 服务器上执行 **dhcp server forbidden-ip** 命令，禁止该 IP 地址参与动态地址分配。

(3) 重新启用客户端的网卡或连接好其网线，在客户端释放并重新获取 IP 地址。以 Windows XP 为例，在 Windows 环境下运行 **cmd** 进入 DOS 环境，使用 **ipconfig /release** 命令释放 IP 地址，之后使用 **ipconfig /renew** 重新获取 IP 地址。

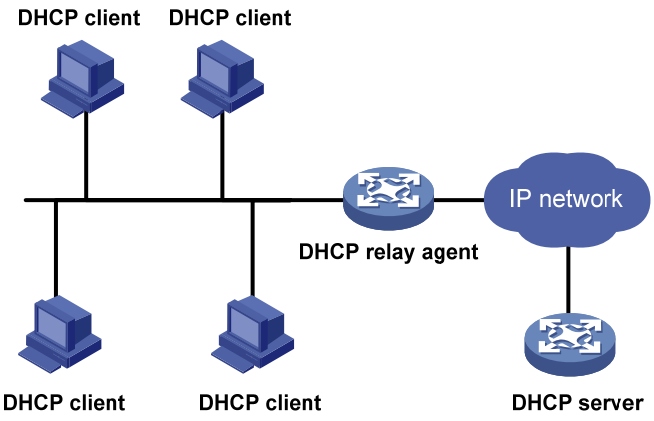
3 DHCP中继

3.1 DHCP中继简介

DHCP 客户端和 DHCP 服务器处于不同物理网段时，客户端可以通过 DHCP 中继与 DHCP 服务器通信，获取 IP 地址及其他配置信息。

图 3-1 是DHCP中继的典型应用示意图。

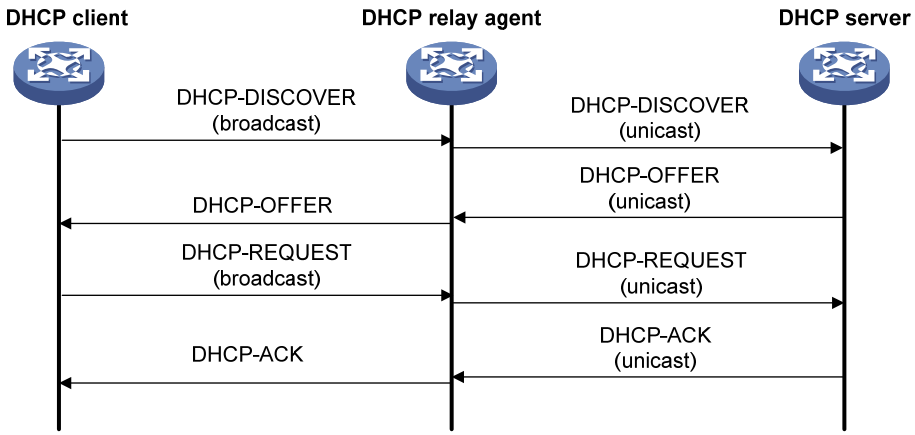
图3-1 DHCP 中继的典型组网应用



3.1.2 DHCP中继的基本原理

通过DHCP中继完成动态配置的过程中，DHCP客户端与DHCP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。下面只说明DHCP中继的转发过程，报文的具体交互过程请参见“1.2.2 IP地址获取过程”。

图3-2 DHCP 中继的工作过程



如 图 3-2 所示，DHCP中继的工作过程为：

(1) 具有 DHCP 中继功能的网络设备收到 DHCP 客户端以广播方式发送的 DHCP-DISCOVER 或 DHCP-REQUEST 报文后，将报文中的 giaddr 字段填充为 DHCP 中继的 IP 地址，并根据配置将报文单播转发给指定的 DHCP 服务器。

(2) DHCP 服务器根据 giaddr 字段为客户端分配 IP 地址等参数，并通过 DHCP 中继将配置信息转发给客户端，完成对客户端的动态配置。

3.1.3 DHCP中继支持Option 82 功能

Option 82 记录了DHCP客户端的位置信息。管理员可以利用该选项定位DHCP客户端，实现根据 Option 82 为客户端分配特定范围的地址、对客户端进行安全和计费等控制。Option 82 的详细介绍请参见“1.6.2 中继代理信息选项（Option 82）”。

如果DHCP中继支持Option 82 功能，则当DHCP中继接收到DHCP请求报文后，将根据报文中是否包含Option 82 以及用户配置的处理策略及填充模式等对报文进行相应的处理，并将处理后的报文转发给DHCP服务器。具体的处理方式见 表 3-1。

如果 DHCP 中继收到的应答报文中带有 Option 82，则会将 Option 82 删除后再转发给 DHCP 客户端。

表3-1 DHCP 中继支持 Option 82 的处理方式

收到 DHCP 请求报文	处理策略	DHCP 中继对报文的处理
收到的报文中带有 Option 82	Drop	丢弃报文
	Keep	保持报文中的Option 82不变并进行转发
	Replace	根据DHCP中继上配置的填充模式、内容、格式等填充Option 82，替换报文中原有的Option 82并进行转发
收到的报文中不带有Option 82	-	根据DHCP中继上配置的填充模式、内容、格式等填充Option 82，添加到报文中并进行转发

3.1.4 DHCP中继支持MCE

设备作为 MCE（Multi-VPN-instance Customer Edge，多 VPN 实例用户网络边界设备）时，在设备上配置 DHCP 中继功能，不仅可以为公网上的 DHCP 服务器和 DHCP 客户端转发 DHCP 报文，还可以实现为私网内的 DHCP 服务器和 DHCP 客户端转发 DHCP 报文。MCE 的详细介绍，请参见“MPLS 配置指导” 中的“MCE”。

3.2 DHCP中继配置任务简介

DHCP 中继配置任务如下：

(1) 开启DHCP服务

(2) 配置接口工作在DHCP中继模式

(3) 指定DHCP服务器的地址

(4) （可选）指定DHCP客户端对应的DHCP中继地址池

(5) （可选）配置DHCP中继的安全功能

(6) （可选）配置通过DHCP中继释放客户端的IP地址

(7) （可选）配置DHCP中继支持Option 82 功能

(8) （可选）配置DHCP中继发送DHCP报文的DSCP优先级

(9) （可选）配置DHCP中继在DHCP报文中填充的中继地址

(10) （可选）指定DHCP中继向DHCP服务器转发报文的源地址

3.3 开启DHCP服务

1. 配置限制和指导

只有开启 DHCP 服务后，其它相关的 DHCP 中继配置才能生效。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启 DHCP 服务。

dhcp enable

缺省情况下，DHCP 服务处于关闭状态。

3.4 配置接口工作在DHCP中继模式

1. 功能简介

配置接口工作在中继模式后，当接口收到 DHCP 客户端发来的 DHCP 报文时，会将报文转发给 DHCP 服务器，由服务器分配地址。

DHCP 客户端通过 DHCP 中继获取 IP 地址时，DHCP 服务器上需要配置与 DHCP 中继连接 DHCP 客户端的接口 IP 地址所在网段（网络号和掩码）匹配的地址池，否则会导致 DHCP 客户端无法获得正确的 IP 地址。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置接口工作在 DHCP 中继模式。

dhcp select relay

缺省情况下，开启 DHCP 服务后，接口工作在 DHCP 服务器模式。

3.5 指定DHCP服务器的地址

3.5.1 指定DHCP中继对应的DHCP服务器地址

1. 功能简介

为了提高可靠性，可以在一个网络中设置多个 DHCP 服务器。DHCP 中继上配置多个 DHCP 服务器后，DHCP 中继会将客户端发来的 DHCP 报文转发给所有的服务器。

2. 配置限制和指导

指定的 DHCP 服务器的 IP 地址不能与 DHCP 中继的接口 IP 地址在同一网段。否则，可能导致客户端无法获得 IP 地址。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 指定 DHCP 中继对应的 DHCP 服务器地址。

dhcp relay server-address *ip-address*

缺省情况下，未指定 DHCP 服务器的地址。

通过多次执行 **dhcp relay server-address** 命令可以指定多个 DHCP 服务器，一个接口下最多可以指定 8 个 DHCP 服务器。

3.5.2 指定中继地址池对应的DHCP服务器地址

1. 功能简介

对于某些特定的用户接入方式，基于用户接入位置信息的不同，网络中存在大量不同类型的用户。为了使相同类型的用户可以从指定的 DHCP 服务器申请 IP 地址等网络参数，接入模块根据用户注册信息，使不同的用户选择不同的 DHCP 中继地址池，并从中继地址池下配置的 DHCP 服务器获取 IP 地址等网络参数。

为了提高可靠性，一个 DHCP 中继地址池下配置多个 DHCP 服务器地址，当 DHCP 客户端匹配该中继地址池后，DHCP 中继会将 DHCP 客户端发来的 DHCP 报文转发给该地址池对应所有的 DHCP 服务器。

一台 DHCP 中继的一个接口下可能连接不同类型的用户，当 DHCP 中继转发 DHCP 客户端请求报文给 DHCP 服务器时，不能再以中继接口的 IP 地址作为选择地址池的依据。为了解决这个问题，需要使用 **gateway-list** 命令指定某个类型用户所在的网段，并将该地址添加到转发给 DHCP 服务器的报文字段中，为 DHCP 服务器选择地址池提供依据。

2. 配置限制和指导

配置本功能需要注意：

- 当 PPPoE 用户下线时，DHCP 中继需要查询中继用户地址表项，若存在对应表项，则会向 DHCP 服务器发送 Release 报文，通知 DHCP 服务器释放该地址租约。这就需要在 DHCP 中

继上使用 **dhcp relay client-information record** 命令开启 DHCP 中继用户地址表项记录功能。

- 和 PPPoE 配合使用时，如果设备的地址池中配置了 **remote-server** 命令，则可以认定该设备一定是 DHCP 中继设备，所以不需要在接口视图下执行 **dhcp select relay** 命令。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 DHCP 中继地址池，并进入中继地址池视图。

dhcp server ip-pool *pool-name*

(3) 指定匹配该地址池的 DHCPv4 客户端所在的网段地址。

gateway-list *ip-address*&<1-64> [**export-route**]

缺省情况下，未指定匹配该地址池的 DHCP 客户端所在的网段地址。

(4) 指定中继地址池对应的 DHCP 服务器地址。

remote-server *ip-address*&<1-8>

缺省情况下，未指定中继地址池对应的 DHCP 服务器的地址。

通过执行 **remote-server** 命令一次最多可以指定 8 个 DHCP 服务器的地址信息。

3.6 指定DHCP客户端对应的DHCP中继地址池

1. 功能简介

在 DHCP 中继上可能存在多个 DHCP 中继地址池，可以在接口下直接指定 DHCP 客户端对应的地址池。如果希望更进一步根据 DHCP 客户端报文的 Option 信息来选择对应的 DHCP 中继地址池，则可以指定 Option 参数。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 DHCP 中继地址池视图。

dhcp server ip-pool *pool-name*

(3) 指定中继地址池对应的 DHCP 服务器地址。

remote-server *ip-address*&<1-8>

缺省情况下，未指定中继地址池的 DHCP 服务器的地址。

(4) 指定匹配该地址池的 DHCP 客户端所在的网段的地址。

gateway-list *ip-address*&<1-64>

缺省情况下，未指定匹配该地址池的 DHCP 客户端所在的网段地址。

3.7 配置DHCP中继的安全功能

3.7.1 配置DHCP中继用户地址表项记录功能

1. 功能简介

为了防止非法主机静态配置一个 IP 地址并访问外部网络，设备支持 DHCP 中继用户地址表项记录功能。

开启该功能后，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 地址与硬件地址的绑定关系，生成 DHCP 中继的用户地址表项。

本功能与其他 IP 地址安全功能（如 ARP 地址检查、授权 ARP 和 IP Source Guard）配合，可以实现只允许匹配用户地址表项中绑定关系的报文通过 DHCP 中继。从而，保证非法主机不能通过 DHCP 中继与外部网络通信。

2. 配置限制和指导

同异步串口作为DHCP客户端申请IP地址时，DHCP中继不会记录该客户端对应的用户地址表项。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启 DHCP 中继的用户地址表项记录功能。

dhcp relay client-information record

缺省情况下，DHCP 中继用户地址表项记录功能处于关闭状态。

3.7.2 配置DHCP中继动态用户地址表项定时刷新功能

1. 功能简介

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 中继每隔指定时间采用客户端获取到的 IP 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 中继会删除动态用户地址表中对应的表项。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。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启 DHCP 中继动态用户地址表项定时刷新功能。

dhcp relay client-information refresh enable

缺省情况下，DHCP 中继动态用户地址表项定时刷新功能处于开启状态。

(3) （可选）配置 DHCP 中继动态用户地址表项的定时刷新周期。

dhcp relay client-information refresh [**auto** | **interval** *interval*]

缺省情况下，定时刷新周期为 **auto**，即根据表项的数目自动计算刷新时间间隔。

3.7.3 配置防止DHCP饿死攻击

1. 功能简介

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，则限制三层接口上可以学习到的 ARP 表项数，或限制二层端口上可以学习到的 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，在一定程度上缓解 DHCP 饿死攻击。

如果封装 DHCP 请求报文的数据帧的源 MAC 地址都相同，则通过上述方法无法防止 DHCP 饿死攻击。在这种情况下，需要开启 DHCP 中继的 MAC 地址检查功能。开启该功能后，DHCP 中继检查接收到的 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，将其转发给 DHCP 服务器；如果不一致，则丢弃该报文。

因为 DHCP 中继转发 DHCP 报文时会修改报文的源 MAC 地址，所以只能在靠近 DHCP 客户端的第一跳 DHCP 中继设备上开启 MAC 地址检查功能。

设备支持配置 DHCP 中继的 MAC 地址检查表项老化时间，当老化时间到达以后，该表项信息会被老化掉，DHCP 中继收到该 MAC 地址对应的 DHCP 请求报文后重新进行合法性检查。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 DHCP 中继的 MAC 地址检查表项的老化时间。

dhcp relay check mac-address aging-time *time*

缺省情况下，DHCP 中继的 MAC 地址检查表项的老化时间为 30 秒。

如果未通过 **dhcp relay check mac-address** 命令开启 DHCP 中继的 MAC 地址检查功能，则本命令的配置不会生效。

(3) 进入接口视图。

interface *interface-type interface-number*

(4) 开启 DHCP 中继的 MAC 地址检查功能。

dhcp relay check mac-address

缺省情况下，DHCP 中继的 MAC 地址检查功能处于关闭状态。

3.7.4 配置DHCP中继支持代理功能

1. 功能简介

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 中继当做自己的服务器，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。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置 DHCP 中继支持代理功能。

dhcp select relay proxy

缺省情况下，开启 DHCP 服务后，接口工作在 DHCP 服务器模式。

3.7.5 配置DHCP中继的用户下线探测功能

1. 功能简介

DHCP 中继的用户下线探测功能以 ARP 表项老化功能为基础，当 ARP 表项老化时认为该表项对应的用户已经下线。

如果在接口上配置了 DHCP 中继的用户下线检测功能，则当 ARP 表项老化时，DHCP 中继认为该表项对应的用户已经下线，删除对应的用户地址表项，并通过发送 Release 报文通知 DHCP 服务器删除下线用户的 IP 地址租约。

2. 配置限制和指导

手工删除 ARP 表项，不会触发 DHCP 中继删除对应的用户地址表项。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启 DHCP 中继的用户地址表项记录功能。

dhcp relay client-information record

缺省情况下，DHCP 中继用户地址表项记录功能处于关闭状态。

用户需要开启 DHCP 中继用户地址表项记录功能，否则用户下线探测功能无法完全生效。

(3) 进入接口视图。

interface *interface-type interface-number*

(4) 配置接口工作在 DHCP 中继模式。

dhcp select relay

缺省情况下，开启 DHCP 服务后，接口工作在 DHCP 服务器模式。

(5) 开启 DHCP 中继的用户下线探测功能。

dhcp client-detect

缺省情况下，DHCP 中继的用户下线探测功能处于关闭状态。

3.8 配置通过DHCP中继释放客户端的IP地址

1. 功能简介

在某些情况下，可能需要通过 DHCP 中继手工释放客户端申请到的 IP 地址。如果 DHCP 中继上存在客户端 IP 地址对应的动态用户地址表项，则配置通过 DHCP 中继释放该客户端 IP 地址后，DHCP 中继会主动向 DHCP 服务器发送 DHCP-RELEASE 报文。DHCP 服务器收到该报文后，将会释放指定 IP 地址的租约。DHCP 中继也会删除该动态用户地址表项。

释放的客户端 IP 地址必须是动态用户地址表项中存在的 IP 地址，否则 DHCP 中继无法释放该 IP 地址。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 向 DHCP 服务器请求释放客户端申请到的 IP 地址。

dhcp relay release ip *ip-address* [**vpn-instance** *vpn-instance-name*]

3.9 配置DHCP中继支持Option 82功能

1. 配置限制和指导

为使Option 82 功能正常使用，需要在DHCP服务器和DHCP中继上都进行相应配置。DHCP服务器的相关配置请参见“2.10 配置Option 82 的处理方式”。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 开启 DHCP 中继支持 Option 82 功能。

dhcp relay information enable

缺省情况下，DHCP 中继支持 Option 82 功能处于关闭状态。

(4) （可选）配置 DHCP 中继对包含 Option 82 的请求报文的处理策略。

dhcp relay information strategy { **drop** | **keep** | **replace** }

缺省情况下，处理策略为 **replace**。

DHCP 中继对包含 Option 82 请求报文的处理策略为 **replace** 时，需要配置 Option 82 的填充模式和填充格式；处理策略为 **keep** 或 **drop** 时，不需要配置 Option 82 的填充模式和填充格式。

(5) （可选）配置 Circuit ID 子选项的填充模式和填充格式。

dhcp relay information circuit-id { **bas** [**sub-interface-vlan**] | **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] [**interface**] } [**sub-interface-vlan**] [**format** { **ascii** | **hex** }] }

缺省情况下，Circuit ID 子选项的填充模式为 Normal，填充格式为 hex。

如果以设备的系统名称（**sysname**）作为节点标识填充 DHCP 报文的 Option 82，则系统名称中不能包含空格；否则，DHCP 中继添加或替换 Option 82 失败。

(6) （可选）配置 Remote ID 子项的填充模式和填充格式。

dhcp relay information remote-id { { **ap-mac** | **ap-mac-ssid** | **normal** } [**format** { **ascii** | **hex** }] | **ap-name** | **ap-name-ssid** | **string** *remote-id* | **sysname** }

缺省情况下，Remote ID 子选项的填充模式为 Normal；填充格式为 hex。

3.10 配置DHCP中继发送DHCP报文的DSCP优先级

1. 功能简介

DSCP 优先级用来体现报文自身的优先等级，决定报文传输的优先程度。通过本配置可以指定 DHCP 中继发送的 DHCP 报文的 DSCP 优先级。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 DHCP 中继发送 DHCP 报文的 DSCP 优先级。

dhcp dscp *dscp-value*

缺省情况下，DHCP 中继发送的 DHCP 报文的 DSCP 优先级为 56。

3.11 配置DHCP中继在DHCP报文中填充的中继地址

3.11.1 手工指定在DHCP报文中填充的中继地址

1. 功能简介

当未开启该功能时，DHCP 中继收到 DHCP 客户端的请求报文后，只能将接口的主 IP 地址添加到报文中，然后转发给 DHCP 服务器。对于某些特定需求，DHCP 中继需要添加指定的地址到报文中，这时就需要配置此功能。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 手工指定在 DHCP 报文中填充的中继地址。

dhcp relay gateway *ip-address*

缺省情况下，DHCP 中继填充的中继地址是接口下的主 IP 地址。

3.11.2 通过smart-relay功能指定DHCP报文中填充的中继地址

1. 功能简介

当 DHCP 中继收到 DHCP 客户端发来的请求报文时，会使用中继接口的主 IP 地址填充请求报文的 giaddr 字段，然后转发给 DHCP 服务器，DHCP 服务器根据 giaddr 字段中的地址选择合适的地址池为客户端分配 IP 地址。当 DHCP 服务器中该网段地址分配完毕后，不管 DHCP 服务器上是否存在其他网段的地址，都不会再为该 DHCP 中继下的其他 DHCP 客户端分配 IP 地址。

DHCP 中继通过 smart-relay 解决上述问题，开启该功能后，DHCP 中继可以使用除中继接口主地址外的其他 IP 地址来填充 giaddr 字段，从而使 DHCP 客户端可以获取到其他网段的 IP 地址。

DHCP 中继转发 3 次 DHCP-DISCOVER 报文后，若还未收到 DHCP 服务器的应答报文，DHCP 中继将使用下一个可用 IP 地址来填充 giaddr 字段。DHCP 中继使用所有配置的 IP 地址填充 giaddr 字段之后，将重新选择第一个配置的 IP 地址进入下一个循环。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启 DHCP 中继支持 smart-relay 功能。

dhcp smart-relay enable

缺省情况下，DHCP 中继支持 smart-relay 功能处于关闭状态。

3.12 指定DHCP中继向DHCP服务器转发报文的源地址

1. 功能简介

在某些组网中，多个 DHCP 中继接口 IP 地址相同或者中继接口 IP 到服务器没有可达路由，用户需要配置本命令指定一个 IP 地址或选择中继设备上的另一个接口（一般选择的是 Loopback 口）的 IP 地址填充到发送到 DHCP 服务器的 DHCP 请求报文中的源地址字段和 Giaddr 中。

当多个 DHCP 中继接口 IP 地址相同时，导致 DHCP 中继转发 DHCP 应答报文时候无法根据目的 IP 地址找到唯一的出接口。配置本功能时需要先开启 DHCP 中继支持 Option 82 功能，DHCP 中继收到 DHCP 请求报文时在 Option 82 中的子选项 sub-option5 填充正确的子网网段，服务器可以根据中继填充的 sub-option5 来分配地址，之后 DHCP 中继处理 DHCP 应答报文时通过 MAC 地址表中的接口信息转发 DHCP 报文。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 指定 DHCP 中继向 DHCP 服务器转发报文的源地址。

dhcp relay source-address { *ip-address* | **gateway** | **relay-interface** }

缺省情况下，DHCP 中继向 DHCP 服务器转发报文的源地址为向 DHCP 服务器转发报文出接口的地址。

3.13 DHCP中继显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 DHCP 中继的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令清除 DHCP 中继的统计信息。

表3-2 DHCP 中继显示和维护

操作	命令
显示DHCP中继的MAC地址检查表项	**display dhcp relay check mac-address**
显示DHCP中继的用户地址表项信息	**display dhcp relay client-information** [**interface** *interface-type interface-number* | **ip** *ip-address* [**vpn-instance** *vpn-instance-name*]]
显示DHCP中继上的Option 82配置信息	**display dhcp relay information** [**interface** *interface-type interface-number*]
显示接口上指定的DHCP服务器地址信息	**display dhcp relay server-address** [**interface** *interface-type interface-number*]
显示DHCP中继的相关报文统计信息	**display dhcp relay statistics** [**interface** *interface-type interface-number*]
清除DHCP中继的用户地址表项信息	**reset dhcp relay client-information** [**interface** *interface-type interface-number* | **ip** *ip-address* [**vpn-instance** *vpn-instance-name*]]
清除DHCP中继的相关报文统计信息	**reset dhcp relay statistics** [**interface** *interface-type interface-number*]

3.14 DHCP中继典型配置举例

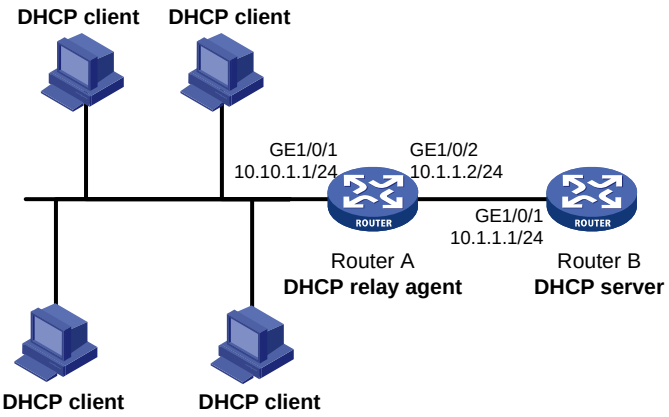
3.14.1 DHCP中继基本组网配置举例

1. 组网需求

- DHCP 客户端所在网段为 10.10.1.0/24，DHCP 服务器的 IP 地址为 10.1.1.1/24；
- 由于 DHCP 客户端和 DHCP 服务器不在同一网段，因此，需要在客户端所在网段设置 DHCP 中继设备，以便客户端可以从 DHCP 服务器申请到 10.10.1.0/24 网段的 IP 地址及相关配置信息；
- Router A 作为 DHCP 中继通过 GigabitEthernet1/0/1 接口连接到 DHCP 客户端所在的网络，GigabitEthernet1/0/1 接口的 IP 地址为 10.10.1.1/24，GigabitEthernet1/0/2 接口的 IP 地址为 10.1.1.2/24。

2. 组网图

图3-3 DHCP 中继组网示意图



3. 配置步骤

配置各接口的 IP 地址（略）。

开启 DHCP 服务。

```
<RouterA> system-view
[RouterA] dhcp enable
```

配置 GigabitEthernet1/0/1 接口工作在 DHCP 中继模式。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] dhcp select relay
```

指定 DHCP 服务器的地址。

```
[RouterA-GigabitEthernet1/0/1] dhcp relay server-address 10.1.1.1
```

配置完成后，DHCP 客户端可以通过 DHCP 中继从 DHCP 服务器获取 IP 地址及相关配置信息。通过 **display dhcp relay statistics** 命令可以显示 DHCP 中继转发的 DHCP 报文统计信息；如果在 DHCP 中继上通过 **dhcp relay client-information record** 命令开启了 DHCP 中继的用户地址表项记录功能，则可以通过 **display dhcp relay client-information** 命令可以显示通过 DHCP 中继获取 IP 地址的客户端信息。

说明

- 由于 DHCP 中继连接 DHCP 客户端的接口 IP 地址与 DHCP 服务器的 IP 地址不在同一网段，因此需要在 DHCP 服务器上通过静态路由或动态路由协议保证两者之间路由可达。
- 为了使DHCP客户端能从DHCP服务器获得IP地址，还需要在DHCP服务器上进行一些配置。DHCP服务器的配置方法，请参见“2.18 DHCP服务器典型配置举例”。

3.14.2 DHCP中继支持Option 82 配置举例

1. 组网需求

- 在 DHCP 中继 Router A 上开启 Option 82 功能；
- 对包含 Option 82 的请求报文的处理策略为 **replace**；

- Circuit ID 填充内容为 company001，Remote ID 填充内容为 device001；
- Router A 将添加 Option 82 的 DHCP 请求报文转发给 DHCP 服务器 Router B，使得 DHCP 客户端可以获取到 IP 地址。

2. 组网图

如 图 3-3 所示。

3. 配置步骤

配置各接口的 IP 地址（略）。

开启 DHCP 服务。

```
<RouterA> system-view
[RouterA] dhcp enable
```

配置 GigabitEthernet1/0/1 接口工作在 DHCP 中继模式。

```
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] dhcp select relay
```

指定 DHCP 服务器的地址。

```
[RouterA-GigabitEthernet1/0/1] dhcp relay server-address 10.1.1.1
```

配置 Option 82 的处理策略和填充内容。

```
[RouterA-GigabitEthernet1/0/1] dhcp relay information enable
[RouterA-GigabitEthernet1/0/1] dhcp relay information strategy replace
[RouterA-GigabitEthernet1/0/1] dhcp relay information circuit-id string company001
[RouterA-GigabitEthernet1/0/1] dhcp relay information remote-id string device001
```

说明

为使 Option 82 功能正常使用，DHCP 服务器也需要进行相应配置。

3.15 DHCP中继常见故障处理

3.15.1 DHCP客户端无法通过DHCP中继获取配置信息

1. 故障现象

DHCP 客户端无法通过 DHCP 中继获得配置信息。

2. 故障分析

DHCP 中继或 DHCP 服务器的配置可能有问题。可以打开调试开关显示调试信息，并通过执行 **display** 命令显示接口状态信息的方法来分析定位。

3. 故障处理

- 检查 DHCP 服务器和 DHCP 中继是否开启了 DHCP 服务。
- 检查 DHCP 服务器是否配置有 DHCP 客户端所在网段的地址池。
- 检查具有 DHCP 中继功能的网络设备和 DHCP 服务器是否配置有相互可达的路由。
- 检查具有 DHCP 中继功能的网络设备是否在连接 DHCP 客户端所在网段的接口上指定了正确的 DHCP 服务器地址。

4 DHCP客户端

4.1 DHCP客户端简介

为了方便用户配置和集中管理，可以指定设备的接口作为 DHCP 客户端，使用 DHCP 协议从 DHCP 服务器动态获得 IP 地址等参数。

4.2 DHCP客户端配置限制和指导

DHCP 客户端中对于接口的相关配置，目前只能在三层以太网接口（包括子接口）、VLAN 接口和三层聚合接口上进行。

4.3 DHCP客户端配置任务简介

DHCP 客户端配置任务如下：

(1) 配置接口通过DHCP协议获取IP地址

(2) 配置接口使用的DHCP客户端ID

DHCP 客户端使用客户端 ID 从 DHCP 服务器获取特定地址时配置。

(3) （可选）开启地址冲突检查功能

(4) （可选）配置DHCP客户端发送DHCP报文的DSCP优先级

4.4 配置接口通过DHCP协议获取IP地址

1. 配置限制和指导

配置接口通过 DHCP 协议获取 IP 地址，需要注意：

- 接口作为 DHCP 客户端多次申请 IP 地址失败后，将停止申请，并为接口配置缺省 IP 地址。
- 接口可以采用多种方式获得 IP 地址，新的配置方式会覆盖原有的配置方式。
- 当接口被配置为通过 DHCP 动态获取 IP 地址后，不能再给该接口配置从 IP 地址。
- 如果 DHCP 服务器为接口分配的 IP 地址与设备上其他接口的 IP 地址在同一网段，则该接口不会使用该 IP 地址，且会再向 DHCP 服务器重新申请 IP 地址。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置接口通过 DHCP 协议获取 IP 地址。

ip address dhcp-alloc

缺省情况下，接口不通过 DHCP 协议获取 IP 地址。

4.5 配置接口使用的DHCP客户端ID

1. 功能简介

DHCP 客户端 ID 用来填充 DHCP 报文 Option 61，作为识别 DHCP 客户端的唯一标识。DHCP 服务器可以根据客户端 ID 为特定的客户端分配特定的 IP 地址。DHCP 客户端 ID 包括类型和取值两部分，用户可以通过 ASCII 字符串、十六进制数和指定接口的 MAC 地址来指定 DHCP 客户端 ID：

- 当客户端 ID 的取值为 ASCII 字符串时，对应的类型值为 00；
- 当客户端 ID 的取值为十六进制数时，对应的类型值为该十六进制数的前两个字符；
- 当客户端 ID 使用指定接口的 MAC 地址时，对应的类型值为 01。

DHCP 客户端 ID 类型值可通过命令 **display dhcp server ip-in-use** 或 **display dhcp client** 进行查看。

2. 配置限制和指导

用户在指定客户端 ID 时，需要确保不同客户端的客户端 ID 不能相同。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置接口使用的 DHCP 客户端 ID。

dhcp client identifier { **ascii** *ascii-string* | **hex** *hex-string* | **mac** *interface-type interface-number* }

缺省情况下，根据本接口 MAC 地址生成 DHCP 客户端 ID，如果本接口没有 MAC 地址，则获取设备第一个以太接口的 MAC 地址生成 DHCP 客户端 ID。

4.6 开启地址冲突检查功能

1. 功能简介

通常情况下，DHCP 客户端上开启地址冲突检查功能，通过发送和接收 ARP 报文，对 DHCP 服务器分配的 IP 地址进行地址冲突检测。

如果攻击者仿冒地址拥有者进行 ARP 应答，就可以欺骗 DHCP 客户端，导致 DHCP 客户端无法正常使用分配到的 IP 地址。在网络中存在上述攻击者时，建议在客户端上关闭地址冲突检查功能。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启地址冲突检查功能。

dhcp client dad enable

缺省情况下，地址冲突检查功能处于开启状态。

4.7 配置DHCP客户端发送DHCP报文的DSCP优先级

1. 功能简介

DSCP优先级用来体现报文自身的优先等级，决定报文传输的优先程度。通过本配置可以指定DHCP客户端发送的DHCP报文的DSCP优先级。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置DHCP客户端发送DHCP报文的DSCP优先级。

dhcp client dscp *dscp-value*

缺省情况下，DHCP客户端发送的DHCP报文的DSCP优先级为56。

4.8 DHCP客户端显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后DHCP客户端的信息，通过查看显示信息验证配置的效果。

表4-1 DHCP客户端显示和维护

操作	命令
显示DHCP客户端的相关信息	**display dhcp client** [**verbose**] [**interface** *interface-type interface-number*]

4.9 DHCP客户端典型配置举例

4.9.1 DHCP客户端基本组网典型配置举例

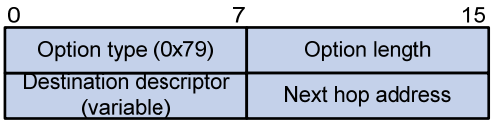
1. 组网需求

Router B的以太网接口GigabitEthernet1/0/1接入局域网，通过DHCP协议从DHCP服务器获取IP地址、DNS服务器地址和静态路由信息：

- DHCP客户端的IP地址所在网段为10.1.1.0/24；
- DNS服务器地址为20.1.1.1；
- 静态路由信息为到达20.1.1.0/24网段的下一跳地址是10.1.1.2。

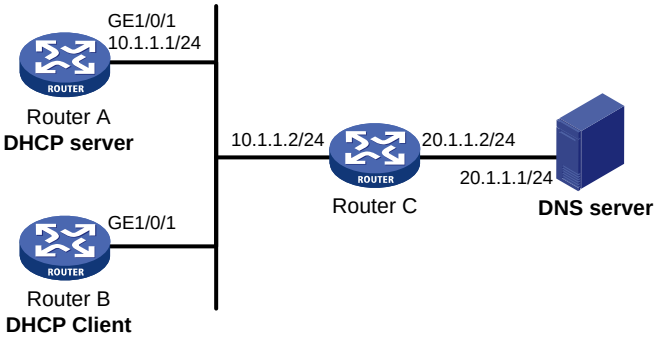
DHCP服务器需要通过自定义选项的方式配置Option 121的内容，以便为客户端分配静态路由信息。Option 121的格式如 图 4-1 所示。其中，目的描述符由子网掩码长度和目的网络地址两部分组成。在本例中，目的描述符字段取值为18 14 01 01（十六进制数值，表示子网掩码长度为24，目的网络地址为20.1.1.0）；下一跳地址字段取值为0A 01 01 02（十六进制数值，表示下一跳地址为10.1.1.2）。

图4-1 Option 121 选项格式



2. 组网图

图4-2 DHCP 客户端配置举例组网图



3. 配置步骤

(1) 配置 DHCP 服务器 Router A

配置接口的 IP 地址。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ip address 10.1.1.1 24
[RouterA-GigabitEthernet1/0/1] quit
```

配置不参与自动分配的 IP 地址。

```
[RouterA] dhcp server forbidden-ip 10.1.1.2
```

配置 DHCP 地址池 0，采用动态绑定方式分配 IP 地址。可分配的网段为 10.1.1.0/24，租约有效期限为10天，DNS服务器地址为20.1.1.1，到达20.1.1.0/24网段的下一跳地址是10.1.1.2。

```
[RouterA] dhcp server ip-pool 0
[RouterA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
[RouterA-dhcp-pool-0] expired day 10
[RouterA-dhcp-pool-0] dns-list 20.1.1.1
[RouterA-dhcp-pool-0] option 121 hex 181401010A010102
[RouterA-dhcp-pool-0] quit
```

开启 DHCP 服务。

```
[RouterA] dhcp enable
```

(2) 配置 DHCP 客户端 Router B

配置接口 GigabitEthernet1/0/1 通过 DHCP 动态获取地址。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] ip address dhcp-alloc
```

```
    [RouterB-GigabitEthernet1/0/1] quit
```

4. 验证配置

通过 **display dhcp client** 命令可以查看 Router B 申请到的 IP 地址和网络配置参数。

```
[RouterB] display dhcp client verbose
GigabitEthernet1/0/1 DHCP client information:
 Current state: BOUND
 Allocated IP: 10.1.1.3 255.255.255.0
 Allocated lease: 864000 seconds, T1: 331858 seconds, T2: 756000 seconds
 Lease from May 21 19:00:29 2012   to   May 31 19:00:29 2012
 DHCP server: 10.1.1.1
 Transaction ID: 0xcde72232
 Classless static routes:
   Destination: 20.1.1.0, Mask: 255.255.255.0, NextHop: 10.1.1.2
 DNS servers: 20.1.1.1
 Client ID type: acsii(type value=00)
 Client ID value: 000c.29d3.8659-GE1/0/1
 Client ID (with type) hex: 0030-3030-632e-3239-
                            6433-2e38-3635-392d-
                            4574-6830-2f30-2f32
 T1 will timeout in 3 days 19 hours 48 minutes 43 seconds
```

通过 **display ip routing-table** 命令可以查看 Router B 的路由表中添加了到达 20.1.1.0/24 网络的静态路由。

```
[RouterB] display ip routing-table

Destinations : 11        Routes : 11

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.3        GE1/0/1
10.1.1.3/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Static 70   0            10.1.1.2        GE1/0/1
10.1.1.255/32       Direct 0    0            10.1.1.3        GE1/0/1
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

5 DHCP Snooping

5.1 DHCP Snooping简介

DHCP Snooping 是 DHCP 的一种安全特性。

DHCP Snooping 设备只有位于 DHCP 客户端与 DHCP 服务器之间，或 DHCP 客户端与 DHCP 中继之间时，DHCP Snooping 功能配置后才能正常工作；设备位于 DHCP 服务器与 DHCP 中继之间时，DHCP Snooping 功能配置后不能正常工作。

5.1.1 DHCP Snooping作用

1. 保证客户端从合法的服务器获取IP地址

网络中如果存在私自架设的非法 DHCP 服务器，则可能导致 DHCP 客户端获取到错误的 IP 地址和网络配置参数，从而无法正常通信。为了使 DHCP 客户端能通过合法的 DHCP 服务器获取 IP 地址，DHCP Snooping 安全机制允许将端口设置为信任端口和不信任端口：

- 信任端口正常转发接收到的 DHCP 报文。
- 不信任端口接收到 DHCP 服务器响应的 DHCP-ACK 和 DHCP-OFFER 报文后，丢弃该报文。

在 DHCP Snooping 设备上指向 DHCP 服务器方向的端口需要设置为信任端口，其他端口设置为不信任端口，从而保证 DHCP 客户端只能从合法的 DHCP 服务器获取 IP 地址，私自架设的伪 DHCP 服务器无法为 DHCP 客户端分配 IP 地址。

2. 记录DHCP客户端IP地址与MAC地址的对应关系

DHCP Snooping 通过监听 DHCP-REQUEST 报文和信任端口收到的 DHCP-ACK 报文，记录 DHCP Snooping 表项，其中包括客户端的 MAC 地址、DHCP 服务器为 DHCP 客户端分配的 IP 地址、与 DHCP 客户端连接的端口及 VLAN 等信息。利用这些信息可以实现：

- ARP 快速应答：根据 DHCP Snooping 表项来判断是否进行 ARP 快速应答，从而减少 ARP 广播报文。ARP 快速应答的详细介绍请参见“三层技术-IP 业务配置指导”中的“ARP 快速应答”。
- ARP Detection：根据 DHCP Snooping 表项来判断发送 ARP 报文的用户是否合法，从而防止非法用户的 ARP 攻击。ARP Detection 的详细介绍请参见“安全配置指导”中的“ARP 攻击防御”。
- MFF（MAC-Forced Forwarding）：在 MFF 的自动方式中，设备截获到用户发送的 ARP 请求后，根据 DHCP Snooping 表项查找该用户对应的网关地址，并回复网关的 MAC 地址，强制用户将所有流量发送到网关，使得网关可以监控用户之间的数据流量，从而防止用户之间的恶意攻击，更好的保障网络安全。MFF 的详细介绍请参见“安全配置指导”中的“MFF”。
- IP Source Guard：通过动态获取 DHCP Snooping 表项对端口转发的报文进行过滤，防止非法报文通过该端口。IP Source Guard 的详细介绍请参见“安全配置指导”中的“IP Source Guard”。

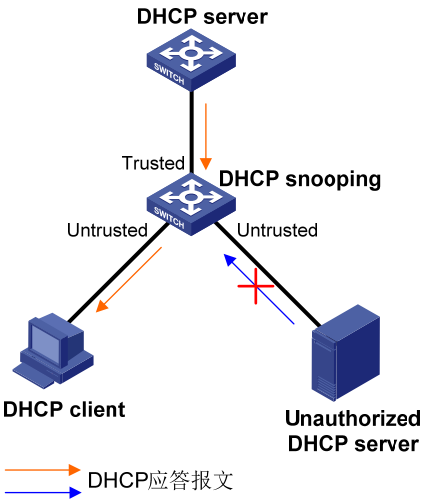
- VLAN 映射：发送给用户的报文通过查找指定 VLAN 对应的 DHCP Snooping 表项中的 DHCP 客户端 IP 地址、MAC 地址和原始 VLAN 的信息，将报文的指定 VLAN 修改为原始 VLAN。VLAN 映射的详细介绍请参见“二层技术-以太网交换配置指导”中的“VLAN 映射”。

5.1.2 信任端口的典型应用环境

1. DHCP Snooping直联DHCP服务器和DHCP客户端网络

如 图 5-1 所示，在DHCP Snooping设备上指向DHCP服务器方向的端口需要设置为信任端口，以便DHCP Snooping设备正常转发DHCP服务器的应答报文，保证DHCP客户端能够从合法的DHCP服务器获取IP地址。

图5-1 信任端口和非信任端口



2. DHCP Snooping级联网络

在多个 DHCP Snooping 设备级联的网络中，为了节省系统资源，不需要每台 DHCP Snooping 设备都记录所有 DHCP 客户端的 IP 地址和 MAC 地址的绑定信息，只需在与客户端直接相连不信任端口上记录绑定信息。间接与 DHCP 客户端相连的不信任端口不需要记录 IP 地址和 MAC 地址绑定信息。

图5-2 DHCP Snooping 级联组网图

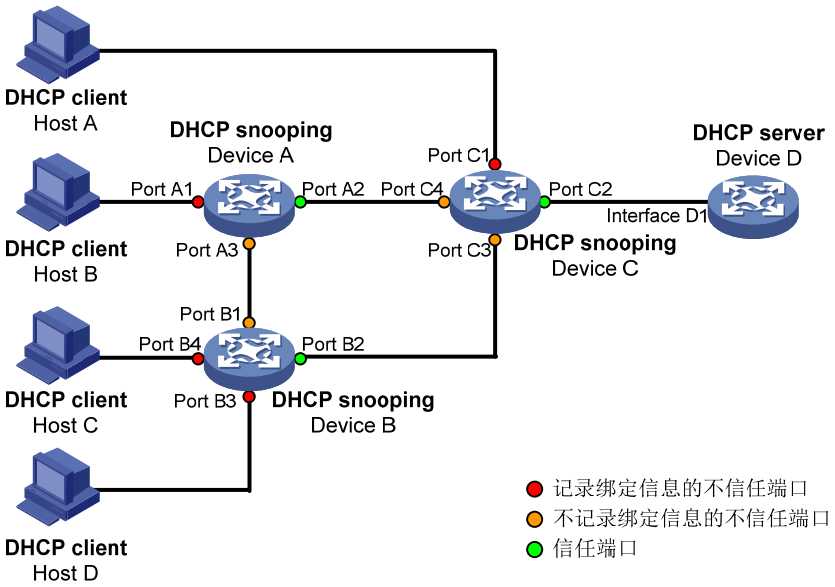


图 5-2 中设备各端口的角色如 表 5-1 所示。

表5-1 端口的角色

设备	记录绑定信息的不信任端口	不记录绑定信息的不信任端口	信任端口
Device A	Port A1	Port A3	Port A2
Device B	Port B3和Port B4	Port B1	Port B2
Device C	Port C1	Port C3和Port C4	Port C2

5.1.3 DHCP Snooping支持Option 82 功能

Option 82 记录了DHCP客户端的位置信息。管理员可以利用该选项定位DHCP客户端，实现对客户端的安全和计费等控制。Option 82 的详细介绍请参见“1.6.2 中继代理信息选项（Option 82）”。

如果DHCP Snooping支持Option 82 功能，则当设备接收到DHCP请求报文后，将根据报文中是否包含Option 82 以及用户配置的处理策略及填充模式等对报文进行相应的处理，并将处理后的报文转发给DHCP服务器。具体的处理方式见 表 5-2。DHCP Snooping对Option 82 的处理策略、填充模式与DHCP中继相同。

当设备接收到 DHCP 服务器的响应报文时，如果报文中含有 Option 82，则删除 Option 82，并转发给 DHCP 客户端；如果报文中不含有 Option 82，则直接转发。

表5-2 DHCP Snooping 支持 Option 82 的处理方式

收到 DHCP 请求报文	处理策略	DHCP Snooping 对报文的处理
收到的报文中带有Option 82	Drop	丢弃报文
	Keep	保持报文中的Option 82不变并进行转发
	Replace	根据DHCP Snooping上配置的填充模式、内容、格式等填充Option 82，替换报文中原有的Option 82并进行转发
收到的报文中不带有Option 82	-	根据DHCP Snooping上配置的填充模式、内容、格式等填充Option 82，添加到报文中并进行转发

本特性的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
MSR810、MSR810-W、MSR810-W-DB、MSR810-LM、MSR810-W-LM、MSR810-10-PoE、MSR810-LM-HK、MSR810-W-LM-HK、MSR810-LM-CNDE-SJK	支持
MSR810-LMS、MSR810-LUS	支持
MSR810-LMS-EA、MSR810-LME	支持
MSR2600-6-X1、MSR2600-10-X1	支持
MSR 2630	支持
MSR3600-28、MSR3600-51	支持
MSR3600-28-SI、MSR3600-51-SI	支持
MSR3600-28-X1、MSR3600-28-X1-DP、MSR3600-51-X1、MSR3600-51-X1-DP	支持
MSR3610-I-DP、MSR3610-IE-DP、MSR3610-IE-ES	不支持
MSR3610-X1、MSR3610-X1-DP、MSR3610-X1-DC、MSR3610-X1-DP-DC	支持
MSR 3610、MSR 3620、MSR 3620-DP、MSR 3640、MSR 3660	支持
MSR3610-G、MSR3620-G	支持

型号	说明
MSR810-W-WiNet、MSR810-LM-WiNet	支持
MSR830-4LM-WiNet	支持
MSR830-5BEI-WiNet、MSR830-6EI-WiNet、MSR830-10BEI-WiNet	支持
MSR830-6BHI-WiNet、MSR830-10BHI-WiNet	支持
MSR2600-6-WiNet、MSR2600-10-X1-WiNet	支持
MSR2630-WiNet	支持
MSR3600-28-WiNet	支持

型号	说明
MSR3610-X1-WiNet	支持
MSR3610-WiNet、MSR3620-10-WiNet、MSR3620-DP-WiNet、MSR3620-WiNet、MSR3660-WiNet	支持

型号	说明
MSR2630-XS	支持
MSR3600-28-XS	支持
MSR3610-XS	支持
MSR3620-XS	支持
MSR3610-I-XS	不支持
MSR3610-IE-XS	不支持

5.2 DHCP Snooping配置限制和指导

配置 DHCP Snooping 基本功能时，需要注意：

- 如果二层以太网接口加入聚合组，则在该接口上进行的 DHCP Snooping 相关配置不会生效；该接口退出聚合组后，之前的配置才会生效。
- 为了使 DHCP 客户端能从合法的 DHCP 服务器获取 IP 地址，必须将与合法 DHCP 服务器相连的端口设置为信任端口，设置的信任端口和与 DHCP 客户端相连的端口必须在同一个 VLAN 内。
- 目前，可以设置为 DHCP Snooping 信任端口的接口类型包括：二层以太网接口、二层聚合接口、三层以太网接口、三层聚合接口。关于聚合接口的详细介绍，请参见“二层技术-以太网交换配置指导”中的“以太网链路聚合”。
- VXLAN 组网中，除了信任端口配置外，以太网服务实例采用该实例所在二层以太网接口上的 DHCP Snooping 配置。以太网服务实例的详细介绍，请参见“VXLAN 配置指导”中的“VXLAN”。

5.3 DHCP Snooping配置任务简介

DHCP Snooping 配置任务如下：

(1) 配置DHCP Snooping基本功能

(2) （可选）配置DHCP Snooping支持Option 82 功能

(3) （可选）配置DHCP Snooping表项固化功能

(4) （可选）配置接口动态学习DHCP Snooping表项的最大数目

(5) （可选）配置DHCP Snooping安全功能

(6) （可选）开启DHCP Snooping日志信息功能

5.4 配置DHCP Snooping基本功能

1. 功能简介

在一台 DHCP Snooping 设备上，如果全局开启了 DHCP Snooping 功能，则设备上所有 VLAN 内的 DHCP Snooping 功能也同时开启。

对于某些组网来说，管理员只需要在设备在某些特定 VLAN 内开启 DHCP Snooping 功能，而不需要在整个设备上开启 DHCP Snooping 功能。为了满足此需求，设备支持在指定 VLAN 内开启 DHCP Snooping 功能，并在 VLAN 内配置 DHCP Snooping 信任端口和开启端口的 DHCP Snooping 表项记录功能。

2. 配置限制和指导

在一台设备上，全局 DHCP Snooping 功能和 VLAN 内的 DHCP Snooping 功能关系如下：

- 如果全局开启了 DHCP Snooping 基本功能（包括开启 DHCP Snooping 功能、配置信任端口和配置 DHCP Snooping 表项记录功能），只能使用对应的全局命令关闭功能，使用 VLAN 内的命令关闭功能不生效；
- 如果 VLAN 内开启了 DHCP Snooping 基本功能（包括开启 DHCP Snooping 功能、配置信任端口和配置 DHCP Snooping 表项记录功能），只能使用对应的 VLAN 内命令关闭功能，使用全局命令关闭功能不生效。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启 DHCP Snooping 功能。

dhcp snooping enable

缺省情况下，DHCP Snooping 功能处于关闭状态。

(3) 进入接口视图。

interface *interface-type interface-number*

此接口为连接 DHCP 服务器的接口。

(4) 配置端口为信任端口。

dhcp snooping trust

缺省情况下，在开启 DHCP Snooping 功能后，设备的所有端口均为不信任端口。

(5) （可选）开启端口的 DHCP Snooping 表项记录功能。

a. 退回系统视图。

quit

b. 进入接口视图。

interface *interface-type interface-number*

此接口为连接 DHCP 客户端的接口。

c. 开启 DHCP Snooping 表项记录功能。

dhcp snooping binding record

缺省情况下，DHCP Snooping 表项记录功能处于关闭状态。

5.5 配置DHCP Snooping支持Option 82功能

1. 配置限制和指导

配置 DHCP Snooping 支持 Option 82 功能时，需要注意：

- 如果二层以太网接口加入聚合组，则在该接口上进行的 DHCP Snooping 支持 Option 82 功能的配置不会生效；该接口退出聚合组后，之前的配置才会生效。
- 为使Option 82 功能正常使用，需要在DHCP服务器和DHCP Snooping设备上都进行相应配置。DHCP服务器的相关配置请参见“2.10 配置Option 82 的处理方式”。
- 如果以设备名称（**sysname**）作为节点标识填充 DHCP 报文的 Option 82，则设备名称中不能包含空格；否则，DHCP Snooping 将不处理该报文。用户可以通过 **sysname** 命令配置设备名称，该命令的详细介绍请参见“基本配置命令参考”中的“设备管理”。
- DHCP Snooping 功能和 QinQ 功能同时使用，或 DHCP Snooping 设备接收到的 DHCP 报文带有两层 VLAN Tag 时，如果采用 verbose 模式填充 Option 82，则 sub-option 1 中 VLAN ID 字段的格式为“第一层 VLAN Tag.第二层 VLAN Tag”。例如，第一层 VLAN Tag 为 10（十六进制值为 a），第二层 VLAN Tag 为 20（十六进制值为 14），则 VLAN ID 字段的内容为“000a.0014”。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 开启 DHCP Snooping 支持 Option 82 功能。

dhcp snooping information enable

缺省情况下，DHCP Snooping 支持 Option 82 功能处于关闭状态。

(4) （可选）配置 DHCP Snooping 对包含 Option 82 的请求报文的处理策略。

dhcp snooping information strategy { **drop** | **keep** | **replace** }

缺省情况下，对带有 Option 82 的请求报文的处理策略为 **replace**。

DHCP Snooping 对包含 Option 82 请求报文的处理策略 **replace** 时，需要配置 Option 82 的填充模式和填充格式；处理策略为 **keep** 或 **drop** 时，不需要配置 Option 82 的填充模式和填充格式。

(5) （可选）配置 Circuit ID 子选项的填充模式和填充格式。

dhcp snooping information circuit-id { [**vlan** *vlan-id*] **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] } [**format** { **ascii** | **hex** }] }

缺省情况下，Circuit ID 子选项的填充模式为 Normal，填充格式为 hex。

如果以设备的系统名称（**sysname**）作为节点标识填充 DHCP 报文的 Option 82，则系统名称中不能包含空格；否则，DHCP Snooping 添加或替换 Option 82 失败。

(6) （可选）配置 Remote ID 子选项的填充模式和填充格式。

dhcp snooping information remote-id { **normal** [**format** { **ascii** | **hex** }] | [**vlan** *vlan-id*] **string** *remote-id* | **sysname** }

缺省情况下，Remote ID 子选项的填充模式为 Normal，填充格式为 hex。

5.6 配置DHCP Snooping表项固化功能

1. 功能简介

DHCP Snooping 设备重启后，设备上记录的 DHCP Snooping 表项将丢失，DHCP Snooping 与安全模块（如 IP Source Guard）配合使用，则表项丢失会导致安全模块无法通过 DHCP Snooping 获取到相应的表项，进而导致 DHCP 客户端不能顺利通过安全检查、正常访问网络。

DHCP Snooping 表项固化功能将 DHCP Snooping 表项保存到指定的文件中，DHCP Snooping 设备重启后，自动根据该文件恢复 DHCPDHCP Snooping 表项，从而保证 DHCP Snooping 表项不会丢失。

2. 配置限制和指导

执行 **undo dhcp snooping enable** 命令关闭 DHCP Snooping 功能后，设备会删除所有 DHCP Snooping 表项，文件中存储的 DHCP Snooping 表项不会被马上删除，需要在下一次 DHCP Snooping 表项保存文件操作时才能删除所有的 DHCP Snooping 表项。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 指定存储 DHCP Snooping 表项的文件名称。

dhcp snooping binding database filename { *filename* | **url** *url* [**username** *username* [**password** { **cipher** | **simple** } *string*]] }

缺省情况下，未指定存储文件名称。

执行本命令后，会立即触发一次表项备份。

(3) （可选）将当前的 DHCP Snooping 表项保存到用户指定的文件中。

dhcp snooping binding database update now

本命令只用来触发一次 DHCP Snooping 表项的备份。

(4) （可选）配置刷新 DHCP Snooping 表项存储文件的延迟时间。

dhcp snooping binding database update interval *interval*

缺省情况下，若 DHCP Snooping 表项不变化，则不刷新存储文件；若 DHCP Snooping 表项发生变化，默认在 300 秒之后刷新存储文件。

5.7 配置接口动态学习DHCP Snooping表项的最大数目

1. 功能简介

通过本配置可以限制接口动态学习 DHCP Snooping 表项的最大数目，以防止接口学习到大量 DHCP Snooping 表项，占用过多的系统资源。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置接口动态学习 DHCP Snooping 表项的最大数目。

dhcp snooping max-learning-num *max-number*

缺省情况下，不限制接口动态学习 DHCP Snooping 表项的数目。

5.8 配置DHCP Snooping安全功能

5.8.1 配置防止DHCP饿死攻击

1. 功能简介

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。DHCP报文字段的相关内容请参见“1.3 DHCP报文格式”。

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，在一定程度上缓解 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。在这种情况下，需要开启 DHCP Snooping 的 MAC 地址检查功能。开启该功能后，DHCP Snooping 设备检查接收到的 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，将其转发给 DHCP 服务器；如果不一致，则丢弃该报文。**mac-address max-mac-count** 命令的详细介绍，请参见“二层技术-以太网交换”中的“MAC 地址表”。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 开启 DHCP Snooping 的 MAC 地址检查功能。

dhcp snooping check mac-address

缺省情况下，DHCP Snooping 的 MAC 地址检查功能处于关闭状态。

5.8.2 配置防止伪造DHCP请求方向报文攻击

1. 功能简介

本功能用来检查 DHCP 续约报文、DHCP-DECLINE 和 DHCP-RELEASE 三种 DHCP 请求方向的报文，以防止非法客户端伪造这三种报文对 DHCP 服务器进行攻击。

伪造DHCP续约报文攻击是指攻击者冒充合法的DHCP客户端，向DHCP服务器发送伪造的DHCP续约报文，导致DHCP服务器和DHCP客户端无法按照自己的意愿及时释放IP地址租约。如果攻击者冒充不同的DHCP客户端发送大量伪造的DHCP续约报文，则会导致大量IP地址被长时间占用，DHCP服务器没有足够的地址分配给新的DHCP客户端。

伪造DHCP-DECLINE/DHCP-RELEASE报文攻击是指攻击者冒充合法的DHCP客户端，向DHCP服务器发送伪造的DHCP-DECLINE/DHCP-RELEASE报文，导致DHCP服务器错误终止IP地址租约。

在DHCP Snooping设备上开启DHCP请求方向报文检查功能，可以有效地防止伪造DHCP请求方向报文攻击。如果开启了该功能，则DHCP Snooping设备接收到上述报文后，检查本地是否存在与请求方向报文匹配的DHCP Snooping表项。若存在，则接收报文信息与DHCP Snooping表项信息一致时，认为该报文为合法的DHCP请求方向报文，将其转发给DHCP服务器；不一致时，认为该报文为伪造的DHCP请求方向报文，将其丢弃。若不存在，则认为该报文合法，将其转发给DHCP服务器。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 开启DHCP Snooping的DHCP请求方向报文检查功能。

dhcp snooping check request-message

缺省情况下，DHCP Snooping的DHCP请求方向报文检查功能处于关闭状态。

5.8.3 开启DHCP Snooping报文阻断功能

1. 功能简介

在某些组网环境下，用户需要在DHCP Snooping设备的某一端口上丢弃该端口收到的所有DHCP请求方向报文，而又不影响其他端口正常接收DHCP报文。这时，用户可以在该端口上开启DHCP Snooping报文阻断功能。

当端口上开启了DHCP Snooping报文阻断功能后，该端口收到的所有DHCP请求方向的报文都将被丢弃。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 开启DHCP Snooping报文阻断功能。

dhcp snooping deny

缺省情况下，DHCP Snooping报文阻断功能处于关闭状态。

5.9 开启DHCP Snooping日志信息功能

1. 功能简介

DHCP Snooping 日志可以方便管理员定位问题和解决问题。DHCP Snooping 设备生成 DHCP Snooping 日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

2. 配置限制和指导

当 DHCP Snooping 设备输出大量日志信息时，可能会降低设备性能。为了避免该情况的发生，用户可以关闭 DHCP Snooping 日志信息功能，使得 DHCP Snooping 设备不再输出日志信息。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启 DHCP Snooping 日志信息功能。

dhcp snooping log enable

缺省情况下，DHCP Snooping 日志信息功能处于关闭状态。

5.10 DHCP Snooping显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 DHCP Snooping 的配置情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 DHCP Snooping 的统计信息。

表5-3 DHCP Snooping 显示和维护

操作	命令
显示DHCP Snooping表项信息	**display dhcp snooping binding** [**ip** *ip-address* [**vlan** *vlan-id*]] [**verbose**]
显示DHCP Snooping表项备份信息	**display dhcp snooping binding database**
显示DHCP Snooping上Option 82的配置信息	**display dhcp snooping information** { **all** | **interface** *interface-type interface-number* }
显示DHCP Snooping设备上的DHCP报文统计信息	（独立运行模式） **display dhcp snooping packet statistics** （IRF模式） **display dhcp snooping packet statistics** [**slot** *slot-number*]
显示信任端口信息	**display dhcp snooping trust**
清除DHCP Snooping表项	**reset dhcp snooping binding** { **all** | **ip** *ip-address* [**vlan** *vlan-id*] }
清除DHCP Snooping设备上的DHCP报文统计信息	（独立运行模式） **reset dhcp snooping packet statistics** （IRF模式） **reset dhcp snooping packet statistics**

操作	命令
	[**slot** *slot-number*]

5.11 DHCP Snooping典型配置举例

5.11.1 开启DHCP Snooping配置举例

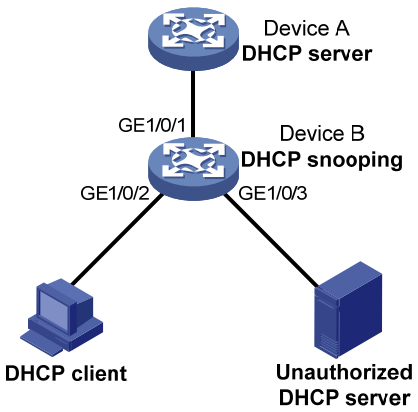
1. 组网需求

Device B 通过以太网端口 GigabitEthernet1/0/1 连接到合法 DHCP 服务器，通过以太网端口 GigabitEthernet1/0/3 连接到非法 DHCP 服务器，通过 GigabitEthernet1/0/2 连接到 DHCP 客户端。要求：

- 与合法 DHCP 服务器相连的端口可以转发 DHCP 服务器的响应报文，而其他端口不转发 DHCP 服务器的响应报文。
- 记录 DHCP-REQUEST 报文和信任端口收到的 DHCP-ACK 报文中 DHCP 客户端 IP 地址及 MAC 地址的绑定信息。

2. 组网图

图5-3 DHCP Snooping 组网示意图



3. 配置步骤

开启 DHCP Snooping 功能。

```
<DeviceB> system-view
[DeviceB] dhcp snooping enable
```

设置 GigabitEthernet1/0/1 端口为信任端口。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] dhcp snooping trust
[DeviceB-GigabitEthernet1/0/1] quit
```

在 GigabitEthernet1/0/2 上开启 DHCP Snooping 表项功能。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] dhcp snooping binding record
[DeviceB-GigabitEthernet1/0/2] quit
```

4. 验证配置

配置完成后，DHCP 客户端只能从合法 DHCP 服务器获取 IP 地址和其它配置信息，非法 DHCP 服务器无法为 DHCP 客户端分配 IP 地址和其他配置信息。且使用 **display dhcp snooping binding** 可查询到获取到的 DHCP Snooping 表项。

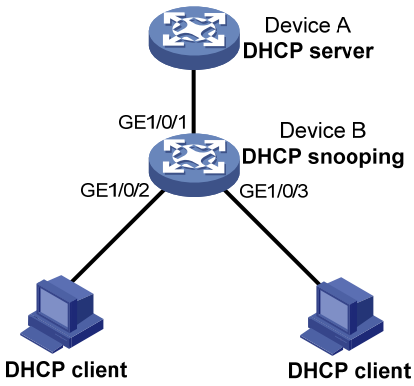
5.11.2 DHCP Snooping支持Option 82 配置举例

1. 组网需求

- Device B 上开启 DHCP Snooping 功能，并支持 Option 82 功能；
- 对包含 Option 82 的请求报文的处理策略为 **replace**；
- 在 GigabitEthernet1/0/2 上配置 Circuit ID 填充内容为 company001，Remote ID 填充内容为 device001；
- 在 GigabitEthernet1/0/3 上配置 Circuit ID 以 verbose 模式填充，接入节点标识为 **sysname**，填充格式为 ASCII 格式，Remote ID 填充内容为 device001；

2. 组网图

图5-4 DHCP Snooping 支持 Option 82 配置示意图



3. 配置步骤

开启 DHCP Snooping 功能。

```
<DeviceB> system-view
[DeviceB] dhcp snooping enable
```

设置 GigabitEthernet1/0/1 端口为信任端口。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] dhcp snooping trust
[DeviceB-GigabitEthernet1/0/1] quit
```

在 GigabitEthernet1/0/2 上配置 DHCP Snooping 支持 Option 82 功能。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] dhcp snooping information enable
[DeviceB-GigabitEthernet1/0/2] dhcp snooping information strategy replace
[DeviceB-GigabitEthernet1/0/2] dhcp snooping information circuit-id string company001
[DeviceB-GigabitEthernet1/0/2] dhcp snooping information remote-id string device001
[DeviceB-GigabitEthernet1/0/2] quit
```

在端口 GigabitEthernet1/0/3 上配置 DHCP Snooping 支持 Option 82 功能。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] dhcp snooping information enable
[DeviceB-GigabitEthernet1/0/3] dhcp snooping information strategy replace
[DeviceB-GigabitEthernet1/0/3] dhcp snooping information circuit-id verbose node-identifier sysname format ascii
[DeviceB-GigabitEthernet1/0/3] dhcp snooping information remote-id string device001
```

4. 验证配置

配置完成后，使用 **`display dhcp snooping information`** 命令可查看到 DHCP Snooping 在端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 上 Option 82 的配置信息。

6 BOOTP客户端

6.1 BOOTP客户端简介

6.1.1 BOOTP客户端的应用环境

BOOTP 是 Bootstrap Protocol（自举协议）的简称。指定设备的接口作为 BOOTP 客户端后，该接口可以通过 BOOTP 协议从 BOOTP 服务器获取 IP 地址等信息，从而方便用户配置。

使用 BOOTP 协议时，管理员需要在 BOOTP 服务器上为每个 BOOTP 客户端配置 BOOTP 参数文件，该文件包括 BOOTP 客户端的 MAC 地址及其对应的 IP 地址等信息。当 BOOTP 客户端向 BOOTP 服务器发起请求时，服务器会查找 BOOTP 参数文件，并返回相应的配置信息。

由于 BOOTP 协议需要在 BOOTP 服务器上为每个客户端事先配置参数文件，BOOTP 一般运行在相对稳定的环境中。当网络变化频繁时，推荐采用 DHCP 协议。

由于 DHCP 服务器可以与 BOOTP 客户端进行交互，因此用户可以不配置 BOOTP 服务器，而使用 DHCP 服务器为 BOOTP 客户端分配 IP 地址。

6.1.2 IP地址动态获取过程

BOOTP 客户端从 BOOTP 服务器动态获取 IP 地址的具体过程如下：

(1) BOOTP 客户端以广播方式发送 BOOTP 请求报文，其中包含了 BOOTP 客户端的 MAC 地址；

(2) BOOTP 服务器接收到请求报文后，根据报文中的 BOOTP 客户端 MAC 地址，从配置文件数据库中查找对应的 IP 地址等信息，并向客户端返回包含这些信息的 BOOTP 响应报文；

(3) BOOTP 客户端从接收到的响应报文中即可获得 IP 地址等信息。

在下面的 IP 地址动态获取过程中，BOOTP 服务器的功能可以用 DHCP 服务器替代。

6.1.3 协议规范

与 BOOTP 相关的协议规范有：

- RFC 951：Bootstrap Protocol (BOOTP)
- RFC 2132：DHCP Options and BOOTP Vendor Extensions
- RFC 1542：Clarifications and Extensions for the Bootstrap Protocol

6.2 配置接口通过BOOTP协议获取IP地址

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

BOOTP 客户端中对于接口的相关配置，目前只能在三层以太网接口（包括子接口）、三层聚合接口和 VLAN 接口上进行。

(3) 配置接口通过 BOOTP 协议获取 IP 地址。

ip address bootp-alloc

缺省情况下，接口不通过 BOOTP 协议获取 IP 地址。

6.3 BOOTP客户端显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 BOOTP 客户端的运行情况，通过查看显示信息验证配置的效果。

表6-1 BOOTP 客户端显示和维护

操作	命令
显示BOOTP客户端的相关信息	**display bootp client** [**interface** *interface-type interface-number*]

6.4 BOOTP客户端典型配置举例

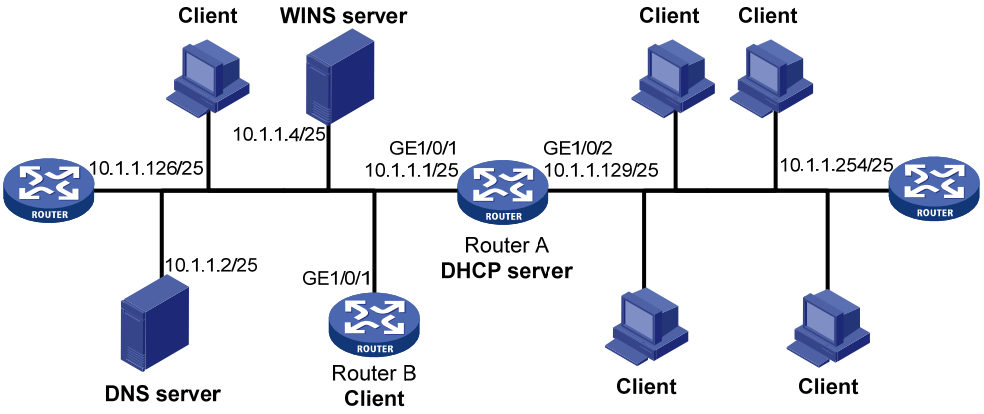
6.4.1 BOOTP客户端基本组网典型配置举例

1. 组网需求

Router B 的以太网接口 GigabitEthernet1/0/1 接入局域网，通过 BOOTP 协议从 DHCP 服务器获取 IP 地址。

2. 组网图

图6-1 BOOTP 客户端基本组网图



3. 配置步骤

下面只列出作为客户端的 Router B 的配置。

配置接口 GigabitEthernet1/0/1 通过 BOOTP 动态获取地址。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] ip address bootp-alloc
```

通过 **display bootp client** 命令可以查看 BOOTP 客户端申请到的 IP 地址。

说明

为了使BOOTP客户端能从DHCP服务器获得IP地址，还需要在DHCP服务器上进行一些配置，具体内容请参见“2.18 DHCP服务器典型配置举例”。