



## 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	计算机学院	班 级	软工 1 班	组长	崔子潇
学号	19308024	19335286	19335040		
学生	崔子潇	郑有为	丁维力		
实验分工					
崔子潇	上机操作 PC1，实验报告		丁维力	上机操作 PC2，完善实验报告	
郑有为	上机操作 PC3，完善实验报告		共同	遇到困难上网找解决方案，讨论和分析实验结果	

【实验题目】搭建自组网（Ad-Hoc）模式无线网络。

【实验目的】掌握自组网（Ad-Hoc）模式无线网络的概念及搭建方法。

【实验拓扑】

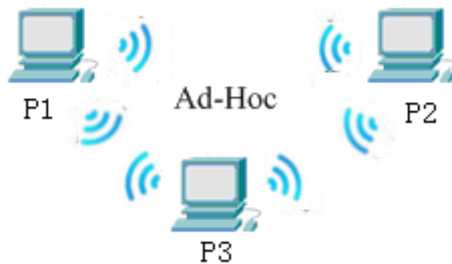


图 Ad-Hoc 无线网络

【实验设备】

带无线网卡的 PC 3 台（参考教材 P400）。

【实验原理】

自组网（Ad-Hoc）模式无线网络是一种省去了无线接入点而搭建起的对等网络结构，也称 SoftAP，只要安装了无线网卡的计算机彼此之间即可实现无线互联。

自组网（Ad-Hoc）模式无线网络的架设过程较为简单，但是传输距离相当有限，因此该种模式较适合满足一些临时性的计算机无线互联需求。

【实验步骤】

步骤 4:

配置过程如下:



```
C:\Users\Administrator>netsh wlan set hostednetwork Mode=allow ssid="TEST" key=12345678
承载网络模式已设置为允许。
已成功更改承载网络的 SSID。
已成功更改托管网络的用户密钥密码。

C:\Users\Administrator>netsh wlan start hostednetwork
已启动承载网络。
```

测试的 ping 的结果如下：可以互相 ping 通。

```
C:\Users\Administrator>ping 192.168.0.2

正在 Ping 192.168.0.2 具有 32 字节的数据:
来自 192.168.0.2 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.0.2 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.0.2 的回复: 字节=32 时间=5ms TTL=64
来自 192.168.0.2 的回复: 字节=32 时间=1ms TTL=64

192.168.0.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 5ms, 平均 = 1ms

C:\Users\Administrator>ping 192.168.0.3

正在 Ping 192.168.0.3 具有 32 字节的数据:
来自 192.168.0.3 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.0.3 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.0.3 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.0.3 的回复: 字节=32 时间<1ms TTL=64

192.168.0.3 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

## 步骤 5:

三台电脑使用同一系列的网卡，无线网卡信道号都为 1，互 ping 结果同步骤 4。

```
SSID 7 : TEST
Network type           : 结构
身份验证               : WPA2 - 个人
加密                   : CCMP
BSSID 1                : 00:0d:0a:4b:17:af
信号                   : 100%
无线由类型             : 802.11g
频道                   : 1
基本速率(Mbps)         : 1 2 5.5 11
其他速率(Mbps)         : 6 9 12 18 24 36 48 54
```



```
C:\Users\Administrator>netsh wlan show hostednetwork
```

## 承载网络设置

```
模式 : 已启用
SSID 名称 : "TEST"
最多客户端数 : 100
身份验证 : WPA2 - 个人
密码 : CCMP
```

## 承载网络状态

```
状态 : 已启动
BSSID : 00:0d:0a:4b:17:af
无线由类型 : 802.11b
频道 : 1
各客户端数 : 2
00:0d:0a:4b:18:89 已经过身份验证
00:0d:0a:4b:0a:c8 已经过身份验证
```

### 步骤 6:

捕获了数据包，主要使用了 ICMP, ARP 和 UDP 等协议。

9	3.469428	192.168.0.1	192.168.0.2	ICMP	74 Echo (ping) request id=0x0001, seq=13/3328, ttl=64 (reply in 10)
10	3.470292	192.168.0.1	192.168.0.2	ICMP	74 Echo (ping) reply id=0x0001, seq=13/3328, ttl=64 (request in 9)
11	4.125396	192.168.0.3	192.168.0.1	ICMP	74 Echo (ping) request id=0x0001, seq=9/2304, ttl=64 (reply in 12)
12	4.125508	192.168.0.1	192.168.0.3	ICMP	74 Echo (ping) reply id=0x0001, seq=9/2304, ttl=64 (request in 11)
13	4.472705	192.168.0.1	192.168.0.2	ICMP	74 Echo (ping) request id=0x0001, seq=14/3504, ttl=64 (reply in 14)
14	4.472793	192.168.0.2	192.168.0.1	ICMP	74 Echo (ping) reply id=0x0001, seq=14/3504, ttl=64 (request in 13)
15	5.128547	192.168.0.3	192.168.0.1	ICMP	74 Echo (ping) request id=0x0001, seq=10/2560, ttl=64 (reply in 16)
16	5.128641	192.168.0.1	192.168.0.3	ICMP	74 Echo (ping) reply id=0x0001, seq=10/2560, ttl=64 (request in 15)
17	5.474542	192.168.0.1	192.168.0.2	ICMP	74 Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (reply in 18)
18	5.480428	192.168.0.2	192.168.0.1	ICMP	74 Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 17)
19	6.131583	192.168.0.3	192.168.0.1	ICMP	74 Echo (ping) request id=0x0001, seq=11/2816, ttl=64 (reply in 20)
20	6.131675	192.168.0.1	192.168.0.3	ICMP	74 Echo (ping) reply id=0x0001, seq=11/2816, ttl=64 (request in 19)
21	6.477763	192.168.0.1	192.168.0.2	ICMP	74 Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (reply in 22)
22	6.478792	192.168.0.2	192.168.0.1	ICMP	74 Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 21)
23	7.137260	192.168.0.3	192.168.0.1	ICMP	74 Echo (ping) request id=0x0001, seq=12/3072, ttl=64 (reply in 24)
24	7.137353	192.168.0.1	192.168.0.3	ICMP	74 Echo (ping) reply id=0x0001, seq=12/3072, ttl=64 (request in 23)
25	8.320400	BarcoPro_4b:0a:c8	BarcoPro_4b:17:af	ARP	42 Who has 192.168.0.1? Tell 192.168.0.2
26	8.320422	BarcoPro_4b:17:af	BarcoPro_4b:0a:c8	ARP	42 192.168.0.1 is at 00:0d:0a:4b:17:af
27	8.443105	BarcoPro_4b:17:af	BarcoPro_4b:0a:c8	ARP	42 Who has 192.168.0.2? Tell 192.168.0.1
28	8.447747	BarcoPro_4b:0a:c8	BarcoPro_4b:17:af	ARP	42 192.168.0.2 is at 00:0d:0a:4b:0a:c8
29	9.555142	192.168.0.2	192.168.0.255	UDP	1482 51991 -> 1689 Len=1440
30	11.067147	BarcoPro_4b:18:89	BarcoPro_4b:17:af	ARP	42 Who has 192.168.0.1? Tell 192.168.0.3
31	11.067170	BarcoPro_4b:17:af	BarcoPro_4b:18:89	ARP	42 192.168.0.1 is at 00:0d:0a:4b:17:af
32	13.006090	192.168.0.1	192.168.0.3	ICMP	74 Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 33)
33	13.006665	192.168.0.3	192.168.0.1	ICMP	74 Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 32)
34	14.008137	192.168.0.1	192.168.0.3	ICMP	74 Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (reply in 35)
35	14.008981	192.168.0.3	192.168.0.1	ICMP	74 Echo (ping) reply id=0x0001, seq=18/4608, ttl=64 (request in 34)
36	14.084574	192.168.0.3	192.168.0.255	NBNS	92 Name query NB WPA0:000
37	14.084740	fe80::4537:40fb:f13a:7...	ff02::1:3	LLMNR	84 Standard query 0xe7e0 A wpa0
38	14.085882	192.168.0.3	224.0.0.252	LLMNR	64 Standard query 0xe7e0 A wpa0
39	14.085978	fe80::4537:40fb:f13a:7...	ff02::1:3	LLMNR	84 Standard query 0x63a9 AAAA wpa0
40	14.086934	192.168.0.3	224.0.0.252	LLMNR	64 Standard query 0x63a9 AAAA wpa0
41	14.495005	fe80::4537:40fb:f13a:7...	ff02::1:3	LLMNR	84 Standard query 0x63a9 AAAA wpa0
42	14.495089	fe80::4537:40fb:f13a:7...	ff02::1:3	LLMNR	84 Standard query 0xe7e0 A wpa0
43	14.495132	192.168.0.3	224.0.0.252	LLMNR	64 Standard query 0xe7e0 A wpa0
44	14.495198	192.168.0.3	224.0.0.252	LLMNR	64 Standard query 0x63a9 AAAA wpa0
45	14.835660	192.168.0.3	192.168.0.255	NBNS	92 Name query NB WPA0:000
46	15.011447	192.168.0.1	192.168.0.3	ICMP	74 Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (reply in 47)
47	15.012127	192.168.0.3	192.168.0.1	ICMP	74 Echo (ping) reply id=0x0001, seq=19/4864, ttl=64 (request in 46)
48	15.507319	192.168.0.3	192.168.0.255	NBNS	92 Name query NB WPA0:000
49	16.014466	192.168.0.1	192.168.0.3	ICMP	74 Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (reply in 50)
50	16.015355	192.168.0.3	192.168.0.1	ICMP	74 Echo (ping) reply id=0x0001, seq=20/5120, ttl=64 (request in 49)
51	17.942943	BarcoPro_4b:17:af	BarcoPro_4b:18:89	ARP	42 Who has 192.168.0.3? Tell 192.168.0.1
52	17.944445	BarcoPro_4b:18:89	BarcoPro_4b:17:af	ARP	42 192.168.0.3 is at 00:0d:0a:4b:18:89
53	18.089297	192.168.0.2	192.168.0.255	UDP	1482 51991 -> 1689 Len=1440

实验思考：三道题均见下面的实验报告。

### 【实验原理】

自组网（Ad-Hoc）模式无线网络是一种省去了无线接入点而搭建起的对等网络结构，也称 SoftAP，只要安装了无线网卡的计算机彼此之间即可实现无线互联。

自组网（Ad-Hoc）模式无线网络的架设过程较为简单，但是传输距离相当有限，因此该种模式较适合满足一些临时性的计算机无线互联需求。

### 【实验步骤】

要求 1：了解所用无线网卡的品牌、性能特点，将无线网卡信息填入下表。

品牌	插槽形式	支持标准	传输速率	天线	信号传输范围
----	------	------	------	----	--------



# 计算机网络实验报告

Ralink RT61	PCI	802.11b	54Mbps	2dBi 高增益天	10m 内
Turbo		802.11g		线一根	
Wireless LAN					
Card					

**要求 2:** 用 ipconfig 命令查看无线网卡信息，贴出截图（注意：只贴出无线网卡的信息），并进行解读。

信息截图
信息解读
此时并没有连接 WLAN，因此显示断开连接，也没有特定的 DNS 后缀。

**要求 3:** 右击桌面右下角网卡图标，点击“管理无线网络”选项；点击“添加”选项卡；点击“创建临时网络”，在“手动连接到无线网络”窗口贴出输入信息后的截图。指出所输入信息意义。在组网的其他 PC 上做相应设置。

信息截图												
<div><pre>C:\Users\Administrator&gt;netsh wlan set hostednetwork mode=allow ssid="wifiwifi" key=12345678 承载网络模式已设置为允许。 已成功更改承载网络的 SSID。 已成功更改托管网络的用户密钥密码。  C:\Users\Administrator&gt;netsh wlan start hostednetwork 已启动承载网络。</pre></div>												
信息解读												
用命令行设置成功。承载网络模式设置为允许，设置了无线局域网的 SSID 名称和密码。												
确定后，ipconfig 查看无线网卡信息，其 IP 地址是：												
<table><tr><th>IP</th><th>子网掩码</th><th>网关</th></tr><tr><td>PC1： 192.168.137.203</td><td>225.225.225.0</td><td>192.168.137.1</td></tr><tr><td>PC2： 192.168.137.1</td><td>225.225.225.0</td><td>192.168.137.1</td></tr><tr><td>PC3： 192.168.137.40</td><td>225.225.225.0</td><td>192.168.137.1</td></tr></table>	IP	子网掩码	网关	PC1： 192.168.137.203	225.225.225.0	192.168.137.1	PC2： 192.168.137.1	225.225.225.0	192.168.137.1	PC3： 192.168.137.40	225.225.225.0	192.168.137.1
IP	子网掩码	网关										
PC1： 192.168.137.203	225.225.225.0	192.168.137.1										
PC2： 192.168.137.1	225.225.225.0	192.168.137.1										
PC3： 192.168.137.40	225.225.225.0	192.168.137.1										
解读信息：												
检查各 PC 的连通性，说明原因												



```
C:\Users\Administrator>ping 192.168.137.40

正在 Ping 192.168.137.40 具有 32 字节的数据:
来自 192.168.137.40 的回复: 字节=32 时间=19ms TTL=64
来自 192.168.137.40 的回复: 字节=32 时间=9ms TTL=64
来自 192.168.137.40 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.137.40 的回复: 字节=32 时间=1ms TTL=64

192.168.137.40 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 19ms, 平均 = 7ms

C:\Users\Administrator>ping 192.168.137.203

正在 Ping 192.168.137.203 具有 32 字节的数据:
来自 192.168.137.203 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.137.203 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.137.203 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.137.203 的回复: 字节=32 时间=1ms TTL=64

192.168.137.203 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 2ms, 平均 = 0ms
```

关闭了校园网之后，三台电脑之间都可以 ping 通。

手工设置无级网卡的 IP 信息，检查各 PC 的连通性，说明与上一步骤区别

```
C:\Users\Administrator>ping 192.168.5.2

正在 Ping 192.168.5.2 具有 32 字节的数据:
来自 192.168.5.2 的回复: 字节=32 时间=1293ms TTL=64
来自 192.168.5.2 的回复: 字节=32 时间=22ms TTL=64
来自 192.168.5.2 的回复: 字节=32 时间=13ms TTL=64
来自 192.168.5.2 的回复: 字节=32 时间<1ms TTL=64

192.168.5.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1293ms, 平均 = 332ms

C:\Users\Administrator>ping 192.168.5.3

正在 Ping 192.168.5.3 具有 32 字节的数据:
来自 192.168.5.3 的回复: 字节=32 时间=2114ms TTL=64
来自 192.168.5.3 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.5.3 的回复: 字节=32 时间=14ms TTL=64
来自 192.168.5.3 的回复: 字节=32 时间=257ms TTL=64

192.168.5.3 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 2114ms, 平均 = 596ms
```

仍然可以 ping 通，区别在于这次是手动配置，只要配置在同一个子网下，依然可以 ping 通。

**要求 4:** 共享其中一台 PC 的文件，进行文件传输。一台传输与多台同时传输时，测试传输速率。解释原因。

以下都是传输同一个文件（3.81MB），分别捕获第一个数据包很最后一个数据包，从而得出传输时间，算出速率。

1 对 1 传输

文件下载过程的第一个 SMB2 包:



192.168.5.3	192.168.5.1	SMB2	374 Create Request File: c.txt
192.168.5.1	192.168.5.3	SMB2	410 Create Response File: c.txt

Wireshark · 分组 271 · 本地连接\* 9

▼ Frame 271: 374 bytes on wire (2992 bits), 374 bytes captured (2992 bits) on interface \Device\NPF\_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA}, id 0

> Interface id: 0 (\Device\NPF\_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA})

Encapsulation type: Ethernet (1)

Arrival Time: Apr 23, 2021 17:52:18.819795000

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1619171538.819795000 seconds

[Time delta from previous captured frame: 0.004390000 seconds]

[Time delta from previous displayed frame: 0.004390000 seconds]

[Time since reference or first frame: 157.310405000 seconds]

文件下载过程的最后一个 SMB2 包:

Frame 4473: 892 bytes on wire (7136 bits), 892 bytes captured (7136 bits) on interface \Device\NPF\_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA}, id 0

> Interface id: 0 (\Device\NPF\_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA})

Encapsulation type: Ethernet (1)

Arrival Time: Apr 23, 2021 17:52:24.766727000

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1619171544.766727000 seconds

[Time delta from previous captured frame: 0.000014000 seconds]

[Time delta from previous displayed frame: 0.462622000 seconds]

[Time since reference or first frame: 163.257337000 seconds]

时间 6s, 速率 0.635MB/s

## 1 对 2 传输

文件下载过程的第一个 SMB2 包: (两台 PC 同时下载)

192.168.5.2	192.168.5.1	SMB2	374 Create Request File: a.txt
192.168.5.1	192.168.5.2	SMB2	410 Create Response File: a.txt

Wireshark · 分组 20 · 本地连接\* 9

▼ Frame 20: 374 bytes on wire (2992 bits), 374 bytes captured (2992 bits) on interface \Device\NPF\_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA}, id 0

> Interface id: 0 (\Device\NPF\_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA})

Encapsulation type: Ethernet (1)

Arrival Time: Apr 23, 2021 17:57:06.280625000

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1619171826.280625000 seconds

[Time delta from previous captured frame: 0.013728000 seconds]

[Time delta from previous displayed frame: 0.013728000 seconds]

[Time since reference or first frame: 2.791161000 seconds]

文件下载过程的最后一个 SMB2 包 (PC2 和 PC3):

Frame 4172: 161 bytes on wire (1288 bits), 161 bytes captured (1288 bits) on interface \Device\NPF\_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA}, id 0

> Interface id: 0 (\Device\NPF\_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA})

Encapsulation type: Ethernet (1)

Arrival Time: Apr 23, 2021 17:57:08.854420000

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1619171828.854420000 seconds

[Time delta from previous captured frame: 0.000028000 seconds]

[Time delta from previous displayed frame: 0.000866000 seconds]

[Time since reference or first frame: 5.364956000 seconds]

192.168.5.3	192.168.5.1	SMB2	374 Create Request File: a.txt
-------------	-------------	------	--------------------------------

Wireshark · 分组 1173 · 本地连接\* 9

▼ Frame 1173: 374 bytes on wire (2992 bits), 374 bytes captured (2992 bits) on interface \Device\NPF\_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA}, id 0

> Interface id: 0 (\Device\NPF\_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA})

Encapsulation type: Ethernet (1)

Arrival Time: Apr 23, 2021 17:57:07.032740000

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1619171827.032740000 seconds

[Time delta from previous captured frame: 0.000265000 seconds]

[Time delta from previous displayed frame: 0.006207000 seconds]

[Time since reference or first frame: 3.543276000 seconds]

平均时间 4s, 速率 0.9525MB/s

## 1 对 3 传输

PC2 下载过程的第一个 SMB2 包和最后一个 SMB2 包:

Frame 549: 374 bytes on wire (2992 bits), 374 bytes captured (2992 bits) on interface \Device\NPF\_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA}, id 0

> Interface id: 0 (\Device\NPF\_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA})

Encapsulation type: Ethernet (1)

Arrival Time: Apr 23, 2021 17:41:34.223774000

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1619170894.223774000 seconds

[Time delta from previous captured frame: 0.005640000 seconds]

[Time delta from previous displayed frame: 0.005640000 seconds]

[Time since reference or first frame: 32.823617000 seconds]





```
✓ Frame 12757: 364 bytes on wire (2912 bits), 364 bytes captured (2912 bits) on interface \Device\NPF_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA}, id 0
  > Interface id: 0 (\Device\NPF_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA})
    Encapsulation type: Ethernet (1)
      Arrival Time: Apr 23, 2021 17:41:46.479445000
      [Time shift for this packet: 0.000000000 seconds]
      Epoch Time: 1619170906.479445000 seconds
      [Time delta from previous captured frame: 0.000000000 seconds]
      [Time delta from previous displayed frame: 0.142492000 seconds]
      [Time since reference or first frame: 45.079288000 seconds]
```

PC3 下载过程的第一个 SMB2 包和最后一个 SMB2 包:

```
Frame 6: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits) on interface \Device\NPF_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA}, id 0
  > Interface id: 0 (\Device\NPF_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA})
    Encapsulation type: Ethernet (1)
      Arrival Time: Apr 23, 2021 17:41:12.938416000
      [Time shift for this packet: 0.000000000 seconds]
      Epoch Time: 1619170872.938416000 seconds
      [Time delta from previous captured frame: 0.081215000 seconds]
      [Time delta from previous displayed frame: 0.081215000 seconds]
      [Time since reference or first frame: 11.538259000 seconds]
    Frame Number: 6
```

```
Frame 12034: 453 bytes on wire (3624 bits), 453 bytes captured (3624 bits) on interface \Device\NPF_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA}, id 0
  > Interface id: 0 (\Device\NPF_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA})
    Encapsulation type: Ethernet (1)
      Arrival Time: Apr 23, 2021 17:41:46.141516000
      [Time shift for this packet: 0.000000000 seconds]
      Epoch Time: 1619170906.141516000 seconds
      [Time delta from previous captured frame: 0.000000000 seconds]
      [Time delta from previous displayed frame: 0.639788000 seconds]
      [Time since reference or first frame: 44.741359000 seconds]
```

PC4 下载过程的第一个 SMB2 包和最后一个 SMB2 包:

```
Frame 83: 374 bytes on wire (2992 bits), 374 bytes captured (2992 bits) on interface \Device\NPF_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA}, id 0
  > Interface id: 0 (\Device\NPF_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA})
    Encapsulation type: Ethernet (1)
      Arrival Time: Apr 23, 2021 17:41:32.130365000
      [Time shift for this packet: 0.000000000 seconds]
      Epoch Time: 1619170892.130365000 seconds
      [Time delta from previous captured frame: 0.002178000 seconds]
      [Time delta from previous displayed frame: 0.002178000 seconds]
      [Time since reference or first frame: 30.730208000 seconds]
```

```
Frame 4240: 595 bytes on wire (4760 bits), 595 bytes captured (4760 bits) on interface \Device\NPF_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA}, id 0
  > Interface id: 0 (\Device\NPF_{99D12194-5E74-4FC7-9FA5-85BEA6707DFA})
    Encapsulation type: Ethernet (1)
      Arrival Time: Apr 23, 2021 17:41:41.395152000
      [Time shift for this packet: 0.000000000 seconds]
      Epoch Time: 1619170901.395152000 seconds
      [Time delta from previous captured frame: 0.000000000 seconds]
      [Time delta from previous displayed frame: 0.630251000 seconds]
      [Time since reference or first frame: 39.994995000 seconds]
```

平均传输时间 18.3s, 速率 0.208MB/s

## 上述传输情况分析

基本上是遵从传输数量越多、平均传输速率越慢的规则进行的。不过由于数据传输量较小, 在 WIFI 下传输可能会导致两次的传输时间与期望不符 (1 对 1 和 1 对 2 的情况), 且由于实验室中的 WIFI 较多, 信号互相干扰不稳定, 因此这合理。

要求 5: 尝试捕获实验时的无线数据包, 并解读。

41	0.878289	192.168.0.2	192.168.0.1	SMB2	148 Close Request File:
42	0.878270	192.168.0.1	192.168.0.2	SMB2	162 Close Response
43	0.891515	192.168.0.2	192.168.0.1	SMB2	162 GetInfo Request SEC_INFO/SMB2_SEC_INFO_00 File: tmp.txt
44	0.891516	192.168.0.1	192.168.0.2	SMB2	206 GetInfo Response
45	0.900430	192.168.0.3	192.168.0.1	SMB2	218 Create Request File:
46	0.900424	192.168.0.1	192.168.0.3	SMB2	242 Create Response File:
47	0.912989	192.168.0.2	192.168.0.1	SMB2	318 SetInfo Request SEC_INFO/SMB2_SEC_INFO_00 File: tmp.txt
48	0.913187	192.168.0.1	192.168.0.2	SMB2	124 SetInfo Response
49	0.920905	192.168.0.3	192.168.0.1	SMB2	146 Close Request File:
50	0.921036	192.168.0.1	192.168.0.3	SMB2	182 Close Response
51	0.934702	192.168.0.2	192.168.0.1	SMB2	162 SetInfo Request FILE_INFO/SMB2_FILE_ENDOFFILE_INFO File: tmp.txt
52	0.934933	192.168.0.1	192.168.0.2	SMB2	124 SetInfo Response
53	0.942132	192.168.0.3	192.168.0.1	SMB2	362 Create Request File: desktop.ini
54	0.942509	192.168.0.1	192.168.0.3	SMB2	131 Create Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
55	0.951088	192.168.0.2	192.168.0.1	TCP	1514 7862 -> 445 [ACK] Seq=3196 Ack=4895 Win=61 Len=1460 [TCP segment of a reassembled PDU]
56	0.951719	192.168.0.2	192.168.0.1	TCP	1514 7862 -> 445 [ACK] Seq=3164 Ack=4895 Win=61 Len=1460 [TCP segment of a reassembled PDU]
57	0.951778	192.168.0.1	192.168.0.2	TCP	54 445 -> 7862 [ACK] Seq=4095 Ack=6024 Win=1962 Len=0
58	0.951839	192.168.0.2	192.168.0.1	TCP	1514 7862 -> 445 [ACK] Seq=3164 Ack=4895 Win=61 Len=1460 [TCP segment of a reassembled PDU]
59	0.954315	192.168.0.2	192.168.0.1	TCP	1514 7862 -> 445 [ACK] Seq=30804 Ack=4895 Win=61 Len=1460 [TCP segment of a reassembled PDU]
60	0.954373	192.168.0.1	192.168.0.2	TCP	54 445 -> 7862 [ACK] Seq=4095 Ack=9544 Win=1958 Len=0
61	0.954445	192.168.0.2	192.168.0.1	TCP	1514 7862 -> 445 [ACK] Seq=30844 Ack=4895 Win=61 Len=1460 [TCP segment of a reassembled PDU]
62	0.955349	192.168.0.2	192.168.0.1	TCP	1514 7862 -> 445 [ACK] Seq=31884 Ack=4895 Win=61 Len=1460 [TCP segment of a reassembled PDU]
63	0.955361	192.168.0.1	192.168.0.2	TCP	54 445 -> 7862 [ACK] Seq=4095 Ack=12464 Win=1939 Len=0
64	0.955514	192.168.0.2	192.168.0.1	TCP	1514 7862 -> 445 [ACK] Seq=31844 Ack=4895 Win=61 Len=1460 [TCP segment of a reassembled PDU]
65	0.955962	192.168.0.2	192.168.0.1	TCP	1514 7862 -> 445 [ACK] Seq=31924 Ack=4895 Win=61 Len=1460 [TCP segment of a reassembled PDU]
66	0.956019	192.168.0.1	192.168.0.2	TCP	54 445 -> 7862 [ACK] Seq=4095 Ack=15384 Win=1928 Len=0
67	0.956068	192.168.0.2	192.168.0.1	TCP	1514 7862 -> 445 [ACK] Seq=315384 Ack=4895 Win=61 Len=1460 [TCP segment of a reassembled PDU]
68	0.956796	192.168.0.2	192.168.0.1	TCP	1514 7862 -> 445 [ACK] Seq=318844 Ack=4895 Win=61 Len=1460 [TCP segment of a reassembled PDU]
69	0.956864	192.168.0.1	192.168.0.2	TCP	54 445 -> 7862 [ACK] Seq=4095 Ack=15394 Win=1916 Len=0
70	0.956914	192.168.0.2	192.168.0.1	TCP	1514 7862 -> 445 [ACK] Seq=318384 Ack=4895 Win=61 Len=1460 [TCP segment of a reassembled PDU]
71	0.957629	192.168.0.2	192.168.0.1	TCP	1514 7862 -> 445 [ACK] Seq=31784 Ack=4895 Win=61 Len=1460 [TCP segment of a reassembled PDU]
72	0.957636	192.168.0.1	192.168.0.2	TCP	54 445 -> 7862 [ACK] Seq=4095 Ack=15394 Win=1916 Len=0

可以看出, 传输的协议包括 SMB2 和 TCP 协议, 抓捕到了数据包如图所示。可以看出, 在 PC1 (网关) 得到的 Wireshark 捕捉包中可以捕捉到向其它三台主机发送的数据包, 并且包括了共享文件夹请求文件的报文和 PC1 数据传输的报文, 包括了控制和数据报文。



# 计算机网络实验报告

本次实验完成后，请根据组员在实验中的贡献，请实事求是，自评在实验中应得的分数。（按百分制）

学号	学生	自评分
19308024	崔子潇	100
19335040	丁维力	100
19335286	郑有为	100

## 【交实验报告】

上传实验报告：截止日期（不迟于）：1 周之内

上传包括两个文件：

（1）小组实验报告。上传文件名格式：小组号\_Ftp 协议分析实验.pdf （由组长负责上传）

例如：文件名“10\_Ftp 协议分析实验.pdf”表示第 10 组的 Ftp 协议分析实验报告

（2）小组成员实验体会。每个同学单独交一份只填写了实验体会的实验报告。只需填写自己的学号和姓名。

文件名格式：小组号\_学号\_姓名\_Ftp 协议分析实验.pdf （由组员自行上传）

例如：文件名“10\_05373092\_张三\_Ftp 协议分析实验.pdf”表示第 10 组的 Ftp 协议分析实验报告。

**注意：不要打包上传！**