IS-IS

Ce chapitre décrit le protocole de routage IS-IS (Intermediate System to Intermediate System).

À propos d'IS-IS

Le protocole de routage IS-IS est un protocole IGP (Interior Gateway Protocol) à état de liaison. Les protocoles à état de liaison se caractérisent par la propagation des renseignements nécessaires pour créer une carte complète de la connectivité du réseau sur chaque périphérique participant. Cette carte est ensuite utilisée pour calculer le chemin le plus court vers les destinations. La mise en œuvre d'IS-IS prend en charge IPv4 et IPv6.

Vous pouvez diviser un domaine de routage en un ou plusieurs sous-domaines. Chaque sous-domaine est appelé une zone et se voit attribuer une adresse de zone. Le routage dans une zone est appelé routage de niveau 1. Le routage entre les zones de niveau 1 est appelé routage de niveau 2. Un routeur est appelé système intermédiaire (IS). Un IS peut fonctionner au niveau 1, au niveau 2 ou aux deux. Les IS qui fonctionnent au niveau 1 échangent des renseignements de routage avec d'autres IS de niveau 1 dans la même zone. Les IS qui fonctionnent au niveau 2 échangent des renseignements de routage avec d'autres routeurs de niveau 2, qu'ils se trouvent ou non dans la même zone de niveau 1. L'ensemble de routeurs de niveau 2 et les liaisons qui les relient forment le sous-domaine de niveau 2, qui ne doit pas être partitionné pour que le routage fonctionne correctement.

À propos de NET

Un IS est identifié par une adresse appelée Network Entity Title (NET). Le NET est l'adresse d'un point d'accès de service de réseau (NSAP), qui identifie une instance du protocole de routage IS-IS exécuté sur un IS. Le NET comporte de 8 à 20 octets et comprend les trois parties suivantes :

- Adresse de zone : ce champ a une longueur de 1 à 13 octets et est composé des octets de poids fort de l'adresse.

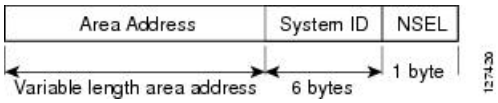
Remarque Vous pouvez attribuer plusieurs adresses de zone à une instance IS-IS; dans ce cas, toutes les adresses de zone sont considérées comme synonymes. Plusieurs adresses de zone synonymes sont utiles lors de la fusion ou de la division de zones dans le domaine. Une fois la fusion ou la division terminée, vous n'avez pas besoin d'attribuer plusieurs adresses de zone à une instance IS-IS.

- ID de système : ce champ a une longueur de 6 octets et suit immédiatement l'adresse de zone. Lorsque l'IS fonctionne au niveau 1, l'ID système doit être unique pour les périphériques de niveau 1 dans la même zone. Lorsque l'IS fonctionne au niveau 2, l'ID système doit être unique parmi tous les périphériques du domaine.

Remarque Vous attribuez un ID système à une instance IS.

- NSEL : le champ du sélecteur N a une longueur de 1 octet et suit immédiatement l'ID système. Il doit être défini sur 00.

Illustration 1 : Format NET



Nom de domaine dynamique IS-IS

Dans le domaine de routage IS-IS, l'ID système est utilisé pour représenter chaque ASA. L'ID système fait partie du NET configuré pour chaque ASA IS-IS. Par exemple, un ASA avec un NET configuré de 49.0001.0023.0003.000a.00 a un ID système de 0023.0003.000a. Le mappage du nom de l'ASA à l'ID système est difficile à mémoriser pour les administrateurs réseau lors de la maintenance et de la résolution des problèmes des ASA.

La saisie de la commande **show isis hostname** affiche les entrées du tableau de mappage de l'ID système au nom de l'ASA.

Le mécanisme de nom d'hôte dynamique utilise le protocole LSP (Link State Protocol) pour distribuer les renseignements de mappage du nom de l'ASA à l'D système sur l'ensemble du réseau. Chaque ASA du réseau tentera d'installer les renseignements de mappage de l'ID système au nom de l'ASA dans sa table de routage.

Si un ASA qui a annoncé le type de nom dynamique, la longueur et la valeur (TLV) sur le réseau cesse soudainement l'annonce, les derniers renseignements de mappage reçus resteront dans le tableau de mappage de l'hôte dynamique pendant une heure maximum, ce qui permettra à l'administrateur réseau d'afficher les entrées du tableau de mappage à un moment où le réseau rencontre des problèmes.

Types de PDU IS-IS

Les IS échangent des renseignements de routage avec leurs homologues à l'aide d'unités de données de protocole (PDU). Les types de PDU Hello Intermediate System-to-Intermediate System (IIH), de PDU d'état de liaison (LSP) et de PDU de numéro de séquence (SNP) sont utilisés.

IIH

Les IIH sont échangés entre les voisins IS sur les circuits sur lesquels le protocole IS-IS est activé. Les IIH comprennent l'ID système de l'expéditeur, la ou les adresses de zone attribuées et l'identité des voisins sur ce circuit connus de l'IS expéditeur. Des renseignements facultatifs supplémentaires peuvent également être inclus.

Il existe deux types d'IIH :

- IIH LAN de niveau 1 : ceux-ci sont envoyés sur les circuits multiaccès lorsque l'IS d'envoi fonctionne comme un appareil de niveau 1 sur ce circuit.
- IIH LAN de niveau 2 : ceux-ci sont envoyés sur les circuits multiaccès lorsque l'IS d'envoi fonctionne comme un appareil de niveau 2 sur ce circuit.

LSP

Un IS génère des LSP pour annoncer ses voisins et les destinations qui sont directement connectées à cet IS. Un LSP est identifié de façon unique par les éléments suivants :

- ID de système du IS qui a généré le LSP
- ID de pseudo-nœud : cette valeur est toujours égale à 0, sauf lorsque le LSP est un LSP de pseudo-nœud.
- Numéro LSP (0 à 255)
- Numéro de séquence de 32 bits

Chaque fois qu'une nouvelle version d'un LSP est générée, le numéro de séquence est incrémenté.

Les LSP de niveau 1 sont générés par les IS qui prennent en charge le niveau 1. Les LSP de niveau 1 sont inondés dans toute la zone de niveau 1. L'ensemble de LSP de niveau 1 généré par tous les IS de niveau 1 d'une zone constitue la base de données LSP de niveau 1 (LSPDB). Tous les IS de niveau 1 d'une zone ont une LSPDB de niveau 1 identique et, par conséquent, une carte de connectivité réseau identique pour la zone.

Les LSP de niveau 2 sont générés par les IS qui prennent en charge le niveau 2. Les LSP de niveau 2 sont inondés dans tout le sous-domaine de niveau 2. L'ensemble de LSP de niveau 2 généré par tous les IS de niveau 2 du domaine constitue la base de données LSP de niveau 2 (LSPDB). Tous les IS de niveau 2 ont une LSPDB de niveau 2 identique et, par conséquent, une carte de connectivité identique pour le sous-domaine de niveau 2.

SNP

Les SNP contiennent une description sommaire d'un ou de plusieurs LSP. Il existe deux types de SNP pour les niveaux 1 et 2 :

- Les PDU à numéro de séquence complet (CSNP) sont utilisées pour envoyer un résumé de la base de données LSPDB dont dispose un IS pour un niveau donné.
- Les PDU à numéro de séquence partiel (PSNP) sont utilisées pour envoyer un résumé d'un sous-ensemble des LSP pour un niveau donné qu'un IS possède dans sa base de données ou doit obtenir.

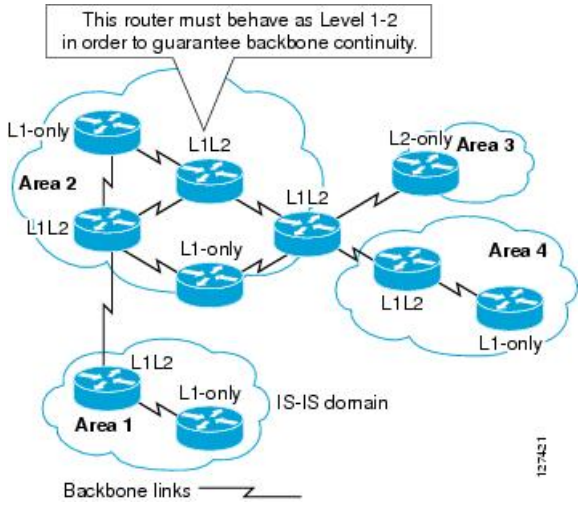
Fonctionnement d'IS-IS sur les circuits multiaccès

Les circuits multiaccès prennent en charge plusieurs IS, c'est-à-dire deux ou plus fonctionnant sur le circuit. Pour les circuits multiaccès, une condition préalable nécessaire est la capacité d'adresser plusieurs systèmes à l'aide d'une adresse de multidiffusion ou de diffusion. Un IS qui prend en charge le niveau 1 sur un circuit multiaccès envoie des IIH de niveau 1 LAN sur le circuit. Un IS qui prend en charge le niveau 2 sur un circuit multiaccès envoie des IIH LAN de niveau 2 sur le circuit. Les IS forment des contiguïtés distinctes pour chaque niveau avec les IS voisins sur le circuit.

Un IS forme une contiguïté de niveau 1 avec d'autres IS qui prennent en charge le niveau 1 sur le circuit et qui ont une adresse de zone correspondante. Deux ISE avec des ensembles dissociés d'adresses de zone prenant en charge le niveau 1 sur le même circuit multiaccès ne sont PAS pris en charge. Un IS forme une contiguïté de niveau 2 avec d'autres IS qui prennent en charge le niveau 2 sur le circuit.

Les périphériques de la topologie du réseau IS-IS dans la figure suivante effectuent le routage de niveau 1, de niveau 2 ou de niveau 1 et 2 le long du réseau fédérateur.

Illustration 2 : Périphériques de niveau 1, de niveau 2 et de niveau 1-2 dans une topologie de réseau IS-IS



Choix de l'IS désigné IS-IS

Si chaque IS annonce toutes ses contiguïtés sur un circuit de multiaccès dans ses LSP, le nombre total d'annonces requis serait de N 2 (où N est le nombre d'ISE qui fonctionnent à un niveau donné sur le circuit). Pour résoudre ce problème d'évolutivité, IS-IS définit un pseudo-nœud pour représenter le circuit de multiaccès. Tous les IS qui fonctionnent sur le circuit à un niveau donné choisissent un des IS pour qu'il agisse en tant que système intermédiaire désigné (DIS) sur ce circuit. Un DIS est choisi pour chaque niveau actif sur le circuit.

Le DIS est responsable de l'émission de LSP de pseudo-nœuds. Les LSP de pseudo-nœuds comprennent des annonces de voisins pour tous les IS qui fonctionnent sur ce circuit. Tous les IS qui fonctionnent sur le circuit (y compris le DIS) fournissent une annonce de voisin au pseudo-nœud dans leurs LSP non pseudo-nœuds et n'annoncent aucun de leurs voisins sur le circuit de multiaccès. De cette façon, le nombre total d'annonces requises varie en fonction du N, le nombre d'ISE qui fonctionnent sur le circuit.

Un LSP de pseudo-nœud est classifié de manière unique par les identifiants suivants :

- ID de système du DIS qui a généré le LSP

- Identifiant de pseudo-nœud (TOUJOURS NON ZÉRO)
- Numéro LSP (0 à 255)
- Numéro de séquence de 32 bits

L'ID de pseudo-nœud non zéro est ce qui différencie un LSP de pseudo-nœud d'un LSP non pseudo-nœud. Il est choisi par le DIS pour être unique parmi tous les autres circuits LAN pour lesquels il est également le DIS à ce niveau.

Le DIS est également responsable de l'envoi des CSNP périodiques sur le circuit. Cela fournit une description complète du contenu actuel de la LSPDB sur le DIS. D'autres IS sur le circuit peuvent alors effectuer les activités suivantes, ce qui synchronise de manière efficace et fiable les LSPDB de tous les IS sur un circuit multiaccès :

- Inonder les LSP qui sont absents de ou sont plus récents que ceux décrits dans les CSNP envoyés par le DIS.
- Demander un LSP en envoyant un PSNP pour les LSP décrits dans les CSNP envoyés par le DIS qui sont absents de la base de données locale ou plus anciens que ce qui est décrit dans l'ensemble CSNP.

Synchronisation LSPDB IS-IS

Le bon fonctionnement d'IS-IS nécessite un processus fiable et efficace pour synchroniser les LSPDB sur chaque IS. Dans IS-IS, ce processus s'appelle le processus de mise à jour. Le processus de mise à jour fonctionne indépendamment à chaque niveau pris en charge. Les LSP générés localement sont toujours de nouveaux LSP. Les LSP reçus d'un voisin sur un circuit peuvent être générés par un autre IS ou être une copie d'un LSP généré par l'IS local. Les LSP reçus peuvent être plus anciens, identiques ou plus récents que le contenu actuel de la LSPDB locale.

Traitement des nouveaux LSP

Lorsqu'un nouveau LSP est ajouté à la LSPDB locale, il remplace une ancienne copie du même LSP dans la LSPDB. Le nouveau LSP est marqué pour être envoyé sur tous les circuits sur lesquels l'IS a actuellement une contiguïté dans l'état UP au niveau associé au nouveau LSP, à l'exception du circuit sur lequel le nouveau LSP a été reçu.

Pour les circuits multiaccès, l'IS inonde une fois le nouveau LSP. L'IS examine l'ensemble des CNSP qui sont envoyés périodiquement par le DIS pour le circuit multiaccès. Si la LSPDB locale contient un ou plusieurs LSP plus récents que ceux décrits dans l'ensemble CSNP (y compris les LSP qui ne figurent pas dans l'ensemble CSNP), ces LSP sont rechargés sur le circuit multiaccès. Si la LSPDB locale contient un ou plusieurs LSP plus anciens que ceux décrits dans l'ensemble CSNP (y compris les LSP décrits dans l'ensemble CSNP qui sont absents de la LSPDB locale), un PSNP est envoyé sur le circuit multiaccès avec les descriptions des LSP qui nécessitent une mise à jour. Le DIS pour le circuit multiaccès répond en envoyant les LSP demandés.

Gestion des anciens LSP

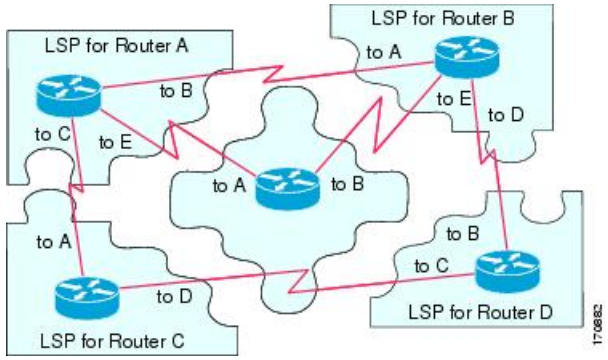
Un IS peut recevoir un LSP plus ancien que la copie dans la LSPDB locale. Un IS peut recevoir un SNP (complet ou partiel) qui décrit un LSP plus ancien que la copie dans la LSPDB locale. Dans les deux cas, l'IS marque le LSP dans la base de données locale à inonder sur le circuit sur lequel le LSP plus ancien ou le SNP contenant le LSP plus ancien a été reçu. Les actions entreprises sont les mêmes que celles décrites ci-dessus après l'ajout d'un nouveau LSP à la base de données locale.

Gestion des LSP du même âge

En raison de la nature distribuée du processus de mise à jour, il est possible qu'un IS reçoive des copies d'un LSP qui sont identiques au contenu actuel de la LSPDB locale. Dans les circuits multiaccès, la réception d'un LSP du même âge est ignorée. La transmission périodique d'un CSNP défini par le DIS pour ce circuit sert de confirmation implicite à l'expéditeur que le LSP a été reçu.

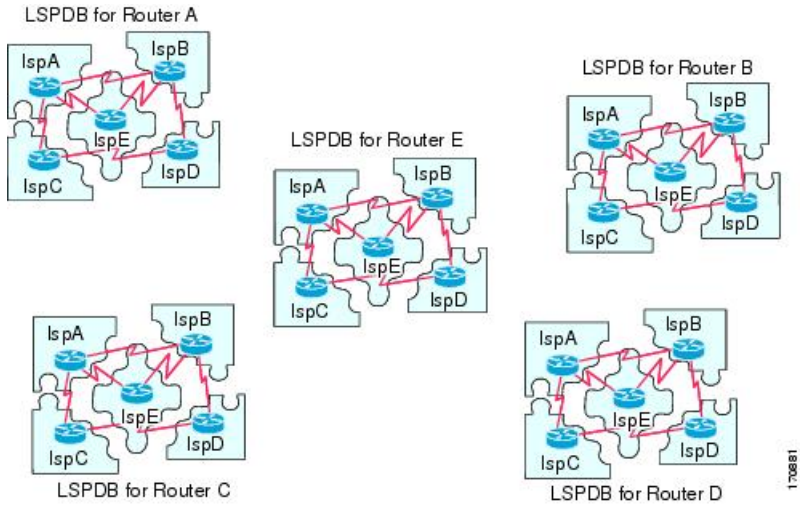
La figure suivante montre comment les LSP sont utilisés pour créer une carte du réseau. Considérez la topologie du réseau comme un casse-tête. Chaque LSP (représentant un IS) est l'une des pièces. Elle s'applique à tous les appareils de niveau 1 dans une zone ou à tous les appareils de niveau 2 dans un sous-domaine de niveau 2.

Illustration 3 : Carte du réseau IS-IS



La figure suivante montre chaque appareil du réseau IS-IS avec sa base de données d'état des liaisons entièrement mise à jour après la formation des contiguïtés entre les appareils voisins. Elle s'applique à tous les appareils de niveau 1 dans une zone ou à tous les appareils de niveau 2 dans un sous-domaine de niveau 2.

Illustration 4 : Périphériques IS-IS avec LSPDB synchronisées



Calcul du chemin le plus court IS-IS

Lorsque le contenu de la LSPDB change, chaque IS exécute indépendamment un calcul du chemin le plus court. L'algorithme est basé sur l'algorithme bien connu de Dijkstra pour trouver les chemins les plus courts le long d'un graphique orienté où les IS sont les sommets du graphe et les liaisons entre les IS sont des arêtes avec un poids non négatif. Une vérification de la connectivité bidirectionnelle est effectuée avant de prendre

en compte une liaison entre deux IS dans le graphique. Cela empêche l'utilisation de renseignements obsolètes dans la LSPDB, par exemple, lorsqu'un IS n'est plus opérationnel dans le réseau, mais n'a pas purgé l'ensemble de LSP qu'il a généré avant d'arrêter son fonctionnement.

La sortie du SPF est un ensemble de tuples (destination, prochain saut). Les destinations sont propres au protocole. Plusieurs chemins à coût égal sont pris en charge, auquel cas plusieurs sauts suivants seront associés à la même destination.

Des SPF indépendants sont effectués pour chaque niveau pris en charge par l'IS. Lorsque la même destination est accessible par les chemins de niveau 1 et 2, le chemin de niveau 1 est privilégié.

Un IS de niveau 2 qui indique qu'il a un ou plusieurs voisins de niveau 2 dans d'autres zones peut être utilisé par des périphériques de niveau 1 dans la même zone que le chemin de dernier recours, également appelé route par défaut. L'IS de niveau 2 indique sa liaison à d'autres zones en définissant un bit de connexion (ATT) dans son LSP de niveau 1 sur 0.

Remarque Un IS peut générer jusqu'à 256 LSP à chaque niveau. Les LSP sont identifiés par les numéros de 0 à 255. Le LSP 0 a des propriétés spéciales, notamment l'importance du réglage du bit ATT pour indiquer l'annexion à d'autres zones. Lorsque les LSP numérotés de 1 à 255 ont le bit ATT activé, ce n'est pas important.

Protocole d'arrêt IS-IS

Vous pouvez fermer IS-IS (le mettre dans un état administratif arrêté) pour apporter des modifications à la configuration du protocole IS-IS sans perdre vos paramètres de configuration. Vous pouvez fermer IS-IS au niveau du processus IS-IS global ou au niveau de l'interface. Si le périphérique a été redémarré lorsque le protocole a été désactivé, celui-ci devrait redémarrer dans un état désactivé. Lorsque le protocole est défini sur l'état administratif désactivé, les administrateurs réseau sont autorisés à désactiver administrativement le fonctionnement du protocole IS-IS sans perdre la configuration du protocole, à apporter une série de modifications à la configuration du protocole sans que le fonctionnement du protocole ne passe par des états intermédiaires, voire indésirables, puis à réactiver le protocole au moment opportun.

Conditions préalables d'IS-IS

Les conditions préalables suivantes sont nécessaires avant de configurer IS-IS :

- Connaissance des protocoles IPv4 et IPv6.
- Vous devez connaître la conception de votre réseau et la façon dont vous souhaitez que le trafic y passe avant de configurer IS-IS.
- Définissez les zones, préparez un plan d'adressage pour les périphériques (y compris la définition des réseaux) et déterminez les interfaces qui exécuteront IS-IS.
- Avant de configurer vos périphériques, préparez une matrice de contiguïtés qui indique les voisins attendus dans le tableau de contiguïté. Cela facilitera la vérification.

Lignes directrices relatives à IS-IS

Directives sur le mode pare-feu

Pris en charge uniquement en mode pare-feu routé. Le mode pare-feu transparent n'est pas pris en charge.

Lignes directrices relatives à la grappe

Pris en charge uniquement en mode d'interface individuelle; le mode EtherChannel étendu n'est pas pris en charge.

Directives supplémentaires

IS-IS n'est pas pris en charge avec le transfert bidirectionnel.

Configurer IS-IS

Cette section décrit comment activer et configurer le processus IS-IS sur votre système.

Procédure

Étape 1 Activer le routage IS-IS globalement, à la page 8.
Étape 2 Activer l'authentification IS-IS, à la page 12.
Étape 3 Configurer LSP IS-IS, à la page 16
Étape 4 Configurer les adresses de résumé IS-IS, à la page 20.
Étape 5 Configurer les interfaces passives IS-IS, à la page 21.
Étape 6 Configurer les interfaces IS-IS, à la page 22.
Étape 7 Configurer le remplissage d'interfaces Hello IS-IS, à la page 27
Étape 8 Configurer la famille d'adresses IPv4 IS-IS, à la page 29.
Étape 9 Configurer la famille d'adresses IPv6 IS-IS, à la page 34.

Activer le routage IS-IS globalement

La configuration IS-IS est effectuée en deux parties. Tout d'abord, vous configurez le processus IS-IS en mode de configuration globale, puis spécifiez le NET et le niveau de routage pour IS-IS en mode de configuration du routeur. D'autres paramètres généraux que vous pouvez configurer en mode de configuration du routeur peuvent avoir plus de sens pour votre réseau que de les configurer par interface. Cette section contient ces commandes.

Ensuite, vous activez le protocole IS-IS sur des interfaces individuelles en mode de configuration d'interface afin que l'interface participe au routage dynamique et forme des contiguïtés avec les appareils voisins. Vous devez activer le routage sur au moins une interface avant que des contiguïtés puissent être établies et que le

routage dynamique soit possible. Consultez Configurer les interfaces IS-IS, à la page 22 pour connaître les procédures de configuration IS-IS sur les interfaces.

Cette procédure décrit comment activer IS-IS en tant que protocole de routage IP sur l'ASA et d'autres options générales en mode de configuration du routeur.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, entrez la commande **changeto context** *name*.

Procédure

Étape 1 Activez IS-IS comme protocole de routage sur l'ASA :

router isis

Exemple :

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

Étape 2 Spécifiez le NET pour le processus de routage :

net *network-entity-title*

Exemple :

```
ciscoasa(config-router)# net 49.1234.aaaa.bbbb.cccc.00
```

Le NET identifie le périphérique pour IS-IS. Consultez À propos de NET, à la page 1 pour de plus amples renseignements sur le NET.

Étape 3 (Facultatif) Attribuez le niveau de routage pour le processus de routage IS-IS :

is-type [level-1 | level-2-only | level-1-2]

Exemple :

```
ciscoasa(config-router)# is-type level-1
```

- (Facultatif) **level-1** : indique le routage intra-zone. L'ASA apprend uniquement les destinations à l'intérieur de sa zone.
- (Facultatif) **level-2-only** : indique le routage inter-zone. L'ASA fait partie du réseau fédérateur et ne communique pas avec les routeurs de niveau 1 dans sa propre zone.
- (Facultatif) **level-1-2** : l'ASA effectue le routage de niveau 1 et de niveau 2. Ce routeur exécute deux instances du processus de routage. Il possède une LSDB pour les destinations à l'intérieur de la zone (routage de niveau 1) et exécute un calcul SPF pour découvrir la topologie de la zone. Il a également une autre LSDB avec les LSP de tous les autres routeurs du réseau fédérateur (niveau 2), et exécute un autre calcul SPF pour découvrir la topologie du réseau fédérateur et l'existence de toutes les autres zones.

Dans les configurations IS-IS traditionnelles, l'ASA agit à la fois comme un routeur de niveau 1 (intra-zone) et de niveau 2 (inter-zone). Dans les configurations IS-IS multizones, la première instance du processus de routage IS-IS configuré est par défaut un routeur de niveau 1-2 (intra-zone et inter-zone). Les autres instances du processus IS-IS configurées par défaut sont des routeurs de niveau 1.

Remarque
Nous vous conseillons fortement de configurer le type de processus de routage IS-IS.

Étape 4 Activez la fonctionnalité de nom d'hôte dynamique IS-IS sur l'ASA :

hostname dynamic

Cette commande est activée par défaut. Consultez Nom de domaine dynamique IS-IS, à la page 2 pour obtenir des renseignements détaillés sur le nom d'hôte dynamique dans IS-IS.

Étape 5 Configurez le remplissage des messages Hello pour toutes les interfaces de l'ASA :

hello padding multi-point

Cette commande est activée par défaut. Elle configure les messages Hello IS-IS à la taille MTU complète. Cela permet une détection précoce des erreurs résultant de problèmes de transmission avec de grandes trames ou d'erreurs résultant de MTU non concordantes sur des interfaces adjacentes.

Vous pouvez désactiver le remplissage Hello (**no hello padding multi-point** pour toutes les interfaces sur un routeur pour le processus de routage IS-IS) pour éviter de gaspiller la bande passante du réseau dans le cas où la MTU des deux interfaces est identique ou en cas de pontage translationnel. Lorsque le remplissage Hello est désactivé, l'ASA envoie toujours les cinq premiers Hellos IS-IS remplis à la taille MTU complète afin de conserver les avantages de la détection des incompatibilités MTU.

Saisissez la commande **show clns interface** en mode d'exécution privilégié pour indiquer que le remplissage des messages Hello a été désactivé au niveau du routeur. Consultez Supervision IS-IS, à la page 39 pour en savoir plus.

Étape 6 (Facultatif) Activez l'ASA pour générer un message de journal lorsqu'une contiguïté NLSP IS-IS change d'état (actif ou inactif) :

log-adjacency-changes [all]

Cette commande est désactivée par défaut. La journalisation des modifications de contiguïté est utile lors de la surveillance de grands réseaux. Les messages sont sous la forme suivante :

Exemple :

```
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

all : (Facultatif) Comprend les modifications générées par les événements non_IIH.

Étape 7 (Facultatif) Désactivez le protocole IS-IS afin qu'il ne puisse former aucune contiguïté sur aucune interface et effacez la base de données LSP :

protocol shutdown

Cette commande vous permet de désactiver le protocole IS-IS pour une instance de routage donnée, sans supprimer les paramètres de configuration IS-IS existants. Lorsque vous saisissez cette commande, le protocole IS-IS continue de s'exécuter sur le routeur et vous pouvez utiliser la configuration IS-IS actuelle, mais IS-IS ne forme aucune contiguïté sur aucune interface et efface également la base de données LSP IS-IS. Pour

désactiver IS-IS pour une interface en particulier, utilisez la commande **isis protocol shutdown**. Reportez-vous à Configurer les interfaces IS-IS, à la page 22 pour connaître la procédure.

Étape 8 (Facultatif) Attribuez une priorité élevée à un préfixe IP IS-IS :

route priority high tag *tag-value*

Exemple :

```
ciscoasa(config-router)# route priority high tag 100
```

tag *tag-value* : affecte une priorité élevée à l'adresse IP IS-IS préfixée avec une balise de route spécifique. La plage va de 1 à 4294967295.

Utilisez cette commande pour baliser les préfixes IP IS-IS de priorité plus élevée pour un traitement et une installation plus rapides dans la table de routage globale, ce qui entraîne une convergence plus rapide. Par exemple, vous pouvez aider les adresses de passerelle VoIP à être traitées en premier pour que le trafic VoIP soit mis à jour plus rapidement que d'autres types de paquets.

Étape 9 (Facultatif) Modifiez globalement la valeur de la mesure pour toutes les interfaces IS-IS :

metric *default-value* **[level-1 | level-2]**

Exemple :

```
ciscoasa(config-router)# metric 55 level-1
```

- *default-value* : la valeur de la mesure à attribuer au lien et à utiliser pour calculer le coût du chemin par les liaisons vers les destinations. La plage est de 1 à 63. La valeur par défaut est 10.
- (Facultatif) **level-1** : définit la mesure IPv4 ou IPv6 de niveau 1.
- (Facultatif) **level-2** : définit la mesure IPv4 ou IPv6 de niveau 2.

Nous vous conseillons d'utiliser la commande **metric** lorsque vous devez modifier la mesure par défaut pour toutes les interfaces IS-IS. Ceci évite les erreurs d'utilisateur, par exemple en supprimant involontairement une mesure définie d'une interface sans configurer de nouvelle valeur et en permettant à l'interface de revenir à la mesure par défaut de 10, devenant ainsi une interface privilégiée dans le réseau.

Étape 10 (Facultatif) Configurez l'ASA pour générer et accepter uniquement les nouveaux objets de longueur et de valeur (TLV) de nouveau type :

metric-style narrow | transition | wide [level-1 | level-2 | level-1-2]

Exemple :

```
ciscoasa(config-router)# metric-style wide level-1
```

- **narrow** : utilise l'ancien type de TLV avec des mesures limitées.
- **transition** : demande à l'ASA d'accepter les anciens et les nouveaux types de TLV.
- **wide** : utilise le nouveau type de TLV pour transporter des mesures plus larges.
- (Facultatif) **level-1** : active cette commande sur le niveau de routage 1.
- (Facultatif) **level-2** : active cette commande sur le niveau de routage 2.

- (Facultatif) **level-1-2** : active cette commande sur les niveaux de routage 1 et 2.

Cette commande permet à l'ASA de générer et d'accepter uniquement de nouveaux TLV, ce qui fait que l'ASA utilise moins de mémoire et d'autres ressources que s'il génère à la fois des TLV d'ancien et de nouveau type.

Étape 11 (Facultatif) Configurez la priorité des ASA désignés sur toutes les interfaces :

priority *number-value*

Exemple :

```
ciscoasa(config-router)# priority 80
```

number-value : la priorité de l'ASA. La valeur doit être comprise entre 0 et 127. La valeur par défaut est 64.

Étape 12 (Facultatif) Configurez les adresses manuelles supplémentaires pour une zone IS-IS :

max-area-addresses *number*

Exemple :

```
ciscoasa(config-router)# max-area-addresses 3
```

number : le nombre d'adresses manuelles à ajouter. La plage se situe entre 3 et 254. Il n'y a pas de valeur par défaut.

Cette commande vous permet de maximiser la taille d'une zone IS-IS en configurant des adresses manuelles supplémentaires. Vous spécifiez le nombre d'adresses que vous souhaitez ajouter et attribuez une adresse NET pour créer chaque adresse manuelle. Consultez À propos de NET, à la page 1 pour obtenir des renseignements sur le NET.

Étape 13 Configurez le partage de charge à chemins multiples pour IS-IS :

maximum-paths *number-of-paths*

Exemple :

```
ciscoasa(config-router)# maximum-paths 8
```

number-of-paths : le nombre de routes à installer dans la table de routage. La plage va de 1 à 8. La valeur par défaut est 1.

La commande **maximum-path** est utilisée pour configurer le partage de charges multiples IS-IS lorsque ECMP est configuré dans l'ASA.

Activer l'authentification IS-IS

L'authentification du routage IS-IS empêche l'introduction de messages de routage non autorisés ou faux provenant de sources non approuvées. Vous pouvez définir un mot de passe pour chaque zone ou domaine IS-IS afin d'éviter que des routeurs non autorisés injectent de faux renseignements de routage dans la base de données sur l'état des liens, ou vous pouvez configurer un type d'authentification IS-IS, soit IS-IS MD5, soit une authentification en texte clair améliorée. Vous pouvez également définir l'authentification par interface.

Tous les voisins IS-IS sur les interfaces configurées pour l'authentification des messages IS-IS doivent être configurés avec le même mode d'authentification et la même clé pour que les contiguïtés soient établies.

Consultez À propos d'IS-IS, à la page 1 pour en savoir plus sur les zones et les domaines.

Avant de commencer

Avant de pouvoir activer l'authentification du routage IS-IS, vous devez activer IS-IS et configurer une zone. Reportez-vous à Activer le routage IS-IS globalement, à la page 8 pour connaître la procédure.

Procédure

Étape 1 Entrez en mode de configuration du routeur IS-IS et configurez un mot de passe d'authentification de zone IS-IS :

area-password *password* [**authenticate snp {validate | send-only}**]

Exemple :

```
ciscoasa(config)# router isis
ciscoasa(config-router)# area-password track authenticate snp validate
```

- *password* : le mot de passe que vous attribuez.
- (Facultatif) **authenticate snp** : le système insère le mot de passe dans les SNP.
- **validate** : demande au système d'insérer le mot de passe dans les SNP et de vérifier le mot de passe dans les SNP qu'il reçoit.
- **send-only** : demande au système d'insérer uniquement le mot de passe dans les SNP, mais de ne pas vérifier le mot de passe dans les SNP qu'il reçoit. Utilisez ce mot clé lors d'une mise à niveau logicielle pour faciliter la transition.

L'utilisation de cette commande sur tous les ASA d'une zone empêche les routeurs non autorisés d'injecter de faux renseignements de routage dans la base de données sur l'état des liens. Cependant, ce mot de passe est échangé en texte brut et n'offre donc qu'une sécurité limitée.

Le mot de passe est inséré dans les LSP, CSNP et PSNP de niveau 1 (niveau du routeur de station). Si vous ne spécifiez pas le mot clé **authenticate snp** avec le mot clé **validate** ou **send-only**, le protocole IS-IS n'insère pas le mot de passe dans les SNP.

Étape 2 Entrez en mode de configuration du routeur IS-IS et configurez un mot de passe d'authentification de domaine IS-IS :

domain-password *password* [**authenticate snp {validate | send-only}**]

Exemple :

```
ciscoasa(config-router)# domain-password users2j45 authenticate snp validate
```

- *password* : le mot de passe que vous attribuez.
- (Facultatif) **authenticate snp** : permet au système d'insérer le mot de passe dans les unités PDU de numéro de séquence (SNP).

- **validate** : demande au système d'insérer le mot de passe dans les SNP et de vérifier le mot de passe dans les SNP qu'il reçoit.
- **send-only** : demande au système d'insérer uniquement le mot de passe dans les SNP, mais de ne pas vérifier le mot de passe dans les SNP qu'il reçoit. Utilisez ce mot clé lors d'une mise à niveau logicielle pour faciliter la transition.

Ce mot de passe est échangé en texte brut et n'offre donc qu'une sécurité limitée.

Le mot de passe est inséré dans les LSP, CSNP et PSNP de niveau 2 (niveau du routeur de zone). Si vous ne spécifiez pas le mot clé **authenticate snp** avec le mot clé **validate** ou **send-only**, le protocole IS-IS n'insère pas le mot de passe dans les SNP.

Étape 3 Configurez l'instance IS-IS globalement ou par interface pour que l'authentification soit effectuée uniquement sur les paquets IS-IS envoyés (non reçus) :

Mode de routeur :**authentication send-only [level-1 | level-2]**

Exemple :

```
ciscoasa(config-router)# authentication send-only level-1
```

Mode d'interface :**isis authentication send-only [level-1 | level-2]**

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis authentication send-only level-1
```

- (Facultatif) **level-1** : l'authentification n'est effectuée que sur les paquets de niveau 1 qui sont envoyés (non reçus).
- (Facultatif) **level-2** : l'authentification n'est effectuée que sur les paquets de niveau 2 qui sont envoyés (non reçus).

Utilisez cette commande avant de configurer le mode d'authentification et la chaîne de clés d'authentification afin que la mise en œuvre de l'authentification se déroule en douceur. Si vous ne spécifiez pas le niveau 1 ou le niveau 2, l'envoi s'applique uniquement aux deux niveaux.

Remarque
Les ASA auront plus de temps pour que les clés soient configurées sur chaque ASA si l'authentification est insérée uniquement dans les paquets en cours d'envoi, et n'est pas vérifiée sur les paquets en cours de réception. Une fois que tous les ASA qui doivent communiquer ont été configurés avec cette commande, activez le mode d'authentification et la chaîne de clés sur chaque ASA.

Étape 4 Précisez le type de mode d'authentification utilisé dans les paquets IS-IS pour l'instance IS-IS, globalement ou par interface :

Mode de routeur :**authentication mode {md5 | text} [level-1 | level-2]**

Exemple :

```
ciscoasa(config-router)# authentication mode md5 level-1
```

Mode d'interface :**isis authentication mode {md5 | text} [level-1 | level-2]**

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)#  isis authentication mode md5 level-1
```

- **md5** : active l'authentification Message Digest 5.
- **text** : utilise l'authentification en texte clair.
- (Facultatif) **level-1** : active l'authentification spécifiée pour les paquets de niveau 1 uniquement.
- (Facultatif) **level-2** : active l'authentification spécifiée pour les paquets de niveau 2 uniquement.

Si vous avez configuré l'authentification en texte clair à l'aide de **area-password** ou **domain-password**, le mode d'authentification IS-IS remplace ces deux commandes. Si vous configurez **isis authentication mode** puis essayez de configurer **area-password** ou **domain-password**, vous n'êtes pas autorisé à le faire. Si vous ne spécifiez pas le niveau 1 ou le niveau 2, le mode s'applique uniquement aux deux niveaux.

Étape 5 Activez l'authentification pour IS-IS globalement ou par interface :

Mode de routeur : **authentication key [0 | 8]** *password* **[level-1 | level-2]**

Exemple :

```
ciscoasa(config-router)# authentication key 0 site1 level-1
```

Mode d'interface : **isis authentication key [0 | 8]** *password* **[level-1 | level-2]**

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# router isis
ciscoasa(config-if)# isis authentication key 0 second level-1
```

- **0** : indique qu'un mot de passe non chiffré suivra.
- **8** : indique qu'un mot de passe chiffré suivra.
- *password* : active l'authentification et spécifie la clé.
- (Facultatif) **level-1** : active l'authentification pour les paquets de niveau 1 uniquement.
- (Facultatif) **level-2** : active l'authentification pour les paquets de niveau 2 uniquement.

Si aucun mot de passe n'est configuré avec la commande **key**, aucune authentification par clé n'est effectuée. L'authentification par clé peut s'appliquer à l'authentification en texte clair ou à l'authentification MD5. Reportez-vous à l'étape 4 pour définir le mode. Une seule clé d'authentification est appliquée à IS-IS à la fois. Si vous configurez une deuxième clé, la première est remplacée. Si vous ne spécifiez pas le niveau 1 ou le niveau 2, le mot de passe s'applique uniquement aux deux niveaux.

Étape 6 Configurez le mot de passe d'uthentification pour une interface :

isis password *password* **[level-1 | level-2]**

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
```

```
ciscoasa(config-if)# isis password analyst level-1
```

- *password* : mot de passe d'authentification que vous attribuez à une interface.
- (Facultatif) **level-1** : configure le mot de passe d'authentification pour le niveau 1 de manière indépendante. Pour le routage de niveau 1, l'ASA agit en tant que routeur de station uniquement.
- (Facultatif) **level-2** : configure le mot de passe d'authentification pour le niveau 2 de manière indépendante. Pour le routage de niveau 2, l'ASA agit en tant que routeur de zone uniquement.

Cette commande vous permet d'empêcher des routeurs non autorisés de former des contiguïtés avec cet ASA et protège ainsi le réseau contre les intrusions. Le mot de passe est échangé en texte brut et offre ainsi une sécurité limitée. Vous pouvez attribuer différents mots de passe pour différents niveaux de routage en utilisant les mots clés **level-1** et **level-2**.

Exemples

L'exemple suivant montre une instance IS-IS avec l'authentification MD5 effectuée sur les paquets de niveau 1 et pour envoyer n'importe quelle clé appartenant à la chaîne de clés nommée site1 :

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0101.0101.0101.00
ciscoasa(config-router)# is-type level-1
ciscoasa(config-router)# authentication send-only level-1
ciscoasa(config-router)# authentication mode md5 level-1
ciscoasa(config-router)# authentication key 0 site1 level-1
```

Configurer LSP IS-IS

Un IS génère des LSP pour annoncer ses voisins et les destinations qui sont directement connectées à IS-IS. Consultez Types de PDU IS-IS, à la page 2 pour en savoir plus sur les LSP.

Utilisez les commandes suivantes pour configurer les LSP afin d'avoir une configuration de convergence plus rapide.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, entrez la commande **changeto context** *name*.

Procédure

Étape 1 Entrez en mode de configuration du routeur :

router isis

Exemple :

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

Étape 2 Configurez l'ASA pour ignorer les LSP IS-IS qui sont reçus avec des erreurs de somme de contrôle interne plutôt que de purger les LSP :

ignore-lsp-errors

Exemple :

```
ciscoas(config-router)# ignore-lsp-errors
```

IS-IS exige qu'un LSP avec une somme de contrôle de liaison de données incorrecte soit purgé par le récepteur, ce qui oblige l'initiateur du paquet à le régénérer. Si un réseau a une liaison qui provoque la corruption de données tout en fournissant des LSP avec des sommes de contrôle de liaison de données correctes, un cycle continu de purge et de génération d'un grand nombre de paquets peut se produire, ce qui peut rendre le réseau non fonctionnel. Utilisez cette commande pour ignorer les LSP plutôt que de les purger. La valeur par défaut est Enabled (Activé).

Étape 3 Configurez IS-IS pour annoncer uniquement les préfixes appartenant aux interfaces passives :

advertise passive-only

Cette commande exclut les préfixes IP des réseaux connectés des annonces LSP et réduit ainsi le temps de convergence IS-IS, car moins de préfixes sont annoncés dans le LSP non pseudonode du routeur.

Étape 4 Configurez les LSP IS-IS pour qu'ils soient complets :

fast-flood *lsp-number*

Exemple :

```
ciscoasa(config-router)# fast-flood 7
```

(Facultatif) *lsp-number* : le nombre de LSP à inonder avant de lancer SPF.

Cette commande envoie un nombre spécifié de LSP à partir de l'ASA. Les LSP invoquent SPF avant d'exécuter SPF. L'accélération du processus d'inondation LSP améliore le temps de convergence global. La plage est comprise entre 1 et 15. La valeur par défaut est égale à 5.

Remarque
Nous vous conseillons d'activer l'inondation rapide des LSP avant que le routeur exécute le calcul SPF.

Étape 5 Configurez la taille MTU des LSP IS-IS :

lsp-mtu *bytes*

Exemple :

```
ciscoasa(config-router)# lsp-mtu 1300
```

bytes : taille maximale des paquet en octets. Le nombre d'octets doit être inférieur ou égal à la plus petite MTU de toute liaison du réseau. La plage se situe entre 128 et 4352.

Étape 6 Définissez la durée maximum pendant laquelle les LSP persistent dans la base de données de l'ASA sans être actualisés :

max-lsp-lifetime *seconds*

Exemple :

```
ciscoasa(config-router)# max-lsp-lifetime 2400
```

seconds : la durée de vie du LSP en secondes. La plage valide est de 1 à 65535. La valeur par défaut est 1200.

Si la durée de vie est dépassée avant qu'un LSP d'actualisation arrive, ce dernier est supprimé de la base de données.

Étape 7 Personnalisez la limitation IS-IS des calculs SPF :

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

Exemple :

```
ciscoasa(config-router)#  spf-interval level-1 5 10 20
```

- (Facultatif) **level-1** : appliquer les intervalles aux zones de niveau 1 uniquement.
- (Facultatif) **level-2** : appliquer les intervalles aux zones de niveau 2 uniquement.
- *sf-max-wait* : indique l'intervalle maximal entre deux calculs SPF consécutifs. La plage est comprise entre 1 et 120 secondes. La valeur par défaut est de 10 secondes.
- (Facultatif) *sf-initial-wait* : indique le délai d'attente initial après une modification de topologie avant le premier calcul SPF. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 500 millisecondes (5,5 secondes).

  Chaque intervalle d'attente ultérieur est deux fois plus long que le précédent jusqu'à ce que l'intervalle d'attente atteigne l'intervalle d'attente SPF maximum spécifié.
- (Facultatif) *spf-second-wait* : indique l'intervalle entre le premier et le deuxième calcul SPF. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 500 millisecondes (5,5 secondes).

Les calculs SPF sont effectués uniquement lorsque la topologie change. Cette commande contrôle la fréquence à laquelle le logiciel effectue le calcul SPF.

Remarque
Le calcul SPF est exigeant pour le processeur. Par conséquent, il peut être utile de limiter la fréquence à laquelle il est effectué, en particulier lorsque la zone est vaste et que la topologie change souvent. L'augmentation de l'intervalle SPF réduit la charge du processeur de l'ASA, mais retarde potentiellement le taux de convergence.

Étape 8 Personnalisez la limitation IS-IS de la génération LSP :

lsp-gen-interval [level-1 | level-2] *lsp-max-wait [lsp-intial-wait lsp-second wait]*

Exemple :

```
ciscoasa(config-router)#  lsp-gen-interval level-1 2 50 100
```

- (Facultatif) **level-1** : appliquer les intervalles aux zones de niveau 1 uniquement.

- (Facultatif) **level-2** : appliquer les intervalles aux zones de niveau 2 uniquement.
- *lsp-max-wait* : indique l'intervalle maximum entre deux occurrences consécutives de génération d'un LSP. La plage est comprise entre 1 et 120 secondes. La valeur par défaut est de 5 secondes.
- (Facultatif) *lsp-initial-wait* : indique le délai d'attente initial avant de générer le premier LSP. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 50 millisecondes.

  Chaque intervalle d'attente ultérieur est deux fois plus long que le précédent jusqu'à ce que l'intervalle d'attente atteigne l'intervalle d'attente LSP maximum spécifié.
- (Facultatif) *lsp-second-wait* : indique l'intervalle entre la première et la deuxième génération de LSP. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 000 millisecondes (5 secondes).

  Cette commande contrôle le délai entre la génération des LSP.

Étape 9 Définissez l'intervalle d'actualisation du LSP :

lsp-refresh-interval *seconds*

Exemple :

```
ciscoasa(config-router)# lsp-refresh-interval 1080
```

(Facultatif) *seconds* : intervalle auquel les LSP sont actualisés. La plage valide est de 1 à 65 535 secondes. La valeur par défaut est 900 secondes (15 minutes).

L'intervalle d'actualisation détermine la vitesse à laquelle le logiciel transmet périodiquement dans les LSP les renseignements sur la topologie des routes qu'il génère. Il en est ainsi pour éviter que les renseignements de la base de données ne deviennent trop anciens.

Remarque
Les LSP doivent être actualisés périodiquement avant l'expiration de leur durée de vie. La valeur définie pour la commande **lsp-refresh-interval** doit être inférieure à la valeur définie pour la commande **max-lsp-lifetime**; sinon, les LSP expirent avant d'être actualisés. Si vous définissez une durée de vie des LSP trop faible par rapport à l'intervalle d'actualisation des LSP, le logiciel réduit l'intervalle d'actualisation des LSP pour empêcher les LSP d'expirer.

Étape 10 Personnalisez la limitation IS-IS des PRC :

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

Exemple :

```
ciscoasa(config-router)#  prc-interval 5 10 20
```

- *prc-max-wait* : indique l'intervalle maximum entre deux calculs PRC consécutifs. La plage est comprise entre 1 et 120 secondes. La valeur par défaut est de 5 secondes.
- (Facultatif) *prc-initial-wait* : indique le délai d'attente initial du PRC après une modification de la topologie. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 2 000 millisecondes.

  Chaque intervalle d'attente ultérieur est deux fois plus long que le précédent jusqu'à ce que l'intervalle d'attente atteigne l'intervalle d'attente PRC maximum spécifié.
- (Facultatif) *prc-second-wait* : indique l'intervalle entre le premier et le deuxième calcul PRC. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 000 millisecondes (5 secondes).

Le PRC est le processus logiciel de calcul des routes sans effectuer de calcul SPF. Cela est possible lorsque la topologie du système de routage lui-même n'a pas changé, mais qu'une modification est détectée dans les renseignements annoncés par un IS particulier ou lorsqu'il est nécessaire de tenter de réinstaller de telles routes dans la RIB.

Étape 11 Configurez les routes supprimées lorsque la PDU est pleine :

lsp-full suppress {external [interlevel] | interlevel [external] | none}

Exemple :

```
ciscoasa(config-router)# lsp-full suppress interlevel external
```

- **external** : supprime toutes les routes redistribuées sur cet ASA.
- **interlevel** : supprime toutes les routes provenant de l'autre niveau. Par exemple, si le LSP de niveau 2 est complet, les routes du niveau 1 sont supprimées.
- **none** : ne supprime aucune route.

Dans les réseaux où il n'y a aucune limite au nombre de routes redistribuées dans IS-IS (c'est-à-dire que la commande **redistribute maximum-prefix** n'est pas configurée), il est possible que le LSP soit saturé et que les routes soient supprimées. Utilisez la commande **lsp-full suppress** pour définir à l'avance quelles routes sont supprimées si le LSP est saturé.

Configurer les adresses de résumé IS-IS

Plusieurs groupes d'adresses peuvent être récapitulés pour un niveau donné. Les routes apprises d'autres protocoles de routage peuvent également être résumées. La métrique utilisée pour annoncer le résumé est la plus petite de toutes les routes spécifiques. Cela permet de réduire la taille de la table de routage.

Vous devez définir manuellement les adresses sommaires si vous souhaitez créer des adresses sommaires qui ne se produisent pas à la limite d'un numéro de réseau, ou si vous souhaitez utiliser des adresses sommaires sur l'ASA avec le récapitulatif de routage automatique désactivé.

Procédure

Étape 1 Entrez en mode de configuration du routeur :

router isis

Exemple :

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

Étape 2 Créez des adresses agrégées pour IS-IS :

summary-address *address mask* **[level-1 | level-1-2 | level-2] tag** *tag-number* **metric** *metric-value*

Exemple :

```
ciscoasa(config-router)# summary-address 10.1.0.0 255.255.0.0 tag 100 metric 110
```

- *address* : adresse sommaire désignée pour une plage d'adresses IP.
- *mask* – filtre d'adresse locale IP utilisé pour la route récapitulative.
- (Facultatif) **level-1** : seules les routes redistribuées au niveau 1 sont récapitulées avec l'adresse configurée et la valeur de masque.
- (Facultatif) **level-1-2** : les routes récapitulatives sont appliquées lors de la redistribution des routes de niveau 1 et niveau 2 et lorsque IS-IS de niveau 2 annonce des routes de niveau 1 comme accessibles dans sa zone.
- (Facultatif) **level-2** : les routes apprises par le routage de niveau 1 sont récapitulées dans le réseau fédérateur de niveau 2 avec l'adresse configurée et la valeur de masque. Les routes redistribuées dans IS-IS de niveau 2 sont également résumées.
- (Facultatif) **tag** *tag-number* : spécifie le numéro utilisé pour baliser la route récapitulative. La plage va de 1 à 4294967295.
- (Facultatif) **metric** *metric-value* : spécifie la valeur de la mesure appliquée à la route récapitulative. Le mot clé **metric** est attribué à la liaison et utilisé pour calculer le coût du chemin via les liaisons vers les destinations. Vous pouvez configurer cette mesure pour le routage de niveau 1 ou 2 uniquement. La plage va de 1 à 4294967295. La valeur par défaut est 10.

Saisissez la commande **show clns interface** pour vérifier les valeurs de mesure des interfaces. Consultez Supervision IS-IS, à la page 39 pour en savoir plus.

Configurer les interfaces passives IS-IS

Vous pouvez désactiver les paquets Hello IS-IS et les mises à jour de routage sur les interfaces tout en incluant les adresses d'interface dans la base de données de topologie. Ces interfaces ne formeront pas de contiguïtés de voisins IS-IS.

Si vous avez une interface que vous ne souhaitez pas faire participer au routage IS-IS, mais qui est associée à un réseau que vous souhaitez annoncer, configurez les interfaces passives (à l'aide de la commande **passive-interface**) pour empêcher cette interface d'utiliser IS-IS. En outre, vous pouvez spécifier la version d'IS-IS utilisée par l'ASA pour les mises à jour. Le routage passif aide à contrôler l'annonce des renseignements de routage IS-IS et désactive l'envoi et la réception des mises à jour de routage IS-IS sur une interface.

Procédure

Étape 1 Entrez en mode de configuration du routeur :

router isis

Exemple :

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

Étape 2 Configurez une interface passive sur l'ASA :

passive-interface *interface-name*

Exemple :

```
ciscoasa(config-router)# passive-interface inside
```

- **default** : supprimez les mises à jour de routage sur toutes les interfaces.
- **management** : supprimez les mises à jour sur l'interface de gestion Management 0/1.
- **management2** : supprimez les mises à jour sur l'interface de gestion Management 0/2.
- **inside** : supprimez les mises à jour sur l'interface interne.

Cette commande configure les interfaces NON pas pour former des contiguïtés de voisins IS-IS, mais pour inclure les adresses d'interface dans la base de données IS-IS.

Étape 3 Configurez l'ASA pour annoncer les interfaces passives :

advertise passive-only

Exemple :

```
ciscoasa(config-router)# advertise passive-only
```

Cette commande configure IS-IS pour annoncer uniquement les préfixes qui appartiennent aux interfaces passives. Elle exclut les préfixes IP des réseaux connectés des annonces LSP, ce qui réduit le temps de convergence IS-IS.

Configurer les interfaces IS-IS

Cette procédure décrit comment modifier les interfaces ASA individuelles pour le routage IS-IS. Vous pouvez modifier les éléments suivants :

- Paramètres généraux tels que l'activation IS-IS, l'activation du protocole d'arrêt IS-IS, les priorités, les balises et les filtres de contiguïté sur une interface.
- Clé et mode d'authentification : consultez Activer l'authentification IS-IS, à la page 12 pour connaître les procédures de configuration de l'authentification sur les interfaces.
- Valeurs de remplissage Hello : consultez Configurer le remplissage d'interfaces Hello IS-IS, à la page 27 pour connaître les procédures de configuration du remplissage Hello sur les interfaces.
- Paramètres LSP
- La mesure du délai d'interface utilisée dans les calculs des mesures d'IS-IS.

Avant de commencer

Avant que le processus de routage IS-IS ne soit utile, vous devez attribuer un NET et certaines interfaces doivent avoir activé IS-IS. Vous ne pouvez configurer qu'un seul processus pour effectuer le routage de niveau 2 (inter-zone). Si le routage de niveau 2 est configuré sur un processus, tous les processus supplémentaires sont automatiquement configurés en tant que niveau 1. Vous pouvez configurer ce processus pour effectuer un routage intra-zone (niveau 1) en même temps. Une interface ne peut pas faire partie de plusieurs zones, sauf dans le cas où le processus de routage associé effectue à la fois le routage de niveau 1 et de niveau 2. Reportez-vous à Activer le routage IS-IS globalement, à la page 8 pour connaître la procédure.

Procédure

Étape 1 Entrez le mode de configuration d'interface :

interface *interface_id*

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis
```

Étape 2 Filtrez l'établissement des contiguïtés IS-IS :

isis adjacency-filter *nom* **[match-all]**

Exemple :

```
ciscoasa(config-if)# isis adjacency-filter ourfriends match-all
```

- *name* : nom de l'ensemble de filtres ou de l'expression à appliquer.
- (Facultatif) **match-all** : toutes les adresses NSAP doivent correspondre au filtre pour accepter la contiguïté. Si elle n'est pas spécifiée (par défaut), une seule adresse doit correspondre au filtre pour que la contiguïté soit acceptée.

Le filtrage est effectué en créant des adresses NSAP à partir des paquets Hello IS-IS entrants en combinant chaque adresse de zone du Hello avec l'ID de système. Chacune de ces adresses NSAP est ensuite transmise par le filtre. Si un NSAP correspond, le filtre est considéré comme transmis, sauf si le mot clé **match-all** est spécifié, auquel cas toutes les adresses doivent passer. La fonctionnalité du mot clé **match-all** est utile pour effectuer des tests négatifs, comme l'acceptation d'une contiguïté uniquement si une adresse particulière n'est pas présente.

Étape 3 Annoncez les préfixes IS-IS des réseaux connectés dans des annonces LSP sur une interface IS-IS :

isis advertise prefix

Exemple :

```
ciscoasa(config-if)# isis advertise prefix
```

Par défaut, cette commande est activée. Ainsi, les routes connectées sont distribuées même si elles ne sont pas destinées à être distribuées. Pour mettre fin à la redistribution inutile des routes connectées et améliorer

le temps de convergence IS-IS, utilisez la commande **no isis advertise prefix**. Cela exclut les préfixes IP du réseau connecté des annonces LSP et réduit le temps de convergence IS-IS.

Remarque
La configuration de la forme **no** de cette commande par interface IS-IS est une solution à petite échelle visant à réduire le temps de convergence IS-IS, car moins de préfixes sont annoncés dans le LSP non pseudo-nœud du routeur. Une alternative à la commande **isis advertise prefix** est la commande **advertise passive-only**, qui est une solution évolutive, car elle est configurée par instance IS-IS.

Étape 4 Activez IPv6 sur une interface IS-IS :

ipv6 router isis

Exemple :

```
ciscoasa(config-if)# ipv6 router isis
```

Étape 5 Configurez le délai entre les transmissions LSP IS-IS successives par interface :

isis lsp-interval *milliseconds*

Exemple :

```
ciscoasa(config-if)# isis lsp-interval 100
```

milliseconds : délai entre des LSP successifs. La plage se situe entre 1 et 4294967298. La valeur par défaut est de 33 millisecondes.

Dans les topologies avec un grand nombre de voisins et d'interfaces IS-IS, un ASA peut avoir de la difficulté avec la charge de CPU imposée par la transmission et la réception des LSP. Cette commande réduit le débit de transmission des LSP (et, par conséquent, le débit de réception des autres systèmes).

Étape 6 Configurez la valeur d'une mesure IS-IS :

isis metric {*metric-value* | **maximum**} [**level-1 | level-2**]

Exemple :

```
ciscoasa(config-if)# isis metric 15 level-1
```

- *metric-value* : mesure attribuée au lien et utilisée pour calculer le coût de chaque autre routeur par les liaisons du réseau vers d'autres destinations. Vous pouvez configurer cette mesure pour le routage de niveau 1 ou 2. La plage est comprise entre 1 et 63. La valeur par défaut est 10.
- **maximum** : exclut un lien ou une contiguïté dans le calcul SPF.
- (Facultatif) **level-1** : précise que cette mesure doit être utilisée uniquement dans le calcul SPF pour le routage de niveau 1 (intra-zone). Si aucun mot clé facultatif n'est spécifié, la mesure est activée sur les niveaux de routage 1 et 2.
- (Facultatif) **level-2** : précise que cette mesure doit être utilisée uniquement dans le calcul SPF pour le routage de niveau 2 (inter-zone). Si aucun mot clé facultatif n'est spécifié, la mesure est activée sur les niveaux de routage 1 et 2.

Étape 7 Configurez la priorité des ASA désignés sur l'interface :

isis priority *number-value* **[level-1 | level-2]**

Exemple :

```
ciscoasa(config-if)# isis priority 80 level-1
```

- *number-value* : définissez la priorité d'un ASA. La valeur doit être comprise entre 0 et 127. La valeur par défaut est 64.
- (Facultatif) **level-1** : définissez la priorité du niveau 1 indépendamment.
- (Facultatif) **level-2** : définissez la priorité du niveau 2 indépendamment.

La priorité est utilisée pour déterminer quel ASA d'un réseau local sera le routeur désigné ou le DIS. Les priorités sont annoncées dans les paquets Hello. L'ASA ayant la priorité la plus élevée devient le DIS.

Remarque
Dans IS-IS, il n'y a pas de routeur désigné de secours. La définition de la priorité à 0 réduit la probabilité que ce système devienne le DIS, mais ne l'empêche pas. Si un routeur ayant une priorité plus élevée entre en ligne, il prend le rôle du DIS actuel. En cas de priorités égales, l'adresse MAC la plus élevée rompt le lien.

Étape 8 Désactivez le protocole IS-IS afin qu'il ne puisse pas former de contiguïtés sur une interface spécifiée et placez l'adresse IP de l'interface dans le LSP généré par l'ASA :

isis protocol shutdown

Exemple :

```
ciscoasa(config-if)# isis protocol shutdown
```

Cette commande vous permet de désactiver le protocole IS-IS pour une interface spécifiée sans supprimer les paramètres de configuration. Le protocole IS-IS ne forme aucune contiguïté pour l'interface pour laquelle cette commande a été configurée, et l'adresse IP de l'interface est placée dans le LSP généré par le routeur. Utilisez la commande **protocol shutdown** si vous ne souhaitez pas que IS-IS forme une contiguïté sur n'importe quelle interface et efface la base de données LSP IS-IS. Reportez-vous à Activer le routage IS-IS globalement, à la page 8 pour connaître la procédure.

Étape 9 Configurez le temps entre la retransmission de chaque LSP IS-IS :

isis retransmit-interval *seconds*

Exemple :

```
ciscoasa(config-if)#  isis retransmit-interval 60
```

(Facultatif) *seconds* : délai entre la retransmission de chaque LSP. Le nombre doit être supérieur au délai aller-retour attendu entre deux routeurs du réseau connecté. La valeur est comprise entre 0 et 65 535. La valeur par défaut est de 5 secondes.

Assurez-vous que l'argument *seconds* est prudent, sinon cela pourrait entraîner des retransmissions inutiles. Cette commande est sans effet sur les interfaces LAN (multipoint).

Étape 10 Configurez le temps entre les retransmissions de chaque LSP IS-IS :

isis retransmit-throttle-interval *milliseconds*

Exemple :

```
ciscoasa(config-if)#  isis retransmit-throttle-interval 300
```

(Facultatif) *milliseconds* : délai minimum entre les retransmissions des LSP sur l'interface. La valeur est comprise entre 0 et 65 535.

Cette commande peut être utile dans les très grands réseaux avec de nombreux LSP et de nombreuses interfaces comme moyen de contrôler le trafic de retransmission des LSP. Cette commande contrôle le débit auquel les LSP peuvent être renvoyés sur l'interface.

Cette commande est distincte du débit auquel les LSP sont envoyés sur l'interface (contrôlée par la commande **isis lsp-interval**) et de la période entre les retransmissions d'un seul LSP (contrôlée par la commande **isis retransmit-interval**). Vous pouvez utiliser ces commandes en combinaison pour contrôler la charge offerte de trafic de routage d'un ASA à ses voisins.

Étape 11 Définissez une balise sur l'adresse IP configurée pour une interface lorsque le préfixe IP est placé dans un LSP IS-IS :

isis tag *tag-number*

Exemple :

```
ciscoasa(config-if)# isis tag 100
```

tag-number : le numéro qui sert de balise sur une route IS-IS. La plage va de 1 à 4294967295.

Aucune action ne se produit sur une route balisée jusqu'à ce que la balise soit utilisée, par exemple, pour redistribuer ou synthétiser les routes. La configuration de cette commande déclenche l'ASA pour générer de nouveaux LSP, car la balise est une nouvelle information dans le paquet.

Exemples

Dans cet exemple, deux interfaces sont marquées avec des valeurs de balise différentes. Par défaut, ces deux adresses IP auraient été placées dans la base de données IS-IS de niveau 1 et de niveau 2. Cependant, si vous utilisez la commande **redistribute** avec une carte de routage pour faire correspondre la balise 110, seule l'adresse IP 172.16. 0.0 est placée dans la base de données de niveau 2.

```
ciscoasa (config)# interface GigabitEthernet1/0
ciscoasa (config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa (config-if)# isis
ciscoasa (config-if)# isis tag 120
ciscoasa (config)# interface GigabitEthernet1/1
ciscoasa (config-if)# ip address 172.16.0.0
ciscoasa (config-if)# isis
ciscoasa (config-if)# isis tag 110
ciscoasa (config-router)# route-map match-tag permit 10
ciscoasa (config-router)# match tag 110
ciscoasa (config)# router isis
ciscoasa (config-router)# net 49.0001.0001.0001.0001.00
ciscoasa (config-router)# redistribute isis ip level-1 into level-2 route-map match-tag
```

Configurer le remplissage d'interfaces Hello IS-IS

Les paquets Hello sont responsables de la découverte et de la maintenance des voisins. Vous pouvez configurer les paramètres de remplissage Hello suivants au niveau de l'interface. Consultez Activer le routage IS-IS globalement, à la page 8 pour activer/désactiver le remplissage Hello pour l'ensemble de l'IS-IS.

Procédure

Étape 1 Entrez le mode de configuration d'interface :

interface *interface_id*

Exemple :

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis
```

Étape 2 Entrez dans le mode de configuration d'interface pour configurer le remplissage sur les unités de données de protocole Hello IS-IS (IIH PDU) pour toutes les interfaces de l'ASA :

isis hello padding

Exemple :

```
ciscoasa(config-if)# isis hello padding
```

Les messages Hello sont ajoutés à la MTU complète, ce qui permet une détection précoce des erreurs résultant de problèmes de transmission avec de grandes trames ou d'erreurs résultant de MTU non concordantes sur des interfaces adjacentes. Le remplissage Hello IS-IS est activé par défaut.

Remarque
Vous pouvez désactiver le remplissage Hello pour éviter de gaspiller la bande passante du réseau dans le cas où la MTU des deux interfaces est identique ou en cas de pontage translationnel. Bien que le remplissage Hello soit désactivé, les ASA envoient toujours les cinq premiers Hellos IS-IS remplis à la taille MTU complète afin de conserver les avantages de la détection des incompatibilités MTU.

Étape 3 Précisez la durée entre des paquets Hello consécutifs envoyés par IS-IS :

isis hello-interval {*seconds* | **minimal**} **[level-1 | level-2]**

Exemple :

```
ciscoasa(config-if)# isis hello-interval 5 level-1
```

- *seconds* : la durée entre les paquets Hello. Par défaut, une valeur de trois fois les secondes d'intervalle Hello est annoncée comme délai de rétention dans les paquets Hello envoyés. Vous pouvez modifier le multiplicateur de 3 en configurant la commande **isis hello-multiplier**. Avec des intervalles Hello plus petits, les modifications topologiques sont détectées plus rapidement, mais le trafic de routage est plus élevé. La valeur est comprise entre 0 et 65 535. La valeur par défaut est 10.
- **minimal** : le système calcule l'intervalle Hello en fonction du multiplicateur Hello (spécifié par la commande **isis hello-multiplier**) de sorte que le délai de rétention résultant soit de 1 seconde.

- (Facultatif) **level-1** : configure l'intervalle Hello pour le niveau 1 indépendamment. Utilisez-le sur X.25, le service de données SMDS (Switched Multimegabit Data Service) et les réseaux multiaccès de relayage de trames.
- (Facultatif) **level-2** : configure l'intervalle Hello pour le niveau 2 indépendamment. Utilisez-le sur X.25, le SMDS et les réseaux multiaccès de relayage de trames.

Remarque
Bien qu'un intervalle Hello plus lent permette d'économiser de la bande passante et de réduire l'utilisation du processeur, il existe certaines situations où un intervalle Hello plus rapide est préférable, par exemple, une configuration de grande envergure qui utilise des tunnels d'ingénierie de trafic (TE). Si le tunnel TE utilise IS-IS comme protocole IGP (Interior Gateway Protocol) et que le processus de routage IP est redémarré au niveau du routeur au point d'entrée du réseau (tête), tous les tunnels TE sont resignalisés avec l'intervalle Hello par défaut. Un intervalle Hello plus rapide empêche cette nouvelle signalisation. Pour configurer un intervalle Hello plus rapide, vous devez augmenter l'intervalle Hello IS-IS manuellement à l'aide de la commande **isis hello-multiplier**.

Étape 4 Spécifiez le nombre de paquets Hello IS-IS qu'un voisin doit manquer avant que l'ASA déclare la contiguïté comme étant inactive :

isis hello-multiplier *multiplier* **[level-1 | level-2]**

Exemple :

```
ciscoasa(config-if)# isis hello-multiplier 10 level-1
```

- *multipler* : le délai de rétention annoncé dans les paquets Hello IS-IS est défini comme le produit du multiplicateur Hello par l'intervalle Hello. Les voisins déclarent une contiguïté à cet ASA après n'avoir reçu aucun paquet Hello IS-IS pendant le délai de rétention annoncé. Vous pouvez définir le délai de rétention (et donc le multiplicateur Hello et l'intervalle Hello) par interface, et il peut être différent entre les différents routeurs d'une même zone. La valeur doit être comprise entre 3 et 1 000. La valeur par défaut est de 3.
- (Facultatif) **level-1** : configure le multiplicateur Hello indépendamment pour les contiguïtés de niveau 1.
- (Facultatif) **level-2** : configure le multiplicateur Hello indépendamment pour les contiguïtés de niveau 2.

Utilisez cette commande dans les circonstances où les paquets Hello sont fréquemment perdus et que les contiguïtés IS-IS échouent inutilement.

Remarque
L'utilisation d'un multiplicateur Hello de petite taille entraînera une convergence rapide, mais peut entraîner une plus grande instabilité du routage. Modifiez le multiplicateur Hello à une valeur plus élevée pour contribuer à la stabilité du réseau, au besoin. Ne configurez jamais un multiplicateur Hello inférieur à la valeur par défaut de 3.

Étape 5 Configurez le type de contiguïté utilisé pour IS-IS :

isis circuit-type [level-1 | level-1-2 | level-2-only]

Exemple :

```
ciscoasa(config-if)# isis circuit-type level-2-only
```

- (Facultatif) **level-1** : configure un ASA pour la contiguïté de niveau 1 uniquement.
- (Facultatif) **level-1-2** : configure un ASA pour la contiguïté des niveaux 1 et 2.
- (Facultatif) **level-2** : configure un ASA pour la contiguïté de niveau 2 uniquement.

Vous n'avez normalement pas besoin de configurer cette commande. La méthode appropriée consiste à configurer le niveau sur un ASA. Reportez-vous à Activer le routage IS-IS globalement, à la page 8 pour connaître la procédure. Vous devez configurer certaines interfaces comme niveau 2 uniquement sur les ASA situés entre les zones (routeurs de niveau 1-2). Cela permet d'économiser de la bande passante en envoyant des paquets Hello de niveau 1 inutilisés.

Étape 6 Configurez l'intervalle auquel les paquets CSNP périodiques sont envoyés sur les interfaces de diffusion :

isis csnp-interval *seconds* **[level-1 | level-1-2 | level-2]**

Exemple :

```
ciscoasa(config-if)#  isis csnp-interval 30 level-1
```

- *seconds* : intervalle entre la transmission des CSNP sur les réseaux multiaccès. Cet intervalle s'applique uniquement à l'ASA désigné. La valeur est comprise entre 0 et 65535. La valeur par défaut est de 10 secondes.
- (Facultatif) **level-1** : configure l'intervalle de temps entre la transmission des CSNP pour le niveau 1 indépendamment.
- (Facultatif) **level-2** : configure l'intervalle de temps entre la transmission des CSNP pour le niveau 2 indépendamment.

Il est peu probable que vous deviez modifier la valeur par défaut de cette commande.

Cette commande s'applique uniquement au DR pour une interface spécifiée. Seuls les DR envoient des paquets CSNP pour maintenir la synchronisation de la base de données. Vous pouvez configurer l'intervalle CSNP indépendamment pour les niveaux 1 et 2.

Configurer la famille d'adresses IPv4 IS-IS

Les routeurs sont autorisés à redistribuer des préfixes externes ou des routes apprises à partir de tout autre protocole de routage, configuration statique ou interface connectée. Les routes redistribuées sont autorisées dans un routeur de niveau 1 ou dans un routeur de niveau 2.

Vous pouvez configurer la contiguïté, Shortest Path First (SPF) et vous pouvez définir les conditions pour la redistribution des routes à partir d'un autre domaine de routage dans IS-IS (redistribution) pour les adresses IPv4.

Avant de commencer

Avant de pouvoir activer l'authentification du routage IS-IS, vous devez activer IS-IS et configurer une zone. Reportez-vous à Activer le routage IS-IS globalement, à la page 8 pour connaître la procédure.

Procédure

Étape 1 Entrez en mode de configuration du routeur pour configurer une famille d'adresses IPv4 :

router isis

Exemple :

```
ciscoasa(config)# router isis
cisco(config-router)#
```

Étape 2 Effectuez une vérification de la contiguïté pour vérifier la prise en charge du protocole IS-IS :

adjacency-check

Exemple :

```
cisco(config-router)# adjacency-check
```

Étape 3 Définissez la distance administrative attribuée aux routes détectées par le protocole IS-IS :

distance *weight*

weight : distance administrative attribuée aux routes IS-IS. La plage va de 1 à 255. La valeur par défaut est 115.

Exemple :

```
ciscoasa(config-router)# distance 20
```

Cette commande configure les distances appliquées aux routes IS-IS lorsqu'elles sont insérées dans la RIB et influe sur la probabilité que ces routes soient préférées aux routes vers les mêmes adresses de destination découvertes par d'autres protocoles.

Remarque
En général, plus la valeur de la distance administrative est élevée, plus le taux de confiance est bas. Une distance administrative de 255 signifie que la source de renseignements de routage n'est pas du tout fiable et doit être ignorée. Les valeurs de poids sont subjectives; il n'existe aucune méthode quantitative pour choisir les valeurs de poids.

Étape 4 Configurez le partage de charge à chemins multiples pour IS-IS :

maximum-paths *number-of-paths*

Exemple :

```
ciscoasa(config-router)# maximum-paths 8
```

number-of-paths : nombre de routes à installer dans la table de routage. La plage va de 1 à 8. La valeur par défaut est 1.

La commande **maximum-path** est utilisée pour configurer le partage de charges multiples IS-IS lorsque ECMP est configuré dans l'ASA.

Étape 5 Générez une route par défaut dans un domaine de routage IS-IS :

default-information originate [**route-map** *map-name*]

Exemple :

```
ciscoasa(config-router)# default-information originate route-map RMAP
```

(Facultatif) **route-map** *map-name* : le processus de routage génère la route par défaut si la carte de routage est satisfaite.

Si un ASA configuré avec cette commande a une route vers 0.0.0.0 dans la table de routage, IS-IS générera une annonce pour 0.0.0.0 dans ses LSP. Sans carte de routage, la valeur par défaut est annoncée uniquement dans les LSP de niveau 2. Pour le routage de niveau 1, il existe un autre mécanisme pour trouver la route par défaut, qui consiste à rechercher le routeur de niveau 1 ou 2 le plus proche. Le routeur de niveau 1 ou 2 le plus proche peut être trouvé en examinant l'ATT dans les LSP de niveau 1. Avec une commande **match ip address** *standard-access-list*, vous pouvez spécifier une ou plusieurs routes IP qui doivent exister avant que l'ASA annonce 0/0.

Étape 6 Définissez la mesure IS-IS globalement pour les niveaux 1 et 2 :

metric *default-value* **[level-1 | level-2]**

Exemple :

```
ciscoasa(config-router)# metric 55 level-1
ciscoasa(config-router)# metric 45 level-2
```

- *default-value* : la valeur de la mesure à attribuer au lien et à utiliser pour calculer le coût du chemin par les liaisons vers les destinations. La plage est de 1 à 63. La valeur par défaut est 10.
- (Facultatif) **level-1** : définit la mesure IPv4 ou IPv6 de niveau 1.
- (Facultatif) **level-2** : définit la mesure IPv4 ou IPv6 de niveau 2.

Étape 7 Spécifiez le style de mesure et les niveaux auxquels l'appliquer :

metric-style [narrow | transition | wide] [level-1 | level-2 | level-1-2]

Exemple :

```
ciscoasa(config-router)# metric-style wide level-1
```

- **narrow** : demande à l'ASA d'utiliser l'ancien type de TLV avec la mesure restrictive.
- **transition** : demande à l'ASA d'accepter les anciens et les nouveaux types TLV pendant la transition.
- **wide** : demande à l'ASA d'utiliser le nouveau type de TLV pour le transport de la mesure plus large.
- (Facultatif) **level-1** : définit la mesure IPv4 ou IPv6 de niveau 1.
- (Facultatif) **level-2** : définit la mesure IPv4 ou IPv6 de niveau 2.
- (Facultatif) **level-1-2** : définit la mesure IPv4 ou IPv6 des niveaux 1 et 2.

Étape 8 Spécifiez les contraintes concernant le moment où un routeur de niveau 1 au niveau 2 doit définir son bit associé :

set-attached-bit route-map *map-tag*

Exemple :

```
ciscoasa(config-router)# set-attached-bit route-map check-for-L2_backbone_connectivity
```

route-map *map-tag* : identifiant d'une carte de routage configurée. Si la carte de routage indiquée correspond, le routeur continue de définir son bit associé. Cette commande est désactivée par défaut.

Dans la mise en œuvre IS-IS actuelle, comme le spécifie la norme ISO 10589, les routeurs de niveau 1 et 2 définissent leur bit LSP associé de niveau 1 lorsqu'ils détectent d'autres zones dans leur propre domaine ou détectent d'autres domaines. Cependant, dans certaines topologies de réseau, les routeurs de niveau 1 au niveau 2 adjacents dans des zones différentes peuvent perdre la connectivité au réseau fédérateur de niveau 2. Les routeurs de niveau 1 peuvent ensuite envoyer le trafic destiné à l'extérieur de la zone ou du domaine aux routeurs de niveau 1 de niveau 2 qui peuvent ne pas avoir une telle connectivité.

Cette commande permet de mieux contrôler le paramètre de bit associé pour les routeurs de niveau 1 au niveau 2. La carte de routage peut spécifier une ou plusieurs routes CLNS. Si au moins une des clauses de correspondance des cartes de routage d'adresses de correspondance correspond à une route dans la table de routage CLNS de niveau 2 et si toutes les autres exigences de définition du bit associé sont respectées, le routeur de niveau 1 au niveau 2 continue de définir le bit associé dans son LSP de niveau 1. Si les exigences ne sont pas respectées ou si aucune clause de la carte de routage d'adresse de correspondance ne correspond à une route dans la table de routage CLNS de niveau 2, le bit associé n'est pas défini.

Étape 9 Configurez l'ASA pour signaler aux autres routeurs de ne pas l'utiliser comme saut intermédiaire dans leurs calculs SPF :

set-overload-bit [on-startup {*seconds* | **wait-for bgp**}] [**suppress [[interlevel] [external**]]]

Exemple :

```
ciscoasa(config-router)# set-overload-bit on-startup wait-for-bgp suppress interlevel
external
```

- (Facultatif) **on-startup** : définit le bit de surcharge au démarrage du système. Le bit de surcharge reste défini pendant le nombre de secondes configurées ou jusqu'à ce que le protocole BGP ait convergé, selon l'argument ou le mot clé ultérieur spécifié.
- (Facultatif) *seconds* : le nombre de secondes pendant lesquelles le bit de surcharge est défini au démarrage du système et reste défini. La plage va de 5 à 86 400.
- (Facultatif) **wait-for-bgp** : lorsque le mot clé **on-startup** est configuré, le bit de surcharge est défini au démarrage du système et reste défini jusqu'à ce que le protocole BGP ait convergé.
- (Facultatif) **suppress** : supprime le type de préfixe identifié par le ou les mots clés suivants.
- (Facultatif) **interlevel** : lorsque le mot clé **suppress** est configuré, empêche l'annonce des préfixes IP appris à partir d'un autre niveau IS-IS.
- (Facultatif) **external** : lorsque le mot clé **suppress** est configuré, empêche l'annonce des préfixes IP appris à partir d'autres protocoles.

Cette commande force l'ASA à définir le bit de surcharge (également connu sous le nom de bit hello) dans ses LSP non pseudo-nœuds. Normalement, le réglage du bit de surcharge est autorisé uniquement lorsqu'un ASA rencontre des problèmes. Par exemple, lorsqu'un ASA manque de mémoire, il se peut que la base de données de l'état des liaisons ne soit pas complète, ce qui entraîne une table de routage incomplète ou inexacte. En définissant le bit de surcharge dans ses LSP, les autres routeurs peuvent ignorer le routeur non fiable dans

leurs calculs SPF jusqu'à ce que le routeur ait résolu ses problèmes. Il en résulte qu'aucun chemin passant par ce routeur n'est visible par d'autres routes dans la zone IS-IS. Cependant, les préfixes IP et CLNS sont directement connectés à ce routeur.

Étape 10 Personnalisez la limitation IS-IS des PRC :

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

Exemple :

```
ciscoasa(config-router)#  prc-interval 5 10 20
```

- *prc-max-wait* : indique l'intervalle maximum entre deux calculs PRC consécutifs. La plage est comprise entre 1 et 120 secondes. La valeur par défaut est de 5 secondes.
- (Facultatif) *prc-initial-wait* : indique le délai d'attente initial du PRC après une modification de la topologie. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 2 000 millisecondes.

  Chaque intervalle d'attente ultérieur est deux fois plus long que le précédent jusqu'à ce que l'intervalle d'attente atteigne l'intervalle d'attente PRC maximum spécifié.
- (Facultatif) *prc-second-wait* : indique l'intervalle entre le premier et le deuxième calcul PRC. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 000 millisecondes (5 secondes).

  Le PRC est le processus logiciel de calcul des routes sans effectuer de calcul SPF. Cela est possible lorsque la topologie du système de routage lui-même n'a pas changé, mais qu'une modification est détectée dans les renseignements annoncés par un IS particulier ou lorsqu'il est nécessaire de tenter de réinstaller de telles routes dans la RIB.

Étape 11 Personnalisez la limitation IS-IS des calculs SPF :

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

Exemple :

```
ciscoasa(config-router)#  spf-interval level-1 5 10 20
```

- (Facultatif) **level-1** : appliquer les intervalles aux zones de niveau 1 uniquement.
- (Facultatif) **level-2** : appliquer les intervalles aux zones de niveau 2 uniquement.
- *spf-max-wait* : indique l'intervalle maximum entre deux calculs SPF consécutifs. La plage est comprise entre 1 et 120 secondes. La valeur par défaut est de 10 secondes.
- (Facultatif) *spf-initial-wait* : indique le délai d'attente initial après une modification de topologie avant le premier calcul SPF. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 500 millisecondes (5,5 secondes).

  Chaque intervalle d'attente ultérieur est deux fois plus long que le précédent jusqu'à ce que l'intervalle d'attente atteigne l'intervalle d'attente SPF maximum spécifié.
- (Facultatif) *spf-second-wait* : indique l'intervalle entre le premier et le deuxième calcul SPF. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 500 millisecondes (5,5 secondes).

Les calculs SPF sont effectués uniquement lorsque la topologie change. Cette commande contrôle la fréquence à laquelle le logiciel effectue le calcul SPF.

Remarque
Le calcul SPF est exigeant pour le processeur. Par conséquent, il peut être utile de limiter la fréquence à laquelle il est effectué, en particulier lorsque la zone est vaste et que la topologie change souvent. L'augmentation de l'intervalle SPF réduit la charge du processeur de l'ASA, mais retarde potentiellement le taux de convergence.

Étape 12 Configurez IS-IS pour respecter les mesures externes lors des calculs SFP :

use external-metrics

Étape 13 Configurez une redistribution des routes BGP, connectées, IS-IS, OSPF ou statiques :

redistribute bgp | connected | isis | ospf | static | level-1 | level-2 | level 1-2 metric-type internal | external metric *number*

Exemple :

```
ciscoasa(config-router)# redistribute bgp level-1 metric-type internal metric 6
```

Remarque
La redistribution des routes statiques avec une carte de routage correspondant à une mesure n'est pas prise en charge.

metric *number* : valeur de la mesure. La plage va de 1 à 4294967295.

Configuration du bit associé

Dans l'exemple suivant, le bit associé restera défini lorsque le routeur correspondra à 49.00aa dans la table de routage L2 CLNS :

```
ciscoasa(config)# router isis
 ciscoasa(config-router)# clns filter-set L2_backbone_connectivity permit 49.00aa
 ciscoasa(config-router)# route-map check-for-L2_backbone_connectivity
 ciscoasa(config-router)# match clns address L2_backbone_connectivity
ciscoasa(config)# router isis
 ciscoasa(config-router)#set-attached-bit route-map check-for-L2_backbone_connectivity
 ciscoasa(config-router)# end
 ciscoasa# show clns route 49.00aa

Known via "isis", distance 110, metric 30, Dynamic Entry
Routing Descriptor Blocks:
 via tr2, Serial0
   isis, route metric is 30, route version is 58
```

Configurer la famille d'adresses IPv6 IS-IS

Vous pouvez configurer la contiguïté, SPF et vous pouvez définir les conditions pour la redistribution des routes à partir d'un autre domaine de routage dans IS-IS (redistribution) pour les adresses IPv6.

Avant de commencer

Avant de pouvoir activer l'authentification du routage IS-IS, vous devez activer IS-IS et configurer une zone. Reportez-vous à Activer le routage IS-IS globalement, à la page 8 pour connaître la procédure.

Procédure

Étape 1 Entrez en mode de configuration du routeur :

router isis

Exemple :

```
cisco(config-router)#
```

Étape 2 Spécifiez le style de mesure comme large :

metric-style wide [transition] [level-1 | level-2 | level-1-2]

Exemple :

```
ciscoas(config)# router isis
ciscoasa(config-router)# metric-style wide level-1
```

- (Facultatif) **transition** : demande au routeur d'accepter les TLV de style ancien et nouveau.
- (Facultatif) **level-1** : définit la mesure IPv4 ou IPv6 de niveau 1.
- (Facultatif) **level-2** : définit la mesure IPv4 ou IPv6 de niveau 2.
- (Facultatif) **level-1-2** : définit la mesure IPv4 ou IPv6 des niveaux 1 et 2.

Nous vous conseillons d'utiliser la commande **metric** lorsque vous devez modifier la mesure par défaut pour toutes les interfaces IS-IS. Ceci évite les erreurs d'utilisateur, par exemple en supprimant involontairement une mesure définie d'une interface sans configurer de nouvelle valeur et en permettant à l'interface de revenir à la mesure par défaut de 10, devenant ainsi une interface privilégiée dans le réseau.

Étape 3 Passez en mode de configuration de famille d'adresses pour configurer les sessions de routage IS-IS qui utilisent des préfixes d'adresse IPv4 ou IPv6 standard :

address-family ipv6 [unicast]

Exemple :

```
ciscoasa(config-router)# address-family ipv6 unicast
cisco(config-router-af)#
```

Étape 4 Effectuez une vérification de la contiguïté pour vérifier la prise en charge du protocole IS-IS :

adjacency-check

Exemple :

```
cisco(config-router-af)# adjacency-check
```

Étape 5 Configurez le partage de charge à chemins multiples pour IS-IS :

maximum-paths *number-of-paths*

Exemple :

```
ciscoasa(config-router-af)# maximum-paths 8
```

number-of-paths : le nombre de routes à installer dans la table de routage. La plage va de 1 à 8. La valeur par défaut est 1.

La commande **maximum-path** est utilisée pour configurer le partage de charges multiples IS-IS lorsque ECMP est configuré dans l'ASA.

Étape 6 Définissez la distance administrative attribuée aux routes détectées par le protocole IS-IS :

distance *weight*

weight : la distance administrative attribuée aux routes IS-IS. La plage va de 1 à 255. La valeur par défaut est 115.

Exemple :

```
ciscoasa(config-router-af)# distance 20
```

Cette commande configure les distances appliquées aux routes IS-IS lorsqu'elles sont insérées dans la RIB et influe sur la probabilité que ces routes soient préférées aux routes vers les mêmes adresses de destination découvertes par d'autres protocoles.

Remarque
En général, plus la valeur de la distance administrative est élevée, plus le taux de confiance est bas. Une distance administrative de 255 signifie que la source de renseignements de routage n'est pas du tout fiable et doit être ignorée. Les valeurs de poids sont subjectives; il n'existe aucune méthode quantitative pour choisir les valeurs de poids.

Étape 7 Générez une route par défaut dans un domaine de routage IS-IS :

default-information originate [**route-map** *map-name*]

Exemple :

```
ciscoasa(config-router-af)# default-information originate route-map TEST7
```

(Facultatif) **route-map** *map-name* : le processus de routage génère la route par défaut si la carte de routage est satisfaite.

Si un ASA configuré avec cette commande a une route vers 0.0.0.0 dans la table de routage, IS-IS générera une annonce pour 0.0.0.0 dans ses LSP. Sans carte de routage, la valeur par défaut est annoncée uniquement dans les LSP de niveau 2. Pour le routage de niveau 1, il existe un autre mécanisme pour trouver la route par défaut, qui consiste à rechercher le routeur de niveau 1 ou 2 le plus proche. Le routeur de niveau 1 ou 2 le plus proche peut être trouvé en examinant l'ATT dans les LSP de niveau 1. Avec une commande **match ip address** *standard-access-list*, vous pouvez spécifier une ou plusieurs routes IP qui doivent exister avant que l'ASA annonce 0/0.

Étape 8 Configurez l'ASA pour signaler aux autres routeurs de ne pas l'utiliser comme saut intermédiaire dans leurs calculs SPF :

set-overload-bit [on-startup {*seconds* | **wait-for bgp**}] [**suppress [[interlevel] [external**]]]

Exemple :

```
ciscoasa(config-router-af)# set-overload-bit on-startup wait-for-bgp suppress interlevel
external
```

- (Facultatif) **on-startup** : définit le bit de surcharge au démarrage du système. Le bit de surcharge reste défini pendant le nombre de secondes configurées ou jusqu'à ce que le protocole BGP ait convergé, selon l'argument ou le mot clé ultérieur spécifié.
- (Facultatif) *seconds* : le nombre de secondes pendant lesquelles le bit de surcharge est défini au démarrage du système et reste défini. La plage va de 5 à 86 400.
- (Facultatif) **wait-for-bgp** : lorsque le mot clé **on-startup** est configuré, le bit de surcharge est défini au démarrage du système et reste défini jusqu'à ce que le protocole BGP ait convergé.
- (Facultatif) **suppress** : supprime le type de préfixe identifié par le ou les mots clés suivants.
- (Facultatif) **interlevel** : lorsque le mot clé **suppress** est configuré, empêche l'annonce des préfixes IP appris à partir d'un autre niveau IS-IS.
- (Facultatif) **external** : lorsque le mot clé **suppress** est configuré, empêche l'annonce des préfixes IP appris à partir d'autres protocoles.

Cette commande force l'ASA à définir le bit de surcharge (également connu sous le nom de bit hello) dans ses LSP non pseudo-nœuds. Normalement, le réglage du bit de surcharge est autorisé uniquement lorsqu'un ASA rencontre des problèmes. Par exemple, lorsqu'un ASA manque de mémoire, il se peut que la base de données de l'état des liaisons ne soit pas complète, ce qui entraîne une table de routage incomplète ou inexacte. En définissant le bit de surcharge dans ses LSP, les autres routeurs peuvent ignorer le routeur non fiable dans leurs calculs SPF jusqu'à ce que le routeur ait résolu ses problèmes. Il en résulte qu'aucun chemin passant par ce routeur n'est visible par d'autres routes dans la zone IS-IS. Cependant, les préfixes IP et CLNS sont directement connectés à ce routeur.

Étape 9 Personnalisez la limitation IS-IS des PRC :

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

Exemple :

```
ciscoasa(config-router-af)#  prc-interval 5 10 20
```

- *prc-max-wait* : indique l'intervalle maximum entre deux calculs PRC consécutifs. La plage est comprise entre 1 et 120 secondes. La valeur par défaut est de 5 secondes.
- (Facultatif) *prc-initial-wait* : indique le délai d'attente initial du PRC après une modification de la topologie. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 2 000 millisecondes.

  Chaque intervalle d'attente ultérieur est deux fois plus long que le précédent jusqu'à ce que l'intervalle d'attente atteigne l'intervalle d'attente PRC maximum spécifié.
- (Facultatif) *prc-second-wait* : indique l'intervalle entre le premier et le deuxième calcul PRC. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 000 millisecondes (5 secondes).

  Le PRC est le processus logiciel de calcul des routes sans effectuer de calcul SPF. Cela est possible lorsque la topologie du système de routage lui-même n'a pas changé, mais qu'une modification est détectée dans les renseignements annoncés par un IS particulier ou lorsqu'il est nécessaire de tenter de réinstaller de telles routes dans la RIB.

Étape 10 Personnalisez la limitation IS-IS des calculs SPF :

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

Exemple :

```
ciscoasa(config-router-af)#  spf-interval level-1 5 10 20
```

- (Facultatif) **level-1** : appliquer les intervalles aux zones de niveau 1 uniquement.
- (Facultatif) **level-2** : appliquer les intervalles aux zones de niveau 2 uniquement.
- *spf-max-wait* : indique l'intervalle maximum entre deux calculs SPF consécutifs. La plage est comprise entre 1 et 120 secondes. La valeur par défaut est de 10 secondes.
- (Facultatif) *spf-initial-wait* : indique le délai d'attente initial après une modification de topologie avant le premier calcul SPF. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 500 millisecondes (5,5 secondes).

  Chaque intervalle d'attente ultérieur est deux fois plus long que le précédent jusqu'à ce que l'intervalle d'attente atteigne l'intervalle d'attente SPF maximum spécifié.
- (Facultatif) *spf-second-wait* : indique l'intervalle entre le premier et le deuxième calcul SPF. La plage va de 1 à 120 000 millisecondes. La valeur par défaut est de 5 500 millisecondes (5,5 secondes).

Les calculs SPF sont effectués uniquement lorsque la topologie change. Cette commande contrôle la fréquence à laquelle le logiciel effectue le calcul SPF.

Remarque
Le calcul SPF est exigeant pour le processeur. Par conséquent, il peut être utile de limiter la fréquence à laquelle il est effectué, en particulier lorsque la zone est vaste et que la topologie change souvent. L'augmentation de l'intervalle SPF réduit la charge du processeur de l'ASA, mais retarde potentiellement le taux de convergence.

Étape 11 Configurez une redistribution des routes BGP, connectées, IS-IS, OSPF ou statiques :

redistribute bgp | connected | isis | ospf | static | level-1 | level-2 | level 1-2 metric-type internal | external metric *number*

Exemple :

```
ciscoasa(config-router-af)# redistribute static level-1 metric-type internal metric 6
```

metric *number*—The value for metric. La plage va de 1 à 4294967295.

Étape 12 Redistribuez les routes IS-IS uniquement du niveau 1 au niveau 2 ou du niveau 2 au niveau 1 :

redistribute isis {level-1 | level-2} into {level-2 | level-1} [[distribute-list *list-number* | **[route-map** *map-tag***]]**

Exemple :

```
ciscoasa(config-router-af)# redistribute isis level-1 into level-2
distribute-list 100
```

- **level-1 | level-2** : le niveau à partir duquel et vers lequel vous redistribuez les routes IS-IS.
- **into** : le mot clé qui sépare le niveau de routes redistribuées du niveau auquel vous redistribuez les routes.

- (Facultatif) **distribute-list** *list-number* : le numéro d'une liste de distribution qui contrôle la redistribution IS-IS. Vous pouvez spécifier une liste de distribution ou une carte de routage, mais pas les deux.
- (Facultatif) **route-map** *map-tag* : le nom d'une carte de routage qui contrôle la redistribution IS-IS. Vous pouvez spécifier une liste de distribution ou une carte de routage, mais pas les deux.

Remarque
Vous devez spécifier la commande **metric-style wide** pour que la commande **redistribute isis** fonctionne. Reportez-vous à l'étape 1 de cette procédure.

Dans IS-IS, toutes les zones sont des zones tampons, ce qui signifie qu'aucun renseignement de routage ne fuite du réseau fédérateur (niveau 2) vers les zones (niveau 1). Les routeurs de niveau 1 uniquement utilisent le routage par défaut vers le routeur de niveau 1-niveau 2 le plus proche dans leur zone. Cette commande vous permet de redistribuer les routes IP de niveau 2 dans les zones de niveau 1. Cette redistribution permet aux routeurs de niveau 1 uniquement de choisir le meilleur chemin pour qu'un préfixe IP sorte de la zone. Il s'agit d'une fonctionnalité IP uniquement, le routage CLNS est toujours un routage stub.

Remarque
Pour plus de contrôle et de stabilité, vous pouvez configurer une liste de distribution ou une carte de routage afin de contrôler les routes IP de niveau 2 pouvant être redistribuées dans le niveau 1. Cela permet aux grands réseaux IS-IS-IP d'utiliser la zone pour une meilleure évolutivité.

Étape 13 Créez des préfixes agrégés pour les routes IS-IS IPv6 :

summary-prefix *ipv6-prefix* **[level-1 | level-1-2 | level-2]**

Exemple :

```
cisco(config-router-af)# summary-prefix 2001::/96 level-1
```

- *ipv6 address* : le préfixe IPv6 sous la forme X.X.X.X.::X/0-128.
- (Facultatif) **level-1** : seules les routes redistribuées au niveau 1 sont récapitulées avec l'adresse configurée et la valeur de masque.
- (Facultatif) **level-1-2** : les routes récapitulatives sont appliquées lors de la redistribution des routes dans IS-IS de niveau 1 et niveau 2 et lorsque IS-IS de niveau 2 annonce des routes de niveau 1 comme accessibles dans sa zone.
- (Facultatif) **level-2** : les routes apprises par le routage de niveau 1 sont récapitulées dans le réseau fédérateur de niveau 2 avec l'adresse configurée et la valeur de masque. Les routes redistribuées dans IS-IS de niveau 2 sont également résumées.

Supervision IS-IS

Vous pouvez utiliser les commandes suivantes pour superviser le processus de routage IS-IS. Pour obtenir des exemples et des descriptions de la sortie de la commande, consultez la référence de commande.

Supervision de la base de données IS-IS

Utilisez les commandes suivantes pour superviser la base de données IS-IS :

- **show isis database [level-1 | l1] [level-2 | l2] [detail]** : affiche la base de données sur l'état des liaisons IS-IS pour les niveaux 1 et 2, ainsi que le contenu détaillé de chaque LSP.
- **show isis database verbose** : affiche plus de renseignements sur la base de données IS-IS, tels que le numéro de séquence, la somme de contrôle et le délai de rétention pour les LSP.

Supervision des entrées du tableau de mappage IS-IS

Utilisez la commande suivante pour superviser les noms d'hôte IS-IS :

show isis hostname : affiche les entrées du tableau de mappage de nom de routeur à ID système pour un routeur IS-IS.

Supervision IS-IS IPv4

Utilisez les commandes suivantes pour superviser IS-IS IPv4 :

- **show isis ip rib** : affiche la RIB spécifique à la famille d'adresses IPv4 pour un processus de routage IS-IS.
- **show isis ip spf-log** : affiche les journaux SPF spécifiques à la famille d'adresses IPv4 pour un processus de routage IS-IS.
- **show isis ip topology** : affiche la topologie spécifique à la famille d'adresses IPv4 pour un processus de routage IS-IS.
- **show isis ip redistribution** [**level-1** | **level-2**] [*network-prefix*] – Affiche les routes IPv6 IS-IS apprises et installées.
- **show isis ip unicast** : affiche la RIB, les journaux SPF et les chemins d'accès aux IS de la famille d'adresses IPv4.

Supervision IS-IS IPv6

Utilisez les commandes suivantes pour superviser IS-IS IPV6 :

- **show isis ipv6 rib** : affiche la RIB spécifique à la famille d'adresses IPv6 pour un processus de routage IS-IS.
- **show isis ipv6 spf-log** : affiche les journaux SPF spécifiques à la famille d'adresses IPv6 pour un processus de routage IS-IS.
- **show isis ipv6 topology** : affiche la topologie spécifique à la famille d'adresses IPv6 pour un processus de routage IS-IS.
- **show isis ipv6 redistribution** [**level-1** | **level-2**] [*network-prefix*] – Affiche les routes IPv6 IS-IS apprises et installées.
- **show isis ipv6 unicast** : affiche la RIB, les journaux SPF et les chemins d'accès aux IS de la famille d'adresses IPv6.

Supervision des journaux IS-IS

Utilisez les commandes suivantes pour superviser les journaux IS-IS :

- **show isis lsp-log** : affiche le journal IS-IS LSP de niveau 1 et 2 sur les interfaces qui ont déclenché le nouveau LSP.
- **show isis spf-log** : affiche la fréquence et la raison de l'exécution d'un calcul SPF par l'ASA.

Supervision du protocole IS-IS

Utilisez la commande suivante pour superviser le protocole IS-IS :

show clns protocol : affiche les renseignements sur le protocole pour chaque processus de routage IS-IS sur l'ASA.

Supervision des routes et des voisins IS-IS

Utilisez les commandes suivantes pour superviser les voisins IS-IS :

- **show isis topology** : affiche une liste de tous les routeurs connectés dans toutes les zones. Cette commande vérifie la présence et la connectivité entre tous les routeurs dans toutes les zones.
- **show isis neighbors [detail]** : affiche les renseignements de contiguïté IS-IS.
- **show clns neighbors** [*process-tag*] [*interface-name*] [**detail**] : affiche le système terminal (ES), le système intermédiaire (IS) et les voisins à topologie IS-IS (M-ISIS). Cette commande affiche la contiguïté apprise par la multitopologie IS-IS pour IPv6.
- **show clns is-neighbors** *[interface-name]* **[detail]** : affiche les renseignements IS-IS pour les contiguïtés des périphériques IS-IS.

Supervision de la RIB IS-IS

Utilisez les commandes suivantes pour superviser la RIB IS-IS :

- **show isis rib** [*ip-address* | *ip-address-mask*] : affiche les chemins pour une route donnée ou pour toutes les routes d'un réseau principal qui sont stockées dans la RIB.
- **show isis rib redistribution** [**level-1** | **level-2**] [*network-prefix*] : affiche les préfixes dans le cache de redistribution local.
- **show route isis** : affiche l'état actuel de la table de routage.

Supervision du trafic IS-IS

Utilisez la commande suivante pour superviser le trafic IS-IS :

show clns traffic [since {bootup | show}] : affiche les statistiques de trafic CLNS observées par l'ASA.

Débogage IS-IS

Utilisez les commandes suivantes pour déboguer IS-IS :

debug isis [adj-packets | authentication | checksum-errors | ip | ipv6 | local-updates | [rptpcp;-errors | rob | snp-packets | spf-events | spf-statistics | spf-triggers | update-packets] : débogue divers aspects du protocole de routage IS-IS.

Historique d'IS-IS

Tableau 1 : Historique des fonctionnalités pour IS-IS

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Routage IS-IS	9.6(1)	L'ASA prend désormais en charge le protocole de routage IS-IS (Intermediate System to Intermediate System). Une prise en charge a été ajoutée pour le routage des données, l'exécution de l'authentification, ainsi que la redistribution et la supervision des informations de routage à l'aide du protocole de routage IS-IS. Nous avons introduit les commandes suivantes : **advertise passive-only, area-password, authentication key, authentication mode, authentication send-only, clear, debug isis, distance, domain-password, fast-flood, hello padding, hostname dynamic, ignore-lsp-errors, isis adjacency-filter, isis advertise prefix, isis authentication key, isis authentication mode, isis authentication send-only, isis circuit-type, isis csnp-interval, isis hello-interval, isis hello-multiplier, isis hello padding, isis lsp-interval, isis metric, isis password, isis priority, isis protocol shutdown, isis retransmit-interval, isis retransmit-throttle-interval, isis tag, is-type, log-adjacency-changes, lsp-full suppress, lsp-gen-interval, lsp-refresh-interval, max-area-addresses, max-lsp-lifetime, maximum-paths, metric, metric-style, net, passive-interface, prc-interval, protocol shutdown, redistribute isis, route priority high, router isis, set-attached-bit, set-overload-bit, show clns, show isis, show route isis, spf-interval, summary-address**.

Exemples d'IS-IS

Cette section décrit des exemples de configuration avec une topologie pour différents aspects d'IS-IS.

Configuration du routage IS-IS

```
router isis
   net 49.1234.aaaa.bbbb.cccc.00

interface GigabitEthernet0/0
   nameif outside
   security-level 0
   ip address 192.16.32.1 255.255.255.0
   isis
```

Configuration du routage IPv6 IS-IS

```
router isis
   net 49.1234.aaaa.bbbb.cccc.00

interface GigabitEthernet0/0
   ipv6 address 2001:192:16:32::1/64
   ipv6 router isis
```

Routage dynamique dans la même zone

```
iRouter --------(inside G0/1) ASA (G0/0 outside)------------ oRouter

ASA Configuration
  interface GigabitEthernet0/0
   nameif outside
   security-level 0
   ip address 192.16.32.1 255.255.255.0
   ipv6 address 2001:192:16:32::1/64
   isis
   ipv6 router isis

  interface GigabitEthernet0/1
   nameif inside
   security-level 100
   ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
   ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
   isis
   ipv6 router isis

  router isis
   net 49.1234.2005.2005.2005.00
   is-type level-1
   metric-style wide

  interface GigabitEthernet0/0
   ip address 172.16.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:172:16:32::3/64
   ipv6 router isis
   isis priority 120

  interface GigabitEthernet0/1
   ip address 172.26.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:172:26:32::3/64
   ipv6 router isis

IOS Configuration
  iRouter
  router isis
   net 49.1234.2035.2035.2035.00
   is-type level-1
   metric-style wide

  oRouter
  interface GigabitEthernet0/0
   ip address 192.16.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:192:16:32::3/64
   ipv6 router isis

  oRouter
  interface GigabitEthernet0/1
   ip address 192.26.32.3 255.255.255.0
```

```
  ip router isis
  ipv6 address 2001:192:26:32::3/64
  ipv6 router isis

 oRouter
 router isis
  net 49.1234.2036.2036.2036.00
  is-type level-1
  metric-style wide
```

Routage dynamique dans plusieurs zones

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
  ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
  isis
  ipv6 router isis

 interface GigabitEthernet0/1.201
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
  ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
  isis
  ipv6 router isis

 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  maximum-paths 5
 !
 address-family ipv6 unicast
  maximum-paths 5
  exit-address-family
 !

IOS Configuration
 iRouter
 interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
  isis priority 120


 iRouter
 interface GigabitEthernet0/1
  ip address 172.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:26:32::3/64
  ipv6 router isis


 iRouter
 router isis
  net 49.1234.2035.2035.2035.00
  net 49.2001.2035.2035.2035.00
  is-type level-2-only
```

```
 metric-style wide

oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis


oRouter
interface GigabitEthernet0/1
 ip address 192.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:26:32::3/64
 ipv6 router isis


oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide

oRouter
 interface GigabitEthernet0/0
  ip address 192.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:16:32::3/64
  ipv6 router isis


 oRouter
 interface GigabitEthernet0/1
  ip address 192.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:26:32::3/64
  ipv6 router isis


 oRouter
 router isis
  net 49.1234.2036.2036.2036.00
  is-type level-1
  metric-style wide
```

Routage dynamique dans des zones qui se chevauchent

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0
 ipv6 address 2001:172:16:32::1/64
 isis
 ipv6 router isis

interface GigabitEthernet0/0.301
 nameif outside
 security-level 80
 ip address 192.16.32.1 255.255.255.0
```

```
 ipv6 address 2001:192:16:32::1/64
 isis
 ipv6 router isis

router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 maximum-paths 5
!
 address-family ipv6 unicast
  redistribute static level-1-2
  maximum-paths 6
 exit-address-family

IOS Configuration
iRouter
interface GigabitEthernet0/0
 ip address 172.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:16:32::3/64
 ipv6 enable
 ipv6 router isis
 isis priority 120
 isis ipv6 metric 600


interface GigabitEthernet0/1
 ip address 172.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:26:32::3/64
 ipv6 router isis


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 authentication mode md5
 authentication key-chain KeyChain level-2
 metric-style wide
 maximum-paths 6
!
 address-family ipv6
 summary-prefix 2001::/8 tag 301
 summary-prefix 6001::/16 level-1-2 tag 800
 redistribute static metric 800 level-1-2
exit-address-family


oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip pim sparse-dense-mode
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis
 isis tag 301


oRouter
```

```
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide

ASA Configuration
router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 maximum-paths 5
!
 address-family ipv6 unicast
  redistribute static level-1-2
  maximum-paths 6
 exit-address-family
!
```

Redistribution de routes

```
iRouter ---------- ASA ------------ oRouter


 ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
  ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
  isis
  ipv6 router isis


 interface GigabitEthernet0/1.201
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
  ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
  isis
  ipv6 router isis


 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  redistribute isis level-2 into level-1 route-map RMAP
  maximum-paths 5
 !
 address-family ipv6 unicast
  maximum-paths 6
 exit-address-family
!

IOS Configuration
iRouter
 interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
  isis priority 120
```

```
 iRouter
 interface GigabitEthernet0/1
  ip address 172.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:26:32::3/64
  ipv6 router isis


 iRouter
 router isis
  net 49.1234.2035.2035.2035.00
  net 49.2001.2035.2035.2035.00
  is-type level-2-only
  metric-style wide

oRouter
 interface GigabitEthernet0/0
  ip address 192.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:16:32::3/64
  ipv6 router isis


 oRouter
 interface GigabitEthernet0/1
  ip address 192.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:26:32::3/64
  ipv6 router isis


 oRouter
 router isis
  net 49.1234.2036.2036.2036.00
  is-type level-1
  metric-style wide
```

Adresse sommaire

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0
 ipv6 address 2001:172:16:32::1/64
 isis
 ipv6 router isis
 isis authentication key cisco#123 level-2
 isis authentication mode md5


interface GigabitEthernet0/0
 nameif outside
 security-level 80
 ip address 192.16.32.1 255.255.255.0
 ipv6 address 2001:192:16:32::1/64
 isis
 ipv6 router isis
```

```
router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 redistribute static
 maximum-paths 5
address-family ipv6 unicast
 maximum-paths 6
exit-address-family
```

Interface passive

```
 iRouter ---------- ASA ------------ oRouter


 ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0
  ipv6 address 2001:192:16:32::1/64
  isis
  ipv6 router isis


 interface GigabitEthernet0/1
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0
  ipv6 address 2001:172:16:32::1/64
  isis
  ipv6 router isis


 interface GigabitEthernet0/2
  nameif dmz
  security-level 0
  ip address 40.40.50.1 255.255.255.0
  ipv6 address 2040:95::1/64


 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  redistribute isis level-2 into level-1 route-map RMAP
  passive-interface default

IOS Configuration
 iRouter
  interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
  isis priority 120

 iRouter
 interface GigabitEthernet0/1
  ip address 172.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:26:32::3/64
```

```
 ipv6 router isis

iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 metric-style wide

oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis

oRouter
interface GigabitEthernet0/1
 ip address 192.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:26:32::3/64
 ipv6 router isis

oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide
```

Authentication (Authentification)

```
ASA ------------ Router

ASA Configuration

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
 ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
 isis
 ipv6 router isis
 isis authentication key cisco#123 level-2
 isis authentication mode md5


interface GigabitEthernet0/0.301
 nameif outside
 security-level 80
 ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
 ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
 isis
 ipv6 router isis


router isis
 net 49.1234.2005.2005.2005.00
 metric-style wide
 authentication mode md5
 authentication key cisco#123 level-2

IOS Configuration
iRouter
```

```
interface GigabitEthernet0/0
 ip address 172.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:16:32::3/64
 ipv6 enable
 ipv6 router isis
 isis authentication mode md5
 isis authentication key-chain KeyChain level-2
 isis priority 120
 isis ipv6 metric 600


iRouter
key chain KeyChain
 key 1
  key-string cisco#123


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 authentication mode md5
 authentication key-chain KeyChain level-2
```

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.