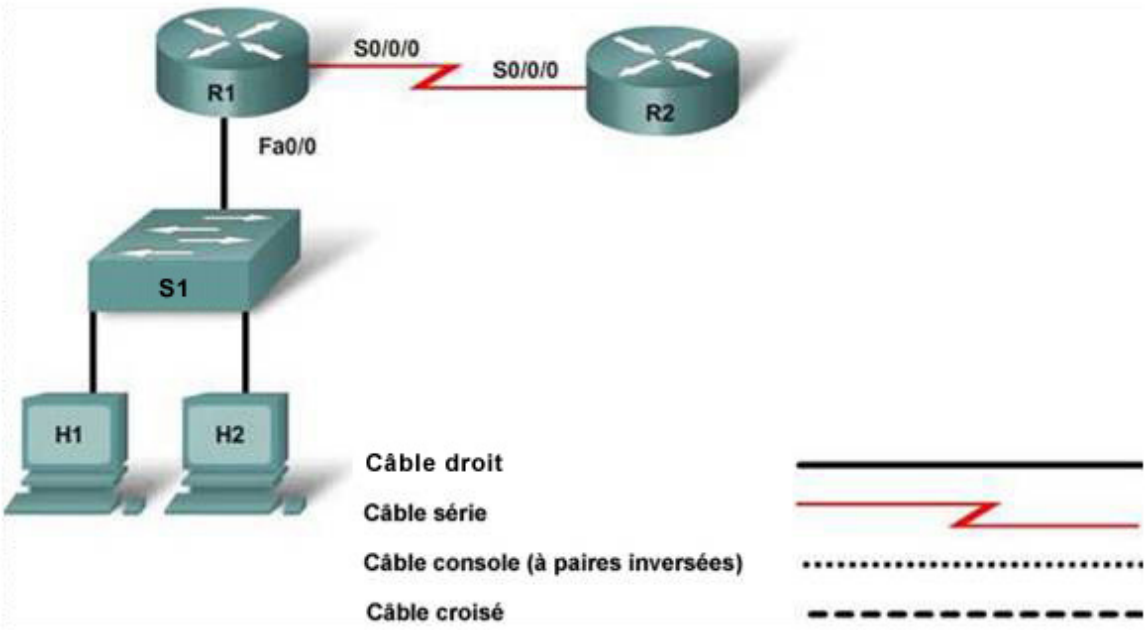
Travaux pratiques 8.3.5 : Configuration et vérification de listes de contrôle d'accès nommées étendues



Périphérique	Nom d'hôte	Adresse IP FastEthernet 0/0	Adresse IP Serial 0/0/0	Type d'interface Serial 0/0/0	Passerelle par défaut	Mot de passe secret actif	Mot de passe actif, vty et de console
Routeur 1	R1	192.168.15.1/24	209.165.201.1/30	ETTD		class	cisco
Routeur 2	R2		209.165.201.2/30	DCE		class	cisco
Commutateur 1	S1					class	cisco
Hôte 1	H1	192.168.15.2/24			192.168.15.1		
Hôte 2	H2	192.168.15.3/24			192.168.15.1		

Objectifs

- Créer des listes de contrôle d'accès nommées standard et étendues
- Tester les listes de contrôle d'accès pour déterminer si elles donnent les résultats souhaités
- Modifier une liste de contrôle d'accès nommée

Contexte / Préparation

Au cours de ces travaux pratiques, vous allez travailler avec des listes de contrôle d'accès nommées standard et étendues pour contrôler le trafic réseau sur la base d'adresses IP hôtes. Tout routeur doté d'une interface indiquée dans le schéma de topologie 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 aux routeurs 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 1841 ou autres routeurs comparables, chacun doté d'une connexion série et d'une interface Ethernet
- Deux PC Windows équipés d'un programme d'émulation de terminal et configurés comme hôtes
- Au moins un câble console à connecteur RJ-45/DB-9 pour configurer les routeurs et le commutateur
- Trois 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, comme indiqué dans le schéma et la table d'adressage.

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

d. Connectez l'hôte H2 au port Fa0/3 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

a. Effectuez la configuration de base du routeur R2 conformément à la table d'adressage et à la table topologique. Enregistrez la configuration.

Étape 4 : configuration de base du commutateur S1

a. Configurez le commutateur S1 avec un nom d'hôte et des mots de passe de console, Telnet et du mode privilégié conformément à la table d'adressage et à la table topologique.

Étape 5 : configuration des hôtes avec l'adresse IP, le masque de sous-réseau et la passerelle par défaut

a. Configurez l'adresse IP, le masque de sous-réseau et la passerelle par défaut des hôtes, conformément à la table d'adressage et au schéma de topologie.

b. Chaque station de travail doit pouvoir envoyer une requête ping à R1 et aux autres stations. Si les requêtes ping échouent, 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 : vérification du fonctionnement du réseau

a. À partir des hôtes connectés, envoyez une requête ping à l'interface FastEthernet du routeur de passerelle par défaut.

   La requête ping à partir de l'hôte H1 a-t-elle abouti ? _____

   La requête ping à partir de l'hôte H2 a-t-elle abouti ? _____

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

b. À l'aide de la commande **`show ip interface brief`**, vérifiez l'état de chaque interface.

   Quel est l'état des interfaces sur chaque routeur ?

   R1 :

   FastEthernet 0/0 : _____

   Serial 0/0/0 : _____

   Serial 0/0/1 : _____

   R2 :

   FastEthernet 0/0 : _____

   Serial 0/0/0 : _____

   Serial 0/0/1 : _____

c. Envoyez une requête ping de l'interface Serial 0/0/0 du routeur R1 à l'interface Serial 0/0/0 du routeur R2.

   La commande a-t-elle été exécutée correctement ? _____

   Si la réponse est non, vérifiez les configurations des routeurs pour trouver l'erreur. Envoyez de nouvelles requêtes ping jusqu'à ce qu'elles aboutissent.

Étape 7 : configuration du routage statique et par défaut sur les routeurs

a. Configurez une route par défaut sur R1. Utilisez l'interface de tronçon suivant comme chemin sur R2.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.2
```

b. À partir de l'un des PC hôtes sur R1, envoyez une requête ping à R2.

Pourquoi la requête ping n'a-t-elle pas abouti ?

_____

c. Configurez une route statique sur R2 vers le réseau 192.168.15.0 de R1. Utilisez l'interface de tronçon suivant comme chemin sur R1.

```
R2(config)#ip route 192.168.15.0 255.255.255.0 209.165.201.1
```

d. À partir de l'un des PC hôtes sur R1, envoyez une requête ping à R2.

La requête ping a-t-elle abouti ? _____

Si la requête ping a échoué, dépannez les routes statique et par défaut.

Étape 8 : configuration et test d'une liste de contrôle d'accès standard nommée simple

a. Créez une liste de contrôle d'accès nommée qui permet à H2 d'atteindre d'autres hôtes sur le réseau local, mais pas d'accéder à des réseaux distants. À l'invite de configuration, utilisez la séquence de commandes suivante :

```
R1(config)#ip access-list standard H2_no_access
R1(config-std-nacl)#deny host 192.168.15.3
R1(config-std-nacl)#permit any
```

Pourquoi la troisième instruction est-elle nécessaire ? _____

b. Appliquez la liste de contrôle d'accès à l'interface.

```
R1(config)#interface fastethernet0/0
R1(config-if)#ip access-group H2_no_access in
```

Indiquez comment vous devez tester cette liste de contrôle d'accès : _____

_____

c. Effectuez les tests pour vérifier que cette liste de contrôle d'accès remplit ses objectifs. Si ce n'est pas le cas, procédez à un dépannage en affichant le résultat d'une commande **show running-config** pour vérifier que la liste de contrôle d'accès est présente et appliquée à l'interface qui convient.

Étape 9 : création et test d'une liste de contrôle d'accès étendue nommée

a. Créez une liste de contrôle d'accès nommée qui ne permet pas à H1 d'envoyer une requête ping à R2 mais l'autorise à atteindre le réseau local et R1.

```
R1(config)#ip access-list extended H1_limit_access
R1(config-ext-nacl)#deny ip host 198.168.15.2 host 209.165.201.2
R1(config-ext-nacl)#permit ip any any
```

b. Appliquez la liste de contrôle d'accès à l'interface.

```
R1(config)#interface s0/0/0
R1(config-if)#ip access-group H1_limit_access out
```

Indiquez comment vous allez tester cette liste de contrôle d'accès : _____

_____

c. Effectuez les tests pour vérifier que cette liste de contrôle d'accès remplit ses objectifs. Si ce n'est pas le cas, procédez à un dépannage en affichant le résultat d'une commande **show running-config** pour vérifier que la liste de contrôle d'accès est présente et appliquée à l'interface qui convient.

Étape 10 : modification d'une liste de contrôle d'accès standard nommée

a. Vous avez décidé de modifier la liste de contrôle d'accès standard nommée. Affichez les instructions de la liste en mode d'exécution privilégié.

```
R1#show access-lists
Standard IP access list H2_no_access
    10 deny host 192.168.15.3
    20 permit any
```

b. Ajoutez une ligne à cette liste de contrôle d'accès standard nommée pour empêcher H1 de joindre R1, tout en permettant à H1 et H2 de communiquer entre eux.

Tapez les commandes de configuration (une par ligne). Terminez par **CNTL/Z**.

```
R1(config)#ip access-list standard H2_no_access
R1(config-std-nacl)#15 deny host 192.168.15.2
```

c. Affichez la liste de contrôle d'accès modifiée pour vérifier que toutes les instructions sont présentes.

```
R1#show access-lists
Standard IP access list H2_no_access
    10 deny host 192.168.15.3
    15 deny host 192.168.15.2
    20 permit any
```

Si vous ajoutez un nouveau PC à la topologie, le connectez à S1 et lui donnez l'adresse IP 192.168.15.4/24, pourra-t-il accéder à R1 ? _____

Étape 11 : remarques générales

a. Pourquoi est-il recommandé d'effectuer des configurations de base et de vérifier la connectivité avant d'ajouter des listes de contrôle d'accès à des routeurs ?

_____

_____.

b. Quels avantages les listes de contrôle d'accès nommées offrent-elles ?

_____

_____