# Reparación de puntos de acceso C9105AXW con bloques defectuosos en Flash

## Contenido



## Introducción

Varios puntos de acceso C9105AXW (todos los PID) se fabricaron con un subsistema de flash NAND que, con el tiempo, puede marcar erróneamente los bloques como defectuosos. Una vez que se han marcado 94 bloques como malos, la tabla de bloques malos de flash está llena. Como resultado, el AP puede sufrir varios síntomas:

- El sistema de archivos flash puede quedar bloqueado por escritura, de modo que el AP ya no pueda confirmar cambios de configuración, escribir nuevos registros o descargar una nueva imagen. Pueden observarse errores similares a los siguientes:
  sync_log: no se pudo abrir /storage/syslogs/7: Sistema de archivos de sólo lectura
- El AP puede fallar, con un pánico del kernel que muestra errores UBIFS similares a los siguientes:
  <3>[02/06/2023 05:06:06.0290] Error UBIFS (ubi0:1 pid 5454): do_writepage: no se puede escribir la página 8 del nodo 54848, error -30
- Es posible que el AP no pueda arrancar; el registro de la consola muestra un error similar al siguiente:
  [01/01/1970 00:00:05.0600] error ubi0: ubi_eba_init: no hay suficientes bloques de borrado físicos (0, necesidad 1)
  [*01/01/1970 00:00:06.4720] error de montaje

En algunos casos, puede ser necesario reemplazar el AP.

Cisco ha implementado dos correcciones de errores para solucionar este problema.

## Correcciones de errores

### ID de bug de Cisco CSCwf50177 C9105AXW: gran número de bloques defectuosos

Este bugfix evita que los bloques flash sean marcados incorrectamente como "malos". Sin embargo, no repara los AP que ya tienen un número excesivo de bloques defectuosos.

### ID de bug de Cisco CSCwf68131 Supervisión y reparación de bloques defectuosos en C9105AXW

Esta corrección de errores repara los AP con bloques defectuosos excesivos. En el momento del arranque (en u-boot), si la tabla de bloques defectuosos del AP excede un número de umbral de entradas (predeterminado: 40; controlado por la variable u-boot SCRUB_LIMIT), la tabla de bloques defectuosos se vaciará, antes de que el AP arranque.

## Unidades afectadas

Solo los AP C9105AXW se ven afectados por este problema, no otros modelos de AP. Para determinar si las unidades C9105AXW dadas, abra el ID de bug de Cisco CSCwf50177 en BST y haga clic en "Verificar la Aplicabilidad del Bug", para ingresar los números de serie de los AP.

## Software fijo

Si ha afectado a C9105AXW, debe actualizar al software con correcciones para **ambos** errores de Cisco ID CSCwf50177 y el ID de bug de Cisco CSCwf68131 . Realice un seguimiento de este último error para conocer la disponibilidad de las correcciones en las distintas sucursales; a partir del 5 de septiembre de 2023, las correcciones estarán disponibles en las siguientes versiones:

### AireOS

- 8.10 MR10 EFT (8.10.189.111 o superior - ya disponible; 8.10 MR10 CCO versión prevista para finales de septiembre/octubre de 2023)
- 8.10 MR9 ESC (8.10.185.7 o superior - disponible en TAC ahora)

### Cisco IOS® XE

- 17.3.7 APSP5 o superior (caso TAC abierto)
- 17.3.8 (CCO a finales de septiembre/octubre de 2023)
- 17.6.5 APSP5 o superior (en CCO)
- 17.6.6 (CCO a finales de septiembre/octubre de 2023)
- 17.9.3 APSP5 o superior (en CCO)
- 17.9.4 APSP1 o superior (en CCO)
- 17.9.5 (CCO 2024)
- 17.12.2 (CCO noviembre de 2023)
- 17.13.1 (CCO diciembre de 2023)

## Verificación de APs Susceptibles para Bloques Malos Excesivos

En primer lugar, compruebe todos los C9105AXW susceptibles para ver cuántos bloques defectuosos tienen. Si ninguno tiene más de 60 bloques defectuosos, puede actualizar directamente.

### Comprobación de bloques defectuosos: 17,6 o superior

En cada C9105AXW sensible (determinado a partir de "Comprobar la aplicabilidad del error" para CSCwf50177) ), recopile la salida de "**show flash statistics**". Busque "recuento de bloques de borrado físicos defectuosos". Para automatizar la comprobación de un gran número de AP, utilice WLAN Poller.

### Comprobación de bloques defectuosos: 8.10 y 17.3

El TAC (u otro empleado de Cisco con acceso SWIMS) tendrá que ejecutar devshell en cada C9105AXW susceptible y ejecutar el siguiente comando:

```
ubinfo -a
```

Busque "recuento de bloques de borrado físicos defectuosos". Para automatizar la comprobación de un gran número de AP, utilice RADKit.

## Procedimiento de actualización

Si ha afectado a las unidades C9105AXW con bloques defectuosos excesivos, siga el siguiente procedimiento al actualizar al software fijo.

### Actualización en una sola implementación de controlador: completa nueva imagen de controlador

1. (Opcional) puede instalar la nueva imagen del controlador, pero **no la** active y **no** descargue previamente el nuevo software del punto de acceso a los C9105AXW afectados.

2. Mientras se sigue ejecutando la imagen del controlador **antiguo**, reinicie los C9105AXW afectados. Esto, en la mayoría de los casos, permitirá que los AP afectados se actualicen. (En algunos casos, es posible que sea necesario reemplazar algunos AP)

3. Ahora puede predescargar la nueva imagen del AP, si así lo desea.

4. Recargue el controlador, ejecute el nuevo software

### Actualización en una sola implementación de controlador: APSP

1. (Opcional) puede instalar el nuevo APSP, pero **no** lo active y **no** descargue previamente el nuevo software AP a los C9105AXW afectados.

2. Reinicie los C9105AXW afectados. Esto, en la mayoría de los casos, permitirá que los AP afectados se actualicen. (En algunos casos, es posible que sea necesario reemplazar algunos AP)

3. Ahora puede predescargar, activar y confirmar el APSP.

### Actualización en una implementación N+1

En esta situación, se utiliza un controlador de copia de seguridad para actualizar los C9105AXW afectados.

1. Mientras que los AP afectados todavía están unidos al controlador antiguo, actualice el controlador de respaldo al software fijo (versión completa del controlador, o APSP)

2. Recargue los AP afectados: haga que se vuelvan a unir al controlador antiguo. (En algunos casos, es posible que sea necesario reemplazar algunos AP)

3. Ahora reconfigure los AP afectados, para establecer su controlador principal en el actualizado, y haga que se unan al controlador de respaldo.

4. Después de que el controlador principal se haya actualizado al software fijo, puede mover los C9105AXW de nuevo a él.

---

# 8.10 Disponibilidad MR10 EFT

Formulario de inscripción: http://cs.co/810MR10-EFT-Signup

Release Notes: https://www.cisco.com/web/software/280926587/165753/Release_Notes_8_10_189_111.pdf

**8.10.189.111 Enlaces de descarga EFT (8.10.189.11)**
Controlador inalámbrico 8540
Controlador inalámbrico 5520
Controlador inalámbrico 3504
Controlador inalámbrico virtual
Mobility Express (1815)
Mobility Express 1850
Mobility Express 3800
Mobility Express 2800
Mobility Express 4800

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).