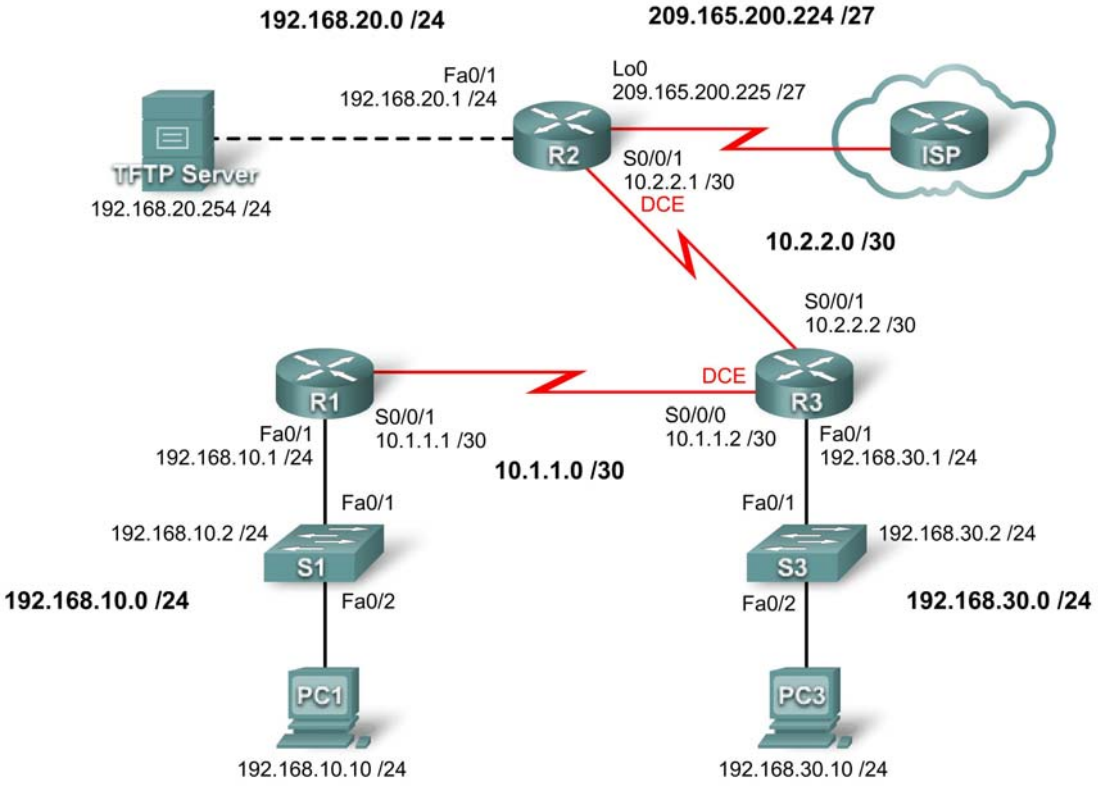
实验 4.6.3：安全配置故障排除

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
- 删除启动配置并将所有路由器恢复为默认状态
- 使用所提供的脚本加载路由器
- 查找并纠正所有网络错误
- 记录纠正后的网络

场景

贵公司刚招聘一名新的网络工程师，他由于配置错误及疏忽等原因而在网络中引入了一些安全问题。您的上级要求您将这位新工程师在配置路由器时犯下的错误纠正过来。在纠正错误的过程中，应确保所有设备安全、而且管理员仍能访问它们，并且保证所有网络均可到达。所有路由器必须能通过 SDM 从 PC1 上访问到。请使用 Telnet 和 ping 之类的工具来检查设备是否安全。如果使用此类工具进行未经授权的访问，则应加以拒绝，但同时必须确保授权的访问得以正常进行。在本实验中，请不要对任何控制台线路使用登录保护或口令保护功能，以免意外注销。请在本场景中统一使用 **ciscoccna** 口令。

任务 1：使用所提供的脚本加载路由器

将以下配置加载到拓扑中的设备。

R1:

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 10 log
security passwords min-length 6
enable secret ciscoccna
!
aaa new-model
!
aaa authentication login LOCAL_AUTH local
!
aaa session-id common
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip source-route
```

```
no ip gratuitous-arps
ip cef
!
no ip dhcp use vrf connected
!
no ip bootp server
!
key chain RIP_KEY
 key 1
  key-string cisco
username ccna password ciscoccna
!
 interface FastEthernet0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no shutdown
duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 duplex auto
 speed auto
 no shutdown
!
!
interface Serial0/0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no shutdown
 no fair-queue
 clockrate 125000
!
interface Serial0/0/1
 ip address 10.1.1.1 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no shutdown
!
interface Serial0/1/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no shutdown
 clockrate 2000000
!
```

```
interface Serial0/1/1
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
!
router rip
 version 2
 passive-interface default
 no passive-interface Serial0/0/0
 network 10.0.0.0
 network 192.168.10.0
 no auto-summary
!
ip classless
!
no ip http server
!
logging 192.168.10.150
no cdp run
!
line con 0
 exec-timeout 5 0
 logging synchronous
 transport output telnet
line aux 0
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport output telnet
line vty 0 4
 exec-timeout 5 0
 logging synchronous
 login authentication local_auth
!
end
```

R2：

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname R2
!
security authentication failure rate 10 log
security passwords min-length 6
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
!
resource policy
!
```

```
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no ip source-route
no ip gratuitous-arps
ip cef
!
no ip dhcp use vrf connected
!
no ip bootp server
!
!
username ccna password ciscoccna
!
!
interface FastEthernet0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 shutdown
 no fair-queue
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 clockrate 128000
 no shutdown
!
```

```
interface Serial0/1/0
 ip address 209.165.200.224 255.255.255.224
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 no shutdown
!
interface Serial0/1/1
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 shutdown
 clockrate 2000000
!
router rip
 version 2
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.20.0
 no auto-summary
!
ip classless
!
no ip http server
!
logging trap debugging
logging 192.168.10.150
!
line con 0
 exec-timeout 5 0
 logging synchronous
 transport output telnet
line aux 0
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport output telnet
line vty 0 4
 exec-timeout 0 0
 logging synchronous
 login authentication local_auth
 transport input telnet
!
end
```

R3：

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
```

```
boot-start-marker
boot-end-marker
!
security authentication failure rate 10 log
security passwords min-length 6
enable secret ciscoccna
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip source-route
no ip gratuitous-arps
ip cef
!
!
no ip dhcp use vrf connected
!
no ip bootp server
!
key chain RIP_KEY
 key 1
  key-string Cisco
!
interface FastEthernet0/0
 no ip address
 no ip redirects
 no ip proxy-arp
 no ip directed-broadcast
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 ip address 192.168.30.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 no shutdown
 duplex auto
 speed auto
!
```

```
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 clockrate 125000
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
!
router rip
 version 2
 passive-interface default
 passive-interface Serial0/0/0
 passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.30.0
 no auto-summary
!
ip classless
!
no ip http server
!
logging trap debugging
logging 192.168.10.150
no cdp run
!
control-plane
!
line con 0
 exec-timeout 5 0
 logging synchronous
 transport output telnet
line aux 0
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport output telnet
line vty 0 4
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport input telnet
!
end
```

任务 2：查找并纠正所有网络错误

使用标准的故障排除方法，查找、记录并纠正每一处错误。

注：对工作异常的生产网络排除故障时，许多微小的错误都可能导致网络完全无法运转。首先应该检查的是所有口令、密钥链名称和密钥，以及验证列表名称的拼写和大小写。许多时候，导致整个网络故障的原因往往是大小写或拼写错误。最好的办法是从最基本的项目开始逐渐往上检查。首先问自己是否所有名称和密钥都匹配。接下来，如果配置使用列表或密钥链之类的事物，请检查所引用的项目是否实际存在、在所有设备上是否一致。最好在某台设备上配置一次，然后将其复制粘贴到其它设备，这样即可确保配置完全一致。然后，当考虑禁用或限制服务时，问问自己这些服务的用途是什么、是否需要。另外还需明确路由器应送出的信息是什么。谁应该接收该信息、谁不应该接收。最后，询问自己这些服务可供用户执行什么操作、您是否希望用户执行那些操作。一般而言，如果您能想到服务可能被通过某种途径滥用，您就应该采取措施来预防此情况的发生。

任务 3：记录纠正后的网络

任务 4：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。