

中国科学院大学

《计算机网络(研讨课)》实验报告

姓名 寇逸欣 学号 2023K8009922004 专业 计算机科学与技术
实验项目编号 01 实验名称 互联网协议实验

一、实验一：互联网协议实验

1.1 实验内容

本实验主要包括以下内容：

- 在节点 h1 上开启 wireshark 抓包,用 wget 下载 www.ucas.ac.cn 页面。
- 调研说明 wireshark 抓到的几种协议——ARP, DNS, TCP, HTTP, HTTPS。
- 调研解释 h1 下载 ucas 页面的整个过程几种协议的运行机制。

1.2 实验步骤

实验环境:virtualbox + ubuntu24.04 server + mininet + wireshark

由于使用 ubuntu server 版本,默认没有图形界面,因此采用终端命令行操作。并将抓包结果保存为.cap 文件,之后在本地电脑上使用 wireshark 打开分析。在终端中输入以下命令进行实验:

```
sudo apt install wireshark xterm ifupdown
sudo mn --nat
mininet> h1 echo "nameserver 1.2.4.8" > /etc/resolv.conf
mininet> h1 wget www.ucas.ac.cn
```

1.3 实验结果

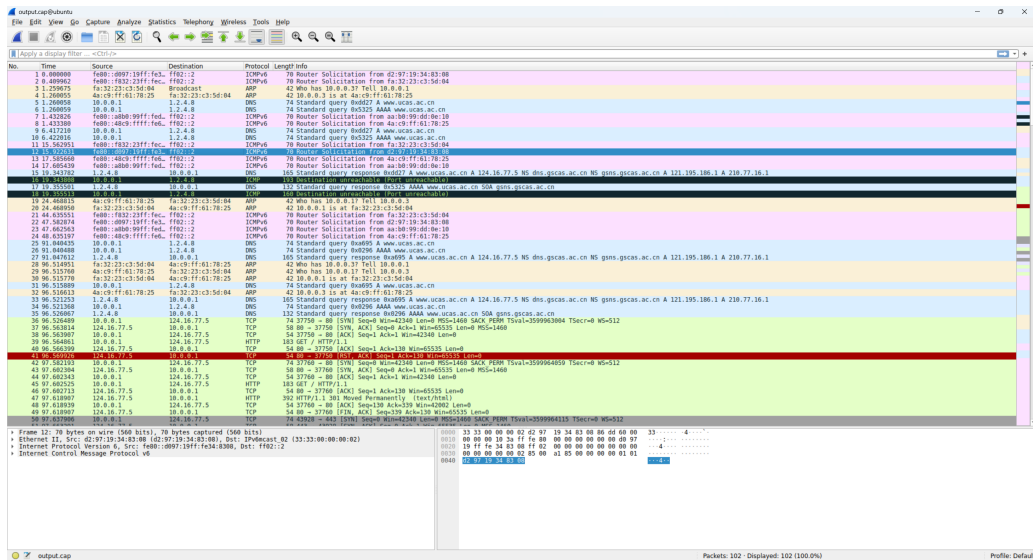


图 1: Wireshark 抓包结果

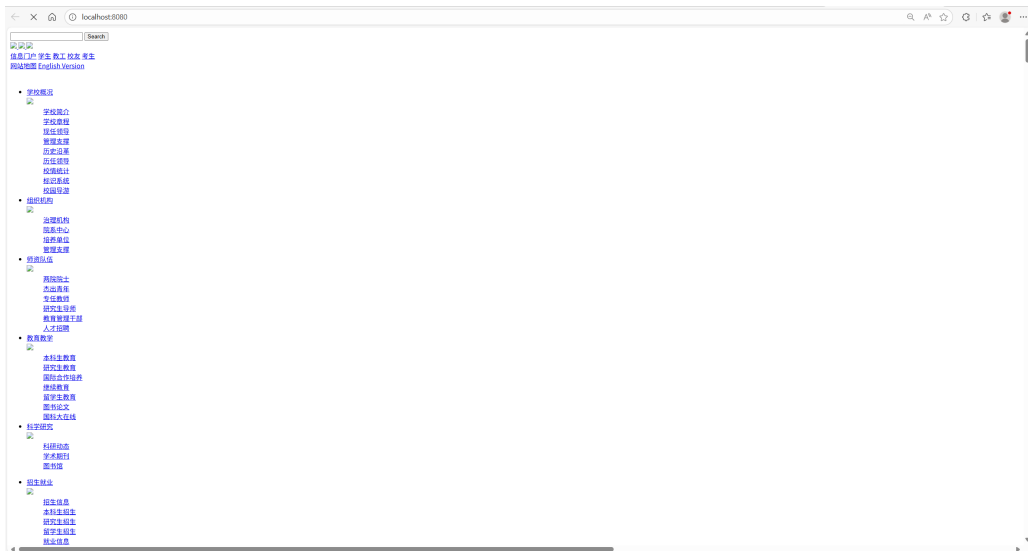


图 2: html 文件

如图1所示,抓包结果中包含了 ARP, DNS, TCP, HTTP, HTTPS 等多种协议。

1.4 实验分析

1.4.1 ARP 协议

ARP 协议(Address Resolution Protocol,地址解析协议)用于将网络层地址(如 IP 地址)解析为数据链路层地址(如 MAC 地址)。在局域网中,当一个主机需要与另一个主机通信时,它需要知道对方的 MAC 地址。ARP 协议通过广播 ARP 请求来实现地址解析。请求包含发送方的 IP 地址和 MAC 地址,以及目标主机的 IP 地址。所有接收到 ARP 请求的主机都会检查请求中的目标 IP 地址,如果匹配自己的 IP 地址,则会发送一个 ARP 响应,包含自己的 MAC 地址。发送方接收到 ARP 响应后,就可以将目标主机的 MAC 地址缓存起来,以便后续通信使用。

No.	Time	Source	Destination	Protocol	Length	Info
20	24.468950	fa:32:23:c3:5d:04	4a:c9:ff:61:78:25	ARP	42	10.0.0.1 is at fa:32:23:c3:5d:04
30	96.515770	fa:32:23:c3:5d:04	4a:c9:ff:61:78:25	ARP	42	10.0.0.1 is at fa:32:23:c3:5d:04
73	218.511843	fa:32:23:c3:5d:04	4a:c9:ff:61:78:25	ARP	42	10.0.0.1 is at fa:32:23:c3:5d:04
4	1.260955	4a:c9:ff:61:78:25	fa:32:23:c3:5d:04	ARP	42	10.0.0.3 is at 4a:c9:ff:61:78:25
32	96.516613	4a:c9:ff:61:78:25	fa:32:23:c3:5d:04	ARP	42	10.0.0.3 is at 4a:c9:ff:61:78:25
75	218.780007	4a:c9:ff:61:78:25	fa:32:23:c3:5d:04	ARP	42	10.0.0.3 is at 4a:c9:ff:61:78:25
19	24.468815	4a:c9:ff:61:78:25	fa:32:23:c3:5d:04	ARP	42	Who has 10.0.0.1? Tell 10.0.0.3
29	96.515760	4a:c9:ff:61:78:25	fa:32:23:c3:5d:04	ARP	42	Who has 10.0.0.1? Tell 10.0.0.3
72	218.511828	4a:c9:ff:61:78:25	fa:32:23:c3:5d:04	ARP	42	Who has 10.0.0.1? Tell 10.0.0.3
3	1.259675	fa:32:23:c3:5d:04	Broadcast	ARP	42	Who has 10.0.0.3? Tell 10.0.0.1
28	96.514951	fa:32:23:c3:5d:04	4a:c9:ff:61:78:25	ARP	42	Who has 10.0.0.3? Tell 10.0.0.1
74	218.779947	fa:32:23:c3:5d:04	4a:c9:ff:61:78:25	ARP	42	Who has 10.0.0.3? Tell 10.0.0.1

图 3: ARP 协议

3 图中展示了 ARP 协议的工作流程。主机 A 需要与主机 B 通信,但不知道主机 B 的 MAC 地址。于是主机 A 广播一个 ARP 请求,询问谁拥有 IP 地址 10.0.0.3。主机 B 收到请求后,发现请求中的目标 IP 地址与自己的 IP 地址匹配,于是发送一个 ARP 响应,告诉主机 A 自己的 MAC 地址为 4a:c9:ff:61:78:25。主机 A 收到响应后,就可以使用该 MAC 地址与主机 B 进行通信。

1.4.2 DNS 协议

DNS 协议 (Domain Name System, 域名系统) 用于将域名解析为 IP 地址。在互联网中, 主机之间的通信是通过 IP 地址进行的, 但为了方便用户记忆, 通常使用域名来代替 IP 地址。当用户在浏览器中输入一个域名时, 计算机首先向 DNS 服务器发送一个 DNS 请求, 请求解析该域名。DNS 服务器收到请求后, 会查找该域名对应的 IP 地址, 并将结果返回给客户端。客户端收到响应后, 就可以使用该 IP 地址与目标主机进行通信。

No.	Time	Source	Destination	Protocol	Length	Info
16	19.343888	10.0.0.1	1.2.4.8	ICMP	163	Destination unreachable (Port unreachable)
18	19.355313	10.0.0.1	1.2.4.8	TCP	160	Destination unreachable (Port unreachable)
26	91.040488	10.0.0.1	1.2.4.8	DNS	74	Standard query 0x0296 AAAA www.ucas.ac.cn
34	96.521368	10.0.0.1	1.2.4.8	DNS	74	Standard query 0x0296 AAAA www.ucas.ac.cn
6	1.268059	10.0.0.1	1.2.4.8	DNS	74	Standard query 0x5325 AAAA www.ucas.ac.cn
10	6.422016	10.0.0.1	1.2.4.8	DNS	74	Standard query 0x5325 AAAA www.ucas.ac.cn
70	213.430621	10.0.0.1	1.2.4.8	DNS	73	Standard query 0x0d66 AAAA www.baidu.com
78	218.704637	10.0.0.1	1.2.4.8	DNS	74	Standard query 0x0d66 AAAA www.baidu.com
82	218.801145	10.0.0.1	1.2.4.8	DNS	86	Standard query 0x09a5 PTR 21.69.242.110.in-addr.arpa
65	126.533637	10.0.0.1	1.2.4.8	DNS	74	Standard query 0xa095 A www.ucas.ac.cn
67	133.653490	10.0.0.1	1.2.4.8	DNS	74	Standard query 0xa095 A www.ucas.ac.cn
25	91.804035	10.0.0.1	1.2.4.8	DNS	74	Standard query 0xa095 A www.ucas.ac.cn
31	96.515889	10.0.0.1	1.2.4.8	DNS	74	Standard query 0xa095 A www.ucas.ac.cn
69	212.430577	10.0.0.1	1.2.4.8	DNS	73	Standard query 0xa0a5 A www.baidu.com
76	218.704940	10.0.0.1	1.2.4.8	DNS	73	Standard query 0xa0a5 A www.baidu.com
5	1.268058	10.0.0.1	1.2.4.8	DNS	74	Standard query 0xb027 A www.ucas.ac.cn
9	6.437210	10.0.0.1	1.2.4.8	DNS	74	Standard query 0xb027 A www.ucas.ac.cn
66	128.551758	10.0.0.1	1.2.4.8	DNS	74	Standard query 0xb784 AAAA www.ucas.ac.cn
68	133.653071	10.0.0.1	1.2.4.8	DNS	74	Standard query 0xb784 AAAA www.ucas.ac.cn
35	96.526067	1.2.4.8	10.0.0.1	DNS	132	Standard query response 0x0296 AAAA www.ucas.ac.cn 50A gns.gscas.ac.cn
17	19.355031	1.2.4.8	10.0.0.1	DNS	132	Standard query response 0x5325 AAAA www.ucas.ac.cn 50A gns.gscas.ac.cn
79	218.708399	1.2.4.8	10.0.0.1	DNS	156	Standard query response 0x0d66 AAAA www.baidu.com CNAME www.a.shifen.com AAAA 2408:871a:2100:186c:0:ff:b07e:3fbc AAAA 2408:871a:2100:1b23:0:ff:b07a:7ebc
83	218.800753	1.2.4.8	10.0.0.1	DNS	175	Standard query response 0x09a5 No such name PTR 21.69.242.110.in-addr.arpa SOA ns1.gnic.net
27	91.847612	1.2.4.8	10.0.0.1	DNS	165	Standard query response 0xa095 A www.ucas.ac.cn A 124.16.77.5 NS dns.gscas.ac.cn NS gns.gscas.ac.cn A 121.195.186.1 A 210.77.16.1
31	96.521253	1.2.4.8	10.0.0.1	DNS	165	Standard query response 0xa095 A www.ucas.ac.cn A 124.16.77.5 NS dns.gscas.ac.cn NS gns.gscas.ac.cn A 121.195.186.1 A 210.77.16.1
71	213.489148	1.2.4.8	10.0.0.1	DNS	132	Standard query response 0xa0a5 A www.baidu.com CNAME www.a.shifen.com A 110.242.69.21 A 110.242.70.57
77	218.704640	1.2.4.8	10.0.0.1	DNS	132	Standard query response 0xa0a5 A www.baidu.com CNAME www.a.shifen.com A 110.242.69.21 A 110.242.70.57
15	19.343782	1.2.4.8	10.0.0.1	DNS	165	Standard query response 0xb027 A www.ucas.ac.cn A 124.16.77.5 NS dns.gscas.ac.cn NS gns.gscas.ac.cn A 121.195.186.1 A 210.77.16.1

图 4: DNS 协议

我们可以选择 Follow UDP Stream 来查看 DNS 请求和响应的详细内容, 如图 5 所示。10.0.0.1 向 1.2.4.8 发送 DNS 查询, 请求解析 www.ucas.ac.cn 的 IPv4(A 记录)和 IPv6(AAAA 记录)地址。1.2.4.8 向 10.0.0.1 返回 DNS 响应, 响应中包含了 www.ucas.ac.cn 的 A 记录(IPv4 地址)、NS 记录(域名服务器)、SOA 记录(起始授权机构)等信息。查询和响应中均显示了 DNS 查询的 ID、类型(A/AAAA/SOA/NS)、目标域名和解析结果。

26	91.040488	10.0.0.1	1.2.4.8	DNS	74	Standard query 0x0296 AAAA www.ucas.ac.cn
34	96.521368	10.0.0.1	1.2.4.8	DNS	74	Standard query 0x0296 AAAA www.ucas.ac.cn
25	91.040435	10.0.0.1	1.2.4.8	DNS	74	Standard query 0xa095 A www.ucas.ac.cn
31	96.515889	10.0.0.1	1.2.4.8	DNS	74	Standard query 0xa095 A www.ucas.ac.cn
35	96.526067	1.2.4.8	10.0.0.1	DNS	132	Standard query response 0x0296 AAAA www.ucas.ac.cn 50A gns.gscas.ac.cn
27	91.847612	1.2.4.8	10.0.0.1	DNS	165	Standard query response 0xa095 A www.ucas.ac.cn A 124.16.77.5 NS dns.gscas.ac.cn NS gns.gscas.ac.cn A 121.195.186.1 A 210.77.16.1
31	96.521253	1.2.4.8	10.0.0.1	DNS	165	Standard query response 0xa095 A www.ucas.ac.cn A 124.16.77.5 NS dns.gscas.ac.cn NS gns.gscas.ac.cn A 121.195.186.1 A 210.77.16.1
33	96.521253	1.2.4.8	10.0.0.1	DNS	165	Standard query response 0xa095 A www.ucas.ac.cn A 124.16.77.5 NS dns.gscas.ac.cn NS gns.gscas.ac.cn A 121.195.186.1 A 210.77.16.1

图 5: DNS 请求和响应的详细内容

1.4.3 TCP 协议

TCP 协议 (Transmission Control Protocol, 传输控制协议) 是一种面向连接的、可靠的传输层协议。它为应用层提供了可靠的数据传输服务, 确保数据包按照顺序到达目的地, 并且在丢失或损坏的情况下能够进行重传。TCP 协议通过三次握手建立连接, 通过四次挥手关闭连接。在数据传输过程中, TCP 协议会对数据进行分段, 并为每个数据段分配序列号, 以便接收方能够按照正确的顺序重组数据。

No.	Time	Source	Destination	Protocol	Length	Info
38	96.563907	10.0.0.1	124.16.77.5	TCP	54	37750 → 80 [ACK] Seq=1 Ack=1 Win=42340 Len=0
36	96.526489	10.0.0.1	124.16.77.5	TCP	74	37750 → 80 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM TSval=3599963084 TSecr=0 WS=512
44	97.602343	10.0.0.1	124.16.77.5	TCP	54	37760 → 80 [ACK] Seq=1 Ack=1 Win=42340 Len=0
48	97.618039	10.0.0.1	124.16.77.5	TCP	54	37760 → 80 [ACK] Seq=130 Ack=330 Win=42002 Len=0
53	97.664476	10.0.0.1	124.16.77.5	TCP	54	37760 → 80 [ACK] Seq=130 Ack=340 Win=42002 Len=0
58	97.697015	10.0.0.1	124.16.77.5	TCP	54	37760 → 80 [FIN, ACK] Seq=130 Ack=340 Win=42002 Len=0
42	97.582193	10.0.0.1	124.16.77.5	TCP	74	37760 → 80 [SYN] Seq=0 Win=42340 Len=0 MSS=1460 SACK_PERM TSval=3599964059 TSecr=0 WS=512
52	97.663358	10.0.0.1	124.16.77.5	TCP	54	43928 → 443 [ACK] Seq=1 Ack=1 Win=42340 Len=0
50	97.637996	10.0.0.1	124.16.77.5	TCP	74	43928 → 443 [SYN] Seq=0 Win=42340 Len=0 MSS=1460 SACK_PERM TSval=3599964115 TSecr=0 WS=512
57	97.696056	124.16.77.5	10.0.0.1	TCP	54	443 → 43928 [ACK] Seq=2 Ack=409 Win=65535 Len=0
59	97.697272	124.16.77.5	10.0.0.1	TCP	54	443 → 43928 [ACK] Seq=2 Ack=417 Win=65535 Len=0
54	97.667348	124.16.77.5	10.0.0.1	TCP	54	443 → 43928 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
51	97.663391	124.16.77.5	10.0.0.1	TCP	58	443 → 43928 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
40	96.566399	124.16.77.5	10.0.0.1	TCP	54	80 → 37750 [ACK] Seq=1 Ack=130 Win=65535 Len=0
41	96.569326	124.16.77.5	10.0.0.1	TCP	54	80 → 37750 [RST, ACK] Seq=1 Ack=130 Win=65535 Len=0
37	96.563314	124.16.77.5	10.0.0.1	TCP	58	80 → 37750 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
47	97.602713	124.16.77.5	10.0.0.1	TCP	54	80 → 37760 [ACK] Seq=1 Ack=130 Win=65535 Len=0
60	97.697273	124.16.77.5	10.0.0.1	TCP	54	80 → 37760 [ACK] Seq=340 Ack=131 Win=65535 Len=0
49	97.618007	124.16.77.5	10.0.0.1	TCP	54	80 → 37760 [FIN, ACK] Seq=130 Ack=130 Win=65535 Len=0
43	97.602384	124.16.77.5	10.0.0.1	TCP	58	80 → 37760 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
56	97.696667	10.0.0.1	124.16.77.5	ICMPv6	68	Client Hello (SHA1-www.ucas.ac.cn)
55	97.696535	10.0.0.1	124.16.77.5	TLSv1	462	Client Hello (SHA1-www.ucas.ac.cn)
39	96.564861	10.0.0.1	124.16.77.5	HTTP	183	GET / HTTP/1.1
45	97.602525	10.0.0.1	124.16.77.5	HTTP	183	GET / HTTP/1.1
47	97.618007	124.16.77.5	10.0.0.1	HTTP	392	HTTP/1.1 301 Moved Permanently (text/html)

图 6: TCP 协议

图 7 展示了一个完整的 HTTP 请求与响应, 以及 TCP 连接的建立和正常关闭过程, 具体如下:

• TCP 三次握手建立连接

- 10.0.0.1 → 124.16.77.5:SYN
- 124.16.77.5 → 10.0.0.1:SYN, ACK

3. 10.0.0.1 → 124.16.77.5: ACK

- HTTP 请求与响应

1. 10.0.0.1 → 124.16.77.5: 发送 HTTP GET 请求

2. 124.16.77.5 → 10.0.0.1: 返回 HTTP/1.1 301 Moved Permanently(网页永久重定向)

- TCP 四次挥手正常断开连接

1. 10.0.0.1 → 124.16.77.5: ACK

2. 10.0.0.1 → 124.16.77.5: FIN, ACK(主动关闭连接)

3. 124.16.77.5 → 10.0.0.1: ACK

4. 124.16.77.5 → 10.0.0.1: FIN, ACK(被动关闭连接)

5. 10.0.0.1 → 124.16.77.5: ACK

No.	Time	Source	Destination	Protocol	Length	Info
42	97.582193	10.0.0.1	124.16.77.5	TCP	74	37760 → 80 [SYN] Seq=0 Win=42340 Len=0 MSS=1460 SACK_PERM TSval=3599964859 TSecr=0 WS=512
43	97.602304	124.16.77.5	10.0.0.1	TCP	58	80 → 37760 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
44	97.602343	10.0.0.1	124.16.77.5	TCP	54	37760 → 80 [ACK] Seq=1 Ack=1 Win=42340 Len=0
45	97.602525	10.0.0.1	124.16.77.5	HTTP	183	GET / HTTP/1.1
46	97.602713	124.16.77.5	10.0.0.1	TCP	54	80 → 37760 [ACK] Seq=1 Ack=130 Win=65535 Len=0
47	97.618907	124.16.77.5	10.0.0.1	HTTP	392	HTTP/1.1 301 Moved Permanently (text/html)
48	97.618939	10.0.0.1	124.16.77.5	TCP	54	37760 → 80 [ACK] Seq=130 Ack=339 Win=42002 Len=0
49	97.618907	124.16.77.5	10.0.0.1	TCP	54	80 → 37760 [FIN, ACK] Seq=339 Ack=130 Win=65535 Len=0
53	97.664476	10.0.0.1	124.16.77.5	TCP	54	37760 → 80 [ACK] Seq=130 Ack=340 Win=42002 Len=0
58	97.697015	10.0.0.1	124.16.77.5	TCP	54	37760 → 80 [FIN, ACK] Seq=130 Ack=340 Win=42002 Len=0
60	97.697273	124.16.77.5	10.0.0.1	TCP	54	80 → 37760 [ACK] Seq=340 Ack=131 Win=65535 Len=0

图 7: TCP 连接的详细内容

1.4.4 HTTP 协议

HTTP 协议(Hypertext Transfer Protocol, 超文本传输协议)是应用层协议,用于在客户端和服务端之间传输超文本数据。当用户在浏览器中输入一个 URL 时,浏览器会向服务器发送一个 HTTP 请求,请求获取指定的资源。服务器收到请求后,会返回一个 HTTP 响应,包含请求的资源 and 状态码。HTTP 协议是无状态的,即每个请求都是独立的,服务器不会记录客户端的状态信息。

No.	Time	Source	Destination	Protocol	Length	Info
39	96.564861	10.0.0.1	124.16.77.5	HTTP	183	GET / HTTP/1.1
45	97.602525	10.0.0.1	124.16.77.5	HTTP	183	GET / HTTP/1.1
47	97.618907	124.16.77.5	10.0.0.1	HTTP	392	HTTP/1.1 301 Moved Permanently (text/html)

图 8: HTTP 协议

1.4.5 HTTPS 协议

HTTPS 协议(Hypertext Transfer Protocol Secure, 安全超文本传输协议)是在 HTTP 协议的基础上,加入了 SSL/TLS 协议进行加密和身份验证。它通过在客户端和服务端之间建立一个安全的加密通道,确保数据在传输过程中的安全性和完整性。HTTPS 协议广泛应用于在线支付、网上银行等对安全性要求较高的场景。

二、 实验二:流完成时间实验

2.1 实验内容

本实验主要包括以下内容:

1. 利用 fct_exp.py 脚本复现上页幻灯片中的图,每个数据点做 3 次实验,取均值
2. 调研解释图中的现象,提示:TCP 传输、慢启动机制

2.2 实验数据

表 1: 流完成时间实验数据

Size (MB)	10.0 Mbps	50.0 Mbps	100.0 Mbps	500.0 Mbps	1000.0 Mbps
1.0	1.154964	0.721915	0.798944	0.792040	0.793336
10.0	8.696521	2.234174	1.484441	1.046817	1.100703
100.0	84.854350	17.423328	9.137862	2.552476	1.797471

根据表1中的数据,我们可以绘制出流完成时间与带宽的关系图,如图9所示。

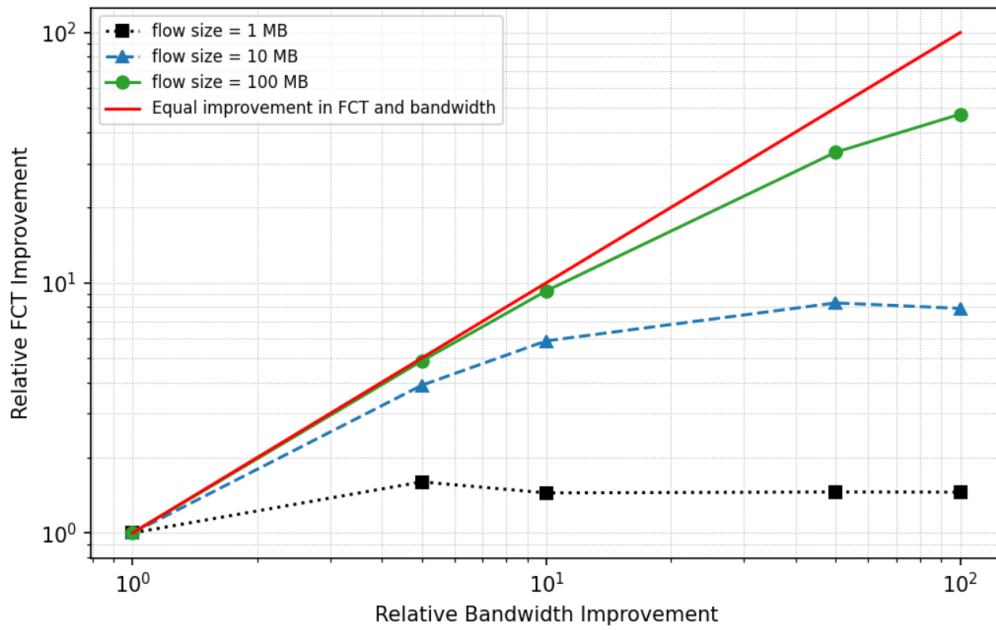


图 9: 流完成时间与带宽的关系图

2.3 实验分析

从图9中可以看出,随着带宽的增加,流完成时间呈现出下降的趋势。这是因为更高的带宽允许更多的数据在单位时间内传输,从而减少了传输所需的时间。然而,流完成时间的下降并不是线性的,尤其是在较低带宽下,流完成时间的变化较为显著,而在较高带宽下,流完成时间的变化趋于平缓。这种现象可以通过 TCP 的慢启动机制来解释。TCP 在连接建立初期采用慢启动算法,初始拥塞窗口较小,随着数据的成功传输,拥塞窗口逐渐增大,从而提高了传输速率。在低带宽下,慢启动阶段占据了较大的比例,因此流完成时间变化较大。而在高带宽下,慢启动阶段相对较短,传输速率更快,流完成时间的变化趋于平缓。此外,随着带宽的增加,其他因素如延迟和协议开销可能会对流完成时间产生更大的影响,从而导致流完成时间的下降幅度减小。