Exercice PT 5.2.8 : configuration de listes de contrôle d'accès standard

Diagramme de topologie

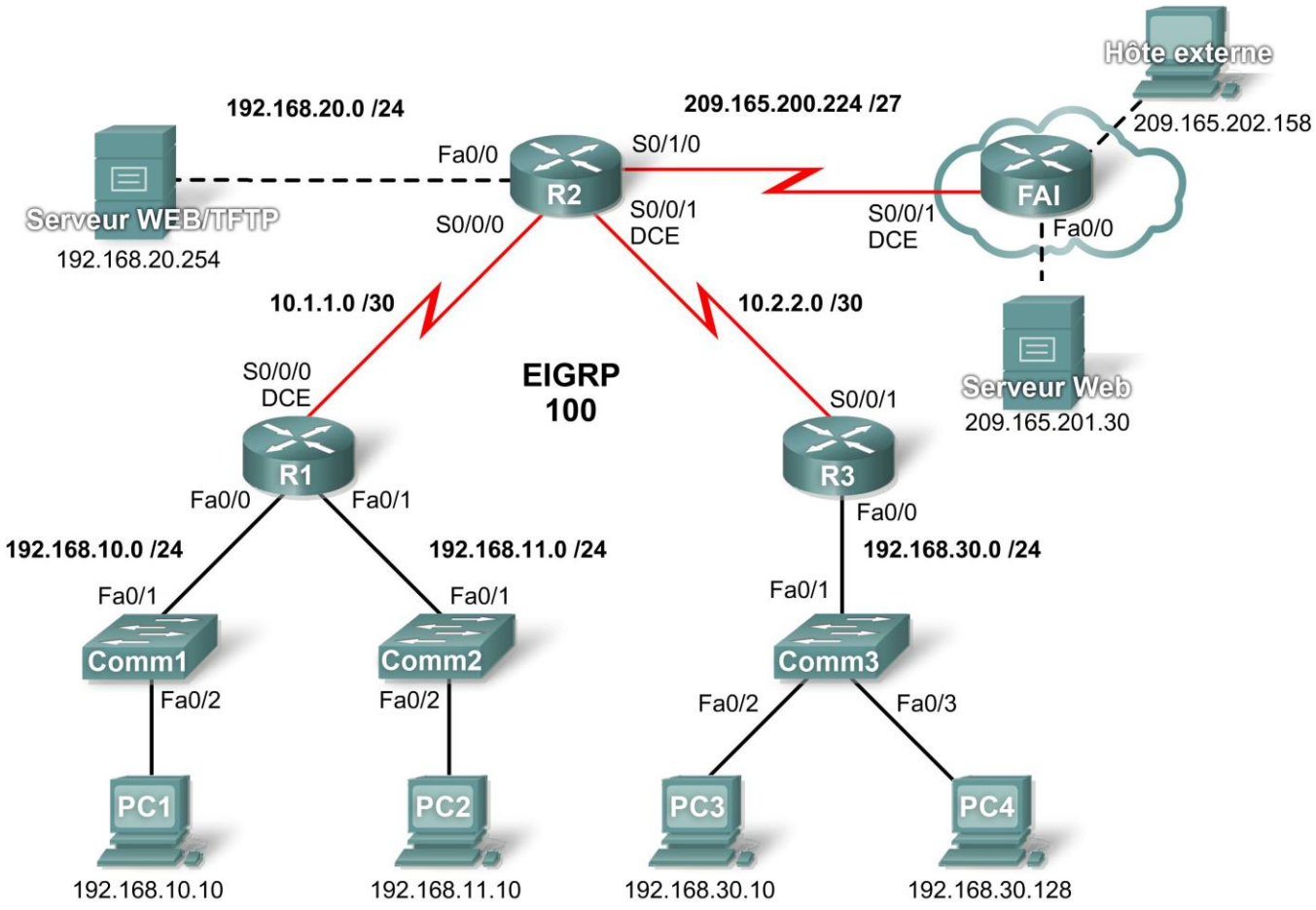

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
R1	**S0/0/0**	10.1.1.1	255.255.255.252
	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
R2	**S0/0/0**	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
	Fa0/0	192.168.20.1	255.255.255.0
R3	**S0/0/1**	10.2.2.2	255.255.255.252
	Fa0/0	192.168.30.1	255.255.255.0
FAI	**S0/0/1**	209.165.200.226	255.255.255.224
	Fa0/0	209.165.201.1	255.255.255.224
	Fa0/1	209.165.202.129	255.255.255.224
PC1	**Carte réseau**	192.168.10.10	255.255.255.0
PC2	**Carte réseau**	192.168.11.10	255.255.255.0
PC3	**Carte réseau**	192.168.30.10	255.255.255.0
PC4	**Carte réseau**	192.168.30.128	255.255.255.0
Serveur TFTP/Web	**Carte réseau**	192.168.20.254	255.255.255.0
Serveur Web	**Carte réseau**	209.165.201.30	255.255.255.224
Hôte externe	**Carte réseau**	209.165.202.158	255.255.255.224

Objectifs pédagogiques

- Étudier la configuration actuelle du réseau
- Évaluer une stratégie de réseau et planifier la mise en œuvre de listes de contrôle d'accès
- Configurer des listes de contrôle d'accès standard numérotées
- Configurer des listes de contrôle d'accès standard nommées

Présentation

Les listes de contrôle d'accès standard sont des scripts de configuration du routeur qui définissent si celui-ci autorise ou refuse des paquets en fonction de l'adresse source. Cet exercice porte principalement sur la définition de critères de filtrage, la configuration de listes de contrôle d'accès standard, l'application de ces listes aux interfaces des routeurs, ainsi que sur la vérification et le test de leur mise en œuvre. Les routeurs sont déjà configurés, notamment les adresses IP et le routage EIGRP. Le mot de passe d'exécution utilisateur est **cisco** et le mot de passe d'exécution privilégié est **class**.

Tâche 1 : étude de la configuration actuelle du réseau

Étape 1. Affichage de la configuration en cours sur les routeurs

Affichez les configurations en cours sur les trois routeurs à l'aide de la commande **show running-config** en mode d'exécution privilégié. Remarquez que les interfaces et le routage sont entièrement configurés. Comparez les configurations d'adresses IP à la table d'adressage ci-dessus. Aucune liste de contrôle d'accès ne doit être configurée sur les routeurs à ce stade.

Aucune configuration du routeur FAI n'est nécessaire au cours de cet exercice. Considérez que vous n'êtes pas responsable du routeur FAI et que celui-ci est configuré et entretenu par l'administrateur FAI.

Étape 2. Vérification que tous les périphériques ont accès à tous les autres emplacements

Avant d'appliquer des listes de contrôle d'accès à un réseau, il est important de vérifier que vous disposez d'une connectivité complète. Si vous ne testez pas la connectivité de votre réseau avant d'appliquer une liste de contrôle d'accès, le dépannage sera plus difficile.

Pour tester la connectivité, vous pouvez afficher la table de routage de chaque périphérique et vérifier que tous les réseaux y sont présents. Sur R1, R2 et R3, lancez la commande **show ip route**. Vous devez voir que chaque périphérique dispose de routes connectées vers les réseaux reliés et de routes dynamiques vers tous les autres réseaux distants. Tous les périphériques ont accès à tous les autres emplacements.

Bien que la table de routage soit utile pour évaluer l'état du réseau, vous pouvez cependant tester la connectivité à l'aide de la commande **ping**. Effectuez les tests suivants :

- À partir de PC1, envoyez une requête ping à PC2.
- À partir de PC2, envoyez une requête ping à Hôte externe.
- À partir de PC4, envoyez une requête ping au serveur Web/TFTP.

Tous ces tests de connectivité doivent réussir.

Tâche 2 : évaluation d'une stratégie de réseau et planification de la mise en œuvre de listes de contrôle d'accès

Étape 1. Évaluation de la stratégie pour les réseaux locaux de R1

- Le réseau 192.168.10.0/24 a accès à tous les emplacements, à l'exception du réseau 192.168.11.0/24.
- Le réseau 192.168.11.0/24 a accès à toutes les destinations, à l'exception des réseaux connectés à FAI.

Étape 2. Planification de la mise en œuvre des listes de contrôle d'accès pour les réseaux locaux de R1

- Deux listes de contrôle d'accès permettent de mettre en œuvre intégralement la stratégie de sécurité pour les réseaux locaux de R1.
- La première liste de contrôle d'accès sur R1 refuse le trafic du réseau 192.168.10.0/24 vers le réseau 192.168.11.0/24 mais autorise tout autre trafic.
- Cette première liste, appliquée en sortie sur l'interface Fa0/1, surveille tout le trafic envoyé vers le réseau 192.168.11.0.
- La seconde liste de contrôle d'accès sur R2 refuse au réseau 192.168.11.0/24 l'accès à FAI mais autorise tout autre trafic.
- Le trafic sortant de l'interface S0/1/0 est contrôlé.
- Classez les instructions des listes de contrôle d'accès par ordre décroissant de spécificité. Le refus de l'accès d'un trafic réseau à un autre réseau est prioritaire sur l'autorisation de tout autre trafic.

Étape 3. Évaluation de la stratégie pour le réseau local de R3

- Le réseau 192.168.30.0/10 a accès à toutes les destinations.
- L'hôte 192.168.30.128 n'est pas autorisé à accéder hors du réseau local.

Étape 4. Planification de la mise en œuvre des listes de contrôle d'accès pour le réseau local de R3

- Une liste de contrôle d'accès permet de mettre en œuvre intégralement la stratégie de sécurité pour le réseau local de R3.
- La liste de contrôle d'accès est placée sur R3 et refuse à l'hôte 192.168.30.128 l'accès hors du réseau local mais autorise le trafic en provenance de tous les autres hôtes du réseau local.
- Si elle est appliquée en entrée sur l'interface Fa0/0, cette liste de contrôle d'accès surveille tout trafic essayant de quitter le réseau 192.168.30.0/10.
- Classez les instructions des listes de contrôle d'accès par ordre décroissant de spécificité. Le refus de l'accès de l'hôte 192.168.30.128 est prioritaire sur l'autorisation de tout autre trafic.

Tâche 3 : configuration de listes de contrôle d'accès standard numérotées

Étape 1. Définition du masque générique

Le masque générique d'une instruction de liste de contrôle d'accès détermine la proportion d'une adresse de destination ou d'une adresse source IP qui doit être vérifiée. Un bit à 0 indique que cette valeur doit correspondre dans l'adresse, tandis qu'un bit à 1 ignore cette valeur dans l'adresse. N'oubliez pas que les listes de contrôle d'accès standard peuvent uniquement contrôler les adresses source.

- Étant donné que la liste de contrôle d'accès sur R1 refuse tout trafic du réseau 192.168.10.0/24, toute adresse IP source commençant par 192.168.10 est refusée. Le dernier octet de l'adresse IP pouvant être ignoré, le masque générique qui convient est 0.0.0.255. Chaque octet de ce masque peut être considéré comme « contrôler, contrôler, contrôler, ignorer ».
- La liste de contrôle d'accès sur R2 refuse également le trafic du réseau 192.168.11.0/24. Vous pouvez appliquer le même masque générique, 0.0.0.255.

Étape 2. Définition des instructions

- Les listes de contrôle d'accès sont configurées en mode de configuration globale.
- Pour les listes de contrôle d'accès standard, utilisez un nombre entre 1 et 99. Le nombre **10** est utilisé pour cette liste sur R1 afin de rappeler que celle-ci surveille le réseau 192.168.**10**.0.
- Sur R2, la liste d'accès **11 refuse** tout trafic en provenance du réseau 192.168.**11**.0 vers tout réseau FAI. Par conséquent, l'option **deny** est configurée avec le réseau **192.168.11.0** et le masque générique **0.0.0.255**.
- Tout autre trafic doit être autorisé à l'aide de l'option **permit** en raison du refus implicite (« deny any ») à la fin des listes de contrôle d'accès. L'option **any** indique tout hôte source.

Configurez ce qui suit sur R1 :

```
R1(config)#access-list 10 deny 192.168.10.0 0.0.0.255
R1(config)#access-list 10 permit any
```

Remarque : Packet Tracer évalue une configuration de liste de contrôle d'accès seulement lorsque toutes les instructions sont saisies dans l'ordre correct.

Créez maintenant une liste de contrôle d'accès sur R2 pour refuser le réseau 192.168.11.0 et autoriser tous les autres réseaux. Utilisez le numéro **11** pour cette liste de contrôle d'accès. Configurez ce qui suit sur R2 :

```
R2(config)#access-list 11 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 11 permit any
```

Étape 3. Application des instructions aux interfaces

Sur R1, passez en mode de configuration pour l'interface Fa0/1.

Lancez la commande **ip access-group 10 out** pour appliquer la liste de contrôle d'accès standard en sortie de l'interface.

```
R1(config)#interface fa0/1
R1(config-if)#ip access-group 10 out
```

Sur R2, passez en mode de configuration pour l'interface S0/1/0.

Lancez la commande **ip access-group 11 out** pour appliquer la liste de contrôle d'accès standard en sortie de l'interface.

```
R2(config)#interface s0/1/0
R2(config-if)#ip access-group 11 out
```

Étape 4. Vérification et test des listes de contrôle d'accès

Une fois les listes de contrôle d'accès configurées et appliquées, PC1 (192.168.10.10) ne doit pas être en mesure d'envoyer de requête ping à PC2 (192.168.11.10) car la liste de contrôle d'accès est appliquée en sortie de Fa0/1 sur R1.

PC2 (192.168.11.10) ne doit pas être en mesure d'envoyer de requête ping au serveur Web (209.165.201.30) ni à Hôte externe (209.165.202.158) mais doit pouvoir le faire vers toutes les autres destinations, car la liste de contrôle d'accès est appliquée en sortie de l'interface S0/1/0 sur R2. Cependant, PC2 ne peut pas envoyer de requête ping à PC1 car la liste de contrôle d'accès 10 sur R1 empêche la réponse d'écho de PC1 à PC2.

Étape 5. Vérification des résultats

Votre taux de réalisation doit être de 67 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 4 : configuration d'une liste de contrôle d'accès standard nommée

Étape 1. Définition du masque générique

- La stratégie d'accès pour R3 indique que l'hôte à l'adresse 192.168.30.128 ne doit pas pouvoir accéder hors du réseau local. Tous les autres hôtes du réseau 192.168.30.0 doivent pouvoir accéder à tous les autres emplacements.
- Pour vérifier un seul hôte, il est nécessaire de vérifier l'intégralité de l'adresse IP. Le mot de passe **host** permet cela.
- Tous les paquets ne correspondant pas à l'instruction relative à l'hôte sont autorisés.

Étape 2. Définition des instructions

- Sur R3, passez en mode de configuration globale.
- Créez une liste de contrôle d'accès nommée NO_ACCESS à l'aide de la commande **ip access-list standard NO_ACCESS**. Vous passez en mode de configuration de liste de contrôle d'accès. Toutes les instructions permit et deny sont configurées à partir de ce mode de configuration.
- Refusez le trafic en provenance de l'hôte 192.168.30.128 à l'aide de l'option **host**.
- Autorisez tout autre trafic à l'aide de **permit any**.

Configurez la liste de contrôle d'accès nommée suivante sur R3 :

```
R3(config)#ip access-list standard NO_ACCESS
R3(config-std-nacl)#deny host 192.168.30.128
R3(config-std-nacl)#permit any
```

Étape 3. Application des instructions à l'interface correcte

Sur R3, passez en mode de configuration pour l'interface Fa0/0.

Lancez la commande **ip access-group NO_ACCESS in** pour appliquer la liste de contrôle d'accès nommée en entrée de l'interface. Avec cette commande, tout le trafic entrant sur l'interface Fa0/0 en provenance du réseau local 192.168.30.0/24 est contrôlé par rapport à la liste de contrôle d'accès.

```
R3(config)#interface fa0/0
R3(config-if)#ip access-group NO_ACCESS in
```

Étape 4. Vérification et test des listes de contrôle d'accès

Cliquez sur **Check Results**, puis sur **Connectivity Tests**. Les tests suivants doivent échouer :

- PC1 vers PC2
- PC2 vers Hôte externe
- PC2 vers Serveur Web
- Toutes les requêtes ping en provenance de/vers PC4, sauf entre PC3 et PC4.

Étape 5. Vérification des résultats

Votre taux de réalisation doit être de 100 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.