Sous-interfaces VLAN

Ce chapitre explique comment configurer les sous-interfaces VLAN.

Remarque Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.

À propos des sous-interfaces VLAN

Les sous-interfaces VLAN vous permettent de diviser une interface physiqueou EtherChannel en plusieurs interfaces logiques qui sont étiquetées avec différents ID de VLAN. Une interface avec une ou plusieurs sous-interfaces VLAN est automatiquement configurée comme une ligne principale 802.1Q. Comme les réseaux VLAN vous permettent de garder le trafic séparé sur une interface physique donnée, vous pouvez augmenter le nombre d'interfaces disponibles pour votre réseau sans ajouter d'interfaces physiques ou d'ASA supplémentaires. Cette fonctionnalité est particulièrement utile en mode de contexte multiple, car vous pouvez affecter des interfaces uniques à chaque contexte.

Vous pouvez configurer un VLAN principal ainsi qu'un ou plusieurs VLAN secondaires. Lorsque l'ASA reçoit le trafic sur les VLAN secondaires, il le mappe au VLAN principal.

Licences pour les sous-interfaces VLAN

Modèle	Exigence de licence
Firepower 1010	Licence Essentials : 60

Modèle	Exigence de licence
Firepower 1120	Licence Essentials : 512
Firepower 1140, 1150	Licence Essentials : 1 024
Firepower de la série 2100	Licence Essentials : 1 024
Secure Firewall 3100	Licence Essentials : 1 024
Firepower 4100	Licence Essentials : 1 024
Firepower 9300	Licence Essentials : 1 024
ASA virtuel	Capacité de débit : 100 Mbit/s : 25 1 Gbit/s : 50 2 Gbit/s : 200 10 Gbit/s : 1 024
ISA 3000	LicenceEssentials : 5 Licence Security Plus : 100

Remarque Pour qu'une interface soit prise en compte dans la limite de VLAN, vous devez lui attribuer un VLAN.Par exemple :

```
interface gigabitethernet 0/0.100
  vlan 100
```

Lignes directrices et limites pour les sous-interfaces VLAN

Prise en charge des modèles

- Firepower 1010 : les sous-interfaces VLAN ne sont pas prises en charge sur les ports de commutation ou les interfaces VLAN.
- Pour la des modèles ASA, vous ne pouvez pas configurer de sous-interface sur l'interface de gestion. Consultez L'interface de logement/port de gestion pour la prise en charge des sous-interfaces.

Directives supplémentaires

- Prévention des paquets non balisés sur l'interface physique : Si vous utilisez des sous-interfaces, vous ne souhaitez généralement pas que l'interface physique achemine le trafic, car l'interface physique peut transmettre des paquets non balisés. Cette propriété est également vraie pour l'interface physique active

pour les liaisons EtherChannel. Étant donné que l'interface physique ou EtherChannel doit être activée pour que la sous-interface achemine le trafic, assurez-vous que l'interface physique ou EtherChannel ne transmet pas le trafic en omettant la commande **nameif**. Si vous voulez laisser l'interface physique ou EtherChannel passer des paquets non balisés, vous pouvez configurer la commande **nameif** comme d'habitude.

- Toutes les sous-interfaces de la même interface parente doivent soit être des membres de groupes de ponts, soit des interfaces routées; vous ne pouvez pas combiner les deux types.
- L'ASA ne prend pas en charge le protocole DTP (Dynamic Trunking Protocol), vous devez donc configurer le port de commutation connectée pour qu'il assure la liaison sans condition.
- Vous pourriez souhaiter affecter des adresses MAC uniques aux sous-interfaces définies sur l'ASA, car elles utilisent la même adresse MAC gravée de l'interface parente. Par exemple, votre fournisseur de services peut effectuer un contrôle d'accès en fonction de l'adresse MAC. 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 ASA. Vous pouvez générer automatiquement des adresses MAC uniques; voir Attribuer automatiquement des adresses MAC.

Remarque Si vous attribuez manuellement une adresse MAC, veillez à attribuer des adresses MAC à toutes les sous-interfaces sur la même interface physique pour éviter les comportements imprévus et les pannes.

Paramètres par défaut pour les sous-interfaces VLAN

Cette section répertorie les paramètres par défaut des interfaces si vous n'avez pas de configuration d'usine par défaut.

État par défaut des interfaces

L'état par défaut d'une interface dépend du type d'interface et du mode de contexte.

En mode de contexte multiple, toutes les interfaces allouées sont activées par défaut, quel que soit l'état de l'interface dans l'espace d'exécution du système. Cependant, pour que le trafic passe par l'interface, celle-ci doit également être activée dans l'espace d'exécution du système. Si vous désactivez une interface dans l'espace d'exécution du système, cette interface est désactivée dans tous les contextes qui la partagent.

En mode unique ou dans l'espace d'exécution du système, les interfaces ont les états par défaut suivants :

- Interfaces physiques : désactivées.
- Sous-interfaces VLAN : activées. Cependant, pour que le trafic passe par la sous-interface, l'interface physique doit également être activée.

Configurer les sous-interfaces VLAN et la jonction 802.1Q

Ajoutez une sous-interface VLAN à une interface physique ou EtherChannel.

Avant de commencer

Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.

Procédure

Étape 1 Spécifiez la nouvelle sous-interface :

interface {*physical_interface* | **port-channel** *number*}.*subinterface*

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/1.100
```

L'argument **port-channel** *number* est l'ID de l'interface EtherChannel, tel que **port-channel 1**.

L'ID de la *sous-interface* est un nombre entier compris entre 1 et 4294967293.

Étape 2 Spécifiez le VLAN de la sous-interface :

vlan *vlan_id* [**secondary** *vlan_range*]

Exemple :

```
ciscoasa(config-subif)# vlan 101 secondary 52 64,66-74
```

Le *vlan_id* est un entier compris entre 1 et 4094. Certains numéros de VLAN peuvent être réservés sur les commutateurs connectés. Consultez la documentation du commutateur pour en savoir plus.

Les réseaux VLAN secondaires peuvent être séparés par des espaces, des virgules et des tirets (pour une plage contiguë). Lorsque l'ASA reçoit le trafic sur les VLAN secondaires, il mappe le trafic au VLAN principal.

Vous ne pouvez pas attribuer le même réseau VLAN à plusieurs sous-interfaces. Vous ne pouvez pas attribuer de réseau VLAN à l'interface physique. Chaque sous-interface doit avoir un ID VLAN avant de pouvoir transmettre du trafic. Pour modifier un ID VLAN, vous n'avez pas besoin de supprimer l'ancien ID VLAN avec l'option **no** (non); vous pouvez saisir la commande **vlan** avec un autre ID VLAN et l'ASA modifie l'ancien ID. Pour supprimer certains VLAN secondaires de la liste, vous pouvez utiliser la commande **no** (non) et répertorier uniquement les VLAN à supprimer. Vous pouvez uniquement supprimer de manière sélective les VLAN répertoriés; vous ne pouvez pas supprimer un seul VLAN dans une plage, par exemple.

Exemples

L'exemple suivant mappe un ensemble de VLAN secondaires au VLAN 200 :

```
interface gigabitethernet 0/6.200
   vlan 200 secondary 500 503 600-700
```

Dans l'exemple suivant, le VLAN 503 secondaire est supprimé de la liste :

```
no vlan 200 secondary 503
```

```
show running-config interface gigabitethernet0/6.200
!
interface GigabitEthernet0/6.200
 vlan 200 secondary 500 600-700
 no nameif
 no security-level
 no ip address
```

Sujets connexes

Licences pour les sous-interfaces VLAN, à la page 1

Supervision des sous-interfaces VLAN

Consultez les commandes suivantes :

- **show interface**

  Affiche des statistiques sur l'interface.

- **show interface ip brief**

  Affiche les adresses IP et l'état de l'interface.

- **show vlan mapping**

  Affiche l'interface, les VLAN secondaires et les VLAN principaux auxquels ils sont mappés.

Exemples de sous-interfaces VLAN

L'exemple suivant configure les paramètres d'une sous-interface en mode unique :

```
interface gigabitethernet 0/1
  no nameif
  no security-level
  no ip address
  no shutdown
interface gigabitethernet 0/1.1
  vlan 101
  nameif inside
  security-level 100
  ip address 192.168.6.6 255.255.255.0
  no shutdown
```

L'exemple suivant montre comment le mappage de VLAN fonctionne avec le commutateur Catalyst 6500. Consultez le guide de configuration du commutateur Catalyst 6500 pour savoir comment connecter des nœuds à des PVLAN.

ASA Configuration

```
interface GigabitEthernet1/1
  description Connected to Switch GigabitEthernet1/5
  no nameif
  no security-level
  no ip address
```

```
  no shutdown
!
interface GigabitEthernet1/1.70
  vlan 70 secondary 71 72
  nameif vlan_map1
  security-level 50
  ip address 10.11.1.2 255.255.255.0
  no shutdown
!
interface GigabitEthernet1/2
  nameif outside
  security-level 0
  ip address 172.16.171.31 255.255.255.0
  no shutdown
```

Catalyst 6500 Configuration

```
vlan 70
  private-vlan primary
  private-vlan association 71-72
!
vlan 71
  private-vlan community
!
vlan 72
  private-vlan isolated
!
interface GigabitEthernet1/5
  description Connected to ASA GigabitEthernet1/1
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 70-72
  switchport mode trunk
!
```

Historique des sous-interfaces VLAN

Tableau 1 : Historique des sous-interfaces VLAN

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Augmentation du nombre de VLAN	7.0(5)	Augmentation des limites suivantes : • VLAN de licences de base ASA 5510 de 0 à 10. • VLAN de licences Security Plus ASA 5510, 10 à 25. • VLAN ASA 5520 de 25 à 100. • VLAN ASA 5540 de 100 à 200.
Augmentation du nombre de VLAN	7.2(2)	Les limites de VLAN ont été augmentées pour l'ASA 5510 (de 10 à 50 pour la licence de base et de 25 à 100 pour la licence Security Plus), l'ASA 5520 (de 100 à 150), l'ASA 5550 (de 200 à 250).
Augmentation du nombre de VLAN pour l'ASA 5580	8.1(2)	Le nombre de VLAN pris en charge sur l'ASA 5580 est passé de 100 à 250.

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Prise en charge du mappage d'un VLAN secondaire à un VLAN principal	9.5(2)	Vous pouvez maintenant configurer un ou plusieurs VLAN secondaires pour une sous-interface. Lorsque l'ASA reçoit le trafic sur les VLAN secondaires, il le mappe au VLAN principal. Nous avons introduit ou modifié les commandes suivantes : **vlan secondary, show vlan mapping**
Augmentation du nombre de VLAN pour l'ISA 3000	9.13(1)	Le nombre maximum de VLAN pour l'ISA 3000 avec la licence Security Plus est passé de 25 à 100.

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.