第 3 章

数据链路层实验

实验 7　PPP 的配置与分析

7.1　实 验 目 的

（1）掌握基于 PAP 认证的 PPP 配置方法。

（2）掌握基于 CHAP 认证的 PPP 配置方法。

（3）理解 PPP 的工作过程和报文格式。

7.2　实 验 要 求

（1）设备要求：计算机两台以上（装有 Windows 操作系统、华为 eNSP 模拟器软件，安装有网卡已联网）。

（2）分组要求：1 人一组，但部分步骤需相互合作完成。

7.3　实验预备知识

点对点协议（Point-to-Point Protocol，PPP）是目前使用最广泛的点对点数据链路层协议。PPP 由以下三个部分组成。

（1）一个将上层数据（如 IP 数据报）封装到串行链路的方法。

（2）一个链路控制协议（Link Control Protocol，LCP），用来建立、配置和测试数据链路连接。

（3）一套网络控制协议（Network Control Protocol，NCP），能支持不同的网络层协议，如 IP、OSI 的网络层、DECnet，以及 AppleTalk 等。

1. PPP 协议帧格式

如图 3-1 所示，PPP 的帧格式主要由**首部**、**信息字段**、**尾部**三部分组成。

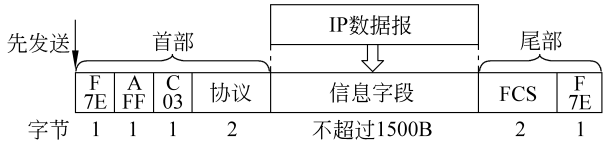

图 3-1　PPP 协议帧格式

1）**首部**

首部字段由 5B 构成：**标志字段 F**，占 1B，规定为 0x7E，表示一个帧的开始或结束。此标志字段就是 PPP 帧的定界符。连续两帧之间只需要用一个标志字段。若出现连续两个标志字段，则表示这是一个空帧，应当丢弃。**地址字段 A**，占 1B，规定为 0xFF。**控制字段 C**，占 1B，规定为 0x03。**协议字段**，表示信息字段数据所使用的协议。当协议字段为 0x0021 时，PPP 帧的信息字段就是 IP 数据报；若为 0xC021，则信息字段是 PPP 链路控制协议（LCP）的数据；若为 0x8021，表示这是 NCP 的 IPCP 分组；若为 0xC023，表示信息字段就是 PAP 认证协议；而 0xC223 则表示信息字段为 CHAP 认证协议。

2）**信息字段**

信息字段的长度是可变的，但不超过 1500B。

3）**尾部**

尾部由 3B 构成：**使用 CRC 的帧检验序列 FCS，占 2B；标志字段 F，占 1B（首部标志字段）**。

在 PPP 中，异步传输时一般使用字节填充保证透明传输，而在同步传输时一般使用零比特填充的方法来保证透明传输。

2. PPP 建立连接的过程

PPP 的状态图如图 3-2 所示，其主要工作过程如下。

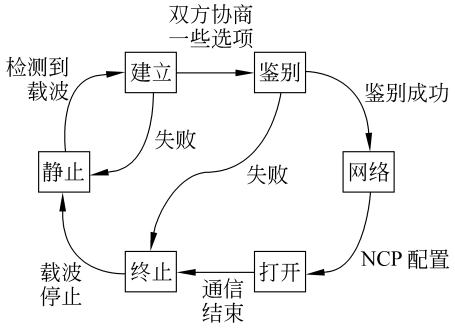

图 3-2 PPP 状态图

（1）开始“静止”阶段没有进行任何连接，没有可用链路，当两端检测到特定接口被激活时，转入“建立”阶段（即链路建立阶段）。

（2）在“建立”阶段，PPP 链路进行 LCP 参数协商。协商内容主要包括最大接收单元（MRU）、认证方式、魔术字等。LCP 参数协商成功后可进入“鉴别”阶段（若不需要进行鉴别，可直接进入“网络”阶段）。

（3）在“鉴别”阶段，通信双方可互相鉴别身份，也可只进行单向鉴别。鉴别成功后即可进入“网络”阶段，鉴别失败则转入“终止”状态，结束已建立的 PPP 链路。

（4）在“网络”阶段，PPP 链路进行 NCP（典型的是 IPCP）协商，只有相应的网络层协议（如 IP）协商成功后，网络层协议才可通过这条 PPP 链路发送数据分组。

（5）通信任何一方不需要使用该链路时，都可以终止建立的 PPP 连接，最后回到“静止”阶段。

3. PPP 认证方式

在“鉴别”阶段，PPP 认证方式主要有两种：口令认证协议（PAP）和挑战握手认证协议（CHAP）。

PAP 认证（两次握手）：

（1）被认证方将用户名和口令以明文方式发送给认证方。

（2）认证方根据本地用户表验证被认证方的用户名及口令是否匹配，若匹配，则通过

认证，发送认证确认帧；若不匹配，则认证失败，发送认证否认帧。

CHAP 认证（三次握手）：

（1）Challenge 过程：由认证端发送 Challenge 挑战报文，该报文主要由两个值组成：name 和 value。在这里没有 name 所以为空，value1 取一串随机的 128b 数。

（2）Response 过程：被认证方收到 Challenge 报文中的 value1 后，将和接口下配置的 chap 密码做 MD5 计算，最终生成自己的 MD5 摘要 value2，然后向认证方发送 Response 响应报文，并将自己的 name 和计算出来的 value2 带回给认证方。

（3）Success 过程：如果验证成功，由认证方回复 Success 报文，否则回复 Failure 报文。认证方收到 Response 报文后，会取出其中的 name 字段，跑到 aaa 配置下查找该用户名，假设找到该用户名，认证方会执行 MD5 计算过程，将密码和 value1 做 MD5 计算，得到 MD5 摘要 value3，如果对比 value2＝value3，则认证成功，认证方向被认证方回复 Success 报文。

由于 CHAP 在认证过程中没有明文传输用户口令，所以安全性比 PAP 高。

4. PPP 的基本配置

```
[R1]interface S1/0/0                          //进入 S1/0/0 接口视图
[R1-Serial1/0/0]link-protocol ppp             //S1/0/0 接口的链路层协议使用 PPP
[R1-Serial1/0/0]ip addr 192.168.1.1 30        //设置接口 IP 地址
```

7.4　实验内容与步骤

1. 建立网络拓扑

网络拓扑如图 3-3 所示，两台路由器通过串行线互连。本实验路由器型号为 AR3260，默认情况下，此型号路由器只提供 GigabitEthernet 接口，没有串口，需要增加一块 2SA 接口卡（拖入 1 号槽位），如图 3-4 所示，各设备的 IP 地址分配如表 3-1 所示。

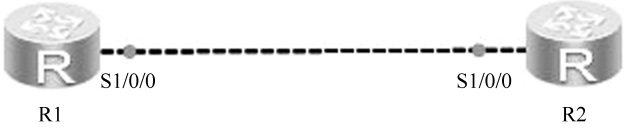

图 3-3　网络拓扑

表 3-1　设备 IP 地址分配

设　　备	接　　口	IP 地址
R1	S1/0/0	192.168.1.1/30
R2	S1/0/0	192.168.1.2/30

2. 基于 PAP 认证的 PPP 配置与分析

1）基于 PAP 认证的 PPP 配置（R1 对 R2 的单向认证）

认证方 R1 配置如下。

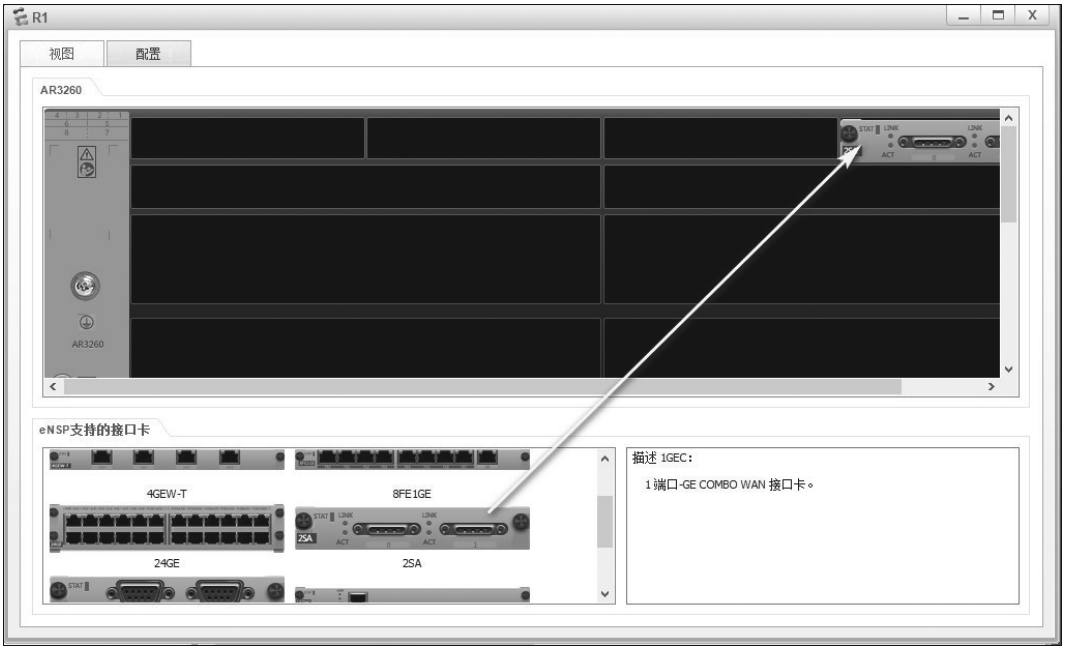

图 3-4　AR3260 路由器增加 2SA 接口卡

```
<Huawei>sys
[Huawei]sysn R1
[R1]aaa
[R1-aaa]local-user R2 password cipher seig    //创建用户 R2,密码为 seig
[R1-aaa]local-user R2 service-type ppp        //设置 R2 用户的业务类型为 PPP
[R1-aaa]q
[R1]interface s1/0/0
[R1-Serial1/0/0]link-protocol ppp             //S1/0/0 接口的链路层协议使用 PPP
[R1-Serial1/0/0]ppp authentication-mode pap //设置认证方式为 PAP
[R1-Serial1/0/0]ip addr 192.168.1.1 30        //设置接口 IP 地址
```

被认证方 R2 配置如下。

```
<Huawei>sys
[Huawei]sysn R2
[R2]interface s1/0/0
[R2-Serial1/0/0]link-protocol ppp
[R2-Serial1/0/0]ppp pap local-user R2 password cipher seig    //提供用户名和密码
[R2-Serial1/0/0]ip address 192.168.1.2 30                     //设置接口 IP 地址
```

在 R1 的 S1/0/0 接口启动抓包(自动运行 Wireshark 软件),选择链路类型为 PPP。在 R2 上执行“shutdown”命令关闭 S1/0/0 接口,然后再执行“undo shutdown”命令启动 S1/0/0 接口,查看启动接口后 Wireshark 软件捕获的分组,分析 PPP 的 LCP 协商过程、PAP 认证过程和 NCP 协商过程。

2) 分析 LCP 协商过程

在 LCP 建立链路阶段,通信双方通过相互发送 Configuration-Request 帧和 Configuration-

Ack 帧协商链路参数。一些常见的配置参数包括 MRU、认证协议、魔术字等。在华为设备上，MRU 参数使用接口上配置的最大传输单元（Maximum Transfer Unit，MTU）。LCP 使用魔术字 Magic-Number（随机产生）检测链路环路和其他异常情况。请分析 LCP 协商过程中的 Configuration-Request 帧，如图 3-5 所示，填写表 3-2。

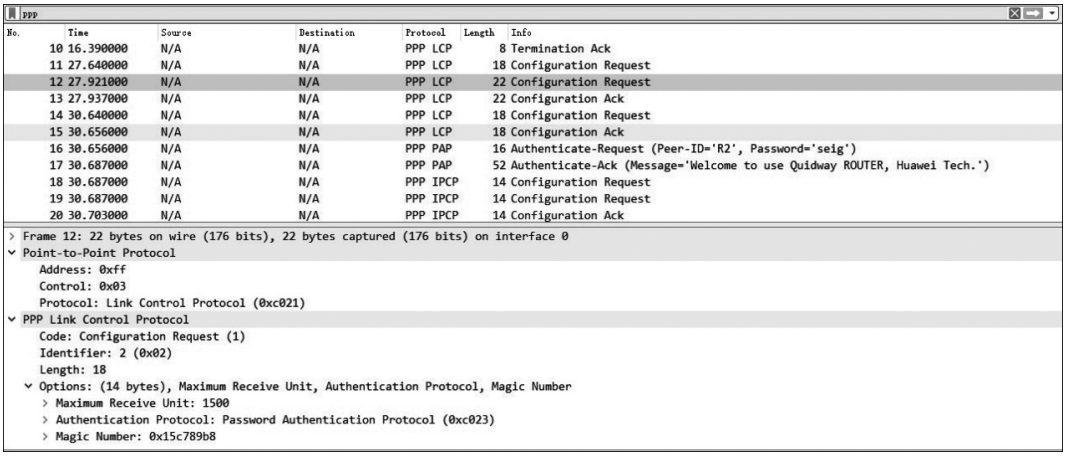

图 3-5　Configuration-Request 帧

表 3-2　Configuration-Request 帧相关参数值

MRU		魔术字	
认证协议		PPP 首部中“协议”字段值及含义	

3）分析 PAP 认证过程

LCP 协商成功后，进入 PAP 认证过程，被认证方发送 Authentication-Request 帧提供用户名和密码（明文），如图 3-6 所示。认证方验证用户名和密码是否正确，如通过认证，则发送 Authentication-Ack 帧，否则发送 Authentication-Nak 帧。请分析 PAP 认证过程中的 Authentication-Ack 帧，填写表 3-3。

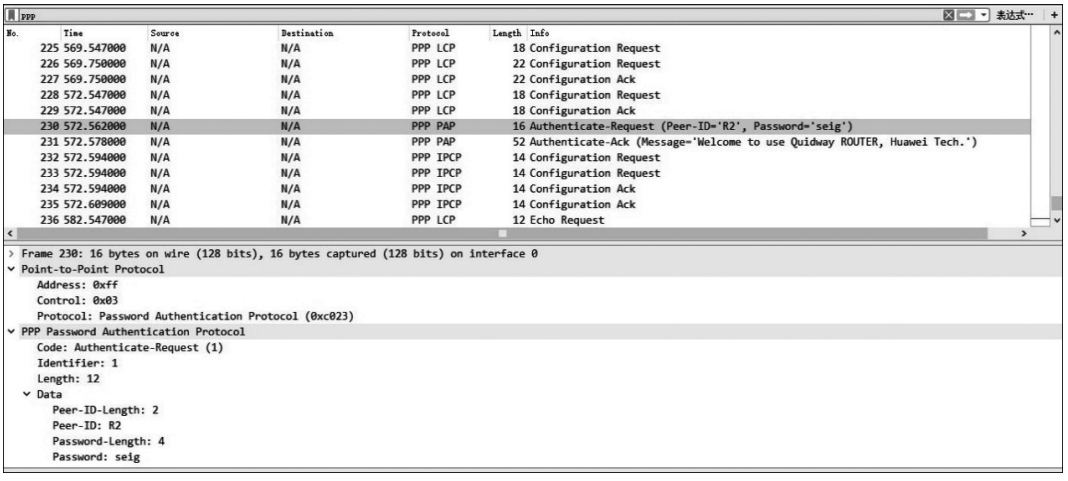

图 3-6　Authentication-Request 帧

表 3-3　Authentication-Request 帧相关参数值

用户名		密码	
PPP 首部中“协议”字段值及含义			

4）分析 NCP 协商过程

认证通过后，进入 NCP 协商过程，如图 3-7 所示。IPCP 支持静态地址协商和动态地址协商。本实验使用静态地址协商，由通信双方互相发送 Configuration-Request 帧告知对方自己的 IP 地址等信息，对方回复 Configuration-Ack 帧表示同意。请填写表 3-4。

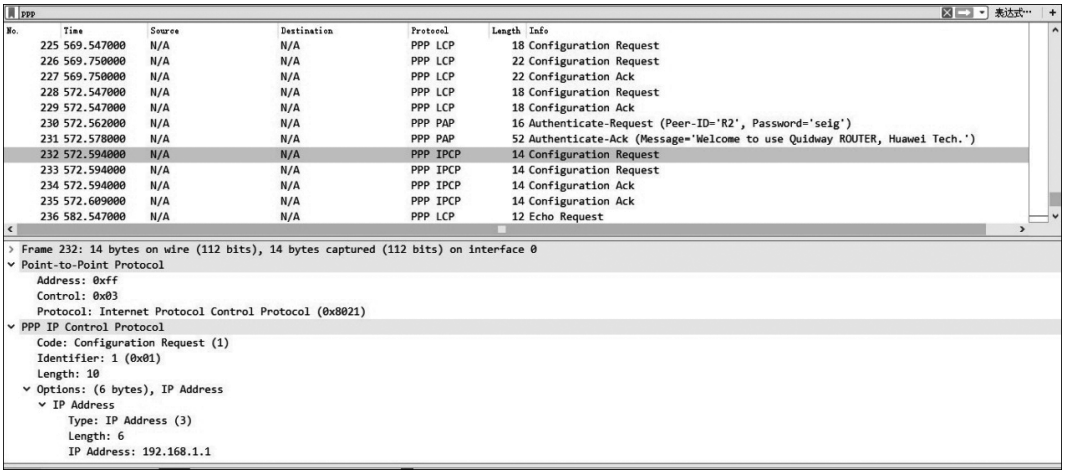

图 3-7　NCP 协商过程

表 3-4　Configuration-Request 帧相关参数值

数据帧的发送方		IP 地址	
PPP 首部中“协议”字段值及含义			

5）测试连通性

NCP 协商成功后，通信双方就可以通过这个链路传输数据了。在路由器 R1 上执行“ping 192.168.1.2”命令测试 R1 与 R2 间的连通性，并分析捕获的 ICMP 分组，如图 3-8

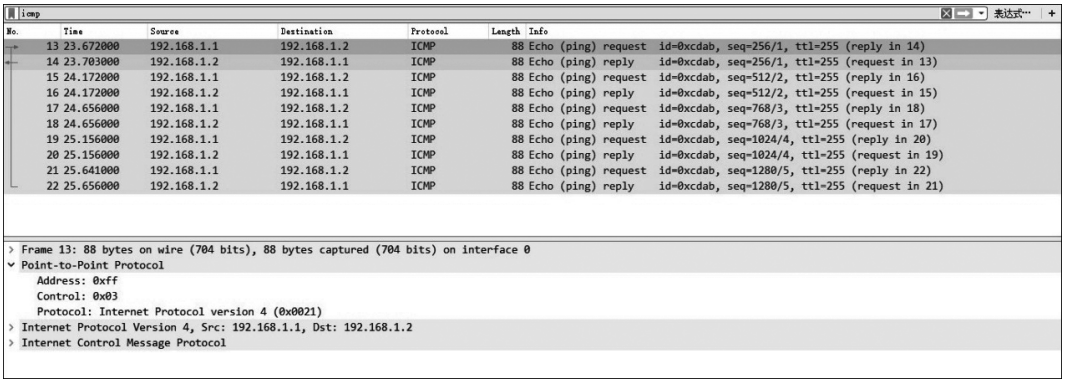

图 3-8　捕获的 ICMP 分组

所示。填写表 3-5。

表 3-5　ICMP 分组

ICMP 分组的链路层协议	
PPP 首部中“协议”字段值及含义	

3. 基于 CHAP 认证的 PPP 配置与分析

1）基于 CHAP 认证的 PPP 配置(R1 对 R2 的单向认证)

先清除 R1 和 R2 的 PPP 配置：

```
[R1]interface s1/0/0
[R1-Serial1/0/0]undo ppp authentication-mode
[R1-Serial1/0/0]undo ip address 192.168.1.1 30
```

```
[R2]interface s1/0/0
[R2-Serial1/0/0]undo ppp pap local-user
[R2-Serial1/0/0]undo ip address 192.168.1.2 30
```

认证方 R1 配置如下。

```
[R1]aaa
[R1-aaa]local-user R2 password cipher seig     //创建用户 R2,密码为 seig
[R1-aaa]local-user R2 service-type ppp         //设置 R2 用户的业务类型为 PPP
[R1-aaa]interface s1/0/0
[R1-Serial1/0/0]link-protocol ppp              //S1/0/0 接口的链路层协议使用 PPP
[R1-Serial1/0/0]ppp authentication-mode chap //设置认证方式为 CHAP
[R1-Serial1/0/0]ip address 192.168.1.1 30      //设置接口 IP 地址
[R1-Serial1/0/0]remote address 192.168.1.2     //为对端分配 IP 地址 192.168.1.2
```

被认证方 R2 配置如下。

```
[R2]interface s1/0/0
[R2-Serial1/0/0]link-protocol ppp
[R2-Serial1/0/0]ppp pap local-user R2 password cipher seig   //提供用户名和密码
[R2-Serial1/0/0]ppp chap user R2                //提供 CHAP 用户
[R2-Serial1/0/0]ppp chap password cipher seig  //提供 CHAP 用户密码
[R2-Serial1/0/0]ip address ppp-negotiate       //通过 PPP 协商获取 IP 地址
```

在 R1 的 S1/0/0 接口启动抓包(自动运行 Wireshark 软件)，选择链路类型为 PPP。在 R2 上执行“shutdown”命令关闭 S1/0/0 接口，然后再执行“undo shutdown”命令启动 S1/0/0 接口，查看启动接口后 Wireshark 软件捕获的分组，分析 PPP 的 LCP 协商过程、CHAP 认证过程和 NCP(IPCP)协商过程。

2）分析 LCP 协商过程

Configuration-Request 帧如图 3-9 所示。请填写表 3-6。

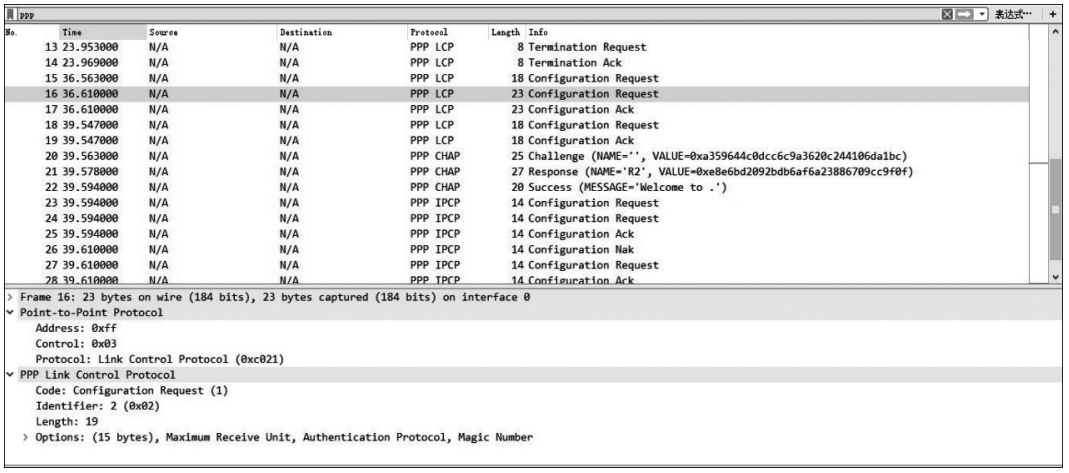

图 3-9 Configuration-Request 帧

表 3-6 Configuration-Request 帧相关参数值

MRU		魔术字	
认证协议		PPP 首部中“协议”字段值及含义	

3）分析 CHAP 认证过程

捕获的 CHAP 认证过程中的相关分组如图 3-10 所示，请分析图中的三个 CHAP 帧，简单描述这三个帧的作用，并填写表 3-7。

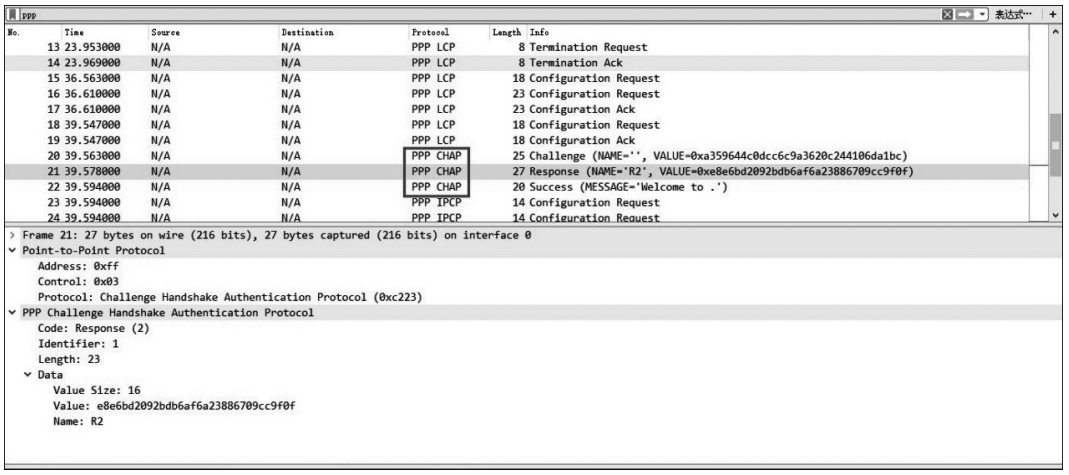

图 3-10 CHAP 认证过程

表 3-7 CHAP 帧作用

Challenge	
Response	
Success	
是否能看到 R2 发送的用户名和密码	

4）分析 NCP 协商过程

PPP 通过认证后进入 NCP 协商过程，如图 3-11 所示，R2 通过 IPCP 从 R1 动态获取 IP 地址。R2 首先发送 Configuration-Request 帧，请求分配的 IP 地址为空(0.0.0.0)，R1 会应答 Configuration-Nak 帧，并给 R2 指派一个 IP 地址(192.168.1.2)。R2 收到后会两次发送一个 Configuration-Request 帧，请求配置该 IP 地址(192.168.1.2)，R1 应答 Configuration-Ack 帧进行确认。这期间 R1 也会发送 Configuration-Request 帧进行静态地址协商，R2 会用 Configuration-Ack 帧进行确认(这个过程可能会与前面的动态地址协商同步进行)。

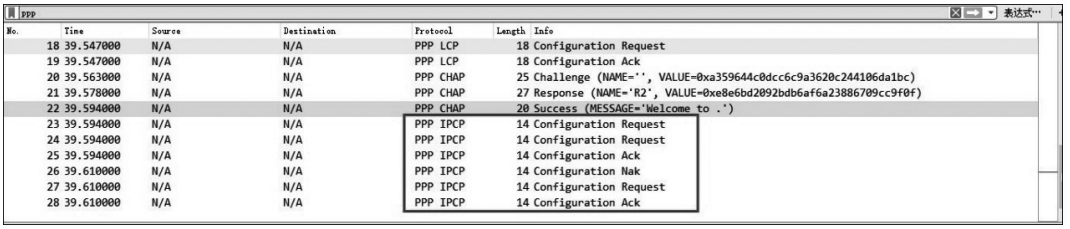

图 3-11　NCP 协商过程

从捕获的分组中找到 R2 向 R1 动态请求 IP 地址过程中所有交互的帧(不包括静态地址协商帧)并进行分析，简单描述这 4 个帧的作用，并填写表 3-8。

表 3-8　NCP 协商数据帧

Configuration-Request	
Configuration-Nak	
Configuration-Request	
Configuration-Ack	

5）测试连通性

NCP 协商成功后，通信双方就可以通过这个链路传输数据了。在路由器 R1 上执行“ping 192.168.1.2”命令测试 R1 与 R2 间的连通性，如图 3-12 所示。

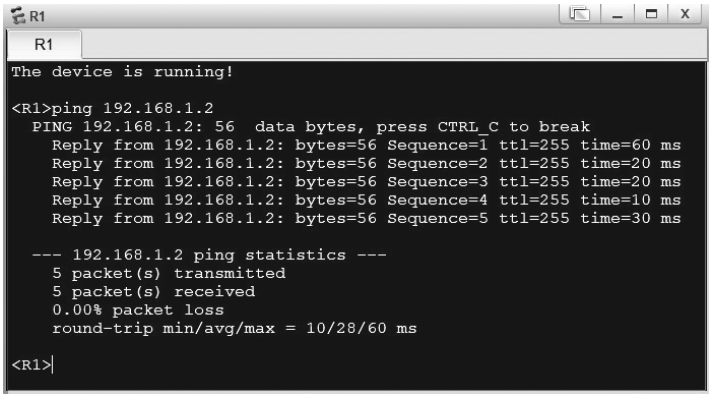

图 3-12　连通性测试

7.5 练习与思考

1.【单选题】局域网数据链路层分为(　　)两个子层功能。

A. IP 子层和 MAC 子层　　B. MAC 子层和 TCP 子层

C. MAC 子层和 LLC 子层　　D. LLC 子层和 ICMP 子层

2.【单选题】PPP 提供的功能有(　　)。

A. 一种成帧方法　　B. 链路控制协议 LCP

C. 网络控制协议 NCP　　D. 全都是

3.【单选题】PPP 是哪一层的协议?(　　)

A. 数据链路层　　B. 物理层　　C. 高层　　D. 网络层

4.【单选题】当 PPP 使用同步传输时,使用(　　)填充方法来实现透明传输。

A. 字节　　B. 字符　　C. 数字　　D. 零比特

5.【单选题】哪种通信中,采用零比特填充实现透明传输?(　　)

A. 同步通信　　B. 异步通信　　C. 串行通信　　D. 并行通信

实验 8　集线器与交换机原理分析

8.1　实 验 目 的

(1) 理解集线器与交换机的工作原理。

(2) 掌握简单交换式以太网的组网方法及连通性测试。

(3) 熟悉使用华为 eNSP 网络模拟软件。

8.2　实 验 要 求

(1) 设备要求：计算机两台以上(安装有 Windows 操作系统、华为 eNSP 模拟器软件，安装有网卡已联网)。

(2) 分组要求：1 人一组，但部分步骤需相互合作完成。

8.3　实验预备知识

1. 集线器与共享式以太网

在认识集线器之前，先了解一下中继器。在我们接触到的网络中，最简单的就是两台主机通过两块网卡构成“双机互连”，两块网卡之间通常是由非屏蔽双绞线来连接的。因为双绞线在传输信号时信号功率会逐渐衰减，当信号衰减到一定程度时将造成信号失真，因此在保证信号质量的前提下，双绞线的最大传输距离为 100m。当两台计算机之间的距离超过 100m 时，为了实现双机互连，人们便在这两台计算机之间安装一个“中继器”。它的作用就是将已经衰减得不完整的信号经过整理，再一次产生出完整的信号继续传送。

集线器实际上就是一种多端口的中继器。通过这些端口，集线器便能为对应数量的主机完成“中继”功能。因为它在网络中处于一种“中心”位置，因此集线器也叫作“Hub”。集线器本身不能识别目的物理地址，当同一局域网内的 A 主机给 B 主机传输数据时，数据包在以集线器为架构的网络上是以广播方式传输的，由每一台终端通过验证数据包头的地址信息来确定是否接收，因此，集线器是一种“共享”设备。使用集线器组建的以太网，物理上为星状结构而逻辑上为总线型结构，以共享传输介质为最大特点，如图 3-13 所示，称之为共享式以太网(所有的设备在同一个冲突域中，也在同一个广播域中)。

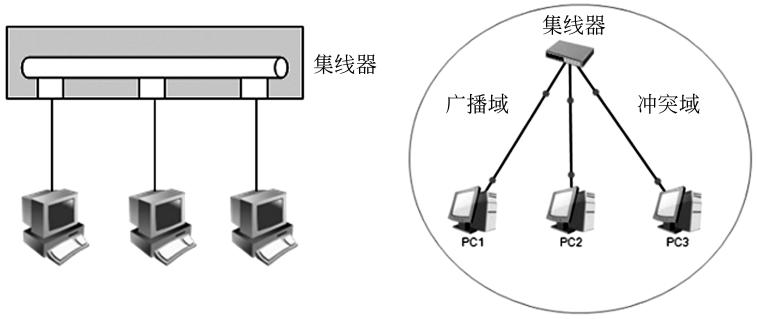

图 3-13　集线器组建的共享式以太网

共享式以太网是最简单、最便宜、最常用的一种组网方式。但是，在网络应用和组网过程中，共享式以太网也暴露出了它的弱点。

（1）覆盖的地理范围有限。按照 CSMA/CD 的有关规定，以太网覆盖的地理范围随着网络速度的增加而减小。一旦网络速率固定下来，网络的覆盖范围也就固定下来。因此，只要两个节点处于同一个以太网中，它们之间的最大距离就不能超过这一固定值，不管它们之间的连接跨越一个集线器还是多个集线器。如果超过这个值，网络通信就会出现问题。

（2）网络总带宽容量固定。共享式以太网的固定带宽容量被网络上的所有节点共同拥有，随机占用。网络中的节点越多，每个节点平均可以使用的带宽越窄，网络的响应速度也会越慢。例如，对于一个 100Mb/s 的以太网，如果连接 10 个节点，则每个节点平均带宽为 10Mb/s，如果连接节点增加到 100 个，则每个节点平均带宽下降为 1Mb/s。

（3）不能支持多种速率。由于以太网共享传输介质，因此，网络中的设备必须保持相同的传输速率。否则一个设备发送的信息，另一个设备不可能收到。单一的共享式以太网不可能提供多种速率的设备支持。

2. 交换机与交换式以太网

通常，人们利用“分段”的方法解决共享式以太网存在的问题。所谓的“分段”，就是将一个大型的以太网分隔成两个或多个小型的以太网，每个段（分隔后的每个小以太网）使用 CSMA/CD 介质访问控制方法维持段内用户的通信。段与段之间通过一种“交换”设备进行沟通。这种交换设备可以将在一段接收到的信息，经过简单的处理转发给另一段，这就是交换式以太网。

如图 3-14 所示，给出了一个通过集线器级联组成的大型以太网。尽管部门 1、部门 2 和部门 3 都通过各自的集线器组网，但是，由于使用共享式集线器连接各个部门的集线器，因此，所构成的网络仍然属于一个大的以太网（所有的设备都仍然在同一个广播域中，也在同一个冲突域中）。这样，每台计算机发送的信息将在全网流动，即使它访问的部门的服务器也是如此。

通常，部门内部计算机之间的相互访问是最频繁的。为了限制部门内部信息在全网流动，利用交换设备将整个大的以太网分段，每个部门组成一个小的以太网，部门之间通过交换设备相互连接，如图 3-15 所示。通过分段，既可以保证部门内部信息不会流至其

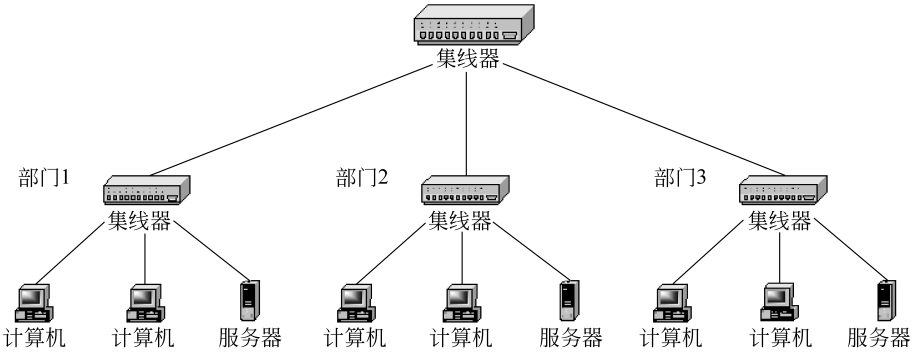

图 3-14　通过集线器级联组成大型的共享以太网

他部门，又可以保证部门之间的信息交互。以太网节点的减少使冲突和碰撞的概率更小，网络的效率更高。不仅如此，分段之后，各段可按需要选择自己的网络速率，组成性能价格比更高的交换式网络。

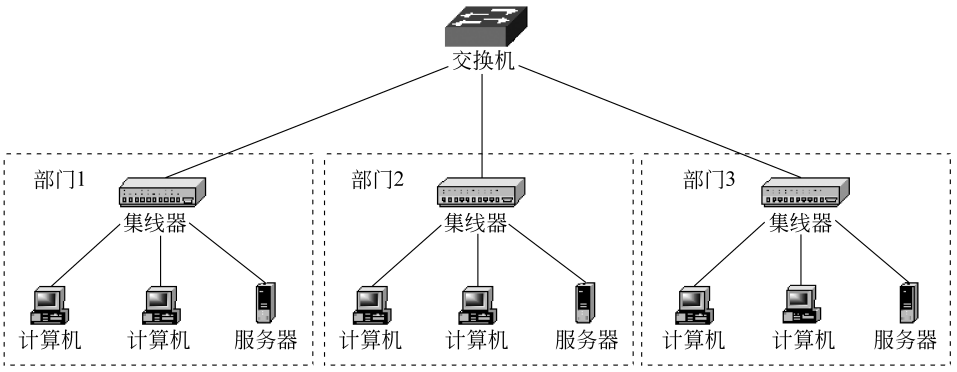

图 3-15　通过交换机对共享以太网分段

交换设备有多种类型，局域网交换机、路由器等都可以作为交换设备。交换机工作于数据链路层，用于连接较为相似的网络（例如以太网-以太网）；而路由器工作于互联层，可以实现异型网络的互联（例如以太网-帧中继）。

典型的局域网交换机是以太网交换机。以太网交换机可以通过交换机端口之间的多个并发连接，实现多节点之间数据的并发传输。这种并发数据传输方式与共享式以太网在某一时刻只允许一个节点占用共享信息的方式完全不同。

交换式以太网建立在以太网基础之上。利用以太网交换机组网，既可以将计算机直接连到交换机的端口上，也可以将它们连入一个网段，然后将这个网段连到交换机的端口。如图 3-16 所示，利用以太网交换机将两台服务器和两个以太网连成一个交换式的局域网。如果将计算机直接连到计算机的端口，那么它将独享该端口提供的带宽；如果计算机通过以太网连入交换机，那么该以太网的所有计算机共享交换机端口提供的带宽。此时交换机的每一个接口分别处在不同的冲突域中，但所有的接口仍然处在同一个广播域中，如图 3-17 所示。

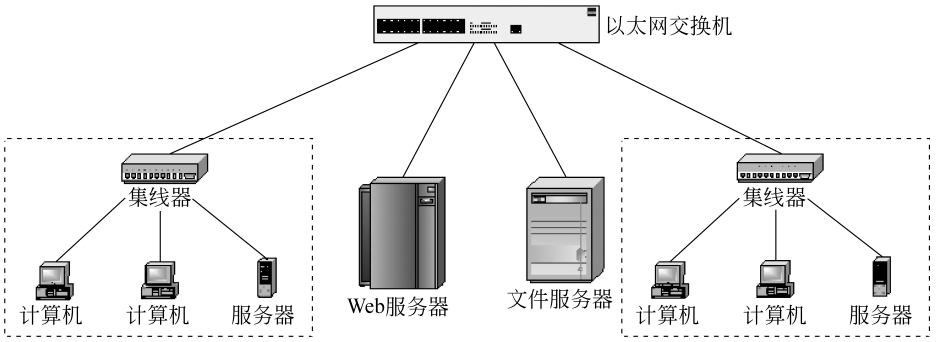

图 3-16　利用交换机连接计算机和以太网

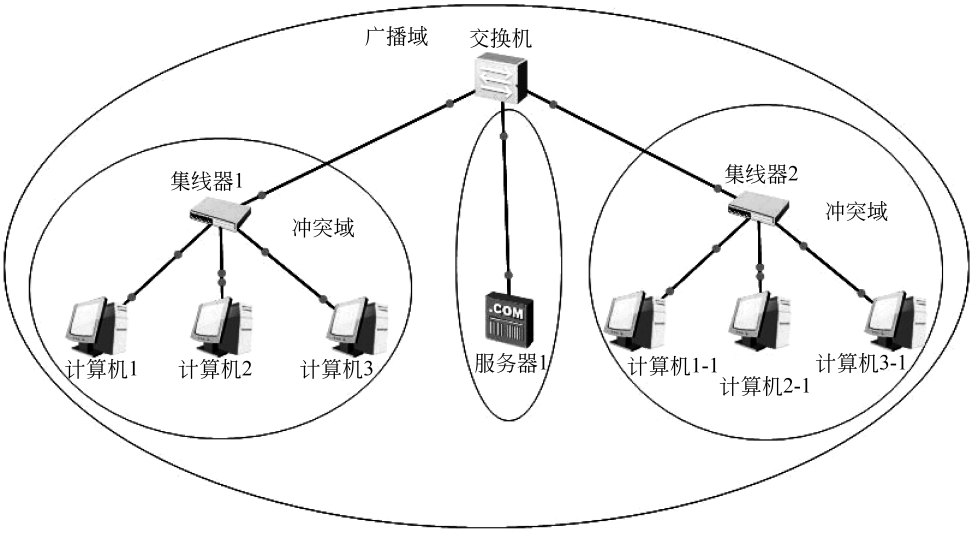

图 3-17　冲突域与广播域

8.4　实验内容与步骤

1. 集线器原理分析

建立共享式网络拓扑如图 3-18 所示。各设备 IP 地址分配如表 3-9 所示。

表 3-9　设备 IP 地址分配表

设　备	接　口	IP 地址	子网掩码
PC1	Ethernet 0/0/1	192.168.1.1	255.255.255.0
PC2	Ethernet 0/0/1	192.168.1.2	255.255.255.0
PC3	Ethernet 0/0/1	192.168.1.3	255.255.255.0

在 Hub 的 Ethernet 0/0/1 接口上启动抓包，然后在 PC1 上执行“ping 192.168.1.3”命令，如图 3-19 所示。Wireshark 软件捕获到的分组如图 3-20 所示，分析所捕获的分组

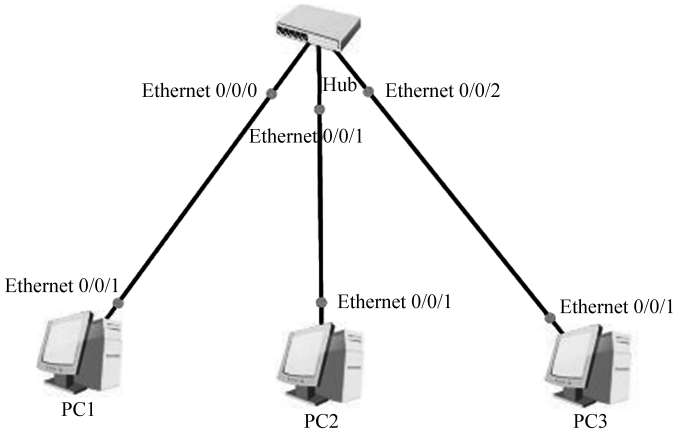

图 3-18　共享式网络拓扑

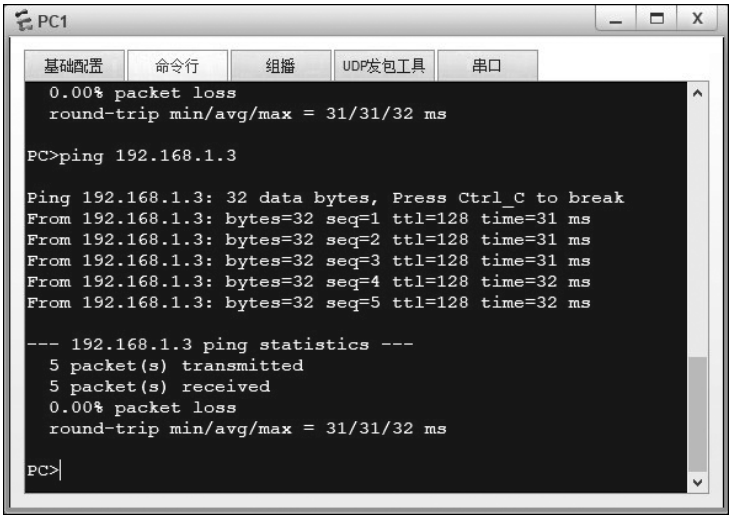

图 3-19　PC1 ping PC3

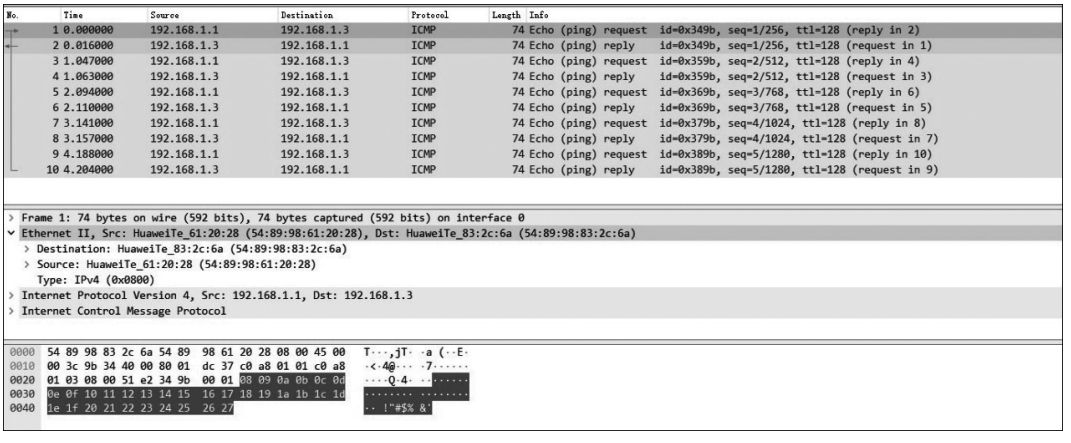

图 3-20　在 Hub 的 Ethernet 0/0/1 接口上所捕获的分组

(以图中 1 号、2 号分组为例进行分析),填写表 3-10。

表 3-10 Hub 转发数据分组分析

1 号分组源 IP 地址		1 号分组目的 IP 地址	
2 号分组源 IP 地址		2 号分组目的 IP 地址	
为什么 PC2 能收到 PC1 ping PC3 的数据分组			

2. 交换机原理分析

(1)建立交换式网络拓扑如图 3-21 所示。各设备的 IP 地址等配置如表 3-11 所示。

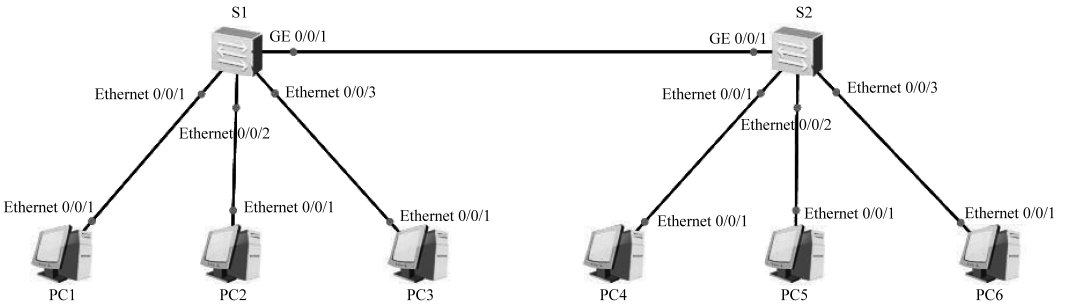

图 3-21 交换式网络拓扑

表 3-11 设备 IP 地址分配表

设 备	接 口	IP 地址	子网掩码	MAC 地址
PC1	Ethernet 0/0/1	192.168.1.1	255.255.255.0	54-89-98-61-20-28
PC2	Ethernet 0/0/1	192.168.1.2	255.255.255.0	54-89-98-A6-1B-2A
PC3	Ethernet 0/0/1	192.168.1.3	255.255.255.0	54-89-98-83-2C-6A
PC4	Ethernet 0/0/1	192.168.1.4	255.255.255.0	54-89-98-D4-34-50
PC5	Ethernet 0/0/1	192.168.1.5	255.255.255.0	54-89-98-1C-1A-57
PC6	Ethernet 0/0/1	192.168.1.6	255.255.255.0	54-89-98-66-74-24

下面依次在不同的主机间发送数据帧:PC1 →PC4,PC5 →PC6,PC4 →PC1,PC6 →PC5。查看交换机 S1 和交换机 S2 的 MAC 地址表,以及主机 PC3、PC4、PC6 的接口捕获的分组,分析交换机 MAC 地址表形成过程。

在这个实验中,利用 eNSP 模拟 PC 的 UDP 发包工具来发送数据(产生以太网帧),UDP 发包工具配置如图 3-22～图 3-25 所示。注意,要正确配置源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址,这里 UDP“源端口号”和“目的端口号”均设置为“888”。为避免操作时间过长导致 MAC 地址表项超时,建议把所有主机的 UDP 发包工具都配置好后再进行下面的实验。

图 3-22　PC1 发包工具配置

图 3-23　PC5 发包工具配置

图 3-24　PC4 发包工具配置

图 3-25　PC6 发包工具配置