Adresses, protocoles et ports

Ce chapitre fournit une référence rapide des adresses IP, des protocoles et des applications.

Adresses IPv4 et filtres d'adresse locale

Cette section décrit comment utiliser les adresses IPv4 dans l'ASA. Une adresse IPv4 est un nombre de 32 bits écrits en notation décimale à points : quatre champs de 8 bits (octets) convertis de nombres binaires en nombres décimaux, séparés par des points. La première partie d'une adresse IP identifie le réseau sur lequel réside l'hôte, tandis que la seconde partie identifie l'hôte sur le réseau donné. Le champ de numéro de réseau s'appelle le préfixe réseau. Tous les hôtes sur un réseau donné partagent le même préfixe réseau, mais doivent avoir un numéro d'hôte unique. Dans un réseau avec des classes d'adresses IP, la classe de l'adresse détermine la limite entre le préfixe de réseau et le numéro d'hôte.

Classes

Les adresses IP des hôtes sont divisées en trois classes d'adresses différentes : la classe A, la classe B et la classe C. Chaque classe fixe la limite entre le préfixe réseau et le numéro d'hôte à un point différent dans l'adresse de 32 bits. Les adresses de classe D sont réservées à l'IP de multidiffusion.

- Les adresses de classe A (1.xxx.xxx.xxx à 126.xxx.xxx.xxx) utilisent uniquement le premier octet comme préfixe réseau.
- Les adresses de classe B (128.0.xxx.xxx à 191.255.xxx.xxx) utilisent les deux premiers octets comme préfixe réseau.
- Les adresses de classe C (192.0.0.xxx à 223.255.255.xxx) utilisent les trois premiers octets comme préfixe réseau.

Comme les adresses de classe A ont 16 777 214 adresses d'hôtes et les adresses de classe B de 65 534 hôtes, vous pouvez utiliser le filtrage d'adresse locale pour diviser ces énormes réseaux en sous-réseaux plus petits.

Réseaux privés

Si vous avez besoin d'un grand nombre d'adresses sur votre réseau, et qu'elles n'ont pas besoin d'être acheminées sur Internet, vous pouvez utiliser des adresses IP privées que l'autorité d'attribution de numéros par Internet (IANA) recommande (voir RFC 1918). Les plages d'adresses suivantes sont désignées comme des réseaux privés qui ne doivent pas être annoncés :

- 10.0.0.0 à 10.255.255.255
- 172.16.0.0 à 172.31.255.255
- 192.168.0.0 à 192.168.255.255

Filtres d'adresse locale

Un filtre d'adresse locale vous permet de convertir un seul réseau de classe A, B ou C en plusieurs réseaux. Avec un filtre d'adresse locale, vous pouvez créer un préfixe de réseau étendu qui ajoute des bits du numéro d'hôte au préfixe de réseau. Par exemple, un préfixe de réseau de classe C est toujours composé des trois premiers octets de l'adresse IP. Mais un préfixe de réseau étendu de classe C utilise également une partie du quatrième octet.

Le filtrage d'adresse locale est facile à comprendre si vous utilisez la notation binaire au lieu de la notation décimale à points. Les bits du filtre d'adresse locale ont une correspondance un-à-un avec l'adresse Internet :

- Les bits sont définis sur 1 si le bit correspondant dans l'adresse IP fait partie du préfixe de réseau étendu.
- Les bits sont définis sur 0 si le bit fait partie du numéro d'hôte.

Exemple 1 : si vous avez l'adresse de classe B 129.10.0.0 et que vous souhaitez utiliser le troisième octet dans le préfixe du réseau étendu au lieu du numéro d'hôte, vous devez spécifier un filtre d'adresse locale 11111111.11111111.11111111.00000000. Ce filtre d'adresse locale convertit l'adresse de classe B en équivalent d'une adresse de classe C, où le numéro d'hôte est composé uniquement du dernier octet.

Exemple 2 : si vous souhaitez utiliser une partie du troisième octet pour le préfixe de réseau étendu, vous devez préciser un filtre d'adresse locale comme 11111111.11111111.11111000.00000000, qui utilise seulement 5 bits du troisième octet pour le préfixe de réseau étendu.

Vous pouvez écrire un filtre d'adresse locale sous forme de masque décimal à points ou de masque /*bits* (« barre oblique *bits* »). Dans l'exemple 1, pour un masque décimal à points, vous convertissez chaque octet binaire en un nombre décimal : 255.255.255.0. Pour un masque /*bits*, vous ajoutez le nombre de 1 : /24. Dans l'exemple 2, le nombre décimal est 255.255.248.0 et le /bits est /21.

Vous pouvez également regrouper plusieurs réseaux de classe C dans un réseau plus vaste en utilisant une partie du troisième octet pour le préfixe de réseau étendu. Par exemple, 192.168.0.0/20.

Déterminer le filtre d'adresse locale

Consultez le tableau suivant pour déterminer le filtre d'adresse locale en fonction du nombre d'hôtes souhaité.

Remarque Le premier et le dernier numéro d'un sous-réseau sont réservés, à l'exception de /32, qui identifie un seul hôte.

Tableau 1 : Hôtes, bits et masques décimaux à points

Hôtes	/Masque de bits	Masque décimal à points
16,777,216	/8	Réseau de classe A 255.0.0.0
65,536	/16	Réseau de classe B 255.255.0.0
32,768	/17	255.255.128.0
16,384	/18	255.255.192.0
8192	/19	255.255.224.0
4096	/20	255.255.240.0
2048	/21	255.255.248.0
1024	/22	255.255.252.0
512	/23	255.255.254.0
256	/24	Réseau de classe C 255.255.255.0
128	/25	255.255.255.128
64	/26	255.255.255.192
32	/27	255.255.255.224
16	/28	255.255.255.240
8	/29	255.255.255.248
4	/30	255.255.255.252
Ne pas utiliser	/31	255.255.255.254
1	/32	Adresse d'hôte unique 255.255.255.255

Déterminer l'adresse à utiliser avec le filtre d'adresse locale

Les sections suivantes décrivent comment déterminer l'adresse réseau à utiliser avec un filtre d'adresse locale pour un réseau de classe C et de classe B.

Adresse réseau de classe C

Pour un réseau compris entre 2 et 254 hôtes, le quatrième octet tombe sur un multiple du nombre d'adresses d'hôte, en commençant par 0. Par exemple, le tableau suivant montre les sous-réseaux de 8 hôtes (/29) de 192.168.0.x.

Remarque La première et la dernière adresses d'un sous-réseau sont réservées. Dans le premier exemple de sous-réseau, vous ne pouvez pas utiliser 192.168.0.0 ou 192.168.0.7.

Tableau 2 : Adresse réseau de classe C

Sous-réseau avec le masque /29 (255.255.255.248)	Plage d'adresses
192.168.0.0	De 192.168.0.0 à 192.168.0.7
192.168.0.8	De 192.168.0.8 à 192.168.0.15
192.168.0.16	De 192.168.0.16 à 192.168.0.31
—	—
192.168.0.248	De 192.168.0.248 à 192.168.0.255

Adresse réseau de classe B

Pour déterminer l'adresse réseau à utiliser avec le filtre d'adresse locale pour un réseau de 254 à 65 534 hôtes, vous devez déterminer la valeur du troisième octet pour chaque préfixe de réseau étendu possible. Par exemple, vous pouvez créer une adresse de sous-réseau comme 10.1.*x*.0, où les deux premiers octets sont fixes, car ils sont utilisés dans le préfixe de réseau étendu, et le quatrième octet est 0, car tous les bits sont utilisés pour le numéro d'hôte.

Pour déterminer la valeur du troisième octet, procédez comme suit :

1. Calculez le nombre de sous-réseaux que vous pouvez créer à partir du réseau en divisant 65 536 (le nombre total d'adresses en utilisant le troisième et le quatrième octet) par le nombre d'adresses d'hôtes souhaitées.

   Par exemple, 65 536 divisés par 4 096 hôtes équivaut à 16. Par conséquent, il existe 16 sous-réseaux de 4 096 adresses chacun dans un réseau de classe B.

2. Déterminez le multiple de la valeur du troisième octet en divisant 256 (le nombre de valeurs pour le troisième octet) par le nombre de sous-réseaux :

   Dans cet exemple, 256/16 = 16.

   Le troisième octet correspond à un multiple de 16, commençant par 0.

Le tableau suivant présente les 16 sous-réseaux du réseau 10.1.

Remarque La première et la dernière adresses d'un sous-réseau sont réservées. Dans le premier exemple de sous-réseau, vous ne pouvez pas utiliser 10.1.0.0 ou 10.1.15.255.

Tableau 3 : Sous-réseaux du réseau

Sous-réseau avec le masque /20 (255.255.240.0)	Plage d'adresses
10/100	De 10.1.0.0 à 10.1.15.255
10.1.16.0	De 10.1.16.0 à 10.1.31.255
10.1.32.0	De 10.1.32.0 à 10.1.47.255
—	—

Sous-réseau avec le masque /20 (255.255.240.0)	Plage d'adresses
10.1.240.0	De 10.1.240.0 à 10.1.255.255

Adresses IPv6

IPv6 est la prochaine génération de protocole Internet après IPv4. Il fournit un espace d'adressage étendu, un format d'en-tête simplifié, une prise en charge améliorée des extensions et des options, une capacité d'étiquetage des flux, ainsi que des capacités d'authentification et de confidentialité. IPv6 est décrit dans la RFC 2460. L'architecture d'adressage IPv6 est décrite dans la RFC 3513.

Cette section décrit le format et l'architecture de l'adresse IPv6.

Format d'adresses IPv6

Les adresses IPv6 sont représentées par une série de huit champs hexadécimaux de 16 bits séparés par des deux-points (:) au format : x:x:x:x:x:x:x:x. Voici deux exemples d'adresses IPv6 :

- 2001:0DB8:7654:3210:FEDC:BA98:7654:3210
- 2001:0DB8:0000:0000:0008:0800:200C:417A

Remarque Les lettres hexadécimales dans les adresses IPv6 ne sont pas sensibles à la casse.

Vous n'avez pas besoin d'inclure les zéros initiaux dans un champ individuel de l'adresse, mais chaque champ doit contenir au moins un chiffre. Ainsi, l'exemple d'adresse 2001:0DB8:0000:0000:0008:0800:200C:417A peut être raccourci à 2001:0DB8:0:0:8:800:200C:417A en supprimant les zéros initiaux du troisième au cinquième champs à partir de la gauche. Les champs qui contiennent tous des zéros (les troisième et quatrième champs à partir de la gauche) ont été raccourcis à un seul zéro. Les trois zéros initiaux ont été supprimés dans le cinquième champ à partir de la gauche, ce qui a laissé un seul 8 dans ce champ, et le zéro initial a été supprimé dans le sixième champ à partir de la gauche, laissant 800 dans ce champ.

Il est courant que les adresses IPv6 contiennent plusieurs champs hexadécimaux consécutifs de zéros. Vous pouvez utiliser deux signes de deux-points (::) pour compresser des champs consécutifs de zéros au début, au milieu ou à la fin d'une adresse IPv6 (les deux-points représentent les champs hexadécimaux successifs de zéros). Le tableau suivant présente plusieurs exemples de compression d'adresses pour différents types d'adresses IPv6.

Tableau 4 : Exemples de compression d'adresses IPv6

Type d'adresse	Forme standard	Forme compressée
Monodiffusion	2001:0DB8:0:0:0:BA98:0:3210	2001:0DB8::BA98:0:3210
Multicast (multidiffusion)	FF01:0:0:0:0:0:0:101	FF01::101
Boucle avec retour	0:0:0:0:0:0:0:1	::1

Type d'adresse	Forme standard	Forme compressée
Non défini	0:0:0:0:0:0:0:0	::

Remarque Deux signes de deux-points (::) ne peuvent être utilisés qu'une seule fois dans une adresse IPv6 pour représenter des champs successifs de zéros.

Une autre forme du format IPv6 est souvent utilisée lorsqu'il s'agit d'un environnement contenant des adresses IPv4 et IPv6. Cette alternative a le format x:x:x:x:x:x:y.y.y.y, où x représente les valeurs hexadécimales des six parties de l'adresse IPv6 et y représente les valeurs décimales de la partie IPv4 de 32 bits de l'adresse (qui prend la place des deux autres parties de 16 bits de l'adresse IPv6). Par exemple, l'adresse IPv4 192.168.1.1 pourrait être représentée comme l'adresse IPv6 0:0:0:0:0:0:FFFF:192.168.1.1 ou ::FFFF:192.168.1.1.

Types d'adresses IPv6

Les trois principaux types d'adresses IPv6 sont les suivants :

- **Monodiffusion** : une adresse de monodiffusion est un identifiant pour une seule interface. Un paquet envoyé à une adresse de monodiffusion est livré à l'interface identifiée par cette adresse. Une interface peut avoir plusieurs adresses de monodiffusion.
- **Multidiffusion** : une adresse de multidiffusion est un identifiant pour un ensemble d'interfaces. Un paquet envoyé à une adresse de multidiffusion est transmis à toutes les adresses identifiées par cette adresse.
- **Anycast** : une adresse Anycast est un identifiant pour un ensemble d'interfaces. Contrairement à une adresse de multidiffusion, un paquet envoyé à une adresse Anycast n'est livré qu'à l'interface « la plus proche », comme déterminé par la mesure des distances pour le protocole de routage.

Remarque Il n'y a pas d'adresses de diffusion dans IPv6. Les adresses de multidiffusion fournissent la fonctionnalité de diffusion.

Adresses de monodiffusion

Cette section décrit les adresses de monodiffusion IPv6. Les adresses de monodiffusion identifient une interface sur un nœud de réseau.

Adresse globale

Le format général d'une adresse de monodiffusion globale IPv6 est un préfixe de routage global suivi d'un ID de sous-réseau suivi d'un ID d'interface. Le préfixe de routage global peut être n'importe quel préfixe non réservé par un autre type d'adresse IPv6.

Toutes les adresses de monodiffusion globales, hormis celles commençant par le binaire 000, ont un ID d'interface de 64 bits au format EUI-64 modifié.

Les adresses de monodiffusion globales commençant par le binaire 000 n'ont aucune contrainte quant à la taille ou à la structure de la partie ID d'interface de l'adresse. Un exemple de ce type d'adresse est une adresse IPv6 avec une adresse IPv4 intégrée.

Adresse Site-Local

Les adresses Site-Local sont utilisées pour l'adressage au sein d'un site. Elles peuvent être utilisées pour traiter un site entier sans utiliser de préfixe globalement unique. Les adresses Site-Local ont le préfixe FEC0::/10, suivi d'un ID de sous-réseau de 54 bits, et se terminent par un ID d'interface de 64 bits au format EUI-64 modifié.

Les routeurs Site-Local ne transfèrent pas les paquets qui ont une adresse Site-Local pour une source ou une destination à l'extérieur du site. Par conséquent, les adresses Site-Local peuvent être considérées comme des adresses privées.

Adresse Link-Local

Toutes les interfaces doivent avoir au moins une adresse Link-Local. Vous pouvez configurer plusieurs adresses IPv6 par interface, mais une seule adresse Link-Local.

Une adresse Link-Local est une adresse de monodiffusion IPv6 qui peut être configurée automatiquement sur n'importe quelle interface à l'aide du préfixe de lien local FE80::/10 et de l'identifiant d'interface au format EUI-64 modifié. Les adresses Link-Local sont utilisées dans le protocole de découverte de voisin et dans le processus de configuration automatique sans état. Les nœuds ayant une adresse Link-Local peuvent communiquer; ils n'ont pas besoin d'une adresse locale au site ou d'une adresse unique au niveau mondial pour communiquer.

Les routeurs ne transfèrent pas les paquets qui ont une adresse Link-Local pour un contrôleur source ou de destination. Par conséquent, les adresses Link-Local peuvent être considérées comme des adresses privées.

Adresses IPv6 compatibles avec IPv4

Il existe deux types d'adresses IPv6 qui peuvent contenir des adresses IPv4.

Le premier type est l'adresse IPv6 compatible avec IPv4. Les mécanismes de transition IPv6 comprennent une technique permettant aux hôtes et aux routeurs de tunneler de manière dynamique les paquets IPv6 sur l'infrastructure de routage IPv4. Les nœuds IPv6 qui utilisent cette technique se voient attribuer des adresses de monodiffusion IPv6 spéciales qui transportent une adresse IPv4 globale dans les 32 bits de poids faible. Ce type d'adresse est appelé adresse IPv6 compatible avec IPv4 et a le format ::y.y.y.y, où y.y.y.y est une adresse de monodiffusion IPv4.

Remarque L'adresse IPv4 utilisée dans l'adresse IPv6 compatible avec IPv4 doit être une adresse de monodiffusion IPv4 globalement unique.

Le deuxième type d'adresse IPv6, qui contient une adresse IPv4 intégrée, s'appelle l'adresse IPv6 mappée en IPv4. Ce type d'adresse est utilisé pour représenter les adresses des nœuds IPv4 en tant qu'adresses IPv6. Ce type d'adresse est au format ::FFFF:y.y.y.y, où y.y.y.y est une adresse de monodiffusion IPv4.

Adresse non spécifiée

L'adresse non spécifiée, 0:0:0:0:0:0:0:0, indique l'absence d'adresse IPv6. Par exemple, un nœud nouvellement initialisé sur un réseau IPv6 peut utiliser l'adresse non spécifiée comme adresse source dans ses paquets jusqu'à ce qu'il reçoive son adresse IPv6.

Remarque L'adresse IPv6 non spécifiée ne peut pas être attribuée à une interface. Les adresses IPv6 non spécifiées ne doivent pas être utilisées comme adresses de destination dans les paquets IPv6 ou dans l'en-tête de routage IPv6.

Adresse de la boucle avec retour

L'adresse de boucle avec retour, 0:0:0:0:0:0:0:1, peut être utilisée par un nœud pour s'envoyer un paquet IPv6. L'adresse de boucle avec retour dans IPv6 fonctionne de la même manière que l'adresse de boucle avec retour dans IPv4 (127.0.0.1).

Remarque L'adresse de boucle avec retour IPv6 ne peut pas être attribuée à une interface physique. Un paquet qui a l'adresse de boucle avec retour IPv6 comme adresse source ou de destination doit rester dans le nœud qui a créé le paquet. Les routeurs IPv6 ne transfèrent pas les paquets qui ont l'adresse de boucle avec retour IPv6 comme adresse source ou de destination.

Identifiants de l'interface

Les identifiants d'interface dans les adresses de monodiffusion IPv6 sont utilisés pour identifier les interfaces sur une liaison. Ils doivent être uniques dans un préfixe de sous-réseau. Dans de nombreux cas, l'identifiant d'interface est dérivé de l'adresse de la couche de liaison de l'interface. Le même identifiant d'interface peut être utilisé sur plusieurs interfaces d'un seul nœud, tant que ces interfaces sont associées à des sous-réseaux différents.

Pour toutes les adresses de monodiffusion, à l'exception de celles qui commencent par le binaire 000, l'identifiant d'interface doit comporter 64 bits et être généré au format EUI-64 modifié. Le format EUI-64 modifié est créé à partir de l'adresse MAC de 48 bits en inversant le bit universel/local dans l'adresse et en insérant le numéro hexadécimal FFFE entre les trois octets supérieurs et les trois octets inférieurs de l'adresse MAC.

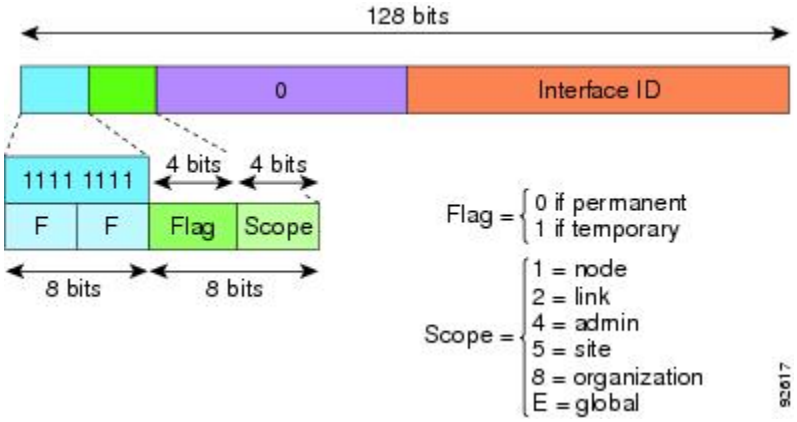
Par exemple, une interface ayant l'adresse MAC 00E0.b601.3B7A aura un ID d'interface de 64 bits 02E0:B6FF:FE01:3B7A.

Multicast Address (Adresse multidiffusion)

Une adresse de multidiffusion IPv6 est un identifiant pour un groupe d'interfaces, généralement sur des nœuds différents. Un paquet envoyé à une adresse de multidiffusion est transmis à toutes les interfaces identifiées par l'adresse de multidiffusion. Une interface peut appartenir à un nombre illimité de groupes de multidiffusion.

Une adresse de multidiffusion IPv6 a un préfixe FF00::/8 (1111 1111). L'octet suivant le préfixe définit le type et la portée de l'adresse de multidiffusion. Une adresse de multidiffusion attribuée de façon permanente (bien connue) a un paramètre d'indicateur égal à 0; une adresse de multidiffusion temporaire (transitoire) a un paramètre d'indicateur égal à 1. Une adresse de multidiffusion qui a la portée d'un nœud, d'une liaison, d'un site ou d'une organisation, ou une portée globale, a un paramètre de portée de 1, 2, 5, 8 ou E, respectivement. Par exemple, une adresse de multidiffusion avec le préfixe FF02::/16 est une adresse de multidiffusion permanente avec une portée de liaison. La figure suivante montre le format d'adresse de multidiffusion IPv6.

Illustration 1 : Format d'adresse de multidiffusion IPv6



Les nœuds IPv6 (hôtes et routeurs) doivent se joindre aux groupes de multidiffusion suivants :

- Les adresses de multidiffusion de tous les nœuds :
  - FF01:: (interface locale)
  - FF02:: (liaison locale)
- L'adresse du nœud sollicité pour chaque adresse de monodiffusion IPv6 et toute adresse Anycast sur le nœud : FF02:0:0:0:0:1:FFXX:XXXX/104, où XX:XXXX correspond aux 24 bits de poids faible de l'adresse de monodiffusion ou de l'adresse Anycast.

Remarque Les adresses de nœud sollicité sont utilisées dans les messages de demande de voisin.

Les routeurs IPv6 doivent se joindre aux groupes de multidiffusion suivants :

- FF01::2 (interface locale)
- FF02::2 (liaison locale)
- FF05::2 (site local)

L'adresse de multidiffusion ne doit pas être utilisée comme adresses source dans les paquets IPv6.

Remarque Il n'y a pas d'adresses de diffusion dans IPv6. Les adresses de multidiffusion IPv6 sont utilisées à la place des adresses de diffusion.

Adresse Anycast

L'adresse Anycast IPv6 est une adresse de monodiffusion attribuée à plusieurs interfaces (appartenant généralement à des nœuds différents). Un paquet qui est acheminé vers une adresse Anycast est acheminé vers l'interface la plus proche ayant cette adresse, la proximité étant déterminée par le protocole de routage en vigueur.

Les adresses Anycast sont attribuées à partir de l'espace d'adressage de monodiffusion. Une adresse Anycast est simplement une adresse de monodiffusion qui a été attribuée à plusieurs interfaces, et les interfaces doivent être configurées pour reconnaître l'adresse comme une adresse Anycast.

Les restrictions suivantes s'appliquent aux adresses Anycast :

- Une adresse Anycast ne peut pas être utilisée comme adresse source pour un paquet IPv6.
- Une adresse Anycast ne peut pas être attribuée à un hôte IPv6; elle ne peut être attribuée qu'à un routeur IPv6.

Remarque Les adresses Anycast ne sont pas prises en charge sur l'ASA.

Adresses requises

Les hôtes IPv6 doivent au moins être configurés avec les adresses suivantes (automatiquement ou manuellement) :

- Une adresse Link-Local pour chaque interface
- L'adresse de boucle avec retour
- Les adresses de multidiffusion de tous les nœuds
- Une adresse de multidiffusion de nœud sollicité pour chaque adresse de monodiffusion ou Anycast

Les routeurs IPv6 doivent au moins être configurés avec les adresses suivantes (automatiquement ou manuellement) :

- Les adresses d'hôte requises
- Les adresses Anycast du routeur de sous-réseau pour toutes les interfaces pour lesquelles il est configuré pour agir en tant que routeur
- Les adresses de multidiffusion de tous les routeurs

Préfixes de l'adresse IPv6

Un préfixe d'adresse IPv6, au format ipv6-prefix/prefix-length, peut être utilisé pour représenter les blocs contigus de bit de l'ensemble de l'espace d'adressage. Le préfixe IPv6 doit être sous la forme documentée dans la RFC 2373, où l'adresse est spécifiée en format hexadécimal en utilisant des valeurs de 16 bits entre les deux-points. La longueur du préfixe est une valeur décimale qui indique le nombre de bits contigus de poids fort de l'adresse qui composent le préfixe (la partie réseau de l'adresse). Par exemple, 2001:0DB8:8086:6502::/32 est un préfixe IPv6 valide.

Le préfixe IPv6 identifie le type d'adresse IPv6. Le tableau suivant affiche les préfixes pour chaque type d'adresse IPv6.

Tableau 5 : Préfixes de type d'adresse IPv6

Type d'adresse	Préfixe binaire	Notation IPv6
Non défini	000...0 (128 bits)	::/128

Type d'adresse	Préfixe binaire	Notation IPv6
Boucle avec retour	000...1 (128 bits)	::1/128
Multicast (multidiffusion)	11111111	FF00::/8
Lien local (monodiffusion)	1111111010	FE80::/10
Site local (monodiffusion)	1111111111	FEC0::/10
Global (monodiffusion)	Toutes les autres adresses.	
Anycast	Tiré de l'espace d'adressage de monodiffusion.	

Protocoles et applications

Le tableau suivant répertorie les valeurs littérales du protocole et les numéros de port; l'un ou l'autre peut être saisi dans les commandes ASA.

Tableau 6 : Valeurs littérales du protocole

Littéral	Valeur	Description
ah	51	En-tête d'authentification pour IPv6, RFC 1826.
eigrp	88	Protocole de routage de passerelle intérieure amélioré.
esp	50	Charge utile de sécurité encapsulée pour IPv6, RFC 1827.
gre	47	Encapsulation générale du routeur.
ICMP	1	Internet Control Message Protocol, RFC 792.
icmp6	58	Internet Control Message Protocol pour IPv6, RFC 2463.
igmp	2	Internet Group Management Protocol, RFC 1112.
igrp	9	Protocole de routage de passerelle intérieure.
ip	0	Protocole Internet.
ipinip	4	Encapsulation IP-en-IP.
IPsec	50	Sécurité IP. La saisie du littéral de protocole ipsec équivaut à la saisie du littéral de protocole esp.
nos	94	Système d'exploitation réseau (NetWare de Novell).
ospf	89	Protocole de routage Open Shortest Path First, RFC 1247.
pcp	108	Protocole de compression de charge utile.
pim	103	Protocol Independent Multicast.

Littéral	Valeur	Description
pptp	47	Protocole Point-to-Point Tunneling. La saisie du littéral de protocole pptp équivaut à la saisie du littéral de protocole gre.
snp	109	Protocole de réseau Sitara.
TCP	6	Protocole de commande de transmission, RFC 793.
UDP	17	Protocole de datagramme d'utilisateur, RFC 768.

Vous pouvez consulter les numéros de protocole en ligne sur le site Web de l'IANA :

http://www.iana.org/assignments/protocol-numbers

Ports TCP et UDP

Le tableau suivant répertorie les valeurs littérales et les numéros de port; l'un ou l'autre peut être saisi dans les commandes ASA. Consultez les avertissements suivants :

- L'ASA utilise le port 1521 pour SQL*Net. Il s'agit du port par défaut utilisé par Oracle pour SQL*Net. Cette valeur n'est toutefois pas conforme aux attributions de ports de l'IANA.
- L'ASA écoute RADIUS sur les ports 1645 et 1646. Si votre serveur RADIUS utilise les ports standard 1812 et 1813, vous pouvez configurer l'ASA pour qu'il écoute ces ports à l'aide des commandes **authentication-port** et **accounting-port**.
- Pour attribuer un port pour l'accès DNS, utilisez la valeur littérale **domain**, et non **dns**. Si vous utilisez **dns**, l'ASA suppose que vous souhaitez utiliser la valeur littérale **dnsix**.

Vous pouvez consulter les numéros de port en ligne sur le site Web de l'IANA :

http://www.iana.org/assignments/port-numbers

Tableau 7 : Valeurs littérales des ports

Littéral	TCP ou UDP?	Valeur	Description
aol	TCP	5190	Amérique en ligne
bgp	TCP	179	Protocole de passerelle frontière, RFC 1163
biff	UDP	512	Utilisé par le système de messagerie pour informer les utilisateurs de la réception d'un nouveau message
bootpc	UDP	68	Client du protocole de démarrage
bootps	UDP	67	Serveur du protocole de démarrage
chargen	TCP	19	Générateur de caractères
cifs	TCP, UDP	3020	Protocole CIFS

Littéral	TCP ou UDP?	Valeur	Description
citrix-ica	TCP	1494	Protocole Citrix Independent Computing Architecture (ICA)
CMD	TCP	514	Similaire à exec, sauf que cmd dispose d'une authentification automatique
ctiqbe	TCP	2748	Encodage rapide de tampon de l'interface de téléphonie de l'ordinateur
daytime	TCP	13	Heure du jour, RFC 867
supprimer	TCP, UDP	9	Supprimer
dnsix	UDP	195	Redirecteur d'audit du module de gestion des sessions DNSIX
domaine	TCP, UDP	53	DNS
echo	TCP, UDP	7	Écho
exec	TCP	512	Exécution du processus à distance
finger	TCP	79	Finger
ftp	TCP	21	Protocole de transfert de fichier (port de contrôle)
données-ftp	TCP	20	Protocole de transfert de fichier (port de données)
gopher	TCP	70	Gopher
h323	TCP	1720	Signalisation d'appel H.323
nom d'hôte	TCP	101	Serveur de noms d'hôte NIC
http	TCP, UDP	80	HTTP Internet
https	TCP	443	HTTP sur SSL
ident	TCP	113	Service d'authentification Ident
imap4	TCP	143	Protocole IMAP (Internet Message Access Protocol), version 4
irc	TCP	194	Protocole de discussion IRC (Internet Relay Chat)
isakmp	UDP	500	protocole ISAKMP (Internet Security Association and Key Management Protocol)
kerberos	TCP, UDP	750	Kerberos
klogin	TCP	543	KLOGIN
kshell	TCP	544	Korn Shell

Littéral	TCP ou UDP?	Valeur	Description
ldap	TCP	389	Protocole Lightweight Directory Access Protocol
ldaps	TCP	636	Protocole Lightweight Directory Access Protocol (SSL)
connexion	TCP	513	Connexion à distance
lotusnotes	TCP	1352	Lotus Notes IBM
lpd	TCP	515	Démon d'impression en ligne – spouleur d'impression
mobile-ip	UDP	434	Agent IP mobile
nameserver	UDP	42	Serveur de noms d'hôte
netbios-dgm	UDP	138	Service de datagrammes NetBIOS
netbios-ns	UDP	137	Service de noms NetBIOS
netbios-ssn	TCP	139	Service de sessions NetBIOS
nfs	TCP, UDP	2049	Système de fichiers réseau – Sun Microsystems
nntp	TCP	119	Protocole de transfert des informations du réseau
ntp	UDP	123	Protocole de synchronisation réseau
pcanywhere-data	TCP	5631	Données pcAnywhere
pcanywhere-status	UDP	5632	État pcAnywhere
pim-auto-rp	TCP, UDP	496	PIM (Protocole Independent Multicast), inondation de chemin inverse, mode dense
pop2	TCP	109	Protocole du bureau de poste – Version 2
pop3	TCP	110	Protocole du bureau de poste – Version 3
pptp	TCP	1723	Protocole Point-to-Point Tunneling
radius	UDP	1645	Service d'usager commuté à authentification distante
radius-acct	UDP	1646	Service d'usager commuté à authentification distante (comptabilité)
protocole RIP	UDP	520	Protocole d'information de routage
rsh	TCP	514	Shell distant
rtsp	TCP	554	Protocole de diffusion en flux continu en temps réel
secureid-udp	UDP	5510	SecureID sur UDP
sip	TCP, UDP	5060	Protocole d'initiation de session (SIP)

Littéral	TCP ou UDP?	Valeur	Description
smtp	TCP	25	Protocole de transport de messagerie simple
snmp	UDP	161	Protocole SNMP (gestion de réseau simple)
snmptrap	UDP	162	Protocole simple de gestion de réseau – Interruption
sqlnet	TCP	1521	Réseau SQL (Structured Query Language)
ssh	TCP	22	Protocole SSH (Secure Shell)
sunrpc	TCP, UDP	111	Appel de procédure à distance Sun
syslog	UDP	514	System Log (journal du système)
tacacs	TCP, UDP	49	Système de contrôle d'accès du contrôleur d'accès du terminal Plus
talk	TCP, UDP	517	Talk
telnet	TCP	23	Telnet RFC 854
tftp	UDP	69	protocole TFTP (Trivial File Transfer Protocol)
de temps	UDP	37	Durée
uucp	TCP	540	Programme de copie UNIX à UNIX
vxlan	UDP	4789	Réseau local extensible virtuel (VXLAN)
who	UDP	513	Qui
Whois	TCP	43	Qui est
www	TCP, UDP	80	Internet
xdmcp	UDP	177	Protocole de contrôle du gestionnaire d'affichage X

Ports et protocoles locaux

Le tableau suivant répertorie les protocoles, les ports TCP et les ports UDP que l'ASA peut ouvrir pour traiter le trafic destiné à l'ASA. À moins que vous activiez les fonctionnalités et les services énumérés dans ce tableau, l'ASA *n'ouvre* aucun protocole local ni port TCP ou UDP. Vous devez configurer une fonctionnalité ou un service pour que l'ASA ouvre le protocole d'écoute ou le port par défaut. Dans de nombreux cas, vous pouvez configurer des ports autres que le port par défaut lorsque vous activez une fonctionnalité ou un service.

Tableau 8 : Protocoles et ports ouverts par les fonctionnalités et services

Fonctionnalité ou service	Protocole	Numéro de port	Commentaires
DHCP (protocole de configuration dynamique des hôtes)	UDP	67,68	—
Contrôle du basculement	105	s.o.	—
HTTP	TCP	80	—
HTTPS	TCP	443	—
ICMP	1	S.O.	—
IGMP	2	S. O.	Protocole ouvert uniquement sur l'adresse IP de destination 224.0.0.1
ISAKMP/IKE	UDP	500	Configurable.
IPsec (ESP)	50	S. O.	—
IPsec sur UDP (NAT-T)	UDP	4500	—
IPsec sur TCP (CTCP)	TCP	—	Aucun port par défaut n'est utilisé. Vous devez spécifier le numéro de port lors de la configuration d'IPsec sur TCP.
NTP;	UDP	123	—
OSPF	89	s.o.	Protocole ouvert uniquement sur les adresses IP de destination 224.0.0.5 et 224.0.0.6
Protocole PIM	103	s.o.	Protocole ouvert uniquement sur l'adresse IP de destination 224.0.0.13
RIP	UDP	520	—
Protocole RIPv2	UDP	520	Port ouvert uniquement sur l'adresse IP de destination 224.0.0.9
SNMP	UDP	161	Configurable.
SSH	TCP	22	—
Mise à jour de l'état	8 (non sécurisé) 9 (sécurisé)	S. O.	—
Telnet	TCP	23	—
Équilibrage de la charge VPN	UDP	9023	Configurable.

Fonctionnalité ou service	Protocole	Numéro de port	Commentaires
Mandataire d'authentification de l'utilisateur individuel pour le VPN	UDP	1645, 1646	Port accessible uniquement sur le tunnel VPN.

Types ICMP

Le tableau suivant répertorie les numéros et les noms de type ICMP que vous pouvez saisir dans les commandes ASA.

Tableau 9 : Types ICMP

Numéro ICMP	Nom ICMP
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
30	traceroute
31	conversion-error

Numéro ICMP	Nom ICMP
32	mobile-redirect

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.