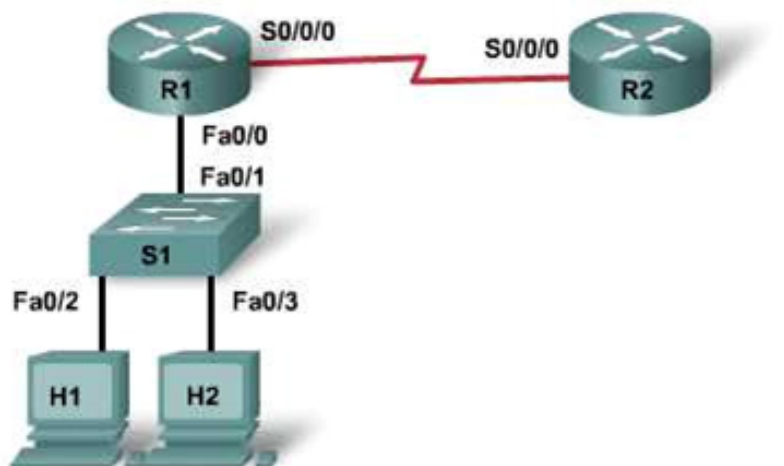


Travaux pratiques 8.4.3 : Configuration d'une liste de contrôle d'accès avec la fonction NAT

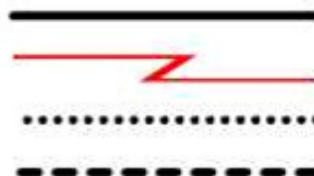


Câble droit

Câble série

Câble console (à paires inversées)

Câble croisé



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	192.168.1.1/24	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	192.168.1.2/24			192.168.1.1		
Hôte 2	H2	192.168.1.3/24			192.168.1.1		

Objectifs

- Configurer les fonctions NAT et PAT et vérifier leur fonctionnement
- Configurer et appliquer une liste de contrôle d'accès à une interface où la fonction NAT est en vigueur
- Observer les effets du placement d'une liste de contrôle d'accès lors de l'utilisation de la fonction NAT

Contexte / Préparation

Installez un réseau similaire à celui du schéma. 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 de la gamme 1841. Elles s'appliquent aussi à 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 de la gamme Cisco 1841 ou équivalents, chacun avec une connexion série et 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 série en 2 parties (ETTD/DCE)

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

- 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.
- Connectez l'interface Fa0/0 du routeur R1 à l'interface Fa0/1 du commutateur S1 à l'aide d'un câble droit.
- Connectez chaque PC à l'aide d'un câble console pour procéder aux configurations sur le routeur et les commutateurs.
- Connectez l'hôte H1 au port Fa0/2 du commutateur S1 à l'aide d'un câble droit.
- 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

- Connectez un PC au port console du routeur pour procéder aux configurations à l'aide d'un programme d'émulation de terminal.
- Configurez le routeur R1 avec un nom d'hôte, des interfaces, des adresses IP et des mots de passe de console, Telnet et privilégié, selon la table d'adressage et le schéma de topologie. Enregistrez la configuration.

Étape 3 : configuration de base du routeur R2

Procédez à la configuration de base du routeur R2 comme routeur de passerelle, avec un nom d'hôte, des interfaces et des mots de passe de console, Telnet et privilégié, selon la table d'adressage et le schéma de topologie. 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 privilégié, selon la table et le schéma de topologie.

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

- a. Configurez chaque hôte avec l'adresse IP, le masque de sous-réseau et la passerelle par défaut corrects.
- b. Chaque station de travail doit pouvoir envoyer un paquet 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 des routes statique et par défaut sur les routeurs

- a. Configurez une route statique sur le routeur R2 pour atteindre le réseau privé de R1. Utilisez l'interface de tronçon suivant comme chemin sur R1.

```
R2(config)#ip route 192.168.1.0 255.255.255.0 209.165.201.1
```

- b. Configurez une route par défaut sur le routeur R1 pour réacheminer tout trafic ayant une destination inconnue vers l'interface de tronçon suivant sur R2.

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

Étape 7 : 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 partir de chaque hôte, envoyez une requête ping à l'interface Serial 0/0/0 de R2.

Chaque requête ping devrait aboutir. Si ce n'est pas le cas, vérifiez les configurations des routes statique et par défaut pour trouver l'erreur. Envoyez de nouvelles requêtes ping jusqu'à ce qu'elles aboutissent.

Étape 8 : configuration des fonctions NAT et PAT sur R1

- a. Définissez une liste de contrôle d'accès correspondant aux adresses IP privées internes.

```
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

- b. Définissez la traduction PAT de l'intérieur de la liste vers l'extérieur.

```
R1(config)#ip nat inside source list 1 interface s0/0/0 overload
```

- c. Indiquez les interfaces.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ip nat outside
```

En quoi l'adresse IP privée d'un hôte sera-t-elle traduite ? _____

Étape 9 : test et vérification de la configuration

- a. Envoyez une requête ping de PC2 à PC1.

A-t-elle abouti ? _____

- b. Envoyez une requête ping à l'interface série sur R2 à partir de PC1 et PC2.

A-t-elle abouti ? _____

- c. Vérifiez que les traductions NAT ont bien lieu en utilisant la commande **show ip nat translations** (un exemple de sortie est affiché).

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.201.1:2	192.168.1.2:2	209.165.201.2:2	209.165.201.2:2
icmp	209.165.201.1:3	192.168.1.2:3	209.165.201.2:3	209.165.201.2:3
icmp	209.165.201.1:4	192.168.1.2:4	209.165.201.2:4	209.165.201.2:4
icmp	209.165.201.1:5	192.168.1.2:5	209.165.201.2:5	209.165.201.2:5
icmp	209.165.201.1:10	192.168.1.3:10	209.165.201.2:10	209.165.201.2:10
icmp	209.165.201.1:7	192.168.1.3:7	209.165.201.2:7	209.165.201.2:7
icmp	209.165.201.1:8	192.168.1.3:8	209.165.201.2:8	209.165.201.2:8
icmp	209.165.201.1:9	192.168.1.3:9	209.165.201.2:9	209.165.201.2:9

Comment la sortie indique-t-elle que la fonction PAT est utilisée ?

Étape 10 : configuration et application d'une liste de contrôle d'accès conçue pour filtrer le trafic à partir d'un hôte

- a. Empêchez PC1 d'atteindre R2, tout en autorisant le reste du trafic à circuler librement.

```
R1(config)#access-list 10 deny 192.168.1.2
R1(config)#access-list 10 permit any
```

- b. Appliquez la liste de contrôle d'accès à l'interface série de R1.

```
R1(config)#interface s0/0/0
R1(config-if)#ip access-group 10 out
```

Étape 11 : test des effets de la liste de contrôle d'accès sur le trafic réseau

- a. Envoyez une requête ping de PC1 à PC2 et de PC1 à sa passerelle par défaut.

La requête ping a-t-elle abouti ? _____

- b. Envoyez une requête ping de PC1 à l'interface série de R2.

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

- c. Envoyez une requête ping de PC2 à l'interface série de R2.
La commande a-t-elle été exécutée correctement ? _____
La liste de contrôle d'accès produit-elle les résultats souhaités ? _____
Que vous attendriez-vous à voir en consultant la table de traduction NAT ? _____
-

Étape 12 : déplacement de la liste de contrôle d'accès et nouveau test

- a. Supprimez la liste de contrôle d'accès de l'interface série de R1.
- ```
R1(config)#interface s0/0/0
R1(config-if)#no ip access-group 10 out
```
- b. Placez plutôt la liste de contrôle d'accès sur l'interface FastEthernet.
- ```
R1(config)#interface fastethernet 0/0  
R1(config-if)#ip access-group 10 in
```
- c. Testez à nouveau la liste de contrôle d'accès à l'aide des requêtes ping de l'étape 11.
Décrivez les résultats cette fois-ci.
-

La liste de contrôle d'accès produit-elle les résultats souhaités ? _____

Étape 13 : remarques générales

- a. Quel est le rôle de l'adresse IP de l'interface série de R1 dans les fonctions NAT et PAT ?
(Reportez-vous à la sortie présentée à l'étape 9.)
- _____
- _____
- b. Citez, dans leur ordre d'exécution, les modifications apportées à l'adresse IP de PC1 lorsque la liste de contrôle d'accès a été placée sur l'interface série de R1.
- _____
- _____
- _____
- c. Pourquoi le déplacement de la liste de contrôle d'accès vers l'interface FastEthernet a-t-il produit les résultats souhaités ?
- _____
- _____