Affectation dynamique VLAN sur le point d'accès autonome pour l'exemple de configuration de la version 15.2(2) JB

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Informations générales
Configurez
Diagramme du réseau
Configuration AP
Configuration CLI
Configuration du serveur RADIUS
Profils d'autorisation
Protocoles permis
Règles d'identité
Règles d'autorisation
Vérifiez
Dépannez
Commandes de débogage

Introduction

Ce document décrit le concept de l'affectation dynamique VLAN. Il décrit également comment configurer le point d'accès autonome et un serveur de RADIUS - le serveur de contrôle d'accès (ACS) ce exécute la version 5.2 - afin d'affecter les clients réseau local de radio (WLAN) à une particularité VLAN dynamiquement.

Conditions préalables

Conditions requises

Cisco recommande de posséder des connaissances sur les sujets suivants avant de tenter cette configuration :

- Point d'accès autonome
- Serveur d'Authentification, autorisation et comptabilité (AAA)
- Réseaux sans fil et questions de sécurité sans fil

Composants utilisés

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

- Point d'accès (AP) 3602 qui exécute le logiciel autonome Release15.2(2)JB de Cisco IOS®
- iPhone 4S qui exécute la version 6.1.3 en tant que client
- Cisco Secure ACS qui exécute la version 5.2
- Commutateur de gamme Cisco Catalyst 3560

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Dans la plupart des systèmes WLAN, chaque WLAN a une stratégie statique qui s'applique à tous les clients associés à un SSID (Service Set Identifier), ou WLAN dans la terminologie du contrôleur. Bien que puissante, cette méthode a des limites, parce qu'elle exige des clients de s'associer avec le SSID différent afin d'hériter du différents Qualité de service (QoS) et stratégies de sécurité.

Cependant, la solution WLAN de Cisco prend en charge la mise en réseau d'identités. Ceci permet au réseau pour annoncer un SSID simple, mais permet aux utilisateurs spécifiques pour hériter de QoS différent, d'attributs VLAN, et/ou de stratégies de sécurité basées sur les identifiants utilisateurs.

L'affectation de VLAN dynamique est une fonction qui place un utilisateur sans fil dans un VLAN spécifique en fonction des informations fournies par l'utilisateur. Cette tâche d'assigner des utilisateurs à une particularité VLAN est gérée par un serveur d'authentification RADIUS, tel que le Cisco Secure ACS. Ceci peut être utilisé, par exemple, afin de permettre à l'hôte sans fil pour rester sur le même VLAN qu'il déplace dans un réseau campus.

En conséquence, quand les tentatives d'un client de s'associer à un point d'accès léger (LAP) se sont inscrites à un contrôleur, le RECOUVREMENT passe les qualifications de l'utilisateur au serveur de RADIUS pour la validation. Une fois que l'authentification est réussie, le serveur RADIUS passe certains attributs de l'Internet Engineering Task Force (IETF) à l'utilisateur. Ces attributs RADIUS décident de l'ID de VLAN qui doit être affecté au client sans fil. Le SSID, le WLAN en termes de contrôleur LAN Sans fil (WLC), du client n'importe pas, parce que l'utilisateur est toujours assigné à cet ID DE VLAN prédéterminé.

Les attributs d'utilisateur RADIUS utilisés pour l'affectation de l'ID de VLAN sont :

- IETF 64 (type de tunnel) - Ceci est placé au **VLAN**.
- IETF 65 (type de support de tunnel) - ceci est placé à **802**.

- IETF 81 (identification groupe privée de tunnel) - ceci est placé à l'**ID DE VLAN**.

L'ID du VLAN est de 12 bits et prend une valeur entre 1 et 4 094, inclus. Puisque le Tunnel-Private-Group-ID est un type de chaîne, comme défini dans RFC 2868 pour l'usage avec le 802.1X d'IEEE, la valeur entière d'ID DE VLAN est encodée comme chaîne. Quand ces attributs de tunnel sont envoyés, il est nécessaire de renseigner la zone Tag.

Comme observé dans RFC2868 , section 3.1 : **La zone Tag a une longueur d'un octet et sa fonction est de fournir un moyen de regrouper les attributs dans le même paquet qui fait référence au même tunnel.** Les valeurs valides pour cette zone sont comprises entre 0x01 et 0x1F, inclus. Si la zone Tag est inutilisée, elle doit avoir pour valeur zéro (0x00). Référez-vous à RFC 2868 pour plus d'informations sur tous les attributs RADIUS.

Configurez

Diagramme du réseau

Configuration AP

1. Naviguez vers **GUI > services > VLAN** afin de configurer les VLAN sur AP, et créez les VLAN comme les conditions requises spécifient. Cet exemple utilise deux VLAN - **100** et **200**.

2. Naviguez vers **GUI > Security > Server Manager** afin de configurer le **serveur de sauvegarde de RADIUS** sur AP. Écrivez le **nom du serveur de sauvegarde de RADIUS**, l'**adresse Internet ou l'adresse IP**, et le **secret partagé** (ce secret partagé devrait apparier RADIUS).

3. Pour les les deux les VLAN, le cryptage devrait s'assortir. Cet exemple trace le portail de Gestion de centre de contact de Norme AES (Advanced Encryption Standard) de chiffrements (**CCMP**) pour VLAN **100** et **200**.

4. Naviguez vers **SSID > Security > SSID Manager** afin de configurer le gestionnaire SSID. Tracez-le à la **radio** correcte dans le domaine d'interface.

   Sur l'**écran Settings d'authentification client**, cochez la **case à cocher Open Authentication**, et la sélectionnez **avec l'EAP**. Cliquez sur les cases d'option de **par défaut d'utilisation** pour les deux champs sous des priorités de serveur. Ceci se termine la configuration AP.

Configuration CLI

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname MAIB-3602
!
!
logging rate-limit console 9
enable secret 5 $1$iGJu$80f61xvQRPNeSejmOJhko0
!
aaa new-model
!
!
aaa group server radius rad_eap
 server name RADIUS
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
!
!
!
!
!
aaa session-id common
no ip routing
no ip cef
!
!
!
!
dot11 syslog
dot11 vlan-name Teacher vlan 200
dot11 vlan-name student vlan 100
!
dot11 ssid DVAAP
   vlan 100
   authentication open eap eap_methods
   authentication key-management wpa version 2
!
!
dot11 guest
!
!
!
username Cisco password 7 032752180500
```

```
!
!
bridge irb
!
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 100 mode ciphers aes-ccm
 !
 encryption vlan 200 mode ciphers aes-ccm
 !
 ssid DVAAP
 !
 antenna gain 0
 stbc
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.100
 encapsulation dot1Q 100
 no ip route-cache
 bridge-group 100
 bridge-group 100 subscriber-loop-control
 bridge-group 100 spanning-disabled
 bridge-group 100 block-unknown-source
 no bridge-group 100 source-learning
 no bridge-group 100 unicast-flooding
!
interface Dot11Radio0.200
 encapsulation dot1Q 200
 no ip route-cache
 bridge-group 200
 bridge-group 200 subscriber-loop-control
 bridge-group 200 spanning-disabled
 bridge-group 200 block-unknown-source
 no bridge-group 200 source-learning
 no bridge-group 200 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 encryption vlan 100 mode ciphers aes-ccm
 !
 encryption vlan 200 mode ciphers aes-ccm
 !
 ssid DVAAP
 !
 antenna gain 0
 peakdetect
 dfs band 3 block
 stbc
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
```

```
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1.100
 encapsulation dot1Q 100
 no ip route-cache
 bridge-group 100
 bridge-group 100 subscriber-loop-control
 bridge-group 100 spanning-disabled
 bridge-group 100 block-unknown-source
 no bridge-group 100 source-learning
 no bridge-group 100 unicast-flooding
!
interface Dot11Radio1.200
 encapsulation dot1Q 200
 no ip route-cache
 bridge-group 200
 bridge-group 200 subscriber-loop-control
 bridge-group 200 spanning-disabled
 bridge-group 200 block-unknown-source
 no bridge-group 200 source-learning
 no bridge-group 200 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface GigabitEthernet0.100
 encapsulation dot1Q 100
 no ip route-cache
 bridge-group 100
 bridge-group 100 spanning-disabled
 no bridge-group 100 source-learning
!
interface GigabitEthernet0.200
 encapsulation dot1Q 200
 no ip route-cache
 bridge-group 200
 bridge-group 200 spanning-disabled
 no bridge-group 200 source-learning
!
interface BVI1
 ip address 10.105.135.240 255.255.255.128
 no ip route-cache
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
!
radius-server attribute 32 include-in-access-req format %h
radius-server vsa send accounting
```

```
!
radius server RADIUS
 address ipv4 10.106.102.50 auth-port 1645 acct-port 1646
 key 7 123A0C0411045D5679
!
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
 transport input all
!
end
```

Configuration du serveur RADIUS

Ajoutez AP en tant que client d'AAA sur le serveur de RADIUS avec le secret partagé précédent-mentionné. Créez les **utilisateurs** et les **groupes d'utilisateurs**. Cet exemple utilise l'**étudiant et enseignant**.

Profils d'autorisation

Terminez-vous ces étapes afin de configurer le profil d'autorisation pour l'étudiant et enseignant au match vlan **100** et au **VLAN 200**.

1. Naviguez vers le **>Network Access d'éléments > d'autorisation et d'autorisations de stratégie > les profils d'autorisation**, et cochez la case d'**étudiant**.

2. Sur les **fonctionnalités usuelles** tabulez, **charge statique** choisie pour le champ VLAN ID/Name, et **100** pour la valeur VLAN.

3. Sous l'**autorisation les profils** cochent la case de **professeur**. Sur les **fonctionnalités usuelles** tabulez, **charge statique** choisie pour le champ VLAN ID/Name, et **200** pour la valeur VLAN.

Protocoles permis

1. Naviguez **pour accéder à des stratégies > des services d'accès > l'accès au réseau de par défaut**, pour sélectionner l'**onglet Général**, et pour écrire les détails pour le nom et la description. Dans le cadre de la stratégie Sturcture, vérifiez les cases d'**identité** et d'**autorisation**.

2. Sur les **protocoles permis** tabulez, vérifiez les cases de **Protocoles d'authentification**, comme décrit ici.

Règles d'identité

Afin de permettre des utilisateurs du Protected Extensible Authentication Protocol (PEAP), naviguez **pour accéder à des stratégies > des services d'accès > l'accès au réseau > l'identité de par défaut**. Cochez la case à côté du **PEAP**.

Règles d'autorisation

Afin de tracer l'étudiant et enseignant aux profils d'autorisation pour l'étudiant et enseignant pour VLAN 100 et 200, naviguez **pour accéder à des stratégies > des services d'accès > l'accès au réseau > l'autorisation de par défaut**.

Vérifiez

Ces images illustrent comment vérifier votre configuration avec l'utilisation de votre iPhone. Afin de vérifier, connectez votre iPhone au SSID DVAAP aux groupes d'enseignant et étudiant, et assurez-vous que l'affichage correct d'adresses IP.

Dépannez

Complétez ces étapes afin de dépanner votre configuration.

1. Afin d'éliminer la possibilité que les questions de Radiofréquence (RF) empêchent l'authentification réussie, placez la méthode sur le SSID **pour s'ouvrir** afin de désactiver temporairement l'authentification.

2. Du GUI à la page de **gestionnaire SSID**, décochez la case de **Network-EAP**, et cochez **ouvert**.

3. Du CLI, ne sélectionnez l'**authentication open** et **aucune** commande d'**eap_methods d'authentication network-eap**. Si le client s'associe avec succès, le rf ne contribue pas au problème d'association.

4. Vérifiez que tous les mots de passe secret partagés sont synchronisés. Ces lignes doivent contenir la même chose mot de passe secret partagé :
<shared_secret> principal du l'acct-port X du l'authentique-port X de l'hôte x.x.x.x de RADIUS-serveur<shared_secret> de clé du nas x.x.x.x
5. Retirez tous les groupes d'utilisateurs et leurs configurations associées. Parfois les conflits peuvent se produire entre les groupes d'utilisateurs définis par AP et les groupes d'utilisateurs sur le domaine.

Commandes de débogage

> **Note**: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Voici une liste de commandes de débogage utiles.

- **l'authentificateur de debug dot11 aaa entièrement** ceci mettent au point des expositions les diverses négociations qu'un client intervient pendant que le client s'associe et authentifie par le 802.1x ou le processus d'EAP de la perspective de l'authentificateur (AP). Ce débogage a été introduit dans le logiciel Cisco IOS Version 12.2(15)JA. Ce **dot1x tout de debug dot11 aaa d'**obsoletes de commande en cela et des versions ultérieures.
- **authentification de debug radius** - Ceci mettent au point des expositions les négociations de RADIUS entre le serveur et client, qui, dans ce cas, sont AP.
- **client de debug radius local-server** - Ceci mettent au point des expositions l'authentification du client de la perspective du serveur de RADIUS.

Voici un exemple :

```
MAIB-3602#debug radius authentication
Radius protocol debugging is on
Radius protocol brief debugging is off
Radius protocol verbose debugging is off
Radius packet hex dump debugging is off
Radius packet protocol (authentication) debugging is on
Radius packet protocol (accounting) debugging is off
Radius elog debugging debugging is off
Radius packet retransmission debugging is off
Radius server fail-over debugging is off
Radius elog debugging debugging is off
MAIB-3602#
MAIB-3602#show deb
General OS:
 AAA Authentication debugging is on
Radius protocol debugging is on
Radius packet protocol (authentication) debugging is on
dot1x:
 Dot1x registry info debugging is on
 Dot1x redundancy info debugging is on
 Dot1x packet info debugging is on
 Dot1x events debugging is on
 Dot1x State machine transitions and actions debugging is on
 Dot1x Errors debugging is on
 Dot1x Supplicant EAP-FAST debugging is on
 Dot1x Manager debugging is on
 Dot1x Supplicant State Machine debugging is on

MAIB-3602#debug radius authentication
Radius protocol debugging is on
Radius protocol brief debugging is off
Radius protocol verbose debugging is off
Radius packet hex dump debugging is off
Radius packet protocol (authentication) debugging is on
Radius packet protocol (accounting) debugging is off
Radius elog debugging debugging is off
Radius packet retransmission debugging is off
Radius server fail-over debugging is off
```

```
Radius elog debugging debugging is off
MAIB-3602#
MAIB-3602#show deb
General OS:
 AAA Authentication debugging is on
Radius protocol debugging is on
Radius packet protocol (authentication) debugging is on
dot1x:
 Dot1x registry info debugging is on
 Dot1x redundancy info debugging is on
 Dot1x packet info debugging is on
 Dot1x events debugging is on
 Dot1x State machine transitions and actions debugging is on
 Dot1x Errors debugging is on
 Dot1x Supplicant EAP-FAST debugging is on
 Dot1x Manager debugging is on
 Dot1x Supplicant State Machine debugging is on
```