

## TP3 : Le protocole de routage BGP

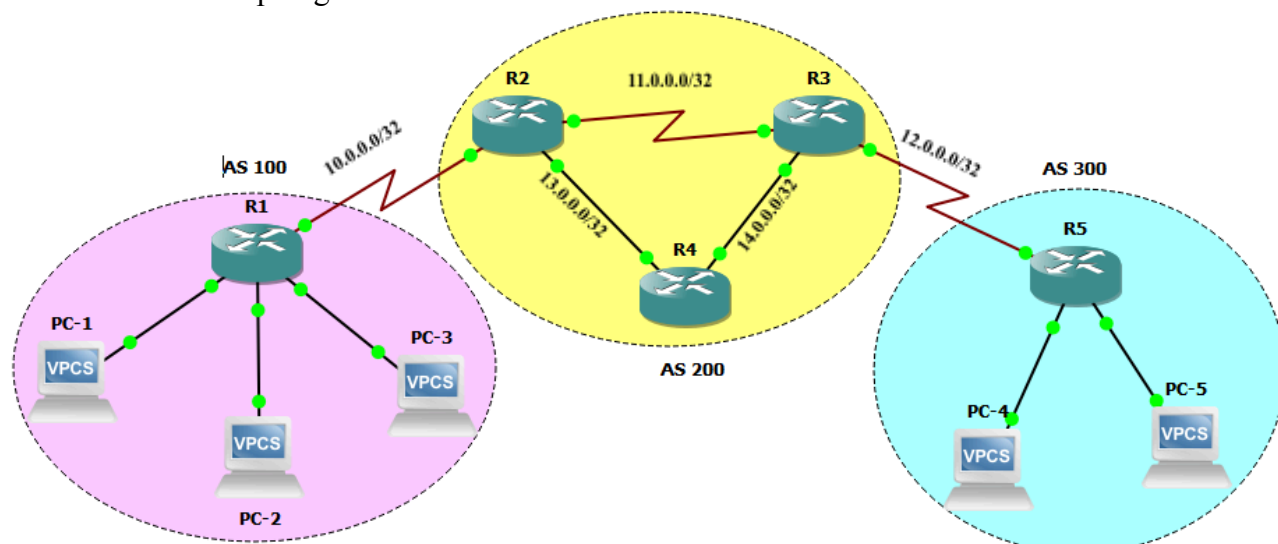
### Partie II

#### Objectifs :

1. Analyser les filtre BGP
2. Modifier les attributs BGP

#### Mise en place de la topologie du TP

- Utiliser la topologie du TP-BGP Partie I.



#### Tables d'adressage

Périphérique	Interface avec	Adresse IPv4	Masque de sous-réseau
R1	R2	10.0.0.1	255.255.255.252
	PC1	192.168.1.1	255.255.255.0
	PC2	192.168.2.1	255.255.255.0
	PC3	192.168.3.1	255.255.255.0
R2	R1	10.0.0.2	255.255.255.252
	R3	11.0.0.1	255.255.255.252
	R4	13.0.0.1	255.255.255.252
R3	R2	11.0.0.2	255.255.255.252
	R5	12.0.0.1	255.255.255.252
	R4	14.0.0.2	255.255.255.252
R4	R2	13.0.0.2	255.255.255.252
	R3	14.0.0.1	255.255.255.252
	R3	12.0.0.2	255.255.255.252
R5	PC4	192.168.4.1	255.255.255.0
	PC5	192.168.5.1	255.255.255.0
PC1	NIC	192.168.1.10	255.255.255.0
PC2	NIC	192.168.2.10	255.255.255.0
PC3	NIC	192.168.3.10	255.255.255.0
PC4	NIC	192.168.4.10	255.255.255.0
PC5	NIC	192.168.5.10	255.255.255.0

### Activité 3 : Filtrage de routes BGP

**NB :** Après chaque configuration, vérifier les tables de routage, les tables bgp et utiliser les commandes ping/traceroute pour valider le résultat.

Pour voir l'effet rapide des commandes, exécuter la commande **#clear ip bgp \***

#### A. Filtrage des routes par adresses réseaux :

Au niveau de la configuration de BGP, associer une ACL au voisin BGP. La syntaxe est :

```
#neighbor Adresse_voisin distribute-list N°_ACL  
[in|out]
```

**IN** pour indiquer de ne pas accepter des réseaux de l'extérieur

**OUT** pour indiquer de ne pas diffuser des réseaux vers l'extérieur.

Par la suite, en mode de configuration global, il faut créer une liste d'accès ACL :

```
#access-list N°_ACL deny NET_ID masque_inverse  
#access-list N°_ACL permit 0.0.0.0 255.255.255.255
```

L'objectif est de :

1. Interdire à l'AS100 d'annoncer le réseau 192.168.1.0/24 à l'AS200

**R1 :**

```
R1#config  
Configuring from terminal, memory, or network [terminal]?  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#router bgp 100  
R1(config-router)#neighbor 10.0.0.2 distribute-list 10 out  
R1(config-router)#end  
R1#config  
Configuring from terminal, memory, or network [terminal]?  
*Nov 4 12:45:01.870: %SYS-5-CONFIG_I: Configured from console by console  
  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#access-list 10 deny 192.168.1.0 0.0.0.255  
R1(config)#access-list 10 permit 0.0.0.0 255.255.255.255
```

2. Interdire à l'AS200 d'accepter le réseau 192.168.5.0/24 depuis l'AS300

**R3 :**

```
R3#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router bgp 200
R3(config-router)#neighbor 12.0.0.2 distribute-list 10 in
R3(config-router)#access-list 10 deny 192.168.1.5 0.0.0.255
R3(config)#router bgp 200
R3(config-router)#no access-list 10 deny 192.168.1.5 0.0.0.255
R3(config)#end
R3#con
*Nov 4 12:50:45.582: %SYS-5-CONFIG_I: Configured from console by console
R3#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 10 deny 192.168.5.0 0.0.0.255
R3(config)#access-list 10 permit 0.0.0.0 255.255.255.255
```

## B. Filtrage par AS-path :

Au niveau de la configuration de BGP, associer une ACL au voisin BGP. La syntaxe est :

```
#neighbor Adresse_voisin filter-list N°_ACL [in|out]
```

Par la suite, en mode de configuration global, créer une ACL comme suit :

```
#ip as-path access-list N°_ACL deny As_path
#ip as-path access-list N°_ACL permit .*
```

**As\_path** : est une expression régulière.

La commande **show ip bgp regexp** permet d'afficher les expressions régulières.

L'objectif est d' :

3. Interdire à l'AS100 d'annoncer ses réseaux à l'AS200

**R1 :**

```
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router bgp 100
R1(config-router)#neighbor 10.0.0.2 filter-list 10 out
R1(config-router)#exit
R1(config)#ip as-path access-list 10 deny ^$
R1(config)#ip as-path access-list 10 permit .*
```

4. Interdire à l'AS200 d'accepter les réseaux de l'AS300

**R3 :**

```
R3#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router bgp 200
R3(config-router)#neighbor 12.0.0.2 filter-list 10 in
R3(config-router)#exit
R3(config)#ip as-path access-list 10 deny ^$
R3(config)#ip as-path access-list 10 permit .*
```

## Activité 4 : Influencer les chemin BGP

1. Enlever tous les filtres de l'activité 3.
2. Connecter le routeur R1 et R5 (utiliser le réseau 15.0.0.0/30).

**R1 :**

```
R1(config)#interface serial 1/1
R1(config-if)#ip address 15.0.0.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
```

**R5 :**

```
R5(config)#interface serial 1/1
R5(config-if)#ip address 15.0.0.2 255.255.255.252
R5(config-if)#no shutdown
R5(config-if)#exit
```

3. Configurer BGP entre R1 et R5.

**R1 :**

```
R1(config)#router bgp 100
R1(config-router)#neighbor 15.0.0.2 remote-as 300
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.2.0
R1(config-router)#network 192.168.3.0
R1(config-router)#
*Nov  4 13:30:16.937: %BGP-5-ADJCHANGE: neighbor 15.0.0.2 Up
```

**R5 :**

```
R5(config)#router bgp 300
R5(config-router)#neighbor 15.0.0.1 remote-as 100
R5(config-router)#network 192.1
*Nov  4 13:06:56.326: %BGP-5-ADJCHANGE: neighbor 15.0.0.1 Up
R5(config-router)#network 192.168.5.0
R5(config-router)#network 192.168.4.0
```

4. Quel est le chemin emprunté par les paquets de l'AS100 à l'AS300 ?

AS100 —> AS300.

5. Sur quel attribut BGP le choix du meilleur chemin est effectué ?

Le nombre de saut entre les 2 AS ,

Pour la première liaison : AS100 - AS 200 - AS 300 => 2 saut

Pour la deuxième liaison : AS100 - AS 300 => 1 saut

donc il va choisir la deuxième liaison grâce au nombre de saut minimal

6. Forcer l'AS100 à emprunter le chemin qui passe par l'AS200 pour atteindre l'AS300.  
7. Utiliser le paramètre **Weight** en utilisant la commande :

```
#neighbor Adresse_voisin weight valeur
```

Utiliser la valeur **15** pour le voisin R2 et la valeur **10** pour le voisin R5

```
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router bgp 100
R1(config-router)#neighbor 10.0.0.2 weight 15
% Specify remote-as or peer-group commands first
R1(config-router)#neighbor 10.0.0.2 weight 15
R1(config-router)#neighbor 15.0.0.2 weight 10
```

8. Quel est le chemin emprunté par les paquets de l'AS100 à l'AS300 ?

AS 100 —> AS 200 —> AS300.

9. Quel est le chemin emprunté par les paquets de l'AS300 à l'AS100 ?

AS 300 —> AS 100.

10. Interpréter le résultat

Même si on a forcé R1 à choisir le chemin passant par l'AS 200, on remarque que R5 continue de privilégier l'ancien lien direct entre l'AS 300 et l'AS 100. Cela s'explique par le fait que la configuration et la modification du poids (weight) ont été faites uniquement sur R1.

Pour que les paquets sortant de R5 vers R1 empruntent aussi le chemin passant par l'AS 200, on doit mettre à jour et configurer les poids (weight) des deux chemins sur R5.