Asignación del VLAN dinámico en el Punto de acceso autónomo para el ejemplo de configuración de la versión 15.2(2) JB

Contenido

Introducción

Este documento describe el concepto de asignación del VLAN dinámico. También describe cómo configurar el Punto de acceso autónomo y a un servidor de RADIUS - el Access Control Server (ACS) ese funciona con la versión 5.2 - para asignar a los clientes del Wireless LAN (red inalámbrica (WLAN)) a un VLA N específico dinámicamente.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento de estos temas antes de que usted intente esta configuración:

- Punto de acceso autónomo
- Servidor del Authentication, Authorization, and Accounting (AAA)
- Redes inalámbricas y problemas de seguridad de red inalámbrica

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Punto de acceso 3602 que ejecuta el Cisco IOS ® Software autónomo Release15.2(2)JB
- iPhone 4S que funciona con la versión 6.1.3 como cliente
- Cisco Secure ACS que funciona con la versión 5.2
- Cisco Catalyst 3560 Series Switch

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

En la mayoría de los sistemas WLAN, cada red inalámbrica (WLAN) tiene una directiva estática que se aplique a todos los clientes asociados a un Service Set Identifier (SSID), o red inalámbrica (WLAN) en la terminología del controlador. Aunque sea potente, este método tenga limitaciones, porque requiere a los clientes asociarse a diversos SSID para heredar el diversos Calidad de Servicio (QoS) y políticas de seguridad.

Sin embargo, la solución de Cisco WLAN soporta el establecimiento de una red de la identidad. Esto permite la red haga publicidad de un solo SSID, pero permite que los usuarios específicos hereden diverso QoS, los atributos del VLA N, y/o las políticas de seguridad basadas en los credenciales de usuario.

La asignación del VLAN dinámico es una tal característica que coloca a un usuario de red inalámbrica en un VLA N específico basado en las credenciales suministradas por el usuario. Esta tarea de asignar a los usuarios a un VLA N específico es manejada por un servidor de autenticación de RADIUS, tal como el Cisco Secure ACS. Esto se puede utilizar, por ejemplo, para permitir que el host inalámbrico permanezca en el mismo VLA N que mueve dentro de una red de oficinas centrales.

Como consecuencia, cuando un cliente intenta asociarse a un Lightweight Access Point (REVESTIMIENTO) registrado a un regulador, el REVESTIMIENTO pasa las credenciales del usuario al servidor de RADIUS para la validación. Una vez que la autenticación es acertada, el servidor de RADIUS pasa ciertos atributos de la Fuerza de tareas de ingeniería en Internet (IETF) (IETF) al usuario. Estos atributos de RADIUS deciden al VLAN ID que se debe asignar al cliente de red inalámbrica. El SSID, la red inalámbrica (WLAN) en términos de regulador del Wireless LAN (WLC), del cliente no importa, porque asignan el usuario siempre a este VLAN ID predeterminado.

Los atributos del usuario de RADIUS usados para la asignación VLAN ID son:

- IETF 64 (tipo de túnel) - Esto se fija al **VLA N**.

- El IETF 65 (tipo medio del túnel) - esto se fija a **802**.
- El IETF 81 (ID de grupo privado del túnel) - esto se fija al **VLAN ID**.

El VLAN ID es 12-bits, y toma un valor entre 1 y 4094, inclusivo. Porque el Túnel-Soldado-Grupo-ID es un tipo de cadena, según lo definido en el RFC 2868 para el uso con el IEEE 802.1X, el valor del número entero VLAN ID se codifica como cadena. Cuando se envían estos atributos del túnel, es necesario completar el campo de la etiqueta.

Como se apunta en el RFC2868 , sección 3.1: **El campo de la etiqueta es un octeto de largo y se piensa proporcionar los medios de agrupar los atributos en el mismo paquete que refieren al mismo túnel.** Los valores válidos para este campo son **0x01** con **0x1F**, inclusivo. Si el campo de la etiqueta es inusitado, debe ser cero (**0x00**). Refiera al RFC 2868 para más información sobre todos los atributos de RADIUS.

Configurar

Diagrama de la red

Configuración AP

1. Navegue al **> Services (Servicios) > al VLA N GUI** para configurar los VLA N en el AP, y cree los VLA N como los requisitos especifican. Este ejemplo utiliza dos VLA N - **100** y **200**.

2. Navegue al **> Security (Seguridad) > al administrador de servidor GUI** para configurar al **servidor de RADIUS de reserva** en el AP. Ingrese el **nombre de servidor de RADIUS de reserva**, el **nombre de host o el IP Address**, y el **secreto compartido** (este secreto compartido debe corresponder con el RADIO).

3. Para ambos los VLA N, el cifrado debe hacer juego. Este ejemplo asocia el portal de la Administración del Centro de contacto del Advanced Encryption Standard (AES) de las cifras (**CCMP**) para el VLAN 100 y **200**.

4. Navegue al **> Security (Seguridad) > al administrador SSID SSID** para configurar al administrador SSID. Asocíelo a la **radio** correcta en el campo de la interfaz.

   En la **autenticación de cliente las configuraciones** defienden, marcan el **casilla "Abrir autenticación"**, y lo seleccionan **con el EAP**. Haga clic los botones de radio de los **valores por defecto del uso** para ambos campos bajo prioridades del servidor. Esto completa la

configuración AP.

Configuración de 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
```

Configuración del servidor de RADIUS

Agregue el AP como el cliente AAA en el servidor de RADIUS con el secreto compartido anteriormencionado. Cree los **usuarios** y a los **grupos de usuarios**. Este ejemplo utiliza el **estudiante** y al **profesor**.

Perfiles de la autorización

Complete estos pasos para configurar el perfil de la autorización para que el estudiante y el profesor hagan juego el **VLAN 100** y el **VLA N 200**.

1. Navegue los **perfiles del acceso > de la autorización al >Network de los elementos > de la autorización y de los permisos de la directiva**, y marque la casilla de verificación del **estudiante**.

2. En las **tareas comunes** tabule, seleccione los **parásitos atmosféricos** para el campo del VLA N ID/Name, y **100** para el valor del VLA N.

3. Bajo **autorización los perfiles** marcan la casilla de verificación del **profesor**. En las **tareas comunes** tabule, seleccione los **parásitos atmosféricos** para el campo del VLA N ID/Name, y **200** para el valor del VLA N.

Protocolos permitidos

1. Navegue a las **políticas de acceso > al acceso mantiene > acceso de red predeterminada**, selecciona la **ficha general**, y ingresa los detalles para el nombre y la descripción. Bajo

directiva Sturcture, marque los cuadros de la **identidad** y de **comprobación de autorización**.

2. En los **protocolos permitidos** tabule, marque las casillas de verificación de los **Protocolos de autenticación**, según lo representado aquí.

Reglas de la identidad

Para permitir protegió a los usuarios del protocolo extensible authentication (PEAP), navega a las **políticas de acceso > al acceso mantiene > acceso > identidad de red predeterminada**. Marque la casilla de verificación al lado de **Peap**.

Reglas de la autorización

Para asociar al estudiante y el profesor a los perfiles de la autorización para el estudiante y el profesor para el VLAN 100 y 200, navegue a las **políticas de acceso > al acceso mantiene > acceso > autorización de red predeterminada**.

Verificación

Estas imágenes ilustran cómo verificar su configuración con el uso de su iPhone. Para verificar, conecte su iPhone con el SSID DVAAP con el profesor y los grupos de estudiantes, y asegúrese de que la visualización correcta de los IP Addresses.

Troubleshooting

Complete estos pasos para resolver problemas su configuración.

1. Para eliminar la posibilidad que los problemas del Radiofrecuencia (RF) previenen la autenticación satisfactoria, fije el método en el SSID **para abrirse** para inhabilitar temporalmente la autenticación.

2. Del GUI en la página del **administrador SSID**, desmarque **Casilla de verificación EAP de la red.**, y marque **abierto**.

3. Del CLI, ingrese la **autenticación abierta** y los **comandos no authentication network-eap eap_methods**. Si el cliente se asocia con éxito, el RF no contribuye al problema de asociación.

4. Verifique que todas las contraseñas secretas compartidas estén sincronizadas. Estas líneas deben contener la misma contraseña del secreto compartido:
clave del acct-puerto x del auténtico-puerto x del host de servidor RADIUS x.x.x.x <shared_secret>clave NAS x.x.x.x <shared_secret>

5. Quite cualquier grupo de usuarios y sus configuraciones asociadas. Los conflictos pueden ocurrir a veces entre los grupos de usuarios definidos por el AP y los grupos de usuarios en el dominio.

Comandos de Debug

> **Note**: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Aquí está una lista de comandos debug útiles.

- **authenticator todo aaa del dot11 del debug** - Este debug muestra a diversas negociaciones que va un cliente a través mientras que el cliente se asocia y autentica con el 802.1x o el proceso EAP desde la perspectiva del authenticator (AP). Este debug fue introducido en el Cisco IOS Software Release 12.2(15)JA. Este **dot1x todo aaa del dot11 del debug de los** obsoletes del comando en esto y posterior versiones.
- **autenticación de RADIUS del debug** - Este debug muestra las negociaciones RADIUS entre el servidor y el cliente, que, en este caso, son el AP.
- **cliente del servidor local del radio del debug** - Este debug muestra la autenticación del cliente desde la perspectiva del servidor de RADIUS.

Aquí tiene un ejemplo:

```
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
```