⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐**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

当windows client的上网方式是DHCP时，可以通过命令行命令来触发dhcp

**ipconfig /release** #释放所有适配器ipv4地址租约，该命令执行完毕后client无ip地址

ipconfig /release "以太网 3" #释放指定网卡的ipv4地址

ipconfig /release6

ipconfig /release6 "以太网 3"

#ipconfig命令执行后，client会向dhcp server发出请求租用一个ip地址，一般情况下会获得和原来一样的ip地址，只有原有地址被占用的情况下会获得新的ip地址

#更新所有适配器ipv4、6地址租约

**ipconfig /renew**

ipconfig /renew6

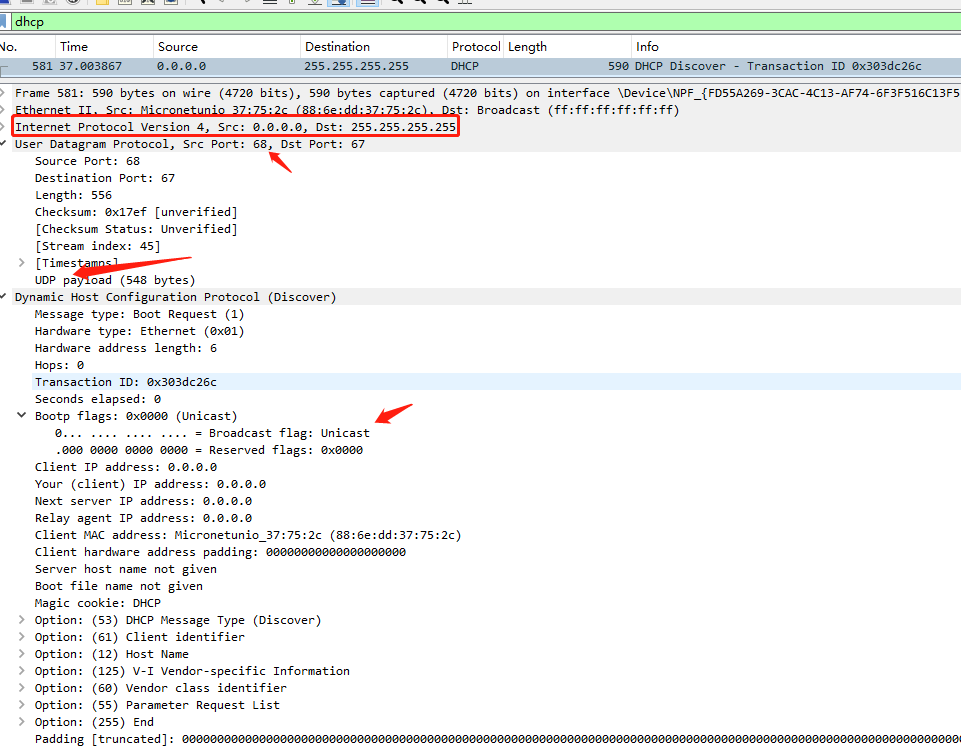
#更新指定适配器ipv4、6地址租约

ipconfig /renew “以太网 3”

ipconfig /renew6 “以太网 3”

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

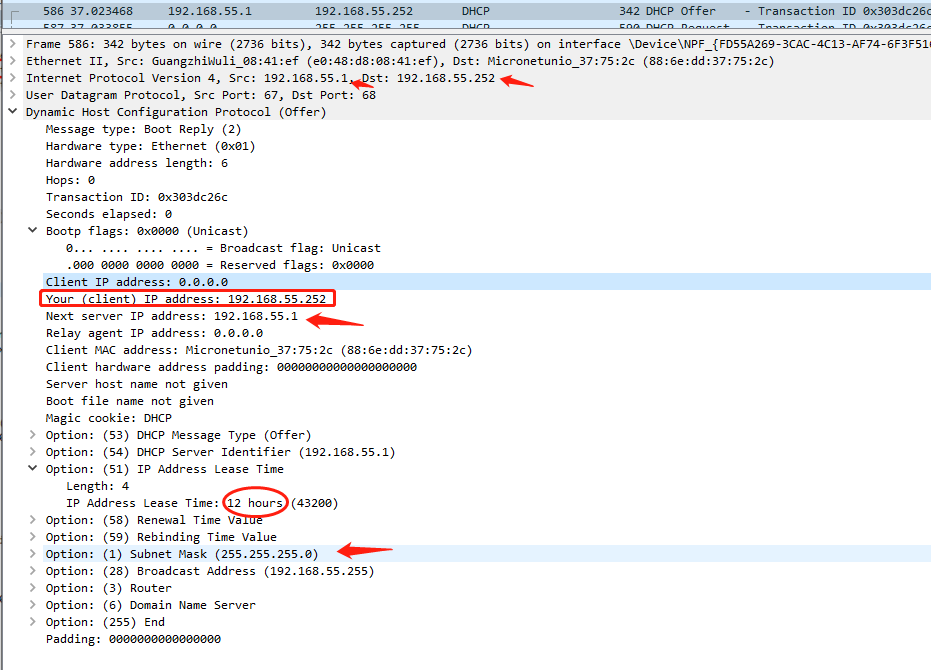


Offer报文分析

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

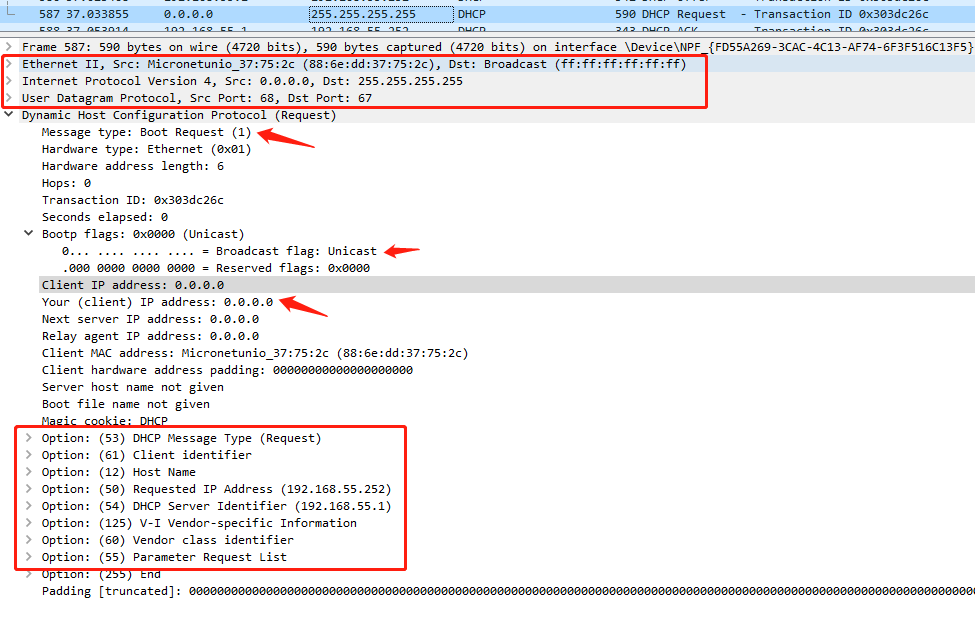
③Client只收到了一个Offer



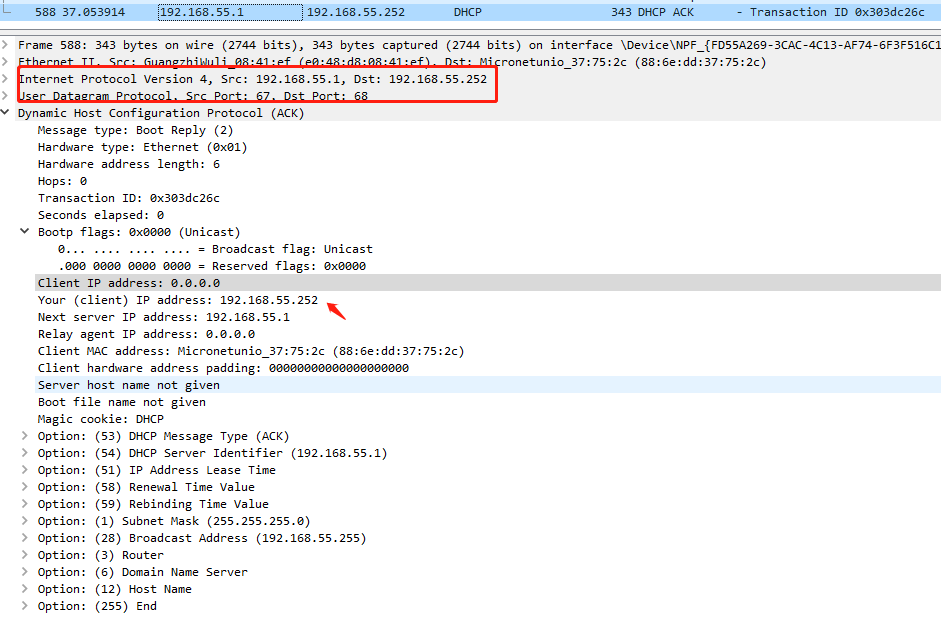
Request报文分析

①广播发送，IP地址仍为0.0.0.0

**如果环境中存在多个dhcp server给client发送offer报文，client一般会选择第一个收到的offer，然后广播通知所有dhcp server，告知它的选择**



Ack报文分析



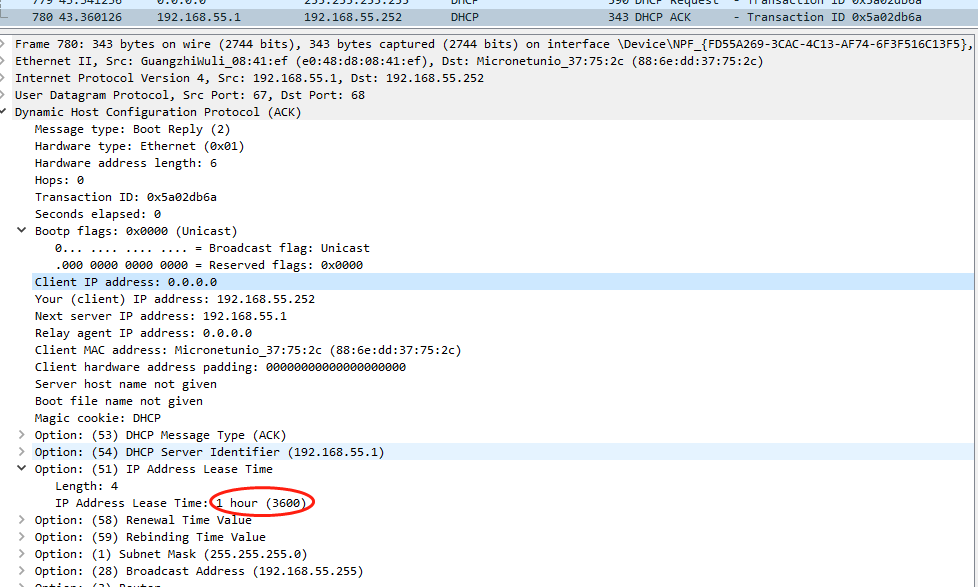
DUT作为DHCP客户端，实际连接拓扑图如上，现验证“**DHCP客户端更新租期**”

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

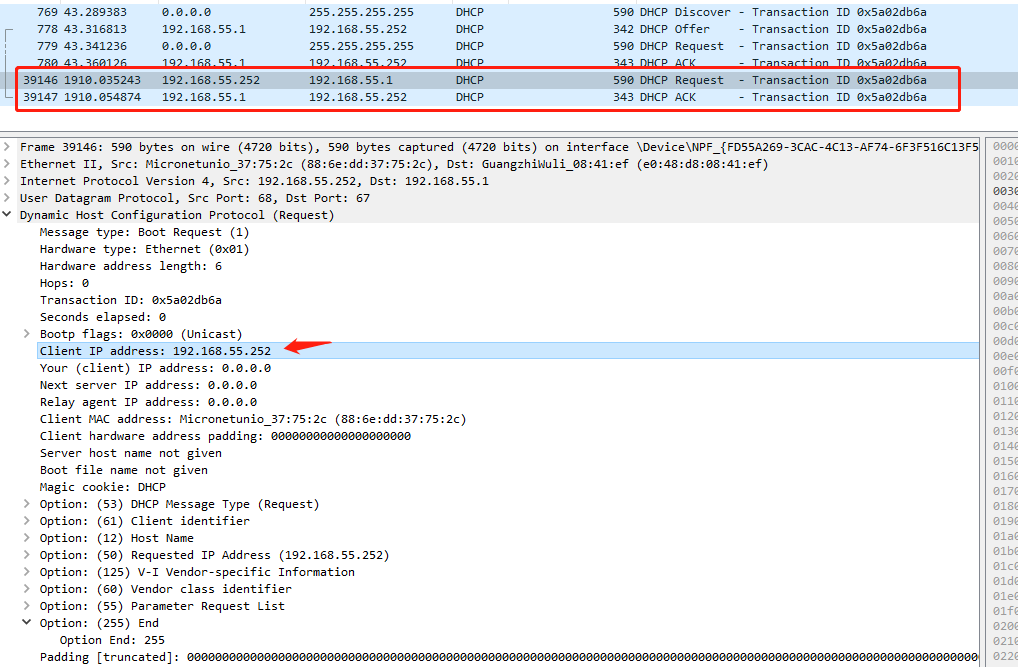
1. 将DUT 上网方式设置为“静态IP”
2. 开启wireshark，开始抓包
3. 将DUT上网方式设置为“DHCP”，等待半小时
4. 验证抓包，筛选dhcp包

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

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

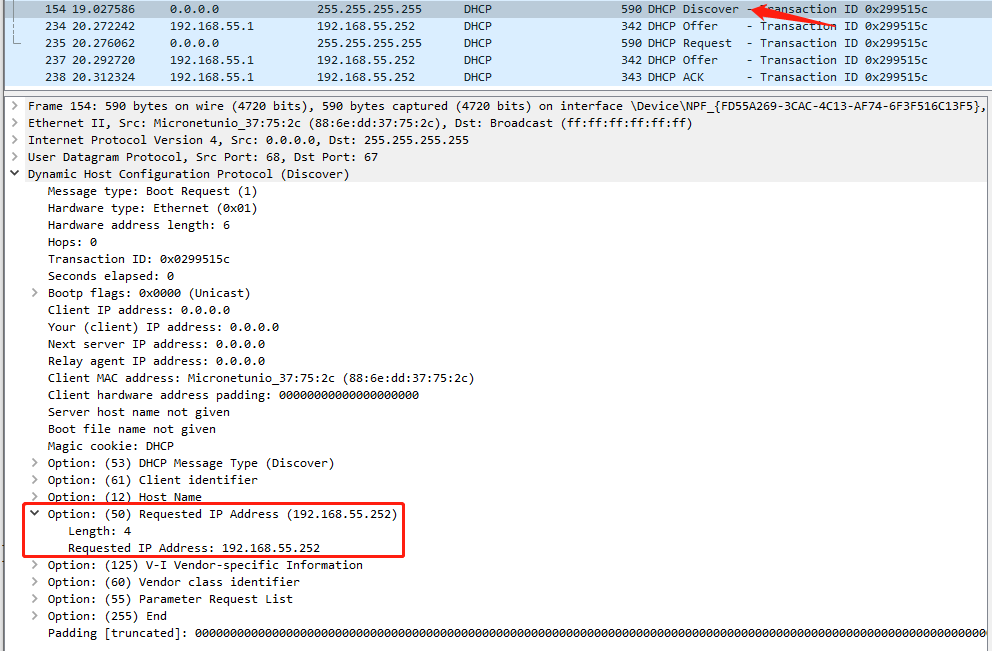
DUT作为DHCP客户端，实际连接拓扑图如上，现验证“**DHCP客户端重用曾经使用过的地址”**

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

断开DUT超过1小时后重连



超过租期重连的情况下，再次DHCP，依旧会发生四报文交互，但Discover报文携带Option 50，即客户端期望获取的IP地址

ip冲突实验

说明

DUT 配置

上网方式为DHCP

PC配置

PC上网方式设置为“静态IP”

DHCP Server

DUT

PC

步骤：1、DUT配置为DHCP，获得的ip地址为：192.168.55.252 2、在DUT再次续租之前，将PC的ip地址设置为192.168.55.252

**PC：ip地址分配不成功，查看分配的ip地址为：169.254.4.87**

IP地址169.254.x.x常用于网络配置出现问题时自动分配给计算机的地址，这一范围的IP地址为APIPA（自动私有IP寻址）地址。它使设备能够与同一子网内的其他计算机通讯，但不能连接外部网络。

详细描述：当计算机试图通过DHCP从网络服务器获取IP地址但失败时，操作系统会自动生成一个169.254.x.x范围内的IP地址。此措施保证即便没有获得网络管理员分配的IP地址，计算机在本地网络仍保持通信能力。

1. 将DUT的ip地址释放：ifconfig eth0 0.0.0.0，该命令表示将eth0的IP地址设置为零，表示释放当前分配的IP地址，可通过ipconfig命令查看释放情况。
2. PC静态配置：192.168.55.252
3. DUT重新获取ip地址

**PC：ip地址分配成功，查看分配的ip地址为：192.168.55.252**

**DUT：获得新地址，查看获得的ip地址为：192.168.55.122**

原因：dhcp server并没有检测ip冲突的功能，而是dhcp client拿到dhcp server分配的ip地址后会进行冲突检测，若发现有ip冲突，则会向dhcp server发送Decline报文，告知其分配的ip不可用，请求重新分配ip。而server则会将此地址列为冲突地址。当服务器没有空闲地址可分配时，再选择冲突地址进行分配

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

WAN口

说明

DUT 配置

LAN口为镜像端口

WAN口为被镜像口

PC配置

PC上网方式设置为“DHCP”

DUT

DHCP Relay

LAN口

DHCP Client

PC

目标：抓取DHCP Client和DHCP Relay之间的收发包以及DHCP Relay和DHCP Server之间的收发包

抓包步骤如下

1. DUT配置DHCP中继

注明：本司路由器无DHCP中继功能，故此实验搁浅

DUT作为DHCP服务器，实际连接拓扑图如下，现验证“无中继时为客户端分配IP”

DUT

PC

Internet

LAN口

WAN口

DHCP Client

DHCP Server

说明

DUT 配置

DHCP地址池：192.168.11.100~192.168.11.200

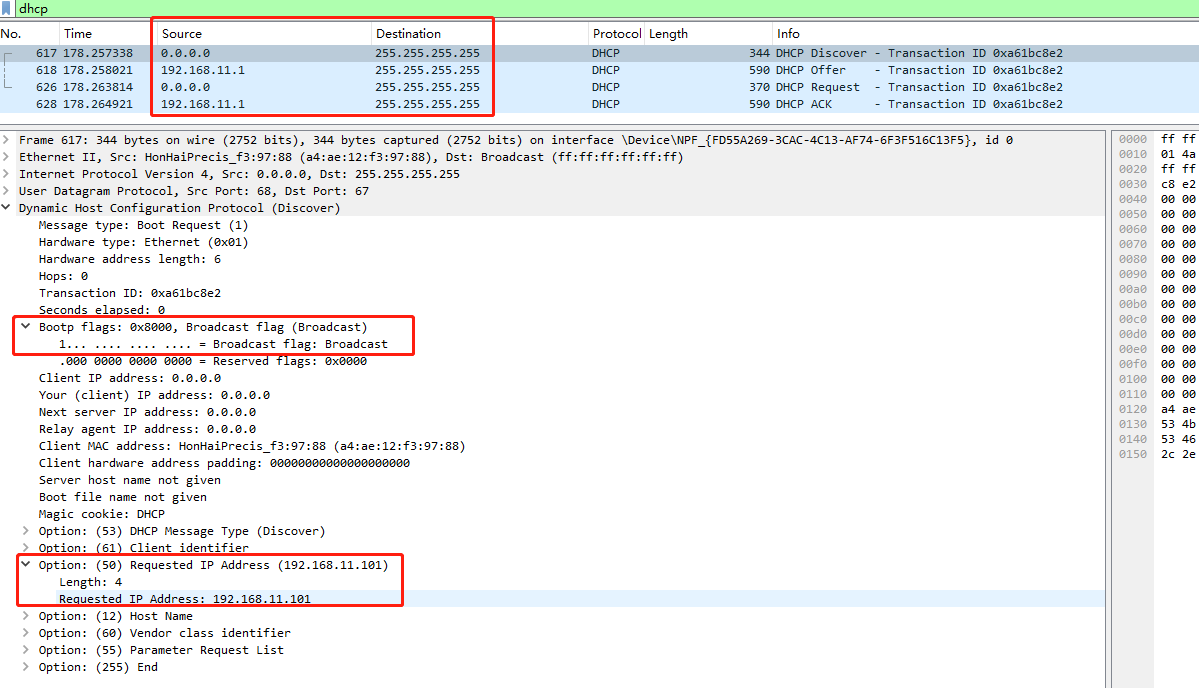
租期时长：20分钟

目标：抓取PC和DUT之间的DHCP数据包

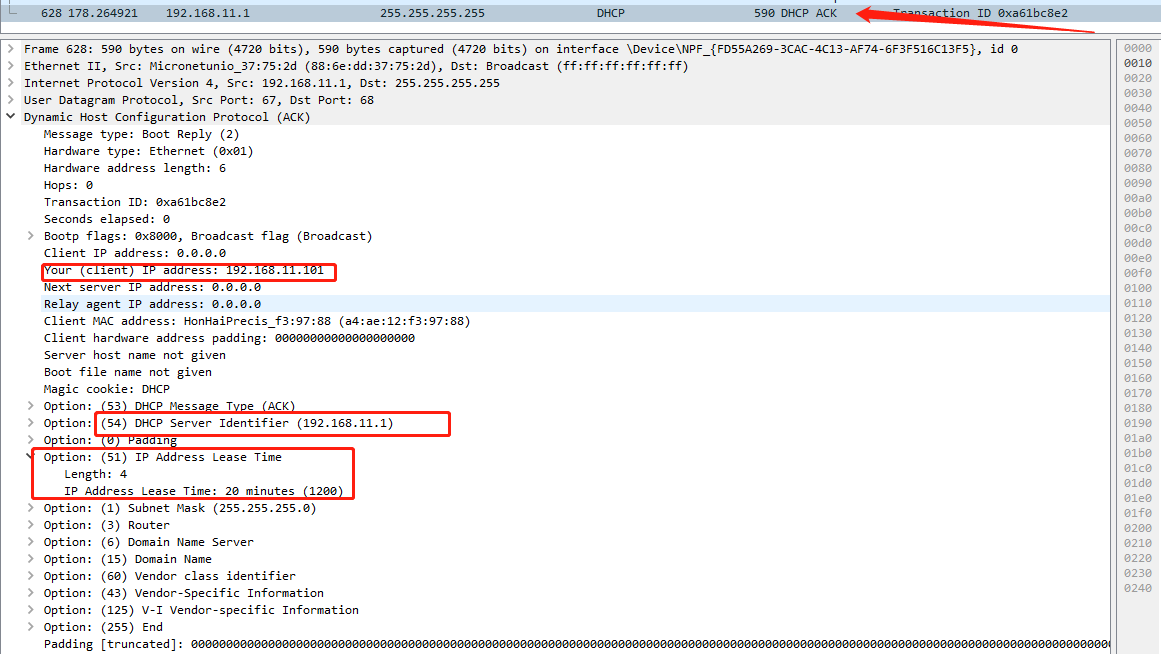
抓包步骤

1. 打开PC的wireshark，选定连接DUT的网口，点击开始捕获
2. PC上网方式从“静态IP”切换为“DHCP”
3. 等待一段时间后wireshark筛选DHCP数据包，查看抓包情况

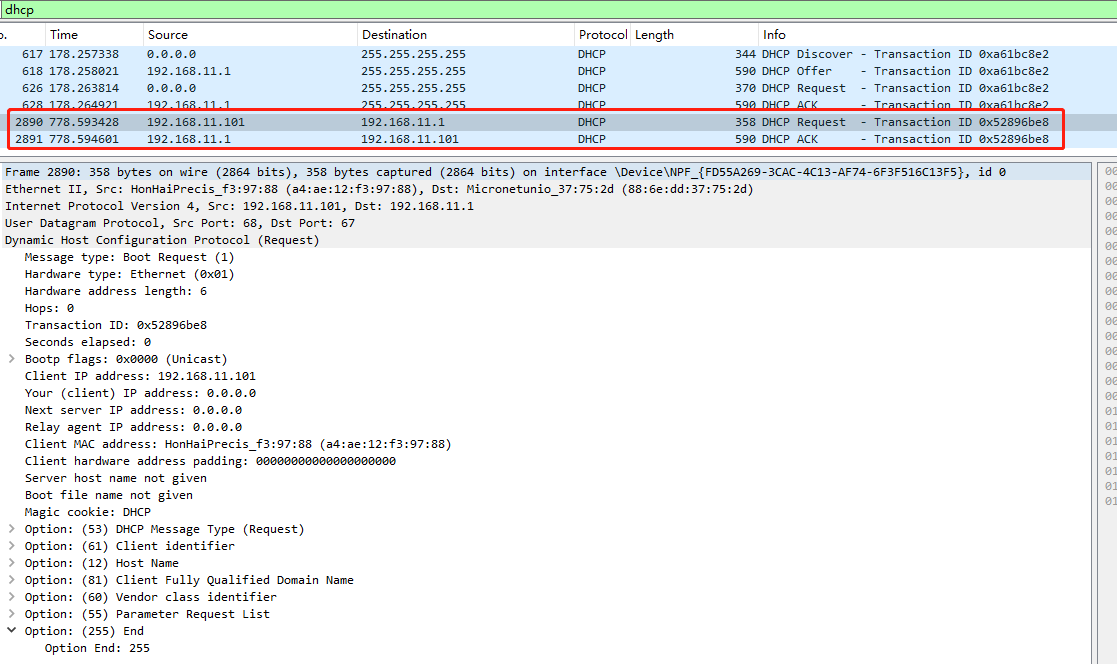
如下图：四报文交互，均以广播形式发送，Discover报文携带上次使用的IP



期望IP分配成功，租期为20分钟



等待50%的租期时间，即10分钟后，单播申请更新租期



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

**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

PPPoE Client

PC

DUT

Switch

说明

Switch配置

恢复默认设置，不设置镜像端口

DUT 配置

LAN2口为镜像端口

WAN口为被镜像口

PPPoE Server

1号口

2号口

WAN口

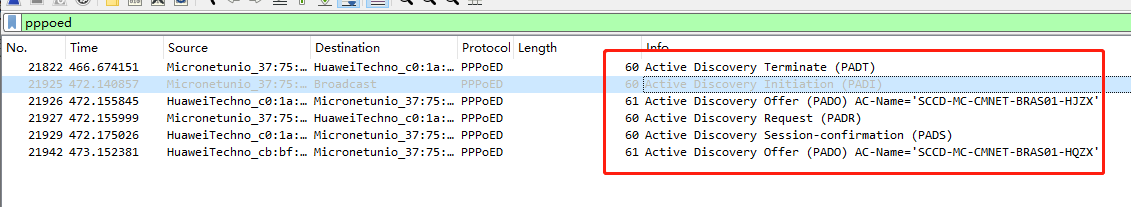
LAN2口

目标：抓取DUT拨号的包，即WAN口的收发包

抓包步骤如下：

1. DUT工作在路由模式，配置端口镜像
2. Wireshark选择正确的网络接口，开始捕获
3. DUT进行PPPoE拨号
4. 筛选出”pppoe”的包

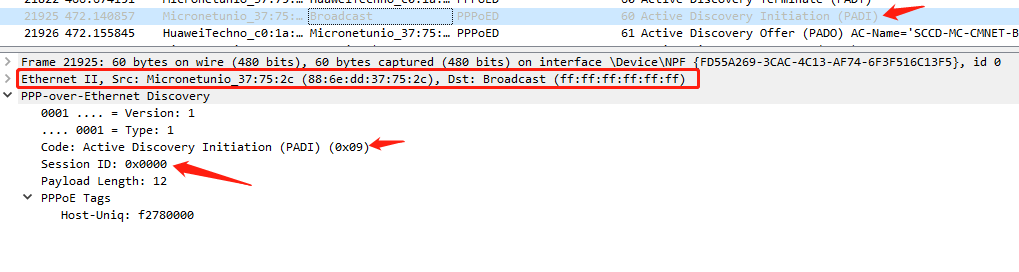
结果分析

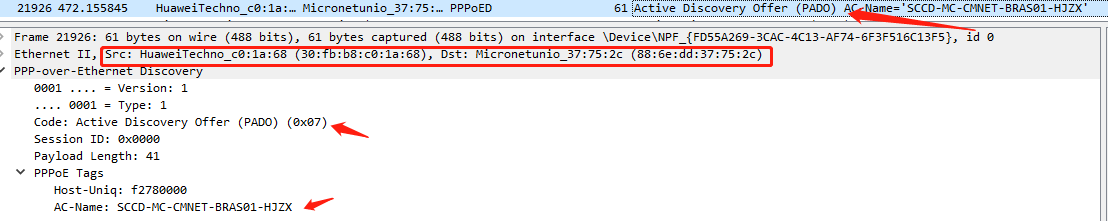


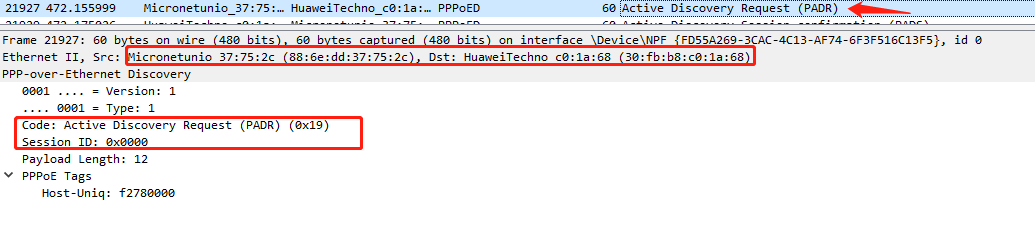
PPPoE协商过程分为三阶段：Discover，Session，Teminate

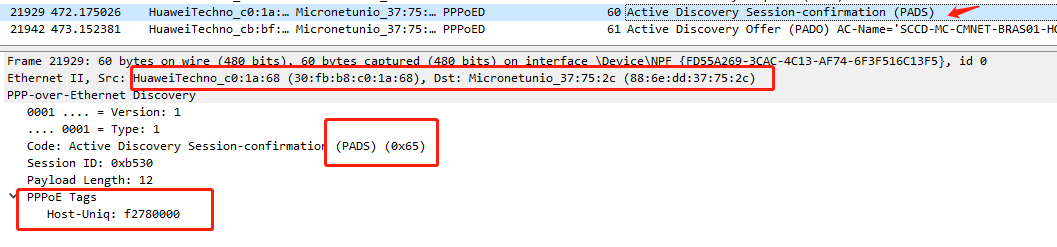
如上图所示

**Discover阶段**：PADI、PADO、PADR、PADS

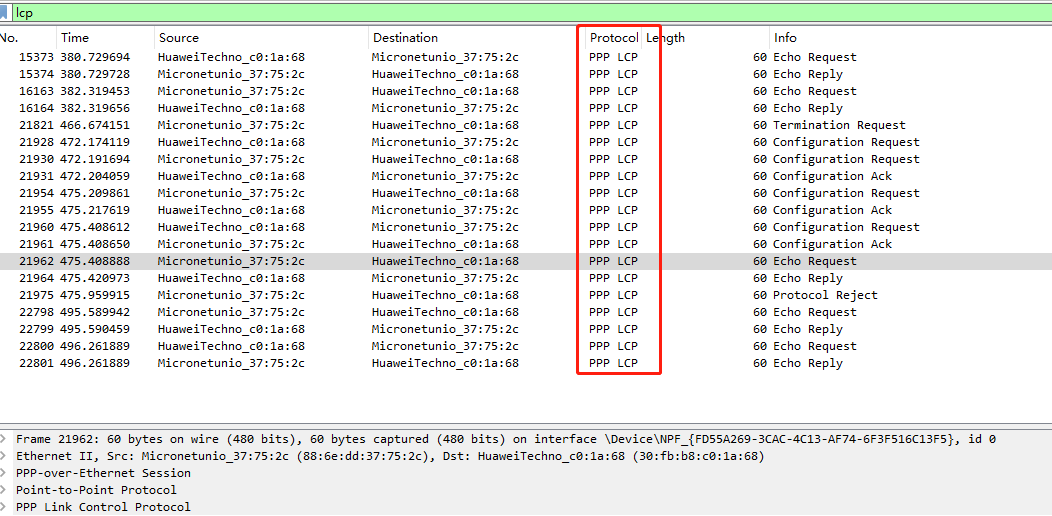




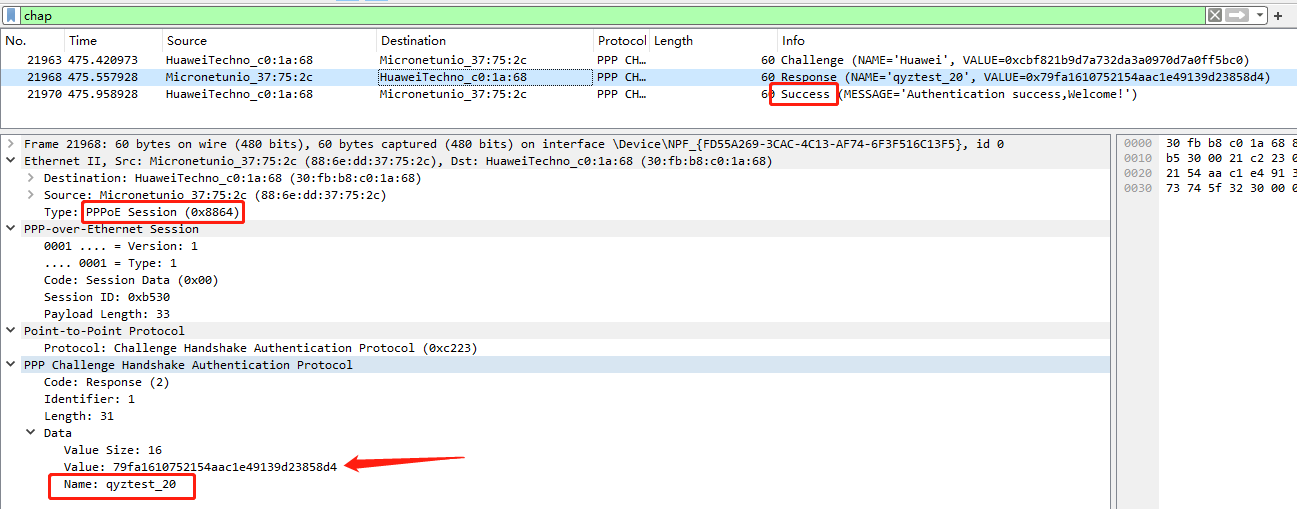




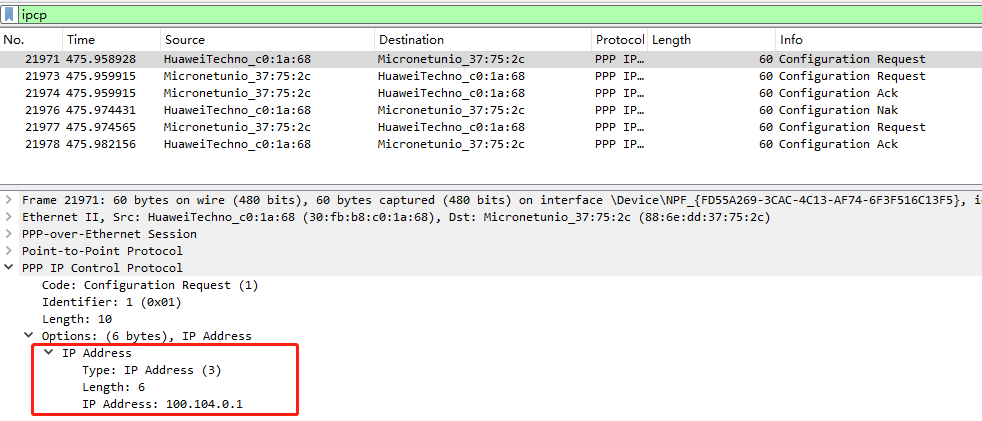
**Session阶段**：LCP阶段主要完成建立、配置和检测数据链路连接，完成这个阶段即协商成功

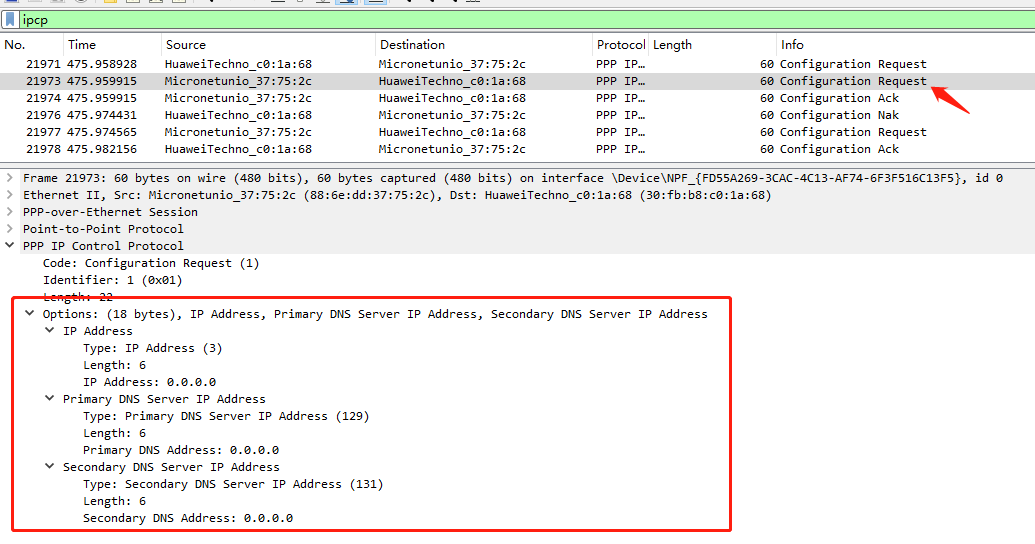


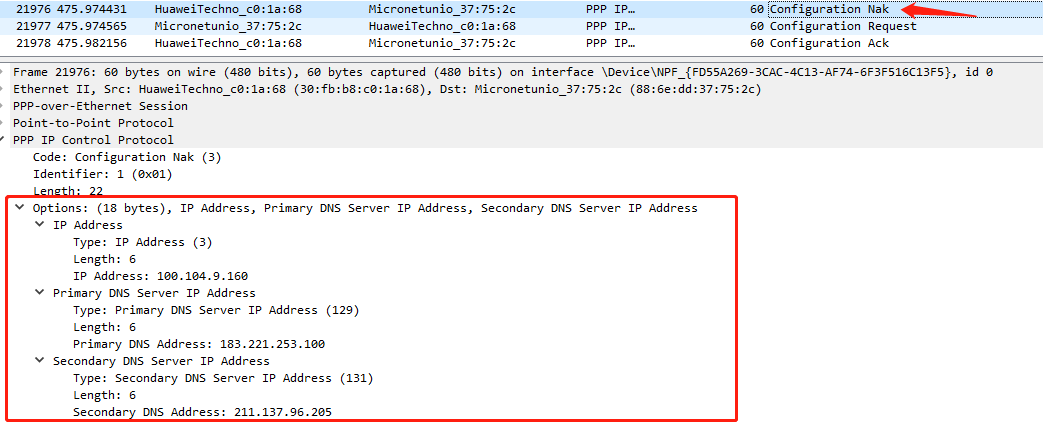
**Session阶段**：CHAP阶段进行认证工作，认证协议类型由LCP协商结果决定

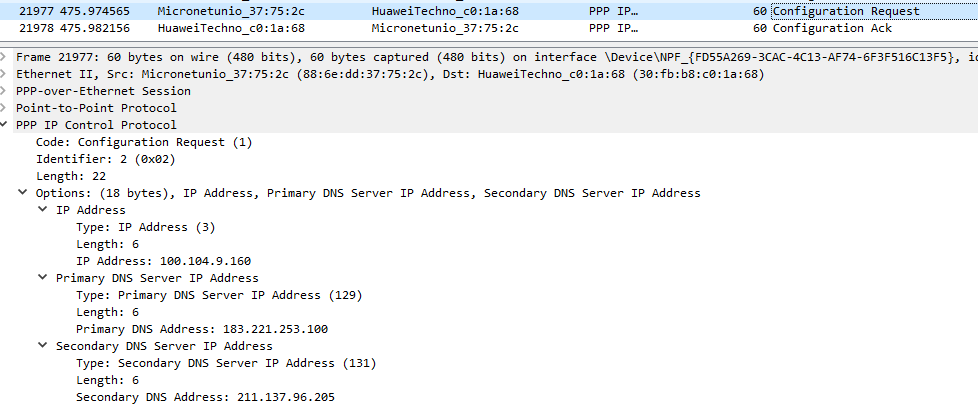


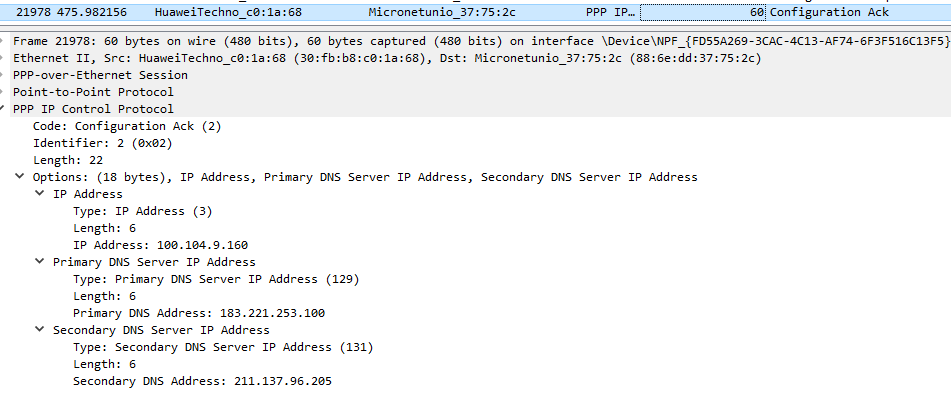
**Session阶段**：认证成功后，PPP进入NCP阶段。NCP是一个协议族，用于配置不同的网络层协议，常用的是IP控制协议（IPCP），它负责配置用户的IP和DNS等工作



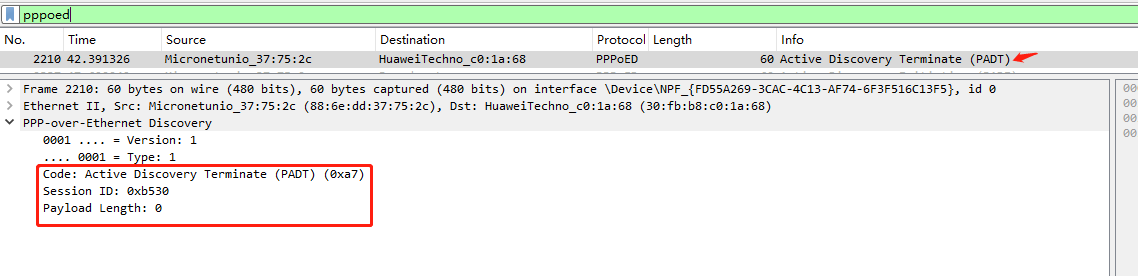








**Terminate阶段：**进入PPPoE Session阶段后，PPPoE Client和PPPoE Server都可以通过发送PADT报文的方式来结束PPPoE连接。PADT报文可以在会话建立以后的任意时刻单播发送。在发送或接收到PADT后，就不允许再使用该会话发送PPP流量，即使是常规的PPP结束数据包也不允许发送。



⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐**Wireshark抓DNS包验证**⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐

**路由器DNS功能测试点**

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

DNS Server

192.168.55.1

192.168.55.252

WAN口

说明

DUT 配置

LAN3口为镜像端口

WAN口为被镜像口

DNS Client

DUT

192.168.11.1

LAN3口

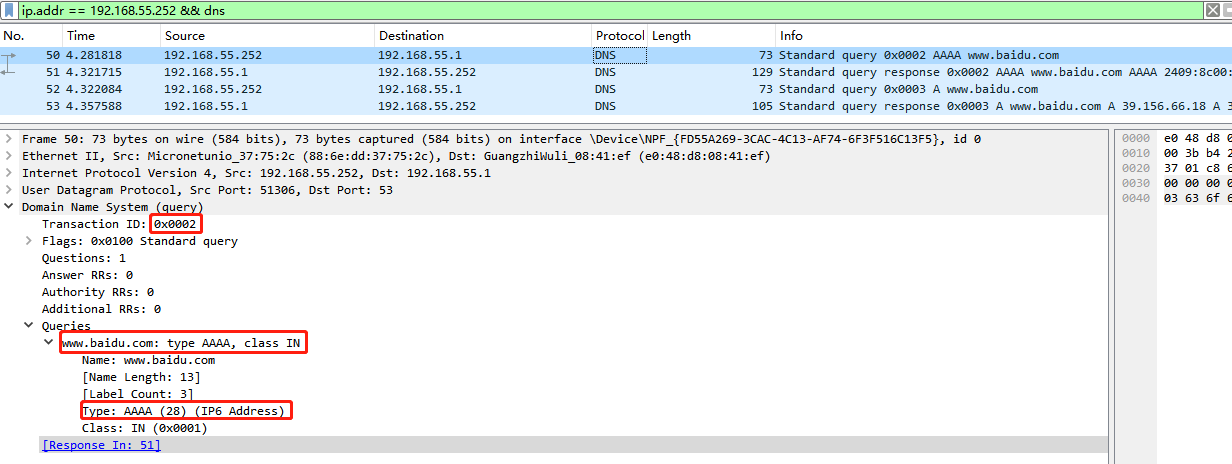
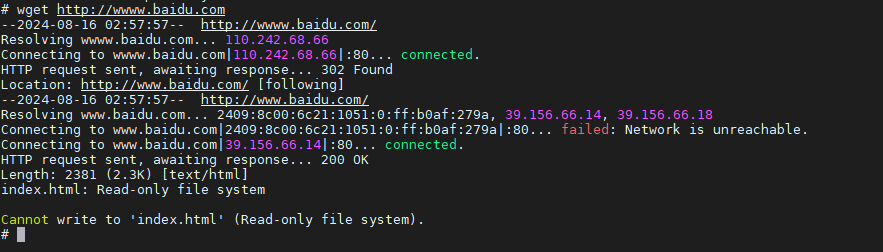
192.168.11.101

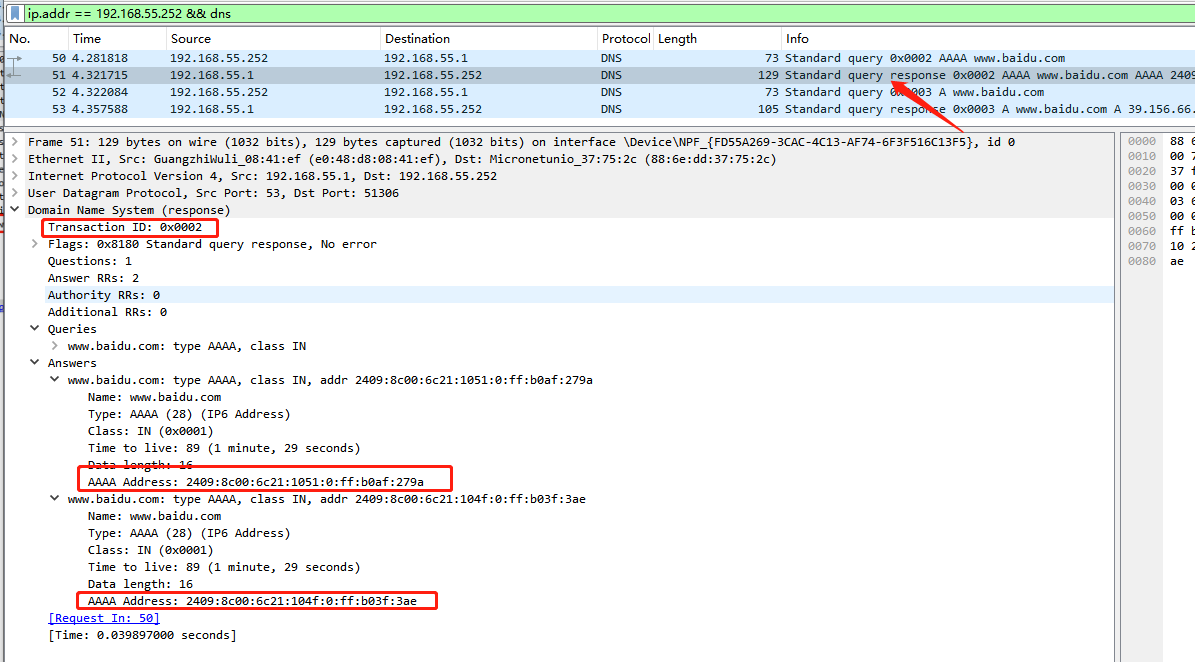
PC

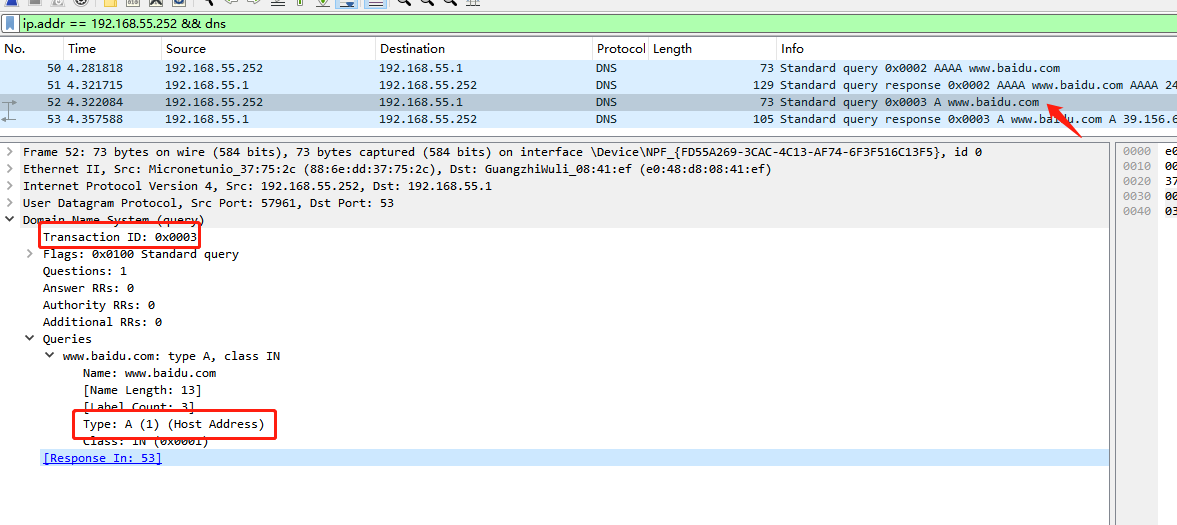
目标：DUT作为DNS客户端，在PC上抓取DUT与DNS Server交互的DNS报文

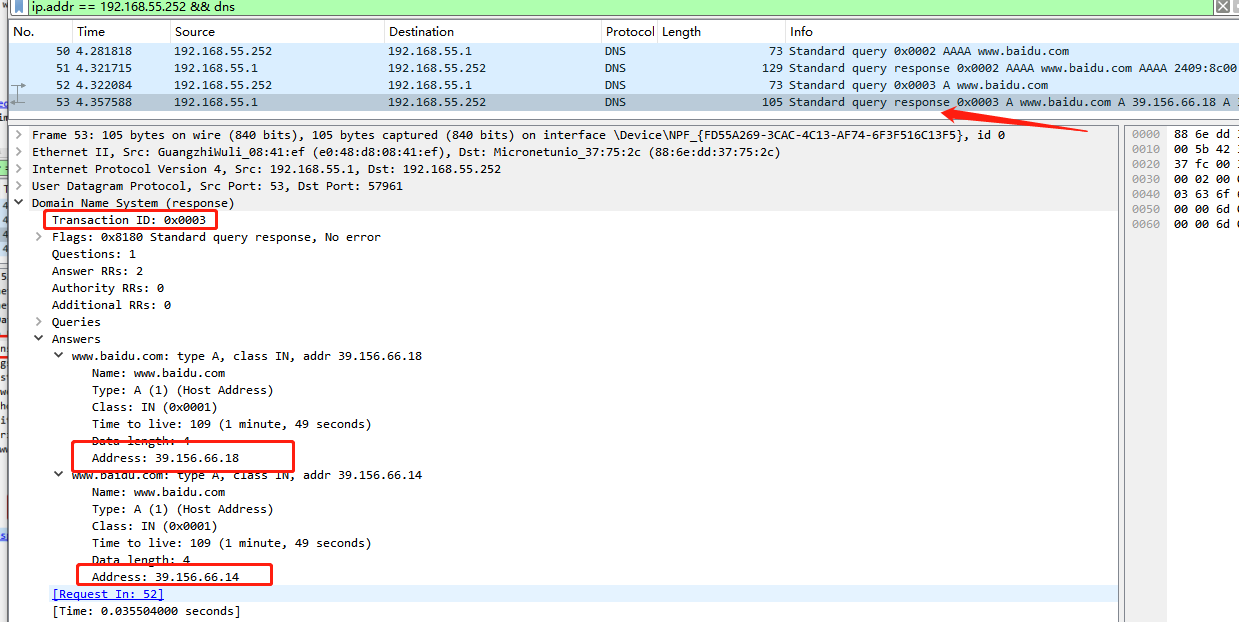
1. DUT工作在路由模式，配置端口镜像
2. Wireshark选择正确的网络接口，开始捕获
3. 在DUT上执行“wget [http://www.baidu.com](http://www.baidu.com/)”的命令，该命令表示访问百度首页并下载该页面到本地
4. Wireshark筛选出”DNS && ip.addr==192.168.55.252 ”的包

根据以下抓到的信息可以看到，DUT发起了两次DNS解析，分别解析了域名“baidu.com”的IPv4地址和IPv6地址

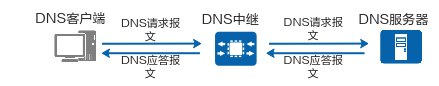








**DNS中继**

当DNS服务器的IP地址发生变化时，用户网络中每个DNS客户端上的配置都需要改变，这样工作量极大并且容易出错。此时，可以通过部署DNS中继解决该问题。DNS客户端上配置DNS中继的IP地址，DNS服务器的IP地址在DNS中继上配置。之后，DNS客户端会将DNS请求报文直接发送给DNS中继，由DNS中继将收到的DNS请求报文转发至DNS服务器。由此，当DNS服务器的IP地址发生变化时，仅需改变DNS中继上的配置即可，简化了网络管理。DNS中继的工作原理如下图所示。

DNS中继的工作原理

DNS客户端将DNS请求报文发送给DNS中继，即请求报文的目的地址为DNS中继的IP地址。

DNS中继收到请求报文后，将报文转发给DNS服务器，通过DNS服务器进行域名解析。

DNS Server

192.168.55.1

说明

DUT 配置

LAN3口为镜像端口

WAN口为被镜像口

192.168.55.252

DNS 中继

DUT

192.168.11.1

DNS Client

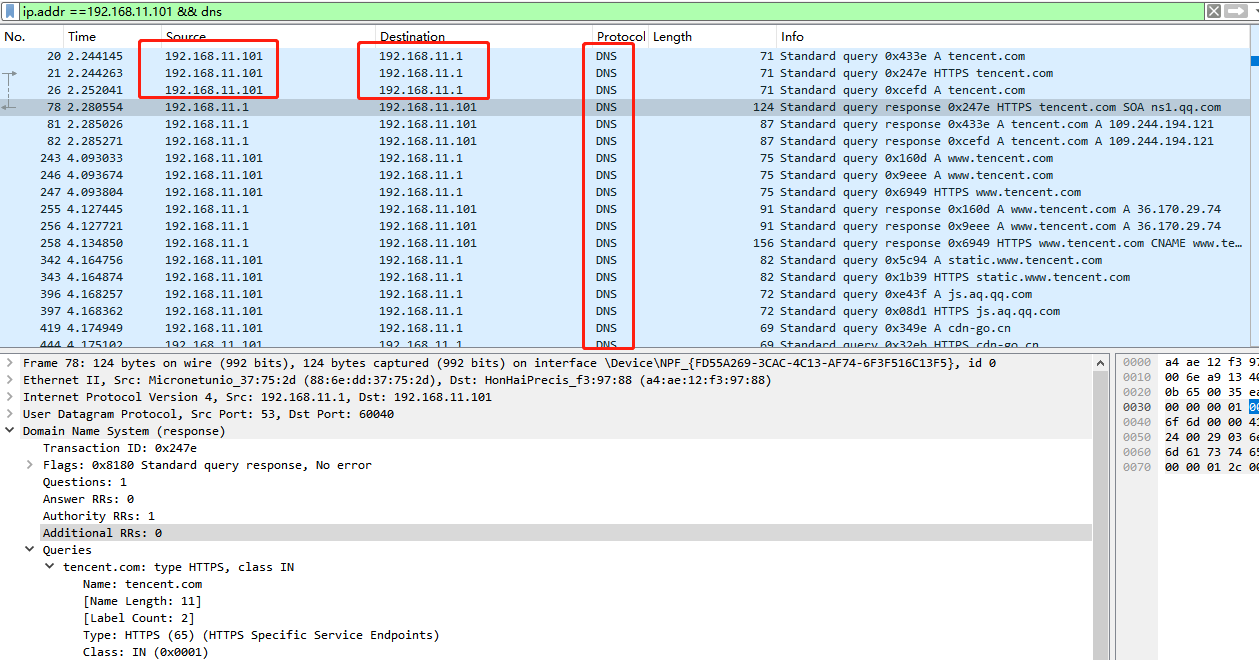
PC

192.168.11.101

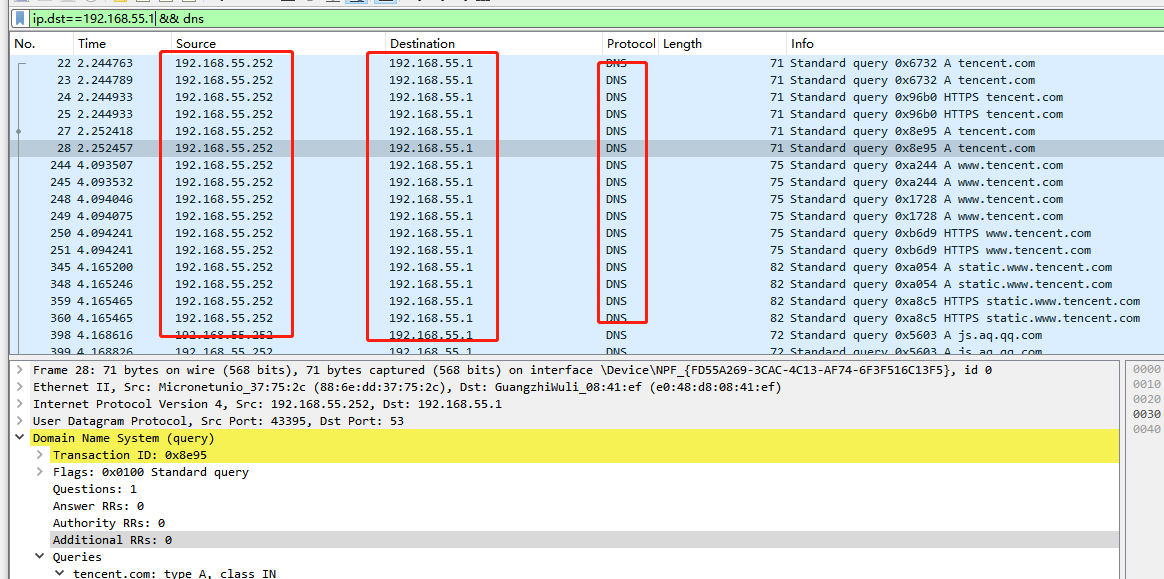
目标：DUT作为DNS中继，抓取DUT与DNS Server交互，PC与DUT交互的DNS报文

1. DUT工作在路由模式，配置端口镜像
2. Wireshark选择正确的网络接口，开始捕获
3. 在PC上访问“[http://www.tencent.com](http://www.baidu.com/)”的命令
4. Wireshark筛选出”DNS && ip.addr==192.168.55.252 ”的包

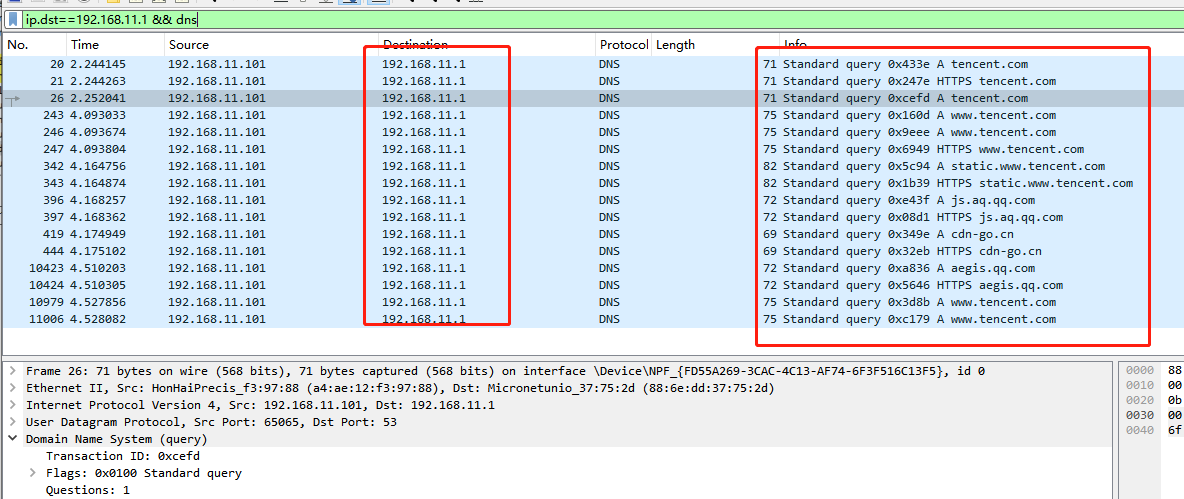
PC和DUT的交互包

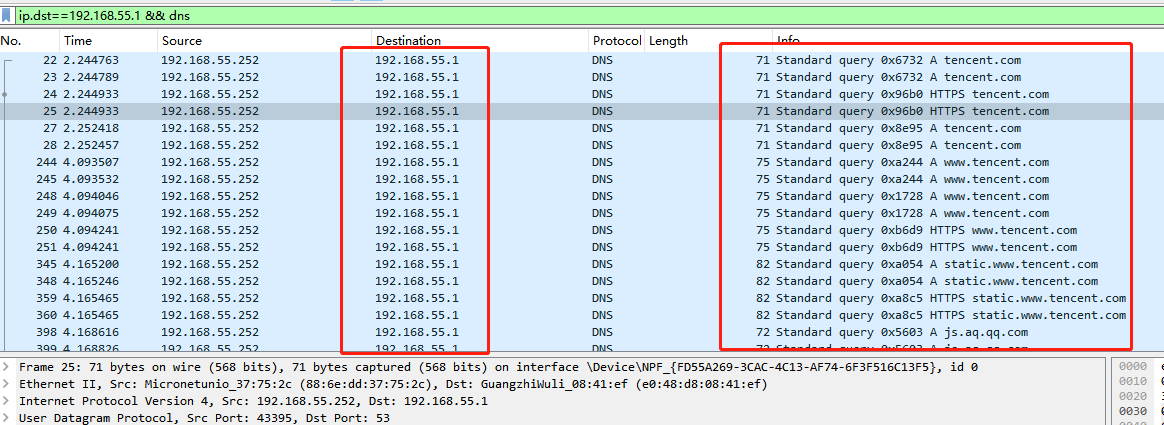


DUT和DNS Server的DNS交互包

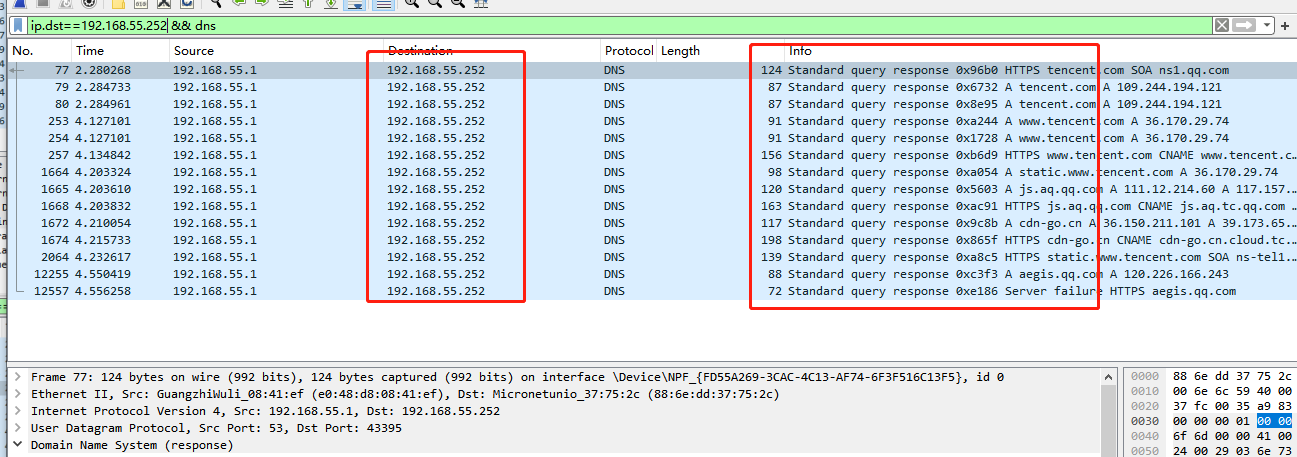


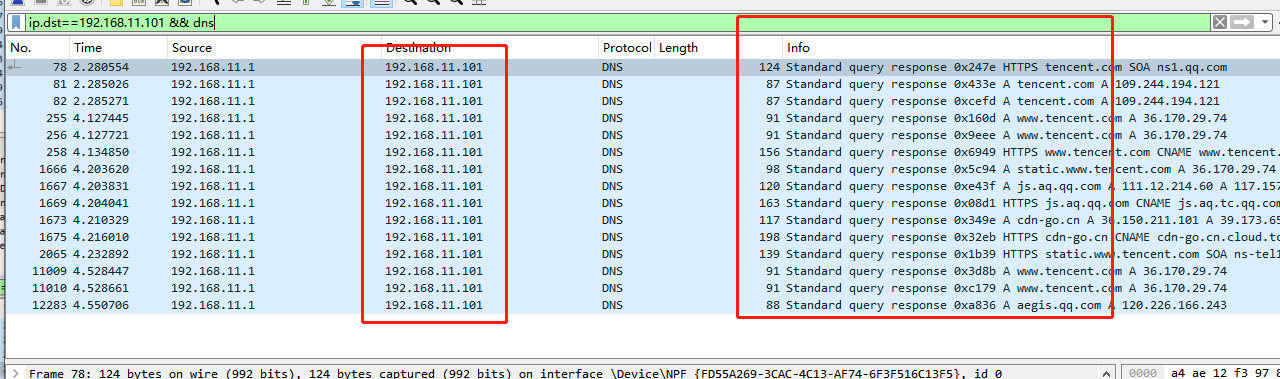
DNS查询包：PC发给DUT，DUT发给DNS Server





DNS回应包：DNS Server发给DUT，DUT发给PC





Internet

说明

DNS Server

DUT

192.168.11.1

DNS Client

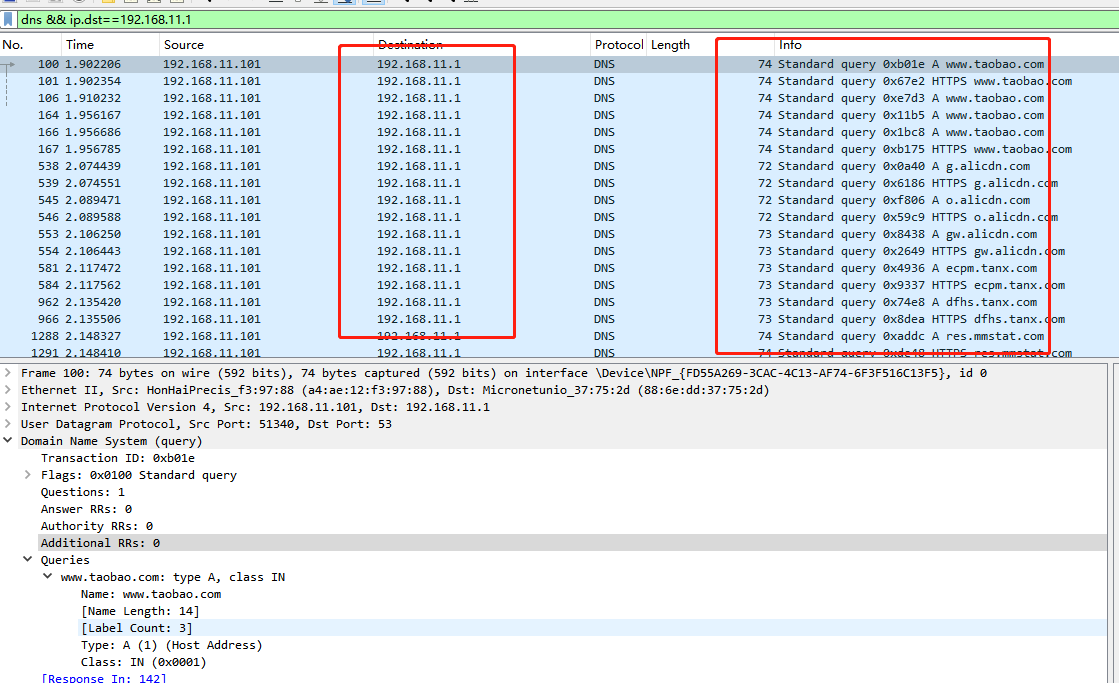
192.168.11.101

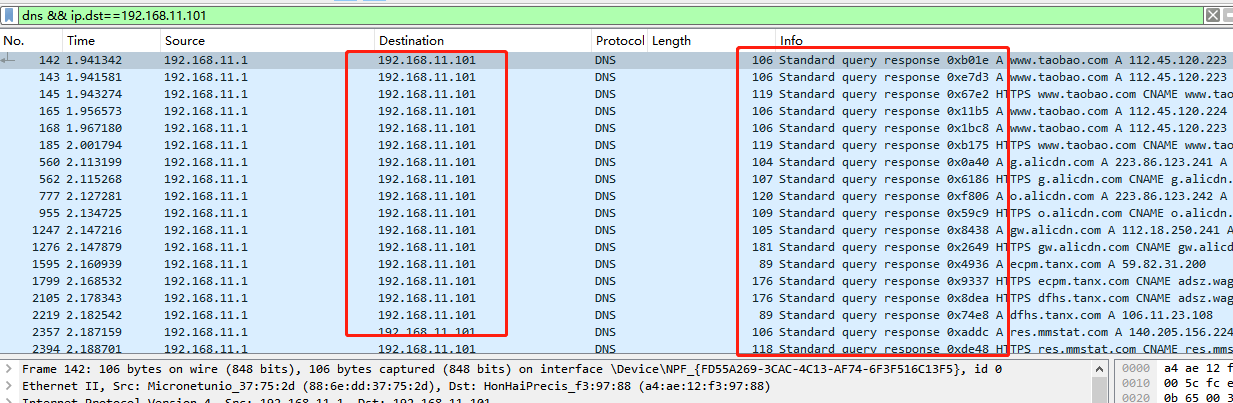
PC

目标：DUT作为DNS Server，抓取PC与DUT交互的DNS报文

抓包步骤

1. DUT工作在路由模式
2. Wireshark选择正确的网络接口，开始捕获
3. 在PC上访问“[http://www.taobao.com](http://www.baidu.com/)”的命令
4. Wireshark筛选出”DNS && ip.dst==192.168.11.1/192.168.11.101 ”的包





⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐**Wireshark抓ICMP包验证**⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐

**路由器ICMP功能测试点**

1. DUT的ping功能
2. DUT的tracert功能

ICMP并不是高层协议，而是IP层的协议，ICMP报文封装在IP数据报中，作为其中的数据部分

首部

数据部分

Internet

192.168.55.252

说明

DUT配置

WAN口为被镜像端口

LAN口为镜像端口

DUT

192.168.11.1

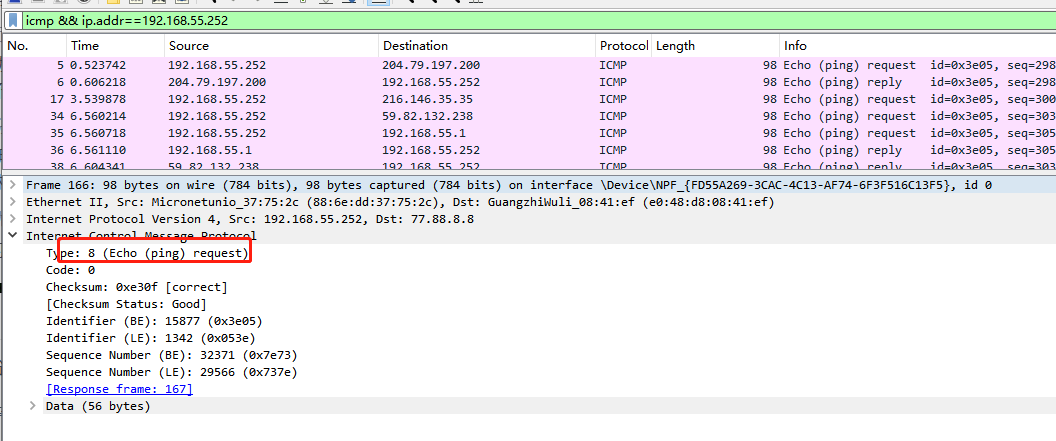
192.168.11.101

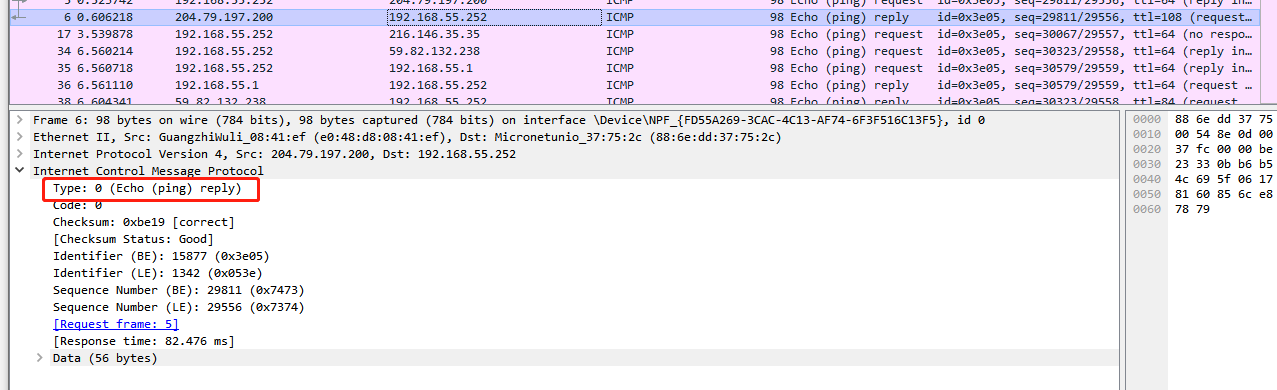
PC

目标：测试DUT的ping功能

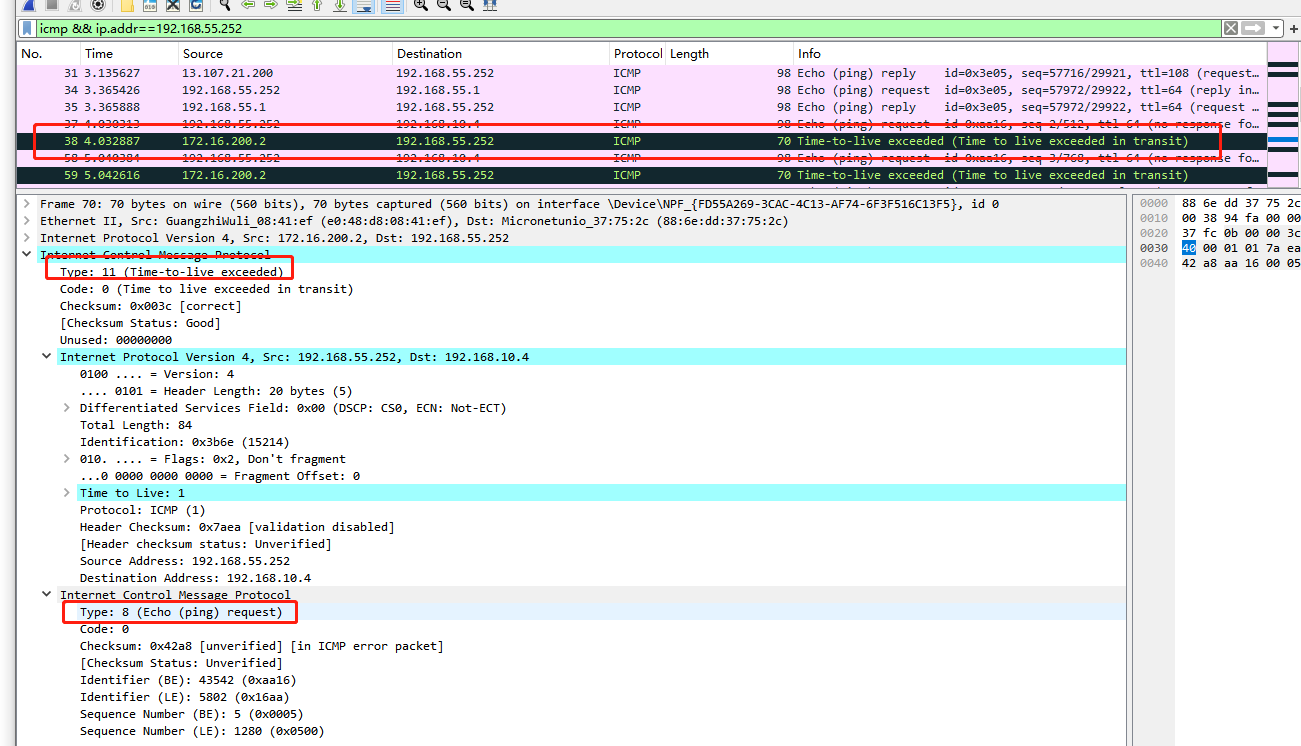
1. DUT工作在路由模式，并配置端口镜像，使得PC可以监控DUT-WAN口的数据包
2. Wireshark选择正确的网络接口，开始捕获
3. 在DUT管理网页上，测试ping功能（ping tencent.com）；在DUT控制端口执行”ping 192.168.10.4（到该地址有环）”
4. Wireshark筛选出”icmp && ip.addr==192.168.55.252 ”的包

抓取回送请求报文和回答报文，类型为8、0





抓取差错报告报文--时间超过，所构造的目的地址有环



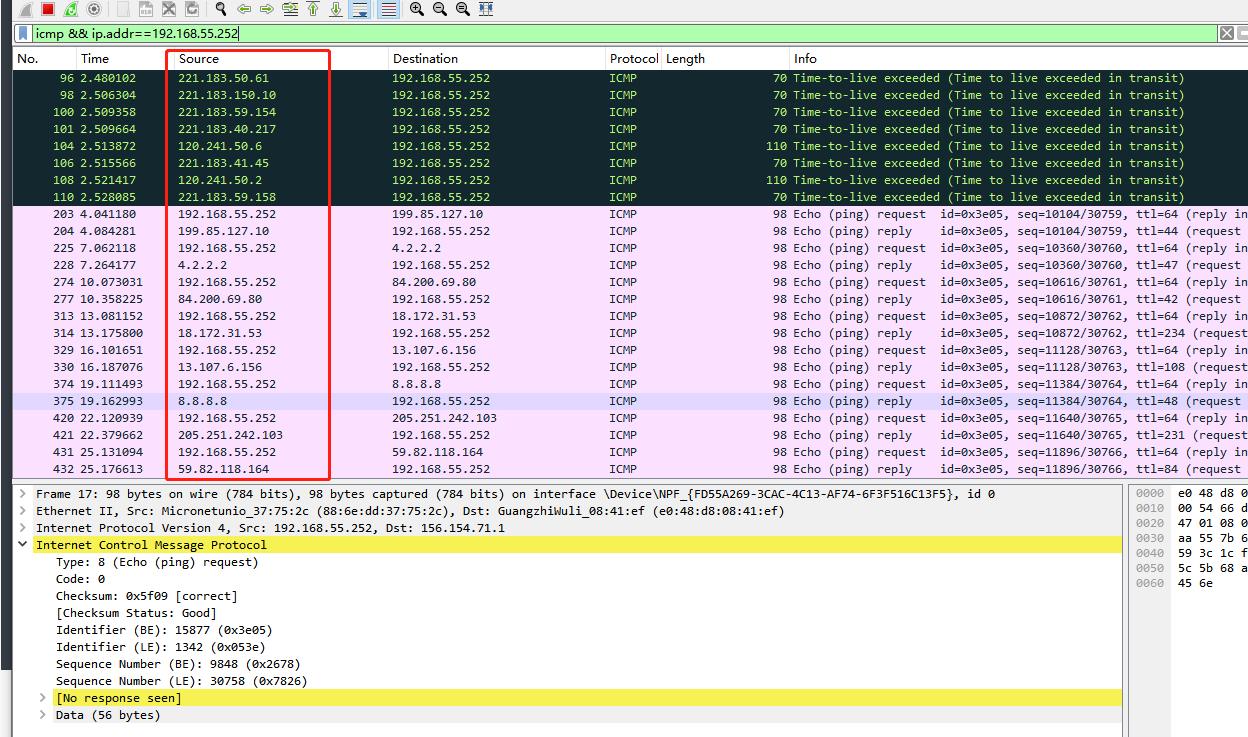
目标：测试DUT的tracert功能

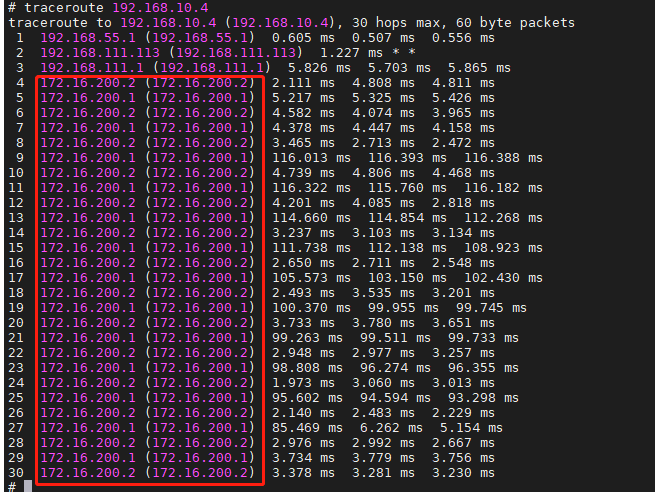
1. DUT工作在路由模式，并配置端口镜像，使得PC可以监控DUT-WAN口的数据包
2. Wireshark选择正确的网络接口，开始捕获
3. 在DUT管理网页上，测试tracert功能（tracert tencent.com）；在DUT控制端口执行”traceroute 192.168.10.4（到该地址有环）”
4. Wireshark筛选出”icmp && ip.addr==192.168.55.252 ”的包

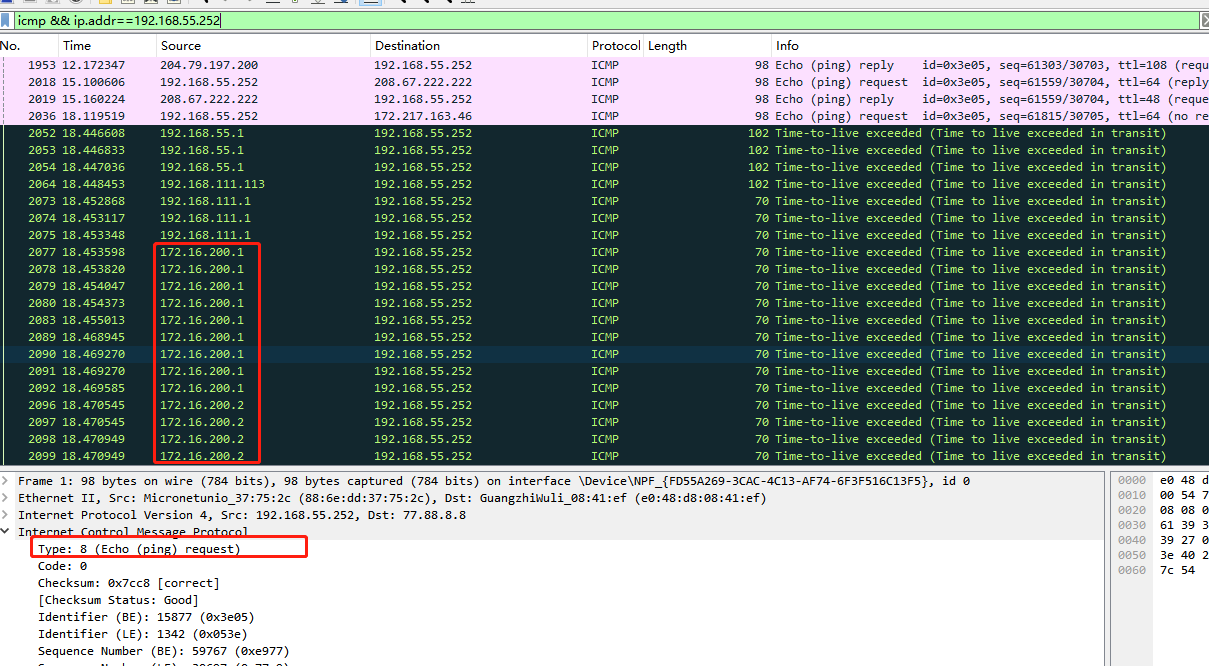
在执行traceroute路由追踪命令的时候，检测发出数据包的主机到目标主机之间所经过的网关数量的工具。traceroute的原理是试图以最小的TTL（存活时间）发出探测包来跟踪数据包到达目标主机所经过的网关，然后监听一个来自网关ICMP的应答。

原理：程序利用增加存活时间（TTL）来实现其功能。每当数据包(3个数据包包括源地址，目的地址和包发出的时间标签)经过一个路由器，其存活时间就会减1。当其存活时间是0时，主机便取消数据包，并传送一个ICMP（Internet控制报文协议。它是TCP/IP协议族的一个子协议，用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。） TTL数据包给原数据包的发出者。

traceroute程序完整过程：首先它发送一份TTL字段为1的IP数据包给目的主机，处理这个数据包的第一个路由器将TTL值减1，然后丢弃该数据报，并给源主机发送一个ICMP报文（“超时”信息，这个报文包含了路由器的IP地址，这样就得到了第一个路由器的地址），然后traceroute发送一个TTL为2的数据报来得到第二个路由器的IP地址，继续这个过程，直至这个数据报到达目的主机。







⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐**Wireshark抓ARP包验证**⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐

**路由器ARP功能测试点**

1. DUT的ARP功能

Router

192.168.55.1

e0:48:d8:08:41:ef

192.168.55.252

88-6E-DD-37-75-2C

说明

DUT配置

WAN口为被镜像端口

LAN口为镜像端口

DUT

192.168.11.1

88-6E-DD-37-75-2D

192.168.11.101

97:88 (a4:ae:12:f3:97:88)

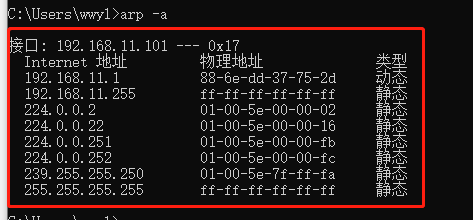
PC

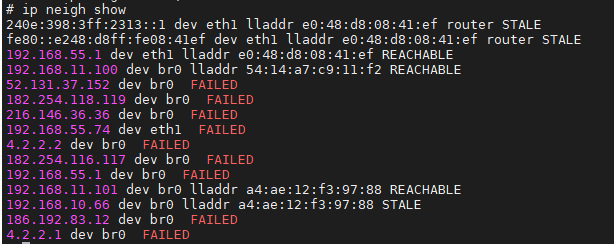
目标：PC（192.168.11.101）和Router（192.168.55.1）通信以及PC与192.168.55.74（不可达），抓取PC与DUT，DUT与Router之间的ARP数据包

步骤

1. DUT工作在路由模式，并配置端口镜像，使得PC可以监控DUT-WAN口的数据包
2. Wireshark选择正确的网络接口，开始捕获
3. 访问目的IP
4. 筛选ARP包并分析

查看PC、DUT的ARP表项





由ARP表信息可以看出，PC拥有到DUT的动态ARP表项，而DUT拥有Router的动态ARP表项

预设：根据理论知识，若PC与Router通信（不在一个网段），则会经历PC广播纠正：arp表里有网关的mac地址，故应该是单播；若没有mac地址才是广播。到DUT（PC的网关），DUT广播到Router（DUT网关）

**PC会查找ARP表，若找不到目的IP的MAC地址，于是查询ARP，ARP缓存也没有该IP的MAC地址信息，而且通过子网掩码计算不是本网段，跨网段就需要找网关，查询ARP表内没有网关的MAC地址，则广播查找（此时查找的目的IP是网关的IP）；若有则直接封包发送；**

根据理论知识可知，PC会定期向DUT发送老化探测报文，即ARP请求报文，同理，DUT也会，并且这种老化探测报文跟设置的老化参数（老化超时时间、老化探测次数和老化探测模式）有关，即缺省情况下，设备只在最后一次发送ARP老化探测报文是广播模式，其余均为单播模式发送

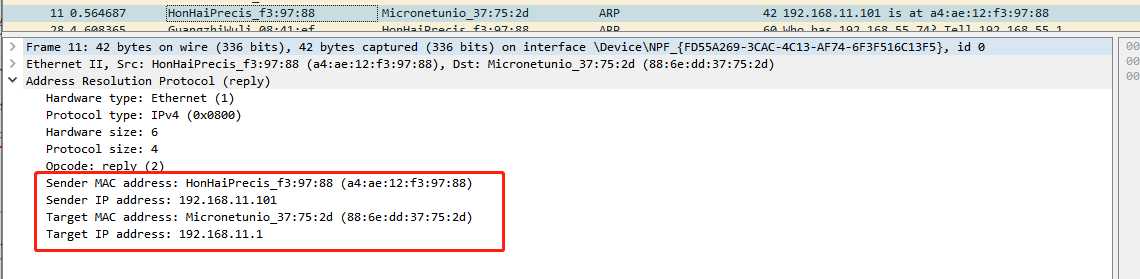
因此，整个通信过程会变成

1、PC会发送ARP请求报文，请求网关DUT的IP地址对应的MAC地址，但由于本机有该缓存且动态维护着，故抓不到PC广播的ARP数据包，只有PC发给DUT的老化探测报文，此为单播(最后一次老化探测为广播)

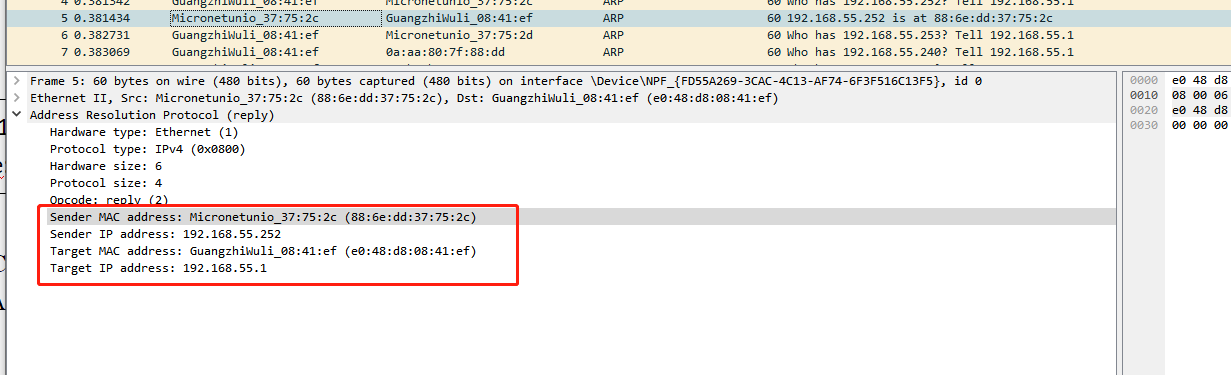
2、DUT与Router在同一个网段，且本地有相关表项，直接交付

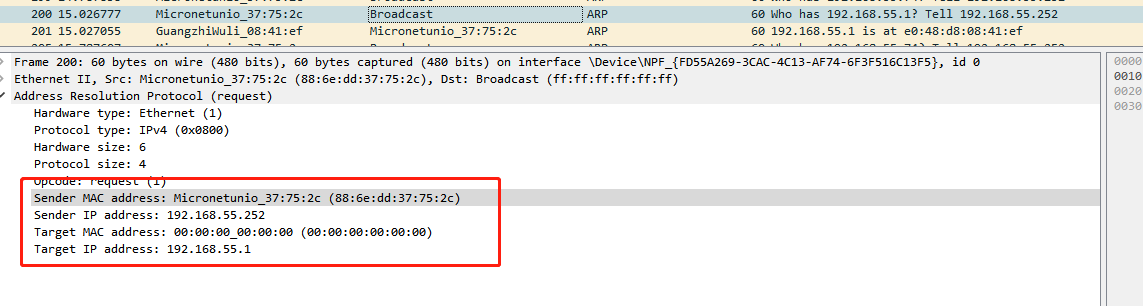
抓包结果如下：

PC发给DUT的老化探测报文：

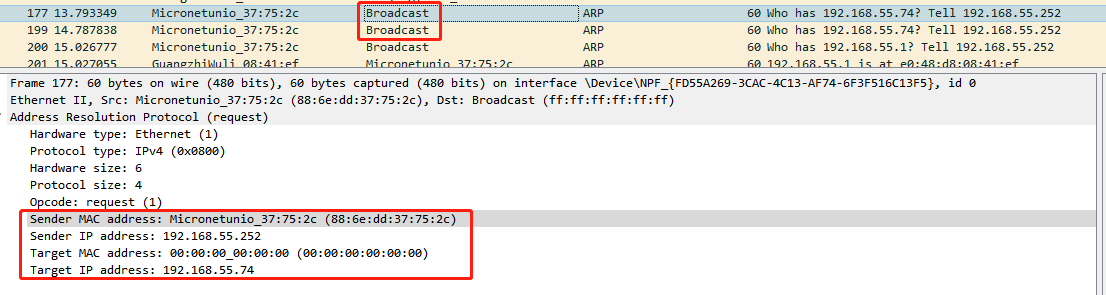


DUT发给Router的老化探测报文（单播和广播）：





PC访问192.168.55.74，则PC先发给DUT，由DUT去完成查找目的MAC地址的功能，由于DUT没有该目的地址的表项，故广播发送



⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐**Wireshark抓IP包验证**⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐⭐

