了解远程部署的接入点映像升级

目录

简介

思科接入点映像升级方法

挑战:通过广域网下载标准CAPWAP映像

CAPWAP映像下载窗口增强

- 流程概述
- 配置(CLI)
- 验证(CLI)
- 限制/注意事项

FlexConnect模式下的高效映像升级

- 流程概述
- 好处
- 配置(CLI)
- 验证(CLI)
- 限制/注意事项

基于带外HTTP的AP映像下载

- 使用案例
- 流程概述
- 配置(CLI)
- 配置(GUI)
- 验证(CLI)
- 限制/注意事项

通过TFTP/SFTP手动升级单个AP

- 流程概述
- 配置(AP CLI)
- 确认
- 限制/注意事项

使用哪种方法

结论

参考

简介

本文档介绍如何通过广域网高效升级思科AP映像，解决延迟和可靠性难题。

思科接入点映像升级方法

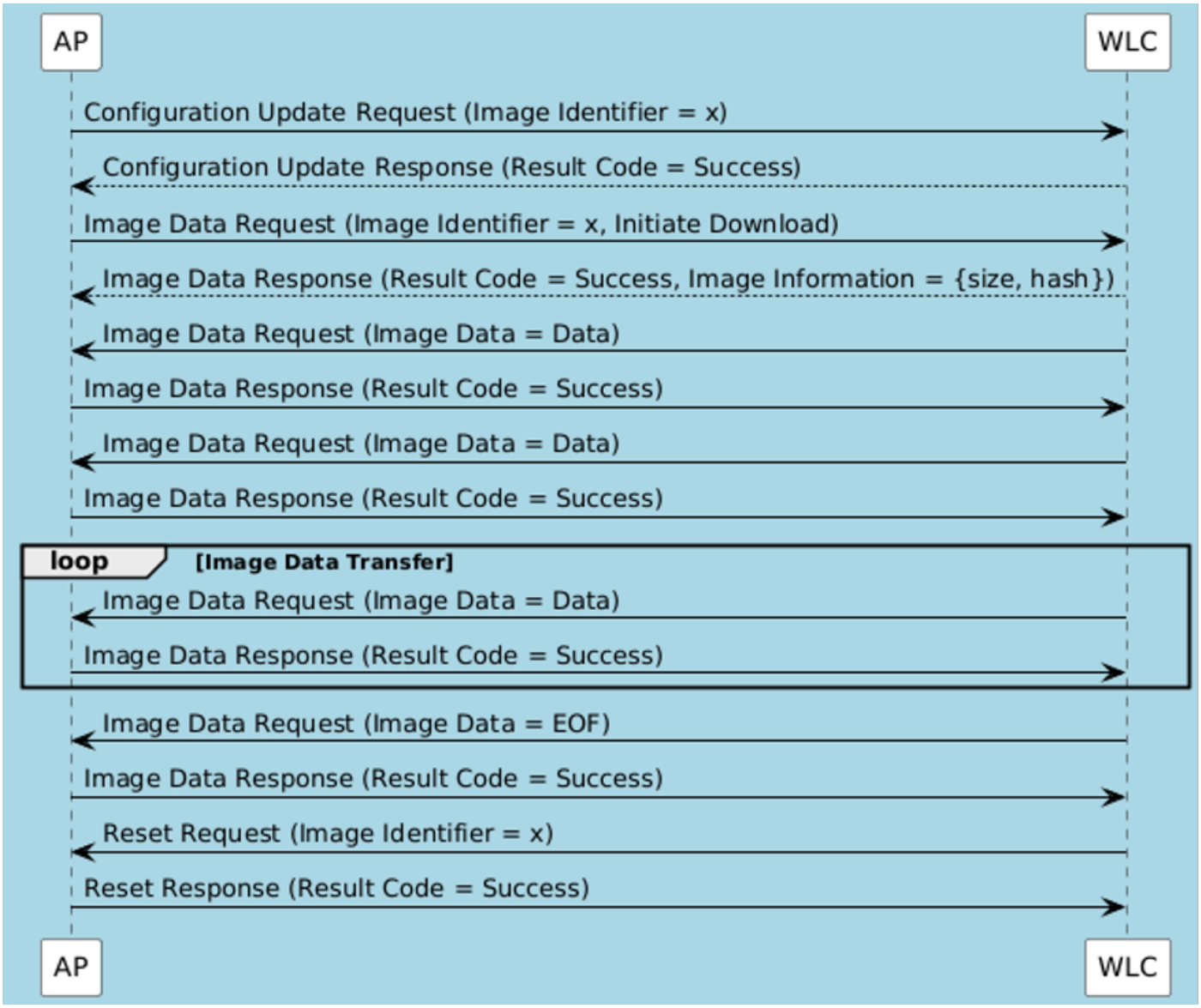
定期映像升级对于思科接入点(AP)至关重要，但是通过高延迟广域网(WAN)链路执行到远程站点的升级可能颇具挑战性。标准CAPWAP映像下载方法虽然对本地网络有效，但速度较慢，而且在

WAN上的可靠性可能较低。本部分探讨为什么会出现这种情况，并概述为高效远程升级而设计的替代和增强方法。

挑战:通过广域网下载标准CAPWAP映像

通过CAPWAP升级AP映像的基本过程在RFC 5415第9.1节中定义。此机制允许无线局域网控制器(WLC)通过CAPWAP隧道将新的AP映像直接提供给连接的AP。 对于包含固件数据块的每个图像数据请求消息（RFC 5415,9.1.1部分），WLC在发送下一个块之前，会等待来自AP的相应图像数据响应确认（RFC 5415,9.1.2部分）。

该图说明当AP处于运行状态时AP和WLC之间的映像传输过程。

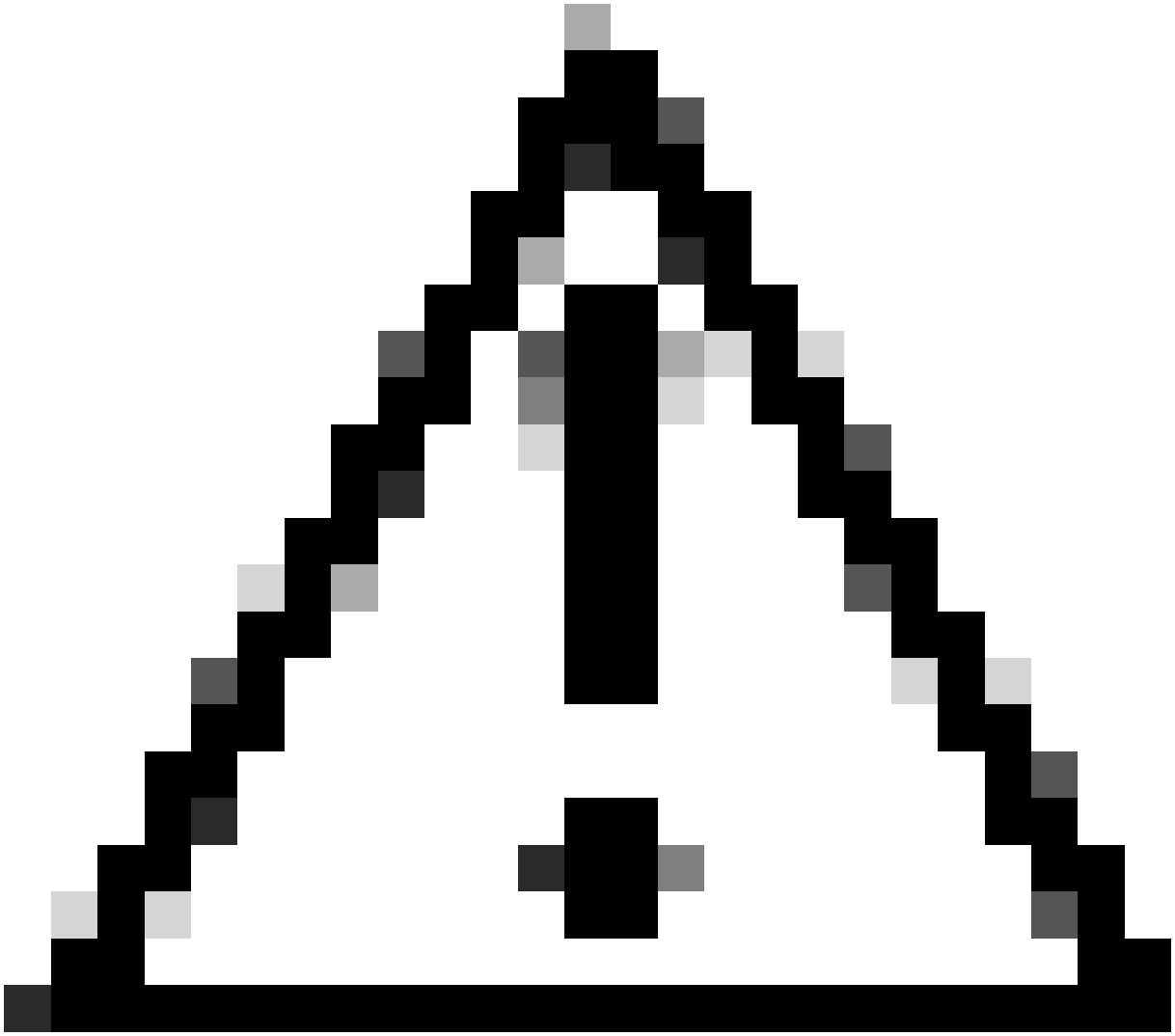


AP映像传输处理流程

如前所述，WLC发送包含固件图像数据块的Image Data Request消息。AP通过发送图像数据响应消息确认收到这些数据块。此交换将持续到传输整个映像为止。

对于每个图像数据请求消息，相应的图像数据响应消息应作为确认。这意味着AP必须等待每个图像数据包到达，确认数据包，然后等待下一个数据包。这会导致WAN环境中的映像下载缓慢。

举个例子：如果AP和WLC之间的往返时间(RTT)为100ms，这实际上将传输速率限制为每秒大约10个数据包。如果每个数据包大小为1000字节，则表示最大吞吐量为10 KB/秒。如果AP映像为50MB，理论上的完成传输的最小时间大约为5120秒。这说明，即使有大量的带宽可用，CAPWAP映像下载也会因为这种停止等待确认机制而感觉缓慢。在WLC和AP属于同一园区网络且延迟最小的本地图像传输中，此效果不太明显。



警告：有损耗的WAN链路可能会导致映像损坏。请参阅Cisco bug IDCSCwf09053 了解更多信息。

为了缓解标准CAPWAP控制路径传输机制固有的这些限制，尤其是对于高延迟或带宽受限的广域网环境，引入了三项增强功能。

1. CAPWAP窗口增强功能通过实现多数据包滑动窗口来改进CAPWAP控制路径本身，该滑动窗口允许在要求确认之前发送多个数据包，从而在CAPWAP框架内的高延迟链路上增加吞吐量。

2. FlexConnect模式下的高效映像升级是专门为FlexConnect AP设计的优化方法，FlexConnect AP通常部署在广域网带宽有限的分支机构中。此方法通过分配映像下载任务来最大程度降低WAN负载。
3. 基于带外HTTPs的AP映像下载方法利用在控制器上的专用Web服务器上运行的独立、更高效的HTTPs协议进行映像传输，将其移至限制性CAPWAP控制隧道之外，从而解决这一问题。

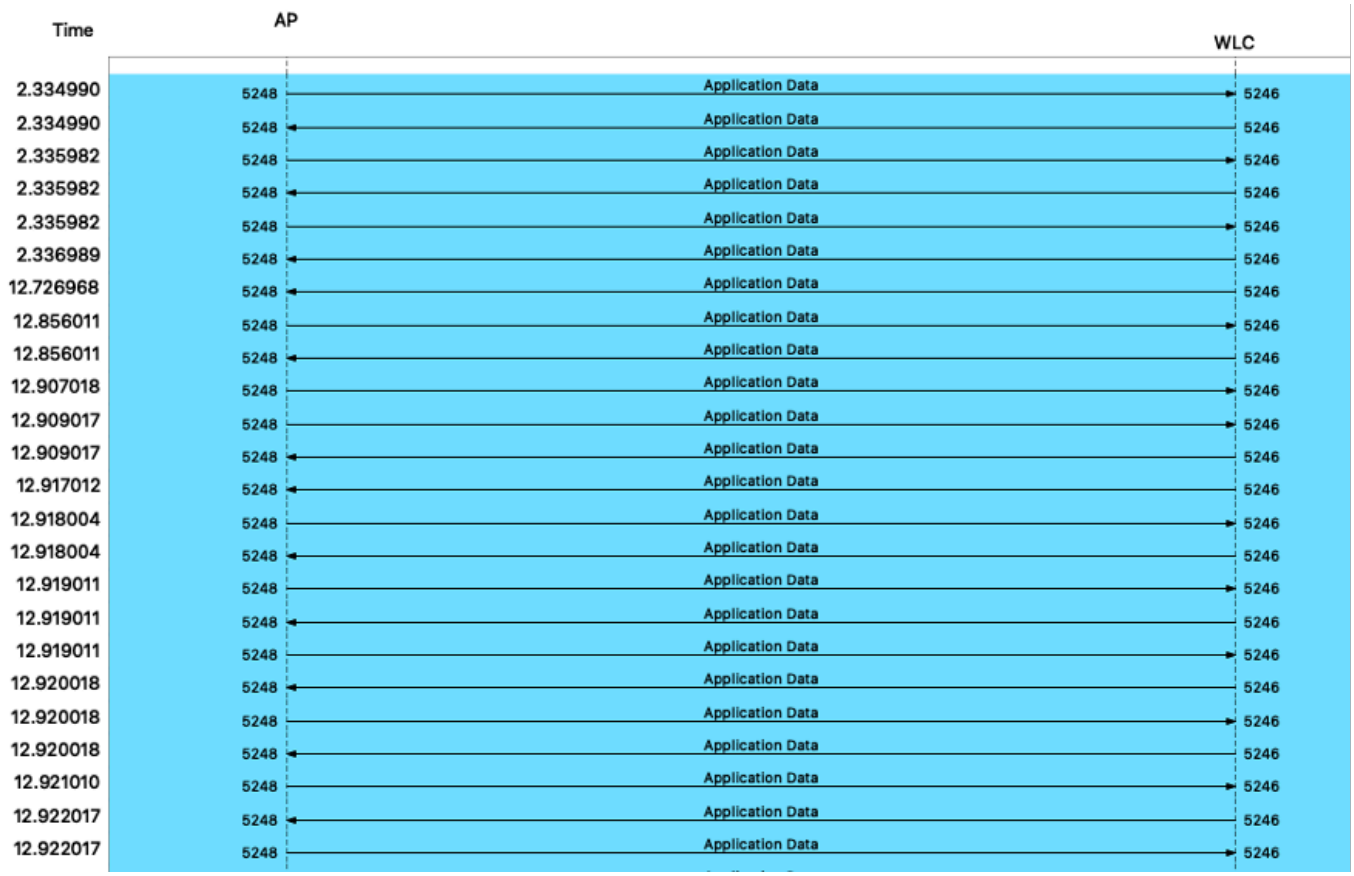
CAPWAP映像下载窗口增强

此功能可提高Office Extend无线接入点(OEAP)或远程工作人员AP专用的基于CAPWAP的映像下载速度。它解决了标准CAPWAP控制通道具有单一窗口的限制，该窗口要求每个数据包在发送下一个数据包之前进行确认，从而降低了高延迟链路上的传输速度。此增强功能增加了对控制数据包的多个滑动窗口的支持。

CAPWAP窗口大小的影响

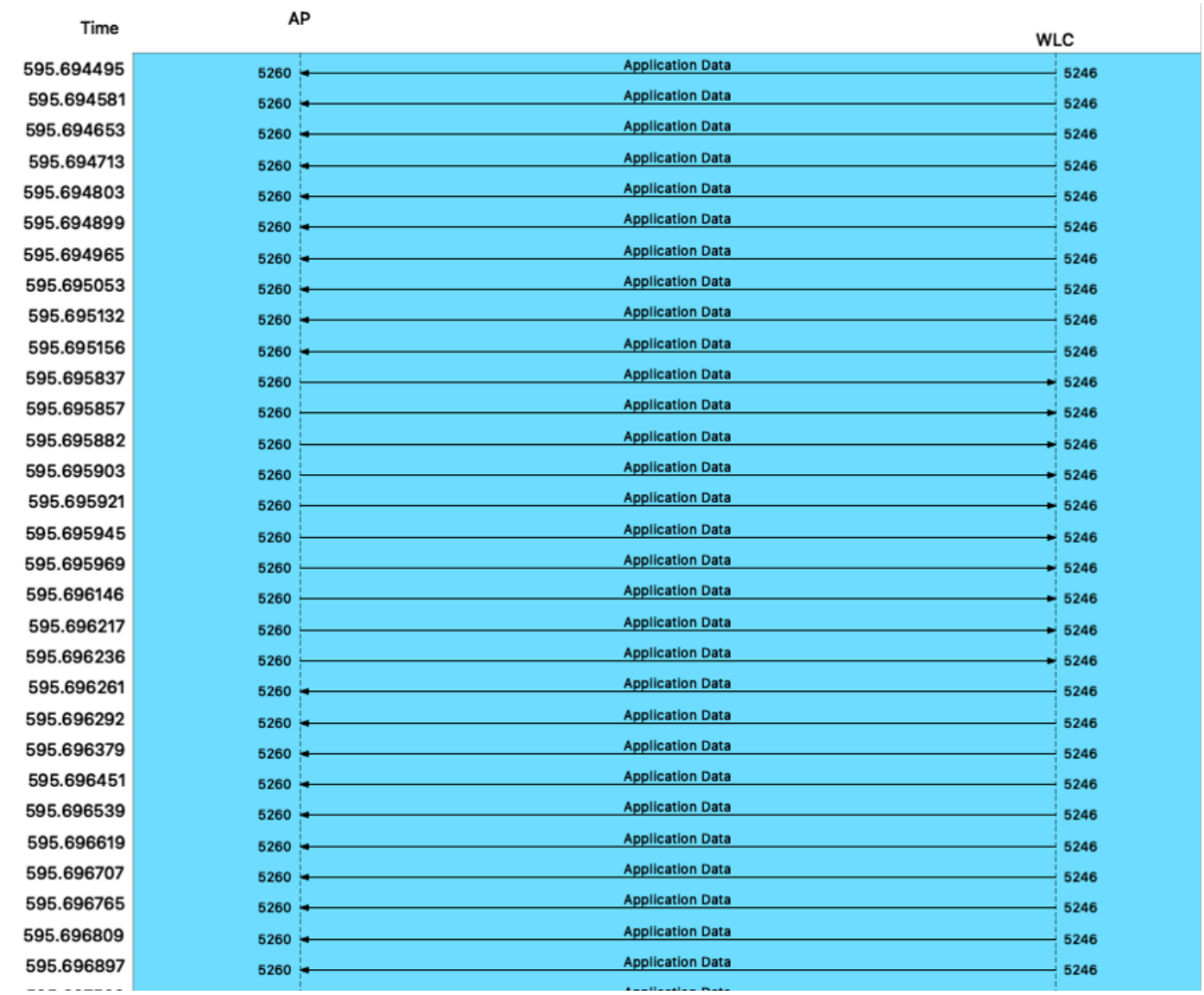
通过控制信道的CAPWAP映像下载过程的效率受配置的窗口大小影响显着，尤其是在高延迟链路上。

CAPWAP窗口大小= 1（默认/标准）：数据包流表现出严格的停止和等待行为。对于WLC发送的每个图像数据请求数据包，WLC会暂停并等待来自AP的图像数据响应确认，然后再发送下一个数据包。



窗口大小为1的CAPWAP映像升级流程

CAPWAP窗口大小= N（例如，20）：数据包流演示了滑动窗口机制。滑动窗口允许多个数据包在需要确认之前通过链路传输，从而有效地屏蔽了延迟。



窗口大小为20的CAPWAP映像升级流程

流程概述

1. 专门为OEAP/远程工作人员AP配置AP配置文件。
2. 在此配置文件中将CAPWAP窗口大小设置为大于1。
3. 将此AP配置文件关联到OEAP/远程工作人员AP。
4. 在AP加入过程中，将应用配置的窗口大小。
5. 后续的CAPWAP映像下载使用更大的窗口大小，从而提高吞吐量。

配置(CLI)

配置AP配置文件并设置CAPWAP窗口大小：

<#root>

```
configure terminal ap-profile capwap window size
```

```
  <- Between 3 to 20
```

```
end
```

将AP配置文件关联到站点标记并应用于AP（类似于高效映像升级中的步骤2和3，确保正确的AP配置文件通过站点标记链接）。

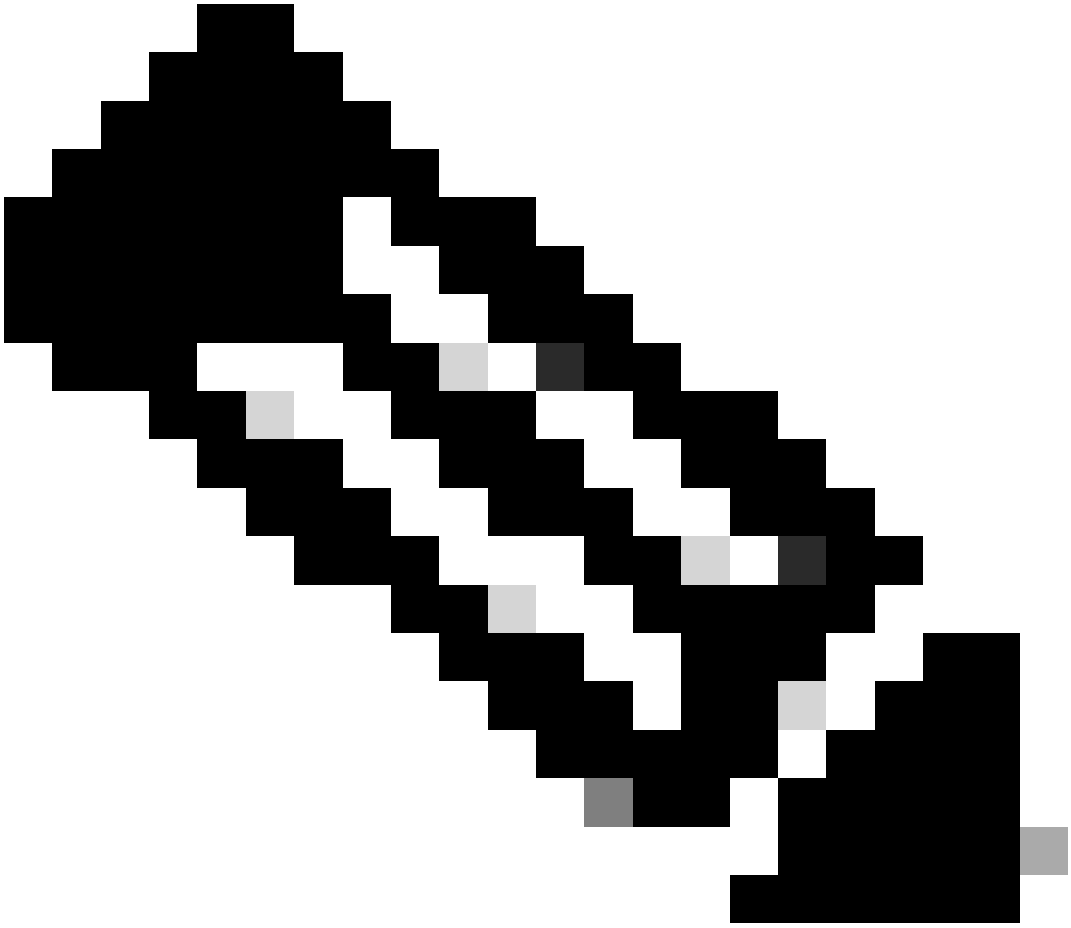
验证(CLI)

```
<#root>

show ap profile name detailed
 | in indo <- View CAPWAP window size in an AP profile
show capwap client rcb
 | in Window <- View CAPWAP status and modes for a specific AP(Look for CAPWAP Sliding Window and Activ
show ap config general
 | in indo <- View AP configuration details(Shows Capwap Active Window Size)
```

限制/注意事项

- 仅OEAP配置文件支持此增强功能。
- 仅在AP加入过程中在AP上更新窗口大小。
- 如果AP上已存在最新的升级映像，则不会触发预下载。



注意：虽然此增强功能主要针对OEAP进行记录，但是也观察到其适用于常规FlexConnect AP。但是，FlexConnect部署未对此进行充分测试/支持。

FlexConnect模式下的高效映像升级

高效映像升级是专门为FlexConnect AP设计的优化方法，尤其适用于广域网带宽有限的分支机构部署。此方法通过指定站点标记内的主AP从控制器下载映像，然后允许同一站点标记内的其他从属AP通过TFTP从主AP下载映像，从而最大限度地降低WAN负载。主AP是每个站点标签的每个型号一个AP。

流程概述

1. 新的AP映像在WLC上暂存。
2. FlexConnect AP分配给为高效映像升级配置的站点标签。
3. WLC在站点标签内为每个型号选择一个AP作为主AP。
4. 主AP通过WAN链路（通常通过CAPWAP）从WLC下载映像。

5. 主AP获得映像后，位于同一站点标签中的从属AP会通过TFTP通过本地网络从主AP下载映像。
6. 最多可以从一个主AP同时下载三个从属AP。
7. 下载后，AP重新加载以运行新映像。

好处

- 通过仅让主AP通过WAN下载映像，降低WAN带宽消耗。
- 利用更快的本地网络链路（通过TFTP）将映像分配到从属AP。

配置(CLI)

<#root>

```
Enable Predownload in Flex Profile:

configure terminal
wireless profile flex




predownload



 <- Enables the Efficient Image Upgrade option.

end


Configure a Site Tag and Associate Flex Profile:

configure terminal
wireless tag site




flex-profile




<- Ensure 'no local-site' is configured if not already, for Flexconnect mode

end
```

Attach Policy Tag and Site Tag to AP(s):

configure terminal
ap

<- Use wired MAC address

policy-tag

site-tag

rf-tag

end

Trigger Predownload to a Site Tag:

enable
ap image predownload site-tag

start

验证(CLI)

<#root>

```
show ap primary list
 <- Display list of primary APs
show ap image
 <- Display predownload status of APs: (Initially shows 'Predownloading', then 'Complete')
show ap name
          image
 <- Display image details for a specific AP
show capwap client rcb
 <- Check if Flex efficient image upgrade is enabled on the AP console
```

限制/注意事项

- 通过站点标记加入的AP必须位于同一物理位置，以实现有效的本地TFTP传输。
- 将TCP端口8443用于侦听程序服务（也用于客户端调试捆绑包和Clean Air文件等其他功能）。 即使禁用此功能，此端口仍保持打开状态。
- 需要WLC处于安装模式。

基于带外HTTP的AP映像下载

基于OOB HTTP的AP映像下载是Cisco IOS® XE Dublin 17.11.1中引入的增强方法，用于通过将映像传输到标准CAPWAP控制路径之外来提高AP映像升级性能。HTTP下载失败时，其自动回退到标准带内CAPWAP下载是主要优势和安全网。

OOB HTTPs方法使用标准TCP和HTTP进行图像传输。与CAPWAP控制信道的停止和等待机制不同，TCP本身使用滑动窗口机制，允许通过高延迟链路进行有效的批量数据传输。

此方法使用在控制器上运行的Web服务器(nginx)通过HTTP直接向AP提供AP映像。这绕过了大文件传输的CAPWAP控制路径限制，提供了可能更快更灵活的下载机制。

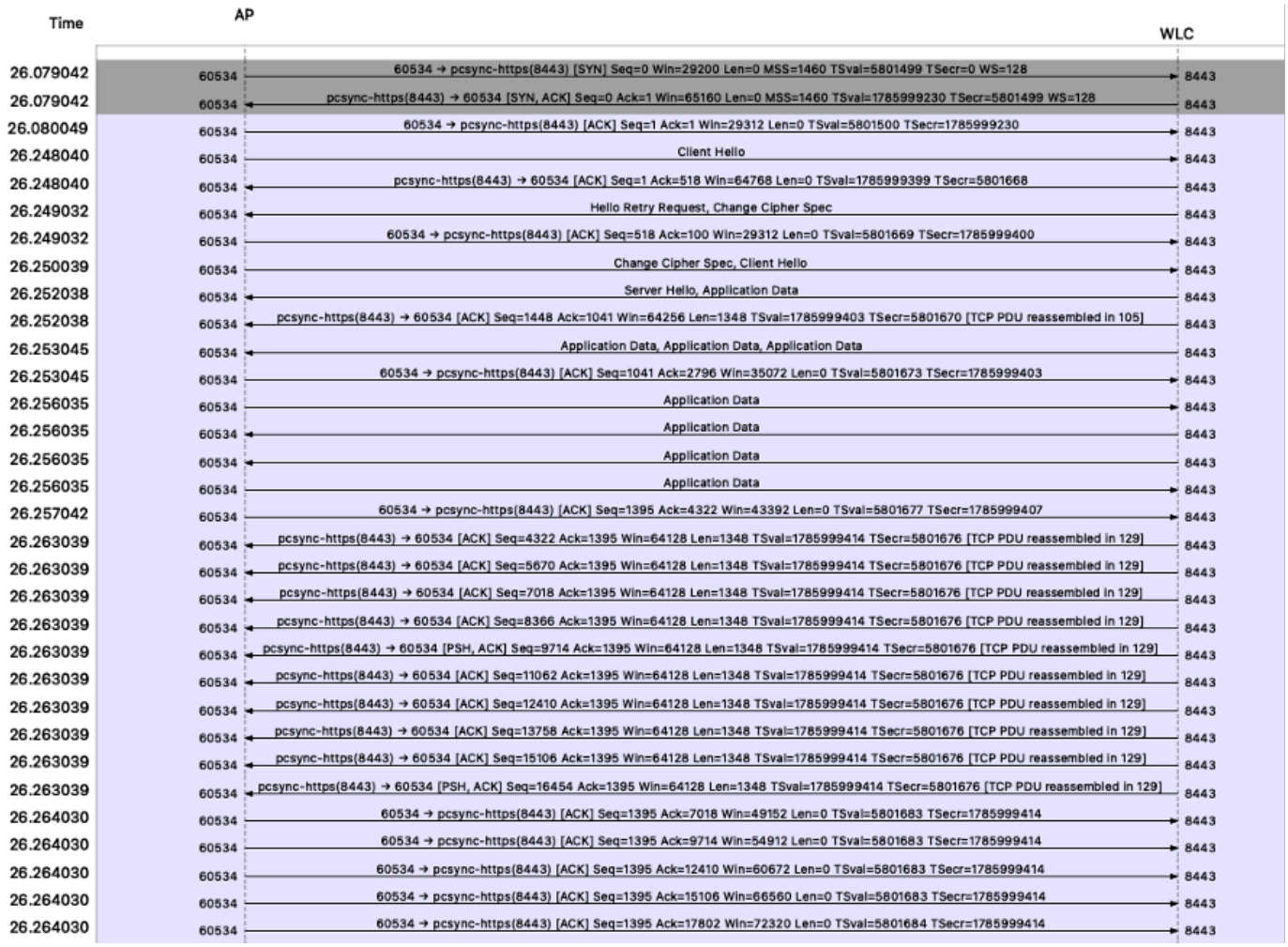
使用案例

此方法有利于加快AP映像升级，特别是在大型部署或远程站点中，因为CAPWAP控制隧道的延迟和带宽限制会使传统的带内下载非常耗时。

流程概述

1. 新的AP映像在WLC上暂存。
2. 已在控制器上启用并配置OOB HTTPs升级方法。
3. 如果AP支持OOB方法，它会尝试通过已配置端口上的HTTP从控制器上的nginx webserver下载所需的映像。
4. 如果HTTP下载成功，AP将继续执行升级过程。
5. 如果HTTPs下载失败，AP将自动回退到标准的带内CAPWAP下载方法。

数据包捕获显示WLC充当HTTPs服务器，而AP充当HTTPs客户端，通过端口8443和文件下载启动标准TCP连接。



基于HTTPS的映像升级数据包流

配置(CLI)

<#root>

Enable the HTTPS upgrade method:

configure terminal

```
ap upgrade method https
end
```

```
Configure a custom HTTPS port (Optional - default is 8443):
```

```
configure terminal
ap file-transfer https port




end
```

配置(GUI)

1. 导航到配置>无线>无线全局。
2. 在AP Image Upgrade部分中，Enable HTTPs Method。
3. （可选）在HTTPs Port字段中输入值。
4. 点击应用到设备。

验证(CLI)

```
<#root>


show ap upgrade method

 <- Check global HTTPS method status

show ap file-transfer https summary

 <- View configured and operational HTTPS file transfer port

show ap name




          config general | sec Upgrade



 <- Check if a specific AP supports OOB capability (Look for "AP Upgrade Out-Of-Band Capability : Enabl

show wireless stats ap image-download

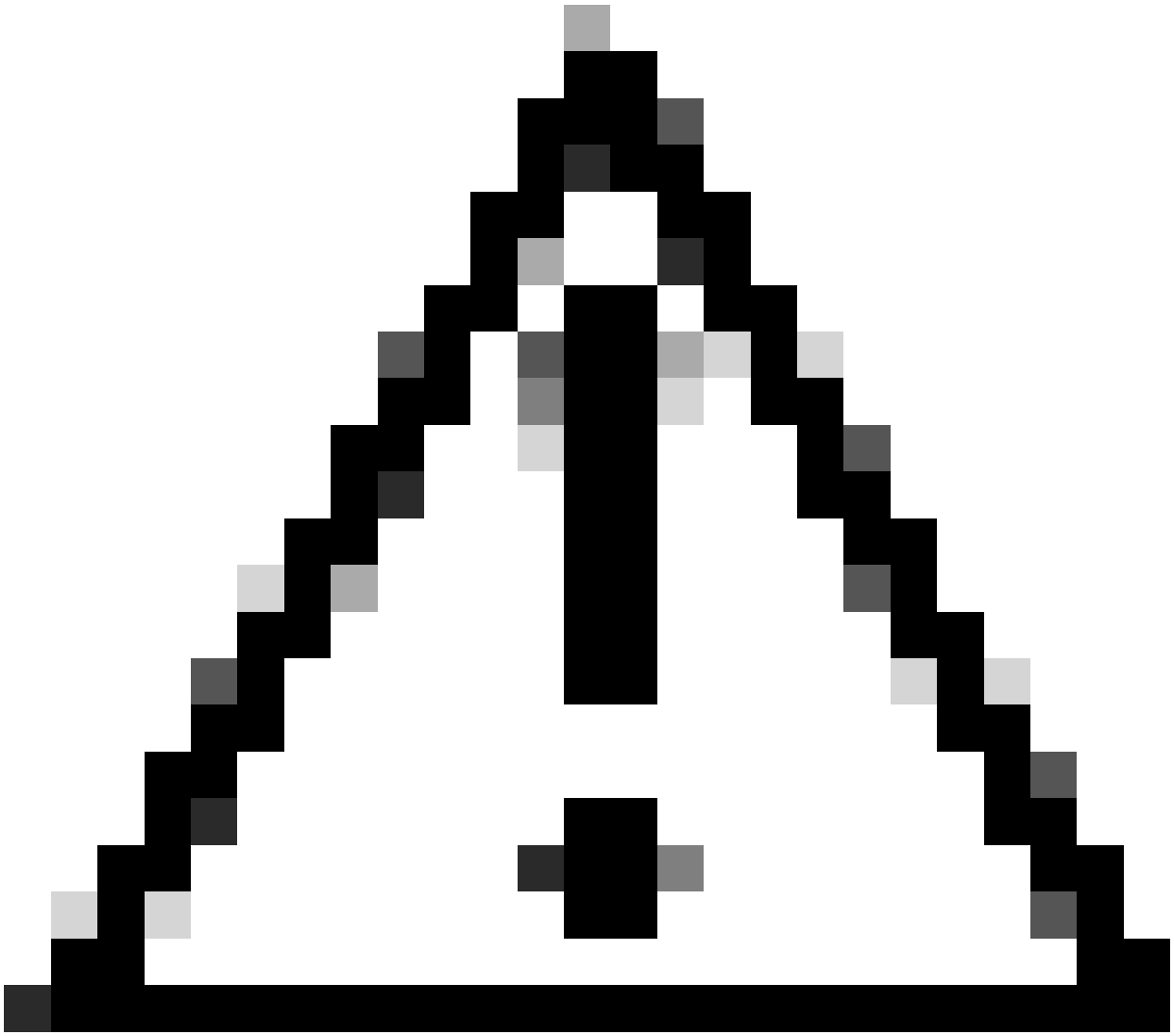
 <- View the method used for recent downloads (Check the Method column)

show platform software yang-management process
```

```
<- Verify nginx server status
```

限制/注意事项

- 需要Cisco IOS® XE Dublin 17.11.1或更高版本。
- 思科嵌入式无线控制器或Cisco Wave 1接入点不支持。
- 需要在控制器上启用全局HTTPS配置。
- Nginx服务器必须在控制器上运行。
- 配置的端口必须在控制器和AP之间可达。
- 如果HTTPS服务器信任点具有CA证书链，升级可能会失败。
- 在降级到Cisco IOS® XE 17.11.1之前的版本之前必须禁用（无ap升级方法https）。
- 保留端口443。避免使用其他标准/公认端口。
- 默认端口8443冲突：如果控制器GUI HTTPS访问也使用8443，请为AP文件传输或GUI访问配置不同的端口。



警告：请务必了解与文件上传相关的安全建议，例如Cisco IOS XE无线控制器软件任意文

件上传漏洞始终确保您的WLC软件使用最新的安全补丁。

通过TFTP/SFTP手动升级单个AP

此方法包括通过控制台或SSH直接访问AP CLI并从TFTP或SFTP服务器启动映像下载。这对于排除特定AP故障、升级当前未加入控制器的AP或加载TAC提供的调试映像非常有用。

查找AP映像：

此过程实际上会将AP映像直接加载到AP。对于基于WLC的升级，WLC负责从WLC映像包为AP选择正确的映像。此处，需要手动选择。

AP映像版本使用的命名约定与WLC映像命名约定不同。

导航至Cisco Catalyst 9800系列无线控制器软件版本中支持的接入点链接

Cisco Catalyst 9800系列无线控制器软件版本中支持的接入点

Cisco IOS XE 17.12.4	17.12.4.22	15.3(3)JPQ3	Cisco Catalyst APs: 9105AX (I/W), 9115AX (I/E), 9117AX (I), 9120AX (I/E/P), 9130AX (I/E), 9136 (I), 9162 (I), 9163 (E), 9164 (I), 9166 (I/D1) Cisco Aironet APs: 1815 (I/W/M/T), 1830 (I),1840 (I), 1852 (I/E), 1800 (I), 2800 (I/E), 3800 (I/E/P), 4800 (I) Outdoor and Industrial APs: 1542, 1560, 1570, and IW3702 Integrated Access Point in Cisco 1100 ISR (ISR-AP1100AC, ISR-AP1101AC, and ISR-AP1101AX) Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Point, Cisco 6300 Series Embedded Services Access Point, Cisco Catalyst 9124AX (I/D/E) Access Points, Cisco Catalyst Industrial Wireless 9167 (I/E) Heavy Duty Access Points Sensors: Cisco Aironet 1800s Active Sensor Pluggable Modules: Wi-Fi 6 Pluggable Module for Industrial Routers

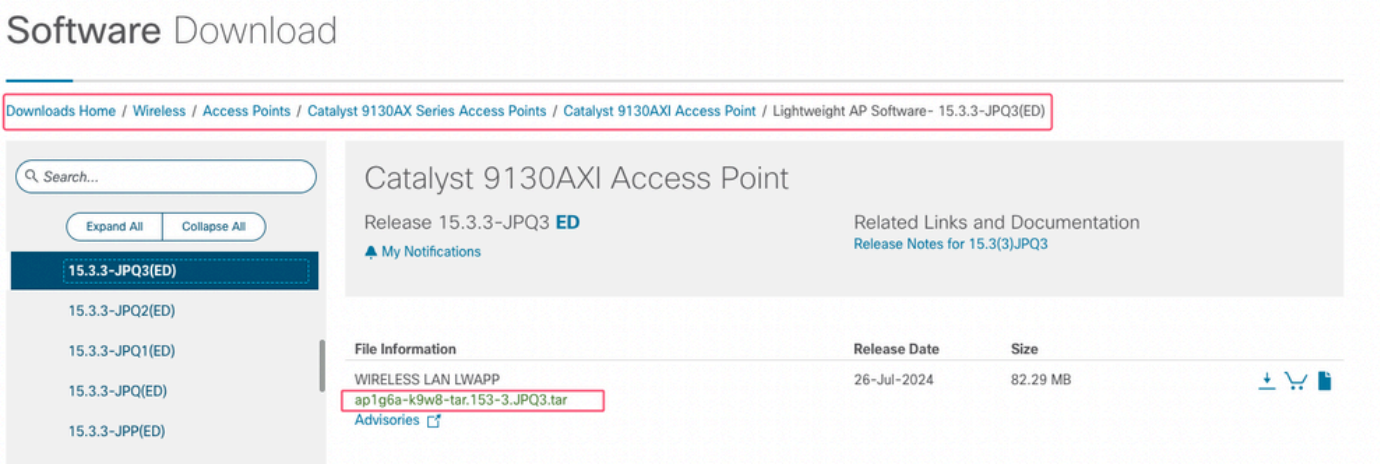
无线AP兼容性矩阵

第一列介绍9800 WLC的CCO映像。第三列列出各个映像版本，第四列列出该版本支持的接入点。假设需要在AP 9130上为版本17.12.4安装AP映像。检查表后会显示AP映像名称为15.3(3)JPQ3，且9130被列为受支持的型号。

下一步是导航到software.cisco.com并从AP下载文件夹获取映像。

下载家庭/无线/接入点/ Catalyst 9130AX系列接入点/ Catalyst 9130AXI接入点/轻量AP软件 — 15.3.3-JPQ3(ED)

软件下载 — Catalyst 9130AXI接入点



AP映像位置



警告：下载路径因AP型号和AP映像版本而异。

流程概述

1. 将目标AP映像文件存放到可访问的TFTP或SFTP服务器上。
2. 访问AP CLI（控制台或SSH）。
3. 运行命令archive download-sw，指定服务器和映像文件路径。
4. AP下载映像。
5. 下载完成后，重新启动CAPWAP进程或重新加载AP以使新映像生效。

配置(AP CLI)

<#root>

archive download-sw /no-reload tftp:///

<- Using TFTP:

archive download-sw /no-reload sftp:/// Username:

Password:

<- Using SFTP:

reload

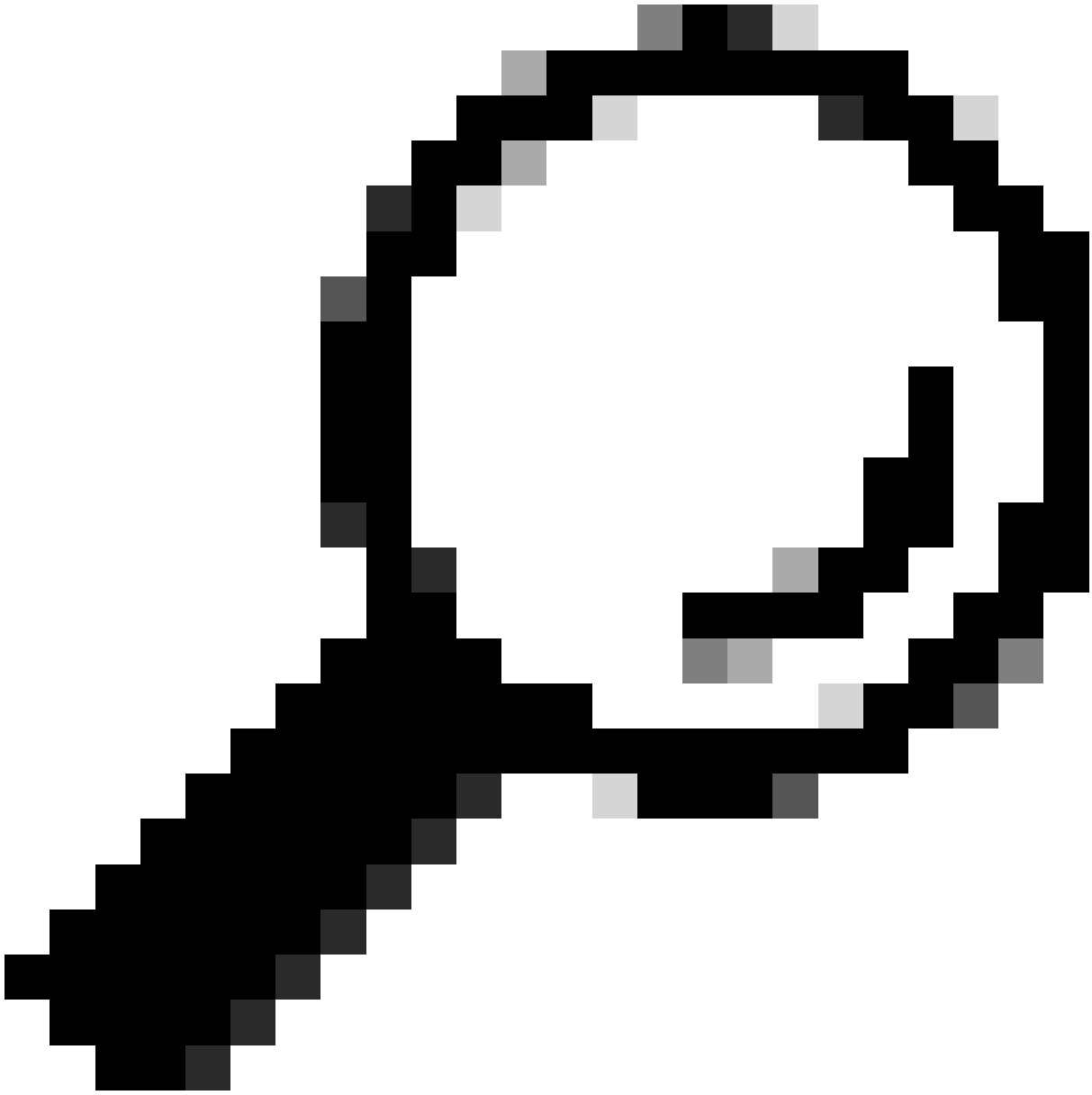
<- Restart CAPWAP process after download:

确认

- 监控TFTP/SFTP服务器日志以确认下载。
- 观察AP控制台下载进度和完成情况。
- 重新启动/重新加载后，验证AP CLI或WLC上的新映像版本。

限制/注意事项

- 需要对每个AP进行直接CLI访问。
- 不可扩展，无法单独升级大量AP（脚本是一个选项）。
- TFTP性能对延迟敏感；SFTP（使用TCP）在高延迟路径上性能更佳，但需要交互式身份验证（用户名/密码）。
- /no-reloadation可防止AP在下载后立即重新加载，从而允许手动控制重新启动/重新加载计时。
- 如果将AP从AireOS迁移到9800，建议在加入9800之前，首先使用修复程序将AP升级到特定AireOS版本（8.10.190.0或更高版本）。



提示：WLAN轮询器是一个工具，可用于创建脚本以手动升级多个AP。在此位置找到WLAN轮询器。[WLAN轮询器]

使用哪种方法

- 对于通过高延迟链路的OEAP或远程工作人员AP:
  启用CAPWAP映像下载时间增强功能。这是专门为通过使用滑动窗口来提高CAPWAP性能而设计的，可直接解决CAPWAP框架内的延迟问题。
- 对于广域网带宽有限的分支机构中的FlexConnect AP:
  在FlexConnect模式下利用高效的映像升级。强烈建议使用此方法，因为它通过使用主AP通过TFTP进行本地分配，利用更快的内部网络速度，从而显着减少WAN负载。
- 对于受支持平台(Cisco IOS® XE 17.11.1+)上的本地模式AP（或者，如果前面讨论的方法不适用或不够用，则为FlexConnect/OEAP）：

考虑带外基于HTTP的AP映像下载。此方法使用TCP/HTTP进行批量传输，与标准CAPWAP相比，它在高延迟链路上的效率更高。如果OOB传输失败，它还提供回退到标准CAPWAP的功能。

- 对于排除单个AP故障，升级未加入WLC的AP，或者在紧急情况下升级：通过TFTP/SFTP执行手动单个AP升级。这样可以直接控制特定设备的升级过程，但不适用于没有自动化的大规模部署。由于使用TCP，SFTP通常优先于TFTP，因此其性能优于高延迟路径。
- 标准CAPWAP升级：默认情况下通常不建议将其用作通过高延迟WAN链路升级远程AP的主要方法，因为其固有的停止和等待机制会导致传输缓慢，并且旧版本中可能存在可靠性问题。尽可能对远程站点使用所述优化方法。

选择最适合您的AP操作模式、网络条件、WLC软件版本和升级操作规模的方法，以确保远程AP的流程顺畅而高效。

结论

虽然标准CAPWAP映像下载方法适用于本地网络，但通过广域网链路的远程AP部署可显着受益于优化的升级技术。了解标准CAPWAP对高延迟的限制有助于选择正确的方法。CAPWAP映像下载时间增强功能提高了OEAP/远程工作人员AP的性能，有效的映像升级通过减少WAN负载来优化FlexConnect部署，带外HTTP为受支持的平台提供了更快的替代方案。手动TFTP/SFTP方法仍然是故障排除和特定场景的重要工具。

参考

高效映像升级

带外AP映像下载

AP映像下载时间增强（仅限OEAP或远程工作人员）

思科无线控制器平台软件版本支持的思科接入点

WLAN轮询器

从AireOS WLC迁移到带WLANPoller的Catalyst 9800

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）。