Laboratório 4.6.3: Identificação e solução de problemas de configuração de segurança

Diagrama de topologia

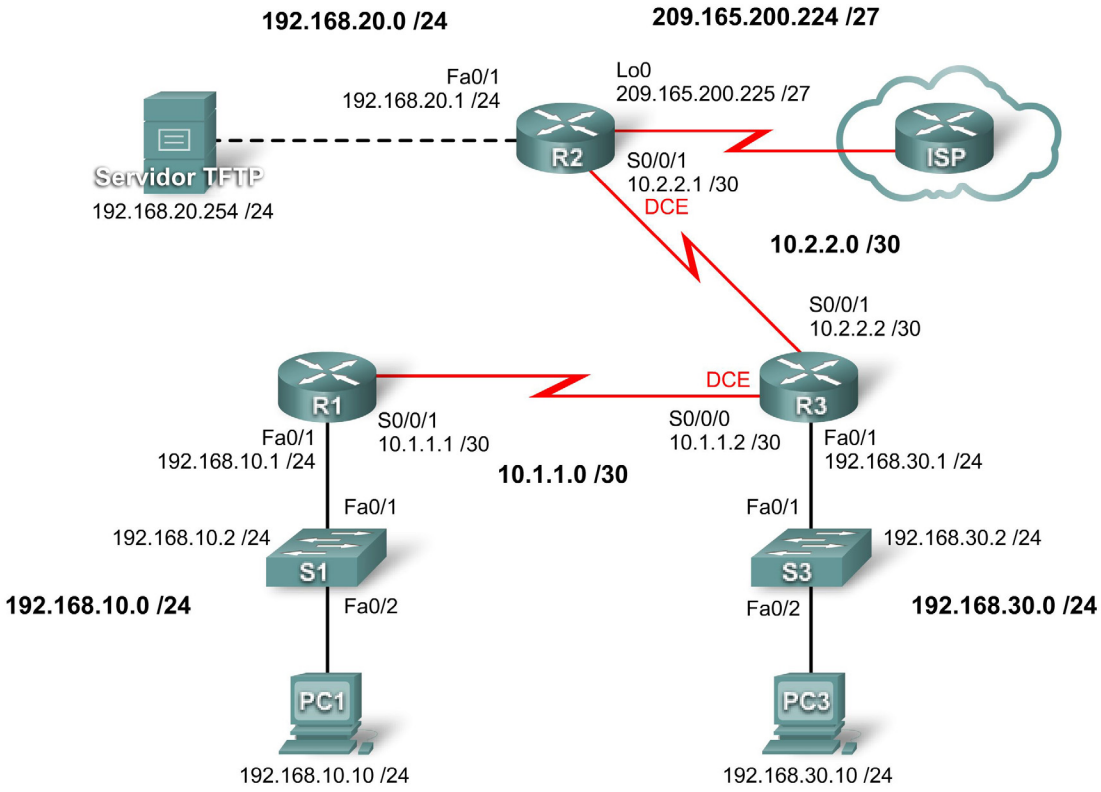

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede	Gateway padrão
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	Placa de rede	192.168.10.10	255.255.255.0	192.168.10.1
PC3	Placa de rede	192.168.30.10	255.255.255.0	192.168.30.1
Servidor TFTP	Placa de rede	192.168.20.254	255.255.255.0	192.168.20.1

Objetivos de aprendizagem

Após concluir este laboratório, você será capaz de:

- Cabo de rede de acordo com o diagrama de topologia.
- Apagar a configuração de inicialização e restaurar o estado padrão de todos os roteadores.
- Carregar roteadores com scripts fornecidos.
- Localize e corrija todos os erros de rede.
- Documentar a rede corrigida.

Cenário

Sua empresa contratou recentemente um novo engenheiro de rede que criou alguns problemas de segurança na rede com configurações incorretas e omissões. Seu chefe lhe pediu para corrigir os erros que o novo engenheiro cometeu ao configurar os roteadores. Enquanto corrige os problemas, verifique se todos os dispositivos estão seguros, mas ainda acessíveis para administradores, e que todas as redes são alcançáveis. Todos os roteadores devem ser acessíveis com SDM em PC1. Verificar se um dispositivo é seguro usando ferramentas como Telnet e ping. O uso não autorizado dessas ferramentas deve ser bloqueado. Por outro lado, o uso autorizado deve ser permitido. Para este laboratório, não use a proteção por login ou senha em nenhuma linha de console para impedir o bloqueio acidental. Use **ciscoccna** para todas as senhas deste cenário.

Tarefa 1: Carregar roteadores com os scripts fornecidos

Carregue as configurações a seguir nos dispositivos da topologia.

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
```

Tarefa 2: Localizar e corrigir todos erros de rede

Com o uso de métodos de solução de problemas padrão, encontre, documente e corrija todos os erros.

Nota: durante a identificação e solução de problemas de uma rede de produção que não esteja funcionando, muitos equívocos menores podem impedir que tudo funcione corretamente. O primeiro item a ser verificado é a ortografia e a maiúsculas ou minúsculas de todas as senhas, nomes de cadeias de chave e chaves, além dos nomes da lista de autenticação. Costuma ser um equívoco no uso de maiúsculas/minúsculas ou na ortografia a causa da falha total. A prática recomendada é iniciar com o mais básico e ir avançando. Primeiro pergunte se todos os nomes e chaves correspondem. Em seguida, se a configuração utilizar uma lista ou cadeia de chaves, verifique se o item referenciado efetivamente existe e se é o mesmo em todos os dispositivos. Configurar algo uma vez em um dispositivo, copiar e colá-lo em outro dispositivo é a melhor maneira de assegurar que a configuração é exatamente a mesma. Em seguida, pensando em desabilitar ou restringir serviços, pergunte quais são os serviços utilizados e se eles são necessários. Também peça as informações sobre o que o roteador deve enviar. Quem deve e quem não deve receber essas informações. Por fim, pergunte quais serviços são permitidos aos usuários e se eles devem ser capazes de usá-los. Em geral, se pensar em uma forma de abuso do serviço, você deverá seguir as etapas para impedir isso.

Tarefa 3: Documentar a rede corrigida

Tarefa 4: Limpar

Apague as configurações e recarregue os roteadores. Desconecte e guarde o cabeamento. Para hosts PC normalmente conectados a outras redes (como a LAN escolar ou a Internet), reconecte o cabeamento apropriado e restaure as configurações TCP/IP.