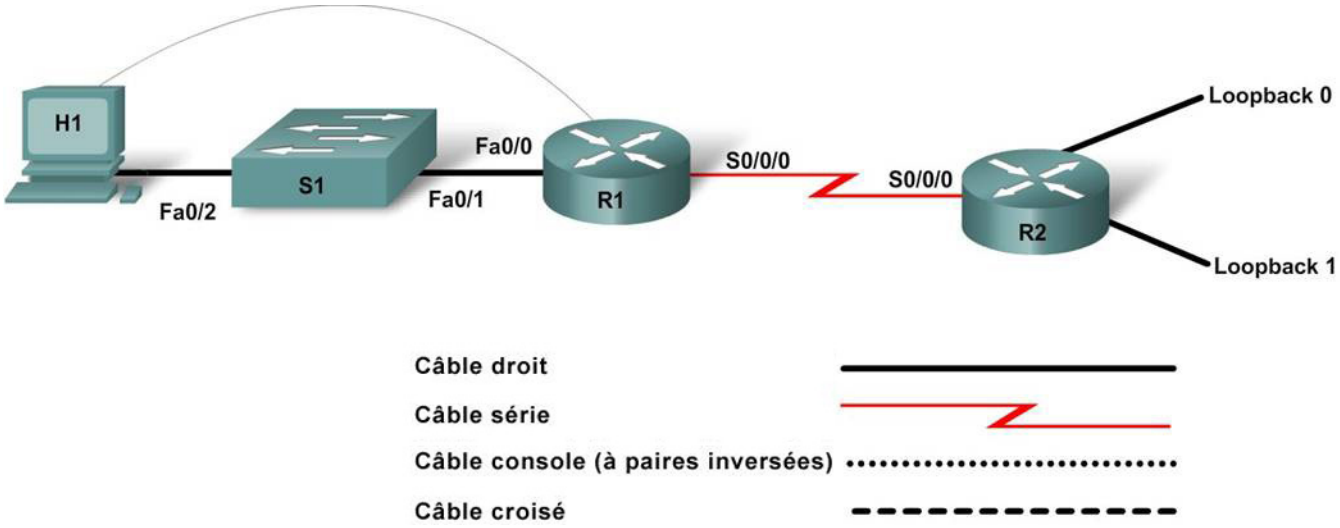
Travaux pratiques 8.3.3 : Configuration et vérification de listes de contrôle d'accès standard



Périphérique	Nom d'hôte	Adresse IP FastEthernet 0/0	Adresse IP Serial 0/0/0	Type d'interface Serial 0/0/0	Adresses d'interface de bouclage	Mot de passe secret actif	Mot de passe actif, vty et de console
Routeur 1	R1	192.168.200.1/24	192.168.100.1/30	DCE	n/d	class	cisco
Routeur 2	R2	n/d	192.168.100.2/30	ETTD	Lo0 192.168.1.1/32 Lo1 192.168.2.1/32	class	cisco
Commutateur 1	S1	n/d	n/d	n/d	n/d	class	cisco

Objectifs

- Configurer des listes de contrôle d'accès standard pour limiter le trafic
- Vérifier le fonctionnement des listes de contrôle d'accès

Contexte / Préparation

Au cours de ces travaux pratiques, vous allez travailler avec des listes de contrôle d'accès standard pour contrôler le trafic réseau sur la base d'adresses IP hôtes. Tout routeur doté d'une interface telle que celle indiquée dans le schéma ci-dessus peut être utilisé. Exemple : les routeurs de la gamme 800, 1600, 1700, 1800, 2500, 2600, 2800 ou toute combinaison de ces routeurs sont utilisables.

Les informations présentées dans ces travaux pratiques s'appliquent au routeur de la gamme 1841. Il est possible d'utiliser d'autres routeurs ; cependant la syntaxe des commandes peut varier. Les interfaces peuvent être différentes en fonction du modèle de routeur. Par exemple, sur certains routeurs, Serial 0 peut être Serial 0/0 ou Serial 0/0/0 et Ethernet 0 peut être FastEthernet 0/0. Le commutateur Cisco Catalyst 2960 est fourni préconfiguré : il ne nécessite que l'affectation d'informations de sécurité de base avant la connexion à un réseau.

Ressources requises :

- Un commutateur Cisco 2960 ou autre commutateur comparable
- Deux routeurs Cisco de la gamme 1841 ou équivalents, chacun avec une interface série et Ethernet
- Un PC Windows équipé d'un programme d'émulation de terminal et configuré comme hôte
- Au moins un câble console RJ-45/DB-9 pour configurer les routeurs et le commutateur
- Deux câbles droits Ethernet
- Un câble croisé série ETTD/DCE en 2 parties

REMARQUE : assurez-vous que les routeurs et commutateurs ont été réinitialisés et ne possèdent aucune configuration de démarrage. Les instructions d'effacement et de rechargement de la mémoire du commutateur et du routeur figurent dans la section Tools du site Academy Connection.

REMARQUE : Routeurs SDM − Si la configuration initiale (startup-config) est effacée dans un routeur SDM, le gestionnaire SDM ne s'affiche plus par défaut lorsque le routeur est redémarré. Il est alors nécessaire de définir une configuration de base de routeur à l'aide des commandes IOS. La procédure indiquée dans ces travaux pratiques utilise des commandes IOS et ne nécessite pas l'utilisation de SDM. Si vous voulez utiliser SDM, reportez-vous aux instructions du Manuel de travaux pratiques que vous pouvez télécharger depuis la section Tools du site Academy Connection. Consultez votre formateur si besoin.

Étape 1 : connexion du matériel

a. Connectez l'interface Serial 0/0/0 du routeur R1 à l'interface Serial 0/0/0 du routeur R2 à l'aide d'un câble série.

b. Connectez l'interface Fa0/0 du routeur R1 à l'interface Fa0/1 du commutateur S1 à l'aide d'un câble droit.

c. Connectez un câble console au PC pour procéder aux configurations sur les routeurs et le commutateur.

d. Connectez H1 au port Fa0/2 du commutateur S1 à l'aide d'un câble droit.

Étape 2 : configuration de base du routeur R1

a. Connectez un PC au port console du routeur pour procéder aux configurations à l'aide d'un programme d'émulation de terminal.

b. Sur le routeur R1, configurez le nom d'hôte, les interfaces, les mots de passe et la bannière du message du jour, et désactivez les recherches DNS conformément à la table d'adressage et au schéma de topologie. Enregistrez la configuration.

Étape 3 : configuration de base du routeur R2

Procédez à la configuration de base du routeur R2 et enregistrez-la.

Étape 4 : configuration de base du commutateur S1

Configurez S1 avec un nom d'hôte et des mots de passe selon la table d'adressage et le schéma de topologie.

Étape 5 : configuration de l'hôte avec une adresse IP, un masque de sous-réseau et une passerelle par défaut

a. Configurez l'hôte avec l'adresse IP, le masque de sous-réseau et la passerelle par défaut corrects. L'adresse 192.168.200.10/24 et la passerelle par défaut 192.168.200.1 doivent être attribuées à l'hôte.

b. La station de travail doit pouvoir envoyer une requête ping au routeur auquel elle est connectée. Si cette requête échoue, procédez au dépannage requis. Vérifiez soigneusement qu'une adresse IP spécifique et une passerelle par défaut ont été attribuées à la station de travail.

Étape 6 : configuration du routage RIP et vérification de la connectivité de bout en bout dans le réseau

a. Sur R1, activez le protocole de routage RIP et configurez-le de façon à annoncer les deux réseaux connectés.

b. Sur R2, activez le protocole de routage RIP et configurez-le de façon à annoncer les trois réseaux connectés.

c. Envoyez une requête ping de l'hôte H1 aux deux interfaces de bouclage sur R2.

Les requêtes ping de l'hôte H1 ont-elles abouti ? _____

Si la réponse est non, vérifiez la configuration de l'hôte et du routeur pour trouver l'erreur. Envoyez de nouvelles requêtes ping jusqu'à ce qu'elles aboutissent.

Étape 7 : configuration et test d'une liste de contrôle d'accès standard

Dans la topologie de ces travaux pratiques, les interfaces de bouclage sur R2 simulent deux réseaux de classe C connectés au routeur. Des listes de contrôle d'accès vont être utilisées pour contrôler l'accès à ces sous-réseaux. L'interface de bouclage 0 représente un réseau de stations de travail de gestion, tandis que l'interface 1 représente un réseau d'ingénierie à accès limité.

Dans ce réseau, il est nécessaire de disposer d'au moins une station de travail de gestion sur le sous-réseau 192.168.200.0/24 en même temps que les stations des utilisateurs. L'adresse IP statique 192.168.200.10 est allouée à la station de travail de gestion. Les autres adresses IP du réseau sont occupées par les stations de travail des utilisateurs.

La liste de contrôle d'accès doit permettre d'accéder aux réseaux connectés à R2 à partir de la station de gestion, mais pas à partir des autres hôtes du réseau 192.168.200.0.

Une liste de contrôle d'accès standard est utilisée et sera placée sur R2, qui est le plus proche de la destination.

a. Créez une liste de contrôle d'accès standard sur R2 pour permettre l'accès aux réseaux connectés. Cette liste autorisera un accès à l'hôte 192.168.200.10 et refusera tous les autres.

```
R2(config)#access-list 1 permit 192.168.200.10
R2(config)#access-list 1 deny any
```

REMARQUE : l'instruction **deny** implicite à la fin d'une liste de contrôle d'accès remplit la même fonction. Cependant, il est recommandé d'ajouter la ligne à la fin de la liste afin d'en conserver une trace. Lorsque cette instruction est ajoutée explicitement, le nombre de paquets correspondant à l'instruction est compté, ce qui permet à l'administrateur de savoir combien de paquets ont été refusés.

b. Après avoir créé la liste de contrôle d'accès, vous devez l'appliquer à une interface sur le routeur. Utilisez l'interface Serial 0/0/0 pour permettre un contrôle des réseaux 192.168.1.0 et 192.168.2.0. Le trafic potentiel circulerait en direction de l'interface ; par conséquent, appliquez la liste de contrôle d'accès dans le sens des entrées.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip access-group 1 in
```

c. Une fois la liste de contrôle d'accès créée et appliquée, utilisez la commande **show access-lists** sur R2 pour afficher cette liste.

L'une des instructions de la liste de contrôle d'accès renvoie-t-elle des correspondances ?

_____

```
R2#show access-lists
Standard IP access list 1
    10 permit 192.168.200.10
    20 deny   any
```

Le résultat de la commande **show access-lists** indique-t-il la liste de contrôle d'accès qui a été créée ?

_____

Le résultat de la commande **show access-lists** indique-t-il comment la liste de contrôle d'accès est appliquée ?

_____

d. Utilisez la commande **show ip interface s0/0/0** pour afficher l'application de la liste de contrôle d'accès.

Que vous indique le résultat de la commande **show ip interface** sur la liste de contrôle d'accès ?

_____

Étape 8 : test de la liste de contrôle d'accès

a. À partir de l'hôte H1, envoyez une requête ping à l'adresse de bouclage 192.168.1.1.

Le ping a-t-il abouti ? _____

b. À partir de l'hôte H1, envoyez une requête ping à l'adresse de bouclage 192.168.2.1.

Le ping a-t-il abouti ? _____

c. Exécutez de nouveau la commande **show access-list**.

Combien y a-t-il de correspondances pour la première instruction de la liste de contrôle d'accès (permit) ? _____

```
R2#show access-lists
Standard IP access list 1
    permit 192.168.200.10 (16 matches)
    deny   any
```

Combien y a-t-il de correspondances pour la deuxième instruction de la liste de contrôle d'accès (deny) ? _____

d. Affichez la table de routage de R2 à l'aide de la commande **show ip route**.

Quelle route est absente de la table de routage ? _____

Cette route ne figure pas dans la table de routage parce que la liste de contrôle d'accès autorise uniquement les paquets provenant de l'adresse 192.168.200.10. Les paquets de mise à jour RIP sur R1 proviennent de l'interface Serial 0/0/0 192.168.100.1 du routeur et sont refusés par la liste de contrôle d'accès. Étant donné que les mises à jour RIP R1 annonçant le réseau 192.168.200.0 sont bloquées par la liste de contrôle d'accès, R2 n'a pas connaissance du réseau 192.168.200.0. Les requêtes ping émises précédemment n'ont pas été bloquées par la liste. Elles ont échoué parce que R2 ne pouvait pas renvoyer la réponse d'écho, ne sachant comment atteindre le réseau 192.168.200.0.

Cet exemple montre pourquoi les listes de contrôle d'accès doivent être programmées avec soin et leur fonctionnement testé de façon approfondie.

e. Recréez la liste de contrôle d'accès sur R2 pour permettre la réception de mises à jour de routage depuis R1.

```
R2(config)#no access-list 1
R2(config)#access-list 1 permit 192.168.200.10
R2(config)#access-list 1 permit 192.168.100.1
R2(config)#access-list 1 deny any
```

f. Envoyez une requête ping à 192.168.1.1 et 192.168.2.1 à partir de l'hôte H1.

Les requêtes ping aboutissent-elles maintenant ? _____

g. Changez l'adresse IP de l'hôte H1 en 192.168.200.11.

h. Envoyez de nouveau une requête ping à 192.168.1.1 et 192.168.2.1 à partir de l'hôte H1.

Les requêtes ping aboutissent-elles ? _____

Affichez de nouveau la liste de contrôle d'accès à l'aide de la commande **show access-lists**.

L'instruction 192.168.100.1 de la liste de contrôle d'accès renvoie-t-elle des correspondances ?

_____

REMARQUE : vous pouvez effacer les compteurs de la liste de contrôle d'accès en exécutant la commande `clear` **ip access-list counters** à partir de l'invite du mode d'exécution privilégié.

Étape 9 : remarques générales

a. Pourquoi est-il nécessaire de procéder à une planification et à des tests minutieux des listes de contrôle d'accès ?

_____

b. Quelle est la principale limite des listes de contrôle d'accès standard ?

_____