Affectation dynamique VLAN avec l'exemple de configuration NGWC et ACS 5.2

Contenu

Introduction

Ce document décrit le concept de l'affectation dynamique VLAN. Il décrit également comment configurer le contrôleur LAN Sans fil (WLC) et un serveur de RAYON afin d'affecter les clients Sans fil du RÉSEAU LOCAL (WLAN) à une particularité VLAN dynamiquement. Dans ce document, le serveur de RAYON est un serveur de contrôle d'accès (ACS) cette version 5.2 de Système de contrôle d'accès sécurisé Cisco de passages.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base du WLC et du Point d'accès léger (recouvrements)

- La connaissance fonctionnelle du serveur d'Authentification, autorisation et comptabilité (AAA)
- Avoir une connaissance complète des réseaux sans fil et des problèmes liés à la sécurité sans fil

Composants utilisés

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

- Contrôleur LAN de radio de Cisco 5760 avec la version logicielle 3.2.2 (armoire de câblage du Cisco IOS® XE de nouvelle génération, ou le NGWC)
- Point d'accès léger de gamme 3602 de Cisco Aironet
- Microsoft Windows XP avec le suppliant d'Intel Proset
- Version 5.2 de Système de contrôle d'accès sécurisé Cisco
- 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.

Affectation de VLAN dynamique avec le serveur RADIUS

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 limitations parce qu'elle exige que les clients soient associés à des SSID différents afin d'hériter de QoS et de stratégies de sécurité différentes.

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'affectation d'utilisateur à une particularité VLAN est gérée par un serveur d'authentification RADIUS, tel qu'un Cisco Secure ACS. Cette caractéristique peut être utilisée, 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 RECOUVREMENT enregistré avec un contrôleur, le RECOUVREMENT passe les qualifications de l'utilisateur au serveur de RAYON 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 du client (le WLAN, en termes de WLC) 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) - Placez au VLAN.

- IETF 65 (type de support de tunnel) - placez à 802.
- IETF 81 (Tunnel-Private-Group-ID) - Placez à l'ID DE VLAN.

L'ID DE VLAN est 12 bits et prend une valeur entre 1 et 4094, inclus. Puisque le Tunnel-Private-Group-ID est de chaîne de type, comme défini dans RFC 2868, des attributs RADIUS pour le soutien de Protocol de tunnel de l'utilisation avec le 802.1X d'IEEE, la valeur entière d'ID DE VLAN est encodés comme chaîne. Quand ces attributs de tunnel sont envoyés, il est nécessaire de renseigner la zone Tag.

Comme observé dans RFC2868 , section 3.1 :

« Le champ Tag est un octet de longueur et est destiné pour fournir des moyens des attributs de groupement dans le même paquet qui se rapportent au même tunnel. »

Les valeurs valides pour le champ Tag sont 0x01 par 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

La configuration d'une affectation dynamique VLAN se compose de deux étapes distinctes :

1. Configurez le WLC avec l'interface de ligne de commande (CLI) ou avec le GUI.
2. Configurez le serveur de RAYON.

   Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Ce document utilise le 802.1X avec le Protected Extensible Authentication Protocol (PEAP) comme mécanisme de sécurité.

Suppositions

- Des Commutateurs sont configurés pour toute la couche 3 (L3) VLAN.
- Le serveur DHCP est assigné une portée de DHCP.
- La Connectivité L3 existe entre tous les périphériques dans le réseau.
- Le RECOUVREMENT est déjà joint au WLC.
- Chaque VLAN a un masque de /24.
- ACS 5.2 a un certificat auto-signé installé.

Configurez WLC avec le CLI

Configurez le WLAN

C'est un exemple de la façon configurer un WLAN avec le SSID de DVA :

```
wlan DVA 3 DVA
 aaa-override
 client vlan VLAN0020
 security dot1x authentication-list ACS
 session-timeout 1800
 no shutdown
```

Configurez le serveur de RAYON sur WLC

C'est un exemple de la configuration du serveur de RAYON sur le WLC :

```
aaa new-model
!
!
aaa group server radius ACS
 server name ACS
!
aaa authentication dot1x ACS group ACS

radius server ACS
 address ipv4 10.106.102.50 auth-port 1645 acct-port 1646
 key Cisco123

dot1x system-auth-control
```

Configurez le pool DHCP pour le client VLAN

C'est un exemple de la configuration du pool DHCP pour le client VLAN 30 et VLAN 40 :

```
interface Vlan30
 ip address 30.30.30.1 255.255.255.0
!
interface Vlan40
 ip address 40.40.40.1 255.255.255.0

ip dhcp pool vla30
 network 30.30.30.0 255.255.255.0
 default-router 30.30.30.1
!
ip dhcp pool vlan40
 network 40.40.40.0 255.255.255.0
 default-router 40.40.40.1

ip dhcp snooping vlan 30,40
ip dhcp snooping
```

Configurez WLC avec le GUI

Configurez le WLAN

Cette procédure décrit comment configurer le WLAN.

1. Naviguez vers la **configuration** > la **radio** > le **WLAN** > **NOUVEL** onglet.

2. Cliquez sur l'**onglet Général** afin de voir que le WLAN est configuré pour WPA2-802.1X, et tracer l'interface/groupe d'Interfrace (G) à VLAN 20 (**VLAN0020**).

3. Cliquez sur l'**onglet Avancé**, et cochez la case d'**Allow AAA Override**. Le dépassement doit être activé pour que cette caractéristique fonctionne.

4. Cliquez sur l'**onglet Sécurité** et l'onglet **Layer2**, cochez la case du chiffrement WPA2 **AES**, et sélectionnez le **802.1x de la** liste déroulante authentique de clé gestion.

Configurez le serveur de RAYON sur WLC

Cette procédure décrit comment configurer le serveur de RAYON sur le WLC.

1. Naviguez vers la **configuration** > l'**onglet Sécurité**.

2. Naviguez vers l'**AAA** > les **groupes de serveurs** > le **rayon** afin de créer les groupes de serveurs de rayon. Dans cet exemple, le groupe de serveurs de rayon s'appelle l'ACS.

3. Éditez l'entrée de serveur de rayon afin d'ajouter l'adresse IP du serveur et le secret partagé. Ceci secret partagé doit apparier le secret partagé sur le WLC et le serveur de RAYON.

   C'est un exemple d'une configuration complète :

Configurez le serveur de RAYON

Cette procédure décrit comment configurer le serveur de RAYON.

1. Sur le serveur de RAYON, naviguez vers des **utilisateurs et l'identité enregistre** > **identité interne enregistre** > des **utilisateurs**.

2. Créez les noms d'utilisateur et les groupes appropriés d'identité. Dans cet exemple, c'est étudiant et tous les groupes : Étudiants, et professeur et AllGroups : Professeurs.

3. Naviguez vers des **éléments de stratégie** > l'**autorisation et des autorisations** > des **profils d'accès au réseau** > d'**autorisation**, et créez les profils d'autorisation pour le dépassement d'AAA.

4. Éditez le profil d'autorisation pour l'étudiant.

5. Placez le VLAN ID/Name en tant que **charge statique** avec une valeur de **30** (VLAN 30).

6. Éditez le profil d'autorisation pour le professeur.

7. Placez le VLAN ID/Name en tant que **charge statique** avec une valeur de **40** (VLAN 40).

8. Naviguez **pour accéder à des stratégies** > des **services d'accès** > l'**accès au réseau de par défaut**, et cliquez sur l'onglet **permis de protocoles**. Vérifiez la case à cocher de l'**autoriser PEAP**.

9. Naviguez vers l'**identité**, et définissez les règles afin de permettre des utilisateurs PEAP.

10. Naviguez vers l'**autorisation**, et tracez l'étudiant et enseignant à la stratégie d'autorisation ; dans cet exemple, le mappage devrait être étudiant pour le VLAN 30 et professeur pour VLAN 40.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration. Ce sont les processus de vérification :

- Surveillez la page sur l'ACS ce les expositions que des clients sont authentifié.

- Connectez au DVA WLAN au groupe d'étudiants, et passez en revue l'utilitaire de connexion de WiFi de client.

- Connectez au DVA WLAN au groupe de professeur, et passez en revue l'utilitaire de connexion de WiFi de client.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

> Remarques :
>
> Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.
>
> L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.
>
> Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Utile met au point incluent **mettent au point le** *MAC d'***adresse MAC du client**, aussi bien que ces commandes trace NGWC :

- **le niveau de groupe-radio-client de set trace mettent au point**
- **MAC** *xxxx.xxxx.xxxx de* **filtre de groupe-radio-client de set trace**
- **système-filtrer-suivis de show trace**

Le suivi NGWC n'inclut pas dot1x/AAA, ainsi utilisez cette liste entière de suivis combinés pour dot1x/AAA :

- **le niveau de groupe-radio-client de set trace mettent au point**
- **le niveau d'événement du set trace wcm-dot1x mettent au point**
- **l'AAA du set trace wcm-dot1x de niveau mettent au point**
- **les événements Sans fil d'AAA de set trace de niveau mettent au point**
- **le niveau SM de noyau d'Access-session de set trace mettent au point**
- **le dot1x de méthode d'Access-session de set trace de niveau mettent au point**
- **MAC** *xxxx.xxxx.xxxx de* **filtre de groupe-radio-client de set trace**
- **MAC** *xxxx.xxxx.xxxx de* **filtre d'événement du set trace wcm-dot1x**
- **MAC** *xxxx.xxxx.xxxx de* **filtre d'AAA du set trace wcm-dot1x**
- **MAC Sans fil** *xxxx.xxxx.xxxx de* **filtre d'événements d'AAA de set trace**
- **MAC** *xxxx.xxxx.xxxx de* **filtre SM de noyau d'Access-session de set trace**

- MAC *xxxx.xxxx.xxxx de* filtre de dot1x de méthode d'Access-session de set trace
- système-filtrer-suivis de show trace

Quand l'affectation dynamique VLAN fonctionne correctement, vous devriez voir que ce type de sortie de met au point :

```
09/01/13 12:13:28.598 IST 1ccc 5933] 0021.5C8C.C761 1XA: Received Medium tag (0)
Tunnel medium type (6) and Tunnel-Type tag (0) and Tunnel-type (13)
Tunnel-Private-Id (30)
[09/01/13 12:13:28.598 IST 1ccd 5933] 0021.5C8C.C761 Tunnel-Group-Id is 30
[09/01/13 12:13:28.598 IST 1cce 5933] 0021.5C8C.C761 Checking Interface
Change - Current VlanId: 40 Current Intf: VLAN0040 New Intf: VLAN0030 New
GroupIntf:  intfChanged: 1
[09/01/13 12:13:28.598 IST 1ccf 5933] 0021.5C8C.C761 Incrementing the
Reassociation Count 1 for client (of interface VLAN0040)
 --More--         [09/01/13 12:13:28.598 IST 1cd0 5933] 0021.5C8C.C761
Clearing Address 40.40.40.2 on mobile
[09/01/13 12:13:28.598 IST 1cd1 5933] 0021.5C8C.C761 Applying new AAA override
for station  0021.5C8C.C761
[09/01/13 12:13:28.598 IST 1cd2 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
    vlanIfName: 'VLAN0030', aclName: ''

[09/01/13 12:13:28.598 IST 1cd3 5933] 0021.5C8C.C761 Clearing Dhcp state for
station  ---
[09/01/13 12:13:28.598 IST 1cd4 5933] 0021.5C8C.C761 Applying WLAN ACL policies
to client
[09/01/13 12:13:28.598 IST 1cd5 5933] 0021.5C8C.C761 No Interface ACL used for
Wireless client in WCM(NGWC)
[09/01/13 12:13:28.598 IST 1cd6 5933] 0021.5C8C.C761 Inserting AAA Override
struct for mobile
   MAC:  0021.5C8C.C761 , source 4

[09/01/13 12:13:28.598 IST 1cd7 5933] 0021.5C8C.C761 Inserting new RADIUS
override into chain for station  0021.5C8C.C761
[09/01/13 12:13:28.598 IST 1cd8 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0030', aclName: ''

 --More--         [09/01/13 12:13:28.598 IST 1cd9 5933] 0021.5C8C.C761
Applying override policy from source Override Summation:

[09/01/13 12:13:28.598 IST 1cda 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0030', aclName: ''

[09/01/13 12:13:28.598 IST 1cdb 5933] 0021.5C8C.C761 Applying local bridging
Interface Policy for station  0021.5C8C.C761  - vlan 30, interface 'VLAN0030'
[09/01/13 12:13:28.598 IST 1cdc 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds from WLAN config
[09/01/13 12:13:28.598 IST 1cdd 5933] 0021.5C8C.C761 1XA: Setting reauth timeout
to 1800 seconds
[09/01/13 12:13:28.598 IST 1cde 5933] 0021.5C8C.C761 1XK: Creating a PKC PMKID
Cache entry (RSN 1)
[09/01/13 12:13:28.598 IST 1cdf 5933] 0021.5C8C.C761 1XK: Set Link Secure: 0


[09/01/13 12:08:59.553 IST 1ae1 5933] 0021.5C8C.C761 1XA: Received Medium tag (0)
Tunnel medium type (6) and Tunnel-Type tag (0) and Tunnel-type (13)
Tunnel-Private-Id (40)
[09/01/13 12:08:59.553 IST 1ae2 5933] 0021.5C8C.C761 Tunnel-Group-Id is 40
 --More--         [09/01/13 12:08:59.553 IST 1ae3 5933] 0021.5C8C.C761
Checking Interface Change - Current VlanId: 20 Current Intf: VLAN0020 New Intf:
```

VLAN0040 New GroupIntf: intfChanged: 1
[09/01/13 12:08:59.553 IST 1ae4 5933] 0021.5C8C.C761 Applying new AAA override for station 0021.5C8C.C761
[09/01/13 12:08:59.553 IST 1ae5 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
**   vlanIfName: 'VLAN0040', aclName: ''**

[09/01/13 12:08:59.553 IST 1ae6 5933] 0021.5C8C.C761 Clearing Dhcp state for station ---
[09/01/13 12:08:59.553 IST 1ae7 5933] 0021.5C8C.C761 Applying WLAN ACL policies to client
[09/01/13 12:08:59.553 IST 1ae8 5933] 0021.5C8C.C761 No Interface ACL used for Wireless client in WCM(NGWC)
[09/01/13 12:08:59.553 IST 1ae9 5933] 0021.5C8C.C761 Inserting AAA Override struct for mobile
   MAC: 0021.5C8C.C761 , source 4

[09/01/13 12:08:59.553 IST 1aea 5933] 0021.5C8C.C761 Inserting new RADIUS override into chain for station 0021.5C8C.C761
[09/01/13 12:08:59.553 IST 1aeb 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0040', aclName: ''
 --More--
[09/01/13 12:08:59.553 IST 1aec 5933] 0021.5C8C.C761 Applying override policy from source Override Summation:

[09/01/13 12:08:59.553 IST 1aed 5933] 0021.5C8C.C761 Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
   vlanIfName: 'VLAN0040', aclName: ''

[09/01/13 12:08:59.553 IST 1aee 5933] 0021.5C8C.C761 Applying local bridging Interface Policy for station 0021.5C8C.C761 - vlan 40, interface 'VLAN0040'
[09/01/13 12:08:59.553 IST 1aef 5933] 0021.5C8C.C761 1XA: Setting reauth timeout to 1800 seconds from WLAN config
[09/01/13 12:08:59.553 IST 1af0 5933] 0021.5C8C.C761 1XA: Setting reauth timeout to 1800 seconds
[09/01/13 12:08:59.553 IST 1af1 5933] 0021.5C8C.C761 1XK: Creating a PKC PMKID Cache entry (RSN 1)