Configurer la fonctionnalité d'autorisation d'accès dans BGP

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
  - Conventions
    - Exemple
- Informations générales
- Configurer
  - Diagramme du réseau
  - Configurations
- Vérifier
- Dépannage
  - Message d'erreur
- Informations connexes

Introduction

Ce document décrit une situation où deux routeurs de branche se connectent via un FAI et exécutent BGP entre eux.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Fournisseur d'accès Internet (FAI)
- Protocole BGP (Border Gateway Protocol)

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Conventions

Pour configurer les routeurs de périphérie du fournisseur (PE) afin d'autoriser la réannonce de tous les préfixes contenant des numéros de système autonome (ASN) dupliqués, utilisez la commande neighbor allowas-in en mode de configuration du routeur. Pour désactiver la réannonce de l'ASN du routeur PE, utilisez la forme de cette commande.

neighbor ip-address allowas-in [numéro]

no neighbor allowas-in [nombre]

ip-address	Adresse IP du routeur voisin.
numéro	(Facultatif) Spécifie le nombre de fois où l'annonce du numéro de système autonome d'un routeur PE est autorisée. La plage est comprise entre 1 et 10. Si aucun nombre n'est fourni, la valeur par défaut de 3 est utilisée.

Dans une configuration Hub and Spoke, un routeur PE annonce à nouveau tous les préfixes contenant des numéros de système autonome dupliqués. Utilisez la commande neighbor allowas-in pour configurer deux VRF sur chaque routeur PE afin de recevoir et de réannoncer les préfixes suivants :

- Une instance VRF (Virtual Private Network Routing and Forwarding) reçoit des préfixes avec ASN de tous les routeurs PE, puis les annonce aux routeurs PE voisins.
- L'autre VRF reçoit des préfixes avec des ASN du routeur de périphérie client (CE) et les annonce à nouveau à tous les routeurs PE dans la configuration Hub and Spoke.

Vous contrôlez le nombre de fois qu'un ASN est annoncé en spécifiant un nombre compris entre 1 et 10.

Exemple

Cet exemple montre comment configurer le routeur PE avec l'ASN 100 pour autoriser les préfixes de la famille d'adresses VRF VPN IPv4 vrf1. Le routeur PE voisin avec l'adresse IP 192.168.255.255 est configuré pour être annoncé à nouveau à d'autres routeurs PE avec le même ASN six fois.

<#root>

```
Router(config)#
```

router bgp 100

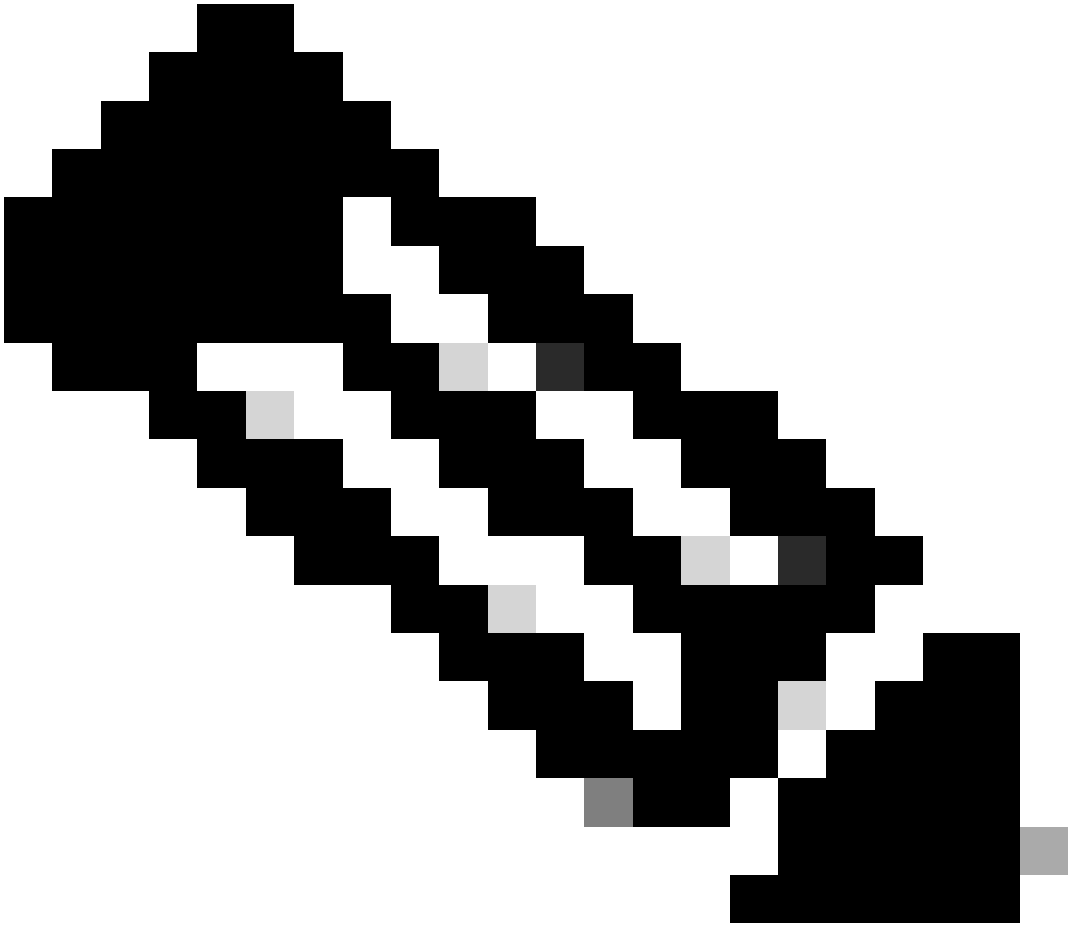
```
Router(config-router)#
```

```
address-family ipv4 vrf vrf1


Router(config-router)#
neighbor 192.168.255.255 allowas-in 6
```

Informations générales

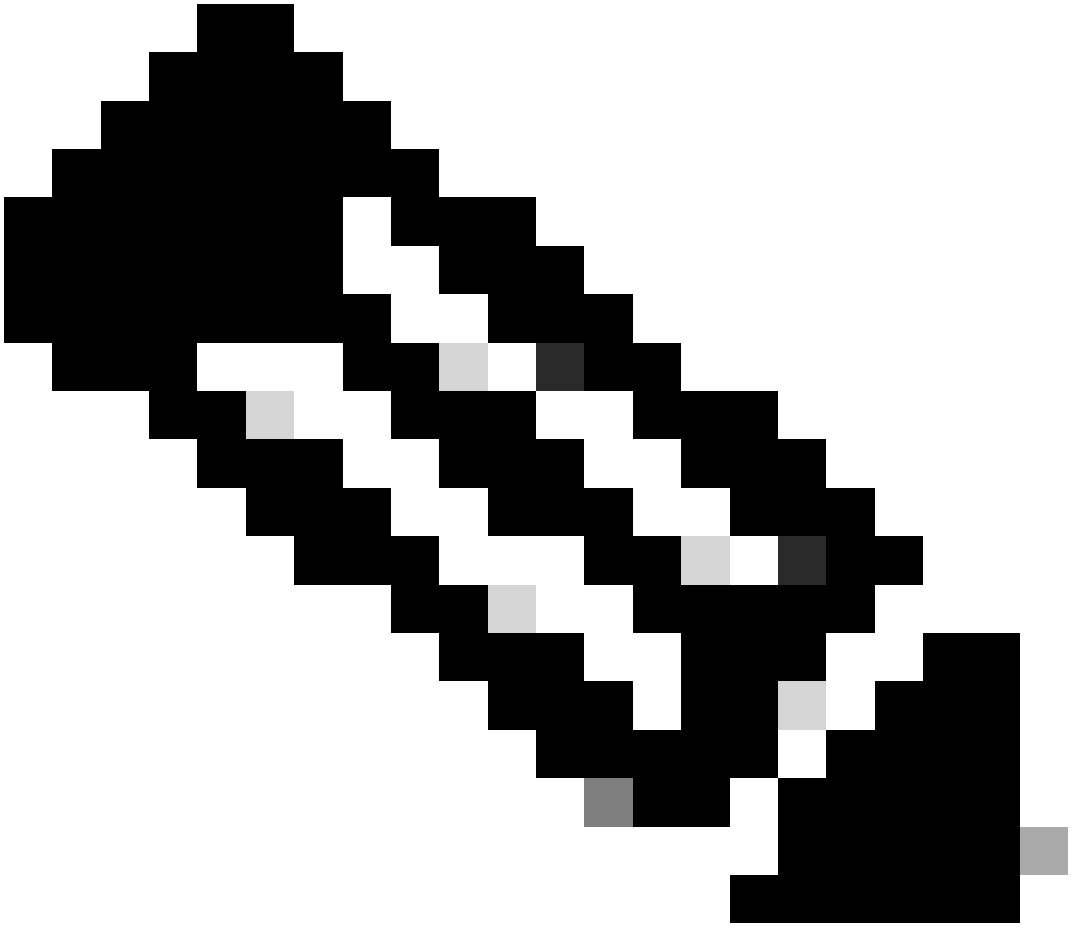
Ce document décrit un scénario dans lequel deux routeurs de filiale sont connectés via un fournisseur de serveur Internet (ISP) et exécutent le protocole BGP (Border Gateway Protocol) entre eux. Les deux routeurs de branche (R1 et R2), bien qu'ils se trouvent à des emplacements différents, partagent le même numéro de système autonome. Une fois que les routes arrivent d'une filiale (R1 dans ce cas) vers le réseau du fournisseur de services (SP), elles peuvent être étiquetées avec l'utilisateur AS. Lorsque le SP le passe à l'autre routeur de branche (R2), par défaut, les routes peuvent être abandonnées si l'autre branche exécute également BGP avec le SP et utilise le même numéro de système autonome. Dans ce scénario, la commande neighbor allowas-in est émise afin de permettre au BGP de l'autre côté d'injecter des mises à jour. Ce document fournit un exemple de configuration qui vous aide à comprendre la fonctionnalité d'autorisation d'accès dans BGP.



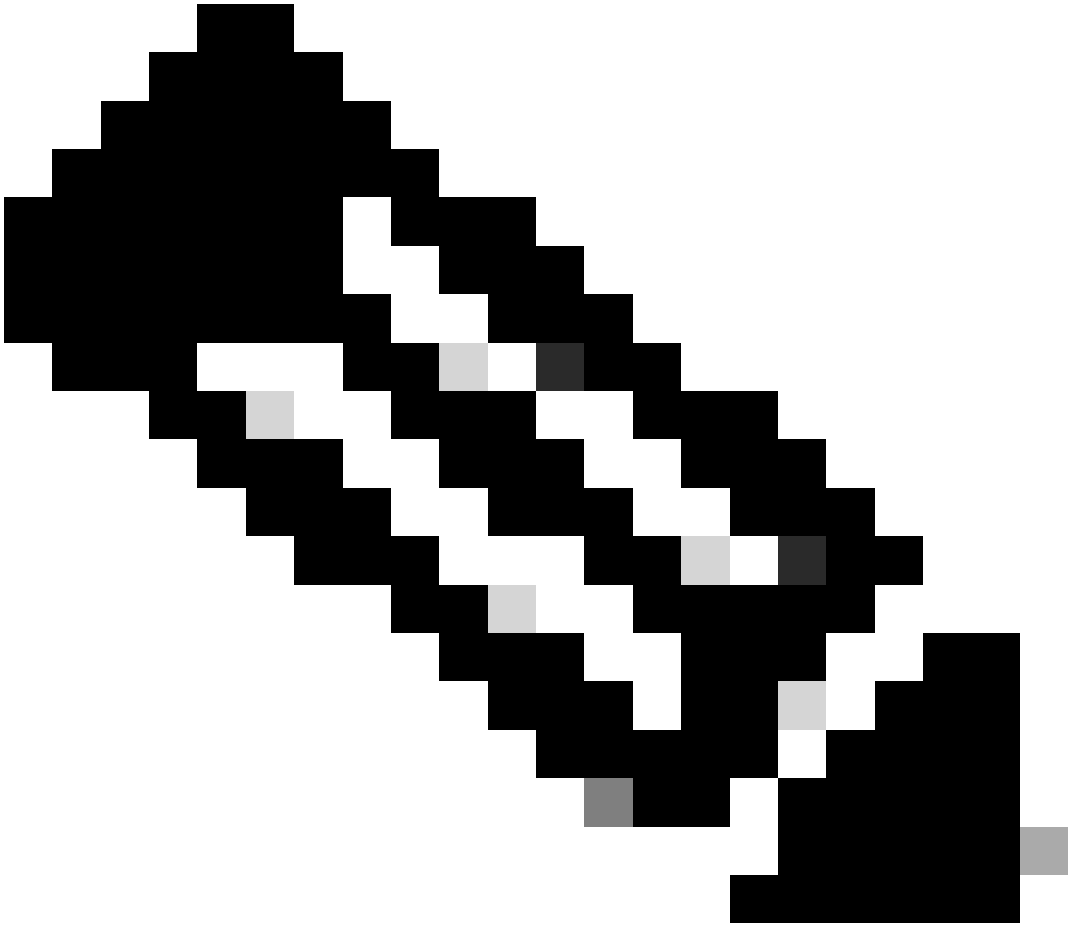
Remarque : Cette fonctionnalité ne peut être utilisée que pour les vrais homologues eBGP. Vous ne pouvez pas utiliser cette fonctionnalité pour deux homologues qui sont membres de différents sous-AS de confédération.

Configurer

Cette section vous présente les informations permettant de configurer les fonctionnalités décrites dans ce document.



Remarque : Utilisez l'outil Command Lookup Tool pour obtenir plus d'informations sur les commandes utilisées dans ce document.



Remarque : Seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations et aux outils Cisco internes.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

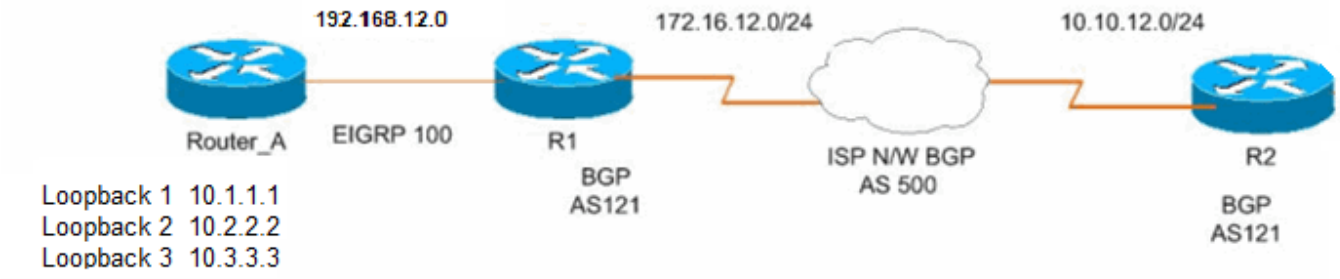


Diagramme du réseau

Configurations

Ce document utilise les configurations suivantes :

- Routeur A
- Routeur R1
- Routeur R2

Configuration sur le routeur A

```
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
interface Loopback2
 ip address 10.2.2.2 255.255.255.255
!
interface Loopback3
 ip address 10.3.3.3 255.255.255.255
!
interface GigabitEthernet0/1
 no switchport
 ip address 192.168.12.2 255.255.255.0
!
router eigrp 100
 network 10.1.1.1 0.0.0.0
 network 10.2.2.2 0.0.0.0
 network 10.3.3.3 0.0.0.0
 network 192.168.12.0
 auto-summary
!
```

Configuration sur le routeur R1

```
interface Loopback22
 ip address 10.22.22.22 255.255.255.255
!
interface FastEthernet0/0
 ip address 192.168.12.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial1/0
 ip address 172.16.12.1 255.255.255.0
!
!
router eigrp 100
 network 192.168.12.0
 no auto-summary
!
router bgp 121
 no synchronization
```

```
 bgp router-id 10.22.22.22
 bgp log-neighbor-changes
 network 10.22.22.22 mask 255.255.255.255

!--- This is the advertising loopback address.

 redistribute eigrp 100

!--- This shows the redistributing internal routes in BGP.

 neighbor 172.16.12.2 remote-as 500

!--- This shows the EBGP connection with ISP.

 neighbor 172.16.12.2 ebgp-multihop 5
 no auto-summary
!
```

Cet exemple montre que le protocole EIGRP s'exécute entre le routeur A et le routeur R1 :

<#root>

r1#

show ip eigrp neighbors

```
IP-EIGRP neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.12.2              Fa0/0            14 01:17:12  828  4968  0  7
```

Cet exemple montre comment le routeur R1 apprend les routes à partir du routeur A via le protocole EIGRP :

<#root>

r1#

show ip route eigrp 100

```
D    10.0.0.1/8 [90/156160] via 192.168.12.2, 00:02:24, FastEthernet0/0
D    10.0.0.2/8 [90/156160] via 192.168.12.2, 00:02:24, FastEthernet0/0
D    10.0.0.3/8 [90/156160] via 192.168.12.2, 00:02:24, FastEthernet0/0
```

Cet exemple montre comment le routeur R1 établit une connexion BGP avec un FAI exécutant BGP AS500 :

<#root>

r1#

show ip bgp summary

```
BGP router identifier 10.22.22.22, local AS number 121
BGP table version is 19, main routing table version 19
7 network entries using 924 bytes of memory
7 path entries using 364 bytes of memory
5/4 BGP path/bestpath attribute entries using 840 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 2) using 32 bytes of memory
BGP using 2184 total bytes of memory
BGP activity 40/33 prefixes, 42/35 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.12.2     4          500      86      76       19    0    0 00:25:13        2
```

Cet exemple montre comment R1 annonce les routes apprises BGP :

<#root>

r1#

show ip bgp

```
BGP table version is 19, local router ID is 10.22.22.22
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.0.0.1         192.168.12.2           156160         32768 ?
*> 10.0.0.2         192.168.12.2           156160         32768 ?
*> 10.0.0.3         192.168.12.2           156160         32768 ?
*> 10.10.12.0/24    172.16.12.2                0             0 500 i
*> 10.22.22.22/32   0.0.0.0                    0         32768 i
r> 172.16.12.0/24   172.16.12.2                0             0 500 i
*> 192.168.12.0     0.0.0.0                    0         32768 ?
```

<#root>

r1#

ping 10.10.12.2

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.12.2, timeout is 2 seconds:
!!!!!
!--- This is the connectivity with Router 2 across the Internet cloud.
```

Configuration sur le routeur R2
interface Loopback33 ip address 10.33.33.33 255.255.255.255

```
!
interface Serial1/0
 ip address 10.10.12.1 255.255.255.0
!
router bgp 121
 no synchronization
 bgp router-id 10.33.33.33
 bgp log-neighbor-changes
 network 10.33.33.33 mask 255.255.255.255

!--- This is the advertising loopback address.

 neighbor 10.10.12.2 remote-as 500

!--- This is the EBGP connection with ISP.

 neighbor 10.10.12.2 ebgp-multihop 5
 no auto-summary
!
```

Le routeur R2 n’apprend aucune route du routeur R1.

C'est un comportement naturel car le BGP essaie d'éviter les boucles de routage. Par exemple, la réannonce de tous les préfixes contenant des numéros de système autonome (ASN) en double est désactivée par défaut.

Les routes EIGRP redistribuées (10.0.0.1, 10.0.0.2, 10.0.0.3) et la route interne BGP 10.22.22.22 de R1 ne sont pas reçues par R2 car elles proviennent du même ASN sur Internet. Comme R2 voit son propre numéro de système autonome (121) dans l'AS-PATH, R2 n'emprunte pas ces routes.

<#root>

r2#

show ip bgp

```
BGP table version is 20, local router ID is 10.33.33.33
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
r> 10.10.12.0/24    10.10.12.2               0             0 500 i
*> 10.33.33.33/32   0.0.0.0                  0         32768 i
*> 172.16.12.0/24   10.10.12.2               0             0 500 i
```

Afin de permettre la réannonce de tous les préfixes qui contiennent des ASN dupliqués, utilisez la commande neighbor allowas-in en mode de configuration de routeur dans le routeur R2.

<#root>

```
r2(config-router)#
neighbor 10.10.12.2 allowas-in
r2#
clear ip bgp *
r2#
show ip bgp
BGP table version is 10, local router ID is 10.33.33.33
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.0.0.1          10.10.12.2                             0 500 121 ?
*> 10.0.0.2          10.10.12.2                             0 500 121 ?
*> 10.0.0.3          10.10.12.2                             0 500 121 ?
r> 10.10.12.0/24     10.10.12.2               0             0 500 i
*> 10.22.22.22/32    10.10.12.2                             0 500 121 i
*  10.33.33.33/32    10.10.12.2                             0 500 121 i
*>                   0.0.0.0                  0         32768 i
*> 172.16.12.0/24    10.10.12.2               0             0 500 i
*> 192.168.12.0      10.10.12.2                             0 500 121 ?
```

Essayez à présent d'envoyer une requête ping de R1 à R2 :

```
<#root>
r2#
ping 10.22.22.22
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.22.22.22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/57/60 ms
```

Vérifier

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Message d'erreur

La route fictive de récupération A.B.C.D du voisin « %BGP% » : Message d'erreur « AS loop » reçu.

Cette notification signifie que la route BGP reçue par le routeur CE a son propre numéro AS dans

le chemin AS et est considérée comme une boucle de routeur pour le routeur CE. Pour contourner ce problème, configurez le routeur CE avec la fonctionnalité « allowas-in », comme illustré dans l'exemple précédent.

Informations connexes

- Protocole BGP (Border Gateway Protocol)
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.