



## EIGRP

---

Cette section décrit comment configurer la défense contre les menaces pour acheminer les données, effectuer l'authentification et redistribuer les informations de routage à l'aide du protocole EIGRP (Enhanced Interior Gateway Routing Protocol).

- [À propos du routage de protocole EIGRP \(Enhanced Interior Gateway Routing Protocol, Protocole de routage de passerelle intérieure amélioré\), à la page 1](#)
- [Exigences et conditions préalables pour EIGRP, à la page 2](#)
- [Directives et limites pour le routage EIGRP, à la page 3](#)
- [Configurer le protocole EIGRP, à la page 4](#)

## À propos du routage de protocole EIGRP (Enhanced Interior Gateway Routing Protocol, Protocole de routage de passerelle intérieure amélioré)

Le protocole EIGRP (Enhanced Interior Gateway Routing Protocol), développé par Cisco, est une version améliorée du protocole IGRP. Contrairement à IGRP et RIP, EIGRP n'envoie pas de mises à jour périodiques de routage. Les mises à jour du protocole EIGRP sont envoyées uniquement lorsque la topologie du réseau change. Les principales fonctionnalités qui distinguent le protocole EIGRP des autres protocoles de routage comprennent la convergence rapide, la prise en charge des masques de sous-réseau de longueur variable, des mises à jour partielles et de plusieurs protocoles de couche réseau.

Un routeur exécutant EIGRP stocke toutes les tables de routage des voisins afin qu'il puisse s'adapter rapidement aux autres routes. Si aucune route appropriée n'existe, le protocole EIGRP interroge ses voisins pour découvrir une autre route. Ces requêtes se propagent jusqu'à ce qu'une autre voie de routage soit trouvée. La prise en charge du protocole EIGRP pour les masques de sous-réseau de longueur variable permet aux routes d'être récapitulées automatiquement sur une limite de réseau. En outre, EIGRP peut être configuré pour résumer n'importe quelle limite de bits à n'importe quelle interface.

Le protocole EIGRP ne fait pas de mises à jour périodiques. Au lieu de cela, il envoie des mises à jour partielles lorsque la métrique d'une voie de routage change. La propagation des mises à jour partielles est automatiquement limitée de sorte que seuls les routeurs qui ont besoin des informations sont mis à jour. En raison de ces deux fonctionnalités, EIGRP consomme beaucoup moins de bande passante qu'IGRP.

Pour se familiariser dynamiquement avec la présence d'autres routeurs sur les réseaux directement connectés, la défense contre les menaces utilise la découverte de voisin. Les routeurs EIGRP envoient des paquets Hello en multidiffusion pour annoncer leur présence sur le réseau. Lorsque le périphérique EIGRP reçoit un paquet

Hello d'un nouveau voisin, il envoie son tableau de topologie au voisin avec un bit d'initialisation activé. Lorsque le voisin reçoit la mise à jour de la topologie avec le bit d'initialisation activé, le voisin renvoie sa table de topologie au périphérique.

Les paquets Hello sont envoyés en tant que messages en multidiffusion. Aucune réponse n'est attendue pour un message Hello. Les voisins définis de manière statique constituent une exception à cette règle. Si vous configurez manuellement un voisin, les messages Hello, les mises à jour de routage et les accusés de réception sont envoyés en tant que messages monodiffusion.

Une fois cette relation de voisin établie, les mises à jour de routage ne sont pas échangées, sauf en cas de modification de la topologie du réseau. La relation de voisin est maintenue tout au long des paquets Hello. Chaque paquet Hello reçu d'un voisin comprend un temps d'attente. Le délai d'attente est le délai pendant lequel la défense contre les menaces peut s'espérer recevoir un paquet Hello de ce voisin. Si le périphérique ne reçoit pas de paquet Hello de ce voisin dans le délai d'attente annoncé par ce voisin, le périphérique considère que ce voisin n'est pas disponible.

Le protocole EIGRP utilise la découverte/récupération du voisin, le protocole RTP (Reliable Transport Protocol) et l'algorithme de diffusion de mise à jour (DUAL) pour les calculs de routage. DUAL enregistre tous les routages vers une destination dans le tableau de topologie, et pas seulement le routage le moins coûteux. La voie de routage la moins coûteuse est insérée dans la table de routage. Les autres routages demeurent dans le tableau de topologie. En cas de défaillance de la voie principale, une autre voie est choisie parmi les successeurs possibles. Un successeur est un routeur voisin utilisé pour le transfert de paquets qui a un chemin de moindre coût vers une destination. Un calcul de faisabilité garantit que le chemin ne fait pas partie d'une boucle de routage.

Si un successeur possible n'est pas trouvé dans le tableau de topologie, un recalcul de routage a lieu. Lors du recalcul de la route, DUAL interroge les voisins EIGRP pour déterminer une route. La requête est transmise aux voisins successifs. Si un successeur possible n'est pas trouvé, un message unreachable est renvoyé.

Lors du recalcul de la route, DUAL marque la route comme active. Par défaut, la défense contre les menaces attend trois minutes avant de recevoir une réponse de ses voisins. Si le périphérique ne reçoit pas de réponse d'un voisin, la voie de routage est marquée comme bloquée active. Tous les routages dans le tableau de topologie qui désignent le voisin qui ne répond pas comme un successeur de faisabilité sont supprimés.

## Exigences et conditions préalables pour EIGRP

### Prise en charge des modèles

Défense contre les menaces

Défense contre les menaces virtuelles

### Domaines pris en charge

N'importe quel

### Rôles utilisateur

Admin

Administrateur de réseau

# Directives et limites pour le routage EIGRP

## Directives sur le mode pare-feu

Pris en charge uniquement en mode pare-feu routé.

## Directives relatives aux périphériques

- Un seul processus EIGRP autorisé par périphérique.
- EIGRP peut être configuré par le biais de l'interface utilisateur du centre de gestion sur défense contre les menaces 6.6 et versions ultérieures.

## Directives relatives à l'interface

- Seules les interfaces routées avec des noms logiques et une adresse IP peuvent être associées à un processus de routage EIGRP.
- Seules les interfaces appartenant au routeur virtuel global peuvent faire partie de EIGRP. EIGRP peut apprendre, filtrer et redistribuer les routes entre les protocoles de routage dans un routeur virtuel global.
- Prend en charge les sous-interfaces physiques EtherChannel redondantes uniquement. Cependant, les membres des interfaces EtherChannel ne sont pas pris en charge.
- Les BVI et VNI ne peuvent pas faire partie de EIGRP.
- Une interface passive ne peut pas être configurée comme interface voisine.

## Prise en charge des adresses IP et des objets de réseau

- Seule les adresses IPv4 sont prises en charge.
- La plage, le nom de domaine complet (FQDN) et le masque générique ne sont pas pris en charge.
- Seuls les objets de liste d'accès standard sont pris en charge.

## Directives de redistribution

- BGP, OSPF et IPS dans le routeur virtuel global peuvent effectuer une redistribution vers EIGRP.
- EIGRP peut effectuer une redistribution vers BGP, OSPF, IPS, statique et connecté dans le routeur virtuel global.
- Lorsque EIGRP est configuré sur un périphérique qui fait partie du réseau OSPF ou inversement, assurez-vous que le routeur OSPF est configuré pour baliser le routage (EIGRP ne prend pas en charge la balise de routage).

Lors de la redistribution d'EIGRP dans OSPF et d'OSPF dans EIGRP, une boucle de routage se produit en cas de panne sur une des liaisons ou interfaces ou même lorsque l'expéditeur de la route est en panne. Pour empêcher la redistribution des routages d'un domaine vers le même domaine, un routeur peut marquer un routage qui appartient à un domaine pendant qu'il redistribue, et ces routages peuvent être filtrés sur le routeur distant en se basant sur la même balise. Comme les routes ne seront pas installées dans la table de routage, elles ne seront pas redistribuées dans le même domaine.

### Directives en matière de processus déploiement

Lorsque vous souhaitez modifier le numéro de système autonome existant d'une configuration EIGRP déployée, vous devez désactiver le protocole EIGRP et le déployer. Cette étape effacera la configuration du protocole EIGRP déployé sur la défense contre les menaces. Ensuite, recréez les configurations du protocole EIGRP avec un nouveau numéro de système autonome, puis déployez-le. Ainsi, ce processus empêche tout échec de déploiement du fait que la même configuration EIGRP est déployée sur la défense contre les menaces.

### Directives de mise à niveau

Lorsque vous effectuez une mise à niveau vers la version 7.2 ou une version ultérieure, lorsque la version précédente comporte des politiques EIGRP FlexConfig, le centre de gestion affiche un message d'avertissement pendant le déploiement. Cependant, cela n'arrête pas le processus de déploiement. Toutefois, après le déploiement, pour gérer les politiques EIGRP à partir de l'interface utilisateur (**Device (Edit) > Routing > EIGRP**) (Périphérique (Modifier) > Routage > EIGRP), vous devez refaire la configuration dans la page **Device (Edit) > Routing > EIGRP** et supprimer la configuration de FlexConfig. Pour automatiser la création des politiques dans l'interface utilisateur, centre de gestion offre une option de migration des politiques de FlexConfig vers l'interface utilisateur. Pour en savoir plus, consultez [Migration des politiques FlexConfig](#).

## Configurer le protocole EIGRP

Vous pouvez activer et configurer le protocole EIGRP sur le périphérique de pare-feu dans l'onglet **Routing** (routage).

### Procédure

- 
- Étape 1** Sélectionnez **Devices (appareils) > Device Management (gestion des appareils)**, et modifiez l'appareil défense contre les menaces .
- Étape 2** Cliquez sur l'onglet **Routage**.
- Étape 3** Sous Global, cliquez sur **EIGRP**.
- Étape 4** Cochez la case **Enable EIGRP** (activer le protocole EIGRP) pour activer le processus de routage par protocole EIGRP.
- Étape 5** Dans le champ **AS Number** (numéro de système autonome), saisissez le numéro de système autonome (AS) pour le processus EIGRP. Le numéro AS comprend plusieurs numéros autonomes. Le numéro AS peut être compris entre 1 et 65535 et c'est une valeur attribuée de façon unique qui identifie chaque réseau sur Internet.
- Étape 6** Pour configurer d'autres propriétés du protocole EIGRP, consultez les rubriques suivantes :
1. [Configurer les paramètres EIGRP, à la page 5.](#)
  2. [Configurer les paramètres des voisins EIGRP, à la page 5.](#)
  3. [Configurer les paramètres des règles de filtre EIGRP, à la page 6.](#)
  4. [Configurer les paramètres de redistribution EIGRP, à la page 6.](#)
  5. [Configurer les paramètres de l'adresse de résumé EIGRP, à la page 8.](#)
  6. [Configurer les paramètres des interfaces EIGRP, à la page 8.](#)

7. [Configurer les paramètres avancés EIGRP, à la page 9.](#)

---

## Configurer les paramètres EIGRP

### Procédure

---

- Étape 1** Dans la page **EIGRP**, cliquez sur l'onglet **Setup** (Configuration).
- Étape 2** Cochez la case **Auto Summary** (Résumé automatique) pour permettre au protocole EIGRP de résumer les limites des numéros de réseau.
- Remarque** L'activation du résumé automatique peut entraîner des problèmes de routage si vous avez des réseaux non contigus.
- Étape 3** Dans la zone **Réseaux/Hôtes disponibles**, cliquez sur les réseaux ou les hôtes qui doivent participer au processus de routage par protocole EIGRP, puis cliquez sur **Ajouter**. Pour ajouter un nouvel objet réseau, cliquez sur **Ajouter** (+). Consultez [Réseau](#) pour connaître la procédure d'ajout de réseaux.
- Étape 4** Pour configurer des interfaces passives, cochez la case **Passive Interface** (interface passive). Dans EIGRP, une interface passive n'envoie ni ne reçoit de mises à jour de routage.
- a) Pour définir des interfaces sélectives comme passives, cliquez sur le bouton radio **Interface sélectionnée**. Pour associer des interfaces, sélectionnez-les dans la zone **Interfaces disponibles**, puis cliquez sur **Add** (Ajouter).
  - b) Pour définir toutes les interfaces comme passives, cliquez sur le bouton radio **All Interfaces** (Toutes les interfaces).
- Étape 5** Cliquez sur **OK** et **Save** (Enregistrer) pour enregistrer les paramètres.
- 

## Configurer les paramètres des voisins EIGRP

Vous pouvez définir des voisins statiques pour le processus EIGRP. Lorsque vous définissez un voisin EIGRP, les paquets Hello sont monodiffusés pour ce voisin.

### Procédure

---

- Étape 1** Dans la page **EIGRP**, cliquez sur l'onglet **Neighbors** (Voisins).
- Étape 2** Cliquez sur **Add** (ajouter).
- Étape 3** Dans la liste déroulante **Interface**, choisissez l'interface par laquelle le voisin est disponible.
- Étape 4** Dans la liste déroulante **Neighbor** (voisin), choisissez l'adresse IP du voisin statique. Pour ajouter l'objet réseau, cliquez sur **Ajouter** (+). Consultez [Réseau](#) pour connaître la procédure d'ajout d'objets réseau.
- Étape 5** Cliquez sur **OK** et **Save** (Enregistrer) pour enregistrer les paramètres.
-

## Configurer les paramètres des règles de filtre EIGRP

Vous pouvez configurer des règles de filtrage de routage pour le processus de routage EIGRP. Les règles de filtrage vous permettent de contrôler les routages acceptés ou annoncés par le processus de routage par protocole EIGRP.

### Procédure

- 
- Étape 1** Dans la page **EIGRP**, cliquez sur l'onglet **Filter Rules** (Règles de filtrage).
- Étape 2** Cliquez sur **Ajouter** (+).
- Étape 3** Dans la boîte de dialogue **Add Filter Rules** (ajouter des règles de filtre), dans la liste déroulante **Filter Direction** (direction du filtre), choisissez la direction de la règle :
- Entrante : la règle filtre les informations de routage par défaut des mises à jour de routage par protocole EIGRP entrantes.
  - Sortante : la règle filtre les informations de routage par défaut des mises à jour de routage EIGRP sortantes.
- Étape 4** Pour sélectionner l'interface à laquelle la règle de filtrage s'applique, cliquez sur le bouton radio **Interface** et dans la liste déroulante, sélectionnez l'interface.
- Étape 5** Pour sélectionner le protocole auquel la règle de filtrage s'applique, cliquez sur le bouton radio **Protocol** (protocole) et dans la liste déroulante, sélectionnez le protocole : BGP, IPS, Static, Connected ou OSPF. Pour les protocoles BGP et OSPF, vous pouvez spécifier l'ID de processus approprié.
- Étape 6** Dans la liste déroulante **Access List** (liste d'accès), sélectionnez la liste d'accès. La liste définit les réseaux qui doivent être reçus et qui doivent être supprimés dans les mises à jour de routage. Pour ajouter un nouvel objet à la liste d'accès standard, cliquez sur **Ajouter** (+) et consultez [Configurer les objets ACL standard](#) pour connaître la procédure détaillée.
- Étape 7** Cliquez sur **OK** et **Save** (Enregistrer) pour enregistrer les paramètres.
- 

## Configurer les paramètres de redistribution EIGRP

Précisez les règles de redistribution des routages à partir d'autres protocoles de routage vers le processus de routage par protocole EIGRP.

### Procédure

- 
- Étape 1** Dans la page **EIGRP**, cliquez sur l'onglet **Redistribution**.
- Étape 2** Cliquez sur **Ajouter** (+).
- Étape 3** Dans la boîte de dialogue **Add Redistribution** (Ajouter une redistribution), dans la liste déroulante **Protocol** (protocole), choisissez le protocole source à partir duquel les routes sont redistribuées :
- BGP : redistribue les routages découverts par le processus de routage BGP vers EIGRP.
  - IPS : Redistribue les routages détectés par le processus de routage IPS vers le protocole EIGRP.

- **Statique** : redistribue les routes statiques vers le processus de routage EIGRP. Les routes statiques qui entrent dans la portée d'un relevé du réseau sont automatiquement redistribuées vers EIGRP; vous n'avez pas besoin de définir de règle de redistribution les concernant.
- **Connectée** : redistribue les routes connectées (les routes sont établies automatiquement parce que l'adresse IP est activée sur l'interface) au processus de routage EIGRP. Les routes connectées qui entrent dans la portée d'un relevé de réseau sont automatiquement redistribuées vers EIGRP; vous n'avez pas besoin de définir de règle de redistribution les concernant.
- **OSPF** : redistribue les routages détectés par le processus de routage OSPF vers le protocole EIGRP. Si vous choisissez ce protocole, les options de correspondance de cette boîte de dialogue deviennent disponibles sous **Redistribution OSPF facultative** :
  - **Internal** : routes internes à un système autonome spécifique.
  - **External1** : routes externes au système autonome et importées dans OSPF en tant que route externe de type 1.
  - **External2** : routes externes au système autonome et importées dans le processus sélectionné en tant que route externe de type 2.
  - **Nsaa-External1** : routes Not-So-Stubby Area (NSSA) externes au système autonome et importées dans le processus sélectionné en tant que routes externes de type 1.
  - **Nsaa-External2** : routes (NSSA) externes au système autonome et importées dans le processus sélectionné en tant que routes externes de type 2.

**Remarque** Ces options ne sont pas disponibles lors de la redistribution de routes statiques, connectées, IPS ou BGP.

**Étape 4** Sous **Mesures facultatives**, saisissez les valeurs pertinentes :

- **Bande passante** : la bande passante minimale de la voie de routage en kilobits par seconde. Les valeurs valides sont comprises entre 0 et 4294967294.
- **Temps de retard** le retard de routage en dizaines de microsecondes. Les valeurs valides vont de 0 à 4294967295.
- **Fiabilité** : la probabilité de transmission réussie des paquets est exprimée par un nombre de 0 à 255. La valeur 255 indique une fiabilité de 100 %; 0 signifie l'absence de fiabilité.
- **Chargement** : la bande passante effective de la route. Les valeurs valides sont comprises entre 0 et 255. La valeur 255 indique un chargement à 100 %.
- **MTU** : la plus petite valeur autorisée pour l'unité de transmission maximale du chemin. Cette valeur peut être comprise entre 1 et 65 535.

**Étape 5** Dans la liste déroulante **Route Map** (carte de routage), choisissez l'objet de carte de routage à appliquer à l'entrée de redistribution. Pour créer un nouvel objet de carte de routage, cliquez sur **Ajouter** (+). Voir [Configurer l'entrée de la carte de routage](#) pour connaître la procédure d'ajout d'une nouvelle carte de routage.

**Étape 6** Cliquez sur **OK** et **Save** (Enregistrer) pour enregistrer les paramètres.

## Configurer les paramètres de l'adresse de résumé EIGRP

Vous pouvez configurer des adresses sommaires pour chaque interface. Vous devez définir manuellement les adresses de récapitulatif si vous souhaitez créer des adresses de récapitulatif qui ne se produisent pas à une limite du réseau, ou si vous souhaitez utiliser des adresses de récapitulatif dans la défense contre les menaces avec le récapitulatif de routage automatique désactivé. Si des routes plus spécifiques sont disponibles dans la table de routage, EIGRP annonce l'adresse sommaire avec une métrique égale au minimum de toutes les routes plus spécifiques.

### Procédure

- 
- Étape 1** Dans la page **EIGRP**, cliquez sur l'onglet **Summary Address** (adresse sommaire).
  - Étape 2** Cliquez sur **Add** (ajouter).
  - Étape 3** Dans la liste déroulante **Interface**, choisissez l'interface à partir de laquelle l'adresse sommaire est annoncée.
  - Étape 4** Dans la liste déroulante **Network** (réseau), choisissez l'objet réseau avec une adresse IP et un masque de réseau spécifiques à résumer. Pour ajouter un nouveau réseau, cliquez sur **Ajouter** (+). Consultez [Réseau](#) pour connaître la procédure d'ajout de réseaux.
  - Étape 5** Dans le champ **Distance administrative**, saisissez la distance administrative pour l'acheminement résumé. Les valeurs valides sont comprises entre 0 et 255.
  - Étape 6** Cliquez sur **OK** et **Save** (Enregistrer) pour enregistrer les paramètres.
- 

## Configurer les paramètres des interfaces EIGRP

Vous pouvez configurer les propriétés de routage par protocole EIGRP spécifiques à l'interface dans l'onglet Interfaces.

### Procédure

- 
- Étape 1** Dans la page **EIGRP**, cliquez sur l'onglet **Interfaces**.
  - Étape 2** Cliquez sur **Ajouter** (+).
  - Étape 3** Dans la liste déroulante **Interface**, choisissez le nom de l'interface à laquelle la configuration s'applique.
  - Étape 4** Dans le champ **Hello Interval**, saisissez l'intervalle, en secondes, entre les paquets Hello du protocole EIGRP qui sont envoyés sur une interface. Cette valeur peut être comprise entre 1 et 65 535. La valeur par défaut est de 5 secondes.
  - Étape 5** Dans le champ **Hold Time** (temps d'attente), saisissez le temps d'attente annoncé par le périphérique dans les paquets Hello du protocole EIGRP. Cette valeur peut être comprise entre 3 et 65 535. La valeur par défaut est 15secondes.
  - Étape 6** Pour activer le mode partagé par protocole EIGRP sur l'interface, cochez la case **Split Horizon** (Diviser l'horizon).
  - Étape 7** Dans le champ **Delay Time**, (Délai de retard) saisissez le temps de retard en dixièmes de microsecondes. Cette valeur peut être comprise entre 1 et 16 777 215. Cette option n'est pas prise en charge pour les périphériques en mode contexte multiple.
  - Étape 8** Précisez les valeurs des propriétés d'authentification :



- **Enable MD5 Authentication** (activer l'authentification MD5) : Cochez la case pour utiliser l'algorithme de hachage MD5 pour l'authentification des paquets EIGRP.
- **Key Type** (type de clé) : Dans la liste déroulante, sélectionnez l'un des types de clé suivants :
  - **None** (Aucun) : Pour indiquer qu'aucune authentification n'est requise.
  - **Unencrypted** (non chiffré) : Pour indiquer que la chaîne de clé à utiliser est un mot de passe en texte clair pour l'authentification.
  - **Encrypted** (chiffré) : Pour indiquer que la chaîne de clé à utiliser est un mot de passe chiffré pour l'authentification.
  - **Auth Key** (clé d'authentification) : Pour indiquer que la chaîne de clé à utiliser est une clé d'authentification EIGRP.
- **Key ID** (ID de la clé) : ID de la clé utilisée pour authentifier les mises à jour du protocole EIGRP. Saisissez un identifiant de clé numérique. Les valeurs valides sont comprises entre 0 et 255.
- **Key** (clé) : chaîne de caractères alphanumériques comptant jusqu'à 17 caractères. Pour une authentification de type chiffré, ce champ doit comporter un minimum de 17 caractères.
- **Confirm Key** (Confirmer la clé) : Saisissez à nouveau la clé.

**Étape 9** Cliquez sur **OK** et **Save** (Enregistrer) pour enregistrer les paramètres.

---

## Configurer les paramètres avancés EIGRP

Vous pouvez configurer les paramètres avancés du protocole EIGRP tels que l'ID du routeur, le routage de dérivation (stub) et les modifications de contiguïté.

### Procédure

---

**Étape 1** Dans la page **EIGRP**, cliquez sur l'onglet **Advanced** (Avancé).

**Étape 2** Sous **Default Route Information** (informations sur la route par défaut), vous pouvez spécifier l'envoi et la réception des informations de route par défaut dans les mises à jour du protocole EIGRP.

- (S'affiche pour les périphériques hors grappe et les grappes en mode EtherChannel étendu) **Router ID (IP Address)** : saisissez l'ID utilisé pour identifier le routeur d'origine pour les routages externes. Si une voie de routage externe est reçue avec l'ID du routeur local, la voie de routage est rejetée. Pour éviter ce problème, spécifiez une adresse globale pour l'ID du routeur. Une valeur unique doit être configurée pour chaque routeur EIGRP.
- (S'affiche uniquement pour une grappe en mode d'interface individuel) : sélectionnez la valeur du regroupement (pool) d'**adresses IPv4** : Sélectionnez la valeur du regroupement d'adresses IPv4 appropriée. (objet d'ensemble d'adresses IPv4). Pour créer le regroupement d'adresses, consultez [Réerves d'adresses](#).
- **Accept Default Route Info** (Accepter les informations de routage par défaut) : cochez la case pour configurer le protocole EIGRP pour qu'il accepte les informations de routage par défaut de l'extérieur.
  - **Access List** (liste d'accès) : dans la liste déroulante **Access List** (liste d'accès), spécifiez une liste d'accès standard qui définit les réseaux autorisés et les réseaux qui ne le sont pas lors de la réception

des informations de routage par défaut. Pour ajouter un nouvel objet à la liste d'accès standard, cliquez sur **Ajouter** (+) et consultez [Configurer les objets ACL standard](#) pour connaître la procédure détaillée.

- **Send Default Route Info** (envoyer les informations de routage par défaut) : cochez la case pour configurer le protocole EIGRP afin d'annoncer les informations de routage par défaut externes.
  - **Access List**(liste d'accès) : dans la liste déroulante **Access List** (liste d'accès), spécifiez une liste d'accès standard qui définit les réseaux autorisés et les réseaux qui ne le sont pas lors de l'envoi d'informations de routage par défaut. Pour ajouter un nouvel objet à la liste d'accès standard, cliquez sur **Ajouter** (+) et consultez [Configurer les objets ACL standard](#) pour connaître la procédure détaillée.

**Étape 3** Sous **administrative Distance** (Distance administrative), spécifiez :

- **Internal Distance** (Distance interne) : distance administrative pour les routages internes par EIGRP. Les routes internes sont celles qui sont apprises d'une autre entité du même système autonome. Les valeurs valides sont comprises entre 0 et 255. La valeur par défaut est 90.
- **External Distance** (Distance externe) : distance administrative pour les routages externes EIGRP. Les routes externes sont celles pour lesquelles le meilleur chemin est appris d'un voisin externe au système autonome. Les valeurs valides sont comprises entre 0 et 255. La valeur par défaut est 170.

**Étape 4** Sous **contiguïté Changes** (Changements de contiguïté), spécifiez :

- **Log Neighbor Changes** : cochez la case pour activer la journalisation des modifications de contiguïté du protocole EIGRP.
- **Log Neighbor Warnings** : cochez la case pour activer la journalisation des messages d'avertissement de voisins EIGRP.
- (Facultatif) Saisissez l'intervalle de temps (en secondes) entre les messages d'avertissement de voisin répété. Cette valeur peut être comprise entre 1 et 65 535. Les avertissements répétés ne sont pas journalisés s'ils se produisent pendant cet intervalle.

**Étape 5** Sous **Stub**, pour activer le périphérique en tant que processus de routage de dérivation EIGRP, cochez une ou plusieurs des cases de processus de routage de dérivation EIGRP suivantes :

- **Receive only** : configure le processus de routage du protocole EIGRP pour recevoir les informations de routage des routeurs voisins, mais n'envoie pas d'informations de routage aux routeurs voisins. Si cette option est sélectionnée, vous ne pouvez pas sélectionner les autres options de routage stub.
- **Connecté** : annonce les routages connectés.
- **Redistribué** : annonce les routages redistribués.
- **Statique** : annonce les routages statiques.
- **Résumé** : annonce les récapitulatifs des routages.

**Étape 6** Sous **Default Metrics**(métriques par défaut), définissez les métriques par défaut pour les routes redistribuées au processus de routage par protocole EIGRP :

- **Bande passante** : la bande passante minimale du routage en kilobits par seconde. Les valeurs valides sont comprises entre 0 et 4294967294.
  - **Retard** : le retard de routage en dizaines de microsecondes. Les valeurs valides vont de 0 à 4294967295.
  - **Fiabilité** : la probabilité de transmission réussie des paquets, exprimée par un nombre de 0 à 255. La valeur 255 indique une fiabilité de 100 %; 0 signifie l'absence de fiabilité.
  - **Chargement** : la bande passante effective de la route. Les valeurs valides vont de 1 à 255; La valeur 255 indique un chargement à 100 %.
  - **MTU** : la plus petite valeur autorisée pour l'unité de transmission maximale du chemin. Cette valeur peut être comprise entre 1 et 65 535.
-



## À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d'incohérence, la version anglaise du présent contenu prévaudra.