Utilisation de réseaux locaux virtuels à l'aide d'équipement sans fil Aironet Cisco

Table des matières

[Introduction](#)
[Conditions préalables](#)
[Exigences](#)
[Composants utilisés](#)
[Produits connexes](#)
[Conventions](#)
[Réseaux locaux virtuels (VLAN)](#)
[Importance du réseau local virtuel natif](#)
[VLAN sur des points d'accès](#)
[Concepts liés aux points d'accès](#)
[Configuration de point d'accès](#)
[VLAN sur des ponts](#)
[Concepts liés aux ponts](#)
[Configuration du pont](#)
[Utilisez un serveur RADIUS pour affecter des utilisateurs aux VLAN](#)
[Utilisation d'un serveur RADIUS pour l'affectation dynamique de groupe de mobilité](#)
[Configuration de groupe de pontage sur des points d'accès et des ponts](#)
[Integrated Routing and Bridging (IRB)](#)
[Interaction avec les commutateurs relatifs](#)
[Configuration du commutateur — Catalyst OS](#)
[Configuration du commutateur - Commutateurs Catalyst basés sur l'IOS](#)
[Configuration du commutateur — Catalyst 2900XL/3500XL](#)
[Vérifier](#)
[Vérification de l'équipement sans fil](#)
[Vérification du commutateur](#)
[Dépannage](#)
[Informations connexes](#)

Introduction

Ce document fournit un exemple de configuration pour utiliser des LAN virtuels (VLAN) avec l'équipement sans fil de Cisco Aironet.

Conditions préalables

Exigences

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Familiarité avec l'équipement sans fil de Cisco Aironet
- Familiarité avec des concepts de commutation LAN des VLAN et de jonction du VLAN

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Points d'accès Cisco Aironet et ponts sans fil
- Commutateurs Cisco Catalyst

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Produits connexes

Vous pouvez utiliser le côté commutateur de cette configuration avec l'un de ces matériels ou logiciels :

- Catalyst 6x00/5x00/4x00 qui exécute CatOS ou IOS
- Catalyst 35x0/37x0/29xx qui exécute IOS
- Catalyst 2900XL/3500XL qui exécute IOS

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Réseaux locaux virtuels (VLAN)

UN VLAN est un réseau commuté qui est logiquement segmenté par des fonctions, des équipes de projet ou des applications plutôt que sur une base physique ou géographique. Par exemple, tous les serveurs et toutes les stations de travail utilisé(e)s par une équipe particulière de groupe de travail peuvent être connecté(e)s au même VLAN, indépendamment de leurs connexions physiques au réseau ou du fait qu'ils/elles peuvent être mélangé(e)s avec d'autres équipes. Employez les VLAN pour reconfigurer le réseau à travers le logiciel plutôt que de débrancher ou déplacer physiquement les périphériques ou les fils.

Un VLAN peut être vu comme un domaine de diffusion existant dans un ensemble défini de commutateurs. Un VLAN se compose d'un certain nombre de systèmes d'extrémité, hôtes ou d'équipement réseau (tel que des ponts et des routeurs), connectés par un seul domaine de

pontage. Le domaine de pontage est pris en charge sur différentes pièces d'équipement réseau, telles que les commutateurs LAN, qui actionnent des protocoles de pontage entre eux avec un groupe distinct pour chaque VLAN.

Lorsque vous connectez un périphérique à un commutateur Cisco Catalyst, le port auquel le périphérique est connecté est membre du VLAN 1. L'adresse MAC de ce périphérique fait partie du VLAN 1. Vous pouvez définir plusieurs VLAN sur un seul commutateur et configurer un port de commutateur sur la plupart des modèles Catalyst comme membre de plusieurs VLAN.

Quand le nombre de ports dans un réseau dépasse la capacité portuaire du commutateur, vous devez effectuer une connexion transversale interne de plusieurs châssis de commutateurs, qui définit une agrégation. L'agrégation n'est pas un membre de VLAN, mais un conduit sur lequel passe le trafic pour un ou plusieurs VLAN.

Fondamentalement, le point essentiel de la configuration d'un point d'accès devant être connecté à un VLAN spécifique est de configurer son SSID de manière à ce qu'il identifie ce VLAN. Comme les VLAN sont identifiés par un ID VLAN ou un nom, si le SSID sur un point d'accès est configuré pour identifier un ID VLAN ou un nom spécifique, une connexion au VLAN est établie. Quand ce rapport est établi, les périphériques client sans fil associés qui ont le même SSID peuvent accéder le VLAN par le point d'accès. Le VLAN traite des données vers et depuis des clients de la même façon qu'il traite des données vers et depuis des connexions câblées. Vous pouvez configurer jusqu'à 16 SSID sur votre point d'accès, et pouvez donc prendre en charge jusqu'à 16 VLAN. Vous pouvez attribuer seulement un SSID à un VLAN.

Vous prolongez des VLAN dans un LAN sans fil quand vous ajoutez la conscience de tag IEEE 802.11Q au point d'accès. Des trames destinées à différents VLAN sont transmises par le point d'accès sans fil sur différents SSID avec différentes clés WEP. Seuls les clients liés à ce VLAN reçoivent ces paquets. Par contre, les paquets provenant d'un client lié à un certain VLAN sont marqués 802.11Q avant d'être transférés sur le réseau câblé.

Par exemple, les employés et les invités peuvent accéder le réseau sans fil d'une société en même temps et être administrativement distincts. Un VLAN est mappé à un SSID et le client sans fil est attaché au SSID approprié. Dans les réseaux avec des ponts sans fil, vous pouvez passer plusieurs VLAN à travers la liaison sans fil afin de fournir la connectivité à un VLAN depuis des emplacements distincts.

Si le 802.1q est configuré sur l'interface FastEthernet d'un point d'accès, le point d'accès envoie toujours des keepalives sur VLAN1 même si le VLAN 1 n'est pas défini sur le point d'accès. En conséquence, le commutateur Ethernet se connecte au point d'accès et génère un message d'avertissement. Il n'y a aucune perte de fonction sur le point d'accès ou le commutateur, mais le journal de commutateur contient des messages sans signification à cause desquels des messages plus importants risquent d'être enveloppés et non consultés.

Ce comportement crée un problème quand tous les SSID d'un point d'accès sont associés aux réseaux de mobilité. Si tous les SSID sont associés aux réseaux de mobilité, le port du commutateur Ethernet auquel le point d'accès est connecté peut être configuré comme port d'accès. Le port d’accès est normalement attribué au VLAN natif du point d’accès, qui n’est pas nécessairement VLAN1. Cela entraîne la génération de messages d’avertissement par le

commutateur Ethernet, indiquant que le trafic avec une étiquette 802.1q est envoyé à partir du point d’accès.

Vous pouvez éliminer les messages excessifs sur le commutateur en désactivant la fonction de keepalive.

Si vous ignorez les points mineurs dans ces concepts quand vous déployez des VLAN avec l'équipement sans fil de Cisco Aironet, vous pouvez constater des performances inattendues, par exemple :

- L'impossibilité de limiter les VLAN autorisés sur l'agrégation à ceux définis sur le périphérique sans fil

  Si les VLAN 1, 10, 20, 30 et 40 sont définis sur le commutateur, mais que seuls les VLAN 1, 10 et 30 sont définis sur l'équipement sans fil, vous devez supprimer les autres du port de commutateur d'agrégation.

- Utilisation abusive de la désignation du SSID d'infrastructure

  Quand vous installez des Points d'accès, assignez seulement le SSID d'infrastructure quand vous utilisez un SSID sur :

  - des périphériques de pont de groupe de travail
  - des points d'accès de répéteur
  - des ponts non-racines

  Cela constitue une erreur d'indiquer le SSID d'infrastructure pour un SSID uniquement avec des ordinateurs portables sans fil pour des clients, et cela entraîne des résultats imprévisibles.

  Dans les installations de pont, vous pouvez seulement avoir un SSID d'infrastructure. Le SSID d'infrastructure doit être le SSID qui effectue des corrélations au réseau local virtuel natif.

- Utilisation abusive ou conception incorrecte de la désignation de SSID de mode d'invité

  Quand vous définissez des SSID/VLAN multiples sur l'équipement sans fil de Cisco Aironet, un (1) SSID peut être attribué en tant que SSID de mode d'invité avec le SSID diffusé dans des radiobalises de 802.11. Les autres SSID ne sont pas diffusés. Les périphériques clients doivent indiquer quel SSID connecter.

- Si les VLAN et SSID multiples ne sont pas reconnus, cela indique qu'il y a des sous-réseaux multiples de la couche du modèle OSI 3

  Les versions obsolètes du logiciel Cisco Aironet permettent de lier des SSID multiples à un VLAN. Les versions actuelles ne le permettent pas.

- Pannes de d'acheminement de la couche du modèle OSI 3 ou conceptions incorrectes

Chaque SSID et son VLAN joint doivent avoir un périphérique de routage et une certaine source pour s'adresser à des clients, par exemple un serveur DHCP ou la portée sur un serveur DHCP.

- Incompréhension ou configuration incorrecte du réseau local virtuel natif

  Les routeurs et les commutateurs qui composent l'infrastructure physique d'un réseau sont gérés d'une manière différente que les PC clients qui s'attachent à cette infrastructure physique. Le VLAN dont ces interfaces de routeur et commutateur sont membres est appelé Réseau local virtuel natif (par défaut, VLAN 1). Les PC de client sont des membres d'un VLAN différent, de même que les téléphones IP sont des membres d'un autre VLAN encore. L'interface administrative du point d'accès ou du pont (interface BVI1) est considérée et numérotée comme une partie du réseau local virtuel natif, quels que soient les VLAN ou SSID qui traversent ce périphérique sans fil.

Importance du réseau local virtuel natif

Quand vous utilisez un port de jonction IEEE 802.1Q, toutes les trames sont marquées, sauf celles sur le VLAN configuré comme « réseau local virtuel natif » pour le port. Les trames sur le VLAN natif sont toujours transmises sans marqueur et normalement reçues sans marqueur. Par conséquent, quand un point d'accès est connecté au port de commutateur, le réseau local virtuel natif configuré sur le point d'accès doit correspondre au réseau local virtuel natif configuré sur le port de commutateur.

Remarque : S'il y a une correspondance dans les réseaux locaux virtuels natifs, les trames sont déposées.

Ce scénario s'explique plus facilement avec un exemple. Si le réseau local virtuel natif sur le port de commutateur est configuré comme VLAN 12 et que sur l'AP le réseau local virtuel natif est configuré comme VLAN 1, quand le point d'accès envoie une trame sur son réseau local virtuel natif au commutateur, le commutateur considère la trame comme appartenant au VLAN 12 puisque les trames du réseau local virtuel natif d'AP sont non-balisées. Ceci entraîne la confusion dans le réseau et donne lieu à des problèmes de connectivité. La même chose se produit quand le port de commutateur transfère une trame de son réseau local virtuel natif au point d'accès.

La configuration du réseau local virtuel natif devient encore plus importante quand vous avez une configuration de point d'accès du répéteur dans votre réseau sans fil. Vous ne pouvez pas configurer plusieurs VLAN sur les points d'accès du répéteur. Les points d'accès du répéteur prennent en charge seulement le réseau local virtuel natif. Par conséquent, la configuration du réseau local virtuel natif sur le point d'accès racine, le port de commutation auquel le point d'accès est connecté et le point d'accès du répéteur doivent être identiques. Autrement le trafic par le commutateur ne passe pas vers et depuis le point d'accès du répéteur.

Un exemple de scénario où une erreur de correspondance dans la configuration du réseau local virtuel natif du point d'accès du répéteur peut créer des problèmes, est quand il y a un serveur DHCP derrière le commutateur auquel le point d'accès racine est connecté. Dans ce cas les clients liés au point d'accès du répéteur ne reçoivent pas d'adresse IP du serveur DHCP parce

que les trames (requêtes DHCP dans notre cas) du réseau local virtuel natif du point d'accès du répéteur (qui n'est pas le même que le point d'accès racine et le commutateur) sont déposées.

De plus, quand vous configurez le port du commutateur, assurez-vous que tous les VLAN configurés sur les points d'accès sont autorisés sur le port de commutateur. Par exemple, si les VLAN 6, 7 et 8 existent sur le point d'accès (réseau sans fil), les VLAN doivent être autorisés sur le port de commutateur. Ceci peut être fait en utilisant cette commande dans le commutateur :

<#root>

```
switchport trunk allowed vlan add 6,7,8
```

Par défaut, un port de commutateur configuré comme agrégation permet à tous les VLAN de passer par le port de jonction. Consultez la section Interaction avec les commutateurs relatifs pour plus d'informations sur la façon de configurer le port de commutateur.

Remarque : autoriser tous les VLAN sur le point d'accès peut également devenir un problème dans certains cas, en particulier s'il s'agit d'un grand réseau. Ceci peut avoir comme conséquence l'utilisation élevée de la CPU sur les points d'accès. Élaguez les VLAN sur le commutateur de manière à ce que seul le trafic du VLAN auquel le point d'accès est intéressé passe par le point d'accès pour éviter une utilisation élevée de la CPU.

VLAN sur des points d'accès

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : afin de trouver des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commandes (clients enregistrés uniquement) .

Concepts liés aux points d'accès

Cette section discute des concepts liés à la façon de déployer des VLAN sur des points d'accès et se rapporte à ce schéma de réseau.

Dans cet exemple de réseau, le VLAN 1 est le réseau local virtuel natif, et les VLAN 10, 20, 30 et 40 existent, et sont joints à un autre châssis de commutateur. Seuls les VLAN 10 et 30 sont prolongés dans le domaine sans fil. Le réseau local virtuel natif est requis pour fournir la capacité de gestion et les authentifications du client.

Configuration de point d'accès

Afin de configurer le point d'accès pour des VLAN, procédez comme suit :

1. Dans l'interface graphique AP, cliquez sur Services > VLAN pour accéder à la page Services : VLAN .

a. La première étape consiste à configurer le réseau VLAN. Dans la liste actuelle de VLAN, sélectionnez Nouveau.

b. Entrez le numéro de VLAN du réseau local virtuel natif dans la case d'ID VLAN. Le numéro de VLAN doit correspondre au réseau local virtuel natif configuré sur le commutateur.

c. Comme l'interface BVI 1 est associée à la sous-interface du réseau local virtuel natif, l'adresse IP attribuée à l'interface BVI 1 doit être dans le même sous-réseau IP que d'autres équipements d'infrastructure sur le réseau (c'est-à-dire, l'interface SC0 sur un commutateur Catalyst qui exécute CatOS.)

d. Cochez la case du réseau local virtuel natif.

e. Cochez les cases de l'interface radio ou des interfaces auxquelles ce VLAN s'applique.

f. Cliquez sur Apply.

Ou encore, depuis la CLI, émettez ces commandes :

```
<#root>

AP#

configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)#

interface Dot11Radio0.1

AP(config-subif)#

encapsulation dot1Q 1 native

AP(config-subif)#

interface FastEthernet0.1

AP(config-subif)#

encapsulation dot1Q 1 native

AP(config-subif)#

end

AP#

write memory
```

2. Afin de configurer d'autres VLAN, procédez comme suit :

a. Dans la liste actuelle de VLAN, sélectionnez Nouveau.

b. Entrez le numéro de VLAN du VLAN souhaité dans la case d'ID VLAN. Le numéro de

VLAN doit correspondre au VLAN configuré sur le commutateur.

c. Cochez les cases de l'interface radio ou des interfaces auxquelles ce VLAN s'applique.

d. Cliquez sur Apply.

Ou encore, depuis la CLI, émettez ces commandes :

```
<#root>

AP#

configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)#

interface Dot11Radio0.10

AP(config-subif)#

encapsulation dot1Q 10

AP(config-subif)#

interface FastEthernet0.10

AP(config-subif)#

encapsulation dot1Q 10

AP(config-subif)#

end

AP#

write memory
```

e. Répétez les étapes 2a à 2d pour chaque VLAN désiré ou sélectionnez ces commandes de la CLI avec les modifications appropriées à la sous-interface et aux numéros de VLAN :

```
<#root>

AP#

configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)#

interface Dot11Radio0.30

AP(config-subif)#

encapsulation dot1Q 30

AP(config-subif)#
```

```
interface FastEthernet0.30

AP(config-subif)#

encapsulation dot1Q 30

AP(config-subif)#

end

AP#

write memory
```

3. L'étape suivante consiste à associer les VLAN configurés aux SSID. Pour ce faire, cliquez sur Security > SSID Manager.

   Remarque : vous n'avez pas besoin d'associer chaque VLAN défini sur le point d'accès à un SSID. Par exemple, pour des raisons de sécurité, la plupart des installations de point d'accès n'associent pas un SSID au réseau local virtuel natif.

   a. Pour créer un nouveau SSID, sélectionnez New.

   b. Entrez le SSID désiré (sensible à la casse) dans la case SSID.

   c. Sélectionnez le numéro de VLAN désiré pour associer ce SSID à de la liste déroulante.

      Remarque : afin de maintenir ce document dans sa portée prévue, la sécurité d'un SSID n'est pas abordée.

   d. Cliquez sur Apply-RadioX pour créer le SSID sur la radio sélectionnée, ou sur Apply-all pour la créer sur toutes les radios.

      Ou encore, depuis la CLI, émettez ces commandes :

      <#root>

```
AP#

configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)#

interface Dot11Radio0

AP(config-if)#

ssid Red

AP(config-if-ssid)#

vlan 10

AP(config-if-ssid)#

end
```

```
AP#
write memory
```

4. Répétez les étapes 3a à 3d pour chaque SSID désiré ou saisissez ces commandes depuis la CLI avec les modifications appropriées au SSID.

```
<#root>
AP#
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)#
interface Dot11Radio0
AP(config-if)#
ssid Green
AP(config-if-ssid)#
vlan 30
AP(config-if-ssid)#
end
AP#
write memory
```

Remarque : ces exemples n'incluent pas l'authentification. Une forme d'authentification (ouverte, Réseau-EAP) est requise pour que des clients s'associent.

VLAN sur des ponts

Concepts liés aux ponts

Cette section discute des concepts liés à la façon de déployer des VLAN sur des ponts et se rapporte à ce schéma de réseau.

Dans cet exemple de réseau, le VLAN 1 est le réseau local virtuel natif, et les VLAN 10, 20, 30 et 40 existent. Seuls les VLAN 10 et 30 sont prolongés à l'autre côté de la liaison. La liaison sans fil est chiffrée.

Afin de chiffrer les données qui passent sur la liaison radio, appliquez le chiffrement uniquement au SSID du réseau local virtuel natif. Ce chiffrement s'applique à tous autres VLAN. Quand vous placez un pont, il n'est pas nécessaire d'associer un SSID distinct à chaque VLAN. Les configurations de VLAN sont identiques sur les ponts racines et non-racines.

Configuration du pont

Afin de configurer le pont pour des VLAN, comme dans l'exemple de schéma de réseau, procédez comme suit :

1. Dans l'interface graphique AP, cliquez sur Services > VLAN pour accéder à la page Services : VLAN .

    a. La première étape consiste à configurer le réseau VLAN. Pour ce faire, choisissez <New> dans la liste actuelle de VLAN.

    b. Entrez le numéro de VLAN du réseau local virtuel natif dans la case d'ID VLAN. Celui-ci doit correspondre au réseau local virtuel natif configuré sur le commutateur.

    c. Comme l'interface BVI 1 est associée à la sous-interface du réseau local virtuel natif, l'adresse IP attribuée à l'interface BVI 1 doit être dans le même sous-réseau IP que d'autres équipements d'infrastructure sur le réseau (c'est-à-dire, l'interface SC0 sur un commutateur Catalyst qui exécute CatOS.)

    d. Cochez la case du réseau local virtuel natif.

    e. Cliquez sur Apply.

    Ou encore, depuis la CLI, émettez ces commandes :

    <#root>

    ```
    bridge#
    configure terminal
    Enter configuration commands, one per line.  End with CNTL/Z.
    bridge(config)#
    interface Dot11Radio0.1
    bridge(config-subif)#
    encapsulation dot1Q 1 native
    bridge(config-subif)#
    interface FastEthernet0.1
    bridge(config-subif)#
    encapsulation dot1Q 1 native
    bridge(config-subif)#
    end
    bridge#
    write memory
    ```

2. Afin de configurer d'autres VLAN, procédez comme suit :

   a. Dans la liste actuelle de VLAN, sélectionnez Nouveau.

   b. Entrez le numéro de VLAN du VLAN souhaité dans la case d'ID VLAN. Le numéro de VLAN doit correspondre au VLAN configuré sur le commutateur.

   c. Cliquez sur Apply.

      Ou encore, depuis la CLI, émettez ces commandes :

```
<#root>

bridge#

configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
bridge(config)#

interface Dot11Radio0.10

bridge(config-subif)#

encapsulation dot1Q 10

bridge(config-subif)#

interface FastEthernet0.10

bridge(config-subif)#

encapsulation dot1Q 10

bridge(config-subif)#

end

bridge#

write memory
```

   d. Répétez les étapes 2a à 2c pour chaque VLAN désiré ou sélectionnez les commandes de la CLI avec les modifications appropriées à la sous-interface et aux numéros de VLAN.

```
<#root>

AP#

configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
bridge(config)#

interface Dot11Radio0.30

bridge(config-subif)#
```

```
encapsulation dot1Q 30

bridge(config-subif)#

interface FastEthernet0.30

bridge(config-subif)#

encapsulation dot1Q 30

bridge(config-subif)#

end

bridge#

write memory
```

3. Depuis le gestionnaire de SSID (sous la commande de menu Security > SSID Manager) associez le réseau local virtuel natif à un SSID.

   Remarque : lorsque vous établissez un pont, le seul SSID que vous devez associer à un VLAN est celui qui établit une corrélation avec le VLAN natif. Vous devez indiquer ce SSID comme SSID d'infrastructure.

   a. Dans la liste actuelle de SSID, sélectionnez Nouveau.

   b. Entrez le SSID désiré (sensible à la casse) dans la case SSID.

   c. Sélectionnez le numéro de VLAN qui effectue des corrélations au réseau local virtuel natif de la liste déroulante.

      Remarque : afin de maintenir ce document dans sa portée prévue, la sécurité d'un SSID n'est pas abordée.

   d. Cliquez sur Apply pour créer le SSID sur la radio et l'associer au réseau local virtuel natif.

   e. Accédez de nouveau au bas de la page, et sous Global Radio0-802.11G SSID Properties sélectionnez le SSID dans la liste déroulante Set Infrastructure SSID. Cliquez sur Apply.

      Ou encore, depuis la CLI, émettez ces commandes :

      <#root>

      ```
      AP#

      configure terminal

      Enter configuration commands, one per line.  End with CNTL/Z.
      AP(config)#

      interface Dot11Radio0

      AP(config-if)#
      ```

```
ssid Black

AP(config-if-ssid)#

vlan 1

AP(config-if-ssid)#

infrastructure-ssid

AP(config-if-ssid)#

end

AP#

write memory
```

Remarque : lorsque des VLAN sont utilisés, les SSID sont configurés sous l'interface Dot11Radio physique, et non sous une sous-interface logique.

Remarque : cet exemple n'inclut pas l'authentification. La racine et les ponts non racine exigent une certaine forme d'authentification (ouverte, Réseau-EAP, etc.) afin de s'associer.

Utilisez un serveur RADIUS pour affecter des utilisateurs aux VLAN

Vous pouvez configurer votre serveur d'authentification RADIUS pour affecter des utilisateurs ou des groupes d'utilisateurs à un VLAN spécifique quand ils s'authentifient dans le réseau. Pour des informations sur cette fonctionnalité, consultez la section Utilisation d'un serveur RADIUS pour affecter des utilisateurs aux VLAN du document Guide de configuration du logiciel Cisco IOS pour les points d'accès Cisco Aironet, 12.4(3g)JA & 12.3(8)JEB.

Utilisation d'un serveur RADIUS pour l'affectation dynamique de groupe de mobilité

Vous pouvez également configurer un serveur RADIUS pour affecter dynamiquement des groupes de mobilité aux utilisateurs ou aux groupes d'utilisateurs. Ceci élimine la nécessité de configurer des SSID multiples sur le point d'accès. Au lieu de cela, vous devez configurer seulement un SSID par point d'accès. Pour des informations sur cette fonctionnalité, consultez la section Utilisation d'un serveur RADIUS pour l'affectation dynamique de groupe de mobilité du document Guide de configuration du logiciel Cisco IOS pour les points d'accès Cisco Aironet, 12.4(3g)JA & 12.3(8)JEB.

Configuration de groupe de pontage sur des points d'accès et des ponts

Généralement les groupes de pontage créent des domaines de commutation segmentés. Le trafic est confiné aux hôtes au sein de chaque groupe de pontage, mais pas entre les groupes de pontage. Le commutateur transfère le trafic seulement parmi les hôtes qui composent le groupe de pontage, ce qui restreint la diffusion et le trafic de multidiffusion (inondation) seulement à ces

hôtes. Les groupes de pontage soulagent la congestion de réseau et fournissent plus de sécurité réseau quand ils segmentent le trafic à certaines zones du réseau.

Consultez la section Présentation du pontage pour des informations détaillées.

Dans un réseau sans fil, des groupes de pontage sont configurés sur les points d'accès sans fil et les ponts afin que le trafic de données d'un VLAN soit transmis depuis des supports sans fil vers le côté câblé et vice versa.

Effectuez cette étape depuis la CLI du point d'accès afin d'activer des groupes de pontage globalement sur le point d'accès/pont.

Cet exemple utilise le groupe de pontage numéro 1.

Ap(configure)#bridge 1

Remarque : vous pouvez numéroter vos groupes de ponts de 1 à 255.

Configurez l'interface radio et l'interface Fast Ethernet du périphérique sans fil de manière à ce qu'elles soient dans le même groupe de pontage. Ceci crée un chemin entre ces deux interfaces différentes, et elles sont dans le même VLAN pour des raisons de marquage. En conséquence, les données transmises depuis le côté sans fil via l'interface radio sont transmises à l'interface Ethernet à laquelle le réseau câblé est connecté et vice versa. En d'autres termes, les interfaces radio et Ethernet qui appartiennent au même groupe de pontage placent en fait un pont entre les données.

À un point d'accès/pont, vous devez avoir un groupe de pontage par VLAN de sorte que le trafic de routage puisse passer du fil au sans fil et vice versa. Plus vous avez de VLAN devant passer du trafic à travers le sans fil, plus vous avez besoin de groupes de pontage.

Par exemple, si vous avez seulement un VLAN pour passer le trafic du côté sans fil au côté câblé de votre réseau, configurez seulement un groupe de pontage depuis la CLI du point d'accès/pont. Si vous avez des plusieurs VLAN pour passer le trafic du côté sans fil au côté câblé et vice versa, configurez des groupes de pontage pour chaque VLAN à la sous-interface par radio, ainsi que la sous-interface de Fast Ethernet.

1. Configurez le groupe de pontage dans l'interface sans fil avec la commande bridge group dot11radio.

   Voici un exemple :

   <#root>

   ```
   AP#

   configure terminal

   Enter configuration commands, one per line.  End with CNTL/Z.
   AP(config)#

   interface Dot11Radio0.1
   ```

```
Ap(config-subif)#

encapsulation dot1q 1 native

Ap(config-subif)#

bridge group 1
 !--- Here "1" represents the bridge group number.

ap(config-subif)#

exit
```

2. Configurez le groupe de pontage avec le même numéro de groupe de pontage (« 1 » dans cet exemple) dans l'interface Fast Ethernet de sorte que le trafic VLAN 1 soit passé à travers l'interface sans fil vers le côté câblé et vice versa.

<#root>

```
Ap(config)#

interface fastEthernet0.1

Ap(config-subif)#

encapsulation dot1q 1 native

Ap(config-subif)#

bridge group 1
 !--- Here "1" represents the bridge group number.

Ap(config-subif)#

exit
```

Remarque : lorsque vous configurez un groupe de pontage sur l'interface radio, ces commandes sont définies automatiquement.

- bridge-group 1 subscriber-loop-control
- bridge-group 1 block-unknown-source
- no bridge-group 1 source-learning
- no bridge-group 1 unicast-flood
- bridge-group 1 spanning-disabled

Remarque : lorsque vous configurez un groupe de pontage sur l'interface Fast Ethernet, ces commandes sont définies automatiquement.

- no bridge-group 1 source-learning

- bridge-group 1 spanning-disabled

Integrated Routing and Bridging (IRB)

Le routage et le pontage intégrés permet d'acheminer un protocole spécifique entre les interfaces et les groupes de pontage routés, ou d'acheminer un protocole spécifique entre des groupes de pontage. Le trafic local ou non routable peut être ponté parmi les interfaces pontées du même groupe de pontage, alors que le trafic routable peut être acheminé à d'autres interfaces ou groupes de pontage routés

Avec le routage et le pontage intégrés, vous pouvez faire ceci :

- Basculer des paquets d'une interface pontée à une interface routée
- Basculer des paquets d'une interface pontée à une interface routée
- Basculer des paquets au sein du même groupe de pontage

Autoriser IRB sur les points d'accès sans fil et les ponts afin d'acheminer votre trafic entre les groupes de pontage ou entre les interfaces et les groupes de pontage routés. Vous avez besoin d'un routeur externe ou d'un commutateur de couche 3 afin d'effectuer l'acheminement entre les groupes de pontage ou entre les groupes de pontage et les interfaces routées.

Émettez cette commande afin d'activer IRB dans le point d'accès/pont.

AP(configure)#bridge irb

Le routage et le pontage intégrés emploient le concept d'une interface virtuelle de groupe de pontage (BVI) afin d'acheminer le trafic entre les interfaces et les groupes de pontage routés ou entre les groupes de pontage.

Une BVI est une interface virtuelle dans le routeur du commutateur de la couche 3 qui agit comme une interface routée normale. Une BVI ne prend pas en charge le pontage mais représente réellement le groupe de pontage correspondant aux interfaces routées dans le routeur du commutateur de la couche 3. Elle a tous les attributs de couche réseau (tels qu'une adresse et des filtres de couche réseau) qui s'appliquent au groupe de pontage correspondant. Le numéro d'interface attribué à cette interface virtuelle correspond au groupe de pontage que cette interface virtuelle représente. Ce numéro est la liaison entre l'interface virtuelle et le groupe de pontage.

Effectuez ces étapes afin de configurer la BVI sur des points d'accès et des ponts.

1. Configurez la BVI et affectez le numéro correspondant du groupe de pontage à la BVI. Cet exemple attribue le groupe de pontage numéro 1 à la BVI.

<#root>

```
Ap(configure)#
interface BVI 1
```

```
AP(config-if)#

ip address 10.1.1.1 255.255.0.0
 !--- Assign an IP address to the BVI.

Ap(config-if)#

no shut
```

2. Permettez à une BVI d'accepter et d'acheminer les paquets routables reçus de son groupe de pontage correspondant.

<#root>

```
Ap(config)#

bridge 1 route ip!---


!--- This example enables the BVI to accept and route the IP packet.
```

Il est important de comprendre que vous avez besoin seulement d'une BVI pour la gestion/le réseau local virtuel natif dans lesquels se trouve le point d'accès (dans cet exemple, VLAN 1). Vous n'avez besoin d'une BVI pour aucune autre sous-interface, indépendamment de combien de VLAN et de groupes de pontage vous configurez sur votre point d'accès/pont. Cela est dû au fait que vous marquez le trafic dans tous les autres VLAN (excepté le réseau local virtuel natif) et l'envoyez au commutateur à travers une interface dot1q jointe sur le côté câblé. Par exemple, si vous avez 2 VLAN sur votre réseau, vous avez besoin de deux groupes de pontage, mais une seule BVI correspondant au VLAN de gestion est suffisante dans votre réseau sans fil.

Quand vous activez le routage pour un protocole donné sur l'interface virtuelle du groupe de pontage, les paquets qui proviennent d'une interface routée mais qui sont destinés à un hôte dans un domaine ponté, sont routés vers l'interface virtuelle du groupe ponté et transférés à l'interface pontée correspondante.

Tout le trafic qui est routé à l'interface virtuelle du groupe de pontage est transféré au groupe de pontage correspondant en tant que trafic ponté. Tout le trafic routable reçu sur une interface pontée est routé vers d'autres interfaces routées comme s'il provenait directement de l'interface virtuelle du groupe de pontage.

Consultez la section Configuration du pontage pour des informations plus détaillées sur le pontage et l'IRB.

Interaction avec les commutateurs relatifs

Dans cette section, nous vous indiquons comment configurer (ou vérifier la configuration) des

commutateurs Cisco qui se connectent à l'équipement sans fil de Cisco Aironet.

Remarque : afin de trouver des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commandes (clients enregistrés uniquement) .

Configuration du commutateur — Catalyst OS

Afin de configurer un commutateur qui exécute le système d'exploitation Catalyst pour lier des VLAN à un point d'accès, la syntaxe de commande est set trunk <module #/port #> on dot1q and set trunk <module #/port #> <vlan list>.

Voici un exemple du schéma de réseau :

<#root>

```
set trunk 2/1 on dot1q
set trunk 2/1 1,10,30
```

Configuration du commutateur - Commutateurs Catalyst basés sur l'IOS

Du mode de configuration de l'interface, sélectionnez ces commandes, si vous souhaitez :

- Configurer le port de commutateur pour lier les VLAN à un point d'accès
- Sur un commutateur Catalyst qui exécute l'IOS
- Le CatIOS inclut mais n'est pas limité à :
    - 6x00
    - 4x00
    - 35x0
    - 295 x

<#root>

```
switchport mode trunk
switchport trunk encapsulation dot1q
switchport nonegotiate
switchport trunk native vlan 1
switchport trunk allowed vlan add 1,10,30
```

Remarque : l'équipement sans fil Cisco Aironet basé sur IOS ne prend pas en charge le protocole DTP (Dynamic Trunking Protocol). Le commutateur ne doit donc pas essayer de le négocier.

Configuration du commutateur — Catalyst 2900XL/3500XL

Depuis le mode de configuration de l'interface, sélectionnez ces commandes si vous voulez configurer le port de commutateur de manière à ce qu'il lie les VLAN à un point d'accès sur un commutateur Catalyst 2900XL ou 3500XL qui exécute l'IOS :

<#root>

```
switchport mode trunk
switchport trunk encapsulation dot1q
switchport trunk native vlan 1
switchport trunk allowed vlan 1,10,30
```

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Vérification de l'équipement sans fil

- show vlan - affiche tous les VLAN actuellement configurés sur le point d'accès, et leur état

<#root>

ap#

show vlan

```
Virtual LAN ID:  1 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  FastEthernet0.1
Dot11Radio0.1
Virtual-Dot11Radio0.1

 This is configured as native Vlan for the following interface(s) :

FastEthernet0
Dot11Radio0
Virtual-Dot11Radio0

   Protocols Configured:   Address:          Received:        Transmitted:
        Bridging        Bridge Group 1          36954                  0
        Bridging        Bridge Group 1          36954                  0

Virtual LAN ID:  10 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  FastEthernet0.10
Dot11Radio0.10
Virtual-Dot11Radio0.10
```

```
   Protocols Configured:   Address:          Received:        Transmitted:
        Bridging        Bridge Group 10          5297                  0
        Bridging        Bridge Group 10          5297                  0
        Bridging        Bridge Group 10          5297                  0

Virtual LAN ID:  30 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  FastEthernet0.30
Dot11Radio0.30
Virtual-Dot11Radio0.30

   Protocols Configured:   Address:          Received:        Transmitted:
        Bridging        Bridge Group 30          5290                  0
        Bridging        Bridge Group 30          5290                  0
        Bridging        Bridge Group 30          5290                  0

ap#
```

- show dot11 associations - affiche des informations au sujet des clients associés, par SSID/VLAN

<#root>

```
ap#
show dot11 associations

802.11 Client Stations on Dot11Radio0:

SSID [Green] :

SSID [Red] :

Others:  (not related to any ssid)

ap#
```

Vérification du commutateur

- Sur un commutateur basé sur le système d'exploitation Catalyst, show trunk <module #/port #> - affiche l'état d'une agrégation sur un port donné

<#root>

```
Console> (enable) show trunk 2/1
* - indicates vtp domain mismatch
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/1      on           dot1q          trunking      1
```

```
Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------

 2/1      1,10,30


Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------
 2/1      1,10,30

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------
 2/1      1,10,30
Console> (enable)
```

- Sur un commutateur basé sur IOS, show interface fastethernet <module #/port #> trunk - affiche l'état d'une agrégation sur une interface donnée

<#root>

```
2950g#show interface fastEthernet 0/22 trunk

Port        Mode         Encapsulation  Status        Native vlan

Fa0/22      on           802.1q         trunking      1


Port        Vlans allowed on trunk

Fa0/22      1,10,30


Port        Vlans allowed and active in management domain
Fa0/22      1,10,30

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/22      1,10,30
2950gA#
```

- Sur un commutateur Catalyst 2900XL/3500XL, show interface fastethernet <module #/port #> switchport - affiche l'état d'une agrégation sur une interface donnée

<#root>

```
cat3524xl#show interface fastEthernet 0/22 switchport
Name: Fa0/22
Switchport: Enabled
Administrative mode: trunk

Operational Mode: trunk

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q
```

```
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)

Trunking VLANs Enabled: 1,10,30,1002-1005

Trunking VLANs Active: 1,10,30

Pruning VLANs Enabled: 2-1001

Priority for untagged frames: 0
Override vlan tag priority: FALSE
Voice VLAN: none
Appliance trust: none
Self Loopback: No
wlan-cat3524xl-a#
```

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Configuration des VLAN (Guide de configuration des points d'accès)
- Configuration des VLAN (Guide de configuration du pont)
- Assistance technique d'agrégation
- Interaction avec les commutateurs relatifs
- Configuration requise pour l'implémentation du mode Trunk
- Présentation du pontage
- Exemple de configuration des types d'authentification sans fil sur un routeur ISR fixe
- Exemple de configuration des types d'authentification sans fil sur un routeur ISR fixe via SDM
- Exemple de configuration de la connectivité LAN sans fil à l'aide d'un ISR avec chiffrement WEP et authentification LEAP
- Exemple de configuration de connexion LAN sans fil de base
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.