Travaux Pratiques - Configurer NAT pour IPv4

Topologie



# Table d'adressage

|  |  |  |  |
| --- | --- | --- | --- |
| Appareil | Interface | Adresse IP | Masque de sous-réseau |
| R1 | G0/0/0 | 209.165.200.230 | 255.255.255.248 |
| R1 | G0/0/1 | 192.168.1.1 | 255.255.255.0 |
| R2 | G0/0/0 | 209.165.200.225 | 255.255.255.248 |
| R2 | Lo1 | 209.165.200.1 | 255.255.255.224 |
| S1 | VLAN 1 | 192.168.1.11 | 255.255.255.0 |
| S2 | VLAN 1 | 192.168.1.12 | 255.255.255.0 |
| PC-A | Carte réseau | 192.168.1.2 | 255.255.255.0 |
| PC-B | Carte réseau | 192.168.1.3 | 255.255.255.0 |

# Objectifs

Partie 1 : Création d'un réseau et configuration des paramètres de base des périphériques

Partie 2 : Configurer et vérifier le NAT pour IPv4

Partie 3 : Configurer et vérifier le PAT pour IPv4

Partie 4 : Configurer et vérifier le NAT statique pour IPv4

# Contexte/scénario

La traduction d'adresses réseau (NAT) est le processus par lequel un périphérique réseau, tel qu'un routeur Cisco, attribue une adresse publique aux périphériques hôtes à l'intérieur d'un réseau privé. La raison principale de l'utilisation de la fonction NAT est la diminution du nombre d'adresses IP publiques utilisées par une entreprise, car le nombre d'adresses publiques IPv4 disponibles est limité.

Un ISP a attribué à une entreprise l'espace public d'adresses IP 209.165.200.224/29. Ce réseau est utilisé pour traiter la liaison entre le routeur ISP (R2) et la passerelle de l'entreprise (R1). La première adresse (209.165.200.225) est attribuée à l'interface g0/0/0 sur R2 et la dernière adresse (209.165.200.230) est attribuée à l'interface g0/0/0 sur R1. Les adresses restantes (209.165.200.226-209.165.200.229) seront utilisées pour fournir un accès Internet aux hôtes de la société. Une route par défaut est utilisée de R1 à R2. L'internet est simulé par une adresse en boucle sur R2.

Dans ce TP, vous allez configurer différents types de NAT. Vous testerez, afficherez et vérifierez les traductions, et interpréterez les statistiques NAT/PAT pour contrôler le processus.

**Remarque**: les routeurs utilisés dans les travaux pratiques CCNA sont Cisco 4221 version 16.9.3 de Cisco IOS XE (image universalk9). Les commutateurs utilisés dans les laboratoires sont des Cisco Catalyst 2960s avec Cisco IOS Release 15.2(2) (image lanbasek9). D'autres routeurs, commutateurs et versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent varier de ce qui est indiqué dans les travaux pratiques. Reportez-vous au tableau récapitulatif de l'interface du routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

**Remarque**: Assurez-vous que les routeurs et les commutateurs ont été réinitialisés et ne possèdent aucune configuration initiale. En cas de doute, contactez votre formateur.

# Ressources requises

* 2 Routeurs (Cisco 4221 équipé de Cisco IOS version 16.9.4, image universelle ou similaire)
* 2 commutateurs (Cisco 2960 équipés de Cisco IOS version 15.2(2) image lanbasek9 ou similaires)
* 2 PC (Windows, équipés d'un programme d'émulation de terminal tel que Tera Term)
* Câbles de console pour configurer les appareils Cisco IOS via les ports de console
* Câbles Ethernet conformément à la topologie

# Instructions

## Création du réseau et configuration des paramètres de base des périphériques

Dans la Partie 1, vous allez configurer la topologie du réseau et les paramètres de base sur les hôtes de PC et les commutateurs.

### Câblez le réseau conformément à la topologie indiquée.

Fixez les appareils comme indiqué dans le diagramme de la topologie et raccordez-les au câble si nécessaire.

### configuration des paramètres de base pour chaque routeur.

Ouvrez la fenêtre de configuration.

* + - 1. Attribuez un nom de l'appareil au routeur.
      2. Désactivez la recherche DNS pour empêcher le routeur d'essayer de traduire les commandes saisies comme s'il s'agissait de noms d'hôtes.
      3. Attribuez **class** comme mot de passe chiffré d'exécution privilégié.
      4. Attribuez **cisco** comme mot de passe de console et activez la connexion.
      5. Attribuez **cisco** comme mot de passe VTY et activez la connexion.
      6. Cryptez les mots de passe en texte brut.
      7. Créez une bannière qui avertit quiconque accède au périphérique que tout accès non autorisé est interdit.
      8. Configurez l'adressage IP de l'interface comme spécifié dans le tableau ci-dessus.
      9. Configurez une route par défaut vers R2 à partir de R1.
      10. Enregistrez la configuration en cours dans le fichier de configuration initiale.

Fermez la fenêtre de configuration.

### Configurez les paramètres de base pour chaque commutateur.

Ouvrez la fenêtre de configuration.

* + - 1. Attribuez un nom de périphérique au commutateur.
      2. Désactivez la recherche DNS pour empêcher le routeur d'essayer de traduire les commandes saisies comme s'il s'agissait de noms d'hôtes.
      3. Attribuez **class** comme mot de passe chiffré d'exécution privilégié.
      4. Attribuez **cisco** comme mot de passe de console et activez la connexion.
      5. Attribuez **cisco** comme mot de passe VTY et activez la connexion.
      6. Cryptez les mots de passe en texte brut.
      7. Créez une bannière qui avertit quiconque accède à l'appareil que tout accès non autorisé est interdit.
      8. Arrêtez toutes les interfaces qui ne seront pas utilisées.
      9. Configurez l'adressage IP de l'interface comme spécifié dans le tableau ci-dessus.
      10. Enregistrez la configuration en cours dans le fichier de configuration initiale.

Fermez la fenêtre de configuration.

## Configurer et vérifier NAT pour IPv4.

Dans la partie 2, vous allez configurer et vérifier NAT pour IPv4.

### Configurez NAT sur R1 à l'aide d'un pool de trois adresses, 209.165.200.226-209.165.200.228.

Ouvrez la fenêtre de configuration.

* + - 1. Configurez une liste d'accès simple qui définit les hôtes qui seront autorisés pour la traduction. Dans ce cas, tous les appareils du réseau local R1 sont éligibles pour la traduction.

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

* + - 1. Créez le pool NAT et donnez-lui un nom et une plage d'adresses à utiliser.

R1(config)# **ip nat pool PUBLIC\_ACCESS 209.165.200.226 209.165.200.228 netmask 255.255.255.248**

**Remarque** : Le paramètre de masque de réseau n'est pas un délimiteur d'adresse IP. Il doit être le masque de sous-réseau correct pour les adresses assignées, même si vous n'utilisez pas toutes les adresses de sous-réseau dans le pool.

* + - 1. Configurez la traduction, en associant l'ACL et le pool au processus de traduction.

R1(config)# **ip nat inside source list 1 pool PUBLIC\_ACCESS**

**Note** : Trois points très importants. Premièrement, le mot 'inside' est essentiel au fonctionnement de ce type de NAT. Si vous l'omettez, NAT ne fonctionnera pas. Deuxièmement, le numéro de liste est le numéro ACL configuré lors d'une étape précédente. Troisièmement, le nom du pool est sensible à la casse.

* + - 1. Spécifiez l'interface interne.

R1(config)# **interface g0/0/1**

R1(config-if)# **ip nat inside**

* + - 1. Définissez l'interface externe.

R1 (config) # **interface g0/0/1**

R1(config-if)# **ip nat outside**

### Testez et vérifiez la configuration.

* + - 1. À partir de PC-B, ping l'interface Lo1 (209.165.200.1) sur R2. Si la requête ping échoue, dépannez et corrigez les problèmes. Sur R1, affichez la table NAT sur R1 avec la commande **show ip nat translations**.

R1# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

--- 209.165.200.226 192.168.1.3 --- ---

icmp 209.165.200.226:1 192.168.1.3:1 209.165.200.1:1 209.165.200.1:1

Total number of translations: 2

#### Questions :

Quelle est l'adresse locale interne de PC-B traduite ?

Saisissez vos réponses ici

Quel type d'adresse NAT est l'adresse traduite ?

Saisissez vos réponses ici

* + - 1. À partir de PC-A, ping l'interface Lo1 (**209.165.200.1**) sur R2. Si la requête ping échoue, dépannez et corrigez les problèmes. Sur R1, affichez la table NAT sur R1 avec la commande **show ip nat translations**.

R1# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

--- 209.165.200.227 192.168.1.2 --- ---

--- 209.165.200.226 192.168.1.3 --- ---

icmp 209.165.200.227:1 192.168.1.2:1 209.165.200.1:1 209.165.200.1:1

icmp 209.165.200.226:1 192.168.1.3:1 209.165.200.1:1 209.165.200.1:1

Total number of translations: 4

* + - 1. Notez que la traduction précédente de PC-B est toujours dans le tableau. À partir de S1, ping l'interface Lo1 (**209.165.200.1**) sur R2. Si la requête ping échoue, dépannez et corrigez les problèmes. Sur R1, affichez la table NAT sur R1 avec la commande **show ip nat translations**.

R1# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

--- 209.165.200.227 192.168.1.2 --- ---

--- 209.165.200.226 192.168.1.3 --- ---

--- 209.165.200.228 192.168.1.11 --- ---

icmp 209.165.200.226:1 192.168.1.3:1 209.165.200.1:1 209.165.200.1:1

icmp 209.165.200.228:0 192.168.1.11:0 209.165.200.1:0 209.165.200.1:0

Total number of translations: 5

* + - 1. Maintenant, essayez de pinger R2 Lo1 à partir de S2. Cette fois, les traductions échouent, et vous obtenez ces messages (ou similaires) sur la console R1 :

Sep 23 15:43:55.562: %IOSXE-6-PLATFORM: R0/0: cpp\_cp: QFP:0.0 Thread:000 TS:00000001473688385900 %NAT-6-ADDR\_ALLOC\_FAILURE: Address allocation failed; pool 1 may be exhausted [2]

* + - 1. C'est un résultat attendu, car seulement 3 adresses sont allouées, et nous avons essayé de ping Lo1 à partir de quatre appareils. Rappelons que NAT est une traduction individuelle. Combien de temps les traductions sont-elles allouées ? Émettez la commande **show ip nat translations verbose** et vous verrez que la réponse est pour 24 heures.

R1# **show ip nat translations verbose**

Pro Inside global Inside local Outside local Outside global

--- 209.165.200.226 192.168.1.3 --- ---

create: 09/23/19 15:35:27, use: 09/23/19 15:35:27, timeout: 23:56:42

Map-Id(In): 1

<output omitted>

* + - 1. Étant donné que le pool est limité à trois adresses, NAT à un pool d'adresses ne convient pas à notre application. Effacez les traductions et les statistiques NAT et nous passerons à PAT.

R1# **clear ip nat translations \***

R1# **clear ip nat statistics**

Fermez la fenêtre de configuration.

## Configurer et vérifier PAT pour IPv4.

Dans la partie 3, vous allez configurer le remplacement NAT par PAT à un pool d'adresses, puis avec PAT à l'aide d'une interface.

### Supprimez la commande de traduction sur R1.

Ouvrez la fenêtre de configuration.

Les composants d'une configuration de traduction d'adresses sont fondamentalement les mêmes : quelque chose (une liste d'accès) pour identifier les adresses pouvant être traduites, un pool d'adresses configuré en option pour les traduire et les commandes nécessaires pour identifier les interfaces internes et externes. À partir de la partie 1, notre liste d'accès (liste d'accès 1) est toujours correcte pour le scénario réseau, il n'est donc pas nécessaire de la recréer. Nous allons utiliser le même pool d'adresses, donc il n'est pas nécessaire de recréer cette configuration non plus. En outre, les interfaces internes et externes ne changent pas. Pour commencer dans la partie 3, supprimez la commande qui lie l'ACL et le pool.

R1(config)# **ip nat inside source list 1 pool PUBLIC\_ACCESS**

### Ajoutez la commande PAT sur R1.

Maintenant, configurez pour la traduction PAT vers un pool d'adresses (rappelez-vous, l'ACL et le pool sont déjà configurés, donc c'est la seule commande que nous devons passer de NAT à PAT).

R1(config)# **ip nat inside source list 1 pool PUBLIC\_ACCESSoverload**

### Testez et vérifiez la configuration.

* + - 1. Vérifions que PAT fonctionne. À partir de PC-B, ping l'interface Lo1 (209.165.200.1) sur R2. Si la requête ping échoue, dépannez et corrigez les problèmes. Sur R1, affichez la table NAT sur R1 avec la commande **show ip nat translations**.

R1# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.226:1 192.168.1.3:1 209.165.200.1:1 209.165.200.1:1

Total number of translations: 1#

#### Questions :

Quelle est l'adresse locale interne de PC-B traduite ?

Saisissez vos réponses ici

Quel type d'adresse NAT est l'adresse traduite ?

Saisissez vos réponses ici

Quelle est la différence sur la sortie de la commande **show ip nat translations** de l'exercice NAT ?

Saisissez vos réponses ici

* + - 1. À partir de PC-A, ping l'interface Lo1 (209.165.200.1) sur R2. Si la requête ping échoue, dépannez et corrigez les problèmes. Sur R1, affichez la table NAT sur R1 avec la commande **show ip nat translations**.

R1# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.226:1 192.168.1.2:1 209.165.200.1:1 209.165.200.1:1

Total number of translations: 1

Notez qu'il n'y a qu'une seule traduction à nouveau. Envoyez le ping une fois de plus, et rapidement revenir au routeur et émettez la commande **show ip nat translations verbose** et vous verrez ce qui s'est passé.

R1# **show ip nat translations verbose**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.226:1 192.168.1.2:1 209.165.200.1:1 209.165.200.1:1

create: 09/23/19 16:57:22, use: 09/23/19 16:57:25, timeout: 00:01:00

<output omitted>

Comme vous pouvez le voir, le délai de traduction a été réduit de 24 heures à 1 minute.

* + - 1. Générez du trafic à partir de plusieurs périphériques pour observer le PAT. Sur PC-A et PC-B, utilisez le paramètre -t avec la commande ping pour envoyer un ping non-stop à l'interface Lo1 de R2 (**ping -t 209.165.200.1**), puis revenez à R1 et émettez la commande **show ip nat translations** :

R1# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.226:1 192.168.1.2:1 209.165.200.1:1 209.165.200.1:1

icmp 209.165.200.226:2 192.168.1.3:1 209.165.200.1:1 209.165.200.1:2

Total number of translations: 2

Notez que l'adresse globale interne est la même pour les deux sessions.

#### Question :

Comment le routeur garde-t-il une trace de ce que les réponses vont où ?

Saisissez vos réponses ici

* + - 1. PAT à un pool est une solution très efficace pour les petites et moyennes entreprises. Cependant, il y a des adresses IPv4 inutilisées impliquées dans ce scénario. Nous passerons à PAT avec surcharge d'interface pour éliminer ce gaspillage d'adresses IPv4. Arrêtez les pings sur PC-A et PC-B avec la combinaison de touches Ctrl-C, puis effacez les traductions et les statistiques de traduction :

R1# **clear ip nat translations \***

R1# **clear ip nat statistics**

### Sur R1, supprimez les commandes de traduction nat pool.

Encore une fois, notre liste d'accès (liste d'accès 1) est toujours correcte pour le scénario réseau, donc il n'est pas nécessaire de la recréer. En outre, les interfaces internes et externes ne changent pas. Pour commencer avec PAT à une interface, nettoyez la configuration en supprimant le pool NAT et la commande qui lie l'ACL et le pool.

R1(config)# **no ip nat inside source list 1 pool PUBLIC\_ACCESSoverload**

R1(config)# **no ip nat pool PUBLIC\_ACCESS**

### Ajoutez la commande PAT surcharge en spécifiant l'interface externe.

Ajoutez la commande PAT qui provoquera une surcharge à l'interface externe.

R1(config)# **ip nat inside source list 1 interface g0/0/0 overload**

### Testez et vérifiez la configuration.

* + - 1. Vérifions que PAT à l'interface fonctionne. À partir de PC-B, ping l'interface Lo1 (209.165.200.1) sur R2. Si la requête ping échoue, dépannez et corrigez les problèmes. Sur R1, affichez la table NAT sur R1 avec la commande **show ip nat translations**.

R1# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.230:1 192.168.1.3:1 209.165.200.1:1 209.165.200.1:1

Total number of translations: 1

* + - 1. Générez du trafic à partir de plusieurs périphériques pour observer le PAT. Sur PC-A et PC-B, utilisez le paramètre -t avec la commande ping pour envoyer un ping non-stop à l'interface Lo1 de R2 **(ping -t 209.165.200.1**). Sur S1 et S2, émettez la commande privilégiée exec ping 209.165.200.1 répéter 2000. Ensuite, revenez à R1 et émettez la commande **show ip nat translations** .

R1# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.230:3 192.168.1.11:1 209.165.200.1:1 209.165.200.1:3

icmp 209.165.200.230:2 192.168.1.2:1 209.165.200.1:1 209.165.200.1:2

icmp 209.165.200.230:4 192.168.1.3:1 209.165.200.1:1 209.165.200.1:4

icmp 209.165.200.230:1 192.168.1.12:1 209.165.200.1:1 209.165.200.1:1

Total number of translations: 4

Maintenant, toutes les adresses Inside Global sont mappées à l'adresse IP de l'interface g0/0/0.

Arrêtez tous les pings. Sur PC-A et PC-B, en utilisant la combinaison de touches CTRL-C.

Fermez la fenêtre de configuration.

## Configurer et vérifier NAT statique pour IPv4.

Dans la partie 4, vous allez configurer le NAT statique de sorte que PC-A soit directement accessible depuis Internet. PC-A sera accessible depuis R2 via l'adresse 209.165.200.229.

**Remarque** : La configuration que vous êtes sur le point de terminer ne suit pas les pratiques recommandées pour les passerelles connectées à Internet. Ce TP omet complètement les pratiques de sécurité standard pour se concentrer sur la configuration réussie de NAT statique. Dans un environnement de production, une coordination rigoureuse entre l'infrastructure réseau et les équipes de sécurité serait essentielle pour répondre à cette exigence.

### Sur R1, effacer les traductions et les statistiques actuelles.

Ouvrez la fenêtre de configuration.

R1# **clear ip nat translations \***

R1# **clear ip nat statistics**

### Sur R1, configurez la commande NAT requise pour mapper statiquement une adresse interne à une adresse externe.

Pour cette étape, configurez un mappage statique entre 192.168.1.11 et 209.165.200.1 à l'aide de la commande suivante :

R1(config)# **ip nat inside source static 192.168.1.2 209.165.200.229**

### Testez et vérifiez la configuration.

* + - 1. Vérifions que le NAT statique fonctionne. Sur R1, affichez la table NAT sur R1 avec la commande **show ip nat translations**, et vous devriez voir le mappage statique.

R1# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

--- 209.165.200.227 192.168.1.2 --- ---

Total number of translations: 1

* + - 1. Le tableau de traduction indique que la traduction statique est en vigueur. Vérifiez cela en ping de R2 à 209.165.200.229. Les pings devraient fonctionner.

Remarque : vous devrez peut-être désactiver le pare-feu du PC pour que les pings fonctionnent.

* + - 1. Sur R1, affichez la table NAT sur R1 avec la commande **show ip nat translations**, et vous devriez voir le mappage statique et la traduction au niveau du port pour les pings entrants.

R1# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

--- 209.165.200.227 192.168.1.2 --- ---

icmp 209.165.200.229:3 192.168.1.2:3 209.165.200.225:3 209.165.200.225:3

Total number of translations: 2

Cela valide que le NAT statique fonctionne.

Fermez la fenêtre de configuration.

# Tableau récapitulatif des interfaces des routeurs

| Modèle du routeur | Interface Ethernet 1 | Interface Ethernet 2 | Interface série 1 | Interface série 2 |
| --- | --- | --- | --- | --- |
| 1.800 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Série 0/0/0 (S0/0/0) | Série 0/0/1 (S0/0/1) |
| 1.900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Série 0/0/0 (S0/0/0) | Série 0/0/1 (S0/0/1) |
| 2.801 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Série 0/1/0 (S0/1/0) | Série 0/1/1 (S0/1/1) |
| 2.811 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Série 0/0/0 (S0/0/0) | Série 0/0/1 (S0/0/1) |
| 2.900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Série 0/0/0 (S0/0/0) | Série 0/0/1 (S0/0/1) |
| 4221 | Gigabit Ethernet 0/0/0 (G0/0/0) | Gigabit Ethernet 0/0/1 (G0/0/1) | Série 0/1/0 (S0/1/0) | Série 0/1/1 (S0/1/1) |
| 4300 | Gigabit Ethernet 0/0/0 (G0/0/0) | Gigabit Ethernet 0/0/1 (G0/0/1) | Série 0/1/0 (S0/1/0) | Série 0/1/1 (S0/1/1) |

**Remarque**: Pour savoir comment le routeur est configuré, observez les interfaces afin d'identifier le type de routeur ainsi que le nombre d'interfaces qu'il comporte. Il n'est pas possible de répertorier de façon exhaustive toutes les combinaisons de configurations pour chaque type de routeur. Ce tableau inclut les identifiants des différentes combinaisons d'interfaces Ethernet et série possibles dans l'appareil. Il ne comporte aucun autre type d'interface, même si un routeur particulier peut en contenir un. L’exemple de l’interface RNIS BRI peut illustrer ceci. La chaîne de caractères entre parenthèses est l'abréviation normalisée qui permet de représenter l'interface dans les commandes Cisco IOS.

Fin du document