实验五: ARP 协议分析

一、实验目的

- 1、掌握报文分析的基本方法;
- 2、掌握 Wireshark 软件的基本使用方法;
- 3、掌握使用 Wireshark 进行数据包抓取和分析的基本操作;
- 4、理解 ARP 报文格式和各字段含义;
- 5、理解 ARP 协议的通信过程。

二、实验学时

2 学时

三、实验类型

验证型

四、实验需求

1、硬件

每人配备计算机1台。

2、软件

Windows 7 以上操作系统, 安装 Wireshark 网络嗅探软件。

3、网络

实验室局域网支持,能够访问校园网。

4、工具

无。

五、实验理论

- 1、网络嗅探的工作原理;
- 2、Wireshark 软件的基本使用方法;
- 3、ARP 协议原理与报文结构;
- 4、请查阅资料,列举几种常见的网络分析工具,并填写表 5-1。

表 5-1 网络分析工具对比分析一览表

序号	软件名称	版本号	软件开发商	安装环境
1				

六、实验任务

1、完成 Wireshark 软件的安装和基本操作的学习;

2、完成 ARP 报文结构的分析;

3、完成 ARP 通信过程的分析。

七、实验内容及步骤

1、Wireshark 的基本操作

(1) 下载软件包

可通过官方网站(http://www.wireshark.org)获得Wireshark软件安装程序;

可通过本课程网站(http://network.ke.51xueweb.cn)下载本教程所使用的 Wireshark 软件版本。

(2) 安装软件

①双击Wireshark安装程序,进入如图5-1所示的Wireshark安装界面,点击【Next>】 开始进行安装。在安装过程中,会提示用户选择安装相关组件程序,选择默认安装组件,具体如图 5-2 所示。

Wireshark 2.2.6 (64-bit) Setup Welcome to Wireshark 2.2.6 (64-bit) Setup	Choose Components Choose which features of Wireshark 2.2.6 (64-bit) you want to install.	
This weard will guide you through the installation of Wireshark. Before starting the installation, make sure Wireshark is not running. Click 'Next' to continue.	The following components are available for installation. Select components to install:	
	B-IV Pupins & Extensions B-IV Tools Tools Description Space required: 171.0MB Position your mouse over a component to see its description.	
Next > Cancel	Wireshark Installer (tm) < Back Next > Cancel	
图 5-1 安装提示	图 5-2 组件选择	

②选择自定义配置,如创建快捷方式和文件扩展等,如图 5-3 所示。③用户可使用默认的 Wireshark 安装目录,也可自行修改安装路径,如图 5-4 所示。

Select Additional Tasks Which additional tasks should be done?	Choose Install Location Choose the folder in which to install Wireshark 2.2.6 (64-bit).
Create Shortcuts Ø Wreshark Start Menu Item Ø Wreshark Desktop Icon Ø Wreshark Legacy Start Menu Item Ø Wreshark Legacy Desktop Icon Ø Wreshark Legacy Desktop Icon Ø Wreshark Legacy Desktop Icon	Choose a directory in which to install Wireshark.
Wessian Legacy Quark Lead of Loon Fel Extensions Associate trace file extensions to Wireshark Associate trace file extensions to Wireshark Legacy None Extensions: 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, ipfix, mplog, out, pcap, pcapng, pkg, pkt, rf5, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, wpz vershark Installer (tm)	Destination Folder Space required: 171.0MB Space available: 20.8GB Wireshark Installer (tm) <back< td=""> Next ></back<>
图 5-3 选择自定义配置	图 5-4 安装路径

④选择安装 WinPcap 软件。WinPcap 是针对 Windows 32 平台上的抓包和网络分析的一个框架软件,是 Windows 平台下免费、公共的网络访问系统。选择安装该框架软件,如图 5-5 所示,点击【Next>】继续进行 Wireshark 软件安装。

Install WinPcap?	Install USBPcap?
WinPcap is required to capture live network data. Should WinPcap be installed?	USBPcap is required to capture USB traffic. Should USBPcap be installed (experimental)?
Currently installed WinPcap version	Currently installed USBPcap version
WinPcap 4.1.3	USBPcap is currently not installed
Install	Instal
V Install WinPcap 4.1.3	Install USBPcap 1.1.0.0-g794bf26-5
If selected, the currently installed WinPcap 4.1.3 will be uninstalled first.	(Use Add/Remove Programs first to uninstall any undetected old USBPcap versions)
	Important notice
	In case of issue after installation, please use the system restore point created or read https://github.com/desowin/usbpcap/issues/3
What is WinPcap?	What is USBPcap?
/ireshark Installer (tm)	Wireshark Installer (tm)
< Back Next > Cancel	< Back Install Cancel
	四 F C 不完准 USPingeon

⑤不安装 USBPcap 软件。USBPcap 是针对 USB 设备进行分析的一个框架软件,本 实验不针对 USB 设备进行网络分析,所以不安装该框架,如图 5-6 所示。点击【Install】, 开始进行 Wireshark 软件安装。

⑥Wireshark 软件在安装过程中将安装 WinPcap 框架,根据默认安装提示,完成该框架的安装,如图 5-7 所示。

⑦点击【Finish】完成 Wireshark 软件的安装,如图 5-8 所示。

WinPcap 4.1.3 Setup Installing Please wait while WinPcap 4.1.3 is being installed. Extract: Packet.dl 100%	Wireshark 2.2.6 (64-bit) Setup Completing Wireshark 2.2.6 (64-bit) Setup Wireshark 2.2.6 (64-bit) has been installed on your Click Finish to dose Setup. Dom Wireshark 2.2.6 (64-bit)
Nullsoft Install System v2.46	Show News
图 5-7 安装 Winpcap	图 5-8 安装完成

⑧打开 Wireshark 软件,界面展示如图 5-9 所示,选择某一网卡适配器,选择【Start】,可查看该网卡上所传输的数据报文信息,如图 5-10 所示。



2、ARP 数据包分析

(1) 创建 ARP 协议抓包任务

打开 Wireshark, 在【Filter】选项中输入报文过滤条件"<u>arp</u>",选择【Start】, 开始 进行报文采集, 如图 5-11 所示。

Filter: arp	Expression Clear Apply Save	
WIRESHARK The World Version 2.2.6 (s Most Popular Network Protocol Analyzer v2.2.6-0-g32dac6a)	
Capture	Files	Online
 Interface List (continetion) packet) Start Coose one or more interfaces to capture from, then 本地送版 Capture Options Sura capture who detailed options Capture Help How to Capture 	Start Open Recent:	Website Website Website User's Guide The User's Guide (online version) Security Work with Winehark as securely as possible
Step by step to a successful capture setup		

(2) 对数据包进行分析

在 Wireshark 的抓包窗体中,可以发现整个软件分为三个区域,如图 5-12 所示。上



部分为抓取的数据包,中间部分为数据详细分析,下部分为数据包的内容。

(3) 从多条 ARP 协议数据报文中任意选择其中一条数据报文,对该数据报文进行 详细分析,并填写表 5-2。

序号	字段名称	字段长度	起始	位置	字段值	字段表示的信息
1	Hardware type		第	位		
2	Protocol type		第	位		
3	Hardware size		第	位		
4	Protocol size		第	位		
5	Opcode		第	位		
6	Sender MAC address		第	位		
7	Sender IP address		第	位		
8	Target MAC address		第	位		
9	Target IP address		第	位		
	抓取数据包的详细内	內容:				
10						

表 5-2 ARP 报文分析

3、ARP 通信过程数据包分析

(1) 创建 ARP 协议抓包任务

根据过程2中的方法获取ARP协议通信过程的数据包。

(2) ARP 请求报文分析

在 Wireshark 的抓包窗体中,选择一条请求数据报文进行详细分析,如图 5-13 所示,并填写表 5-3。

ile Edit View Go Capture An	nalyze Statistics Telephony Tools	Internals He	elp	
0 0 🛋 🔳 🔬 🗎 🗎	8 2 9 4 4 4 4 5 4		2, 0, 0, 17 🚆 🖾 🥵 % 📜	
ilter: arp		- Expressio	n Clear Apply Save	
o. Time Source	Destination	Protocol	Length Info	
6245 2303.8940/ Compaiin_	_e5:T8:44 DIGITAIC_IA:/6:	22 ARP	42 Who has 1/2.1/.101.1? Tell 1/2.1/.101.2	
6246 2303.89539 Digitalc_	_1a:76:22	44 ARP	60 172.17.101.1 is at 00:03:0f:1a:76:22	
6330 2332.39344 Compalin_	_e5:f8:44 DigitalC_1a:76:	22 ARP	42 Who has 172.17.101.1? Tell 172.17.101.2	
6331 2332.39472 DigitalC.	_1a:76:22 Compalin_e5:f8:	44 ARP	60 172.17.101.1 1s at 00:03:01:1a:76:22	
6402 2361.39383 Compalin_	_e5:f8:44 DigitalC_1a:76:	22 ARP	42 who has 172.17.101.1? Tell 172.17.101.2	
6403 2361.39502 DigitalC	_1a:76:22 Compalin_e5:18:	44 ARP	60 172.17.101.1 15 at 00:03:01:1a:76:22	
6471 2379.63049 AsustekC_	_89:92:e9 Broadcast	ARP	60 Who has 172.17.101.1? Tell 172.17.101.4	
6515 2386. 89311 Compalin_	_e5:f8:44 DigitalC_1a:/6:	22 ARP	42 Who has 1/2.1/.101.1? Tell 1/2.1/.101.2	
6516 2386.89432 DigitalC_	_1a:/6:22 Compaiin_es:t8:	44 ARP	60 1/2.1/.101.1 15 at 00:03:07:14:/6:22	
6584 2415. 39245 Comparin	_e5:16:44 DigitalC_ta:/6:	ZZ ARP	42 Who has 1/2.1/.101.1? Tell 1/2.1/.101.2	
6585 2415. 39366 DigitalC	_ia:/6:22 Compalin_es:r8:	44 ARP	60 1/2.1/.101.1 15 at 00:03:07:1a:/6:22	
6605 2428 20285 pigitalc	_es:16:44 DigitalC_Id:/6:	ZZ ARP	42 WHO Has 1/2.1/.101.1: Tell 1/2.1/.101.2	
6606 2438, 59585 Digitale	Comparin_es.re.	44 ARP	60 the has 172 17 101 12 Tell 172 17 101 4	
0050 2458.05000 ASUSCERC	as as a stroadcast	AKE	00 WHO HAS 172.17.101.1: TETT 172.17.101.4	
Frame 6584: 42 bytes on	wire (336 bits), 42 bytes	captured (336 bits) on interface 0	
Ethernet II Src: Compal	Tn e5.f8.44 (20.1a.06:e5:1	8:44), Dst:	: DigitalC_1a:76:22 (00:03:0f:1a:76:22)	
Address Resolution Proto	col (request)			
Haroware type: Etherne	π (1)			
Protocol type: IPv4 (0	x0800)			
Hardware size: 6				
Protocol size: 4				
Opcode: request (1)				
000 0000000 00000011 00	001111 00011010 01110110 0	0100010 001	.00000 00011010	
008 00000110 11100101 11:	111000 01000100 00001000 0	0000110 000	000000 00000001D	
	000110 00000100 00000000 0	0000001 001	.00000 00011010	
020 0000000 00000011 00	001111 00011010 01110110 0	0100010 101	01100 00010001	
			е.	
028 01100101 00000001				

图 5-13 ARP 请求报文

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Hardware type		第 位		
2	Protocol type		第 位		
3	Hardware size		第 位		
4	Protocol size		第 位		
5	Opcode		第 位		
6	Sender MAC address		第 位		
7	Sender IP address		第 位		
8	Target MAC address		第 位		
9	Target IP address		第 位		
	抓取数据包的详细内	9容:			
10					

表 5-3 ARP 请求报文分析

(3) ARP 应答报文分析

在 Wireshark 的抓包窗体中,选择上述请求报文所对应的应答报文进行详细分析, 如图 5-14 所示,并填写表 5-4。

^ 本地连接 [Wireshark 2.2.6 (v2.2.6-0-g32dac6a)	1		
e <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatist	ics Telephon <u>y T</u> ools Internals <u>H</u>	elp	
	🗢 🔿 🐬 👱 🗐 🖬 G	R Q Q 🖭 👪 🗹 🥵 % 💢	
lter: arp	 Expression 	on Clear Apply Save	
. Time Source	Destination Protocol	Length Info	
0245 2303.8940/ Compaiin_e5:T8:44	DIGITAIC_LA:/6:22 ARP	42 Who has 1/2.1/.101.1? Tell 1/2.1/.101.2	
6246 2303.89539 DigitalC_1a:76:22	Compalin_e5:t8:44 ARP	60 172.17.101.1 1s at 00:03:0f:1a:76:22	
6330 2332.39344 Compalin_e5:t8:44	DigitalC_1a:76:22 ARP	42 Who has 172.17.101.1? Tell 172.17.101.2	
6331 2332.394/2 DigitalC_1a:/6:22	Compalin_e5:t8:44 ARP	60 1/2.1/.101.1 is at 00:03:0f:1a:/6:22	
6402 2361.39383 Comparin_e5:T8:44	DigitalC_1a:/6:22 ARP	42 Who has 1/2.1/.101.1? Tell 1/2.1/.101.2	
6403 2361.39502 DigitalC_1a:/6:22	Compaiin_e5:T8:44 ARP	60 1/2.1/.101.1 15 at 00:03:0T:1a:/6:22	
64/1 23/9.63049 ASUSTEKC_89:92:69	Broadcast ARP	60 Who has 1/2.1/.101.1? Tell 1/2.1/.101.4	
6515 2386.89311 Comparin_e5:T8:44	DigitalC_Ia:/6:22 ARP	42 Who has 1/2.1/.101.1? Tell 1/2.1/.101.2	
6510 2380.89432 DigitalC_1a:/0:22	Compatin_es:18:44 ARP	60 1/2.1/.101.1 IS at 00:03:01:14:/6:22	
6584 2415.39245 Comparin_e5:18:44	Compality of the ARP	42 WHO HAS 1/2.1/.101.1: Tell 1/2.1/.101.2	
6585 2415.39366 DigitalC_1a:/6:22	Digitalc 12:76:22 APP	42 who has 172 17 101 12 Toll 172 17 101 2	
6605 2428 20285 pigitalc 12:76:22	Compalin o5:f8:44	42 WHO Has 1/2.1/.101.1: Tell 1/2.1/.101.2	
6606 2428 62066 Asustoka 80:02:00	Readcast ARP	60 who has 172 17 101 12 Toll 172 17 101 4	
CO30 2430. 03000 ASUSCERC_03.52.125	- · · · · · · · · · · · · · · · · · · ·		
Frame 6585: 60 bytes on wire (480	bits), 60 bytes captured (4	480 bits) on interface O	
Ethernet II, Src: DigitalC_1a:76:2	2 (00:03:0f:1a:76:22), Dst	: CompalIn_e5:f8:44 (20:1a:06:e5:f8:44)	
Address Resolution Protocol (reply	0		
Hardware type: Ethernet (1)	_		
Protocol type: IPv4 (0x0800)			
Hardware size: 6			
Protocol size: 4			
Opcode: reply (2)			
00 00100000 00011010 00000110 111	00101 11111000 01000100 000	000000 00000011 D	
08 00001111 00011010 01110110 001	00010 00001000 00000110 000	000000 00000001v"	
10 00001000 0000000 00000110 000	00100 00000000 00000010 000	000000 00000011	
18 00001111 00011010 01110110 001	00010 10101100 00010001 01	L00101 00000001Ve.	
28 01100101 00000010 01000101 000	00000 00000000 01001111 000	000000 00000000 e.EO	
30 0000000 0000001 0000000 000	000000 0000000 0000000 000		
★地连接: ive capture in progress> File:	Packets: 18824 · Displayed: 320 (1.7	%)	Profile: Default

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Hardware type		第 位		
2	Protocol type		第 位		
3	Hardware size		第 位		
4	Protocol size		第 位		
5	Opcode		第 位		
6	Sender MAC address		第 位		
7	Sender IP address		第 位		
8	Target MAC address		第 位		
9	Target IP address		第 位		
	抓取数据包的详细内]容:			
10					

表 5-4 ARP 应答报文分析

(4) 对比分析

根据 ARP 请求和应答的报文内容,比较两个数据报文内容的 5 个关键差别,并填

写表 5-5。

序号	字段名称	请	求报文	应答报文		
		字段值	字段表示信息	字段值	字段表示的信息	
1						
2						
3						
4						
5						
	对比描述详细内容:					
6						

表 5-5 ARP 通信过程报文对比分析

八、实验分析

1、ARP 原理

(1) ARP 的基本原理是什么?

(2) ARP 的主要作用是什么?

2、ARP 通信报文分析

(1)观察实验过程中捕获的多个 ARP 请求报文,观察这些报文的以太网目的地址 是否相同,分析其原因?

(2)观察实验过程中捕获的多个 ARP 应答报文,观察这些报文的以太网目的地 址是否相同,分析其原因?