## DHCP(Dynamic Host Configuration Protocol)

**什么是DHCP？**

动态主机配置协议，是一种网络管理协议，用于集中对用户IP地址进行动态管理和配置，工作在osi的应用层。采用客户端/服务器通信模式，由客户端（DHCP Client）向服务器（DHCP Server）提出配置申请，DHCP Server为网络上的每个设备动态分配IP地址、子网掩码、默认网关地址，域名服务器（DNS）地址和其他相关配置参数。

**为什么要用DHCP？**

* 准确的IP配置：IP地址配置参数必须准确，并且在处理“ 192.168.XXX.XXX”之类的输入时，很容易出错。另外印刷错误通常很难解决，使用DHCP服务器可以最大程度地降低这种风险。
* 减少IP地址冲突：每个连接的设备都必须有一个IP地址。但是，每个地址只能使用一次，重复的地址将导致无法连接一个或两个设备的冲突。当手动分配地址时，尤其是在存在大量仅定期连接的端点（例如移动设备）时，可能会发生这种情况。DHCP的使用可确保每个地址仅使用一次。
* IP地址管理的自动化：如果没有DHCP，网络管理员将需要手动分配和撤消地址。跟踪哪个设备具有什么地址可能是徒劳的，因为几乎无法理解设备何时需要访问网络以及何时需要离开网络。DHCP允许将其自动化和集中化，因此网络专业人员可以从一个位置管理所有位置。
* 高效的变更管理：DHCP的使用使更改地址，范围或端点变得非常简单。例如，组织可能希望将其IP寻址方案从一个范围更改为另一个范围。DHCP服务器配置有新信息，该信息将传播到新端点。同样，如果升级并更换了网络设备，则不需要网络配置。

**DHCP是如何工作的？**

DHCP协议采用UDP作为传输协议，DHCP客户端发送请求消息到DHCP服务器的67号端口，DHCP服务器回应应答消息给DHCP客户端的68号端口。

只有跟DHCP客户端在同一个网段的DHCP服务器才能收到DHCP客户端广播的DHCP DISCOVER报文。当DHCP客户端与DHCP服务器不在同一个网段时，必须部署DHCP中继来转发DHCP客户端和DHCP服务器之间的DHCP报文。在DHCP客户端看来，DHCP中继就像DHCP服务器；在DHCP服务器看来，DHCP中继就像DHCP客户端。

PS：(1)直接广播 (能够跨越不同网络的广播)；本地广播 (只在本地网络中的广播)；

(2)往往一个网段中，网关、DNS、Web、DHCP等服务器地址都是同一个；且在一个网段中，一些重要主机一般需配置静态ip地址，因此DHCP服务器的地址池需要预留一段以供静态配置使用。

**不同场景下的DHCP工作原理**

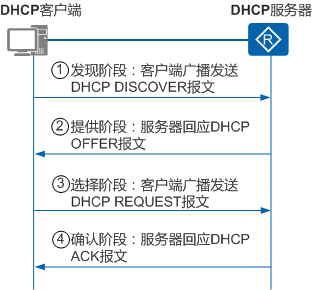
⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐**无中继场景时DHCP客户端首次接入网络**⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐

①**发现阶段：客户端广播发送DHCP DISCOVER报文（**0.0.0.0作为源IP地址，然后广播地址255.255.255.255作为目的地址+客户端MAC地址，发给同一网段的所有设备，包括DHCP服务器或中继；若无回复，则等待1s后继续发送3个DISCOVER报文，等待时延分别为9秒、13秒和16秒加上一个长度为0～1000毫秒之间的随机时延。如果仍然无法联系DHCP服务器，则认为自动获取IP地址失败，默认情况下将随机使用APIPA（自动专有IP地址，169.254.0.0/16）中定义的未被其他客户使用的IP地址，子网掩码为255.255.0.0，但是不会配置默认网关和其他TCP/IP选项，因此只能和同子网的使用APIPA地址的客户端进行通讯。**）**

**②提供阶段：服务器广播回应DHCP OFFER报文（**源IP地址为DHCP服务器的IP地址，而广播地址255.255.255.255作为目的地址--因为没客户端地址，此消息包括【客户端MAC地址；DHCP服务器提供的客户端IP地址、客户端子网掩码、DNS服务器、网关、租约期限等；】DHCP服务器选择跟接收DHCP DISCOVER报文接口的IP地址处于同一网段的地址池，并且从中选择一个可用的IP地址，然后通过DHCP OFFER报文发送给DHCP客户端，等待客户端回应时长为16秒；**）**

**③选择阶段：客户端广播发送 DHCP REQUEST报文（**0.0.0.0作为源IP地址，广播地址255.255.255.255作为目的地址，消息中包含了【DHCP客户端的MAC地址、接受的租约中的IP地址、提供此租约的DHCP服务器地址等】，若有多个DHCP服务器回应DHCP OFFER报文，则DHCP客户端一般只接收第一个收到的DHCP OFFER报文，然后以广播方式发送DHCP REQUEST报文，该报文中包含客户端想选择的DHCP服务器标识符（即Option50，填充了接收的DHCP OFFER报文中yiaddr字段的IP地址，DHCP客户端广播发送DHCP REQUEST报文通知所有的DHCP服务器，它将选择某个DHCP服务器提供的IP地址，其他DHCP服务器可以重新将曾经分配给客户端的IP地址分配给其他客户端。**）**

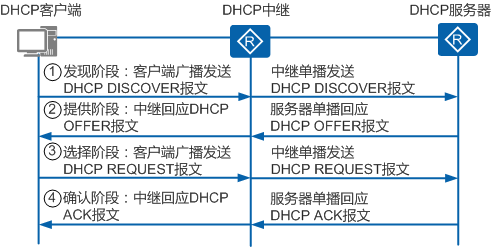
**④确认阶段：服务器回应DHCP ACK报文（**单播，当DHCP服务器收到DHCP客户端发送的DHCP REQUEST报文后，DHCP服务器回应DHCP ACK报文，表示DHCP REQUEST报文中请求的IP地址（Option50填充的）分配给客户端使用。如果DHCP客户端的操作系统为Windows版本，当DHCP客户端接收到DHCP ACK广播消息后，会向网络发出三个针对此IP地址的ARP解析请求以执行冲突检测，确认网络上没有其他主机使用DHCP服务器提供的IP地址，从而避免IP地址冲突。如果发现该IP已经被其他主机所使用（有其他主机应答此ARP解析请求），则DHCP客户端则会广播发送（因为它仍然没有有效的IP地址）DHCP DECLINE消息给DHCP服务器拒绝此IP地址租约，然后重新发起DHCP DISCOVER进程。此时，在DHCP服务器管理控制台中，会显示此IP地址为BAD\_ADDRESS。如果没有其他主机使用此IP地址，则DHCP客户端的TCP/IP使用租约中提供的IP地址完成初始化，从而可以和其他网络中的主机进行通讯。至于其他TCP/IP选项，如DNS服务器和WINS服务器等，本地手动配置将覆盖从DHCP服务器获得的值。**）**



⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐**有中继场景时DHCP客户端首次接入网络**⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐

有DHCP中继的场景中，首次接入网络的DHCP客户端和DHCP服务器的工作原理与无中继场景时DHCP客户端首次接入网络的工作原理相同。主要差异是DHCP中继在DHCP服务器和DHCP客户端之间转发DHCP报文，以保证DHCP服务器和DHCP客户端可以正常交互。下面仅针对DHCP中继的工作原理进行介绍。

如下图所示，在部署DHCP中继的场景下，首次接入网络DHCP客户端与DHCP服务器的报文交互过程。



①**发现阶段**：DHCP中继接收到DHCP客户端广播发送的DHCP DISCOVER报文后，进行如下处理：

1. 检查DHCP报文中的hops字段，如果大于16，则丢弃DHCP报文；否则，将hops字段加1（表明经过一次DHCP中继），并继续下面的操作。
2. 检查DHCP报文中的giaddr字段。如果是0，将giaddr字段设置为接收DHCP DISCOVER报文的接口IP地址。如果不是0，则不修改该字段，继续下面的操作。
3. 将DHCP报文的目的IP地址改为DHCP服务器或下一跳中继的IP地址，源地址改为中继连接客户端的接口地址，通过路由转发将DHCP报文单播发送到DHCP服务器或下一跳中继。

如果DHCP客户端与DHCP服务器之间存在多个DHCP中继，后面的中继接收到DHCP DISCOVER报文的处理流程同前面所述。

②**提供阶段**：DHCP服务器接收到DHCP DISCOVER报文后，选择与报文中giaddr字段为同一网段的地址池，并为客户端分配IP地址等参数，然后向giaddr字段标识的DHCP中继单播发送DHCP OFFER报文。DHCP中继收到DHCP OFFER报文后，会进行如下处理：

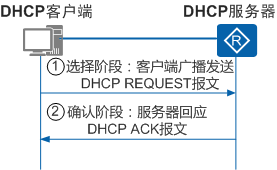
1. 检查报文中的giaddr字段，如果不是接口的地址，则丢弃该报文；否则，继续下面的操作。
2. DHCP中继检查报文的广播标志位。如果广播标志位为1，则将DHCP OFFER报文广播发送给DHCP客户端；否则将DHCP OFFER报文单播发送给DHCP客户端。

③**选择阶段：**中继接收到来自客户端的DHCP REQUEST报文的处理过程同无中继场景下的选择阶段。

④**确认阶段：**中继接收到来自服务器的DHCP ACK报文的处理过程同无中继场景下的确认阶段。

⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐**DHCP客户端重用曾经使用过的地址**⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐

DHCP客户端非首次接入网络时，可以重用曾经使用过的地址。如下图所示，DHCP客户端与DHCP服务器交互DHCP报文，以重新获取之前使用的IP地址等网络参数，该过程称为两步交互。

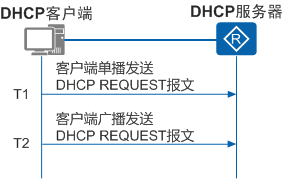


①**选择阶段：**客户端广播发送包含前一次分配的IP地址的DHCP REQUEST报文，报文中的Option50（请求的IP地址选项）字段填入曾经使用过的IP地址。

②**确认阶段：**DHCP服务器收到DHCP REQUEST报文后，根据DHCP REQUEST报文中携带的MAC地址来查找有没有相应的租约记录，如果有则返回DHCP ACK报文，通知DHCP客户端可以继续使用这个IP地址。否则，保持沉默，等待客户端重新发送DHCP DISCOVER报文请求新的IP地址。

⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐**DHCP客户端更新租期**⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐

DHCP服务器采用动态分配机制给客户端分配IP地址时，分配出去的IP地址有租期限制。DHCP客户端向服务器申请地址时可以携带期望租期，服务器在分配租期时把客户端期望租期和地址池中租期配置比较，分配其中一个较短的租期给客户端。租期到期或者客户端下线释放地址后，服务器会收回该IP地址，收回的IP地址可以继续分配给其他客户端使用。这种机制可以提高IP地址的利用率，避免客户端下线后IP地址继续被占用。如果DHCP客户端希望继续使用该地址，需要更新IP地址的租期（如延长IP地址租期）。



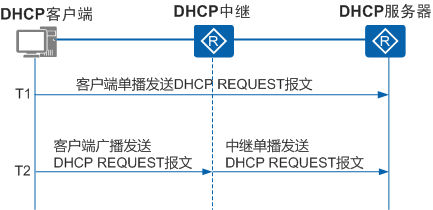
①**当租期达到50%（T1）时**，DHCP客户端会自动以单播的方式向DHCP服务器发送DHCP REQUEST报文，请求更新IP地址租期。如果收到DHCP服务器回应的DHCP ACK报文，则租期更新成功（即租期从0开始计算）；如果收到DHCP NAK报文，则重新发送DHCP DISCOVER报文请求新的IP地址。

②**当租期达到87.5%（T2）时**，如果仍未收到DHCP服务器的应答，DHCP客户端会自动以广播的方式向DHCP服务器发送DHCP REQUEST报文，请求更新IP地址租期。如果收到DHCP服务器回应的DHCP ACK报文，则租期更新成功（即租期从0开始计算）；如果收到DHCP NAK报文，则重新发送DHCP DISCOVER报文请求新的IP地址。

③**如果租期时间到**时都没有收到服务器的回应，客户端停止使用此IP地址，重新发送DHCP DISCOVER报文请求新的IP地址。

客户端在租期时间到之前，如果用户不想使用分配的IP地址（例如客户端网络位置需要变更），会触发DHCP客户端向DHCP服务器发送DHCP RELEASE报文，通知DHCP服务器释放IP地址的租期。DHCP服务器会保留这个DHCP客户端的配置信息，将IP地址列为曾经分配过的IP地址中，以便后续重新分配给该客户端或其他客户端。客户端可以通过发送DHCP INFORM报文向服务器请求更新配置信息。

如下图所示，部署DHCP中继时，更新租期的过程与上述过程相似。



⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐**DHCP使用场景**⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐

DHCP提供了两种地址分配机制，网络管理员可以根据网络需求为不同的主机选择不同的分配策略。

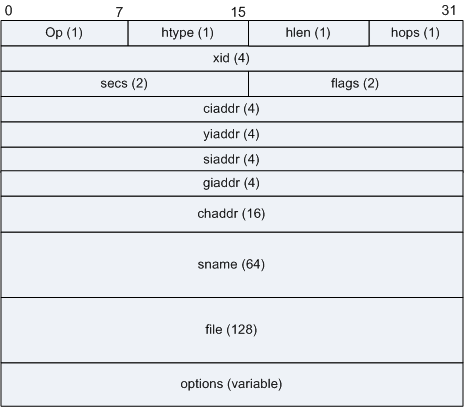
* 动态分配机制：通过DHCP为主机分配一个有使用期限的IP地址。

DHCP使用了租期的概念，或称为设备IP地址的有效期。租用时间是不定的，主要取决于用户在某地连接Internet需要多久，这种分配机制适用于主机需要临时接入网络或者空闲地址数小于网络主机总数且主机不需要永久连接网络的场景。

* 静态分配机制：网络管理员通过DHCP为指定的主机分配固定的IP地址。

相比手工静态配置IP地址，通过DHCP方式静态分配机制避免人工配置发生错误，方便管理员统一维护管理。

⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐**DHCP报文格式**⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐



DHCP报文中各字段的含义：

**Op**：表示报文的类型，取值为1或2，含义如下：

1：客户端请求报文

2：服务器响应报文

**Htype**：表示硬件类型。不同的硬件类型取值不同，最常见的值是1，表示以太网。

**Hlen**：表示硬件地址的长度。对于以太网，该值为6。

**Hops**：表示当前的DHCP报文经过的DHCP中继的数目。该字段由客户端设置为0，每经过一个DHCP中继时，该字段加1。

**Xid**：事务ID，由客户端选择的一个随机数，被服务器和客户端用来在它们之间交流请求和响应，客户端用它对请求和应答进行匹配。该ID由客户端设置并由服务器返回，为32位整数。

**Secs**：表示客户端从开始获取地址或地址续租更新后所用的时间，单位是秒。

**Flags**：只有标志字段的最高位才有意义，其余的位均被置为0。

最左边的字段被解释为广播响应标志位，内容如下所示：

0：客户端请求服务器以单播形式发送响应报文

1：客户端请求服务器以广播形式发送响应报文

**Ciaddr**：客户端的IPv4地址。只有客户端是Bound、Renew、Rebinding状态，并且能响应ARP请求时，才能被填充。

**Yiaddr**：表示服务器分配给客户端的IPv4地址。

**Siaddr**：表明DHCP协议流程的下一个阶段要使用的服务器的IPv4地址。

**Giaddr**：表示第一个DHCP中继的IPv4地址。当客户端发出DHCP请求时，如果服务器和客户端不在同一个网段，那么第一个DHCP中继在将DHCP请求报文转发给DHCP服务器时，会把自己的IPv4地址填入此字段，DHCP服务器会根据此字段来判断出客户端所在的网段地址，从而选择合适的地址池，为客户端分配该网段的IPv4地址。

服务器还会根据此地址将响应报文发送给此DHCP中继，再由DHCP中继将此报文转发给客户端。若在到达DHCP服务器前经过了多个DHCP中继，该字段作为客户端所在的网段的标记，填充了第一个DHCP中继的IPv4地址后不会再变更，只是每经过一个DHCP中继，hops字段的数值会加1。

**Chaddr**：该字段表示客户端的MAC地址，此字段与前面的“Hardware Type”和“Hardware Length”保持一致。当客户端发出DHCP请求时，将自己的硬件地址填入此字段。对于以太网，当“Hardware Type”和“Hardware Length”分别为“1”和“6”时，此字段必须填入6字节的以太网MAC地址。

**Sname**：该字段表示客户端获取配置信息的服务器名字。此字段由DHCP Server填写，是可选的。如果填写，必须是一个以0结尾的字符串。

**File**：该字段表示客户端的启动配置文件名。此字段由DHCP Server填写，是可选的，如果填写，必须是一个以0结尾的字符串。

**Options**：该字段表示DHCP的选项字段，至少为312字节，格式为"代码+长度+数据"。DHCP通过此字段包含了服务器分配给终端的配置信息，如网关IPv4地址，DNS服务器的IPv4地址，客户端可以使用IPv4地址的有效租期等信息。

⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐**Wireshark抓dhcp包验证**⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐

**路由器DHCP功能测试点**

1. DUT作为DHCP客户端
2. DUT作为DHCP中继
3. DUT作为DHCP服务器

DHCP Server

说明

Switch 配置

2号端口为镜像端口

5号端口为被镜像口

PC配置

PC上网方式设置为“静态IP”

1

Switch

5

2

DUT

PC

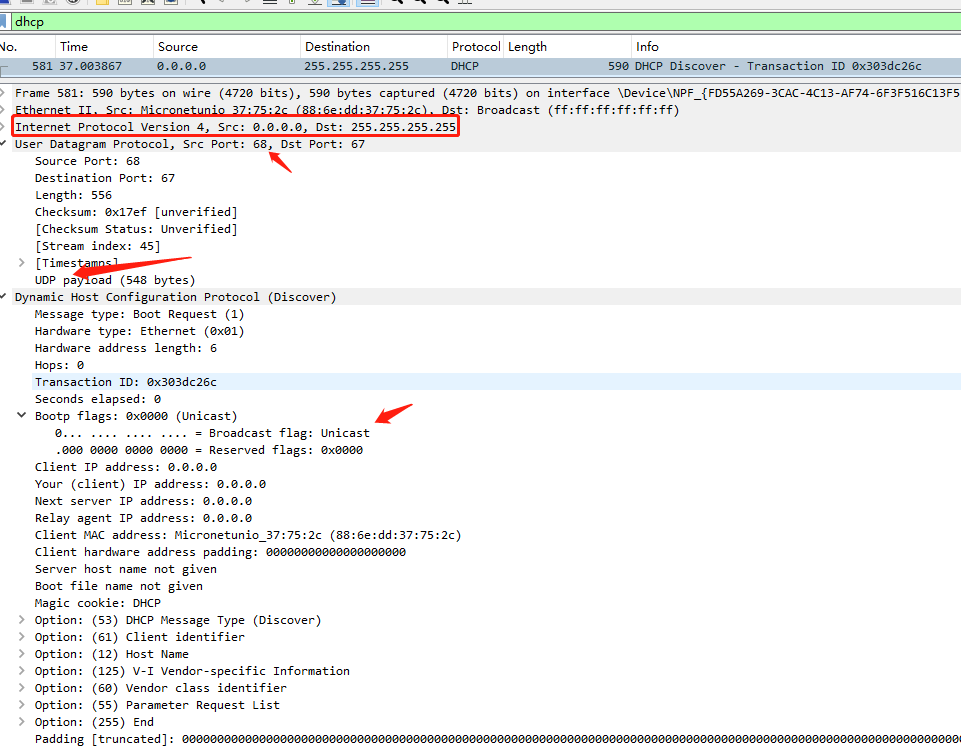
DUT作为DHCP客户端，实际连接拓扑图如上，现验证“**无中继场景时DHCP客户端首次接入网络**”

抓包步骤如下

1. 首先将DUT 上网方式设置为“静态IP”
2. 开启wireshark，开始抓包
3. 将DUT上网方式设置为“DHCP”
4. 筛选dhcp包

Discover报文分析：

1. Broadcast flag:0，告知服务器，请使用单播方式和“我”通信
2. Dst：255.255.255.255，该报文是以广播形式发送的

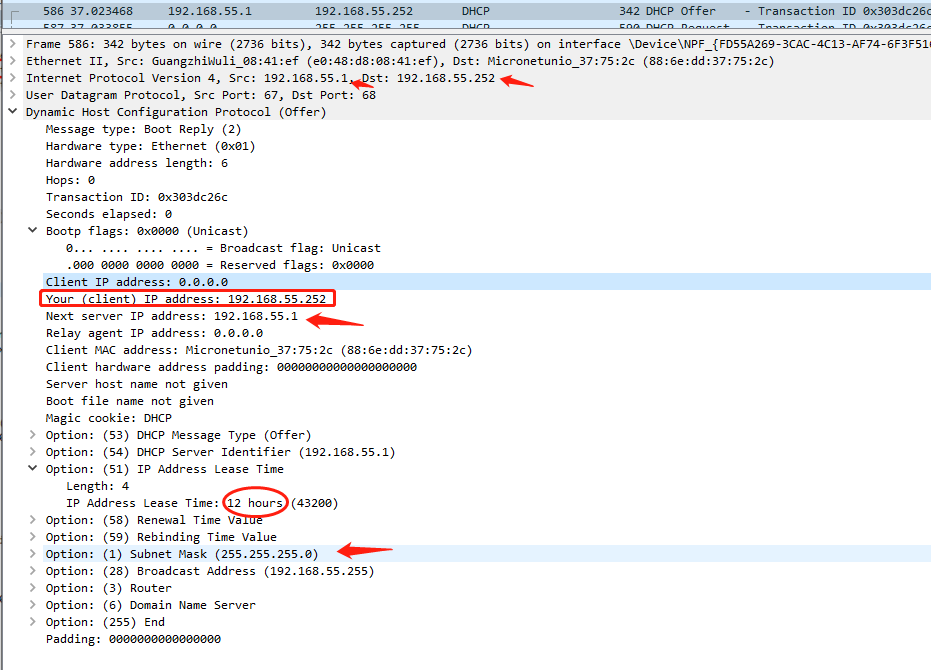


Offer报文分析

①DHCP server以单播形式和DHCP client通信

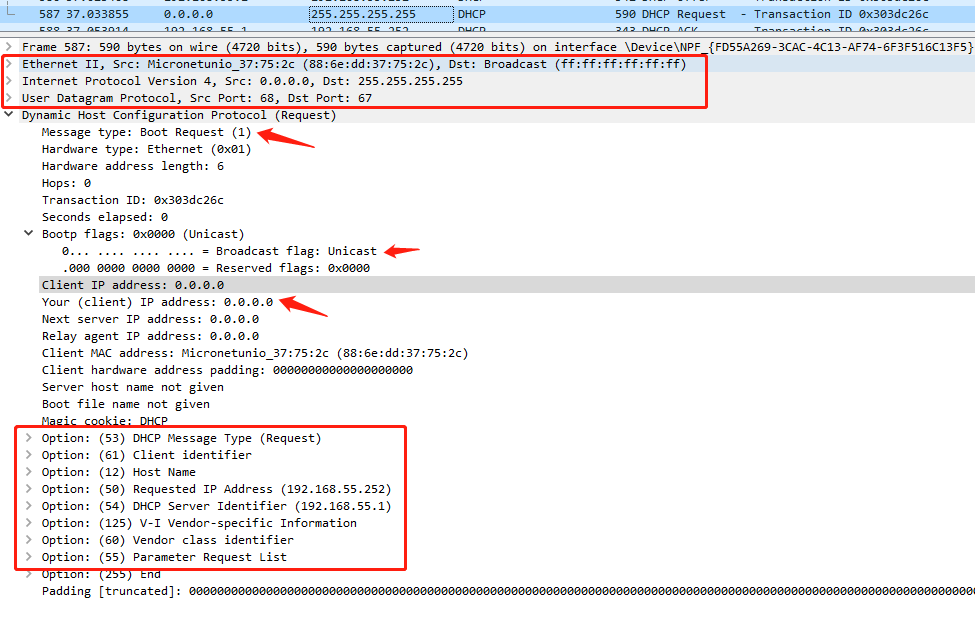
②给Client分配的IP地址为：192.168.55.252，网关为：192.168.55.1，租期为12小时

③Client只收到了一个Offer

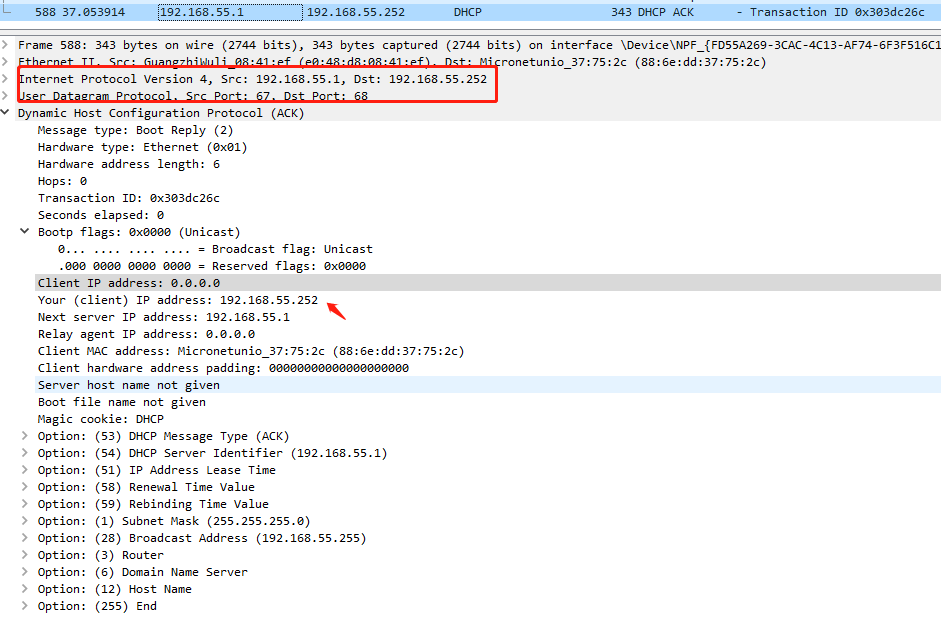


Request报文分析

①广播发送，IP地址仍为0.0.0.0



Ack报文分析



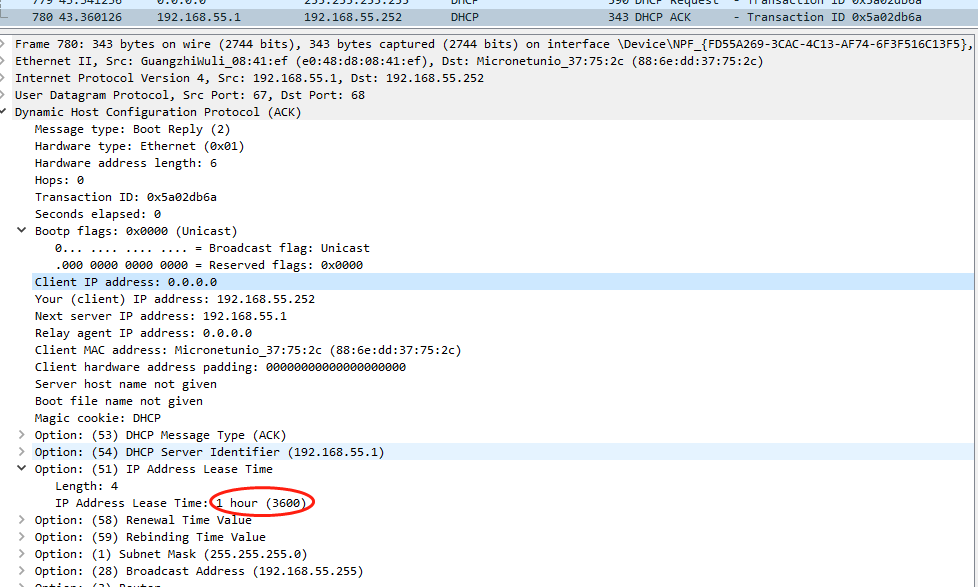
DUT作为DHCP客户端，实际连接拓扑图如上，现验证“**DHCP客户端更新租期**”

抓包步骤如下

1、登入DHCP Server管理界面，将DHCP租期设置为1小时

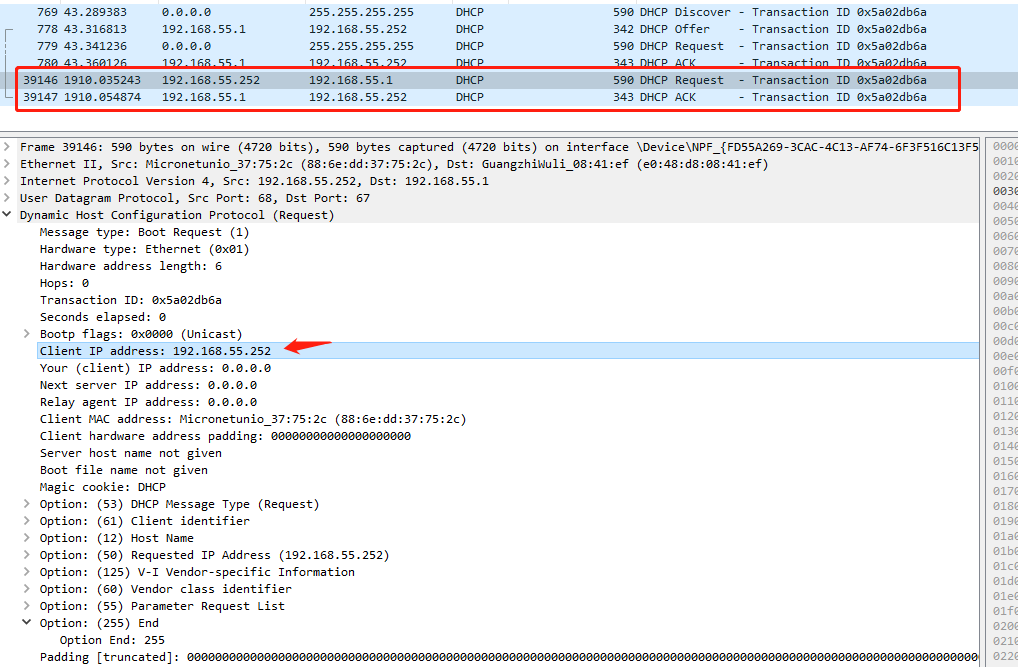
1. 将DUT 上网方式设置为“静态IP”
2. 开启wireshark，开始抓包
3. 将DUT上网方式设置为“DHCP”
4. 验证抓包，筛选dhcp包

验证租期，在该步骤下，DUT再次通过4报文交互获取IP地址，租期等信息



从抓的包中可以看出，新申请的IP租期确为1小时，续租时间为半小时。

Wireshark继续监听，等待抓取DHCP客户端更新租期的报文，半小时后，以单播方式发送Request报文给服务器请求续租，DHCP服务器回应ACK表示续租成功



DUT作为DHCP客户端，实际连接拓扑图如上，现验证“**DHCP客户端重用曾经使用过的地址”**

抓包步骤如下

1. DUT 断电重启，重启DHCP服务，拔掉网线
2. 开启wireshark，开始抓包
3. 将DUT上网方式设置为“DHCP”
4. 筛选dhcp包

尝试1中所有情况，DUT再次连接不会携带上次重用地址，依旧发生4报文交互，但分配的地址依旧是上次使用的IP地址

DUT作为DHCP中继，实际连接拓扑图如下，现验证“**有中继场景时DHCP客户端首次接入网络**”

DHCP Server

DUT

PC

**前置条件**

①DUT一台(作为DHCP服务器)，WAN连接可上行网线，LAN口连接本机

②找到本机对应网卡，确定监听位置

③本机安装wireshark并能检测到DUT对应网卡

**步骤**

**------先关闭DHCP，禁用网卡----**

①打开wireshark，选定上述网卡，点击开始捕

②将对应网卡IP地址获取设置为DHCP方式

③筛选分组，筛选条件为协议：dhcp

**或**

**------确保DHCP打开，不禁用网卡------**

①打开控制台端口，执行 ipconfig.exe /release "以太网 3"，释放网卡（英文空格）

②启动wireshark抓包，设置筛选条件

③打开控制台窗口，执行ipconfig.exe /renew "以太网 3"，启用网卡（英文空格）

**预期输出**

抓到四个DHCP包，分别是

**DISCOVER：**

**OFFER:**

**REQUEST：**

**ACK**

**实际结果**

**DISCOVER:**本机MAC地址，源ip为0.0.0.0，目的ip为255.255.255.255，源端口为68，目的端口为67，消息类型为1(DHCPDISCOVER)，Option: (50) Requested IP Address (192.168.10.100)，Option: (55) Parameter Request List，Destination: Broadcast (ff:ff:ff:ff:ff:ff)，Source: NanjingQinhe\_c9:11:f2 (54:14:a7:c9:11:f2)

**OFFER:**Destination:NanjingQinhe\_c9:11:f2 (54:14:a7:c9:11:f2)，Source: Micronetunio\_37:75:2d (88:6e:dd:37:75:2d)，Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.100，Src Port: 67, Dst Port: 68，Message type: Boot Reply (2)，IP Address Lease Time: 8 hours (28800)

**REQUEST:**Destination: Broadcast (ff:ff:ff:ff:ff:ff)，Source: NanjingQinhe\_c9:11:f2 (54:14:a7:c9:11:f2)，Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255，User Datagram Protocol, Src Port: 68, Dst Port: 67，Message type: Boot Request (1)

**ACK:**Internet Protocol Version 4, Src: 192.168.10.1, Dst: 192.168.10.100，User Datagram Protocol, Src Port: 67, Dst Port: 68，Ethernet II, Src: Micronetunio\_37:75:2d (88:6e:dd:37:75:2d), Dst: NanjingQinhe\_c9:11:f2 (54:14:a7:c9:11:f2)

**结果分析**：预期结果中OFFER和ACK阶段报文的目的地址为广播地址255.255.255.255，但实际结果中OFFER和ACK阶段报文目的地址为192.168.10.100

即OFFER和ACK阶段，DHCP服务器采用的是单播方式而不是广播

**问题：DHCP offer和ack 报文到底是单播还是广播？**

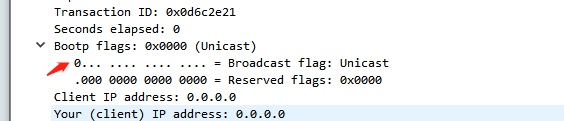
DHCP在设计之初，充分考虑到TCP/IP协议实现的多样性，具体和DHCP有关的多样性体现在：TCP/IP协议栈没有完成IP地址配置前，是否可以接受单播(Unicast)报文？

有些IP协议栈在完成IP地址的配置前，可以接收Destination IP = Any的IP报文，只要该IP报文能够被硬件网卡接收并过滤给IP协议栈。而有些IP协议栈在完成IP地址的配置前，是不会接收任何单播IP报文的，只会接收广播IP报文，即Destination IP = 255.255.255.255。**无论是哪种IP协议栈，都是可以接收广播报文**

DHCP为了增强协议的健壮性(Robustness)，是这样规定的：

如果协议栈在初始化时，不接收单播IP报文，请在DHCP Discovery / Request报文的Flags里明确告知服务器，通过设置“BROADCAST flag = 1”，那么服务器就使用广播来和客户端通信。

如果协议栈在初始化时，可以接收单播IP报文，请在DHCP Discovery / Request报文的Flags里明确告知服务器，通过设置“BROADCAST flag = 0”，那么服务器就使用单播来和客户端通信。



问题：为什么DHCP REQUEST报文不能单播（已经知道目的ip）？

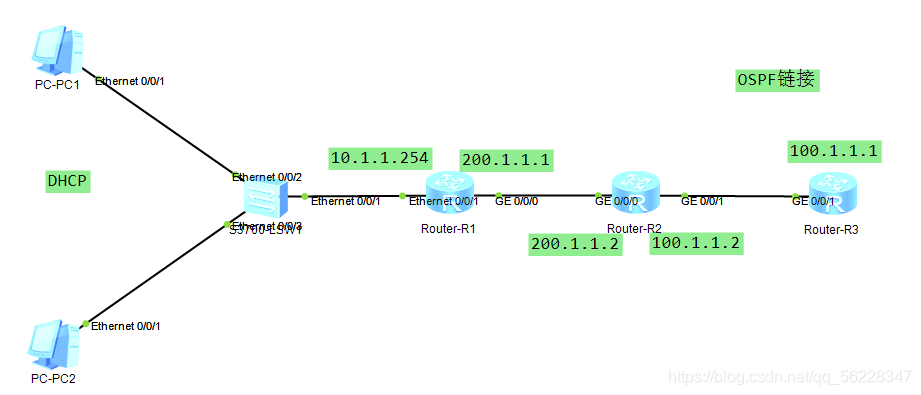
收到offer报文后，发送request广播报文进一步确认，同时通知其他dhcp服务器已经收到租约

############################**DHCP中继配置**#####################################

**DHCP中继原理**

    DHCP客户使用IP广播来寻找同一网段上的DHCP服务器。当服务器和客户段处在不同网段，即被路由器分割开来时，路由器是不会转发这样广播包的。因此可能需要在每个网段上设置一个DHCP服务器，虽然DHCP只消耗很小的一部分资源的，但多个 DHCP服务器，毕竟要带来管理上的不方便。DHCP中继的使用使得一个DHCP服务器同时为多个网段服务成为可能，配置DHCP中继的网络设备可以在不同网段上从DHCP总服务器获取IP地址分配给下面的各主机，路由器或者三层交换机都可以充当DHCP中继。

**网络拓扑及实验要求**



R3为DHCP服务器，现在PC1，PC2需要自动获取IP地址和网关等信息，在R1上配置DHCP中继，使得PC1，PC2可以自动获取IP地址等信息。

#各路由器的接口IP地址配置此处省略

#R1、R2、R3路由器之间使用OSPF协议联通，此处省略配置

在R3上使用dhcp enable开启DHCP功能，创建全局地址池dhcp-pool，可分配地址为10.1.1.0/24，出口网关为10.1.1.254，并在接口上开启DHCP服务功能，指定从全局地址池分配地址。

[R3]dhcp enable

[R3]ip pool dhcp-pool

[Huawei-ip-pool-dhcp-pool]network 10.1.1.0 mask 255.255.255.0

[Huawei-ip-pool-dhcp-pool]gateway-list 10.1.1.254

[Huawei-ip-pool-dhcp-pool]interface g0/0/1

[Huawei-GigabitEthernet0/0/1]dhcp select global

配置DHCP中继：

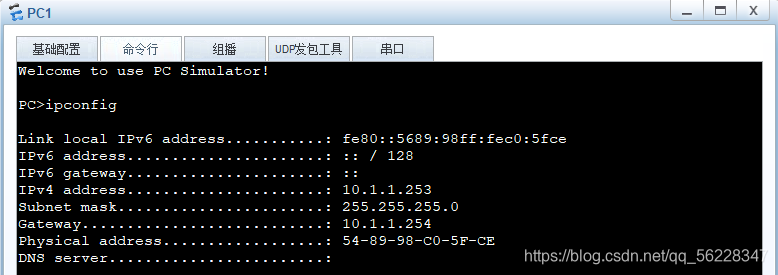
[R1]dhcp enable

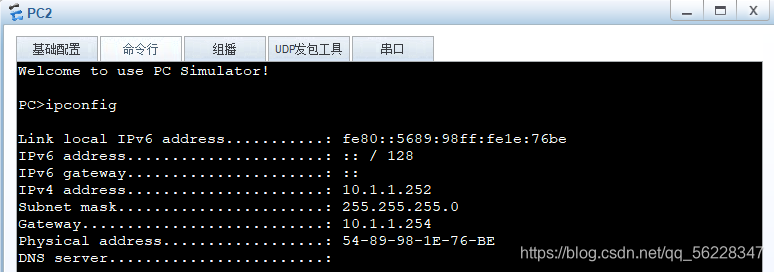
[R1]interface e0/0/1

[Huawei-Ethernet0/0/1]dhcp select relay

[Huawei-Ethernet0/0/1]dhcp relay server-ip 100.1.1.1 //填写DHCP服务器地址

查看PC1，PC2获取IP地址的情况：





配置成功

## PPPoE（Point-to-Point Protocol over Ethernet）

**什么是PPPoE？**

以太网上的点对点协议，是将点对点协议（PPP）封装在以太网（Ethernet）框架中的一种网络隧道协议。

**为什么要用PPPoE？**

PPPoE技术将以太网技术的经济性与PPP协议的可管理控制性结合在一起，提供接入互联网的功能。对于运营商来说，它能够最大限度地利用电信接入网现有的体系结构，利用现有的拨号网络资源，运营和管理的模式也不需要很大的改变；对于用户来说，使用感与原来的拨号上网没有太大区别，较容易接受。

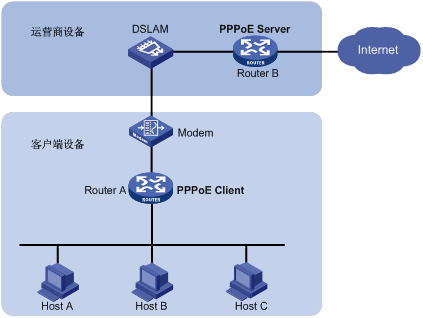
**PPPoE是如何工作的？**

应用在链路层，PPPoE使用Client/Server模型。PPPoE Client向PPPoE Server发起连接请求，两者之间会话协商通过后，就建立PPPoE会话，此后PPPoE Server向PPPoE Client提供接入控制、认证、计费等功能。PPPoe的最主要作用就是使得多台设备可以借助以太网多点接入多点访问的特点去和一台设备做上网认证请求，这样运营商一台认证设备就可以满足多个用户的认证请求。

根据PPPoE会话的起点所在位置的不同，PPPoE分为Router-Initiated和Host-Initiated两种组网结构。

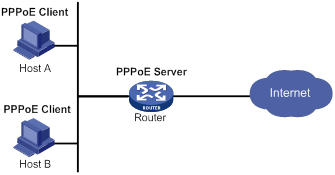
⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐**Router-Initiated组网结构**⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐

如下图所示，Router-Initiated组网结构是在两台路由器之间建立PPPoE会话，所有主机通过同一个PPPoE会话传送数据，主机上不用安装PPPoE客户端拨号软件，一般是一个企业共用一个账号接入网络（图中PPPoE Client位于企业/公司内部，PPPoE Server是运营商的设备）。

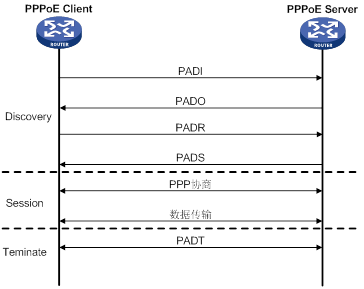


⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐**Host-Initiated组网结构**⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐

如图2所示，Host-Initiated组网结构是将PPPoE会话建立在Host和运营商的路由器之间，为每一个Host建立一个PPPoE会话，每个Host都是PPPoE Client，每个Host使用一个帐号，方便运营商对用户进行计费和控制。Host上必须安装PPPoE客户端拨号软件。



⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐**PPPoE的协商过程**⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐



**①Discovery阶段：**该阶段完成之后通信双方都会知道PPPoE的Session ID以及对方以太网地址，它们共同确定了唯一的PPPoE Session。

Discovery阶段由四个过程组成，具体如下：

1. PPPoE Client广播发送一个PADI报文，在此报文中包含PPPoE Client想要得到的服务类型信息。
2. 所有的PPPoE Server收到PADI报文之后，将其中请求的服务与自己能够提供的服务进行比较，如果可以提供，则单播回复一个PADO报文。
3. 根据网络的拓扑结构，PPPoE Client可能收到多个PPPoE Server发送的PADO报文，PPPoE Client选择最先收到的PADO报文对应的PPPoE Server做为自己的PPPoE Server，并单播发送一个PADR报文。
4. PPPoE Server产生一个唯一的会话ID（Session ID），标识和PPPoE Client的这个会话，通过发送一个PADS报文把会话ID发送给PPPoE Client，从而建立会话，并进入PPPoE Session阶段。

**②Session阶段：**PPPoE Session上的PPP协商和普通的PPP协商方式一致，分为LCP、认证、NCP三个阶段，具体如下：

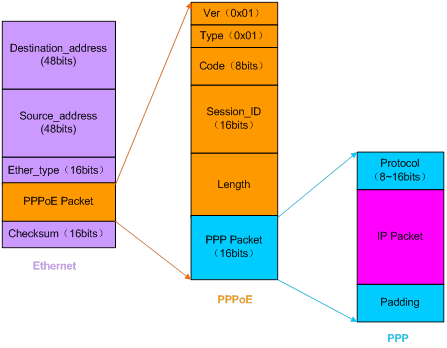
1. LCP阶段主要完成建立、配置和检测数据链路连接。
2. LCP协商成功后，开始进行认证工作，认证协议类型由LCP协商结果（CHAP或者PAP）决定。
3. 认证成功后，PPP进入NCP阶段。NCP是一个协议族，用于配置不同的网络层协议，常用的是IP控制协议（IPCP），它负责配置用户的IP和DNS等工作。

PPPoE Session的PPP协商成功后，其上就可以承载PPP数据报文。

在PPPoE Session阶段所有的以太网数据包都是单播发送的。

**③Terminate阶段：**进入PPPoE Session阶段后，PPPoE Client和PPPoE Server都可以通过发送PADT报文的方式来结束PPPoE连接。PADT报文可以在会话建立以后的任意时刻单播发送。在发送或接收到PADT后，就不允许再使用该会话发送PPP流量，即使是常规的PPP结束数据包也不允许发送。

⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐**PPPoE报文格式**⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐



各个字段解释如下：

**Destination\_address域**：一个以太网单播目的地址或者以太网广播地址（0xffffffff）。在Discovery阶段，该域的值可以是单播或者广播地址，PPPoE Client寻找PPPoE Server的过程使用广播地址，确认PPPoE Server后使用单播地址。在Session阶段，该域的值必须是Discovery阶段已确定的通信对方的单播地址。

**Source\_address域**：源设备的以太网MAC地址。

**Ether\_type**：取值为0x8863表示Discovery阶段或Terminate阶段，0x8864表示Session阶段。

**Ver域**：4bits，PPPoE版本号，值为0x1。

**Type域**：4bits，PPPoE类型，值为0x1。

**Code域**：8bits，PPPoE报文类型，取值包括：

* 0x00，表示会话数据。
* 0x09，表示PADI（PPPoE Active Discovery Initiation）报文。
* 0x07，表示PADO（PPPoE Active Discovery Offer）或PADT（PPPoE Active Discovery Terminate）报文。
* 0x19，表示PADR（PPPoE Active Discovery Request）报文。
* 0x65，表示PADS（PPPoE Active Discovery Session-confirmation）报文。

**Session\_ID域**：16bits，对于一个给定的PPP会话，该值是一个固定值，并且与以太网Source\_address和Destination\_address一起实际地定义了一个PPP会话。值0xffff为将来的使用保留，不允许使用。

**Length域：**16bits，定义PPPoE的Payload域长度。不包括以太网头部和PPPoE头部的长度。

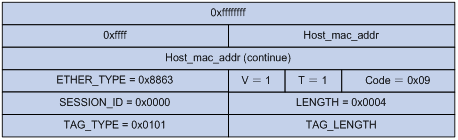
⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐**PADI报文**⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐

PADI报文的主要字段包括：

Code域为0x09。

Session\_ID域为0x0000。

TAG\_TYPE域为0x0101（Service-Name），表明后面紧跟的是服务的名称。有且只有一个TAG\_TYPE为Service-Name的TAG，其他类型的TAG可选。



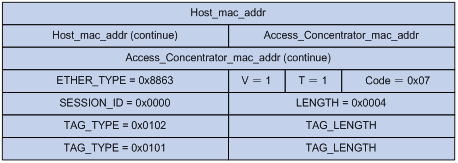
⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐**PADO报文**⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐

PADO报文的主要字段包括：

Code域为0x07。

SESSION\_ID域为0x0000。

TAG\_TYPE域为0x0101（Service-Name），表明后面紧跟的是服务的名称；为0x0102（AC-Name）表明后面紧跟的字符串唯一地表示了某个特定的访问集中器。有且只有一个TAG\_TYPE为AC-Name的TAG，至少一个TAG\_TYPE为Service-Name的TAG。



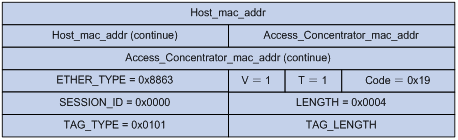
⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐**PADR报文**⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐

PADR报文的主要字段包括：

Code域为0x19。

SESSION\_ID为0x0000。

TAG\_TYPE域为0x0101（Service-Name），表明后面紧跟的是服务的名称。有且只有一个TAG\_TYPE为Service-Name的TAG，其他类型的TAG可选。



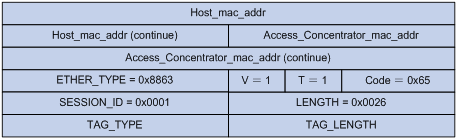
⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐PADS报文⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐

PADS报文的主要字段包括：

Code域为0x65。

SESSION\_ID为Discovery阶段分配的数值。

TAG为可选。



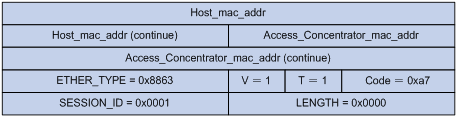
⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐PADT报文⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐

PADT报文的主要字段包括：

Code域为0xa7。

SESSION\_ID域为Discovery阶段分配的数值。

无TAG。



⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐**Wireshark抓pppoe包验证**⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐

**前置条件**

①DUT一台，WAN连接可上行网线，LAN口连接本机

②找到本机对应网卡，确定监听位置

③本机安装wireshark并能检测到DUT对应网卡

**步骤**

**预期输出**

**实际输出**

**结果分析**

**路由器PPPoE功能测试点**

1. DUT作为PPPoE客户端
2. DUT作为PPPoE服务器