

Asignación del VLAN dinámico con el servidor de RADIUS ACS 5.2 y el ejemplo de configuración del WLC

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Asignación del VLAN dinámico con un servidor de RADIUS](#)

[Configurar](#)

[Diagrama de la red](#)

[Suposición](#)

[Pasos de configuración](#)

[Configure al servidor de RADIUS](#)

[Configure a los recursos de red](#)

[Configure a los usuarios](#)

[Defina los elementos de la directiva](#)

[Aplique las políticas de acceso](#)

[Configure el WLC](#)

[Configure el WLC con los detalles del servidor de autenticación](#)

[Configure las interfaces dinámicas \(los VLAN\)](#)

[Configure los WLAN \(el SSID\)](#)

[Configure la utilidad del cliente de red inalámbrica](#)

[Verificación](#)

[Verifique Student-1](#)

[Verifique Teacher-1](#)

[Troubleshooting](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

[Introducción](#)

Este documento presenta el concepto de asignación de VLAN dinámica. También describe cómo configurar el controlador de LAN inalámbrico (WLC) y un servidor de RADIUS -Access Control Server (ACS) que ejecuta la versión 5.2- para asignar clientes de LAN inalámbricos (WLAN) a una VLAN específica dinámicamente.

prerrequisitos

Requisitos

Asegurese que usted cumple estos requisitos antes de que usted intente esta configuración:

- Tenga un conocimiento básico del WLC y de los Puntos de acceso ligeros (los revestimientos)
- Tenga un conocimiento funcional del servidor de AAA
- Tenga un conocimiento completo de las redes inalámbricas y de los problemas de seguridad de red inalámbrica

Componentes Utilizados

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

- WLC de Cisco 5508 que funciona con la versión de firmware 7.0.220.0
- REVESTIMIENTO de las Cisco 3502 Series
- Supplicant del natural de Microsoft Windows 7 con la versión del driver 14.3 de Intel 6300-N
- Cisco Secure ACS que funciona con la versión 5.2
- Cisco 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.

Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

Asignación del VLAN dinámico con un servidor de RADIUS

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 diverso QoS y las 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 VLAN, 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 VLAN específico basado en las credenciales suministradas por el usuario. Esta tarea de asignar a los usuarios a un VLAN específico es manejada por un servidor de

autenticación de RADIUS, tal como 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 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 (red inalámbrica (WLAN), en términos de 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) - Fije esto al **VLA N**.
- IETF 65 (tipo medio del túnel) - fije esto a **802**.
- IETF 81 (ID de grupo privado del túnel) - fije esto al VLAN ID.

El VLAN ID es 12-bits, y toma un valor entre 1 y 4094, inclusivo. Porque el Túnel-Soldado-Grupo-ID está de tipo string, 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](#)

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Note: Utilice la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos utilizados en esta sección.

[Diagrama de la red](#)

En este documento, se utiliza esta configuración de red:

Éstos son los detalles de la configuración de los componentes usados en este diagrama:

- La dirección IP del servidor ACS (RADIUS) es 192.168.150.24.
- La Administración y el direccionamiento de la interfaz del AP manager del WLC es 192.168.75.44.
- Los servidores DHCP dirigen 192.168.150.25.
- El VLA N 253 y el VLA N 257 se utilizan en esta configuración. Student-1 se configura para la colocación en el VLA N 253 y Teacher-1 es configurado para la colocación en el VLA N 257 por el servidor de RADIUS cuando ambos usuarios conectan con el mismo SSID "goa".VLA N 253: 192.168.153.x/24. Gateway: 192.168.153.1VLA N 257: 192.168.157.x/24. Gateway:

192.168.157.1VLA N 75: 192.168.75.x/24. Gateway: 192.168.75.1

- Este documento utiliza el 802.1x con el PEAP como el mecanismo de seguridad.**Note:** Cisco recomienda que usted utiliza los métodos de autenticación avanzados, tales como EAP-FAST y autenticación EAP-TLS, para asegurar la red inalámbrica (WLAN).

Suposición

- El Switches se configura para todos los VLA N de la capa 3.
- Asignan el servidor DHCP un alcance de DHCP.
- La Conectividad de la capa 3 existe entre todos los dispositivos en la red.
- El REVESTIMIENTO se une a ya al WLC.
- Cada VLA N tiene máscara de /24.
- El ACS 5.2 tiene un certificado autofirmado instalado.

Pasos de configuración

Esta configuración se separa en tres pasos de alto nivel:

1. [Configure al servidor de RADIUS.](#)
2. [Configure el WLC.](#)
3. [Configure la utilidad del cliente de red inalámbrica.](#)

Configure al servidor de RADIUS

La configuración del servidor de RADIUS se divide en cuatro pasos:

1. [Recursos de red de la configuración.](#)
2. [Usuarios de la configuración.](#)
3. [Defina los elementos de la directiva.](#)
4. [Aplique las políticas de acceso.](#)

El ACS 5.x es un Sistema de control de acceso del policy basado. Es decir, el ACS 5.x utiliza un modelo basado en las reglas de la directiva en vez del modelo basado en el grupo usado en las versiones 4.x.

El modelo basado en las reglas de la directiva ACS 5.x proporciona un control de acceso más potente y más flexible comparado al más viejo acercamiento basado en el grupo.

En el más viejo modelo basado en el grupo, un grupo define la directiva porque contiene y ata juntos tres tipos de información:

- Información de identidad - Esta información se puede basar en la calidad de miembro en los grupos AD o LDAP o una asignación estática para los usuarios de ACS internos.
- Otras restricciones o condiciones - Restricciones de tiempo, restricciones del dispositivo, y así sucesivamente.
- Permisos - Niveles de privilegio del [®] de los VLA N o del Cisco IOS.

El modelo de la directiva ACS 5.x se basa en las reglas de la forma:

- Si entonces resulta la condición

Por ejemplo, utilizamos la información descrita para el modelo basado en el grupo:

- Si identidad-condición, autorización-perfil de la restricción-condición entonces.

Como consecuencia, esto nos da la flexibilidad para limitar bajo qué condiciones permiten el usuario que accedan la red así como se permite qué nivel de la autorización cuando se cumplen las condiciones específicas.

Recursos de red de la configuración

Este procedimiento explica cómo agregar el WLC como cliente AAA en el servidor de RADIUS de modo que el WLC pueda pasar los credenciales de usuario al servidor de RADIUS.

Complete estos pasos:

1. Del ACS GUI, vaya a los **recursos de red** > a los **grupos de dispositivos de red** > a la **ubicación**, y el tecleo **crea** (en la parte inferior).
2. Agregue los campos obligatorios, y el tecleo **somete**. Usted ahora verá esta pantalla:
3. **El tipo de dispositivo del tecleo > crea**.
4. Haga clic en Submit (Enviar). Usted ahora verá esta pantalla:
5. Vaya a los **recursos de red** > a los **dispositivos de red y a los clientes AAA**.
6. El tecleo **crea**, y completa los detalles como se muestra aquí:
7. Haga clic en Submit (Enviar). Usted ahora verá esta pantalla:

Usuarios de la configuración

En esta sección, usted creará a los usuarios locales en el ACS (Student-1 y Teacher-1). Student-1 se asigna al grupo de los “estudiantes” y Teacher-1 se asigna al grupo de los “profesores”.

1. Vaya a los **usuarios y la identidad salva** > los **grupos de la identidad** > **crea**.
2. Una vez que usted tecleo **somete**, la página parecerá esto:
3. Cree y asigne a usuarios Student-1 y Teacher-1 a sus grupos correspondientes.
4. Haga clic a los **usuarios y la identidad salva** > los **grupos de la identidad** > **Users** > **crea**.
5. Semejantemente, cree Teacher-1. La pantalla parecerá esto:

Defina los elementos de la directiva

Complete estos pasos para definir los atributos IETF para los usuarios:

1. Vaya a los **elementos** > a la **autorización de la directiva y los permisos** > los **perfiles del acceso a la red** > de la **autorización** > **crean**.
2. De la lengüeta común de las tareas:
3. Agregue estos atributos IETF: Tipo de Túnel = 64 = VLA NTúnel-Media-tipo = 802Túnel-Soldado-Grupo-ID = 253 (Student-1) y 257 (Teacher-1) Para los estudiantes del grupo: Para los profesores del grupo:
4. Una vez que se agregan ambos atributos, la pantalla parecerá esto:

Aplique las políticas de acceso

Complete estos pasos para seleccionar qué métodos de autenticación deben ser utilizados y cómo las reglas deben ser configuradas (basado en los pasos anteriores):

1. Va a las **políticas de acceso** > al **acceso mantiene** > el **acceso de red predeterminada** > **edita: "Acceso de red predeterminada"**.
2. Seleccione que el método EAP usted como los clientes de red inalámbrica autenticaría. En este ejemplo, utilizamos **PEAP- MSCHAP-V2**.
3. Haga clic en Submit (Enviar).
4. Verifique al grupo de la identidad que usted ha seleccionado. En este ejemplo, utilizamos a los **usuarios internos**, que creamos en el ACS. Guarde los cambios.
5. Para verificar el perfil de la autorización, vaya a las **políticas de acceso** > al **acceso mantiene** > **acceso** > **autorización de red predeterminada**. Usted puede personalizar bajo qué condiciones usted no prohibirá a acceso del usuario a la red y qué perfil de la autorización (atributos) usted pasará autenticado una vez. Este granularity está solamente disponible en ACS5.x. En este ejemplo, seleccionamos la **ubicación**, el **tipo de dispositivo**, el **protocolo**, el **grupo de la identidad**, y el **método de autenticación EAP**.
6. Haga Click en OK, y **cambios de la salvaguardia**.
7. El siguiente paso es crear una regla. Si no se define ningunas reglas, no prohíben el cliente el acceso sin ningunas condiciones.El tecleo **crea** > **Rule-1**. Esta regla está para Student-1.
8. Semejantemente, cree una regla para Teacher-1. Haga clic los **cambios de la salvaguardia**.La pantalla parecerá esto:
9. Ahora definiremos las reglas de selección del servicio. Utilice esta página para configurar una directiva simple o basada en las reglas determinar que mantengan para aplicarse a los pedidos entrantes. En este ejemplo, se utiliza una directiva basada en las reglas.

[Configure el WLC](#)

La configuración requiere estos pasos:

1. [Configure el WLC con los detalles del servidor de autenticación.](#)
2. [Configure las interfaces dinámicas \(VLA N\).](#)
3. [Configure los WLAN \(SSID\).](#)

[Configure el WLC con los detalles del servidor de autenticación](#)

Es necesario configurar el WLC así que puede comunicar con el servidor de RADIUS para autenticar a los clientes, y también para cualquier otra transacción.

Complete estos pasos:

1. Del regulador GUI, haga clic la **Seguridad**.
2. Ingrese el IP Address del servidor de RADIUS y de la clave secreta compartida usados entre el servidor de RADIUS y el WLC.Esta clave secreta compartida debe ser lo mismo que la que está configurada en el servidor de RADIUS.

[Configure las interfaces dinámicas \(los VLA N\)](#)

Este procedimiento describe cómo configurar las interfaces dinámicas en el WLC. Según lo

explicado anterior en este documento, el VLAN ID especificado bajo atributo del Túnel-Soldado-grupo ID del servidor de RADIUS debe también existir en el WLC.

En el ejemplo, Student-1 se especifica con el Túnel-Soldado-grupo ID de 253 (VLAN =253) en el servidor de RADIUS. Semejantemente, Teacher-1 se especifica con el Túnel-Soldado-grupo ID de 257 (VLAN =257) en el servidor de RADIUS. Vea la sección de los [atributos IETF RADIUS de la ventana de la configuración de usuario](#).

Complete estos pasos:

1. La interfaz dinámica se configura del regulador GUI, en la ventana del **regulador > de las interfaces**.
2. Haga clic en Apply (Aplicar).Esto le lleva a la ventana del editar de esta interfaz dinámica (VLAN N 253 aquí).
3. Ingrese el IP Address y el default gateway de esta interfaz dinámica.
4. Haga clic en Apply (Aplicar).
5. Semejantemente, crearemos una interfaz dinámica para el VLAN N 257 para Teacher-1.
6. Las interfaces configuradas parecerán esto:

[Configure los WLAN \(el SSID\)](#)

Complete estos pasos para configurar los WLAN en el WLC:

1. Del regulador GUI, van a los **WLAN > crean nuevo** para crear una nueva red inalámbrica (WLAN). Se visualiza la nueva ventana del WLAN.
2. Ingrese la información del ID DE WLAN y WLAN SSID.Usted puede ingresar cualquier nombre como el WLAN SSID. Este ejemplo utiliza el **goa** como la red inalámbrica (WLAN) SSID.
3. El tecleo **se aplica** para ir a la ventana del editar del goa de la red inalámbrica (WLAN).
4. Habilite la opción de la **invalidación de la permit AAA** en el regulador para cada red inalámbrica (WLAN) (SSID) configurada. La opción de la invalidación de la permit AAA de una red inalámbrica (WLAN) permite que usted configure la red inalámbrica (WLAN) para el establecimiento de una red de la identidad. Permite que usted aplique marcar con etiqueta, QoS, y los ACL del VLAN a los clientes individuales basados en los atributos de RADIUS vueltos del servidor de AAA. En este ejemplo, se utiliza para asignar un VLAN a los clientes.La mayor parte de la configuración para permitir la invalidación AAA se hace en el servidor de RADIUS. Habilitar este parámetro permite que el regulador valide los atributos vueltos por el servidor de RADIUS. El regulador entonces aplica estos atributos a sus clientes.**Note:** Cuando asocian al grupo de interfaces a una red inalámbrica (WLAN) y los clientes conectan con la red inalámbrica (WLAN), el cliente no consigue la dirección IP en un estilo de ordenamiento cíclico. La invalidación AAA con el grupo de interfaces no se soporta.

[Configure la utilidad del cliente de red inalámbrica](#)

En nuestro probar cliente, estamos utilizando el supplicant nativo de Windows 7 con un indicador luminoso LED amarillo de la placa muestra gravedad menor de Intel 6300-N que funciona con la versión del driver 14.3. Se recomienda para probar usando los últimos drivers de los vendedores.

Complete estos pasos para crear un perfil en Windows cero Config (WZC):

1. Vaya al **panel de control** > a la **red y Internet** > **maneja las redes inalámbricas**.
 2. Haga clic la lengüeta del **agregar**.
 3. El teclado **crea manualmente un perfil de la red**.
 4. Agregue los detalles según lo configurado en el WLC. **Note:** El SSID es con diferenciación entre mayúsculas y minúsculas.
 5. Haga clic en Next (Siguiente).
 6. **Configuraciones de la conexión del cambio del teclado** para comprobar las configuraciones con minuciosidad.
 7. En este ejemplo, no estamos validando el certificado de servidor. Si usted marca este cuadro y no puede conectar, intente inhabilitar la característica y la prueba otra vez.
 8. Alternativamente, usted puede utilizar sus credenciales de Windows para iniciar sesión. Sin embargo, en este ejemplo no vamos a utilizar eso. Click OK.
 9. **Configuraciones avanzadas del teclado** para configurar el nombre de usuario y contraseña.
 10. Una vez que usted ha acabado de probar Student-1, pruebe Teacher-1. Click OK.
- Su utilidad de cliente está lista ahora para conectar.

Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Verifique Student-1

Del WLC GUI, vaya al **monitor** > a los **clientes**, y seleccione la dirección MAC.

Stats del WLC RADIUS:

```
(Cisco Controller) >show radius auth statistics
Authentication Servers:
Server Index..... 1
Server Address..... 192.168.150.24
Msg Round Trip Time..... 1 (msec)
First Requests..... 8
Retry Requests..... 0
Accept Responses..... 1
Reject Responses..... 0
Challenge Responses..... 7
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0
```

Registros ACS:

1. Complete estos pasos para ver las cuentas del golpe: Si usted marca los registros en el plazo de 15 minutos de autenticación, asegúrese de restaurar la cuenta del golpe. Usted tiene una lengüeta para la **cuenta del golpe** en la parte inferior de la misma página.
2. **La supervisión del teclado y los informes** y una nueva ventana emergente aparece. Vaya a las

autenticaciones – Radio – Hoy. Usted puede también hacer clic los **detalles** para verificar que mantienen la regla de selección eran aplicados.

[Verifique Teacher-1](#)

Del WLC GUI, vaya al **monitor** > a los **clientes**, y seleccione la dirección MAC.

El ACS registra:

1. Complete estos pasos para ver las cuentas del golpe: Si usted marca los registros en el plazo de 15 minutos de autenticación, asegúrese le restaurar la cuenta del GOLPE. Usted tiene una lengüeta para la **cuenta del golpe** en la parte inferior de la misma página.
2. **La supervisión del teclado y los informes** y una nueva ventana emergente aparece. Vaya a las **autenticaciones – Radio – Hoy**. Usted puede también hacer clic los **detalles** para verificar que mantienen la regla de selección eran aplicados.

[Troubleshooting](#)

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

[Comandos para resolución de problemas](#)

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Note: Consulte [Información Importante sobre Comandos de Debug](#) antes de usar un **comando debug**.

1. Si usted experimenta cualesquiera problemas, publique estos comandos en el WLC: *el <mac del cliente del debug agrega del client>debug aaa all enable muestre el addr> del <mac del detalle del cliente* - Verifique el estado del administrador de la directiva. **muestre las estadísticas del auth del radio** - Verifique la razón del error. **haga el debug de neutralización- todo** - Apague los debugs. **borre las estadísticas del radio del cese de alarma del auth del radio stats** sobre el WLC.
2. Verifique abre una sesión el ACS y observa la razón del error.

[Información Relacionada](#)

- [Asignación del VLAN dinámico con el servidor de RADIUS ACS 4.1 y el ejemplo de la configuración de controlador del Wireless LAN](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)