Preguntas Frecuentes sobre el Diseño y las Funciones de Wireless LAN Controller (WLC)

Contenido

Introducción

Este documento proporciona información sobre las preguntas más frecuentes (FAQ) sobre el diseño y las funciones disponibles con un Controlador de LAN inalámbrica (WLC).

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Preguntas frecuentes de diseño

P. ¿Cómo configuro el switch para conectar con el WLC?

A. Configure el puerto del switch, al cual el WLC está conectado, como un puerto troncal IEEE 802.1Q. Asegúrese de que sólo se permiten las VLAN necesarias en el switch. Generalmente, la administración y la interfaz AP-Manager del WLC se dejan sin etiqueta. Esto significa que asumen la VLAN nativa del switch conectado. Esto no es necesario. Puede asignar una VLAN independiente a estas interfaces. Para obtener más información, consulte la sección *Configuración del Switch para el WLC* de Ejemplo de Configuración Básica del Controlador de LAN Inalámbrica y el Punto de Acceso Ligero.

P. ¿Todo el tráfico de red desde y hacia un túnel de cliente WLAN a través de un controlador de LAN inalámbrica (WLC) una vez que el punto de acceso (AP) se registra con el controlador?

R. Cuando el AP se une a un WLC, se forma un túnel de control y abastecimiento de los puntos de acceso inalámbricos (CAPWAP) entre los dos dispositivos. Todo el tráfico, que incluye todo el tráfico del cliente, se envía a través del túnel CAPWAP.

La única excepción a esto es cuando un AP está en modo de hybrid-REAP. Los puntos de acceso de hybrid-REAP pueden conmutar el tráfico de datos del cliente localmente y realizar la autenticación del cliente localmente cuando se pierde su conexión con el controlador. Cuando se conectan al controlador, también pueden enviar el tráfico de vuelta al controlador.

P. ¿Puedo instalar puntos de acceso ligeros (LAP) en una oficina remota e instalar un controlador de LAN inalámbrica (WLC) de Cisco en mi sede central? ¿El LWAPP/CAPWAP funciona sobre una WAN?

R. Sí, puede tener los WLC a través de la WAN de los AP. LWAPP/CAPWAP funciona sobre una WAN cuando los LAPs se configuran en el modo Remote Edge AP (REAP) o Hybrid Remote Edge AP (H-REAP). Cualquiera de estos modos permite el control de un AP por un controlador remoto que se conecta a través de un link WAN. El tráfico se enlaza localmente al link LAN, lo que evita la necesidad de enviar innecesariamente tráfico local a través del link WAN. Esta es precisamente una de las mayores ventajas de tener WLCs en su red inalámbrica.

Nota: No todos los puntos de acceso ligeros admiten estos modos. Por ejemplo, el modo H-REAP se soporta solamente en los LAPs 1131, 1140, 1242, 1250 y AP801. El modo REAP se soporta solamente en el AP 1030, pero los AP 1010 y 1020 no soportan REAP. Antes de que planee implementar estos modos, verifique para determinar si los LAPs lo soportan. Los Cisco IOS® Software AP (Autonomous AP) que se han convertido a LWAPP no soportan REAP.

P. ¿Cómo funcionan los modos REAP y H-REAP?

R. En el modo **REAP**, todo el tráfico de control y administración, que incluye el tráfico de autenticación, se tuneliza de nuevo al WLC. Pero todo el tráfico de datos se conmuta localmente dentro de la LAN de la oficina remota. Cuando se pierde la conexión al WLC, todas las WLANs se terminan excepto la primera WLAN (WLAN1). Se conservan todos los clientes que están asociados actualmente a esta WLAN. Para permitir que los nuevos clientes autentiquen y reciban correctamente el servicio en esta WLAN durante el tiempo de inactividad, configure el método de autenticación para esta WLAN como WEP o WPA-PSK de modo que la autenticación se realice localmente en el REAP. Para obtener más información sobre la implementación de REAP, consulte la Guía de implementación de REAP en la sucursal.

En el modo **H-REAP**, un punto de acceso tuneliza el tráfico de control y administración, que incluye el tráfico de autenticación, de nuevo al WLC. El tráfico de datos de una WLAN se puentea localmente en la oficina remota si la WLAN se configura con el switching local de H-REAP, o el tráfico de datos se envía de vuelta al WLC. Cuando se pierde la conexión al WLC, todas las WLANs se terminan excepto las primeras ocho WLANs configuradas con el switching local de H-REAP. Se conservan todos los clientes que están asociados actualmente a estas WLAN. Para permitir que los nuevos clientes autentiquen y reciban correctamente el servicio en estas WLAN dentro del tiempo de inactividad, configure el método de autenticación para esta WLAN como WEP, WPA PSK o WPA2 PSK de modo que la autenticación se realice localmente en H-REAP.

Para obtener más información sobre H-REAP, consulte la Guía de diseño e implementación de H-REAP.

P. ¿Cuál es la diferencia entre Remote-Edge AP (REAP) e Hybrid-REAP (H-REAP)?

R. **REAP no soporta etiquetado IEEE 802.1Q VLAN.** Como tal, no admite varias VLAN. El tráfico de todos los identificadores de conjunto de servicios (SSID) termina en la misma subred, pero H-REAP admite etiquetado IEEE 802.1Q VLAN. El tráfico de cada SSID se puede segmentar en una VLAN única.

Cuando se pierde la conectividad con el WLC, es decir, en el modo autónomo, REAP sirve

solamente una WLAN, es decir, la WLAN primera. Todas las demás WLAN están desactivadas. En H-REAP, se admiten hasta 8 WLAN durante el tiempo de inactividad.

Otra diferencia importante es que, en el modo REAP, el tráfico de datos solo se puede conectar localmente. No se puede volver a conmutar a la oficina central, pero, en el modo H-REAP, tiene la opción de volver a conmutar el tráfico a la oficina central. El tráfico de las WLANs configuradas con switching local de H-REAP se conmuta localmente. El tráfico de datos de otras WLAN se conmuta de nuevo a la oficina central.

Consulte Ejemplo de Configuración de Remote-Edge AP (REAP) con Lightweight AP y Wireless LAN Controllers (WLCs) para obtener más información sobre REAP.

Consulte Configuración de Hybrid REAP para obtener más información sobre H-REAP.

P. ¿Cuántas WLAN se soportan en el WLC?

R. Desde la versión de software 5.2.157.0, el WLC ahora puede controlar hasta 512 WLAN para los puntos de acceso ligeros. Cada WLAN tiene un ID de WLAN independiente (1 a 512), un nombre de perfil independiente y un SSID de WLAN, y se le pueden asignar políticas de seguridad únicas. El controlador publica hasta 16 WLAN en cada punto de acceso conectado, pero puede crear hasta 512 WLAN en el controlador y, a continuación, publicar selectivamente estas WLAN (mediante grupos de puntos de acceso) en diferentes puntos de acceso para gestionar mejor la red inalámbrica.

Nota: los controladores Cisco 2106, 2112 y 2125 solo admiten hasta 16 WLAN.

Nota: Para obtener información detallada sobre las pautas para configurar WLANs en WLCs, lea la sección Creación de WLANs de la Guía de Configuración del Controlador de LAN Inalámbrica de Cisco, Versión 7.0.116.0.

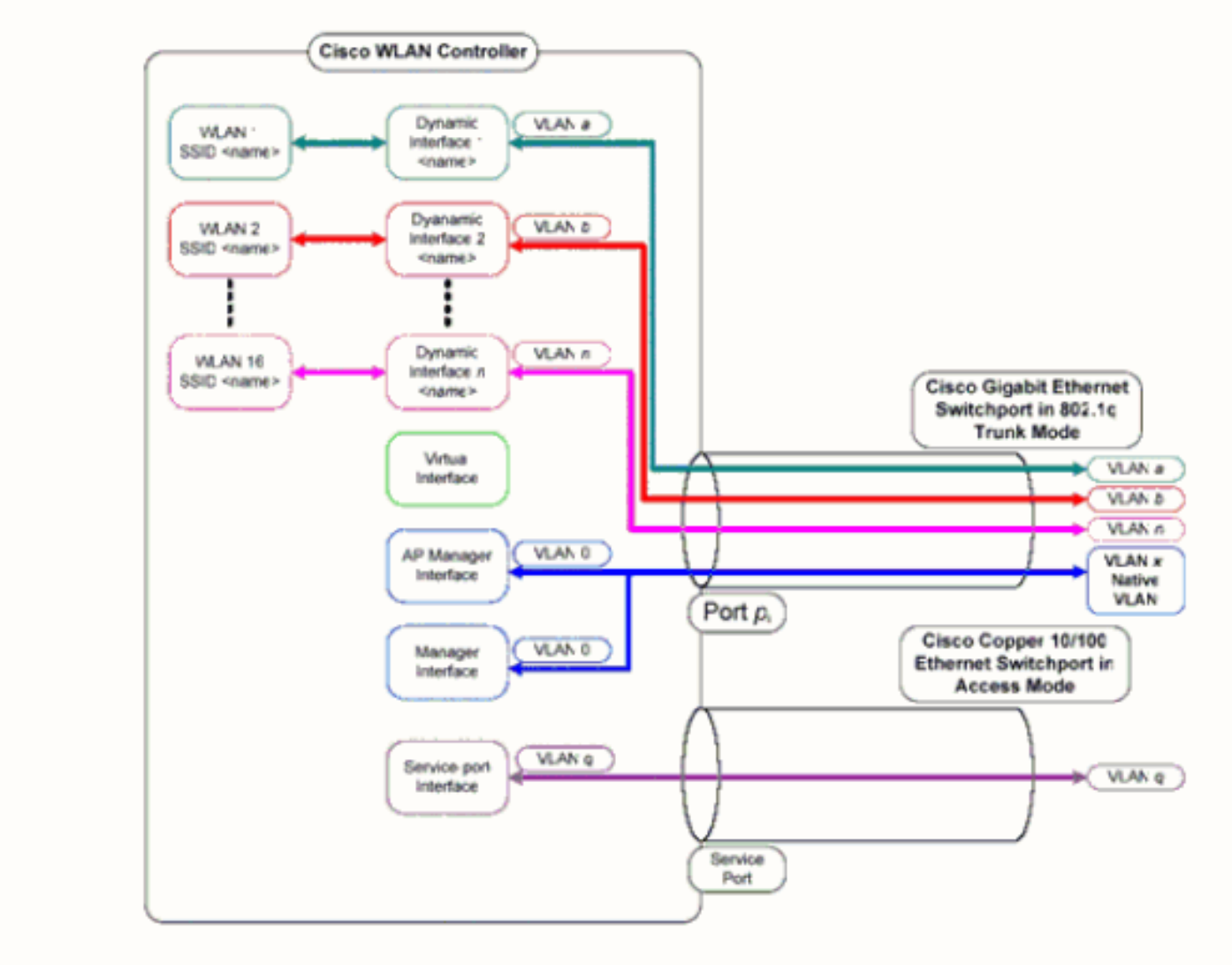
P. ¿Cómo puedo configurar las VLAN en mi controlador de LAN inalámbrica (WLC)?

R. En el WLC, las VLAN están ligadas a una interfaz configurada en una subred IP única. Esta interfaz está asignada a una WLAN. A continuación, los clientes que se asocian a esta WLAN pertenecen a la VLAN de la interfaz y se les asigna una dirección IP de la subred a la que pertenece la interfaz. Para configurar las VLAN en su WLC, complete el procedimiento en el Ejemplo de Configuración de VLAN en Controladores de LAN Inalámbricos.

P. Hemos aprovisionado dos WLAN con dos interfaces dinámicas diferentes. Cada interfaz tiene su propia VLAN, que es diferente a la VLAN de la interfaz de administración. Esto parece funcionar, pero no hemos aprovisionado los puertos troncales para permitir las VLAN que utilizan nuestras WLAN. ¿El punto de acceso (AP) etiqueta los paquetes con la VLAN de la interfaz de administración?

R. El AP no etiqueta los paquetes con la VLAN de la interfaz de administración. El AP encapsula los paquetes de los clientes en el protocolo ligero AP (LWAPP)/CAPWAP, y después pasa los paquetes en el WLC. El WLC entonces quita el encabezado LWAPP/CAPWAP y reenvía los paquetes al gateway con la etiqueta VLAN apropiada. La etiqueta VLAN depende de la WLAN a la que pertenece el cliente. El WLC depende del gateway para rutear los paquetes a su destino. Para poder pasar el tráfico para varias VLAN, debe configurar el switch de link ascendente como

un puerto trunk. Este diagrama explica cómo funcionan las VLAN con los controladores:



P. ¿Qué dirección IP del WLC se utiliza para la autenticación con el servidor AAA?

R. El WLC utiliza la dirección IP de la interfaz de administración para cualquier mecanismo de autenticación (Capa 2 o Capa 3) que involucre un servidor AAA. Para obtener más información sobre los puertos e interfaces en el WLC, consulte la sección *Configuración de Puertos e Interfaces* de la Guía de Configuración del Controlador de LAN Inalámbrica de Cisco, Versión 7.0.116.0.

P. Tengo diez puntos de acceso ligeros (LAP) Cisco serie 1000 y dos controladores de LAN inalámbrica (WLC) en la misma VLAN. ¿Cómo puedo registrar seis LAPs para asociar al WLC1, y los otros cuatro LAPs para asociar al WLC2?

R. El LWAPP/CAPWAP permite la redundancia dinámica y el balanceo de carga. Por ejemplo, si especifica más de una dirección IP para la opción 43, un LAP envía solicitudes de detección de LWAPP/CAPWAP a cada una de las direcciones IP que recibe el AP. En la respuesta de detección de LWAPP/CAPWAP del WLC, el WLC incrusta esta información:

- Información sobre la carga del LAP actual, que se define como el número de LAP que se unen al WLC en el momento
- La capacidad del LAP

- El número de clientes inalámbricos conectados al WLC

El LAP entonces intenta unirse al WLC menos cargado, que es el WLC con la mayor capacidad disponible del LAP. Además, después de que un LAP se une a un WLC, el LAP aprende las direcciones IP de los otros WLC en el grupo de la movilidad de su WLC unido.

Una vez que un LAP se une a un WLC, usted puede hacer que el LAP se una a un WLC específico dentro de su próximo reinicio. Para hacer esto, asigne un WLC primario, secundario, y terciario para un LAP. Cuando el LAP se reinicia, busca el WLC primario y se une a ese WLC independiente de la carga en ese WLC. Si el WLC primario no responde, busca el secundario y, si no responde, el terciario. Para obtener más información sobre cómo configurar el WLC primario para un LAP, consulte la sección *Asignación de Controladores Primarios, Secundarios y Terciarios para el Lightweight AP* del Ejemplo de Configuración de Failover de Controlador WLAN para Lightweight Access Points.

P. ¿Cuáles son las características que no se soportan en los 2100 Series Wireless LAN Controllers (WLCs)?

R. Estas características de hardware no son compatibles con los controladores de la serie 2100:

- Puerto de servicio (interfaz Ethernet de 10/100 Mb/s de gestión fuera de banda independiente)

Estas características de software no son compatibles con los controladores de la serie 2100:

- Terminación VPN (tal como IPSec y L2TP)
- Terminación de los túneles del controlador de invitado (se admite el origen de los túneles del controlador de invitado)
- Lista del servidor Web de la autenticación del Web externa
- Layer 2 LWAPP
- Spanning Tree
- Reflejo de Puerto
- Cranita
- Fortaleza
- AppleTalk
- Contratos de ancho de banda de QoS por usuario
- Traspaso IPv6
- Agregación de enlaces (LAG)
- Modo de unidifusión multidifusión
- Acceso de invitado por cable

P. ¿Qué funciones no son compatibles con los controladores de la serie 5500?

R. Estas funciones de software no son compatibles con los controladores de la serie 5500:

- Interfaz de administrador de AP estática**Nota:** Para los controladores de la serie 5500, no es necesario configurar una interfaz de administrador de AP. La interfaz de administración actúa como una interfaz de administrador de AP de forma predeterminada, y los puntos de acceso pueden unirse en esta interfaz.
- Tunelización de movilidad asimétrica
- Spanning Tree Protocol (STP)

- Reflejo de Puerto
- Compatibilidad con lista de control de acceso (ACL) de capa 2
- Terminación VPN (tal como IPSec y L2TP)
- opción de paso a través de VPN
- Configuración del puente 802.3, AppleTalk y el protocolo punto a punto sobre Ethernet (PPPoE)

P. ¿Qué funciones no son compatibles con las redes de malla?

R. Estas características del controlador no se soportan en las redes de malla:

- Asistencia en varios países
- CAC basado en carga (las redes de malla solo admiten CAC basado en ancho de banda o estático).
- Alta disponibilidad (latido rápido y temporizador de conexión de detección principal)
- Autenticación EAP-FASTv1 y 802.1X
- El punto de acceso se une a la prioridad (los puntos de acceso de malla tienen una prioridad fija).
- Certificado con importancia local
- Servicios basados en la ubicación

P. ¿Cuál es el período de validez de los certificados instalados por el fabricante (MIC) en un controlador de LAN inalámbrica y de los certificados de punto de acceso ligero?

R. El período de validez de un MIC en un WLC es de 10 años. El mismo período de validez de 10 años se aplica a los certificados del punto de acceso ligero desde su creación (ya sea un MIC o un certificado autofirmado (SSC)).

P. Tengo dos controladores de LAN inalámbrica (WLC) denominados WLC1 y WLC2 configurados dentro del mismo grupo de movilidad para conmutación por fallas. Mi Lightweight Access Point (LAP) está registrado actualmente con el WLC1. Si el WLC1 falla, ¿el AP registrado para el reinicio del WLC1 durante su transición hacia el WLC superviviente (WLC2)? Además, durante este failover, ¿el cliente WLAN pierde la conectividad WLAN con el LAP?

R. Sí, el LAP cancela el registro del WLC1, reinicia, y después vuelve a registrarse con el WLC2, si el WLC1 falla. Debido a que el LAP se reinicia, los clientes WLAN asociados pierden la conectividad con el LAP que se reinicia. Para obtener información relacionada, consulte Equilibrio de carga de AP y reserva de AP en redes inalámbricas unificadas.

P. ¿El roaming depende del modo de protocolo de punto de acceso ligero (LWAPP) para el que está configurado el controlador de LAN inalámbrica (WLC)? ¿Puede un WLC que opera en el modo LWAPP de la capa 2 realizar el roaming de la capa 3?

R. Mientras la agrupación de movilidad en los controladores esté configurada correctamente, el roaming del cliente debería funcionar bien. El modo LWAPP (ya sea Capa 2 o Capa 3) no afecta la itinerancia. Sin embargo, se recomienda utilizar el LWAPP de la capa 3 siempre que sea

posible.

Nota: El modo de la capa 2 es soportado solamente por los Cisco 410x y 440x Series de los WLC y los Cisco 1000 Series Access Points. El LWAPP de la capa 2 no es soportado por el otro controlador del Wireless LAN y las plataformas del Lightweight Access Point.

P. ¿Cuál es el proceso de roaming que se produce cuando un cliente decide desplazarse a un nuevo punto de acceso (AP) o controlador?

R. Esta es la secuencia de eventos que ocurre cuando un cliente se traslada a un nuevo AP:

1. El cliente envía una solicitud de reasociación al WLC a través del LAP.
2. El WLC envía el mensaje de la movilidad a otros WLCs en el grupo de la movilidad para averiguar con qué WLC el cliente fue asociado previamente.
3. El WLC original responde con información, como la dirección MAC, la dirección IP, QoS, el contexto de seguridad, etc. sobre el cliente a través del mensaje de movilidad.
4. El WLC actualiza su base de datos con los detalles del cliente proporcionados; el cliente luego pasa a través del proceso de reautenticación, si es necesario. El nuevo LAP con el cual el cliente está asociado actualmente también se actualiza junto con otros detalles en la base de datos del WLC. De esta manera, la dirección IP del cliente se retiene entre los roaming entre los WLC, lo que ayuda a proporcionar roaming sin problemas.

Para obtener más información sobre el roaming en un entorno unificado, refiérase a la sección *Configuración de Grupos de Movilidad* de la Guía de Configuración del Controlador de LAN Inalámbrica de Cisco, Versión 7.0.116.0.

Nota: El cliente inalámbrico no envía una solicitud de autenticación (802.11) durante la reasociación. El cliente inalámbrico simplemente envía la reasociación de inmediato. A continuación, pasará por la autenticación 802.1x.

P. ¿Qué puertos necesito permitir para la comunicación LWAPP/CAPWAP cuando hay un firewall en la red?

R. Debe habilitar estos puertos:

- Habilite estos puertos UDP para el tráfico LWAPP:Datos - 12222Control - 12223
- Habilite estos puertos UDP para el tráfico CAPWAP:Datos - 5247Control - 5246
- Habilite estos puertos UDP para el tráfico de movilidad:16666 - Modo seguro16667 - Modo no seguro

Los mensajes de datos y movilidad se intercambian normalmente a través de paquetes EtherIP. Se debe permitir el **protocolo IP 97** en el firewall para permitir los paquetes EtherIP. Si utiliza **ESP** para encapsular paquetes de movilidad, debe permitir que **ISAKMP** atraviese el firewall cuando abra el **puerto UDP 500**. También debe abrir el **protocolo IP 50** para permitir que los datos cifrados pasen a través del firewall.

Estos puertos son opcionales (dependiendo de sus requisitos):

- TCP 161 y 162 para SNMP (para el sistema de control inalámbrico [WCS])
- UDP 69 para TFTP
- TCP 80 y/o 443 para HTTP o HTTPS para acceso a GUI

- TCP 23 o 22 para Telnet o Secure Shell (SSH) para acceso CLI

P. ¿Admiten los controladores de LAN inalámbrica SSHv1 y SSHv2?

R. Los controladores de LAN inalámbrica sólo admiten SSHv2.

P. ¿Es compatible el ARP inverso (RARP) con los controladores de LAN inalámbrica (WLC)?

R. El protocolo de resolución de dirección inversa (RARP) es un protocolo de capa de link utilizado para obtener una dirección IP para una dirección de capa de link determinada, como una dirección Ethernet. RARP es compatible con WLC con la versión de firmware 4.0.217.0 o posterior. RARP no es compatible con ninguna de las versiones anteriores.

P. ¿Puedo utilizar el servidor DHCP interno en el controlador del Wireless LAN (WLC) para asignar las direcciones IP a los Lightweight Access Points (LAPs)?

R. Los controladores contienen un servidor DHCP interno. Este servidor se utiliza normalmente en sucursales que aún no tienen un servidor DHCP. Para acceder al servicio DHCP, haga clic en el menú **Controlador** de la GUI del WLC; luego haga clic en la opción **Servidor DHCP Interno** en el lado izquierdo de la página. Para obtener más información sobre cómo configurar el alcance DHCP en el WLC, consulte la sección *Configuración de DHCP* de la Guía de Configuración del Controlador de LAN Inalámbrica de Cisco, Versión 7.0.116.0.

El servidor interno proporciona direcciones DHCP a clientes inalámbricos, LAP, AP en modo de dispositivo en la interfaz de administración y solicitudes DHCP que se transmiten desde los LAP. Los WLC nunca ofrecen direcciones a los dispositivos de flujo ascendente en la red cableada. La opción DHCP 43 no se soporta en el servidor interno, por lo que el AP debe utilizar un método alternativo para localizar la dirección IP de la interfaz de administración del controlador, tal como la difusión de subred local, DNS, Priming, o la detección de Over-the-air.

Nota: Las versiones del firmware del WLC antes de 4.0 no soportan el servicio DHCP para los LAPs a menos que los LAPs estén conectados directamente al WLC. La función de servidor DHCP interno sólo se utilizó para proporcionar direcciones IP a los clientes que se conectan a la red LAN inalámbrica.

P. ¿Qué significa el campo DHCP Required bajo una WLAN?

R. DHCP requerido es una opción que se puede habilitar para una WLAN. Es necesario que todos los clientes que se asocian a esa WLAN en particular obtengan direcciones IP a través de DHCP. Los clientes con direcciones IP estáticas no pueden asociarse a la WLAN. Esta opción se encuentra en la ficha Advanced (Opciones avanzadas) de una WLAN. El WLC permite el tráfico hacia/desde un cliente solamente si su dirección IP está presente en la tabla MSCB del WLC. El WLC registra la dirección IP de un cliente durante su solicitud DHCP o la renovación DHCP. Esto requiere que un cliente renueve su dirección IP cada vez que se vuelve a asociar al WLC porque cada vez que el cliente se desasocia como parte de su proceso de roaming o tiempo de espera de sesión, su entrada se borra de la tabla MSCB. El cliente debe volver a autenticarse y reasociarse al WLC, lo que vuelve a hacer la entrada del cliente en la tabla.

P. ¿Cómo funciona Cisco Centralized Key Management (CCKM) en un entorno

LWAPP/CAPWAP?

R. Durante la asociación inicial del cliente, el AP o WLC negocia una clave maestra de par (PMK) después de que el cliente inalámbrico pase la autenticación 802.1x. El WLC o WDS AP almacena en caché el PMK para cada cliente. Cuando un cliente inalámbrico se reasocia o se traslada, omite la autenticación 802.1x y valida el PMK inmediatamente.

La única implementación especial del WLC en CCKM es que los WLC intercambian el PMK del cliente a través de paquetes de movilidad, tales como UDP 16666.

P. ¿Cómo configuro la configuración dúplex en el controlador de LAN inalámbrica (WLC) y los Lightweight Access Points (LAP)?

R. Los productos inalámbricos de Cisco funcionan mejor cuando la velocidad y el dúplex son autonegociados, pero usted tiene la opción de fijar las configuraciones del dúplex en el WLC y los LAP. Para establecer los ajustes de velocidad/dúplex del AP, puede configurar los ajustes dúplex para los LAPs en el controlador y luego, a su vez, los empuja a los LAPs.

configure ap ethernet duplex <auto/half/full> speed <auto/10/100/1000> <all/Cisco AP Name> es el comando para establecer la configuración de dúplex a través de la CLI. Este comando es compatible solamente con las versiones 4.1 y posteriores.

Para establecer la configuración dúplex para las interfaces físicas de WLC, utilice el **puerto config modo físico {all | port} {100h | 100 septies | 10 h | 10f}**.

Este comando configura los puertos Ethernet 10/100BASE-T especificados o todos los del panel frontal para un funcionamiento dedicado de 10 Mbps o 100 Mbps, semidúplex o dúplex completo. Tenga en cuenta que debe inhabilitar la negociación automática con el comando **config port autoneg disable** antes de configurar manualmente cualquier modo físico en el puerto. Además, observe que el comando **config port autoneg** invalida las configuraciones realizadas con el comando **config port physical mode**. De forma predeterminada, todos los puertos están configurados para la negociación automática.

Nota: No hay forma de cambiar la configuración de velocidad en los puertos de fibra.

P. ¿Hay alguna manera de rastrear el nombre del Lightweight Access Point (LAP) cuando no está registrado al controlador?

R. Si su AP está completamente abajo y no está registrado al controlador, no hay manera de que pueda seguir el LAP a través del controlador. La única manera que queda es que usted pueda acceder al switch en el que estos AP están conectados, y usted puede encontrar el switchport en el que están conectados usando este comando:

```
show mac-address-table address
```

Esto le da el número de puerto en el switch al cual está conectado este AP. Luego, ejecute este comando:

```
show cdp nei detail
```

La salida de este comando también da el nombre del LAP. Sin embargo, este método sólo es posible cuando el AP está encendido y conectado al switch.

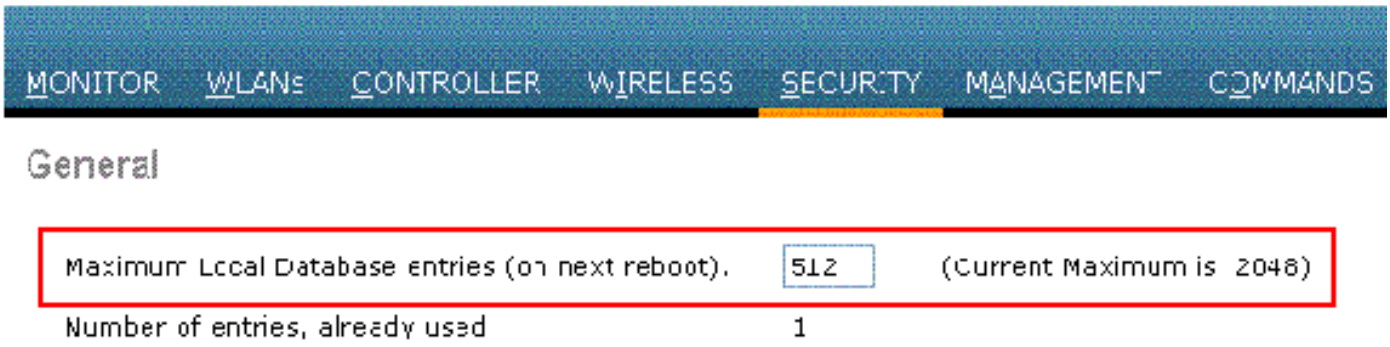
P. He configurado 512 usuarios en mi controlador. ¿Hay alguna forma de aumentar el número de usuarios en el controlador de LAN inalámbrica (WLC)?

R. La base de datos de usuarios locales está limitada a un máximo de 2048 entradas en la página **Security > General**. Esta base de datos la comparten los usuarios de gestión local (incluidos los embajadores en la recepción), los usuarios de red (incluidos los usuarios invitados), las entradas de filtros MAC, las entradas de la lista de autorización de puntos de acceso y las entradas de la lista de exclusión. Juntos, todos estos tipos de usuarios no pueden superar el tamaño de base de datos configurado.

Para aumentar la base de datos local, utilice este comando de la CLI:

```
<Cisco Controller>config database size ?
<count>  Enter the maximum number of entries (512-2048)
```

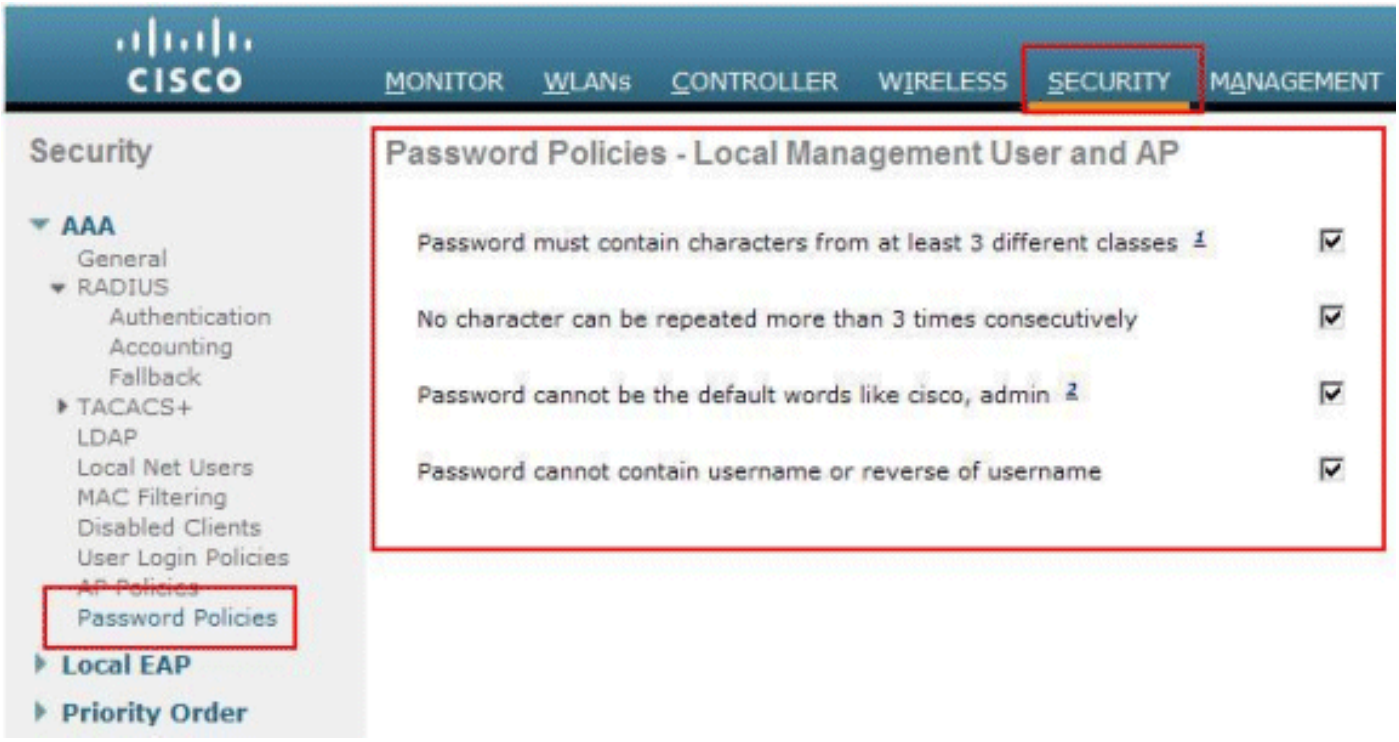
Nota: Debe guardar la configuración y restablecer el sistema (mediante el comando **reset system**) para que el cambio surta efecto.



P. ¿Cómo hago cumplir una política de contraseña fuerte en los WLC?

R. Los WLC le permiten definir una política de contraseña fuerte. Esto se puede realizar mediante la CLI o la GUI.

En la GUI, vaya a **Security > AAA > Password Policies**. Esta página tiene una serie de opciones que se pueden seleccionar para forzar una contraseña segura. Aquí tiene un ejemplo:



Para hacer esto desde el WLC CLI, utilice el **config switchconfig strong-pwd** {case-check | *control consecutivo | default-check | username-check | all-check} {enable | disable}* :

- **case-check**: verifica la aparición del mismo carácter tres veces consecutivamente.
- **comprobación consecutiva**: verifica si se están utilizando los valores predeterminados o sus variantes.
- **default-check**: verifica si se está utilizando el nombre de usuario o su inversa.
- **all-checks** - Activa/desactiva todas las comprobaciones de contraseña segura.

P. ¿Cómo se utiliza la función de cliente pasivo en los controladores de LAN inalámbrica?

R. Los clientes pasivos son dispositivos inalámbricos, como escalas e impresoras que se configuran con una dirección IP estática. Estos clientes no transmiten ninguna información IP como la dirección IP, la máscara de subred y la información de la puerta de enlace cuando se asocian con un punto de acceso. Como resultado, cuando se utilizan clientes pasivos, el controlador nunca conoce la dirección IP a menos que utilice el DHCP.

Los WLC actúan actualmente como proxy para las solicitudes ARP. Al recibir una solicitud ARP, el controlador responde con una respuesta ARP en lugar de pasar la solicitud directamente al cliente. Este escenario tiene dos ventajas:

- El dispositivo ascendente que envía la solicitud ARP al cliente no sabrá dónde está ubicado el cliente.
- La alimentación de los dispositivos que funcionan con baterías, como teléfonos móviles e impresoras, se mantiene porque no tienen que responder a todas las solicitudes ARP.

Dado que el controlador inalámbrico no tiene ninguna información relacionada con IP sobre los clientes pasivos, no puede responder a ninguna solicitud ARP. El comportamiento actual no permite la transferencia de solicitudes ARP a clientes pasivos. Cualquier aplicación que intente

acceder a un cliente pasivo fallará.

La función de cliente pasivo permite el intercambio de solicitudes y respuestas ARP entre clientes por cable e inalámbricos. Esta función, cuando está habilitada, permite que el controlador pase las solicitudes ARP de los clientes por cable a los clientes inalámbricos hasta que el cliente inalámbrico deseado llegue al estado RUN.

Para obtener información sobre cómo configurar la función de cliente pasivo, lea la sección Uso de la GUI para Configurar el Cliente Pasivo en la Guía de Configuración del Controlador de LAN Inalámbrica de Cisco, Versión 7.0.116.0.

P. ¿Cómo puedo configurar el cliente para que se reautentique con el servidor RADIUS cada tres minutos o en cualquier período de tiempo especificado?

R. El parámetro de tiempo de espera de sesión en el WLC se puede utilizar para lograr esto. De forma predeterminada, el parámetro de tiempo de espera de la sesión se configura durante 1800 segundos antes de que se produzca una nueva autenticación.

Cambie este valor a 180 segundos para hacer que el cliente se reautentique después de tres minutos.

Para acceder al parámetro de tiempo de espera de sesión, haga clic en el menú **WLANs** en la GUI. Muestra la lista de WLANs configuradas en el WLC. Haga clic en la WLAN a la que pertenece el cliente. Vaya a la pestaña **Advanced** y encontrará el parámetro *Enable Session Timeout*. Cambie el valor predeterminado a 180 y haga clic en **Apply** para que los cambios surtan efecto.

Cuando se envía en un Access-Accept, junto con un valor de Termination-Action de RADIUS-Request, el atributo Session-Timeout especifica el número máximo de segundos de servicio proporcionado antes de la reautenticación. En este caso, el atributo Session-Timeout se utiliza para cargar la constante ReAuthPeriod en la máquina de estado de temporizador de reautenticación de 802.1X.

P. Tengo una tunelización de invitado, túnel Ethernet sobre IP (EoIP), configurado entre mi controlador de LAN inalámbrica (WLC) 4400, que actúa como el WLC de anclaje, y varios WLC remotos. ¿Puede este WLC de anclaje reenviar las difusiones de subred a través del túnel EoIP de la red cableada a los clientes inalámbricos asociados con los controladores remotos?

R. No, el WLC 4400 no reenvía las difusiones de subred IP del lado cableado a los clientes inalámbricos a través del túnel EoIP. Esta función no es compatible. Cisco no admite la tunelización de difusión de subred o multidifusión en la topología de acceso de invitados. Dado que la WLAN de invitado fuerza el punto de presencia del cliente a una ubicación muy específica en la red, principalmente fuera del firewall, la tunelización de la difusión de subred puede ser un problema de seguridad.

P. En una configuración de controlador de LAN inalámbrica (WLC) y protocolo de punto de acceso ligero (LWAPP), ¿qué valores de punto de código de servicios diferenciados (DSCP) se transfieren para el tráfico de voz? ¿Cómo se implementa QoS en el WLC?

R. Las WLAN de la solución Cisco Unified Wireless Network (UWN) admiten cuatro niveles de QoS:

- Platino/Voz
- Gold/Vídeo
- Silver/Best Effort (opción predeterminada)
- Bronce/fondo

Puede configurar la WLAN de tráfico de voz para utilizar QoS Platinum, asignar la WLAN de ancho de banda bajo para utilizar QoS Bronze y asignar el resto del tráfico entre los otros niveles de QoS. Consulte Asignación de un Perfil de QoS a una WLAN para obtener más información.

P. ¿Son compatibles los puentes Ethernet de Linksys con una solución Cisco Wireless Unified Solution?

R. No, el WLC soporta solamente los productos de Cisco WGB. No se admiten WGB de Linksys. Aunque la solución Cisco Wireless Unified Solution no es compatible con los puentes Ethernet WET54G y WET11B de Linksys, puede utilizar estos dispositivos en una configuración de Wireless Unified Solution si sigue estas instrucciones:

- Conecte un solo dispositivo al puente Ethernet WET54G o WET11B.
- Active la función de clonación de MAC en el puente Ethernet WET54G o WET11B para clonar el dispositivo conectado.
- Instale los controladores y el firmware más recientes en los dispositivos conectados al puente Ethernet WET54G o WET11B. Esta directriz es especialmente importante para las impresoras JetDirect porque las versiones de firmware anteriores causan problemas con DHCP.

Nota: No se admiten otros puentes de terceros. Los pasos mencionados también se pueden probar para otros puentes de terceros.

P. ¿Cómo almaceno los archivos de configuración en el Wireless LAN Controller (WLC)?

A. El WLC contiene dos tipos de memoria:

- RAM volátil: contiene la configuración actual del controlador activo
- RAM no volátil (NVRAM): contiene la configuración de reinicio

Cuando configura el sistema operativo en el WLC, usted está modificando la RAM volátil. Debe guardar la configuración de la RAM volátil a la NVRAM para asegurarse de que el WLC se reinicia en la configuración actual.

Es importante saber qué memoria está modificando cuando realiza estas tareas:

- Utilice el asistente de configuración.
- Borre la configuración del controlador.
- Guardar configuraciones.
- Reinicie el controlador.
- Cierre la sesión de la CLI.

Preguntas frecuentes sobre características

P. ¿Cómo configuro el tipo de protocolo de autenticación extensible (EAP) en el controlador de LAN inalámbrica (WLC)? Deseo realizar la autenticación con un dispositivo Access Control Server (ACS) y obtengo un tipo de "EAP no compatible" en los registros.

A. No hay configuración separada del tipo EAP en el WLC. Para EAP ligero (LEAP), EAP autenticación flexible a través de tunelación segura (EAP-FAST) o EAP protegido de Microsoft (MS-PEAP), configure IEEE 802.1x o acceso protegido Wi-Fi (WPA) (si utiliza 802.1x con WPA). Cualquier tipo de EAP que se admita en el extremo posterior de RADIUS y en el cliente se admite mediante la etiqueta 802.1x. La configuración EAP del cliente y del servidor RADIUS debe coincidir.

Complete estos pasos para habilitar EAP a través de la GUI en el WLC:

1. Desde la GUI del WLC , haga clic en **WLANs**.
2. Aparece una lista de WLANs configuradas en el WLC. Haga clic en una WLAN.
3. En **WLANs > Edit**, haga clic en la pestaña **Security**.
4. Haga clic en **Layer 2**, y elija Layer 2 Security as 802.1x or WPA+WPA2. También puede configurar los parámetros 802.1x que están disponibles en la misma ventana. Luego, el WLC reenvía los paquetes de autenticación EAP entre el cliente inalámbrico y el servidor de autenticación.
5. Haga clic en los servidores **AAA**, y elija el servidor de autenticación del menú desplegable para esta WLAN. Suponemos que el servidor de autenticación ya está configurado globalmente. Para obtener información sobre cómo habilitar la opción EAP en WLCs a través de la interfaz de línea de comandos (CLI), consulte la sección *Uso de CLI para Configurar RADIUS* de la Guía de Configuración de Cisco Wireless LAN Controller, Release 7.0.116.0.

P. ¿Qué es el cambio rápido de SSID?

R. El cambio rápido de SSID permite a los clientes moverse entre SSID. Cuando el cliente envía una nueva asociación para un SSID diferente, la entrada del cliente en la tabla de conexión del controlador se borra antes de que el cliente se agregue al nuevo SSID. Cuando se inhabilita el cambio rápido de SSID, el controlador aplica un retraso antes de que los clientes puedan moverse a un nuevo SSID. Para obtener información sobre cómo habilitar Fast SSID Changing, refiérase a la sección *Configuring Fast SSID Changing* de la Guía de Configuración de Cisco Wireless LAN Controller, Release 7.0.116.0.

P. ¿Puedo establecer un límite en el número de clientes que pueden conectarse a una LAN inalámbrica?

R. Puede establecer un límite en el número de clientes que pueden conectarse a una WLAN, lo cual es útil en escenarios donde tiene un número limitado de clientes que pueden conectarse a un controlador. El número de clientes que puede configurar por WLAN depende de la plataforma que esté utilizando.

Lea la sección Configuración del Número Máximo de Clientes por WLAN de la Guía de

Configuración del Controlador de LAN Inalámbrica de Cisco, Versión 7.0.116.0 para obtener información sobre los límites de clientes por WLAN para las diferentes plataformas de Controladores de LAN Inalámbrica.

P. ¿Qué es PKC y cómo funciona con el Wireless LAN Controller (WLC)?

A. PKC significa Proactive Key Caching. Se diseñó como una extensión del estándar IEEE 802.11i.

PKC es una función habilitada en los Cisco 2006/410x/440x Series Controllers que permite a los clientes inalámbricos correctamente equipados desplazarse sin una reautenticación completa con un servidor AAA. Para comprender el PKC, primero debe entender el Key Caching.

El almacenamiento en caché de claves es una función que se ha agregado a WPA2. Esto permite que una estación móvil almacene en caché las claves maestras (Pairwise Master Key [PMK]) que obtiene mediante una autenticación exitosa con un punto de acceso (AP), y **reutilice en una futura asociación con el mismo AP**. Esto significa que un dispositivo móvil determinado necesita autenticarse una vez con un AP específico y almacenar en caché la clave para su uso futuro. El Key Caching se maneja a través de un mecanismo conocido como el PMKID (Identificador PMK), que es un hash del PMK, una cadena, la estación y las direcciones MAC del AP. El PMKID identifica de forma exclusiva al PMK.

Incluso con Key Caching, una estación inalámbrica debe autenticarse con cada AP del que desea obtener el servicio. Esto introduce una latencia y unos gastos generales significativos, que retrasan el proceso de transferencia y pueden inhibir la capacidad de admitir aplicaciones en tiempo real. Para resolver este problema, PKC se introdujo con WPA2.

PKC permite que una estación reutilice un PMK que había obtenido previamente a través de un proceso de autenticación exitoso. Esto elimina la necesidad de que la estación se autentique contra los nuevos AP cuando esté en roaming.

Por lo tanto, en un roaming dentro del controlador, cuando un dispositivo móvil se mueve de un AP a otro en el mismo controlador, el cliente vuelve a calcular un PMKID usando el PMK usado anteriormente y lo presenta durante el proceso de asociación. El WLC busca su caché PMK para determinar si tiene tal entrada. Si lo hace, omite el proceso de autenticación 802.1x e inicia inmediatamente el intercambio de claves WPA2. Si no es así, se somete al proceso de autenticación estándar 802.1X.

PKC se activa de forma predeterminada con WPA2. Por lo tanto, cuando usted habilita WPA2 como seguridad de la capa 2 bajo la configuración WLAN del WLC, el PKC se habilita en el WLC. Además, configure el servidor AAA y el cliente inalámbrico para la autenticación EAP adecuada.

El suplicante utilizado en el lado del cliente también debe soportar WPA2 para que PKC funcione. PKC también se puede implementar en un entorno de roaming entre controladores.

Nota: PKC no funciona con Aironet Desktop Utility (ADU) como el cliente solicitante.

P. ¿Cuáles son las explicaciones para esta configuración de tiempo de espera en el controlador: Tiempo de espera del protocolo de resolución de direcciones (ARP), Tiempo de espera de inactividad del usuario y Tiempo de espera de sesión?

R. El **tiempo de espera ARP** se utiliza para eliminar las entradas ARP en el WLC para los

dispositivos aprendidos de la red.

El **tiempo de espera de inactividad del usuario:** Cuando un usuario está inactivo sin ninguna comunicación con el LAP durante la cantidad de tiempo establecida como tiempo de espera de inactividad del usuario, el cliente es desautenticado por el WLC. El cliente tiene que reautenticar y volver a asociar al WLC. Se utiliza en situaciones donde un cliente puede abandonar su LAP asociado sin notificar al LAP. Esto puede ocurrir si la batería se agota en el cliente o si los asociados del cliente se mueven.

Nota: Para acceder ARP y User Idle Timeout en el WLC GUI , vaya al menú **Controlador**. Elija **General** en el lado izquierdo para encontrar los campos ARP y User Idle Timeout.

El tiempo de espera de la sesión es el tiempo máximo para una sesión del cliente con el WLC. Después de este tiempo, el WLC desautentica al cliente, y el cliente pasa a través de todo el proceso de autenticación (re-autenticación) otra vez. Esto forma parte de una precaución de seguridad para girar las claves de cifrado. Si utiliza un método de protocolo de autenticación extensible (EAP) con administración de claves, la nueva generación de claves se produce a intervalos regulares para obtener una nueva clave de cifrado. Sin administración de claves, este valor de tiempo de espera es el tiempo que los clientes inalámbricos necesitan para realizar una reautenticación completa. El tiempo de espera de la sesión es específico de la WLAN. Se puede acceder a este parámetro desde el menú **WLANs > Edit**.

P. ¿Qué es un sistema RFID? ¿Qué etiquetas RFID admite actualmente Cisco?

R. La identificación por radiofrecuencia (RFID) es una tecnología que utiliza la comunicación por radiofrecuencia para una comunicación de corto alcance. Un sistema RFID básico está compuesto por etiquetas RFID, lectores RFID y el software de procesamiento.

Actualmente, Cisco admite etiquetas RFID de AeroScout y Pango. Para obtener más información sobre cómo configurar las etiquetas de AeroScout, consulte Configuración de WLC para Etiquetas RFID de AeroScout.

P. ¿Puedo realizar la autenticación EAP localmente en el WLC? ¿Hay algún documento que explique esta función de EAP local?

R. Sí, la autenticación EAP se puede realizar localmente en el WLC. EAP local es un método de autenticación que permite que los usuarios y los clientes inalámbricos sean autenticados localmente en el WLC. Está diseñado para oficinas remotas que deseen mantener la conectividad con clientes inalámbricos cuando el sistema back-end se interrumpa o cuando el servidor de autenticación externo deje de funcionar. Cuando habilita el EAP local, el WLC sirve como el servidor de autenticación. Para obtener más información sobre cómo configurar un WLC para la autenticación EAP-Fast local, consulte el Ejemplo de Configuración de Autenticación EAP Local en el Controlador de LAN Inalámbrica con EAP-FAST y el Servidor LDAP.

P. ¿Qué es la función de anulación de WLAN? ¿Cómo se configura esta función? ¿Los LAP mantendrán los valores de invalidación de WLAN cuando conmuten por error al WLC de respaldo?

R. La función de invalidación de WLAN nos permite elegir WLANs de entre las WLANs configuradas en un WLC que se pueden utilizar activamente en una base LAP individual. Complete estos pasos para configurar una invalidación de WLAN:

1. En la GUI del WLC, haga clic en el menú **Wireless**.
2. Haga clic en la opción **Radios** en el lado izquierdo y elija **802.11 a/n** u **802.11 b/g/n**.
3. Haga clic en el enlace **Configure** del menú desplegable que se encuentra en el lado derecho que corresponde al nombre del AP en el que desea configurar la invalidación de WLAN.
4. Elija **Enable** en el menú desplegable WLAN Override. El menú WLAN Override (Anulación de WLAN) es el último elemento de la parte izquierda de la ventana.
5. Aparece la lista de todas las WLAN que se configuran en el WLC.
6. De esta lista, verifique las **WLANs** que desea que aparezcan en el LAP, y haga clic en **Aplicar** para que los cambios tengan efecto.
7. Guarde la configuración después de realizar estos cambios.

Los AP retienen los valores de invalidación de WLAN cuando se registran a otros WLC, siempre que los perfiles WLAN y los SSID que usted desea invalidar se configuren a través de todos los WLC.

Nota: En la versión 5.2.157.0 del software del controlador, se ha eliminado la función de anulación de WLAN de la GUI y la CLI del controlador. Si su controlador está configurado para la invalidación de WLAN y usted actualiza a la versión 5.2.157.0 del software del controlador, el controlador elimina la configuración de WLAN y transmite todas las WLAN. Puede especificar que sólo se transmitan ciertas WLAN si configura los grupos de puntos de acceso. Cada punto de acceso anuncia solamente las WLANs habilitadas que pertenecen a su grupo de punto de acceso.

Nota: Los grupos de puntos de acceso no permiten que las WLANs se transmitan en por interfaz de radio del AP.

P. ¿Es compatible IPv6 con los controladores de LAN inalámbrica (WLC) y los puntos de acceso ligeros (LAP) de Cisco?

R. Actualmente, los controladores de las series 4400 y 4100 sólo admiten el paso a través de clientes IPv6. No se admite la compatibilidad con IPv6 nativo.

Para habilitar IPv6 en el WLC, marque la casilla de verificación **IPv6 Enable** en la configuración WLAN SSID bajo la página WLAN > Edit.

Además, se necesita el modo de multidifusión Ethernet (EMM) para admitir IPv6. Si desactiva EMM, los dispositivos cliente que utilizan IPv6 perderán la conectividad. Para habilitar EMM, vaya a la página Controller > General y en el menú desplegable Ethernet Multicast Mode, elija **Unicast** o **Multicast**. Esto habilita la multidifusión en modo unidifusión o en modo multidifusión. Cuando la multidifusión se habilita como unidifusión de multidifusión, los paquetes se replican para cada AP. Esto puede requerir un uso intensivo del procesador, así que utilícelo con precaución. La multidifusión habilitada como multidifusión multidifusión utiliza la dirección de multidifusión asignada por el usuario para realizar una multidifusión más tradicional hacia los puntos de acceso (AP).

Nota: IPv6 no es compatible con los controladores de 2006.

Además, existe el ID de bug Cisco CSCsg78176, que impide el uso del paso a través de IPv6 cuando se utiliza la función de anulación de AAA.

P. ¿El controlador de LAN inalámbrica (WLC) de Cisco serie 2000 admite

autenticación Web para usuarios invitados?

R. La autenticación Web se soporta en todos los WLCs de Cisco. La autenticación Web es un método de autenticación de capa 3 que se utiliza para autenticar a los usuarios con credenciales de autenticación simple. No hay cifrado involucrado. Complete estos pasos para habilitar esta función:

1. En la GUI, haga clic en el menú **WLAN**.
2. Haga clic en una **WLAN**.
3. Vaya a la pestaña **Security** y elija **Layer 3**.
4. Marque la casilla **Web Policy** y elija **Authentication**.
5. Haga clic en **Aply para guardar los cambios.**
6. Para crear una base de datos en el WLC contra la cual autenticar a los usuarios, vaya al menú **Seguridad** en la GUI, elija **Usuario de Red Local**, y complete estas acciones: Defina el nombre de usuario y la contraseña de invitado que debe utilizar el invitado para iniciar sesión. Estos valores distinguen entre mayúsculas y minúsculas.Elija el ID de WLAN que utiliza.**Nota:** Para obtener una configuración más detallada, consulte el Ejemplo de Configuración de Autenticación Web del Controlador de LAN Inalámbrica.

P. ¿Se puede administrar el WLC en el modo inalámbrico?

R. El WLC se puede administrar a través del modo inalámbrico una vez que está habilitado. Para obtener más información sobre cómo habilitar el modo inalámbrico, refiérase a la sección *Habilitación de las Conexiones Inalámbricas a la GUI y la CLI* de la Guía de Configuración del Controlador de LAN Inalámbrica de Cisco, Versión 7.0.116.0.

P. ¿Qué es la agregación de enlaces (LAG)? ¿Cómo activo LAG en los controladores de LAN inalámbrica (WLC)?

R. LAG agrupa todos los puertos en el WLC en una sola interfaz EtherChannel. El sistema gestiona dinámicamente el equilibrio de carga de tráfico y la redundancia de puertos con LAG.

Generalmente, la interfaz en el WLC tiene varios parámetros asociados con él, que incluyen la dirección IP, default-gateway (para la subred IP), puerto físico primario, puerto físico secundario, etiqueta VLAN, y servidor DHCP. Cuando no se utiliza LAG, cada interfaz se asigna generalmente a un puerto físico, pero las interfaces múltiples también se pueden asignar a un solo puerto WLC. Cuando se utiliza LAG, el sistema asigna dinámicamente las interfaces al canal de puerto agregado. Esto ayuda en la redundancia de puertos y el balanceo de carga. Cuando un puerto falla, la interfaz se mapea dinámicamente al siguiente puerto físico disponible y los LAPs se equilibran a través de los puertos.

Cuando el LAG se habilita en un WLC, el WLC reenvía las tramas de datos en el mismo puerto en el que se recibieron. El WLC depende del switch vecino para equilibrar la carga del tráfico a través del EtherChannel. El WLC no realiza ningún balanceo de carga EtherChannel por sí solo.

P. ¿Qué modelos de controladores de LAN inalámbrica (WLC) admiten la agregación de enlaces (LAG)?

R. Los Cisco 5500 Series Controllers admiten LAG en la versión de software 6.0 o posterior, los Cisco 4400 Series Controllers admiten LAG en la versión de software 3.2 o posterior, y LAG se

habilita automáticamente en los controladores dentro de Cisco WiSM y el Catalyst 3750G Integrated Wireless LAN Controller Switch. Sin LAG, cada puerto del sistema de distribución de un Cisco 4400 Series Controller admite hasta 48 puntos de acceso. Con LAG habilitado, el puerto lógico de un controlador Cisco 4402 admite hasta 50 puntos de acceso, el puerto lógico de un controlador Cisco 4404 admite hasta 100 puntos de acceso y el puerto lógico del switch del controlador LAN inalámbrico integrado Catalyst 3750G y de cada controlador Cisco WiSM admite hasta 150 puntos de acceso.

Los WLC 2006 y 2006 de Cisco no soportan LAG. Los modelos anteriores, como el WLC de la serie 4000 de Cisco, no soportan LAG.

P. ¿Qué es la función de movilidad de anclaje automático en las redes inalámbricas unificadas?

R. La movilidad de anclaje automático (o movilidad de WLAN de invitado) se utiliza para mejorar el equilibrio de carga y la seguridad para los clientes de roaming en sus LAN inalámbricas (WLAN). En condiciones normales de roaming, los dispositivos cliente se unen a una WLAN y se anclan al primer controlador con el que se ponen en contacto. Si un cliente se traslada a una subred diferente, el controlador al que el cliente se traslada configura una sesión externa para el cliente con el controlador de anclaje. Con el uso de la función de movilidad de anclaje automático, puede especificar un controlador o conjunto de controladores como puntos de anclaje para los clientes en una WLAN.

Nota: El anclaje de movilidad no se debe configurar para la movilidad de capa 3. El anclaje de movilidad se utiliza únicamente para la tunelización de invitados.

P. ¿Se puede configurar un controlador de LAN inalámbrica (WLC) de Cisco 2006 como anclaje para una WLAN?

R. Un WLC de la serie 2000 de Cisco no se puede designar como un ancla para un WLAN. Sin embargo, una WLAN creada en un WLC de Cisco serie 2000 puede tener un WLC de Cisco serie 4100 y un WLC de Cisco serie 4400 como su ancla.

P. ¿Qué tipo de tunelización de movilidad utiliza el controlador de LAN inalámbrica?

A. Las versiones 4.1 a 5.1 del software del controlador admiten tunelización de movilidad asimétrica y simétrica. La versión 5.2 o posterior del software del controlador sólo admite tunelización de movilidad simétrica, que ahora está siempre habilitada de forma predeterminada.

En la tunelización asimétrica, el tráfico del cliente a la red cableada se rutea directamente a través del controlador externo. La tunelización asimétrica se interrumpe cuando un router ascendente tiene habilitado el filtrado de trayectoria inversa (RPF). En este caso, el tráfico del cliente se descarta en el router porque la verificación RPF garantiza que la trayectoria de regreso a la dirección de origen coincida con la trayectoria de la cual proviene el paquete.

Cuando se habilita la tunelización de movilidad simétrica, todo el tráfico del cliente se envía al controlador de anclaje y luego puede pasar satisfactoriamente la verificación RPF. La tunelización de movilidad simétrica también es útil en estas situaciones:

- Esto es útil si una instalación de firewall en el trayecto del paquete del cliente descarta paquetes porque la dirección IP de origen no coincide con la subred en la que se reciben los

paquetes.
- Si la VLAN del grupo de punto de acceso en el controlador de anclaje es diferente de la VLAN de interfaz WLAN en el controlador externo: en este caso, el tráfico del cliente se puede enviar en una VLAN incorrecta durante los eventos de movilidad.

P. ¿Cómo accedemos al WLC cuando la red está inactiva?

R. Cuando la red está inactiva, el puerto de servicio puede acceder al WLC. A este puerto se le asigna una dirección IP en una subred completamente diferente de otros puertos del WLC y por lo tanto se le llama administración fuera de banda. Para obtener más información, consulte la sección *Configuración de Puertos e Interfaces* de la Guía de Configuración del Controlador de LAN Inalámbrica de Cisco, Versión 7.0.116.0.

P. ¿Admiten los controladores de LAN inalámbrica de Cisco (WLC) la función de conmutación por fallo (o redundancia)?

R. Sí, si usted tiene dos o más WLCs en su red WLAN, usted puede configurarlos para la redundancia. Generalmente, un LAP se une al WLC primario configurado. Una vez que el WLC primario falla, el LAP se reinicia y se une a otro WLC en el grupo de la movilidad. La conmutación por fallas es una característica en la que el LAP sondea para el WLC primario y se une al WLC primario una vez que es funcional. Consulte el Ejemplo de Configuración de Failover del Controlador WLAN para los Lightweight Access Points para obtener más información.

P. ¿Cuál es el uso de las listas de control de acceso (ACL) de autenticación previa en los controladores de LAN inalámbrica (WLC)?

R. Con la ACL de autenticación previa, como el nombre implica, puede permitir el tráfico del cliente hacia y desde una dirección IP específica incluso antes de que el cliente se autentique. Cuando se utiliza un servidor web externo para la autenticación web, algunas de las plataformas WLC necesitan una ACL de autenticación previa para el servidor web externo (Cisco 5500 Series Controller, Cisco 2100 Series Controller, Cisco 2000 Series y el módulo de red del controlador). Para las otras plataformas WLC, la ACL de autenticación previa no es obligatoria. Sin embargo, se recomienda configurar una ACL de autenticación previa para el servidor web externo cuando se utiliza la autenticación web externa.

P. Tengo una WLAN filtrada por MAC y una WLAN completamente abierta en mi red. ¿El cliente elige la WLAN abierta de forma predeterminada? ¿O el cliente se asocia automáticamente con el ID de WLAN que se establece en el filtro MAC? Además, ¿por qué hay una opción de "interfaz" en un filtro MAC?

R. El cliente puede asociarse a cualquier WLAN a la que el cliente esté configurado para conectarse. La opción de interfaz en el filtro MAC permite aplicar el filtro a una WLAN o a una interfaz. Si hay varias WLAN vinculadas a la misma interfaz, puede aplicar el filtro MAC a la interfaz sin necesidad de crear un filtro para cada WLAN individual.

P. ¿Cómo puedo configurar la autenticación TACACS para los usuarios de administración en el Wireless LAN Controller (WLC)?

R. A partir de la versión 4.1 del WLC, TACACS se soporta en los WLC. Consulte Configuración de

TACACS+ para comprender cómo configurar TACACS+ para autenticar a los usuarios de administración del WLC.

P. ¿Cuál es el uso de la configuración de falla de autenticación excesiva en un controlador de LAN inalámbrica (WLC)?

R. Esta configuración es una de las directivas de exclusión de clientes. La exclusión del cliente es una función de seguridad en el controlador. La política se utiliza para poner en la lista negra a los clientes para evitar el acceso ilegal a la red o ataques a la red inalámbrica.

Con esta política de falla de autenticación web excesiva habilitada, cuando el número de intentos fallidos de autenticación web de un cliente excede 5, el controlador considera que el cliente ha excedido el número máximo de intentos de autenticación web y pone en lista negra al cliente.

Complete estos pasos para habilitar o inhabilitar esta configuración:

1. Desde la GUI del WLC, vaya a **Security > Wireless Protection Policies > Client Exclusion Policies**.
2. Marque o desmarque **Errores de autenticación web excesivos**.

P. He convertido mi punto de acceso autónomo (AP) al modo ligero. En el modo del protocolo ligero del AP (LWAPP) con el servidor RADIUS AAA para la contabilización del cliente, se hace normalmente el seguimiento del cliente con la contabilización RADIUS basada en la dirección IP del WLC. ¿Es posible establecer la contabilización de RADIUS basada en la dirección MAC del AP asociada a ese WLC y no en la dirección IP del WLC?

R. Sí, esto se puede hacer con la configuración del lado del WLC. Complete estos pasos:

1. Desde la GUI del controlador, en **Seguridad > Contabilidad Radius**, hay un cuadro desplegable para Tipo de ID de estación de llamada. Elija **AP MAC Address**.
2. Verifique esto a través del registro AP LWAPP. Allí, puede ver el campo de ID de la estación llamada que muestra la dirección MAC del AP al cual el cliente particular está asociado.

P. ¿Cómo cambia el valor del tiempo de espera de entrada en contacto de acceso Wi-Fi protegido (WPA) en un controlador de LAN inalámbrica (WLC) a través de CLI? Sé que puedo hacer esto en los puntos de acceso (AP) del IOS® de Cisco con el comando dot11 wpa handshake timeout *value*, pero ¿cómo lo realiza en un WLC?

R. La capacidad de configurar el tiempo de espera de WPA-Handshake a través de los WLC fue integrada en la versión de software 4.2 y posterior. Usted no necesita esta opción en versiones anteriores del software del WLC.

Estos comandos se pueden utilizar para cambiar el tiempo de espera del protocolo de enlace WPA:

```
config advanced eap eapol-key-timeout <value>
```

```
config advanced eap eapol-key-retries <value>
```

Los valores predeterminados continúan reflejando el comportamiento actual del WLC.

```
- the default value for eapol-key-timeout is 1 second.
- the default value for eapol-key-retries is 2 retries
```

Nota: En los AP IOS, esta configuración se puede configurar con el comando **dot11 wpa handshake**.

También puede configurar los otros parámetros EAP con las opciones bajo el comando **config advanced eap**.

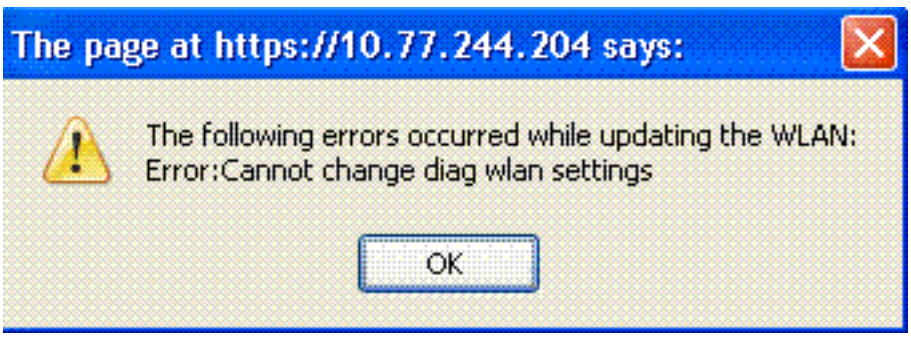
```
(Cisco Controller) >config advanced eap ?

eapol-key-timeout
   Configures EAPOL-Key Timeout in seconds.
eapol-key-retries
   Configures EAPOL-Key Max Retries.
identity-request-timeout
   Configures EAP-Identity-Request Timeout in seconds.
identity-request-retries
   Configures EAP-Identity-Request Max Retries.
key-index
   Configure the key index used for
   dynamic WEP(802.1x) unicast key (PTK).
max-login-ignore-identity-response
   Configure to ignore the same username count
   reaching max in the EAP identity response
request-timeout
   Configures EAP-Request Timeout in seconds.
request-retries
   Configures EAP-Request Max Retries.
```

P. ¿Cuál es el propósito de la función de canal de diagnóstico en la página WLAN > Edit > Advanced?

R. La función de canal de diagnóstico le permite resolver problemas con respecto a la comunicación del cliente con una WLAN. El cliente y los puntos de acceso se pueden someter a un conjunto definido de pruebas para identificar la causa de las dificultades de comunicación que experimenta el cliente y, a continuación, permitir que se tomen medidas correctivas para que el cliente funcione en la red. Puede utilizar la GUI o CLI del controlador para habilitar el canal de diagnóstico, y puede utilizar la CLI o WCS del controlador para ejecutar las pruebas de diagnóstico.

El canal de diagnóstico sólo se puede utilizar para realizar pruebas. Si intenta configurar la autenticación o el cifrado para la WLAN con el canal de diagnóstico habilitado, verá este error:



P. ¿Cuál es el número máximo de grupos de AP que se pueden configurar en un WLC?

R. Esta lista muestra el número máximo de grupos de AP que puede configurar en un WLC:

- Un máximo de 50 grupos de puntos de acceso para los módulos de red del controlador y el controlador Cisco 2100 Series Controller
- Un máximo de 300 grupos de puntos de acceso para los controladores de la serie Cisco 4400, Cisco WiSM y el switch controlador de LAN inalámbrica Cisco 3750G
- Un máximo de 500 grupos de puntos de acceso para los controladores de Cisco serie 5500

Información Relacionada

- Preguntas frecuentes sobre el controlador LAN inalámbrico (WLC)
- Preguntas Más Frecuentes sobre Mensajes de Error y de Sistema del Controlador de la LAN inalámbrica (WLC)
- Preguntas frecuentes sobre los puntos de acceso ligeros
- Guía de Configuración de Cisco Wireless LAN Controller, Versión 7.0.116.0
- Compatibilidad con IPv6 en el controlador de LAN inalámbrica
- Soporte de Productos de Red Inalámbrica
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).