Travaux pratiques 5.5.1 : listes de contrôle d'accès de base

Diagramme de topologie

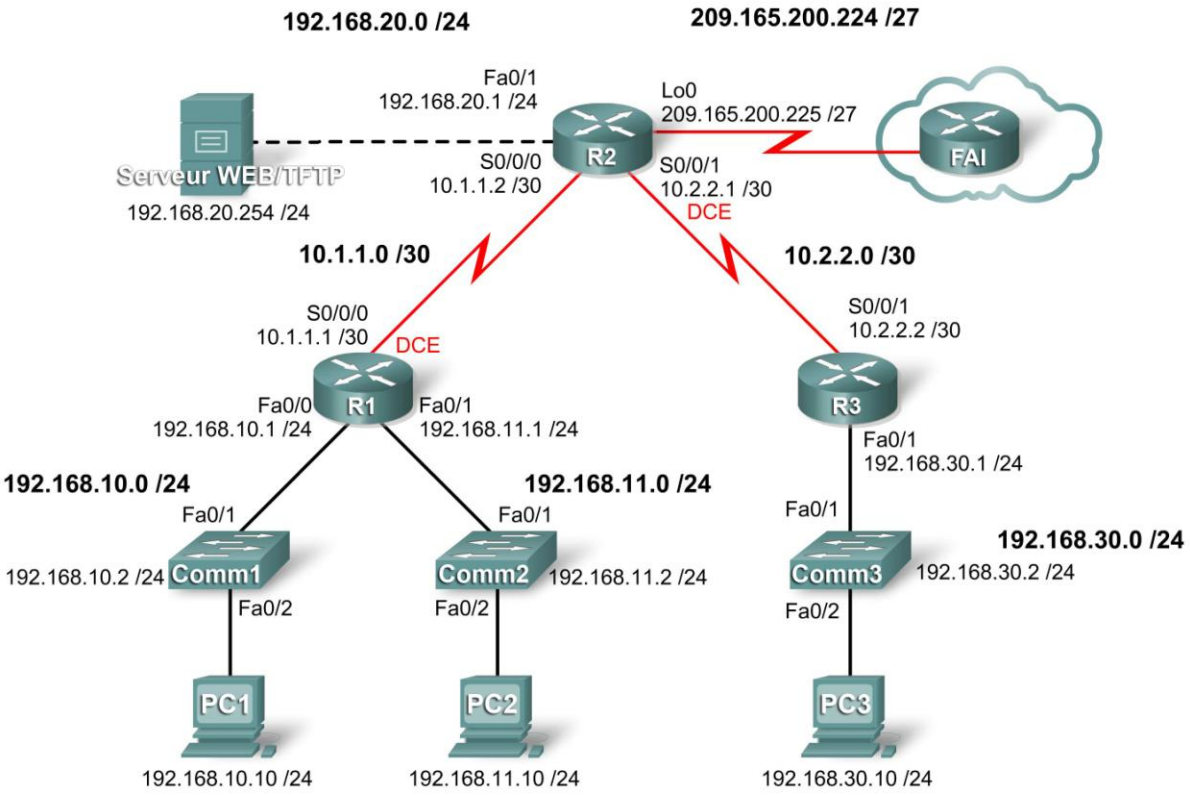

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	**Fa0/0**	192.168.10.1	255.255.255.0	
	Fa0/1	192.168.11.1	255.255.255.0	
	S0/0/0	10.1.1.1	255.255.255.252	
R2	**Fa0/1**	192.168.20.1	255.255.255.0	
	S0/0/0	10.1.1.2	255.255.255.252	
	S0/0/1	10.2.2.1	255.255.255.252	
	Lo0	209.165.200.225	255.255.255.224	
R3	**Fa0/1**	192.168.30.1	255.255.255.0	
	S0/0/1	10.2.2.2	255.255.255.252	
Comm1	**Vlan1**	192.168.10.2	255.255.255.0	192.168.10.1

Comm2	**Vlan1**	192.168.11.2	255.255.255.0	192.168.11.1
Comm3	**Vlan1**	192.168.30.2	255.255.255.0	192.168.30.1
PC1	**Carte réseau**	192.168.10.10	255.255.255.0	192.168.10.1
PC2	**Carte réseau**	192.168.11.10	255.255.255.0	192.168.11.1
PC3	**Carte réseau**	192.168.30.10	255.255.255.0	192.168.30.1
Serveur Web	**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 :

- Concevoir des listes de contrôle d'accès nommées standard et étendues
- Appliquer des listes de contrôle d'accès nommées standard et étendues
- Tester des listes de contrôle d'accès nommées standard et étendues
- Résoudre les problèmes liés aux listes de contrôle d'accès nommées standard et étendues

Scénario

Dans le cadre de ces travaux pratiques, vous apprendrez à configurer la sécurité d'un réseau de base à l'aide des listes de contrôle d'accès. Vous appliquerez des listes de contrôles d'accès standard et étendues.

Tâche 1 : préparation du réseau

Étape 1 : câblage d'un réseau similaire à celui du diagramme de topologie

Vous pouvez utiliser n'importe quel routeur disponible durant les travaux pratiques, pourvu qu'il dispose des interfaces requises, comme illustré sur le diagramme de topologie.

Remarque : ces travaux pratiques ont été développés et testés à l'aide de routeurs 1841. Si vous utilisez les routeurs 1700, 2500 ou 2600, les sorties des routeurs et les descriptions des interfaces apparaîtront différemment. Certaines commandes peuvent être différentes ou ne pas exister sur d'anciens routeurs ou des versions du système IOS antérieures à la version 12.4.

Étape 2 : suppression des configurations existantes sur les routeurs

Tâche 2 : exécution des configurations de routeur de base

Configurez les routeurs R1, R2 et R3, ainsi que les commutateurs Comm1, Comm2 et Comm3 en respectant les consignes suivantes :

- Configurez le nom d'hôte du routeur conformément au diagramme de topologie.
- Désactivez la recherche DNS.
- Configurez un mot de passe **class** pour le mode d'exécution privilégié.
- Configurez une bannière de message du jour.
- Configurez un mot de passe cisco pour les connexions de consoles.
- Configurez un mot de passe pour les connexions de terminaux virtuels (vty).

- Configurez des adresses IP et des masques sur tous les périphériques.
- Activez la zone OSPF 0 pour l'ensemble des routeurs de tous les réseaux.
- Configurez une interface en mode bouclé sur R2 pour simuler le FAI.
- Configurez des adresses IP pour l'interface VLAN 1 sur chaque commutateur.
- Configurez chaque commutateur avec la passerelle par défaut appropriée.
- Vérifiez l'intégralité de la connectivité IP à l'aide de la commande **ping**.

Tâche 3 : configuration d'une liste de contrôle d'accès standard

Les listes de contrôle d'accès standard ne peuvent filtrer le trafic qu'en fonction de l'adresse IP source. Il est généralement recommandé de configurer une liste de contrôle d'accès standard aussi proche que possible de la destination. Dans cette tâche, vous allez configurer une liste de contrôle d'accès standard. La liste de contrôle d'accès est conçue pour bloquer le trafic provenant du réseau 192.168.11.0/24 correspondant à la salle de travaux pratiques des participants, et ce afin de l'empêcher d'accéder à des réseaux locaux sur R3.

Cette liste est appliquée en entrée, sur l'interface série de R3. N'oubliez pas que chaque liste de contrôle d'accès comporte une instruction « deny all » implicite. Cette dernière bloque tous les trafics qui ne correspondent à aucune instruction de la liste. C'est la raison pour laquelle il est nécessaire d'ajouter l'instruction **permit any** à la fin de la liste.

Avant de configurer et d'appliquer cette liste, veillez à vérifier la connectivité depuis PC1 (ou l'interface Fa0/1 sur R1) vers PC3 (ou l'interface Fa0/1 sur R3). Les tests de connectivité doivent aboutir avant d'appliquer cette liste.

Étape 1 : création de la liste de contrôle d'accès sur le routeur R3

En mode de configuration globale, créez une liste de contrôle d'accès standard nommée **STND-1**.

```
R3(config)#ip access-list standard STND-1
```

En mode de configuration de liste de contrôle d'accès standard, ajoutez une instruction chargée de refuser tous les paquets dont l'adresse source est 192.168.11.0/24 et d'ajouter un message dans la console pour chaque paquet correspondant.

```
R3(config-std-nacl)#deny 192.168.11.0 0.0.0.255 log
```

Autorisez le reste du trafic.

```
R3(config-std-nacl)#permit any
```

Étape 2 : application de la liste de contrôle d'accès

Appliquez la liste de contrôle d'accès **STND-1** pour filtrer les paquets entrant dans R3, par le biais de l'interface série 0/0/1.

```
R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group STND-1 in
R3(config-if)#end
R3#copy run start
```

Étape 3 : test de la liste de contrôle d'accès

Avant de tester la liste de contrôle d'accès, assurez-vous que la console de R3 est visible. De cette manière, vous pouvez visualiser les messages du journal de la liste d'accès lorsque le paquet est refusé.

Vérifiez la liste de contrôle d'accès en envoyant une requête ping vers le PC3 à partir du PC2. La liste de contrôle d'accès étant conçue pour bloquer le trafic dont l'adresse source fait partie du réseau 192.168.11.0/24, le PC2 (192.168.11.10) ne peut normalement pas envoyer de requêtes ping vers le PC3.

Vous pouvez également utiliser une commande ping étendue à partir de l'interface Fa0/1 sur R1, vers l'interface Fa0/1 sur R3.

```
R1#ping ip
Target IP address: 192.168.30.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.11.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.11.1
U.U.U
Success rate is 0 percent (0/5)
```

Le message suivant doit s'afficher sur la console de R3 :

```
*Sep  4 03:22:58.935: %SEC-6-IPACCESSLOGNP: list STND-1 denied 0
0.0.0.0 -> 192.168.11.1, 1 packet
```

En mode d'exécution privilégié sur R3, lancez la commande **show access-lists**. Une sortie similaire à la suivante s'affiche. Chaque ligne d'une liste de contrôle d'accès possède un compteur associé, qui affiche le nombre de paquets correspondants à la règle.

```
Standard IP access list STND-1
    10 deny   192.168.11.0, wildcard bits 0.0.0.255 log (5 matches)
    20 permit any (25 matches)
```

L'objectif de cette liste était de bloquer les hôtes du réseau 192.168.11.0/24. Tous les autres hôtes, notamment ceux du réseau 192.168.10.0/24, doivent être autorisés à accéder aux réseaux sur R3. Effectuez un autre test depuis PC1 vers PC3 pour vérifier que ce trafic n'est pas bloqué.

Vous pouvez également utiliser une commande ping étendue à partir de l'interface Fa0/0 sur R1, vers l'interface Fa0/1 sur R3.

```
R1#ping ip
Target IP address: 192.168.30.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.10.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
```

```
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/43/44 ms
```

Tâche 4 : configuration d'une liste de contrôle d'accès étendue

Lorsque vous souhaitez bénéficier d'un contrôle plus précis, vous pouvez utiliser une liste de contrôle d'accès étendue. Les listes de contrôle d'accès étendues peuvent filtrer le trafic en fonction d'autres critères que l'adresse source. Ainsi, le filtrage peut être basé sur le protocole, l'adresse IP source, l'adresse IP de destination, le numéro de port source et le numéro de port de destination.

Une autre stratégie mise en place pour ce réseau indique que les périphériques du réseau local 192.168.10.0/24 ne peuvent accéder qu'aux réseaux internes. Les ordinateurs de ce réseau local ne sont pas autorisés à accéder à Internet. Par conséquent, ces utilisateurs ne doivent pas pouvoir accéder à l'adresse IP 209.165.200.225. Cette exigence s'appliquant à la source et à la destination, il est nécessaire d'utiliser une liste de contrôle d'accès étendue.

Cette tâche consiste à configurer une liste de contrôle d'accès étendue sur R1, qui sera chargée d'empêcher le trafic en provenance d'un périphérique du réseau 192.168.10.0 /24 d'accéder à l'hôte 209.165.200.255 (l'ISP simulé). Cette liste de contrôle d'accès sera appliquée en sortie de l'interface série 0/0/0 de R1. Pour appliquer de façon optimale des listes de contrôle d'accès étendues, il est conseillé de les placer aussi près que possible de la source.

Avant de commencer, vérifiez que vous pouvez envoyer une requête ping vers 209.165.200.225 depuis le PC1.

Étape 1 : configuration d'une liste de contrôle d'accès étendue nommée

En mode de configuration globale, créez une liste de contrôle d'accès étendue nommée **EXTEND-1**.

```
R1(config)#ip access-list extended EXTEND-1
```

Vous remarquerez que l'invite du routeur change pour indiquer que le routeur est à présent en mode de configuration de liste de contrôle d'accès étendue. À partir de cette invite, ajoutez les instructions nécessaires pour bloquer le trafic provenant du réseau 192.168.10.0 /24 à destination de l'hôte. Utilisez le mot clé **host** lors de la définition de la destination.

```
R1(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225
```

N'oubliez pas que l'instruction implicite « deny all » bloque l'ensemble du trafic si vous n'ajoutez pas d'instruction **permit** supplémentaire. Ajoutez l'instruction **permit** pour vous assurer que d'autres trafics ne sont pas bloqués.

```
R1(config-ext-nacl)#permit ip any any
```

Étape 2 : application de la liste de contrôle d'accès

Dans le cas de listes de contrôle d'accès standard, la meilleure solution consiste à placer la liste aussi près que possible de la destination. En revanche, les listes de contrôle d'accès étendues sont souvent placées près de la source. La liste **EXTEND-1** sera placée sur l'interface série et filtrera le trafic sortant.

```
R1(config)#interface serial 0/0/0
R1(config-if)#ip access-group EXTEND-1 out log
R1(config-if)#end
R1#copy run start
```

Étape 3 : test de la liste de contrôle d'accès

À partir de PC1, envoyez une requête ping à l'interface de bouclage du routeur R2. Ces tests doivent échouer, car l'ensemble du trafic provenant du réseau 192.168.10.0 /24 est filtré lorsque la destination est 209.165.200.225. Si la destination correspond à une autre adresse, les envois de requêtes ping doivent aboutir. Pour le vérifier, envoyez des requêtes ping vers R3 à partir d'un périphérique du réseau 192.168.10.0/24.

Remarque : la fonctionnalité de la commande ping étendue sur R1 ne peut pas être utilisée pour tester cette liste de contrôle d'accès car le trafic est issu de R1 et n'est jamais testé sur la liste de contrôle d'accès appliquée à l'interface série R1.

Vous pouvez effectuer une vérification approfondie en entrant la commande **show ip access-list** sur R1 après l'envoi de la requête ping.

```
R1#show ip access-list
Extended IP access list EXTEND-1
    10 deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225 (4 matches)
    20 permit ip any any
```

Tâche 5 : contrôle de l'accès aux lignes vty par le biais d'une liste de contrôle d'accès standard

Il est généralement conseillé de restreindre l'accès aux lignes vty du routeur pour l'administration à distance. Une liste de contrôle d'accès peut être appliquée aux lignes vty afin de limiter l'accès à des hôtes ou des réseaux spécifiques. Cette tâche consiste à configurer une liste de contrôle d'accès standard autorisant les hôtes de deux réseaux à accéder aux lignes vty. Les autres hôtes se voient refuser l'accès.

Vérifiez que vous pouvez établir un accès Telnet vers R2 à partir de R1 et de R3.

Étape 1 : configuration de la liste de contrôle d'accès.

Configurez une liste de contrôle d'accès standard nommée sur R2 pour autoriser le trafic provenant des réseaux 10.2.2.0/30 et 192.168.30.0/24. Refusez le reste du trafic. Attribuez à la liste de contrôle d'accès le nom Task-5.

```
R2(config)#ip access-list standard TASK-5
R2(config-std-nacl)#permit 10.2.2.0 0.0.0.3
R2(config-std-nacl)#permit 192.168.30.0 0.0.0.255
```

Étape 2 : application de la liste de contrôle d'accès

Accédez au mode de configuration de ligne pour les lignes vty 0 à 4.

```
R2(config)#line vty 0 4
```

Utilisez la commande **access-class** pour appliquer la liste de contrôle d'accès aux lignes vty , dans le sens entrant. Vous remarquerez que cette commande diffère de la commande utilisée pour appliquer des listes de contrôle d'accès aux autres interfaces.

```
R2(config-line)#access-class TASK-5 in
R2(config-line)#end
R2#copy run start
```

Étape 3 : test de la liste de contrôle d'accès

Établissez une connexion Telnet avec R2 depuis R1. R1 ne comporte pas d'adresse IP présente dans la plage d'adresses répertoriée dans les instructions d'autorisation de la liste de contrôle d'accès TASK-5. Les tentatives de connexion sont censées échouer.

```
R1# telnet 10.1.1.2
Trying 10.1.1.2 …
% Connection refused by remote host
```

Établissez une connexion Telnet avec R2 depuis R3. Vous êtes alors invité à entrer le mot de passe des lignes vty.

```
R3# telnet 10.1.1.2
Trying 10.1.1.2 … Open
CUnauthorized access strictly prohibited, violators will be prosecuted
to the full extent of the law.

User Access Verification

Password:
```

Pourquoi les tentatives de connexion à partir d'autres réseaux échouent-elles alors que ces réseaux ne sont pas explicitement répertoriés dans la liste de contrôle d'accès ?

_____

_____

Tâche 6 : dépannage des listes de contrôle d'accès

Lorsqu'une liste de contrôle d'accès est mal configurée, appliquée à une interface inadéquate ou dans un sens incorrect, le trafic réseau peut être affecté de manière imprévisible.

Étape 1 : suppression d'une liste de contrôle d'accès STND-1 à partir de S0/0/1 de R3

Vous avez précédemment créé et appliqué une liste de contrôle d'accès standard nommée sur R3. Utilisez la commande **show running-config** pour afficher la liste de contrôle d'accès et sa position. Vous devriez remarquer qu'une liste de contrôle d'accès appelée **STND-1** a été configurée et appliquée en entrée de l'interface série 0/0/1. Souvenez-vous que cette liste a été conçue pour empêcher l'ensemble du trafic dont l'adresse source provient du réseau 192.168.11.0/24 d'accéder au réseau local de R3.

Pour supprimer la liste de contrôle d'accès, accédez au mode de configuration d'interface de l'interface série 0/0/1 de R3. Utilisez la commande **no ip access-group STND-1 in** pour supprimer la liste de contrôle d'accès de l'interface.

```
R3(config)#interface serial 0/0/1
R3(config-if)#no ip access-group STND-1 in
```

Utilisez la commande **show running-config** pour vérifier que la liste de contrôle d'accès a bien été supprimée de l'interface série 0/0/1.

Étape 2 : application de la liste de contrôle d'accès STND-1 en sortie de l'interface S0/0/1

Pour comprendre l'importance du sens de filtrage des listes de contrôle d'accès, appliquez à nouveau la liste **STND-1** à l'interface série 0/0/1. Cette fois, la liste de contrôle d'accès filtrera le trafic sortant et non le trafic entrant. Pensez à utiliser le mot clé **out** lors de l'application de la liste de contrôle d'accès.

```
R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group STND-1 out
```

Étape 3 : test de la liste de contrôle d'accès

Vérifiez la liste de contrôle d'accès en envoyant une requête ping vers le PC3 à partir du PC2. Vous pouvez également envoyer une requête ping étendue à partir de R1. Vous remarquerez que cette fois, l'envoi de requêtes ping aboutit et que les compteurs de la liste de contrôle d'accès ne sont pas modifiés. Pour le vérifier, entrez la commande **show ip access-list** sur R3.

Étape 4 : restauration de la configuration d'origine de la liste de contrôle d'accès

Supprimez la liste de contrôle d'accès appliquée en sortie et appliquez-la à nouveau en entrée.

```
R3(config)#interface serial 0/0/1
R3(config-if)#no ip access-group STND-1 out
R3(config-if)#ip access-group STND-1 in
```

Étape 5 : application de la tâche TASK-5 à l'interface série Serial 0/0/0 d'entrée de R2

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip access-group TASK-5 in
```

Étape 6 : test de la liste de contrôle d'accès

À partir de R1 ou des réseaux qui y sont connectés, essayez de communiquer avec un périphérique connecté à R2 ou R3. Vous remarquerez que toutes les communications sont bloquées, mais que cette fois les compteurs de liste de contrôle d'accès ne sont pas incrémentés. Cela est dû à la présence d'une instruction « deny all » (refuser tout) implicite à la fin de chaque liste de contrôle d'accès. Cette instruction « deny » bloque tous les trafics entrants de l'interface série Serial 0/0/0 provenant d'une autre source que R3. Cela a pour principale conséquence que les routes provenant de R1 seront supprimées de la table de routage.

Les messages similaires à ce qui suit doivent s'afficher sur les consoles de R1 et R2. Notez que la désactivation de la relation de voisinage du protocole OSPF peut prendre un certain temps.

```
*Sep  4 09:51:21.757: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.11.1
on Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
```

Lorsque vous recevez ce message, exécutez la commande **show ip route** sur R1 et R2 pour afficher les routes ayant été supprimées de la table de routage.

Supprimez la liste de contrôle d'accès TASK-5 de l'interface, puis enregistrez vos configurations.

```
R2(config)#interface serial 0/0/0
R2(config-if)#no ip access-group TASK-5 in
R2(config)#exit
R2#copy run start
```

Tâche 7 : documentation des configurations des routeurs

Configurations

Routeur 1

```
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 no shutdown
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 ip access-group EXTEND-1 out
 clockrate 64000
 no shutdown
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
!
ip access-list extended EXTEND-1
 deny   ip 192.168.10.0 0.0.0.255 host 209.165.200.225
 permit ip any any
!
banner motd ^CUnauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 password cisco
 login
!
```

Routeur 2

```
hostname R2
!
enable secret class
!
no ip domain lookup
!
```

```
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 clockrate 125000
 no shutdown
!
router ospf 1
 no auto-cost
 network 10.1.1.0 0.0.0.3 area 0
 network 10.2.2.0 0.0.0.3 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 209.165.200.224 0.0.0.31 area 0
!
ip access-list standard TASK-5
 permit 10.2.2.0 0.0.0.3
 permit 192.168.30.0 0.0.0.255
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 access-class TASK-5 in
 password cisco
 login
!
```

Routeur 3

```
hostname R3
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/1
 ip address 192.168.30.1 255.255.255.0
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 ip access-group STND-1 out
 no shutdown
```

```
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
!
ip access-list standard STND-1
 deny   192.168.11.0 0.0.0.255 log
 permit any
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 password cisco
 login
!
end
```

Tâche 8 : 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 hôtes PC connectés habituellement aux autres réseaux (réseau local de votre site ou Internet).