Exercice 7.4.1 : configuration de base de DHCP et NAT

Diagramme de topologie

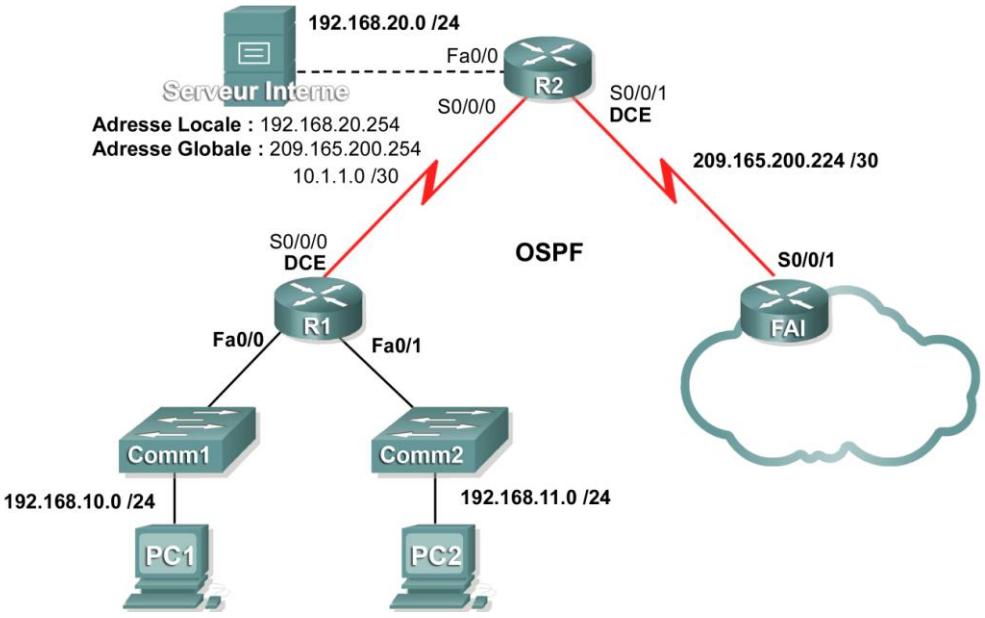

Table d'adressage

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	192.168.20.1	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 base des routeurs
- Configurer un serveur DHCP Cisco IOS
- Configurer le routage statique et par défaut
- Configurer une fonction NAT statique
- Configurer une fonction NAT dynamique avec un pool d'adresses
- Configurer une surcharge NAT

Scénario

Au cours de ces travaux pratiques, vous allez configurer les services IP de la fonction NAT et du protocole DHCP. Le premier routeur est le serveur DHCP. Le second transmet les requêtes DHCP au serveur. Vous allez également établir les configurations NAT statique et dynamique, notamment la surcharge NAT. Lorsque vous aurez terminé les configurations, vérifiez la connectivité entre les adresses internes et externes.

Tâche 1 : configurations de base des routeurs

Configurez les routeurs R1, R2 et FAI selon les instructions suivantes :

- Configurez le nom d'hôte des périphériques.
- Désactivez la recherche DNS.
- Configurez un mot de passe de mode d'exécution privilégié.
- Configurez une bannière du message du jour.
- Configurez un mot de passe pour les connexions de consoles.
- Configurez un mot de passe pour les connexions de terminaux virtuels (vty).
- Configurez des adresses IP sur tous les routeurs. Les PC reçoivent un adressage IP de DHCP plus tard dans l'exercice.
- Activez le protocole OSPF avec l'ID de processus 1 sur R1 et R2. N'annoncez pas le réseau 209.165.200.224/27.

Tâche 2 : configuration d'un serveur DHCP Cisco IOS

Étape 1. Exclusion des adresses attribuées de manière statique

Le serveur DHCP suppose que toutes les adresses IP d'un pool d'adresses DHCP peuvent être affectées à des clients DHCP. Vous devez indiquer les adresses IP que le serveur DHCP ne doit pas affecter aux clients. Ces adresses IP sont généralement des adresses statiques réservées à l'interface de routeur, à l'adresse IP de gestion des commutateurs, aux serveurs et à l'imprimante connectée au réseau local. La commande **ip dhcp excluded-address** empêche le routeur d'attribuer des adresses IP dans la plage configurée. Les commandes suivantes excluent les 10 premières adresses IP de chaque pool pour les réseaux locaux reliés à R1. Ces adresses ne sont alors attribuées à aucun client DHCP.

```
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
R1(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 la de commande **ip dhcp pool** et donnez-lui le nom **R1Fa0**.

```
R1(config)#ip dhcp pool R1Fa0
```

Précisez le sous-réseau à utiliser lors de l'attribution des adresses IP. Les pools DHCP s'associent automatiquement à une interface en fonction de l'instruction réseau. Le routeur fonctionne désormais comme un serveur DHCP et distribue des adresses dans le sous-réseau 192.168.10.0/24 en commençant par 192.168.10.1.

```
R1(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, ainsi qu'une adresse IP.

```
R1(dhcp-config)#dns-server 192.168.11.5
R1(dhcp-config)#default-router 192.168.10.1
```

Remarque : aucun serveur DNS n'est présent sur 192.168.11.5. Vous configurez la commande uniquement dans un objectif d'apprentissage.

```
R1(config)#ip dhcp pool R1Fa1
R1(dhcp-config)#network 192.168.11.0 255.255.255.0
R1(dhcp-config)#dns-server 192.168.11.5
R1(dhcp-config)#default-router 192.168.11.1
```

Étape 3. Vérification de la configuration de DHCP

Il vous est possible de vérifier la configuration du serveur DHCP de plusieurs façons. La façon la plus simple est de configurer un hôte sur le sous-réseau pour recevoir une adresse IP via le protocole DHCP. Vous pouvez ensuite envoyer des commandes sur le routeur pour obtenir plus d'informations. La commande **show ip dhcp binding** fournit des informations sur toutes les adresses DHCP actuellement attribuées. Par exemple, les résultats suivants montrent que l'adresse IP 192.168.10.11 a été attribuée à l'adresse MAC 3031.632e.3537.6563. La période d'utilisation IP expire le 14 septembre 2007 à 19h33.

```
R1#show ip dhcp binding
IP address Client-ID/ Lease expiration Type
Hardware address
192.168.10.11 0007.EC66.8752 -- Automatic
192.168.11.11 00E0.F724.8EDA -- Automatic
```

Tâche 3 : configuration du routage par défaut et statique

FAI utilise un routage statique pour atteindre tous les réseaux au-delà de R2. Cependant, R2 traduit les adresses privées en adresses publiques avant d'envoyer le trafic à FAI. FAI doit donc être configuré avec les adresses publiques qui font partie de la configuration de la fonction NAT sur R2. Saisissez 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 inclut toutes les adresses attribuées à R2 pour une utilisation publique.

Configurez une route par défaut sur R2 et propagez la route dans le protocole 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 quelques secondes que R1 prenne en compte la route par défaut envoyée par R2, puis vérifiez la table de routage de R1. Vous pouvez également effacer la table de routage à l'aide de la commande **clear ip route ***. Une route par défaut pointant vers R2 doit s'afficher dans la table de routage de R1. à partir de R1, envoyez une requête ping à l'interface Serial 0/0/1 sur R2 (209.165.200.225). Les requêtes ping doivent aboutir. Dépannez si elles échouent.

Tâche 4 : configuration de la fonction NAT statique

Étape 1. Mappage statique d'une adresse IP publique vers une adresse IP privée

Le serveur interne relié à R2 est accessible aux hôtes externes au-delà de FAI. Attribuez de façon statique l'adresse IP publique 209.165.200.254 comme l'adresse que NAT utilise pour mapper les paquets sur l'adresse IP privée du serveur interne sur 192.168.20.254.

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

Étape 2. Spécification des interfaces NAT internes et externes

Avant de pouvoir appliquer la fonction NAT, précisez les interfaces qui sont à l'intérieur et celles qui sont à l'extérieur.

```
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
```

Étape 3. Vérification de la configuration NAT statique

À partir de FAI, envoyez une requête ping à l'adresse IP publique 209.165.200.254.

Tâche 5 : configuration d'une fonction NAT dynamique avec un pool d'adresses

Alors que la fonction NAT statique offre un mappage permanent entre une adresse interne et une adresse publique spécifique, la fonction NAT dynamique mappe des adresses IP privées sur des adresses publiques. Ces adresses IP publiques proviennent d'un pool NAT.

Étape 1. Définition d'un pool d'adresses globales

Créez un pool d'adresses vers lesquelles des adresses source correspondantes sont traduites. La commande suivante crée un pool appelé **MY-NAT-POOL** qui traduit 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. Mise en place d'une traduction de source dynamique en reliant le pool à la liste de contrôle d'accès

Un routeur peut posséder plus d'un pool NAT et plusieurs listes de contrôle d'accès. La commande suivante indique au routeur le pool d'adresses à utiliser pour traduire des hôtes que la liste de contrôle d'accès autorise.

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

Étape 4. Spécification des interfaces NAT internes et externes

Vous avez déjà précisé les interfaces internes et externes de votre configuration NAT statique. Ajoutez maintenant l'interface série reliée 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 à FAI à partir de PC1 et de PC2. Utilisez ensuite la commande **show ip nat translations** sur R2 pour vérifier la fonction NAT.

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.241   192.168.10.11      ---                ---
---  209.165.200.242   192.168.11.11      ---                ---
---  209.165.200.254   192.168.20.254     ---                ---
```

Tâche 6 : configuration d'une surcharge NAT

Dans l'exemple précédent, que se passerait-il si vous aviez besoin de plus d'adresses IP publiques que les six autorisées par le pool ?

Par un suivi des numéros de port, la surcharge NAT permet à plusieurs utilisateurs internes de réutiliser une adresse IP publique.

Au cours de cette tâche, vous allez supprimer le pool et l'instruction de mappage configurée dans la tâche précédente. Vous allez ensuite configurer la surcharge NAT sur R2 de telle sorte que les adresses IP internes soient traduites sur l'adresse S0/0/1 de R2 lors de la connexion à tout périphérique externe.

Étape 1. Suppression du pool NAT et de l'instruction de mappage

Utilisez les commandes suivantes pour supprimer le pool NAT et le mappage sur la liste de contrôle d'accès NAT.

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

Si vous recevez le message suivant, effacez vos traductions NAT.

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

Étape 2. Configuration de la fonction PAT sur R2 avec l'adresse IP publique de l'interface Serial 0/0/1

La configuration est similaire à celle de la fonction NAT dynamique, si ce n'est que le mot clé **interface** (et non un pool d'adresses) est utilisé pour identifier l'adresse IP externe. Aucun pool NAT n'est donc défini. Le mot clé **overload** active l'ajout du numéro de port à la traduction.

Puisque vous avez déjà configuré une liste de contrôle d'accès pour identifier les adresses IP internes à traduire, ainsi que les interfaces qui sont internes et celles qui sont externes, vous avez simplement à configurer ce qui suit :

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

Étape 3. Vérification de la configuration

Envoyez une requête ping à FAI à partir de PC1 et de PC2. Utilisez ensuite la commande **show ip nat translations** sur R2 pour vérifier la fonction NAT.

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.225:3 192.168.10.11:3    209.165.200.226:3
209.165.200.226:3
icmp 209.165.200.225:1024192.168.11.11:3    209.165.200.226:3
209.165.200.226:1024
---  209.165.200.254   192.168.20.254     ---                ---
```

Remarque : au cours de la tâche précédente, vous avez 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 7 : documentation du réseau

Sur chaque routeur, exécutez la commande **show run** pour accéder aux configurations.

Tâche 1 : préparation du réseau

Étape 1. installation d'un réseau similaire à celui du diagramme de topologie

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

Remarque : si vous utilisez un routeur série 1700, 2500 ou 2600, les informations affichées sur le routeur et les descriptions d'interface peuvent apparaître différemment.

Étape 2. Suppression des configurations actuelles des routeurs

Tâche 2 : configurations de base des routeurs

Configurez les routeurs R1, R2 et FAI selon les instructions suivantes :

- Configurez le nom d'hôte des périphériques.
- Désactivez la recherche DNS.
- Configurez un mot de passe de mode d'exécution privilégié.
- Configurez une bannière du message du jour.
- Configurez un mot de passe pour les connexions de consoles.
- Configurez un mot de passe pour les connexions de terminaux virtuels (vty).
- Configurez des adresses IP sur tous les routeurs. Les PC reçoivent un adressage IP de DHCP plus tard dans l'exercice.
- Activez le protocole OSPF avec 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 pour utiliser l'adresse IP 192.168.20.254/24. Si vous faites cela, vous n'avez pas besoin de configurer l'interface Fast Ethernet.

Tâche 3 : 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 de faire en sorte que les périphériques des réseaux 192.168.10.0/24 et 192.168.11.0/24 demandent des adresses IP via le protocole DHCP à partir de R2.

Étape 1. Exclusion des adresses attribuées de manière statique

Le serveur DHCP suppose que toutes les adresses IP d'un pool d'adresses DHCP peuvent être affectées à des clients DHCP. Vous devez indiquer les adresses IP que le serveur DHCP ne doit pas affecter aux clients. Ces adresses IP sont généralement des adresses statiques réservées à l'interface du routeur, à l'adresse IP de gestion des commutateurs, aux serveurs et à l'imprimante connectée au réseau local. La commande **ip dhcp excluded-address** empêche le routeur d'attribuer des adresses IP dans la plage configurée. Les commandes suivantes excluent les 10 premières adresses IP de chaque pool pour les réseaux locaux reliés à R1. Ces adresses ne sont alors attribuées à aucun client 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 la de commande **ip dhcp pool** et donnez-lui le nom **R1Fa0**.

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

Précisez le sous-réseau à utiliser lors de l'attribution des adresses IP. Les pools DHCP s'associent automatiquement à une interface en fonction de l'instruction réseau. Le routeur fonctionne désormais comme un serveur DHCP et distribue des adresses dans le 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, ainsi 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 présent sur 192.168.11.5. Vous configurez la commande uniquement dans un objectif d'apprentissage.

Étant donné que des périphériques du réseau 192.168.11.0/24 demandent également des adresses à R2, un pool séparé doit être créé pour les périphériques du réseau en question. Les commandes sont similaires aux commandes indiquées 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. Configuration d'une adresse de diffusion par défaut

Des services réseau tels que le protocole DHCP s'appuient sur des diffusions de couche 2 pour fonctionner. Lorsque les périphériques fournissant ces services existent sur un sous-réseau différent de celui des clients, ils ne peuvent pas recevoir les paquets de diffusion. Puisque le serveur DHCP et les clients DHCP ne se trouvent pas sur le même sous-réseau, configurez R1 pour qu'il transfère les diffusions DHCP à R2, qui est le serveur DHCP, en utilisant la commande de configuration d'interface **ip helper-address**.

Remarquez que la commande **ip helper-address** doit être configurée sur chaque interface impliquée.

```
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 4. Vérification de la configuration de DHCP

Il vous est possible de vérifier la configuration du serveur DHCP de plusieurs façons. La façon la plus simple est de configurer un hôte sur le sous-réseau pour recevoir une adresse IP via le protocole DHCP. Vous pouvez ensuite envoyer des commandes sur le routeur pour obtenir plus d'informations. La commande **show ip dhcp binding** fournit des informations sur toutes les adresses DHCP actuellement attribuées. Par exemple, les résultats suivants montrent que l'adresse IP 192.168.10.11 a été attribuée à l'adresse MAC 3031.632e.3537.6563. La période d'utilisation IP expire le 14 septembre 2007 à 19h33.

```
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 sur tous les pools DHCP actuellement configurés sur le routeur. Elle indique que le pool **R1Fa0** est configuré sur R2. Une adresse de ce pool a été louée. Le prochain client demandant une adresse se verra attribuer 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 être extrêmement utile pour dépanner des locations de DHCP avec un serveur DHCP Cisco IOS. Voici les informations de débogage sur R1 après la connexion d'un hôte. Remarquez que la partie surlignée montre le DHCP attribuant au client une adresse de 192.168.10.12 et un maque de 255.255.255.0.

```
*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 : Adding binding to radix tree (192.168.10.12)
*Sep 13 21:04:20.072: DHCPD : Adding binding to hash tree
*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 4 : configuration du routage par défaut et statique

FAI utilise un routage statique pour atteindre tous les réseaux au-delà de R2. Cependant, R2 traduit les adresses privées en adresses publiques avant d'envoyer le trafic à FAI. FAI doit donc être configuré avec les adresses publiques qui font partie de la configuration de la fonction NAT sur R2. Saisissez 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 inclut toutes les adresses attribuées à R2 pour une utilisation publique.

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

```
R2(config)#ip route 0.0.0.0 0.0.0.0 209 165 200 225
R2(config)#router ospf 1
R2(config-router)#default-information originate
```

Attendez quelques secondes que R1 prenne en compte la route par défaut envoyée par R2, puis vérifiez la table de routage de R1. Vous pouvez également effacer la table de routage à l'aide de la commande **clear ip route *.** Une route par défaut pointant vers R2 doit s'afficher dans la table de routage de R1. À partir de R1, envoyez une requête ping à l'interface Serial 0/0/1 sur R2 (209.165.200.226). Les requêtes ping doivent aboutir. Dépannez si elles échouent.

Tâche 5 : configuration de la fonction NAT statique

Étape 1. Mappage statique d'une adresse IP publique vers une adresse IP privée

Le serveur interne relié à R2 est accessible aux hôtes externes au-delà de FAI. Attribuez de façon statique l'adresse IP publique 209.165.200.254 comme l'adresse que NAT utilise pour mapper les paquets sur l'adresse IP privée du serveur interne sur 192.168.20.254.

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

Étape 2. Spécification des interfaces NAT internes et externes

Avant de pouvoir appliquer la fonction NAT, précisez les interfaces qui sont à l'intérieur et celles qui sont à l'extérieur.

```
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 NAT statique

À partir de FAI, envoyez une requête ping à l'adresse IP publique 209.165.200.254.

Tâche 6 : configuration d'une fonction NAT dynamique avec un pool d'adresses

Alors que la fonction NAT statique offre un mappage permanent entre une adresse interne et une adresse publique spécifique, la fonction NAT dynamique mappe des adresses IP privées sur des adresses publiques. Ces adresses IP publiques proviennent d'un pool NAT.

Étape 1. Définition d'un pool d'adresses globales

Créez un pool d'adresses vers lesquelles des adresses source correspondantes sont traduites. La commande suivante crée un pool appelé **MY-NAT-POOL** qui traduit 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. Mise en place d'une traduction de source dynamique en reliant le pool à la liste de contrôle d'accès

Un routeur peut posséder plus d'un pool NAT et plusieurs listes de contrôle d'accès. La commande suivante indique au routeur le pool d'adresses à utiliser pour traduire des hôtes que la liste de contrôle d'accès autorise.

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

Étape 4. Spécification des interfaces NAT internes et externes

Vous avez déjà précisé les interfaces internes et externes de votre configuration NAT statique. Ajoutez maintenant l'interface série reliée 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 à FAI à partir de PC1 ou de l'interface Fast Ethernet sur R1 à l'aide de la commande **ping** étendue. Utilisez ensuite les commandes **show ip nat translations** et **show ip nat statistics** sur R2 pour vérifier la fonction NAT.

```
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 statique, 1 dynamique ; 0 étendu)
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 dépanner tout problème posé par la fonction NAT, utilisez la commande **debug ip nat**. Activez le débogage de la fonction NAT et renvoyez une requête 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 7 : configuration d'une surcharge NAT

Dans l'exemple précédent, que se passerait-il si vous aviez besoin de plus d'adresses IP publiques que les six autorisées par le pool ?

_____

Par un suivi des numéros de port, la surcharge NAT permet à plusieurs utilisateurs internes de réutiliser une adresse IP publique.

Au cours de cette tâche, vous allez supprimer le pool et l'instruction de mappage configurée dans la tâche précédente. Vous allez ensuite configurer la surcharge NAT sur R2 de telle sorte que les adresses IP internes soient traduites sur l'adresse S0/0/1 de R2 lors de la connexion à tout périphérique externe.

Étape 1. Suppression de l'instruction de mappage et de pool NAT

Utilisez les commandes suivantes pour supprimer le pool NAT et le mappage sur la liste de contrôle d'accès NAT.

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

Si vous recevez le message suivant, effacez vos traductions NAT.

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

Étape 2. Configuration de la fonction PAT sur R2 avec l'adresse IP publique de l'interface Serial 0/0/1

La configuration est similaire à celle de la fonction NAT dynamique, si ce n'est que le mot clé **interface** (et non un pool d'adresses) est utilisé pour identifier l'adresse IP externe. Aucun pool NAT n'est donc défini. Le mot clé **overload** active l'ajout du numéro de port à la traduction.

Puisque vous avez déjà configuré une liste de contrôle d'accès pour identifier les adresses IP internes à traduire, ainsi que les interfaces qui sont internes et celles qui sont externes, vous avez simplement à configurer ce qui suit :

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

Étape 3. Vérification de la configuration

Envoyez une requête ping à FAI à partir de PC1 ou de l'interface Fast Ethernet sur R1 à l'aide de la commande **ping** étendue. Utilisez ensuite les commandes **show ip nat translations** et **show ip nat statistics** sur R2 pour vérifier la fonction NAT.

```
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 statique, 1 dynamique ; 1 étendu)
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 avez 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 8 : documentation du réseau

Sur chaque routeur, exécutez la commande **show run** pour accéder aux configurations.

Tâche 9 : remise en état

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