

SOMMAIRE

Partie 1 : création du réseau et vérification de la connectivité.....	2
Étape 4: Configurez les paramètres de base pour chaque routeur.....	2
Étape 5: Creation d'un serveur Web.....	3
Étape 6: Configurez le routage statique.....	3
Étape 7: Vérifiez la connectivité du réseau.....	4
Partie 2 : configuration et vérification de la fonction NAT statique.....	5
Étape 1: Configurez un mappage statique.....	5
Étape 2: Indiquez les interfaces.....	5
Étape 3: Testez la configuration.....	5
Partie 3 : configuration et vérification de la fonction NAT dynamique.....	7
Étape 1: Effacez les traductions NAT.....	7
Étape 2: Définissez une liste de contrôle d'accès correspondant à la plage d'adresses IP privées du LAN.....	7
Étape 3: Vérifiez que les configurations d'interface NAT sont toujours valides.....	7
Étape 4: Définissez le pool d'adresses IP publiques utilisables.....	8
Étape 5: Définissez la NAT à partir de la liste source interne vers le groupe externe.....	8
Étape 6: Testez la configuration.....	8
Étape 7: Supprimez l'entrée NAT statique.....	9

Partie 1 : création du réseau et vérification de la connectivité

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

a. Désactiver la recherche Dns et Configuration du nom du périphérique conformément à la topologie.

```
Enter configuration commands, one per line. End with CNF
Router(config)#no ip domain loo
Router(config)#no ip domain lookup
Router(config)#host gateway
gateway(config)#int g0/1
gateway(config-if)#ip add 192.168.1.1 255.255.255.0
gateway(config-if)#no shut
```

b. Configuration des 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.

```
gateway#sh ip int br
Interface                IP-Address      OK? Method Status        Protocol
GigabitEthernet0/0      unassigned      YES unset  administratively down  down
GigabitEthernet0/1      192.168.1.1    YES manual  up            up
Serial10/0/0            unassigned      YES manual  down         down
Serial10/0/1            209.165.201.18 YES manual  up            up
Vlan1                   unassigned      YES unset  administratively down  down
gateway#
```

Router ISP

```
Router#conf t
Enter configuration commands, one per line. End with CNF
Router(config)#no ip domain loo
Router(config)#no ip domain lookup
Router(config)#hos
Router(config)#hostname ISP
```

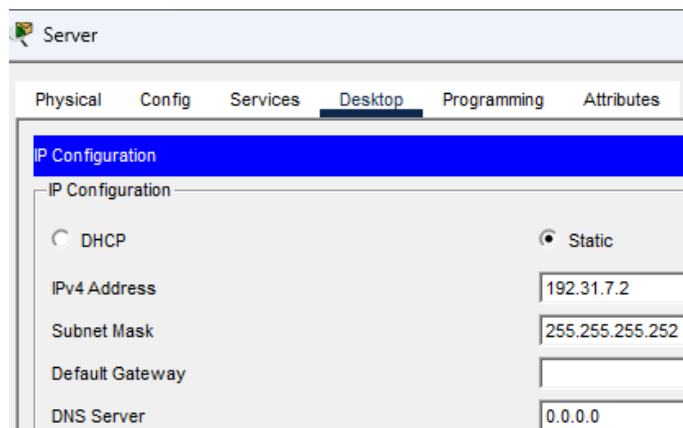
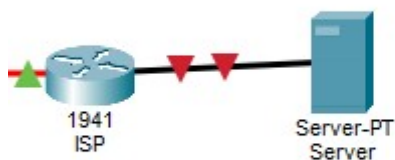
Configuration de fonction NAT dynamique et statique

g0/0 est la liaison avec le serveur

```
sh ip int br
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0      192.31.7.1     YES manual  down       down
GigabitEthernet0/1      unassigned     YES unset   administratively down down
Serial0/0/0             209.165.201.17 YES manual  down       down
Serial0/0/1             unassigned     YES unset   administratively down down
Vlan1                   unassigned     YES unset   administratively down down
ISP#
```

Étape 5: Creation d'un serveur Web

Ajouter un serveur avec l'adresse 192.31.7.2/30



Étape 6: Configurez le routage statique.

a. Création d'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.

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

b. Création d'une route par défaut sur le routeur de passerelle vers le routeur ISP.

```
ISP(config)#ip route 200.165.200.224 255.255.255.224 209.165.201.18
ISP(config)#^Z
```

Étape 7: Vérifiez la connectivité du réseau.

a. À partir des deux hôtes PC, j'ai envoyé un ping sur l'interface G0/1 sur le routeur de passerelle. Les deux ping ont marché confirmant la présence de connectivité.

Configuration de fonction NAT dynamique et statique

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

b. Affichage des 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.

```
Gateway of last resort is not set

  200.165.200.0/27 is subnetted, 1 subnets
S    200.165.200.224/27 [1/0] via 209.165.201.18
  209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.201.16/30 is directly connected, Serial0/0/0
L    209.165.201.17/32 is directly connected, Serial0/0/0

ISP#
```

```
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/1
L    192.168.1.1/32 is directly connected, GigabitEthernet0/1
  209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.201.16/30 is directly connected, Serial0/0/1
L    209.165.201.18/32 is directly connected, Serial0/0/1
S*   0.0.0.0/0 [1/0] via 209.165.201.17

gateway#
```

Partie 2 : configuration et vérification de la fonction NAT statique

Étape 1: Configurez un mappage statique.

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#conf t
Enter configuration commands, one per line. End with CNTL/Z.
gateway(config)#ip nat inside source static 192.168.1.20 209.165.200.225
gateway(config)#
```

Étape 2: Indiquez les interfaces.

Exécuter les commandes ip nat inside sur l'interface g0/1 et ip nat outside pour l'interface s0/0/1.

Configuration de fonction NAT dynamique et statique

```
gateway(config)#int g0/1
gateway(config-if)#ipna
gateway(config-if)#ip na
gateway(config-if)#ip nat inside
gateway(config-if)#int s0/0/1
gateway(config-if)#ip nat outside
gateway(config-if)#
```

Étape 3: Testez la configuration.

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

```
gateway#sh ip nat translatio
gateway#sh ip nat translations
Pro  Inside global  Inside local  Outside local  Outside global
---  209.165.200.225  192.168.1.20  ---            ---
gateway#
```

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

192.168.1.20 = 209.165.200.225

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

Le routeur du pool NAT.

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

L'administrateur de la station de travail.

b. À partir de PC-A, j'envoie une requête ping à l'interface server (192.31.7.2).

```
C:\>ping 192.31.7.2

Pinging 192.31.7.2 with 32 bytes of data:

Reply from 192.31.7.2: bytes=32 time=7ms TTL=126
Reply from 192.31.7.2: bytes=32 time=4ms TTL=126
Reply from 192.31.7.2: bytes=32 time=4ms TTL=126
Reply from 192.31.7.2: bytes=32 time=6ms TTL=126

Ping statistics for 192.31.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 7ms, Average = 5ms
```

Sur le routeur de passerelle, on affiche la table NAT.

```
gateway#show ip nat translations
Pro  Inside global  Inside local  Outside local  Outside global
icmp 209.165.200.225:45 192.168.1.20:45 192.31.7.2:45 192.31.7.2:45
icmp 209.165.200.225:46 192.168.1.20:46 192.31.7.2:46 192.31.7.2:46
icmp 209.165.200.225:47 192.168.1.20:47 192.31.7.2:47 192.31.7.2:47
icmp 209.165.200.225:48 192.168.1.20:48 192.31.7.2:48 192.31.7.2:48
--- 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 192.31.7.2 .

Quel numéro de port a été utilisé dans cet échange ICMP ? 45 mais les réponses peuvent varier.

Configuration de fonction NAT dynamique et statique

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

```
gateway#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:0 192.168.1.20:0    209.165.201.17:0  209.165.201.17:0
--- 209.165.200.225    192.168.1.20     ---                ---
tcp 209.165.200.225:1025 192.168.1.20:1025 192.131.7.2:23    192.131.7.2:23
```

Quel est le protocole utilisé dans cette traduction ? tcp

Quels sont les numéros de port utilisés ?

Global / local interne : 1025

les réponses peuvent varier. Global / local externe : 23

d. vérifier 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 réussi

```
ISP>en
ISP#ping 209.165.200.225

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/5 ms
```

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

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

```
gateway#sh ip nat sta
gateway#sh ip nat statistics
Total translations: 3 (1 static, 2 dynamic, 2 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 67 Misses: 53
Expired translations: 51
Dynamic mappings:
gateway#
gateway#
gateway#
```

Partie 3 : configuration et vérification de la fonction NAT dynamique

Étape 1: Effacez les traductions NAT

Avant de procéder à l'ajout de traductions NAT dynamiques, il faut effacer les traductions NAT de la Partie 2.

```
gateway#clear ip na
gateway#clear ip nat tr
gateway#clear ip nat translation ?
* Deletes all dynamic translations
gateway#clear ip nat translation *
gateway#
```

Configuration de fonction NAT dynamique et statique

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

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

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

```
sh ip nat sta
gateway#sh ip nat statistics
gateway#sh ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 67 Misses: 53
Expired translations: 51
Dynamic mappings:
gateway#
```

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

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

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

Étape 6: Testez la configuration.

a. À partir de PC-B, envoyer une requête ping à l'interface du serveur . Sur le routeur de passerelle, affichez la table NAT.

```
C:\>ping 192.31.7.2

Pinging 192.31.7.2 with 32 bytes of data:

Reply from 192.31.7.2: bytes=32 time=19ms TTL=126
Reply from 192.31.7.2: bytes=32 time=11ms TTL=126
Reply from 192.31.7.2: bytes=32 time=9ms TTL=126
Reply from 192.31.7.2: bytes=32 time=11ms TTL=126

Ping statistics for 192.31.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 19ms, Average = 12ms

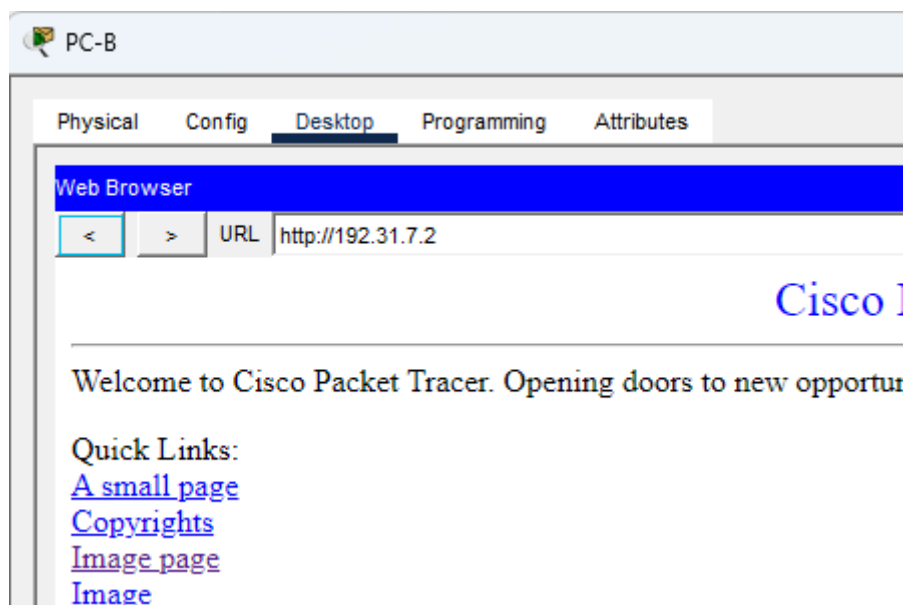
C:\>
```

Configuration de fonction NAT dynamique et statique

```
gateway#sh ip nat translations
gateway#
%SYS-5-CONFIG_I: Configured from console by console
sh ip nat translations
Pro  Inside global      Inside local      Outside local     Outside global
icmp 209.165.200.242:10192.168.1.21:10 192.31.7.2:10    192.31.7.2:10
icmp 209.165.200.242:11192.168.1.21:11 192.31.7.2:11    192.31.7.2:11
icmp 209.165.200.242:12192.168.1.21:12 192.31.7.2:12    192.31.7.2:12
```

Quelle est la traduction de l'adresse d'hôte local interne de PC-B ? 192.168.1.21 = 209.165.200.242
Quel numéro de port a été utilisé dans cet échange ICMP ? 11, mais sa peut varier.

b. À partir de PC-B, on ouvre un navigateur et entre l'adresse IP du serveur Web



c. Affichage de la table NAT.

```
gateway#sh ip nat trans
gateway#sh ip nat translations
Pro  Inside global      Inside local      Outside local     Outside global
---  209.165.200.225    192.168.1.20     ---              ---
:cp  209.165.200.242:1025192.168.1.21:1025 192.31.7.2:80    192.31.7.2:80
:cp  209.165.200.242:1026192.168.1.21:1026 192.31.7.9:80    192.31.7.9:80
:cp  209.165.200.242:1027192.168.1.21:1027 192.31.7.9:80    192.31.7.9:80
:cp  209.165.200.242:1028192.168.1.21:1028 192.31.7.9:80    192.31.7.9:80
:cp  209.165.200.242:1029192.168.1.21:1029 192.31.7.9:80    192.31.7.9:80
:cp  209.165.200.242:1030192.168.1.21:1030 192.31.7.2:80    192.31.7.2:80
:cp  209.165.200.242:1031192.168.1.21:1031 192.31.7.2:80    192.31.7.2:80
:cp  209.165.200.242:1032192.168.1.21:1032 192.31.7.2:80    192.31.7.2:80
:cp  209.165.200.242:1033192.168.1.21:1033 192.31.7.2:80    192.31.7.2:80
:cp  209.165.200.242:1034192.168.1.21:1034 192.31.7.2:80    192.31.7.2:80
```

```
gateway#
```

Quel protocole a été utilisé dans cette traduction ? tcp

Quels sont les numéros de port utilisés ? Interne : de 1025 à 1034.

Externe : 80

Quel numéro de port réservé et quel service ont été utilisés ? port 80 http

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

```
gateway#sh ip nat statistics
Total translations: 11 (1 static, 10 dynamic, 10 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 118 Misses: 23
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 10
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
```

Configuration de fonction NAT dynamique et statique

Étape 7: Supprimez l'entrée NAT statique.

a. Supprimer la traduction NAT statique de la Partie 2. Saisissez **Oui** lorsque nous somme invité à supprimer des entrées enfant et Effacer les traductions NAT ainsi que les statistiques.

```
gateway#clear ip nat translation *
gateway#conf t
Enter configuration commands, one per line. End with CNTL/Z.
gateway(config)#no ip nat inside source static 192.168.1.20 209.165.200.225
```

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

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=7ms TTL=254
Reply from 192.31.7.1: bytes=32 time=7ms TTL=254
Reply from 192.31.7.1: bytes=32 time=7ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 7ms, Average = 5ms

C:\>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.31.7.1

Pinging 192.31.7.1 with 32 bytes of data:

Reply from 192.31.7.1: bytes=32 time=9ms TTL=254
Reply from 192.31.7.1: bytes=32 time=12ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254
Reply from 192.31.7.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.31.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 5ms
```

d. Afficher la table NAT et les statistiques.

```
gateway#sh ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/1
Inside Interfaces: GigabitEthernet0/1
Hits: 126 Misses: 31
Expired translations: 8
Dynamic mappings:
-- Inside Source
access-list 1 pool public_access refCount 0
 pool public_access: netmask 255.255.255.224
   start 209.165.200.242 end 209.165.200.254
   type generic, total addresses 13 , allocated 0 (0%), misses 0
gateway#
```

```
gateway#sh ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.244:10192.168.1.21:10 192.31.7.1:10      192.31.7.1:10
icmp 209.165.200.244:11192.168.1.21:11 192.31.7.1:11      192.31.7.1:11
icmp 209.165.200.244:12192.168.1.21:12 192.31.7.1:12      192.31.7.1:12
icmp 209.165.200.244:9 192.168.1.21:9     192.31.7.1:9       192.31.7.1:9
icmp 209.165.200.245:10192.168.1.20:10 192.31.7.1:10      192.31.7.1:10
icmp 209.165.200.245:11192.168.1.20:11 192.31.7.1:11      192.31.7.1:11
icmp 209.165.200.245:12192.168.1.20:12 192.31.7.1:12      192.31.7.1:12
icmp 209.165.200.245:9 192.168.1.20:9     192.31.7.1:9       192.31.7.1:9
gateway#
```

Remarques générales

1. Pourquoi utiliser la fonction NAT dans un réseau ?

Configuration de fonction NAT dynamique et statique

Les réponses peuvent varier, mais elles devraient indiquer : lorsqu'il n'y a pas suffisamment d'adresses IP publiques et pour éviter le coût lié à l'achat d'adresses publiques auprès d'un fournisseur d'accès Internet (FAI). La fonction NAT peut également constituer une mesure de sécurité, car elle masque les adresses internes pour les réseaux externes.

2. Quelles sont les limites de la fonction NAT ?

La fonction NAT a besoin d'informations IP ou d'informations de numéro de port dans l'en-tête IP et l'en-tête TCP des paquets pour la traduction. Voici une liste non exhaustive des protocoles qui ne peuvent pas être utilisés avec la fonction NAT : SNMP, LDAP, Kerberos version 5.