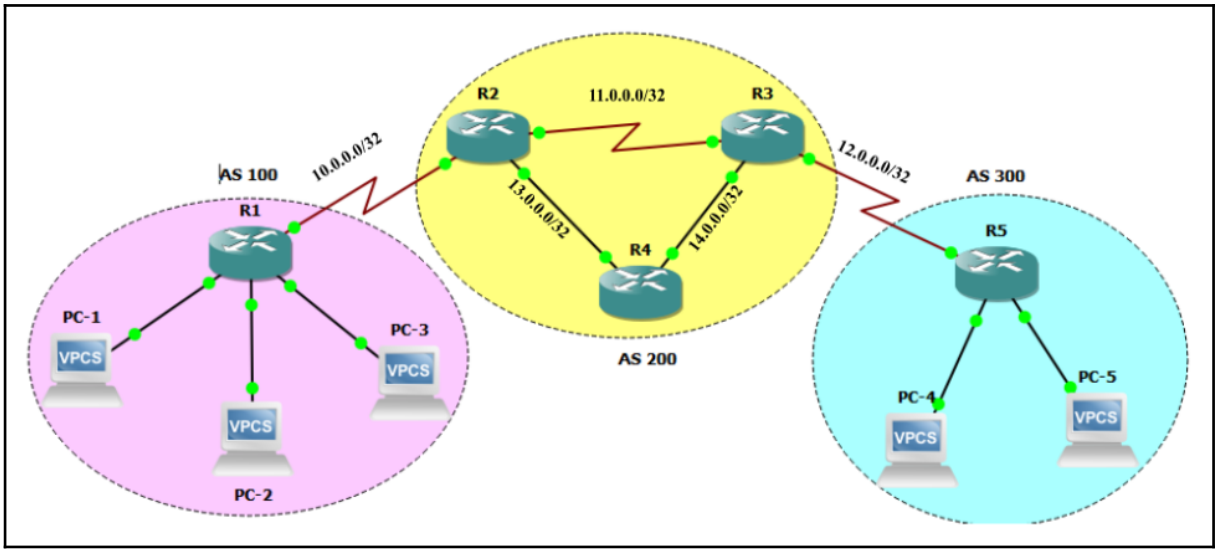
TP3 : Le protocole de routage BGP

Partie II : (à remettre avant mardi 15/11 à 23h59)

Objectifs :

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

Mise en place de la topologie du TP



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
R5	R3	12.0.0.2	255.255.255.252
	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
2. Interdire à l'AS200 d'accepter le réseau 192.168.5.0/24 depuis l'AS300

Pour R1:

```
conf t
access-list 1 deny 192.168.1.0 0.0.0.255
access-list 1 permit 0.0.0.0 255.255.255.255
router bgp 100
neighbor 10.0.0.2 distribute-list 1 out
```

En R2 on trouve:

```
     Network          Next Hop            Metric LocPrf Weight Path
 r>i 11.0.0.0/30      11.0.0.2                 0    100      0 ?
 r>i 13.0.0.0/30      11.0.0.2                 2    100      0 ?
 r>i 14.0.0.0/30      11.0.0.2                 0    100      0 ?
 *>  192.168.2.0      10.0.0.1                 0             0 100 i
 *>  192.168.3.0      10.0.0.1                 0             0 100 i
 *>i 192.168.4.0      11.0.0.2                 0    100      0 300 i
R2#
```

Pour R3:

```
conf t
access-list 2 deny 192.168.5.0 0.0.0.255
access-list 2 permit 0.0.0.0 255.255.255.255
router bgp 200
neighbor 12.0.0.2 distribute-list 2 in
```

En R3 on trouve:

```
   Network          Next Hop            Metric LocPrf Weight Path
r>i 11.0.0.0/30     11.0.0.1                 0    100      0 ?
r>i 13.0.0.0/30     11.0.0.1                 0    100      0 ?
r>i 14.0.0.0/30     11.0.0.1                 2    100      0 ?
*>i 192.168.2.0     11.0.0.1                 0    100      0 100 i
*>i 192.168.3.0     11.0.0.1                 0    100      0 100 i
*>  192.168.4.0     12.0.0.2                 0             0 300 i
```

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' :

1. Interdire à l'AS 100 d'annoncer ses réseaux à l'AS 200
2. Interdire à l'AS 200 d'accepter les réseaux de l'AS 300

Pour R1:

```
conf t
ip as-path access-list 3 deny ^$
ip as-path access-list 3 permit .*
router bgp 100
neighbor 10.0.0.2 filter-list 3 out
```

En R2 on trouve:

```
   Network          Next Hop            Metric LocPrf Weight Path
* i 11.0.0.0/30     11.0.0.2                 0    100      0 ?
*>                  0.0.0.0                  0         32768 ?
* i 13.0.0.0/30     11.0.0.2                 2    100      0 ?
*>                  0.0.0.0                  0         32768 ?
* i 14.0.0.0/30     11.0.0.2                 0    100      0 ?
*>                  13.0.0.2                 2         32768 ?
```

Pour R3:

```
conf t
ip as-path access-list 4 deny ^300_
ip as-path access-list 4 permit .*
router bgp 200
neighbor 12.0.0.2 filter-list 4 in
```

En R3 on trouve:

```
   Network          Next Hop            Metric LocPrf Weight Path
*>  11.0.0.0/30      0.0.0.0                  0         32768 ?
* i                 11.0.0.1                 0    100      0 ?
*>  13.0.0.0/30      14.0.0.1                 2         32768 ?
* i                 11.0.0.1                 0    100      0 ?
*>  14.0.0.0/30      0.0.0.0                  0         32768 ?
* i                 11.0.0.1                 2    100      0 ?
```

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).

R5:

```
conf t
ip route 15.0.0.0 255.255.255.252 se1/1
int se1/1
ip address 15.0.0.2 255.255.255.252
no shutdown
```

R1:

```
conf t
ip route 15.0.0.0 255.255.255.252 se1/1
int se1/1
ip address 15.0.0.1 255.255.255.252
no shutdown
```

3. Configurer BGP entre R1 et R5.

R1:

```
conf t
router bgp 100
neighbor 15.0.0.2 remote-as 300
```

R5:

```
conf t
router bgp 300
neighbor 15.0.0.1 remote-as 100
```

4. Quel est le chemin emprunté par les paquets de l'AS 100 à l'AS 300 ?

Chemin passe directement de l'AS 100 vers l'AS 300 (en transitant par les routeurs de la frontière des deux AS 100 et 300). … → R1 → R5 → …

```
R1#trace 192.168.4.10
Type escape sequence to abort.
Tracing the route to 192.168.4.10
VRF info: (vrf in name/id, vrf out name/id)
  1 15.0.0.2 36 msec 52 msec 52 msec
  2 192.168.4.10 [AS 300] 116 msec 44 msec 48 msec
```

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

Sur l'attribut As_path

6. Forcer l'AS 100 à emprunter le chemin qui passe par l'AS 200 pour atteindre l'AS 300.

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:

```
conf t
router bgp 100
neighbor 15.0.0.2 weight 10
neighbor 10.0.0.2 weight 15
```

8. Quel est le chemin emprunté par les paquets de l'AS 100 à l'AS 300 ?

ils passent de l'AS 100 vers l'AS intermédiaire 200 puis vers l'AS 300

preuve:

```
PC-1> ping 192.168.5.10
84 bytes from 192.168.5.10 icmp_seq=1 ttl=62 time=62.848 ms
84 bytes from 192.168.5.10 icmp_seq=2 ttl=62 time=61.461 ms
84 bytes from 192.168.5.10 icmp_seq=3 ttl=62 time=64.169 ms
84 bytes from 192.168.5.10 icmp_seq=4 ttl=62 time=60.624 ms
84 bytes from 192.168.5.10 icmp_seq=5 ttl=62 time=62.388 ms
```

la capture du lien entre R1 et R2:

10.0.0.1	10.0.0.2	BGP	63 KEEPALIVE Message
10.0.0.2	10.0.0.1	TCP	44 179 → 13781 [ACK] Seq=319

le protocole TCP du ping.

9. Quel est le chemin emprunté par les paquets de l'AS 300 à l'AS 100 ?

ils passent directement de l'AS 300 vers l'AS 100 (par le réseau 15.0.0.0/30)

preuve:

la capture du lien entre R1 et R2:

15.0.0.1	15.0.0.2	BGP	63 KEEPALIVE Message
15.0.0.2	15.0.0.1	TCP	44 179 → 24928 [ACK] Se

le protocole TCP du ping de retour.

10. Interpréter le résultat.

1. L'ordre de propriété entre les attributs BGP (weight et as_path) pour choisir le meilleur chemin est: comparaison des valeurs de weight, si la valeur du weight est différent entre deux routes alors il va choisir celui qui a une plus grande valeur. sinon (si dans le cas ou le weight est identique) alors il va passer dans le choix du l'as_path le plus court. cela justifie le choix du R1 de sortir vers R2 (AS 200) a cause de la valeur du weight la plus grand 15>10.

2. Dans le retour du paquets, le routeur R5 choisit de envoyer vers R1 directement (AS 300 vers AS 100), tout simplement parce que les valeurs de weight a son côté sont par défaut (ne sont pas configurées). et aussi les valeurs de weight ne sont pas partageables du coup les routeurs ne connaissent pas le chemin préférer par l'autre routeur.