



警示

1. 实验报告如有雷同，雷同各方当次实验成绩均以 0 分计。
2. 当次小组成员成绩只计学号、姓名登录在下表中的。
3. 在规定时间内未上交实验报告的，不得以其他方式补交，当次成绩按 0 分计。
4. 实验报告文件以 PDF 格式提交。

院系	数据科学与计算机学院	班 级	教务_1_班	组长	劳马东
学号	16337113	16337102	16337100		
学生	劳马东	黄梓林	黄英桂		
实验分工					
黄英桂	HTTP 协议分析		黄梓林	ftp 协议分析	
劳马东	Telnet 协议分析				

【实验题目】网络嗅探与协议分析实验

【实验目的】通过网络嗅探了解网络数据类型、了解网络工作原理；学习相关工具的使用。

【实验内容】

第二版书：

- (1) HTTP 协议分析：完成实验教程实例 2-3 的实验，回答实验提出的问题及实验思考。(P62)
- (2) FTP 协议分析：完成实验教程实例 2-4。回答实验提出的问题及实验思考。(P66)
- (3) telnet 协议分析：完成实验教程实例 2-5 实验 (P71)

第一版书：

- (1) HTTP 协议分析：完成实验教程实例 9-3 的实验，回答实验提出的问题及实验思考。(P302)
- (2) FTP 协议分析：完成实验教程实例 9-4。回答实验提出的问题及实验思考。(P305)
- (3) telnet 协议分析：完成实验教程实例 9-5 实验 (P311)

【实验要求】

一些重要信息需给出截图。

注意实验步骤的前后对比！

【实验记录】(如有实验拓扑请自行画出，要求自行画出拓扑图)

(一) HTTP 协议分析

(1) 两种 HTTP 报文。七个。服务器使用了 80 端口，客户机使用了 57875、57878、57879、57880、57881、57882、57884 七个端口。

(2) HTTP 请求报文

方法	GET	版本	HTTP1.1	URL	http://sysu.edu.cn
首部字段名	字段值	意义			
Host	sysu.edu.cn	主机名			
Connection	keep-alive	保持持续连接			
Upgrade-Insecure-Requests	1	浏览器自动请求升级			
User-Agent	Mozilla/5.0 (Windows)	所用的网页浏览器			



	ws NT 6.1; WOW64) AppleWeb Kit/53 7.36 (KHTML, like Gecko) Chrome/ 55.0.288 3.87 Safari/5 37.36	
Accept	text/html, application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8	客户端接受的响应类型
Accept-Encoding	gzip, deflate, sdch	优先的内容编码
Accept-Language	zh-CN,zh;q=0.8	指定的自然语言是中文
Cookie	safedog-flow-item=1FD2C37B921D6107F257847C591E5819;UM_distinctid=15f01d389f61b5-0f91d20d96d8d-26596859-1fa400-1	服务器接收到的 Cookie 信息



	5f01d38 9f7ae	
--	------------------	--

HTTP 应答报文

版本	HTTP1.1	状态码	200	短语	OK
首部字段名	字段值	意义			
Vary	Accept-Encoding	代理服务器缓存的管理信息			
Content-Encoding	gzip	实体主体的适用的编码方式			
Last-Modified	Thu, 11 Apr 2013 06:43:52 GMT	资源的最后修改日期时间			
ETag	"2157330749"	资源的匹配信息			
Content-Type	text/html	实体主体的媒体类型			
Accept-Ranges	bytes	可处理范围请求			
Content-Length	276	实体主体的大小（单位：字节）			
Date	Mon, 09 Apr 2018 09:16:57 GMT	创建报文的日期时间			
Server	lighttpd/1.4.35	当前服务器上安装的 http 服务器应用程序的信息			

(3)

客户端端口号	服务器端口号	所包括的报文号	工作过程
57875	80	13	客户机请求连接服务器
57875	80	26	服务器确认客户机请求
57875	80	28	客户机与服务器建立连接
57875	80	42	客户机请求数据
57875	80	44	服务器对请求进行回应

(4) 200 OK

思考题：

(1) 172.18.34.149，也就是客户机。通过输入 ip 地址发送请求然后发送 tcp 包建立连接。

(2) 似乎并没有结束回话，因为建立了长连接。

(3) POST 方法比 GET 方法多了一个 HTML Form URL Encoded (HTML 方式编码) 的表项。里面的内容是一些键值对，似乎说明 POST 是隐式传送。

(二) FTP 协议分析

步骤 6：



(1)

截图：

No.	Time	Source	Destination	Proto	Length	Info
4	0.006935	192.168.1.10	192.168.1.20	FTP	92	Response: 220 Serv-U FTP Server v11.3 ready...
12	14.032953	192.168.1.20	192.168.1.10	FTP	69	Request: USER 16337102
13	14.035195	192.168.1.10	192.168.1.20	FTP	90	Response: 331 User name okay, need password.
15	20.272929	192.168.1.20	192.168.1.10	FTP	69	Request: PASS huang123
16	20.275555	192.168.1.10	192.168.1.20	FTP	84	Response: 230 User logged in, proceed.
18	32.760070	192.168.1.20	192.168.1.10	FTP	60	Request: QUIT
19	32.761872	192.168.1.10	192.168.1.20	FTP	85	Response: 221 Goodbye, closing session.

> Frame 4: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
> Ethernet II, Src: 00:88:99:00:13:51 (00:88:99:00:13:51), Dst: Shenzhen_0e:be:33 (44:33:4c:0e:be:33)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.20
> Transmission Control Protocol, Src Port: 21, Dst Port: 2032, Seq: 1, Ack: 1, Len: 38
> File Transfer Protocol (FTP)

表 9-7 FTP 报文格式分析

源 IP 地址	192.168.1.20	源端口	21
目标 IP 地址	192.168.1.10	目标端口	2032
FTP 地址	字段值	字段所表达的信息	
Response Code	Service ready for new user(220)	为新用户准备服务	
Response Arg	Serv-u FTP server V11.3 ready	ftp 服务器已经准备	

(2)

表 9-8 FTP 指令和响应过程分析

过程	指令/响应	报文号	报文信息
User	Request	12	220 USER 16337102
	Response	13	331 User name okay, need password
Password	Request	15	PASS huang123
	Response	16	User logged in, proceed
Quit	Request	18	QUIT
	Response	19	221 Goodbye, closing session

(3)

截图：



No.	Time	Source	Destination	Protocol	Length	Info
2	0.000012	192.168.1.20	192.168.1.10	TCP	66	2041 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460...
3	0.000375	192.168.1.10	192.168.1.20	TCP	66	21 → 2041 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
4	0.000423	192.168.1.20	192.168.1.10	TCP	54	2041 → 21 [ACK] Seq=1 Ack=1 Win=65700 Len=0
5	0.006855	192.168.1.10	192.168.1.20	FTP	92	Response: 220 Serv-U FTP Server v11.3 ready...
6	0.007993	192.168.1.20	192.168.1.10	FTP	70	Request: USER anonymous
7	0.011055	192.168.1.10	192.168.1.20	FTP	124	Response: 331 User name okay, please send com...
8	0.011447	192.168.1.20	192.168.1.10	FTP	79	Request: PASS chrome@example.com
9	0.013497	192.168.1.10	192.168.1.20	FTP	95	Response: 530 Sorry, no ANONYMOUS access allo...
10	0.013671	192.168.1.20	192.168.1.10	FTP	60	Request: QUIT
11	0.015379	192.168.1.10	192.168.1.20	FTP	85	Response: 221 Goodbye, closing session.
12	0.015540	192.168.1.20	192.168.1.10	TCP	54	2041 → 21 [FIN, ACK] Seq=48 Ack=181 Win=65520...
13	0.015580	192.168.1.10	192.168.1.20	TCP	60	21 → 2041 [FIN, ACK] Seq=181 Ack=48 Win=65536...
14	0.015645	192.168.1.20	192.168.1.10	TCP	54	2041 → 21 [RST, ACK] Seq=49 Ack=182 Win=0 Len=0
15	0.016005	192.168.1.10	192.168.1.20	TCP	60	21 → 2041 [RST, ACK] Seq=182 Ack=49 Win=0 Len=0
21	12.107593	192.168.1.20	192.168.1.10	TCP	66	2042 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460...
22	12.108090	192.168.1.10	192.168.1.20	TCP	66	21 → 2042 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
23	12.108179	192.168.1.20	192.168.1.10	TCP	54	2042 → 21 [ACK] Seq=1 Ack=1 Win=65700 Len=0
24	12.114676	192.168.1.10	192.168.1.20	FTP	92	Response: 220 Serv-U FTP Server v11.3 ready...
25	12.116979	192.168.1.20	192.168.1.10	FTP	69	Request: USER 16337102

> Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Shenzhen_0e:be:33 (44:33:4c:0e:be:33), Dst: 00:88:99:00:13:51 (00:88:99:00:13:51)
> Internet Protocol Version 4, Src: 192.168.1.20, Dst: 192.168.1.10
> Transmission Control Protocol, Src Port: 2041, Dst Port: 21, Seq: 0, Len: 0

No.	Time	Source	Destination	Protocol	Length	Info
26	12.119432	192.168.1.10	192.168.1.20	FTP	90	Response: 331 User name okay, need password.
27	12.119824	192.168.1.20	192.168.1.10	FTP	69	Request: PASS huang123
28	12.120978	192.168.1.10	192.168.1.20	FTP	84	Response: 230 User logged in, proceed.
29	12.121280	192.168.1.20	192.168.1.10	FTP	60	Request: SYST
30	12.121808	192.168.1.10	192.168.1.20	FTP	73	Response: 215 UNIX Type: L8
31	12.122150	192.168.1.20	192.168.1.10	FTP	59	Request: PWD
32	12.122603	192.168.1.10	192.168.1.20	FTP	85	Response: 257 "/" is current directory.
33	12.123087	192.168.1.20	192.168.1.10	FTP	62	Request: TYPE I
34	12.123423	192.168.1.10	192.168.1.20	FTP	74	Response: 200 Type set to I.
35	12.123672	192.168.1.20	192.168.1.10	FTP	62	Request: SIZE /
36	12.124069	192.168.1.10	192.168.1.20	FTP	78	Response: 550 /: Is a directory.
37	12.124192	192.168.1.20	192.168.1.10	FTP	61	Request: CWD /
38	12.124641	192.168.1.10	192.168.1.20	FTP	82	Response: 250 Directory changed to /
39	12.124753	192.168.1.20	192.168.1.10	FTP	60	Request: PASV
40	12.125189	192.168.1.10	192.168.1.20	FTP	102	Response: 227 Entering Passive Mode (192,168,...
41	12.125369	192.168.1.20	192.168.1.10	TCP	66	2043 → 2036 [SYN] Seq=0 Win=8192 Len=0 MSS=14...
42	12.125570	192.168.1.10	192.168.1.20	TCP	66	2036 → 2043 [SYN, ACK] Seq=0 Ack=1 Win=8192 L...
43	12.125600	192.168.1.20	192.168.1.10	TCP	54	2043 → 2036 [ACK] Seq=1 Ack=1 Win=65536 Len=0
44	12.125776	192.168.1.20	192.168.1.10	FTP	63	Request: LIST -1

> Frame 26: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
> Ethernet II, Src: 00:88:99:00:13:51 (00:88:99:00:13:51), Dst: Shenzhen_0e:be:33 (44:33:4c:0e:be:33)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.20
> Transmission Control Protocol, Src Port: 21, Dst Port: 2042, Seq: 39, Ack: 16, Len: 36
✦ File Transfer Protocol (FTP)
 > 331 User name okay, need password.\r\n

No.	Time	Source	Destination	Protocol	Length	Info
45	12.125964	192.168.1.10	192.168.1.20	TCP	60	[TCP Window Update] 2036 → 2043 [ACK] Seq=1 A...
46	12.126540	192.168.1.10	192.168.1.20	FTP	107	Response: 150 Opening ASCII mode data connect...
47	12.126905	192.168.1.10	192.168.1.20	FTP-DATA	461	FTP Data: 407 bytes
48	12.126907	192.168.1.10	192.168.1.20	TCP	60	2036 → 2043 [FIN, ACK] Seq=408 Ack=1 Win=1048...
49	12.127141	192.168.1.20	192.168.1.10	TCP	54	2043 → 2036 [ACK] Seq=1 Ack=409 Win=65280 Len=0
50	12.127617	192.168.1.20	192.168.1.10	TCP	54	2043 → 2036 [RST, ACK] Seq=1 Ack=409 Win=0 Le...
54	12.327456	192.168.1.20	192.168.1.10	TCP	54	2042 → 21 [ACK] Seq=80 Ack=328 Win=65372 Len=0
55	12.327967	192.168.1.10	192.168.1.20	FTP	114	Response: 226 Transfer complete. 407 bytes tr...
56	12.328756	192.168.1.20	192.168.1.10	FTP	60	Request: QUIT
57	12.330094	192.168.1.10	192.168.1.20	FTP	85	Response: 221 Goodbye, closing session.
58	12.330566	192.168.1.20	192.168.1.10	TCP	54	2042 → 21 [FIN, ACK] Seq=86 Ack=419 Win=65280...
59	12.330776	192.168.1.10	192.168.1.20	TCP	60	21 → 2042 [ACK] Seq=419 Ack=87 Win=65536 Len=0
60	12.341297	192.168.1.10	192.168.1.20	TCP	60	21 → 2042 [RST, ACK] Seq=419 Ack=87 Win=0 Len=0
61	20.324994	192.168.1.20	192.168.1.10	TCP	66	2044 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460...
62	20.325312	192.168.1.10	192.168.1.20	TCP	66	21 → 2044 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
63	20.325358	192.168.1.20	192.168.1.10	TCP	54	2044 → 21 [ACK] Seq=1 Ack=1 Win=65700 Len=0
64	20.331909	192.168.1.10	192.168.1.20	FTP	92	Response: 220 Serv-U FTP Server v11.3 ready...
65	20.332240	192.168.1.20	192.168.1.10	FTP	70	Request: USER anonymous
66	20.335120	192.168.1.10	192.168.1.20	FTP	124	Response: 331 User name okay, please send com...

> Frame 26: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
> Ethernet II, Src: 00:88:99:00:13:51 (00:88:99:00:13:51), Dst: Shenzhen_0e:be:33 (44:33:4c:0e:be:33)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.20
> Transmission Control Protocol, Src Port: 21, Dst Port: 2042, Seq: 39, Ack: 16, Len: 36
✦ File Transfer Protocol (FTP)
 > 331 User name okay, need password.\r\n

表 9-9FTP 传送过程中的报文



报文类型	所包括的报文序号	客户端口	服务器端口
控制连接的建立	2、3、4	2041	21
数据连接的建立	21、22、23	2043	2036
FTP 数据传送	47	2036	2043
FTP 指令传送和响应	6、8、10、25、31、33...	2041	21
数据连接的释放	48、59、50	2043	2036
控制连接的释放	无		

(4) 从协议层面分析，FTP-DOS 与 FTP-WEB

相同之处：在建立连接时，使用的都是 TCP 协议，且都是使用两条 TCP 连接完成文件传输：控制连接和数据连接

不同之处：FTP-DOS 连接时，传输数据的默认方式是主动方式；而 FTP-WEB 连接时，传输数据的默认方式是被动方式

(5) 截图：

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000012	192.168.1.20	192.168.1.10	TCP	66	2041 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460...
3	0.000375	192.168.1.10	192.168.1.20	TCP	66	21 → 2041 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
4	0.000423	192.168.1.20	192.168.1.10	TCP	54	2041 → 21 [ACK] Seq=1 Ack=1 Win=65700 Len=0
5	0.006855	192.168.1.10	192.168.1.20	FTP	92	Response: 220 Serv-U FTP Server v11.3 ready...
6	0.007993	192.168.1.20	192.168.1.10	FTP	70	Request: USER anonymous

在步骤 5 中，FTP 中的匿名账户是 anonymous

步骤 7：

(1) TCP 三次握手过程：

- TCP 客户端向服务器发出连接请求报文，报文首部中的 SYN=1，同时选择一个初始序列号 seq=x，客户端进入 SYN-SENT 状态。
- TCP 服务器收到请求报文后，如果同意连接，则发出确认报文，报文段中 SYN=1,ACK=1 确认号是 ack=x+1，同时选择初始序号 seq=y；服务器进程进入 SYN-RCVD 状态。
- TCP 客户进程收到确认后，向服务器发送确认报文，报文中 ACK=1，确认号 ack=y+1，序号 seq=x+1；客户端进入 ESTABLISHED 状态。服务器收到确认报文后也会进入 ESTABLISHED 状态。

四次握手终止过程：

- 客户端发送一个 FIN 报文（序号为 M），用来关闭客户端到服务器的数据传送，客户端进入 FIN_WAIT_1 状态。
- 服务器收到 FIN 报文后，发送一个 ACK 报文给客户端，确认序号为 M+1，服务器进入 CLOSE_WAIT 状态。
- 服务器发送一个 FIN 报文（序号为 N），用来关闭服务器到客户端的数据传送，服务器进入 LAST_ACK 状态。
- 客户端收到 FIN 报文后，进入 TIME_WAIT 状态，接着发送一个 ACK 报文给服务器，序号为 N+1，服务器进入 CLOSED 状态，完成四次挥手。

(2) 从捕获的数据包分析三次握手的过程、四次握手终止的过程：

三次握手截图：

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.20	192.168.1.10	TCP	62	2032 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
2	0.000275	192.168.1.10	192.168.1.20	TCP	62	21 → 2032 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
3	0.000345	192.168.1.20	192.168.1.10	TCP	54	2032 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0



客户端为 190.168.1.20，服务器端为 192.168.1.10；

客户端向服务器发出连接请求报文，报文首部中的 SYN=1，序列号 seq=0，客户端进入 SYN-SENT 状态；

服务器收到请求报文后，发出确认报文，报文段中 SYN=1,ACK=1，初始序号 seq=0，服务器进程进入 SYN-RCVD 状态；

客户进程收到确认后，向服务器发送确认报文，报文中 ACK=1，序号 seq=1；客户端进入 ESTABLISHED 状态。

四次握手终止截图：

12	0.015540	192.168.1.20	192.168.1.10	TCP	54 2041 → 21 [FIN, ACK] Seq=48 Ack=181 Win=65520 Len=0
13	0.015580	192.168.1.10	192.168.1.20	TCP	60 21 → 2041 [FIN, ACK] Seq=181 Ack=48 Win=65536 Len=0
14	0.015645	192.168.1.20	192.168.1.10	TCP	54 2041 → 21 [RST, ACK] Seq=49 Ack=182 Win=0 Len=0
15	0.016005	192.168.1.10	192.168.1.20	TCP	60 21 → 2041 [RST, ACK] Seq=182 Ack=49 Win=0 Len=0

客户端为 190.168.1.20，服务器端为 192.168.1.10；

客户端发送一个 FIN 报文，用来关闭客户端到服务器的数据传送，客户端进入 FIN_WAIT_1 状态；

服务器端收到 FIN 报文后，发送一个 ACK 报文给客户端，服务器进入 CLOSE_WAIT 状态；

服务器发送一个 FIN 报文，用来关闭服务器到客户端的数据传送，服务器进入 LAST_ACK 状态。

客户端收到 FIN 报文后，进入 TIME_WAIT 状态，接着发送一个 ACK 报文给服务器，服务器进入 CLOSED 状态，完成四次挥手。

实验思考

- (1) 使用控制连接：客户端与服务器建立连接或断开连接；客户端与服务器交换传输数据所需的端口信息，控制命令信息；
使用数据连接：当出现文件发送请求时。

- (2) FTP 协议与 HTTP 协议：

- a. HTTP 协议主要用于浏览网站的，而 FTP 主要用于访问和传输文件的；
- b. FTP 在使用时会建立两个 TCP 连接，控制连接以及数据连接，而 HTTP 在双向传输中使用动态端口；
- c. HTTP 协议使用的语言为超文本标记语言，即 html 语言，传输的数据为二进制格式，而 FTP 能传输 ACSII 数据或者二进制格式的数据；
- d. 整个会话期间，FTP 服务器必须维护关于用户的状态，而无状态的 HTTP 不必维护任何用户的状态信息。

- (3) FTP 协议的安全问题：FTP 的控制连接由 FTP 控制命令完成工作，而 FTP 控制命令以 ASCII 码方式传送（即明文方式），固 FTP 协议并不安全，用户名以及密码可以被用户之外的他人捕获，知晓。

- (4) FTP Server 的口令安全能保证用户名和口令的安全，在不加密的情况下，通过捕获 FTP 报文可以得知用户名以及口令，而在进行口令加密后，在报文的对应字段只能观察到乱码。

截图：

No.	Time	Source	Destination	Protocol	Length	Info
4	0.006935	192.168.1.10	192.168.1.20	FTP	92	Response: 220 Serv-U FTP Server v11.3 ready...
12	14.032953	192.168.1.20	192.168.1.10	FTP	69	Request: USER 16337102
13	14.035195	192.168.1.10	192.168.1.20	FTP	90	Response: 331 User name okay, need password.
15	20.272929	192.168.1.20	192.168.1.10	FTP	69	Request: PASS huang123
16	20.275555	192.168.1.10	192.168.1.20	FTP	84	Response: 230 User logged in, proceed.
18	32.760070	192.168.1.20	192.168.1.10	FTP	60	Request: QUIT
19	32.761872	192.168.1.10	192.168.1.20	FTP	85	Response: 221 Goodbye, closing session.



加密前

No.	Time	Source	Destination	Protocol	Length	Info
1046	14.527913	172.18.32.34	172.18.34.172	FTP	91	Request: \027\003\001\000 9\252\251\033\$*:\375\213\005\364\236fz\...
1047	14.528975	172.18.34.172	172.18.32.34	FTP	176	Response: \027\003\001\000 \320\023\314\336\372z\233\237\261\246\...
1048	14.530007	172.18.32.34	172.18.34.172	FTP	139	Request: \027\003\001\000P\001\2127\330\X\342\022@;1\277?\303z\31...
1051	14.531405	172.18.34.172	172.18.32.34	FTP	224	Response: \027\003\001\000 +M\355\320\244`\307\3628#\326pM>\021\...
1085	14.572995	172.18.34.172	172.18.32.34	FTP	192	Response: \025\003\001\000 \213\370\353\261,\034\2137\314\222!\33...
1838	26.245720	172.18.34.172	172.18.32.34	FTP	91	Response: \025\003\001\000 \275\241\263\237\3027\350%,1\227e)\2...
1856	26.376948	172.18.34.172	172.18.32.34	FTP	91	Response: \025\003\001\000 .\3241\270\0269\$\337b\2540\221`H\275M\...

加密后

(三) Telnet 协议分析

为方便查看两台主机之间传输的报文，在筛选框中加入条件：

((ip.src == 192.168.1.10) && (ip.dst == 192.168.1.20)) ||

((ip.src == 192.168.1.20) && (ip.dst == 192.168.1.10))

1. TCP 连接建立后的第一个 Telnet 协议数据报的功能是进行选项协商吗？在这个数据报中对哪些选项进行了协商？列出他们的选项名和选项代码。
第一个报文是选项协商，报文如下图：

No.	Time	Source	Destination	Protocol	Length	Info
36	12.835875	192.168.1.10	192.168.1.20	TCP	66	2317 → 23 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
37	12.835921	192.168.1.20	192.168.1.10	TCP	66	23 → 2317 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
38	12.837279	192.168.1.10	192.168.1.20	TCP	60	2317 → 23 [ACK] Seq=1 Ack=1 Win=17408 Len=0
41	12.949289	192.168.1.10	192.168.1.20	LLMNR	129	Standard query response 0x1431 PTR 10.1.168.192.in-addr.arpa PTR STU58
47	12.951512	192.168.1.20	192.168.1.10	TELNET	75	Telnet Data ...
48	12.953414	192.168.1.10	192.168.1.20	TELNET	69	Telnet Data ...
49	12.953851	192.168.1.20	192.168.1.10	TELNET	97	Telnet Data ...
50	12.955242	192.168.1.10	192.168.1.20	TELNET	69	Telnet Data ...
51	13.154374	192.168.1.20	192.168.1.10	TCP	54	23 → 2317 [ACK] Seq=65 Ack=31 Win=65536 Len=0

> Transmission Control Protocol, Src Port: 23, Dst Port: 2317, Seq: 1, Ack: 1, Len: 21

▼ Telnet

- > Do Authentication Option
- > Will Echo
- > Will Suppress Go Ahead
- > Do New Environment Option
- > Do Negotiate About Window Size
- > Do Binary Transmission
- > Will Binary Transmission

0000	00 88 99 00 13 51 44 33 4c 0e be 33 08 00 45 00QD3 L..3..E.
0010	00 3d 06 58 40 00 80 06 70 f4 c0 a8 01 14 c0 a8	..=.X@... p.....
0020	01 0a 00 17 09 0d 85 ed 7f f8 55 39 56 f5 50 18U9V.P.
0030	01 00 30 f4 00 00 ff fd 25 ff fb 01 ff fb 03 ff	..0.....%.....
0040	fd 27 ff fd 1f ff fd 00 ff fb 00	.'.....

图 1 第一个 Telnet 协议数据报

其中，选项名为请求类型（如 Do、Will）后面的子命令，展开每个命令，点击子命令，就能在下面的十六进制窗口看到对应的选项代码。如下图：

> Do Authentication Option	
▼ Will Echo	选项名
Command: Will (251)	
Subcommand: Echo	
> Will Suppress Go Ahead	
> Do New Environment Option	
> Do Negotiate About Window Size	
> Do Binary Transmission	
> Will Binary Transmission	选项代码

0000	00 88 99 00 13 51 44 33 4c 0e be 33 08 00 45 00QD3 L..3..E.
0010	00 3d 06 58 40 00 80 06 70 f4 c0 a8 01 14 c0 a8	..=.X@... p.....
0020	01 0a 00 17 09 0d 85 ed 7f f8 55 39 56 f5 50 18U9V.P.
0030	01 00 30 f4 00 00 ff fd 25 ff fb 01 ff fb 03 ff	..0.....%.....
0040	fd 27 ff fd 1f ff fd 00 ff fb 00	.'.....

图 2 协商选项

表 1 Telnet 第一个数据报的协商选项

选项名	选项代码
-----	------



Echo	1
Suppress Go Ahead	3
New Environment Option	39
Negotiate About Window Size	31
Binary Transmission	0

2. 分析上面那个报文，写出所有选项的格式并指出格式中每一部分的意义，填入表 9-12。

展开数据报每一项，其中 command 为请求类型，对应代码在请求类型后括号中的数字或十六进制窗口在给出，如下图：

Do Authentication Option
Will Echo
Command: Will (251)
Subcommand: Echo
Will Suppress Go Ahead
Do New Environment Option
Do Negotiate About Window Size
Do Binary Transmission
Will Binary Transmission

0000 00 88 99 00 13 51 44 33 4c 0e be 33 08 00 45 00QD3 L..3..E.
0010 00 3d 06 58 40 00 80 06 70 f4 c0 a8 01 14 c0 a8 ..=.X@... p.....
0020 01 0a 00 17 09 0d 85 ed 7f f8 55 39 56 f5 50 18U9V.P.
0030 01 00 30 f4 00 00 ff fd 25 ff fb 01 ff fb 03 ff ..0..... %. ..
0040 fd 27 ff fd 1f ff fd 00 ff fb 00

图 3 请求类型

表 9-12 Telnet 报文分析

请求类型	请求类型代码	选项（命令）名称	选项代码	意义
Will	251	Echo	1	发送方希望协商终端将接受到的内容返回给发送者
Will	251	Suppress Go Ahead	3	发送方希望开始抑制前进
Do	253	New Environment Option	39	发送方希望与接受方开始协商新环境选项
Do	253	Negotiate About Window Size	31	发送方希望与接受方开始协商窗口尺寸
Do	253	Binary Transmission	0	发送方希望接受方开始二进制传输
Will	251	Binary Transmission	0	发送方希望开始二进制传输

3. 在 TCP 连接时，Telnet 使用的端口号是多少？
端口号为 23。如下图：

Protocol	Length	Info
TCP	66	2317 → 23 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP	66	23 → 2317 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP	60	2317 → 23 [ACK] Seq=1 Ack=1 Win=17408 Len=0

图 4 Telnet 的 TCP 三次握手

4. 从 TCP 连接建立后开始分析截获的报文，填入表 9-13，Telnet 数据传输只填写客户端输入命令的传输报文。



表 9-13 Telnet 协议工作过程

过程	报文号	功能（选项协商/数据传输）	信息及参数	报文作用
Telnet 选项协商	36	选项协商	2317→23 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	TCP 第一次握手
	37	选项协商	23→2317 [SYN,ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	TCP 第二次握手
	38	选项协商	2317 → 23 [ACK] Seq=1 Ack=1 Win=17408 Len=0	TCP 第三次握手
	47-50	选项协商	Telnet Data...	信息交换
	54-56	选项协商	Telnet Data...	子选项协商
	58-59	数据传输	Telnet Data...	虚拟机发送欢迎信息
	82-85	选项协商	Telnet Data...	协商是否开始执行命令行
Telnet 数据传输	62-67	数据传输	Telnet Data...	输入用户名
	70-81	数据传输	Telnet Data...	输入口令
	82-88	选项协商	Telnet Data...	协商是否开始执行命令行
	139-155	数据传输	Telnet Data...	输入“exit”

5. “远程桌面连接”实验。和 Telnet 的异同？

相同点：

- 1) 连接之前都需要输入对方 IP 地址，输入用户名和口令进行身份验证。
- 2) 都是基于连接的，都有 TCP 的三次握手。

ip_addr = 192.168.199.193						目的端口号
No.	Time	Source	Destination	Protocol	Length	Info
3	3.540733	192.168.199.193	192.168.199.169	TCP	74	57953 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=30026719..
4	3.544903	192.168.199.169	192.168.199.193	TCP	66	3389 → 57953 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=1 SACK_PERM=1
5	3.545013	192.168.199.193	192.168.199.169	TCP	54	57953 → 3389 [ACK] Seq=1 Ack=1 Win=65536 Len=0

图 5 远程桌面连接 TCP 三次握手

不同点：

- 1) 远程桌面连接默认使用 3389 号端口，如上图；Telnet 使用 23 号端口。
- 2) 远程桌面连接的数据使用密文，而 Telnet 是明文。



```
> Frame 6: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interf
> Ethernet II, Src: IntelCor_e9:49:3b (dc:53:60:e9:49:3b), Dst: HonHaiPr_d6:8c
> Internet Protocol Version 4, Src: 192.168.199.193, Dst: 192.168.199.169
> Transmission Control Protocol, Src Port: 57953, Dst Port: 3389, Seq: 1, Ack:
✓ Data (43 bytes)
  Data: 0300002b26e00000000000436f6f6b69653a206d73747368...
  [Length: 43]
```

密文

```
0000 18 4f 32 d6 8c 9f dc 53 60 e9 49 3b 08 00 45 00 .02....S`.I;.E.
0010 00 53 13 6a 40 00 40 06 16 7f c0 a8 c7 c1 c0 a8 .S.j@.@. ....
0020 c7 a9 e2 61 0d 3d ef b5 ab 13 3b 63 50 e7 50 18 ...a.=.. ..;cP.P.
0030 01 00 01 e6 00 00 03 00 00 2b 26 e0 00 00 00 00 ..... .+&.....
0040 00 43 6f 6f 6b 69 65 3a 20 6d 73 74 73 68 61 73 .Cookie: mstshas
0050 68 3d 6c 61 6f 6d 64 0d 0a 01 00 08 00 0b 00 00 h=laomd. ....
0060 00 .
```

图 6 远程桌面连接数据传输

3) 远程桌面连接会使用 UDP 传输数据，而 Telnet 使用 TCP。

ip.addr == 192.168.199.193						
No.	Time	Source	Destination	Protocol	Length	Info
64	8.370729	192.168.199.193	192.168.199.169	UDP	1274	58707 → 3389 Len=1232
65	8.374944	192.168.199.169	192.168.199.193	UDP	1274	3389 → 58707 Len=1232
66	8.381178	192.168.199.193	192.168.199.169	UDP	209	58707 → 3389 Len=167
67	8.393884	192.168.199.169	192.168.199.193	UDP	1208	3389 → 58707 Len=1166
68	8.395259	192.168.199.193	192.168.199.169	UDP	155	58707 → 3389 Len=113
69	8.399966	192.168.199.169	192.168.199.193	UDP	113	3389 → 58707 Len=71
70	8.400623	192.168.199.193	192.168.199.169	UDP	119	58707 → 3389 Len=77
71	8.402391	192.168.199.169	192.168.199.193	UDP	99	3389 → 58707 Len=57
72	8.402675	192.168.199.193	192.168.199.169	TCP	109	57954 → 3389 [PSH, ACK]

```
> Frame 64: 1274 bytes on wire (10192 bits), 1274 bytes captured (10192 bits) on interface 0
> Ethernet II, Src: IntelCor_e9:49:3b (dc:53:60:e9:49:3b), Dst: HonHaiPr_d6:8c:9f (18:4f:32:d6:8c:9f)
> Internet Protocol Version 4, Src: 192.168.199.193, Dst: 192.168.199.169
> User Datagram Protocol, Src Port: 58707, Dst Port: 3389
✓ Data (1232 bytes)
  Data: ffffffff00401801330e098904d004d0269dc17c2a6d4bae...
  [Length: 1232]
```

图 7 远程桌面连接使用 UDP 传输协议

6. Telnet 的口令是否明文传输？

是。70 号报文开始虚拟机要求输入口令，从“password”字样可以看出。之后，开始输出并传输输入的口令，每输入一个字符就发送一个 Telnet 报文和一个 TCP 报文。73-74 是‘4’，75-76 是‘1’，77-78 是‘2’，79-80 是回车换行（口令为“412”），从报文看到，“412”都以明文传输。



No.	Time	Source	Destination	Protocol	Length	Info
70	17.419827	192.168.1.20	192.168.1.10	TELNET	66	Telnet Data ...
73	17.620958	192.168.1.10	192.168.1.20	TCP	60	2317 → 23 [ACK] Seq=575 Ack=426 Win=16896 Len=0
74	18.211176	192.168.1.10	192.168.1.20	TELNET	60	Telnet Data ...
76	18.411227	192.168.1.20	192.168.1.10	TCP	54	23 → 2317 [ACK] Seq=426 Ack=576 Win=65024 Len=0
77	18.412906	192.168.1.10	192.168.1.20	TELNET	60	Telnet Data ...
78	18.612222	192.168.1.20	192.168.1.10	TCP	54	23 → 2317 [ACK] Seq=426 Ack=577 Win=65024 Len=0
79	18.635177	192.168.1.10	192.168.1.20	TELNET	60	Telnet Data ...
80	18.832213	192.168.1.20	192.168.1.10	TCP	54	23 → 2317 [ACK] Seq=426 Ack=578 Win=65024 Len=0
81	19.371045	192.168.1.10	192.168.1.20	TELNET	60	Telnet Data ...

> Frame 70: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Shenzhen_0e:be:33 (44:33:4c:0e:be:33), Dst: 00:88:99:00:13:51 (00:88:99:00:13:51)
> Internet Protocol Version 4, Src: 192.168.1.20, Dst: 192.168.1.10
> Transmission Control Protocol, Src Port: 23, Dst Port: 2317, Seq: 414, Ack: 575, Len: 12
v Telnet
Data: \n
Data: \rpassword:

0000	00 88 99 00 13 51 44 33	4c 0e be 33 08 00 45 00QD3 L...E.
0010	00 34 06 62 40 00 80 06	70 f3 c0 a8 01 14 c0 a8	.4.b@... p.....
0020	01 0a 00 17 09 0d 85 ed	81 95 55 39 59 33 50 18U9Y3P.
0030	00 fe 5a 6a 00 00 0a 0d	70 61 73 77 77 6f 72 64	..Zj....password
0040	3a 20	:	:

图 8 口令输入-70 号报文

No.	Time	Source	Destination	Protocol	Length	Info
70	17.419827	192.168.1.20	192.168.1.10	TELNET	66	Telnet Data ...
73	17.620958	192.168.1.10	192.168.1.20	TCP	60	2317 → 23 [ACK] Seq=575 Ack=426 Win=16896 Len=0
74	18.211176	192.168.1.10	192.168.1.20	TELNET	60	Telnet Data ...
76	18.411227	192.168.1.20	192.168.1.10	TCP	54	23 → 2317 [ACK] Seq=426 Ack=576 Win=65024 Len=0
77	18.412906	192.168.1.10	192.168.1.20	TELNET	60	Telnet Data ...
78	18.612222	192.168.1.20	192.168.1.10	TCP	54	23 → 2317 [ACK] Seq=426 Ack=577 Win=65024 Len=0
79	18.635177	192.168.1.10	192.168.1.20	TELNET	60	Telnet Data ...
80	18.832213	192.168.1.20	192.168.1.10	TCP	54	23 → 2317 [ACK] Seq=426 Ack=578 Win=65024 Len=0
81	19.371045	192.168.1.10	192.168.1.20	TELNET	60	Telnet Data ...

> Frame 74: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: 00:88:99:00:13:51 (00:88:99:00:13:51), Dst: Shenzhen_0e:be:33 (44:33:4c:0e:be:33)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.20
> Transmission Control Protocol, Src Port: 2317, Dst Port: 23, Seq: 575, Ack: 426, Len: 1
v Telnet
Data: 4

图 9 传输字符‘4’的 Telnet 报文

【实验评分】

姓名/学号	评分
劳马东/16337113	99
黄梓林/16337102	99
黄英桂/16337100	99