# 安全升级接入点，避免导致引导环路的图像损坏

## 目录

## 简介

某些思科接入点(AP)可能会通过CAPWAP从9800系列控制器下载损坏的映像。 根据AP的软件版本，AP可能会尝试引导损坏的映像，从而导致引导循环。 本文说明哪些AP型号、哪些网络路径容易出现映像损坏，以及如何安全升级。

如果AP此时由于此问题进入引导循环，请参阅从第2波和11ax接入点上因映像损坏引起的引导循环恢复(CSCvx32806)一文，了解恢复步骤的指导。

## 如何判断升级是否容易损坏映像

如果以下情况与您的部署有关，您的AP可能会下载损坏的软件，然后尝试启动该软件：

## 不受影响的产品

- 无线局域网控制器(WLC)：从AireOS无线局域网控制器下载的接入点不受影响
- Mobility Express、嵌入式无线控制器

- AP - Aironet 1800/1540/1100AC系列Wave 2 11ac和Wave 1 11ac接入点(1700/2700/3700/1570/IW3700)不受影响（即使这些AP注册到9800 WLC，它们也不会受影响）
- 自2023年起推出的Wi-Fi 6E AP：IW9167、IW9165、C9163

## 受影响的产品

- WLC：从Cisco Catalyst 9800系列无线局域网控制器下载的AP可能会受到影响
- AP：注册到Cisco Catalyst 9800系列无线局域网控制器的以下AP型号会受到影响：
  - Aironet Wave2 11ac无线接入点(2800/3800/4800/1560/IW6330/ESW6300)
  - Catalyst 9100系列Wi-Fi6接入点(9105/9115/9117/9120/9124/9130/WP-WIFI6/ISR-AP1101AX)
  - Catalyst 9100系列Wi-FI6E无线接入点(9136/9162/9164/9166)

## 受影响的版本：启动不良映像综合症

AP尝试引导它知道已损坏的映像时出现此问题，此问题通过以下Cisco漏洞ID解决：CSCvx32806、CSCwc72021、CSCwd90081，这些漏洞已在以下版本中修复：

- 8.10.185.0及更高版本
- 17.3.7及以上
- 17.6.6及以上
- 17.9.3及以上
- 17.11.1及以上

一旦接入点升级到带有上述修复程序的软件，它仍可能下载损坏的映像；但是，它不会尝试启动该映像，而是将继续重新尝试下载，直到其成功为止。

## 受影响的网络路径

在9800和AP之间的LAN路径中未发现AP映像损坏问题，即具有完整1500字节IP MTU、低延迟和极低数据包丢失的路径不会受到影响。 此问题更可能发生在广域网的CAPWAP隧道上，它具有以下路径特征：

- 高数据包丢失
- capwap MTU低（小于1485字节）- MTU越低，风险越高
  - 低CAPWAP MTU可能是数据包丢失的症状

## 如何判断您的网络路径是否有风险

- 在9800上，使用

```
<#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

  multicast Mc1
Capwap2       084F.F983.4A40 192.168.203.203 5247    192.168.6.103    5253

1005

  multicast Mc1
```

    - 如果给定AP的MTU波动，则这是一个强大的风险指标
- 或**show ap config general | include CAPWAP\ Path\ MTU** (在show tech-support wireless中)
    - 在9800的“show tech-support wireless”输出上使用无线配置分析器Express (WCAE)，在“Access Points”>“Configuration”下查看AP的MTU
- 在9800上，使用“show ap uptime”查找具有较长“AP运行时间”和较短“关联运行时间”的AP
    - 如果没有理由使AP具有短的关联运行时间（即无重新配置），则这可能表示存在风险的网络路径

# 如何从非固定AP软件版本安全升级

注意：如果您的部署易受映像损坏的影响（例如，受影响的AP型号、运行没有引导不良映像综合征修复程序的软件、存在有风险的WAN特性），则不要通过简单地升级9800软件来升级，也不要让AP重新加入和下载新软件-它们可能会受到映像损坏并进入引导环路的影响。 请改用以下方法之一：

## 使用本地到AP的WLC升级

如果可能，在AP的LAN上放置暂存控制器-这可能是9800-CL，或者（对于Wave 2/Wi-Fi 6 AP）在EWC模式下的AP，并将AP升级到目标版本。 然后，他们就可以安全地加入生产控制器。

## 通过AireOS控制器升级

如果您拥有运行8.10.190.0或更高版本的AireOS控制器，并且AireOS支持您的AP型号，请将AP加入到该控制器。 这样可以安全地将AP升级到固定软件，然后它们就可以安全地加入生产控制器。

## 使用archive download-sw升级

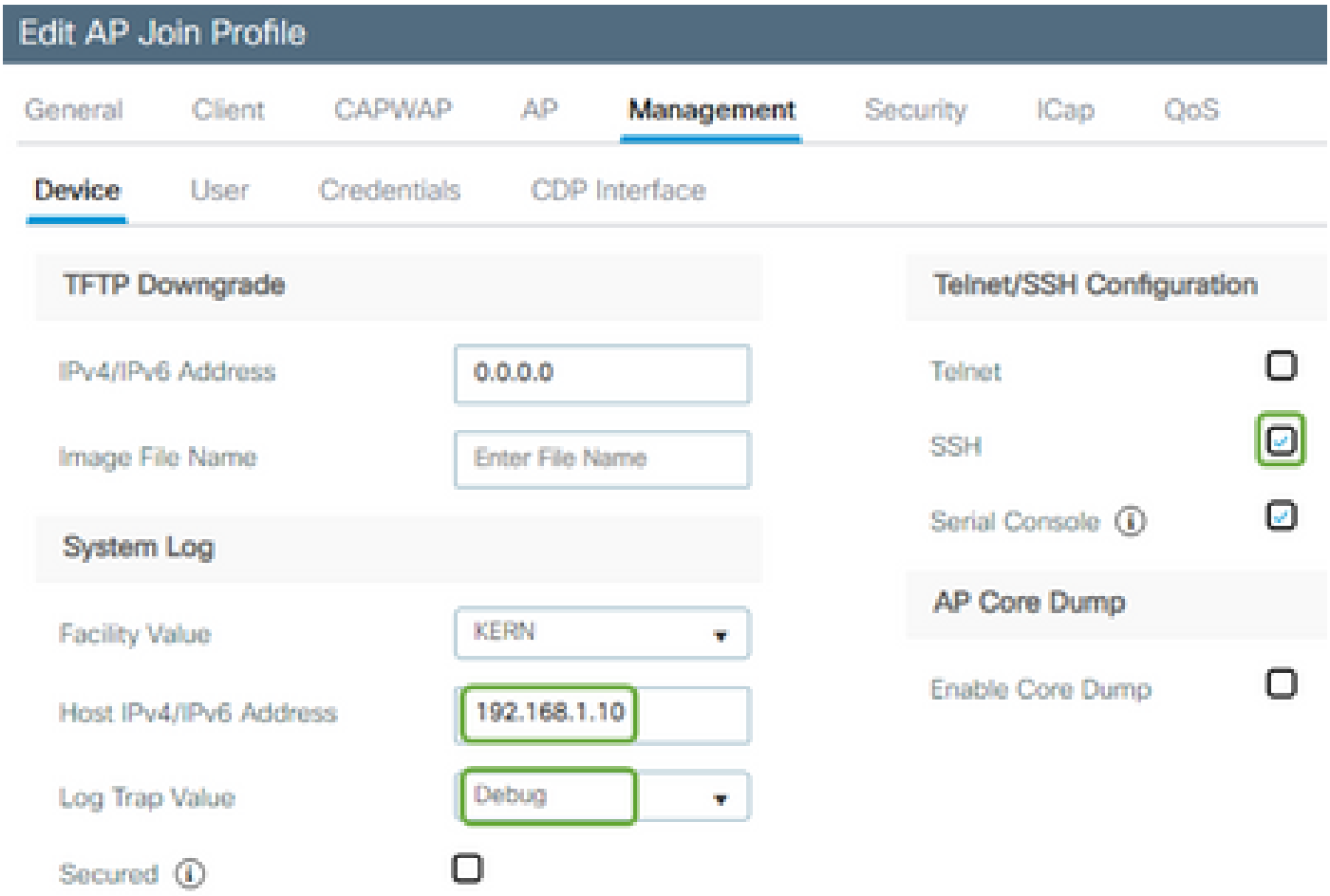
将目标AP映像暂存到升级AP可访问的TFTP/SFTP服务器上。 通过TFTP或SFTP升级的AP映像不存在映像损坏问题。 AP可以从AP CLI或（如果AP已加入控制器）从控制器CLI发起映像下载请求。

1. 在AP可访问的位置设置TFTP或SFTP服务器。 请注意，TFTP性能受延迟限制，因此，如果TFTP服务器与AP相距较远，下载速度会较慢。 由于SFTP使用TCP，因此如果采用高延迟路径，其吞吐量会好得多。 但是，无法从WLC触发SFTP，因为它需要交互式对话来输入用户名和密码。
2. 将所需的AP映像暂存到TFTP或SFTP服务器上。 请参阅15.3(3)J* AP版本的兼容性矩阵中的表4，该版本映射到所需的IOS-XE版本，然后从software.cisco.com下载适合受影响的AP型号的轻量AP软件映像。
    1. 例如，CW9162的17.9.5 AP映像isap1g6b-k9w8-tar.153-3.JPN4.tar。
3. 通过AP CLI升级：如果可以通过控制台或SSH访问AP的CLI：
    1. 输入TFTP或SFTP命令：
       **archive download-sw /no-reload tftp://<*ip-address*>/<*apimage*>**
       或
       **archive download-sw /no-reload sftp://<*ip-address*>/<*apimage*>**
       **用户名：*USER***
       **密码：*XXX***
       这将用有效映像覆盖损坏的映像。
    2. 映像下载完成后，发出：
       **test capwap restart**
       这将重新启动CAPWAP进程，以便AP能够识别新安装的映像。
    3. 要通过“archive download-sw”升级大量AP，而不是在每个AP中单独输入命令，您可以使用脚本编写方法。 请参阅下面的通过WLAN轮询器升级AP。
4. 如果AP已加入控制器，您可以从控制器CLI升级AP（仅限TFTP）：
    1. 在IOS-XE中：**ap nameAPNAMEtftp-*downgradeip.addr.of.server imagename.tar***
    2. 在AireOS中：**config ap tftp-*downgradeip.addr.of.server imagename.tarAPNAME***
        1. 虽然从AireOS下载的CAPWAP不易损坏映像，但如果您计划将AP从AireOS迁移到9800，则应在将AP加入9800之前，首先下载包含Alt-boot修复和Boot a Bad Image综合征（8.10.190.0或更高版本）的修复的AP映像。
    3. 监控TFTP或SFTP服务器日志，以验证每个AP是否已成功下载映像。 下载完成后，每个AP将重新加载，运行新下载的映像。

## 通过预下载和监控升级AP以发现错误

在9800上加载目标映像，并使用AP预下载将新映像推送到AP，同时监控AP映像损坏的实例。

步骤1:验证是否已在C9800 WLC上的AP加入配置文件下启用SSH。 在网络中设置系统日志服务器。在AP Join Profile for allthitests下配置系统日志服务器的IP地址，并将日志陷阱值设置为Debug。验证系统日志服务器是否正在从AP接收系统日志。




第二步：将软件映像下载到C9800 WLC，以准备通过CLI进行预下载：

```
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
```

第三步：在Cisco C9800 WLC上运行AP映像预下载：

```
C9800# ap image predownload
```

注意：根据部署规模和类型，这可能需要几分钟至几小时之间的任意时间。 请勿重新启动控制器或AP，直到验证其映像是否有效！

第四步： 所有AP的预下载完成后，在syslog服务器上检查以下两条日志消息之一：

- 映像签名验证成功。
- 映像签名验证失败： -3

此外，请检查**`show ap image summary`**命令的输出，并检查Failed to Download的所有实例。

如果计数器不为零，则通过show ap image查找出现故障的AP | include Failed。

注意：如果任何AP记录映像签名验证失败，或者任何AP下载失败，则不要继续升级过程。如果所有AP都显示“Image signing verify success”消息，则所有AP都已正确下载映像，您可以安全继续进行9800升级。

第5步：如果任何AP显示验证失败或下载失败，则为避免引导循环，您需要使用以下过程用单独的AP映像的归档文件下载覆盖AP备份分区中的映像。

如果故障AP的数量很少，则只需通过SSH连接到每个AP并启动以下步骤。

```
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
```

注意：需要“测试capwap重新启动”，以便AP的CAPWAP进程能够识别备份分区中的映像已更新。这会导致服务短暂中断，因为CAPWAP与9800的连接会重新启动。 如果这是操作问题，可以将此步骤延迟到维护窗口。

# 使用WLAN轮询器升级AP

如果要通过archive download-sw升级的AP数量很大，您可以使用WLAN轮询器的自动进程。

步骤1a.在Mac或Windows计算机上安装WLAN轮询器。

步骤1b.用相关故障AP填充aplist csv文件。

步骤1c.用以下命令填充cmdlist文件（您可以自行决定是否添加更多）：

```
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
```

步骤1d.执行WLAN轮询器。

步骤1e.执行完成后，请检查每个AP的日志文件以验证是否成功完成。

第二步：立即激活C9800 WLC上的映像并重新加载。

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

步骤3.在C9800 WLC上提交映像。跳过此步骤将导致WLC回滚到以前的软件映像

```
C9800#install commit
```

## 常见问题解答

问：我几天前运行了预下载，但尚未重新启动我的Cisco C9800 WLC和AP。我没有系统日志来验证映像是否已损坏。如何验证映像是否已损坏？

A.在AP/syslog上检查show logging。如果在show logging输出中看不到成功或失败消息，可以使用“show flash syslogs”命令归档执行预下载时的syslog输出。 如果您看到“Image signing verify success”消息，则表明此AP已成功下载映像。

问：我拥有本地模式下的AP集中部署。是否仍需要执行“解决方法/解决方案”部分列出的步骤？

答：仅当通过WAN连接升级AP时，才会报告此问题。本地模式下的AP和本地网络上的AP极有可能遇到此问题，因此如果您确信控制器和AP之间的数据包丢失率极低，则无需执行此升级过程。

问：我有新的开箱即用的AP。如何在不遇到此问题的情况下部署它们？

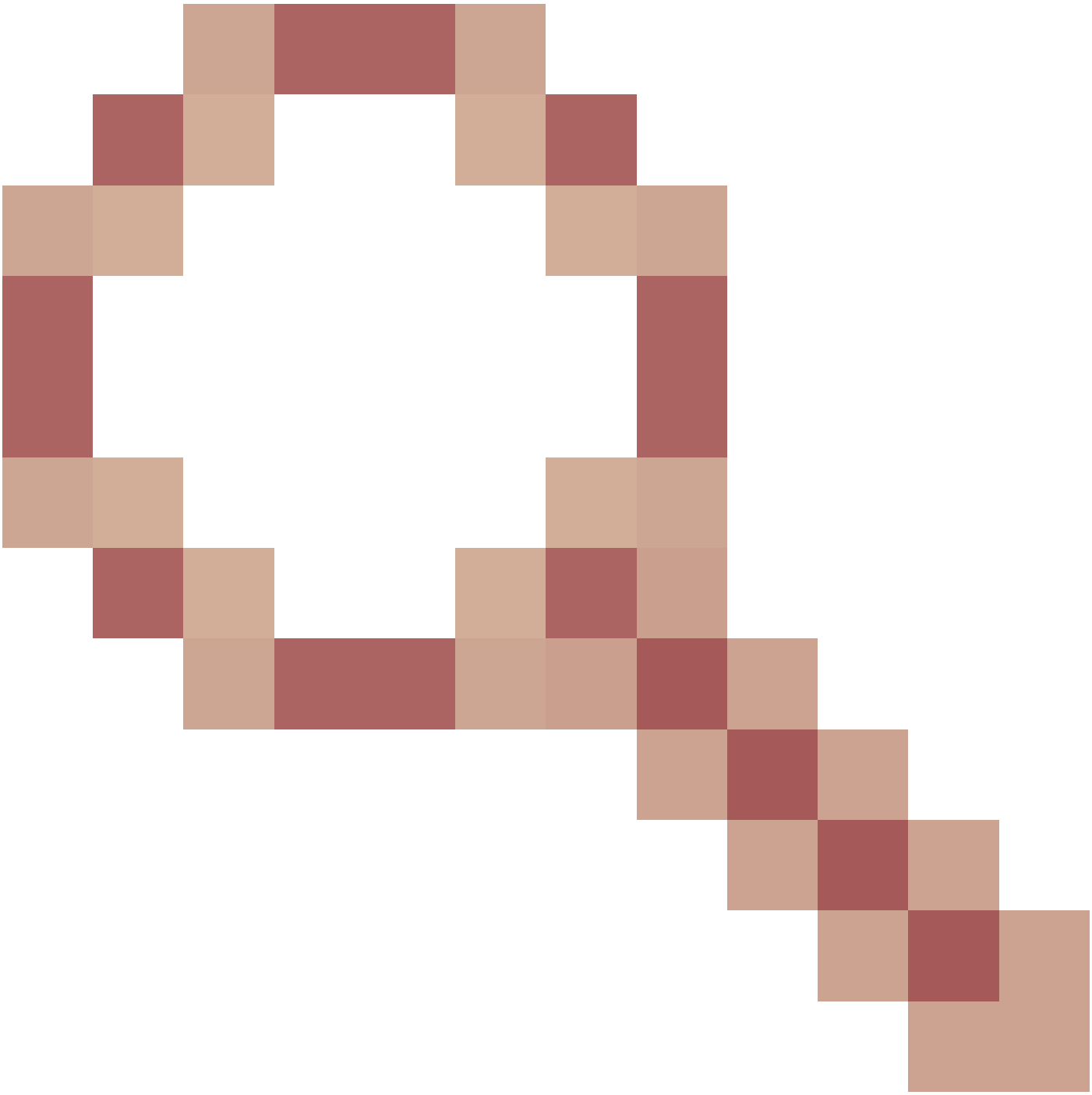
答：除非在2023年12月之后生产，否则通过广域网下载代码的新开箱即用无线接入点也容易出现此问题。

问：从长远来看，思科如何解决从9800下载的CAPWAP映像损坏的问题？

答：当AP已运行17.11或更高版本时，它可以使用带外映像下载功能通过HTTPS从控制器中提取映像。TCP使用滑动窗口可靠地传输数据-因此在WAN上传输数据的速度也比CAPWAP（或TFTP）快得多

问：我有AP现在处于引导环路中。 如何恢复它们？

答：请参阅文章“Recover from a boot loop caused by image corruption on Wave 2 and 11ax Access Points (CSCvx32806



)”。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。