

Configurer EIGRP IPV6 sur ASA

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Plates-formes logicielles et matérielles minimales prises en charge](#)

[Exigences](#)

[Composants utilisés](#)

[Protocole EIGRP pour IPV6](#)

[Quoi de neuf ?](#)

[Limites](#)

[Pris en charge](#)

[Non pris en charge](#)

[Détails des fonctionnalités](#)

[Description des fonctionnalités](#)

[Fonctionnalités EIGRP](#)

[Présentation fonctionnelle du protocole EIGRP](#)

[Comment ça fonctionne](#)

[Flux de messages EIGRP](#)

[Établissement du voisinage](#)

[Vue interne / CLI ASA](#)

[Voisinage : configuration de base et multidiffusion/monodiffusion](#)

[Voisinage : spécifier l'interface et l'ID de routeur](#)

[Voisinage de base](#)

[Vérifier](#)

[Vérifier l'état du voisinage](#)

[Configuration des intervalles Hello et de mise en attente](#)

[Configuration d'interface passive](#)

[Distribuer la liste pour le filtrage de route](#)

[Redistribution de routes à partir d'autres protocoles](#)

[EIGRP IPv6 dans ASDM](#)

[Présentation des nouvelles options pour EIGRPv6](#)

[Configuration EIGRPv6 dans l'interface](#)

[Configuration des paramètres EIGRPv6 pour une interface](#)

[Instances de processus et interfaces passives](#)

[Configuration des interfaces passives](#)

[Configuration du routage EIGRP et des métriques par défaut](#)

[Configuration des règles de filtre \(Distribute-List\)](#)

[Redistribuer la configuration des routes](#)

[Voisin : mode routeur de monodiffusion](#)

[Mode routeur multidiffusion](#)

[EIGRP IPv6 dans CSM](#)

[Présentation des nouvelles options dans CSM pour EIGRPv6](#)

[Activer la prise en charge EIGRP IPv6](#)

[Onglet EIGRP IPv6 Setup](#)

[Onglet Voisins EIGRP IPv6](#)

[Onglet Redistribution IPv6 EIGRP](#)

[Onglet Résumé de l'adresse IPv6 EIGRP](#)

[Onglet Interfaces EIGRP IPv6](#)

[Dépannage](#)

[Étapes de dépannage](#)

[Exemple de problème](#)

[Historique de révision](#)

Introduction

Ce document décrit comment configurer EIGRP IPV6 sur Cisco Adaptive Security Appliance (ASA).

Conditions préalables

Plates-formes logicielles et matérielles minimales prises en charge

Version min. du gestionnaire supportée	Périphériques gérés	Version minimale du périphérique géré prise en charge requise	Remarques
ASA	Toutes les plates-formes ASA	9.20.1	CLI
CSM	Toutes les plates-formes ASA	4.27	GUI CSM
ASDM	Toutes les plates-formes ASA	7.20.1	GUI ASDM

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Gestionnaire de sécurité Cisco
- Gestionnaire des appareils de sécurité adaptatifs

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appareil de sécurité adaptatif Cisco (ASA), version 9.20.1 ou ultérieure
- Cisco Security Manager (CSM) exécutant 4.27
- Cisco Adaptive Security Device Manager exécutant 7.20.1

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.

Protocole EIGRP pour IPV6

- Le protocole EIGRP est déjà pris en charge et disponible sur ASA. La demande pour le protocole EIGRP IPV6 augmente.
- La configuration des protocoles EIGRPv4 et EIGRPv6 est similaire, mais ils peuvent être configurés et gérés indépendamment.
- En raison des différences dans les protocoles, la configuration et le fonctionnement diffèrent légèrement.

Quoi de neuf ?

- Dans les versions antérieures, le protocole EIGRP était pris en charge uniquement pour IPv4 et, à partir de la version 9.20 d'ASA, le protocole EIGRP était pris en charge avec IPV6.
- Prise en charge du protocole EIGRP IPv6 avec adresse link-local sur ASA uniquement.

Limites

Pris en charge

- EIGRPv6 est actuellement pris en charge sur ASA uniquement en mode routé, HA et cluster.
- Le voisinage EIGRPv6 peut être activé uniquement avec l'adresse link-local.

Non pris en charge

- Mode transparent

- Multicontexte
- Authentification
- Sur FTD

Détails des fonctionnalités

Description des fonctionnalités

- Le protocole EIGRP pour IPv6 utilise le même cadre que le protocole EIGRP pour IPv4.
- Le protocole EIGRP IPv6 communiquerait uniquement avec les homologues IPv6 et annoncerait uniquement les routes IPv6.

Les protocoles EIGRP IPV4 et EIGRP IPv6 partagent des caractéristiques similaires, notamment :

- Les tables de voisinage, de routage et de topologie sont gérées.
- Il utilise la pile DUAL pour une convergence rapide et un réseau sans boucle.

Les différences sont les suivantes :

- La commande network en mode routeur n'est pas utilisée pour EIGRP IPv6.
- Utilisez ipv6 router eigrp <AS> pour activer le processus du routeur EIGRP IPV6.
- Configurez explicitement ipv6 eigrp <AS> pour activer EIGRP IPv6 sur une interface spécifique.
- L'adresse IPv6 configurée par l'utilisateur ne peut pas être utilisée pour établir un voisinage.
- L'authentification n'est pas prise en charge dans la version actuelle.

Fonctionnalités EIGRP

Présentation fonctionnelle du protocole EIGRP

- Le protocole EIGRP pour IPv6 serait identique au protocole EIGRP pour IPv4.
- Le protocole EIGRP utilise l'algorithme DUAL (Diffusing Update Algorithm) pour réaliser une convergence rapide.

DUAL calcule non seulement les meilleures routes, mais également les routes sans boucle.

Il y a principalement deux tables utilisées par DUAL pour calculer la meilleure route. Il s'agit de la table de routage de voisinage, de la table topologique.

DUAL calcule un autre chemin en fonction de la distance de faisabilité signalée.

- La table de voisinage conserve une trace de tous les voisins connectés directement. Les paquets Hello sont utilisés pour vérifier l'état du voisin.
- La table topologique conserve des informations sur les métriques de toutes les routes du réseau. Le successeur et le successeur potentiel conservent les informations relatives au meilleur chemin et au chemin alternatif.

Comment ça fonctionne

Les messages Hello sont utilisés pour détecter le voisin avant d'établir la contiguïté.

Les messages de mise à jour sont échangés entre les voisins pour créer la table topologique et la

table de routage.

Les messages de requête sont envoyés à d'autres voisins EIGRP pour un successeur potentiel lorsque DUAL recalcule une route dans laquelle le pare-feu n'a pas de successeur potentiel.

Les messages de réponse sont envoyés comme réponse à un paquet de requête EIGRP.

Les messages Accuser réception sont utilisés pour accuser réception des mises à jour, des requêtes et des réponses EIGRP.

Flux de messages EIGRP

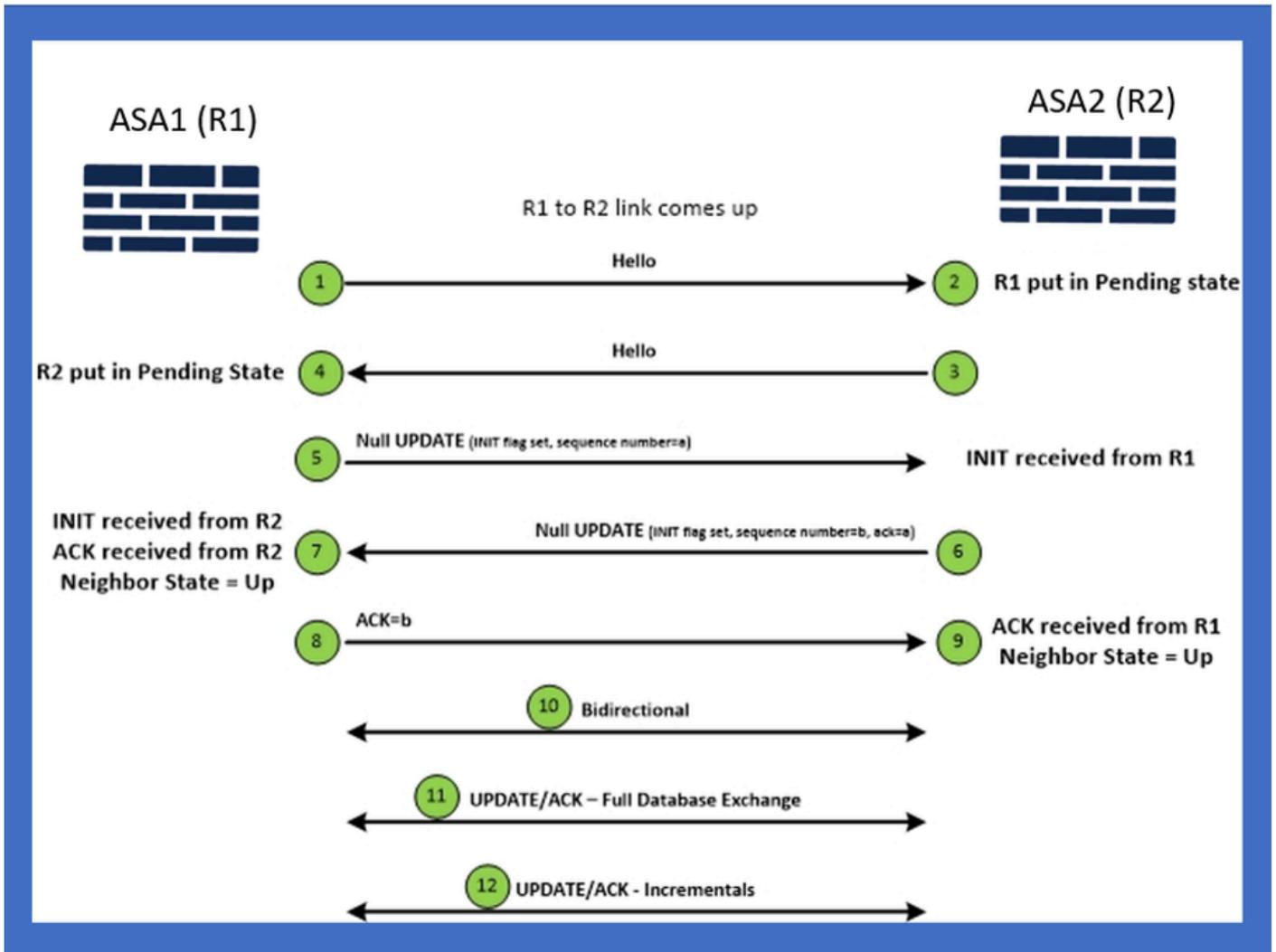
EIGRP IPv6 utilise un paquet Hello pour détecter d'autres périphériques compatibles EIGRP sur des liaisons directement connectées et pour établir des relations de voisinage.

EIGRP IPv6 transmet des paquets Hello avec une adresse source qui est l'adresse link-local de l'interface de transmission.

Les messages Hello sont comme des messages de maintien de la connexion pour garder une trace de l'état du voisin.

Le minuteur par défaut du message Hello est de 5 secondes. Lors de l'échange de messages Hello, un message de mise à jour est reçu et envoyé. Elle permet de créer la table topologique et d'installer les routes dans le RIB en conséquence.

Établissement du voisinage



Vue interne / CLI ASA

Voisinage : configuration de base et multidiffusion/monodiffusion

Pour établir le voisinage, la configuration du mode routeur est nécessaire. Il en va de même pour IPv4, à l'exception du mot clé config starts with IPv6.

Il doit également relier l'interface participante au système autonome.

Le voisinage peut être formé de deux manières, en utilisant la multidiffusion ou la monodiffusion.

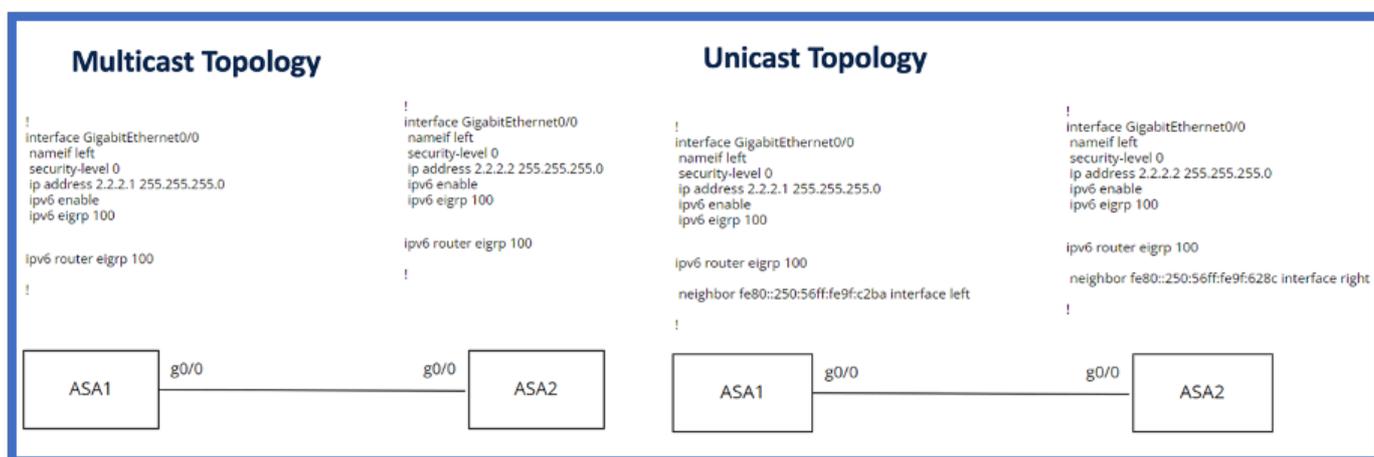
Multicast router mode config	Unicast router mode config
<pre> ciscoasa(config-rtr)# ipv6 router eigrp 100 ciscoasa(config-rtr)# show run ipv6 ! ipv6 router eigrp 100 ! </pre>	<pre> ipv6 router eigrp 100 neighbor fe80::250:56ff:fe9f:9e3d interface r0 ! </pre>

Voisinage : spécifier l'interface et l'ID de routeur

- En plus de la configuration en mode routeur, l'interface qui participe au voisinage doit être connectée à un système autonome respectif.
- Assurez-vous d'activer IPv6 sur l'interface.
- L'ID de routeur est nécessaire pour que le voisinage se forme. Elle serait prise implicitement à partir de l'interface IPv4, ou elle doit être configurée explicitement en mode routeur, sinon le voisinage ne serait pas formé.

Voisinage de base

Vous avez simplement dirigé la topologie et la configuration connectées pour le voisinage monodiffusion et multidiffusion.



Vérifier

Vérifier l'état du voisinage

`show ipv6 eigrp neighbors` est utilisé pour vérifier l'état de voisinage.

```
<#root>
```

```
ciscoasa(config-rtr)# show ipv6 eigrp neighbors
```

```
EIGRP-IPv6 Neighbors for AS(50)
```

H	Address	Interface	Hold	Uptime	SRTT	RTO	Q	Seq
				(sec)	(ms)		Cnt	Num
1	Link-local address:	m3	12	1w3d	270	1620	0	153 fe80::250:56ff:fe9f:e7e8
0	Link-local address:	m2	12	1w3d	174	1044	0	152 fe80::250:56ff:fe9f:8d83

Configuration des intervalles Hello et de mise en attente

- L'intervalle Hello et l'intervalle Hold peuvent être configurés à l'aide des configurations sous interface.
- Pour les interfaces NBMA (Non-Broadcast Multiple Access Network), la valeur par défaut du minuteur Hello est de 5 secondes et la valeur par défaut du temps d'attente est de 15 secondes.

<#root>

```
ciscoasa(config-if)# ipv6 hello-interval eigrp 100 ?
```

```
interface mode commands/options:
```

```
<1-65535> Seconds between hello transmissions
```

```
ciscoasa(config-if)#
```

```
ciscoasa(config-if)# ipv6 hold-time eigrp 200 ?
```

```
interface mode commands/options:
```

```
<1-65535> Seconds before neighbor is considered down
```

```
ciscoasa(config-if)#
```

Configuration d'interface passive

- Si vous ne voulez pas qu'une interface forme un voisinage, passive-interface config peut être utilisé de sorte que Hellos sur l'interface ne soit pas envoyé et ne forme pas de contiguïté.

<#root>

```
ciscoasa(config-rtr)# passive-interface ?
```

```
ipv6-router mode commands/options:
```

```
Current available interface(s):
```

```
default Suppress routing updates on all interfaces
```

```
g0 Name of interface GigabitEthernet0/0
```

```
mgmt Name of interface Management0/0
```

```
ciscoasa(config-rtr)#
```

Distribuer la liste pour le filtrage de route

- La liste de distribution peut être utilisée avec la configuration de préfixe pour filtrer les mises à jour de routage entrantes ou sortantes pour une interface donnée.

<#root>

```
ciscoasa(config-rtr)# distribute-list prefix-list abc ?
```

ipv6-router mode commands/options:

in Filter incoming routing updates

out Filter outgoing routing updates

```
ciscoasa(config-rtr)#
```

Redistribution de routes à partir d'autres protocoles

- Les routes d'autres protocoles de routage peuvent être redistribuées dans le protocole EIGRP.
- Utilisez la commande redistribute sous router.

<#root>

```
ciscoasa(config-rtr)# redistribute ?
```

ipv6-router mode commands/options:

bgp Border Gateway Protocol (BGP)

connected Connected Routes

eigrp Enhanced Interior Gateway Routing Protocol (EIGRP)

isis ISO IS-IS

ospf Open Shortest Path First (OSPF)

static Static Routes

```
ciscoasa(config-rtr)#
```

EIGRP IPv6 dans ASDM

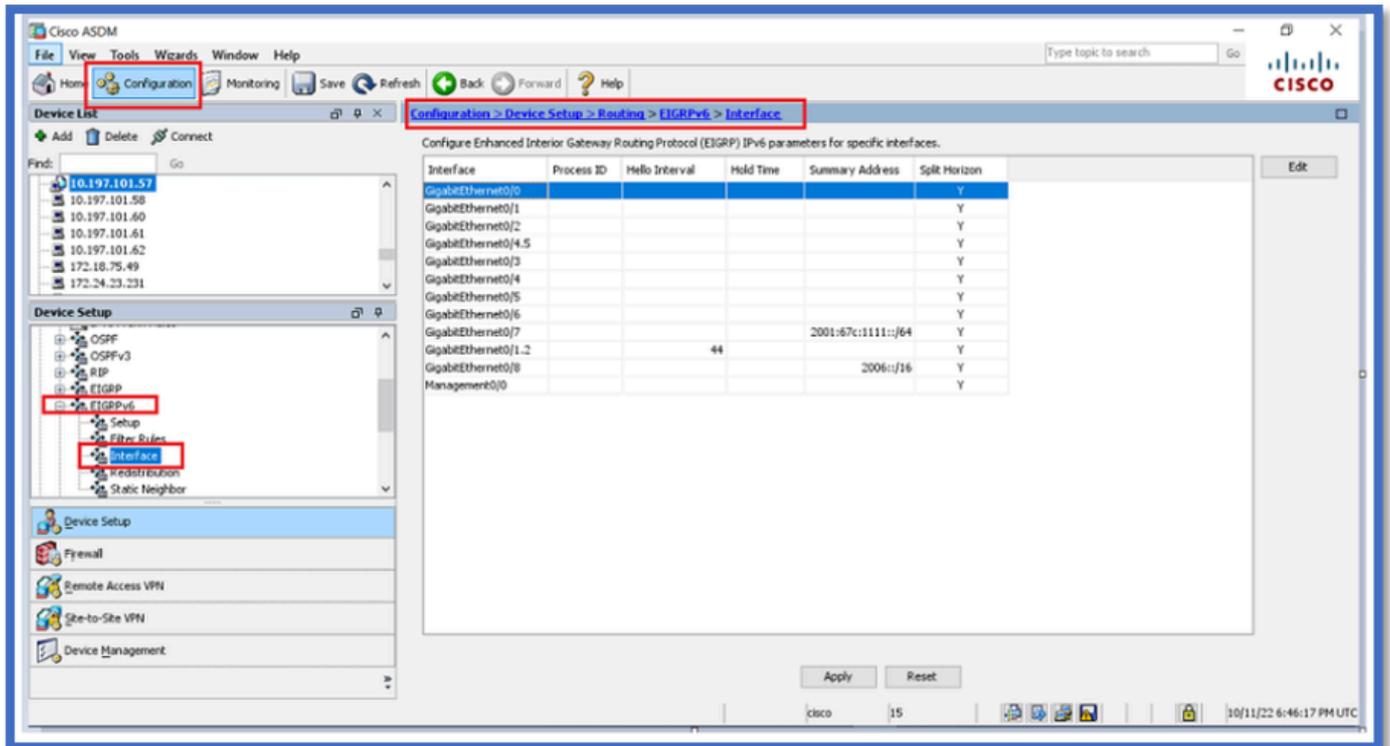
Présentation des nouvelles options pour EIGRPv6

- La prise en charge d'EIGRPv6 est ajoutée dans le cadre de l'ASDM 7.20.1.

- Configuration EIGRPv6 ajoutée dans le cadre de la commande interface sub CLI.
- Configuration EIGRPv6 ajoutée dans les commandes du routeur et prise en charge du routeur.

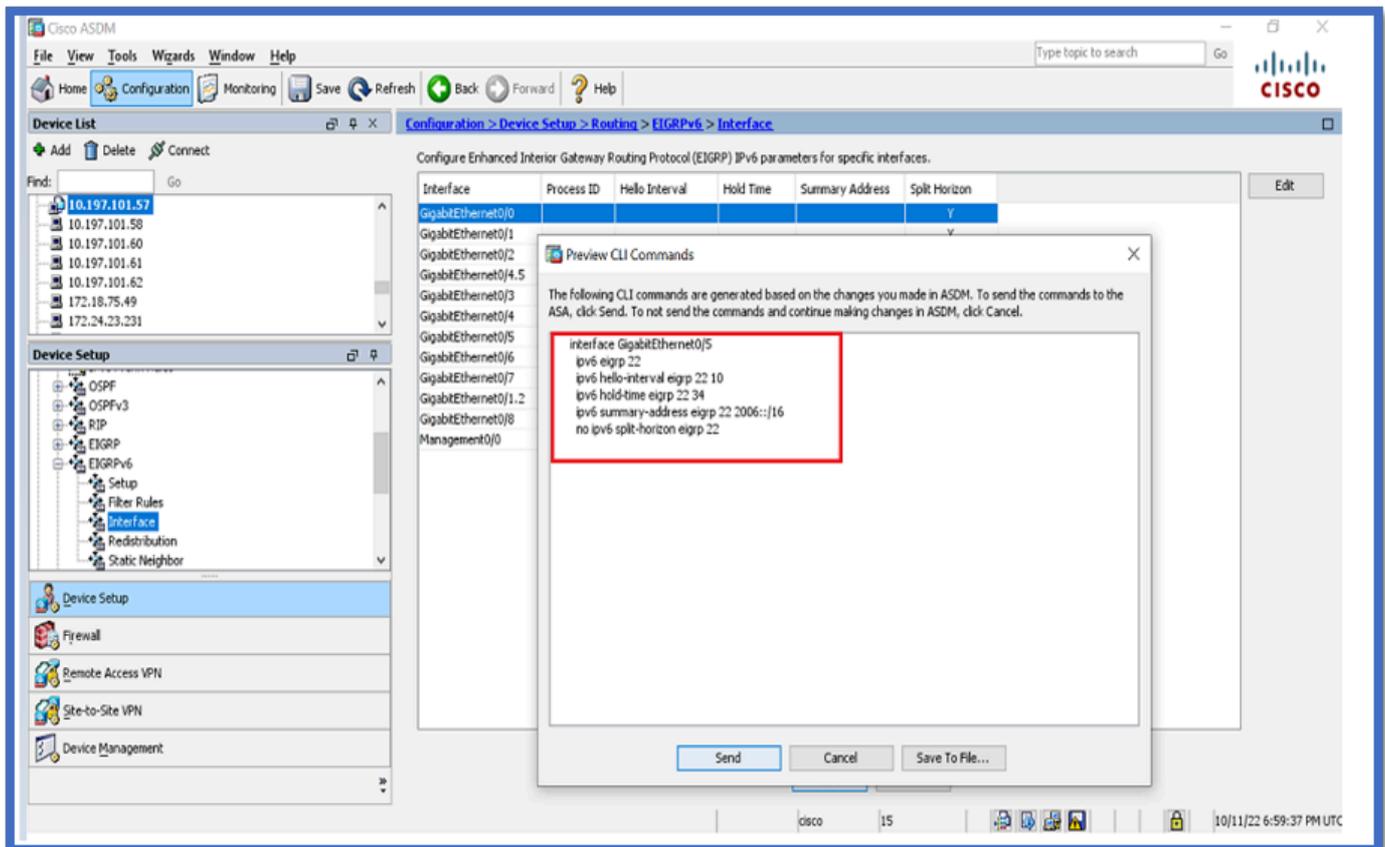
Configuration EIGRPv6 dans l'interface

1. Accédez à Configuration > Device Setup > Routing > EIGRPv6.
2. Sélectionnez Interface pour afficher toutes les interfaces prises en charge.



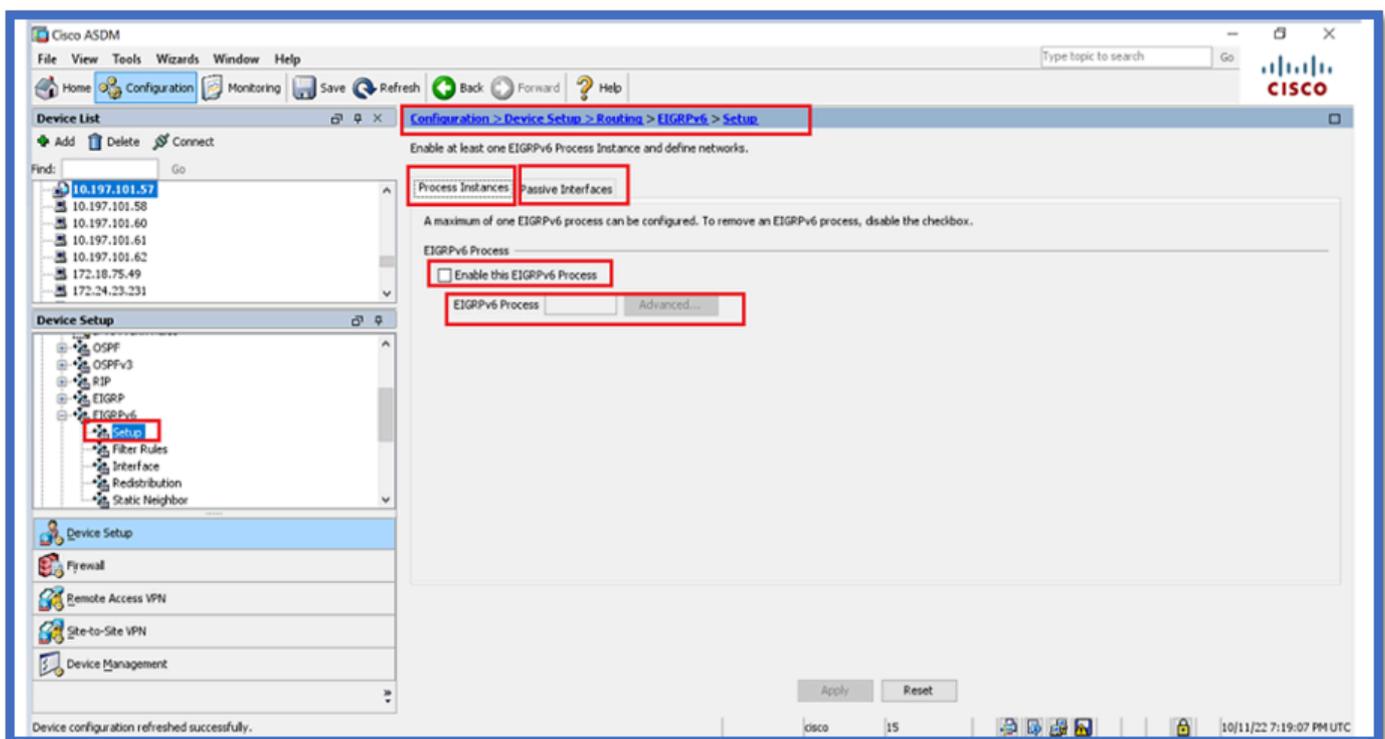
Configuration des paramètres EIGRPv6 pour une interface

1. Accédez à Configuration > Device Setup > Routing > EIGRPv6 > Interface.
2. Sélectionnez Interface et cliquez sur Edit.
3. Cochez les cases pour configurer l'ID de processus, l'intervalle Hello, le temps d'attente, le découpage d'horizon et/ou l'adresse récapitulative.
4. Configurez les paramètres, puis cliquez sur OK.
5. Cliquez sur Envoyer.
6. Lorsque l'interface de ligne de commande apparaît, cliquez sur Send, Cancel ou Save to File.



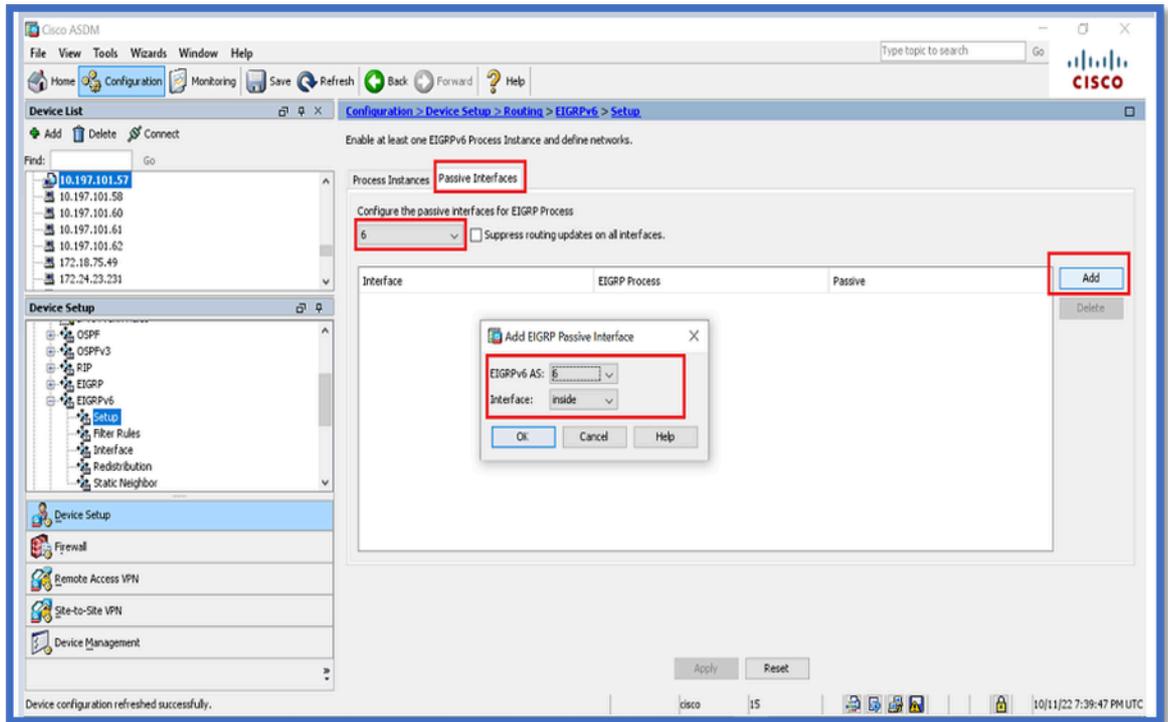
Instances de processus et interfaces passives

1. Accédez à Configuration > Device Setup > Routing > EIGRPv6 > Set up.
2. Affichage des instances de processus et des interfaces passives.
3. Sous Instances de processus, activez le processus EIGRPv6.

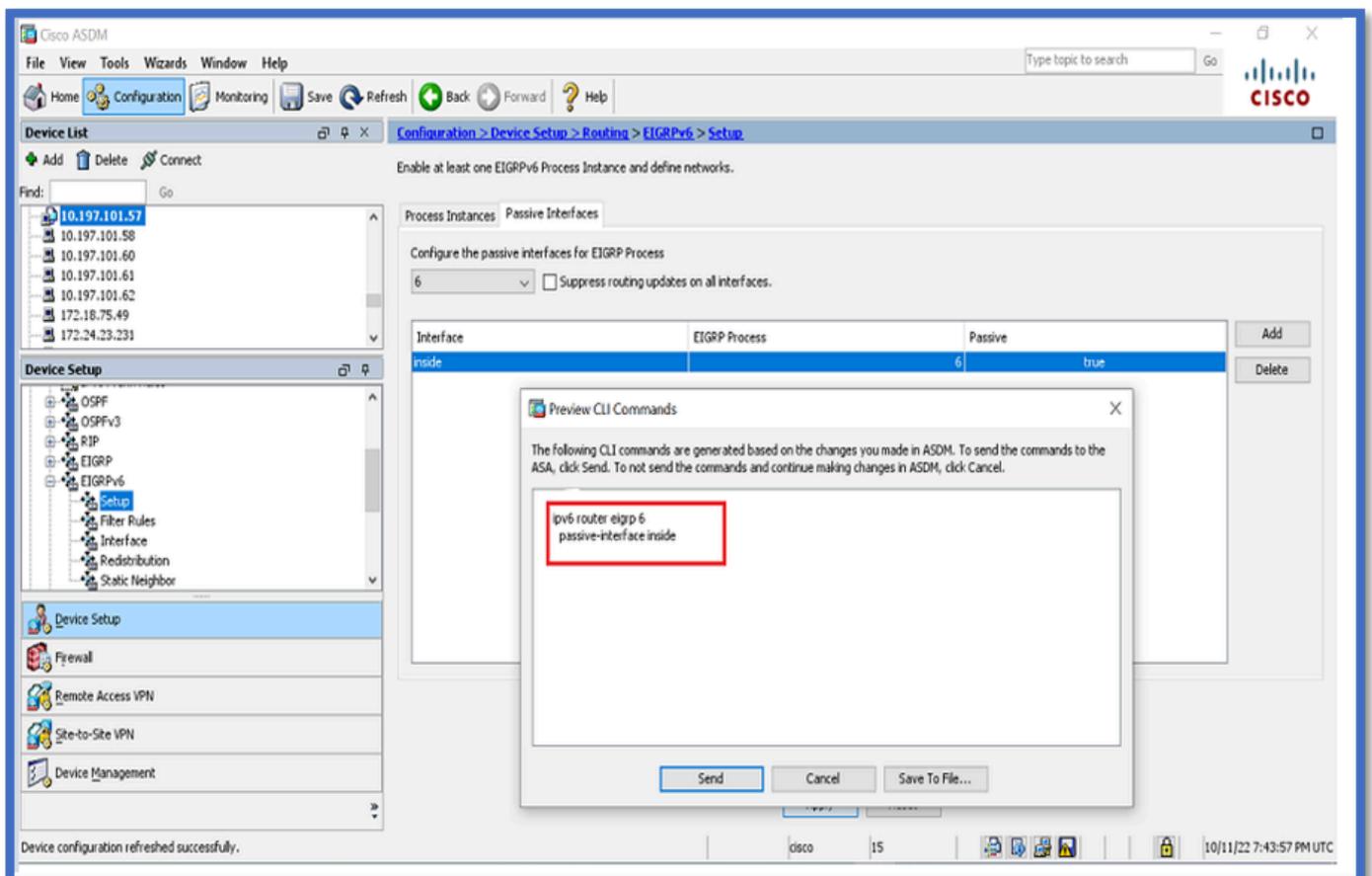


Configuration des interfaces passives

1. Accédez à Configuration > Device Setup > Routing > EIGRPv6 > Set up.
2. Cliquez sur Passive Interfaces > Add > Select Interface.

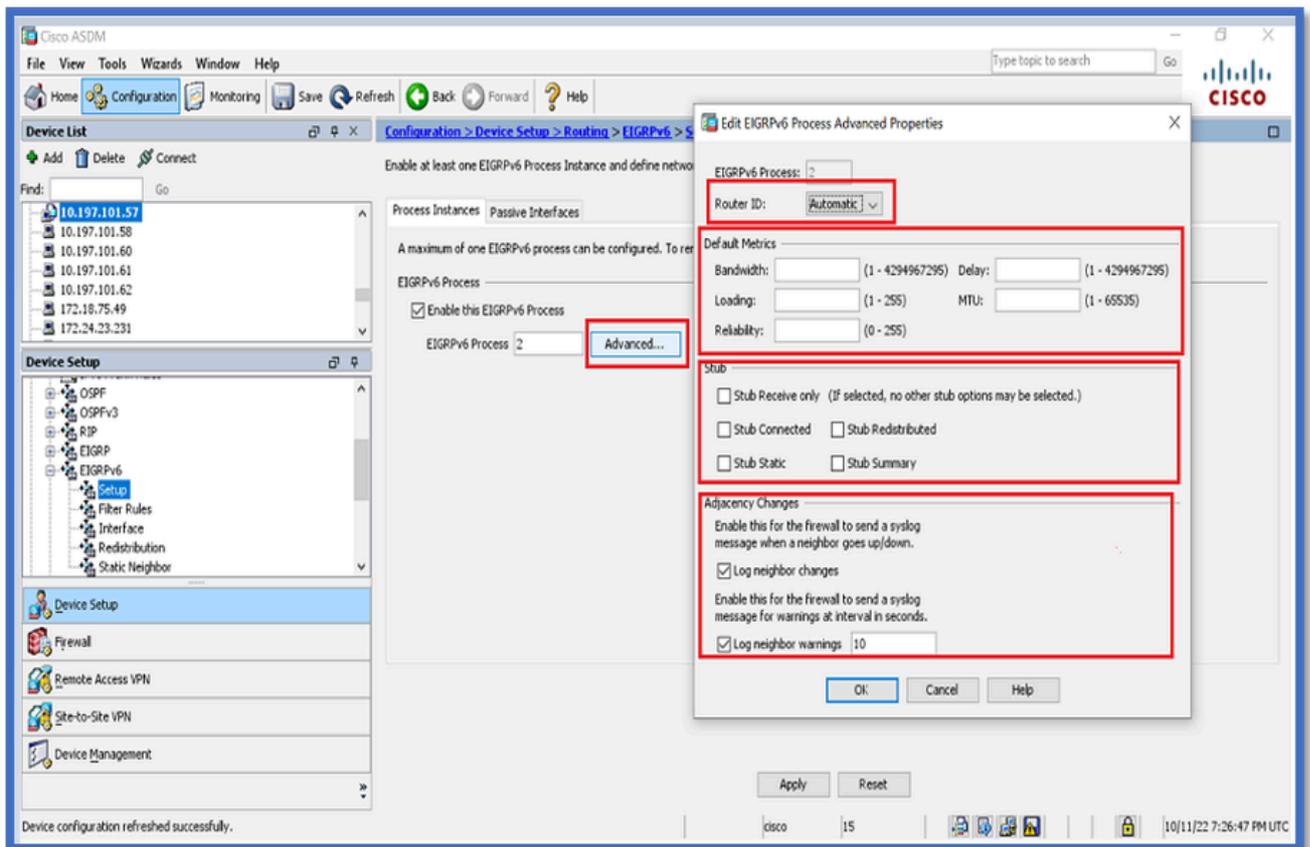


3. Click OK.
4. Cliquez sur Apply.
5. La fenêtre CLI s'affiche.

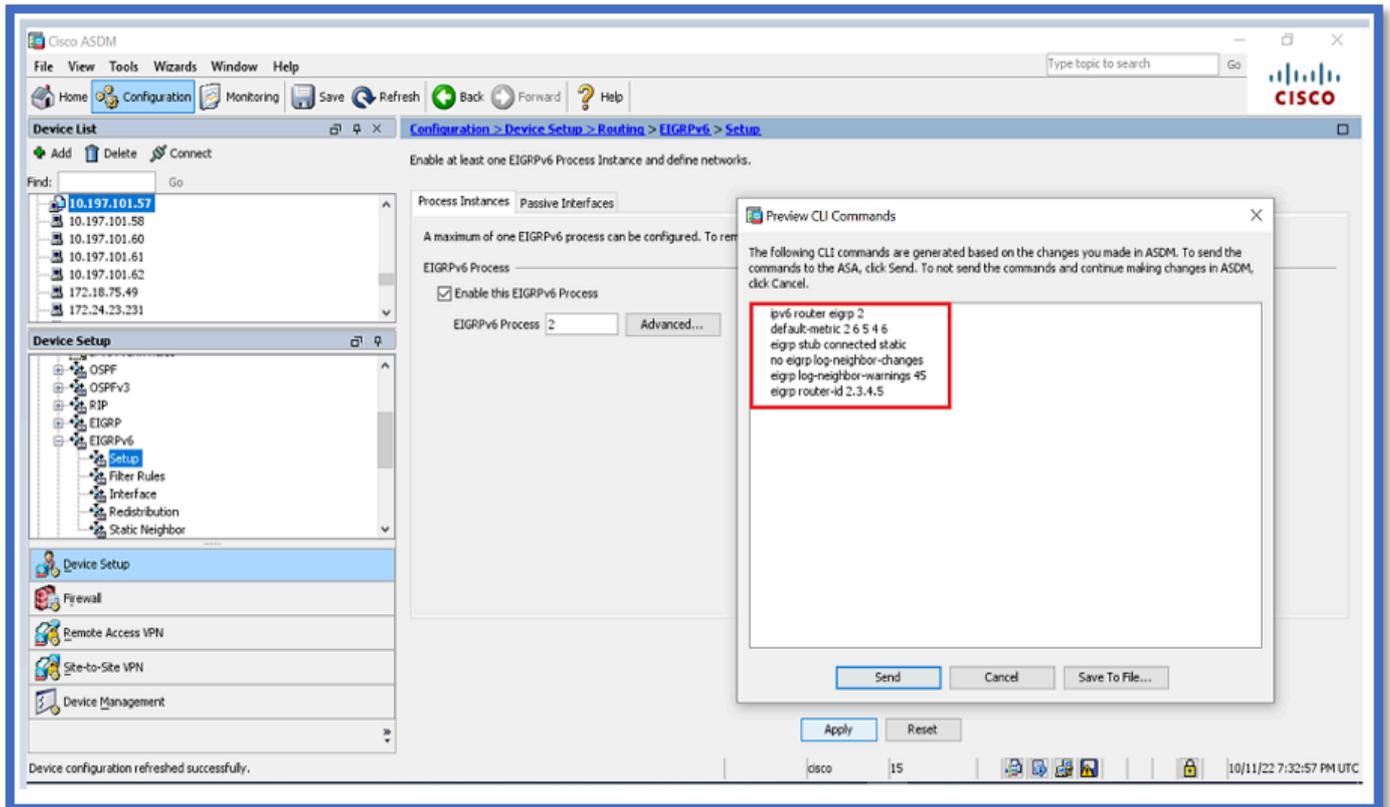


Configuration du routage EIGRP et des métriques par défaut

1. Accédez à Device Setup > Routing > EIGRPv6 > Set up.
2. Cliquez sur Instances de processus > Fournir une valeur d'ID de processus.
3. Cliquez sur le bouton Avancé.
4. Fournissez l'ID de routeur, les métriques par défaut, le stub et les valeurs de voisinage du journal.

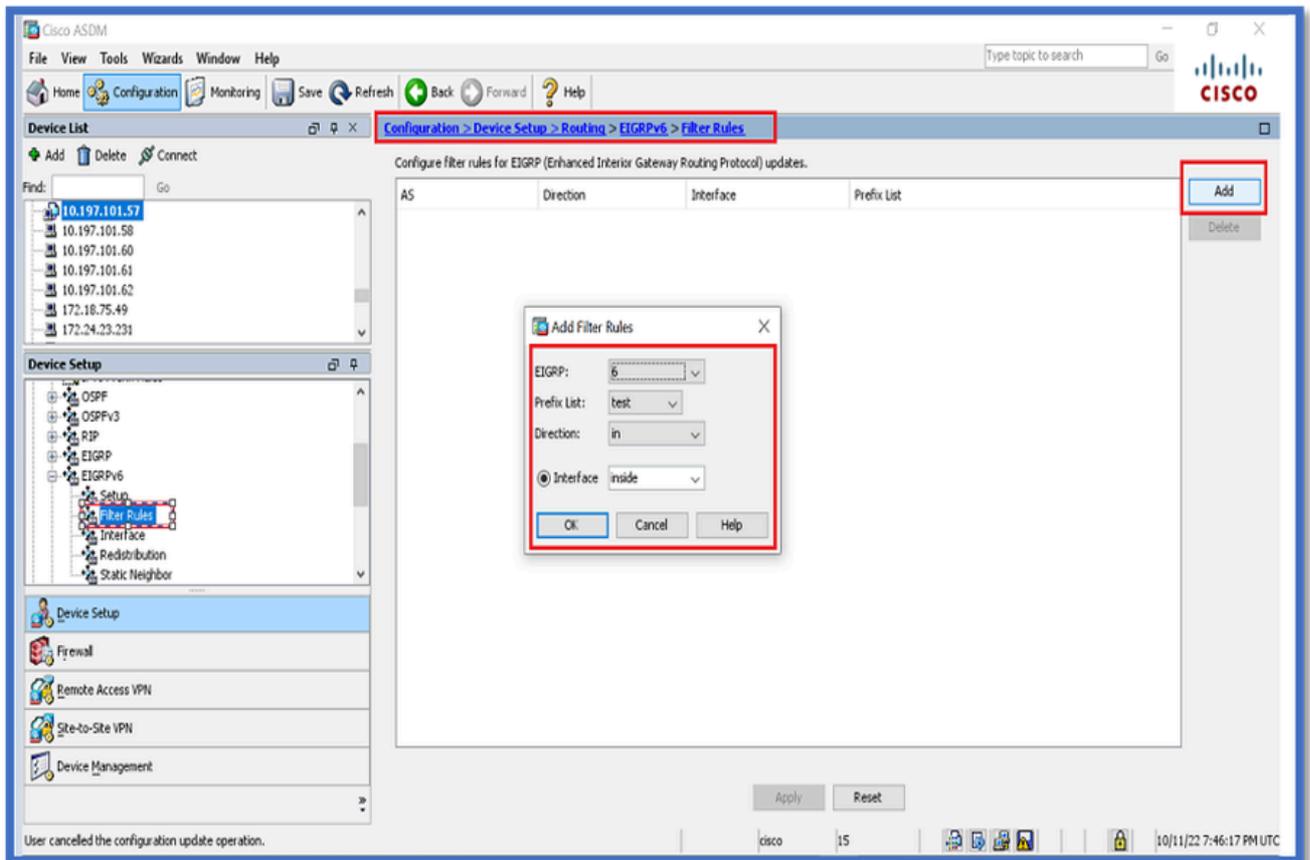


5. Cliquez sur Apply.
6. La fenêtre CLI s'affiche.

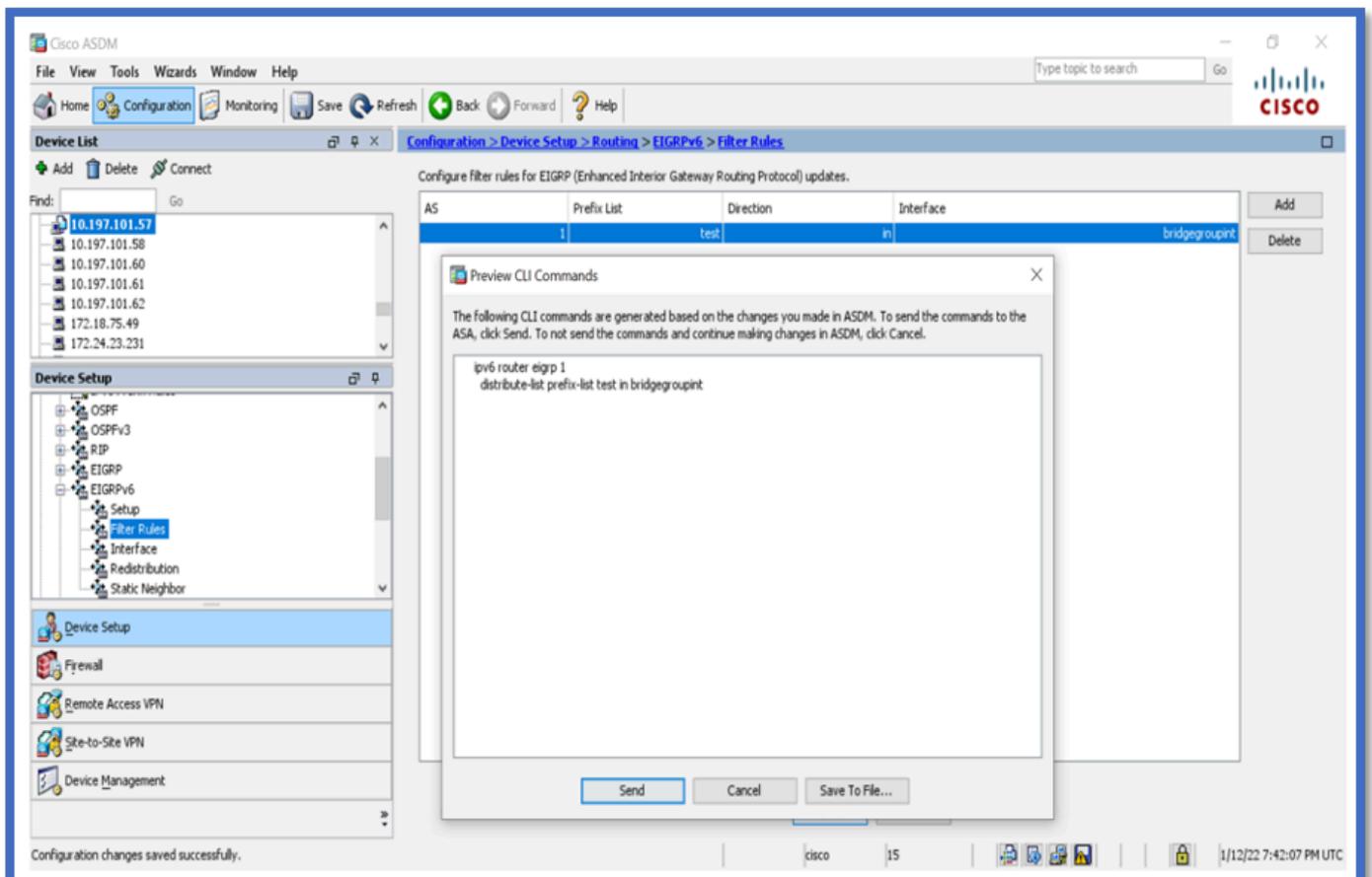


Configuration des règles de filtre (Distribute-List)

1. Accédez à Configuration > Device Setup > Routing > EIGRPv6 > Filter Rules.
2. Cliquez sur Add > Select Prefix list > Direction > Interface.
3. Click OK.

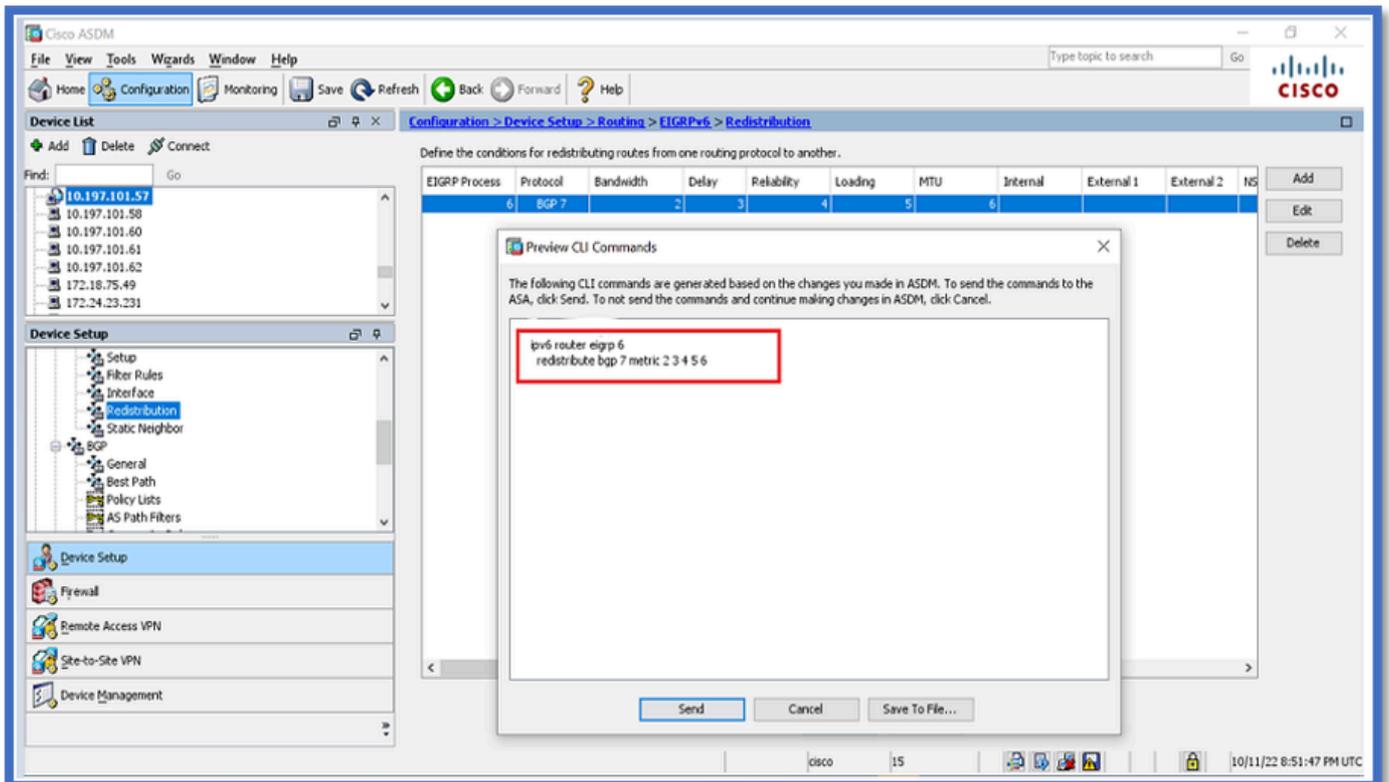
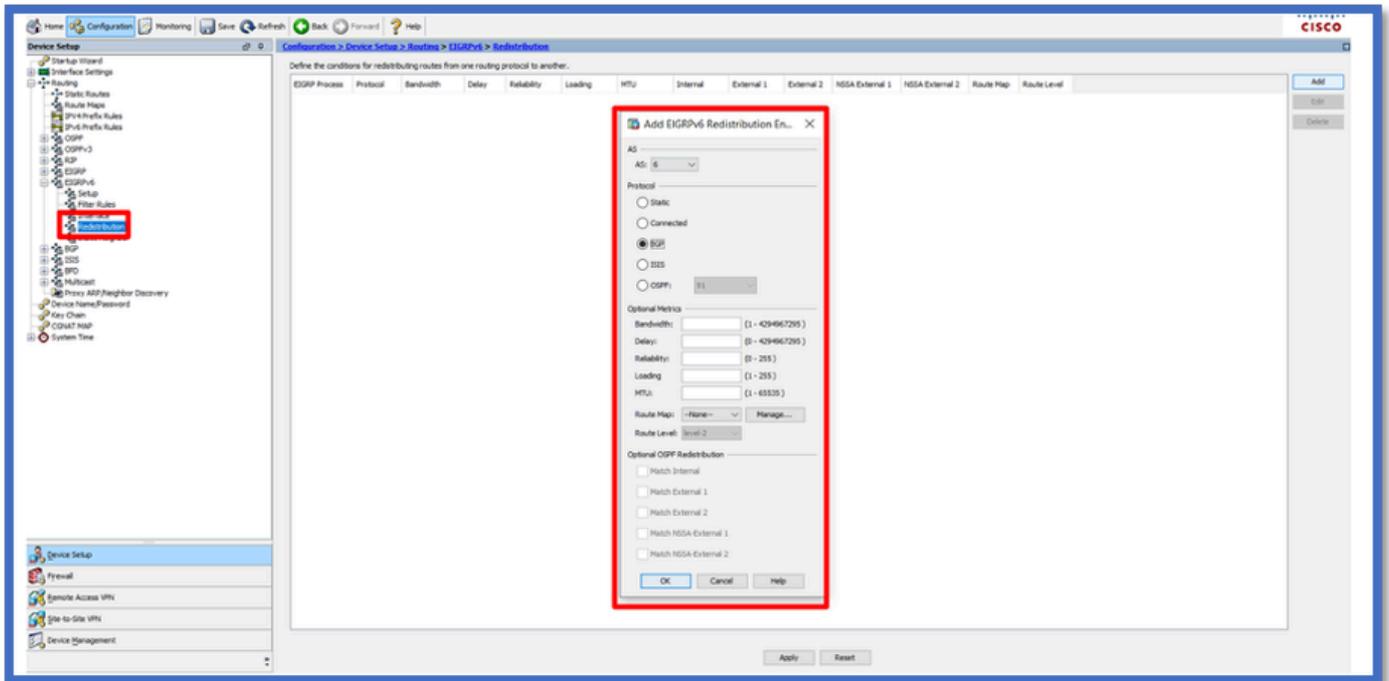


4. Cliquez sur Apply.
5. La fenêtre CLI s'affiche.



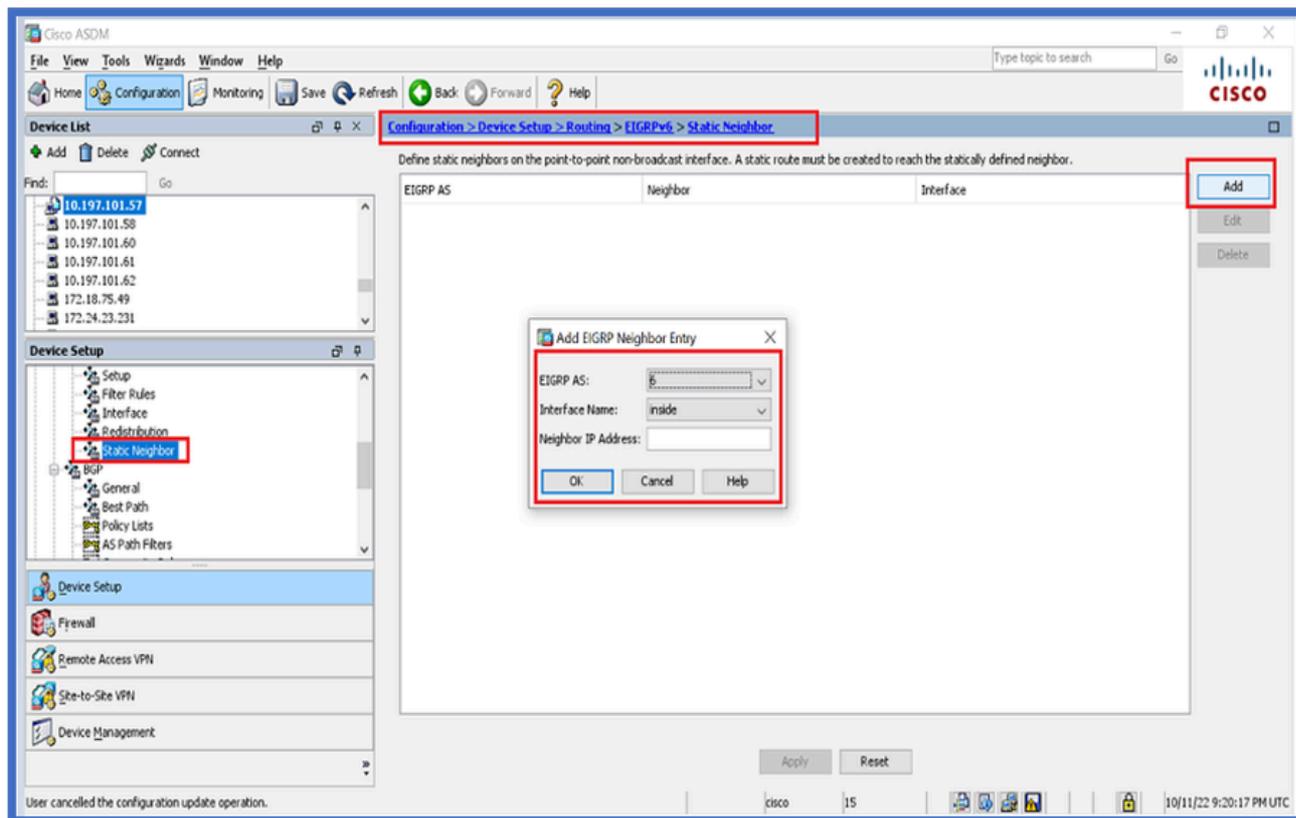
Redistribuer la configuration des routes

1. Accédez à Configuration > Device Setup > Routing > EIGRPv6 > Redistribution.
2. Cliquez sur Add > Select protocol.
3. Fournir des indicateurs facultatifs
4. Click OK.
5. Cliquez sur Apply.
6. La fenêtre CLI apparaît

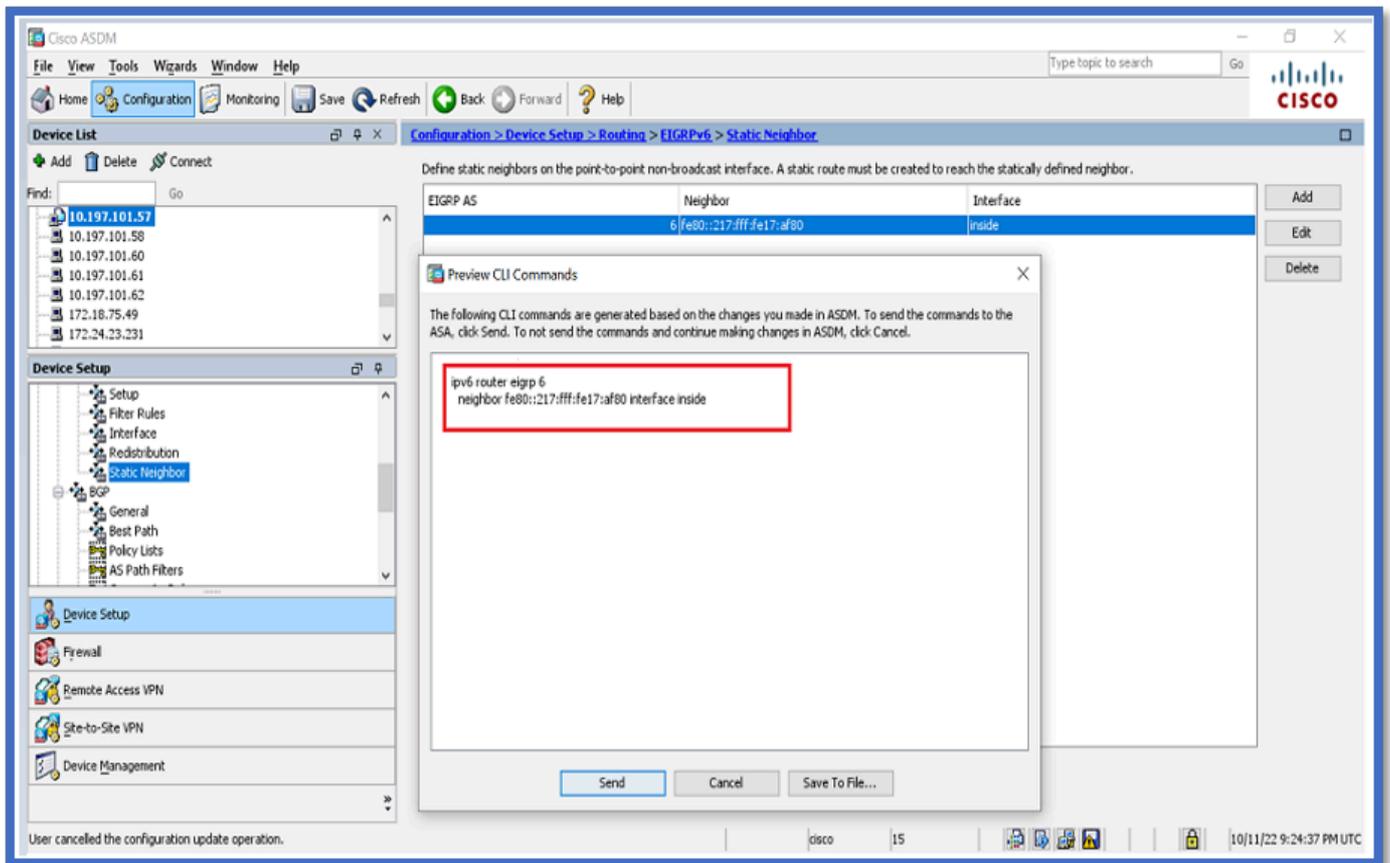


Voisin : mode routeur de monodiffusion

1. Accédez à Configuration > Device Setup > Routing > EIGRPv6 > Static Neighbor.
2. Cliquez sur Add > Select Interface.
3. Indiquez l'adresse du voisin.
4. Click OK.



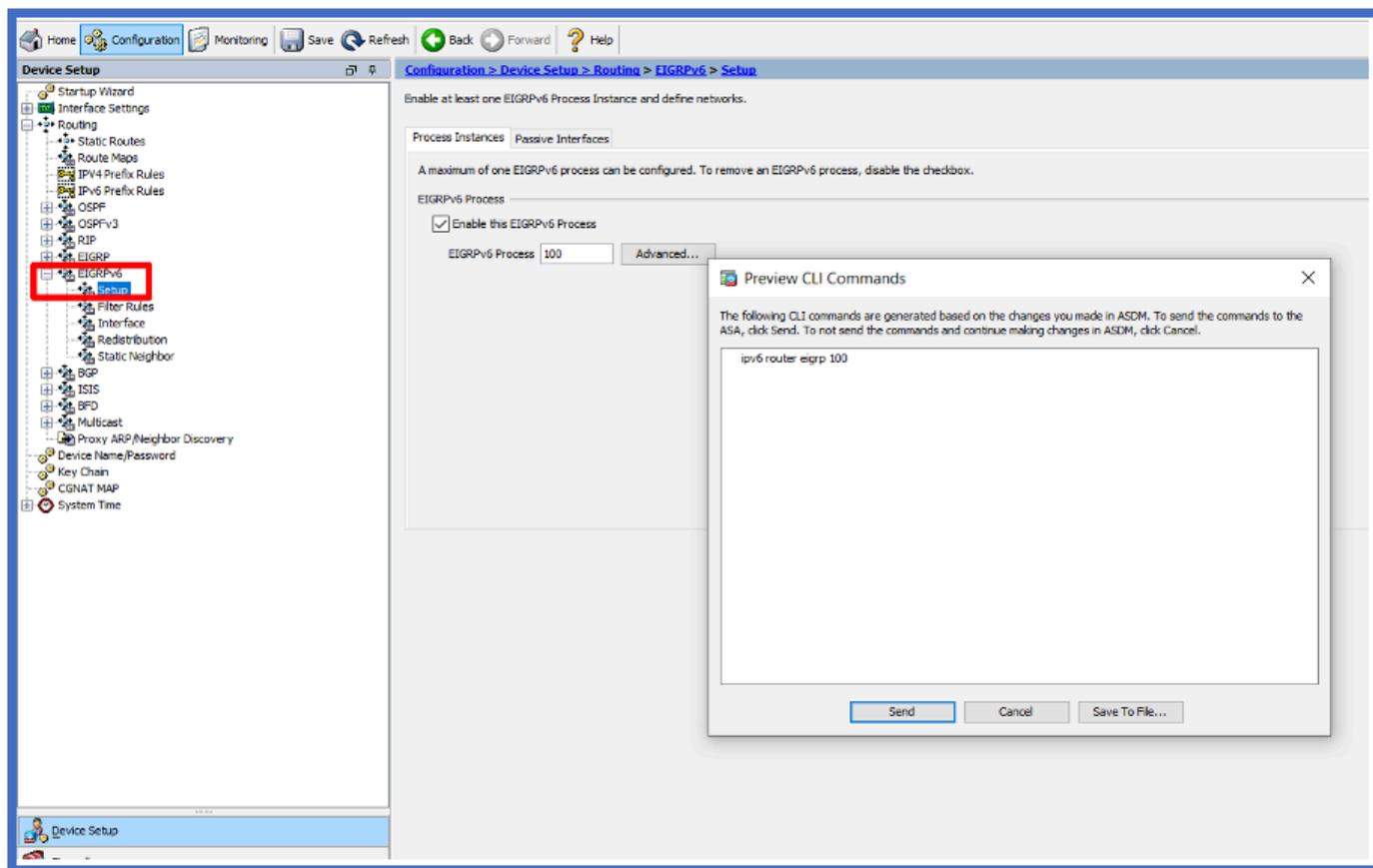
5. Cliquez sur Apply.
6. La fenêtre CLI s'affiche.



Mode routeur multidiffusion

La configuration du mode routeur multidiffusion est similaire à celle du mode routeur monodiffusion.

1. Accédez à Configuration > Device Setup > Routing > EIGRPv6 > Setup.
2. Case à cocher Activer pour activer le processus EIGRPv6.
3. Entrez une valeur dans le champ d'entrée Processus EIGRPv6.
4. Cliquez sur Apply.
5. Affichage de l'interface de ligne de commande



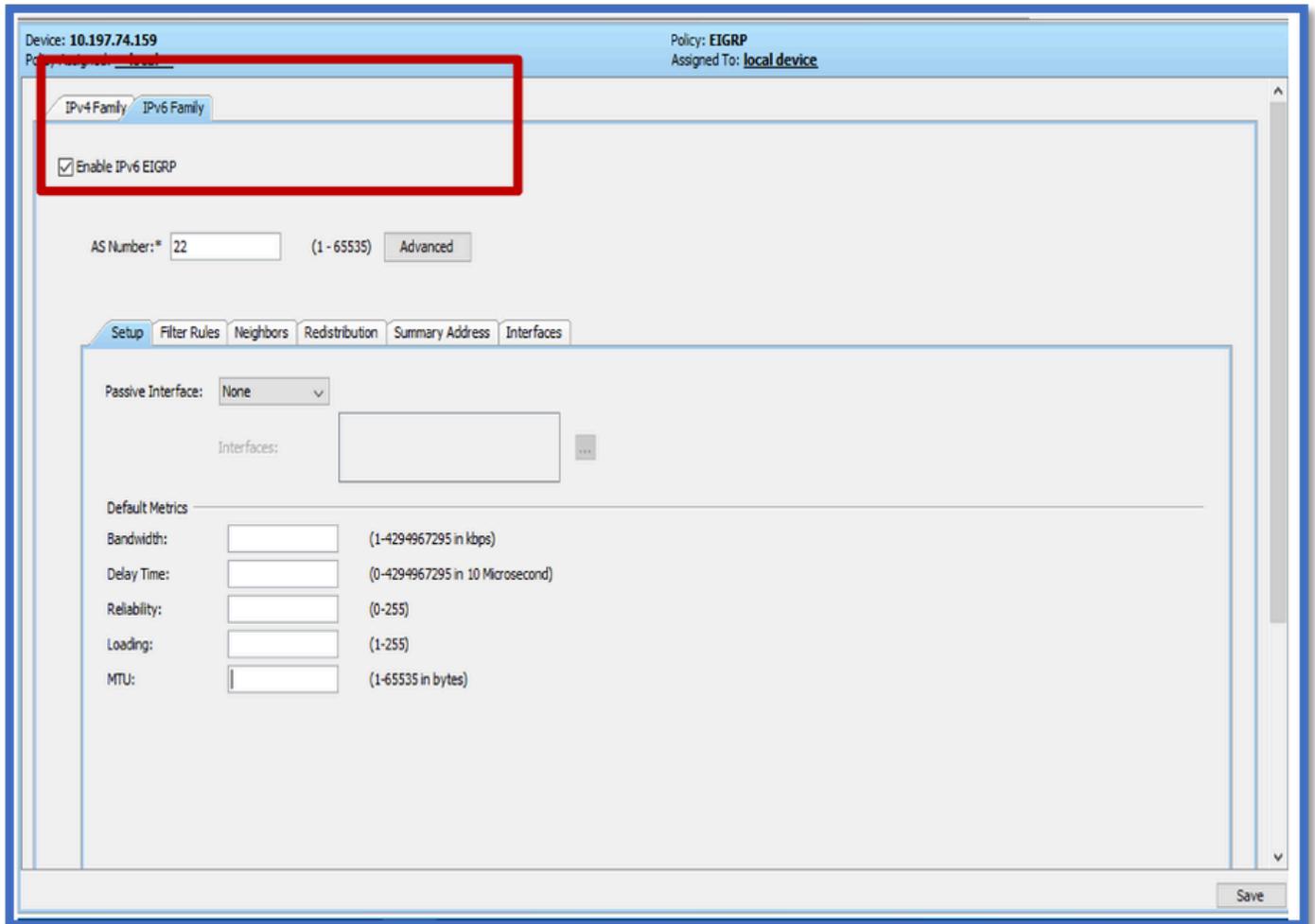
EIGRP IPv6 dans CSM

Présentation des nouvelles options dans CSM pour EIGRPv6

- La prise en charge EIGRPv6 est ajoutée dans le cadre de CSM 4.27.
- Configuration EIGRPv6 ajoutée dans le cadre de la commande Interfaces Sub CLI.
- Configuration EIGRPv6 ajoutée dans les commandes Router et Support Router.

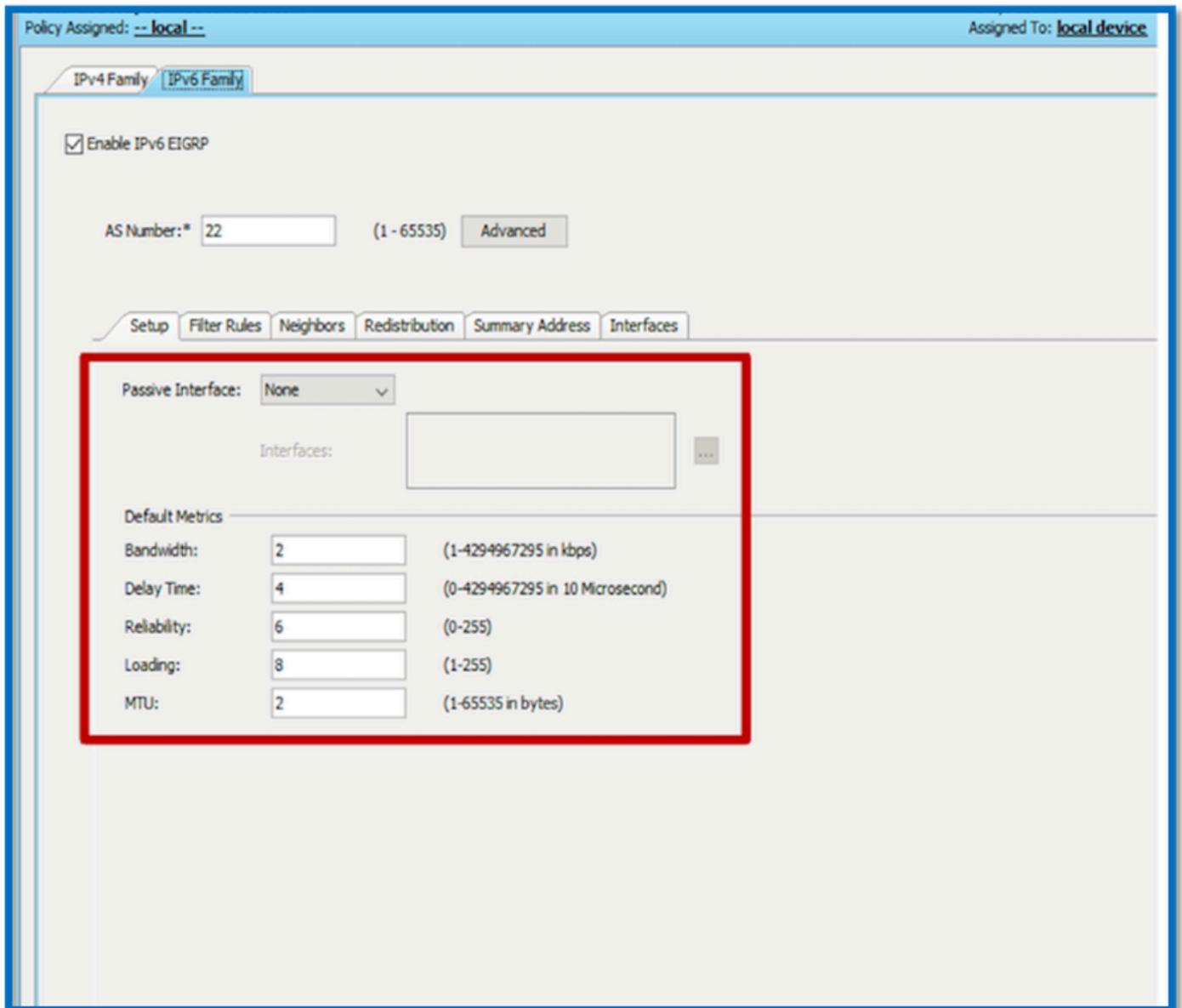
Activer la prise en charge EIGRP IPv6

1. Accédez à Platform > Routing > EIGRP > IPv6 Family.
2. Activez IPv6 en cochant la case Enable IPv6 EIGRP.
3. Indiquez un numéro AS compris entre 1 et 65535.
4. Les onglets permettent de configurer la configuration (illustrée ici), les règles de filtre, les voisins, la redistribution, l'adresse récapitulative et les interfaces.



Onglet EIGRP IPv6 Setup

1. Accédez à Platform > Routing > EIGRP > IPv6 Family > Setup.
2. L'interface passive a 3 options
 1. Aucune
 2. Valeur par défaut
 3. Interface spécifique
3. Par défaut Supprime les mises à jour de routage sur toutes les interfaces.
4. Dans Interface spécifique, sélectionnez interface dans le sélecteur Interface.
5. Affectez des valeurs aux mesures par défaut.
6. Cliquez sur OK et sur Save.



Onglet EIGRP IPv6 Filter Rules

1. Accédez à Platform > Routing > EIGRP > IPv6 Family > Filter Rules tab.
2. Sélectionnez la direction du filtre Eigrp selon la direction (entrante ou sortante).
3. Sélectionnez Interface.
4. Entrez la liste de préfixes IPv6 pour filtrer les connexions en fonction d'une liste de préfixes IPv6.

Device: **10.197.74.159** Policy: **EIGRP**
Policy Assigned: **-- local --** Assigned To: **lo**

IPv4 Family IPv6 Family

Enable IPv6 EIGRP

AS Number:* (1 - 65535)

Setup Filter Rules Neighbors Redistribution Summary Address Interfaces

No.	Direction	Interface	Prefix List
1	Inbound	outside	IPv6Prefix
2	Outbound	sstest	IPv6Prefix

Add/Edit IPv6 Eigrp Filter Page

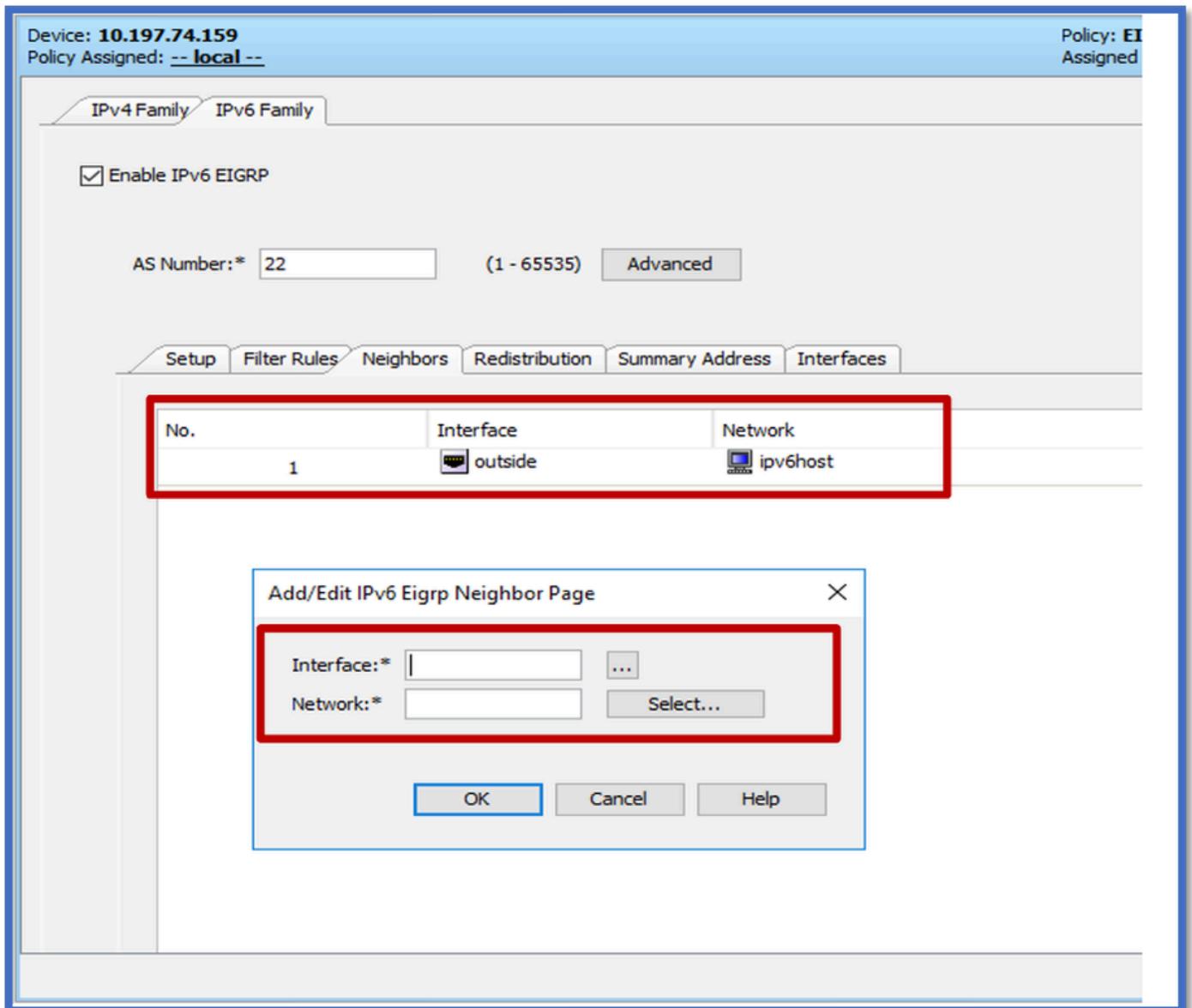
Eigrp Filter Direction:

Interface :* ...

IPv6 Prefix List:* ...

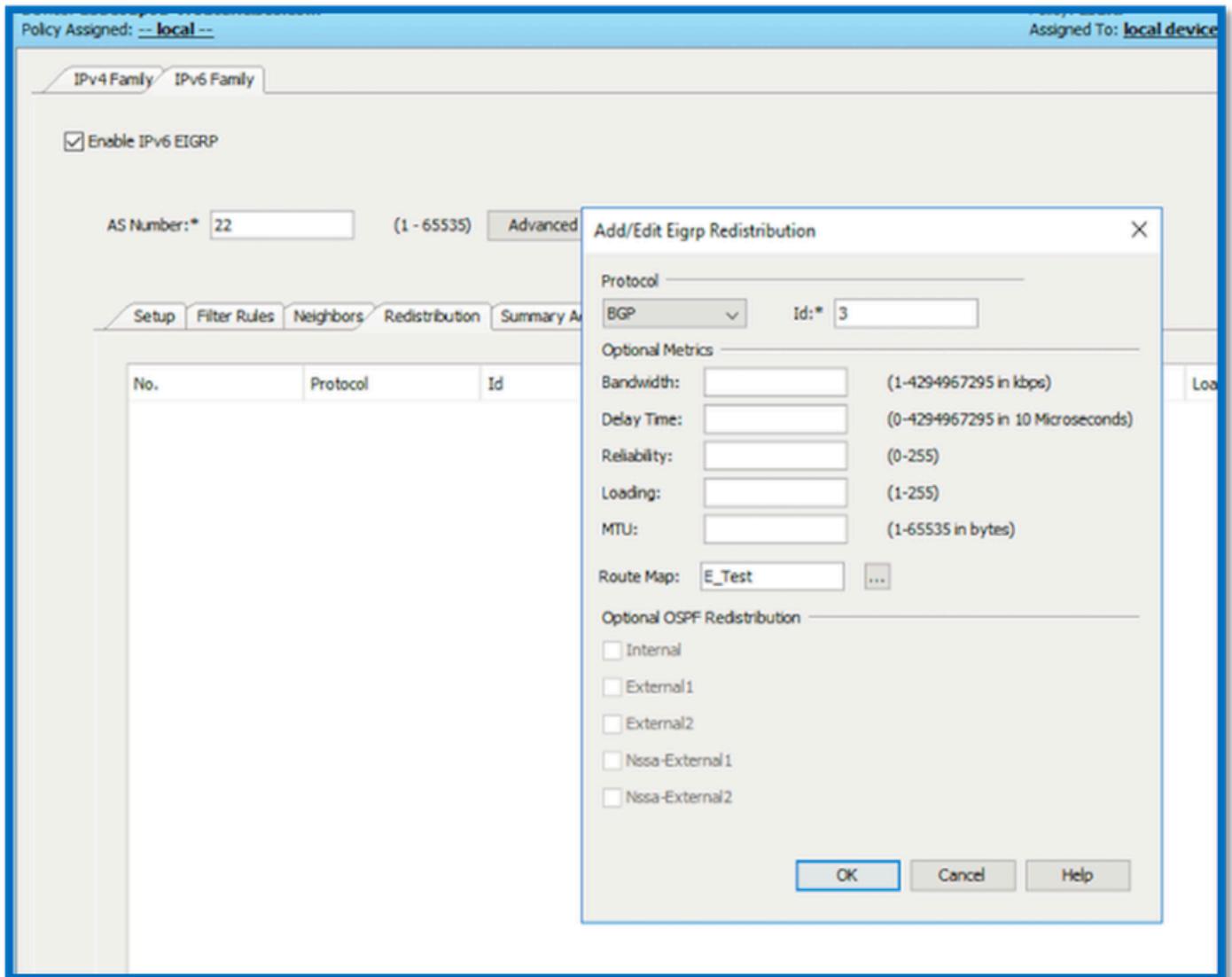
Onglet Voisins EIGRP IPv6

1. Accédez à Platform > Routing > EIGRP > IPv6 Family > Neighbors.
2. Entrez Interface et Network dans la boîte de dialogue Add/Edit IPv6 Eigrp Neighbor Page.



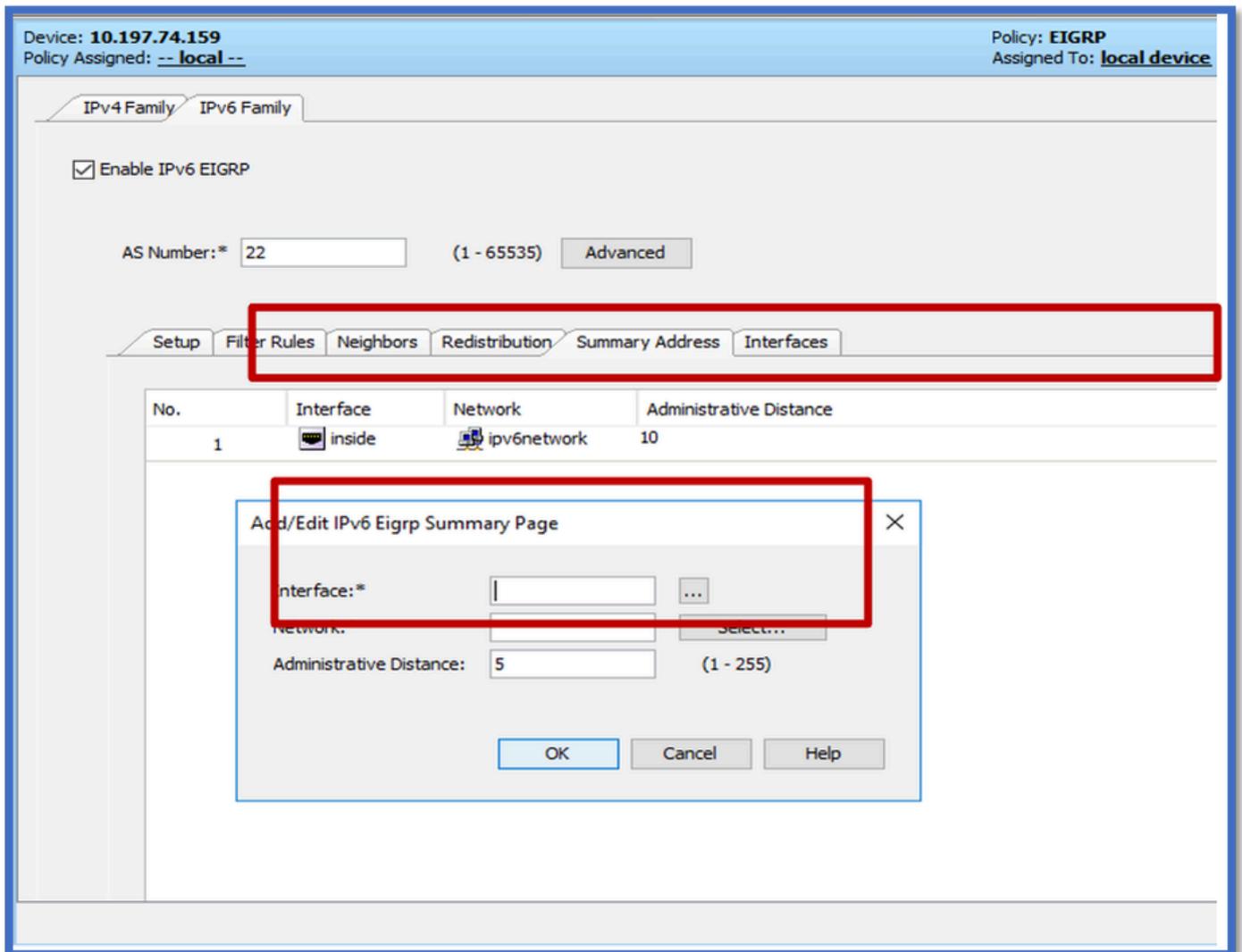
Onglet Redistribution IPv6 EIGRP

1. Accédez à Platform > Routing > EIGRP > IPv6 Family > Redistribution.
2. Cliquez sur le bouton Ajouter et sélectionnez Protocole. En fonction de la sélection du protocole, d'autres options sont activées.
3. Pour BGP et OSPF, ID textbox activé.
4. Si OSPF est activé, Options de redistribution OSPF facultatives activées
5. Si ISIS est activé Le niveau ISIS est activé.



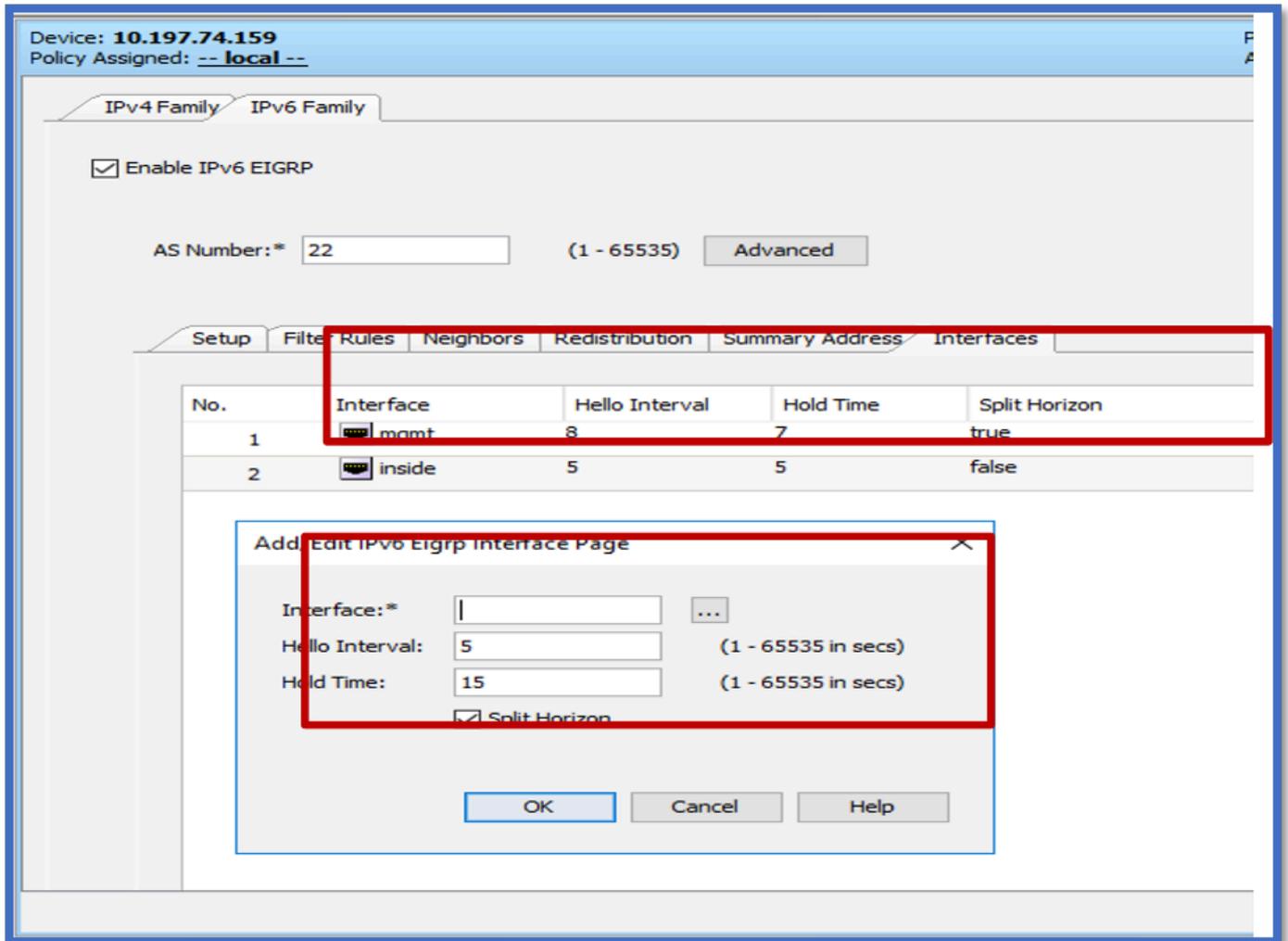
Onglet Résumé de l'adresse IPv6 EIGRP

1. Accédez à Platform > Routing > EIGRP > IPv6 Family > Summary Address.
2. Cliquez sur le bouton Add et sélectionnez interface dans le sélecteur Interface.
3. Dans Réseau, sélectionnez l'adresse IPv6 et la valeur de la distance administrative.
4. Cliquez sur OK et sur Save.



Onglet Interfaces EIGRP IPv6

1. Accédez à Platform > Routing > EIGRP > IPv6 Family > Interfaces.
2. Cliquez sur le bouton Ajouter et sélectionnez interface dans le sélecteur d'interface.
3. Vous pouvez modifier l'intervalle Hello et la durée d'attente (facultatif).
4. Le découpage d'horizon est activé par défaut. Elle peut être décochée.
5. Cliquez sur OK et sur Save.



Dépannage

Étapes de dépannage

- Vérifiez l'état du voisinage à l'aide des commandes show.
- Vérifiez le résultat de la commande show ipv6 eigrp topology pour vérifier le contenu de la table topologique.
- Utilisez la commande show ipv6 eigrp events, qui peut fournir des informations utiles sur les événements majeurs liés au protocole EIGRP.
- Utilisez la commande show eigrp tech-support detailed pour vérifier les valeurs du minuteur de la table de voisinage et de topologie.

Show ipv6 eigrp events

show ipv6 eigrp events affiche la journalisation des événements importants dans les systèmes qui sont utiles pour le débogage.

<#root>

```
ciscoasa(config-rtr)# show ipv6 eigrp events
```

Event information for AS 50:

```
1 18:05:56.203 Metric set: 1001::/64 768
2 18:05:56.203 Route installing: 1001::/64 fe80::250:56ff:fe9f:e7e8
4 18:05:56.203 FC sat rdbmet/succmet: 768 512
5 18:05:56.203 Rcv update dest/nh: 1001::/64 fe80::250:56ff:fe9f:e7e8
6 18:05:56.203 Change queue emptied, entries: 1
7 18:05:56.203 Metric set: 1001::/64 768
8 18:05:56.203 Update reason, delay: new if 4294967295
```

Show ipv6 eigrp timers

show ipv6 eigrp timers affiche le minuteur Hello actuel et le minuteur d'attente appliqué.

- Le minuteur par défaut pour l'intervalle Hello et le minuteur de mise en attente est de 5 secondes et 15 secondes.
- Si l'interface NBMA présente une bande passante plus faible, la valeur par défaut du minuteur Hello est de 15 secondes ; pour le minuteur d'attente, elle est de 180 secondes

<#root>

```
ciscoasa(config-rtr)# show ipv6 eigrp timers
```

```
EIGRP-IPv6 Timers for AS(50)
```

```
Hello Process
```

```
Expiration      Type
```

```
|      0 .406 (parent)
```

```
|      0 .406 Hello (m2)
```

```
Update Process
```

```
Expiration      Type
```

```
|     11.600 (parent)
```

```
|     11.600 (parent)
```

```
|     11.600 Peer holding
```

```
|     11.930 (parent)
```

```
|     11.930 Peer holding
```

Show ipv6 eigrp topology

show ipv6 eigrp topology La table topologique comprend toutes les destinations annoncées par un routeur voisin.

<#root>

```
ciscoasa(config-rtr)# show ipv6 eigrp topology
```

```
EIGRP-IPv6 Topology Table for AS(50)/ID(172.27.173.103)
```

```
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
```

```
       r - reply Status, s - sia Status
```

```
P 1001::/64, 1 successors, FD is 768, serno 8907
```

```
       via fe80::250:56ff:fe9f:8d83 (768/512), m2
```

```
P 3001::/64, 1 successors, FD is 768, serno 8906
```

```
       via fe80::250:56ff:fe9f:8d83 (768/512), m2
```

```
P 2001::/64, 1 successors, FD is 768, serno 8905
```

```
       via fe80::250:56ff:fe9f:8d83 (768/512), m2
```

Show Tech pour EIGRP

Show tech peut être utilisé pour le dépannage car il collecte des informations utiles, notamment les paramètres de minuteur, les détails de voisinage, les statistiques de trafic pour le protocole EIGRP, les compteurs d'utilisation de la mémoire, etc.

<#root>

```
ciscoasa(config-if)# show eigrp tech-support detailed ?
```

```
exec mode commands/options:
```

```
| Output modifiers
```

```
<cr>
```

```
ciscoasa(config-if)#
```

Exemple de problème

Problème avec la formation de voisins

- Si un problème se produit avec la formation de voisins :
 - Vérifiez si vous avez au moins une adresse IPv4 configurée si router-id n'est pas explicitement configuré dans la configuration en mode routeur.
 - Assurez-vous de configurer router-id sous router mode configuration.

Historique de révision

Révision	Date de publication	Commentaires
2.0	19-juil-2024	Mise en forme mise à jour.
1.0	18-juil-2024	Première publication

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.