

Redistribuer OSPF entre différents processus OSPF

Table des matières

[Introduction](#)

[Informations générales](#)

[Pourquoi redistribuer entre deux processus OSPF](#)

[Filtrer la route OSPF](#)

[Itinéraires intra-zone](#)

[Routes inter-zones](#)

[Filtrage des routes externes](#)

[Séparer les différents domaines OSPF](#)

[Redistribuer entre différents processus OSPF](#)

[Règle de préférence de routage OSPF](#)

[Un point de redistribution unique](#)

[Deux points de redistribution](#)

[Distance administrative](#)

[Fonctionnement du réseau sans défaillance du réseau](#)

[Fonctionnement du réseau avec défaillance du réseau](#)

[Solution proposée](#)

[Utiliser la commande Distance 255](#)

[Filtrer les routes en fonction des balises](#)

[Utiliser le mot-clé interne lors de la redistribution](#)

[Filtrage basé sur le préfixe](#)

[Filtrage basé sur le préfixe et distance administrative basée sur le préfixe](#)

[Résumé](#)

[Informations connexes](#)

Introduction

Ce document décrit les directives pour la redistribution d'Open Shortest Path First (OSPF) entre différents processus.

Informations générales

La redistribution entre différents processus est difficile, et des mesures spéciales sont nécessaires pour le bon fonctionnement du réseau. Ce document met en valeur également quelques changements apportés dans le logiciel Cisco IOS®.

Pourquoi redistribuer entre deux processus OSPF

Il peut y avoir plusieurs raisons pour la redistribution entre plusieurs processus. En voici quelques exemples :

- Filtrer une route OSPF depuis une partie du domaine
- Séparer les différents domaines OSPF
- Migrer entre des domaines distincts

Bien que la redistribution entre différents processus puisse être nécessaire dans certains cas, une solution de conception alternative (si possible) est un choix plus approprié et est traitée dans les sous-sections de cette section.

Filtrer la route OSPF

Itinéraires intra-zone

Dans OSPF, les préfixes IP d'une zone ne sont pas échangés directement entre les routeurs. Ils font partie de la LSA (Link State Advertisement) qui annonce également la topologie du réseau ; par conséquent, il n'y a aucun moyen de filtrer les routes dans une zone.

 Remarque : le filtrage local sur un routeur (qui peut être effectué afin d'empêcher certaines routes d'être installées dans un routeur donné) n'est pas considéré comme un filtrage de route réel. Ceci est normalement accompli avec la commande `distribute-list` sous le routeur OSPF.

Une solution consisterait à utiliser un processus différent et à filtrer les routes souhaitées sur les routeurs de redistribution ; cependant, cela sépare réellement la zone en deux domaines. Une meilleure conception consisterait à séparer la zone en différentes zones et à utiliser la fonctionnalité de filtrage de type 3 de Cisco IOS, qui est expliquée plus loin.

Routes inter-zones

Dans le protocole OSPF, tous les routeurs d'une zone ont la même topologie. Une zone ne connaît pas la topologie d'une autre zone ; par conséquent, elle s'appuie sur les informations annoncées par les routeurs ABR (Area Border Routers) connectés.

Les informations annoncées à l'intérieur d'une zone par un ABR (sous la forme d'une LSA de type 3) sont en fait les préfixes IP qui sont appris à partir de zones distantes ou qui sont calculés pour d'autres zones connectées.

Un ABR crée ces routes :

- Routes intra-zone non fédératrices vers le réseau fédérateur
- Routes de backbone intra-zone et inter-zone vers une zone non de backbone

Par conséquent, entre les zones, un comportement de vecteur de distance peut être utilisé pour filtrer les routes entre les zones.

La plate-forme logicielle Cisco IOS® a mis en oeuvre une fonction de filtrage interzone. Pour plus d'informations sur cette fonctionnalité, référez-vous à [Filtrage LSA OSPF ABR Type 3](#).

Filtrage des routes externes

Étant donné que les routes externes sont annoncées en tant que LSA de type 5 et qu'elles sont diffusées à l'échelle du domaine, sauf dans les zones d'extrémité et les zones non d'extrémité (NSSA), il n'existe actuellement aucun moyen de filtrer une LSA de type 5. Une solution est d'avoir un processus différent et de filtrer entre les processus tout en redistribuant.

Séparer les différents domaines OSPF

Il est courant d'utiliser différents processus OSPF afin de séparer différents domaines de routage IP, soit à des fins administratives, soit pour segmenter le domaine de routage et pour contrôler les informations de routage dans le point de redistribution.

On peut toutefois noter que l'instabilité dans un domaine peut affecter l'autre domaine. Par exemple, en cas de modification du réseau OSPF (types 1 et 2) où un routeur ASBR (Autonomous System Border Router) réside entre les deux domaines, toutes les LSA de type 5 sont réinitialisées et diffusées dans tout le domaine distant. Ainsi, s'il y a une instabilité constante dans un réseau, cela peut conduire à une injection et un retrait constants des LSA de type 5 dans l'autre domaine.

Un meilleur choix de conception consiste à utiliser le protocole BGP (Border Gateway Protocol) entre différents domaines. Dans ce cas, l'échange OSPF entre différents domaines passe par BGP ; et, parce que BGP a la capacité d'amortissement, l'instabilité dans un domaine peut être moins visible dans l'autre domaine.

Redistribution entre différents processus OSPF

Comme mentionné précédemment, il peut y avoir une solution alternative à la redistribution entre plusieurs processus. La section montre comment la redistribution entre différents processus peut être planifiée avec soin, en fonction du nombre de points de redistribution.

Règle de préférence de routage OSPF

La règle de sélection de route OSPF est que les routes intra-zone sont préférées aux routes inter-zone, qui sont préférées aux routes externes. Cependant, cette règle peut s'appliquer aux routes apprises via le même processus. En d'autres termes, il n'y a pas de préférence entre les routes externes d'un processus par rapport aux routes internes d'un autre processus.

La règle de préférence entre un processus OSPF donné et tout autre processus (qu'il s'agisse d'OSPF ou d'un autre protocole de routage) peut utiliser la règle de distance administrative. Cependant, étant donné que différents processus OSPF ont la même distance administrative par

défaut, la distance OSPF peut être configurée explicitement pour différents processus OSPF afin d'obtenir le comportement souhaité.

 Remarque : avant l'ID de bogue Cisco CSCdi7001 - corrigé dans le logiciel Cisco IOS Version 11.1 et ultérieure - la distance administrative entre les processus ne fonctionnait pas correctement, et les routes internes d'un processus étaient préférées aux routes externes d'un autre processus.

Un point de redistribution unique

Lorsqu'il y a un seul point de redistribution, tous les échanges entre les domaines se produisent en un seul point et il n'y a aucun moyen qu'une boucle de redistribution puisse se former. Voici un exemple de configuration :

Image 1



Configuration du routeur A

```
router ospf 1
redistribute ospf 2 subnet

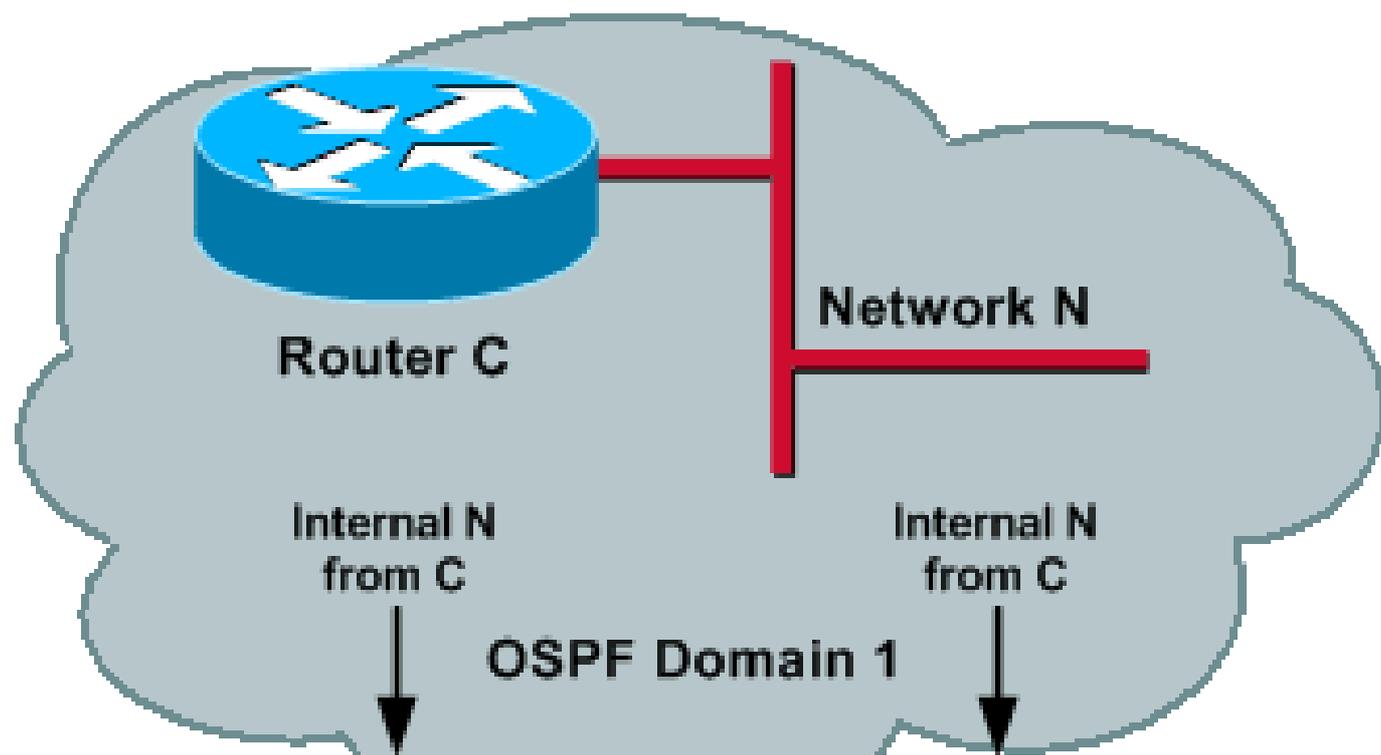
router ospf 2
redistribute ospf 1 subnet
```

Deux points de redistribution

C'est plus compliqué quand il y a deux points de redistribution. Si la redistribution est effectuée dans les deux points d'un réseau sans aucun soin particulier, il peut y avoir des résultats inattendus.

Considérez la topologie suivante, où les routeurs A et B se redistribuent mutuellement entre les deux domaines. Cette configuration ne fonctionne pas et est présentée plus loin dans cette section.

Image 2



Configuration des routeurs A et B

```
router ospf 1  
redistribute ospf 2 subnet
```

```
router ospf 2  
redistribute ospf 1 subnet
```

Avec un réseau N dans le domaine 1, les routeurs A et B apprennent le réseau N comme route interne dans le domaine 1. Comme ils redistribuent le processus 1 dans le processus 2, le même réseau N est appris dans le domaine 2 en tant que route externe.

Désormais, dans chaque routeur, le réseau interne acquis via un processus est en concurrence avec le réseau externe d'un autre processus. Comme mentionné précédemment, il n'y a pas de règle de préférence entre les différents processus ; par conséquent, le résultat serait indéterministe, car les deux processus ont la même distance administrative.

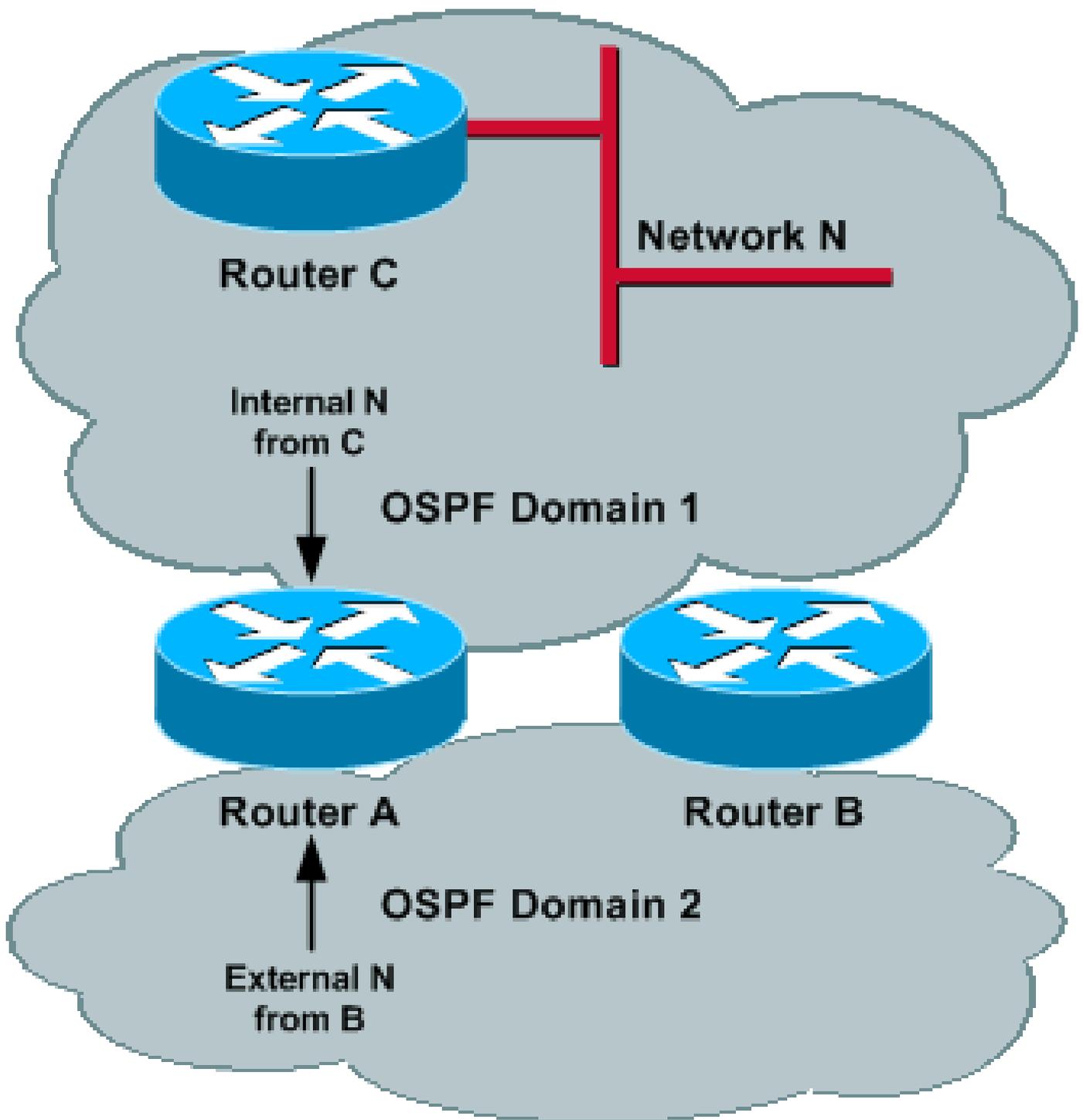
 Note : Ceci pourrait conduire à une injection et un retrait constants d'un type 5 d'un procédé à l'autre.

Avant le bogue Cisco ayant l'ID [CSCdw10987](#) (clients [enregistrés](#) uniquement et intégrés dans les versions du logiciel Cisco IOS® 12.2(07.04)S, 12.2(07.04)T et ultérieures), le dernier processus de création d'un algorithme SPF (Shortest Path First Algorithm) aurait gagné, et les deux processus écraseraient les autres routes dans la table de routage. Maintenant, si une route est installée via un processus, elle n'est pas écrasée par un autre processus OSPF avec le même domaine administratif (AD), sauf si la route est d'abord supprimée de la table de routage par le processus qui a initialement installé la route dans la table de routage.

Distance administrative

Lorsque vous utilisez la redistribution entre plusieurs processus, vous pouvez utiliser la distance administrative afin de préférer un processus à un autre processus, car les préférences de routage OSPF s'appliquent uniquement au sein du même processus. Cependant, cela ne suffit pas pour un fonctionnement correct sur le réseau, comme expliqué plus loin dans cette section.

Image 3



Configuration des routeurs A et B

```

<#root>
router ospf 1
redistribute ospf 2 subnet
distance ospf external 200

router ospf 2
redistribute ospf 1 subnet
distance ospf external 200

```



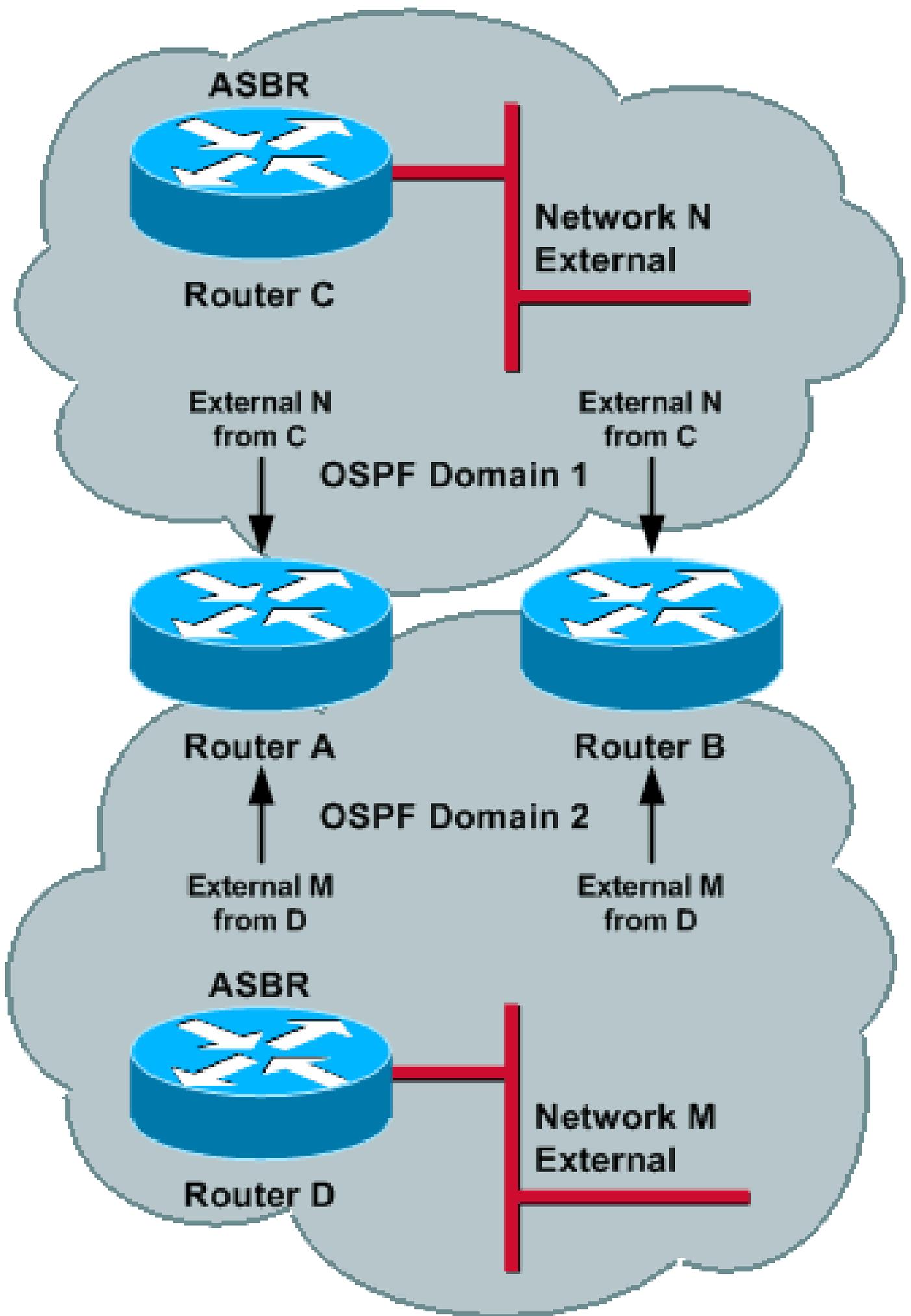
Fonctionnement du réseau sans défaillance du réseau

Considérez un réseau N dans le domaine 1, où N est connu comme une route interne dans le domaine 1 et est redistribué à la fois par le routeur A et par le routeur B. Comme la distance administrative des routes externes a été augmentée, les routeurs A et B ont choisi le processus OSPF 1 pour atteindre le réseau N.

De manière plus générale, tous les réseaux internes au domaine 1 sont atteints via le domaine 1 et tous les réseaux internes au domaine 2 sont atteints via le domaine 2, à la fois par le routeur A et le routeur B. Les autres routeurs de chaque domaine choisissent le routeur ASBR le plus proche (si la métrique de type 2 est utilisée) ou le chemin le plus court via l'un des routeurs ASBR (si la métrique de type 1 est utilisée).

S'il existe des préfixes externes aux deux domaines (provenant d'autres points de redistribution), le même problème se produit toujours car la distance administrative pour ces routes externes est la même dans les deux processus. Si vous définissez une distance administrative différente pour les processus externes, le problème n'est pas résolu. Voici un exemple :

Image 4



Le routeur C (ASBR) annonce N externe dans le domaine 1. Ce préfixe est redistribué par les rout

2. Étant donné que la distance administrative du domaine 1 est inférieure à celle du domaine 2, le routeur A (routeur B) installe M via le domaine 1 et définit pour maximiser sa LSA initiale précédente (événement 1) dans le domaine 1.
3. Comme M a été défini sur maxage dans le domaine 2, le routeur A (routeur B) installe M via le domaine 2 et, par conséquent, redistribue M dans le domaine 2.
4. Identique à l'événement 1.

Ce cycle continue et la façon de le résoudre est d'avoir le préfixe de domaine 2 accessible via le domaine 2. Toutefois, si la distance administrative est définie à une valeur inférieure pour le domaine 2, le même problème se produit pour le domaine 1 et pour le préfixe N.

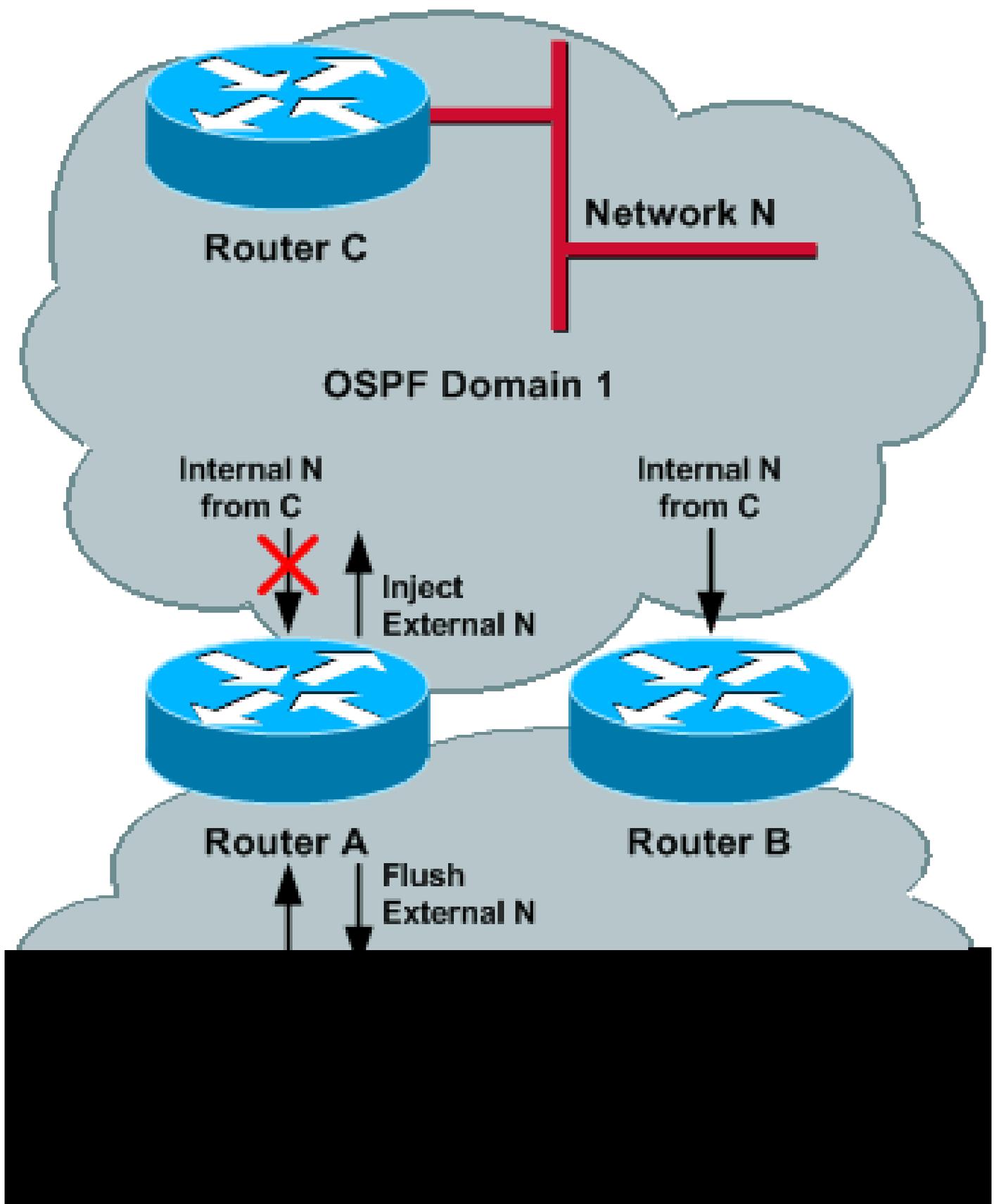
La solution consiste à définir la distance administrative en fonction du préfixe. Consultez les sections [Filtrage basé sur le préfixe](#) et [Filtrage basé sur le préfixe et Distance administrative basée sur le préfixe](#) pour plus d'informations.

Fonctionnement du réseau avec défaillance du réseau

Vous voulez qu'un domaine sauvegarde l'autre domaine, au cas où un domaine serait inaccessible.

Par exemple, considérez le cas où le routeur A a perdu la connectivité au réseau N via le domaine 1. Une fois que le routeur A a perdu sa connectivité via le domaine 1, il vide sa LSA précédemment générée annonçant le réseau N dans le domaine 2 et installe le chemin vers le réseau N via le domaine 2 via le réseau externe reçu de B. Comme le processus 2 est redistribué dans le processus 1, le routeur A injecte également un réseau externe N dans le domaine 1.

 Remarque : lorsque le routeur A était connecté au réseau N, il utilisait le processus 1 en raison de la meilleure distance administrative, et le processus 2 était conservé pour les informations de sauvegarde. Une fois que le chemin à travers le processus 1 devient inaccessible, le processus 2 est utilisé pour la connectivité.



Maintenant, tous les routeurs du domaine 2 utilisent le routeur B pour atteindre le réseau N ; et le routeur A (ou la partie du domaine 1 qui a perdu la connectivité au réseau N via le domaine 1) utilise le domaine 2 pour la connectivité au réseau N. Ce scénario reste valide si le routeur B a perdu la connectivité au réseau N, au lieu du routeur A.

Si les routeurs A et B perdent tous deux la connectivité au réseau N (par exemple, si le routeur C tombe en panne), cette séquence d'événements peut se produire :

1. Avant que le réseau N ne devienne inaccessible, les routeurs A et B ont appris le réseau N via le processus 1 et l'ont redistribué dans le processus 2 en tant qu'externe.
2. Les routeurs A et B détectent (presque en même temps) que le réseau N est inaccessible via le domaine 1 ; par conséquent, ils vidant leur réseau N précédemment externe dans le domaine 2.
3. Avant que le routeur A (routeur B) ne reçoive la LSA vidée du routeur B (routeur A), il installe le N externe via le domaine 2 (une distance administrative plus élevée) en tant que route de secours.
4. Comme le routeur A (routeur B) a installé N par le processus 2, il génère un N externe dans le domaine 1.
5. Le routeur A (routeur B) reçoit la LSA vidée (événement 1) du routeur B (routeur A). Il supprime le réseau N au cours du processus 2 et, par conséquent, vide le réseau N externe dans le domaine 1. Le réseau N a été appris via le domaine 2 et redistribué dans le domaine 1.
6. Avant que le routeur A (routeur B) ne reçoive la LSA vidée du routeur B (routeur A), il installe le réseau externe N via le domaine 1, car N a été vidé via le domaine 2.
7. Comme le routeur A (routeur B) a installé le réseau N par le processus 1, il génère un réseau N externe dans le domaine 2.

Vous pouvez voir qu'il y a une condition de race qui peut apparaître d'un domaine à l'autre domaine. Dans les événements 1, 4 et 7, le routeur A génère un réseau externe N dans le domaine 2 ; et dans les événements 2 et 5, le routeur A retire le préfixe. Le problème se produit parce que les routes apprises via un domaine sont redistribuées vers le même domaine.

Solution proposée

Cette section montre comment empêcher une route qui appartient à un domaine de redistribuer vers le même domaine afin d'éviter les boucles de routage.

Utiliser la commande Distance 255

La section précédente montre comment une boucle de routage est créée si les préfixes appris d'un domaine sont redistribués au même domaine. Comme la redistribution a lieu à partir d'une table de routage, vous pouvez empêcher l'installation dans la table de routage d'une route qui appartient au domaine 1 et qui est apprise à partir du routeur distant sur le domaine 2. Par conséquent, le routeur ne redistribue pas ces routes vers le domaine 1.

Pour ce faire, entrez la commande `distance 255 router_ID inverse_mask access-list`. Cette commande indique au routeur de refuser tous les préfixes reçus par un routeur distant avec l'ID de

routeur spécifié et qui correspondent à la liste de contrôle d'accès (ACL) de la table de routage.

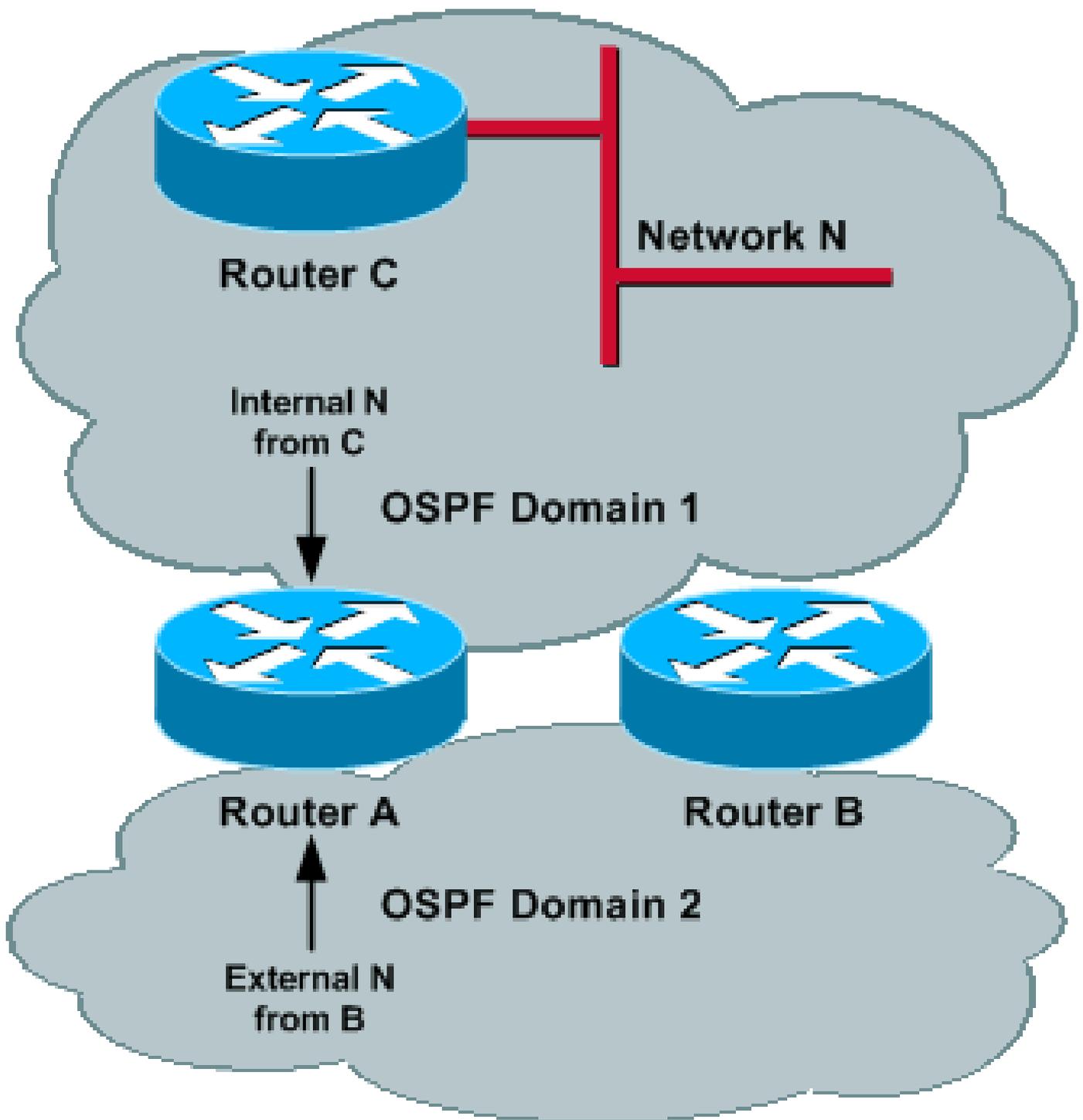
 Remarque : la commande distance 255 donne une distance de 255 à ces routes et, par conséquent, empêche leur installation dans la table de routage.

Dans l'image 6, le routeur A utilise la commande access-list 1 afin de faire correspondre toutes les routes dans le domaine 1 et utilise la commande distance 255 sous le processus 1 afin de refuser les routes reçues du routeur B qui correspondent aux préfixes qui appartiennent au domaine 1.

Lorsque vous utilisez la commande distance 255, elle refuse toute route reçue du routeur B qui appartient au domaine 1. Étant donné que le routeur B redistribue toutes les routes du domaine 1 dans le domaine 2, le routeur A n'installe pas ces routes et, par conséquent, ne redistribue pas à nouveau dans le domaine 1.

 Remarque : l'interface connectée du routeur B dans le domaine 1 peut être exclue de la liste de contrôle d'accès.

Image 6



Configuration du routeur A	Configuration du routeur B
<pre> router ospf 1 redistribute ospf 2 subnet distance 255 <Router B> 0.0.0.0 2 ! access-list 1 !--- Matches the router in Domain 2. router ospf 2 </pre>	<pre> router ospf 1 redistribute ospf 2 subnet distance 255 <Router A> 0.0.0.0 2 ! access-list 1 !--- Matches the router in Domain 2. router ospf 2 </pre>

<pre>redistribute ospf 1 subnet distance 255 <Router B> 0.0.0.0 1 ! access-list 2 !--- Matches the route in Domain 1.</pre>	<pre>redistribute ospf 1 subnet distance 255 <Router A> 0.0.0.0 1 ! access-list 2 !--- Matches the route in Domain 1.</pre>
--	--

La commande `distance ospf external 200` précédente n'est plus nécessaire parce que les routes apprises du routeur distant via l'un des processus ne sont pas installées.

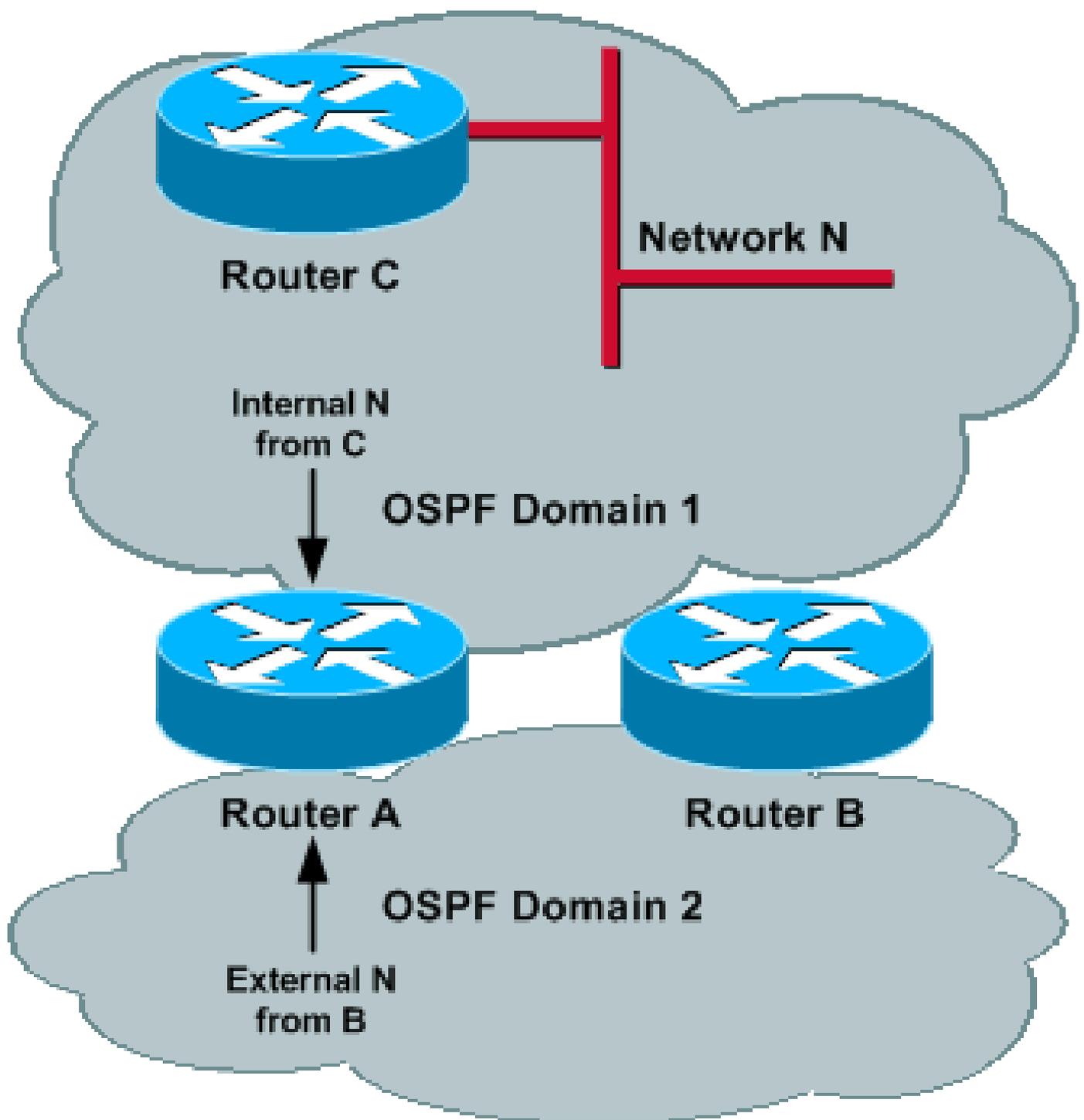
Cette configuration fonctionne correctement dans les cas où les deux routeurs perdent la connectivité au réseau (comme décrit dans [Fonctionnement du réseau sans défaillance du réseau](#) et [Fonctionnement du réseau avec défaillance du réseau](#)). Cependant, comme les préfixes sont refusés de la table de routage, les domaines ne peuvent pas se sauvegarder mutuellement.

 Remarque : vous devez répertorier explicitement tous les préfixes de chaque domaine dans une liste de contrôle d'accès. La maintenance d'une telle liste de contrôle d'accès peut être très difficile.

Filtrer les routes en fonction des balises

Il existe une nouvelle fonctionnalité dans le logiciel Cisco IOS (de l'ID de bogue Cisco [CSCdt43016](#) (clients [enregistrés](#) uniquement)) qui vous permet de filtrer les routes en fonction de la balise. Pour empêcher la redistribution de routes d'un domaine vers le même domaine, un routeur peut marquer une route qui appartient à un domaine pendant qu'il redistribue, et vous pouvez filtrer ces routes sur le routeur distant en fonction de la même balise. Les routes ne pouvant pas être installées dans la table de routage, elles ne sont pas redistribuées dans le même domaine.

Image 7



Configuration des routeurs A et B

```

router ospf 1
redistribute ospf 2 subnet tag 1
distribute-list 1 route-map filter_domain2 in
!
route-map filter_domain2 deny 10
match tag 2
route-map filter_domain2 permit 20

router ospf 2
redistribute ospf 1 subnet tag 2
  
```

```
distribute-list 1 route-map filter_domain1 in
!  
route-map filter_domain1 deny 10  
match tag 1  
route-map filter_domain1 permit 20
```

Lorsque vous effectuez une redistribution à partir du domaine 1, les routes sont étiquetées avec l'étiquette 1 et sont filtrées sur le routeur distant en fonction de la même étiquette. Lorsque vous effectuez une redistribution à partir du domaine 2, les routes sont étiquetées avec l'étiquette 2 et sont filtrées sur le routeur distant en fonction de la même étiquette.

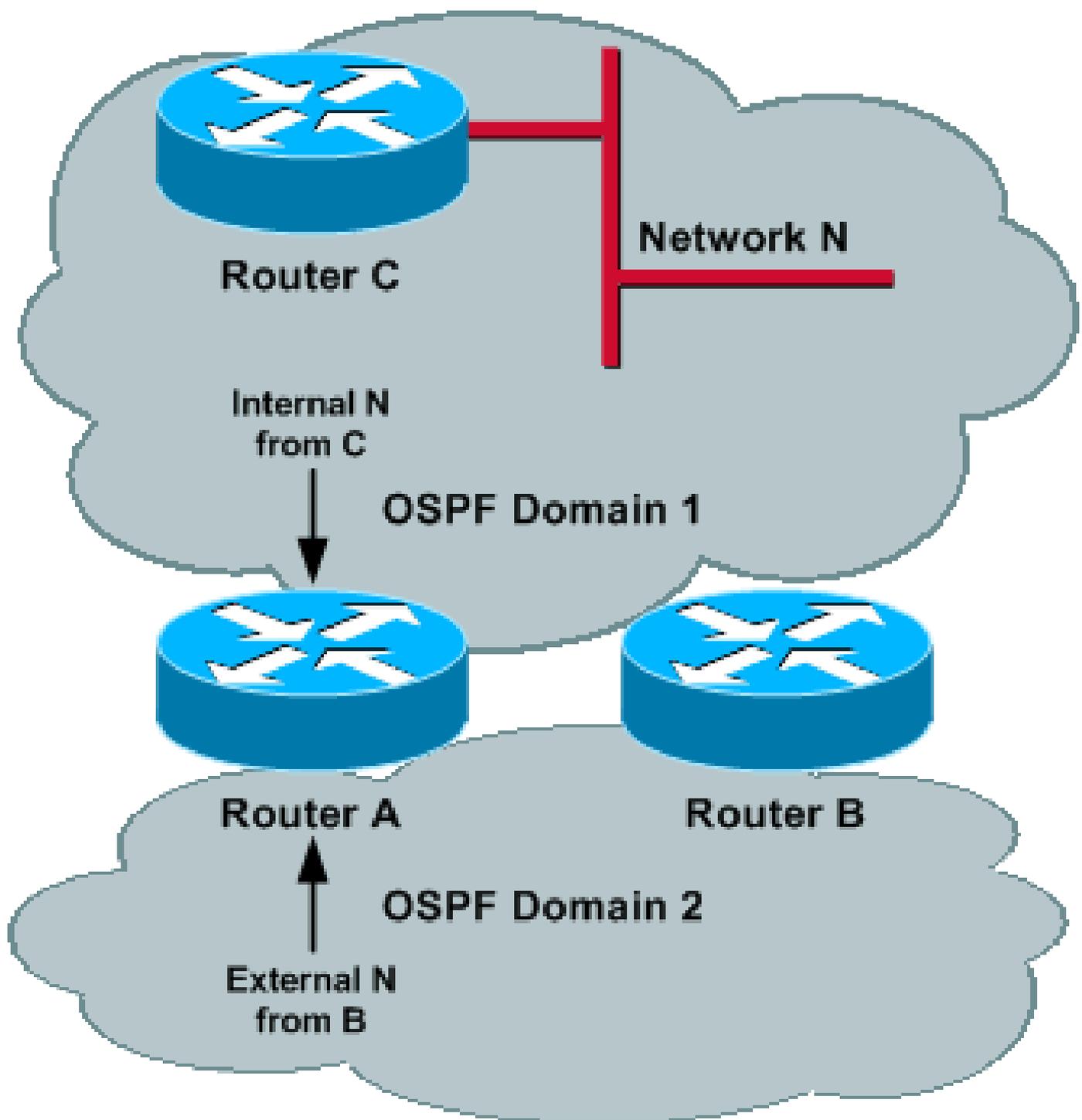
 Remarque : la commande précédente `distance ospf external 200` n'est plus nécessaire car la route apprise du routeur distant via l'un des processus n'est pas installée.

Cette configuration fonctionne correctement dans les cas où les deux routeurs perdent la connectivité au réseau (comme décrit dans [Fonctionnement du réseau sans défaillance du réseau](#) et [Fonctionnement du réseau avec défaillance du réseau](#)). Cependant, comme les préfixes sont refusés de la table de routage, les domaines ne peuvent pas se sauvegarder mutuellement.

Utiliser le mot-clé interne lors de la redistribution

Lorsque vous redistribuez à partir d'un domaine, vous pouvez utiliser le mot clé `match internal` pour redistribuer uniquement les routes internes qui appartiennent à un domaine dans un autre domaine. Cela empêche la redistribution des préfixes qui sont déjà externes dans le même domaine.

Image 8



Configuration des routeurs A et B

```

router ospf 1
redistribute ospf 2 subnet match internal
distance ospf external 200
!

router ospf 2
redistribute ospf 1 subnet match internal
distance ospf external 200
!

```

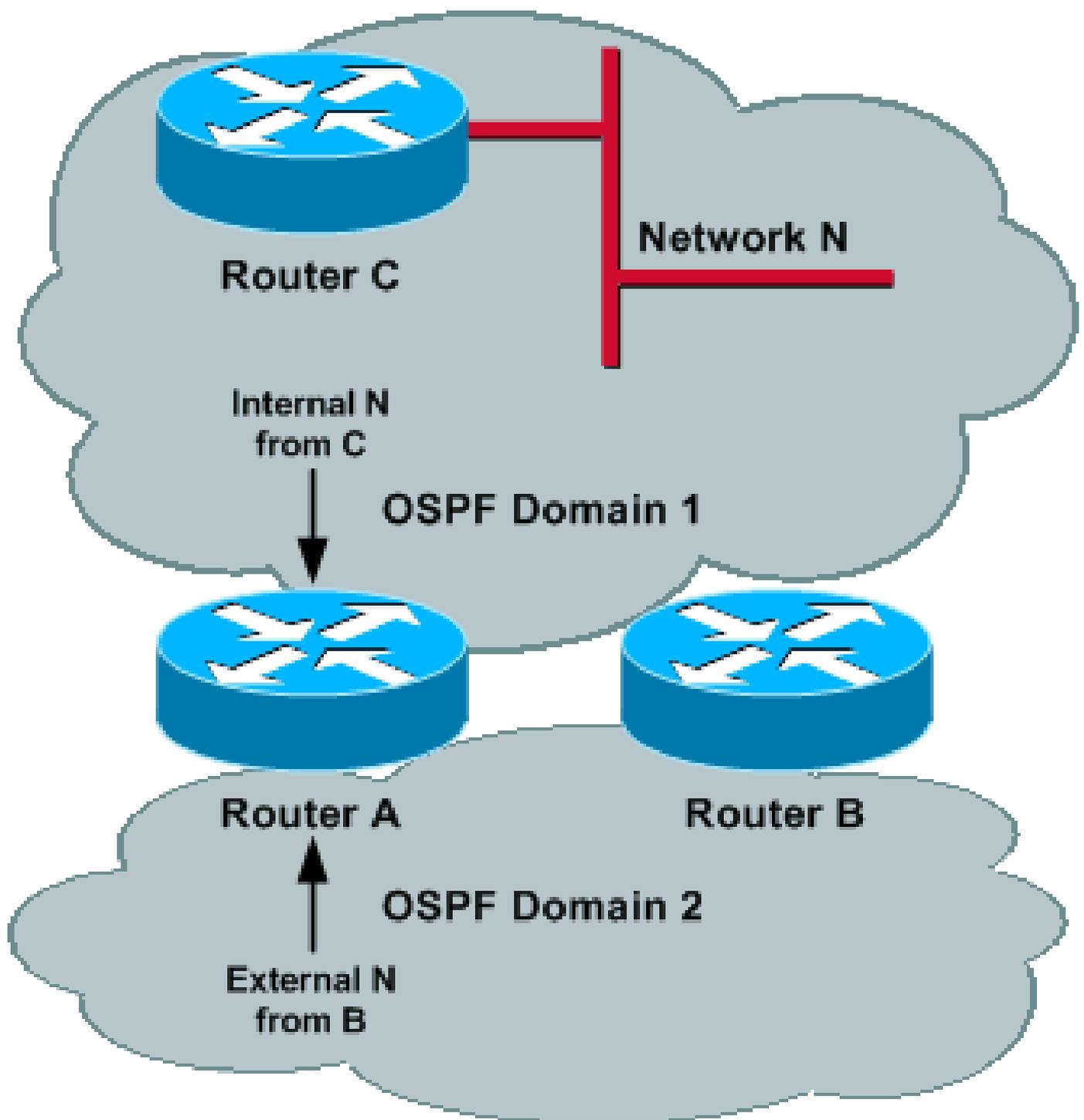
Cette configuration fonctionne correctement dans les cas où les deux routeurs perdent la connectivité au réseau (comme décrit dans [Fonctionnement du réseau sans défaillance du réseau](#) et [Fonctionnement du réseau avec défaillance du réseau](#)). Un domaine peut sauvegarder l'autre domaine.

S'il existe déjà des préfixes externes dans l'un des domaines (tels que des préfixes externes qui ont été redistribués via un autre protocole), ces préfixes ne sont pas redistribués vers d'autres domaines, car seuls les préfixes internes sont redistribués. En outre, il n'y a aucun contrôle sur les préfixes externes, et tous les préfixes externes peuvent être bloqués.

Filtrage basé sur le préfixe

Lorsque vous effectuez une redistribution à partir d'un domaine, les préfixes peuvent être associés à une liste de contrôle d'accès pour éviter la redistribution des préfixes qui appartiennent à un domaine dans le même domaine.

Image 9



Configuration des routeurs A et B

```

router ospf 1
redistribute ospf 2 subnet route-map filter_domain2
distance ospf external 200
!
route-map filter_domain2 permit 10
match ip address 1
!
access-list 1

!--- Matches the prefix in Domain 1.

```

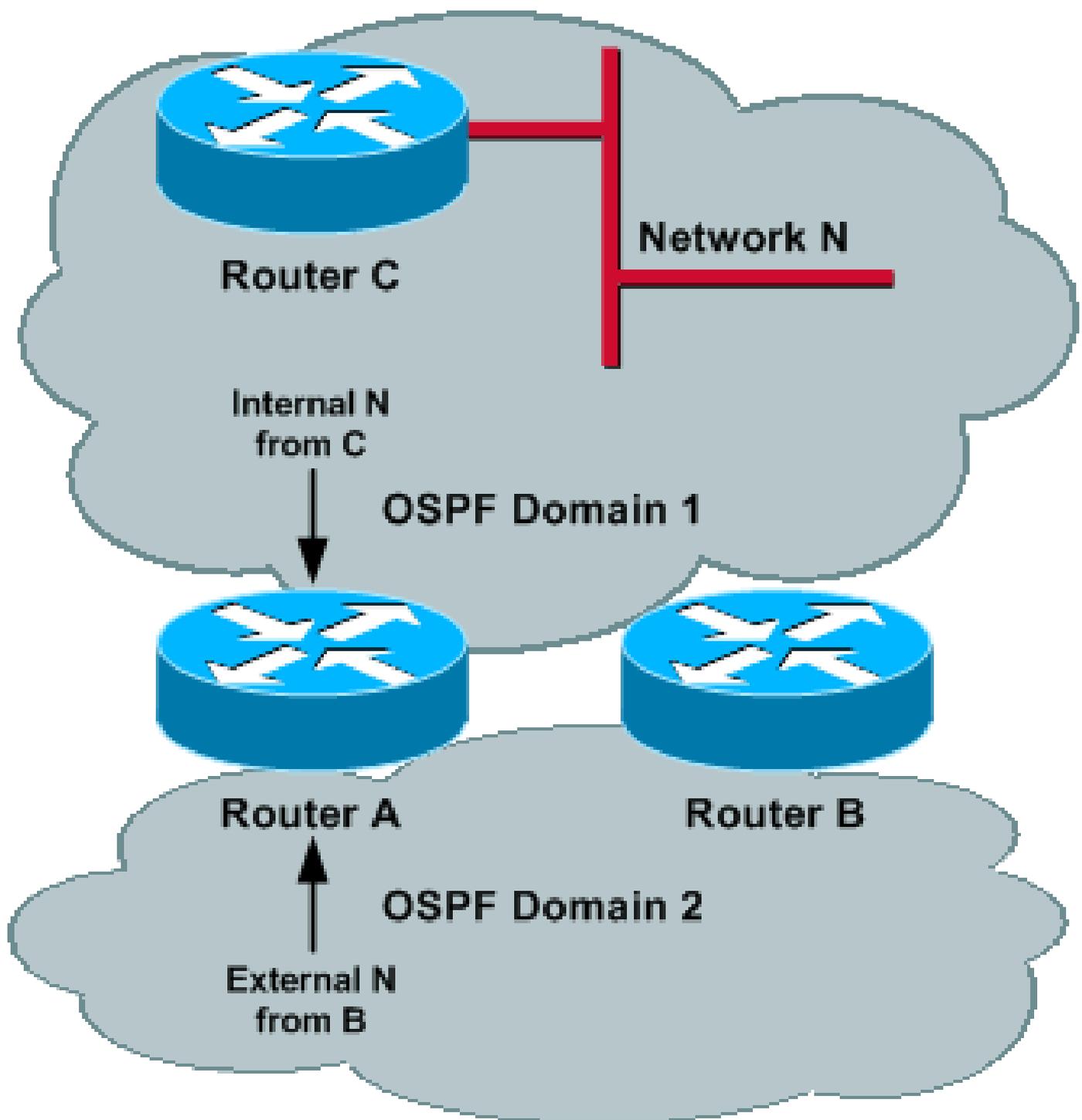
```
router ospf 2
redistribute ospf 1 subnet route-map filter_domain1
distance ospf external 200
!
route-map filter_domain1 permit 20
match ip address 2
!
access-list 2

!--- Matches the prefix in Domain 2.
```

Cette configuration fonctionne correctement dans les cas où les deux routeurs perdent la connectivité au réseau (comme décrit dans [Fonctionnement du réseau sans défaillance du réseau](#) et [Fonctionnement du réseau avec défaillance du réseau](#)). Un domaine peut sauvegarder l'autre domaine.

 Remarque : vous devez répertorier explicitement tous les préfixes de chaque domaine dans une liste de contrôle d'accès. La maintenance d'une telle liste de contrôle d'accès peut être très difficile. Une autre solution consiste à marquer les préfixes pendant la distribution, puis à filtrer les balises correspondantes.

Image 10



Configuration des routeurs A et B

```

router ospf 1
redistribute ospf 2 subnet tag 1 route-map filter_domain2
distance ospf 2 external 200
!
route-map filter_domain2 deny 10
match tag 2
route-map filter_domain2 permit 20

router ospf 2
redistribute ospf 1 subnet tag 2 route-map filter_domain1

```

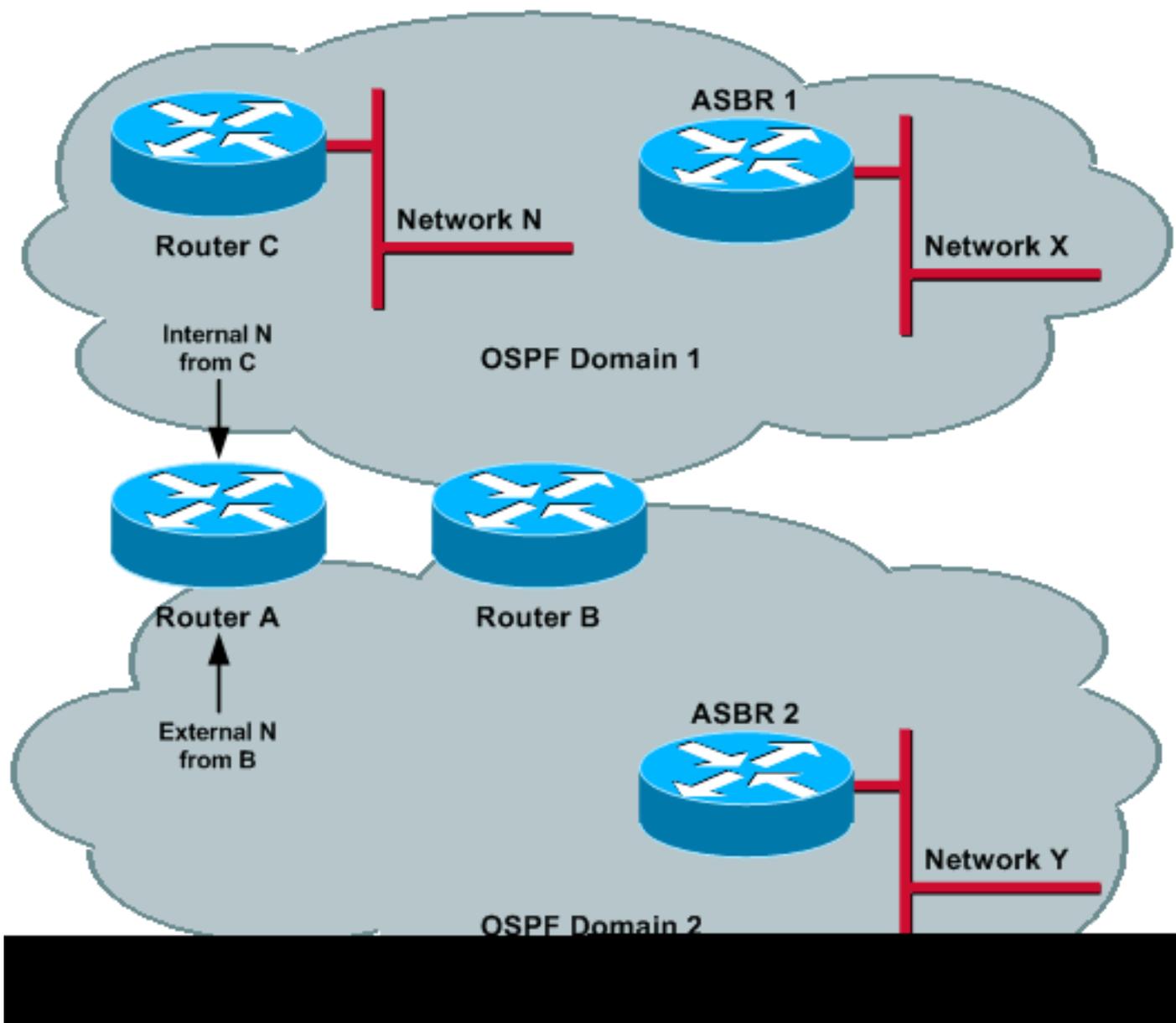
```
distance ospf 1 external 200
!
route-map filter_domain1 deny 10
match tag 1
route-map filter_domain1 permit 20
```

Filtrage basé sur le préfixe et distance administrative basée sur le préfixe

Comme indiqué dans la section [Distance administrative](#), il est nécessaire d'avoir une distance administrative basée sur un préfixe où il y a des préfixes externes provenant d'autres ASBR dans chaque domaine. Dans l'exemple de topologie suivant, ASBR1 et ASBR2 redistribuent les réseaux X et Y dans le domaine 1 et le domaine 2, respectivement.

Cet exemple utilise une liste de contrôle d'accès afin de faire correspondre tous les préfixes (internes et externes) qui appartiennent à un domaine, et il utilise la commande distance afin d'augmenter la distance administrative des préfixes qui n'appartiennent pas initialement au domaine correspondant.

Image 11



Configuration des routeurs A et B

```

router ospf 1
redistribute ospf 2 subnet route-map filter_domain2
distance 200 0.0.0.0 255.255.255.255 2
!
route-map filter_domain2 permit 10
match ip address 2
!
access-list 1

!--- Matches the prefixes in Domain 1.

access-list 2

!--- Matches the prefixes in Domain 2.

router ospf 2
redistribute ospf 1 subnet route-map filter_domain1

```

```
distance 200 0.0.0.0 255.255.255.255 1
!  
route-map filter_domain1 permit 10  
match ip address 1  
!  
access-list 1  
  
!--- Matches the prefixes in Domain 1.  
  
access-list 2  
  
!--- Matches the prefixes in Domain 2.
```

La commande `distance 200 0.0.0.0 255.255.255.255 2` sous le processus 1 définit la distance administrative de tous les préfixes qui appartiennent au domaine 2 à 200 ; par conséquent, les routeurs A et B utilisent le domaine 1 pour atteindre les préfixes qui appartiennent au domaine 1.

 Remarque : vous devez répertorier explicitement tous les préfixes externes de chaque domaine dans une liste de contrôle d'accès. La maintenance d'une telle liste de contrôle d'accès peut être très difficile.

Résumé

Lorsqu'il existe plusieurs points de redistribution entre les domaines OSPF, des boucles de routage peuvent facilement se produire. Afin d'empêcher les boucles de routage, les préfixes qui appartiennent à un domaine ne peuvent pas être redistribués au même domaine. En outre, les distances administratives des processus OSPF peuvent être définies correctement. Ces cinq méthodes ont été proposées dans le présent document :

- Utilisez la commande `distance 255`.
- Filtrer en fonction des balises.
- Utilisez le mot clé `match internal` pendant la redistribution.
- Utiliser le filtrage basé sur le préfixe pendant la redistribution.
- Utiliser le filtrage basé sur le préfixe et la distance administrative basée sur le préfixe.

Les deux premières solutions empêchent les routes appartenant à un domaine d'être installées dans la table de routage, ce qui empêche leur redistribution vers le même domaine.

 Remarque : les préfixes étant refusés dans la table de routage, les domaines ne peuvent pas se sauvegarder mutuellement.

Vous pouvez utiliser les trois dernières solutions pour sauvegarder un domaine avec un autre domaine, si nécessaire. Cependant, vous pouvez noter ces avertissements :

- La solution interne de correspondance ne vous permet pas de contrôler les préfixes, et tous les préfixes externes sont bloqués de la redistribution. En d'autres termes, s'il existe des préfixes externes provenant d'autres ASBR, ces LSA ne sont pas redistribuées d'un domaine à l'autre.
- La solution de filtrage basé sur le préfixe lors de la redistribution permet à un domaine de sauvegarder un autre domaine. Cependant, la sauvegarde ne fonctionne correctement que lorsqu'il n'y a pas de routes externes à partir de l'autre ASBR.
- La solution de filtrage basé sur le préfixe et de distance administrative basée sur le préfixe est la seule solution qui permet à un domaine de sauvegarder un autre domaine en présence de routes externes provenant d'autres routeurs ASBR.

Ce document fait référence à plusieurs reprises à l'utilisation d'un domaine pour sauvegarder un autre domaine. Il est à noter que la sauvegarde signifie que le routeur A peut-il perdre sa connexion à une partie du domaine par le biais d'un domaine donné (tel que le domaine 1), puis il peut utiliser l'autre domaine (domaine 2) afin d'acheminer correctement vers les destinations qui ne peuvent pas être atteintes par le biais du domaine 1.

Cependant, si un domaine est partitionné parce que les préfixes ne sont pas redistribués au domaine d'origine, l'autre domaine ne peut pas sauvegarder le domaine partitionné à moins que les préfixes ne soient redistribués au domaine d'origine. Cependant, comme indiqué dans les sections [Distance administrative](#) et [Fonctionnement](#) du [réseau avec défaillance du réseau](#), cela peut introduire d'autres problèmes.

Informations connexes

- [Page de support OSPF](#)
- [Assistance et documentation techniques - Cisco Systems](#)

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.