

Travaux pratiques 7.4.3 : dépannage de DHCP et NAT

Diagramme de topologie

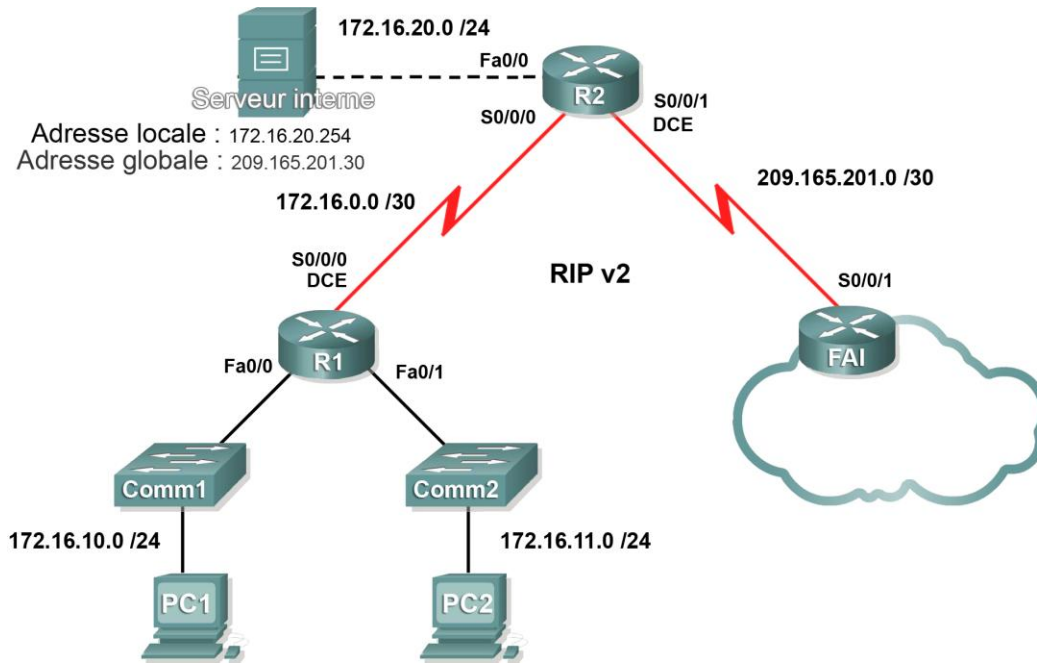


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
R1	S0/0/0	172.16.0.1	255.255.255.252
	Fa0/0	172.16.10.1	255.255.255.0
	Fa0/1	172.16.11.1	255.255.255.0
R2	S0/0/0	172.16.0.2	255.255.255.252
	S0/0/1	209.165.201.1	255.255.255.252
	Fa0/0	172.16.20.1	255.255.255.0
FAI	S0/0/1	209.165.201.2	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
- Charger les routeurs avec les scripts fournis
- Détecter et corriger des erreurs réseau
- Documenter le réseau corrigé

Scénario

Les routeurs R1 et R2 de votre société ont été configurés par un ingénieur réseau peu expérimenté. La présence de plusieurs erreurs dans la configuration a provoqué des problèmes de connectivité. Votre responsable vous demande de détecter les erreurs de configuration et de les corriger, puis de décrire le travail réalisé. En utilisant vos connaissances en matière de services DHCP et NAT, ainsi que des méthodes de vérification standard, détectez les erreurs et corrigez-les. Vérifiez que tous les clients disposent d'une connectivité complète. Le FAI a été correctement configuré.

Assurez-vous que le réseau prend en charge les conditions suivantes :

1. Le routeur R2 doit faire office de serveur DHCP pour les réseaux 172.16.10.0/24 et 172.16.11.0/24, connectés au routeur R1.
2. Tous les PC connectés au routeur R1 doivent recevoir une adresse IP dans le réseau approprié via le protocole DHCP.
3. Le trafic provenant des réseaux locaux de R1, entrant dans l'interface série Serial 0/0/0 et sortant de l'interface série Serial 0/0/1 de R2, doit recevoir une traduction NAT avec un pool d'adresses fourni par le FAI.
4. Le serveur interne doit être accessible à partir des réseaux externes à l'aide de l'adresse IP 209.165.201.30 et à partir des réseaux internes à l'aide de l'adresse IP 172.16.20.254.

Tâche 1 : préparation du réseau

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

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

Étape 3 : importation des configurations

R1

```
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 172.16.10.1 255.255.255.0
 ip helper-address 172.16.0.2
 no shutdown
!
interface FastEthernet0/1
 ip address 172.16.11.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.0.1 255.255.255.252
 clock rate 125000
 no shutdown
!
router rip
 version 2
```

```
network 172.16.0.0
no auto-summary
!
banner motd $AUTHORIZED ACCESS ONLY$
!
line con 0
password cisco
logging synchronous
login
line vty 0 4
password cisco
logging synchronous
login
!
end
```

R2

```
hostname R2
!
enable secret class
!
ip dhcp excluded-address 172.16.10.1 172.16.10.3
ip dhcp excluded-address 172.16.10.1 172.16.11.3
!
ip dhcp pool R1_LAN10
network 172.16.10.0 255.255.255.0
dns-server 172.16.20.254
!
ip dhcp pool R1_LAN11
network 172.16.11.0 255.255.255.0
dns-server 172.16.20.254
!
no ip domain lookup
!
interface FastEthernet0/0
ip address 172.16.20.1 255.255.255.0
ip nat inside
no shutdown
!
interface Serial0/0/0
ip address 172.16.0.2 255.255.255.252
no shutdown
!
interface Serial0/0/1
ip address 209.165.201.1 255.255.255.252
ip nat outside
clock rate 125000
no shutdown
!
router rip
version 2
network 172.16.0.0
default-information originate
```

```
no auto-summary
!
ip route 0.0.0.0 0.0.0.0 209.165.201.2
!
ip nat pool NAT_POOL 209.165.201.9 209.165.201.14 netmask 255.255.255.248
ip nat inside source list NAT_ACL pool NATPOOL overload
!
ip access-list standard NAT_ACL
 permit 172.16.10.0 0.0.0.255
!
banner motd $AUTHORIZED ACCESS ONLY$
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 logging synchronous
 login
!
end
```

FAI

```
hostname FAI
!
enable secret class
!
interface Serial0/0/1
 ip address 209.165.201.2 255.255.255.252
 no shutdown
!
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!
banner motd $AUTHORIZED ACCESS ONLY$
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 logging synchronous
 login
!
end
```

Tâche 2 : recherche et correction des erreurs sur le réseau

Lorsque le réseau est correctement configuré :

- Les ordinateurs PC1 et PC2 doivent être en mesure de recevoir des adresses IP depuis le pool DHCP approprié, comme l'indique la commande `ipconfig`. En outre, une commande `show ip dhcp bindings` exécutée sur le routeur R2 doit indiquer que les deux PC ont reçu des adresses IP.
- Les requêtes ping envoyées depuis les ordinateurs PC1 et PC2 au FAI doivent recevoir une traduction NAT avec surcharge, comme indiqué par la commande `show ip nat translations` sur le routeur R2.
- Les requêtes ping envoyées depuis le serveur interne au FAI doivent recevoir la traduction NAT statique indiquée dans la topologie. Pour le vérifier, utilisez la commande `show ip nat translations`.
- L'envoi d'une requête ping depuis le FAI à l'adresse globale du serveur interne doit aboutir.
- Les requêtes ping envoyées depuis le FAI au routeur R1 ne doivent recevoir aucune traduction d'adresses de réseau (NAT), comme indiqué par la commande `show ip nat translations` ou `debug ip nat` sur le routeur R2.

Tâche 3 : documentation des configurations des routeurs

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

Tâche 4 : 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).