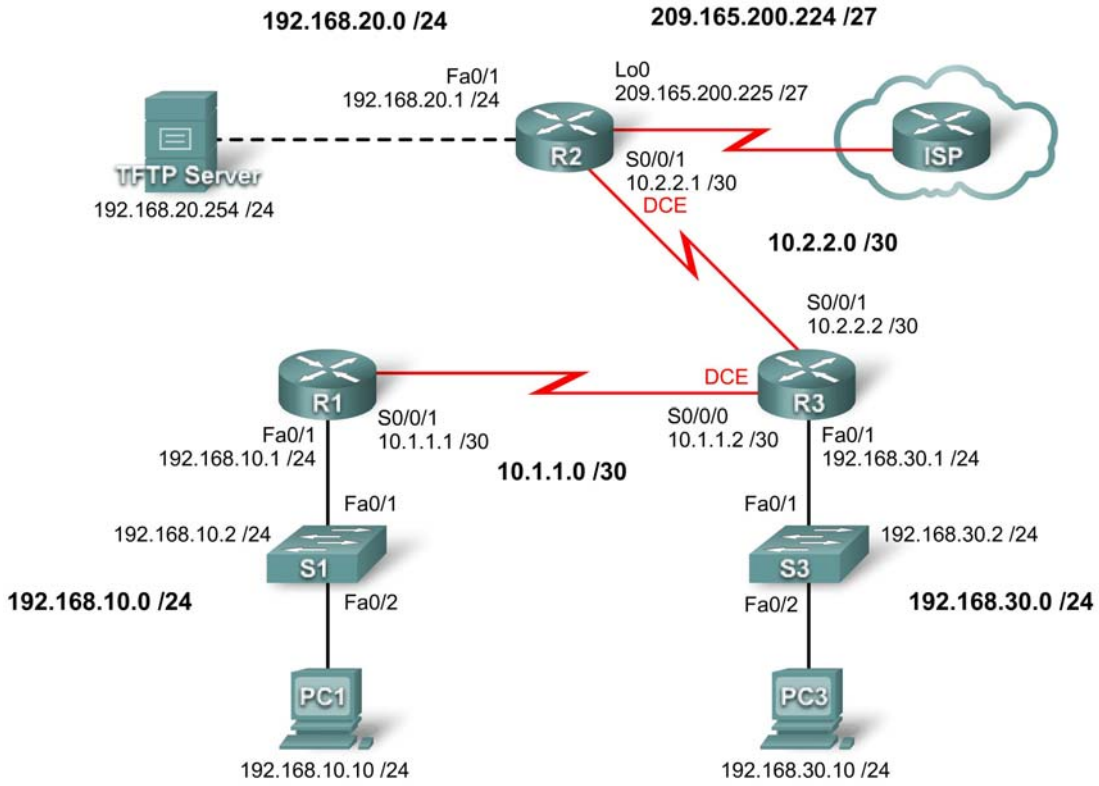
实验 4.6.2：安全配置练习

拓扑图



地址表

设备	接口	IP 地址	子网掩码	默认网关
R1	Fa0/1	192.168.10.1	255.255.255.0	不适用
	S0/0/1	10.1.1.1	255.255.255.252	不适用
R2	Fa0/1	192.168.20.1	255.255.255.0	不适用
	S0/0/1	10.2.2.1	255.255.255.252	不适用
	Lo0	209.165.200.225	255.255.255.224	不适用
R3	Fa0/1	192.168.30.1	255.255.255.0	不适用
	S0/0/1	10.2.2.2	255.255.255.252	不适用
	S0/0/0	10.1.1.2	255.255.255.252	不适用
S1	VLAN10	192.168.10.2	255.255.255.0	不适用
S3	VLAN30	192.168.30.2	255.255.255.0	不适用
PC1	网卡	192.168.10.10	255.255.255.0	192.168.10.1
PC3	网卡	192.168.30.10	255.255.255.0	192.168.30.1
TFTP Server	网卡	192.168.20.254	255.255.255.0	192.168.20.1

学习目标

完成本实验后，您将能够：

- 根据拓扑图完成网络电缆连接
- 清除启动配置，重新启动路由器使其处于默认状态
- 在路由器上执行基本配置任务
- 配置并激活接口
- 配置基本路由器安全功能
- 禁用未使用的 Cisco 服务和接口
- 保护企业网络免遭基本的外部和内部攻击
- 了解并管理 Cisco IOS 配置文件和 Cisco 文件系统
- 设置并使用 Cisco SDM（安全设备管理器）来配置基本的路由器安全功能

场景

在本实验中，您将对拓扑图中显示的网络配置安全性。如果需要协助，请参考“基本安全”实验。不过，请尽量多动手练习。在本实验中，请不要对任何控制台线路使用口令保护或登录保护功能，因为这样可能导致意外注销。但是，您还是应该通过其它方式保护控制台线路。在本实验中，请统一使用 **ciscoccna** 口令。

任务 1：准备网络

步骤 1：根据拓扑图所示完成网络电缆连接。

步骤 2：清除路由器的所有配置。

任务 2：执行基本的路由器配置

步骤 1：配置路由器。

根据以下说明配置 R1、R2 和 R3 路由器：

- 依照拓扑图配置路由器主机名。
- 禁用 DNS 查找。
- 配置当日消息标语。
- 在 R1、R2 和 R3 上配置 IP 地址。
- 在所有路由器上对全部网络启用 RIPv2。
- 在 R2 上创建环回接口以模拟通往 Internet 的连接。
- 在交换机 S1 和 S3 上创建 VLAN，并配置各个接口以参与到 VLAN 中
- 配置路由器 R3，使用 SDM 来保护连接
- 在 PC3 或 R3 上安装 SDM（如果尚未安装）

步骤 2：配置以太网接口。

使用本实验开头部分地址表中的 IP 地址和默认网关配置 PC1、PC3 和 TFTP Server 的以太网接口。

步骤 3：通过在每台 PC 和 TFPT Server 上 ping 默认网关测试 PC 配置。

任务 3：保护对路由器的访问

步骤 1：使用本地数据库配置安全口令和 AAA 身份验证。

为路由器访问创建安全口令。创建用户名 **ccna**，将其存储在路由器本地。将路由器配置为使用本地身份验证数据库。记住在本实验中统一使用 **ciscoccna** 口令。

步骤 2：保护控制台线路和 vty 线路。

配置控制台线路和 vty 线路，使之阻止在 2 分钟内 5 次输入错误用户名和口令的用户。禁止这些用户在接下来的 2 分钟内进行的其它登录尝试。

步骤 3：检验在达到规定的失败尝试限制后，连接是否会遭到拒绝。

任务 4：保护对网络的访问

步骤 1：保护 RIP 路由协议。

不要对非网络路由器（即不属于本场景的路由器）发送 RIP 更新。对 RIP 更新进行身份验证并加密。

步骤 2：确保 RIP 路由仍能正常工作。

任务 5：使用 SNMP（简单网络管理协议）记录活动

步骤 1：将所有设备上的 SNMP 日志记录配置为发送到位于 192.168.10.250 的 syslog 服务器。

步骤 2：将严重级别为 4 的所有消息记录到 syslog 服务器上。

任务 6：禁用未使用的 Cisco 网络服务

步骤 1：在所有设备上禁用未使用的接口。

步骤 2：禁用 R1 上未使用的全局服务。

步骤 3：禁用 R1 上未使用的接口服务。

步骤 4：使用 AutoSecure 保护 R2。

记住在本实验中统一使用 **ciscoccna** 口令。

任务 7：管理 Cisco IOS 和配置文件

步骤 1：确定运行配置文件位于路由器内存的哪个位置。

步骤 2：使用 TFTP 将运行配置文件从 R1 传输到 R2。

步骤 3：对 R1 执行 Break 操作，然后使用 ROMmon 将其还原。

将下列命令复制粘贴到 R1 上，然后使用 ROMmon 还原 R1。

```
line vty 0 4
 exec-timeout 0 20
line console 0
 exec-timeout 0 20
end
copy run start
exit
```

步骤 4：使用 TFTP 将所保存的配置从 R2 恢复到 R1。

步骤 5：擦除 R2 上保存的配置。

任务 8：使用 SDM 保护 R2

步骤 1：使用 PC1 连接到 R2。

步骤 2：导航至 Security Audit（安全审计）功能。

步骤 3：执行安全审计。

步骤 4：选择要应用到路由器的设置。

步骤 5：将配置提交至路由器。

任务 9：记录路由器配置

在每台路由器上发出 **show run** 命令捕获配置信息。

任务 10：实验后清理

清除配置，然后重新启动路由器。拆下电缆并放回保存处。对于通常连接到其它网络（例如学校 LAN 或 Internet）的 PC 主机，请重新连接相应的电缆并恢复原有的 TCP/IP 设置。