2019年秋学期《计算机网络安全技术》实验二

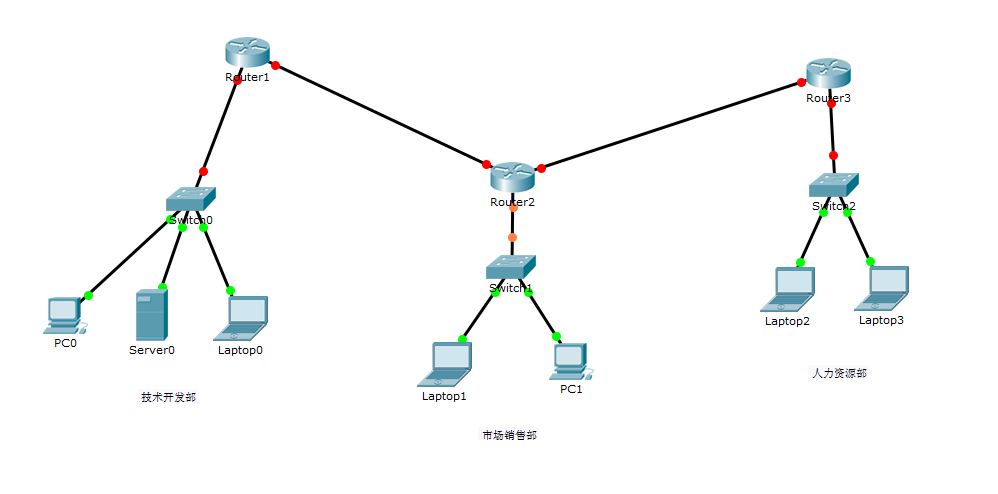
访问控制及VPN技术

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

近日，T公司从大兴区搬迁至了宇宙中心五道口，因此身为公司网络管理员的你需要在公司新址进行内网的重新设计与部署。在这次重部署的过程中，你也希望使公司网络能够更加安全、高效地发挥作用。目前公司主要分为三个部门：技术开发部、市场销售部和人力资源部。由于分工不同，各个部门均选用不同的子网便于管理。您在前期已经初步搭建起了网络，并完成了路由部分，现在你将着手完成网络的安全化工作。

##### 网络预拓扑



技术开发部（192.168.1.0/24）：Router1, Switch0, Server0, PC0, Laptop0

市场销售部（192.168.2.0/24）：Router2, Switch1, PC1, Laptop1

人力资源部（192.168.3.0/24）：Router3, Switch2, Laptop2, Laptop3

注意：除图中设备外，各个部门内还有若干其他设备处于各自的子网中

##### 任务6 网络的职务权限控制 6’

为了便于公司的管理，你需要从技术层面对网络进行权限设置，以达到控制访问的效果。公司部分设备的使用情况如下表所示：

|  |  |  |  |
| --- | --- | --- | --- |
| 设备名称 | 使用人 | 部门 | 备注 |
| PC0 | X部长（你） | 技术开发部 | - |
| Server0 | 丁部员 | 技术开发部 | 资源管理 |
| Laptop0 | 杨助手 | 技术开发部 | 联络人 |
| Laptop1 | 王部长 | 市场销售部 | - |
| PC1 | 李秘书 | 市场销售部 | 联络人 |
| Laptop2 | 冯部长 | 人力资源部 | - |
| Laptop3 | 刘秘书 | 人力资源部 | 联络人 |

为了便于进行安全管理，公司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，在必要时可以在部门内略微调整网络：

1. 一般地，各个部门内部的所有成员均能相互交流。
2. 然而，在部门之间的相互通信只能通过几位助手和秘书进行，即A部门的成员只能与B部门的联络人（杨助手、李秘书和刘秘书）进行通信。
3. 另外，三个部长可以互相讨论工作，进行部长会议。
4. 特别地，由于Server0存放了大量的技术资源，在整个公司只有其直属上司你可以通信。

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 程序员也可以有“最高”权限 4’

由于你兼任公司的网络管理者，所以你需要经常对各个设备的网络连通性进行探测。请在前一任务的基础上进行相应的配置，使得你能够对公司所有设备进行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 蒸蒸日上 10’

由于公司事业蒸蒸日上，尹董事在三里屯购下了一处地皮成立分部，现决定将技术开发部搬迁至该处。由于公司总部与分部距离较远，因而公司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为公司分部与公司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部门正常通信，请简述原因。

为了解决通信问题，你使用了助手的提议，决定配置IPSec VPN，让公司内网可以穿越公网。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，重构后的公司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 探究新的应用场景3’

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。

可参考之前的同事曾经完成过的课题进行（最多2’），也可以自行发现其他更有价值的场景（最多3’），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……