Travaux Pratiques : Configuration de Switch et Maîtrise du NAT Cisco

Durée estimée : 3h00

Environnement : Cisco Packet Tracer

Objectifs du TP

1. **Préparation de l'environnement :** Effacer et recharger la configuration des périphériques.
2. **Configuration de base du Routeur (R1) :** Nom d'hôte, mots de passe, et configuration des interfaces.
3. **Configuration de base du Commutateur (Comm1) :** Paramètres globaux initiaux, configuration d'une adresse IP VLAN de gestion (VLAN 1).
4. **Sécurité et performance du Switch :** Configuration de la sécurité de base des ports et des paramètres de vitesse/duplex.
5. **Mise en œuvre du NAT :** Configurer les trois types de NAT (Statique, Dynamique avec Pool, PAT/Surcharge) pour permettre l'accès à Internet.
6. **Vérification :** Tester la connectivité et les tables de translation NAT.

Phase 0 : Préparation de la Topologie et Configuration Initiale

0.1. Topologie requise

Basée sur les exigences du TP NAT et du TP Switch, la topologie devra inclure :

- Un routeur central (R1).
- Un routeur simulant l'ISP (Internet Service Provider) avec l'adresse 8.8.8.8/32 configurée sur une interface Loopback.
- Un commutateur (Comm1, Cisco 2960).
- Trois hôtes internes (H1, H2, H3) connectés à Comm1.
- Un second réseau interne pour le NAT dynamique avec surcharge (ex: 192.168.0.0/24).

Schéma Logique de la Topologie NAT et Switch

Cette topologie est centrée autour du routeur **R1 (CustomerRouter)**, qui agit comme le point de démarcation et effectue la **Network Address Translation (NAT)** pour permettre aux réseaux privés d'accéder à l'Internet simulé (ISP).

I. Réseau Externe (Côté *Outside*)

Périphérique	Interface	Adresse IP	Rôle	Source(s)
ISP Router	Loopback 0	**8.8.8.8 /32**	Simule Internet (Destination Publique)	

R1 (CustomerRouter)	S0/0 (Série)	(Exemple: **201.49.10.29**)	Déclarée `ip nat outside`. Interface connectée à l'ISP.	

II. Réseau Interne 1 (192.168.1.0/24) – Connecté à Comm1

Ce réseau est utilisé pour le NAT Statique et le NAT Dynamique avec Pool. L'interface de R1 est déclarée `ip nat inside`.

Périphérique	Interface	Adresse IP	Passerelle	Connexion à Comm1	Source(s)
R1 (CustomerRouter)	Fa0/1	**192.168.1.1 /24**	N/D	Fa0/5 (Routeur vers Switch)	
Comm1 (CustomerSwitch 2960)	VLAN 1 (Gestion)	**192.168.1.5 /24**	192.168.1.1	N/D	
H1 (Hôte)	Carte réseau	**192.168.1.2 /24**	192.168.1.1	Fa0/11	
H2 (Hôte)	Carte réseau	**192.168.1.4 /24**	192.168.1.1	Fa0/18	
H3 (Hôte/Static NAT)	Carte réseau	**192.168.1.100 /24**	192.168.1.1	Port libre (Ex: Fa0/12)	

Rôles NAT spécifiques pour le Réseau 192.168.1.0/24 :

- **H3 (192.168.1.100)** utilise le **NAT Statique** (Inside Local) vers une adresse publique spécifique (Inside Global, ex: 201.49.10.30).
- **H1 et H2** (et le reste du réseau, hors H3) utilisent le **NAT Dynamique avec Pool** (plage d'adresses publiques, ex: 201.49.10.31 - 201.49.10.40).

III. Réseau Interne 2 (192.168.0.0/24)

Ce réseau est dédié au **NAT dynamique avec surcharge (PAT/Overload)**. L'interface de R1 est également déclarée `ip nat inside`.

Périphérique	Interface	Adresse IP	Passerelle	Connexion à R1
R1 (CustomerRouter)	Fa0/0	**192.168.0.254 /24**	N/D	N/D
H4 (Hôte)	Carte réseau	**192.168.0.10 /24**	192.168.0.254	Connecté directement à R1 Fa0/0

Rôle NAT spécifique pour le Réseau 192.168.0.0/24 :

- Les hôtes de ce réseau, comme H4, utilisent l'adresse IP de l'interface S0/0 de R1 (201.49.10.29) pour le PAT, grâce au mécanisme de surcharge (`overload`) et de suivi des numéros de port.

Synthèse des connexions et des rôles NAT

Le flux logique des données pour cette topologie est le suivant:

- **Commutateur (Comm1/2960)** : Permet aux hôtes H1, H2, et H3 de communiquer localement et d'accéder à la passerelle R1 (Fa0/1).
- **R1 (Routeur Central)** : Assure la translation entre les adresses IP privées (définies par la RFC 1918, ex: 192.168.0.0/16) et l'adresse IP publique. Les interfaces Fa0/0 et Fa0/1 sont les interfaces *inside*, et S0/0 est l'interface *outside*.

- **Translation NAT :** R1 effectue les trois types de translation: Statique, Dynamique (pool), et PAT (surcharge).

0.2. Adressage (Synthèse des Sources)

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut	Rôle NAT	Source
R1	Fa0/1	192.168.1.1	255.255.255.0	N/D	Inside	
R1	Fa0/0	192.168.0.254	255.255.255.0	N/D	Inside	
R1	S0/0	*Adresse Publique* (Ex: 201.49.10.29)	/xx	N/D	Outside	
Comm1	VLAN 1	192.168.1.5	255.255.255.0	192.168.1.1	N/D	
H1	Carte réseau	192.168.1.2	255.255.255.0	192.168.1.1	N/D	
H2	Carte réseau	192.168.1.4	255.255.255.0	192.168.1.1	N/D	
H3 (Static NAT)	Carte réseau	192.168.1.100	255.255.255.0	192.168.1.1	Inside Local	

Note : Les interfaces Fa0/0 et Fa0/1 de R1 sont du côté privé (`inside`), et l'interface S0/0 est du côté public (`outside`).

0.3. Nettoyage des configurations

Avant de commencer, assurez-vous que les configurations sont effacées.

1. Effacez la configuration de démarrage (`startup-config`) sur R1 et Comm1.
2. Supprimez le fichier `vlan.dat` sur Comm1 si nécessaire.
3. Rechargez (reload) les périphériques.

Phase 1 : Configuration de Base du Commutateur

1.1. Configuration des Hôtes et Connexion

1. Configurez H1, H2, et H3 avec les adresses IP et passerelles par défaut spécifiées dans la table.
2. Connectez H1 au port Fa0/11 et H2 au port Fa0/18 de Comm1. Connectez H3 à un port libre (ex: Fa0/12).

1.2. Configuration de R1 (Passerelle par défaut)

Configurez R1 avec les informations de base :

```
R1(config)# hostname CustomerRouter
R1(config)# enable secret cisco123
R1(config)# interface Fa0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface Fa0/0
R1(config-if)# ip address 192.168.0.254 255.255.255.0
R1(config-if)# no shutdown
```

1.3. Configuration de Comm1 (CustomerSwitch)

1. Configurez les paramètres de sécurité et d'accès sur le commutateur :

```
Comm1(config)# hostname CustomerSwitch
Comm1(config)# enable password cisco
Comm1(config)# enable secret cisco123
Comm1(config)# line console 0
Comm1(config-line)# password cisco123
Comm1(config-line)# login
Comm1(config-line)# line vty 0 15
Comm1(config-line)# password cisco123
   Comm1(config-line)# login
   Comm1(config-line)# end
```

12. Configurez l'interface de gestion VLAN 1 :

```
   Comm1# configure terminal
   Comm1(config)# interface vlan 1
   Comm1(config-if)# ip address 192.168.1.5 255.255.255.0
   Comm1(config-if)# exit
   Comm1(config)# ip default-gateway 192.168.1.1
   Comm1(config)# end
```

19. Vérifiez la connectivité : Envoyez une requête `ping` de Comm1 vers R1 (192.168.1.1). Testez la session Telnet depuis H1 vers Comm1 (192.168.1.5).

1.4. Sécurité de base des ports (Port Security) (Optionnel si temps disponible)

Configurez le port Fa0/18 pour n'accepter qu'un seul périphérique et utilisez l'option *sticky* pour mémoriser l'adresse MAC, avec l'action de violation *Shutdown* :

```
Comm1(config)# interface fastEthernet 0/18
Comm1(config-if)# switchport mode access
Comm1(config-if)# switchport port-security
Comm1(config-if)# switchport port-security mac-address sticky
Comm1(config-if)# end
```

Test : Déconnectez H2 et connectez un autre hôte (H3 ou un PC alternatif) au port Fa0/18. Tentez une requête ping pour provoquer une violation et vérifiez l'état du port (`err-disable`). Réactivez le port Fa0/18.

Phase 2 : Configuration du NAT (R1)

La configuration du NAT s'effectue sur R1. Nous allons configurer l'interface S0/0 (côté Internet) pour être l'interface `outside` et les interfaces internes (Fa0/0 et Fa0/1) comme `inside`.

2.1. Configuration des interfaces NAT communes

Désignez les interfaces *inside* et *outside* :

```
CustomerRouter# configure terminal
CustomerRouter(config)# interface Fa0/0
CustomerRouter(config-if)# ip nat inside
CustomerRouter(config-if)# exit

CustomerRouter(config)# interface Fa0/1
CustomerRouter(config-if)# ip nat inside
CustomerRouter(config-if)# exit

# Configurez l'interface publique (S0/0)
CustomerRouter(config)# interface S0/0
CustomerRouter(config-if)# ip address [Adresse publique, ex: 201.49.10.29]
[Masque]
CustomerRouter(config-if)# ip nat outside
```

```
CustomerRouter(config-if)# no shutdown
CustomerRouter(config-if)# exit

# Simuler l'Internet (ISP)
# Configurez un routeur ISP avec une interface loopback 8.8.8.8/32
```

(Remarque : Assurez-vous que R1 possède une route par défaut pointant vers l'ISP pour que les paquets sortent.)

2.2. Scénario A : NAT Statique (Hôte H3, 192.168.1.100)

L'hôte H3 (192.168.1.100) doit être accessible depuis Internet via une adresse publique spécifique (201.49.10.30). C'est une translation statique un-à-un.

1. **Définition de la translation statique :**

```
# Syntaxe : ip nat inside source static <ip_source> <ip_dest>
CustomerRouter(config)# ip nat inside source static 192.168.1.100
201.49.10.30
```

4. **Vérification :** Tentez d'envoyer un paquet depuis H3 (192.168.1.100) vers l'ISP (8.8.8.8). Vérifiez ensuite la connectivité inverse (ISP vers 201.49.10.30). L'adresse source 192.168.1.100 doit être remplacée par 201.49.10.30 à la sortie de S0/0.

2.3. Scénario B : NAT Dynamique avec Pool (Réseau 192.168.1.0/24, sauf H3)

Le réseau 192.168.1.0/24 (à l'exception de 192.168.1.100) utilisera un pool d'adresses publiques pour la translation dynamique.

1. **Définition du Pool d'adresses publiques :** Créez une plage d'adresses IP globales internes (ex : 201.49.10.31 à 201.49.10.40).

```
# Syntaxe : ip nat pool <nom> <start-ip> <end-ip>
CustomerRouter(config)# ip nat pool NAT_POOL 201.49.10.31
201.49.10.40 netmask 255.255.255.0
```

4. **Définition des adresses locales autorisées (ACL) :** Créez une Access-List Standard pour identifier les IP locales internes qui ont le droit de sortir, excluant H3 (192.168.1.100).

```
# Exemple pour autoriser tout le réseau 192.168.1.0/24 :
# access-list 1 permit 192.168.1.0 0.0.0.255
# Pour exclure 192.168.1.100, une ACL étendue serait préférable,
# mais en se basant sur la source fournie, nous autorisons l'ensemble
du réseau 192.168.1.0/24 :
CustomerRouter(config)# access-list 2 permit 192.168.1.0 0.0.0.255
```

10. **Associer l'ACL au Pool :**

```
    CustomerRouter(config)# ip nat inside source list 2 pool NAT_POOL
```

12. **Vérification :** Depuis H1 (192.168.1.2) ou H2 (192.168.1.4), faites un ping vers l'ISP (8.8.8.8). L'adresse source utilisée sera piochée dans le pool $201.49.10.31 - 201.49.10.40$.

2.4. Scénario C : PAT / NAT Dynamique avec Surcharge (Réseau 192.168.0.0/24)

Le réseau 192.168.0.0/24 utilisera le NAT dynamique avec surcharge (PAT/Overload) en utilisant l'adresse IP de l'interface publique de R1 (S0/0). C'est la configuration la plus courante (domestique).

1. **Définition des adresses locales autorisées (ACL) :**

```
CustomerRouter(config)# access-list 3 permit 192.168.0.0 0.0.0.255
```

3. **Configuration de la Surcharge (Overload) :** La translation se fait en utilisant l'adresse de l'interface de sortie (`outside` interface) S0/0.

```
4. # Syntaxe : ip nat inside source list <number> interface <interface>
   overload
5. CustomerRouter(config)# ip nat inside source list 3 interface S0/0
   overload
```

6. **Vérification :** Créez un hôte dans le réseau 192.168.0.0/24 (ex: 192.168.0.10). Depuis cet hôte, faites un ping vers l'ISP (8.8.8.8). L'adresse source utilisée sera l'adresse IP configurée sur S0/0 de R1 (201.49.10.29).

2.5. Vérification Générale des Translations NAT (R1)

Utilisez les commandes `show` pour vérifier l'état des translations :

1. **Affichez les translations actives :**

```
2. CustomerRouter# show ip nat translations
```

3. **Vérifiez les statistiques :**

```
4. CustomerRouter# show ip nat statistics
```

Conclusions du TP

1. Décrivez la différence principale entre le NAT Statique et le PAT (Network Address Port Translation).
2. Expliquez pourquoi le NAT est nécessaire lorsque des adresses privées (telles que 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) sont utilisées en interne.
3. Dans le scénario C (PAT), comment le routeur peut-il suivre les connexions de plusieurs hôtes sortant avec la même adresse IP publique ?
4. Quel type de configuration NAT est le plus courant dans un réseau modeste et pourquoi ?