Travaux pratiques : configuration de la fonction NAT dynamique et statique

Topologie

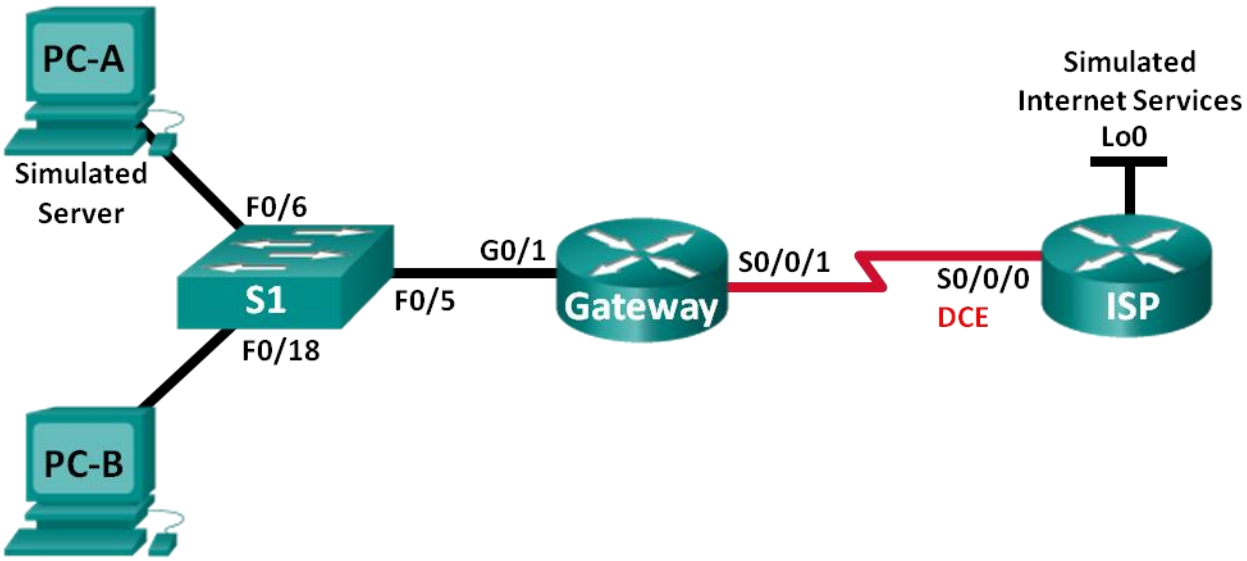

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
Passerelle	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A (serveur simulé)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

Objectifs

Partie 1 : création du réseau et vérification de la connectivité

Partie 2 : configuration et vérification de la fonction NAT statique

Partie 3 : configuration et vérification de la fonction NAT dynamique

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.

Dans ces travaux pratiques, un fournisseur d'accès Internet (FAI) a attribué l'espace d'adressage IP public 209.165.200.224/27 à une entreprise. Cela permet à l'entreprise de disposer de 30 adresses IP publiques. Les adresses 209.165.200.225 à 209.165.200.241 concernent l'attribution statique tandis que les adresses 209.165.200.242 à 209.165.200.254 concernent l'attribution dynamique. Une route statique est utilisée entre le FAI et le routeur de passerelle, et une route par défaut est utilisée entre la passerelle et le routeur ISP. La connexion à Internet (FAI) est simulée par une adresse de bouclage au niveau du routeur ISP.

Remarque : les routeurs utilisés lors des travaux pratiques CCNA sont des routeurs à services intégrés (ISR) Cisco 1941 équipés de Cisco IOS version 15.2(4)M3 (image universalk9). Les commutateurs utilisés sont des modèles Cisco Catalyst 2960s équipés de Cisco IOS version 15.0(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 ceux indiqués dans les travaux pratiques. Reportez-vous au tableau récapitulatif des interfaces de routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

Remarque : assurez-vous que les routeurs et le commutateur ont été réinitialisés et ne possèdent aucune configuration initiale. En cas de doute, contactez votre instructeur.

Ressources requises

- 2 routeurs (Cisco 1941 équipé de Cisco IOS version 15.2(4)M3 image universelle ou similaire)
- 1 commutateur (Cisco 2960 équipé de Cisco IOS version 15.0(2) image lanbasek9 ou similaire)
- 2 PC (Windows 7, Vista ou XP, équipés d'un programme d'émulation du terminal tel que Tera Term)
- Câbles de console pour configurer les périphériques Cisco IOS via les ports de console
- Câbles Ethernet et série conformément à la topologie

Partie 1: Création du réseau et vérification de la connectivité

Dans la Partie 1, vous allez configurer la topologie du réseau et les paramètres de base, tels que les adresses IP de l'interface, le routage statique, l'accès des périphériques et les mots de passe.

Étape 1: Câblez le réseau conformément à la topologie.

Fixez les périphériques conformément au schéma de la topologie, ainsi que les câbles, le cas échéant.

Étape 2: Configurez les hôtes de PC.

Étape 3: Initialisez et redémarrez les routeurs et les commutateurs, le cas échéant.

Étape 4: Configurez les paramètres de base pour chaque routeur.

a. Désactivez la recherche DNS.

b. Configurez les adresses IP pour les routeurs comme indiqué dans la table d'adressage.

c. Réglez la fréquence d'horloge sur **128000** pour les interfaces série DCE.

d. Configurez le nom du périphérique conformément à la topologie.

e. Attribuez **cisco** comme mots de passe de console et vty.

f. Attribuez **class** comme mot de passe chiffré du mode d'exécution privilégié.

g. Configurez **logging synchronous** pour empêcher les messages de console d'interrompre l'entrée de commande.

Étape 5: Créez un serveur Web simulé sur le routeur ISP.

a. Créez un utilisateur local nommé **webuser** avec le mot de passe chiffré **webpass**.

```
ISP(config)# username webuser privilege 15 secret webpass
```

b. Activez le service serveur HTTP sur le routeur ISP.

```
ISP(config)# ip http server
```

c. Configurez le service HTTP de manière à utiliser la base de données des utilisateurs locaux.

```
ISP(config)# ip http authentication local
```

Étape 6: Configurez le routage statique.

a. Créez une route statique depuis le routeur ISP jusqu'au routeur de passerelle en utilisant la plage d'adresses réseau publiques 209.165.200.224/27 attribuée.

```
ISP(config)# ip route 209.165.200.224 255.255.255.224 209.165.201.18
```

b. Créez une route par défaut sur le routeur de passerelle vers le routeur ISP.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

Étape 7: Enregistrez la configuration en cours en tant que configuration initiale.

Étape 8: Vérifiez la connectivité du réseau.

a. À partir des hôtes PC, envoyez une requête ping à l'interface G0/1 sur le routeur de passerelle. Dépannez si les requêtes ping échouent.

b. Affichez les tables de routage sur les deux routeurs afin de vérifier que les routes statiques figurent dans cette table et qu'elles sont configurées correctement sur les deux routeurs.

Partie 2: Configuration et vérification de la fonction NAT statique

La fonction NAT statique utilise un mappage de type « un à un » des adresses locales et globales, et ces mappages restent constants. La fonction NAT statique est particulièrement utile pour les serveurs Web ou les périphériques qui doivent posséder des adresses statiques accessibles depuis Internet.

Étape 1: Configurez un mappage statique.

La configuration d'un mappage statique permet d'indiquer au routeur d'établir une traduction entre l'adresse privée du serveur interne 192.168.1.20 et l'adresse publique 209.165.200.225. Cela permet à un utilisateur d'accéder à PC-A depuis Internet. PC-A simule un serveur ou un périphérique avec une adresse constante qui est accessible depuis Internet.

```
Gateway(config)# ip nat inside source static 192.168.1.20 209.165.200.225
```

Étape 2: Indiquez les interfaces.

Exécutez les commandes **ip nat inside** et **ip nat outside** pour les interfaces.

```
Gateway(config)# interface g0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```

Étape 3: Testez la configuration.

a. Affichez la table NAT statique en exécutant la commande **show ip nat translations**.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.225    192.168.1.20       ---                ---
```

Quelle est la traduction de l'adresse d'hôte local interne ?

192.168.1.20 = _____

Qui est chargé d'attribuer l'adresse globale interne ?

_____

Qui est chargé d'attribuer l'adresse locale interne ?

_____

b. À partir de PC-A, envoyez une requête ping à l'interface Lo0 (192.31.7.1) sur le routeur ISP. Si la requête ping échoue, dépannez et corrigez les problèmes. Sur le routeur de passerelle, affichez la table NAT.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.225:1 192.168.1.20:1     192.31.7.1:1       192.31.7.1:1
--- 209.165.200.225    192.168.1.20       ---                ---
```

Une entrée NAT a été ajoutée à la table avec ICMP répertorié en guise de protocole lorsque PC-A a envoyé une requête ICMP (ping) vers 192.31.7.1 sur le routeur ISP.

Quel numéro de port a été utilisé dans cet échange ICMP ? _____

Remarque : il peut être nécessaire de désactiver le pare-feu de PC-A pour que les requêtes ping puissent aboutir.

c. À partir de PC-A, envoyez une requête Telnet vers l'interface Lo0 du routeur ISP et affichez la table NAT.

```
Pro Inside global        Inside local       Outside local      Outside global
icmp 209.165.200.225:1   192.168.1.20:1     192.31.7.1:1       192.31.7.1:1
tcp 209.165.200.225:1034 192.168.1.20:1034  192.31.7.1:23      192.31.7.1:23
--- 209.165.200.225      192.168.1.20       ---                ---
```

Remarque : la fonction NAT de la requête ICMP a peut-être expiré et été supprimée de la table NAT.

Quel est le protocole utilisé dans cette traduction ? _____

Quels sont les numéros de port utilisés ?

Global / local interne : _____

Global / local externe : _____

d. Étant donné que la fonction NAT statique a été configurée pour PC-A, vérifiez que l'envoi d'une requête ping à partir du routeur ISP vers PC-A à l'adresse publique NAT statique (209.165.200.225) a réussi.

e. Sur le routeur de passerelle, affichez la table NAT afin de vérifier la traduction.

```
Gateway# show ip nat translations
Pro Inside global       Inside local       Outside local      Outside global
icmp 209.165.200.225:12 192.168.1.20:12    209.165.201.17:12  209.165.201.17:12
--- 209.165.200.225     192.168.1.20       ---                ---
```

Notez que les adresses locales et globales externes sont identiques. Cette adresse est l'adresse source du réseau distant du routeur ISP. Afin de garantir le succès de la requête ping issue du routeur ISP, l'adresse NAT statique globale interne 209.165.200.225 a été traduite en l'adresse locale interne de PC-A (192.168.1.20).

f. Vérifiez les statistiques NAT à l'aide de la commande **show ip nat statistics** sur le routeur de passerelle.

```
Gateway# show ip nat statics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Peak translations: 2, occurred 00:02:12 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 39  Misses: 0
CEF Translated packets: 39, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Remarque : ceci n'est qu'un exemple de résultat. Le résultat que vous obtenez peut ne pas correspondre exactement.

Partie 3: Configuration et vérification de la fonction NAT dynamique

La NAT dynamique utilise un pool d'adresses publiques et les attribue selon la méthode du premier arrivé, premier servi. Lorsqu'un périphérique interne demande l'accès à un réseau externe, la NAT dynamique attribue une adresse IPv4 publique disponible du pool. La fonction NAT dynamique se traduit par un mappage d'adresses de type « plusieurs vers plusieurs » entre les adresses locales et globales.

Étape 1: Effacez les traductions NAT.

Avant de procéder à l'ajout de traductions NAT dynamiques, effacez les traductions NAT ainsi que les statistiques de la Partie 2.

```
Gateway# clear ip nat translation *
Gateway# clear ip nat statistics
```

Étape 2: Définissez une liste de contrôle d'accès correspondant à la plage d'adresses IP privées du LAN.

La liste de contrôle d'accès 1 est utilisée pour permettre la traduction du réseau 192.168.1.0/24.

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

Étape 3: Vérifiez que les configurations d'interface NAT sont toujours valides.

Exécutez la commande **show ip nat statistics** sur le routeur de passerelle afin de vérifier les configurations NAT.

Étape 4: Définissez le pool d'adresses IP publiques utilisables.

```
Gateway(config)# ip nat pool public_access 209.165.200.242 209.165.200.254
netmask 255.255.255.224
```

Étape 5: Définissez la NAT à partir de la liste source interne vers le groupe externe.

Remarque : rappelez-vous que les noms de pool NAT sont sensibles à la casse et que le nom de pool entré ici doit correspondre à celui utilisé à l'étape précédente.

```
Gateway(config)# ip nat inside source list 1 pool public_access
```

Étape 6: Testez la configuration.

a. À partir de PC-B, envoyez une requête ping à l'interface Lo0 (192.31.7.1) sur le routeur ISP. Si la requête ping échoue, dépannez et corrigez les problèmes. Sur le routeur de passerelle, affichez la table NAT.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.225    192.168.1.20       ---                ---
icmp 209.165.200.242:1 192.168.1.21:1     192.31.7.1:1       192.31.7.1:1
--- 209.165.200.242    192.168.1.21       ---                ---
```

Quelle est la traduction de l'adresse d'hôte local interne de PC-B ?

192.168.1.21 = _____

Une entrée NAT dynamique a été ajoutée à la table avec ICMP répertorié en guise de protocole lorsque PC-B a envoyé un message ICMP vers 192.31.7.1 sur le routeur ISP.

Quel numéro de port a été utilisé dans cet échange ICMP ? _____

b. À partir de PC-B, ouvrez un navigateur et entrez l'adresse IP du serveur Web simulé ISP (interface Lo0). Lorsque vous y êtes invité, connectez-vous en tant que **webuser** avec le mot de passe **webpass**.

c. Affichez la table NAT.

```
Pro Inside global        Inside local       Outside local      Outside global
--- 209.165.200.225      192.168.1.20       ---                ---
tcp 209.165.200.242:1038 192.168.1.21:1038 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1039 192.168.1.21:1039 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1040 192.168.1.21:1040 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1041 192.168.1.21:1041 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1042 192.168.1.21:1042 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1043 192.168.1.21:1043 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1044 192.168.1.21:1044 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1045 192.168.1.21:1045 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1046 192.168.1.21:1046 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1047 192.168.1.21:1047 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1048 192.168.1.21:1048 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1049 192.168.1.21:1049 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1050 192.168.1.21:1050 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1051 192.168.1.21:1051 192.31.7.1:80     192.31.7.1:80
```

```
tcp 209.165.200.242:1052 192.168.1.21:1052 192.31.7.1:80     192.31.7.1:80
--- 209.165.200.242    192.168.1.22       ---                ---
```

Quel protocole a été utilisé dans cette traduction ? _____

Quels sont les numéros de port utilisés ?

Interne : _____

Externe : _____

Quel numéro de port réservé et quel service ont été utilisés ? _____

d. Vérifiez les statistiques NAT à l'aide de la commande **show ip nat statistics** sur le routeur de passerelle.

```
Gateway# show ip nat statistics
Total active translations: 3 (1 static, 2 dynamic; 1 extended)
Peak translations: 17, occurred 00:06:40 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 345  Misses: 0
CEF Translated packets: 345, CEF Punted packets: 0
Expired translations: 20
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 2
 pool public_access: netmask 255.255.255.224
        start 209.165.200.242 end 209.165.200.254
        type generic, total addresses 13, allocated 1 (7%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Remarque : ceci n'est qu'un exemple de résultat. Le résultat que vous obtenez peut ne pas correspondre exactement.

Étape 7: Supprimez l'entrée NAT statique.

À l'étape 7, l'entrée NAT statique est supprimée et vous pouvez observer l'entrée NAT.

a. Supprimez la traduction NAT statique de la Partie 2. Saisissez **Oui** lorsque vous êtes invité à supprimer des entrées enfant.

```
Gateway(config)# no ip nat inside source static 192.168.1.20 209.165.200.225

Static entry in use, do you want to delete child entries? [no]: yes
```

b. Effacez les traductions NAT ainsi que les statistiques.

c. Envoyez une requête ping au routeur ISP (192.31.7.1) à partir des deux hôtes.

d. Affichez la table NAT et les statistiques.

```
Gateway# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
```

```
Peak translations: 15, occurred 00:00:43 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 16  Misses: 0
CEF Translated packets: 285, CEF Punted packets: 0
Expired translations: 11
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 4
 pool public_access: netmask 255.255.255.224
        start 209.165.200.242 end 209.165.200.254
        type generic, total addresses 13, allocated 2 (15%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0

Gateway# show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.243:512 192.168.1.20:512 192.31.7.1:512     192.31.7.1:512
--- 209.165.200.243    192.168.1.20       ---                ---
icmp 209.165.200.242:512 192.168.1.21:512 192.31.7.1:512     192.31.7.1:512
--- 209.165.200.242    192.168.1.21       ---                ---
```

Remarque : ceci n'est qu'un exemple de résultat. Le résultat que vous obtenez peut ne pas correspondre exactement.

Remarques générales

1. Pourquoi utiliser la fonction NAT dans un réseau ?

   _____

   _____

   _____

2. Quelles sont les limites de la fonction NAT ?

   _____

   _____

   _____

Tableau récapitulatif des interfaces de routeur

Résumé des interfaces de routeur				
Modèle du routeur	**Interface Ethernet 1**	**Interface Ethernet 2**	**Interface série 1**	**Interface série 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

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 combinaisons possibles des interfaces Ethernet et série dans le périphérique. Ce tableau 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 de Cisco IOS.