Wireshark Lab: TCP

本次实验满分 20 分。

一、学习任务

1）借助 Wireshark 工具深入理解 TCP 协议的运行规则（可靠传输控制、连接建立、流量控制）、头部信息。
2）深入理解 TCP 协议拥塞控制协议的运行规则，掌握基本的性能参数统计方法。
3）体会网络传输层协议的设计方法。

二、作业要求

1、仔细阅读\WiresharkLab\Wireshark_TCP_v8.0.pdf 文件。
2、完成文件中 1-14 题。
3、要使用自己 wireshark 捕获的数据包的数据，已有的 trace 文件仅供参考。
注：如果 Wireshark 抓到的 TCP 包长度大于 1460，请参考附录 1 解决该问题，生成自己的 trace 文件。
4、要有截图，作为对回答问题的支撑。截图要有说明。
5、提交文档，word 或者 pdf 均可。
6、个人独立完成。

三、评分标准

1）满分 20 分。

2）wireshark 作业存在题目没做完，少一题扣一分。

3）作业中需要截图佐证的地方没有截图，只有文字，扣除该次作业总分 20%。

4）单次作业中存在个别题目错答或者操作错误，视情况扣除 1-2 分。

5）作业存在抄袭、复制别人答案/截图的情况，一律按 0 分处理。

附录：

1、关于 Wireshark 抓到的 TCP 包长度大于 1460 的问题

问题描述：

假如用户正在向服务器上传一些数据，同时在用户的机器上捕捉数据包。如图所示，用户捕获的 TCP 数据包长度大于 1500 字节。

No.	Time	Source	Destination	Protocol	Length	Info
108	3.178159	172.18.0.10	172.16.0.10	TCP	2974	[Continuation to #61] 445→42902
109	3.178189	172.16.0.10	172.18.0.10	TCP	60	42902→445 [ACK] Seq=8017 Ack=274
110	3.178213	172.18.0.10	172.16.0.10	TCP	5894	[Continuation to #61] 445→42902
111	3.178243	172.16.0.10	172.18.0.10	TCP	60	42902→445 [ACK] Seq=8017 Ack=318
112	3.178274	172.18.0.10	172.16.0.10	TCP	5894	[Continuation to #61] 445→42902
113	3.178865	172.16.0.10	172.18.0.10	TCP	60	42902→445 [ACK] Seq=8017 Ack=347
114	3.178883	172.18.0.10	172.16.0.10	TCP	2974	[Continuation to #61] 445→42902
115	3.178916	172.16.0.10	172.18.0.10	TCP	60	42902→445 [ACK] Seq=8017 Ack=391
116	3.178935	172.18.0.10	172.16.0.10	TCP	4434	[Continuation to #61] 445→42902
117	3.178969	172.16.0.10	172.18.0.10	TCP	60	42902→445 [ACK] Seq=8017 Ack=434
118	3.178995	172.18.0.10	172.16.0.10	TCP	4434	[Continuation to #61] 445→42902
119	3.179020	172.16.0.10	172.18.0.10	TCP	60	42902→445 [ACK] Seq=8017 Ack=464
120	3.179042	172.18.0.10	172.16.0.10	TCP	4434	[Continuation to #61] 445→42902
121	3.179592	172.16.0.10	172.18.0.10	TCP	60	42902→445 [ACK] Seq=8017 Ack=493

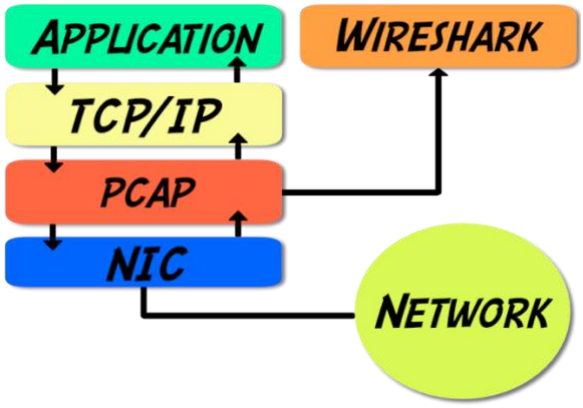
问题解析：

TCP 分段卸载：

许多操作系统和网卡驱动程序支持 TCP 分段卸载（TCP Segmentation Offload , TSO），又称大段卸载（Large Segment Offload , LSO），又称通用分段卸载（Generic Segment Offload , GSO）。这意味着 TCP 协议栈发送一大块数据给 NIC，让它分解成最大段大小（Maximum Segment Size , MSS）的片段发送到网络上。例如，TCP 可能会把 16K 的数据交给 NIC，NIC 会把它分成许多长度为 MSS 的小块：11 个 1460 字节的段和剩余的一个 324 字节的段。这样就把分段任务移交给了网卡，节省了主机资源的开销。

Wireshark 抓包原理：

如图所示，Wireshark 使用 libpcap 或 winpcap 来抓取数据，然后再将其交给网卡。根据上文描述，大块数据的分解发生于网卡，而 wireshark 抓包发生在数据分解之前，所以除非使用 tap 或 span（交换机的端口镜像技术）端口在发送主机外部进行抓包，否则看不到在 network 上实际传送的数据包（经网卡分解后的段）。



参考解决方案：

Disable Large Send Offloads [1,2]

1. From the Windows operating Start menu, open Control Panel.
2. In Control Panel, open Network and Internet and Network and Sharing Center .
3. In Network and Sharing Center, select Change adapter settings. Network Connections opens and displays network adapters, including the following:

1) Control Connection #1
2) Control Connection #2
3) Media Connection #1
4) Media Connection #2

4. For each Control Connection and each Media Connection, do the following:
   1) Right-click the connection and select Properties. The Connection Properties dialog box opens.
   2) In the Connection Properties dialog box, click Configure. The Adapter Properties dialog box opens.
   3) In the Adapter Properties dialog box, click the Advanced tab.
   4) On the Advanced tab, in the Settings list select Large Send Offload v2 (IPv4) and then in the Value drop-down list select Disabled.
   5) Click OK to save settings and close.
   6) Repeat these steps for each Control Connection and each Media Connection.

[1] https://wwwapps.grassvalley.com/manuals/k2_summit_v10.1.3/core/x-cc/content/topic/k2/service/t_largesendoffloads_disable.html）

[2] https://docs.microsoft.com/en-us/powershell/module/netadapter/disable-netadapterlso?view=windowsserver2022-ps