**2023年秋季学期《计算机网络安全技术》实验一**

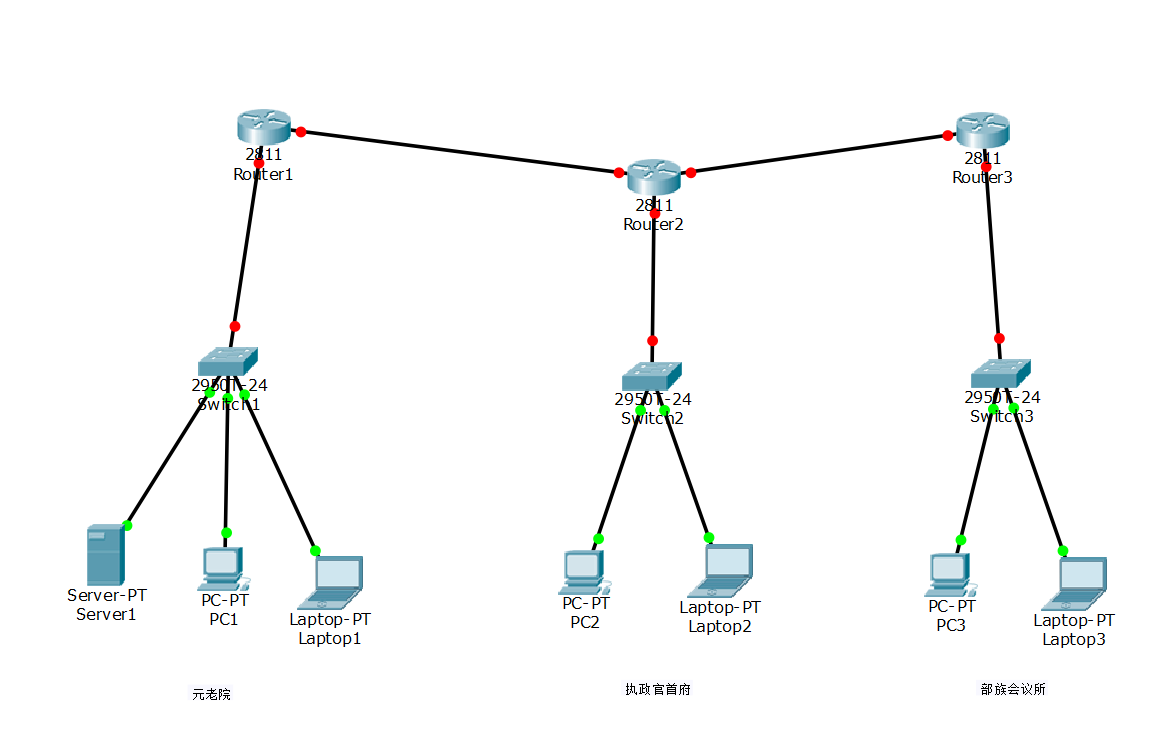
**网络搭建及路由配置**

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

“我来过，我看见，我征服”。2023年的某一天，凯撒大帝穿越到宇宙中心五道口的T大，他在茫茫人海中选中了你作为他的辅佐官。为了在现代继续他的征服计划，凯撒希望能够建立一个属于罗马共和国的内网，用于内部通信。但由于他目前对网络知识的了解十分有限，所以他希望你能来帮助他设计这个网络。目前“共和国”内主要包含三个权利机构：元老院、执政官首府和部族会议所。由于三者分工不同，所以它们均选用不同的子网以便管理。凯撒在临走前留给了你一份网络拓扑草图和一张写着IP地址分配方案的莎草纸。

# 网络拓扑草图



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

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

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

# IP分配方案

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Port | IP | Mask | Gateway |
| Router1 | 端口1 | 192.168.1.1 | /24 | - |
| 端口2 | 10.0.1.1 | /24 | - |
| Router2 | 端口1 | 10.0.1.2 | /24 | - |
| 端口2 | 20.0.2.2 | /24 | - |
| 端口3 | 192.168.2.1 | /24 | - |
| Router3 | 端口1 | 192.168.2.1 | /24 | - |
| 端口2 | 192.168.3.1 | /24 | - |
| PC1 | 端口1 | 192.168.1.2 | /24 | 192.168.1.1 |
| PC2 | 端口1 | 192.168.2.2 | /24 | 192.168.2.1 |
| PC3 | 端口1 | 192.168.2.1 | /24 | 192.168.3.1 |
| Server1 | 端口1 | 192.168.1.3 | /24 | 192.168.1.1 |
| Laptop1 | 端口1 | 192.168.1.4 | /24 | 192.168.1.1 |
| Laptop2 | 端口1 | 192.168.2.3 | /24 | 192.168.2.1 |
| Laptop3 | 端口1 | 192.168.3.3 | /24 | 192.168.3.1 |

# 任务1：破旧的莎草纸（）

你发现，由于年代久远，写有IP地址分配方案的莎草纸有三处破损。除此之外，由于凯撒在网络知识方面的欠缺，他给的IP地址分配方案有一处纰漏。请补全方案，并将方案有错的地方指出并更正。为了便于网络管理，请尽可能用便于记忆的方式规划IP地址。

# 任务2：“一天建起的罗马城”（）

在完善网络搭建方案后，请选择合适的设备及连线将该网络搭建起来，并且为各个接口配置对应的IP等属性。请提供必要的截图向凯撒证明，你亲自参与了网络搭建工作。

# 任务3：要点防卫（）

公网与“共和国”内网的接入点位于元老院的Router1上，为了防止他人的恶意入侵，凯撒要求你至少给Router1设置登录口令。你一共需要为它设置三种口令：通过console口进入用户模式的口令password1，用户模式进入特权模式的口令password2，通过telnet方式登录路由器的口令password3。

当你在思考口令如何设置时，凯撒来到你身边，他要求不论你的口令最终如何设置，里面最好都能够包含一段展现他特点的文字。然后他留下一张莎草纸，上面写着一段奇怪的文字“YHQL, YLGL, YLFL”。同时凯撒也交代给你一句话，“如果无法离开迷雾，就朝着扑克牌里我面庞的方向走三步”。凭借着你在计算机网络安全技术课上学到的知识，你似乎明白了这段文字背后的含义。

请至少在Router1上设置上述三种口令（设置口令时请酌情考虑凯撒的要求），在假设路由器配置文件不会泄露的情况下，自行用适合的口令保证路由器一定程度上的登录安全。如果路由器配置文件可能泄露，你的设置是否有所变化？

试分析，当你使用如下四种复杂程度的密码进行配置时，攻击者进行暴力破解时时间需求的变化，假设暴力尝试一次密码的时间为1：

（1）总长六位的纯数字密码（2）总长六位的混合有数字及小写字母的密码（3）总长六位的混合有数字、大写字母、小写字母的密码（4）总长八位的混合有数字、大写字母、小写字母的密码

另外凯撒还是放心不下你，留下一张纸条，并让你查看辅佐官工牌背面的文字。这张纸条不计入最后的分数，只是为了给你一些小小提示：

|  |  |
| --- | --- |
| 辅佐官工牌背面  RSA-PKCS1 | -----BEGIN PRIVATE KEY-----  MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQD29p3WPq+0FbdI  zDJmaCu0LUHYXnJwLfjtP+toBZQu0qdVL1AfHYMf9cMrCj1M4PMbD6BiBh4daouH  ccpSrgHYV/tLuo7ewJnET9Yu/9/lR3IjuuTI7O1EACofgQnTdngbeWON/SnqQ5s5  Puq1GKdUQpOK682Ra5JeFdsWv+QdwyzZmaHgAFZGCPP0JiaLUNZ6kKOD7mJ/yu2K  6p+JszFvQzOSaLOtwbGkBwfcyX0KtpD+pSPwzmWcwqwrtKHhxS7bbdmV9kXCsFzo  ngNI33cD0SWmbT+K5aNGkXjEUXLT2FZ60TGDDqq9NjEe2rJtZAgWWNYIT+ngMkKP  c9mpT1dTAgMBAAECggEAQwMCKxtRY+UsmaVG28DScw6AumxOUyA2VnIst0okPlxM  qXGwJPFGHkr6jVg28ABuFt6zn0WXsFWzzKnUw4CR4ZlmB9N0Zv8N+lXLgW9O2pD7  aLSS1e5sJzKAO5IxD18rEhFrMSEL2ZREr1DiMQeih9uU23JGknoE+mCl1VN2W5iM  w0p4v4G7M+hsRXDqY+57KX6RjH2VmWthj5zU6GF6WgKMfm95u98YdA8mTY3uW9Hz  S77JgAXJT97kOv3ljPUiXiXpTUYdcj1tQGFp7PKsC8HksYG9XAL8GiBCv1mTM7Fw  48RSvy5AcdgpP38/Efv0lIU6sm4HA/Y98UoGIH0tSQKBgQD7wNYv04ERdHJNqbc/  lFvamhhwJQs9LAbQSRhx3O6+G5WH1VGKRBKNXgezzYAxx/sV0jtMNLrnId2DC6Zz  vyP/Wgb74BQ4E3XxwQ0eQtW0N/C+6YYqd0Ln2uBN6o6XzQiTce+Kb9CeB/MFT5C3  vdlAe0P7fWOB5am/cvIKFi0dhwKBgQD7IRhhRy6KoQXEmIcPjG4byuiWfBR6lDOq  2qBgPoEu0yPWpxRslBi3McbrpsUG4mQyqpdYHnA2YGdtMKqRbM0aNcbdby3sVrmO  ESvGOc+lMUgATmT9WyYe5NPG0ezav81oLhO6ZsRETZqnJKnGYe8jjyK+Ep85WdRd  ZrQPfA2K1QKBgEzdwgf0QhI8RbIkwYiuGaWTKycCiH3y9VmfF9GcLWDqNyu0HCNl  SWzUavGhKyUH9EfjWquX5gEwO9wJMJdiovESYdOBxWqhtn9L/F9i9LED64O+9XH9  2/XCxH3FwifjOF0cipDwNvgpYTAb7QnM84pWmJku3bUJlFyaEgC2aKv9AoGARMJT  Ao+S1rIv+hwpHsC8hS+Rb2KZ2NYrL2Sc9L0occGt1l/436HNApvGc08+MxxZguXi  emYbI0hSCTuB+D9qCPsgcBC46jT0qUlaSvQZPom3xR2x2QzT6zGMKqvfxiUuAJBd  JnRs2KbG6WzIb2DxMTNHt/MxVWqbEtfEBVlZ++ECgYEAlH7kpWMIr3UYN4rYYxZO  kna3L+IA1QLaWEdAYImpHrTh8D2ceJAGE0Iu7rvbt4MWEDFUuZuNQiSeWCVR2BZ+  EvOAM/G8HuEg11mXmFiTOoxVrVwF7L8rZl3m5mJNotKgrLl6WoQMvzq6CMk2qOdy  XHOZ/kBWQeFAiEIsNNLvbMQ=  -----END PRIVATE KEY----- |
| 纸条 | BhD2DfVacwpOh44EieQrhYpmbZLkptThbpov+0FWopiMImvqP4FSBSPZpUqo8KbSvmJigBjeqxI2F1cWjrJVe+gqCI7Y5nft5cySh/2FDS4MSwD2XsP61YjoIOVlveudTCQZwejMCMb0+0yExxtKgATRvt2O8U0KprImU6FCpKpBgWzdBAJBQc9MZfWDqPj3AvPjTGzAOEu3r9GXjkWNgx8VsENhamHH7D5RbjJuWSeVzzdxa3D6dbR01uDOQCszJoYjbFlbIf6pKqEsSA7lG8avMNXi3mOEXIWjTbsGKVjIOhR71xVm4onJPBtNsABqc/Z/mLdKfnn0O/8dDoK7XQ== |

# 任务4：“三权”间的初步通信（）

在搭建好网络之后，你想要测试一下“共和国”的各个权力部门网络是否联通，ICMP协议为你提供了合适的网络控制信息进行探测。由于“共和国”的网络结构相对简单，你决定使用静态路由保证内网的正常通信。然而静态路由的不当使用容易给网络维护带来不便，例如，当对网络进行扩展时，冗余的静态路由也可能对新网络产生影响。因此，请在不使用冗余的静态路由的前提下，让三个权力部门能够相互通讯。

# 任务5：“三权”间的高效通信（）

为了减轻网络的维护成本，提高通信效率，你向凯撒建议使用路由协议动态地管理和维护路由。在讨论使用何种路由协议时，凯撒提出希望在元老院和部族会议所的路由器之间建立一条新的通信链路，让两者可以直接通信，而不是像之前那样需要经过执政官首府的路由器。他表示：“我不希望有些信息被执政官首府那些家伙听到，考虑到‘共和国’目前网络规模较小，接入网络的PC、笔记本和服务器加起来还不到16台，我们应该可以使用适合小型网络的路由协议RIP进行管理”（显然他趁这段时间学习了一些网络知识）。

在凯撒离开后，执政官首府的联系人布鲁图找到了你，他表示：“执政官首府可以支付在元老院和部族会议所之间新建链路的资金，但我们还是希望能够获取到元老院和部族会议所间的秘密信息。或许我们可以想个办法，比如弄一条带宽很小的链路。如果你做到了，我们执政官首府会说服助教多给你些分数”（显然布鲁图有自己的打算）。

经过一番思考之后，你最终决定选择\_\_\_\_\_\_路由协议维护“共和国”目前的局域网。请完成拓扑的修改以及动态路由协议的配置，并展示元老院和部族会议所之间的实际通信路径（使用Cisco Packet Tracer的仿真功能）。同时请思考凯撒的观点是否存在问题？为什么？当前能否使用RIP作为路由协议？

# Bonus任务（只需进行一项）：谁的馈赠（）

1. 你按照凯撒的要求在元老院和部族会议所之间建立一条**可通信的**链路，凯撒表示十分满意。但凯撒近日来突然对“共和国”内网的密码安全产生了兴趣，他要求“共和国”内网的特权模式密码应使用secret指令在配置文件中进行一定程度的加密存储。试探究使用该指令存储的密码是用何种方式进行加密。

2. 你在任务5中完成了布鲁图的要求，一股神秘的力量直接赠予你奖励分数。