

OSPF

Ce chapitre décrit comment configurer l'ASA pour acheminer les données, effectuer l'authentification et redistribuer les informations de routage à l'aide du protocole de routage Open Shortest Path First (OSPF).

- Routage OSPF, à la page 1
- Directives pour OSPF, à la page 5
- Configurer le protocole OSPFv2, à la page 8
- Configurer l'ID de routeur OSPFv2, à la page 11
- Personnaliser le protocole OSPFv2, à la page 13
- Configurer le protocole OSPFv3, à la page 33
- Configurer le redémarrage progressif, à la page 44
- Exemple de protocole OSPFv2, à la page 49
- Exemples de protocole OSPFv3, à la page 51
- Supervision OSPF, à la page 52
- Historique OSPF, à la page 54

Routage OSPF

OSPF est un protocole de routage de passerelle intérieure qui

- utilise des états de liaison plutôt que des vecteurs de distance pour la sélection de chemin,
- propage des annonces d'état de liaison plutôt que des mises à jour de la table de routage, et
- converge plus rapidement que les réseaux RIP parce que seuls les LSA sont échangés au lieu des tableaux de routage complets.

Fonctionnalités et caractéristiques d'OSPF

OSPF utilise un algorithme d'état de liens pour créer et calculer le chemin le plus court vers toutes les destinations connues. Chaque routeur d'une zone OSPF contient une base de données d'états de liaison identique, qui est une liste de chacune des interfaces utilisables et des voisins accessibles du routeur.

Les avantages d'OSPF par rapport à RIP comprennent les caractéristiques suivantes :

- Les mises à jour de la base de données d'états de liens OSPF sont envoyées moins fréquemment que les mises à jour RIP, et la base de données d'états de liens est mise à jour instantanément, plutôt que lentement, à mesure que les informations périmées expirent.

- Les décisions de routage sont basées sur le coût, qui est une indication du surdébit nécessaire pour envoyer des paquets sur une certaine interface. ASA calcule le coût d'une interface en fonction de la bande passante du lien plutôt que du nombre de sauts vers la destination. Le coût peut être configuré pour préciser les chemins privilégiés.

L'inconvénient des algorithmes du chemin le plus court d'abord est qu'ils nécessitent beaucoup de cycles du processeur et de mémoire.

L'ASA peut exécuter deux processus du protocole OSPF simultanément sur différents ensembles d'interfaces. Vous pourriez souhaiter exécuter deux processus si vous avez des interfaces qui utilisent les mêmes adresses IP (la NAT permet à ces interfaces de coexister, mais OSPF ne permet pas le chevauchement d'adresses). Ou vous pouvez exécuter un processus à l'intérieur et un autre à l'extérieur et redistribuer un sous-ensemble de routes entre les deux processus. De même, vous devrez peut-être séparer les adresses privées des adresses publiques.

Vous pouvez redistribuer les routages dans un processus de routage OSPF à partir d'un autre processus de routage OSPF, d'un processus de routage IP ou de routes statiques et connectées configurées sur des interfaces activées pour OSPF.

L'ASA prend en charge les fonctionnalités OSPF suivantes :

- Routages intra-zones, inter-zones et externes (type I et type II).
- Liens virtuels.
- Inondation de LSA.
- Authentification pour les paquets OSPF (authentification par mot de passe et authentification MD5).
- Configuration de l'ASA en tant que routeur désigné ou routeur de secours désigné. L'ASA peut également être configuré comme un ABR.
- Zones tampons et zones tampons.
- Routeur de frontière de zone, filtrage LSA de type 3

OSPF prend en charge MD5 et l'authentification du voisin en texte clair. L'authentification doit être utilisée avec tous les protocoles de routage lorsque cela est possible, car la redistribution de routage entre OSPF et d'autres protocoles (comme RIP) peut être utilisée par des agresseurs pour détourner les informations de routage.

Si la NAT est utilisée, si OSPF fonctionne sur des zones publiques et privées, et si le filtrage d'adresses est requis, vous devez exécuter deux processus OSPF, un pour les zones publiques et un pour les zones privées.

Un routeur qui a des interfaces dans plusieurs zones est appelé routeur de frontière de zone (ABR). Un routeur qui agit comme une passerelle pour redistribuer le trafic entre les routeurs utilisant OSPF et les routeurs utilisant d'autres protocoles de routage est appelé un routeur de frontière de système autonome (ASBR).

Un ABR utilise des LSA pour envoyer des informations sur les routes disponibles à d'autres routeurs OSPF. Le filtrage des LSA de type 3 d'un ABR vous permet de disposer de zones privées et publiques distinctes, l'ASA agissant comme ABR. Les LSA de type 3 (routes inter-zones) peuvent être filtrées d'une zone à une autre, ce qui vous permet d'utiliser la NAT et l'OSPF ensemble sans annoncer de réseaux privés.

Remarque Seuls les LSA de type 3 peuvent être filtrés. Si vous configurez l'ASA comme ASBR dans un réseau privé, il enverra des LSA de type 5 décrivant les réseaux privés, qui seront inondés à l'ensemble du système autonome, y compris les zones publiques.

Si la NAT est utilisée, mais qu'OSPF s'exécute uniquement dans les zones publiques, les routes vers les réseaux publics peuvent être redistribuées dans le réseau privé, soit par défaut, soit sous forme de LSA externes de type 5. Cependant, vous devez configurer des routes statiques pour les réseaux privés protégés par ASA. De plus, vous ne devez pas combiner réseaux publics et réseaux privés sur la même interface ASA.

Vous pouvez avoir deux processus de routage OSPF, un processus de routage RIP et un processus de routage EIGRP en même temps sur l'ASA.

Prise en charge OSPF pour les paquets Fast Hello

La prise en charge OSPF pour les paquets Fast Hello

- permet de configurer l'envoi de paquets Hello par intervalles inférieurs à une seconde, et
- entraîne une convergence plus rapide dans un réseau OSPF (Open Shortest Path First).

Conditions préalables à la configuration des paquets Hello rapide d'OSPF

OSPF doit déjà être configuré dans le réseau ou configuré en même temps que la fonction de prise en charge OSPF des paquets Fast Hello.

À propos de la prise en charge OSPF pour les paquets Hello rapides

Les concepts clés liés à la prise en charge OSPF pour les paquets Fast Hello et aux avantages des paquets OSPF Fast Hello sont décrits ci-dessous :

Intervalle Hello et intervalle mort OSPF

L'intervalle Hello et l'intervalle mort d'OSPF sont des paramètres de temps configurables qui

- maintiennent la connectivité entre les voisins OSPF par des échanges réguliers de paquets Hello,
- détectent les défaillances de voisins lorsque les paquets Hello ne sont pas reçus dans les délais spécifiés, et
- doivent être cohérents sur tous les routeurs d'un même réseau pour assurer un fonctionnement adéquat.

Détails de la configuration des intervalles Hello et des intervalles morts

Les paquets Hello OSPF sont des paquets qu'un processus OSPF envoie à ses voisins OSPF pour maintenir la connectivité avec ces derniers. Les paquets Hello sont envoyés à un intervalle configurable (en secondes). Les valeurs par défaut sont de 10 secondes pour une liaison Ethernet et de 30 secondes pour une liaison non diffusée.

Les paquets Hello comprennent une liste de tous les voisins pour lesquels un paquet Hello a été reçu dans l'intervalle mort. L'intervalle mort est également un intervalle configurable (en secondes). Par défaut, il est

quatre fois supérieur à la valeur de l'intervalle Hello. La valeur de tous les intervalles Hello doit être la même dans un réseau. De même, la valeur de tous les intervalles morts doit être la même dans un réseau.

Ces deux intervalles fonctionnent ensemble pour maintenir la connectivité en indiquant que la liaison est opérationnelle. Si un routeur ne reçoit pas de paquet Hello d'un voisin dans l'intervalle mort, il déclarera ce voisin en panne.

Paquets Hello rapides OSPF

Les paquets Hello rapides d'OSPF sont des paquets Hello qui

- sont envoyés à des intervalles inférieurs à 1 seconde,
- sont obtenus à l'aide de la commande OSPF dead-interval avec un intervalle d'inactivité défini à 1 seconde, et
- utilisent une valeur de multiplicateur Hello définie sur le nombre de paquets Hello envoyés pendant cette seconde.

Comportement des paquets Hello rapides

Lorsque des paquets Hello rapides sont configurés sur l'interface, ces comportements se produisent :

- L'intervalle Hello annoncé dans les paquets Hello envoyés par cette interface est réglé à 0.
- L'intervalle Hello dans les paquets Hello reçus sur cette interface est ignoré.

L'intervalle mort doit être cohérent sur un segment, qu'il soit défini à 1 seconde (pour les paquets Hello rapides) ou à une autre valeur. Le multiplicateur Hello n'a pas besoin d'être le même pour tout le segment tant qu'au moins un paquet Hello est envoyé dans l'intervalle mort.

Pour comprendre les paquets Hello rapides, vous devez déjà comprendre la relation entre les paquets Hello d'OSPF et l'intervalle mort. Consultez Intervalle Hello et intervalle mort OSPF, à la page 3.

Avantages des paquets Hello rapides OSPF

Un paquet Hello rapide est une fonctionnalité du protocole OSPF qui

- réduit le temps de convergence du réseau en permettant aux routeurs de détecter plus rapidement les modifications dans le réseau,
- permet la détection rapide des voisins perdus en une seconde, et
- améliore la fiabilité dans les environnements LAN où la perte de voisin peut ne pas être détectée au niveau de la couche physique ou de la couche liaison de données de l'Open Systems Interconnection (OSI).

L'intérêt des paquets Hello rapides OSPF est que votre réseau OSPF peut réagir rapidement aux modifications, ce qui réduit les temps d'arrêt et améliore la stabilité globale du réseau. Cette fonctionnalité est particulièrement utile dans les scénarios où les routeurs ne peuvent pas détecter les voisins perdus par les méthodes traditionnelles, ce qui permet à OSPF de maintenir des tables de routage précises.

Si un routeur sur un segment de réseau local (LAN) est hors tension ou déconnecté et que les couches physique et liaison de données ne signalent pas la perte du voisin, les paquets Hello rapides OSPF détecteront la disparition du voisin en une seconde.

Différences d'implémentation entre OSPFv2 et OSPFv3

Une distinction de protocole est une catégorie de protocole qui

- empêche la rétrocompatibilité entre OSPFv2 et OSPFv3,
- nécessite que les deux versions d'OSPF fonctionnent simultanément pour le routage IPv4 et IPv6, et
- permet à OSPFv2 et OSPFv3 de coexister sans interagir l'un avec l'autre.

Fonctionnalités supplémentaires d'OSPFv3

Les fonctionnalités supplémentaires fournies par OSPFv3 sont les suivantes :

- Traitement du protocole par liaison
- Suppression de la sémantique d'adressage.
- Ajout de la portée de submersion.
- Prise en charge de plusieurs instances par lien.
- Utilisation de l'adresse locale de lien IPv6 pour la découverte de voisin et d'autres fonctionnalités.
- Les LSA sont exprimées en tant que préfixe et longueur de préfixe.
- Ajout de deux types de LSA.
- Gestion des types de LSA inconnus
- Prise en charge de l'authentification par la norme IPsec ESP pour le trafic de protocole de routage OSPFv3, comme le spécifie la RFC 4552.

Directives pour OSPF

Lignes directrices relatives au mode contextuel

OSPFv2 prend en charge les modes à contexte unique et multiple.

- Les instances OSPFv2 ne peuvent pas former de contiguïtés entre elles dans les interfaces partagées car, par défaut, l'échange inter-contextes du trafic de multidiffusion n'est pas pris en charge sur les interfaces partagées. Cependant, vous pouvez utiliser la configuration de voisin statique sous la configuration de processus OSPFv2 sous le processus OSPFv2 pour faire apparaître le voisinage OSPFv2 sur une interface partagée.
- OSPFv2 inter-contexte sur des interfaces distinctes est pris en charge.
- **(Pour la topologie point à point)** En mode de contexte multiple, vous pouvez configurer des voisins OSPFv2 statiques pour annoncer les routes OSPFv2 sur un réseau point à point de non-diffusion. Pour une formation réussie de l'adjacence OSPF, lorsque vous supprimez et reconfigurez OSPF sur une interface partagée, exécutez les commandes dans cet ordre : supprimez la configuration OSPF à l'aide de **no router <OSPF name>**, puis retirez la configuration OSPF point à point sans diffusion sur l'interface à l'aide de **no OSPF network point-to-point non-broadcast**. Lorsque vous reconfigurez OSPF sur l'interface partagée, configurez le routeur OSPF en utilisant **router <OSPF name>**, puis configurez l'interface avec **OSPF network point-to-point non-broadcast**.

- OSPFv3 prend en charge le mode unique uniquement.

Lignes directrices d'authentification par chaîne de clé

OSPFv2 prend en charge l'authentification par chaîne de clés en mode unique et multiple, en modes physique et virtuel. Cependant, en mode multiple, vous pouvez configurer la chaîne de clés uniquement en mode contextuel.

- Les clés pivotantes ne s'appliquent qu'au protocole OSPFv2. L'authentification de zone OSPF avec chaîne de clé n'est pas prise en charge.
- L'authentification MD5 existante sans plage temporelle dans OSPFv2 est toujours prise en charge avec les nouvelles clés alternées.
- Bien que la plateforme prenne en charge les algorithmes cryptographiques SHA1 et MD5, seul l'algorithme cryptographique MD5 est utilisé pour l'authentification.

Lignes directrices sur le mode pare-feu

OSPF ne prend en charge que le mode pare-feu routé. OSPF ne prend pas en charge le mode de pare-feu transparent.

Directives Basculement

OSPFv2 et OSPFv3 prennent en charge le Basculement sans état.

Lignes directrices IPv6

OSPFv2 ne prend pas en charge IPv6, tandis qu'OSPFv3 fournit une prise en charge d'IPv6 avec des capacités d'authentification et de routage spécifiques.

- OSPFv2 ne prend pas en charge IPv6.
- OSPFv3 prend en charge IPv6.
- OSPFv3 utilise IPv6 pour l'authentification.
- L'ASA installe les routages OSPFv3 dans le RIB IPv6, à condition qu'il s'agisse du meilleur routage.
- Les paquets OSPFv3 peuvent être filtrés à l'aide des listes de contrôle d'accès IPv6 dans la commande **capture**.

Paquets Hello OSPFv3 et GRE

En règle générale, le trafic OSPF ne passe pas par le tunnel GRE. Lorsqu'OSPFv3 sur IPv6 est encapsulé à l'intérieur de GRE, la validation de l'en-tête IPv6 pour les vérifications de sécurité telles que la destination de multidiffusion échoue. Le paquet est abandonné en raison de la validation de vérification de sécurité implicite, car ce paquet a une multidiffusion IPv6 de destination.

- Vous pouvez définir une règle de préfiltre pour contourner le trafic GRE. Cependant, avec la règle de préfiltre, les paquets internes ne seraient pas interrogés par le moteur d'inspection.

Lignes directrices de mise en grappe

OSPFv2 et OSPFv3 ont des limites et des comportements spécifiques dans les environnements de mise en grappe.

- Le chiffrement OSPFv3 n'est pas pris en charge. Un message d'erreur s'affiche si vous essayez de configurer le chiffrement OSPFv3 dans un environnement de mise en grappe.
- En mode d'interface étendue, le routage dynamique n'est pas pris en charge sur les interfaces de gestion uniquement.
- En mode d'interface individuel, veillez à définir les unités de contrôle et de données comme des voisins OSPFv2 ou OSPFv3.
- En mode d'interface individuelle, les contiguïtés OSPFv2 ne peuvent être établies qu'entre deux contextes sur une interface partagée sur l'unité de contrôle. La configuration de voisins statiques est prise en charge uniquement sur les liaisons point à point; par conséquent, une seule instruction voisin est autorisée sur une interface.
- Lorsqu'un changement de rôle de contrôle se produit dans la grappe, un comportement spécifique se produit en fonction du mode d'interface. En mode d'interface étendue, le processus du routeur est actif uniquement sur l'unité de contrôle et est à l'état suspendu sur les unités de données. Chaque unité de grappe a le même ID de routeur, car la configuration a été synchronisée à partir de l'unité de contrôle. Par conséquent, un routeur voisin ne remarque aucun changement dans l'ID de routeur de la grappe lors d'un changement de rôle. En mode d'interface individuelle, le processus du routeur est actif sur toutes les unités de la grappe. Chaque unité de grappe choisit son propre ID de routeur dans l'ensemble de grappes configuré. Une modification du rôle de contrôle dans la grappe ne modifie en rien la topologie de routage.

Commutation multiprotocole par étiquette (MPLS) et Lignes directrices OSPF

Lorsqu'un routeur configuré pour MPLS envoie des paquets de mise à jour d'état de liaison (LS) qui contiennent des publicités d'état de liaison (LSA) de type 10 couvrantes qui comprennent un en-tête MPLS, l'authentification échoue et le périphérique abandonne en mode silencieux les paquets de mise à jour plutôt que d'en accuser réception. Finalement, le routeur homologue mettra fin à la relation de voisin, car il n'a reçu aucun accusé de réception.

- Désactivez la capacité d'opacité sur l'ASA pour vous assurer que la relation de voisin reste stable :

```
router ospf process_ID_number
no nsf ietf helper
no capability opaque
```

Ces lignes directrices s'appliquent aux environnements MPLS dans lesquels les LSA opaques peuvent entraîner des échecs d'authentification.

Remarque Les modèles Firepower 4100/9300 peuvent avoir une latence élevée lors de l'utilisation de MPLS, car ils n'ont pas suffisamment d'équilibrage de la charge sur plusieurs files d'attente de réception.

Lignes directrices relatives à la redistribution des voies de routage

La redistribution des voies de routage avec des listes de préfixes et entre les domaines de routage nécessite des considérations de configuration spécifiques.

- La redistribution des cartes de routage avec la liste de préfixes IPv4 sur OSPFv2 est prise en charge. Toutefois, la redistribution des cartes de routage avec la liste de préfixes IPv6 sur OSPFv3 n'est pas prise en charge. Utilisez une liste d'accès dans la carte de routage sur OSPF pour la redistribution.

- Lorsqu'OSPF est configuré sur un périphérique qui fait partie du réseau EIGRP ou inversement, assurez-vous que le routeur OSPF est configuré pour baliser la voie de routage (le protocole EIGRP ne prend pas encore en charge la balise de routage). Lors de la redistribution d'OSPF dans EIGRP et d'EIGRP dans OSPF, une boucle de routage se produit lorsqu'il y a une panne sur l'une des liaisons ou des interfaces ou même lorsque l'expéditeur de la route est en panne. Pour empêcher la redistribution des routages d'un domaine vers le même domaine, un routeur peut marquer un routage qui appartient à un domaine pendant qu'il redistribue, et ces routages peuvent être filtrés sur le routeur distant en se basant sur la même balise. Comme les routes ne seront pas installées dans la table de routage, elles ne seront pas redistribuées dans le même domaine.

Lignes directrices supplémentaires

OSPFv2 et OSPFv3 prennent en charge diverses fonctionnalités et ont des limites spécifiques dans différents scénarios de déploiement.

- OSPFv2 et OSPFv3 prennent en charge plusieurs instances sur une interface.
- OSPFv3 prend en charge le chiffrement par le biais des en-têtes ESP dans un environnement sans grappe.
- OSPFv3 prend en charge le chiffrement sans charge utile.
- OSPFv2 prend en charge les mécanismes de redémarrages progressifs NSF de Cisco et IETF NSF tels que définis dans les RFC 4811, 4812 et 3623 respectivement.
- OSPFv3 prend en charge le mécanisme de redémarrage progressif tel que défini dans la RFC 5187.
- Il y a une limite au nombre de routages intra-zone (type 1) qui peuvent être distribués. Pour ces routes, un seul LSA de type 1 contient tous les préfixes. Comme le système a une limite de 35 Ko pour la taille des paquets, un paquet de 3 000 routages dépasse la limite. Considérez 2900 routes de type 1 comme le nombre maximal pris en charge.
- Pour éviter les oscillations de contiguïté dues aux mises à jour de routage abandonnées si la mise à jour de routage est supérieure à la MTU minimale sur le lien, configurez la même MTU sur les interfaces des deux côtés du lien.
- L'ASA virtuel ne peut pas utiliser les protocoles de routage interne dynamique comme EIGRP et OSPF en raison de la nature du routage dans le nuage Azure. La table de routage effective détermine le saut suivant, que le client virtuel ait ou non une route statique/dynamique configurée. Actuellement, vous ne pouvez pas afficher la table de routage effective ou la table de routage du système.
- OSPFv3 abandonne la mise à jour LS si la taille des paquets dépasse 8190. Par conséquent, le voisinage est interrompu. Ainsi, configurez le commutateur avec la commande « ospfv3 MTU-ignore » pour éviter la fin du voisinage.

Configurer le protocole OSPFv2

Cette section décrit comment activer un processus OSPFv2 sur l'ASA.

Après avoir activé le protocole OSPFv2, vous devez définir une carte de routage. Pour en savoir plus, consultez Définir une carte de routage. Ensuite, vous générez une route par défaut. Pour en savoir plus, consultez Configurer une route statique.

Après avoir défini une carte de routage pour le processus OSPFv2, vous pouvez la personnaliser selon vos besoins particuliers. Pour savoir comment personnaliser le processus OSPFv2 sur l'ASA, consultez Personnaliser le protocole OSPFv2, à la page 13.

Pour activer le protocole OSPFv2, vous devez créer un processus de routage OSPFv2, spécifier la plage d'adresses IP associées au processus de routage, puis attribuer les ID de zone associés à cette plage d'adresses IP.

Vous pouvez activer jusqu'à deux instances de processus OSPFv2. Chaque processus OSPFv2 a ses propres zones et réseaux associés.

Pour activer le processus OSPFv2, procédez comme suit.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.

Dans le volet OSPF Setup (Configuration du protocole OSPF), vous pouvez activer les processus OSPF, configurer les zones et les réseaux OSPF, et définir la synthèse des routes OSPF.

Étape 2 Les trois onglets dans ASDM utilisés pour activer OSPF sont les suivants :

- L'onglet Process Instances (Instances de processus) vous permet d'activer jusqu'à deux instances de processus OSPF pour chaque contexte. Le mode de contexte unique et le mode de contexte multiple sont tous deux pris en charge. Après avoir coché la case **Enable Each OSPF Process** (Activer chaque processus OSPF), vous pouvez saisir un identifiant numérique unique pour ce processus OSPF. Cet ID de processus est utilisé en interne et n'a pas besoin de correspondre à l'ID de processus OSPF sur d'autres appareils OSPF; les valeurs valides sont comprises entre 1 et 65535. Chaque processus OSPF a ses propres zones et réseaux associés.

  Si vous cliquez sur **Advanced** (Avancé), la boîte de dialogue Edit OSPF Process Advanced Properties (Modifier les propriétés avancées du processus OSPF) apparaît. À partir de là, vous pouvez configurer l'ID de routeur, les réserves d'adresses IP de la grappe dans la mise en grappe de l'interface individuelle ou de l'EtherChannel étendu, les modifications de contiguïté, les distances de route administratives, les minuteries et les paramètres d'origine des renseignements par défaut pour chaque processus OSPF. .

- L'onglet Area/Networks (Zone/Réseaux) vous permet d'afficher les zones et les réseaux qu'elles incluent pour chaque processus OSPF sur l'ASA. À partir de cet onglet, vous pouvez afficher l'ID de zone, le type de zone et le type d'authentification défini pour la zone. Pour ajouter ou modifier une zone ou un réseau OSPF, consultez Configurer les paramètres de zone OSPFv2, à la page 21 pour de plus amples renseignements.

- L'onglet Route Summarization (Synthèse des routes) vous permet de configurer un ABR. Dans OSPF, un ABR annoncera des réseaux d'une zone dans une autre zone. Si les numéros de réseau d'une zone sont affectés de manière à ce qu'ils soient contigus, vous pouvez configurer l'ABR pour annoncer une route récapitulative qui inclut tous les réseaux individuels de la zone qui entrent dans la plage spécifiée. Consultez Configurer la synthèse des routes entre les zones OSPFv2, à la page 17 pour de plus amples renseignements.

Configurer une chaîne de clés pour l'authentification

Pour améliorer la sécurité et la protection des données des périphériques, vous pouvez activer des clés changeantes pour l'authentification des homologues IGP. Les clés pivotantes empêchent tout utilisateur malveillant de deviner les clés utilisées pour l'authentification du protocole de routage, protégeant ainsi le réseau contre les annonces de routage incorrect et la redirection du trafic. La modification fréquente des clés réduit le risque qu'elles finissent par être devinées. Lors de la configuration de l'authentification pour les protocoles de routage qui fournissent des chaînes de clés, configurez les clés d'une chaîne de clés pour qu'elles se chevauchent. Cela permet d'éviter la perte de communication à clé en raison de l'absence d'une clé active. Si la durée de vie de la clé expire et qu'aucune clé active n'est trouvée, OSPF utilise la dernière clé valide pour maintenir la contiguïté avec les homologues.

Cette section décrit comment créer une chaîne de clés pour l'authentification des homologues OSPF. Cette section couvre également les étapes pour ajouter ou modifier les attributs d'une chaîne de clés. Après avoir configuré un objet de chaîne de clés, vous pouvez l'utiliser pour définir l'authentification OSPFv2 pour une interface et pour une liaison virtuelle. Utilisez le même type d'authentification (MD5 ou chaîne de clé) et le même ID de clé pour les homologues afin d'établir une contiguïté réussie. Pour savoir comment définir l'authentification pour une interface, consultez Configurer les paramètres d'interface OSPFv2, à la page 17; pour une liaison virtuelle, consultez Configurer un lien virtuel dans OSPF, à la page 31.

Pour configurer une chaîne de clés, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Key Chain (Chaîne de clés)** .

Étape 2 Dans la section **Configure Key Chain** (Configurer la chaîne de clés), cliquez sur **Add** (Ajouter).

Étape 3 Saisissez le nom de la chaîne de clés dans la boîte de dialogue **Add Key Chain** (Ajouter une chaîne de clés), puis cliquez sur **OK**.

Le nom de la chaîne de clés créée est répertorié dans la grille **Configure Key Chain** (Configurer la chaîne de clés).

Étape 4 Sélectionnez le nom de la chaîne de clés dans la section **Configure Key Chain** (Configurer la chaîne de clés), et dans la section **Configure Key** (Configurer la clé), cliquez sur **Add** (Ajouter). Pour modifier une clé existante, sélectionnez le nom de la clé et cliquez sur **Edit** (Modifier).

La boîte de dialogue **Add Key** (Ajouter une clé) ou **Edit Key** (Modifier une clé) apparaît, selon l'action que vous avez sélectionnée.

Étape 5 Précisez l'identifiant de clé dans le champ **Key ID**.

La valeur de l'ID de clé peut être comprise entre 0 et 255. Utilisez la valeur 0 uniquement lorsque vous souhaitez signaler une clé non valide.

Remarque Vous ne pouvez pas modifier un ID de clé enregistré.

Étape 6 Dans la liste déroulante **Cryptographic Algorithm** (Algorithme cryptographique), choisissez **MD5**. MD5 est le seul algorithme pris en charge pour l'authentification de la chaîne de clés.

Étape 7 Sélectionnez le type de chiffrement en cliquant sur le bouton radio **Plain Text** (Texte brut) ou **Encrypted** (Chiffré), puis saisissez le mot de passe dans le champ **Authentication Key** (Clé d'authentification).

- Même si la chaîne de clé peut contenir 80 caractères, seul un maximum de 64 caractères est autorisé pour l'authentification OSPF.
- Les mots de passe ne peuvent pas être un seul chiffre ni ceux commençant par un chiffre suivi d'un espace. Par exemple, « 0 pass » ou « 1 » ne sont pas valides.

Étape 8 Fournissez les valeurs de durée de vie dans les champs **Accept Lifetime** (Accepter la durée de vie) et **Send Lifetime** (Envoyer la durée de vie) :

Vous pouvez spécifier l'intervalle de temps nécessaire pour que le périphérique accepte ou envoie la clé lors de l'échange de clés avec un autre périphérique. L'heure de fin peut correspondre à la durée absolue à laquelle la durée de vie de l'acceptation/envoi se termine ou n'expire jamais.

Voici les règles de validation pour les valeurs de début et de fin :

- La durée de vie de début ne peut pas être nulle lorsque la fin de vie est spécifiée.
- La durée de vie de début pour l'acceptation ou l'envoi de la durée de vie doit être antérieure à la fin de vie.

Étape 9 Pour enregistrer les attributs de la chaîne de clés, cliquez sur **OK**. Dans la page **Key Chain** (Chaîne de clés), cliquez sur **Appy** (Appliquer).

Prochaine étape

Vous pouvez maintenant appliquer la chaîne de clés configurée pour définir l'authentification OSPFv2 pour une interface et pour la liaison virtuelle.

- Configurer les paramètres d'interface OSPFv2, à la page 17
- Configurer un lien virtuel dans OSPF, à la page 31

Configurer l'ID de routeur OSPFv2

L'ID de routeur OSPF est utilisé pour identifier un appareil spécifique dans une base de données OSPF. Deux routeurs d'un système OSPF ne peuvent pas avoir le même ID de routeur.

Si un ID de routeur n'est pas configuré manuellement dans le processus de routage OSPF, le routeur configurera automatiquement un ID de routeur déterminé à partir de l'adresse IP la plus élevée d'une interface active. Lors de la configuration d'un ID de routeur, les voisins ne seront pas mis à jour automatiquement jusqu'à ce que le routeur ait échoué ou que le processus OSPF ait été effacé et que la relation de voisin ait été rétablie.

Configurer manuellement l'ID de routeur OSPF

Cette section décrit comment configurer manuellement l'ID de routeur dans le processus OSPFv2 sur l'ASA.

Procédure

Étape 1 Pour utiliser un ID de routeur fixe, utilisez la commande **router-id**.

router-id *ip-address*

Exemple :

```
ciscoasa(config-router)# router-id 193.168.3.3
```

Étape 2 Pour revenir au comportement précédent de l'ID de routeur OSPF, utilisez la commande **no router-id**.

no router-id *ip-address*

Exemple :

```
ciscoasa(config-router)# no router-id 193.168.3.3
```

Comportement de l'ID de routeur lors de la migration

Lors de la migration de la configuration OSPF d'un ASA, par exemple ASA 1 vers un autre ASA, par exemple l'ASA 2, le comportement suivant est observé en matière de sélection de l'ID du routeur :

1. L'ASA 2 n'utilise aucune adresse IP pour l'ID de routeur OSPF lorsque toutes les interfaces sont en mode d'arrêt. Les possibilités de configuration de l'ID de routeur lorsque toutes les interfaces sont à l'état « arrêt admin » ou en mode d'arrêt sont les suivantes :
   - Si l'ASA 2 n'a pas encore d'ID de routeur configuré, vous verrez ce message :

     `%OSPF: Router process 1 is not running, please configure a router-id` (% OSPF : le processus de routeur 1 n'est pas en cours d'exécution, veuillez configurer un identifiant de routeur)

     Après le déploiement de la première interface, l'ASA 2 utilisera l'adresse IP de cette interface comme ID de routeur.
   - Si l'ASA 2 a déjà configuré l'ID de routeur et que toutes les interfaces étaient à l'état « arrêt admin » lorsque la commande « no router-id » a été exécutée, l'ASA 2 utilisera l'ancien ID de routeur. L'ASA 2 utilise l'ancien ID de routeur, même si les adresses IP de l'interface créée sont modifiées, jusqu'à ce que la commande « clear ospf process » soit émise.
2. L'ASA 2 utilise un nouvel ID de routeur, alors que l'ASA 2 avait déjà configuré l'ID de routeur et qu'au moins une des interfaces n'était pas à l'état « arrêt admin » ou en mode d'arrêt lorsque la commande « no router-id » a été émise. L'ASA 2 utilisera le nouvel ID de routeur de l'adresse IP des interfaces même lorsque les interfaces sont à l'état « arrêt/arrêt ».

Personnaliser le protocole OSPFv2

Cette section explique comment personnaliser les processus OSPFv2.

Redistribuer les routes dans OSPFv2

L'ASA peut contrôler la redistribution des routes entre les processus de routage OSPFv2.



Remarque Si vous souhaitez redistribuer une route en définissant quelles routes du protocole de routage spécifié peuvent être redistribuées dans le processus de routage cible, vous devez d'abord générer une route par défaut. Consultez Configurer une route statique, puis définissez une carte de routage en fonction de Définir une carte de routage.

Pour redistribuer les routes statiques, connectées, RIP ou OSPFv2 dans un processus OSPFv2, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Redistribution**.

Le volet Redistribution affiche les règles de redistribution des routes d'un processus de routage vers un processus de routage OSPF. Vous pouvez redistribuer les routes détectées par RIP et OSPF dans le processus de routage EIGRP. Vous pouvez également redistribuer les routes statiques et connectées dans le processus de routage EIGRP. Vous n'avez pas besoin de redistribuer les routes statiques ou connectées si elles entrent dans la plage d'un réseau qui a été configuré par le biais de l'onglet Setup (Configurer) > Networks (Réseaux).

Étape 2 Cliquez sur **Add** ou **Edit** (ajouter ou modifier).

Sinon, le double-clic sur une entrée de tableau dans le volet Redistribution (le cas échéant) ouvre la boîte de dialogue Add/Edit OSPF Redistribution Entry (Ajouter/modifier une entrée de redistribution OSPF) pour l'entrée sélectionnée.



Remarque Toutes les étapes suivantes sont facultatives.

La boîte de dialogue Add/Edit OSPF Redistribution Entry (Ajouter/modifier une entrée de redistribution OSPF) vous permet d'ajouter une nouvelle règle de redistribution ou de modifier une règle de redistribution existante dans le tableau de redistribution. Certaines informations sur la règle de redistribution ne peuvent pas être modifiées lorsque vous modifiez une règle de redistribution existante.

Étape 3 Choisissez le processus OSPF associé à l'entrée de redistribution des routes. Si vous modifiez une règle de redistribution existante, vous ne pouvez pas modifier ce paramètre.

Étape 4 Choisissez le protocole source à partir duquel les routes sont redistribuées. Vous pouvez choisir l'une des options suivantes :

- Static (statique) : redistribue les routes statiques vers le processus de routage OSPF.

- Connected (Connecté) : redistribue les routes connectées (les routes sont établies automatiquement parce que l'adresse IP est activée sur l'interface) vers le processus de routage OSPF. Les routes connectées sont redistribuées en tant que routes externes vers l'AS.
- OSPF : redistribue les routes à partir d'un autre processus de routage OSPF. Choisissez l'ID de processus OSPF dans la liste. Si vous choisissez ce protocole, les options de correspondance de cette boîte de dialogue deviennent visibles. Ces options ne sont pas disponibles lors de la redistribution de routes statiques, connectées, RIP ou EIGRP. Passez à l'étape 5.
- RIP : redistribue les routes à partir du processus de routage RIP.
- BGP : redistribue les routes à partir du processus de routage BGP.
- EIGRP : redistribue les routes à partir du processus de routage EIGRP. Choisissez le numéro de système autonome du processus de routage EIGRP dans la liste.

Étape 5 Si vous avez choisi OSPF pour le protocole source, choisissez les conditions utilisées pour la redistribution des routes d'un autre processus de routage OSPF dans le processus de routage OSPF sélectionné. Ces options ne sont pas disponibles lors de la redistribution de routes statiques, connectées, RIP ou EIGRP. Les routages doivent correspondre à la condition sélectionnée pour être redistribués. Vous pouvez choisir une ou plusieurs des conditions de correspondance suivantes :

- Internal (Interne) : la route est interne à un AS spécifique.
- External 1 (Externe 1) : les routes sont externes au système autonome, mais importées dans OSPF en tant que routes externes de type 1.
- External 2 (Externe 2) : les routes sont externes au système autonome, mais importées dans OSPF en tant que routes externes de type 2.
- NSSA External 1 (NSSA Externe 1) : les routes sont externes au système autonome, mais importées dans OSPF en tant que routes externes NSSA de type 1.
- NSSA External 2 (NSSA Externe 2) : les routes sont externes au système autonome, mais importées dans OSPF en tant que routes externes NSSA de type 2.

Étape 6 Dans le champ **Metric Value** (Valeur de la mesure), saisissez la valeur de la mesure pour les routes redistribuées. Les valeurs valides sont comprises entre 1 et 16777214.

Lors de la redistribution d'un processus OSPF à un autre processus OSPF sur le même périphérique, la mesure sera transmise d'un processus à l'autre si aucune valeur de mesure n'est spécifiée. Lors de la redistribution d'autres processus vers un processus OSPF, la mesure par défaut est 20 lorsqu'aucune valeur de mesure n'est spécifiée.



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

Étape 7 Choisissez l'une des options suivantes pour le type de mesure.

- Si la mesure est une route externe de type 1, choisissez **1**.
- Si la mesure est une route externe de type 2, choisissez **2**.

Étape 8 Saisissez la valeur de la balise dans le champ **Tag Value** (Valeur de balise).

La valeur de la balise est une valeur décimale sur 32 bits associée à chaque route externe qui n'est pas utilisée par OSPF lui-même, mais qui peut être utilisée pour communiquer des informations entre ASBR. Les valeurs valides vont de 0 à 4294967295.

Étape 9 Cochez la case **Use Subnets** (Utiliser les sous-réseaux) pour activer la redistribution des routes divisées en sous-réseaux. Décochez cette case pour que seules les routes qui ne sont pas divisées en sous-réseaux soient redistribuées.

Étape 10 Choisissez le nom de la carte de routage à appliquer à l'entrée de redistribution dans la liste déroulante Route Map (Carte de routage).

Étape 11 Si vous devez ajouter ou configurer une carte de routage, cliquez sur **Manage** (Gérer).

La boîte de dialogue Configure Route Map (Configurer la carte de routage) apparaît.

Étape 12 Cliquez **Add** (Ajouter) ou **Edit** (Modifier) pour définir les routes du protocole de routage spécifié qui peuvent être redistribuées dans le processus de routage cible. Pour en savoir plus, consultez Définir une carte de routage.

Étape 13 Cliquez sur **OK**.

Configurer la synthèse des routes lors de la redistribution des routes dans OSPFv2

Lorsque les routages d'autres protocoles sont redistribués dans OSPF, chaque routage est annoncée individuellement dans un LSA externe. Cependant, vous pouvez configurer l'ASA pour annoncer une seule route pour toutes les routes redistribuées qui sont incluses pour une adresse et un masque réseau spécifiés. Cette configuration diminue la taille de la base de données d'états de liaison OSPF.

Les routes qui correspondent à la paire de masques d'adresses IP spécifiées peuvent être supprimées. La valeur de balise peut être utilisée comme valeur de correspondance pour contrôler la redistribution par le biais de cartes de routage.

Ajouter une adresse sommaire de route

Le volet Summary Address (Adresse sommaire) affiche des renseignements sur les adresses sommaires configurées pour chaque processus de routage OSPF.

Les routes apprises d'autres protocoles de routage peuvent être résumées. La métrique utilisée pour annoncer le résumé est la plus petite de toutes les routes spécifiques. Les routages récapitulatifs permettent de réduire la taille de la table de routage.

L'utilisation des routages récapitulatifs pour OSPF amène un ASBR OSPF à annoncer une route externe en tant qu'agrégat pour toutes les routes redistribuées qui sont couvertes par l'adresse. Seuls les routages d'autres protocoles de routage qui sont redistribués dans OSPF peuvent être résumés.

Remarque OSPF ne prend pas en charge l'adresse récapitulative 0.0.0.0 0.0.0.0.

Pour configurer l'annonce du logiciel sur une route récapitulative pour toutes les routes redistribuées incluses pour une adresse réseau et un masque, procédez comme suit :

Procédure

Étape 1 Dans la page d'accueil principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Summary Address (Adresse sommaire)**.

Étape 2 Cliquez sur **Add** (ajouter).

La boîte de dialogue Add OSPF Summary Address Entry (Ajouter une entrée d'adresse sommaire OSPF) s'affiche. Vous pouvez ajouter de nouvelles entrées aux entrées existantes dans le tableau d'adresses sommaires. Certains renseignements sur les adresses sommaires ne peuvent pas être modifiés lors de la modification d'une entrée existante.

Étape 3 Choisissez l'ID de processus OSPF spécifié associé à l'adresse sommaire dans la liste déroulante OSPF Process (Processus OSPF). Vous ne pouvez pas modifier ces renseignements lors de la modification d'une entrée existante.

Étape 4 Dans le champ **IP Address** (Adresse IP), saisissez l'adresse IP de l'adresse sommaire. Vous ne pouvez pas modifier ces renseignements lors de la modification d'une entrée existante.

Étape 5 Dans la liste déroulante **Netmask** (Masque réseau), choisissez le masque réseau pour l'adresse sommaire. Vous ne pouvez pas modifier ces renseignements lors de la modification d'une entrée existante.

Étape 6 Cochez la case **Advertise** (Annoncer) pour annoncer la route récapitulative. Décochez cette case pour supprimer les routages qui relèvent de l'adresse résumée. Par défaut, cette case est cochée.

La valeur Tag (Balise) affiche une valeur décimale de 32 bits associée à chaque route externe. Cette valeur n'est pas utilisée par OSPF lui-même, mais peut être utilisée pour communiquer des informations entre ASBR.

Étape 7 Cliquez sur **OK**.

Ajouter ou modifier une adresse sommaire OSPF

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Route Summarization** (Synthèse de routage).

La boîte de dialogue Add/Edit a Route Summarization Entry (Ajouter/modifier une entrée de synthèse de routage) apparaît.

La boîte de dialogue Add/Edit a Route Summarization Entry (Ajouter/modifier une entrée de synthèse de routage) vous permet d'ajouter de nouvelles entrées ou de modifier les entrées existantes dans le tableau des adresses sommaires. Certains renseignements sur les adresses sommaires ne peuvent pas être modifiés lors de la modification d'une entrée existante.

Étape 3 Choisissez l'ID de processus OSPF spécifié associé à l'adresse sommaire dans la liste déroulante **OSPF Process** (Processus OSPF). Vous ne pouvez pas modifier ces renseignements lors de la modification d'une entrée existante.

Étape 4 Dans le champ **IP Address** (Adresse IP), saisissez l'adresse IP de l'adresse sommaire. Vous ne pouvez pas modifier ces renseignements lors de la modification d'une entrée existante.

Étape 5 Dans la liste déroulante **Netmask** (Masque réseau), saisissez le masque réseau pour l'adresse sommaire. Vous ne pouvez pas modifier ces renseignements lors de la modification d'une entrée existante.

Étape 6 Cochez la case **Advertise** (Annoncer) pour annoncer la route récapitulative. Décochez cette case pour supprimer les routages qui relèvent de l'adresse résumée. Par défaut, cette case est cochée.

Configurer la synthèse des routes entre les zones OSPFv2

La synthèse du routage est le regroupement d'adresses annoncées. Cette fonctionnalité permet d'annoncer une seule route récapitulative à d'autres zones par un routeur de délimitation de zone. Dans OSPF, un routeur de délimitation de zone annonce les réseaux d'une zone dans une autre zone. Si les numéros de réseau d'une zone sont affectés de manière à ce qu'ils soient contigus, vous pouvez configurer le routeur de délimitation de zone pour annoncer une route récapitulative qui inclut tous les réseaux individuels de la zone qui entrent dans la plage spécifiée.

Pour définir une plage d'adresses pour la synthèse du routage, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Route Summarization** (Synthèse de routage).

La boîte de dialogue Add/Edit a Route Summarization Entry (Ajouter/modifier une entrée de synthèse de routage) apparaît.

La boîte de dialogue Add/Edit a Route Summarization Entry (Ajouter/modifier une entrée de synthèse de routage) vous permet d'ajouter de nouvelles entrées ou de modifier les entrées existantes dans le tableau des adresses sommaires. Certains renseignements sur les adresses sommaires ne peuvent pas être modifiés lors de la modification d'une entrée existante.

Étape 3 Saisissez l'ID de zone OSPF dans le champ **Area ID** (ID de zone). Vous ne pouvez pas modifier ces renseignements lors de la modification d'une entrée existante.

Étape 4 Dans le champ **IP Address** (Adresse IP), saisissez l'adresse IP de l'adresse sommaire. Vous ne pouvez pas modifier ces renseignements lors de la modification d'une entrée existante.

Configurer les paramètres d'interface OSPFv2

Vous pouvez modifier certains paramètres OSPFv2 propres à l'interface, au besoin. Vous n'êtes pas tenu de modifier ces paramètres, mais les paramètres d'interface suivants doivent être cohérents sur tous les routeurs d'un réseau associé : l'intervalle Hello, l'intervalle de temps mort et la clé d'authentification. Si vous configurez l'un de ces paramètres, assurez-vous que les configurations de tous les routeurs de votre réseau ont des valeurs compatibles.

Dans ASDM, le volet Interface vous permet de configurer les propriétés de routage OSPF spécifiques à l'interface, telles que l'authentification des messages OSPF et les propriétés. Deux onglets vous aident à configurer les interfaces dans OSPF :

- L'onglet Authentication (Authentification) affiche les renseignements d'authentification OSPF pour les interfaces ASA.
- L'onglet Properties (Propriétés) affiche les propriétés OSPF définies pour chaque interface sous forme de tableau.

Pour configurer les paramètres d'interface OSPFv2, procédez comme suit :

Procédure

Étape 1 Cliquez sur l'onglet **Authentication** (Authentification) pour afficher les renseignements d'authentification OSPF pour les interfaces ASA. Un double clic sur une ligne du tableau ouvre la boîte de dialogue Edit OSPF Authentication Interface (Modifier l'interface d'authentification OSPF) pour l'interface sélectionnée.

Étape 2 Cliquez sur **Edit**.

La boîte de dialogue Edit OSPF Authentication Interface (Modifier l'interface d'authentification OSPF) apparaît. La boîte de dialogue Edit OSPF Interface Authentication (Modifier l'interface d'authentification OSPF) vous permet de configurer le type d'authentification et les paramètres OSPF pour l'interface sélectionnée.

Étape 3 Choisissez le type d'authentification en cliquant sur le bouton radio approprié :

- **No authentication** (Aucune authentification) pour désactiver l'authentification OSPF.
- **Area authentication, if defined** (Authentification de zone, si défini) (par défaut) pour utiliser le type d'authentification spécifié pour la zone. Consultez Configurer les paramètres de zone OSPFv2, à la page 21 pour en savoir plus sur la configuration de l'authentification de zone. L'authentification de zone est désactivée par défaut. Par conséquent, à moins que vous ayez déjà spécifié un type d'authentification de zone, les interfaces définies avec l'authentification de zone ont l'authentification désactivée jusqu'à ce que vous configuriez ce paramètre.
- **Password authentication** (Authentification par mot de passe) pour utiliser l'authentification par mot de passe en texte clair (non conseillé lorsque la sécurité est une préoccupation).
- **MD5 authentication** (Authentification MD5) pour utiliser l'authentification MD5.
- **Key chain authentication** (Authentification par chaîne de clés) pour utiliser l'authentification par chaîne de clés (conseillé). Consultez Configurer une chaîne de clés pour l'authentification, à la page 10 pour en savoir plus sur la configuration de la chaîne de clés pour l'authentification.

Étape 4 Si vous avez choisi l'authentification par mot de passe, dans la zone Authentication Password (Mot de passe d'authentification), saisissez le mot de passe :

a) Dans le champ Enter Password (Saisir le mot de passe), saisissez une chaîne de texte de huit caractères maximum.
b) Dans le champ Re-entrer Password (Saisir à nouveau le mot de passe), resaisissez le mot de passe.

Étape 5 Si vous avez choisi l'authentification de la chaîne de clés, saisissez le nom de la chaîne de clés dans le champ Enter Key chain name (Saisir le nom de la chaîne de clés).

Étape 6 Choisissez les paramètres pour les ID et les clés MD5 dans la zone ID, qui comprend les paramètres pour la saisie des clés et des paramètres MD5 lorsque l'authentification MD5 est activée. Tous les appareils de l'interface qui utilisent l'authentification OSPF doivent utiliser la même clé MD5 et le même ID.

a) Dans le champ Key ID (ID de clé), saisissez un identifiant de clé numérique. Les valeurs valides sont comprises entre 0 et 255. L'ID de clé s'affiche pour l'interface sélectionnée.

b) Dans le champ Key (Clé), saisissez une chaîne de caractères alphanumériques d'une durée maximale de 16 octets. La clé s'affiche pour l'interface sélectionnée.
c) Cliquez sur **Add** (Ajouter) ou **Delete** (Supprimer) pour ajouter ou supprimer la clé MD5 spécifiée au tableau d'ID et de clé MD5.

Étape 7 Cliquez sur **OK.**

Étape 8 Cliquez sur l'onglet **Properties** (Propriétés).

Étape 9 Sélectionnez l'interface que vous souhaitez modifier. Un double clic sur une ligne du tableau ouvre la boîte de dialogue de l'onglet Properties (Propriétés) de l'interface sélectionnée.

Étape 10 Cliquez sur **Edit**.

La boîte de dialogue Edit OSPF Interface Properties (Modifier les propriétés de l'interface OSPF) apparaît. Le champ Interface affiche le nom de l'interface pour laquelle vous configurez les propriétés OSPF. Vous ne pouvez pas modifier ce champ.

Étape 11 Cochez ou décochez la case **Broadcast** (Diffusion) pour préciser que l'interface est une interface de diffusion.

Par défaut, cette case est cochée pour les interfaces Ethernet. Décochez cette case pour désigner l'interface comme une interface point à point de non-diffusion. Définir une interface comme point à point, sans diffusion, vous permet de transmettre des routes OSPF sur des tunnels VPN.

Lorsqu'une interface est configurée comme interface point à point sans diffusion, les restrictions suivantes s'appliquent :

- Vous ne pouvez définir qu'un seul voisin pour l'interface.
- Vous devez configurer manuellement le voisin. Consultez Définir les voisins OSPFv2 statiques, à la page 26 pour de plus amples renseignements.
- Vous devez définir une voie de routage statique pointant vers le point terminal de chiffrement. Consultez Configurer une route statique pour de plus amples renseignements.
- Si OSPF sur un tunnel est exécuté sur l'interface, OSPF standard avec un routeur en amont ne peut pas être exécuté sur la même interface.
- Vous devez lier la carte de chiffrement à l'interface avant de spécifier le voisin OSPF pour vous assurer que les mises à jour OSPF passent par le tunnel VPN. Si vous liez la carte de chiffrement à l'interface après avoir précisé le voisin OSPF, utilisez la commande **clear local-host all** pour effacer les connexions OSPF afin que les contiguïtés OSPF puissent être établies sur le tunnel VPN.

Étape 12 Configurez les options suivantes :

- Saisissez une valeur dans le champ Cost (Coût) qui détermine le coût d'envoi d'un paquet par l'interface. La valeur par défaut est 10.
- Dans le champ Priority (Priorité), saisissez la valeur de priorité du routeur OSPF.

  Lorsque deux routeurs se connectent à un réseau, tous deux tentent de devenir le routeur désigné. Le périphérique ayant la priorité de routeur la plus élevée devient le routeur désigné. En cas d'égalité, le routeur ayant l'ID de routeur le plus élevé devient le routeur désigné.

  Les valeurs valides pour ce paramètre sont comprises entre 0 et 255. La valeur par défaut est 1. Si vous saisissez 0 pour ce paramètre, le routeur ne pourra pas devenir le routeur désigné ou le routeur de secours désigné. Ce paramètre ne s'applique pas aux interfaces configurées comme interfaces point à point non de diffusion.

En mode de contexte multiple, pour les interfaces partagées, spécifiez 0 pour vous assurer que le périphérique ne devienne pas le routeur désigné. Les instances OSPFv2 ne peuvent pas former de contiguïtés entre elles sur les interfaces partagées.

- Cochez ou décochez la case **MTU Ignore** (Ignorer la MTU).

  OSPF vérifie si les voisins utilisent la même MTU sur une interface commune. Cette vérification est effectuée lorsque les voisins échangent des paquets DBD. Si la MTU de réception dans le paquet DBD est supérieure à la MTU IP configurée sur l'interface entrante, la contiguïté OSPF ne sera pas établie.

- Cochez ou décochez la case **Database Filter** (Filtre de base de données).

  Utilisez ce paramètre pour filtrer l'interface LSA sortante pendant la synchronisation et l'inondation. Par défaut, OSPF inonde les nouveaux LSA sur toutes les interfaces dans la même zone, sauf l'interface sur laquelle le LSA arrive. Dans une topologie entièrement maillée, cette inondation peut gaspiller de la bande passante et entraîner une utilisation excessive de la liaison et de la CPU. Cocher cette case empêche l'inondation OSPF du LSA sur l'interface sélectionnée.

Étape 13 (Facultatif) Cliquez sur **Advanced** (Avancé) pour afficher la boîte de dialogue Edit OSPF Advanced Interface Properties (Modifier les propriétés de l'interface avancée OSPF), qui vous permet de modifier les valeurs de l'intervalle Hello OSPF, de l'intervalle de retransmission, du délai de transmission et de l'intervalle de temps mort.

Généralement, vous n'avez qu'à modifier ces valeurs par défaut si vous rencontrez des problèmes OSPF sur votre réseau.

Étape 14 Dans la section Intervals (Intervalles), saisissez des valeurs pour les éléments suivants :

- L'intervalle Hello, qui spécifie l'intervalle, en secondes, entre les paquets Hello envoyés sur une interface. Plus l'intervalle Hello est petit, plus les changements topologiques sont détectés rapidement, mais plus de trafic est envoyé sur l'interface. Cette valeur doit être la même pour tous les routeurs et serveurs d'accès sur une interface donnée. Les valeurs valides vont de 1 à 8 192 secondes. La valeur par défaut est 10 secondes.

- L'intervalle de retransmission, qui spécifie le temps en secondes entre les retransmissions de LSA pour les contiguïtés qui appartiennent à l'interface. Lorsqu'un routeur envoie un LSA à son voisin, il le conserve jusqu'à ce qu'il reçoive l'accusé de réception. Si le routeur ne reçoit aucun accusé de réception, il renvoie le LSA. Soyez prudent lors de la définition de cette valeur, sinon une retransmission inutile peut en résulter. La valeur doit être supérieure pour les lignes série et les liaisons virtuelles. Les valeurs valides vont de 1 à 8 192 secondes. La valeur par défaut est de 5 secondes.

- Le délai de transmission, qui spécifie le temps estimé, en secondes, nécessaire pour envoyer un paquet LSA sur l'interface. L'âge des LSA dans le paquet de mise à jour est augmenté de la quantité spécifiée par ce champ avant la transmission. Si le délai n'est pas ajouté avant la transmission sur une liaison, le temps pendant lequel le LSA se propage sur la liaison n'est pas pris en compte. La valeur attribuée doit tenir compte des délais de transmission et de propagation pour l'interface. Ce paramètre a plus d'importance sur les liaisons à très faible vitesse. Les valeurs valides vont de 1 à 8 192 secondes. La valeur par défaut est de 1 seconde.

Étape 15 Dans la section Detecting Lost Neighbors (Détection des voisins perdus), effectuez l'une des opérations suivantes :

- Cliquez sur l'intervalle de configuration dans lequel les paquets Hello ne sont pas reçus avant que le routeur déclare le voisin comme étant en panne. Dans le champ Dead Interval (Intervalle de temps mort), précisez l'intervalle, en secondes, pendant lequel aucun paquet Hello n'est reçu, ce qui amène les voisins

à déclarer un routeur en panne. Les valeurs valides vont de 1 à 8 192 secondes. La valeur par défaut de ce paramètre est quatre fois l'intervalle qui a été défini dans le champ Hello Interval (Intervalle Hello).

- Cliquez sur Send fast hello packets (Envoyer des paquets Hello rapides) dans un intervalle de temps mort de 1 seconde. Dans le champ Hello multiplier (Multiplicateur Hello), spécifiez le nombre de paquets Hello à envoyer par seconde. Les valeurs valides sont comprises entre 3 et 20.

Configurer les paramètres de zone OSPFv2

Vous pouvez configurer plusieurs paramètres de zone OSPF. Ces paramètres de zone (indiqués dans la liste des tâches suivante) comprennent la définition de l'authentification, la définition des zones tampons et l'affectation de coûts spécifiques à la route récapitulative par défaut. L'authentification offre une protection par mot de passe contre l'accès non autorisé à une zone.

Les zones tampons sont des zones dans lesquelles les informations sur les routages externes ne sont pas envoyées. Au lieu de cela, une route externe par défaut est générée par l'ABR dans la zone tampon pour les destinations externes au système autonome. Pour tirer parti de la prise en charge de la zone tampon OSPF, le routage par défaut doit être utilisé dans la zone tampon.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Area/Networks** (Zone/Réseaux).

La boîte de dialogue Add OSPF Area (Ajouter une zone OSPF) apparaît.

Étape 3 Choisissez l'une des options suivantes pour le type de zone :

- **Normal** pour faire de la zone une zone OSPF standard. Cette option est sélectionnée par défaut lorsque vous créez une zone pour la première fois.
- **Stub** (Tampon) pour faire de la zone une zone tampon. Les zones tampons ne comportent aucun routeur ni aucune zone au-delà. Les zones tampons empêchent les LSA externes de l'AS (LSA de type 5) d'être submergées dans la zone tampon. Lorsque vous créez une zone tampon, vous avez la possibilité d'empêcher l'inondation des LSA (types 3 et 4) récapitulatifs dans la zone en décochant la case Summary (Résumé).
- **Summary** (Résumé) Pour empêcher l'envoi de LSA dans la zone tampon lorsque la zone définie est une zone tampon, décochez cette case. Par défaut, cette case est cochée pour les zones tampons.
- **NSSA** pour faire de la zone une zone moins dense. Les contrats NSSA acceptent les LSA de type 7. Lorsque vous créez le NSSA, vous avez la possibilité d'empêcher l'inondation des LSA récapitulatifs dans la zone en décochant la case Summary (Résumé). Vous pouvez également désactiver la redistribution de routes en décochant la case Redistribute (Redistribuer) mais en cochant la case Default Information Originate (Origine des informations par défaut).

Étape 4 Saisissez l'adresse IP dans le champ IP Address (Adresse IP) du réseau ou de l'hôte à ajouter à la zone. Utilisez **0.0.0.0** avec un masque réseau de **0.0.0.0** pour créer la zone par défaut. Vous ne pouvez saisir **0.0.0.0** que dans une zone.

Étape 5 Saisissez le masque réseau dans le champ Network Mask (Masque réseau) de l'adresse IP ou de l'hôte à ajouter à la zone. Si vous ajoutez un hôte, choisissez le masque **255.255.255.255**.

Étape 6 Choisissez le type d'authentification OSPF parmi les options suivantes :

- **None** (Aucun) pour désactiver l'authentification de zone OSPF. Il s'agit du paramètre par défaut.
- **Password** (Mot de passe) pour fournir un mot de passe en clair pour l'authentification de zone, ce qui n'est pas conseillé lorsque la sécurité est un problème.
- **MD5** pour permettre l'authentification MD5.

Étape 7 Saisissez une valeur dans le champ Default Cost (Coût par défaut) pour spécifier un coût par défaut pour la zone OSPF.

Cette valeur peut être comprise entre 0 et 65 535. La valeur par défaut est 1.

Étape 8 Cliquez sur **OK**.

Configurer les règles de filtre OSPFv2

Utilisez la procédure suivante pour filtrer les routes ou les réseaux reçus ou transmis dans les mises à jour OSPF.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Filter Rules (Règles de filtre)**.

Étape 2 Cliquez sur **Add** (ajouter).

Étape 3 Sélectionnez l'ID de processus OSPF dans **OSPF AS** (AS OSPF).

Étape 4 Choisissez une liste d'accès standard dans la lise déroulante Access List (Liste d'accès). Cliquez sur **Manage** (Gérer) pour ajouter une nouvelle ACL.

Étape 5 Choisissez une direction dans la liste déroulante Direction. La direction spécifie si le filtre doit être appliqué aux mises à jour entrantes ou sortantes.

Étape 6 Pour les filtres entrants, vous pouvez éventuellement spécifier une interface pour limiter le filtre aux mises à jour reçues sur cette interface.

Étape 7 Pour les filtres sortants, vous pouvez éventuellement spécifier les types de routes distribués.

a) Choisissez une option dans la liste déroulante Protocol (Protocole).

Vous pouvez choisir un protocole de routage, par exemple, **BGP**, **EIGRP**, **OSPF** ou **RIP**.

Choisissez **Connected** (Connecté) pour filtrer les homologues et les réseaux appris par le biais des routes connectées.

Choisissez **Static** (Statique) pour filtrer les homologues et les réseaux appris par le biais des routes statiques.

b) Si vous avez choisi BGP, EIGRP ou OSPF, choisissez également le **Process ID** (ID de processus) pour ce protocole.

Étape 8 Cliquez sur **OK**.

Étape 9 Cliquez sur **Apply** (Appliquer).

Configurer une NSSA OSPFv2

La mise en œuvre du protocole OSPFv2 d'une zone NSSA est similaire à une zone tampon OSPFv2. NSSA n'inonde pas les LSA externes de type 5 du cœur vers la zone, mais il peut importer des routes externes du système autonome de manière limitée dans la zone.

NSSA importe des routes externes du système autonome de type 7 dans une zone NSSA par redistribution. Ces LSA de type 7 sont traduites en LSA de type 5 par les ABR de NSSA, qui sont inondés dans tout le domaine de routage. La synthèse et le filtrage sont pris en charge pendant la traduction.

Vous pouvez simplifier l'administration si vous êtes un FAI ou un administrateur réseau qui doit connecter un site central à l'aide du protocole OSPFv2 à un site distant qui utilise un protocole de routage différent avec NSSA.

Avant la mise en œuvre de NSSA, la connexion entre le routeur de frontière du site d'entreprise et le routeur distant ne pouvait pas être exécutée en tant que zone tampon OSPFv2, car les routes du site distant ne pourraient pas être redistribuées dans la zone tampon, et deux protocoles de routage devaient être maintenus. Un protocole simple comme RIP était généralement exécuté et gérait la redistribution. Avec NSSA, vous pouvez étendre le protocole OSPFv2 pour couvrir la connexion à distance en définissant la zone entre le routeur d'entreprise et le routeur distant en tant que NSSA.

Veuillez consulter les lignes directrices suivantes avant d'utiliser cette fonctionnalité :

- Vous pouvez définir une route par défaut de type 7 qui peut être utilisée pour atteindre des destinations externes. Une fois configuré, le routeur génère une valeur par défaut de type 7 dans le NSSA ou le routeur de limite de zone NSSA.
- Tous les routeurs d'une même zone doivent convenir que la zone est NSSA; sinon, les routeurs ne peuvent pas communiquer entre eux.

Procédure

Étape 1 Depuis la page d'accueil principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Area/Networks** (Zone/Réseaux).

Étape 3 Cliquez sur **Add** (ajouter).

La boîte de dialogue Add OSPF Area (Ajouter une zone OSPF) apparaît.

Étape 4 Cliquez sur le bouton radio **NSSA** dans la zone Area Type (Type de zone).

Choisissez cette option pour faire de la zone une zone NSSA (not-so-stubby area). Les contrats NSSA acceptent les LSA de type 7. Lorsque vous créez le NSSA, vous avez la possibilité d'empêcher l'inondation des LSA récapitulatifs dans la zone en décochant la case Summary (Résumé). Vous pouvez également désactiver la redistribution de routes en décochant la case Redistribute (Redistribuer) mais en cochant la case Default Information Originate (Origine des informations par défaut).

Étape 5 Saisissez l'adresse IP dans le champ IP Address (Adresse IP) du réseau ou de l'hôte à ajouter à la zone. Utilisez **0.0.0.0** avec un masque réseau de **0.0.0.0** pour créer la zone par défaut. Vous ne pouvez saisir **0.0.0.0** que dans une zone.

Étape 6 Saisissez le masque réseau dans le champ Network Mask (Masque réseau) de l'adresse IP ou de l'hôte à ajouter à la zone. Si vous ajoutez un hôte, choisissez le masque **255.255.255.255**.

Étape 7 Dans la zone Authentication (Authentification), cliquez sur le bouton radio **None** (Aucun) pour désactiver l'authentification de zone OSPF.

Étape 8 Saisissez une valeur dans le champ Default Cost (Coût par défaut) pour spécifier un coût par défaut pour la zone OSPF.

Cette valeur peut être comprise entre 0 et 65 535. La valeur par défaut est 1.

Étape 9 Cliquez sur **OK**.

Configurer un ensemble d'adresses IP pour la mise en grappe (OSPFv2 et OSPFv3)

Vous pouvez attribuer une plage d'adresses IPv4 pour le regroupement de grappes d'ID de routeur si vous utilisez la mise en grappe d'interfaces individuelles.

Pour attribuer une plage d'adresses IPv4 à l'ensemble de grappes d'ID de routeur dans l'interface individuelle pour le protocole OSPFv2, procédez comme suit :

Procédure

Étape 1 Depuis la page d'accueil principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Process Instances** (Instances de processus).

Étape 3 Choisissez le processus OSPF que vous souhaitez modifier, puis cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPF Process Advanced Properties (Modifier les propriétés avancées du processus OSPF) apparaît.

Étape 4 Cliquez sur le bouton radio **Cluster Pool** (Ensemble de grappes). Si vous utilisez la mise en grappe, vous n'avez pas besoin de spécifier d'ensemble d'adresses IP pour l'ID de routeur (c'est-à-dire, laissez le champ vide). Si vous ne saisissez pas d'ensemble d'adresses IP, l'ASA utilise l'ID de routeur généré automatiquement.

Étape 5 Saisissez le nom de l'ensemble d'adresses IP ou cliquez sur les points de suspension pour afficher la boîte de dialogue Select IP Address Pool (Sélectionner un ensemble d'adresses IP).

Étape 6 Cliquez deux fois sur un nom d'ensemble d'adresses IP existant pour l'ajouter au champ Assign (Affecter). Sinon, cliquez sur **Add** (Ajouter) pour créer un nouvel ensemble d'adresses IP.

La boîte de dialogue Add IPv4 Pool (Ajouter un ensemble IPv4) s'affiche.

Étape 7 Saisissez le nom du nouvel ensemble d'adresses IP dans le champ **Name** (Nom).

Étape 8 Saisissez l'adresse IP de départ ou cliquez sur les points de suspension pour afficher la boîte de dialogue Browse Starting IP Address (Parcourir l'adresse IP de départ).

Étape 9 Cliquez deux fois sur une entrée pour l'ajouter dans le champ Starting IP Address (Adresse IP de départ), puis cliquez sur **OK**.

Étape 10 Saisissez l'adresse IP de fin ou cliquez sur les points de suspension pour afficher la boîte de dialogue Browse Ending IP Address (Parcourir l'adresse IP de fin).

Étape 11 Cliquez deux fois sur une entrée pour l'ajouter au champ Ending IP Address (Adresse IP de fin), puis cliquez sur **OK**.

Étape 12 Dans la liste déroulante, choisissez le filtre d'adresse locale, puis cliquez sur **OK**.

Le nouvel ensemble d'adresses IP apparaît dans la liste Select IP Address Pool (Sélectionner un ensemble d'adresses IP).

Étape 13 Cliquez deux fois sur le nom du nouvel ensemble d'adresses IP pour l'ajouter au champ Assign (Affecter), puis cliquez sur **OK**.

Le nom du nouvel ensemble d'adresses IP apparaît dans le champ Cluster Pool (Ensemble de grappes) de la boîte de dialogue Edit OSPF Process Advanced Properties (Modifier les propriétés avancées du processus OSPF).

Étape 14 Cliquez sur **OK**.

Étape 15 Si vous souhaitez modifier les paramètres de l'ensemble d'adresses IP nouvellement ajouté, cliquez sur **Edit** (Modifier).

La boîte de dialogue Edit IPv4 Pool (Modifier un ensemble IPv4) s'affiche.

Étape 16 Répétez les étapes 4 à 14.

Remarque Vous ne pouvez pas modifier ni supprimer un ensemble d'adresses IP existant qui a été attribué et qui est déjà utilisé par un ou plusieurs profils de connexion.

Étape 17 Cliquez sur **OK**.

Étape 18 Pour attribuer une plage d'adresses IPv4 à l'ensemble de grappes d'ID de routeur dans la mise en grappe d'interfaces individuelles pour le protocole OSPFv3, procédez comme suit :

a) Depuis la page d'accueil principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

b) Cliquez sur l'onglet **Process Instances** (Instances de processus).

c) Choisissez le processus OSPF que vous souhaitez modifier, puis cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPFv3 Process Advanced Properties (Modifier les propriétés avancées du processus OSPFv3) apparaît.

d) Sélectionnez l'option Cluster Pool (Ensemble de grappes) dans la liste déroulante Router ID (ID de routeur). Si vous n'avez pas besoin de spécifier d'ensemble d'adresses IP pour l'ID de routeur, sélectionnez l'option Automatic (Automatique). Si vous ne configurez pas d'ensemble d'adresses IP, l'ASA utilise l'ID de routeur généré automatiquement.

e) Saisissez le nom de l'ensemble d'adresses IP. Sinon, cliquez sur les points de suspension pour afficher la boîte de dialogue Select IP Address Pool (Sélectionner un ensemble d'adresses IP).

f) Cliquez deux fois sur un nom d'ensemble d'adresses IP existant pour l'ajouter au champ Assign (Affecter). Sinon, cliquez sur **Add** (Ajouter) pour créer un nouvel ensemble d'adresses IP.

La boîte de dialogue Add IPv4 Pool (Ajouter un ensemble IPv4) s'affiche.

g) Saisissez le nom du nouvel ensemble d'adresses IP dans le champ **Name** (Nom).
h) Saisissez l'adresse IP de départ ou cliquez sur les points de suspension pour afficher la boîte de dialogue Browse Starting IP Address (Parcourir l'adresse IP de départ).
i) Cliquez deux fois sur une entrée pour l'ajouter dans le champ Starting IP Address (Adresse IP de départ), puis cliquez sur **OK**.
j) Saisissez l'adresse IP de fin ou cliquez sur les points de suspension pour afficher la boîte de dialogue Browse Ending IP Address (Parcourir l'adresse IP de fin).
k) Cliquez deux fois sur une entrée pour l'ajouter au champ Ending IP Address (Adresse IP de fin), puis cliquez sur **OK**.
l) Dans la liste déroulante, choisissez le filtre d'adresse locale, puis cliquez sur **OK**.

   Le nouvel ensemble d'adresses IP apparaît dans la liste Select IP Address Pool (Sélectionner un ensemble d'adresses IP).

m) Cliquez deux fois sur le nom du nouvel ensemble d'adresses IP pour l'ajouter au champ Assign (Affecter), puis cliquez sur **OK**.

   Le nom du nouvel ensemble d'adresses IP apparaît dans le champ Cluster Pool (Ensemble de grappes) de la boîte de dialogue Edit OSPF Process Advanced Properties (Modifier les propriétés avancées du processus OSPF).

n) Cliquez sur **OK**.
o) Si vous souhaitez modifier les paramètres de l'ensemble de grappes nouvellement ajouté, cliquez sur **Edit** (Modifier).

   La boîte de dialogue Edit IPv4 Pool (Modifier un ensemble IPv4) s'affiche.

p) Répétez les étapes 4 à 14.

Remarque Vous ne pouvez pas modifier ou supprimer un ensemble d'adresses IP existant qui a été attribué et qui est déjà utilisé par un autre processus OSPFv3.

q) Cliquez sur **OK**.

Définir les voisins OSPFv2 statiques

Vous devez définir des voisins OSPFv2 statiques pour annoncer les routes OSPFv2 sur un réseau point à point de non-diffusion. Cette fonctionnalité vous permet de diffuser des annonces OSPFv2 sur une connexion VPN existante sans avoir à encapsuler les annonces dans un tunnel GRE.

Avant de commencer, vous devez créer une route statique vers le voisin OSPFv2. Consultez Configurer une route statique pour en savoir plus sur la création des routes statiques.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Static Neighbor (Voisin statique)**.

Étape 2 Cliquez sur **Add** ou **Edit** (ajouter ou modifier).

La boîte de dialogue Add/Edit OSPF Neighbor Entry (Ajouter/modifier une entrée de voisin OSPF) s'affiche. Cette boîte de dialogue vous permet de définir un nouveau voisin statique ou de modifier les renseignements d'un voisin statique existant. Vous devez définir un voisin statique pour chaque interface point à point de non-diffusion. Notez les restrictions suivantes :

- Vous ne pouvez pas définir le même voisin statique pour deux processus OSPF différents.
- Vous devez définir une route statique pour chaque voisin statique.

Étape 3 Dans la liste déroulante OSPF Process (Processus OSPF), choisissez le processus OSPF associé au voisin statique. Si vous modifiez un voisin statique existant, vous ne pouvez pas modifier cette valeur.

Étape 4 Dans le champ **Neighbor** (Voisin), saisissez l'adresse IP du voisin statique.

Étape 5 Dans le champ **Interface**, choisissez l'interface associée au voisin statique. Si vous modifiez un voisin statique existant, vous ne pouvez pas modifier cette valeur.

Étape 6 Cliquez sur **OK**.

Configurer les minuteries de calcul de routage

Vous pouvez configurer le délai entre le moment où le protocole OSPFv2 reçoit une modification de topologie et le moment où il démarre un calcul SPF. Vous pouvez également configurer le délai de rétention entre deux calculs SPF consécutifs.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Process Instances** (Instances de processus).

Étape 3 Choisissez le processus OSPF que vous souhaitez modifier, puis cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPF Process Advanced Properties (Modifier les propriétés avancées du processus OSPF) apparaît.

Étape 4 La zone Timers (Minuteries) vous permet de modifier les paramètres utilisés pour configurer les minuteries de calcul de cadence et de SPF. Dans la zone Timers (Minuteries), saisissez les valeurs suivantes :

- Le délai SPF initial spécifie le temps (en millisecondes) entre le moment où OSPF reçoit une modification de topologie et le moment où le calcul SPF commence. Les valeurs valides vont de 0 à 600 000 millisecondes.
- Le délai de rétention SPF minimum spécifie le délai de rétention (en millisecondes) entre des calculs SPF consécutifs. Les valeurs valides sont comprises entre 0 et 600 000 millisecondes.
- Le délai d'attente SPF maximum spécifie le temps d'attente maximum entre deux calculs SPF consécutifs. Les valeurs valides vont de 0 à 600 000 millisecondes.

Étape 5 Cliquez sur **OK**.

Journaliser les voisins en hausse ou en baisse

Par défaut, un message de journal système est généré lorsqu'un voisin OSPFv2 redevient disponible ou tombe en panne.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Process Instances** (Instances de processus).

Étape 3 Cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPF Process Advanced Properties (Modifier les propriétés avancées du processus OSPF) apparaît.

Étape 4 La zone Adjacency Changes (Modifications de contiguïté) comprend des paramètres qui définissent les modifications de contiguïté provoquant l'envoi des messages de journal système. Dans la zone Adjacency Changes (Modifications de contiguïté), saisissez les valeurs suivantes :

- Cochez la case **Log Adjacency Changes** (Journaliser les modifications de contiguïté) pour que l'ASA envoie un message de journal système à chaque fois qu'un voisin OSPFv2 est activé ou désactivé. Ce paramètre est coché par défaut.
- Cochez la case **Log Adjacency Changes Detail** (Journaliser les détails sur le changement de contiguïté) pour que l'ASA envoie un message de journal système chaque fois qu'un changement d'état se produit, pas seulement quand un voisin est activé ou désactivé. Ce paramètre est décoché par défaut.

Étape 5 Cliquez sur **OK**.



Remarque La journalisation doit être activée pour que les messages de voisin activé ou désactivé soient envoyés.

Configurer une chaîne de clés pour l'authentification

Pour améliorer la sécurité et la protection des données des périphériques, vous pouvez activer des clés changeantes pour l'authentification des homologues IGP. Les clés pivotantes empêchent tout utilisateur malveillant de deviner les clés utilisées pour l'authentification du protocole de routage, protégeant ainsi le réseau contre les annonces de routage incorrect et la redirection du trafic. La modification fréquente des clés réduit le risque qu'elles finissent par être devinées. Lors de la configuration de l'authentification pour les protocoles de routage qui fournissent des chaînes de clés, configurez les clés d'une chaîne de clés pour qu'elles se chevauchent. Cela permet d'éviter la perte de communication à clé en raison de l'absence d'une clé active.

Si la durée de vie de la clé expire et qu'aucune clé active n'est trouvée, OSPF utilise la dernière clé valide pour maintenir la contiguïté avec les homologues.

Cette section décrit comment créer une chaîne de clés pour l'authentification des homologues OSPF. Cette section couvre également les étapes pour ajouter ou modifier les attributs d'une chaîne de clés. Après avoir configuré un objet de chaîne de clés, vous pouvez l'utiliser pour définir l'authentification OSPFv2 pour une interface et pour une liaison virtuelle. Utilisez le même type d'authentification (MD5 ou chaîne de clé) et le même ID de clé pour les homologues afin d'établir une contiguïté réussie. Pour savoir comment définir l'authentification pour une interface, consultez Configurer les paramètres d'interface OSPFv2, à la page 17; pour une liaison virtuelle, consultez Configurer un lien virtuel dans OSPF, à la page 31.

Pour configurer une chaîne de clés, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Key Chain (Chaîne de clés)** .

Étape 2 Dans la section **Configure Key Chain** (Configurer la chaîne de clés), cliquez sur **Add** (Ajouter).

Étape 3 Saisissez le nom de la chaîne de clés dans la boîte de dialogue **Add Key Chain** (Ajouter une chaîne de clés), puis cliquez sur **OK**.

Le nom de la chaîne de clés créée est répertorié dans la grille **Configure Key Chain** (Configurer la chaîne de clés).

Étape 4 Sélectionnez le nom de la chaîne de clés dans la section **Configure Key Chain** (Configurer la chaîne de clés), et dans la section **Configure Key** (Configurer la clé), cliquez sur **Add** (Ajouter). Pour modifier une clé existante, sélectionnez le nom de la clé et cliquez sur **Edit** (Modifier).

La boîte de dialogue **Add Key** (Ajouter une clé) ou **Edit Key** (Modifier une clé) apparaît, selon l'action que vous avez sélectionnée.

Étape 5 Précisez l'identifiant de clé dans le champ **Key ID**.

La valeur de l'ID de clé peut être comprise entre 0 et 255. Utilisez la valeur 0 uniquement lorsque vous souhaitez signaler une clé non valide.

Remarque Vous ne pouvez pas modifier un ID de clé enregistré.

Étape 6 Dans la liste déroulante **Cryptographic Algorithm** (Algorithme cryptographique), choisissez **MD5**. MD5 est le seul algorithme pris en charge pour l'authentification de la chaîne de clés.

Étape 7 Sélectionnez le type de chiffrement en cliquant sur le bouton radio **Plain Text** (Texte brut) ou **Encrypted** (Chiffré), puis saisissez le mot de passe dans le champ **Authentication Key** (Clé d'authentification).

- Même si la chaîne de clé peut contenir 80 caractères, seul un maximum de 64 caractères est autorisé pour l'authentification OSPF.
- Les mots de passe ne peuvent pas être un seul chiffre ni ceux commençant par un chiffre suivi d'un espace. Par exemple, « 0 pass » ou « 1 » ne sont pas valides.

Étape 8 Fournissez les valeurs de durée de vie dans les champs **Accept Lifetime** (Accepter la durée de vie) et **Send Lifetime** (Envoyer la durée de vie) :

Vous pouvez spécifier l'intervalle de temps nécessaire pour que le périphérique accepte ou envoie la clé lors de l'échange de clés avec un autre périphérique. L'heure de fin peut correspondre à la durée absolue à laquelle la durée de vie de l'acceptation/envoi se termine ou n'expire jamais.

Voici les règles de validation pour les valeurs de début et de fin :

- La durée de vie de début ne peut pas être nulle lorsque la fin de vie est spécifiée.
- La durée de vie de début pour l'acceptation ou l'envoi de la durée de vie doit être antérieure à la fin de vie.

Étape 9 Pour enregistrer les attributs de la chaîne de clés, cliquez sur **OK**. Dans la page **Key Chain** (Chaîne de clés), cliquez sur **Appy** (Appliquer).

Prochaine étape

Vous pouvez maintenant appliquer la chaîne de clés configurée pour définir l'authentification OSPFv2 pour une interface et pour la liaison virtuelle.

- Configurer les paramètres d'interface OSPFv2, à la page 17
- Configurer un lien virtuel dans OSPF, à la page 31

Configurer le filtrage dans OSPF

Le volet Filtering (Filtrage) affiche les filtres LSA ABR de type 3 qui ont été configurés pour chaque processus OSPF.

Les filtres LSA ABR de type 3 permettent uniquement l'envoi de préfixes spécifiés d'une zone à une autre et restreignent tous les autres préfixes. Ce type de filtrage de zone peut être appliqué hors d'une zone OSPF spécifique, dans une zone OSPF spécifique ou à la fois vers et depuis les mêmes zones OSPF.

Le filtrage LSA OSPF ABR de type 3 améliore votre contrôle de la distribution des routages entre les zones OSPF.

Remarque Seuls les LSA de type 3 qui proviennent d'un ABR sont filtrés.

Pour configurer le filtrage dans OSPF, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Filtering (Filtrage)**.

Étape 2 Cliquez sur **Add** ou **Edit**(ajouter ou modifier) .

La boîte de dialogue Add or Edit OSPF Filtering Entry (Ajouter ou modifier une entrée de filtrage OSPF) vous permet d'ajouter de nouveaux filtres au tableau de filtres ou de modifier un filtre existant. Certains renseignements de filtrage ne peuvent pas être modifiés lorsque vous modifiez un filtre existant.

Étape 3 Choisissez le processus OSPF associé à l'entrée de filtre dans la liste déroulante OSPF Process (Processus OSPF).

Étape 4 Choisissez l'ID de zone associé à l'entrée de filtre dans la liste déroulante Area ID (ID de zone). Si vous modifiez une entrée de filtre existante, vous ne pouvez pas modifier ce paramètre.

Étape 5 Choisissez une liste de préfixes dans la liste déroulante Prefix List (Liste des préfixes).

Étape 6 Choisissez la direction du trafic filtrée dans la liste déroulante Traffic Direction (Direction du trafic).

Choisissez entrant pour filtrer les LSA entrant dans une zone OSPF, ou sortant pour filtrer les LSA sortant d'une zone OSPF. Si vous modifiez une entrée de filtre existante, vous ne pouvez pas modifier ce paramètre.

Étape 7 Cliquez sur **Manage** (Gérer) pour afficher la boîte de dialogue Configure Prefix Lists (Configurer les listes de préfixes), dans laquelle vous pouvez ajouter, modifier ou supprimer des listes de préfixes et des règles de préfixes. Pour plus de renseignements, consultez Configurer les listes de préfixe et Configurer les valeurs de mesure pour une action de routage.

Étape 8 Cliquez sur **OK**.

Configurer un lien virtuel dans OSPF

Si vous ajoutez une zone à un réseau OSPF et qu'il n'est pas possible de connecter la zone directement à la zone du réseau fédérateur, vous devez créer une liaison virtuelle. Une liaison virtuelle connecte deux appareils OSPF qui ont une zone commune, appelée la zone de transit. Un des appareils OSPF doit être connecté à la zone du réseau fédérateur.

Pour définir de nouvelles liaisons virtuelles ou modifier les propriétés des liaisons virtuelles existantes, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Virtual Link (Liaison virtuelle)**.

Étape 2 Cliquez sur **Add** ou **Edit** (ajouter ou modifier).

La boîte de dialogue Add or Edit OSPF Virtual Link (Ajouter ou modifier une liaison virtuelle OSPF) apparaît. Elle vous permet de définir de nouvelles liaisons virtuelles ou de modifier les propriétés des liaisons virtuelles existantes.

Étape 3 Choisissez l'ID de processus OSPF associé à la liaison virtuelle dans la liste déroulante OSPF Process (Processus OSPF). Si vous modifiez une liaison virtuelle existante, vous ne pouvez pas modifier ce paramètre.

Étape 4 Choisissez l'ID de zone associé à la liaison virtuelle dans la liste déroulante Area ID (ID de zone).

Choisissez la zone partagée par les appareils OSPF voisins. La zone sélectionnée ne peut pas être une zone NSSA ou une zone de stub. Si vous modifiez une liaison virtuelle existante, vous ne pouvez pas modifier ce paramètre.

Étape 5 Dans le champ **Peer Router ID** (ID de routeur homologue), saisissez l'ID de routeur du voisin de liaison virtuelle.

Si vous modifiez une liaison virtuelle existante, vous ne pouvez pas modifier ce paramètre.

Étape 6 Cliquez sur **Advanced** (Avancé) pour modifier les propriétés de liaison virtuelle avancées.

La boîte de dialogue Advanced OSPF Virtual Link Properties (Propriétés de liaison virtuelle OSPF avancées) apparaît. Vous pouvez configurer les propriétés OSPF pour la liaison virtuelle dans cette zone. Ces propriétés comprennent les paramètres d'authentification et d'intervalle de paquets.

Étape 7 Dans la zone Authentication (Authentification), choisissez le type d'authentification en cliquant sur le bouton radio à côté de l'une des options suivantes :

- **No authentication** (Aucune authentification) pour désactiver l'authentification OSPF.
- **Password authentication** (Authentification par mot de passe) pour utiliser l'authentification par mot de passe en texte clair (non conseillé lorsque la sécurité est une préoccupation).
- **MD5 authentication** (Authentification MD5) pour utiliser l'authentification MD5.
- **Key chain authentication** (Authentification par chaîne de clés) pour utiliser l'authentification par chaîne de clés (conseillé). Consultez Configurer une chaîne de clés pour l'authentification, à la page 10 pour en savoir plus sur la configuration de la chaîne de clés pour l'authentification.

Étape 8 Dans la zone Authentication Password (Mot de passe d'authentification), entrez et reconfirmez un mot de passe lorsque l'authentification par mot de passe est activée. Les mots de passe doivent être des chaînes de texte de 8 caractères maximum.

Étape 9 Dans la zone MD5 IDs and Key (ID et clé MD5), saisissez les clés et les paramètres MD5 lorsque l'authentification MD5 est activée. Tous les appareils de l'interface qui utilisent l'authentification OSPF doivent utiliser la même clé MD5 et le même ID. Spécifiez les paramètres suivants :

a) Dans le champ **Key ID** (ID de clé), saisissez un identifiant de clé numérique. Les valeurs valides sont comprises entre 0 et 255. L'ID de clé s'affiche pour l'interface sélectionnée.
b) Dans le champ **Key** (Clé), saisissez une chaîne de caractères alphanumériques d'une durée maximale de 16 octets. L'ID de clé s'affiche pour l'interface sélectionnée.
c) Cliquez sur **Add** (Ajouter) ou **Delete** (Supprimer) pour ajouter ou supprimer la clé MD5 spécifiée au tableau d'ID et de clé MD5.

Étape 10 Dans la zone Interval (Intervalle), spécifiez la synchronisation de l'intervalle pour le paquet en choisissant parmi les options suivantes :

- **Hello Interval** (Intervalle Hello) pour spécifier l'intervalle, en secondes, entre les paquets Hello envoyés sur une interface. Plus l'intervalle Hello est petit, plus les changements topologiques sont détectés rapidement, mais plus le trafic acheminé sur l'interface est important. Cette valeur doit être la même pour tous les routeurs et serveurs d'accès sur une interface donnée. Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est 10 secondes.
- **Retransmit Interval** (Intervalle de retransmission) pour spécifier le temps en secondes entre les retransmissions de LSA pour les contiguïtés qui appartiennent à l'interface. Lorsqu'un routeur envoie un LSA à son voisin, il le conserve jusqu'à ce qu'il reçoive l'accusé de réception. Si le routeur ne reçoit aucun accusé de réception, il renvoie le LSA. Soyez prudent lors de la définition de cette valeur, sinon une retransmission inutile peut en résulter. La valeur doit être supérieure pour les lignes série et les liaisons virtuelles. Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est de 5 secondes.

- **Transmit Delay** (Délai de transmission) pour spécifier le temps estimé, en secondes, nécessaire pour envoyer un paquet LSA sur l'interface. L'âge des LSA dans le paquet de mise à jour est augmenté de la quantité spécifiée par ce champ avant la transmission. Si le délai n'est pas ajouté avant la transmission sur une liaison, le temps pendant lequel le LSA se propage sur la liaison n'est pas pris en compte. La valeur attribuée doit tenir compte des délais de transmission et de propagation pour l'interface. Ce paramètre a plus d'importance sur les liaisons à très faible vitesse. Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est de 1 seconde.
- **Dead Interval** (Intervalle de temps mort) pour spécifier l'intervalle, en secondes, pendant lequel aucun paquet Hello n'est reçu, ce qui amène les voisins à déclarer un routeur en panne. Cette valeur peut être comprise entre 1 et 65 535. La valeur par défaut de ce champ est quatre fois l'intervalle défini par le champ Hello Interval (Intervalle Hello).

Étape 11 Cliquez sur **OK**.

Configurer le protocole OSPFv3

Cette section décrit les tâches nécessaires à la configuration d'un processus de routage OSPFv3.

Activer OSPFv3

Pour activer OSPFv3, vous devez créer un processus de routage OSPFv3, créer une zone pour OSPFv3, activer une interface pour OSPFv3, puis redistribuer la route dans les processus de routage OSPFv3 ciblés.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

Étape 2 Sous l'onglet Process Instances (Instances de processus), cochez la case **Enable OSPFv3 Process** (Activer le processus OSPFv3). Vous pouvez activer jusqu'à deux instances de processus OSPF. Seul le mode de contexte unique est pris en charge.

Étape 3 Saisissez un ID de processus dans le champ Process ID (ID de processus). L'ID peut être n'importe quel entier positif.

Étape 4 Cliquez sur **Apply** pour enregistrer vos modifications.

Étape 5 Pour continuer, consultez Configurer les paramètres de zone OSPFv3, à la page 35.

Configurer les paramètres d'interface OSPFv3

Vous pouvez modifier certains paramètres OSPFv3 propres à l'interface, au besoin. Vous n'êtes pas tenu de modifier ces paramètres, mais les paramètres d'interface suivants doivent être cohérents sur tous les routeurs d'un réseau associé : l'intervalle Hello et l'intervalle Dead. Si vous configurez l'un de ces paramètres, assurez-vous que les configurations de tous les routeurs de votre réseau ont des valeurs compatibles.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Interfaces**.

Étape 2 Cliquez sur l'onglet **Authentication** (Authentification).

Étape 3 Pour spécifier les paramètres d'authentification pour une interface, sélectionnez l'interface et cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit OSPFv3 Interface Authentication** (modifier l'authentification de l'interface OSPFv3) apparaît.

Étape 4 Choisissez le type d'authentification à partir de la liste déroulante **Authentication Type** (Type d'authentification). Les options disponibles sont Zone, Interface et Aucun. L'option Aucun indique qu'aucune authentification n'est utilisée.

Étape 5 Choisissez l'algorithme d'authentification dans la liste déroulante **Authentication Algorithm** (Algorithme d'authentification). Les valeurs prises en charge sont SHA-1 et MD5.

Étape 6 Saisissez la clé d'authentification dans le champ **Authentication Key** (Clé d'authentification). Lorsque l'authentification MD5 est utilisée, la clé doit comporter 32 chiffres hexadécimaux (16 octets). Lorsque l'authentification SHA-1 est utilisée, la clé doit comporter 40 chiffres hexadécimaux (20 octets).

Étape 7 Choisissez l'algorithme de chiffrement dans la liste déroulante **Encryption Algorithm** (Algorithme de chiffrement). Les valeurs prises en charge sont AES-CD, 3DES et DES. L'entrée NULL indique qu'il n'y a pas de chiffrement.

Étape 8 Saisissez la clé de chiffrement dans le champ **Encryption Key** (Clé de chiffrement).

Étape 9 Cliquez sur **OK**.

Étape 10 Cliquez sur l'onglet **Properties** (Propriétés).

Étape 11 Sélectionnez l'interface dont vous souhaitez modifier les propriétés, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue Edit OSPFv3 Interface Properties (Modifier les propriétés de l'interface OSPFv3) apparaît.

Étape 12 Cochez la case **Enable OSPFv3 on this interface** (Activer le protocole OSPFv3 sur cette interface).

Étape 13 Choisissez l'ID de processus à partir de la liste déroulante.

Étape 14 Choisissez l'ID de zone à partir de la liste déroulante.

Étape 15 (Facultatif) Spécifiez l'ID d'instance de zone à affecter à l'interface. Une interface ne peut avoir qu'une seule zone OSPFv3. Vous pouvez utiliser la même zone sur plusieurs interfaces, et chaque interface peut utiliser un ID d'instance de zone différent.

Étape 16 Choisissez le type de réseau dans la liste déroulante. Les options prises en charge sont par défaut, diffusion et point à point.

Étape 17 Saisissez le coût d'envoi d'un paquet sur une interface dans le champ Cost (Coût).

Étape 18 Saisissez la priorité du routeur, qui aide à déterminer le routeur désigné pour un réseau dans le champ Priority (Priorité). Les valeurs valides sont comprises entre 0 et 255.

Étape 19 Cochez la case **Disable MTU mismatch detection** (Désactiver la détection de la non-concordance MTU) pour désactiver la détection de la non-concordance MTU OSPF lors de la réception de paquets DBD. La détection des incompatibilités MTU OSPF est activée par défaut.

Étape 20 Cochez la case **Filter outgoing link state advertisements** (Filtrer les annonces d'état de liaison sortantes) pour filtrer les LSA sortants vers une interface OSPFv3. Tous les LSA sortants sont acheminés vers l'interface par défaut.

Étape 21 Cochez la case **OSPF Flood Reduction** (Réduction des inondations OSPF) pour réduire les inondations de données inutiles et l'actualisation des LSA de l'interface.

Étape 22 Dans la zone **Timers** (Minuteries), dans le champ **Dead Interval** (Intervalle de temps mort), saisissez la période en secondes pendant laquelle les paquets Hello ne doivent pas être vus avant que les voisins indiquent que le routeur est en panne. La valeur doit être la même pour tous les nœuds du réseau et peut varier de 1 à 65 535.

Étape 23 Dans le champ **Hello Interval** (Intervalle Hello), saisissez l'intervalle en secondes entre les paquets Hello envoyés sur l'interface. La valeur doit être la même pour tous les nœuds d'un réseau spécifique et peut varier de 1 à 65535. L'intervalle par défaut est de 10 secondes pour les interfaces Ethernet et de 30 secondes pour les interfaces de non-diffusion.

Étape 24 Dans le champ **Retransmit Interval** (Intervalle de retransmission), saisissez le temps en secondes entre les retransmissions de LSA pour les contiguïtés qui appartiennent à l'interface. La durée doit être supérieure au délai aller-retour attendu entre deux routeurs du réseau connecté. Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est de 5 secondes.

Étape 25 Dans le champ **Transmit Delay** (Délai de transmission), saisissez la durée estimée en secondes pour envoyer un paquet de mise à jour d'état de liaison sur l'interface. Les valeurs valides vont de 1 à 65535 secondes. La valeur par défaut est de 1 seconde.

Étape 26 Cliquez sur **OK**.

Étape 27 Cliquez sur **Apply** pour enregistrer vos modifications.

Configurer les paramètres de zone OSPFv3

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Areas** (Zones).

Étape 3 Pour ajouter une nouvelle zone, cliquez sur **Add** (Ajouter). Pour modifier une zone existante, cliquez sur **Edit** (Modifier). Pour supprimer une zone sélectionnée, cliquez sur **Delete** (Supprimer).

La boîte de dialogue Add OSPFv3 Area (Ajouter une zone OSPFv3) ou Edit OSPFv3 Area (Modifier la zone OSPFv3) s'affiche.

Étape 4 Dans la liste déroulante OSPFv3 Process ID (ID de processus OSPFv3), choisissez l'ID de processus.

Étape 5 Saisissez l'ID de zone, qui spécifie la zone pour laquelle les routes doivent être résumées, dans le champ Area ID (ID de zone).

Étape 6 Choisissez le type de zone dans la liste déroulante Area Type (Type de zone). Les options disponibles sont Normal, NSSA et Stub.

Étape 7 Pour autoriser l'envoi de LSA récapitulatifs dans cette zone, cochez la case **Allow sending of summary LSAs into the area** (Autoriser l'envoi de LSA récapitulatifs dans la zone).

Étape 8 Pour autoriser la redistribution afin d'importer les routes vers les zones normales et non vers les zones stubby, cochez la case **Redistribution imports routes to normal and NSSA areas** (La redistribution importe les routes vers les zones normales et NSSA).

Étape 9 Pour générer une route externe par défaut dans un domaine de routage OSPFv3, cochez la case **Default information originate** (Origine des renseignements par défaut).

Étape 10 Saisissez la mesure utilisée pour générer la route par défaut dans le champ Metric (Mesure). La valeur par défaut est 10. Les valeurs de mesure valides sont comprises entre 0 et 16777214.

Étape 11 Dans la liste déroulante Metric Type (Type de mesure), choisissez le type de mesure. Le type de mesure est le type de lien externe associé à la route par défaut annoncée dans le domaine de routage OSPFv3. Les options disponibles sont 1 pour un routage externe de type 1 ou 2 pour un routage externe de type 2.

Étape 12 Saisissez le coût dans le champ Default Cost (Coût par défaut).

Étape 13 Cliquez sur **OK**.

Étape 14 Cliquez sur l'onglet **Route Summarization** (Synthèse de routage).

Étape 15 Pour spécifier une nouvelle plage pour la consolidation et la synthèse des routes, cliquez sur **Add** (Ajouter). Pour modifier une plage existante pour la consolidation et la synthèse des routes, cliquez sur **Edit** (Modifier).

La boîte de dialogue Add Route Summarization (Ajouter une synthèse de routage) ou Edit Route Summarization (Modifier la synthèse de routage) s'affiche.

Étape 16 Dans la liste déroulante Process ID (ID de processus), choisissez l'ID de processus.

Étape 17 Dans la liste déroulante Area ID (ID de zone), choisissez l'ID de zone.

Étape 18 Saisissez le préfixe IPv6 et la longueur du préfixe dans le champ IPv6 Prefix/Prefix Length (Préfixe IPv6/Longueur du préfixe).

Étape 19 (Facultatif) Saisissez la mesure ou le coût de la route récapitulative, qui est utilisé lors des calculs de SPF OSPF pour déterminer les chemins les plus courts vers la destination. Les valeurs valides sont comprises entre 0 et 16 77 77 2015.

Étape 20 Cochez la case **Advertised** (Annoncé) pour définir l'état de la plage d'adresses comme annoncé et générer un LSA récapitulatif de type 3.

Étape 21 Cliquez sur **OK**.

Étape 22 Pour continuer, consultez Configurer un voisin de lien virtuel, à la page 36.

Configurer un voisin de lien virtuel

Pour configurer un voisin de lien virtuel, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Virtual Link (Liaison virtuelle)**.

Étape 2 Pour ajouter un nouveau voisin de lien virtuel, cliquez sur **Add** (Ajouter). Pour modifier un voisin de lien virtuel existant, cliquez sur **Edit** (Modifier). Pour supprimer un voisin de lien virtuel sélectionné, cliquez sur **Delete** (Supprimer).

La boîte de dialogue Add Virtual Link (Ajouter un lien virtuel) ou Edit Virtual Link (Modifier le lien virtuel) apparaît.

Étape 3 Dans la liste déroulante Process ID (ID de processus), choisissez l'ID de processus.

Étape 4 Dans la liste déroulante Area ID (ID de zone), choisissez l'ID de zone.

Étape 5 Saisissez l'ID de routeur homologue (c'est-à-dire l'adresse IP) dans le champ Peer Router ID (ID de routeur homologue).

Étape 6 (Facultatif) Saisissez le nombre de sauts de sécurité TTL (durée de vie) sur un lien virtuel dans le champ TTL Security (Sécurité TTL). La valeur du nombre de sauts peut aller de 1 à 254.

Étape 7 Dans la zone Timers (Minuteries), saisissez la durée en secondes pendant laquelle les paquets Hello ne sont pas vus avant qu'un voisin n'indique que le routeur est en panne dans le champ Dead Interval (Intervalle mort). L'intervalle mort est un entier non signé. La valeur par défaut est quatre fois l'intervalle Hello, soit 40 secondes. La valeur doit être la même pour tous les routeurs et serveurs d'accès connectés à un réseau commun. Les valeurs valides vont de 1 à 8 192.

Étape 8 Saisissez la durée en secondes entre les paquets Hello qui sont envoyés sur une interface dans le champ Hello Interval (Intervalle Hello). L'intervalle Hello est un entier non signé qui doit être annoncé dans les paquets Hello. La valeur doit être la même pour tous les routeurs et serveurs d'accès connectés à un réseau commun. Les valeurs valides vont de 1 à 8 192. La valeur par défaut est 10.

Étape 9 Saisissez la durée en secondes entre les retransmissions de LSA pour les contiguïtés qui appartiennent à l'interface dans le champ Retransmit Interval (Intervalle de retransmission). L'intervalle de retransmission est le délai aller-retour prévu entre deux routeurs du réseau associé. La valeur doit être supérieure au délai aller-retour attendu et peut varier de 1 à 8 192. La valeur par défaut est égale à 5.

Étape 10 Saisissez la durée estimée en secondes qui est requise pour envoyer un paquet de mise à jour d'état de liaison sur l'interface dans le champ Transmit Delay (Délai de transmission). La valeur entière doit être supérieure à zéro. Les LSA dans le paquet de mise à jour ont leur propre âge incrémenté de cette quantité avant transmission. La plage de valeurs peut aller de 1 à 8 192. La valeur par défaut est 1.

Étape 11 Dans la zone Authentication (Authentification), cochez la case **Enable Authentication** (Activer l'authentification) pour activer l'authentification.

Étape 12 Saisissez l'indice de la politique de sécurité, qui doit être un nombre compris entre 256 et 4294967295, dans le champ Security Policy Index (Indice de la politique de sécurité).

Étape 13 Choisissez l'algorithme d'authentification dans la liste déroulante Authentication Algorithm (Algorithme d'authentification). Les valeurs prises en charge sont SHA-1 et MD5. Lorsque l'authentification MD5 est utilisée, la clé doit comporter 32 chiffres hexadécimaux (16 octets). Lorsque l'authentification SHA-1 est utilisée, la clé doit comporter 40 chiffres hexadécimaux (20 octets).

Étape 14 Saisissez la clé d'authentification dans le champ Authentication Key (Clé d'authentification). La clé doit inclure 32 caractères hexadécimaux.

Étape 15 Choisissez l'algorithme de chiffrement dans la liste déroulante Encryption Algorithm (Algorithme de chiffrement). Les valeurs prises en charge sont AES-CD, 3DES et DES. L'entrée NULL indique qu'il n'y a pas de chiffrement.

Étape 16 Saisissez la clé de chiffrement dans le champ Encryption Key (Clé de chiffrement).

Étape 17 Cliquez sur **OK**.

Étape 18 Cliquez sur **Apply** pour enregistrer vos modifications.

Configurer des interfaces passives OSPFv3

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Process Instances** (Instances de processus).

Étape 3 Choisissez le processus OSPFv3 que vous souhaitez modifier, puis cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPFv3 Process Advanced Properties (Modifier les propriétés avancées du processus OSPFv3) apparaît.

Étape 4 La zone Passive Interfaces (Interfaces passives) vous permet d'activer le routage OSPFv3 passif sur une interface. Le routage passif aide à contrôler l'annonce des informations de routage OSPFv3 et désactive l'envoi et la réception des mises à jour de routage OSPFv3 sur une interface. Dans la zone Passive Interfaces (Interfaces passives), choisissez les paramètres suivants :

- Cochez la case **Global passive** (Passif global) pour rendre passives toutes les interfaces répertoriées dans le tableau. Décochez des interfaces individuelles pour les rendre non passives.
- Décochez la case **Global passive** (Passif global) pour rendre toutes les interfaces non passives. Vérifiez les interfaces individuelles pour les rendre passives.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Apply** pour enregistrer vos modifications.

Configurer la distance administrative OSPFv3

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Process Instances** (Instances de processus).

Étape 3 Choisissez le processus OSPF que vous souhaitez modifier, puis cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPFv3 Process Advanced Properties (Modifier les propriétés avancées du processus OSPFv3) apparaît.

La zone Administrative Route Distances (Distances de routage administratif) vous permet de modifier les paramètres qui ont été utilisés pour configurer les distances de routage administratif. La distance de routage administratif doit être un entier compris entre 10 et 254. Dans la zone Administrative Route Distances (Distances de routage administratif), saisissez les valeurs suivantes :

- La valeur inter-zone, qui spécifie les routes inter-zone pour OSPV pour les routes IPv6.
- La valeur intra-zone, qui spécifie les routes intra-zone pour OSPF pour les routes IPv6.
- La valeur externe, qui spécifie les routes externes de type 5 et de type 7 pour OSPF pour les routes IPv6.

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur **Apply** pour enregistrer vos modifications.

Configurer les minuteries mOSPFv3

Vous pouvez définir les minuteries d'arrivée des LSA, de cadence des LSA et de limitation pour le protocole OSPFv3.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Process Instances** (Instances de processus).

Étape 3 Choisissez le processus OSPFv3 que vous souhaitez modifier, puis cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPFv3 Process Advanced Properties (Modifier les propriétés avancées du processus OSPFv3) apparaît.

Étape 4 La zone Timer (Minuterie) vous permet de modifier les paramètres utilisés pour configurer l'arrivée des LSA, la cadence des LSA, la retransmission des LSA, la limitation des LSA et les heures de limitation SPF. Dans la zone Timers (Minuteries), saisissez les valeurs suivantes :

- L'arrivée de LSA, qui spécifie le délai minimum en millisecondes qui doit s'écouler entre l'acceptation de la même LSA provenant des voisins. La plage va de 100 à 1 000 millisecondes. La valeur par défaut est de 1 000 millisecondes.
- Le rythme de débordement de LSA, qui spécifie le temps en millisecondes auquel les LSA de la file d'attente de débordement sont cadencés entre les mises à jour. La plage configurable va de 5 à 100 millisecondes. La valeur par défaut est de 33 millisecondes.
- La cadence du groupe de LSA, qui spécifie l'intervalle en secondes auquel les LSA sont collectés dans un groupe et actualisés, additionnés ou rendus obsolètes. Les valeurs valides vont de 10 à 1 800. La valeur par défaut est 240.
- La cadence de retransmission de LSA, qui spécifie le temps en millisecondes auquel les LSA de la file d'attente de retransmission sont cadencés. La plage configurable va de 5 à 200 millisecondes. La valeur par défaut est de 66 millisecondes.
- La limitation initiale de LSA, qui spécifie le délai en millisecondes pour générer la première occurrence de LSA. La valeur par défaut est de 0 millisecondes.
- Le délai min. de limitation LSA, qui spécifie le délai minimum en millisecondes pour générer le même LSA. La valeur par défaut est de 5000 millisecondes.
- Le délai d'attente max. de la limitation LSA, qui spécifie le délai maximum en millisecondes pour générer le même LSA. La valeur par défaut est de 5000 millisecondes.

Remarque Pour la limitation des LSA, si la durée minimale ou maximale est inférieure à la valeur de première occurrence, OSPFv3 corrige automatiquement cette valeur de première occurrence. De même, si le délai maximal spécifié est inférieur au délai minimal, OSPFv3 corrige automatiquement à la valeur de délai minimal.

- La limitation SPF initiale, qui spécifie le délai en millisecondes avant de recevoir une modification du calcul SPF. La valeur par défaut est de 5000 millisecondes.

- Le délai min. de limitation SPF, qui spécifie le délai en millisecondes entre le premier et le deuxième calcul SPF. La valeur par défaut est de 10 000 millisecondes.
- Le délai d'attente max. de la limitation SPF, qui spécifie le temps d'attente maximum en millisecondes pour les calculs SPF. La valeur par défaut est de 10 000 millisecondes.

Remarque Pour la limitation SPF, si la durée minimale ou maximale est inférieure à la valeur de première occurrence, OSPFv3 corrige automatiquement la valeur de première occurrence. De même, si le délai maximal spécifié est inférieur au délai minimal, OSPFv3 corrige automatiquement à la valeur de délai minimal.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Apply** pour enregistrer vos modifications.

Définir les voisins OSPFv3 statiques

Vous devez définir des voisins OSPFv3 statiques pour annoncer les routes OSPF sur un réseau point à point de non-diffusion. Cette fonctionnalité vous permet de diffuser des annonces OSPFv3 sur une connexion VPN existante sans avoir à encapsuler les annonces dans un tunnel GRE.

Avant de commencer, vous devez créer une route statique vers le voisin OSPFv3. Consultez Configurer une route statique pour en savoir plus sur la création des routes statiques.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Static Neighbor (Voisin statique)**.

Étape 2 Cliquez sur **Add** ou **Edit** (ajouter ou modifier) .

La boîte de dialogue Add or Edit Static Neighbor (Ajouter ou modifier un voisin statique) s'affiche. Cette boîte de dialogue vous permet de définir un nouveau voisin statique ou de modifier les renseignements d'un voisin statique existant. Vous devez définir un voisin statique pour chaque interface point à point de non-diffusion. Notez les restrictions suivantes :

- Vous ne pouvez pas définir le même voisin statique pour deux processus OSPFv3 différents.
- Vous devez définir une route statique pour chaque voisin statique.

Étape 3 Dans la liste déroulante Interface, choisissez l'interface associée au voisin statique. Si vous modifiez un voisin statique existant, vous ne pouvez pas modifier cette valeur.

Étape 4 Dans le champ Link-local Address (Adresse Link-Local), saisissez l'adresse IPv6 du voisin statique.

Étape 5 (Facultatif) Dans le champ Priority (Priorité), saisissez le niveau de priorité.

Étape 6 (Facultatif) Dans le champ Poll Interval (Intervalle entre interrogations), saisissez l'intervalle entre interrogations en secondes.

Étape 7 Cliquez sur **OK**.

Envoyer les messages du journal système

Configurez le routeur pour envoyer un message de journal système lorsqu'un voisin OSPFv3 est actif ou inactif.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Process Instances** (Instances de processus).

Étape 3 Choisissez le processus OSPF que vous souhaitez modifier, puis cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPFv3 Process Advanced Properties (Modifier les propriétés avancées du processus OSPFv3) apparaît.

La zone Adjacency Changes (Modifications de contiguïté) vous permet de modifier les paramètres d'envoi de messages du journal système lorsqu'un voisin OSPFv3 est activé ou désactivé. Dans la zone Adjacency Changes (Modifications de contiguïté), procédez comme suit :

- Pour envoyer un message de journal système lorsqu'un voisin OSPFv3 est activé ou désactivé, cochez la case **Log Adjacency Changes** (Enregistrer les modifications de contiguïté).
- Pour envoyer un message de journal système pour chaque état, pas seulement lorsqu'un voisin OSPFv3 est activé ou désactivé, cochez la case **Include Details** (Inclure les détails).

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur **Apply** pour enregistrer vos modifications.

Supprimer les messages du journal système

Pour supprimer l'envoi des messages de journal système lorsque la route reçoit des paquets LSA de type 6 OSPF multidiffusion (MOSPF) non pris en charge, procédez comme suit :

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Process Instances** (Instances de processus).

Étape 3 Choisissez le processus OSPFv3 que vous souhaitez modifier, puis cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPFv3 Process Advanced Properties (Modifier les propriétés avancées du processus OSPFv3) apparaît.

Étape 4 Cochez la case **Ignore LSA MOSPF** (Ignorer LSA MOSPF), puis cliquez sur **OK**.

Calculer les coûts récapitulatifs de la route

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Process Instances** (Instances de processus).

Étape 3 Choisissez le processus OSPF que vous souhaitez modifier, puis cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPFv3 Process Advanced Properties (Modifier les propriétés avancées du processus OSPFv3) apparaît.

Étape 4 Cochez la case **RFC1583 Compatible** (Compatible avec RFC 1583), puis cliquez sur **OK**.

Générer une route externe par défaut dans un domaine de routage OSPFv3

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

Étape 2 Cliquez sur l'onglet **Process Instances** (Instances de processus).

Étape 3 Choisissez le processus OSPFv3 que vous souhaitez modifier, puis cliquez sur **Advanced** (Avancé).

La boîte de dialogue Edit OSPFv3 Process Advanced Properties (Modifier les propriétés avancées du processus OSPFv3) apparaît.

Étape 4 Dans la zone Default Information Originate (Origine des renseignements par défaut), procédez comme suit :

a) Cochez la case **Enable** (Activer) pour activer le processus de routage OSPFv3.

b) Cochez la case **Always advertise** (Toujours annoncer) pour annoncer toujours la route par défaut, qu'elle existe ou non.

c) Saisissez la mesure utilisée pour générer la route par défaut dans le champ Metric (Mesure). Les valeurs de mesure valides sont comprises entre 0 et 16777214. La valeur par défaut est 10.

d) Dans la liste déroulante Metric Type (Type de métrique), choisissez le type de liaison externe associé à la route par défaut annoncée dans le domaine de routage OSPFv3. Les valeurs valides sont les suivantes :

- 1. Route externe de type 1
- 2. Route externe de type 2

La valeur par défaut est la route externe de type 2.

e) Dans la liste déroulante Route Map (Carte de routage), choisissez le processus de routage qui génère la route par défaut si la carte de routage est satisfaite.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Apply** pour enregistrer vos modifications.

Configurer un préfixe de résumé IPv6

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Summary Prefix (Préfixe de résumé)**.

Étape 2 Pour ajouter un nouveau préfixe de résumé, cliquez sur **Add** (Ajouter). Pour modifier un préfixe de résumé existant, cliquez sur **Edit** (Modifier). Pour supprimer un préfixe de résumé, cliquez sur **Delete** (Supprimer).

La boîte de dialogue Add Summary Prefix (Ajouter un préfixe de résumé) ou Edit Summary Prefix (Modifier le préfixe de résumé) s'affiche.

Étape 3 Dans la liste déroulante Process ID (ID de processus), choisissez l'ID de processus.

Étape 4 Saisissez le préfixe IPv6 et la longueur du préfixe dans le champ IPv6 Prefix/Prefix Length (Préfixe IPv6/Longueur du préfixe).

Étape 5 Cochez la case **Advertise** (Annoncer) pour annoncer les routes qui correspondent à la paire préfixe-masque spécifiée. Décochez cette case pour supprimer les routages qui correspondent à la paire préfixe-masque spécifiée.

Étape 6 Dans le champ Tag (Balise), saisissez la valeur de balise que vous pouvez utiliser comme valeur de correspondance pour contrôler la redistribution par le biais de cartes de routage.

Étape 7 Cliquez sur **OK**.

Étape 8 Cliquez sur **Apply** pour enregistrer vos modifications.

Redistribuer les routes IPv6

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Redistribution**.

Étape 2 Pour ajouter de nouveaux paramètres afin de redistribuer les routes connectées dans un processus OSPFv3, cliquez sur **Add** (Ajouter). Pour modifier les paramètres existants afin de redistribuer les routes connectées dans un processus OSPFv3, cliquez sur **Edit** (Modifier). Pour supprimer un ensemble de paramètres sélectionné, cliquez sur **Delete** (Supprimer).

La boîte de dialogue Add Redistribution (Ajouter une redistribution) ou Edit Redistribution (Modifier la redistribution) s'affiche.

Étape 3 Dans la liste déroulante Process ID (ID de processus), choisissez l'ID de processus.

Étape 4 Dans la liste déroulante Source Protocol (Protocole source), choisissez le protocole source à partir duquel les routes sont redistribuées. Les protocoles pris en charge sont ceux qui sont connectés, statiques et OSPF.

Étape 5 Saisissez la valeur de mesure dans le champ Metric (Mesure). Lors de la redistribution de routes d'un processus OSPF dans un autre processus OSPF sur le même routeur, la mesure est transmise d'un processus à l'autre si aucune valeur de mesure n'est spécifiée. Lors de la redistribution d'autres processus dans un processus OSPF, la mesure par défaut est 20 lorsqu'aucune valeur de mesure n'est spécifiée.

Étape 6 Dans la liste déroulante Metric Type (Type de mesure), choisissez le type de mesure. Les options disponibles sont Aucune, 1 et 2.

Étape 7 (Facultatif) Saisissez la valeur de la balise dans le champ Tag (Balise). Ce paramètre spécifie la valeur décimale de 32 bits associée à chaque route externe, qui peut être utilisée pour communiquer des informations entre ASBR. Si aucune valeur n'est spécifiée, le numéro du système autonome distant est utilisé pour les routages de BGP et EGP. Pour les autres protocoles, zéro est utilisé. Les valeurs valides sont comprises entre 0 et 4294967295.

Étape 8 Choisissez la carte de routage à partir de la liste déroulante Route Map (Carte de routage) pour vérifier le filtrage de l'importation des routes du protocole de routage source au protocole de routage actuel. Si ce paramètre n'est pas spécifié, toutes les routes sont redistribuées. Si ce paramètre est spécifié, mais qu'aucune étiquette de carte de routage n'est répertoriée, aucune route n'est importée.

Étape 9 Pour inclure les routes connectées dans la redistribution, cochez la case **Include connected** (Inclure les routes connectées).

Étape 10 Cochez la case **Match** (Correspondance) pour redistribuer les routes dans d'autres domaines de routage, puis cochez l'une des cases suivantes :

- **Internal** (Interne) pour les routages internes à un système autonome spécifique
- **External 1** (Externe 1) pour les routes externes au système autonome, mais importées dans OSPFv3 en tant que routes externes de type 1
- **External 2** (Externe 2) pour les routes externes au système autonome, mais importées dans OSPFv3 en tant que routes externes de type 2
- **NSSA External 1** (NSSA Exerne 1) pour les routes externes au système autonome, mais importées dans OSPFv3 dans une NSSA pour IPv6 en tant que routes externes de type 1
- **NSSA External 2** (NSSA Externe 2) pour les routes externes au système autonome, mais importées dans OSPFv3 dans une NSSA pour IPv6 en tant que routes externes de type 2

Étape 11 Cliquez sur **OK**.

Étape 12 Cliquez sur **Apply** pour enregistrer vos modifications.

Configurer le redémarrage progressif

L'ASA peut connaître des situations de défaillance connues qui ne devraient pas affecter le transfert de paquets sur la plateforme de commutation. La capacité de transfert sans arrêt (NSF) permet au transfert de données de se poursuivre le long des routes connues, pendant la restauration des informations du protocole de routage.

En mode de haute disponibilité, le processus OSPF redémarre lorsque l'unité active devient inactive et que l'unité en veille devient la nouvelle active. De même, en mode grappe, le processus OSPF redémarre lorsque l'unité de contrôle devient inactive et que l'unité de données est choisie comme nouvelle unité de contrôle. Ces processus de transition OSPF entraînent un retard considérable. Vous pouvez configurer NSF pour éviter

la perte de trafic lors du changement d'état du processus OSPF. La fonctionnalité NSF est également utile lorsqu'une mise à niveau logicielle rapide est planifiée.

Le redémarrage progressif est pris en charge sur les protocoles OSPFv2 et OSPFv3. Vous pouvez configurer le redémarrage progressif sur OSPFv2 en utilisant NSF IETF (RFC 3623). Vous pouvez configurer le redémarrage progressif sur OSPFv3 à l'aide du redémarrage progressif (RFC 5187).

La configuration de la fonction de redémarrage progressif NSF comporte deux étapes : la configuration des capacités et la configuration d'un périphérique compatible avec NSF ou conscient de NSF. Un périphérique compatible NSF peut indiquer ses propres activités de redémarrage aux voisins, et il peut aider un voisin qui redémarre.

Un périphérique peut être configuré comme compatible NSF ou comme conscient de NSF, selon certaines conditions :

- Un périphérique peut être configuré comme compatible NSF, quel que soit le mode dans lequel il se trouve.
- Un périphérique doit être en mode de basculement ou de grappe EtherChannel étendu (L2) pour être configuré comme compatible NSF.
- Pour qu'un périphérique soit compatible NSF ou conscient de NSF, il doit être configuré de manière à traiter les blocs couvrant les publicités d'état de liaison (LSA) opaques et les signalisations locales de liaison (LLS), selon les besoins.

Remarque Lorsque des Hello rapides sont configurés pour le protocole OSPFv2, le redémarrage progressif ne se produit pas lorsque l'unité active est rechargée et que l'unité en veille devient active. En effet, le temps nécessaire au changement de rôle est supérieur à l'intervalle de temps mort configuré.

Configuration du redémarrage progressif pour OSPFv2

Il existe deux mécanismes de redémarrage progressif pour OSPFv2, Cisco NSF et IETF NSF. Un seul de ces mécanismes de redémarrage progressif peut être configuré à la fois pour une instance ospf. Un périphérique conscient de NSF peut être configuré à la fois comme assistant NSF Cisco et comme assistant NSF IETF, mais un périphérique compatible avec NSF peut être configuré en mode Cisco NSF ou IETF NSF à la fois pour une instance ospf.

Configurer le redémarrage progressif de Cisco NSF pour OSPFv2

Configurez le redémarrage progressif de Cisco NSF pour OSPFv2, pour un périphérique compatible avec NSF ou conscient de NSF.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPF > Setup (Configuration) > Advanced (Avancé) > Add NSF Properties (Ajouter des propriétés NSF).

Étape 2 Sous Configuring Cisco NSF (Configuration de Cisco NSF), cochez la case Enable Cisco nonstop forwarding (NSF) (Activer le transfert sans arrêt Cisco (NSF)).

Étape 3 (Facultatif) Cochez la case Cancels NSF restart when non-NSF-aware neighboring networking devices are detected (Annuler le redémarrage de NSF lorsque des appareils réseau voisins non sensibles à NSF sont détectés), le cas échéant.

Étape 4 (Facultatif) Sous Configuring Cisco NSF helper (Configuration de l'assistance Cisco NSF), décochez la case Enable Cisco nonstop forwarding (NSF) (Activer le transfert sans arrêt Cisco (NSF)) pour le mode d'assistance.

Remarque Cette option est cochée par défaut. Décochez cette case pour désactiver le mode d'assistance Cisco NSF sur un périphérique conscient de NSF.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Apply** pour enregistrer vos modifications.

Configuration de la minuterie d'attente de redémarrage progressif pour le OSPF

Configurez le redémarrage progressif IETF NSF pour OSPFv2, pour un périphérique compatible avec NSF ou conscient de NSF.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPF > Setup (Configuration) > Advanced (Avancé) > Add NSF Properties (Ajouter des propriétés NSF)**.

Étape 2 Sous Configuring IETF NSF (Configuration IETF NSF), cochez la case Enable IETF nonstop forwarding (NSF) (Activer le transfert sans arrêt IETF (NSF)).

Étape 3 (Facultatif) Entrez l'intervalle de redémarrage en secondes dans le champ Length of graceful restart interval (Durée de l'intervalle de redémarrage progressif).

Remarque La valeur par défaut est 120secondes. Pour un intervalle de redémarrage inférieur à 30 secondes, le redémarrage progressif sera interrompu.

Étape 4 (Facultatif) Sous Configuring IETF NSF helper (Configuration de l'assistance IETF NSF), décochez la case Enable IETF nonstop forwarding (NSF) (Activer le transfert sans arrêt IETF (NSF)) pour le mode d'assistance.

Cette option est cochée par défaut. Décochez cette case pour désactiver le mode d'assistance IETF NSF sur un périphérique conscient de NSF.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Apply** pour enregistrer vos modifications.

Configuration du redémarrage progressif pour OSPFv3

La configuration de la fonctionnalité de redémarrage progressif NSF pour OSPFv3 comporte deux étapes : la configuration d'un périphérique pour qu'il soit compatible NSF, puis la configuration d'un périphérique pour qu'il soit conscient de NSF.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPFv3 > Setup (Configuration) > Advanced (Avancé) > Add NSF Properties (Ajouter des propriétés NSF)**.

Étape 2 Sous Configuring Graceful Restart (Configuration du redémarrage progressif), cochez la case Enable Graceful Restart (Activer le redémarrage progressif).

Étape 3 (Facultatif) Saisissez une valeur pour l'intervalle de redémarrage dans le champ Restart Interval (Intervalle de redémarrage).

Remarque La valeur par défaut est 120secondes. Pour un intervalle de redémarrage inférieur à 30 secondes, le redémarrage progressif sera interrompu.

Étape 4 Sous Configuring Graceful Restart Helper (Configuration de l'assistance au redémarrage progressif), cochez la case Enable Graceful Restart Helper (Activer l'assistance au redémarrage progressif).

Cette option est cochée par défaut. Décochez cette case pour désactiver le mode d'assistance au redémarrage progressif sur un périphérique compatible avec NSF.

Étape 5 (Facultatif) Cochez la case Enable LSA (Activer LSA) pour activer la vérification stricte des déclarations de l'état des liens.

Lorsqu'elle est cochée, elle indique que le routeur d'assistance mettra fin au processus de redémarrage du routeur s'il détecte une modification d'un LSA qui serait débordé vers le routeur qui redémarre, ou si un LSA modifié figure sur la liste de retransmission du routeur qui redémarre lorsque le processus de redémarrage progressif est lancé.

Étape 6 Cliquez sur **OK**.

Étape 7 Cliquez sur **Apply** pour enregistrer vos modifications.

Configuration de la minuterie d'attente de redémarrage progressif pour OSPF

On s'attend à ce que les routeurs OSPF définissent le bit RS dans l'EO-TLV associé à un paquet Hello lorsqu'on ne sait pas que tous les voisins sont répertoriés dans le paquet, mais que les routeurs qui redémarrent doivent conserver leurs contiguïtés. Cependant, la valeur du bit RS ne doit pas être supérieure aux secondes de RouterDeadInterval. Par conséquent, la commande **timers nsf wait** est introduite pour définir le bit RS dans les paquets Hello inférieurs aux secondes de RouterDeadInterval. La valeur par défaut de la minuterie d'attente de NSF est de 20 secondes.

Avant de commencer

- Pour configurer le délai d'attente de Cisco NSF pour OSPF, le périphérique doit être conscient de NSF ou compatible avec NSF.

Procédure

Étape 1 Entrez en mode de configuration du routeur OSPF.

Exemple :

```
ciscoasa(config)# router ospf
```

Étape 2 Entrez les minuteries et spécifiez nsf.

Exemple :

```
ciscoasa(config-router)# timers?
router mode commands/options:
  lsa       OSPF LSA timers
  nsf       OSPF NSF timer
  pacing    OSPF pacing timers
  throttle  OSPF throttle timers
ciscoasa(config-router)# timers nsf ?
```

Étape 3 Saisissez l'intervalle d'attente du redémarrage progressif. Cette valeur peut être comprise entre 1 et 65 535.

Exemple :

```
ciscoasa(config-router)# timers nsf wait 200
```

En utilisant l'intervalle d'attente du redémarrage progressif, vous pouvez vous assurer que l'intervalle d'attente n'est pas supérieur à l'intervalle de temps mort du routeur.

Supprimer la configuration OSPFv2

Supprimez la configuration OSPFv2.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.

Étape 2 Décochez la case **Enable this OSPF Process** (Activer ce processus OSPF).

Étape 3 Cliquez sur **Apply** (Appliquer).

Supprimer la configuration OSPFv3

Supprimez la configuration OSPFv3.

Procédure

Étape 1 Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.

Étape 2 Décochez la case **Enable this OSPFv3 Process** (Activer ce processus OSPFv3).

Étape 3 Cliquez sur **Apply** (Appliquer).

Exemple de protocole OSPFv2

L'exemple suivant montre comment activer et configurer le protocole OSPFv2 avec différents processus facultatifs :

1. Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.
2. Cliquez sur l'onglet **Process Instances** (Instances de processus) et dans le champ OSPF Process 1 (Processus 1 d'OSPF), tapez **2**.
3. Cliquez sur l'onglet **Area/Networks** (Zone/Réseaux), puis cliquez sur **Add** (Ajouter).
4. Saisissez **0** dans le champ Area ID (ID de zone).
5. Dans la zone Area Networks (Réseaux de zone), saisissez **10.0.0.0** dans le champ IP Address (Adresse IP).
6. Sélectionnez 255.0.0.0 dans la liste déroulante Netmask (Masque réseau).
7. Cliquez sur **OK**.
8. Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Redistribution**.
9. Cliquez sur **Add** (ajouter).

   La boîte de dialogue Add/Edit OSPF Redistribution Entry (Ajouter/modifier une entrée de redistribution OSPF) apparaît.
10. Dans la zone Protocol (Protocole), cliquez sur le bouton radio **OSPF** pour choisir le protocole source à partir duquel les routes sont redistribuées. Choisir OSPF redistribue les routes à partir d'un autre processus de routage OSPF.
11. Choisissez l'ID de processus OSPF dans la liste déroulante OSPF Process (Processus OSPF).
12. Dans la zone Match (Correspondance), cochez la case **Internal** (Interne).
13. Dans le champ Metric Value (Valeur de la mesure), saisissez **5** pour la valeur de mesure des routes redistribuées.
14. Dans la liste déroulante Metric Type (Type de mesure), choisissez 1 pour la valeur de type de mesure.
15. Dans la liste déroulante Route Map (Carte de routage), choisissez 1.

16. Cliquez sur **OK**.
17. Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Interface**.
18. Dans l'onglet Properties (Propriétés), choisissez l'interface **inside** (interne) et cliquez sur **Edit** (Modifier).

    La boîte de dialogue Edit OSPF Properties (Modifier les propriétés OSPF) apparaît.
19. Dans le champ Cost (Coût), saisissez **20**.
20. Cliquez sur **Advanced** (Avancé).
21. Dans le champ Retransmit Interval (Intervalle de retransmission), saisissez **15**.
22. Dans le champ Transmit Delay (Délai de transmission), saisissez **20**.
23. Dans le champ Hello Interval (Intervalle Hello), saisissez **10**.
24. Dans le champ Dead Interval (Intervalle de temps mort), saisissez **40**.
25. Cliquez sur **OK**.
26. Dans la boîte de dialogue Edit OSPF Properties (Modifier les propriétés OSPF), saisissez **20** dans le champ Properties (Priorités), puis cliquez sur **OK**.
27. Cliquez sur l'onglet **Authentication** (Authentification).

    La boîte de dialogue Edit OSPF Authentication (Modifier l'authentification OSPF) s'affiche.
28. Dans la zone Authentication (Authentification), cliquez sur le bouton radio **MD5**.
29. Dans la zone MD5 and Key ID (ID de clé), saisissez **cisco** dans le champ MD5 Key (Clé MD5) et **1** dans le champ MD5 Key ID (ID de clé MD5).
30. Cliquez sur **OK**.
31. Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**, puis cliquez sur l'onglet **Area/Networks** (Zone/Réseaux).
32. Choisissez le processus **OSPF 2** et cliquez sur **Edit** (Modifier).

    La boîte de dialogue Edit OSPF Area (Modifier une zone OSPF) apparaît.
33. Dans la zone Area Type (Type de zone), choisissez **Stub**.
34. Dans la zone Authentication (Authentification), choisissez **None** (Aucun), et saisissez **20** dans le champ Default Cost (Coût par défaut).
35. Cliquez sur **OK**.
36. Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPF** > **Setup (Configuration)**.
37. Cliquez sur l'onglet **Process Instances** (Instances de processus) et cochez la case **OSPF process 2** (Processus 2 d'OSPF).
38. Cliquez sur **Advanced** (Avancé).

    La boîte de dialogue Edit OSPF Area (Modifier une zone OSPF) apparaît.

39. Dans la zone Timers (Minuteries), saisissez **10** dans le champ SPF Delay Time (Délai d'attente SPF) et **20** dans le champ SPF Hold Time (Délai de rétention SPF).
40. Dans la zone Adjacency Changes (Modifications de contiguïté), cochez la case **Log Adjacency Change Details** (Journaliser les détails des modifications de contiguïté).
41. Cliquez sur **OK**.
42. Cliquez sur **Reset** (Réinitialiser).

Exemples de protocole OSPFv3

L'exemple suivant montre comment configurer le routage OSPFv3 dans ASDM :

1. Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Setup (Configuration)**.
2. Sous l'onglet Process Instances (Instances de processus), procédez comme suit :
    1. Cochez la case **Enable this OSPFv3 Process** (Activer ce processus OSPFv3).
    2. Saisissez **1** dans le champ Process ID (ID de processus).
3. Cliquez sur l'onglet **Areas** (Zones), puis sur **Add** (Ajouter) pour afficher la boîte de dialogue Add OSPFv3 Area (Ajouter une zone OSPFv3).
4. Dans la liste déroulante OSPFv3 Process ID (ID de processus OSPFv3), choisissez **1**.
5. Saisissez **22** dans le champ Area ID (ID de zone).
6. Choisissez **Normal** dans la liste déroulante Area Type (Type de zone).
7. Saisissez **10** dans le champ Default Cost (Coût par défaut).
8. Cochez la case **Redistribution imports routes to normal and NSSA areas** (La redistribution importe les routes dans les zones normales et NSSA).
9. Saisissez **20** dans le champ Metric (Mesure).
10. Choisissez **1** dans la liste déroulante Metric Type (Type de mesure).
11. Cochez la case **inside** (interne) en tant qu'interface spécifiée.
12. Cochez la case **Enable Authentication** (Activer l'authentification).
13. Saisissez **300** dans le champ Security Policy Index (Indice de la politique de sécurité).
14. Choisissez **SHA-1** dans la liste déroulante Authentication Algorithm (Algorithme d'authentification).
15. Saisissez **12345ABCDE** dans le champ Authentication Key (Clé d'authentification).
16. Choisissez **DES** dans la liste déroulante Encryption Algorithm (Algorithme de chiffrement).
17. Saisissez **1122334455aabbccddee** dans le champ Encryption Key (Clé de chiffrement).
18. Cliquez sur **OK**.

19. Cliquez sur l'onglet **Route Summarization** (Synthèse du routage), puis sur **Add** (Ajouter) pour afficher la boîte de dialogue Add Route Summarization (Ajouter la synthèse du routage).
20. Choisissez **1** dans la liste déroulante Process ID (ID de processus).
21. Choisissez **22** dans la liste déroulante Area ID (ID de zone).
22. Saisissez **2000:122::/64** dans le champ IPv6 Prefix/Prefix Length (Préfixe IPv6/Longueur du préfixe).
23. (Facultatif) Saisissez **100** dans le champ Cost (Coût).
24. Cochez la case **Advertised** (Annoncé).
25. Cliquez sur **OK**.
26. Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **OSPFv3** > **Interface**.
27. Cliquez sur l'onglet **Properties** (Propriétés).
28. Cochez la case **inside** (interne) et cliquez sur **Edit** (Modifier) pour afficher la boîte de dialogue Edit OSPF Properties (Modifier les propriétés OSPF).
29. Dans le champ Cost (Coût), saisissez **20**.
30. Saisissez **1** dans le champ Priority (Priorité).
31. Cochez la case **point-to-point** (point à point).
32. Dans le champ Dead Interval (Intervalle de temps mort), saisissez **40**.
33. Dans le champ Hello Interval (Intervalle Hello), saisissez **10**.
34. Dans le champ Retransmit Interval (Intervalle de retransmission), saisissez **15**.
35. Dans le champ Transmit Delay (Délai de transmission), saisissez **20**.
36. Cliquez sur **OK**.
37. Dans la fenêtre principale d'ASDM, choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Redistribution**.
38. Choisissez **1** dans la liste déroulante Process ID (ID de processus).
39. Choisissez **OSPF** dans la liste déroulante Source Protocol (Protocole source).
40. Saisissez **50** dans le champ Metric (Mesure).
41. Choisissez **1** dans la liste déroulante Metric Type (Type de mesure).
42. Cliquez sur **OK**.
43. Cliquez sur **Apply** pour enregistrer vos modifications.

Supervision OSPF

Vous pouvez afficher des statistiques spécifiques, comme le contenu des tables de routage IP, des caches et des bases de données. Vous pouvez également utiliser les renseignements fournis pour déterminer l'utilisation

des ressources et résoudre les problèmes de réseau. Vous pouvez également afficher des renseignements sur l'accessibilité des nœuds et découvrir le chemin de routage emprunté par les paquets de votre périphérique à travers le réseau.

Pour superviser ou afficher diverses statistiques de routage OSPFv2 dans ASDM, procédez comme suit :

1. Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **OSPF LSAs (LSA OSPF)**.
2. Vous pouvez sélectionner et superviser les LSA OSPF de type 1 à 5 et 7. Chaque volet affiche un type de LSA, comme suit :
   - Les LSA de type 1 représentent les routes d'une zone en vertu d'un processus.
   - Les LSA de type 2 affichent l'adresse IP du routeur désigné qui annonce les routeurs.
   - Les LSA de type 3 affichent l'adresse IP du réseau de destination.
   - Les LSA de type 4 affichent l'adresse IP du routeur de limite AS.
   - Les LSA de type 5 et de type 7 affichent l'adresse IP du réseau externe de l'AS.
3. Cliquez sur **Refresh** (Actualiser) pour mettre à jour chaque volet de type LSA.
4. Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **OSPF Neighbors (Voisins OSPF)**.

   Dans le volet OSPF Neighbors (Voisins OSPF), chaque ligne représente un voisin OSPF. De plus, le volet OSPF Neighbors (Voisins OSPF) affiche le réseau sur lequel le voisin s'exécute, la priorité, l'état, la durée de temps mort en secondes, l'adresse IP du voisin et l'interface sur laquelle il s'exécute. Pour obtenir la liste des états possibles pour un voisin OSPF, consultez la RFC 2328.
5. Cliquez sur **Refresh** (Actualiser) pour mettre à jour le volet OSPF Neighbors (Voisins OSPF).

Pour superviser ou afficher diverses statistiques de routage OSPFv3 dans ASDM, procédez comme suit :

1. Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **OSPFv3 LSAs (LSA OSPFv3)**.
2. Vous pouvez sélectionner et superviser les LSA OSPFv3. Choisissez un type d'état de liaison pour afficher son état en fonction des paramètres spécifiés dans la liste déroulante Link State type (Type d'état de liaison). Les types d'états de liaison pris en charge sont les suivants : routeur, réseau, préfixe inter-zone, routeur inter-zone, AS externe, NSSA, liaison et préfixe intra-zone.
3. Cliquez sur **Refresh** (Actualiser) pour mettre à jour chaque type d'état de liaison.
4. Dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision)** > **Routing (Routage)** > **OSPFv3 Neighbors (Voisins OSPFv3)**.

   Dans le volet OSPFv3 Neighbors (Voisins OSPFv3), chaque ligne représente un voisin OSPFv3. De plus, le volet OSPFv3 Neighbors (Voisins OSPFv3) affiche l'adresse IP du voisin, la priorité, l'état, la durée de temps mort en secondes et l'interface sur laquelle il s'exécute. Pour obtenir la liste des états possibles pour un voisin OSPFv3, consultez la RFC 5340.
5. Cliquez sur **Refresh** (Actualiser) pour mettre à jour le volet OSPFv3 Neighbors (Voisins OSPFv3).

Historique OSPF

Tableau 1 : Historique des fonctionnalités OSPF

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge OSPF	7.0(1)	Une prise en charge a été ajoutée pour les données de routage, l'authentification, la redistribution et la supervision des informations de routage à l'aide du protocole de routage Open Shortest Path First (OSPF). Nous avons introduit l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPF.
Routage dynamique en mode de contexte multiple	9.0(1)	Le routage OSPFv2 est pris en charge en mode de contexte multiple. Nous avons modifié l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPF > Setup (Configuration)
Mise en grappe	9.0(1)	Pour OSPFv2 et OSPFv3, la synchronisation groupée, la synchronisation du routage et l'équilibrage de charges EtherChannel étendu sont pris en charge dans l'environnement de mise en grappe.
Prise en charge OSPFv3 pour IPv6	9.0(1)	Le routage OSPFv3 est pris en charge pour IPv6. Nous avons introduit les écrans suivants : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPFv3 > Setup, Configuration (Configuration) > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPFv3 > Interface, Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPFv3 > Redistribution, Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPFv3 > Summary Prefix (Préfixe du sommaire), Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPFv3 > Virtual Link, Monitoring (Lien virtuel, Supervision) > Routing (Routage) > OSPFv3 LSAs (LSA OSPFv3), Monitoring (Supervision) > Routing (Routage) > OSPFv3 Neighbors (Voisins OSPFv3).
Prise en charge OSPF pour les Hellos rapides	9.2(1)	OSPF prend en charge la fonctionnalité Paquets Hello rapides, ce qui permet d'obtenir une configuration qui accélère la convergence dans un réseau OSPF. Nous avons modifié l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPF > Interface > Edit OSPF Interface (Modifier les propriétés avancées de l'interface OSPF)
Minuteries	9.2(1)	De nouvelles minuteries OSPF ont été ajoutées; les anciennes ont été rendues obsolètes. Nous avons modifié l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPF > Setup (Configuration) > Edit OSPF Process Advanced Properties (Modifier les propriétés avancées du processus OSPF)

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Filtrage des routes à l'aide de la liste d'accès	9.2(1)	Le filtrage des routes à l'aide d'ACL est désormais pris en charge. Nous avons introduit l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPF > Filtering Rules (Règles de filtrage) > Add Filter Rules (Ajouter des règles de filtre)
Améliorations de la surveillance OSPF	9.2(1)	Des informations supplémentaires sur la surveillance OSPF ont été ajoutées.
OSPF redistribue le BGP	9.2(1)	La fonctionnalité de redistribution OSPF a été ajoutée. Nous avons ajouté l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPF > Redistribution
Prise en charge OSPF pour la transmission sans interruption (NSF)	9.3(1)	La prise en charge des protocoles OSPFv2 et OSPFv3 pour NSF a été ajoutée. Nous avons ajouté les écrans suivants : Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPF > Setup (Configuration) > NSF Properties (Propriétés du NSF), Configuration > Device Setup (Configuration de l'appareil) > Routing (Routage) > OSPFv3 > Setup (Configuration) > NSF Properties (Propriétés du NSF)
Prise en charge OSPF pour la transmission sans interruption (NSF)	9.13(1)	La minuterie d'attente NSF a été ajoutée. Nous avons ajouté une nouvelle commande pour définir la minuterie de l'intervalle de redémarrage NSF. Cette commande a été introduite pour s'assurer que l'intervalle d'attente n'est pas plus long que l'intervalle de temps mort du routeur. Nous avons introduit la commande suivante : **timers nsf wait <seconds>**

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.

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.

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.

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.

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.

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.

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.