

# Actualización segura de puntos de acceso, evitando daños en la imagen que provocan loops de inicio

## Contenido

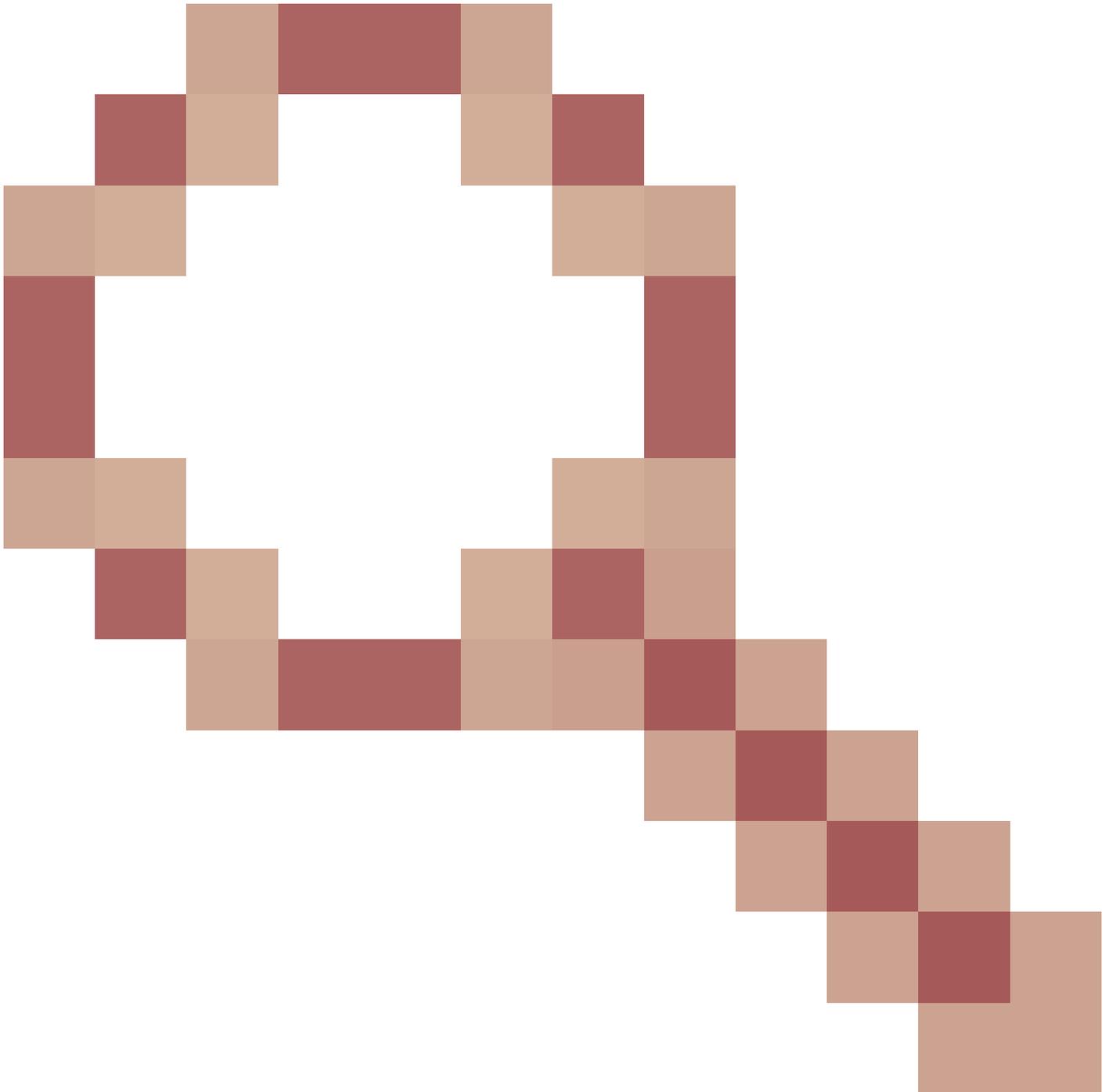
---

---

### Introducción

Algunos puntos de acceso (AP) de Cisco pueden descargar una imagen dañada a través de CAPWAP desde un controlador de la serie 9800. Dependiendo de la versión del software del AP, el AP puede intentar arrancar la imagen corrupta, dando como resultado un loop de arranque. En este artículo se explica qué modelos de punto de acceso y qué rutas de red son susceptibles a la corrupción de imágenes y cómo actualizar de forma segura.

Si sus AP están ahora en un loop de inicio debido a este problema, vea el artículo [Recuperarse de un loop de inicio causado por la corrupción de la imagen en los puntos de acceso de Wave 2 y 11ax \(CSCvx32806\)](#)



) para obtener orientación sobre los pasos de recuperación.

## Cómo saber si una actualización es susceptible a la corrupción de la imagen

Sus AP pueden ser susceptibles de descargar software dañado y luego intentar arrancar ese software, si las siguientes condiciones pertenecen a su implementación:

### Productos no afectados

- Controladores de LAN inalámbrica (WLC): los AP que se descargan de los controladores de LAN inalámbrica de AireOS no se ven afectados

- Mobility Express, controlador inalámbrico integrado
- AP: los AP Aironet 1800/1540/1100AC Series Wave 2 11ac y los puntos de acceso Wave1 11ac (1700/2700/3700/1570/IW3700) no se ven afectados (aunque estos AP se registren en WLC 9800, no se verán afectados)
- AP Wi-Fi 6E introducidos desde 2023: IW9167, IW9165, C9163

## Productos afectados

- WLC: La descarga de AP de los controladores de LAN inalámbrica de Cisco Catalyst serie 9800 puede verse afectada
- AP: Los siguientes modelos de AP que se registran en Cisco Catalyst 9800 Series Wireless LAN Controllers se ven afectados :
  - Puntos de acceso Aironet Wave2 11ac (2800/3800/4800/1560/IW6330/ESW6300)
  - Puntos de acceso Catalyst serie 9100 Wi-Fi6 (9105/9115/9117/9120/9124/9130/WP-WIFI6/ISR-AP1101AX)
  - Puntos de acceso Catalyst serie 9100 Wi-Fi6E (9136/9162/9164/9166)

## Versiones afectadas: el Síndrome de Arrancar una Imagen Mala

Este problema, donde el AP intenta arrancar una imagen que sabe que está dañada, se resuelve con los siguientes ID de bug de Cisco: [CSCvx32806](#), [CSCwc72021](#), [CSCwd90081](#), que se solucionan en las siguientes versiones:

- 8.10.185.0 y superior
- 17.3.7 y superior
- 17.6.6 y superior
- 17.9.3 y superior
- 17.11.1 y superiores

Una vez que el punto de acceso se actualiza al software con las correcciones anteriores, es posible que descargue una imagen dañada; sin embargo, no intentará arrancar esa imagen, sino que continuará intentando realizar la descarga hasta que tenga éxito.

## Rutas de red afectadas

El problema de corrupción de la imagen AP no se ha visto con una trayectoria LAN entre el 9800 y los AP - es decir, las trayectorias con una MTU IP completa de 1500 bytes, con latencia baja y pérdida de paquetes muy baja no se ven afectadas. Es más probable que el problema se produzca en túneles CAPWAP a través de una WAN, con las siguientes características de ruta:

- gran pérdida de paquetes
- MTU CAPWAP baja (menos de 1485 bytes): cuanto menor sea la MTU, mayor será el riesgo
  - la MTU CAPWAP baja puede ser un síntoma de pérdida de paquetes

## Cómo Saber Si Su Ruta De Red Está En Riesgo

- En el 9800, verifique CAPWAP Path MTU con

<#root>

9800-L#show capwap detailed

Name	APMAC	SourceIP	SrcPort	DestIP	DestPort
------	-------	----------	---------	--------	----------

MTU

Mode	McastIf				
Capwap1	D4AD.BDA2.8240	192.168.203.203	5247	192.168.6.100	5248

1485

Mode	McastIf				
Capwap2	084F.F983.4A40	192.168.203.203	5247	192.168.6.103	5253

1005

multicast Mc1

- Si la MTU de un AP determinado está fluctuando, eso es un fuerte indicador de riesgo
- **O show ap config general | incluir CAPWAP\ ruta\ MTU** (en show tech-support wireless)
  - Utilice [Wireless Config Analyzer Express \(WCAE\)](#) en la salida "show tech-support wireless" del 9800 para ver la MTU de los AP en Access Points > Configuration
- En el 9800, utilice "show ap uptime" y busque los AP con un "tiempo de actividad del AP" largo y un "tiempo de actividad de la asociación" corto
  - Si no hay ninguna razón para que los AP tengan un tiempo de actividad de asociación corto (es decir, ninguna reconfiguración), esto puede indicar una trayectoria de red en riesgo

## Cómo actualizar de forma segura desde una versión de software de AP no fija

 Nota: Si su implementación es susceptible a la corrupción de la imagen (es decir, modelos de AP afectados, que ejecuten software sin la corrección para el Síndrome de Arrancar una Imagen Mala, con características de WAN en riesgo), entonces no actualice simplemente actualizando el software 9800, y haciendo que los AP se vuelvan a unir y descarguen el nuevo software; pueden estar sujetos a la corrupción de la imagen y entrar en un loop de arranque. En su lugar, utilice uno de estos métodos:

### Actualización mediante un WLC local a los AP

Si es posible, coloque un controlador de almacenamiento provisional en la LAN de los AP - esto podría ser un 9800-CL, o (para Wave 2 / Wi-Fi 6 AP) un AP en modo EWC, y actualice los AP a la versión de destino. A continuación, podrán unirse de forma segura al controlador de producción.

### Actualización mediante un controlador AireOS

Si tiene un controlador AireOS que ejecuta 8.10.190.0 o superior, y si sus modelos AP son compatibles con AireOS, una los AP a ese controlador. Esto actualizará con seguridad los AP al software fijo, y entonces podrán unirse con seguridad al controlador de producción.

## Actualización mediante archive download-sw

Almacene las imágenes de AP de destino en un servidor TFTP / SFTP que sea accesible para los AP de actualización. Las actualizaciones de la imagen AP a través de TFTP o SFTP no están sujetas al problema de corrupción de la imagen. Los AP pueden iniciar una solicitud de descarga de imagen desde la CLI del AP o (si los AP están unidos al controlador) desde la CLI del controlador.

1. Configure un servidor TFTP o SFTP en una ubicación accesible para los AP. Tenga en cuenta que el rendimiento de TFTP está controlado por la latencia, por lo que las descargas serán lentas si el servidor TFTP es remoto desde los AP. Dado que SFTP utiliza TCP, su rendimiento será mucho mejor si se utiliza una ruta de alta latencia. Sin embargo, SFTP no se puede activar desde el WLC, ya que requiere un diálogo interactivo para introducir el nombre de usuario y la contraseña.
2. Almacene las imágenes AP deseadas en un servidor TFTP o SFTP. [Consulte la Tabla 4 en la Matriz de compatibilidad](#) para la versión 15.3(3)J\* AP que se asigna a la versión IOS-XE deseada, luego descargue las imágenes apropiadas del software Lightweight AP para los modelos de AP afectados [desde software.cisco.com](#).

1. Por ejemplo, la imagen 17.9.5 AP para un CW9162 [isap1g6b-k9w8-tar.153-3.JPN4.tar](#).

3. Para actualizar a través de la CLI del AP: si se puede acceder a la CLI del AP a través de la consola o SSH:

1. Ingrese el comando TFTP o SFTP:

```
archive download-sw /no-reload tftp://<ip-address>/<apimage>
```

or

```
archive download-sw /no-reload sftp://<ip-address>/<apimage>
```

Nombre de usuario: *USER*

Contraseña: *XXX*

Esto sobrescribirá la imagen dañada con la imagen válida.

2. Una vez completada la descarga de la imagen, ejecute:

```
test capwap restart
```

Esto reiniciará el proceso CAPWAP, de modo que el AP reconozca la imagen recién instalada.

3. Para actualizar un gran número de AP a través de "archive download-sw", en lugar de ingresar el comando en cada AP individualmente, puede utilizar un método de scripting. Consulte Upgrade APs Via WLAN Poller a continuación.

4. Si los AP se unen a un controlador, puede actualizar los AP desde la CLI del controlador (sólo TFTP):

1. En IOS-XE: `ap name APNAME tftp-downgrade ip.addr.of.server imagename.tar`

2. En AireOS: `config ap tftp-downgrade ip.addr.of.server imagename.tar APNAME`

1. Aunque las descargas CAPWAP de AireOS no son susceptibles a la corrupción de la imagen, si usted está planeando migrar sus AP de AireOS a 9800, primero debe descargar una imagen AP

con las correcciones para Alt-boot y el síndrome Boot a Bad Image (8.10.190.0 o superior), antes de unir los AP a 9800.

- Supervise los registros del servidor TFTP o SFTP para verificar que cada AP haya descargado correctamente la imagen. Una vez que se complete la descarga, cada AP se recargará, ejecutando la imagen recién descargada.

## Actualice los AP a través de Predownload, Monitoreo de errores

Cargue la imagen de destino en el 9800 y utilice la predescarga de AP para insertar la nueva imagen en el AP, mientras monitorea los casos de corrupción de la imagen de AP.

Paso 1. Verifique que SSH esté habilitado bajo los AP Join Profile(s) en el WLC C9800. Configure un servidor syslog en la red. Configure la dirección IP del servidor syslog en Perfil de unión a AP para todos los sitios y establezca el valor de trampa de registro en Debug. Verifique que el servidor syslog esté recibiendo syslogs del AP.

### Edit AP Join Profile

- General
- Client
- CAPWAP
- AP
- Management**
- Security
- ICap
- QoS

---

- Device**
- User
- Credentials
- CDP Interface

---

#### TFTP Downgrade

IPv4/IPv6 Address:

Image File Name:

#### System Log

Facility Value:

Host IPv4/IPv6 Address:

Log Trap Value:

Secured ⓘ

#### Telnet/SSH Configuration

Telnet

SSH

Serial Console ⓘ

#### AP Core Dump

Enable Core Dump

Paso 2. Descargue la imagen del software en el WLC C9800 para prepararse para la predescarga mediante CLI:

```
C9800# copy tftp://x.x.x.x/C9800-80-universalk9_wlc.17.03.07.SPA.bin bootflash:  
C9800# install add file bootflash:C9800-80-universalk9_wlc.17.03.07.SPA.bin
```

Paso 3. Ejecute la predescarga de la imagen AP en los WLC del Cisco C9800:

```
C9800# ap image predownload
```

Nota: en función de la escala y el tipo de implementación, esta operación puede tardar desde unos minutos hasta unas horas. No reinicie el controlador o los AP hasta que haya validado que sus imágenes son válidas.

Paso 4. Una vez que se haya completado la predescarga para todos los AP, verifique cualquiera de estos dos mensajes de registro en el servidor syslog:

- Firma de imagen verificada correctamente.
- Error de verificación de firma de imagen: -3

Además, verifique la salida del comando **show ap image summary**, verificando cualquier instancia de Failed to Download. Si el contador no es cero, busque los AP fallidos a través de **show ap image | include Failed**.

Precaución: Si algún AP registra falla de verificación de la firma de la imagen, o si algún AP no pudo descargarse, entonces **NO CONTINÚE CON EL PROCESO DE ACTUALIZACIÓN**. Si todos los AP mostraron el mensaje "Image signing success", entonces todos los AP descargaron correctamente la imagen, y puede continuar con seguridad con la actualización 9800.

Paso 5. Si algún AP mostró una falla de verificación o no pudo descargar, entonces, para evitar un loop de inicio, necesitará sobrescribir la imagen en la partición de respaldo del AP con una descarga de archivo de una imagen de AP independiente mediante el siguiente proceso.

Si el número de AP fallidos es pequeño, puede simplemente SSH a cada AP e iniciar los pasos siguientes.

```
COS_AP#term mon
COS_AP#show clock
COS_AP#archive download-sw /no-reload tftp://<ip-address>/%apimage%
COS_AP#show version
COS_AP#test capwap restart
```

Nota: "test capwap restart" es necesario para que el proceso CAPWAP del AP reconozca que la imagen en la partición de respaldo se ha actualizado. Esto provocará una breve interrupción del servicio, ya que se reiniciará la conexión CAPWAP con el 9800. Si se trata de un problema operativo, este paso se puede aplazar a una ventana de mantenimiento.

## Actualización de AP mediante el sondeador WLAN

Si el número de AP para actualizar vía archive download-sw es grande, puede utilizar un proceso automatizado usando el [sondeador WLAN](#).

Paso 1a. Instale el sondeador WLAN en un equipo Mac o [Windows](#).

Paso 1b. Rellene el archivo aplist csv con los AP fallidos relevantes.

Paso 1c. Rellene el archivo cmdlist con los siguientes comandos (siempre puede agregar más, a su discreción):

```
COS_AP#term mon
COS_AP#show clock
COS_AP#archive download-sw /no-reload tftp://<ip-address>/%apimage%
COS_AP#show version
COS_AP#test capwap restart
```

Paso 1d. Ejecute el sondeador WLAN.

Paso 1e. Una vez que se haya completado su ejecución, verifique cada archivo de registro de AP para validar la finalización exitosa.

Paso 2. Active inmediatamente la imagen en el WLC C9800 y recargue.

```
C9800#install activate file bootflash:C9800-80-universalk9_wlc.17.03.07.SPA.bin
- Confirm reload when prompted
```

Paso 3. Confirme la imagen en el WLC C9800. Omitir este paso hará que el WLC vuelva a la imagen de software anterior

```
C9800#install commit
```

## Preguntas Frecuentes

P. Ejecuté una predescarga hace algunos días, pero aún no he reiniciado mi WLC y AP Cisco C9800. No tengo registros del sistema para verificar si la imagen está dañada. ¿Cómo puedo verificar si la imagen está dañada?

A. Marque show logging en el registro del sistema/AP. Si no ve ningún mensaje de éxito o error en el resultado de show logging, puede utilizar el comando "show flash syslogs" para archivar el resultado de syslog desde cuando realizó la predescarga. Si ve el mensaje "Image signing verify success", entonces sabe que este AP ha descargado la imagen exitosamente.

P: Tengo una implementación centralizada con AP en modo local. ¿Debo seguir ejecutando los pasos que se indican en la sección Soluciones/Solución alternativa?

R: Este problema solo se ha notificado al actualizar los AP a través de una conexión WAN. Es muy poco probable que los AP en el modo local y en las redes locales se encuentren con este problema, por lo que no es necesario seguir este procedimiento para las actualizaciones, si está seguro de que hay muy poca pérdida de paquetes entre el controlador y los AP.

P: Tengo nuevos puntos de acceso listos para usar. ¿Cómo puedo implementarlos sin que se produzca este problema?

R: Los AP nuevos y listos para usar que descargan código a través de WAN también serán susceptibles a este problema, a menos que se hayan fabricado después de diciembre de 2023.

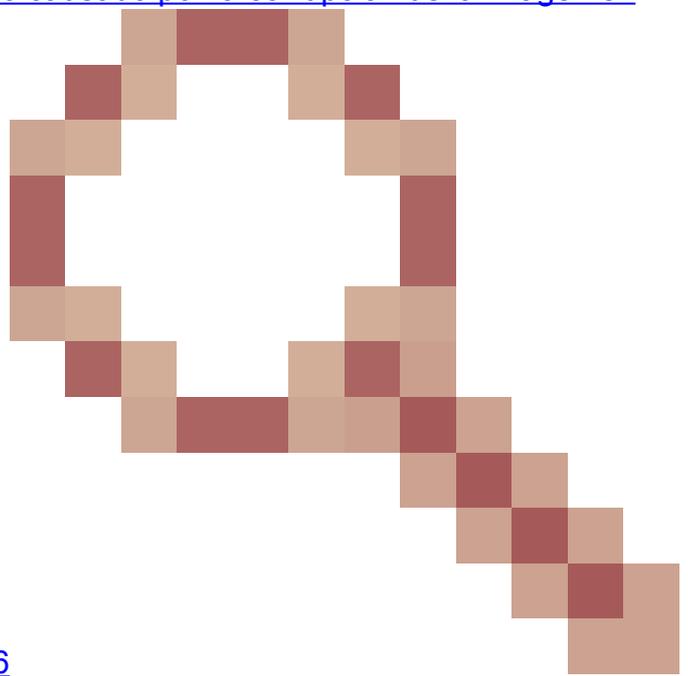
P: ¿Qué está haciendo Cisco a largo plazo para solucionar este problema con las descargas de imágenes CAPWAP del 9800 que se dañan?

R: Una vez que el AP ya está ejecutando 17.11 o superior, puede utilizar la función de descarga de imágenes fuera de banda para extraer la imagen del controlador usando HTTPS. TCP transmite datos de forma fiable mediante una ventana deslizante, por lo que también es mucho más rápido en una WAN que CAPWAP (o TFTP)

P. Tengo AP que ahora están en un loop de inicio. ¿Cómo puedo recuperarlos?

R: Vea el artículo [Recuperarse de un bucle de inicio causado por la corrupción de la imagen en](#)

[los puntos de acceso Wave 2 y 11ax \(CSCvx32806\)](#)  
).



## 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).