

Interfaces en mode routage et en mode transparent

Ce chapitre comprend des tâches pour terminer la configuration de l'interface pour tous les modèles en mode de pare-feu routé ou transparent.

Remarque Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Dans le volet Configuration > Liste des périphériques, double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif.

- À propos des interfaces en mode routage et en mode transparent, à la page 1
- Directives et limites pour les interfaces en mode routé et en mode transparent, à la page 3
- Configurer les interfaces en mode routé, à la page 6
- Configurer les interfaces de groupe de ponts, à la page 10
- Configuration de l'adressage IPv6, à la page 15
- Supervision des interfaces en mode routé et en mode transparent, à la page 27
- Exemples d'interfaces en mode routé et en mode transparent, à la page 30
- Historique des interfaces en mode routé et en mode transparent, à la page 33

À propos des interfaces en mode routage et en mode transparent

L'ASA prend en charge deux types d'interfaces : routées et pontées.

Chaque interface routée de couche 3 nécessite une adresse IP sur un sous-réseau unique.

Les interfaces pontées appartiennent à un groupe de ponts et toutes les interfaces se trouvent sur le même réseau. Le groupe de ponts est représenté par une interface virtuelle de pont (BVI) qui a une adresse IP sur le réseau de ponts. Le mode routé prend en charge les interfaces routées et pontées, et vous pouvez effectuer le routage entre des interfaces routées et des BVI. Le mode de pare-feu transparent ne prend en charge que les interfaces de groupe de ponts et BVI.

Niveaux de sécurité

Chaque interface doit avoir un niveau de sécurité de 0 (le plus bas) à 100 (le plus élevé), y compris les interfaces membres d'un groupe de ponts. Par exemple, vous devez affecter votre réseau le plus sécurisé, comme le réseau d'hôte interne, au niveau 100. Le réseau externe connecté à Internet peut quant à lui être attribué au niveau 0. D'autres réseaux, tels que les DMZ, peuvent être entre les deux. Vous pouvez attribuer des interfaces au même niveau de sécurité.

L'attribution d'un niveau de sécurité à une BVI dépend du mode de pare-feu. En mode transparent, l'interface BVI n'a pas de niveau de sécurité, car elle ne participe pas au routage entre les interfaces. En mode routé, les interfaces BVI ont un niveau de sécurité si vous choisissez d'effectuer le routage entre les BVI et d'autres interfaces. Pour le mode routé, le niveau de sécurité d'une interface membre d'un groupe de ponts s'applique uniquement à la communication au sein du groupe de ponts. De même, le niveau de sécurité BVI s'applique uniquement à la communication inter-BVI/interface de couche 3.

Le niveau contrôle le comportement suivant :

- Accès au réseau : par défaut, il existe une autorisation implicite d'une interface de sécurité supérieure vers une interface de sécurité inférieure (sortante). Les hôtes de l'interface de sécurité supérieure peuvent accéder à n'importe quel hôte sur une interface de sécurité inférieure. Vous pouvez limiter l'accès en appliquant une ACL à l'interface.

  Si vous activez la communication pour des interfaces de même sécurité, il existe une autorisation implicite pour que les interfaces accèdent à d'autres interfaces sur le même niveau de sécurité ou un niveau de sécurité inférieur.

- Moteurs d'inspection : certains moteurs d'inspection d'applications dépendent du niveau de sécurité. Pour les interfaces de même sécurité, les moteurs d'inspection s'appliquent au trafic dans l'une ou l'autre direction.
  - Plateforme d'inspection NetBIOS : s'applique uniquement aux connexions sortantes.
  - Plateforme d'inspection SQL*Net : si une connexion de contrôle pour le port SQL*Net (anciennement OraServ) existe entre une paire d'hôtes, seule une connexion de données entrante est autorisée par l'ASA.

Double pile IP (IPv4 et IPv6)

L'ASA prend en charge les adresses IPv6 et IPv4 sur une interface. Assurez-vous de configurer une voie de routage par défaut pour IPv4 et IPv6.

Masque de sous-réseau 31 bits

Pour les interfaces routées, vous pouvez configurer une adresse IP sur un sous-réseau de 31 bits pour les connexions point à point. Le sous-réseau de 31 bits comprend seulement 2 adresses; normalement, la première et la dernière adresse du sous-réseau sont réservées pour le réseau et la diffusion, donc un sous-réseau à deux adresses n'est pas utilisable. Toutefois, si vous avez une connexion point à point et n'avez pas besoin d'adresses de réseau ou de diffusion, un sous-réseau de 31 bits est un moyen utile de conserver les adresses dans IPv4. Par exemple, la liaison de basculement entre 2 ASA ne nécessite que 2 adresses; les paquets transmis par une extrémité de la liaison sont toujours reçus par l'autre extrémité, et la diffusion n'est pas nécessaire. Vous pouvez également avoir une station de gestion directement connectée exécutant SNMP ou Syslog.

Sous-réseau 31 bits et mise en grappe

Vous pouvez utiliser un masque de sous-réseau de 31 bits de grappe en mode de mise en grappe étendue, à l'exclusion de l'interface de gestion et de la liaison de commande de grappe.

Vous ne pouvez pas utiliser un masque de sous-réseau de 31 bits en mode de mise en grappe individuelle sur une interface.

Sous-réseau 31 bits et basculement

Pour le basculement, lorsque vous utilisez un sous-réseau de 31 bits pour l'adresse IP d'interface ASA, vous ne pouvez pas configurer d'adresse IP de secours pour l'interface, car il n'y a pas assez d'adresses. Normalement, une interface de basculement doit avoir une adresse IP de secours pour que l'unité active puisse effectuer des tests d'interface pour s'assurer de l'intégrité de l'interface de secours. Sans adresse IP de secours, ASA ne peut effectuer aucun test de réseau. seul l'état du lien peut être suivi.

Pour le basculement et le lien à état séparé facultatif, qui sont des connexions point à point, vous pouvez également utiliser un sous-réseau de 31 bits.

Gestion et sous-réseau 31 bits

Si vous avez une station de gestion directement connectée, vous pouvez utiliser une connexion point à point pour SSH ou HTTP sur ASA, ou pour SNMP ou Syslog sur le poste de gestion.

Fonctionnalités 31 bits non prises en charge

Les fonctionnalités suivantes ne prennent pas en charge le sous-réseau de 31 bits :

- Interfaces BVI pour les groupes de ponts : le groupe de ponts nécessite au moins 3 adresses d'hôte : les BVI et deux hôtes connectés à deux interfaces membres du groupe de ponts. vous devez utiliser un sous-réseau /29 ou moins.
- Routage multidiffusion

Directives et limites pour les interfaces en mode routé et en mode transparent

Mode contextuel

- En mode de contexte multiple, vous pouvez seulement configurer les interfaces de contexte que vous avez déjà affectées au contexte dans la configuration système en fonction de Configurer plusieurs contextes.
- PPPoE n'est pas pris en charge en mode de contexte multiple.
- Pour le mode à contextes multiples en mode transparent, chaque contexte doit utiliser des interfaces différentes; vous ne pouvez pas partager une interface entre contextes.
- Pour le mode à contexte multiple en mode transparent, chaque contexte utilise généralement un sous-réseau différent. Vous pouvez utiliser des sous-réseaux qui se chevauchent, mais la topologie de votre réseau nécessite une configuration de routeur et de NAT pour que cela soit possible du point de vue du routage.

- Les options de délégation de préfixe et de DHCPv6 ne sont pas prises en charge avec le mode de contexte multiple.
- En mode de pare-feu routé, les interfaces de groupes de ponts ne sont pas prises en charge dans le mode de contexte multiple.

Basculement, mise en grappe

- Ne configurez pas les liens de basculement selon les procédures de ce chapitre. Consultez le chapitre Basculement pour plus de renseignements.
- Pour les interfaces de grappe, consultez le chapitre sur la mise en grappe pour connaître les exigences.
- Lorsque vous utilisez Basculement, vous devez définir l'adresse IP et l'adresse de secours pour les interfaces de données manuellement. DHCP et PPPoE ne sont pas pris en charge.

IPv6

- IPv6 est pris en charge sur toutes les interfaces.
- Vous ne pouvez que configurer les adresses IPv6 manuellement en mode transparent.
- L'ASA ne prend pas en charge les adresses anycast IPv6.
- Les options de délégation de préfixe et de DHCPv6 ne sont pas prises en charge avec le mode à contexte multiple, le mode transparent, la mise en grappe ou Basculement.

Directives sur les modèles

- Pour l’ASAv50, les groupes de ponts ne sont pas pris en charge en mode transparent ou routé.
- Pour les périphériques Firepower 2100, les groupes de ponts ne sont pas pris en charge en mode routé.

Directives relatives au mode transparent et au groupe de ponts

- Vous pouvez créer jusqu’à 250 groupes de ponts, avec interfaces par groupe de ponts.
- Chaque réseau connecté directement doit se trouver sur le même sous-réseau.
- L'ASA ne prend pas en charge le trafic sur les réseaux secondaires; seul le trafic sur le même réseau que l’adresse IP BVI est pris en charge.
- Une adresse IP pour les BVI est requise pour chaque groupe de ponts pour le trafic de gestion vers le périphérique et en provenance du périphérique, ainsi que pour le trafic de données qui doit passer par ASA. Pour le trafic IPv4, spécifiez une adresse IPv4. Pour le trafic IPv6, spécifiez une adresse IPv6.
- Vous ne pouvez configurer les adresses IPv6 que manuellement.
- L’adresse IP BVI doit se trouver sur le même sous-réseau que le réseau connecté. Vous ne pouvez pas définir le sous-réseau comme sous-réseau d’hôte (255.255.255.255).
- Les interfaces de gestion ne sont pas prises en charge en tant que membres de groupes de ponts.
- Pour l’ASAv50 sur VMware avec des interfaces ixgbevf pontées, le mode transparent n’est pas pris en charge et les groupes de ponts ne sont pas pris en charge en mode routé.

- Pour Série Firepower 2100, les groupes de ponts ne sont pas pris en charge en mode routé.
- Pour le 200/ 1010/ , il n'est pas possible de mélanger des interfaces VLAN logiques et des interfaces de pare-feu physiques au sein du même groupe de ponts.
- En mode transparent, vous devez utiliser au moins un groupe de ponts; les interfaces de données doivent appartenir à un groupe de ponts.
- En mode transparent, ne spécifiez pas l'adresse IP des BVI comme passerelle par défaut pour les périphériques connectés; Les périphériques doivent spécifier le routeur de l'autre côté de la ASA comme passerelle par défaut.
- En mode transparent, la voie de routage *par défaut*, qui est requise pour fournir un chemin de retour au trafic de gestion, n'est appliquée qu'au trafic de gestion provenant d'un réseau de groupe de ponts. En effet, la voie de routage par défaut spécifie une interface dans le groupe de ponts ainsi que l'adresse IP du routeur sur le réseau du groupe de ponts, et vous ne pouvez définir qu'une seule voie de routage par défaut. Si votre trafic de gestion provient de plus d'un réseau de groupes de ponts, vous devez spécifier une voie de routage statique régulière qui identifie le réseau à partir duquel vous attendez le trafic de gestion.
- Le protocole PPPoE n'est pas pris en charge sur l'interface Management (gestion).
- En mode routé, pour le routage entre les groupes de ponts et les autres interfaces routées, vous devez nommer les BVI.
- En mode routé, les interfaces EtherChannel définies par ASA et VNI ne sont pas prises en charge en tant que membres de groupes de ponts. Les EtherChannels sur Firepower 4100/9300 peuvent être des membres de groupes de ponts.
- Les paquets écho de la détection de transfert bidirectionnel (BFD) ne sont pas autorisés par le biais de l'ASA lors de l'utilisation de membres de groupe de ponts. S'il y a deux voisins de chaque côté de l'ASA exécutant BFD, alors l'ASA abandonnera les paquets écho BFD, car ils ont la même adresse IP de source et de destination et semblent faire partie d'une attaque LAND.

Niveau de sécurité par défaut

Le niveau de sécurité par défaut est 0. Si vous nommez une interface « intérieur » et que vous ne définissez pas explicitement le niveau de sécurité, l'ASA le définit à 100.

Remarque Si vous modifiez le niveau de sécurité d'une interface et que vous ne souhaitez pas attendre que les connexions existantes expirent avant d'utiliser les nouveaux renseignements sur la sécurité, vous pouvez effacer les connexions à l'aide de la commande **clear conn**.

Directives et exigences supplémentaires

- L'ASA ne prend en charge qu'un seul en-tête 802.1Q par paquet et ne prend pas en charge plusieurs en-têtes (appelé prise en charge Q-in-Q).
- Des problèmes d'interface, tels que de fréquents changements d'état haut/bas, peuvent empêcher la minuterie de connexion flottante de s'appliquer correctement aux connexions passant par l'interface. Si vous avez des problèmes avec l'état d'une interface, pensez à effacer toutes les connexions une fois que l'état est stabilisé afin de supprimer les connexions non valides.

Configurer les interfaces en mode routé

Pour configurer les interfaces en mode routé, procédez comme suit.

Configurer les paramètres généraux de l'interface en mode routé

Cette procédure décrit comment définir le nom, le niveau de sécurité, l'adresse IPv4 et d'autres options.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet Configuration > Device List, double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.

Étape 2 Choisissez la ligne d'interface, puis cliquez sur modifier (**Edit**).

La boîte de dialogue **Edit Interface** (modifier l'interface) s'affiche sous l'onglet **General** (général).



Remarque Pour le Firepower 1010, vous ne pouvez pas configurer de ports de commutation en tant qu'interfaces en mode routé.

Étape 3 Dans le champ **Interface Name** (Nom d'interface), saisissez un nom renfermant au maximum 48 caractères.

Étape 4 Dans le champ **Security level** (Niveau de sécurité), saisissez un niveau compris entre 0 (le plus bas) et 100 (le plus élevé).



Remarque Pour les interfaces de boucle avec retour, vous ne définissez pas de niveau de sécurité, car l'interface n'est prise en charge que pour le trafic vers/depuis le périphérique.

Étape 5 (Facultatif) Pour définir cette interface comme une interface de gestion uniquement, cochez la case **Dedicate this interface to management-only** (Dédier cette interface à la gestion uniquement).

Le trafic de transit n'est pas accepté sur une interface de gestion uniquement.



Remarque Le champ Channel Group (Groupe de canaux) est en lecture seule et indique si l'interface fait partie d'un EtherChannel.

Remarque Pour les interfaces de boucle avec retour, vous ne définissez pas le mode de gestion, car l'interface n'est prise en charge que pour le trafic vers/depuis le périphérique.

Étape 6 Si l'interface n'est pas déjà activée, cochez la case **Enable Interface** (Activer l'interface).

Étape 7 Pour définir l'adresse IP, utilisez l'une des options suivantes.

Remarque Pour le basculement et la mise en grappe, ainsi que pour les interfaces de boucle avec retour, vous devez définir l'adresse IP manuellement; les protocoles DHCP et PPPoE ne sont pas pris en charge.

- Pour définir l'adresse IP manuellement, cliquez sur le bouton radio **Use Static IP** (Utiliser l'adresse IP statique) et saisissez l'adresse IP et le masque.

  Pour le basculement, définissez les adresses IP de veille dans l'onglet **Configuration > Device Management (Gestion des périphériques) > High Availability (Haute disponibilité) > Failover (Basculement) > Interfaces**. Si vous ne définissez pas l'adresse IP de veille, l'unité active ne peut pas surveiller l'interface de secours en utilisant des tests réseau; elle ne peut que suivre l'état du lien.

  Pour les connexions point à point, vous pouvez spécifier un filtre d'adresse locale de 31 bits (255.255.255.254). Dans ce cas, aucune adresse IP n'est réservée pour les adresses de réseau ou de diffusion. Vous ne pouvez pas définir l'adresse IP de secours dans ce cas.
- Pour obtenir une adresse IP d'un serveur DHCP, cliquez sur le bouton radio **Obtain Address via DHCP** (Obtenir l'adresse par DHCP).

  1. Pour forcer le stockage d'une adresse MAC dans un paquet de demande DHCP pour l'option 61, cliquez sur le bouton radio **Use MAC Address** (Utiliser l'adresse MAC).

     Certains fournisseurs de services Internet s'attendent à ce que l'option 61 soit l'adresse MAC de l'interface. Si l'adresse MAC n'est pas incluse dans le paquet de demande DHCP, aucune adresse IP ne sera attribuée.

  2. Pour utiliser une chaîne générée pour l'option 61, cliquez sur **Use "Cisco-<MAC>-<interface_name>-<host>"** (Utiliser « Cisco-<MAC>-<interface_name>-<host> »).

  3. (Facultatif) Pour obtenir la route par défaut à partir du serveur DHCP, cochez **Obtain Default Route Using DHCP** (Obtenir la route par défaut en utilisant DHCP).

  4. (Facultatif) Pour attribuer une distance administrative à la route apprise, saisissez une valeur comprise entre 1 et 255 dans le champ **DHCP Learned Route Metric** (Mesure de route apprise par DHCP). Si ce champ est laissé vide, la distance administrative pour les routes apprises est de 1.

  5. (Facultatif) Pour activer le suivi des routes apprises par DHCP, cochez la case **Enable Tracking for DHCP Learned Routes** (Activer le suivi des routes apprises par DHCP). Définissez les paramètres suivants :

     Track ID (ID de suivi) : identifiant unique pour le processus de suivi de routage. Cette valeur peut être comprise entre 1 et 500.

     Track IP Address (Suivre l'adresse IP) : saisissez l'adresse IP de la cible suivie. En règle générale, il s'agit de l'adresse IP de la passerelle de saut suivant pour le routage, mais il peut s'agir de tout objet réseau disponible à partir de cette interface.

Remarque Le suivi de routage n'est disponible qu'en mode routé unique.

SLA ID (ID de SLA) : identifiant unique pour le processus de supervision des SLA. Cette valeur peut être comprise entre 1 et 2147483647.

Monitor Options (Options de surveillance) : cliquez sur ce bouton pour ouvrir la boîte de dialogue **Route Monitoring Options** (Options de surveillance du routage). Dans la boîte de dialogue **Route Monitoring Options** (Options de surveillance du routage), vous pouvez configurer les paramètres du processus de surveillance des objets suivis.

6. (Facultatif) Pour définir l'indicateur de diffusion sur 1 dans l'en-tête de paquet DHCP, lorsque le client DHCP envoie une découverte demandant une adresse IP, cochez la case **Enable DHCP Broadcast flag for DHCP request and discover messages** (Activer l'indicateur de diffusion DHCP pour les demandes DHCP et les messages de découverte).

   Le serveur DHCP écoute cet indicateur de diffusion et diffuse le paquet de réponse si l'indicateur est défini sur 1.

7. (Facultatif) Pour renouveler le bail locatif, cliquez sur **Renew DHCP Lease** (Renouveler le bail locatif DHCP).

- (Mode unique seulement) Pour obtenir une adresse IP en utilisant PPPoE, cochez la case **Use PPPoE** (Utiliser PPPoE).

  1. Dans le champ **Group Name** (Nom de groupe), indiquez un nom de groupe.
  2. Dans le champ **PPPoE Username** (Nom d'utilisateur PPPoE), spécifiez le nom d'utilisateur fourni par votre FAI.
  3. Dans le champ **PPPoE Password** (Mot de passe PPPoE), spécifiez le mot de passe fourni par votre FAI.
  4. Dans le champ **Confirm Password** (Confirmer le mot de passe), retapez le mot de passe.
  5. Pour l'authentification PPP, cliquez sur le bouton radio **PAP**, **CHAP** ou **MSCHAP**.

     Le PAP transmet un nom d'utilisateur et un mot de passe en clair lors de l'authentification et n'est pas sécurisé. Avec le protocole CHAP, le client renvoie le [défi plus mot de passe] chiffré, avec un nom d'utilisateur en texte clair en réponse au défi du serveur. Le protocole CHAP est plus sécurisé que le protocole PAP, mais il ne chiffre pas les données. MSCHAP est similaire à CHAP, mais est plus sécurisé, car le serveur stocke et compare uniquement les mots de passe chiffrés plutôt que les mots de passe en clair comme dans CHAP. MSCHAP génère également une clé pour le chiffrement des données par MPPE.

  6. (Facultatif) Pour stocker le nom d'utilisateur et le mot de passe dans la mémoire flash, cochez la case **Store Username and Password in Local Flash** (Enregistrer le nom d'utilisateur et le mot de passe dans la mémoire flash locale).

     L'ASA stocke le nom d'utilisateur et le mot de passe dans un emplacement spécial de la NVRAM. Si un Auto Update Server envoie une commande **clear configure** à l'ASA et que la connexion est interrompue, l'ASA peut lire le nom d'utilisateur et le mot de passe de NVRAM et s'authentifier de nouveau auprès du concentrateur d'accès.

7. (Facultatif) Pour afficher la boîte de dialogue **PPPoE IP Address and Route Settings** (Paramètres d'adresse IP et de routage PPPoE) dans laquelle vous pouvez choisir les options d'adressage et de suivi, cliquez sur **IP Address and Route Settings** (Paramètres d'adresse IP et de routage).

Étape 8 (Facultatif) Dans le champ **Description**, saisissez une description pour cette interface.

La description peut contenir jusqu'à 240 caractères sur une seule ligne (sans retour chariot). Dans le cas d'une liaison de basculement ou d'état, la description fixe est « LAN Failover Interface », « STATE Failover Interface » ou « LAN/STATE Failover Interface » par exemple. Vous ne pouvez pas modifier cette description. La description fixe remplace toute description que vous saisissez ici si vous faites de cette interface une liaison de basculement ou un lien d'état.

Étape 9 Cliquez sur **OK**.

Sujets connexes

Configuration de l'adressage IPv6, à la page 15
Activer l'interface physique et configurer les paramètres Ethernet
Configurer le protocole PPPoE, à la page 9

Configurer le protocole PPPoE

Si l'interface est connectée à une liaison ADSL, à un modem câble ou à une autre connexion à votre FAI et que ce dernier utilise PPPoE pour vous fournir votre adresse IP, configurez les paramètres suivants.

Procédure

Étape 1 Choisissez **Configuration** > **Interfaces** > **Add/Edit Interface (Ajouter/Modifier une interface)** > **General (Général)**, puis cliquez sur **PPPoE IP Address and Route Settings (Paramètres de route et d'adresse IP PPPoE)**.

Étape 2 Dans la zone **IP Address** (Adresse IP), choisissez l'une des options suivantes :

- **Obtain IP Address using PPP** (Obtenir l'adresse IP en utilisant PPP) : configurez l'adresse IP de manière dynamique.
- **Specify an IP Address** (Spécifier une adresse IP) : configurez manuellement l'adresse IP.

Étape 3 Dans la zone **Route Settings** (Paramètres de routage), configurez les éléments suivants :

- **Obtain default route using PPPoE** (Obtenir la route par défaut à l'aide de PPPoE) : définissez les routes par défaut lorsque le client PPPoE n'a pas encore établi de connexion. Lorsque vous utilisez cette option, vous ne pouvez pas avoir de route définie de manière statique dans la configuration.
- **PPPoE learned route metric** (Mesure de la route apprise à l'aide de PPPoE) : attribuez une distance administrative à la route apprise. Cette valeur peut être comprise entre 1 et 255. Si ce champ est laissé vide, la distance administrative pour les routes apprises est de 1.
- **Enable tracking** (Activer le suivi) : activez le suivi de routage pour les routes apprises à l'aide de PPPoE. Le suivi de routage n'est disponible qu'en mode routé unique.
- **Primary Track** (Suivi principal) : configurez le suivi de routage PPPoE principal.

- **Track ID** (ID de suivi) : identifiant unique pour le processus de suivi de routage. Cette valeur peut être comprise entre 1 et 500.
- **Track IP Address** (Suivre l'adresse IP) : saisissez l'adresse IP de la cible suivie. En règle générale, il s'agit de l'adresse IP de la passerelle de saut suivant pour le routage, mais il peut s'agir de tout objet réseau disponible à partir de cette interface.
- **SLA ID** (ID de SLA) : identifiant unique pour le processus de supervision des SLA. Cette valeur peut être comprise entre 1 et 2147483647.
- **Monitor Options** (Options de surveillance) : cliquez sur ce bouton pour ouvrir la boîte de dialogue **Route Monitoring Options** (Options de surveillance du routage). Dans la boîte de dialogue **Route Monitoring Options** (Options de surveillance du routage), vous pouvez configurer les paramètres du processus de surveillance des objets suivis.
- **Secondary Track** (Suivi secondaire) : configurez le suivi de routage PPPoE secondaire.
- **Secondary Track ID** (ID de suivi secondaire) : identifiant unique pour le processus de suivi de routage. Cette valeur peut être comprise entre 1 et 500.

Étape 4 Cliquez sur **OK**.

Configurer les interfaces de groupe de ponts

Un groupe de ponts est un groupe d'interfaces que ASA relie par des ponts au lieu de routes. Les groupes de ponts sont pris en charge à la fois en mode transparent et en mode pare-feu routé. Pour en savoir plus sur les groupes de ponts, consultez Groupes de ponts.

Pour configurer des groupes de ponts et les interfaces associées, procédez comme suit.

Configurer la BVI (Bridge Virtual Interface)

Chaque groupe de ponts nécessite un BVI pour lequel vous configurez une adresse IP. L'ASA utilise cette adresse IP comme adresse source pour les paquets provenant du groupe de ponts. L'adresse IP BVI doit se trouver sur le même sous-réseau que le réseau connecté. Pour le trafic IPv4, l'adresse IP BVI est requise pour laisser passer le trafic. Pour le trafic IPv6, vous devez, au minimum, configurer les adresses de lien locales pour laisser passer le trafic, mais une adresse de gestion globale est recommandée pour les fonctionnalités complètes, y compris la gestion à distance et d'autres opérations de gestion.

Pour le mode routé, si vous fournissez un nom pour les BVI, alors les BVI participent au routage. Sans nom, le groupe de ponts reste isolé comme en mode transparent de pare-feu.

Certains modèles incluent un groupe de ponts et une BVI dans la configuration par défaut. Vous pouvez créer des groupes de ponts et des BVI supplémentaires et réaffecter des interfaces membres entre les groupes.



Remarque Pour une interface de gestion distincte en mode transparent (pour les modèles pris en charge), un groupe de ponts non configurables (ID 301) est automatiquement ajouté à votre configuration. Ce groupe de ponts n'est pas inclus dans la limite de groupes de ponts.

Procédure

Étape 1 Choisissez **Configuration** > **Interfaces**, puis **Add (Ajouter)** > **Bridge Group Interface (Interface de groupe de pont)**.

Étape 2 Dans le champ **Bridge Group ID** (ID de groupe de ponts), saisissez un ID de groupe de ponts compris entre 1 et 250.

Vous attribuerez ultérieurement des interfaces physiques à ce numéro de groupe de ponts.

Étape 3 (Mode routé) Dans le champ **Interface Name** (Nom d'interface), saisissez un nom de 48 caractères maximum.

Vous devez nommer le BVI si vous souhaitez acheminer le trafic extérieur aux membres du groupe de pont, par exemple vers l'interface externe ou vers les membres d'autres groupes de pont.

Étape 4 (Mode routé) Dans le champ **Security level** (Niveau de sécurité), saisissez un niveau compris entre 0 (le plus bas) et 100 (le plus élevé).

Étape 5 (Mode transparent) Définissez l'adresse IP.

a) Dans le champ **IP Address** (Adresse IP), saisissez l'adresse IPv4.

b) Dans le champ **Subnet Mask** (Filtre d'adresse locale), saisissez le filtre d'adresse locale ou choisissez-en un dans le menu.

N'affectez pas d'adresse hôte (/32 ou 255.255.255.255) au pare-feu transparent. De plus, n'utilisez pas d'autres sous-réseaux contenant moins de 3 adresses d'hôte (une pour le routeur en amont, le routeur en aval et le pare-feu transparent), comme un sous-réseau /30 (255.255.255.252). L'ASA abandonne tous les paquets ARP en provenance ou à destination de la première et de la dernière adresse d'un sous-réseau. Par exemple, si vous utilisez un sous-réseau /30 et que vous affectez une adresse réservée de ce sous-réseau au routeur en amont, l'ASA abandonne la demande ARP du routeur en aval au routeur en amont.

Étape 6 (Mode routé) Pour définir l'adresse IP, utilisez l'une des options suivantes.

Pour le basculement et la mise en grappe, vous devez définir l'adresse IP manuellement; le protocole DHCP n'est pas pris en charge.

- Pour définir l'adresse IP manuellement, cliquez sur le bouton radio **Use Static IP** (Utiliser l'adresse IP statique) et saisissez l'adresse IP et le masque.
- Pour obtenir une adresse IP d'un serveur DHCP, cliquez sur le bouton radio **Obtain Address via DHCP** (Obtenir l'adresse par DHCP).

  1. Pour forcer le stockage d'une adresse MAC dans un paquet de demande DHCP pour l'option 61, cliquez sur le bouton radio **Use MAC Address** (Utiliser l'adresse MAC).

     Certains fournisseurs de services Internet s'attendent à ce que l'option 61 soit l'adresse MAC de l'interface. Si l'adresse MAC n'est pas incluse dans le paquet de demande DHCP, aucune adresse IP ne sera attribuée.

  2. Pour utiliser une chaîne générée pour l'option 61, cliquez sur **Use "Cisco-<MAC>-<interface_name>-<host>"** (Utiliser « Cisco-<MAC>-<interface_name>-<host> »).

  3. (Facultatif) Pour obtenir la route par défaut à partir du serveur DHCP, cochez **Obtain Default Route Using DHCP** (Obtenir la route par défaut en utilisant DHCP).

  4. (Facultatif) Pour définir l'indicateur de diffusion sur 1 dans l'en-tête de paquet DHCP, lorsque le client DHCP envoie une découverte demandant une adresse IP, cochez la case **Enable DHCP**

Broadcast flag for DHCP request and discover messages (Activer l'indicateur de diffusion DHCP pour les demandes DHCP et les messages de découverte).

Le serveur DHCP écoute cet indicateur de diffusion et diffuse le paquet de réponse si l'indicateur est défini sur 1.

5. (Facultatif) Pour renouveler le bail locatif, cliquez sur **Renew DHCP Lease** (Renouveler le bail locatif DHCP).

Étape 7 (Facultatif) Dans le champ **Description**, saisissez une description pour le groupe de ponts.

Étape 8 Cliquez sur **OK**.

Une interface virtuelle de pont (BVI) est ajoutée au tableau d'interfaces, avec les interfaces physiques et sous-interfaces.

Configurer les paramètres généraux de l'interface de membre du groupe de ponts

Cette procédure décrit comment définir le nom, le niveau de sécurité et le groupe de ponts pour chaque interface membre du groupe de ponts.

Avant de commencer

- Un même groupe de ponts peut inclure différents types d'interfaces : des interfaces physiques, des sous-interfaces VLAN, des interfaces VNI et des EtherChannels. Le protocole PPPoE n'est pas pris en charge sur l'interface de gestion. En mode routé, les EtherChannels et les VNI ne sont pas pris en charge.
- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet Configuration > Device List, double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif.
- Pour le mode transparent, n'utilisez pas cette procédure pour les interfaces de gestion; consultez Configurer une interface de gestion pour le mode transparent, à la page 13 pour configurer l'interface de gestion.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.

Les BVI apparaissent dans le tableau à côté des interfaces physiques, des sous-interfaceset des interfaces de canal de port EtherChannel. En mode de contexte multiple, seules les interfaces qui ont été affectées au contexte dans l'espace d'exécution du système apparaissent dans le tableau.

Étape 2 Choisissez la ligne correspondant à une interface non BVI, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Interface** (Modifier l'interface) s'affiche sous l'onglet **General** (Général).

Remarque Pour Firepower 1010, vous ne pouvez pas configurer de ports de commutation en tant que membres d'un groupe de ponts.

Vous ne pouvez pas mélanger des interfaces VLAN logiques et des interfaces de routeur physiques dans le même groupe de ponts.

Remarque En mode routé, les interfaces **port-channel** et **vni** ne sont pas prises en charge en tant que membres de groupes de ponts.

Étape 3 Dans le menu déroulant **Bridge Group** (Groupe de ponts), choisissez le groupe de ponts auquel vous souhaitez affecter cette interface.

Étape 4 Dans le champ **Interface Name** (Nom d'interface), saisissez un nom renfermant au maximum 48 caractères.

Étape 5 Dans le champ **Security level** (Niveau de sécurité), saisissez un niveau compris entre 0 (le plus bas) et 100 (le plus élevé).

Étape 6 Si l'interface n'est pas déjà activée, cochez la case **Enable Interface** (Activer l'interface).

Remarque Le champ **Channel Group** (Groupe de canaux) est en lecture seule et indique si l'interface fait partie d'un EtherChannel.

Étape 7 (Facultatif) Si vous installez un module et que vous souhaitez démontrer la fonctionnalité du module sur un ASA hors production, cochez la case **Forward traffic to the ASA module for inspection and reporting** (Transférer le trafic vers le module ASA pour inspection et génération de rapports). Consultez le chapitre du module ou le guide de démarrage rapide pour en savoir plus.

Étape 8 (Facultatif) Dans le champ **Description**, saisissez une description pour cette interface.

La description peut contenir jusqu'à 240 caractères sur une seule ligne (sans retour chariot). Dans le cas d'une liaison de basculement ou d'état, la description fixe est « LAN Failover Interface », « STATE Failover Interface » ou « LAN/STATE Failover Interface » par exemple. Vous ne pouvez pas modifier cette description. La description fixe remplace toute description que vous saisissez ici si vous faites de cette interface une liaison de basculement ou un lien d'état.

Étape 9 Cliquez sur **OK**.

Sujets connexes

Configurer l'adresse MAC manuelle, la MTU et le TCP MSS

Configurer une interface de gestion pour le mode transparent

En mode de pare-feu transparent, toutes les interfaces doivent appartenir à un groupe de ponts. La seule exception est l'interface de gestion (l'interface physique, une sous-interface (si prise en charge pour votre modèle) ou une interface EtherChannel composée d'interfaces de gestion (si vous avez plusieurs interfaces de gestion)) que vous pouvez configurer en tant qu'interface de gestion distincte; pour le Châssis

Firepower 4100/9300 , l'ID de l'interface de gestion dépend de l'interface de type gestion que vous avez attribuée au périphérique logique ASA. Vous ne pouvez pas utiliser d'autres types d'interfaces comme interfaces de gestion. Vous pouvez configurer une interface de gestion en mode unique ou par contexte. Pour obtenir plus de renseignements, consultez Interface de gestion pour le mode transparent.

L'interface de gestion traite uniquement le trafic entrant et sortant et ne peut pas transmettre de trafic de transit.

Avant de commencer

- N'attribuez pas cette interface à un groupe de ponts; un groupe de ponts non configurable (ID 301) est automatiquement ajouté à votre configuration. Ce groupe de ponts n'est pas inclus dans la limite de groupes de ponts.
- Pour le Châssis Firepower 4100/9300 , l'ID de l'interface de gestion dépend de l'interface de type gestion que vous avez attribuée au périphérique logique ASA.
- En mode de contexte multiple, vous ne pouvez partager aucune interface, y compris l'interface de gestion, entre les contextes. Vous devez vous connecter à une interface de données.
- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet Configuration > Device List (Liste des périphériques) et double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.

Étape 2 Choisissez la ligne correspondant à une interface de gestion, une sous-interface ou une interface de canal de port EtherChannel composée d'interfaces de gestion, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Interface** (modifier l'interface) s'affiche sous l'onglet **General** (général).

Pour le Châssis Firepower 4100/9300 , l'ID de l'interface de gestion dépend de l'interface de type gestion (individuelle ou EtherChannel) que vous avez attribuée au périphérique logique ASA.

Étape 3 Dans le menu déroulant **Bridge Group** (Groupe de ponts), laissez la valeur par défaut **--None--** (--Aucune--). Vous ne pouvez pas attribuer une interface de gestion à un groupe de ponts.

Étape 4 Dans le champ **Interface Name** (Nom d'interface), saisissez un nom renfermant au maximum 48 caractères.

Étape 5 Dans le champ **Security level** (Niveau de sécurité), saisissez un niveau compris entre 0 (le plus bas) et 100 (le plus élevé).

Remarque La case **Dedicate this interface to management only** (Dédier cette interface à la gestion uniquement) est activée par défaut et n'est pas configurable.

Étape 6 Si l'interface n'est pas déjà activée, cochez la case **Enable Interface** (Activer l'interface).

Étape 7 Pour définir l'adresse IP, utilisez l'une des options suivantes.

Remarque Pour une utilisation avec le basculement, vous devez définir manuellement l'adresse IP et l'adresse en veille; le protocole DHCP n'est pas pris en charge. Définissez les adresses IP de veille dans l'onglet **Configuration > Device Management (Gestion des périphériques) > High Availability (Haute disponibilité) > Failover (Basculement) > Interfaces**.

- Pour définir l'adresse IP manuellement, cliquez sur le bouton radio **Use Static IP** (Utiliser l'adresse IP statique) et saisissez l'adresse IP et le masque.
- Pour obtenir une adresse IP d'un serveur DHCP, cliquez sur le bouton radio **Obtain Address via DHCP** (Obtenir l'adresse par DHCP).
  - Pour forcer le stockage d'une adresse MAC dans un paquet de demande DHCP pour l'option 61, cliquez sur le bouton radio **Use MAC Address** (Utiliser l'adresse MAC).

    Certains fournisseurs de services Internet s'attendent à ce que l'option 61 soit l'adresse MAC de l'interface. Si l'adresse MAC n'est pas incluse dans le paquet de demande DHCP, aucune adresse IP ne sera attribuée.
  - Pour utiliser une chaîne générée pour l'option 61, cliquez sur **Use "Cisco-<MAC>-<interface_name>-<host>"** (Utiliser « Cisco-<MAC>-<interface_name>-<host> »).
  - (Facultatif) Pour obtenir la route par défaut à partir du serveur DHCP, cochez **Obtain Default Route Using DHCP** (Obtenir la route par défaut en utilisant DHCP).
  - (Facultatif) Pour définir l'indicateur de diffusion sur 1 dans l'en-tête de paquet DHCP, lorsque le client DHCP envoie une découverte demandant une adresse IP, cochez la case **Enable DHCP Broadcast flag for DHCP request and discover messages** (Activer l'indicateur de diffusion DHCP pour les demandes DHCP et les messages de découverte).

    Le serveur DHCP écoute cet indicateur de diffusion et diffuse le paquet de réponse si l'indicateur est défini sur 1.
  - (Facultatif) Pour renouveler le bail locatif, cliquez sur **Renew DHCP Lease** (Renouveler le bail locatif DHCP).

Étape 8 (Facultatif) Dans le champ **Description**, saisissez une description pour cette interface.

La description peut contenir jusqu'à 240 caractères sur une seule ligne (sans retour chariot).

Étape 9 Cliquez sur **OK**.

Configuration de l'adressage IPv6

Cette section décrit comment configurer l'adressage IPv6.

À propos d'IPv6

Cette section comprend des informations sur IPv6.

Adresse IPv6

Vous pouvez configurer deux types d'adresses de monodiffusion pour IPv6 :

- Adresse globale (global) : l'adresse globale est une adresse publique que vous pouvez utiliser sur le réseau public. Pour un groupe de ponts, cette adresse doit être configurée pour les BVI, et non par interface membre. Vous pouvez également configurer une adresse IPv6 globale pour l'interface de gestion en mode transparent.
- Adresse locale du lien (link-local) : l'adresse locale du lien est une adresse privée que vous ne pouvez utiliser que sur le réseau directement connecté. Les routeurs ne transfèrent pas les paquets en utilisant des adresses locales du lien; ils sont uniquement destinés à la communication sur un segment de réseau physique donné. Ils peuvent être utilisés pour la configuration des adresses ou pour les fonctions de découverte du voisin telles que la résolution d'adresses. Dans un groupe de ponts, seules les interfaces membres ont des adresses de lien locales; les BVI n'ont pas d'adresse locale de lien.

Au minimum, vous devez configurer une adresse locale de lien pour que IPv6 fonctionne. Si vous configurez une adresse globale, une adresse locale de lien est automatiquement configurée sur l'interface, vous n'avez donc pas besoin de configurer spécifiquement une adresse locale de lien. Pour les interfaces membres des groupes de ponts, lorsque vous configurez l'adresse globale sur les BVI, ASA génère automatiquement des adresses link-local pour les interfaces membres. Si vous ne configurez pas d'adresse globale, vous devez configurer l'adresse locale de lien. La configuration peut s'effectuer automatiquement ou manuellement.

ID d'interface EUI-64 modifiée

RFC 3513 : IPv6 (Internet Protocol Version 6) exige que la partie identifiant d'interface de toutes les adresses IPv6 de monodiffusion, à l'exception de celles qui commencent par la valeur binaire 000, ait une longueur de 64 bits et soit bâtie au format EUI-64 modifié. L'ASA peut appliquer cette exigence pour les hôtes associés au lien local.

Lorsque cette fonctionnalité est activée sur une interface, les adresses source des paquets IPv6 reçus sur cette interface sont comparées aux adresses MAC sources pour s'assurer que les identifiants d'interface utilisent le format EUI-64 modifié. Si les paquets IPv6 n'utilisent pas le format EUI-64 modifié comme identifiant d'interface, les paquets sont abandonnés et le message de journal système suivant est généré :

```
325003: EUI-64 source address check failed.
```

La vérification du format de l'adresse n'est effectuée que lors de la création d'un flux. Les paquets d'un flux existant ne sont pas vérifiés. De plus, la vérification de l'adresse ne peut être effectuée que pour les hôtes du lien local.

Configurer le client de délégation de préfixe IPv6

L'ASA peut servir de client de délégation de préfixe DHPCv6 de sorte que l'interface client, par exemple l'interface externe connectée à un modem câble, puisse recevoir un ou plusieurs préfixes IPv6 que l'ASA peut ensuite utiliser en sous-réseau et attribuer à ses interfaces internes.

À propos de la délégation de préfixe IPv6

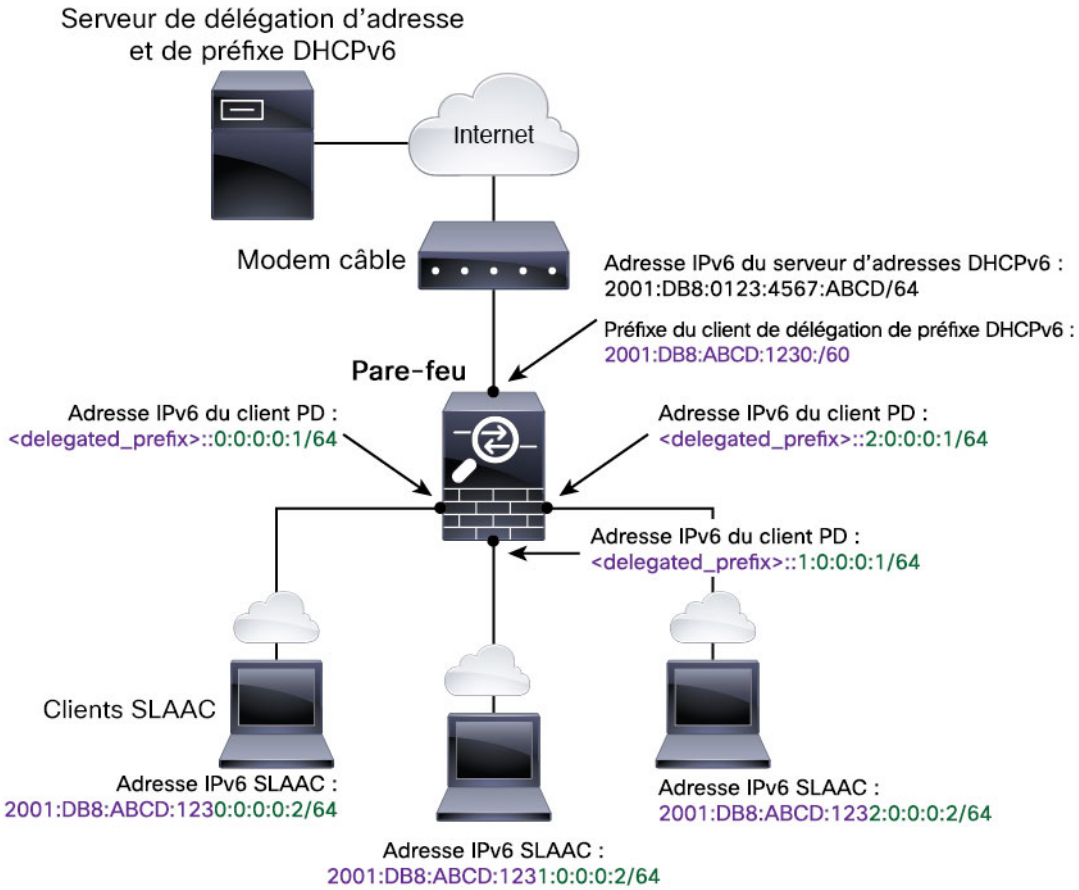
L'ASA peut servir de client de délégation de préfixe DHPCv6 de sorte que l'interface client, par exemple l'interface externe connectée à un modem câble, puisse recevoir un ou plusieurs préfixes IPv6 que l'ASA peut ensuite utiliser en sous-réseau et attribuer à ses interfaces internes. Les hôtes connectés aux interfaces internes

peuvent ensuite utiliser la configuration automatique sans état (SLAAC) pour obtenir des adresses IPv6 globales. Notez que les interfaces ASA internes n'agissent pas à leur tour comme des serveurs de délégation de préfixe; L'ASA ne peut fournir des adresses IP globales qu'aux clients SLAAC. Par exemple, si un routeur est connecté à l'ASA, il peut agir en tant que client SLAAC pour obtenir son adresse IP. Mais si vous souhaitez utiliser un sous-réseau du préfixe délégué pour les réseaux derrière le routeur, vous devez configurer manuellement ces adresses sur les interfaces internes du routeur.

L'ASA comprend un serveur DHCPv6 léger, de sorte que l'ASA peut fournir des informations telles que le serveur DNS et le nom de domaine aux clients SLAAC lorsqu'ils envoient des paquets de demande d'information (IR) à l'ASA. L'ASA accepte uniquement les paquets IR et n'affecte pas d'adresse aux clients. Vous configurerez le client pour générer sa propre adresse IPv6 en activant la configuration automatique IPv6 sur le client. L'activation de la configuration automatique sans état sur un client configure les adresses IPv6 en fonction des préfixes reçus dans les messages de publicité de routeur; en d'autres termes, en fonction du préfixe que ASA a reçu à l'aide de la délégation de préfixe.

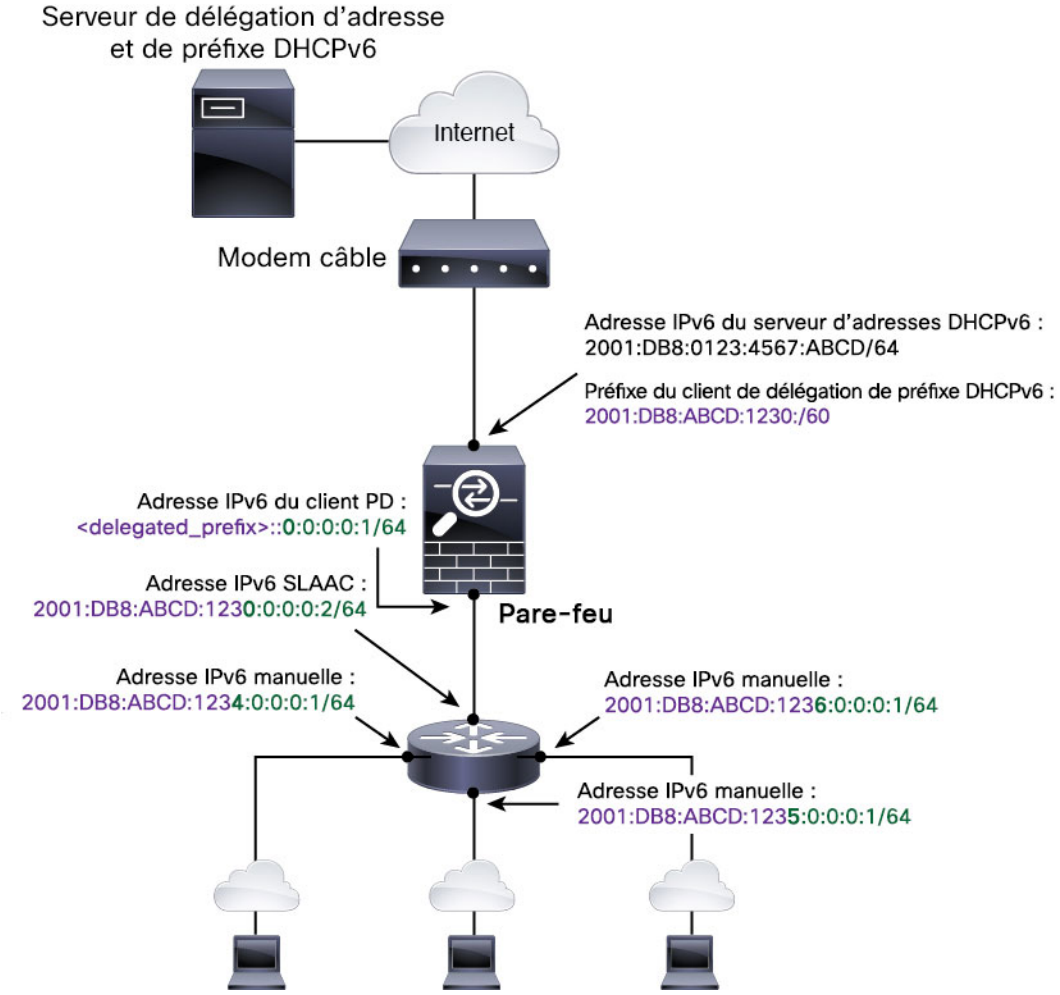
Exemple de délégation de préfixe IPv6 /de sous-réseau 64

L'exemple suivant montre que ASA reçoit une adresse IP sur l'interface externe en utilisant l'adresse DHCPv6. Il obtient également un préfixe délégué à l'aide du client de délégation de préfixe DHCPv6. L'ASA subdivise le préfixe délégué en réseaux /64 et attribue des adresses IPv6 globales à ses interfaces internes de manière dynamique en utilisant le préfixe délégué plus un sous-réseau configuré manuellement (::0, ::1 ou ::2) et une adresse IPv6 (0:0:0:1) par interface. Les clients SLAAC connectés à ces interfaces internes obtiennent des adresses IPv6 sur chaque sous-réseau /64.



Exemple de délégation de préfixe IPv6 /de sous-réseau 62

L'exemple suivant montre la sous-réseaux ASA du préfixe en 4 sous-réseaux /62 : 2001:DB8:ABCD:123**0**:/62, 2001:DB8:ABCD:123**4**:/62, 2001:DB8:ABCD:123**8**::/62 et 2001:DB8:ABCD:123 **C**::/62. ASA utilise l'un des 4 sous-réseaux /64 disponibles sur 2001:DB8:ABCD:1230::/62 pour son réseau interne (::0). Vous pouvez ensuite utiliser manuellement des sous-réseaux /62 supplémentaires pour les routeurs en aval. Le routeur illustré utilise 3 des 4 sous-réseaux /64 disponibles sur 2001:DB8:ABCD:1234::/62 pour ses interfaces internes (::4,::5 et::6). Dans ce cas, les interfaces de routeur internes ne peuvent pas obtenir dynamiquement le préfixe délégué. Vous devez donc afficher le préfixe délégué sur ASA, puis utiliser ce préfixe pour la configuration de votre routeur. Habituellement, les fournisseurs de services Internet délèguent le même préfixe à un client donné à l'expiration du bail, mais si ASA reçoit un nouveau préfixe, vous devrez modifier la configuration du routeur pour utiliser le nouveau préfixe. L'identifiant unique (DUID) de DHCP est persistant pendant les redémarrages.



Activer le client de délégation de préfixe IPv6

Activez le client de délégation de préfixe DHCPv6 sur une ou plusieurs interfaces. L'ASA obtient un ou plusieurs préfixes IPv6 qu'elle peut subdiviser en sous-réseaux et attribuer à des réseaux internes. En règle générale, l'interface sur laquelle vous activez la délégation de préfixe client obtient son adresse IP à l'aide de l'adresse client DHCPv6; Seules les autres interfaces ASA utilisent des adresses dérivées du préfixe délégué.

Avant de commencer

- Cette fonction n'est prise en charge qu'en mode pare-feu routé.
- Cette fonctionnalité n’est pas prise en charge en mode contexte multiple.
- Cette fonctionnalité n’est pas prise en charge lors de la mise en grappe.
- Vous ne pouvez pas configurer cette fonction sur une interface de gestion uniquement.
- Lorsque vous utilisez la délégation de préfixe, vous devez définir l’intervalle d’annonce du routeur de découverte des voisins IPv6 de l’ASA de manière à ce qu’il soit bien inférieur à la durée de vie souhaitée du préfixe attribué par le serveur DHCPv6, afin d’éviter toute interruption du trafic IPv6. Par exemple, si le serveur DHCPv6 définit la durée de vie préférée de délégation de préfixe à 300 secondes, vous devez définir l’intervalle d'annonce de routeur de l’ASA à 150 secondes. Pour définir la durée de vie préférée, utilisez la commande **show ipv6 general-prefix**. Pour définir l’intervalle d’annonce de routeur de l’ASA, consultez Configurer la découverte des voisins IPv6, à la page 23; la valeur par défaut est de 200 secondes.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.

Étape 2 Choisissez une interface et cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Interface** (modifier l’interface) s’affiche sous l’onglet **General** (général).

Étape 3 Cliquez sur l'onglet **IPv6**.

Étape 4 Dans a zone **Interface IPv6 DHCP** (Interface IPv6 DHCP), cliquez sur e bouton radio **Client Prefix Delegation Name** (Nom de la délégation du préfixe du client), et saisissez le nom du préfixe.

Étape 5 (Facultatif) Dans le champ **Prefix Hint** (conseils de préfixe), fournissez un ou plusieurs conseils sur le préfixe délégué que vous souhaitez recevoir.

Typiquement, vous voulez demander une longueur de préfixe particulière, comme ::/60, ou si vous avez déjà reçu un préfixe particulier et que vous voulez vous assurer de l'obtenir à nouveau à l'expiration du bail, vous pouvez saisir le préfixe entier comme indice (2001:DB8:ABCD:1230::/60). Si vous saisissez plusieurs conseils (préfixes ou longueurs différents), il appartient au serveur DHCP de choisir de respecter le conseil ou non.

Étape 6 Cliquez sur **OK**.

Vous retournez au volet **Configuration > Device Setup > Interface Settings > Interfaces** (Configuration > Configuration du périphérique > Paramètres d'interface > Interfaces).

Étape 7 Cliquez sur **Apply** (Appliquer).

Étape 8 Consultez Configuration d’une adresse globale IPv6, à la page 20 pour affecter un sous-réseau du préfixe comme adresse IP globale pour une interface ASA.

Étape 9 (Facultatif) Consultez Configurer le serveur sans état DHCPv6 pour fournir le nom de domaine et les paramètres de serveur aux clients SLAAC.

Étape 10 (Facultatif) Consultez Configurer les paramètres réseau IPv6 pour annoncer le ou les préfixes avec BGP.

Configuration d'une adresse globale IPv6

Pour configurer une adresse IPv6 globale pour une interface en mode routé et pour le BVI en mode transparent ou routé, procédez comme suit.

Les options de délégation de préfixe et de DHCPv6 ne sont pas prises en charge avec le mode de contexte multiple.

Remarque La configuration de l'adresse globale configure automatiquement l'adresse de lien local, de sorte que vous n'avez pas besoin de la configurer séparément. Pour les groupes de ponts, la configuration de l'adresse globale sur les BVI configure automatiquement les adresses de lien locales sur toutes les interfaces membres.

Pour les sous-interfaces, nous vous recommandons de définir également l'adresse MAC manuellement, car elles utilisent la même adresse MAC gravée de l'interface parente. En outre, étant donné que les adresses locales de lien IPv6 sont générées en fonction de l'adresse MAC, l'affectation d'adresses MAC uniques aux sous-interfaces permet d'établir des adresses locales de lien IPv6 uniques, ce qui peut éviter des perturbations de trafic dans certaines instances sur l'ASA. Consultez Configurer l'adresse MAC manuelle, la MTU et le TCP MSS.

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, dans le volet Configuration > Device List (Liste des périphériques), double-cliquez sur le nom du contexte sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.

Étape 2 Choisissez une interface et cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Interface** (modifier l'interface) s'affiche sous l'onglet **General** (général).

En mode transparent ou pour un groupe de ponts en mode routé, sélectionnez un BVI. Pour le mode transparent, vous pouvez également sélectionner une interface de gestion uniquement.

Étape 3 Cliquez sur l'onglet **IPv6**.

Étape 4 Cochez la case **Enable IPv6** (activer IPv6).

Étape 5 (Facultatif) Pour appliquer l'utilisation des identifiants d'interface au format EUI-64 modifié dans les adresses IPv6 sur un lien local, cochez la case **Enforce EUI-64** (appliquer EUI-64).

Étape 6 (Interface routée) Configurez l'adresse IPv6 globale à l'aide de l'une des méthodes suivantes.

Pour le basculement et la mise en grappe, ainsi que pour les interfaces de boucle avec retour, vous devez définir l'adresse IP manuellement. Pour la mise en grappe, la configuration manuelle de l'adresse Link-Local n'est pas prise en charge.

- Autoconfiguration d'adresse sans état (SLAAC) : dans la zone **Interface IPv6 Addresses** (Adresses IPv6 de l'interface), cochez la case **Enable address autoconfiguration** (Activer l'autoconfiguration d'adresse).

L'activation de la SLAAC sur l'interface configure les adresses IPv6 en fonction des préfixes reçus dans les messages d'annonce de routeur. Une adresse Link-Local, basée sur l'ID d'interface EUI-64 modifiée, est automatiquement générée pour l'interface lorsque la SLAAC est activée.



Remarque Bien que la RFC 4862 spécifie que les hôtes configurés pour une SLAAC n'envoient pas de messages d'annonce de routeur, l'ASA envoie ces messages dans ce cas. Cochez la case **Supprimer RA** pour supprimer les messages d'annonce.

Si vous souhaitez installer une route par défaut, choisissez **default trust dhcp** ou **default trust ignore** dans le menu déroulant. **default trust dhcp** spécifie que l'ASA utilise uniquement une route par défaut des annonces de routeurs provenant d'une source de confiance (c'est-à-dire du même serveur qui a fourni l'adresse IPv6). **default trust ignore** spécifie que les annonces de routeurs peuvent provenir d'un autre réseau, ce qui peut constituer une méthode plus risquée.

- Configuration manuelle : pour configurer manuellement une adresse IPv6 globale :

  1. Dans la zone **Interface IPv6 Addresses** (adresses IPv6 de l'interface), cliquez sur **Add** (Ajouter).

     La boîte de dialogue **Add IPv6 Address for Interface** (ajouter une adresse IPv6 pour l'interface) s'affiche.

  2. Dans le champ **Address/Prefix Longueur** (longueur d'adresse/préfixe), la valeur que vous saisissez dépend de la méthode que vous souhaitez utiliser :

     - Full global address (adresse globale complète) : si vous souhaitez saisir manuellement l'adresse complète, saisissez l'adresse complète plus la longueur du préfixe.
     - Modified EUI 64 format (format modifié EUI 64) : saisissez le préfixe et la longueur IPv6, puis cochez la case **EUI 64** pour générer l'ID d'interface en utilisant le format Modified EUI-64. Par exemple, 2001:0DB8::BA98:0:3210/48 (adresse complète) ou 2001:0DB8::/48 (préfixe, avec EUI 64 cochée).
     - Delegated Prefix (préfixe IPv6) : Pour dériver le préfixe IPv6 du préfixe délégué, saisissez l'adresse IPv6 et la longueur. Saisissez ensuite le nom de préfixe que vous avez configuré pour le client de délégation de préfixe DHCPv6 (voir Activer le client de délégation de préfixe IPv6, à la page 18) dans le champ **Prefix Name** (nom de préfixe), puis cliquez sur **Add** (Ajouter).

       En règle générale, le préfixe délégué est /60 ou moins, de sorte que vous pouvez créer un sous-réseau à plusieurs réseaux /64. /64 est la longueur de sous-réseau prise en charge si vous souhaitez prendre en charge SLAAC pour les clients connectés. Vous devez spécifier une adresse qui complète le sous-réseau /60, par exemple ::1:0:0:0:1. Saisissez : avant l'adresse si le préfixe est inférieur à 60. Par exemple, si le préfixe délégué est 2001:DB8:1234:5670::60, l'adresse IP globale attribuée à cette interface est 2001:DB8:1234:5671::1/64. Le préfixe annoncé dans les annonces des routeurs est 2001:DB8:1234:5671::/64. Dans cet exemple, si le préfixe est inférieur à 60, les bits restants du préfixe seront des 0, comme l'indique le préfixe::. Par exemple, si le préfixe est 2001:DB8:1234::/48, l'adresse IPv6 sera 2001:DB8:1234::1:0:0:0:1/64.

  3. Cliquez sur **OK**.

- Obtenez une adresse à l'aide de DHCPv6 :

1. Dans la zone **Interface IPv6 DHCP**, cochez la case **Enable DHCP** (activer DHCP).
2. (Facultatif) Cochez la case **Enable Default** (activer par défaut) pour obtenir une voie de routage par défaut à partir des annonces de routeur.

Étape 7 (interface BVI) Attribuez manuellement une adresse globale aux BVI. Pour une interface de gestion en mode transparent, utilisez également cette méthode.

a) Dans la zone **Interface IPv6 Addresses** (adresses IPv6 de l'interface), cliquez sur **Add** (Ajouter).

La boîte de dialogue **Add IPv6 Address for Interface** (ajouter une adresse IPv6 pour l'interface) s'affiche.

b) Dans le champ **Address/Prefix Longueur** (longueur d'adresse/préfixe), saisissez l'adresse IPv6 globale complète ainsi que la longueur du préfixe IPv6.

c) Cliquez sur **OK**.

Étape 8 Cliquez sur **OK**.

Vous retournez au volet **Configuration > Device Setup > Interface Settings > Interfaces** (Configuration > Configuration du périphérique > Paramètres d'interface > Interfaces).

(Facultatif) Configurer automatiquement les adresses Link-Local

Si vous ne souhaitez pas configurer d'adresse globale et que vous avez seulement besoin de configurer une adresse Link-Local, vous avez la possibilité de générer les adresses Link-Local en fonction des adresses MAC de l'interface (format EUI-64 modifié. Comme les adresses MAC utilisent 48 bits, des bits supplémentaires doivent être insérés pour remplir les 64 bits requis pour l'ID d'interface.)

Pour configurer automatiquement les adresses Link-Local d'une interface, procédez comme suit.

Avant de commencer

Pris en charge en mode routé uniquement.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.

Étape 2 Sélectionnez une interface, puis cliquez sur **Edit**.

Pour les groupes de ponts en mode routé, choisissez la BVI.

La boîte de dialogue **Edit Interface** (Modifier l'interface) s'affiche sous l'onglet **General** (Général).

Étape 3 Cliquez sur l'onglet **IPv6**.

Étape 4 Dans la zone **IPv6 configuration** (Configuration IPv6), cochez la case **Enable IPv6** (Activer IPv6).

Cette option active IPv6 et génère automatiquement l'adresse Link-Local à l'aide de l'ID d'interface EUI-64 modifié en fonction de l'adresse MAC de l'interface.

Pour les groupes de ponts en mode routé, l'activation d'IPv6 pour la BVI génère des adresses Link-Local pour toutes les interfaces membres.

Étape 5 Cliquez sur **OK**.

(Facultatif) Configurer manuellement les adresses Link-Local

Si vous ne souhaitez pas configurer d'adresse globale et que vous avez seulement besoin de configurer une adresse link-local, vous avez la possibilité de définir manuellement cette dernière. Notez que nous vous recommandons d'attribuer automatiquement l'adresse de lien local en fonction du format EUI-64 modifié. Par exemple, si d'autres appareils imposent l'utilisation du format EUI-64 modifié, une adresse de lien local attribuée manuellement peut entraîner la perte de paquets.

Pour attribuer une adresse Link-Local à une interface, procédez comme suit.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.

Étape 2 Sélectionnez une interface, puis cliquez sur **Edit**.

Pour les groupes de ponts, choisissez une interface membre du groupe de ponts.

La boîte de dialogue **Edit Interface** (modifier l'interface) s'affiche sous l'onglet **General** (général).

Étape 3 Cliquez sur l'onglet **IPv6**.

Étape 4 (Facultatif) Pour appliquer l'utilisation des identifiants d'interface au format EUI-64 modifié dans les adresses IPv6 sur un lien local, cochez la case **Enforce EUI-64** (appliquer EUI-64).

Étape 5 Pour définir l'adresse Link-Local, saisissez une adresse dans le champ **Link-Local address** (Adresse Link-Local).

Une adresse de lien local doit commencer par FE8, FE9, FEA ou FEB, par exemple fe80::20d:88ff:feee:6a82. Consultez Adresses IPv6 pour en savoir plus sur l'adressage IPv6.

Étape 6 Cliquez sur **OK**.

Configurer la découverte des voisins IPv6

Le processus de découverte des voisins IPv6 utilise des messages ICMPv6 et des adresses de multidiffusion de nœud sollicité pour déterminer l'adresse de couche de liaison d'un voisin sur le même réseau (lien local), vérifier la lisibilité d'un voisin et suivre les routeurs voisins.

Les nœuds (hôtes) utilisent la découverte des voisins pour déterminer les adresses de couche de liaison des voisins connus pour résider sur les liens attachés et pour purger rapidement les valeurs en cache qui deviennent non valides. Les hôtes ont également recours à la découverte des voisins pour trouver les routeurs voisins qui sont prêts à transférer des paquets en leur nom. En outre, les nœuds utilisent le protocole pour garder activement une trace des voisins accessibles et de ceux qui ne le sont pas, et pour détecter les adresses de couche de liaison modifiées. Lorsqu'un routeur ou le chemin d'accès à un routeur tombe en panne, un hôte recherche activement des solutions de remplacement qui fonctionnent.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.

Étape 2 Choisissez l'interface IPv6 sur laquelle configurer les paramètres de voisin IPv6, puis cliquez sur **Edit** (Modifier).

Étape 3 Cliquez sur l'onglet **IPv6**.

Étape 4 Saisissez le nombre de **tentatives DAD**autorisées.

Les valeurs valides vont de 0 à 600. La valeur 0 désactive le traitement de la DAD sur l'interface spécifiée. La valeur par défaut est de 1 message par seconde.

DAD garantit l'unicité des nouvelles adresses IPv6 de monodiffusion avant qu'elles ne soient attribuées et veille à ce que les adresses IPv6 en double soient détectées dans le réseau selon les liaisons. L'ASA utilise les messages de sollicitation des voisins pour effectuer le DAD.

Lorsqu'une adresse en double est identifiée, l'état de l'adresse est défini à DUPLICATE, l'adresse n'est pas utilisée et le message d'erreur suivant est généré :

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

Si l'adresse en double est l'adresse link-local de l'interface, le traitement des paquets IPv6 est désactivé sur l'interface. Si l'adresse en double est une adresse globale, l'adresse n'est pas utilisée.

Étape 5 Saisissez l'**intervalle NS** en millisecondes pour définir l'intervalle entre les retransmissions de sollicitation des voisins IPv6.

Les valeurs valides pour l'argument de valeur sont comprises entre 1000 et 3600 000 millisecondes.

Les messages de sollicitation des voisins (ICMPv6 de type 135) sont envoyés sur la liaison locale par les nœuds qui tentent de découvrir les adresses de couche de liaison d'autres nœuds sur la liaison locale. Après avoir reçu un message de sollicitation de voisin, le nœud de destination répond en envoyant un message d'annonce de voisin (ICPMv6 type 136) sur la liaison locale.

Une fois que le nœud source a reçu l'annonce de voisin, le nœud source et le nœud de destination peuvent communiquer. Les messages de sollicitation de voisin sont également utilisés pour vérifier l'accessibilité d'un voisin après avoir identifié l'adresse de couche de liaison d'un voisin. Lorsqu'un nœud souhaite vérifier l'accessibilité d'un voisin, l'adresse de destination dans un message de sollicitation de voisin est l'adresse de monodiffusion du voisin.

Des messages d'annonce de voisin sont également envoyés en cas de changement dans l'adresse de couche de liaison d'un nœud sur une liaison locale.

Étape 6 Saisissez la **Durée d'accessibilité** en secondes pour définir combien de temps un nœud IPv6 distant est accessible.

Définissez la durée accessible entre 0 et 3600 000 millisecondes. Lorsque vous définissez la durée sur 0, la durée accessible est envoyée comme indéterminée. Il appartient aux périphériques de réception de définir et de suivre la durée accessible.

La durée d'accessibilité du voisin permet de détecter les voisins non disponibles. Des durées configurées plus courtes permettent de détecter plus rapidement les voisins non disponibles, mais des durées plus courtes consomment plus de bande passante réseau IPv6 et de ressources de traitement dans tous les périphériques

réseau IPv6. Des durées configurées très courtes ne sont pas recommandées pour le fonctionnement normal d'un IPv6.

Étape 7 Saisissez la **durée de vie RA** en secondes pour définir la durée pendant laquelle les nœuds de la liaison locale considèrent l'ASA comme le routeur par défaut sur la liaison.

Les valeurs sont comprises entre 0 et 9 000 secondes. Si la valeur 0 est saisie, l'ASA ne doit pas être considéré comme un routeur par défaut sur l'interface sélectionnée.

Étape 8 Cochez la case **Suppress RA** (Supprimer les annonces de routeur) pour supprimer les annonces de routeur.

Les messages d'annonce de routeur (ICMPv6 Type 134) sont automatiquement envoyés en réponse aux messages de sollicitation de routeur (ICMPv6 Type 133). Les messages de sollicitation de routeur sont envoyés par les hôtes au démarrage du système, ce qui permet à l'hôte de se configurer automatiquement sans avoir à attendre le prochain message de publicité de routeur planifié.

Vous pouvez souhaiter désactiver ces messages sur toute interface pour laquelle vous ne souhaitez pas que l'ASA fournisse le préfixe IPv6 (par exemple, l'interface extérieure).

L'activation de cette option fait en sorte que l'ASA s'affiche comme un voisin IPv6 standard sur la liaison et non comme un routeur IPv6.

Étape 9 Saisissez l'**intervalle RA** pour définir l'intervalle entre les transmissions des annonces du routeur IPv6.

Les valeurs valides vont de 3 à 1 800 secondes. La valeur par défaut est de 200 secondes.

Pour ajouter une valeur d'intervalle de transmission d'annonce de routeur en millisecondes, cochez la case **RA Interval in Milliseconds** (Intervalle d'annonce de routeur en millisecondes) et saisissez une valeur comprise entre 500 et 1 800 000.

Pour empêcher la synchronisation avec d'autres nœuds IPv6, l'ASA ajuste de manière aléatoire la valeur que vous avez définie (gigue).

Étape 10 Cochez la case **Hosts should use DHCP for address config** (Les hôtes doivent utiliser DHCP pour la configuration des adresses) pour informer les clients d'autoconfiguration d'adresse sans état (SLAAC) IPv6 qu'ils doivent utiliser DHCPv6 pour obtenir des adresses, en plus de l'adresse d'autoconfiguration sans état dérivée.

Cette option définit l'indicateur de configuration d'adresse gérée dans le paquet d'annonce du routeur IPv6.

Étape 11 Cochez la case **Hosts should use DHCP for non-address config** (Les hôtes doivent utiliser DHCP pour la configuration sans adresses) pour informer les clients SLAAC IPv6 qu'ils doivent utiliser DHCPv6 pour obtenir des renseignements supplémentaires de DHCPv6, tels que l'adresse du serveur DNS.

Cette option définit l'indicateur Another Address Config (Configuration d'une autre adresse) dans le paquet d'annonce du routeur IPv6.

Étape 12 Configurez les préfixes IPv6 à inclure dans les annonces de routeur IPv6.

a) Dans la zone **Interface IPv6 Prefixes** (Préfixes IPv6 d'interface) , cliquez sur **Add** (Ajouter).
b) Saisissez la **longueur de l'adresse/du préfixe** ou cochez la case **par défaut** pour utiliser le préfixe par défaut.
c) Cochez la case **No Auto-Configuration** pour forcer les hôtes à configurer l'adresse IPv6 manuellement. Les hôtes de la liaison locale avec le préfixe précisé ne peuvent pas utiliser SLAAC IPv6.
d) Cochez la case **Aucune annonce** pour désactiver l'annonce de préfixe. Pour le préfixe **Default** (Par défaut), ce paramètre s'applique uniquement aux préfixes sur la liaison. Les préfixes hors liaison seront toujours annoncés, sauf si vous spécifiez **No Advertisements** (Aucune annonce) pour un préfixe hors liaison précis.

e) Cochez la case **Off Link** (hors-lien) pour configurer le préfixe spécifié comme hors lien. Le préfixe sera annoncé avec le bit L en effacement. Le préfixe ne sera pas inséré dans la table de routage en tant que préfixe connecté.

f) Dans la zone **Prefix Lifetime** (Durée de vie du préfixe), spécifiez une **durée de vie** ou une **date d'expiration** de la durée de vie .

À l'expiration de la durée de vie préférée, l'adresse passe à l'état obsolète. Lorsqu'une adresse est dans un état obsolète, son utilisation est déconseillée, mais pas formellement interdite. Après l'expiration de la durée de vie valide, l'adresse devient non valide et ne peut pas être utilisée. La durée de vie valide doit être supérieure ou égale à la durée de vie préférée.

- **Durée de vie** : les valeurs sont comprises entre 0 et 4294967295. La durée de vie valide par défaut est de 2592000 (30 jours). La durée de vie préférée par défaut est 604800 (7 jours). La valeur maximale représente l'éternité.
- **Lifetime Expiration Date**(date d'expiration de la durée de vie) : choisissez un mois et un jour valides dans les listes déroulantes, puis saisissez une heure au format hh:mm.

g) Cliquez sur**OK** pour sauvegarder vos paramètres.

Étape 13 Cliquez sur **OK**.

Étape 14 Configurer un voisin IPv6 statique.

Les directives et limites suivantes s'appliquent à la configuration d'un voisin IPv6 statique :

- Cette fonctionnalité est similaire à l'ajout d'une entrée ARP statique. Si une entrée pour l'adresse IPv6 précisée existe déjà dans le cache de découverte des voisins (apprise par le processus de découverte des voisins IPv6), elle est automatiquement convertie en entrée statique. Ces entrées sont stockées dans la configuration lorsque la commande copy est utilisée pour stocker la configuration.
- Les entrées statiques de la mémoire cache de découverte du voisin IPv6 ne sont pas modifiées par le processus de découverte du voisin.
- Les journaux système ICMP générés sont provoqués par une actualisation régulière des entrées IPv6 neighbor. La minuterie par défaut de l'ASA pour l'entrée du voisin IPv6 est de 30 secondes, donc l'ASA génère des paquets de découverte et de réponse des voisins ICMPv6 toutes les 30 secondes. Si l'ASA est dotée d'interfaces LAN et d'état de basculement configurées avec des adresses IPv6, toutes les 30 secondes, des paquets de réponse et de découverte de voisin ICMPv6 seront générés par les deux ASA pour les adresses IPv6 configurées et celles liées au lien local. En outre, chaque paquet génère plusieurs syslogs (connexion ICMP et création ou démontage de l'hôte local), de sorte qu'il peut sembler que des syslogs ICMP sont générés en permanence. L'heure d'actualisation de l'entrée du voisin IPV6 peut être configurée sur l'interface de données normale, mais pas sur l'interface de basculement. Cependant, l'impact sur le CPU pour ce trafic de découverte de voisin ICMP est minime.

Consultez aussi Afficher et effacer les voisins détectés dynamiquement, à la page 27.

a) Choisissez **Configuration** > **Device Management** (Gestion des périphériques) > **Advanced** (Avancé) > **IPv6 Neighbor Discovery Cache** (Cache de découverte de voisin IPv6).

b) Cliquez sur **Add** (ajouter).

La boîte de dialogue **Add IPv6 Static Neighbor** (Ajouter un voisin statique IPv6) s'affiche.

c) Dans la liste déroulante **Interface Name** (Nom de l'interface), choisissez une interface à laquelle ajouter le voisin.

d) Dans le champ **IP Address** (adresse IP), saisissez l'adresse IPv6 qui correspond à l'adresse de liaison de données locale, ou cliquez sur les points de suspension (…) pour rechercher une adresse.

e) Dans le champ **MAC address** (adresse MAC), saisissez l'adresse MAC (matérielle) de la ligne de données locale.
f) Cliquez sur **OK**.

Étape 15 Cliquez sur **Apply** (Appliquer) pour enregistrer la configuration en cours d'exécution.

Afficher et effacer les voisins détectés dynamiquement

Lorsqu'un hôte ou un nœud communique avec un voisin, ce voisin est ajouté au cache de découverte de voisin. Le voisin est supprimé du cache lorsqu'il n'y a plus de communication avec lui.

Pour afficher les voisins détectés dynamiquement et effacer ces voisins du cache de découverte des voisins IPv6, procédez comme suit :

Procédure

Étape 1 Choisissez **Monitoring** > **Interfaces** > **IPv6 Neighbor Discovery Cache** (Surveillance > Interfaces > Cache de découverte du voisin IPv6).

Vous pouvez afficher tous les voisins statiques et dynamiques détectés dans le volet du cache de découverte des voisins IPv6.

Étape 2 Pour effacer du cache tous les voisins détectés dynamiquement, cliquez sur **Effacer les entrées des voisins dynamiques**.

Le voisin détecté dynamiquement est supprimé du cache.

Remarque Cette procédure efface uniquement les voisins découverts dynamiquement du cache; elle n'efface pas les voisins statiques.

Supervision des interfaces en mode routé et en mode transparent

Vous pouvez superviser les statistiques d'interface, l'état, PPPoE, etc.

Remarque Pour les modèles Firepower et Secure Firewall, certaines statistiques ne sont pas affichées à l'aide des commandes ASA. Vous devez consulter des statistiques d'interface plus détaillées à l'aide des commandes FXOS.

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**

Pour Firepower 2100 en mode plateforme, consultez aussi les commandes FXOS connect local-mgmt suivantes :

- (local-mgmt)# **show portmanager counters**
- (local-mgmt)# **show lacp**
- (local-mgmt)# **show portchannel**

Consultez le guide de dépannage FXOS pour plus d'informations.

Statistiques et informations sur l'interface

- **Monitoring (Supervision) > Interfaces > Interface Graphs (Graphiques d'interface)**

  Vous permet d'afficher les statistiques d'interface sous forme de graphique ou de tableau. Si une interface est partagée entre les contextes, l'ASA affiche uniquement les statistiques du contexte actuel. Le nombre de statistiques affichées pour une sous-interface est un sous-ensemble du nombre de statistiques affichées pour une interface physique.

- **Monitoring (Supervision) > Interfaces > Interface Graphs (Graphiques d'interface) > Graph/Table (Graphique/Tableau)**

  Affiche un graphique pour les statistiques sélectionnées. La fenêtre Graph (Graphique) peut afficher jusqu'à quatre graphiques et tableaux à la fois. Par défaut, le graphique ou le tableau affiche les statistiques en temps réel. Si vous activez les mesures de l'historique, vous pouvez afficher les statistiques des périodes passées.

Renseignements sur DHCP

- **Monitoring (Supervision)** > **Interfaces** > **DHCP** > **DHCP Client Lease Information (Renseignements sur le bail locatif du client DHCP)**.

  Cet écran affiche les adresses IP configurées des clients DHCP.

- **Monitoring (Supervision)** > **Interfaces** > **DHCP** > **IPV6 DHCP Client PD Statistics (Statistiques PD du client DHCP IPV6)**

  Cet écran affiche les statistiques du client de délégation de préfixe DHCPv6 et indique le résultat du nombre de messages envoyés et reçus.

- **Monitoring (Supervision)** > **Interfaces** > **DHCP** > **IPV6 DHCP Client Statistics (Statistiques du client DHCP IPV6)**

Cet écran affiche les statistiques du client DHCPv6 et indique le résultat du nombre de messages envoyés et reçus.

- **Monitoring (Supervision)** > **Interfaces** > **DHCP** > **IPV6 DHCP Interface Statistics (Statistiques d'interface DHCP IPV6)**

  Cet écran affiche les renseignements DHCPv6 pour toutes les interfaces. Si l'interface est configurée pour la configuration du serveur sans état DHCPv6 (voir Configurer le serveur sans état DHCPv6), cet écran répertorie l'ensemble DHCPv6 utilisé par le serveur. Si l'interface a une configuration de client d'adresse DHCPv6 ou de client de délégation de préfixe, cet écran affiche l'état de chaque client et les valeurs reçues du serveur. Cet écran affiche également les statistiques des messages pour le serveur ou le client DHCP.

- **Monitoring (Supervision)** > **Interfaces** > **DHCP** > **IPV6 DHCP HA Statistics (Statistiques DHCP IPV6 à haute disponibilité)**

  Cet écran affiche les statistiques de transaction entre les unités de basculement, y compris le nombre de fois où les renseignements DUID ont été synchronisés entre les unités.

Suivi du routage statique

- **Monitoring (Supervision) > Interfaces > Interface connection (Connexion d'interface) > Track Status (État du suivi)**

  Affiche des renseignements sur l'objet suivi.

- **Monitoring (Supervision) > Interfaces > Interface connection (Connexion d'interface) > Monitoring Statistics (Statistiques de surveillance)**

  Affiche les statistiques relatives au processus de supervision des SLA.

PPPoE

- **Monitoring (Supervision) > Interfaces > PPPoE Client (Client PPPoE) > PPPoE Client Lease Information (Renseignements sur le bail locatif du client DHCP)**

  Affiche des renseignements sur les connexions PPPoE actuelles.

ACL dynamiques

Monitoring (Supervision) > Interfaces > Dynamic ACLs (ACL dynamiques)

Affiche un tableau des ACL dynamiques, qui sont fonctionnellement identiques aux ACL configurées par l'utilisateur, sauf qu'elles sont créées, activées et supprimées automatiquement par l'ASA. Ces ACL ne s'affichent pas dans la configuration et ne sont visibles que dans ce tableau. Elles sont identifiées par le mot clé « (dynamique) » dans l'en-tête de l'ACL.

Exemples d'interfaces en mode routé et en mode transparent

Exemple de mode transparent avec 2 groupes de ponts

L'exemple suivant de mode transparent comprend deux groupes de ponts de trois interfaces chacun, plus une interface de gestion uniquement :

```
interface gigabitethernet 0/0
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 0/1
  nameif outside1
  security-level 0
  bridge-group 1
  no shutdown
interface gigabitethernet 0/2
  nameif dmz1
  security-level 50
  bridge-group 1
  no shutdown
interface bvi 1
  ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2

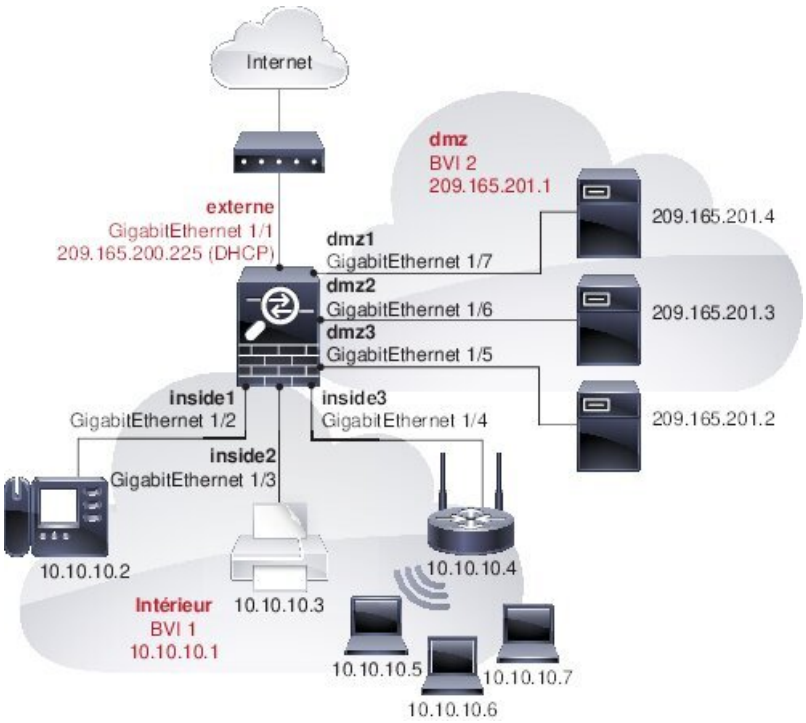
interface gigabitethernet 1/0
  nameif inside2
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/1
  nameif outside2
  security-level 0
  bridge-group 2
  no shutdown
interface gigabitethernet 1/2
  nameif dmz2
  security-level 50
  bridge-group 2
  no shutdown
interface bvi 2
  ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9

interface management 0/0
  nameif mgmt
  security-level 100
  ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
  no shutdown
```

Exemple de segment LAN commuté avec 2 groupes de ponts

Dans l'exemple suivant, deux groupes de ponts de 3 interfaces et une interface routée standard pour l'extérieur sont configurés. Le groupe de ponts 1 est à l'intérieur et le groupe de ponts 2 est une zone DMZ avec des serveurs Web publics. Les interfaces membres du groupe de ponts peuvent communiquer librement au sein du groupe de ponts, car chaque membre se trouve au même niveau de sécurité et nous avons activé la même

communication de sécurité. Bien que le niveau de sécurité du membre interne soit de 100 et que celui du membre de la zone DMZ soit également de 100, ces niveaux de sécurité ne s'appliquent pas aux communications inter-BVI; seuls les niveaux de sécurité BVI affectent le trafic inter-BVI. Les niveaux de sécurité des BVI et de l'extérieur (100, 50 et 0) autorisent implicitement le trafic de l'intérieur vers la zone DMZ et de l'intérieur vers l'extérieur; ainsi que de la zone DMZ vers l'extérieur. Un critère d'accès est appliqué à l'extérieur pour autoriser le trafic vers les serveurs de la zone DMZ.




```
interface gigabitethernet 1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface gigabitethernet 1/2
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 1/3
  nameif inside2
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 1/4
  nameif inside3
  security-level 100
  bridge-group 1
  no shutdown
!
interface bvi 1
  nameif inside
  security-level 100
  ip address 10.10.10.1 255.255.255.0
```

```
!
interface gigabitethernet 1/5
  nameif dmz1
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/6
  nameif dmz2
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/7
  nameif dmz3
  security-level 100
  bridge-group 2
  no shutdown
!
interface bvi 2
  nameif dmz
  security-level 50
  ip address 209.165.201.1 255.255.255.224
!
same-security-traffic permit inter-interface
!
# Assigns IP addresses to inside hosts
dhcpd address 10.10.10.2-10.10.10.200 inside
dhcpd enable inside
!
# Applies interface PAT for inside traffic going outside
nat (inside1,outside) source dynamic any interface
nat (inside2,outside) source dynamic any interface
nat (inside3,outside) source dynamic any interface
!
# Allows outside traffic to each server for specific applications
object network server1
  host 209.165.201.2
object network server2
  host 209.165.201.3
object network server3
  host 209.165.201.4
!
# Defines mail services allowed on server3
object-group service MAIL
  service-object tcp destination eq pop3
  service-object tcp destination eq imap4
  service-object tcp destination eq smtp
!
# Allows access from outside to servers on the DMZ
access-list SERVERS extended permit tcp any object server1 eq www
access-list SERVERS extended permit tcp any object server2 eq ftp
access-list SERVERS extended permit tcp any object server3 object-group MAIL
access-group SERVERS in interface outside
```

Historique des interfaces en mode routé et en mode transparent

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Découverte de voisin IPv6	7.0(1)	Nous avons introduit cette fonctionnalité. Nous avons introduit les écrans suivants : Monitoring (Supervision) > Interfaces > IPv6 Neighbor Discovery Cache (Cache de découverte de voisin IPv6). Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > IPv6 Neighbor Discovery Cache (Cache de découverte de voisin IPv6). Configuration > Device Setup (Gestion des périphériques) > Interface Settings (Paramètres d'interface) > Interfaces > IPv6.
Prise en charge d'IPv6 pour le mode transparent	8.2(1)	La prise en charge d'IPv6 a été introduite pour le mode de pare-feu transparent.
Groupes de ponts pour le mode transparent	v 8.4(1)	Si vous ne souhaitez pas le surdébit des contextes de sécurité ou si vous souhaitez optimiser votre utilisation des contextes de sécurité, vous pouvez regrouper les interfaces dans un groupe de ponts, puis configurer plusieurs groupes de ponts, un pour chaque réseau. Le trafic de groupe de ponts est isolé des autres groupes de ponts. Vous pouvez configurer jusqu'à huit groupes de ponts de quatre interfaces chacun en mode unique ou par contexte. Nous avons modifié ou introduit les écrans suivants : **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces** **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Bridge Group Interface (Ajouter/Modifier l'interface du groupe de ponts)** **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Interface (Ajouter/modifier l'interface)**
Indicateurs de configuration d'adresse pour le relais DHCP IPv6	9.0(1)	Nous avons modifié l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Interfaces > IPv6.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Nombre maximum de groupes de ponts en mode transparent augmenté à 250	9.3(1)	Le nombre maximum de groupes de ponts est passé de 8 à 250 groupes de ponts. Vous pouvez configurer jusqu'à 250 groupes de ponts en mode unique ou par contexte en mode multiple, avec 4 interfaces maximum par groupe de ponts. Nous avons modifié les écrans suivants : **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces** **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Bridge Group Interface (Ajouter/Modifier l'interface du groupe de ponts)** **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Interface (Ajouter/modifier l'interface)**
Nombre maximum d'interfaces en mode transparent par groupe de ponts augmenté à 64	9.6(2)	Le nombre maximum d'interfaces par groupe de ponts est passé de 4 à 64. Nous n'avons pas modifié d'écrans.
DHCP IPv6	9.6(2)	L'ASA prend désormais en charge les fonctionnalités suivantes pour l'adressage IPv6 : • Client d'adresse DHCPv6 : l'ASA obtient une adresse globale IPv6 et une route par défaut facultative du serveur DHCPv6. • Client de délégation de préfixe DHCPv6 : l'ASA obtient le ou les préfixes délégués d'un serveur DHCPv6. L'ASA peut ensuite utiliser ces préfixes pour configurer d'autres adresses d'interface ASA afin que les clients SLAAC (StateLess Address Auto Configuration) puissent configurer automatiquement les adresses IPv6 sur le même réseau. • Annonce de routeur BGP pour les préfixes délégués • Serveur sans état DHCPv6 : l'ASA fournit d'autres renseignements tels que le nom de domaine aux clients SLAAC lorsqu'ils envoient des paquets de demande d'information (IR) à l'ASA. L'ASA accepte uniquement les paquets IR et n'affecte pas d'adresses aux clients. Nous avons ajouté ou modifié les écrans suivants : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Add Interface (Ajouter une interface)** > **IPv6** **Configuration** > **Device Management (Gestion des périphériques)** > **DHCP** > **DHCP Pool (Réserve DHCP)** **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **BGP** > **IPv6 Family (Famille IPv6)** > **Networks (Réseaux)** **Monitoring (Supervision)** > **Interfaces** > **DHCP**

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Routage et pont intégrés	9.7(1)	Le routage et le pont intégrés permettent d'effectuer le routage entre un groupe de ponts et une interface routée. Un groupe de ponts est un groupe d'interfaces que l'ASA relie par des ponts au lieu de routes. L'ASA n'est pas un vrai pont, car l'ASA continue d'agir comme un pare-feu : le contrôle d'accès entre les interfaces est contrôlé et toutes les vérifications de pare-feu usuelles sont en place. Auparavant, vous ne pouviez configurer les groupes de ponts qu'en mode de pare-feu transparent, où vous ne pouvez pas effectuer d'acheminement entre les groupes de ponts. Cette fonctionnalité vous permet de configurer des groupes de ponts en mode de pare-feu routé et pour effectuer le routage entre des groupes de ponts et entre un groupe de ponts et une interface routée. Le groupe de ponts participe au routage en utilisant une interface virtuelle de pont (BVI) pour servir de passerelle au groupe de ponts. Le routage et le pont intégrés offrent une solution de rechange au commutateur de couche 2 externe si vous avez des interfaces supplémentaires sur l'ASA à affecter au groupe de ponts. En mode routé, les BVI peuvent être une interface nommée et participer séparément des interfaces membres à certaines fonctionnalités, telles que les règles d'accès et le serveur DHCP. Les fonctionnalités suivantes, prises en charge en mode transparent, ne sont pas prises en charge en mode routé : mode de contexte multiple, mise en grappe d'ASA. Les fonctionnalités suivantes ne sont pas prises en charge sur les BVI : le routage dynamique et le routage de multidiffusion. Nous avons modifié les écrans suivants : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Static Routes (Routes statiques)** **Configuration** > **Device Management (Gestion des périphériques)** > **DHCP** > **DHCP Server (Serveur DHCP)** **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Critères d'accès)** **Configuration** > **Firewall (Pare-feu)** > **EtherType Rules (Règles EtherType)**

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Masque de sous-réseau 31 bits	9.7(1)	Pour les interfaces routées, vous pouvez configurer une adresse IP sur un sous-réseau de 31 bits pour les connexions point à point. Le sous-réseau de 31 bits comprend seulement 2 adresses; normalement, la première et la dernière adresse du sous-réseau sont réservées pour le réseau et la diffusion, donc un sous-réseau à deux adresses n'est pas utilisable. Toutefois, si vous avez une connexion point à point et n'avez pas besoin d'adresses de réseau ou de diffusion, un sous-réseau de 31 bits est un moyen utile de conserver les adresses dans IPv4. Par exemple, la liaison de basculement entre 2 ASA ne nécessite que 2 adresses; les paquets transmis par une extrémité de la liaison sont toujours reçus par l'autre extrémité, et la diffusion n'est pas nécessaire. Vous pouvez également avoir une station de gestion directement connectée exécutant SNMP ou Syslog. Cette fonctionnalité n'est pas prise en charge pour les BVI pour les groupes de ponts ou avec le routage de multidiffusion. Nous avons modifié les écrans suivants : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Add Interface (Ajouter une interface)** > **General (Général)**

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.