

Catalyst 6500 Series WLSM al Guía de migración de WiSM de las Catalyst 6500 Series

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Overview](#)

[Diferencias arquitectónicas](#)

[Cisco Catalyst 6500 Series WLSM](#)

[Cisco Catalyst 6500 Series WiSM](#)

[Estrategia de migración](#)

[Software del producto de la actualización](#)

[Implemente las configuraciones](#)

[Configure el Catalyst 6500 WiSM para emigrar el SSID del Catalyst 6500 WLSM](#)

[Conversión del LWAPP del Punto de acceso](#)

[Distribución del Punto de acceso entre los reguladores en Cisco WiSM](#)

[Pruebe con un número limitado de Puntos de acceso](#)

[Despliegue completo](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Este documento se centra en la estrategia de migración de un Módulo de servicios existente del Wireless LAN (WLSM) a un módulo de Servicios inalámbricos (WiSM). Las hojas de operación (planning) y la ejecución cuidadosas es absolutamente necesarias en la migración de Cisco WLSM a Cisco WiSM.

La audiencia prevista para el documento incluye los administradores y a los individuos de red para empresas en todos los niveles dentro de la infraestructura TIC de una empresa implicada en las hojas de operación (planning), implementando, o manteniendo las redes inalámbricas WLSM-basadas. Una audiencia secundaria incluye a los individuos implicados en proporcionar a los Productos y los servicios de la integración, o soporte a las organizaciones de la empresa las TIC.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco Catalyst 6500 Series WLSM
- Cisco Catalyst 6500 Series WiSM

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 Cisco](#) para obtener más información sobre las convenciones del documento.

Overview

Una estrategia de migración del Catalyst WLSM a la plataforma de WiSM del Catalyst incluye las hojas de operación (planning) y la ejecución de estas acciones:

- Planee para y instale el Catalyst WiSM.
- Instale la plataforma de WiSM del Catalyst.
- Instale la plataforma de administración de redes del Cisco Wireless Control System (WCS) para el Catalyst WiSM.
- Emigre las configuraciones del Catalyst WLSM a la plataforma WiSM-basada Catalyst para continuar el soporte de los Puntos de acceso autónomos todo ligeros y convertidos.
- Emigre los Puntos de acceso autónomos IOS® al protocolo del Lightweight Access Point (LWAPP) - plataforma IOS habilitada (fuera del alcance del documento).
- Entrene al personal de servicio técnico en la plataforma y la solución de WiSM del Catalyst.
- Limpie las configuraciones heredadas cuando la migración es completa.

Diferencias arquitectónicas

Cisco Catalyst 6500 Series WLSM

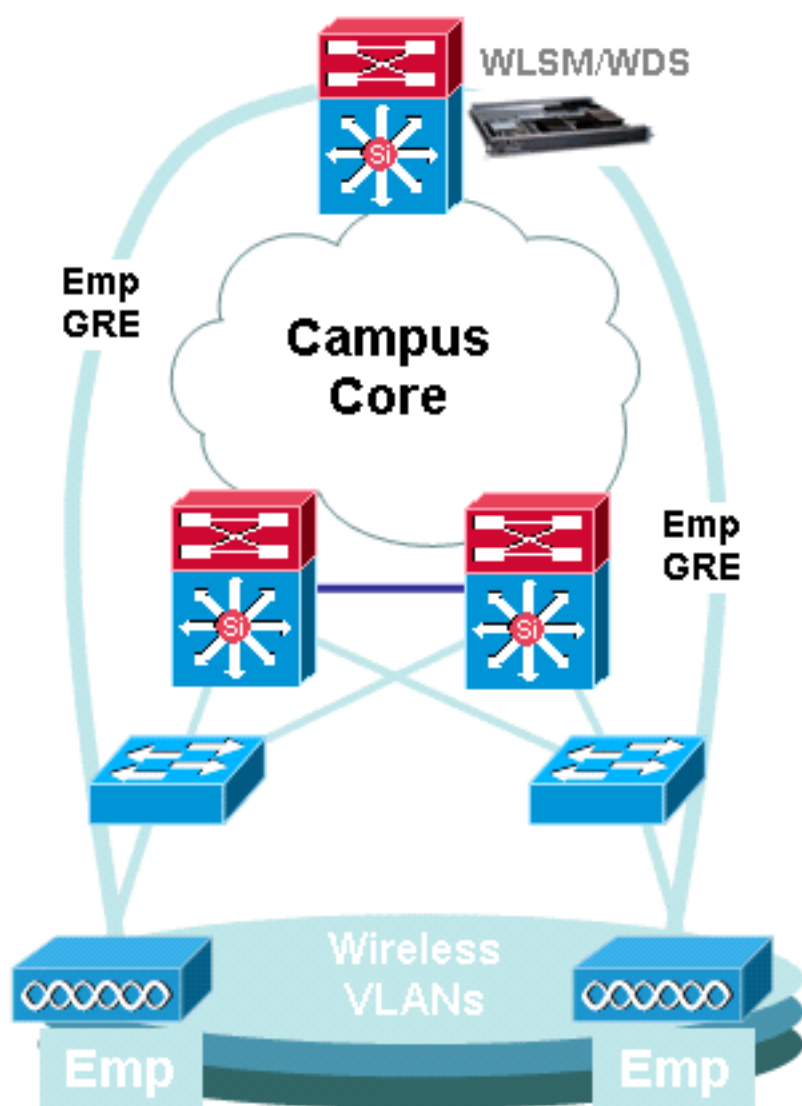
Las Cisco Catalyst 6500 Series WLSM pueden ser instaladas y configurado en ningunos abra el slot de 3, de 6, de 9, o del Cisco Catalyst 6500 Series Switch 13-slot equipado de un Supervisor Engine 720. Las Cisco Catalyst 6500 Series WLSM trabajan con los Puntos de acceso autónomos del Cisco Aironet y Cisco trabaja el Wireless LAN Solution Engine (WLSE).

Las Cisco Catalyst 6500 Series WLSM se despliegan típicamente en la capa de distribución o el centro de datos. Se despliegan raramente en el Wiring Closet. Un Punto de acceso autónomo conecta con cualquier puerto del switch en cualquier red de la capa 3. El Switches o el Routers de la conexión en sentido ascendente no tiene que ser configurado y no se requiere ninguna

asignación VLAN o trunks específicos. Antes de que el tráfico se pase activamente, el Punto de acceso autónomo se puede autenticar como dispositivo de la red de confianza.

Uno de los conceptos más importantes introducidos con el uso del WLSM es el grupo de la movilidad. Un cliente de red inalámbrica experimenta la itinerancia inconsútil (mantiene todas sus sesiones IP) cuando se mueve entre dos Puntos de acceso configurados para ser una parte del mismo grupo de la movilidad. Una asignación única entre el Service Set Identifier (SSID) para el costado de radio y el ID de la red para la cara tela define a un grupo de la movilidad en el Punto de acceso. El ID de la red representa la red lógica sobrepuesta construida encima de la infraestructura existente usando los túneles del Generic Routing Encapsulation (GRE), y su asignación al SSID substituye eso entre el SSID y el VLAN ID.

Refiera al [Guía de despliegue del Módulo de servicios del Wireless LAN de las Cisco Catalyst 6500 Series \(WLSM\)](#) para información detallada sobre cómo configurar y desplegar el WLSM.



Observe que un VLAN todavía está asociado a cada SSID. Estos VLAN ahora se definen solamente en el Punto de acceso y no necesitan ser configurados en los Switches de la capa de acceso o de la capa de distribución. El único propósito de la porción del VLAN de la configuración es proporcionar un atascamiento entre el cifrado asociado al VLAN a un SSID específico.

<pre>dot11 vlan-name Emp vlan 3</pre>	<pre>interface Tunnel3</pre>
---------------------------------------	------------------------------

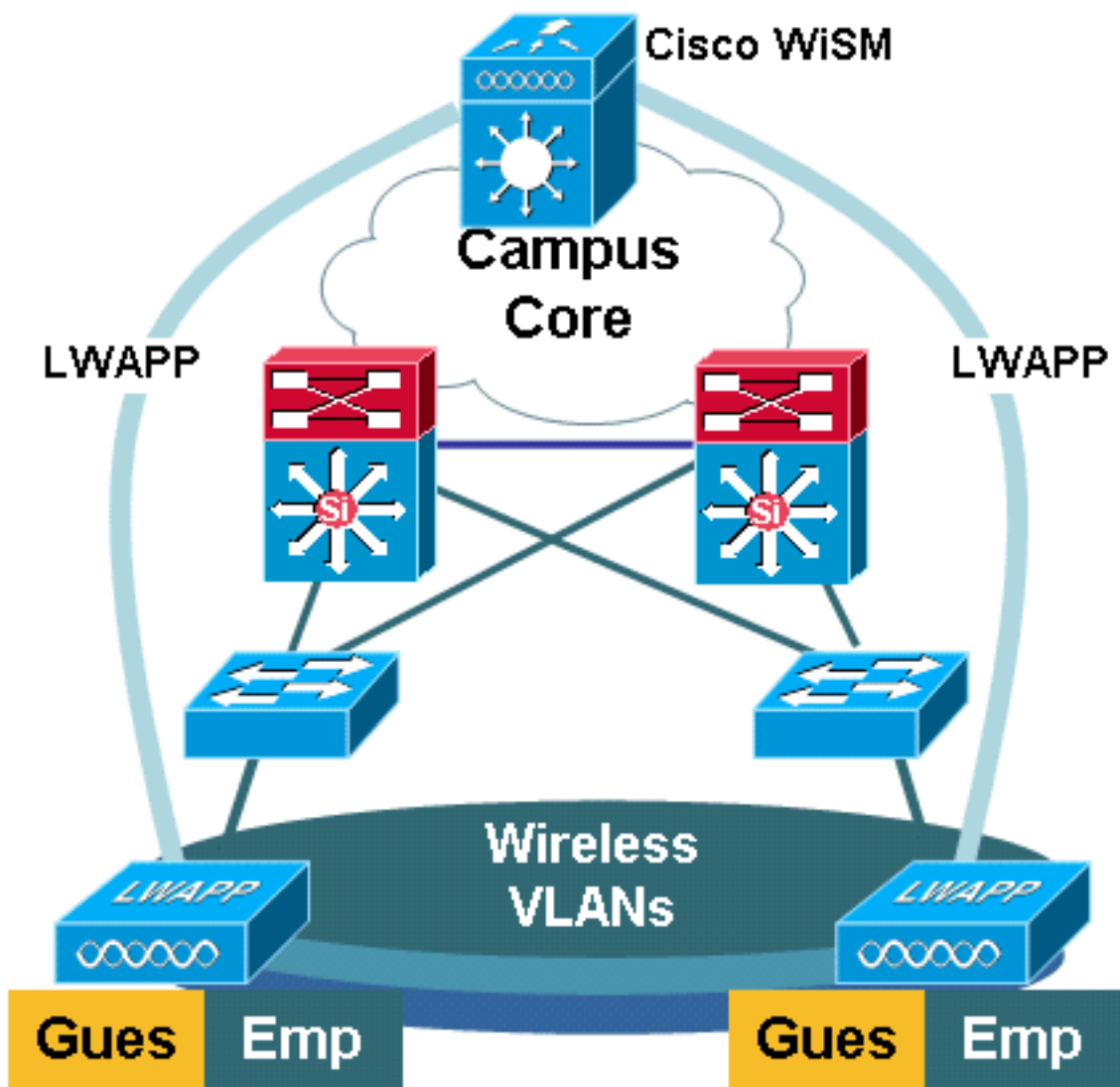
<pre> ! dot11 ssid Employee vlan 3 authentication open eap eap_methods authentication network-eap eap_methods authentication key-management wpa mobility network-id 3 ! interface Dot11Radio0 no ip address no ip route-cache ! encryption vlan 3 mode ciphers tkip ! ssid Employee </pre>	<pre> description mGRE for employees ip address 10.10.3.1 255.255.255.0 no ip redirects ip mtu 1476 ip dhcp snooping packets tunnel source Loopback3 tunnel mode gre multipoint mobility network-id 3 ! </pre>
--	--

Cisco Catalyst 6500 Series WiSM

Las Cisco Catalyst 6500 Series WiSM son un miembro de las redes también llamadas del Cisco Unified Wireless de la familia del controlador LAN de la tecnología inalámbrica de Cisco (WLC). Cisco WiSM trabaja conjuntamente con los Puntos de acceso ligeros del Cisco Aironet (revestimientos) y Cisco WCS. Cisco WiSM integra suavemente en las redes para empresas existentes de las Cisco Catalyst 6500 Series. Escala para entregar el acceso de red inalámbrica seguro, de la empresa a la tubería, la bifurcación, y los campus remotos. Comunica usando el LWAPP para establecer la conectividad segura entre los Puntos de acceso y los módulos a través de las redes de la capa 3. Desde un punto de vista de la gestión de tráfico, todo el tráfico de datos que origina de los clientes de red inalámbrica asociados a los revestimientos es encapsulado por los Puntos de acceso ellos mismos y llevado a un WLC, que agrega el tráfico y representa el monopunto del ingreso y de la salida para el tráfico IP a y desde la red alámbrica.

Sin embargo, estas diferencias existen:

- El tráfico es tunneled de los Puntos de acceso al regulador centralizado, que leverages el LWAPP y no el GRE.
- El control y el tráfico de datos se lleva vía el LWAPP. El tráfico de datos utiliza el puerto 12222 UDP, el tráfico de control se encapsula en el puerto 12223 UDP, y los mensajes de la movilidad utilizan los puertos 16666/16667 UDP.
- El tráfico de control es Advanced Encryption Standard (AES) - cifrado, y los datos está en el claro.
- No hay un túnel lógico separado para cada SSID definido. Solamente un solo túnel lógico se construye entre cada Punto de acceso y el WLC. Este túnel del LWAPP se utiliza para llevar el tráfico de datos para todos los clientes de red inalámbrica asociados al Punto de acceso, sin importar el SSID que se asocian a.



Estrategia de migración

Software del producto de la actualización

Actualice el software en estos Productos:

- Necesidades del supervisor 720 de funcionar con el Cisco IOS Software Release 12.2(18)SXF2 o Posterior
- El Catalyst 6500 WLSM necesita ejecutar 1.4.1 o más adelante
- El Catalyst 6500 WiSM necesita ejecutar 3.2.78.4 o más adelante
- Los Puntos de acceso del Cisco Aironet necesitan funcionar con el Cisco IOS Software Release 12.3.7JA2 o Posterior (para ser convertido al LWAPP)

Implemente las configuraciones

Implemente estas configuraciones:

- Configure al supervisor 720 para soportar Cisco WiSM.

- Configure el VLA N para la interfaz de administración de WiSM en el supervisor 720.
- Configure el VLA N para la interfaz dinámica del WiSM en el supervisor 720.
- Configure el DHCP al alcance para la interfaz del servicio o configure estáticamente la dirección IP.
- Pruebe las nuevas redes de la capa 3 por problemas de ruteo.

Refiera a la [guía de configuración de Cisco WiSM](#) y [resuelva problemas y configure el módulo de Servicios inalámbricos inicial \(WiSM\) puesto](#) para los detalles en cómo completar estas configuraciones.

[Configure el Catalyst 6500 WiSM para emigrar el SSID del Catalyst 6500 WLSM](#)

En el caso de la arquitectura de Cisco WLSM, el SSID configurado en un Punto de acceso se asocia a una red de la movilidad que haga un túnel todo el tráfico del cliente al Catalyst 6500. Este GRE de múltiples puntos (mGRE)) los túneles tienen una sola punta de terminación en el módulo del supervisor 720 del Catalyst 6500 que recibe el WLSM. El otro punto final lógico del túnel existe en todos los Puntos de acceso que participen en la red de la movilidad de la capa 3. En el caso de una plataforma de Cisco WiSM, el SSID se representa como red inalámbrica (WLAN). Cada red inalámbrica (WLAN) se asocia a la interfaz de administración o a una interfaz dinámica operador-definida. Las interfaces dinámicas operador-definidas son análogas a los VLA N y actúan como relé DHCP para los clientes de red inalámbrica.

Un túnel del mGRE se debe definir en el módulo del supervisor 720 para cada grupo de la movilidad. Aquí está un ejemplo de una interfaz de túnel MGRE en un supervisor 720. Todos los clientes de red inalámbrica utilizan la dirección IP de la interfaz del túnel como el default gateway. La red-identificación de la movilidad define esto como red única de la movilidad. La red-identificación de la movilidad definida para este túnel también se define bajo una de las definiciones del Punto de acceso SSID para identificar su participación en esta red de la movilidad de la capa 3.

Nota: Un grupo de la movilidad es un grupo de clientes de red inalámbrica que se agrupan juntos para una cierta característica compartida tal como una autenticación o un esquema de encriptación común, o de tipos de usuario tales como visitantes y empleados.

Esta salida muestra la configuración en el supervisor 720:

```
interface Tunnel172
  description to_wireless_clients
  ip address 172.16.1.1 255.255.255.0
  ip helper-address 10.1.1.11
  no ip redirects
  ip dhcp snooping packets
  tunnel source Loopback100
  tunnel mode gre multipoint
  mobility network-id 172
```

Esta salida muestra la configuración correspondiente en el Punto de acceso:

```
interface Dot11Radio0
  no ip address
  no ip route-cache
  !
  encryption vlan 172 mode ciphers tkip
  !
```

```
ssid light
vlan 172
authentication network-eap eap_methods
authentication key-management wpa
mobility-network-id 172
```

Para convertir esta configuración a la arquitectura de WiSM, usted necesita crear un nuevas dinámico/interfaz VLAN, le asigna una dirección IP en una diversa subred, y la asocia a una red inalámbrica (WLAN).

El nombre de la interfaz de la red inalámbrica (WLAN) corresponde al nombre SSID en los Puntos de acceso del Cisco Aironet. En este ejemplo es "luz". Cuando usted mantiene un nombre similar, la experiencia del usuario es mínima. La única diferencia es el segmento de la dirección IP de donde asignan los clientes de red inalámbrica una dirección IP.

1. Cree el nuevo VLA N en el supervisor 720 y agreguelo a la base de datos de VLAN.

```
c6506-t(config)#interface vlan 45
c6506-t(config-if)#ip add 172.16.2.1 255.255.255.0
c6506-t(config-if)#no shut
c6506-t(config-if)#end
c6506-t(config)#vlan 45
c6506-t(config-vlan)#state active
c6506-t(config-if)#end
```

2. Permita el VLA N en las interfaces Gigabit trunked.

```
c6506-t(config)#interface range gig 1/1-4
c6506-t(config-if-range)#switchport mode trunk
c6506-t(config-if-range)#switchport trunk encap dot1q
c6506-t(config-if-range)#switchport trunk native vlan 201
c6506-t(config-if-range)#switchport trunk allowed vlan 201,45
c6506-t(config-if-range)#mls qos trust dscp
c6506-t(config-if-range)#spanning-tree portfast
c6506-t(config-if-range)#channel-group 1 mode on
c6506-t(config-if-range)#end
```

3. Una vez que el VLA N se permite en la interfaz trunked, se permite automáticamente en la interfaz de canal de puerto.

```
c6506-t#show run interface port-channel 1
!
interface Port-channel1
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 201
  switchport trunk allowed vlan 45,201
  switchport mode trunk
  no ip address
end
c6506-t#
```

4. Complete estos pasos para crear la interfaz dinámica en el Catalyst 6500 WiSM a través de la interfaz Web. Elija el regulador > las interfaces y haga clic nuevo.

Cisco Systems | Save Configuration | Ping | Logout | Refresh

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP

Controller

- General
- Inventory
- Interfaces
- Network Routes
- Internal DHCP Server

Interfaces New...

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
ap-manager	untagged	172.20.225.139	Static	Enabled
management	untagged	172.20.225.138	Static	Not Supported
service-port	N/A	192.168.2.22	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported

Ingrese un nombre de la interfaz y el VLAN ID y el tecleo **se aplican**.

Cisco Systems | Save Configuration | Ping | Logout | Refresh

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP

Controller

- General
- Inventory
- Interfaces

Interfaces > New < Back | Apply

Interface Name

VLAN Id

Ingrese la información apropiada del IP Address y la información y el tecleo del servidor DHCP **se aplican**.

Cisco Systems | Save Configuration | Ping | Logout | Refresh

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP

Controller

- General
- Inventory
- Interfaces
- Network Routes
- Internal DHCP Server
- Mobility Management
 - Mobility Groups
 - Mobility Statistics
- Spanning Tree
- Ports
- Master Controller Mode
- Network Time Protocol
- QoS Profiles

Interfaces > Edit < Back | Apply

General Information

Interface Name

Interface Address

VLAN Identifier

IP Address

Netmask

Gateway

Physical Information

The interface is attached to a LAG.

DHCP Information

Primary DHCP Server

Secondary DHCP Server

Access Control List

ACL Name

Elija los **WLAN** y haga clic **nuevo** para agregar un nuevo SSID en Cisco WISM.

Cisco Systems | Save Configuration | Ping | Logout | Refresh

MONITOR | **WLANs** | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP

WLANs

WLANs
WLANs
AP Groups VLAN

WLANs

WLAN ID	WLAN SSID	Admin Status	Security Policies
1	secure-1	Disabled	802.1X

[Edit](#) [Remove](#) [Mobility Anchors](#)

New...

Agregue la luz SSID y el tecleo se aplica.

Cisco Systems | Save Configuration | Ping | Logout | Refresh

MONITOR | **WLANs** | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP

WLANs

WLANs
WLANs
AP Groups VLAN

WLANs > New

WLAN ID: 2

WLAN SSID: light

[< Back](#) [Apply](#)

Cambie el parámetro del nombre de la interfaz al VLA N apropiado. Otros parámetros de seguridad, tales como el servidor de RADIUS apropiado y las configuraciones de encriptación deben corresponder a la configuración en el Punto de acceso autónomo de Cisco. En este ejemplo, el nombre de la interfaz se cambia a **VLAN45** y cambian al tipo de la Seguridad de la capa 2 al **WPA2**.

Cisco Systems | Save Configuration | Ping | Logout | Refresh

MONITOR | **WLANs** | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP

WLANs

WLANs
WLANs
AP Groups VLAN

WLANs > Edit

WLAN ID: 2

WLAN SSID: light

General Policies

Radio Policy: All

Admin Status: Enabled

Session Timeout (secs): 1800

Quality of Service (QoS): Silver (best effort)

WMM Policy: Disabled

7920 Phone Support: Client CAC Limit AP CAC Limit

Broadcast SSID: Enabled

Allow AAA Override: Enabled

External Policy Validation: Enabled

Client Exclusion: Enabled ** 60 Timeout Value (secs)

DHCP Server: Override

DHCP Addr. Assignment: Required

Interface Name: vlan45

Security Policies

IPv6 Enable:

Layer 2 Security: WPA2

MAC Filtering

Layer 3 Security: None

Web Policy *

* Web Policy cannot be used in combination with IPsec and L2TP.

** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)

[< Back](#) [Apply](#)

Aquí está la nueva luz SSID.

Cisco Systems | Save Configuration | Ping | Logout | Refresh

MONITOR | **WLANs** | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP

WLANs

WLANs
WLANs
AP Groups VLAN

WLANs

WLAN ID	WLAN SSID	Admin Status	Security Policies
1	secure-1	Disabled	802.1X
2	light	Enabled	RSN (802.1x)

[Edit](#) [Remove](#) [Mobility Anchors](#)

[Edit](#) [Remove](#) [Mobility Anchors](#)

New...

Si se utiliza un nuevo SSID, no se requiere ningunas otras configuraciones. Si se utiliza un SSID existente, actualice solamente un en un momento del dominio RF para prevenir los

problemas de la movilidad entre el Catalyst 6500 WSLM y el Catalyst 6500 WiSM. Una vez que se configuran los WLAN, marque si las directivas de la red inalámbrica (WLAN) están correctas. Por ejemplo, ACL, QoS, y así sucesivamente. Asegúrese que Cisco WCS es en servicio y está listo para ser configurado para manejar Cisco WiSM.

Conversión del LWAPP del Punto de acceso

La migración del modo de punto de acceso autónomo al modo ligero es posible en estas Plataformas del Punto de acceso del Cisco Aironet:

- Todo el Cisco Aironet 1130 Puntos de acceso AG
 - Todo el Cisco Aironet 1240 Puntos de acceso AG
 - Para todas las plataformas de punto de acceso modular de la serie 1200 basadas en IOS (Upgrade de Cisco IOS Software 1200/1220, 1210 y 1230 AP), depende de la radio: si se soportan 802.11G, MP21G y MP31G si se soportan el 802.11a, CB21A y CB22A
 - Los Puntos de acceso del Cisco Aironet de la serie 1200 se pueden actualizar con cualquier combinación de radios soportadas — G solamente, A solamente, o G y A.
- . Los Puntos de acceso deben funcionar con el Cisco IOS Software Release 12.3(7)JA o Posterior antes de que usted pueda realizar la actualización. Refiera a [actualizar los Puntos de acceso autónomos del Cisco Aironet al modo ligero](#) para más información sobre el procedimiento de conversión.

Distribución del Punto de acceso entre los reguladores en Cisco WiSM

Si un Punto de acceso se configura ya con un IP Address estático, el Punto de acceso conserva la dirección IP después de que se convierta del modo autónomo al modo LWAPP. Si el Punto de acceso no está en la misma subred IP de la capa 2 que el regulador, después la resolución de DNS de CISCO-LWAPP-CONTROLLER@localdomain es el único mecanismo de detección garantizado del regulador. La utilidad de la actualización puede configurar a un Servidor de nombres antes de que usted cargue el Cisco IOS Software Release 12.3(7)JX. Verifique que el Servidor de nombres pueda resolver correctamente CISCO-LWAPP-CONTROLLER@localdomain antes de que usted comience los procedimientos de actualización.

Usted puede también utilizar la opción DHCP específica del vendedor 43 de volver uno o más IP Addresses del regulador a un Punto de acceso en el mensaje de la oferta de DHCP. El Punto de acceso envía un mensaje de la detección de LWAPP al IP Address de administración del regulador que recibe en la opción DHCP 43. Refiera al [Apéndice A: Configurar la opción DHCP 43 para los Puntos de acceso ligeros del Cisco Aironet en el servidor DHCP de la empresa de Windows 2003](#) para más información sobre cómo configurar la opción DHCP 43 en un servidor DHCP de la empresa de Windows 2003.

Pruebe con un número limitado de Puntos de acceso

Comience el proceso de migración con un solo Punto de acceso en una ubicación que sea fácilmente accesible por el administrador y después intente hacer un lugar remoto. Una vez que los Puntos de acceso se convierten al modo LWAPP y se completa la configuración de Cisco WiSM, pruebe a los clientes de red inalámbrica para:

- Ajustes de seguridad
- Aplicaciones estándares como el correo electrónico, acceso a internet, aplicaciones de base

de datos, y así sucesivamente

- Roaming ininterrumpido entre los Puntos de acceso y el control para ver si los clientes conservan los IP Addresses mientras que vagan por entre los Puntos de acceso.
- Cualquier problema del Maximum Segment Size del Transmission Control Protocol (TCP) (MSS) — descargue las páginas de Internet o los archivos grandes de la transferencia usando el File Transfer Protocol (FTP).
- Producción aceptable de los puntos de acceso de red inalámbrica según el diseño

[Despliegue completo](#)

Para moverse rápidamente con números más grandes del Punto de acceso, instale la utilidad de la actualización en más de una máquina para la conversión simultánea de los Puntos de acceso autónomos múltiples a los Puntos de acceso Lwapp-capaces.

[Troubleshooting](#)

Siga el procedimiento de Troubleshooting normal para los problemas específicos en el WLC. Refiera al [Troubleshooting FAQ del regulador del Wireless LAN \(WLC\)](#) para más detalles en el troubleshooting.

[Información Relacionada](#)

- [Soporte de la Tecnología de la WLAN](#)
- [Consejos de Troubleshooting de la Herramienta de Upgrade de LWAPP](#)
- [Nota de configuración del Módulo de servicios del Wireless LAN de las Catalyst 6500 Series](#)
- [Módulo de servicios del Wireless LAN de las Cisco Catalyst 6500 Series - Q&A](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)