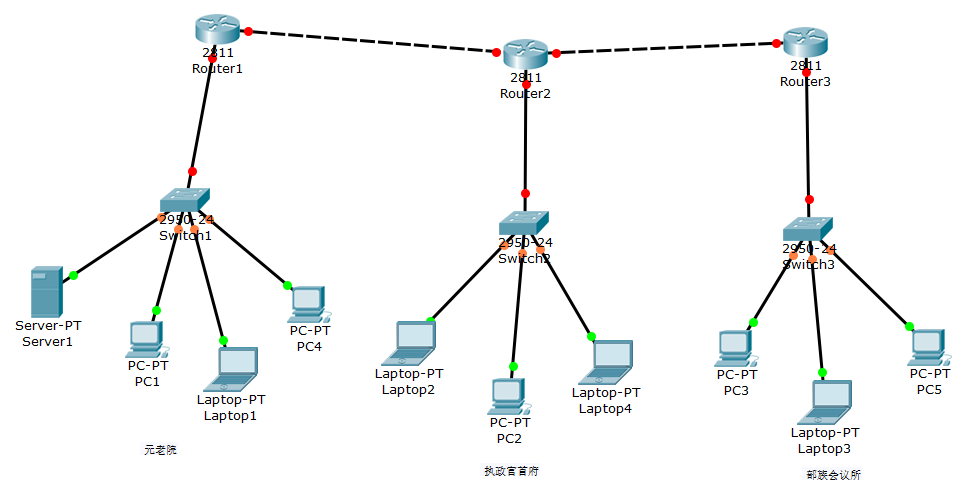
**2022年秋季学期《计算机网络安全技术》实验二**

**访问控制及VPN技术**

请根据下面的实验介绍，完成各个任务。给出证明自己完成了实验的必要文字描述和截图。本实验要求提交实验报告，配置文件自存。

# 实验背景

在上次网络铺设工作结束后，凯撒十分赏识你的才能，他把保管“共和国”最高机密的任务交给了你。同时，凯撒也希望你能进一步推进“共和国”网络安全化的工作。另一方面，在这段时间里，“共和国”的网络规模进一步扩大，新增的设备及IP地址分配方案如下图所示（上一次实验中，元老院与部族会议所之间的新建链路因被人为破坏已被移除）：



元老院（192.168.1.0/24）：Router1, Switch1, Server1, PC1, Laptop1, PC4

执政官首府（192.168.2.0/24）：Router2, Switch2, PC2, Laptop2, Laptop4

部族会议所（192.168.3.0/24）：Router3, Switch3, PC3, Laptop3, PC5

新增设备IP地址分配：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Port | IP | Mask | Gateway |
| PC4 | 端口1 | 192.168.1.5 | /24 | 192.168.1.1 |
| Laptop4 | 端口1 | 192.168.2.4 | /24 | 192.168.2.1 |
| PC5 | 端口1 | 192.168.3.4 | /24 | 192.168.3.1 |

# 任务6：“三权”间的权限控制（）

“共和国”内各个权力部门下的终端设备都有专人使用，为了便于管理，你需要从技术层面对网络进行权限设置，以达到访问控制的效果。

终端设备的使用情况如下表所示：

|  |  |  |  |
| --- | --- | --- | --- |
| 设备名称 | 使用人 | 部门 | 备注 |
| PC1 | 凯撒/你 | 元老院 | 领导人 |
| Server1 | 你 | 元老院 | 机密管理 |
| Laptop1 | 布鲁图 | 元老院 | 联络人 |
| PC4 | 财务官A | 元老院 | --- |
| Laptop2 | 庞培 | 执政官首府 | 领导人 |
| PC2 | 卡西乌斯 | 执政官首府 | 联络人 |
| Laptop4 | 辅助执政官B | 执政官首府 |  |
| PC3 | 克拉苏 | 部族会议所 | 领导人 |
| Laptop3 | 安东尼 | 部族会议所 | 联络人 |
| PC5 | 大祭司C | 部族会议所 | --- |

为了便于进行安全管理，“共和国”新购入了一台路由器和若干交换机。请在最合适的接口处配置访问控制列表，满足以下的安全要求，在必要时可以在权力机构内略微调整网络：

1. 一般地，各个权力机构内部的所有成员均能相互通信。

2. 然而，在权力机构之间的相互通信只能通过几位联络人进行，例如：执政官首府的成员只能与元老院的联络人布鲁图进行通信。

3. 另外，三个权力机构的领导人（凯撒、庞培和克拉苏）可以互相通信讨论工作，进行领导人会议。

4. 特别地，由于Server1存放了大量的国家机密，在整个“共和国”内只有凯撒和你可以与该设备通信。另外，凯撒特别允许你使用他的终端设备PC1。

注：该任务中，不能通信指既不能收数据也不能发数据，可以通信指既能收数据也能发数据。

# 任务7：凯撒赐予的“最高”权限（）

由于你负责“共和国”网络的管理工作，所以你需要经常对各个设备的网络连通性进行探测，凯撒允许你通过他的设备（PC1）进行该测试。请在前一任务的基础上进行相应的配置，使得你能够对“共和国”网络内所有设备进行ping测试，且当你发起测试时，不受上个任务的访问权限影响。

# 任务8：新的远征（）

为了进一步拓展“共和国”的疆域，凯撒计划开展海外业务。经过慎重抉择，凯撒准备在埃及建立新的“共和国”根据地，并决定将元老院搬迁至该处。由于“共和国”的新根据地与原根据地距离较远，因而“共和国”的两个部分只能通过公网相连。请更改网络拓扑，在Router1和Router2中间增加公网路由器Router4，使得Router1和Router2为“共和国”分部与总部的两个边界路由器。

在搬迁之后，使用配置静态路由的方法将无法让各个权力机构正常通信，请简述原因。

为了解决通信问题，你决定配置IPSec VPN，让“共和国”内网可以穿越公网。VPN配置中涉及到的加密算法均使用3des，哈希算法均使用md5，秘钥协商算法使用DH5来协商具有一定强度的秘钥，并使用esp进行加密和认证。请完成相关配置，并表明配置步骤及最终结果。（由于网络重构，ACL的配置将全部清空，重构后的“共和国”内网暂不用考虑之前的ACL配置。）

通过仿真抓包分析，如上配置的IPSec VPN使用了传输模式还是隧道模式，为什么？

# Bonus任务：凯撒的赏赐（）

凯撒命令你进一步探索Packet Tracer的功能，对已经学习过的其他网络知识进行关联和实践，说明其在网络安全的哪些应用中可以被使用，并设计一个场景进行尝试和研究。该任务根据难度及研究程度给分，每人仅可挑选一个探究方向。

可参考的探究方向：交换机的端口聚合、网络地址转换NAT、DHCP的配置、邮件服务器设置、NetFlow流量监控、OSPF协议研究……