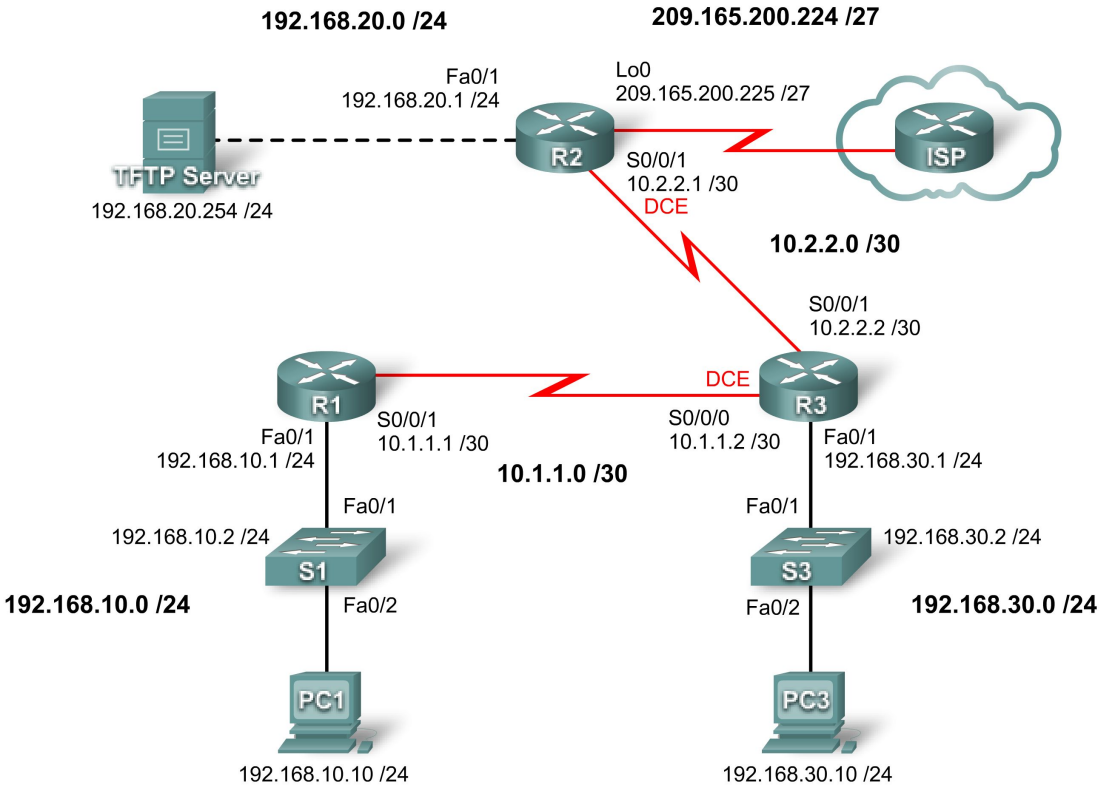
Cisco | Networking Academy®
Mind Wide Open™

# Lab 4.6.3: Troubleshooting Security Configuration

## Topology Diagram




## Addressing Table

| Device | Interface | IP Address | Subnet Mask | Default Gateway |
|---|---|---|---|---|
| **R1** | Fa0/1 | 192.168.10.1 | 255.255.255.0 | N/A |
| | S0/0/1 | 10.1.1.1 | 255.255.255.252 | N/A |
| **R2** | Fa0/1 | 192.168.20.1 | 255.255.255.0 | N/A |
| | S0/0/1 | 10.2.2.1 | 255.255.255.252 | N/A |
| | Lo0 | 209.165.200.225 | 255.255.255.224 | N/A |
| **R3** | Fa0/1 | 192.168.30.1 | 255.255.255.0 | N/A |
| | S0/0/1 | 10.2.2.2 | 255.255.255.252 | N/A |
| | S0/0/0 | 10.1.1.2 | 255.255.255.252 | N/A |
| **S1** | VLAN10 | 192.168.10.2 | 255.255.255.0 | N/A |
| **S3** | VLAN30 | 192.168.30.2 | 255.255.255.0 | N/A |
| **PC1** | NIC | 192.168.10.10 | 255.255.255.0 | 192.168.10.1 |
| **PC3** | NIC | 192.168.30.10 | 255.255.255.0 | 192.168.30.1 |
| **TFTP Server** | NIC | 192.168.20.254 | 255.255.255.0 | 192.168.20.1 |

## Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram.
- Erase the startup configuration and restore all routers to the default state.
- Load routers with supplied scripts.
- Find and correct all network errors.
- Document the corrected network.

## Scenario

Your company just hired a new network engineer who has created some security issues in the network with misconfigurations and oversights. Your boss has asked you to correct the errors the new engineer has made configuring the routers. While correcting the problems, make sure that all the devices are secure but are still accessible by administrators, and that all networks are reachable. All routers must be accessible with SDM from PC1. Verify that a device is secure by using tools such as Telnet and ping. Unauthorized use of these tools should be blocked, but also ensure that authorized use is permitted. For this lab, do not use login or password protection on any console lines to prevent accidental lockout. Use **ciscoccna** for all passwords in this scenario.

### Task 1: Load Routers with the Supplied Scripts

Load the following configurations into the devices in the topology.

**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
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 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
 no 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
 transport input telnet
!
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
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
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 Loopback0
 ip address 209.165.200.225 255.255.255.224
!
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
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 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
 network 209.165.200.224
 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
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.30.0
 no auto-summary
!
ip classless
!
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
```

### Task 2: Find and Correct all Network Errors

Using standard troubleshooting methods, find, document, and correct each error.

Note: When troubleshooting a production network that is not working, many very small mistakes can prevent everything from working correctly. The first item to check is the spelling and case of all passwords, keychain names and keys, and authentication list names. It is often a mismatch in case or spelling that causes total failure. The best practice is to start with the most basic and work upward. First ask whether all the names and keys match up. Next, if the configuration uses a list or keychain and so on, check if the item referenced actually exists and is the same on all devices. Configuring something once on one device and then copying and pasting into the other device is the best way to ensure that the configuration is exactly the same. Next, when thinking about disabling or restricting services, ask what the services are used for and if they are needed. Also ask what information the router should be sending out. Who should and should not receive that information. Finally, ask what the services enable the users to do, and do you want them to be able to do that. Generally, if you can think of a way that a service can be abused, you should take steps to prevent that.

### Task 3: Document the Corrected Network

### Task 4: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.