Exercice PT 5.5.1 : listes de contrôle d'accès de base

Diagramme de topologie

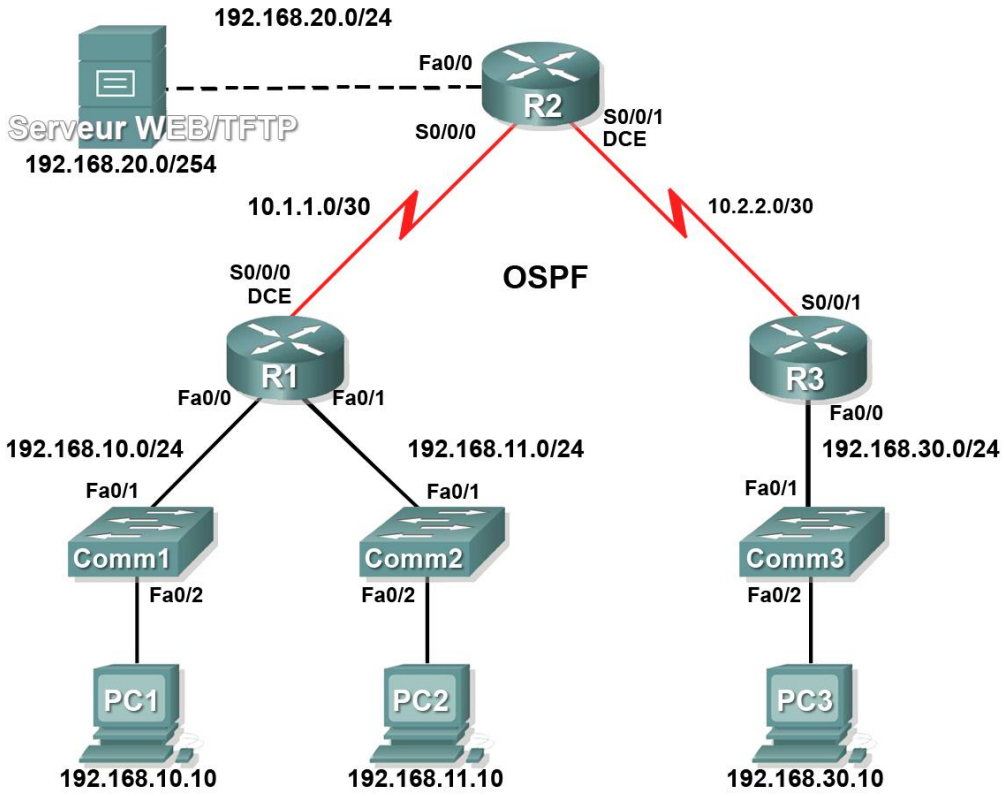

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	**Fa0/0**	192.168.10.1	255.255.255.0	N/D
	Fa0/1	192.168.11.1	255.255.255.0	N/D
	S0/0/0	10.1.1.1	255.255.255.252	N/D
R2	**Fa0/0**	192.168.20.1	255.255.255.0	N/D
	S0/0/0	10.1.1.2	255.255.255.252	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	**Fa0/0**	192.168.30.1	255.255.255.0	N/D
	S0/0/1	10.2.2.2	255.255.255.252	N/D

Table d'adressage à la page suivante

Table d'adressage (suite)

Comm1	**VLAN 1**	192.168.10.2	255.255.255.0	192.168.10.1
Comm2	**VLAN 1**	192.168.11.2	255.255.255.0	192.168.11.1
Comm3	**VLAN 1**	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

- Réaliser des configurations de base de routeurs et de commutateurs
- Configurer une liste de contrôle d'accès standard
- Configurer une liste de contrôle d'accès étendue
- Contrôler l'accès aux lignes vty avec une liste de contrôle d'accès standard
- Dépanner des listes de contrôle d'accès

Présentation

Au cours de cet exercice, vous allez concevoir, appliquer, tester et dépanner des configurations de listes d'accès.

Tâche 1 : configurations de base de routeurs et de commutateurs

Configurez les routeurs et commutateurs R1, R2, R3, Comm1, Comm2 et Comm3 en suivant les directives suivantes :

- Configurez les noms d'hôte relatifs au diagramme de topologie.
- Désactivez la recherche DNS.
- Configurez **class** comme mot de passe secret de mode d'exécution.
- Configurez une **bannière de message du jour**.
- Configurez le mot de passe **cisco** pour les connexions console.
- Configurez le mot de passe **cisco** pour les connexions vty.
- Configurez les adresses IP et les masques sur tous les périphériques. Fréquence d'horloge à **64000**.
- Activez le protocole OSPF en utilisant l'ID de processus 1 sur tous les routeurs pour tous les réseaux.
- Configurez une interface de bouclage sur R2.
- Configurez les adresses IP de l'interface VLAN 1 sur chaque commutateur.
- Configurez chaque commutateur avec la passerelle par défaut adéquate.
- Vérifiez l'ensemble de la connectivité IP à l'aide de la commande **ping**.

Tâche 2 : configuration d'une liste de contrôle d'accès standard

Les listes de contrôle d'accès standard peuvent filtrer le trafic en fonction de l'adresse IP source uniquement. Au cours de cette tâche, vous allez configurer une liste de contrôle d'accès standard qui bloque le trafic en provenance du réseau 192.168.11.0 /24. Cette liste de contrôle d'accès s'applique en entrée à l'interface série R3. N'oubliez pas que chaque liste de contrôle d'accès possède une instruction « deny all » implicite qui entraîne le blocage de tout trafic qui ne correspond pas à une instruction de la liste de contrôle d'accès. C'est pourquoi vous devez ajouter l'instruction **permit any** à la fin de la liste de contrôle d'accès.

Étape 1. Création de la liste de contrôle d'accès

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

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

En mode de configuration d'une liste de contrôle d'accès standard, ajoutez une instruction qui refuse tous les paquets ayant une adresse source 192.168.11.0 /24 et imprimez un message sur la console pour chaque paquet correspondant.

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

Autorisez tout autre trafic.

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

Étape 2. Application de la liste de contrôle d'accès

Appliquez la liste de contrôle d'accès std-1 comme filtre à des paquets entrant dans R3 via l'interface série 0/0/1.

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

Étape 3. Test de la liste de contrôle d'accès

Testez la liste de contrôle d'accès en envoyant une requête ping de PC2 à PC3. Étant donné que la liste de contrôle d'accès est conçue pour bloquer le trafic ayant des adresses source provenant du réseau 192.168.11.0 /24, PC2 (192.168.11.10) ne doit pas pouvoir envoyer de requête ping à PC3.

En mode d'exécution privilégié sur R3, envoyez la commande **show access-lists**. Le résultat généré est similaire à ce qui suit. Chaque ligne de la liste de contrôle d'accès possède un compteur associé indiquant le nombre de paquets ayant suivi la règle.

```
Standard IP access list std-1
    deny 192.168.11.0 0.0.0.255 (3 match(es))
    permit any
```

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

Lorsque vous recherchez une plus grande finesse, utilisez une liste de contrôle d'accès étendue. Les listes de contrôle d'accès étendues filtrent le trafic en ne s'appuyant pas uniquement sur l'adresse source. Les listes de contrôle d'accès étendues filtrent en fonction du protocole, des adresses IP source et de destination, ainsi que des numéros de port source et de destination.

Une stratégie supplémentaire s'appliquant à ce réseau stipule que les périphériques du réseau local 192.168.10.0/24 sont uniquement autorisés à atteindre des réseaux internes. Les ordinateurs de ce réseau local ne sont pas autorisés à accéder à Internet. L'accès de ces utilisateurs à l'adresse IP 209.165.200.225 doit donc être bloqué. Une liste de contrôle d'accès étendue est nécessaire car cette exigence doit mettre en œuvre la source et la destination.

Au cours de cette tâche, vous allez configurer une liste de contrôle d'accès étendue sur R1 qui empêche le trafic en provenance de tout périphérique du réseau 192.168.10.0 /24 d'accéder à l'hôte 209.165.200.255. Cette liste de contrôle d'accès s'applique en sortie de l'interface série 0/0/0 de R1.

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 appelée **extend-1**.

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

Remarquez que l'invite du routeur change pour indiquer que vous êtes désormais en mode de configuration de liste de contrôle d'accès étendue. À partir de cette invite, ajoutez les instructions nécessaires au blocage du trafic partant du réseau 192.168.10.0 /24 vers l'hôte. Utilisez le mot clé **host** lorsque vous définissez 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 le refus global implicite (« deny all ») bloque tout autre trafic sans l'instruction supplémentaire **permit**. Ajoutez l'instruction **permit** pour vous assurer qu'aucun autre trafic n'est bloqué.

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

Étape 2. Application de la liste de contrôle d'accès

Avec les listes de contrôle d'accès standard, la méthode recommandée consiste à placer la liste de contrôle d'accès le plus près possible de la destination. Les listes de contrôle d'accès étendues se trouvent généralement près de la source. Placez la liste de contrôle d'accès **extend-1** sur l'interface série afin de filtrer le trafic sortant.

```
R1(config)#interface serial 0/0/0
R1(config-if)#ip access-group extend-1 out
```

Étape 3. Test de la liste de contrôle d'accès

À partir de PC1 ou de tout autre périphérique du réseau 192.168.10.0 /24, envoyez une requête ping à l'interface de bouclage sur R2. Ces requêtes ping doivent échouer car tout le trafic en provenance du réseau 192.168.10.0 /24 est filtré lorsque la destination est 209.165.200.225. Si la destination est n'importe quelle autre adresse, les requêtes ping doivent aboutir. Assurez-vous que c'est bien le cas en envoyant une requête ping à R3 à partir du périphérique réseau 192.168.10.0/24.

Pour vérifier encore cela, lancez la commande **show ip access-list** sur R1 après l'envoi de la requête ping.

Des correspondances doivent exister pour les deux règles de la liste de contrôle d'accès. En effet, la requête ping de PC1 vers l'interface de bouclage de R2 a été refusée tandis que la requête ping vers R3 a été autorisée.

```
R1#show ip access-list
Extended IP access list extend-1
    deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225 (4 match(es))
    permit ip any any (4 match(es))
```

Tâche 4 : contrôle de l'accès aux lignes vty à l'aide d'une liste de contrôle d'accès standard

Il est recommandé de restreindre l'accès aux lignes vty du routeur pour une administration à distance. Appliquez une liste de contrôle d'accès aux lignes vty pour restreindre l'accès à des hôtes ou à des réseaux spécifiques. Au cours de cette tâche, vous allez configurer une liste de contrôle d'accès standard pour permettre à des hôtes de deux réseaux d'accéder aux lignes vty. Tous les autres hôtes sont rejetés.

Vérifiez que vous pouvez établir une connexion 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 qui autorise le trafic en provenance de 10.2.2.0/30 et de 192.168.30.0/24. Refusez tout autre trafic. Nommez **Task-4** la liste de contrôle d'accès.

```
R2(config)#ip access-list standard Task-4
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 des lignes vty 0 à 16.

```
R2(config)#line vty 0 16
```

Utilisez la commande **access-class** pour appliquer la liste de contrôle d'accès aux lignes vty dans le sens entrant. Remarquez qu'elle diffère de la commande utilisée pour appliquer des listes de contrôle d'accès à d'autres interfaces.

```
R2(config-line)#access-class Task-4 in
```

Étape 3. Test de la liste de contrôle d'accès

Établissez une connexion Telnet avec R2 à partir de R1. Remarquez que R1 ne possède pas d'adresse IP dans la plage d'adresses répertoriée dans les instructions « permit » de la liste de contrôle d'accès Task-4. Les tentatives de connexion doivent échouer.

À partir de R3, établissez une connexion Telnet avec R2 ou avec tout périphérique du réseau 192.168.30.0/24. Une invite vous demandant le mot de passe de la ligne vty s'affiche.

Pourquoi les tentatives de connexion à partir d'autres réseaux échouent-elles même si ceux-ci ne sont pas spécifiquement répertoriés dans la liste de contrôle d'accès ?

_____

_____

Tâche 5 : dépannage des listes de contrôle d'accès

Lorsqu'une liste de contrôle d'accès n'est pas correctement configurée ou est appliquée à une interface erronée ou dans la mauvaise direction, il est possible que le trafic réseau en soit affecté de manière indésirable.

Étape 1. Test de la liste de contrôle d'accès

Au cours d'une tâche précédente, vous avez créé et appliqué une liste de contrôle d'accès standard nommée sur R3. Pour afficher la liste de contrôle d'accès et son emplacement, utilisez la commande **show running-config**. Vous devez voir qu'une liste de contrôle d'accès nommée **std-1** a été configurée et appliquée en entrée sur Serial 0/0/1. Cette liste de contrôle d'accès a été créée pour empêcher tout trafic réseau avec une adresse source du réseau 192.168.11.0/24 d'accéder au réseau local sur R3.

Pour supprimer la liste de contrôle d'accès, passez en mode de configuration d'interface pour Serial 0/0/1 sur R3.

```
R3(config)#interface serial 0/0/1
```

Exécutez la commande **no ip access-group std-1 in** pour supprimer la liste de contrôle d'accès de l'interface.

```
R3(config-if)#no ip access-group std-1 in
```

Exécutez la commande **show running-config** pour vérifier que la liste de contrôle d'accès a été supprimée de Serial 0/0/1.

Étape 2. Application de la liste de contrôle d'accès std-1 à S0/0/1 en sortie

Pour tester l'importance du sens de filtrage de la liste de contrôle d'accès, appliquez à nouveau la liste de contrôle d'accès **std-1** à l'interface Serial 0/0/1. Désormais, la liste de contrôle d'accès doit filtrer le trafic sortant et non entrant. N'oubliez pas d'utiliser le mot clé **out** lorsque vous appliquez la liste de contrôle d'accès.

```
R3(config-if)#ip access-group std-1 out
```

Étape 3. Test de la liste de contrôle d'accès

Testez la liste de contrôle d'accès en envoyant une requête ping à PC3 à partir de PC2. Une autre solution consiste à envoyer une requête ping étendue à partir de R1. Remarquez que, cette fois-ci, les requêtes ping aboutissent et que les compteurs de la liste de contrôle d'accès n'augmentent pas. Pour vérifier cela, envoyez la commande **show ip access-list** sur R3.

Étape 4. Rétablissement de la configuration d'origine de la liste de contrôle d'accès

Supprimez la liste de contrôle d'accès du sens sortant et appliquez-la à nouveau dans le sens entrant.

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

Étape 5. Application de Task-4 en entrée de l'interface série 0/0/0 de R2

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip access-group Task-4 in
```

Étape 6. Test de la liste de contrôle d'accès

Essayez de communiquer avec un périphérique connecté à R2 ou R3 à partir de R1 ou des réseaux qui y sont reliés. Remarquez que toutes les communications sont bloquées. Cependant, les compteurs de la liste de contrôle d'accès n'augmentent pas. Cela est dû au refus global implicite (« deny all ») placé à la fin de chaque liste de contrôle d'accès.

Après expiration des compteurs d'intervalles d'arrêt OSPF, les consoles de R1 et R2 affichent des messages similaires à celui ci :

```
*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
```

Supprimez la liste de contrôle d'accès Task-4 de l'interface.