Travaux pratiques 4.6.3 : dépannage de la configuration de sécurité

Diagramme de topologie

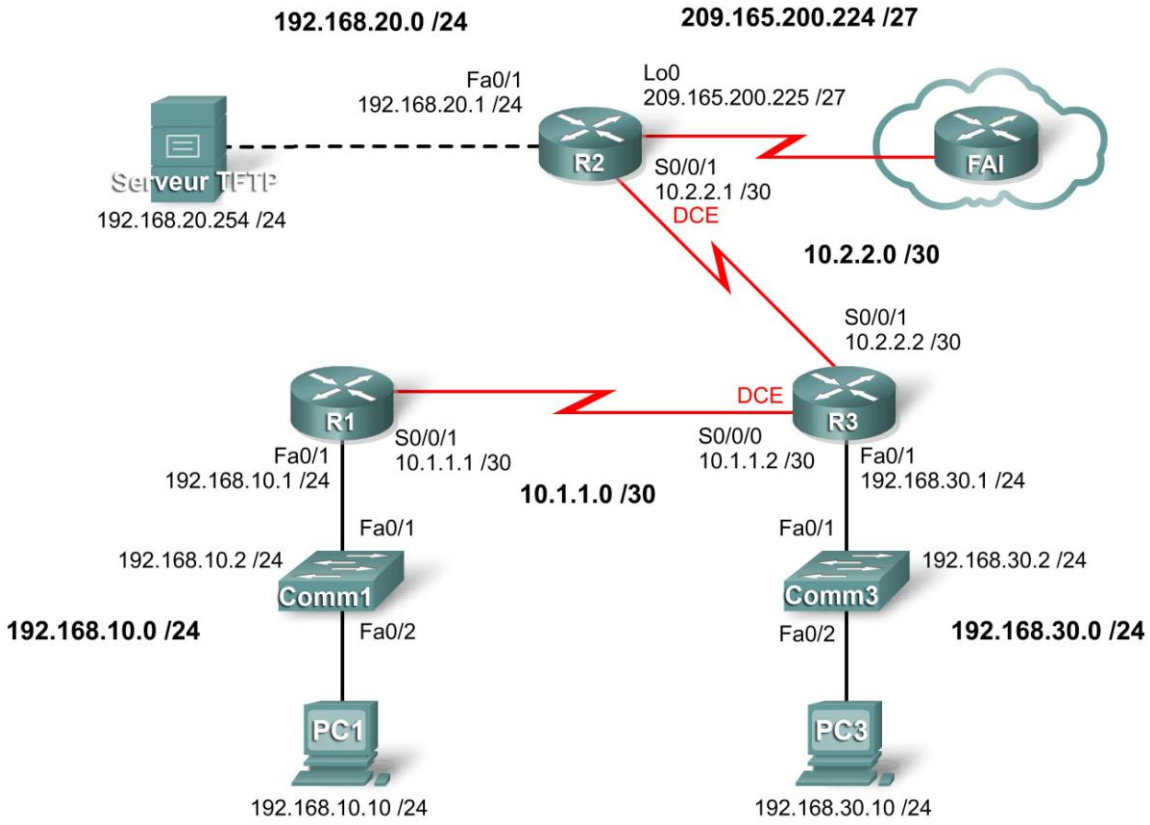

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	Fa0/1	192.168.10.1	255.255.255.0	N/D
	S0/0/1	10.1.1.1	255.255.255.252	N/D
R2	Fa0/1	192.168.20.1	255.255.255.0	N/D
	S0/0/1	10.2.2.1	255.255.255.252	N/D
	Lo0	209.165.200.225	255.255.255.224	N/D
R3	Fa0/1	192.168.30.1	255.255.255.0	N/D
	S0/0/1	10.2.2.2	255.255.255.252	N/D
	S0/0/0	10.1.1.2	255.255.255.252	N/D
Comm1	VLAN10	192.168.10.2	255.255.255.0	N/D
Comm3	VLAN30	192.168.30.2	255.255.255.0	N/D
PC1	Carte réseau	192.168.10.10	255.255.255.0	192.168.10.1
PC3	Carte réseau	192.168.30.10	255.255.255.0	192.168.30.1
Serveur TFTP	Carte réseau	192.168.20.254	255.255.255.0	192.168.20.1

Objectifs pédagogiques

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

- Câbler un réseau conformément au diagramme de topologie
- Supprimer la configuration de démarrage et réinitialiser tous les routeurs dans leur état par défaut
- Charger les routeurs avec les scripts fournis
- Identifier et corriger toutes les erreurs réseau
- Documenter le réseau corrigé

Scénario

Votre entreprise vient d'engager un nouvel ingénieur réseau qui a créé des problèmes de sécurité au niveau du réseau du fait d'erreurs de configuration et d'omissions. Votre responsable vous demande de corriger les erreurs commises par le nouvel ingénieur lors de la configuration des routeurs. Lorsque vous corrigez les erreurs, vérifiez que tous les périphériques sont bien sécurisés, et veillez à ce que ces périphériques et les réseaux restent accessibles aux administrateurs. Tous les routeurs doivent être accessibles via l'application SDM depuis PC1. Pour vérifier qu'un périphérique est sécurisé, utilisez des outils appropriés tels que Telnet et la commande ping. Toute utilisation non autorisée de ces outils devra être bloquée, mais assurez-vous également qu'une utilisation autorisée de ces outils soit possible. Dans le cadre de cet exercice, n'utilisez pas de protection par nom d'utilisateur ou mot de passe sur les lignes de console, afin d'empêcher tout verrouillage accidentel. Dans ce scénario, utilisez **ciscoccna** pour tous les mots de passe.

Tâche 1 : chargement des routeurs avec les scripts fournis

Chargez les configurations suivantes dans les périphériques de la topologie.

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
 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
!
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
```

Tâche 2 : détection et correction de toutes les erreurs réseau

En utilisant les méthodes de dépannage standard, recherchez, documentez et corrigez les erreurs.

Remarque : lorsque vous dépannez un réseau de production défaillant, sachez que de petites erreurs peuvent être à l'origine de dysfonctionnements. Vérifiez en premier lieu l'orthographe et la casse des mots de passe, des clés et des noms de chaînes de clés, ainsi que des noms de listes d'authentification. Les défaillances sont souvent dues au non-respect d'une casse ou à un terme mal orthographié.
La méthode recommandée consiste à commencer par les étapes de base avant de procéder aux étapes suivantes. Vérifiez d'abord si les noms et les clés correspondent. Ensuite, si la configuration utilise une liste ou une chaîne de clés, vérifiez si l'élément référencé existe réellement et s'il est le même sur tous les périphériques. Pour garantir que la configuration est exactement la même, il est recommandé d'effectuer cette configuration une première fois sur un périphérique, puis de la copier et de la coller dans l'autre périphérique. En outre, lorsque vous envisagez de désactiver ou de limiter des services, déterminez à quoi servent ces services et s'ils sont nécessaires. Déterminez également les informations que le routeur doit envoyer, ainsi que les personnes qui doivent les recevoir et celles qui ne doivent pas les recevoir. Enfin, définissez les opérations que les utilisateurs peuvent effectuer grâce à ces services, et si vous souhaitez les autoriser à effectuer ces opérations. En règle générale, vous devez prendre les mesures nécessaires afin d'éviter tout abus d'un service.

Tâche 3 : documentation du réseau corrigé

Tâche 4 : remise en état

Supprimez les configurations et rechargez les routeurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage souhaité et restaurez les paramètres TCP/IP pour les PC hôtes habituellement connectés aux autres réseaux (réseaux locaux de votre site ou Internet).