

Travaux pratiques : configuration de la traduction d'adresses de port (PAT)

Topologie

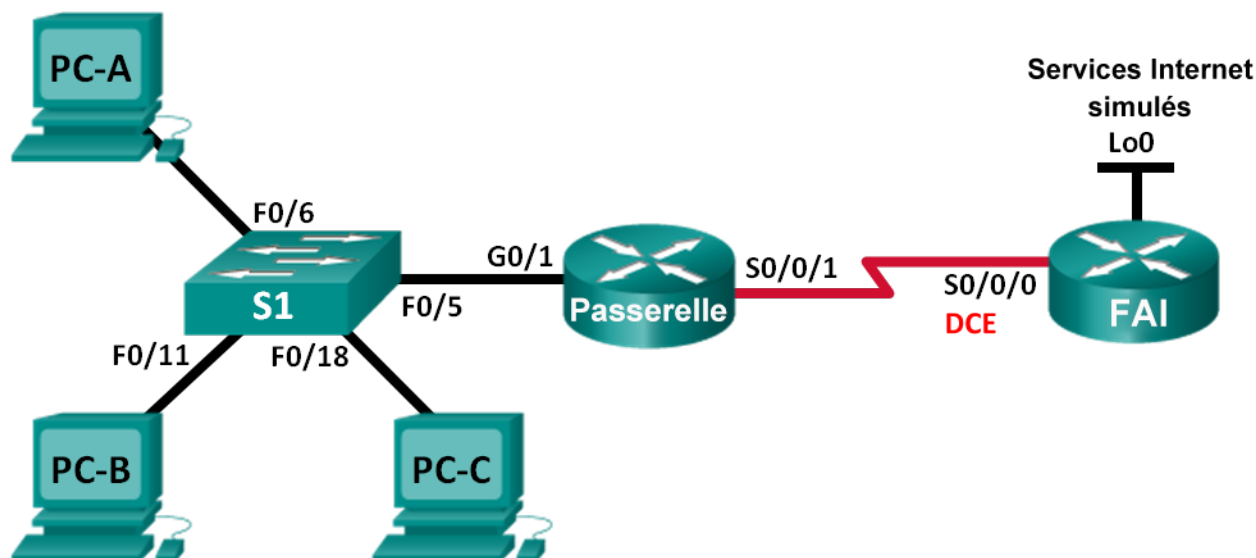


Table d'adressage

Appareil	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 (ETCD)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A	Carte réseau	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	Carte réseau	192.168.1.21	255.255.255.0	192.168.1.1
PC-C	Carte réseau	192.168.1.22	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 surcharge de pool NAT

Partie 3 : configuration et vérification de la PAT

Contexte/scénario

Dans la Partie 1 de ces travaux pratiques, votre fournisseur d'accès Internet (FAI) alloue la plage d'adresses IP publiques 209.165.200.224/29 à votre entreprise. Cela permet à votre entreprise de posséder six adresses IP publiques. La surcharge de pool NAT dynamique utilise un pool d'adresses IP dans une relation de type « plusieurs vers plusieurs ». Le routeur utilise la première adresse IP du pool et attribue des connexions à l'aide de cette adresse IP et d'un numéro de port unique. Une fois que le nombre maximal de traductions pour une même adresse IP a été atteint sur le routeur (en fonction de la plate-forme et du matériel), il utilise l'adresse IP suivante du pool. La surcharge de pool NAT est une forme de traduction d'adresses de port (PAT) qui surcharge un groupe d'adresses IPv4 publiques.

Dans la Partie 2, le fournisseur d'accès Internet (FAI) a attribué une adresse IP unique, à savoir 209.165.201.18, à votre entreprise en vue d'une utilisation sur la connexion Internet à partir du routeur de passerelle de l'entreprise vers le FAI. Vous utiliserez la traduction d'adresses de port (PAT) pour convertir plusieurs adresses internes en une adresse publique utilisable. Vous testerez, afficherez et vérifierez les traductions, et interpréterez les statistiques NAT/PAT pour contrôler le processus.

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 2960 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 formateur.

Ressources requises

- 2 routeurs (Cisco 1941 équipés 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)
- 3 PC (Windows 7, Vista ou XP, équipés d'un programme d'émulation de 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 indiquée.

Étape 2 : Configurez les PC hôtes.

Étape 3 : Initialisez et redémarrez les routeurs et les commutateurs.

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

- Accédez au routeur par la console et passez en mode de configuration globale.
- Copiez la configuration de base suivante et collez-la dans la configuration en cours sur le routeur.

```
no ip domain-lookup
service password-encryption
```

```
enable secret class
banner motd #
Unauthorized access is strictly prohibited. (Accès sans autorisation
strictement interdit.) #
Line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

- c. Configurez le nom d'hôte comme illustré dans la topologie.
- d. Copier la configuration en cours en tant que configuration de démarrage

Étape 5 : Configurez le routage statique.

- a. Créez une route statique depuis le routeur ISP jusqu'au routeur de passerelle.
`ISP(config)# ip route 209.165.200.224 255.255.255.248 209.165.201.18`
- b. Créez une route par défaut sur le routeur de passerelle vers le routeur FAI.
`Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17`

Étape 6 : Vérifier 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. Vérifiez que les routes statiques sont configurées correctement sur les deux routeurs.

Partie 2 : Configuration et vérification de surcharge de pool NAT

Dans la Partie 2, vous allez configurer le routeur de passerelle de manière à traduire les adresses IP du réseau 192.168.1.0/24 en l'une des six adresses utilisables de la plage 209.165.200.224/29.

Étape 1 : Définissez une liste de contrôle d'accès correspondant aux 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 2 : Définissez le pool d'adresses IP publiques utilisables.

```
Gateway(config)# ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
```

Étape 3 : Définissez la NAT à partir de la liste source interne vers le groupe externe.

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

Étape 4 : 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 5 : Vérifiez la configuration de surcharge de pool NAT.

- À partir de chaque PC hôte, envoyez une requête ping à l'adresse 192.31.7.1 sur le routeur ISP.
- Affichez les statistiques NAT sur le routeur de passerelle.

```
Gateway# show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 00:00:25 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 24 Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 3
  pool public_access: netmask 255.255.255.248
    start 209.165.200.225 end 209.165.200.230
    type generic, total addresses 6, allocated 1 (16%), misses 0

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

- Affichez les NAT sur le routeur de passerelle.

```
Gateway# show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:0 192.168.1.20:1    192.31.7.1:1      192.31.7.1:0
icmp 209.165.200.225:1 192.168.1.21:1    192.31.7.1:1      192.31.7.1:1
icmp 209.165.200.225:2 192.168.1.22:1    192.31.7.1:1      192.31.7.1:2
```

Remarque : en fonction du temps écoulé depuis que vous avez effectué les requêtes ping à partir de chaque PC, il se peut que vous ne puissiez pas voir les trois traductions. Les traductions ICMP présentent un délai d'expiration court.

Combien d'adresses IP locales internes sont répertoriées dans l'exemple de résultat ci-dessus ? _____

Combien d'adresses IP globales internes sont répertoriées ? _____

Combien de numéros de port sont jumelés avec les adresses globales internes ? _____

Quel serait le résultat obtenu en cas d'envoi d'une requête ping à l'adresse locale interne de PC-A à partir du routeur ISP ? Pourquoi ?

Partie 3 : Configuration et vérification de la fonction PAT

Dans la Partie 3, vous allez configurer la fonction PAT en utilisant une interface au lieu d'un pool d'adresses pour définir l'adresse externe. Toutes les commandes de la Partie 2 ne seront pas réutilisées dans la Partie 3.

Étape 1 : Effacez les NAT et les statistiques sur le routeur de passerelle.

Étape 2 : Vérifiez la configuration NAT.

- Vérifiez que les statistiques ont été effacées.
- Vérifiez que les interfaces internes et externes sont configurées pour les NAT.
- Vérifiez que la liste de contrôle d'accès est toujours configurée pour les NAT.

Quelle commande avez-vous utilisée pour confirmer les résultats des étapes A à C ?

Étape 3 : Supprimez le pool des adresses IP publiques utilisables.

```
Gateway(config)# no ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
```

Étape 4 : Supprimez la traduction NAT depuis la liste source interne vers le pool externe.

```
Gateway(config)# no ip nat inside source list 1 pool public_access overload
```

Étape 5 : Associez la liste source à l'interface externe.

```
Gateway(config)# ip nat inside source list 1 interface serial 0/0/1 overload
```

Étape 6 : Testez la configuration PAT.

- À partir de chaque PC, envoyez une requête ping à l'adresse 192.31.7.1 sur le routeur ISP.
- Affichez les statistiques NAT sur le routeur de passerelle.

```
Gateway# show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 00:00:19 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 24 Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 2] access-list 1 interface Serial0/0/1 refcount 3

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

- c. Affichez les traductions NAT sur la passerelle.

```
Gateway# show ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.201.18:3	192.168.1.20:1	192.31.7.1:1	192.31.7.1:3
icmp	209.165.201.18:1	192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
icmp	209.165.201.18:4	192.168.1.22:1	192.31.7.1:1	192.31.7.1:4

Remarques générales

Quels sont les avantages de la fonction PAT ?

Tableau récapitulatif des interfaces des routeurs

Résumé 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)	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 différentes combinaisons d'interfaces Ethernet et série possibles 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 Cisco IOS.				