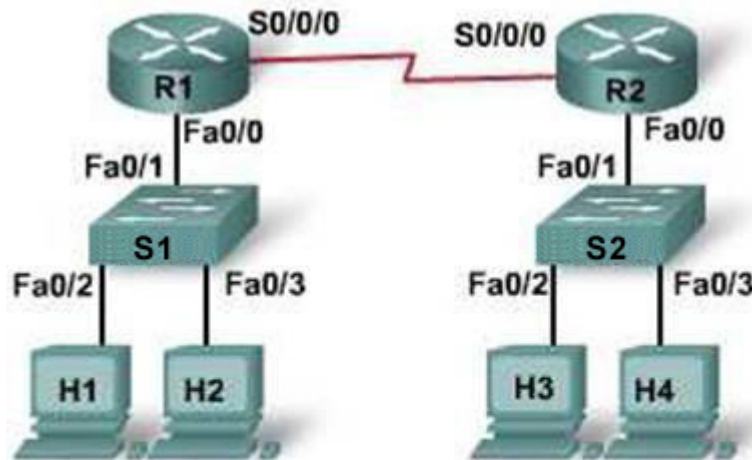


Travaux pratiques 8.3.6 : Configuration et vérification des restrictions VTY

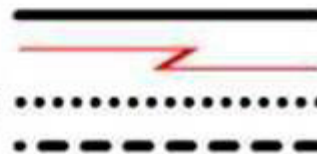


Câble droit

Câble série

Câble console (à paires inversées)

Câble croisé



Périphérique	Nom de l'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 enable/vty et console
Routeur 1	R1	192.168.15.1/24	192.168.16.1/24	ETTD		class	cisco
Routeur 2	R2	192.168.17.1/24	192.168.16.2/24	DCE		class	cisco
Commutateur 1	S1					class	cisco
Commutateur 2	S2					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		
Hôte 3	H3	192.168.17.2/24			192.168.17.1		
Hôte 4	H4	192.168.17.3/24			192.168.17.1		

Objectifs

- Utiliser les commandes access-class et line pour contrôler l'accès à un routeur via Telnet
- Tester les listes de contrôle d'accès pour déterminer si elles donnent les résultats souhaités

Contexte / Préparation

Au cours de ces travaux pratiques, vous allez utiliser des listes de contrôle d'accès vty pour restreindre l'accès à un routeur via Telnet. 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 au routeur 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 nécessaires :

- Deux commutateurs Cisco 2960 ou autres commutateurs comparables
- Deux routeurs Cisco 1841 ou comparables, chacun avec une connexion série et une interface Ethernet
- Quatre 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
- Six câbles droits Ethernet
- Un câble croisé série (ETTD/DCE) en 2 parties

REMARQUE : vérifiez que la mémoire des routeurs et des commutateurs a été effacée et qu'aucune configuration de démarrage n'est présente. 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 S0/0/0 du routeur R1 à l'interface S0/0/0 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 et l'hôte H2 au port Fa0/3 du commutateur S1 à l'aide de câbles droits.
- d. Connectez l'hôte H3 au port Fa0/2 et l'hôte H4 au port Fa0/3 du commutateur S2 à l'aide de câbles droits.

Étape 2 : configuration de base du routeur R1

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

Étape 4 : configuration de base des commutateurs S1 et S2

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

- Configurez l'adresse IP, le masque de sous-réseau et la passerelle par défaut des hôtes, conformément à la table et au schéma de topologie.
- Chaque station de travail doit pouvoir envoyer un paquet ping au routeur auquel elle est connectée. 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 : configuration du routage dynamique sur les routeurs

- Configurez le routage RIP sur R1. Annoncez les réseaux appropriés.
- Configurez le routage RIP sur R2. Annoncez les réseaux appropriés.

Étape 7 : vérification de la connectivité

- Si le réseau est convergent, citez quatre destinations auxquelles H1 doit pouvoir envoyer une requête ping :

- Testez la connectivité en envoyant une requête ping à toutes les destinations. Si des requêtes ping échouent, dépannez les configurations sur les routeurs et les PC hôtes.
- Examinez la table de routage de R1.

R1#**show ip route**

```
Codes : C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static
route
        o - ODR, P - periodic downloaded static route
```

Gateway of last resort is not set

```
C    192.168.15.0/24 is directly connected, FastEthernet0/0
R    192.168.17.0/24 [120/1] via 192.168.16.2, 00:00:09, Serial0/0/0
C    192.168.16.0/24 is directly connected, Serial0/0/0
```

Combien de routes doivent apparaître ? _____

- Vérifiez que toutes les routes figurent dans la table de routage. Si une route est absente, corrigez la configuration des routeurs.

- e. Établissez une connexion Telnet à partir des hôtes vers les deux routeurs. Tous les hôtes doivent être capables d'établir des connexions Telnet aux deux routeurs. Si Telnet échoue, dépannez les configurations des routeurs et des hôtes.

Étape 8 : configuration et test d'une liste de contrôle d'accès pour limiter l'accès Telnet

- a. Créez une liste de contrôle d'accès standard qui représente le réseau local connecté à R1.

```
R1 (config) #access-list 1 permit 192.168.15.0 0.0.0.255
```

- b. Maintenant que vous avez défini le trafic de réseau local, vous devez l'appliquer aux lignes vty. Il s'agit de permettre aux utilisateurs de ce réseau d'établir une connexion Telnet à ce routeur, tout en empêchant les utilisateurs d'autres réseaux d'accéder par Telnet sur ce routeur.

```
R1 (config) #line vty 0 4  
R1 (config-line) #access-class 1 in  
R1 (config-line) #end
```

Quels PC doivent et ne doivent pas être en mesure d'établir une connexion Telnet à R1 ?

-
- c. Testez la restriction.

Étape 9 : création de restrictions vty pour R2

- a. Créez une liste de contrôle d'accès standard qui ne permettra pas aux hôtes du réseau local R1 d'établir une connexion Telnet à R2, mais autorisera les hôtes du réseau R2 d'établir une connexion Telnet au routeur auquel ils sont connectés.

```
R2 (config) #access-list 2 permit 192.168.17.0 0.0.0.255  
R2 (config) #line vty 0 4  
R2 (config-line) #access-class 2 in  
R2 (config-line) #end
```

- b. 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 correctement.

Étape 10 : remarques générales

Pourquoi est-il recommandé de créer une liste de contrôle d'accès de restriction vty lors de la configuration d'un routeur ?
