

## Module 8 - Multi-homing Lab Stratégies

**Objectif:** Introduction à la politique de routage, la manipulation des attributs BGP pour contrôler le flux du trafic dans un réseau multi-homé.

**Prérequis:** Module 6 et 7

Topologie :

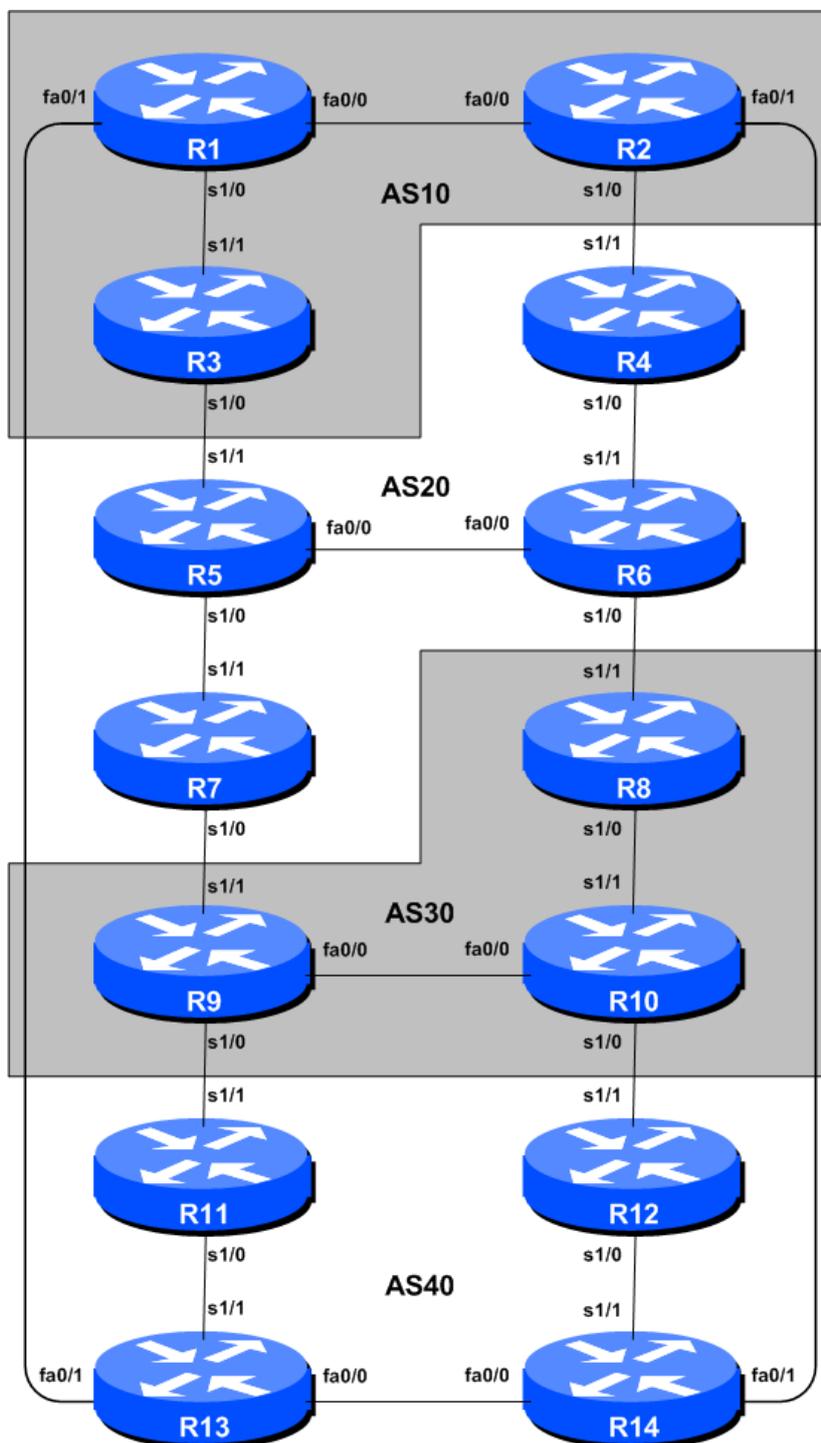


Figure 1 – nombre de BGP AS

## Notes de laboratoire

Ce module illustre comment un AS peut utiliser la *local pref* pour contrôler les chemins de routage sortants, et comment utiliser AS PATH prepend, MEDs (métriques) ou les communautés pour déterminer les chemins de routage entrants. Tous sont des outils très puissants pour les FAI pour contrôler la façon dont leurs liens de peering externes sont utilisés. Reportez-vous aux présentations BGP et de la documentation pour plus d'informations sur le processus de sélection du chemin BGP et les valeurs par défaut, et les priorités de la "LOCAL\_PREF" et les attributs de "métrique".

Avant de commencer ce module, conserver la topologie et les configurations telles qu'elles sont utilisées dans le Module 6. Cela exige le retrait de **toutes** les configurations de filtrage et de communauté examinées dans le module 7.

**Recommandation:** N'oubliez pas que si une configuration sur un routeur n'est pas en cours d'utilisation, **elle doit être retirée**. L'excédent de configuration donne généralement lieu à la détection des erreurs et le débogage de configurations difficile en cas de problèmes d'acheminement ou de défaillances du réseau.

## Exercice de laboratoire

1. **Mettre de l'ordre dans le Module 7.** Si le module précédent terminé était Module 7, la configuration du routeur doit être nettoyée avant la tentative de ce module. Les étapes suivantes montrent exactement ce qui est nécessaire.

### Exemple: Routeur R1

```
Router1#conf t
Router1(config)#router bgp 10
!
! Commencez par retirer la déclaration du plan de route du voisinage BGP
!
Router1(config-router)#no neighbor 10.10.15.14 route-map infiltrer in
!
! Maintenant, enlevez la communauté étiquette de référence du réseau
!
Router1(config-router)#no network 10.10.0.0 mask 255.255.240.0 route-map
community-tag
Router1(config-router)#network 10.10.0.0 mask 255.255.240.0
!
! Maintenant, enlevez les plan de route
!
Router1(config)#no route-map community-tag
Router1(config)#no route-map infiltrer
!
! Maintenant, enlevez liste de la communauté
!
Router1(config)#no ip community-list 1
!
! C'est la configuration jolie et soignée, la façon dont il devrait être.
!
Router1(config)#end
!
! Maintenant, effacez le peering BGP afin que la politique ancienne soit
supprimée
!
```

```
Router1#clear ip bgp 10.10.15.14 in
Router1#
```

**Checkpoint N°1:** Appelez votre instructeur de laboratoire et affichez le message suivant:

- i] Sortie de "show ip route" et "show ip bgp"
- ii] Les sorties de 'ping' et 'tracvers' des destinations différentes au sein du réseau
- iii] Les sorties de 'ping' et 'trace' après que le lien principal tombe en panne.

## 2. But du module:

L'objectif de ce module est de montrer comment obtenir un flux de trafic en utilisant quatre méthodes différentes. Ces quatre méthodes impliquent l'application de politiques pour la modification des flux de trafic sortant, et trois façons d'appliquer des politiques visant à modifier le flux de trafic entrant. Le lecteur doit examiner la présentation BGP donnée avant ce module comme un rappel sur la manière d'influencer le choix des chemins de politique en utilisant BGP.

Le diagramme suivant (Figure 2) montre les flux de trafic désiré entre les routeurs particuliers et AS. Huit flux de trafic doivent être mises en œuvre. Les flèches dans la figure indiquent les flux qui seront configurés. Chaque flèche provient d'un routeur de bordure dans un AS, et se termine sur l'un des routeurs dans un autre AS. Cela signifie que flux de trafic souhaité pour les liens entre les deux systèmes. Chacune des étapes suivantes a une description sur la façon de mettre en œuvre la circulation représenté par chaque flèche. Si à tout moment il y a n'importe quel doute quant à la configuration exigée, consultez la documentation CD de Cisco, ou demandez aux instructeurs de laboratoire.

- 3. Affectation de l'espace d'adresses dans chaque ASN.** Pour rendre les différentes politiques dans ce travail de module, nous allons subdiviser chaque bloc d'adresses attribué à chaque ASN afin que chaque routeur soit responsable d'annoncer chaque sous-préfixe. De cette façon, nous serons en mesure de cibler notre ingénierie de trafic basée sur ce que les routeurs annoncent au reste du réseau de laboratoires. Les affectations pour chaque ASN sont données dans le tableau suivant:

<b>AS10</b>		<b>AS30</b>	
<b>Router1</b>	<b>10.10.0.0/22</b>	<b>Router8</b>	<b>10.30.0.0/22</b>
<b>Router2</b>	<b>10.10.4.0/22</b>	<b>Router9</b>	<b>10.30.4.0/22</b>
<b>Router3</b>	<b>10.10.8.0/22</b>	<b>Router10</b>	<b>10.30.8.0/22</b>
<b>AS20</b>		<b>AS40</b>	
<b>Router4</b>	<b>10.20.0.0/22</b>	<b>Router11</b>	<b>10.40.0.0/22</b>
<b>Router5</b>	<b>10.20.4.0/22</b>	<b>Router12</b>	<b>10.40.4.0/22</b>
<b>Router6</b>	<b>10.20.8.0/22</b>	<b>Router13</b>	<b>10.40.8.0/22</b>
<b>Router7</b>	<b>10.20.12.0/22</b>	<b>Router14</b>	<b>10.40.12.0/22</b>

Chaque équipe de routeur devrait ajouter une instruction de réseau approprié dans leur BGP et route statique afin que leur /22 alloué soit annoncé dans le système BGP Voici un exemple pour Router5:

```
router bgp 20
network 10.20.4.0 mask 255.255.252.0
```

Friday, August 12, 2016

```
!  
ip route 10.20.4.0 255.255.252.0 null0
```

Comme nous allons faire le traceroute à travers le réseau pour vérifier que les politiques ont travaillé, c'est aussi une bonne idée de configurer une autre interface de bouclage avec une adresse hors du bloc adresse / 22. Chaque équipe doit choisir **Loopback1** et de lui donner la première adresse en dehors du bloc. Par exemple, sur le Router8:

```
interface loopback 1  
 ip address 10.30.0.1 255.255.255.255  
!
```

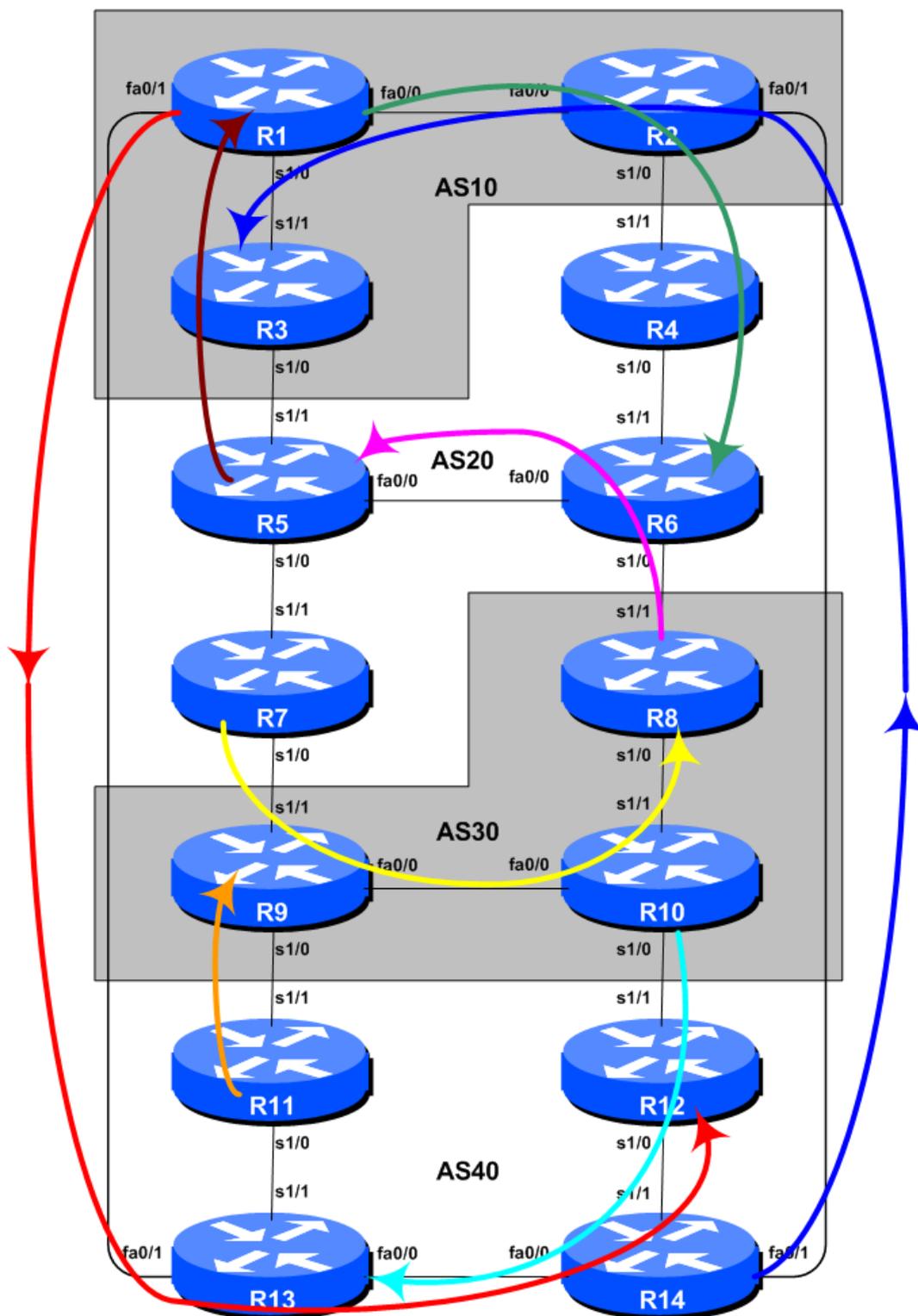


Figure 2 – chemins préférés

#### 4. Mettre en œuvre les politiques suivantes pour influencer sur les flux de trafic sortant à l'aide de LOCAL\_PREF:

Ce scénario montre comment influencer sur les flux de trafic sortant pour chaque AS. La préférence locale est appliquée aux annonces de routage de trafic entrant. Les blocs d'adresses définies à

l'étape précédente sont utilisés en tant que cible: ils sont adaptés sur les **peerings eBGP** et la préférence locale est fixée à un niveau élevé. Alors que nous avons mis la préférence locale à un niveau élevée sur le chemin préféré sortant, il est important que les chemins de sauvegarde devrait encore fonctionner - pour cette raison, nous avons également mis la préférence locale à un niveau suffisamment bas sur les autres sorties de l'ASN. Voici le principaux chemins/routage que nous voulons atteindre:

**AS 10:**

- Tout le trafic **VERS** 10.20.8.0/22 (R6) doit quitter AS 10 via le routeur R2 uniquement.
- Tout le trafic **VERS** 10.40.4.0/22 (R12) doit quitter AS 10 via le routeur R1 uniquement.

**AS 20:**

- Tout le trafic **VERS** 10.0.0/22 (R1) doit quitter AS 20 via le routeur R5 uniquement.
- Tout le trafic **VERS** 10.30.0.0/22 (R8) doit quitter AS 20 via le routeur R7 uniquement.

**AS 30:**

- Tout le trafic **VERS** 10.20.4.0/22 (R5) doit quitter AS 30 via le routeur R8 uniquement.
- Tout le trafic **VERS** 10.40.8.0/22 (R13) doit quitter AS 30 via le routeur R10 uniquement.

**AS 40:**

- Tout le trafic **VERS** 10.10.8.0/22 (R3) doit quitter AS 40 via le routeur R14 uniquement.
- Tout le trafic **VERS** 10.30.4.0/22 (R9) doit quitter AS 40 via le routeur R11 uniquement.

Notez que nous ne faisons que tenter de définir flux de trafic sortant. Le chemin de retour n'a aucune politique mise en application, et le processus de décision du chemin normal du routeur s'applique.

Les exemples de configuration ci-dessous doit être utilisée comme guide pour la configuration du routeur pour chaque équipe de routeur. Notez que pour chaque scénario, un routeur dans chaque AS devra définir les préférences locales à un niveau élevé et les routeurs restants dans l'AS les préférences locales seront réglées à un niveau bas. La motivation pour faire ça est la redondance de configuration. Si, par exemple, le routeur 7 perd sa configuration de préférence locale due à une erreur de l'opérateur, la préférence locale réglée à un niveau bas sur les trois autres routeurs veillera à ce que les politiques de circulation nécessaires seront encore mises en œuvre. Il est assez courant pour de nombreux FAI d'avoir plus d'une configuration à mettre en œuvre une politique en particulier - une configuration primaire, et une configuration "inverse " secondaire sur d'autres routeurs qui pourraient être touchés.

Étant donné qu'il existe deux scénarios pour chaque AS, chaque routeur de l'AS devrez créer un plan de route couvrant les deux scénarios. Notez qu'un seul plan de route peut être utilisé par session eBGP. L'exemple ci-dessous montre ce que la configuration du routeur 7 pourrait ressembler.

**Des exemples de configurations du routeur 7 pour le scénario AS 20 ci-dessus (à l'aide LOCAL\_PREF).**

```
ip prefix-list R1-prefix permit 10.10.0.0/22
ip prefix-list R8-prefix permit 10.30.0.0/22
!
route-map set-local-pref permit 10
  match ip address prefix-list R1-prefix
```

```

    set local-preference 50
    !
    route-map set-local-pref permit 20
    match ip address prefix-list R8-prefix
    set local-preference 200
    !
    route-map set-local-pref permit 30
    !
    router bgp 20
    neighbor 10.30.15.5 remote-as 30
    neighbor 10.30.15.5 route-map set-local-pref in
    !

```

**Checkpoint n° 2: Appelez votre instructeur de laboratoire et affichez le message suivant:**

*i] Chaque routeur dans un AS sera demandé de faire une «trace» vers des destinations sélectionnées, la trace doit montrer paquets qui quittent l'AS tel que spécifié dans l'exercice ci-dessus.*

*ii] Expliquez votre configuration utilisée pour obtenir le résultat souhaité à l'instructeur. Afficher la sortie de "show ip bgp", et "show ip bgp xxxx» pour les réseaux avec une préférence locale est réglée à 200. Montre la sortie de trace conformément aux instructions.*

*iii] Attendez que l'instructeur de laboratoire donne le feu vert pour passer à l'étape suivante.*

## ARRÊTEZ et ATTENDEZ ICI

5. **Supprimer la configuration de l'étape précédente.** Avant de passer à l'étape suivante, il est important que la configuration de l'étape précédente soit retirée. Cela consiste à enlever des plans de route, listes de préfixe et la configuration par voisin pour définir la préférence locale. Toutes les équipes routeur devrait faire ceci, puis effectuez une réinitialisation partielle (soft reset) de leurs peerings eBGP.
6. **Mettre en œuvre les stratégies suivantes pour influencer sur les flux de trafic entrants en utilisant les MEDs.** Cette étape présente l'une des trois méthodes d'influer sur les politiques entrants. Ici MEDs sont utilisés, alors que les prochaines étapes vont introduire l'usage des communautés BGP et AS PATH preprends. Comme pour l'étape précédente, lisez les instructions soigneusement et discuter dans votre équipe et votre AS, comment vous allez mettre en œuvre ce qui suit.

L'exemple de cette étape permet d'obtenir exactement le même flux de trafic entre les ASes voisins comme dans l'étape précédente pour les réseaux en question – n'oubliez pas que préférence locale est utilisée par un AS d'influer sur les chemins de trafic sortant, alors que les MEDs sont utilisés pour influencer sur les chemins de trafic entrant. Reportez-vous à la Figure 2 pour un tableau des flux de trafic...

### AS 10:

- Tout le trafic **VERS** 10.10.0.0/22 (R1) à partir de n'importe où dans AS 20 doit entrer dans AS 10 par le R5 - lien R3. (**Astuce:** cela signifie que R2 doit annoncer 10.10.0.0/22 à AS 20 avec une métrique supérieure à l'annonce équivalent de R3.)

- Tout le trafic **VERS** 10.10.8.0/22 (R3) à partir de n'importe où dans AS 40 doit entrer dans AS 10 par le R14 - lien R2. (**Astuce:** cela signifie que R1 doit annoncer 10.10.8.0/22 à AS 40 avec une métrique supérieure à l'annonce équivalent de R2.)

#### **AS 20:**

- Tout le trafic **VERS** 10.20.4.0/22 (R5) à partir de n'importe où dans AS 30 doit entrer dans AS 20 par le R8 - lien R6. (**Astuce:** cela signifie que R7 doit annoncer 10.20.4.0/22 à AS 30 avec une métrique supérieure à l'annonce équivalent de R6.)
- Tout le trafic **VERS** 10.20.8.0/22 (R6) à partir de n'importe où dans AS 10 doit entrer dans AS20 par le R2 - lien R4. (**Astuce:** cela signifie que R5 doit annoncer 10.20.8.0/22 à AS 10 avec une métrique supérieure à l'annonce équivalent de R4.)

#### **AS 30:**

- Tout le trafic **VERS** 10.30.0.0/22 (R8) à partir de n'importe où dans AS 20 doit entrer dans AS 30 par le R7 - lien R9. (**Astuce:** cela signifie que R8 doit annoncer 10.30.0.0/22 à AS 20 avec une métrique supérieure à l'annonce équivalent de R9.)
- Tout le trafic **VERS** 10.30.4.0/22 (R9) à partir de n'importe où dans AS 40 doit entrer dans AS 30 par le R11 - lien R9. (**Astuce:** cela signifie que R10 doit annoncer 10.30.4.0/22 à AS 40 avec une métrique supérieure à l'annonce équivalent de R9.)

#### **AS 40:**

- Tout le trafic **VERS** 10.40.4.0/22 (R12) à partir de n'importe où dans AS 10 doit entrer dans AS 40 par le R1 - lien R13. (**Astuce:** cela signifie que R14 doit annoncer 10.40.4.0/22 à AS 10 avec une métrique supérieure à l'annonce équivalent de R13.)
- Tout le trafic **VERS** 10.40.8.0/22 (R13) à partir de n'importe où dans AS 30 doit entrer dans AS 40 par le R10 - lien R12. (**Astuce:** cela signifie que R11 doit annoncer 10.40.8.0/22 à AS 30 avec une métrique supérieure à l'annonce équivalent de R12.)

#### **Exemple de configuration pour le routeur 6 pour le scénario AS 20 ci-dessus (à l'aide MED).**

```
ip prefix-list R5-prefix permit 10.20.4.0/22
ip prefix-list R6-prefix permit 10.20.8.0/22
!
route-map set-med permit 10
  match ip address prefix-list R5-prefix
  set metric 10
!
route-map set-med permit 20
  match ip address prefix-list R6-prefix
  set metric 50
!
route-map set-med permit 30
!
router bgp 20
  neighbor 10.20.15.18 remote-as 30
  neighbor 10.20.15.18 route-map set-med out
!
```

**Checkpoint n° 3: Appelez votre instructeur de laboratoire et affichez suivant:**

*i] Chaque routeur dans un AS sera demandé de faire un 'traceroute' vers des destinations sélectionnées, la trace doit montrer les paquets qui quittent l'AS tel que spécifié dans l'exercice ci-dessus.*

*ii] Expliquez votre configuration utilisée pour obtenir le résultat souhaité à l'instructeur. Afficher la sortie de "show ip bgp", et "show ip bgp x.x.x.x" pour les réseaux avec MED fixé à 50. Montre la sortie de trace conformément aux instructions.*

## ARRÊTEZ et ATTENDEZ ICI

7. **Supprimer la configuration de l'étape précédente.** Avant de passer à l'étape suivante, il est important que la configuration de l'étape précédente soit retirée. Cela consiste à enlever les plan de routes, les listes de préfixes et la configuration par voisin pour définir les MEDs. Toutes les équipes de routeur devrait le faire, et puis de faire une actualisation de route de leurs peerings eBGP.
8. **Mise en œuvre de politiques à l'aide des communautés BGP.** Cette section décrit comment utiliser les communautés BGP pour influencer les politiques entrants. Plutôt que d'utiliser les MEDs comme nous l'avons fait dans le scénario précédent (étape 6), on signalera à nos voisins ASN en utilisant les communautés BGP. Pour se préparer à cela, nous devons déterminer quelles communautés mettront en œuvre les politiques de remplacement des MEDs. MED réglé à un niveau bas signifie que le chemin serait préféré à un MED à niveau élevé. Cela pourrait être reproduit dans le pair AS par ce AS réglé à un niveau élevé de la préférence locale sur le chemin qui aurait entendu le MED à niveau bas, et en mettant à niveau bas la préférence locale sur le chemin qui aurait entendu le MED à niveau élevé.
9. **Choisissez les communautés à définir de haute et basse priorité pour le trafic sortant.** En tant que recommandation, configurer la communauté <localASN> : 150 pour définir une priorité élevée pour le trafic sortant et <localASN> : 50 pour définir une priorité basse pour le trafic sortant. Cela signifie que chaque AS devrez configurer une communauté correspondant le plan de route pour définir la valeur appropriée de la préférence locale.

### Exemple de configuration du routeur dans AS20

```
ip community-list 1 permit 20:150
ip community-list 2 permit 20:50
```

10. **Régler la configuration du plan de route pour appliquer la politique** de la communauté. Nous créons maintenant un plan de route qui définira la préférence locale pour chacune des communautés. Si le voisin eBGP nous envoie la communauté attachée à un préfixe, nous appliquerons la préférence locale au préfixe selon la valeur de la communauté attachée

### Exemple de Configuration

```
route-map customer-comm permit 10
  match community 1
  set local-preference 150
!
route-map customer-comm permit 20
```

```
match community 2
set local-preference 50
!
route-map customer-comm permit 30
!
```

**11. Appliquer le plan de route pour eBGP voisins.** Avec la plan de route configuré, nous l'appliquons maintenant à tous nos voisins eBGP Quand ils envoient des préfixes avec la définition appropriée des communautés, nous allons maintenant définir la préférence locale.

### Exemple de configuration du routeur 8

```
router bgp 30
neighbor 10.20.15.17 remote-as 20
neighbor 10.20.15.17 description eBGP peering with R6
neighbor 10.20.15.17 route-map customer-comm in
!
```

Alors que le concept semble plus complexe à première vue, il évolue en fait beaucoup mieux que le prestataire de services est en mesure de standardiser leur configuration de la politique en utilisant les communautés à travers leur réseau d'accès.

**12. Mettre en œuvre les stratégies suivantes pour influencer sur les flux de trafic entrants en utilisant les communautés BGP.** Comme pour l'étape précédente, lisez les instructions soigneusement et discuter dans votre équipe et votre AS, comment vous allez mettre en œuvre ce qui suit.

L'exemple de cette étape permet d'obtenir exactement le même flux de trafic entre les AS voisins comme dans l'étape précédente pour les réseaux en question. Reportez-vous à la Figure 2 pour un tableau des flux de trafic...

#### AS 10:

- Tout le trafic **VERS** 10.10.0.0/22 (R1) à partir de n'importe où dans AS 20 doit entrer dans AS 10 par le R5 - lien R3. (**Astuce** : cela signifie que R2 doit annoncer 10.10.0.0/22 AS 20 avec la communauté de faible priorité de AS20 alors que l'annonce équivalente de R3 a besoin d'une communauté de AS20 de haute priorité)
- Tout le trafic **VERS** 10.10.8.0/22 (R3) à partir de n'importe où dans AS 40 doit entrer dans AS 10 par le R14 - lien R2. (**Astuce** : cela signifie que R1 doit annoncer 10.10.8.0/22 AS 40 avec la communauté de faible priorité de AS40 alors que l'annonce équivalente de R2 a besoin d'une communauté de AS40 de haute priorité)

#### AS 20:

- Tout le trafic **VERS** 10.20.4.0/22 (R5) à partir de n'importe où dans AS 30 doit entrer dans AS 20 par le R8 - lien R6. (**Astuce** : cela signifie que R7 doit annoncer 10.20.4.0/22 AS 30 avec la communauté de faible priorité de AS30 alors que l'annonce équivalente de R6 a besoin d'une communauté de AS30 de haute priorité)
- Tout le trafic **VERS** 10.20.8.0/22 (R6) à partir de n'importe où dans AS 10 doit entrer dans AS 20 par le R2 - lien R4. (**Astuce** : cela signifie que R5 doit annoncer 10.20.8.0/22 AS 10 avec la communauté de faible priorité de AS10 alors que l'annonce équivalente de R4 a besoin d'une communauté de AS10 de haute priorité)

**AS 30:**

- Tout le trafic **VERS** 10.30.0.0/22 (R8) à partir de n'importe où dans AS 20 doit entrer dans AS 30 par le R7 - lien R9. (**Astuce** : cela signifie que R8 doit annoncer 10.30.0.0/22 AS 20 avec la communauté de faible priorité de AS20 alors que l'annonce équivalente de R9 a besoin d'une communauté de AS20 de haute priorité)
- Tout le trafic **VERS** 10.30.4.0/22 (R9) à partir de n'importe où dans AS 40 doit entrer dans AS 30 par le R11 - lien R9. (**Astuce** : cela signifie que R10 doit annoncer 10.30.4.0/22 AS 40 avec la communauté de faible priorité de AS40 alors que l'annonce équivalente de R9 a besoin d'une communauté de AS40 de haute priorité)

**AS 40:**

- Tout le trafic **VERS** 10.40.4.0/22 (R12) à partir de n'importe où dans AS 10 doit entrer dans AS 40 par le R1 - lien R13. (**Astuce** : cela signifie que R14 doit annoncer 10.40.4.0/22 AS 10 avec la communauté de faible priorité de AS10 alors que l'annonce équivalente de R13 a besoin d'une communauté de AS10 de haute priorité)
- All traffic **TO** 10.40.8.0/22 (R13) from anywhere in AS 30 must enter AS 40 via the R10 – R12 link. (**Astuce** : cela signifie que R11 doit annoncer 10.40.8.0/22 AS 30 avec la communauté de faible priorité de AS30 alors que l'annonce équivalente de R12 a besoin d'une communauté de AS30 de haute priorité)

Regardez les exemples suivants pour voir ce qui doit être fait pour chaque équipe de routeur.

**Exemple de configuration pour Router8 pour le scénario AS 20 ci-dessus (à l'aide de la communauté).**

```
ip prefix-list R8-prefix permit 10.30.0.0/22
!
route-map set-comm permit 10
  match ip address prefix-list R8-prefix
  set community 30:50
!
route-map set-comm permit 20
!
router bgp 30
  neighbor 10.20.15.17 remote-as 20
  neighbor 10.20.15.17 description eBGP peering with R6
  neighbor 10.20.15.17 route-map set-comm out
  neighbor 10.20.15.17 route-map customer-comm in
!
```

**Checkpoint n°4: Appelez votre instructeur de laboratoire et affichez le message suivant:**

*i] Chaque routeur dans un AS sera demandé de faire un 'traceroute' vers des destinations sélectionnées, la trace doit montrer les paquets qui quittent l'AS tel que spécifié dans l'exercice ci-dessus.*

*ii] Expliquez votre configuration utilisée pour obtenir le résultat souhaité à l'instructeur. Affichez la sortie de "show ip bgp", et "show ip bgp x.x.x.x" pour les réseaux avec les communautés configurés. Montre la sortie de trace conformément aux instructions.*

## ARRÊTEZ et ATTENDEZ ICI

**13. Supprimer la configuration utilisée pour l'étape précédente.** Avant de passer à l'étape suivante, il est important que la configuration de l'étape précédente soit retirée. Cela consiste à enlever les plans de route, les listes de préfixes et la configuration par voisinage pour définir les communautés. Toutes les équipes routeur devrait faire ceci, puis effectuez une réinitialisation partielle (soft reset) de leurs peerings eBGP.

**14. Mettre en œuvre les politiques suivantes pour influencer sur les flux de trafic entrant en utilisant AS path prepend.** Cette étape introduit le second des deux méthodes pour influencer les politiques entrants. Comme pour l'étape précédente, lisez les instructions soigneusement et discuter dans votre équipe et votre AS, comment vous allez mettre en œuvre ce qui suit.

L'exemple de cette étape permet d'obtenir exactement le même flux de trafic entre les AS voisins comme dans l'étape précédente pour les réseaux en question. Reportez-vous à la Figure 2 pour un tableau des flux de trafic...

### AS 10:

- Tout le trafic **VERS** 10.10.8.0/22 (R3) à partir de n'importe où dans la topologie du laboratoire doit entrer dans AS 10 par le R14 - lien R2. (**Astuce:** cela signifie que le R1 et R3 doivent annoncer 10.10.8.0/22 avec un AS path plus long que les autres réseaux dans AS 10. R2 a besoin d'annoncer 10.10.8.0/22 avec un AS path plus long dans son peering avec R4.)
- Tout le trafic **VERS** 10.10.0.0/22 (R1) à partir de n'importe où dans la topologie du laboratoire doit entrer dans AS 10 par le R5 - lien R3. (**Astuce:** cela signifie que le R1 et R2 doivent annoncer 10.10.0.0/22 avec un AS path plus long que les autres réseaux dans AS 10.)

### AS 20:

- Tout le trafic **VERS** 10.20.4.0/22 (R5) à partir de n'importe où dans la topologie du laboratoire doit entrer dans AS 20 par le R8 - lien R6. (**Astuce:** cela signifie que le R4, R5 et R7 doivent annoncer 10.20.4.0/22 avec un AS path plus long que les autres réseaux dans AS 20.)
- Tout le trafic **VERS** 10.20.8.0/22 (R6) à partir de n'importe où dans la topologie du laboratoire doit entrer dans AS 20 par le R2 - lien R4. (**Astuce:** cela signifie que le R5, R6 et R7 doivent annoncer 10.20.8.0/22 avec un AS path plus long que les autres réseaux dans AS 20.)

### AS 30:

- Tout le trafic **VERS** 10.30.0.0/22 (R8) de n'importe où dans le laboratoire de la topologie doit entrer AS 30 via la R7 – R9 lien. (**Astuce:** cela signifie que le R8 et R10 doivent annoncer 10.30.0.0/22 avec un AS path plus long que les autres réseaux dans AS 30. R9 a besoin d'annoncer 10.30.0.0/22 avec un AS path plus long dans son peering avec R11.)
- Tout le trafic **VERS** 10.30.4.0/22 (R9) à partir de n'importe où dans la topologie du laboratoire doit entrer dans AS 30 par le R11 - lien R9. (**Astuce:** cela signifie que le R8 et R10 doivent annoncer 10.30.4.0/22 avec un AS path plus long que les autres réseaux dans AS 30. R9 a besoin d'annoncer 10.30.4.0/22 avec un AS path plus long dans son peering avec R7.)

### AS 40:

- Tout le trafic **VERS** 10.40.4.0/22 (R12) à partir de n'importe où dans la topologie du laboratoire doit entrer dans AS 40 par le R1 - lien R13. (**Astuce:** cela signifie que le R11, R12 et R14 doivent annoncer 10.40.4.0/22 avec un AS path plus long que les autres réseaux dans AS 40.)

- Tout le trafic **VERS** 10.40.4.0/22 (R12) à partir de n'importe où dans la topologie du laboratoire doit entrer dans AS 40 par le R10 - lien R12. (**Astuce:** cela signifie que le R11, R13 et R14 doivent annoncer 10.40.8.0/22 avec un AS path plus long que les autres réseaux dans AS 40.

AS\_PREPEND est couramment utilisé par les petits FAI qui sont multi-homing à leurs fournisseurs en amont. C'est la convention sur l'Internet d'ajouter au moins deux AS lors de l'utilisation de AS\_PREPEND. Plus généralement, trois AS sont ajoutés, surtout si les FAI en amont ont des liens les uns aux autres, en passant par une tierce partie.

### Exemple de configuration pour le Routeur 9 pour le scénario AS 30 ci-dessus (à l'aide AS PATH prepend).

```
ip prefix-list R8-prefix permit 10.30.0.0/22
ip prefix-list R9-prefix permit 10.30.4.0/22
!
route-map set-path-as20 permit 10
  match ip address prefix-list R9-prefix
  set as-path prepend 30 30 30
!
route-map set-path-as20 permit 20
!
route-map set-path-as40 permit 10
  match ip address prefix-list R8-prefix
  set as-path prepend 30 30 30
!
route-map set-path-as40 permit 20
!
router bgp 30
  neighbor 10.20.15.6 remote-as 20
  neighbor 10.20.15.6 descr eBGP peering with R7
  neighbor 10.20.15.6 route-map set-path-as20 out
  neighbor 10.40.15.1 remote-as 40
  neighbor 10.40.15.1 descr eBGP peering with R11
  neighbor 10.40.15.1 route-map set-path-as40 out
!
```

### **Checkpoint n° 5: Appelez l'instructeur de laboratoire et affichez suivant:**

*i] Chaque routeur dans un AS sera demandé de faire un 'traceroute' vers des destinations sélectionnées, la trace doit montrer les paquets qui quittent l'AS tel que spécifié dans l'exercice ci-dessus.*

*ii] Expliquez votre configuration utilisée pour obtenir le résultat souhaité à l'instructeur. Affichez la sortie de "show ip bgp", et "show ip bgp x.x.x.x» pour les réseaux avec une augmentation de la longueur du chemin AS. Montre la sortie de trace conformément aux instructions.*

*iii] Comment AS Path prepend a changé la table BGP et la décision de routage. La décision peut être annulée en utilisant toute autre configuration BGP dans un AS? **Réponse:** revoir les règles de sélection de route BGP de la diapositive dans la section présentation.*

## 15. Résumé:

Ce module a démontré de plusieurs manières d'influencer les politiques de routage entrant et sortant.

**Q:** Quelle est la différence dans les effets qui en résultent à l'aide des méthodes dans les étapes 6, 8 et 14?

**A:** AS PATH prepend affecte les annonces du routage entre deux AS, et est visible partout, même en dehors des deux AS qui font usage de l'information prepend. MEDs ne s'appliquent qu'entre plusieurs peerings entre le même AS. Si le pair AS annonce le local AS en avant, l'ensemble de la métrique est celle du pair AS, et non l'AS local. Les communautés ne sont généralement utilisées dans les peerings entre voisins ASN.

Consultez la documentation de BGP pour plus d'informations. Il existe de nombreuses variations possibles sur les exemples donnés dans ce module. N'oubliez pas les points suivants :

- La préférence locale est utilisée pour influencer la politique au sein d'un AS
- MEDs servent à influencer les politiques sur les multiples liens entre le local et un AS immédiatement voisin
- BGP communautés peuvent également servir à influencer les politiques sur les multiples liens entre le local et le voisinage AS
- Le AS path prepend est utilisé pour influencer la politique extérieure à l'échelle mondiale (y compris l'AS au voisinage immédiat).

## Questions de révision

1. Quelle est la façon la plus efficace d'influencer la façon dont le trafic quitte votre réseau?
2. Comment utile pensez-vous que les MEDs sont dans Internet? Considérez la réponse à la première question avant de répondre!