

《计算机网络安全技术》课后作业

2017 秋季 • 40240572 • 主讲：尹霞

姓名： _____ 学号： _____

作业要求：

布置作业时间：2017 年 12 月 08 日（第 12 周）

提交作业期限：2017 年 12 月 22 日（第 14 周）

提交作业方式：网络学堂（请使用作业模板提交作业）

迟交与未交的作业都按照零分计算

本次作业在课程最终成绩中记 20 分

作业题目：体验网络配置（20 分+5 分）

下面共有 7 个任务（5 个必做，2 个选做），请认真阅读任务说明，在 Packet Tracer 中完成任务，并提交详细的实验报告。

请在提交的实验报告中，说明工作原理、解决方案和配置步骤。也可以利用 Packet Tracer 截图辅助说明。

《计算机网络安全技术》课后作业

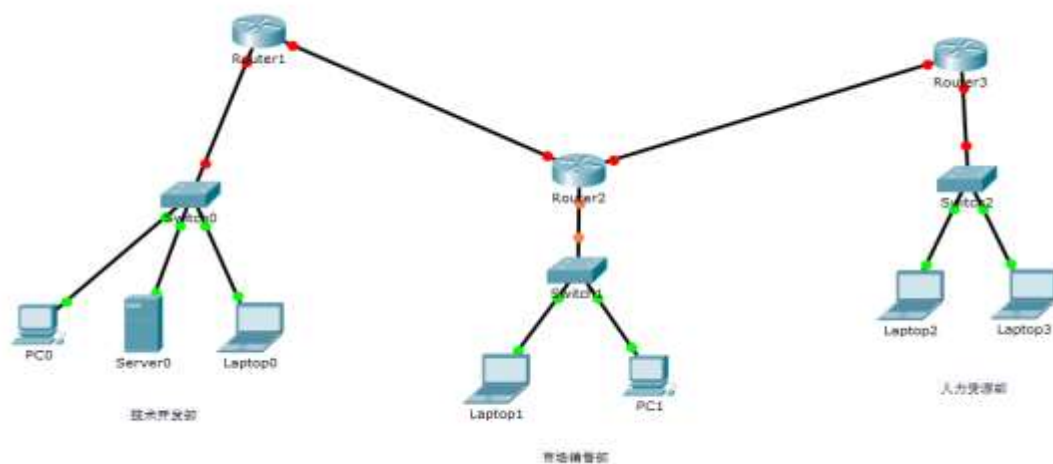
2017 秋季 • 40240572 • 主讲：尹霞

体验网络配置

实验背景

上市不久的 T 公司为了让公司员工能够在一个更加安全、高效、便于管理的环境中工作，决定对公司的内网进行重部署。T 公司的三个重要部门分别为技术开发部、市场销售部和人力资源部，不同部门拟分配不同的网段。你是 T 公司的网络管理人员，你的同事小于已经为公司内网部署做好了一份草案，请逐步完善草案并配置符合要求的网络。

网络预拓扑



技术开发部：Router0, Switch0, Server0, PC0, Laptop0

市场销售部：Router1, Switch1, PC1, Laptop1

人力资源部：Router2, Switch2, Laptop2, Laptop3

IP 分配方案

Device	Port	IP	Mask	Gateway
Router1	端口 1	192.168.1.1	/24	-
	端口 2	10.1.2.1	/24	-
Router2	端口 1	10.1.2.2	/24	-
	端口 2		/24	-
	端口 3	192.168.2.1	/24	-
Router3	端口 1	20.2.3.3	/24	-
	端口 2	192.168.3.1	/24	-
PC0	端口 1	192.168.1.2	/24	192.168.1.1
PC1	端口 1	192.168.2.2	/24	192.168.2.1

《计算机网络安全技术》课后作业

2017 秋季 • 40240572 • 主讲：尹霞

Server0	端口 1	192.168.1.3	/24	
Laptop0	端口 1	192.168.1.4	/24	192.168.1.1
Laptop1	端口 1	192.168.2.3	/24	192.168.2.1
Laptop2	端口 1	192.168.3.2	/24	192.168.3.1
Laptop3	端口 1	192.168.3.3	/24	192.168.3.1

任务 1 粗心的同事 (3 分)

作为一名资深的网络管理员，你很快就发现小于不小心将两滴墨水溅在了 IP 分配方案上，不仅如此，经验不足的他在分配 IP 时还出现了一个纰漏。请补全方案，指出并更正错误。

在完善铺设方案后，请选择合适的设备及连线将该网络铺设出来。并且为各个接口配置对应的 IP 等属性。

任务 2 公网网关安全 (4 分)

公网与公司内网的接入点位于技术开发部的 Router1 上，为了防止他人的恶意入侵，你需要至少给 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。

请至少在 Router1 上设置上述三种口令，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？

任务 3 各部门的正常通信 (3 分)

在铺设好网络之后，你想要测试一下公司的各个部门网络是否联通，ICMP 协议为你提供了合适的网络控制信息进行探测。由于公司的网络结构相对简单，你可以在各个路由器上配置静态路由使得各网段正常通信，使 ICMP 控制报文能够从公司中任一终端访问另一终端。采用这个思路，使用配置静态路由的方法，让三个部门能够顺利通讯。

任务 4 避免设备故障带来的影响 (4 分)

在网络运行一段时间后，你发现技术开发部与市场销售部之间的链路承载了公司最多的流量，然而该链路由于公司装修的原因经常发生物理故障。一旦发生故障，两个部门间没有备用的路由进行通信，使得公司网络极其不稳定。

在领导的授意下，你又为公司购置了几台新的路由器和一些网线。你希望通过这

《计算机网络安全技术》课后作业

2017 秋季 • 40240572 • 主讲：尹霞

些新的设备保障 Router1 和 Router2 之间的通信，使得其间任一链路或者其他路由器发生故障时，流量可以通过另外的备用链路到达目的地。

请自行选择一些网络设备，从拓扑和路由两方面为 Router1 和 Router2 两台路由器间的通信提供一定的鲁棒性，即若其间的链路或者其他设备发生单点故障，网络数据能够自行选择另外一条路径到达目的地。

任务 5 人员精简计划 (6 分)

由于公司正在蓬勃发展，每隔 3 个月就要对内部员工进行能力评定。在最近的一次评定中，公司决定辞退能力较弱的几位职员，转而招聘新成员，辞退名单保存在人力资源部的 Laptop3 上。经规定，除了人力资源部的员工和各个部门的部长（PC0 和 PC1）以外，其他人无法提前查看到该辞退名单。

请你通过访问控制列表 ACL 在 Router3 上配置合适的访问控制规则，过滤一切从 Laptop3 向其他部门部员的流量。

另外，由于 Server0 被用来对公司内网进行联通性调试，需要能够 ping 通公司的任一终端。请通过 CBAC（Context-Based Access Control）技术，让 Server0 能够与 Laptop3 进行 ICMP 通信，但员工无法利用其窃取辞退名单。

bonus 任务 6 利用协议进行路由管理 (2 分)

由于公司的规模日益扩大，一直使用静态路由配置容易出现错误，也不利于网络的管理。公司决定使用路由协议自动形成路由。请从 OSPF、RIP、BGP 中选择你认为合适的一个路由协议，通过对协议进行配置，在不配置静态路由的情况下自动生成路由。

bonus 任务 7 IPsec VPN 跨越公网 (3 分)

公司在郊区购置了一块楼盘作为公司分部，现决定将人力资源部迁往分部。这样，人力资源部与市场销售部的通信需要跨越公网。我们希望在修改已配置的子网 IP 的前提下，通过 IPsec VPN 技术在 Router2 和 Router3 之间建立隧道，使得两个部门仍然能够使用之前的子网 IP 进行通信，并能穿越公网传输。

IPsec 技术中使用 ESP 进行加密和检验，加密算法选择 DES，哈希算法使用 MD5。要求公司的两个分部能够互相通信。（若调试不方便，该任务可以删除之前配置的 ACL）