

Configuration de base de l'interface pour les ports de commutation du Firepower 1010

Vous pouvez configurer chaque interface Firepower 1010 pour qu'elle fonctionne comme une interface pare-feu normale ou comme un port de commutateur matériel de couche 2. Ce chapitre comprend les tâches de démarrage de la configuration de votre port de commutation, notamment l'activation ou la désactivation du mode de commutation, la création d'interfaces VLAN et l'affectation des ports de commutation aux réseaux VLAN. Ce chapitre décrit également comment personnaliser l'alimentation par Ethernet (PoE) sur les interfaces prises en charge.

- À propos des ports de commutation, à la page 1
- Préalables pour les ports de commutation, à la page 2
- Lignes directrices relatives aux ports de commutation, à la page 3
- Configuration des ports de commutation et l'alimentation par Ethernet (PoE), à la page 4
- Supervision des ports de commutation, à la page 9
- Historique des ports de commutation, à la page 10

À propos des ports de commutation

Cette section décrit les ports de commutation pour les modèles avec commutateurs de couche 2.

Comprendre les ports et les interfaces de commutation

Ports et interfaces

Pour chaque interface physique, vous pouvez définir son fonctionnement comme interface de pare-feu ou comme port de commutation. Consultez les renseignements suivants sur les interfaces physiques et les types de port, ainsi que sur les interfaces VLAN logiques auxquelles vous affectez des ports de commutation :

- Interface de pare-feu physique : En mode routé, ces interfaces transmettent le trafic entre les réseaux de la couche 3 en utilisant la politique de sécurité configurée pour appliquer les services de pare-feu et VPN. En mode transparent, ces interfaces sont des membres de groupes de ponts qui acheminent le trafic entre les interfaces du même réseau au niveau de la couche 2, en utilisant la politique de sécurité configurée pour appliquer les services de pare-feu. En mode routé, vous pouvez également utiliser le routage et le pont intégrés avec certaines interfaces comme membres du groupe de ponts et d'autres comme interfaces de couche 3. Par défaut, l'interface Ethernet 1/1 est configurée comme interface de pare-feu.

- Port de commutation physique : les ports de commutation transfèrent le trafic à la couche 2 en utilisant la fonction de commutation dans le matériel. Les ports de commutation sur le même VLAN peuvent communiquer entre eux grâce à la commutation matérielle, et le trafic n'est pas soumis à la politique de sécurité ASA. Les ports d'accès acceptent uniquement le trafic non balisé et vous pouvez les affecter à un seul VLAN. Les ports de ligne principale acceptent le trafic non balisé et peuvent appartenir à plus d'un VLAN. Par défaut, Ethernet 1/2 et supérieur sont configurés comme ports de commutation d'accès sur le VLAN 1. Vous ne pouvez pas configurer l'interface Management (gestion) comme port de commutation.
- Logical VLAN interface (interface VLAN logique) : Ces interfaces fonctionnent de la même façon que les interfaces de pare-feu physiques, à la différence que vous ne pouvez pas créer des sous-interfaces, des , des ou des interfaces EtherChannel. Lorsqu'un port de commutation doit communiquer avec un autre réseau, le périphérique ASA applique la politique de sécurité à l'interface VLAN et achemine le routage vers une autre interface VLAN logique ou une interface de pare-feu. Vous pouvez même utiliser le routage et le pont intégrés avec des interfaces VLAN comme membres du groupe de ponts. Le trafic entre les ports de commutation sur le même VLAN n'est pas soumis à la politique de sécurité, mais le trafic entre les VLAN d'un groupe de ponts est soumis à la politique de sécurité ASA. Vous pouvez donc choisir de superposer les groupes de ponts et les ports de commutation pour appliquer la politique de sécurité entre certains segments.

Alimentation par Ethernet

La PoE est disponible sur Ethernet 1/7 et Ethernet 1/8 en utilisant les protocoles IEEE 802.3af (PoE) et 802.3at (PoE+), jusqu'à 30 W par port.

PoE+ utilise le protocole LLDP (Link Layer Discovery Protocol) pour négocier le niveau de puissance. L'alimentation n'est fournie qu'en cas de besoin.

Si vous désactivez l'interface, vous désactivez l'alimentation du périphérique.

Fonctionnalité Auto-MDI/MDIX

Pour tous les ports de commutation, le paramètre de négociation automatique par défaut inclut également la fonction Auto-MDI/MDIX. La fonction Auto-MDI/MDIX élimine le besoin de câblage croisé en effectuant un croisé interne lorsqu'un câble droit est détecté pendant la phase de négociation automatique. La vitesse ou le duplex doivent être réglés pour qu'ils soient négociés automatiquement afin d'activer Auto-MDI/MDIX pour l'interface. Si vous définissez explicitement la vitesse et le duplex à une valeur fixe, désactivant ainsi la négociation automatique pour les deux paramètres, Auto-MDI/MDIX est également désactivé. Lorsque la vitesse et le mode duplex sont définis à 1000 et que la vitesse maximale est atteinte, l'interface négocie toujours automatiquement; par conséquent, Auto-MDI/MDIX est toujours activé et vous ne pouvez pas le désactiver.

Préalables pour les ports de commutation

Prise en charge des modèles

- Firepower 1010

Lignes directrices relatives aux ports de commutation

Mode contextuel

- Firepower 1010 ne prend pas en charge le mode contexte multiple.
- Le Secure Firewall 1210/1220 ne prend pas en charge le mode de contexte multiple.

Basculement et mise en grappe

- Aucune prise en charge de grappe.
- Prise en charge du basculement actif/veille uniquement.
- Vous ne devez pas utiliser la fonctionnalité de port de commutateur lors de l'utilisation de Basculement. Étant donné que les ports de commutation fonctionnent dans le matériel, ils continuent de faire circuler le trafic sur les unités actives *et* en veille. Basculement est conçu pour empêcher le trafic de passer par l'unité en veille, mais cette fonctionnalité ne s'étend pas aux ports de commutation. Dans une configuration réseau Basculement normale, les ports de commutateur actifs sur les deux unités mèneront à des boucles réseau. Nous vous suggérons d'utiliser des commutateurs externes pour toute capacité de commutation. Notez que les interfaces VLAN peuvent être surveillées par basculement, contrairement aux ports de commutation. Théoriquement, vous pouvez mettre un port de commutation unique sur un réseau VLAN et utiliser Basculement avec succès, mais une configuration plus simple consiste à utiliser des interfaces physiques de pare-feu à la place.
- Vous ne pouvez utiliser qu'une interface de pare-feu comme liaison de basculement.

Interfaces logiques VLAN (SVI)

- Si vous utilisez également des sous-interfaces VLAN sur une interface de pare-feu, vous ne pouvez pas utiliser le même ID VLAN que pour une interface VLAN logique.
- Adresses MAC
  - Mode de pare-feu routé : toutes les interfaces VLAN partagent une adresse MAC. Assurez-vous que tous les commutateurs connectés peuvent prendre en charge ce scénario. Si les commutateurs connectés nécessitent des adresses MAC uniques, vous pouvez attribuer manuellement des adresses MAC. Consultez Configurer l'adresse MAC manuelle, la MTU et le TCP MSS
  - Mode pare-feu transparent : chaque interface VLAN a une adresse MAC unique. Vous pouvez remplacer les adresses MAC générées si vous le souhaitez en attribuant manuellement des adresses MAC. Consultez Configurer l'adresse MAC manuelle, la MTU et le TCP MSS.

Groupes de ponts

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

Fonctionnalités non prises en charge de l'interface VLAN et du port de commutation

Les interfaces VLAN et les ports de commutation ne prennent pas en charge :

- Routage dynamique
- Routage multidiffusion
- Routage basé sur les politiques
- Routage multiples chemins à coûts égaux (ECMP)
- VXLAN
- EtherChannels : les ports de commutation ne peuvent pas faire partie d'un EtherChannel. Le PoE n'est pas non plus pris en charge sur un port d'un EtherChannel.
- Basculement et lien d'état
- Zones de circulation
- Balise du groupe de sécurité (SGT)

Autres directives et limites

- Vous pouvez configurer un maximum de 60 interfaces nommées.
- Vous ne pouvez pas configurer l'interface Management (gestion) comme port de commutation.

Paramètres d'usine

- Ethernet 1/1 est une interface de pare-feu.
- Ethernet 1/2 à Ethernet 1/8 sont des ports de commutation affectés au VLAN 1.
- Vitesse et duplex par défaut: par défaut, la vitesse et le duplex sont configurés pour la négociation automatique.

Configuration des ports de commutation et l'alimentation par Ethernet (PoE)

Pour configurer les ports de commutation et la PoE, procédez comme suit :

Configurer une interface VLAN

Cette section décrit comment configurer les interfaces VLAN (SVI) à utiliser avec les ports de commutation associés. Vous pouvez créer jusqu'à 60 interfaces VLAN associées aux ports de commutation.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres de l'interface)** > **Interfaces** et choisissez **Add (Ajouter)** > **VLAN Interface (Interface VLAN)**.

Étape 2 Dans le champ **VLAN ID** (ID de VLAN), saisissez l'ID de VLAN pour cette interface, entre 1 et 4070, en excluant les ID de 3968 à 4047, qui sont réservés à un usage interne.

Étape 3 (Facultatif) Dans la liste déroulante **Block Traffic From this Interface to** (Bloquer le trafic de cette interface à), choisissez le VLAN vers lequel cette interface VLAN ne peut pas initier le trafic.

Par exemple, vous avez un VLAN affecté à l'extérieur pour l'accès Internet, un VLAN affecté à un réseau interne d'entreprise et un troisième VLAN affecté à votre réseau domestique. Le réseau domestique n'a pas besoin d'accéder au réseau de l'entreprise, vous pouvez donc utiliser l'option **Block Traffic From this Interface to** (Bloquer le trafic de cette interface à) sur le VLAN domestique; le réseau professionnel peut accéder au réseau domestique, mais le réseau domestique ne peut pas accéder au réseau d'entreprise.

Étape 4 Cliquez sur **OK**.

Étape 5 Cliquez sur **Apply** (Appliquer).

Configuration des ports de commutation comme ports d'accès

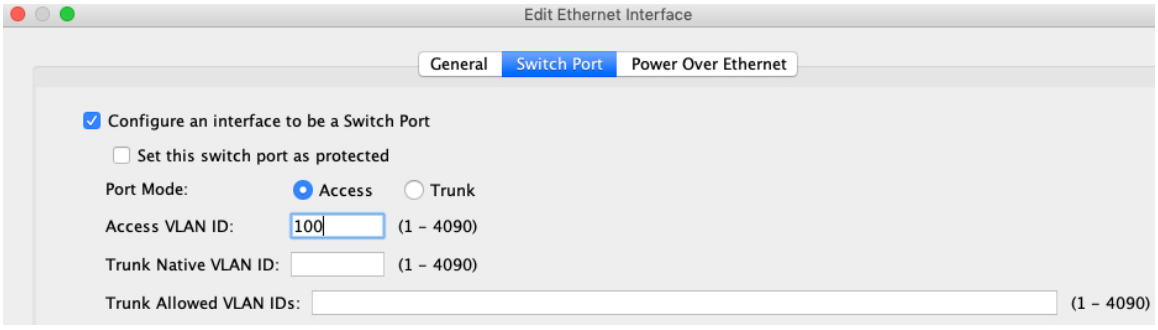
Pour affecter un port de commutation à un seul VLAN, configurez-le comme port d'accès. Les ports d'accès acceptent uniquement le trafic non balisé. Par défaut, Ethernet 1/2 à Ethernet 1/8 sont des ports de commutation affectés au VLAN 1.

Remarque L'appareil ne prend pas en charge le protocole Spanning Tree pour la détection de boucle dans le réseau. Par conséquent, vous devez vous assurer qu'une connexion avec l'ASA ne finit pas dans une boucle de réseau.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**, sélectionnez l'interface que vous souhaitez modifier et cliquez sur **Edit** (Modifier).

Étape 2 Cliquez sur **Switch Port** (Port de commutation).



Étape 3 Cochez la case **Configure an interface to be a Switch Port** (Configurer une interface pour qu'elle soit un port de commutation).

Étape 4 (Facultatif) Cochez la case **Set this switch port as protected** (Définir ce port de commutation comme protégé) pour définir ce port de commutation comme protégé, afin de pouvoir l'empêcher de communiquer avec d'autres ports de commutation protégés sur le même VLAN.

Vous pourriez souhaiter empêcher les ports de commutation de communiquer entre eux dans les cas suivants : les périphériques sur ces ports de commutation sont principalement accessibles à partir d'autres VLAN; vous n'avez pas besoin d'autoriser l'accès intra-VLAN; et vous souhaitez isoler les périphériques les uns des autres en cas d'infection ou de toute autre faille de sécurité. Par exemple, si vous avez une DMZ qui héberge trois serveurs Web, vous pouvez isoler les serveurs Web les uns des autres en appliquant l'option **Set this switch port as protected** (Définir ce port de commutation comme protégé) à chaque port de commutation. Les réseaux interne et externe peuvent tous deux communiquer avec les trois serveurs Web, et inversement, mais les serveurs Web ne peuvent pas communiquer entre eux.

Étape 5 Pour le **Port Mode** (Mode de port), cliquez sur le bouton radio **Access** (Accès).

Étape 6 Saisissez l'**Access VLAN ID** (ID de VLAN d'accès) associé à ce port de commutation, entre 1 et 4070.

La valeur par défaut est VLAN 1.

Étape 7 Cliquez sur **General** (Général).

Étape 8 Cochez **Enable Interface** (Activer l'interface).

Remarque Les autres champs de la page **General** (Général), comme **Interface Name** (Nom de l'interface), ne s'appliquent pas aux ports de commutation.

Étape 9 (Facultatif) Définissez les propriétés matérielles.

a) Cliquez sur **Configure Hardware Properties** (Configurer les propriétés matérielles).

b) Choisissez le mode **Duplex**.

La valeur par défaut est **Auto**.

c) Renseignez le champ **Speed** (Vitesse).

La valeur par défaut est **Auto**.

d) Cliquez sur **OK**.

Étape 10 Cliquez sur **OK**.

Étape 11 Cliquez sur **Apply** (Appliquer).

Configuration des ports de commutation comme ports de ligne principale

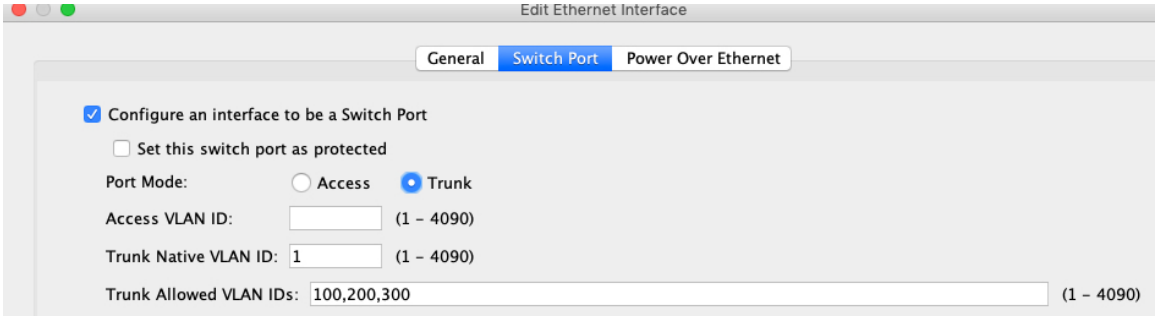
Cette procédure décrit comment créer un port de liaison qui peut acheminer plusieurs VLAN à l'aide du balisage 802.1Q. Les ports de ligne principale acceptent le trafic non balisé et balisé. Le trafic sur les VLAN autorisés passe par le port de liaison sans changement.

Lorsque la ligne principale reçoit un trafic non balisé, elle le balise à l'ID de VLAN natif afin que l'ASA puisse transférer le trafic vers les ports de commutation appropriés ou l'acheminer vers une autre interface de pare-feu. Lorsque l'ASA envoie le trafic d'ID de VLAN natif hors du port de liaison, il supprime la balise VLAN. Assurez-vous de définir le même VLAN natif sur le port de liaison de l'autre commutateur afin que le trafic non balisé soit balisé vers le même VLAN.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**, sélectionnez l'interface que vous souhaitez modifier et cliquez sur **Edit** (Modifier).

Étape 2 Cliquez sur **Switch Port** (Port de commutation).



Étape 3 Cochez la case **Configure an interface to be a Switch Port** (Configurer une interface pour qu'elle soit un port de commutation).

Étape 4 (Facultatif) Cochez la case **Set this switch port as protected** (Définir ce port de commutation comme protégé) pour définir ce port de commutation comme protégé, afin de pouvoir l'empêcher de communiquer avec d'autres ports de commutation protégés sur le même VLAN.

Vous pourriez souhaiter empêcher les ports de commutation de communiquer entre eux dans les cas suivants : les périphériques sur ces ports de commutation sont principalement accessibles à partir d'autres VLAN; vous n'avez pas besoin d'autoriser l'accès intra-VLAN; et vous souhaitez isoler les périphériques les uns des autres en cas d'infection ou de toute autre faille de sécurité. Par exemple, si vous avez une DMZ qui héberge trois serveurs Web, vous pouvez isoler les serveurs Web les uns des autres en appliquant l'option **Set this switch port as protected** (Définir ce port de commutation comme protégé) à chaque port de commutation. Les réseaux interne et externe peuvent tous deux communiquer avec les trois serveurs Web, et inversement, mais les serveurs Web ne peuvent pas communiquer entre eux.

Étape 5 Pour le **Port Mode** (Mode de port), cliquez sur le bouton radio **Trunk** (Liaison).

Étape 6 Saisissez le **Trunk Native VLAN ID** (ID de VLAN natif de la liaison), compris entre 1 et 4070. La valeur par défaut est VLAN 1.

Chaque port ne peut avoir qu'un seul VLAN natif, mais chaque port peut avoir le même VLAN natif ou un différent.

Étape 7 Saisissez les **Trunk Allowed VLAN IDs** (ID de VLAN autorisés pour la liaison) associés à ce port de commutation, séparés par des virgules, entre 1 et 4070.

Si vous incluez le VLAN natif dans ce champ, il est ignoré; Le port de liaison supprime toujours le balisage VLAN lors de l'envoi de trafic VLAN natif hors du port. De plus, il ne recevra pas le trafic qui a toujours un balisage VLAN natif.

Étape 8 Cliquez sur **General** (Général).

Étape 9 Cochez **Enable Interface** (Activer l'interface).

Remarque Les autres champs de la page **General** (Général), comme **Interface Name** (Nom de l'interface), ne s'appliquent pas aux ports de commutation.

Étape 10 (Facultatif) Définissez les propriétés matérielles.

a) Cliquez sur **Configure Hardware Properties** (Configurer les propriétés matérielles).

b) Choisissez le mode **Duplex**.

La valeur par défaut est **Auto**.

c) Renseignez le champ **Speed** (Vitesse).

La valeur par défaut est **Auto**.

d) Cliquez sur **OK**.

Étape 11 Cliquez sur **OK**.

Étape 12 Cliquez sur **Apply** (Appliquer).

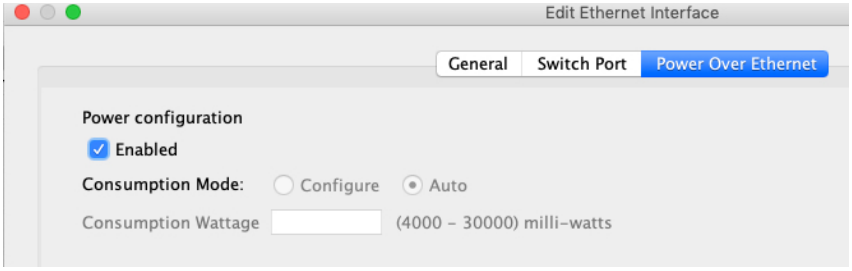
Configurer Power Over Ethernet (alimentation électrique par câble Ethernet)

Les ports Power over Ethernet (PoE) alimentent les périphériques tels que les téléphones IP ou les points d'accès sans fil. Le mode PoE est activé par défaut. Cette procédure décrit comment activer et désactiver la PoE et comment définir les paramètres facultatifs.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**, sélectionnez l'interface que vous souhaitez modifier et cliquez sur **Edit** (Modifier).

Étape 2 Cliquez sur **Power Over Ethernet** (Alimentation par Ethernet).



Étape 3 Cochez la case **Activé**.

Étape 4 Cliquez sur le bouton radio **Consumption Mode** (Mode de consommation) : **Configure** (Configurer) ou **Auto**.

- **Auto** : fournit automatiquement du courant au périphérique alimenté en utilisant une puissance appropriée pour la classe du périphérique alimenté. Le pare-feu utilise LLDP pour négocier davantage la puissance en watts.

- **Configure** (Configurer) : spécifie manuellement la puissance en milliwatts dans le champ **Consumption Wattage** (Consommation en watts), de 4 000 à 30 000. Utilisez cette option si vous souhaitez définir les watts manuellement et désactiver la négociation LLDP.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Apply** (Appliquer).

Étape 7 Choisissez **Monitor (Superviser)** > **Interfaces** > **Power Over Ethernet (Alimentation par Ethernet)** pour afficher l'état PoE actuel.

Supervision des ports de commutation

- **Monitoring (Supervision)** > **Interfaces** > **ARP Table (Tableau ARP)**

  Affiche le tableau ARP, y compris les entrées statiques et dynamiques. Le tableau ARP comprend des entrées qui mappent une adresse MAC à une adresse IP pour une interface donnée.

- **Monitoring (Supervision)** > **Interfaces** > **MAC Address Table (Tableau d'adresses MAC)**

  Affiche les entrées d'adresse MAC statiques et dynamiques.

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

  Affiche les statistiques d'interface sous forme de graphique ou de tableau.

- **Monitoring (Supervision)** > **Interfaces** > **L2 Switching (Commutation L2)**

  Affiche l'association du port VLAN au commutateur et les entrées d'adresses MAC statiques et dynamiques.

- **Monitoring (Supervision)** > **Interfaces** > **Power Over Ethernet (Alimentation par Ethernet)**

  Affiche l'état PoE+.

Historique des ports de commutation

Tableau 1 : Historique des ports de commutation

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Prise en charge du commutateur matériel Firepower 1010	9.13(1)	L'appareil Firepower 1010 prend en charge la définition de chaque interface Ethernet comme port de commutation ou interface de pare-feu. Écrans Nouveaux ou modifiés : • **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Edit (Modifier)** > **Switch Port (Port de commutation)** • **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Add VLAN Interface (Ajouter une interface VLAN)** • **Monitoring (Supervision)** > **Interfaces** > **L2 Switching (Commutation L2)**
Prise en charge du Firepower 1010 PoE+ sur Ethernet 1/7 et Ethernet 1/8	9.13(1)	Le Firepower 1010 prend en charge Power over Ethernet+ (PoE+) sur Ethernet 1/7 et Ethernet 1/8. Écrans Nouveaux ou modifiés : • **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Edit (Modifier)** > **Power Over Ethernet (Alimentation par Ethernet)** • **Monitoring (Supervision)** > **Interfaces** > **Power Over Ethernet (Alimentation par Ethernet)**

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.