实验8 复杂网络综合设计实验报告

注意事项：

1、班号请填写上课的实验班号，例如周一晚上

2、提交电子版实验报告文件和最终配置结果文件的命名方式：实验班号-组号-学号-姓名-实验报告/配置结果

3、请填写同组2位同学任务分工及贡献度系数表

|  |  |  |
| --- | --- | --- |
| 姓名 | 杜金阳 | 李嘉鹏 |
| 学号 | 21373191 | 21373216 |
| 实验任务分工 | AS1 、AS3 | AS2、 AS4 |
| 贡献度系数 | 50% | 50% |

一、按照组网图正确组网( 10 分)（只需要提交完成的ensp文件）

二、如图所示，对交换机上的VLAN进行划分和配置( 10 分) （只需要提交完成的ensp文件和真实设备的配置文件）

三、配置各台设备的各接口的IP地址( 10 分) （只需要提交完成的ensp文件和真实设备的配置文件）

四、完成OSPF路由协议配置，使本自治系统内部互联互通；完成网络可靠性设计，实现VRRP设备备份，ospf路由备份。（教材中交换机之间的**链路聚合、心跳线的链路备份和WAN备份中心不要求**）**请简要写出本人负责部分的设计方案**：( 30 分)

**在AS1中，有以下设备进行备份：**

**路由器rt1和rt2相互作为备份设备。**

**路由器rt3、rt4、rt5相互作为备份设备。**

**交换机ls1和ls2相互作为备份设备。**

**所有这些网络层设备都在运行OSPF协议，以实现链路备份。**

**在AS3中，有以下设备进行备份：**

**路由器rt6、ht7、rt8相互作为备份设备。**

**交换机ls3和ls4相互作为备份设备。**

**在AS3自治区域中，使用VRRP（虚拟路由冗余协议）来进行备份。具体设置如下：**

**对于局域网2.3.16.0/24网段，设置虚拟IP地址为"2.3.16.1"，并通过设置优先级（priority）将rt12作为rt11的备份。**

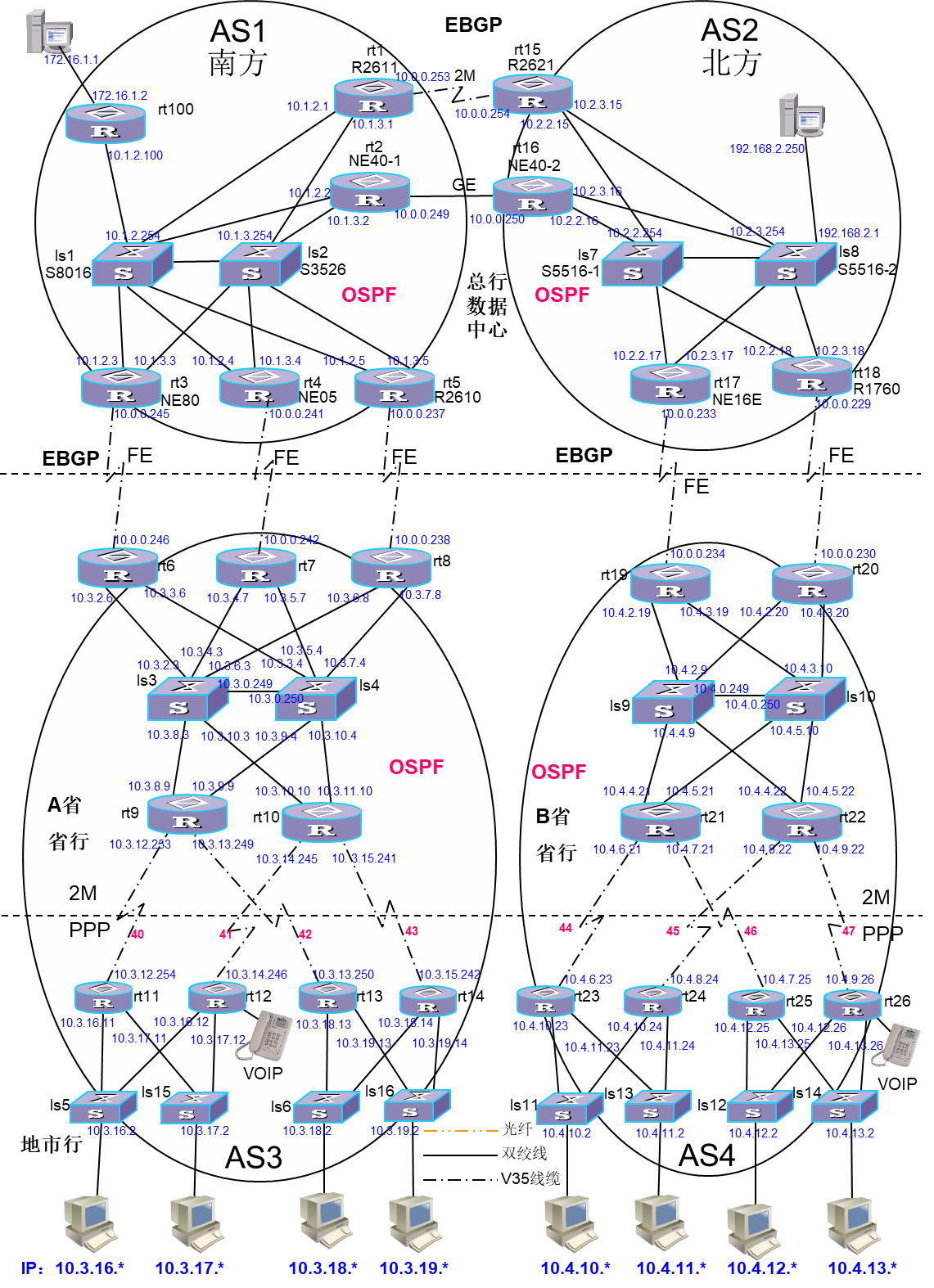
**对于局域网2.3.17.0/24网段，设置虚拟IP地址为"2.3.17.1"，并通过设置优先级（priority）将rt11作为rt12的备份。**

**同样地，路由器rt13和rt14也进行类似的VRRP备份设置。**

**这样设计可以提高网络的可靠性，当主设备出现故障时，备份设备可以接管网络功能，确保网络的持续运行。**

**ospf路由备份：**

**将AS内部的子网掩码为255.255.255.252的边界路由以外的网段均注入ospf协议，以实现路由备份。**



1. 完成BGP和OSPF配置，实现网络管理、访问外网的路由功能，其余网段的路由不允许发布到其它自治系统。**请简要写出本人负责部分的设计方案：**( 15 分)

**1.区域内部路由：IP地址为"2.as-number.x.y/24"，代表区域内部的网段，不能与外部区域互通。**

**2.PC所在路由：IP地址为"2.4.x.y/24"，其中x为10、11、12、13，代表能访问外部网络的主机所在网段，y分别设置为5、6、7、8。**

**3.网管PC所在路由：IP地址为"192.168.0.250"，用于网络管理的IP地址。**

**4.外网路由：IP地址为"172.16.1.0/24"，代表访问外网的网段，外网位于AS1自治区内。**

**5.区域边界路由：IP地址为"2.0.0.y/30"，用于建立EBGP连接。**

**6.网管路由和IBGP路由：设置在loopback0回环接口，具体IP地址见后文，用于网管联系各区域内的路由器/交换机，同时作为IBGP路由地址，用于建立IBGP连接。**

**7.IP电话路由：设置在rt26的loopback1回环接口，IP地址为"2.4.126.2/32"。**

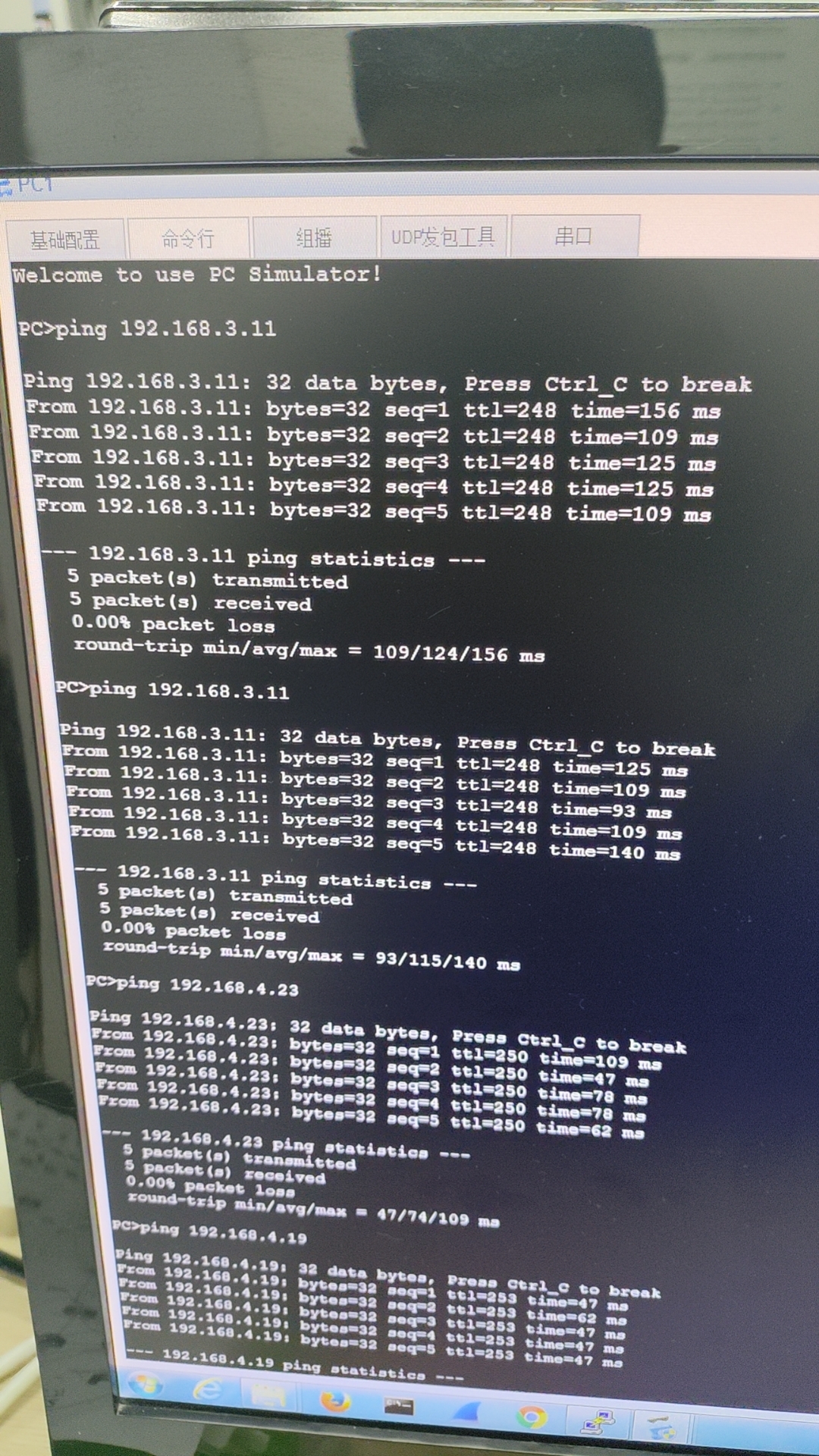
**配置说明：**

**网络管理配置：在所有自治区的所有路由器上的loopback回环接口配置IP地址，IP地址的格式为"192.168.x.y/32"。其中，x为as-number，y为具体编号。如果是路由器，则编号为路由器编号+100；如果是交换机，则编号为交换机编号+200。例如，AS2自治区的RT17路由器的IP地址为"192.168.2.2/32"。这样可以保证网络管理服务器（192.168.0.250）与所有路由器都可以互通，并且可以模拟网络故障发送SNMP Trap报文。**

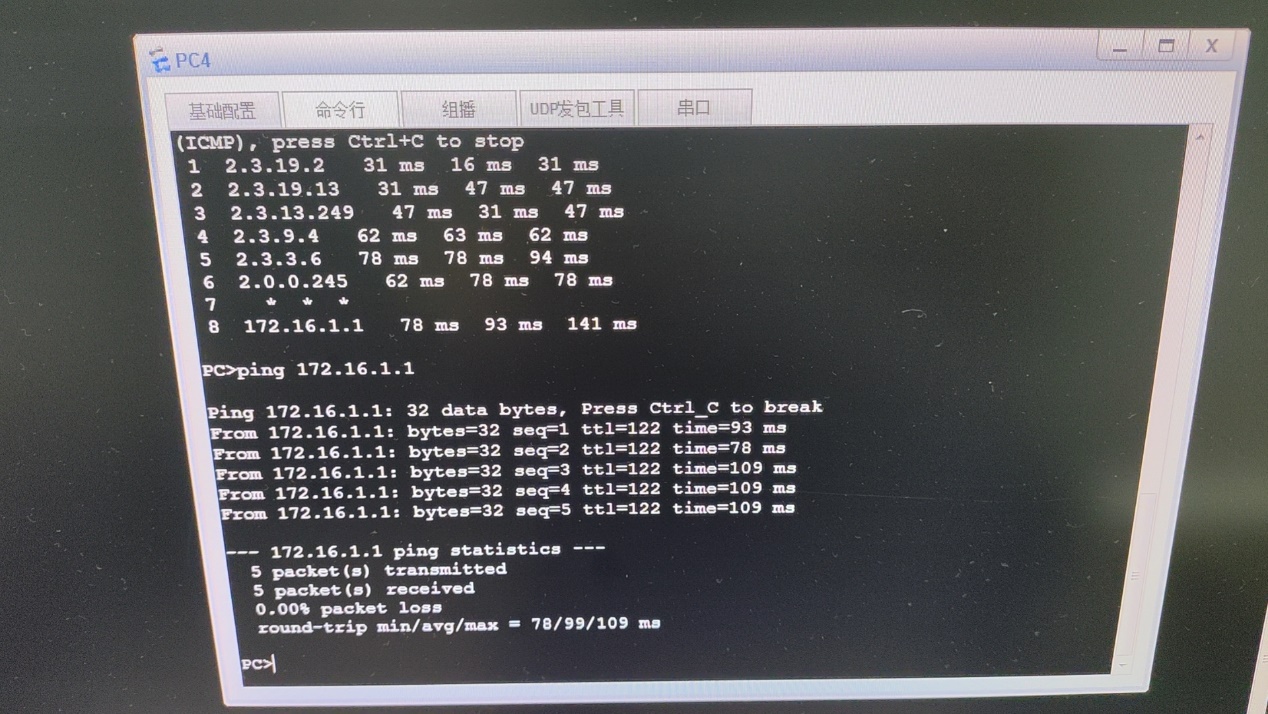
**OSPF配置：在AS2和AS4自治区内部配置OSPF，将AS区域内的接口（loopBack0）的IP地址引入OSPF协议中，以确保自治区内部可以相互ping通。对于配置了BGP协议的自治区域边界路由器，需要将BGP路由注入OSPF协议中。**

**BGP配置：使用IBGP路由建立IBGP连接，使用区域边界路由建立EBGP连接。自治区域边界路由器需要注入PC所在路由、外网路由、网管路由和IP电话路由。**

**网络管理路由：由于自治区域边界路由器将区域内的所有网管路由注入BGP协议，所以网管可以联系到路由器所在的自治区域边界路由器。同时，网管路由也被注入OSPF协议，所以自治区域边界路由器可以在AS内部找到要联系的路由器。反之亦然，网管的IP地址被注入到BGP，路由器也可以联系到网管。在对应自治系统中的BGP边界路由器上设置路由过滤的route-policy，允许网络设备管理IP地址通过。特别地，在AS1中需要设置路由过滤，允许AS1和AS3的网络设备管理地址通过。**

****

**访问外网路由：对于实验任务列表中，本组的组号对应的接入交换机上的网段主机可以访问外网。在路由器RT100上需要配置地址转换（NAT）。在RT100上配置NAT，设置ACL策略仅允许PC所在路由的网段通过。设置地址池，为访问外网设置了xx-xx地址。同时，将外网所在网段注入OSPF协议和BGP协议，以确保AS3和AS4中的PC所在路由可以通过外网网段访问。**

****

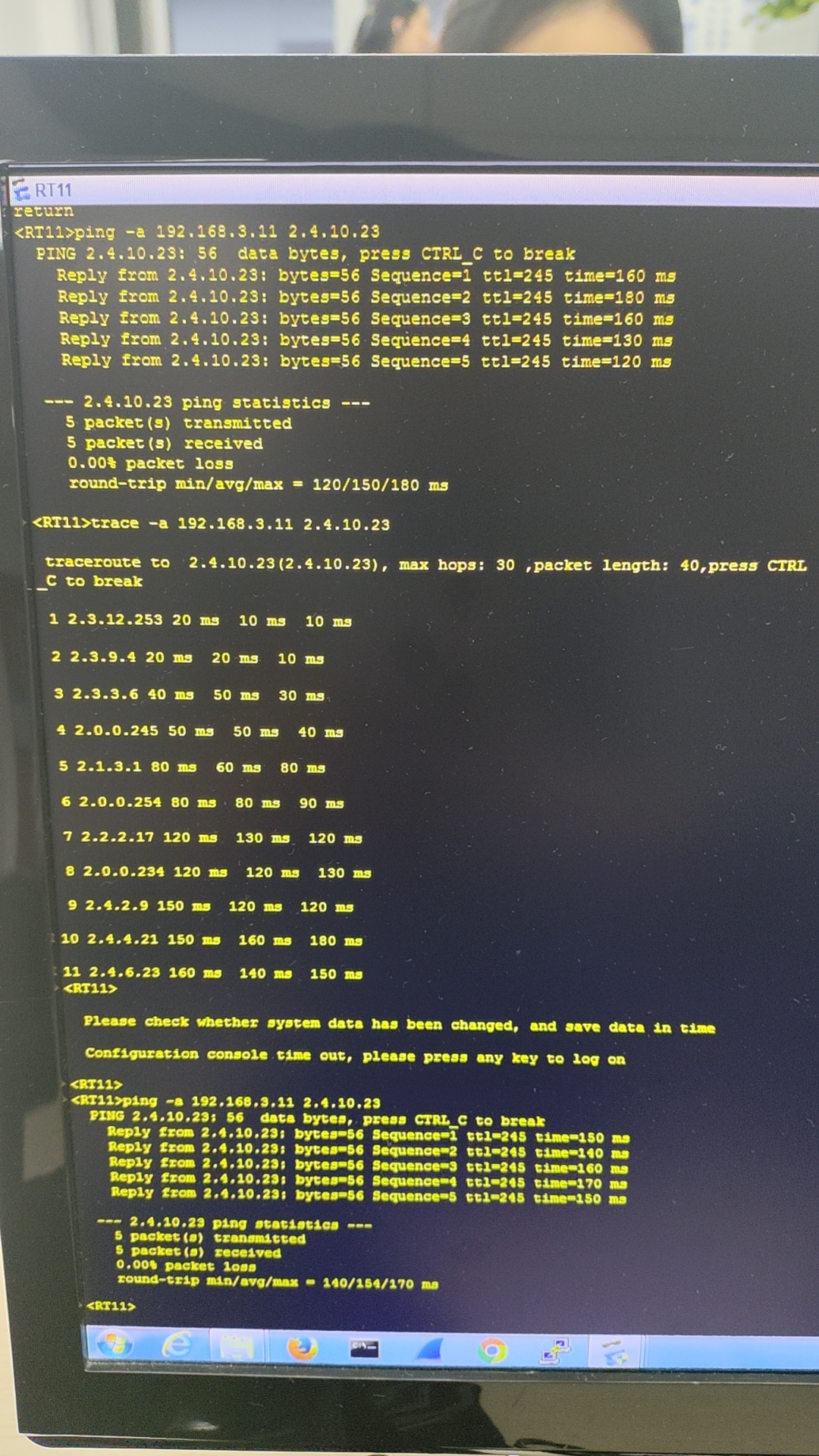
六、按照实验任务的要求，实现IP电话指定网络路径优先，其余路径为备份。**请简要写出本人负责部分的设计方案**：( 15 分)

**本组的IP电话指定了优先路径，并要求两端路由器上配置IP电话地址（loopback）。地址格式为".as-num.rt-num+100./32"，并确保这两个地址可以互通，并且满足优先选择指定路径，其余路径作为备份。**

**首先，在AS3内部的rt12的回环接口loopback2上配置IP地址为"2.as-num.rt-num+100.1/32"，例如："2.3.112.1/32"。在AS4内部的er26的回环接口loopback1上配置IP地址为"2.as-num.rt-num+100.2/32"，例如："2.4.126.2/32"。将这两个Loopback地址引入OSPF协议中。**

**然后，在相应的自治系统边界路由器上使用BGP的network命令将IP电话地址引入BGP中。这样，在所有的BGP对等体路由器中都会有IP电话地址的路由信息。同时，在所有的BGP边界路由器上设置OSPF引入BGP路由表，以确保IP电话地址可以在整个自治系统中被访问。**

**对于路径优选问题，可以使用OSPF的cost来决定自治区内部的路径选择，使用BGP协议的MED（或者使用route-policy）和local-preference来选择自治区之间的路径。当路径发生故障时，网络将自动重新选择新的路径进行访问，最终效果如下:**

****

七、请论述本网络设计方案的优缺点，如可扩展性、合理性等方面（ 10 分）例如：

1. 增加一路ip电话，选择另外的指定优先路径，本方案能否满足？

2. 不同业务流隔离：办理不同业务（如：办公、银行业务等）IP不能互通。给出你的地址规划和方案设计。

**如果路径之间没有交点，可以满足条件。在这种情况下，可以通过以下方式进行配置：**

**1.区域内部路径选择（AS内部）：使用OSPF协议，为两条路径分别设置最小的cost值，确保它们都是最优路径。在AS内部的各个路由器上，根据需要设置路径的cost，使其在OSPF路由选择中被优选。**

**2.区域间路径选择（自治区域之间）：使用BGP协议，通过路由策略中的地址匹配来选择路径。在自治区域边界路由器上，设置BGP路由策略来匹配目标IP电话地址，并根据策略选择优先路径。可以使用BGP的MED属性或本地优先级（local preference）来确定优选路径，确保指定的优先路径被选中。**

**不同业务流隔离没有实现。**

1. 请将实验中完成的所有设备最终配置保存，与实验报告一并压缩为一个文件，发送至任课老师邮箱。注意：所有文件均需要按照要求的规则命名。
2. 课程总结：

在计算机网络的实践与应用课程中，我们踏上了一段将理论知识与实际操作紧密结合的探索之旅。本课程不仅巩固了我们对计算机网络基本架构、协议栈（如TCP/IP）、以及网络服务（DNS、HTTP等）的理论认识，更侧重于通过动手实验来深化这一理解。我们亲历了从物理层的布线与设备配置，到应用层协议的实现与优化的全过程。

实验环节中，我们利用虚拟化技术搭建了多种网络拓扑，包括简单的局域网配置到复杂的广域网模拟，实践了OSI模型各层次的功能与交互。通过配置路由器和交换机，我们学会了如何实施静态与动态路由协议（RIP、OSPF），理解了它们在路径选择与网络效率中的角色。安全方面，我们设计并实施了防火墙规则，进行了渗透测试，掌握了加密技术（如SSL/TLS）在保障数据传输安全中的应用。

每项实验都是一个从理论到实践的转化过程，从设计网络拓扑开始，到细致的设备配置，再到协议的部署与测试，每一步都要求我们细致入微，逻辑清晰。我们利用Wireshark等工具抓包分析，直观地观察网络流量与协议交互，这不仅增强了我们对协议工作原理的认知，也锻炼了我们的问题诊断与解决能力。

团队合作贯穿整个课程，共同面对网络搭建与调试中的挑战，促进了沟通与协作能力的提升。我们学会了如何高效地分工合作，共同攻克难关，这种经验对于未来从事任何团队项目都是极其宝贵的。

总之，计算机网络实践与应用课程是一次深度学习与技能锻造的旅程。它不仅使我们掌握了计算机网络的精髓与实操技能，更为我们在网络规划、设计、安全及性能优化等领域的发展奠定了坚实的基础。通过这次课程，我们不仅成为了网络知识的学者，更是成为了能够解决实际问题的网络工程师，为迎接未来的网络挑战蓄势待发。