

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。



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。





(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。



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]pp authentication-mode pa //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-

实验7 PPP的配置与分析 🗙 63

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。

PP:	P				Σ	× 🖃 🔹
No.	Time	Source	Destination	Protocol Le	agth Info	
	10 16.390000	N/A	N/A	PPP LCP	8 Termination Ack	
	11 27.640000	N/A	N/A	PPP LCP	18 Configuration Request	
	12 27.921000	N/A	N/A	PPP LCP	22 Configuration Request	
	13 27.937000	N/A	N/A	PPP LCP	22 Configuration Ack	
	14 30.640000	N/A	N/A	PPP LCP	18 Configuration Request	
	15 30.656000	N/A	N/A	PPP LCP	18 Configuration Ack	
	16 30.656000	N/A	N/A	PPP PAP	16 Authenticate-Request (Peer-ID='R2', Password='seig')	
	17 30.687000	N/A	N/A	PPP PAP	52 Authenticate-Ack (Message='Welcome to use Quidway ROUTER, Huawei Tech.')	
	18 30.687000	N/A	N/A	PPP IPCP	14 Configuration Request	
	19 30.687000	N/A	N/A	PPP IPCP	14 Configuration Request	
5	20 30.703000	N/A	N/A	PPP IPCP	14 Configuration Ack	
✓ Pc	Address: 0xff Control: 0x03 Protocol: Link 0	tocol Control Protocol (0xc	.021)			
Y PF	PP Link Control P	rotocol				
~	Code: Configurat Identifier: 2 (6 Length: 18 Options: (14 byt > Maximum Recei > Authenticatio	tion Request (1) 0x02) tes), Maximum Receive ve Unit: 1500 n Protocol: Password	• Unit, Authentica	tion Protocol	, Magic Number	

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。

					🛛 🗔 🔹 表达3	t)
lo.	Time	Source	Bestination	Protocol	Length Info	
	225 569.547000	N/A	N/A	PPP LCP	18 Configuration Request	
	226 569.750000	N/A	N/A	PPP LCP	22 Configuration Request	
	227 569.750000	N/A	N/A	PPP LCP	22 Configuration Ack	
	228 572.547000	N/A	N/A	PPP LCP	18 Configuration Request	
	229 572.547000	N/A	N/A	PPP LCP	18 Configuration Ack	
1	230 572.562000	N/A	N/A	PPP PAP	16 Authenticate-Request (Peer-ID='R2', Password='seig')	
	231 572.578000	N/A	N/A	PPP PAP	52 Authenticate-Ack (Message='Welcome to use Quidway ROUTER, Huawei Tech.')	<u> </u>
	232 572.594000	N/A	N/A	PPP IPCP	14 Configuration Request	
	233 572.594000	N/A	N/A	PPP IPCP	14 Configuration Request	
	234 572.594000	N/A	N/A	PPP IPCP	14 Configuration Ack	
	235 572.609000	N/A	N/A	PPP IPCP	14 Configuration Ack	
	236 582.547000	N/A	N/A	PPP LCP	12 Echo Request	-
A					-	/
. Cas		- an idea (139	hits) 16 hutes contune	4 (130 bits) on i	stanface 0	
Fra Poi	me 230: 16 bytes nt-to-Point Prof	s on wire (128 tocol	bits), 16 bytes capture	d (128 bits) on i	nterface 0	
Fra Poi	me 230: 16 bytes nt-to-Point Prot Address: 0xff	s on wire (128 tocol	bits), 16 bytes capture	d (128 bits) on i	nterface 0	
Poi	me 230: 16 bytes nt-to-Point Prot Address: 0xff Control: 0x03	s on wire (128 tocol	bits), 16 bytes capture	d (128 bits) on i	nterface 0	
Poi	me 230: 16 bytes nt-to-Point Prof Address: 0xff Control: 0x03 Protocol: Passwo	s on wire (128 tocol ord Authenticat:	bits), 16 bytes capture	d (128 bits) on i	nterfac 0	
Poi	me 230: 16 bytes nt-to-Point Prof Address: 0xff Control: 0x03 Protocol: Password Password Auther	s on wire (128 tocol ord Authenticat: ntication Proto	bits), 16 bytes capture ion Protocol (0xc023) col	d (128 bits) on i	nterface 0	
Poi	me 230: 16 bytes nt-to-Point Prof Address: 0xff Control: 0x03 Protocol: Passwo Password Auther Code: Authentica	s on wire (128 tocol ord Authenticat: ntication Proto ite-Request (1)	bits), 16 bytes capture ion Protocol (0xc023) col	d (128 bits) on i	nterface 0	
Poi	me 230: 16 bytes nt-to-Point Prof Address: 0xff Ontrol: 0x03 Protocol: Passwo Password Auther Code: Authentica Identifier: 1	s on wire (128 tocol ord Authenticat: ntication Proto nte-Request (1)	bits), 16 bytes capture ion Protocol (0xc023) col	d (128 bits) on i	nterface 0	
Poi Poi	me 230: 16 byte: nt-to-Point Prof Address: 0xff Control: 0x03 Protocol: Passwo Password Auther Code: Authentic Identifier: 1 Length: 12	s on wire (128 tocol ord Authenticat: ntication Proto ite-Request (1)	bits), 16 bytes capture ion Protocol (0xc023) col	d (128 bits) on i	nterface 0	
Poi	me 230: 16 bytes nt-to-Point Prof ddress: 0xff Control: 0x03 Protocol: Passwo Password Authen Code: Authentica Identifier: 1 Length: 12 Data	s on wire (128 tocol ord Authenticat: ntication Proto ite-Request (1)	bits), 16 bytes capture ion Protocol (Øxc023) col	d (128 bits) on i	nterface 0	
Poi Poi	me 230: 16 byte: nt-to-Point Prof lddress: 0xff Control: 0x03 Protocol: Passwo Password Authen Code: Authentica Identifier: 1 Length: 12 Data Peer-ID-Lengti	s on wire (128 tocol wrd Authenticat: ntication Proto ite-Request (1) h: 2	bits), 16 bytes capture ion Protocol (0xc023) col	d (128 bits) on i	nterface 0	
Poi Poi	me 230: 16 byte: nt-to-Point Proi Address: 0xff Control: 0x03 Protocol: Passwor Password Auther Code: Authentica Cdentifier: 1 Length: 12 Jata Peer-ID-Lengti Peer-ID: R2	s on wire (128 tocol and Authenticat: ntication Proto te-Request (1) h: 2	bits), 16 bytes capture ion Protocol (θxc823) col	d (128 bits) on i	nterface 0	
Poi Poi	me 230: 16 bytes nt-to-Point Proi didress: 0xff Control: 0x03 Protocol: Password Auther Code: Authentica Cidentifier: 1 Length: 12 Data Peer-ID-Lengt! Password-Leng	s on wire (128 tocol mrd Authenticat: ntication Proto tte-Request (1) h: 2 th: 4	bits), 16 bytes capture ion Protocol (0xc023) col	d (128 bits) on i	nterface θ	



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。

					◎
lo.	Time	Source	Destination	Protocol	Length Info
	225 569.547000	N/A	N/A	PPP LCP	18 Configuration Request
	226 569.750000	N/A	N/A	PPP LCP	22 Configuration Request
	227 569.750000	N/A	N/A	PPP LCP	22 Configuration Ack
	228 572.547000	N/A	N/A	PPP LCP	18 Configuration Request
	229 572.547000	N/A	N/A	PPP LCP	18 Configuration Ack
	230 572.562000	N/A	N/A	PPP PAP	16 Authenticate-Request (Peer-ID='R2', Password='seig')
	231 572.578000	N/A	N/A	PPP PAP	52 Authenticate-Ack (Message='Welcome to use Quidway ROUTER, Huawei Tech.')
	232 572.594000	N/A	N/A	PPP IPCP	14 Configuration Request
	233 572.594000	N/A	N/A	PPP IPCP	14 Configuration Request
	234 572.594000	N/A	N/A	PPP IPCP	14 Configuration Ack
	235 572.609000	N/A	N/A	PPP IPCP	14 Configuration Ack
					12 Febr Brownet
Fr Po	236 582.547000 ame 232: 14 bytes int-to-Point Prof	N/A s on wire (112 tocol	N/A bits), 14 bytes capture	d (112 bits) on i	12 croo request >
Fr Po	236 582.547000 ame 232: 14 bytes int-to-Point Prot Address: 0xff Control: 0x03 Protocol: Intern P IP Control Prot	N/A s on wire (112 tocol net Protocol Cor tocol	N/A bits), 14 bytes capture trol Protocol (0x8021)	d (112 bits) on i	12 crookequest
Po	236 582.547000 ame 232: 14 bytes int-to-Point Prot Address: 0xff Control: 0x03 Protocol: Intern PIP Control Prot Code: Configurat	N/A s on wire (112 tocol het Protocol Cor tocol cion Request (1)	N/A bits), 14 bytes capture itrol Protocol (0x8021)	d (112 bits) on i	12 CRD Request
PP	236 582.547000 ame 232: 14 byte: int-to-Point Prod Address: 0xff Control: 0x03 Protocol: Intern P IP Control Prod Code: Configurat Identifier: 1 (0	N/A s on wire (112 tocol tocol cion Request (1) xx01)	N/A bits), 14 bytes capture trol Protocol (0x8021)	d (112 bits) on i	trenface 0
Fr Po	236 582.547000 ame 232: 14 byte: int-to-Point Proi Address: 0xff Control: 0x03 Protocol: Intern P IP Control Proi Code: Configurat Identifier: 1 (0 Length: 10	N/A s on wire (112 tocol net Protocol Con tocol cion Request (1) bx01)	N/A bits), 14 bytes capture trol Protocol (0x8021)	d (112 bits) on i	12 CFD0 Request
PPP	236 582.547000 ame 232: 14 byte: int-to-Point Proi Address: 0xff Control: 0x03 Protocol: Intern P IP Control Prot Code: Configurat Identifier: 1 (0 Length: 10 Options: (6 byte V IP Address	N/A s on wire (112 tocol tocol cion Request (1) xx01) es), IP Address	N/A bits), 14 bytes capture trol Protocol (0x8021)	d (112 bits) on i	12 croo κequest γ
r Po PP	236 582.547000 ame 232: 14 bytes int-to-Point Prot Address: 0xff Control: 0x03 Protocol: Intern P IP Control Prot Code: Configurat Identifier: 1 (0 Options: (6 byte > IP Address Type: IP Add	N/A s on wire (112 tocol het Protocol Cor tocol cion Request (1) xx01) es), IP Address Idress (3)	N/A bits), 14 bytes capture trol Protocol (0x8021)	d (112 bits) on i	aterface 0
Fr Po	236 582.547000 ame 232: 14 byte: int-to-Point Prov Address: 0xff Control: 0x03 Protocol: Intern P IP Control Prov Code: Configurat Identifier: 10 Options: (6 byte > IP Address Type: IP Ad Length: 6	N/A s on wire (112 tocol het Protocol Cor tocol (ion Request (1) tx01) es), IP Address (3)	N/A bits), 14 bytes capture trol Protocol (0x8021)	d (112 bits) on i	a z crio request a z cr

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

ю.	Time	Source	Destination	Protocol	Length Info	
*	13 23.672000	192.168.1.1	192.168.1.2	ICMP	88 Echo (ping) request	id=0xcdab, seq=256/1, ttl=255 (reply in 14)
-	14 23.703000	192.168.1.2	192.168.1.1	ICMP	88 Echo (ping) reply	id=0xcdab, seq=256/1, ttl=255 (request in 13)
	15 24.172000	192.168.1.1	192.168.1.2	ICMP	88 Echo (ping) request	id=0xcdab, seq=512/2, ttl=255 (reply in 16)
	16 24.172000	192.168.1.2	192.168.1.1	ICMP	88 Echo (ping) reply	id=0xcdab, seq=512/2, ttl=255 (request in 15)
	17 24.656000	192.168.1.1	192.168.1.2	ICMP	88 Echo (ping) request	id=0xcdab, seq=768/3, ttl=255 (reply in 18)
	18 24.656000	192.168.1.2	192.168.1.1	ICMP	88 Echo (ping) reply	id=0xcdab, seq=768/3, ttl=255 (request in 17)
	19 25.156000	192.168.1.1	192.168.1.2	ICMP	88 Echo (ping) request	id=0xcdab, seq=1024/4, ttl=255 (reply in 20)
	20 25.156000	192.168.1.2	192.168.1.1	ICMP	88 Echo (ping) reply	id=0xcdab, seg=1024/4, ttl=255 (request in 19)
	21 25.641000	192.168.1.1	192.168.1.2	ICMP	88 Echo (ping) request	id=0xcdab, seq=1280/5, ttl=255 (reply in 22)
	22 25.656000	192.168.1.2	192.168.1.1	ICMP	88 Echo (ping) reply	id=0xcdab, seg=1280/5, ttl=255 (request in 21)
F	rame 13: 88 bytes pint-to-Point Pro	on wire (704 bits)), 88 bytes captured ((704 bits) on i	nterface 0	
	Address: Øxtt					
	Control: 0x03					
	Protocol: Inter	net Protocol versio	n 4 (0x0021)			
- T	nternet Protocol	Version 4, Src: 192	2.168.1.1, Dst: 192.16	58.1.2		
-						

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
<pre>[R2-Serial1/0/0]ppp chap password cipher seig</pre>	//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。



PPI	,					表达式…	+
No.	Tine	Source	Destination	Protocol	Length Info		^
	13 23.953000	N/A	N/A	PPP LCP	8 Termination Request		
	14 23.969000	N/A	N/A	PPP LCP	8 Termination Ack		
	15 36.563000	N/A	N/A	PPP LCP	18 Configuration Request		
	16 36.610000	N/A	N/A	PPP LCP	23 Configuration Request		
	17 36.610000	N/A	N/A	PPP LCP	23 Configuration Ack		
	18 39.547000	N/A	N/A	PPP LCP	18 Configuration Request		
	19 39.547000	N/A	N/A	PPP LCP	18 Configuration Ack		
	20 39.563000	N/A	N/A	PPP CHAP	25 Challenge (NAME='', VALUE=0xa359644c0dcc6c9a3620c244106da1bc)	1.0	_
	21 39.578000	N/A	N/A	PPP CHAP	27 Response (NAME='R2', VALUE=0xe8e6bd2092bdb6af6a23886709cc9f0f)		
	22 39.594000	N/A	N/A	PPP CHAP	20 Success (MESSAGE='Welcome to .')		
	23 39.594000	N/A	N/A	PPP IPCP	14 Configuration Request		
	24 39.594000	N/A	N/A	PPP IPCP	14 Configuration Request		
	25 39.594000	N/A	N/A	PPP IPCP	14 Configuration Ack		
	26 39.610000	N/A	N/A	PPP IPCP	14 Configuration Nak		
	27 39.610000	N/A	N/A	PPP IPCP	14 Configuration Request		
	28 39.610000	N/A	N/A	PPP TPCP	14 Configuration Ack	 	~
> Fr	ame 16: 23 bytes	on wire (184 b	oits), 23 bytes captured	(184 bits) on in	terface 0		
v Po	int-to-Point Pro	tocol					
	Address: 0xff						
	Control: 0x03						
	Protocol: Link	Control Protoco	1 (0xc021)				
Y PP	P Link Control P	rotocol					
	Code: Configurat	tion Request (1)				
	Identifier: 2 (0x02)					
	Length: 19						
>	Ontions: (15 hv	tes). Maximum R	eceive Unit Authenticat	ion Protocol Mag	zic Number		

Options: (15 bytes), Maximum Receive Unit, Authentication Protocol, Magic Number

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。

					140004
lo. Time	Source	Destination	Protocol	Length Info	
13 23.953	000 N/A	N/A	PPP LCP	8 Termination Request	
14 23.969	000 N/A	N/A	PPP LCP	8 Termination Ack	
15 36.563	000 N/A	N/A	PPP LCP	18 Configuration Request	
16 36.610	000 N/A	N/A	PPP LCP	23 Configuration Request	
17 36.610	000 N/A	N/A	PPP LCP	23 Configuration Ack	
18 39.547	000 N/A	N/A	PPP LCP	18 Configuration Request	
19 39.547	000 N/A	N/A	PPP LCP	18 Configuration Ack	
20 39.563	000 N/A	N/A	PPP CHAP	<pre>25 Challenge (NAME='', VALUE=0xa359644c0dcc6c9a3620c244106da1bc)</pre>	
21 39.578	000 N/A	N/A	PPP CHAP	27 Response (NAME='R2', VALUE=0xe8e6bd2092bdb6af6a23886709cc9f0f)	
22 20 504	200 N/A	N/A	PPP CHAP	20 Success (MESSAGE='Welcome to .')	
22 39.594	000 11/1				
22 39.594	000 N/A	N/A	PPP IPCP	14 Configuration Request	
22 39.594 23 39.594 24 39.594 Frame 21: 27 Point-to-Poir	000 N/A 000 N/A bytes on wire (216 b t Protocol	N/A N/A sits), 27 bytes captured	PPP IPCP PPP IPCP (216 bits) on in	14 Configuration Request 14 Configuration Request terface θ	
22 39.594 23 39.594 24 39.594 Point-to-Poir Address: 0 Control: 0 Protocol:	000 N/A 000 N/A bytes on wire (216 b t Protocol cff c03 Challenge Handshake /	N/A N/A N/S), 27 bytes captured Authentication Protocol	PPP IPCP PPP IPCP (216 bits) on in (0xc223)	14 Configuration Request 14 Configuration Request terface 0	
<pre>22 39.594 23 39.594 24 39.594 > Frame 21: 27 > Point-to-Poir Address: 0 Control: 0 Protocol: > PPP Challenge</pre>	000 N/A 000 N/A bytes on wire (216 b t Protocol cff 603 Handshake Authentic	N/A N/A its), 27 bytes captured Authentication Protocol ation Protocol	PPP IPCP PPP IPCP (216 bits) on in (0xc223)	14 Configuration Request 14 Configuration Request terface 0	
22 39.594 23 39.594 24 39.594 P Frame 21: 27 Point-to-Point Address: 0 Control: 0 Protocol: PPP Challenge Code: Resp Identifier Length: 23	000 N/A 000 N/A bytes on wire (216 b t Protocol cff cff challenge Handshake A Handshake Authentic onse (2) : 1	N/A N/A its), 27 bytes captured Authentication Protocol ation Protocol	PPP IPCP PPP IPCP (216 bits) on in (0xc223)	14 Configuration Request 14 Configuration Request terface θ	
22 39.594 23 39.594 24 39.594 Prame 21: 27 Point-to-Poir Address: 0 Control: 0 Protocol: 0 PPP Challenge Code: Resp Identifier Length: 23 V Data	000 N/A 000	N/A N/A its), 27 bytes captured Authentication Protocol ation Protocol	PPP IPCP PPP IPCP (216 bits) on in (0xc223)	14 Configuration Request 14 Configuration Request terface θ	
22 99-394 23 39.594 24 39.594 > Frame 21: 27 > Point-to-Point Address: 0 Control: 0 Protocol: > PPP Challenge Code: Resp Identifier Length: 23 > Data Value 51	where the second	N/A N/A its), 27 bytes captured Authentication Protocol ation Protocol	PPP IPCP PPP IPCP (216 bits) on in (0xc223)	14 Configuration Request 14 Configuration Request terface 0	
22 99-394 23 39.594 24 39.594 Prame 21: 27 Address: 0 Control: 0 Protocol: PPP Challenge Code: Resp Identifiez Length: 22 V Data Value 51	which wire (216 b bytes on wire (216 b t Protocol (ff challenge Handshake Handshake Authentic onse (2) : 1 ze: 16 Sechd2992bdb6aff6a238	N/A N/A its), 27 bytes captured Authentication Protocol ation Protocol	PPP IPCP PPP IPCP (216 bits) on in (0xc223)	14 Configuration Request 14 Configuration Request terface 0	

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	

实验7 PPP的配置与分析 🗙 67

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)。

III ppp						▲ 表达式…
No.	Tine	Source	Destination	Protocol	Length Info	
	18 39.547000	N/A	N/A	PPP LCP	18 Configuration Request	
	19 39.547000	N/A	N/A	PPP LCP	18 Configuration Ack	
1	20 39.563000	N/A	N/A	PPP CHAP	25 Challenge (NAME='', VALUE=0xa359644c0dcc6c9a3620c244106da1bc)	
	21 39.578000	N/A	N/A	PPP CHAP	27 Response (NAME='R2', VALUE=0xe8e6bd2092bdb6af6a23886709cc9f0f)	
	22 39.594000	N/A	N/A	PPP CHAP	20 Success (MESSAGE='Welcome to .')	
	23 39.594000	N/A	N/A	PPP IPCP	14 Configuration Request	
	24 39.594000	N/A	N/A	PPP IPCP	14 Configuration Request	
	25 39.594000	N/A	N/A	PPP IPCP	14 Configuration Ack	
	26 39.610000	N/A	N/A	PPP IPCP	14 Configuration Nak	_
	27 39.610000	N/A	N/A	PPP IPCP	14 Configuration Request	
	28 39.610000	N/A	N/A	PPP IPCP	14 Configuration Ack	

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。

岳R1	X
R1	
The device is running!	
<pre><r1>ping 192.168.1.2 PING 192.168.1.2: 56 data bytes, press CTRL C to</r1></pre>	break
Reply from 192.168.1.2: bytes=56 Sequence=2 ttl=	255 time=60 ms
Reply from 192.168.1.2: bytes=56 Sequence=3 ttl=	255 time=20 ms
Reply from 192.168.1.2: bytes=56 Sequence=4 ttl=	255 time=10 ms
Reply from 192.168.1.2: bytes=56 Sequence=5 ttl=	255 time=30 ms
192.168.1.2 ping statistics 5 packet(s) transmitted 5 packet(s) received 0.00% packet loss round-trip min/avg/max = 10/28/60 ms	
<r1></r1>	

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 TO	CP 子层
	C. MAC 子层和 LLC 子层	D. LLC 子层和 ICI	MP 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 L	.CP
	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	F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

70



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。



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

E PC1						_		X	
基础配置	命令行	组播	UDP发包	工具	串口				
0.00% p round-t	acket loss rip min/av	s vq/max = :	31/31/	32 ms				^	
PC>ning 1	92 168 1	3							
		, 							
Ping 192. From 192.	168.1.3: 3 168.1.3: 1	32 data b oytes=32	ytes, seq=1	Press (ttl=128	Ctrl_C = 3 time=:	to break 31 ms			
From 192.	168.1.3: H	oytes=32	seq=2	ttl=128	3 time=:	31 ms			
From 192. From 192.	168.1.3: H	oytes=32 oytes=32	seq=3 seq=4	ttl=128	3 time=:	32 ms			
From 192.	168.1.3: 1	oytes=32	seq=5	tt1=128	3 time=:	32 ms			
192.1	192.168.1.3 ping statistics								
5 packe 5 packe	t(s) trans t(s) rece	smitted ived							
0.00% p	0.00% packet loss								
round-t	rip min/a	rg/max -	51/51/	52 IIIS					
PC>								*	

图 3-19 PC1 ping PC3

No.	Time	Source	Destination	Protocol	Length Info		
	1 0.000000	192.168.1.1	192.168.1.3	ICMP	74 Echo (ping) request	id=0x349b, seq=1/256, ttl=128 (reply in 2)	
	2 0.016000	192.168.1.3	192.168.1.1	ICMP	74 Echo (ping) reply	id=0x349b, seq=1/256, ttl=128 (request in 1)	
	3 1.047000	192.168.1.1	192.168.1.3	ICMP	74 Echo (ping) request	id=0x359b, seq=2/512, ttl=128 (reply in 4)	
	4 1.063000	192.168.1.3	192.168.1.1	ICMP	74 Echo (ping) reply	id=0x359b, seq=2/512, ttl=128 (request in 3)	
	5 2.094000	192.168.1.1	192.168.1.3	ICMP	74 Echo (ping) request	id=0x369b, seq=3/768, ttl=128 (reply in 6)	
	6 2.110000	192.168.1.3	192.168.1.1	ICMP	74 Echo (ping) reply	id=0x369b, seq=3/768, ttl=128 (request in 5)	
	7 3.141000	192.168.1.1	192.168.1.3	ICMP	74 Echo (ping) request	id=0x379b, seq=4/1024, ttl=128 (reply in 8)	
	8 3.157000	192.168.1.3	192.168.1.1	ICMP	74 Echo (ping) reply	id=0x379b, seq=4/1024, ttl=128 (request in 7)	
	9 4.188000	192.168.1.1	192.168.1.3	ICMP	74 Echo (ping) request	id=0x389b, seq=5/1280, ttl=128 (reply in 10)	
L	10 4.204000	192.168.1.3	192.168.1.1	ICMP	74 Echo (ping) reply	id=0x389b, seq=5/1280, ttl=128 (request in 9)	
 Et > > Ir > Ir 	thernet II, Src: Destination: Hu Source: HuaweiT Type: IPv4 (0x0 ternet Protocol ternet Control N	HuaweiTe_61:20:28 aweiTe_83:2c:6a (54 e_61:20:28 (54:89:9 800) Version 4, Src: 19 Message Protocol	(54:89:98:61:20:28), [:89:98:83:2c:6a) 8:61:20:28) 2.168.1.1, Dst: 192.16	0st: HuaweiTe_8 58.1.3	3:2c:6a (54:89:98:83:2c:6a)		
0000 0010 0020 0030 0040	54 89 98 83 2 00 3c 9b 34 4 01 03 08 00 5 0e 0f 10 11 1 1e 1f 20 21 2	c 6a 54 89 98 61 2 0 00 80 01 dc 37 c 1 e2 34 9b 00 01 0 2 13 14 15 16 17 1 2 23 24 25 26 27	0 28 08 00 45 00 T. 0 a8 01 01 c0 a8 8 09 0a 0b 0c 0d 8 19 1a 1b 1c 1d 	,jT. a (E. 4@7 .Q.4 !"#\$% &'			



(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

74

(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。



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。

实验 8 集线器与交换机原理分析 💉 75

PC1			-		;
基础配置命令	行 组播 UDP发包]	具串口			
地址					
IPv4	O IPv6				
目的MAC地址:	54-89-98-D4-34-50	源MAC地址: 54-89-98-61-20-28			
目的IP地址:	192 . 168 . 1 . 4	源IP地址: 192 . 168 . 1 . 1			
目的端口号:	888 (0~65535)	源端口号: 888 (0~65535)			
VLAN		教报包信息			
VLAN Vlan ID:	优先级:	(0~7) 数据包长度: 56 (28~65535) MTU: 1500	(28~)	1500)	
输入十六进制学行	守串数据 :				
┃ □周期发送 时间	间隔: 1000 ms 发	包个数: 0 发送	停止		

图 3-22 PC1 发包工具配置

PC5	_					_				_		
基础配置	命令行	ī	組播し	JDP发包工具	串口							
地址												
● IPv4		O IPv6										
目的MAC地	址:	54-89-98-	66-74-24		源M	IAC地址:	54-89-9	8-1C-1A-5	7			
目的叩地址	t:	192 . 1	68.1.	6	源I	⁹ 地址:	192	168 .	1.5			
目的端口号	<u>-</u> :	888	(0~65535))	源	端口号:	888	(0~	55535)	_		
VLAN					数据包	信息						
	lan ID:		优先级:	(0~7)	数据包	长度: 56	(2	8~65535)	MTU: 15	500	(28~15	00
栽捉												
•••••••••••••••••••••••••••••••••••••	进制字符串	晶数据:										
												1
I												
□ 国期代送	时间间	1000		부는 소 관	20							1

图 3-23 PC5 发包工具配置

▶计算机网络实验教程——基于华为 eNSP+Wireshark	
---------------------------------	--

76 🗙

是伽伽市	命令行		组播	UDP发包T具	串口			
		-	-11/10					
地址								
IPv4		O IPv6						
目的MAC地	5址:	54-89-98-	61-20-28		源MAC地	<u>此</u> : 54-8	9-98-D4-34-50	54
目的IP地址	ŀ	192 . 1	168.1	. 1	源IP地址:	192	2.168.1.4	
日的海口系	2.	888	(0~655	35)	酒牌口号	. 888	(0~65535)	
VLAN					数据包信息			
VLAN	L		신수 서도 신편 .	(0 T	数据包信息		(20 crcar) MTL [500 (20 1500
			PG/G#X*	(0.1)	8X14 C1 1/132*			(20-1000
数据								
输入十六	进制字符串	数据:						
11.22 5 1 2 1								S

图 3-24 PC4 发包工具配置

基础配置	命令行	5.	组播	UDP发包工具	串口				
地址									
● IPv4	C) IPv6							
目的MACH	地址: [54-89-98	3-1C-1A-57		源M	IAC地址:	54-89-98-66-74-24		
目的IP地力	<u>t</u> : [192 .	168 . 1	. 5	源I	P地址:	192 . 168 . 1 . 6		
目的端口等	- €: [8	388	(0~655	35)	源	耑口号:	888 (0~65535)		
VLAN					数据包	信息			
	lan ID:		优先级:	(0~7) 数据包	长度: 56	(28~65535) MTU: 1500	(:	8~150
al de			20400.0003						
300 MA (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	;讲制字符串数	浙据:							
	×2.011.11.443	~ DH -							

图 3-25 PC6 发包工具配置