Travaux pratiques 7.4.1 : configuration de base de DHCP et NAT

Diagramme de topologie

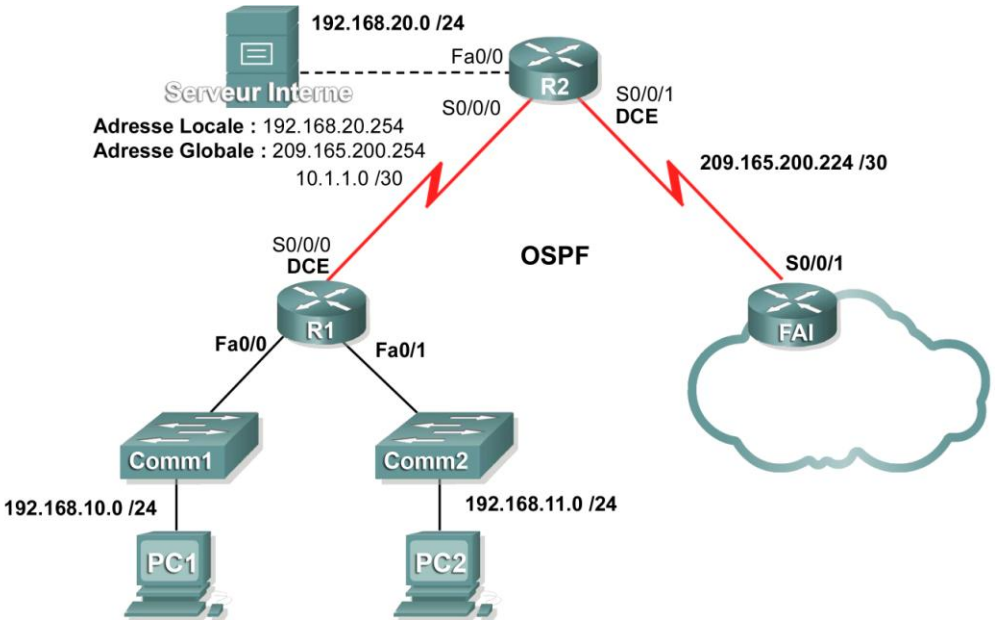


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
R1	S0/0/0	10.1.1.1	255.255.255.252
	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	209.165.200.225	255.255.255.252
	Fa0/0	192.168.20.254	255.255.255.0
FAI	S0/0/1	209.165.200.226	255.255.255.252

Objectifs pédagogiques

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

- Préparer le réseau
- Effectuer des configurations de routeur de base
- Configurer un serveur DHCP Cisco IOS
- Configurer le routage statique et le routage par défaut
- Configurer la fonction NAT statique
- Configurer la fonction NAT dynamique à l'aide d'un pool d'adresses
- Configurer la surcharge de la fonction NAT

Scénario

Au cours de ces travaux pratiques, vous allez configurer les services DHCP et IP NAT. Un routeur joue le rôle de serveur DHCP. L'autre routeur transmet les requêtes DHCP au serveur. Vous apprendrez également à configurer des traductions d'adresses de réseau (NAT) statique et dynamique ainsi que la surcharge de traduction d'adresses de réseau. Une fois les configurations terminées, vous vérifierez la connectivité entre les adresses internes et externes.

Tâche 1 : préparation du réseau

Étape 1 : câblage d'un réseau similaire à celui du diagramme de topologie

Vous pouvez utiliser n'importe quel routeur durant les travaux pratiques, à condition qu'il soit équipé des interfaces indiquées dans la topologie.

Remarque : il est possible que les sorties du routeur ainsi que les descriptions d'interface paraissent différentes si vous utilisez un routeur de type 1700, 2500 ou 2600. Certaines commandes peuvent être différentes ou ne pas exister sur les anciens routeurs.

Étape 2 : suppression de toutes les configurations existantes sur les routeurs

Tâche 2 : exécution des configurations de routeur de base

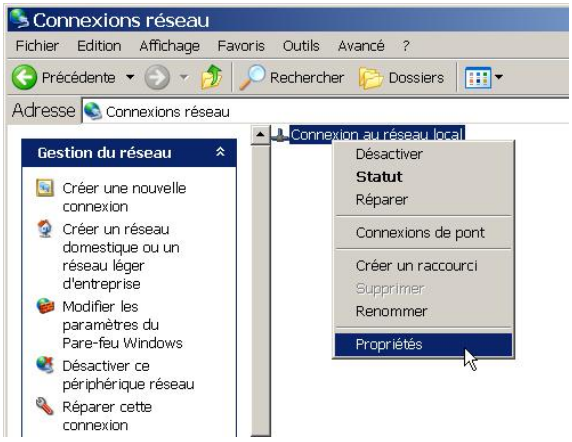
Configurez les routeurs R1, R2 et FAI conformément aux instructions suivantes :

- Configurez le nom d'hôte du périphérique.
- Désactivez la recherche DNS.
- Configurez un mot de passe de mode d'exécution privilégié.
- Configurez une bannière de message du jour.
- Configurez un mot de passe pour les connexions console.
- Configurez un mot de passe pour toutes les connexions de terminaux virtuels (vty).
- Configurez les adresses IP sur tous les routeurs. Plus loin dans cet exercice, les PC se verront attribuer des adresses IP par le service DHCP.
- Activez OSPF en utilisant l'ID de processus 1 sur R1 et R2. N'annoncez pas le réseau 209.165.200.224/27.

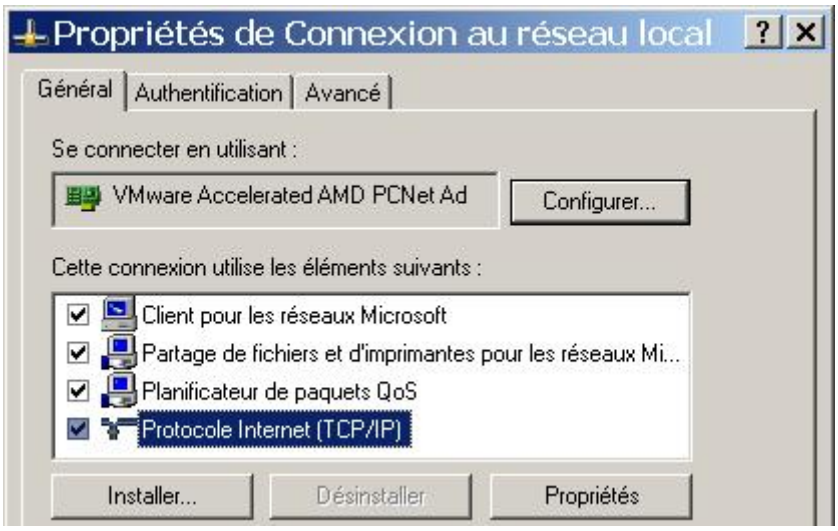
Remarque : au lieu de relier un serveur à R2, vous pouvez configurer une interface de bouclage sur R2 de façon à utiliser l'adresse IP 192.168.20.254/24. De cette façon, il n'est pas nécessaire de configurer l'interface Fast Ethernet.

Tâche 3 : configuration de PC1 et PC2 pour la réception d'une adresse IP via le protocole DHCP

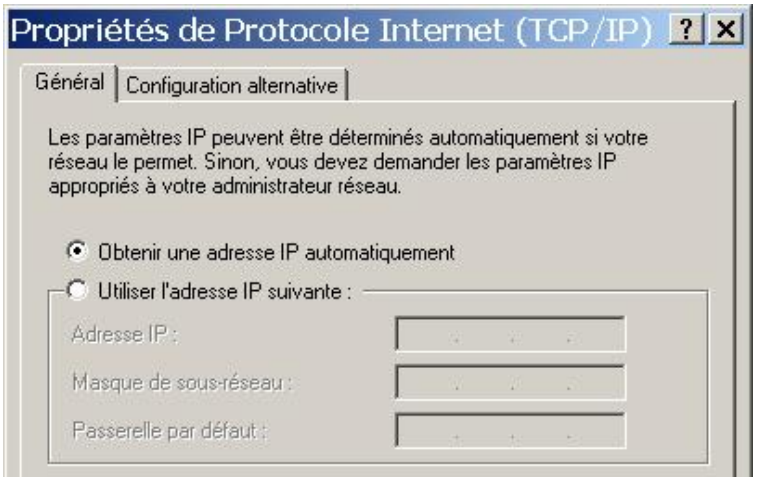
Sur un PC Windows, cliquez sur **Démarrer** -> **Panneau de configuration** -> **Connexions réseau** -> **Connexion au réseau local**. Cliquez avec le bouton droit sur l'icône **Connexion au réseau local** et sélectionnez **Propriétés**.



Faites défiler la page vers le bas et mettez en surbrillance **Protocole Internet (TCP/IP)**. Cliquez sur le bouton **Propriétés**.



Vérifiez que le bouton **Obtenir une adresse IP automatiquement** est sélectionné.



Une fois que ces opérations ont été effectuées pour les ordinateurs PC1 et PC2, ces derniers peuvent recevoir une adresse IP transmise par un serveur DHCP.

Tâche 4 : configuration d'un serveur DHCP Cisco IOS

Le logiciel Cisco IOS prend en charge une configuration de serveur DHCP appelée Easy IP. L'objectif de ces travaux pratiques est que les périphériques présents sur les réseaux 192.168.10.0/24 et 192.168.11.0/24 demandent à R2 des adresses IP via le protocole DHCP.

Étape 1 : exclusion des adresses attribuées de manière statique

Le serveur DHCP suppose que toutes les adresses IP d'un groupe d'adresses DHCP peuvent être affectées à des clients DHCP. Vous devez spécifier les adresses IP que le serveur DHCP ne peut affecter aux clients. Il s'agit généralement d'adresses statiques réservées à l'interface des routeurs, à la console de gestion des commutateurs, aux serveurs et aux imprimantes du réseau local. La commande **ip dhcp excluded-address** empêche le routeur d'attribuer les adresses IP présentes dans la plage configurée. Les commandes suivantes excluent les dix premières adresses IP de chacun des pools des réseaux locaux connectés à R1. Ces adresses ne seront pas affectées à des clients DHCP.

```
R2(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
R2(config)#ip dhcp excluded-address 192.168.11.1 192.168.11.10
```

Étape 2 : configuration du pool

Créez le pool DHCP à l'aide de la commande **ip dhcp pool** et nommez-le **R1Fa0**.

```
R2(config)#ip dhcp pool R1Fa0
```

Spécifiez le sous-réseau à utiliser lors de l'attribution des adresses IP. Les pools DHCP sont associés automatiquement à une interface, en fonction de l'instruction réseau. Le routeur joue désormais le rôle de serveur DHCP et distribue les adresses du sous-réseau 192.168.10.0/24, en commençant par 192.168.10.1.

```
R2(dhcp-config)#network 192.168.10.0 255.255.255.0
```

Configurez le routeur par défaut et le serveur de noms de domaine du réseau. Les clients reçoivent ces paramètres via le protocole DHCP, de même qu'une adresse IP.

```
R2(dhcp-config)#dns-server 192.168.11.5
R2(dhcp-config)#default-router 192.168.10.1
```

Remarque : aucun serveur DNS n'est disponible à l'adresse 192.168.11.5. Cette commande est configurée uniquement à des fins pédagogiques.

Étant donné que les périphériques du réseau 192.168.11.0/24 requièrent également que R2 leur fournissent des adresses, vous devez créer un pool distinct pour répondre à leurs besoins. Les commandes utilisées sont similaires à celles présentées ci-dessus :

```
R2(config)#ip dhcp pool R1Fa1
R2(dhcp-config)#network 192.168.11.0 255.255.255.0
R2(dhcp-config)#dns-server 192.168.11.5
R2(dhcp-config)#default-router 192.168.11.1
```

Étape 3 : test du protocole DHCP

Vérifiez si les ordinateurs PC1 et PC2 ont reçu automatiquement une adresse IP. Sur chaque PC, cliquez sur **Démarrer** -> **Exécuter** -> **cmd** -> **ipconfig**

Quels sont les résultats du test ? _____
Comment interpréter les résultats ? _____

Étape 4 : configuration d'un agent relais DHCP

Les services réseaux tels que le protocole DHCP fonctionnent via les diffusions de couche 2. Si les périphériques fournissant ces services se trouvent sur un sous-réseau différent de celui des clients, ils ne peuvent pas recevoir les paquets de diffusion. Étant donné que le serveur DHCP et les clients DHCP ne figurent pas sur le même sous-réseau, vous devez configurer R1 pour qu'il transmette les messages de diffusion DHCP à R2, qui correspond au serveur DHCP, à l'aide de la commande de configuration d'interface **ip helper-address**.

Notez que la commande **ip helper-address** doit être configurée sur chaque interface concernée.

```
R1(config)#interface fa0/0
R1(config-if)#ip helper-address 10.1.1.2
R1(config)#interface fa0/1
R1(config-if)#ip helper-address 10.1.1.2
```

Étape 5 : émission et renouvellement des adresses IP sur PC1 et PC2

Selon que les PC ont été utilisés ou non dans d'autres travaux pratiques ou que vous les avez connectés ou non à Internet, ils ont peut-être déjà reçu automatiquement une adresse IP transmise par un autre serveur DHCP. Vous devez supprimer cette adresse IP à l'aide des commandes **ipconfig /release** et **ipconfig /renew**.

Étape 6 : vérification de la configuration DHCP

Il existe plusieurs méthodes de vérification de la configuration du serveur DHCP. Exécutez la commande **ipconfig** sur les ordinateurs PC1 et PC2 pour vérifier qu'ils ont reçu une adresse IP de façon dynamique. Vous pouvez ensuite entrer des commandes sur le routeur pour obtenir des informations supplémentaires. La commande **show ip dhcp binding** renvoie des informations sur les adresses DHCP actuellement attribuées. Ainsi, les informations suivantes, renvoyées par la commande, indiquent que l'adresse IP 192.168.10.11 a été associée à l'adresse MAC 3031.632e.3537.6563. Le bail IP expire le 14 septembre 2007 à 19:33:00.

```
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.10.11       0063.6973.636f.2d30.  Sep 14 2007 07:33 PM    Automatic
                    3031.632e.3537.6563.
                    2e30.3634.302d.566c.
                    31
```

La commande **show ip dhcp pool** affiche des informations concernant tous les pools DHCP actuellement configurés sur le routeur. Dans le résultat ci-après, le pool **R1Fa0** est configuré sur R1. L'une des adresses a été louée à partir de ce pool. Le prochain client émettant une demande d'adresse recevra l'adresse 192.168.10.12.

```
R2#show ip dhcp pool
Pool R1Fa0 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                  Leased addresses
 192.168.10.12        192.168.10.1     - 192.168.10.254    1
```

La commande **debug ip dhcp server events** peut s'avérer extrêmement utile pour résoudre les problèmes liés aux baux DHCP avec un serveur DHCP Cisco IOS. Les informations de débogage affichées sur R1 suite à la connexion d'un hôte sont les suivantes. La partie en surbrillance indique que l'adresse 192.168.10.12 et le masque 255.255.255.0 sont attribués au client par le protocole DHCP.

```
*Sep 13 21:04:18.072: DHCPD: Sending notification of DISCOVER:
*Sep 13 21:04:18.072:  DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:  DHCPD: remote id 020a0000c0a80b01010000000000
*Sep 13 21:04:18.072:  DHCPD: circuit id 00000000
*Sep 13 21:04:18.072: DHCPD: Seeing if there is an internally specified pool
class:
*Sep 13 21:04:18.072:  DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:  DHCPD: remote id 020a0000c0a80b01010000000000
*Sep 13 21:04:18.072:  DHCPD: circuit id 00000000
*Sep 13 21:04:18.072: DHCPD: there is no address pool for 192.168.11.1.
*Sep 13 21:04:18.072: DHCPD: Sending notification of DISCOVER:
R1#
*Sep 13 21:04:18.072:  DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:  DHCPD: remote id 020a0000c0a80a01000000000000
*Sep 13 21:04:18.072:  DHCPD: circuit id 00000000
*Sep 13 21:04:18.072: DHCPD: Seeing if there is an internally specified pool
class:
*Sep 13 21:04:18.072:  DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:  DHCPD: remote id 020a0000c0a80a01000000000000
*Sep 13 21:04:18.072:  DHCPD: circuit id 00000000
R1#
*Sep 13 21:04:20.072: DHCPD: Ajout de liaisons à l'arbre de base
(192.168.10.12)
*Sep 13 21:04:20.072: DHCPD: Ajout de liaisons à l'arbre de base
*Sep 13 21:04:20.072: DHCPD: assigned IP address 192.168.10.12 to client
0063.6973.636f.2d30.3031.632e.3537.6563.2e30.3634.302d.566c.31.
*Sep 13 21:04:20.072: DHCPD: Sending notification of ASSIGNMENT:
*Sep 13 21:04:20.072: DHCPD: address 192.168.10.12 mask 255.255.255.0
*Sep 13 21:04:20.072:  DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:20.072:  DHCPD: lease time remaining (secs) = 86400
*Sep 13 21:04:20.076: DHCPD: Sending notification of ASSIGNMENT:
*Sep 13 21:04:20.076: DHCPD: address 192.168.10.12 mask 255.255.255.0
R1#
*Sep 13 21:04:20.076:  DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:20.076:  DHCPD: lease time remaining (secs) = 86400
```

Tâche 5 : configuration du routage statique et du routage par défaut

FAI fait appel au routage statique pour acccéder aux réseaux situés au-delà de R2. Cependant, avant d'envoyer le trafic vers FAI, R2 traduit les adresses privées en adresses publiques. Par conséquent, il est nécessaire de configurer sur FAI les adresses publiques impliquées dans la configuration de la traduction d'adresses de réseau de R2. Indiquez la route statique suivante sur FAI :

```
FAI(config)#ip route 209.165.200.240 255.255.255.240 serial 0/0/1
```

Cette route statique comprend toutes les adresses à usage publique attribuées à R2.

Configurez une route par défaut sur R2 et propagez-la dans OSPF.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
R2(config)#router ospf 1
R2(config-router)#default-information originate
```

Attendez que R1 apprenne la route par défaut transmise par R2, puis consultez la table de routage de R1. Vous pouvez également supprimer le contenu de la table de routage à l'aide de la commande **clear ip route** *. Une route par défaut pointant vers R2 doit figurer dans la table de routage de R1. À partir de R1, envoyez une requête ping vers l'interface série 0/0/1 de FAI (209 165 200 226). En principe, cette requête ping doit aboutir. Envisagez un dépannage en cas d'échec.

Tâche 6 : configuration de la traduction d'adresses de réseau (NAT) statique

Étape 1 : mappage statique d'une adresse IP publique à une adresse IP privée

Les hôtes externes situés derrière FAI peuvent accéder au serveur interne connecté à R2. Désignez de manière statique l'adresse IP publique 209.165.200.254 comme adresse à utiliser lors de la traduction d'adresses de réseau pour associer les paquets à l'adresse IP privée du serveur interne, à l'adresse 192.168.20.254.

```
R2(config)#ip nat inside source static 192.168.20.254 209.165.200.254
```

Étape 2 : désignation des interfaces de traduction d'adresses de réseau internes et externes

Pour que la traduction d'adresses de réseau puisse fonctionner, vous devez désigner les interfaces internes et les interfaces externes.

```
R2(config)#interface serial 0/0/1
R2(config-if)#ip nat outside
R2(config-if)#interface fa0/0
R2(config-if)#ip nat inside
```

Remarque : si vous utilisez un serveur interne simulé, affectez la commande **ip nat inside** à l'interface de bouclage.

Étape 3 : vérification de la configuration de la traduction d'adresses de réseau statique

À partir d'FAI, envoyez une requête ping vers l'adresse IP publique 209.165.200.254.

Tâche 7 : configuration d'un pool d'adresses pour la traduction d'adresses de réseau dynamique

Tandis que la fonction NAT statique fournit un mappage permanent entre une adresse interne et une adresse publique spécifique, la fonction NAT dynamique mappe des adresses IP privées avec des adresses publiques. Ces adresses IP publiques proviennent d'un pool NAT (pool de traduction d'adresses de réseau).

Étape 1 : définition d'un pool d'adresses globales

Créez un pool d'adresses à utiliser pour la traduction des adresses source correspondantes. La commande suivante crée un pool appelé MY-NAT-POOL, qui convertit les adresses correspondantes en une adresse IP disponible dans la plage 209.165.200.241 - -209 165 200 246.

```
R2(config)#ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
```

Étape 2 : création d'une liste de contrôle d'accès étendue permettant d'identifier les adresses internes traduites

```
R2(config)#ip access-list extended NAT
R2(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 any
R2(config-ext-nacl)#permit ip 192.168.11.0 0.0.0.255 any
```

Étape 3 : établissement d'une traduction de source dynamique par association du pool à la liste de contrôle d'accès

Un routeur peut disposer de plusieurs pools de traduction d'adresses de réseau et de plusieurs listes de contrôle d'accès. La commande suivante indique au routeur le pool d'adresses qui doit être utilisé pour convertir les hôtes autorisés par la liste de contrôle d'accès.

```
R2(config)#ip nat inside source list NAT pool MY-NAT-POOL
```

Étape 4 : désignation des interfaces de traduction d'adresses de réseau internes et externes

Vous avez déjà désigné les interfaces internes et externes de votre configuration de traduction d'adresses de réseau statique. Ajoutez maintenant l'interface série connectée à R1 comme interface interne.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip nat inside
```

Étape 5 : vérification de la configuration

Envoyez une requête ping au routeur FAI à partir de PC1 ou de l'interface Fast Ethernet de R1, en utilisant une commande **ping** étendue. Vérifiez ensuite la fonction NAT en exécutant les commandes **show ip nat translations** et **show ip nat statistics** sur R2.

```
R2#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.241:4 192.168.10.1:4     209.165.200.226:4  209.165.200.226:4
--- 209.165.200.241    192.168.10.1       ---                ---
--- 209.165.200.254    192.168.20.254     ---                ---

R2#show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 0 extended)
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0, Loopback0
Hits: 23  Misses: 3
CEF Translated packets: 18, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:
-- Inside Source
[Id: 1] access-list NAT pool MY-NAT-POOL refcount 1
 pool MY-NAT-POOL: netmask 255.255.255.248
        start 209.165.200.241 end 209.165.200.246
        type generic, total addresses 6, allocated 1 (16%), misses 0
Queued Packets: 0
```

Pour résoudre les problèmes relatifs à la fonction NAT, vous pouvez utiliser la commande **debug ip nat**. Activez la commande de débogage de la fonction NAT et réexécutez la commande ping à partir de PC1.

```
R2#debug ip nat
IP NAT debugging is on
```

```
R2#
*Sep 13 21:15:02.215: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [25]
*Sep 13 21:15:02.231: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [25]
*Sep 13 21:15:02.247: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [26]
*Sep 13 21:15:02.263: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [26]
*Sep 13 21:15:02.275: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [27]
*Sep 13 21:15:02.291: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [27]
*Sep 13 21:15:02.307: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [28]
*Sep 13 21:15:02.323: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [28]
*Sep 13 21:15:02.335: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [29]
*Sep 13 21:15:02.351: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [29]
R2#
```

Tâche 8 : configuration de la surcharge de la fonction NAT

Dans l'exemple précédent, que se passerait-il si vous deviez utiliser un nombre d'adresses IP publiques supérieur aux six adresses autorisées dans le pool ?

_____

Grâce au suivi des numéros de port, la fonction de surcharge de traduction d'adresses de réseau permet à plusieurs utilisateurs internes de réutiliser une adresse IP publique.

Dans le cadre de cette tâche, vous supprimerez le pool et l'instruction de mappage configurés au cours de la tâche précédente. Vous configurerez ensuite la surcharge de traduction d'adresses de réseau sur R2, de manière à ce que toutes les adresses IP internes soient traduites en une adresse associée à l'interface S0/0/1 de R2 lors de la connexion à un périphérique externe.

Étape 1 : suppression du pool de traduction d'adresses de réseau et de l'instruction de mappage

Utilisez les commandes suivantes pour supprimer le pool de traduction d'adresses de réseau et l'association à la liste de contrôle d'accès.

```
R2(config)#no ip nat inside source list NAT pool MY-NAT-POOL
R2(config)#no ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
```

Si vous recevez le message suivant, effacez vos traductions d'adresses de réseau.

```
%Pool MY-NAT-POOL in use, cannot destroy
R2#clear ip nat translation *
```

Étape 2 : configuration de la traduction d'adresses de port sur R2 à l'aide de l'adresse IP publique de l'interface série 0/0/1

La configuration est similaire à une traduction d'adresses de réseau dynamique, mais au lieu d'un pool d'adresses, c'est le mot clé interface qui est utilisé pour identifier l'adresse IP externe. Par conséquent, aucun pool de traduction d'adresses de réseau n'est défini. Le mot clé **overload** permet d'ajouter le numéro de port à la traduction.

Comme vous avez déjà configuré une liste de contrôle d'accès pour identifier les adresses IP internes à traduire ainsi que les interfaces internes et externes, il ne vous reste plus qu'à configurer la commande suivante :

```
R2(config)#ip nat inside source list NAT interface S0/0/1 overload
```

Étape 3 : vérification de la configuration

Envoyez une requête ping au routeur FAI à partir de PC1 ou de l'interface Fast Ethernet de R1, en utilisant une commande **ping** étendue. Vérifiez ensuite la fonction NAT en exécutant les commandes **show ip nat translations** et **show ip nat statistics** sur R2.

```
R2#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.225:6 192.168.10.11:6    209.165.200.226:6  209.165.200.226:6
--- 209.165.200.254    192.168.20.254     ---                ---

R2#show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0, Loopback0
Hits: 48  Misses: 6
CEF Translated packets: 46, CEF Punted packets: 0
Expired translations: 5
Dynamic mappings:
-- Inside Source
[Id: 2] access-list NAT interface Serial0/0/1 refcount 1
Queued Packets: 0
```

Remarque : au cours de la tâche précédente, vous auriez pu ajouter le mot clé **overload** à la commande **ip nat inside source list NAT pool MY-NAT-POOL** pour autoriser plus de six utilisateurs simultanés.

Tâche 9 : consignation des informations relatives au réseau

Exécutez la commande **show run** sur chaque routeur et capturez les configurations.

```
R1#show run
<résultat omis>
!
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip helper-address 10.1.1.2
 no shutdown
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 ip helper-address 10.1.1.2
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 125000
!
interface Serial0/0/1
 no ip address
 shutdown
```

```
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
!
!
banner motd ^C
**********************************
  !!!AUTHORIZED ACCESS ONLY!!!
**********************************
^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
!
end

R2#show run
!
hostname R2
!
!
enable secret class
!
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp excluded-address 192.168.11.1 192.168.11.10
!
ip dhcp pool R1Fa0
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
   dns-server 192.168.11.5
!
ip dhcp pool R1Fa1
   network 192.168.11.0 255.255.255.0
   dns-server 192.168.11.5
   default-router 192.168.11.1
!
no ip domain lookup
!
interface Loopback0
 ip address 192.168.20.254 255.255.255.0
 ip nat inside
```

```
 ip virtual-reassembly
!
!
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 ip nat inside
 ip virtual-reassembly
!
interface Serial0/0/1
 ip address 209.165.200.225 255.255.255.252
 ip nat outside
 ip virtual-reassembly
 clock rate 125000
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.20.0 0.0.0.255 area 0
 default-information originate
!
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
!
no ip http server
no ip http secure-server
ip nat inside source list NAT interface Serial0/0/1 overload
ip nat inside source static 192.168.20.254 209.165.200.254
!
ip access-list extended NAT
 permit ip 192.168.10.0 0.0.0.255 any
 permit ip 192.168.11.0 0.0.0.255 any
!
!
banner motd ^C
**********************************
  !!!AUTHORIZED ACCESS ONLY!!!
**********************************
^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
```

```
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
!
end
```

```
FAI#show run
<résultat omis>
!
hostname FAI
!
enable secret class
!
no ip domain lookup
!
interface Serial0/0/1
 ip address 209.165.200.226 255.255.255.252
 no shutdown
!
!
!
ip route 209.165.200.240 255.255.255.240 Serial0/0/1
!
banner motd ^C
**********************************
  !!!AUTHORIZED ACCESS ONLY!!!
**********************************
^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
password cisco
 logging synchronous
 login
!
end
```

Tâche 10 : remise en état

Supprimez les configurations et rechargez les routeurs. Déconnectez le câblage et stockez-le dans un endroit sécurisé. Reconnectez le câblage souhaité et restaurez les paramètres TCP/IP pour les hôtes PC connectés habituellement aux autres réseaux (réseau local de votre site ou Internet).