
华中科技大学计算机学院

《计算机通信与网络》实验报告

班级 CS2109 姓名 卢舒愉 学号 U202110415

项目	Socket 编程 (40%)	数据可靠传输协议设计 (20%)	GPT 组网 (20%)	平时成绩 (20%)	总分
得分					

教师评语：

教师签名：

给分日期：

目 录

实验三 基于 CPT 的组网实验.....	1
1.1 环境	1
1.2 实验要求	1
1.3 基本部分实验步骤说明及结果分析	1
1.4 综合部分实验设计、实验步骤及结果分析	7
1.5 其它需要说明的问题	9
1.6 参考文献	9
心得体会与建议	10
2.1 心得体会	10
2.2 建议	11

实验三 基于 CPT 的组网实验

1.1 环境

本次实验使用的机器硬件配置：

- CPU: Intel Core i5-12400F
- GPU: NVIDIA GeForce RTX 3070 Ti
- RAM: 32G DDR4
- SSD: 1TB

本次实验使用的系统软件组件：

- Windows 11 专业版 22H2
- Cisco Packet Tracer 6.0.0.00045

1.2 实验要求

熟悉使用 Cisco Packet Tracer 软件，并使用该仿真软件完成本次实验。

本次实验共分为以下三个部分：

1. IP 地址规划与 Vlan 分配实验：

通过理解网络规划与配置的基本原理，以及掌握网络连通性的分析与测试方法，运用模拟软件创建一个包含多台个人电脑和路由器的网络拓扑。在此基础上，按照特定的 IP 地址规划，为路由器配置适当的端口地址，并对各个个人电脑之间的连通性进行深入分析。

2. 路由配置实验：

此实验涉及三个主要方面，要求使用模拟软件进行路由器配置和访问控制的实际操作。首先，在基础内容的第一部分中，需构建一个特定的网络拓扑，配置路由器上的 RIP 协议，确保各个个人电脑之间能够相互访问。其次，在基础内容的第二部分中，需要在路由器上配置 OSPF 协议。最后，在基础内容 1 或 2 的基础上，学生需对路由器进行进一步的访问控制设置。

3. 综合实验：

此实验的核心目标是为一个学校设计和搭建网络，满足学院、图书馆、学生宿舍等不同地点的网络需求。通过充分利用提供的 IP 地址块，设计并配置网络以满足复杂的连接和隔离需求，解决实际生活中的网络问题。

1.3 基本部分实验步骤说明及结果分析

1.3.1 IP 地址规划与 Vlan 分配实验的步骤及结果分析

i. 子实验 1

按照实验规定，运用 Cisco Packet Tracer 建立一个与提供的拓扑图等效的网络结构。该网络包含 8 台个人计算机、4 台交换机和 1 台路由器。最终布局如下图 1 所示。

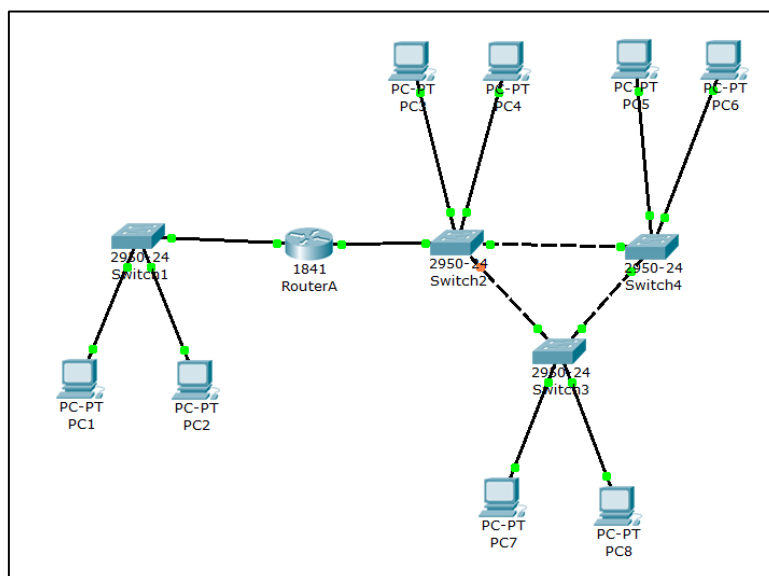


图 1

在实验中，我们采用直通线连接异类设备，而对于同类设备，则使用交叉线进行连接。连接计算机与交换机的过程中，我们使用了直通线以确保它们之间正常通信。同时，连接交换机与交换机的过程中，我们选择了交叉线，以保障它们之间的有效连接。最后，我们采用直通线将交换机与路由器相连。

一旦完成连接，我们为各个计算机和路由器分配了 IP 地址。在路由器的左侧，Gateway 配置为 192.168.0.1，而路由器右侧 PC 的 Gateway 配置为 192.168.1.1。PC1 和 PC2 分别获得了 IP 地址 192.168.0.2 和 192.168.0.3，而 PC3 到 PC8 则分别获得了 IP 地址从 192.168.1.2 到 192.168.1.7 的范围。此外，网络配置信息可通过将鼠标悬停在路由器或计算机上进行查看，如下图 2 所示，以左侧 PC1 配置为例。

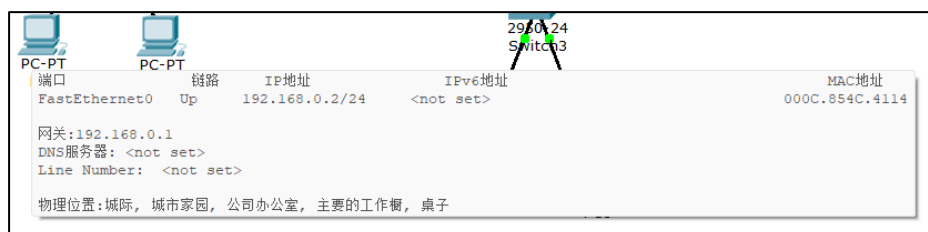


图 2

之后可以通过 Cisco Packet Tracer 提供的工具令各个 PC 之间互相通信，实验结果如图 3 所示，通信正常。

激活	最后状态	来源设备	目的设备
	成功	PC1	PC5
	成功	PC4	PC7

图 3

ii. 子实验 2

在子实验 1 的基础上，需要对 PC4、PC6、PC8 进行重新配置，将它们从 192.168.1.0 子网中分离出来，并将它们的 IP 重新分配到 192.168.2.0 子网。这将导致 PC4、PC6、PC8 与路由器右端接口不再位于同一子网中。由此，192.168.2.0 子网中的设备将无法与其他子网中的设备进行通信，而其他子网中的设备仍然能够成功地相互通信。测试结果如图 4 所示。





	成功	PC1	PC5
	失败	PC2	PC6
	成功	PC4	PC6
	失败	PC4	PC7

图 4

iii. 结果分析

网络设备的端口具有配置 IP 地址的能力，而连接到这些端口的两个网段的个人电脑设置了路由器端口的 IP 地址作为网关。这使得路由器能够转发消息，从而实现了这两个网段之间的通信。然而，由于一个网段（192.168.2.0）没有配置网关，而且路由器只有两个端口，这两个端口已经被其他两个网段占用，导致该网段没有可用的网关。因此，这个网段无法与其他子网进行通信。

此外，通过在交换机上划分虚拟局域网（VLAN），各个主机被分配到不同的 VLAN 中。每个 VLAN 都被视为一个独立的逻辑实体，不受物理空间和子网的限制。因此，位于同一 VLAN 的 PC1 和 PC2 能够相互通信。如果在路由器上没有配置 VLAN，VLAN 内的主机可以互相通信，但无法与其他 VLAN 中的主机通信，形成一种隔离状态。只有在路由器上进行了 VLAN 的配置，VLAN 内的消息才能被路由器正确识别和转发。否则，路由器无法确定消息的目的地，因为本地没有相关的 VLAN 可供选择。

1.3.2 路由配置实验的步骤及结果分析

i. 子实验 1

按照实验规定，运用 Cisco Packet Tracer 建立一个与提供的拓扑图等效的网络结构。该网络包含 8 台个人计算机、3 台交换机和 4 台路由器。最终布局如下图 5 所示。

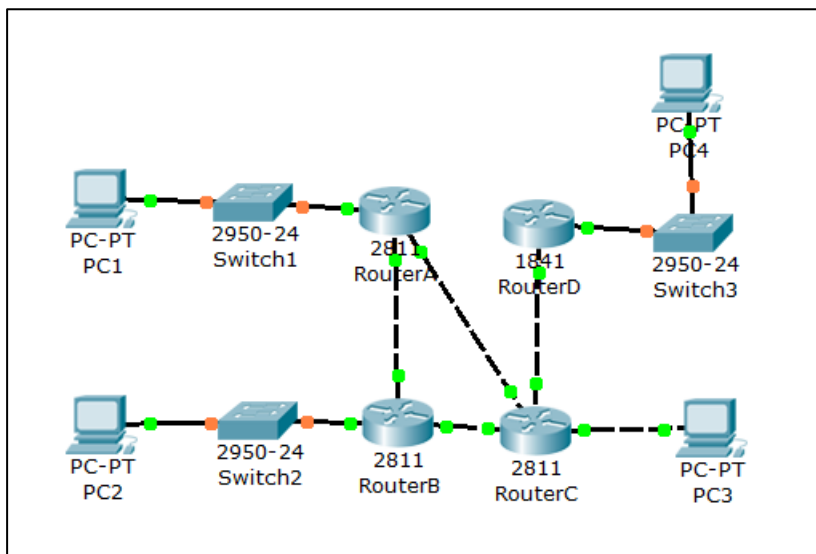


图 5

本次实验涉及四个路由器，每个负责管理一个特定子网，分别对应于 192.168.1.0、192.168.2.0、192.168.3.0 和 192.168.4.0 网段。为确保连接在路由器与 PC 机或交换机之间的端口 IP 与相应网段的 IP 地址匹配，必须进行配置。

RIP (Routing Information Protocol) 是一种专为自治系统内设计的动态路由协议，用于实现路由器之间的路由信息交换，从而实现自动路由更新。在配置 RIP 协议的路由器时，只需指定每个端口的 IP 地址所在的网段。在这个实验中，要配置 RIP 协议，这是一种基于跳数评估路由优劣的距离矢量路由协议。为了为 routerA 配置 RIP 协议，需要进入“配置->路由配置->RIP”选项，然后在相应的界面中输入与这三个 IP 地址相对应的网段，并点击添加。配置完成后，路由器成功完成了 RIP 协议的设置，从而实现了动态路由更新的功能。如图 6 所示。



图 6

其他计算机的 IP 地址和网关设置，以及路由器的配置方法也是相似的。在完成配置后，可以随意选择两台计算机进行相互通信。在测试过程中，可能会出现第一次访问请求失败的情

况，但在之后的第二次尝试中通信通常会成功。这可能是由于软件本身存在的问题，但也表明两台计算机可以正常访问。

ii. 子实验 2

在第二个子实验中，与配置 RIP 协议的子实验相比，配置路由 OSPF 协议有所不同，但其余配置均相似。具体配置如下图 7 所示，四个路由器的配置过程相似，与子实验 1 中的计算机 IP 地址和网关配置也类似。

```
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#network 192.168.5.0 0.0.0.255 area 0
Router(config-router)#network 192.168.6.0 0.0.0.255 area 0
Router(config-router)#end
```

图 7

最后进行访问测试，网络中的任意两对都可以通信，结果如下图 8 所示。




激活	最后状态	来源设备	目的设备
	成功	PC2	PC4
	成功	PC1	PC4
	成功	PC1	PC3

图 8

iii. 子实验 3

在第三个子实验的首个任务中，要对路由器进行访问控制列表的配置。此处使用命令行对路由器 B 进行设置，以使得计算机 A 无法与其他网络子网通信，同时不受其他网络子网的访问。

在路由器 B 与交换机 1 相连接的端口上执行配置，使用 access-list 命令创建一个访问控制列表，选择 ACL 编号在 0 到 99 之间的数字。使用 deny 关键词来拦截特定网络子网的通信，而使用 permit 关键词则表示允许特定网络子网的通信。在这里，我们采用 deny 规则来屏蔽计算机 A 的通信。最后，通过 access-group 命令将 ACL 与路由器关联。配置过程如下图 9 所示。

```
Router(config)#access-list 35 deny 192.168.1.0 0.0.0.255
Router(config)#int fa0/0
Router(config-if)#ip access-group 35 in
Router(config-if)#exit
```

图 9

以下图 10 是网络拓扑检测，其中 PC1 无法成功发起对其他 PC 的请求，同时其他 PC 也无法访问 PC1。




激活	最后状态	来源设备	目的设备
	失败	PC1	PC2
	成功	PC2	PC4
	成功	PC2	PC3

图 10

在实验的第三个子任务的第二个任务中，需要对路由器进行访问控制列表的设置，通过命令对路由器 A 进行调整。此时，要实现 PC1 无法与 PC2 进行通信，但可以与其他计算机进行通讯。前面中使用了“deny”指令来阻止特定通信，而当前要求是部分信息屏蔽且允许另一部分信息通过，因此需要采用“Permit”指令来完成配置。配置过程如下图 11 所示。

```
Router(config)#access-list 36 deny 192.168.2.0 0.0.0.255
Router(config)#access-list 36 permit any
Router(config)#int fa0/0
Router(config-if)#ip access-group 36 in
```

图 11

以下为对网络拓扑的检测，其中 PC1 对 PC2 的请求失败，PC2 对 PC1 的请求也失败，而其他 PC 与 PC1、PC2 的访问正常。如图 12 所示。

激活	最后状态	来源设备	目的设备
	失败	PC1	PC2
	失败	PC2	PC1
	成功	PC1	PC4
	成功	PC2	PC3
	成功	PC3	PC4

图 12

iv. 结果分析

通过学习和应用两种不同的路由选择协议，即路由信息协议（RIP）和开放最短路径优先协议（OSPF），我们在实验中探索了它们的配置和使用。尽管它们在配置层面存在一些不同，但最终都实现了相同的通信目标。由于实验规模较小，无法直观展示 RIP 和 OSPF 之间的差异。然而，通过上课学习和查阅资料，我们了解到 RIP 和 OSPF 在路由协议方面存在显著的差异。

RIP 是一种传统的路由协议，适用于较小规模的网络。然而，随着网络的迅速增长和扩展，RIP 协议已经无法满足当今网络的需求。相反，OSPF 协议是在网络迅速扩展的背景下制定的，克服了 RIP 协议的多个限制。RIP 采用距离矢量路由协议，通过定时广播路由表，而 OSPF 则是链路状态路由协议，只在路由状态发生变化时广播路由表。

此外，访问控制列表（ACL）被用于管理路由器和交换机端口的数据包进出。通过在路由器 A 的端口上使用 deny 规则，我们可以阻止来自 PC1 所在网段的消息，有效过滤与 PC1 相关的所有通信，使得 PC1 无法与外部进行通信。如果需要同时允许某些消息通过并阻止其他消息，我们可以结合使用 deny 和 permit 指令，实现更精细的访问控制。

1.4 综合部分实验设计、实验步骤及结果分析

1.4.1 实验设计

该实验重点在于测试对综合内容的理解，要求学生独立设计现实生活中的网络拓扑结构，特别是在考虑 IP 地址的分配和子网划分方面。

首先，要分配宿舍的 IP 地址，每个宿舍需要支持 200 台主机，其中 8 位用于子网编码，剩余的 50 多台主机则可等待后续使用。学校获得的 IP 地址块是 211.69.4/22，可以利用低 10 位进行划分。因此，通过限定第 8、9 位，低 8 位用于编码，可以分别使用 211.69.4.0/24、211.69.5.0/24、211.69.6.0/24 作为三个宿舍的 IP 地址。

对于图书馆，需要支持 100 台主机，至少需要 7 位，因此限定第 7 位，低 7 位用于编址。图书馆可以使用 211.69.7.0/25 网段。

最后，还有三个学院需要分配 IP 地址，每个学院有 20 台主机。考虑前面剩余的网段还有 7 位可用，因此使用低 5 位进行每个学院的 IP 编址，第 5、6 位用于学院的编码。

在确定了 IP 地址划分方案后，得到了初步的设计图，并在 Cisco Packet Tracer 中绘制了网络拓扑图。如下图 13 所示。

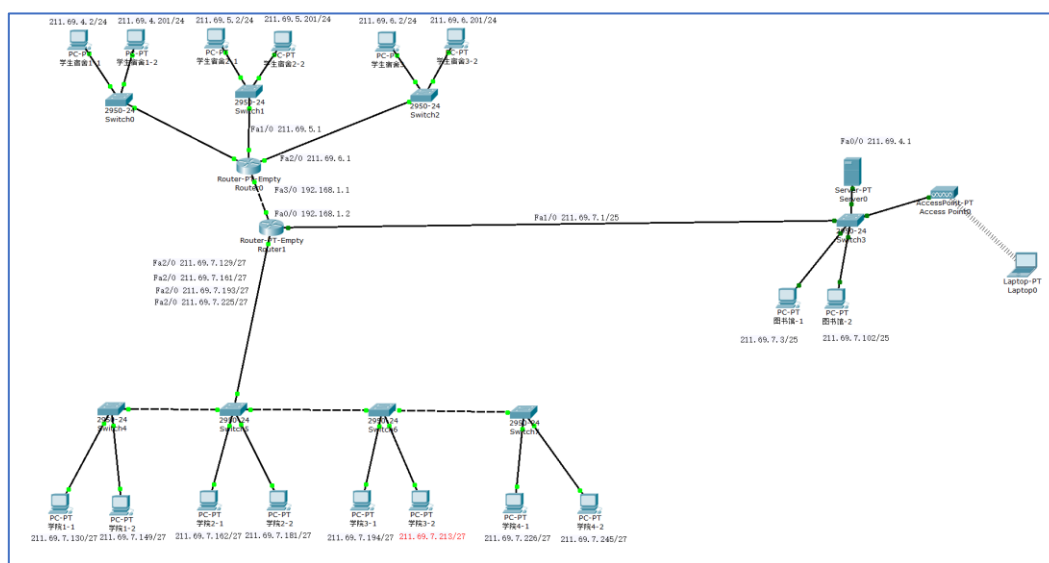
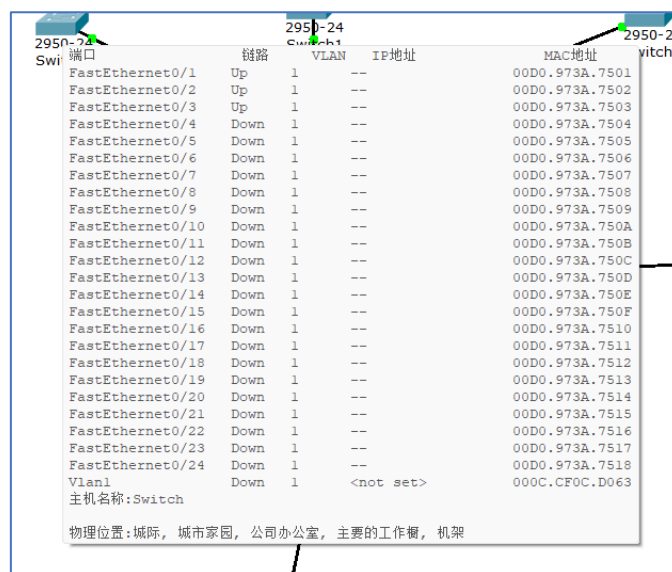


图 13

1.4.2 实验步骤

首先，依照总体网络拓扑结构进行连接，确保同类设备之间采用互交线，异类设备之间使用直通线原则。连接完毕后，为每个计算机分配相应的 IP 地址。对于每一组包含两台计算机的表示整体的组合，分别指定该组的首个和末尾的 IP 地址。对学院总交换机、学生宿舍的三个总交换机以及图书馆总交换机进行虚拟局域网（VLAN）分隔。部分划分如图 14 所示。



端口	链路	VLAN	IP地址	MAC地址
FastEthernet0/1	Up	1	--	00D0.973A.7501
FastEthernet0/2	Up	1	--	00D0.973A.7502
FastEthernet0/3	Up	1	--	00D0.973A.7503
FastEthernet0/4	Down	1	--	00D0.973A.7504
FastEthernet0/5	Down	1	--	00D0.973A.7505
FastEthernet0/6	Down	1	--	00D0.973A.7506
FastEthernet0/7	Down	1	--	00D0.973A.7507
FastEthernet0/8	Down	1	--	00D0.973A.7508
FastEthernet0/9	Down	1	--	00D0.973A.7509
FastEthernet0/10	Down	1	--	00D0.973A.750A
FastEthernet0/11	Down	1	--	00D0.973A.750B
FastEthernet0/12	Down	1	--	00D0.973A.750C
FastEthernet0/13	Down	1	--	00D0.973A.750D
FastEthernet0/14	Down	1	--	00D0.973A.750E
FastEthernet0/15	Down	1	--	00D0.973A.750F
FastEthernet0/16	Down	1	--	00D0.973A.7510
FastEthernet0/17	Down	1	--	00D0.973A.7511
FastEthernet0/18	Down	1	--	00D0.973A.7512
FastEthernet0/19	Down	1	--	00D0.973A.7513
FastEthernet0/20	Down	1	--	00D0.973A.7514
FastEthernet0/21	Down	1	--	00D0.973A.7515
FastEthernet0/22	Down	1	--	00D0.973A.7516
FastEthernet0/23	Down	1	--	00D0.973A.7517
FastEthernet0/24	Down	1	--	00D0.973A.7518
Vlan1	Down	1	<not set>	000C.CF0C.D063

主机名称: Switch

物理位置: 城际, 城市家园, 公司办公室, 主要的工作室, 机架

图 14

接下来，将进行对路由器的设定，进行 IP 地址的分配，确保每个虚拟局域网（VLAN）都拥有独特的 IP 地址。这些 IP 地址将作为各个 VLAN 的默认网关使用。为每个 VLAN 建立虚拟接口，并将其与相应 VLAN 分配的 IP 地址关联。根据需求，进行路由器路由表的配置，以保障各个 VLAN 之间的通信。以下是部分路由器配置的示意图。

端口	链路	IP地址	IPv6地址	MAC地址
FastEthernet0/0	Up	211.69.4.1/24	<not set>	0030.F2C7.2EB0
FastEthernet1/0	Up	211.69.5.1/24	<not set>	0001.C986.7ADC
FastEthernet2/0	Up	211.69.6.1/24	<not set>	0050.0FDD.E134
FastEthernet3/0	Up	192.168.1.1/24	<not set>	0006.2AA0.7C5B

主机名称: Router

物理位置: 城际, 城市家园, 公司办公室, 配线室, 机架

图 15

在最终阶段，对于各个子网之间的访问控制进行设置，实验的要求是确保学院和宿舍之间不能相互通信，但两者都能够访问图书馆。为实现这一目标，需要在学院和宿舍的路由器上配置相应的规则以屏蔽彼此之间的通信信号。

1.4.3 结果分析

1. 测试学校各个部门内部的访问权限，可以发现部门内部均可以正常通信。
2. 测试学院和宿舍之间通信，可以发现学院和宿舍之间通信失败。
3. 测试学院和图书馆之间通信， 可以发现学院和图书馆之间通信成功。
4. 测试宿舍和图书馆之间通信， 可以发现学院和图书馆之间通信成功。
5. 测试宿舍和学院之间通信， 可以发现学院和图书馆之间通信成功。

测试结果图 16 所示。




激活	最后状态	来源设备	目的设备	类型
	成功	学生宿舍1-1	学生宿舍1-2	ICMP
	成功	学生宿舍1-1	学生宿舍3	ICMP
	成功	学院1-1	学院2-1	ICMP
	成功	学院1-1	学院4-1	ICMP
	成功	图书馆-1	Laptop0	ICMP
	失败	学院1-2	学生宿舍2-2	ICMP
	失败	学院3-1	学生宿舍3	ICMP
	成功	学院4-1	图书馆-1	ICMP
	成功	学院3-1	Laptop0	ICMP
	成功	学生宿舍3-2	图书馆-1	ICMP

图 16

1.5 其它需要说明的问题

无

1.6 参考文献

[1] Kurose, J F., & Ross, K.W. 2020.7. 《计算机网络：自顶向下方法》. 北京：机械工业出版社

心得体会与建议

2.1 心得体会

计算机网络实验分为三个部分，每个部分都涉及不同的实验项目。在这一过程中，我积累了丰富的经验和知识，对计算机网络有了更深刻的认识。以下是我的心得体会：

1. 网络套接字服务器：

在这次实验中，我成功地使用套接字完成了一个 Web 服务器。套接字相当于在应用层和传输层之间提供的接口。通过完成这个实验，我对套接字的理解更加深入，深刻体会到套接字在开发上层应用中的便捷性。这个实验虽然相对简单，但让我对计算机网络有了更深刻的认识，尤其是在手动解析 HTTP 协议的过程中，意识到应用层协议需要考虑的复杂性，如错误请求处理和大文件处理等。在修改 bug 并完成 Web 服务器的过程中，我积累了丰富的经验，对 C++ 编程和调试有了更深入的了解，也对计算机网络的分层和应用层协议有了更深入的认识。

2. 可靠数据传输：

在这次实验中，我深入了解了可靠数据传输协议，如 GBN、SR 和 TCP 的工作原理，并在实验系统的框架下实现了这三个协议。在课堂上，我已经初步了解了这三个可靠传输协议，但对协议细节还不够清楚。在实验过程中，我不断查阅课本和 PPT，思考三个协议之间的区别，并不断完善自己的代码。通过完成这个实验，我深刻理解了它们各自的优缺点和应用，认识到了它们在实际通信中的重要性。可靠数据传输协议是传输层的一个重要知识点，相对于第一个实验，这次实验难度更大。但通过完成这个实验，我对计算机网络传输层的理解更加深刻，也深入了解了传输层协议 TCP 和 UDP 之间的区别和应用。

3. 网络仿真：

在这次实验中，我学会了使用 Cisco Packet Tracer 进行网络仿真，并利用该软件实现了复杂的网络拓扑。实验涉及到网络层、链路层和物理层的知识，是一个相对综合的检验。实验难度相较前两个要大一些，需要完成路由器、交换机以及主机的配置，并完成网络拓扑。通过这次实验的第一个子实验，我对网络层 IP 的理解更加深刻，也学会了如何配置路由器。第二个子实验让我更深刻地理解了网络层的路由和寻址，通过深入学习了 RIP 和 OSPF 两个算法。前两个实验的网络拓扑相对简单，让我熟悉了 Cisco Packet Tracer 软件的使用，同时也对网络拓扑有了更深刻的认识。第三个子实验需要自行划分子网，设计网络拓扑，类似于现实生活中的网络问题，完成这一部分花费了很多时间。通过完成这三个子实验，我进一步加深了对大型网络构建与配置的理解，从更高的层面对计算机网络有了新的认识。

感谢课程组老师精心设计的实验，通过完成这三个实验，我收获颇丰。

2.2 建议

1. 建议在实验课或课后，安排学生分享他们的实验进展和面临的挑战。可以进行班级或小组讨论，通过同学间的交流学习，共同应对问题。
2. 期望增加更多难度层次，前两个实验已提供代码框架或参考，降低了一些难度。希望能够建立更为合理的难度梯度，或者引入拓展性内容，并提供更多学习和实践资料。