

瞭解遠端部署的接入點映像升級

目錄

[簡介](#)

[思科存取點映像升級方法](#)

[挑戰：通過WAN下載標準CAPWAP映像](#)

[CAPWAP影像下載視窗增強功能](#)

[流程概述](#)

[組態\(CLI\)](#)

[驗證\(CLI\)](#)

[限制/注意事項](#)

[FlexConnect模式下的高效映像升級](#)

[流程概述](#)

[優勢](#)

[組態\(CLI\)](#)

[驗證\(CLI\)](#)

[限制/注意事項](#)

[帶外HTTPs型AP映像下載](#)

[使用案例](#)

[流程概述](#)

[組態\(CLI\)](#)

[組態\(GUI\)](#)

[驗證\(CLI\)](#)

[限制/注意事項](#)

[通過TFTP/SFTP手動升級各個AP](#)

[流程概述](#)

[配置\(AP CLI\)](#)

[驗證](#)

[限制/注意事項](#)

[使用哪種方法](#)

[結論](#)

[參考資料](#)

簡介

本文檔介紹通過WAN高效升級思科AP映像的方法，以解決延遲和可靠性難題。

思科存取點映像升級方法

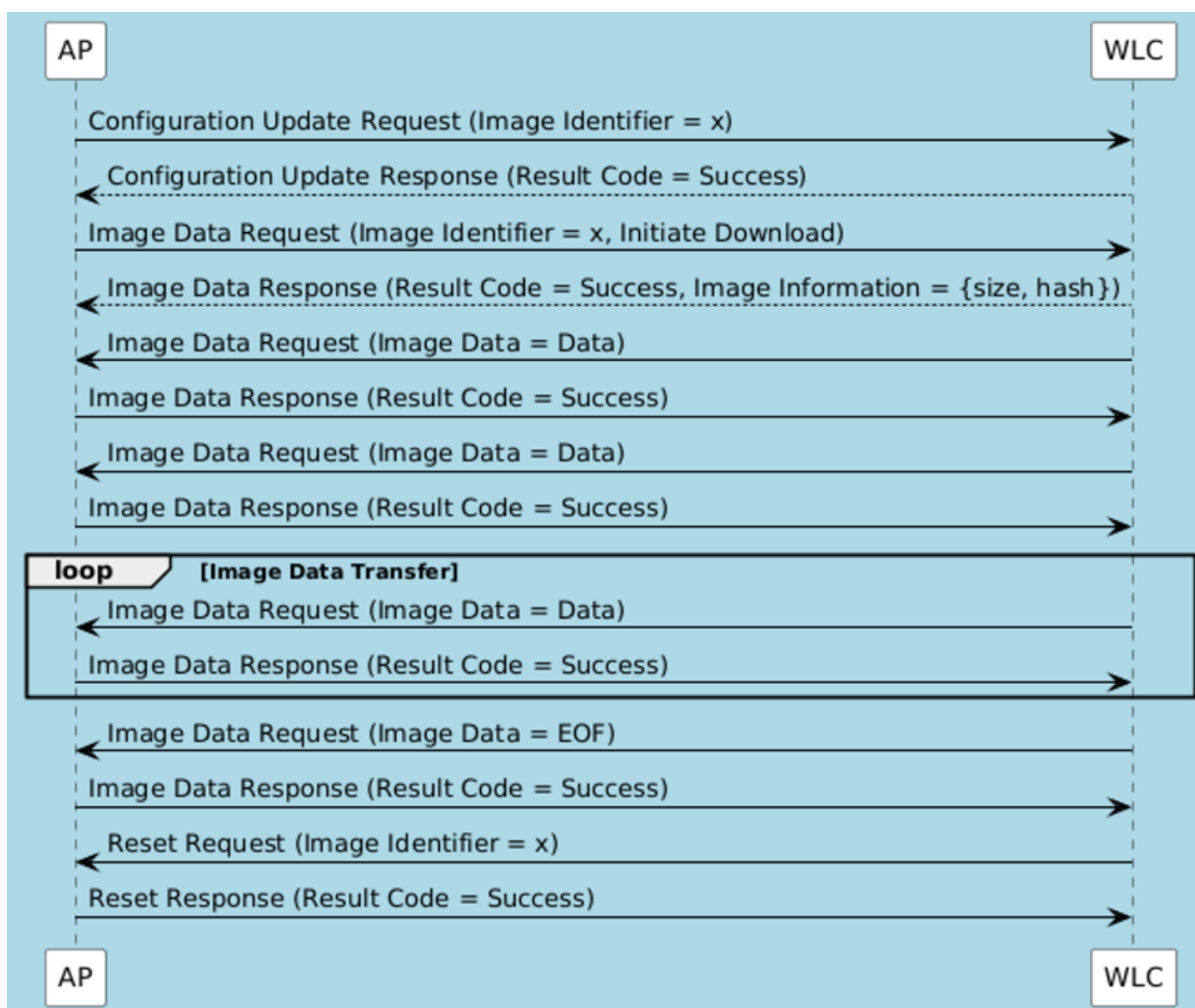
定期映像升級對思科接入點(AP)至關重要，但是通過高延遲廣域網(WAN)鏈路執行到遠端站點可能非常困難。標準CAPWAP映像下載方法雖然對本地網路有效，但速度可能較慢，而且在WAN上的

可靠性可能較低。本節將探討為什麼會發生這種情況，並概述為高效遠端升級而設計的替代和增強方法。

挑戰：通過WAN下載標準CAPWAP映像

[RFC 5415](#) 9.1節中定義了透過CAPWAP升級AP映像的基本程式。此機制允許無線LAN控制器 (WLC)透過CAPWAP通道將新AP映像直接提供到連線的AP。對於包含韌體資料塊的每個影像資料請求消息 (RFC 5415，第9.1.1節)，WLC在傳送下一個塊之前，會等待來自AP的相應影像資料響應確認 (RFC 5415，第9.1.2節)。

此圖說明AP處於運行狀態時，AP和WLC之間的映像傳輸過程。

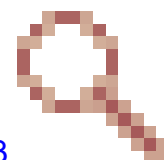
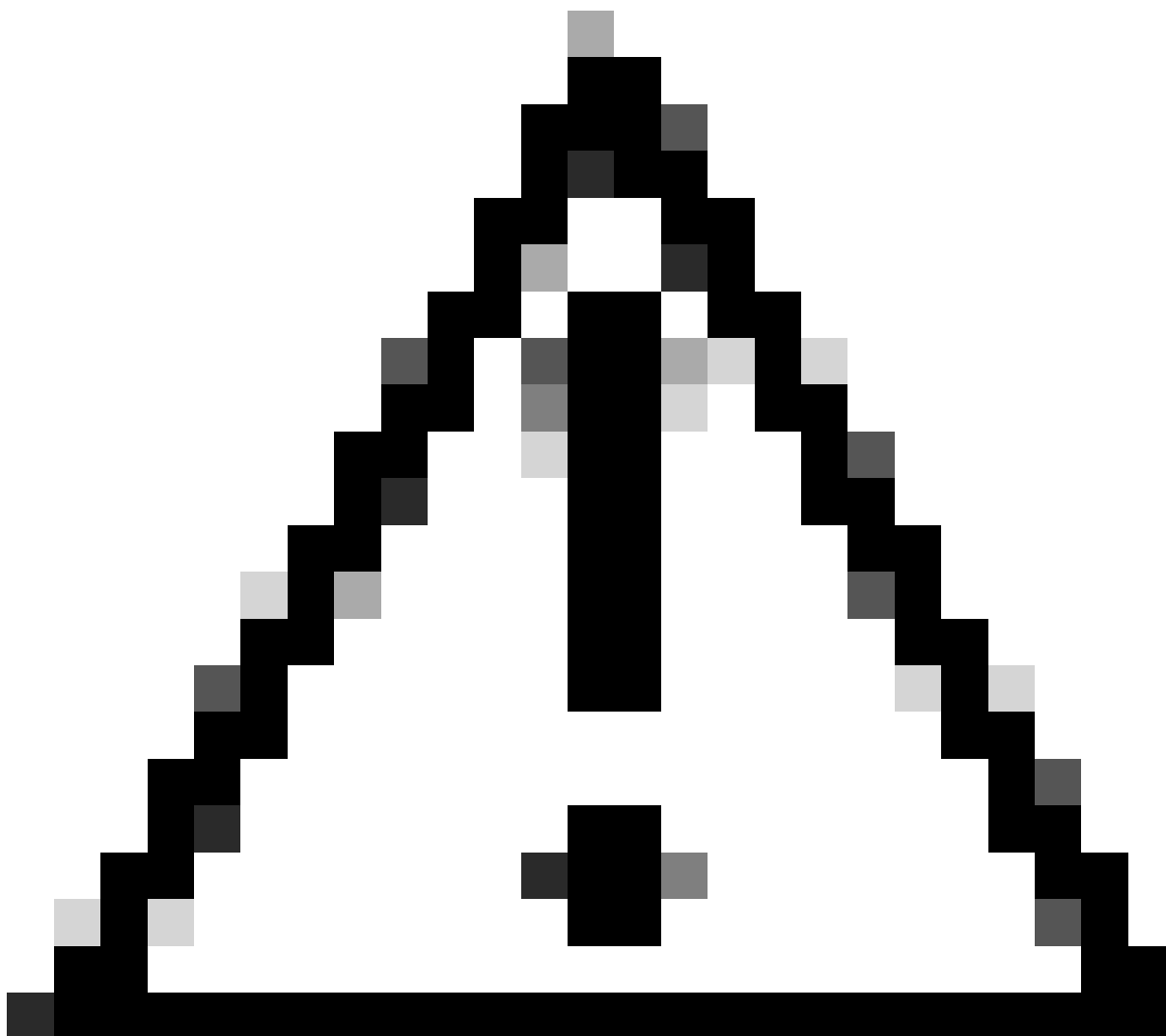


AP影像傳輸處理流程

如前所述，WLC會傳送包含韌體映像資料區塊的影像資料請求訊息。AP通過傳送影像資料響應消息確認收到這些資料塊。此交換會一直持續，直到傳輸整個映像。

對於每個影像資料請求消息，相應的影像資料響應消息被預期為確認。這表示AP必須等待每個影像資料包到達，確認該資料包，然後等待下一個資料包。這會導致WAN環境中的映像下載速度緩慢。

舉個例子：如果AP和WLC之間的來回時間(RTT)為100ms，這實際上將傳輸速率限制為約每秒10個資料包。如果每個資料包大小為1000位元組，則最大吞吐量為10 KB/秒。如果AP映像是50MB，理論上的完成傳輸的最小時間大約為5120秒。這說明，即使有大量的頻寬可用，由於此停止和等待確認機制，CAPWAP映像下載也會感覺緩慢。在WLC和AP屬於同一園區網路且延遲最小的本地映像傳輸中，這種影響不太明顯。



注意：有損的WAN鏈路可能會導致映像損壞。請參閱Cisco bug [IDCSCwf09053](#) 瞭解更多資訊。

為緩解標準CAPWAP控制路徑傳輸機制中固有的這些限制，尤其是在高延遲或頻寬受限的廣域網環境中，引入了三種增強功能。

1. CAPWAP視窗增強通過實現多資料包滑動視窗來改進CAPWAP控制路徑本身，該視窗允許在要求確認之前傳送多個資料包，從而在CAPWAP框架內的高延遲鏈路上增加吞吐量。

2. FlexConnect模式下的高效映像升級是專門為FlexConnect AP設計的最佳化方法，這些接入點通常部署在廣域網頻寬有限的分支機構。此方法通過分發映像下載任務來最大程度降低WAN負載。
3. 基於帶外HTTPs的AP映像下載方法利用在控制器上的專用Web伺服器上運行的單獨、更高效的HTTPs協定進行映像傳輸，將其移出限制性CAPWAP控制隧道之外，解決了這一問題。

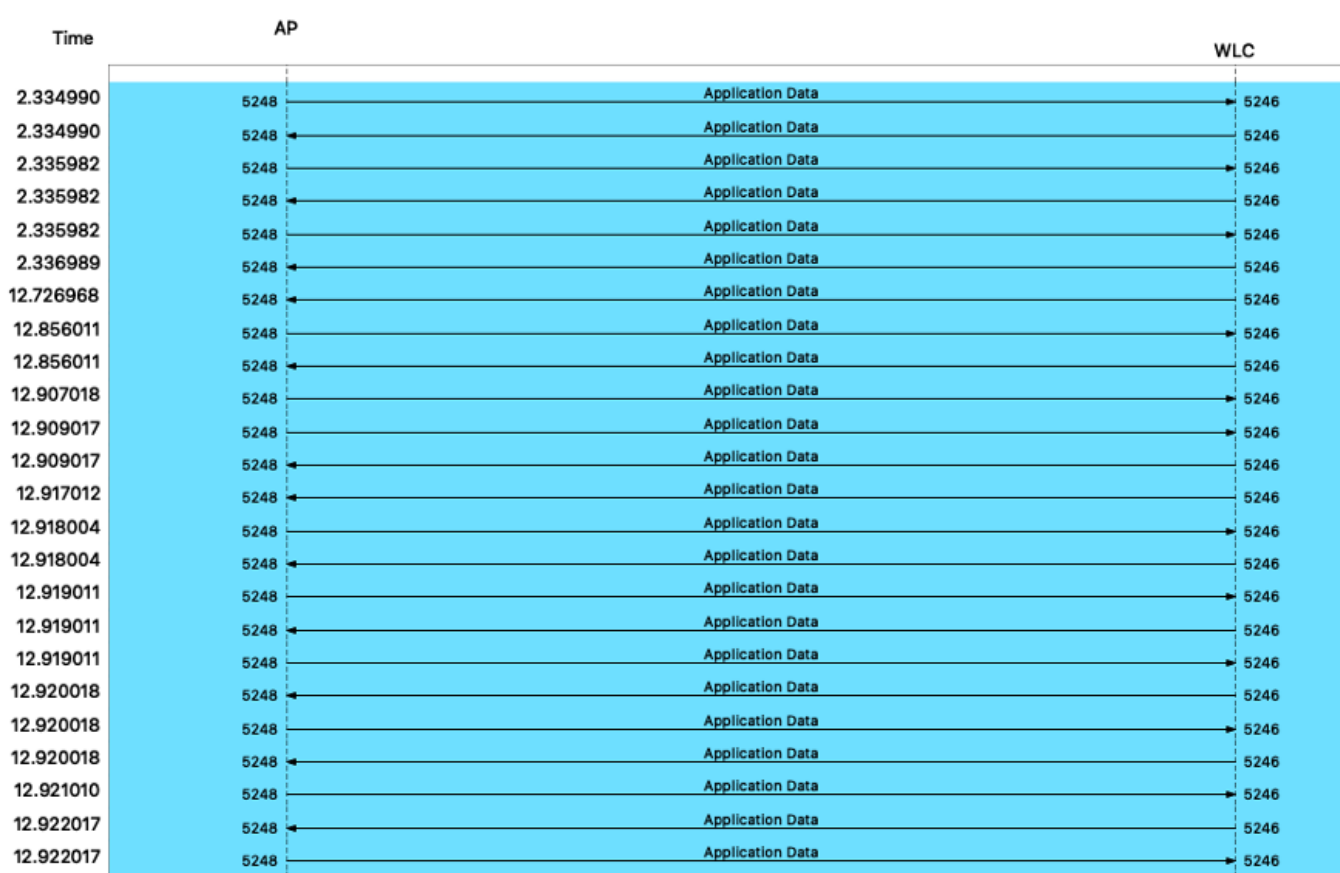
CAPWAP影像下載視窗增強功能

此功能可提高Office Extend接入點(OEAP)或遠端工作人員AP專用的基於CAPWAP的映像下載速度。它解決了標準CAPWAP控制通道只有一個視窗的限制，該視窗要求傳送下一個資料包之前對每個資料包進行確認，從而降低了通過高延遲鏈路進行的傳輸速度。此增強功能增加了對控制資料包的多個滑動視窗的支援。

CAPWAP視窗大小的影響

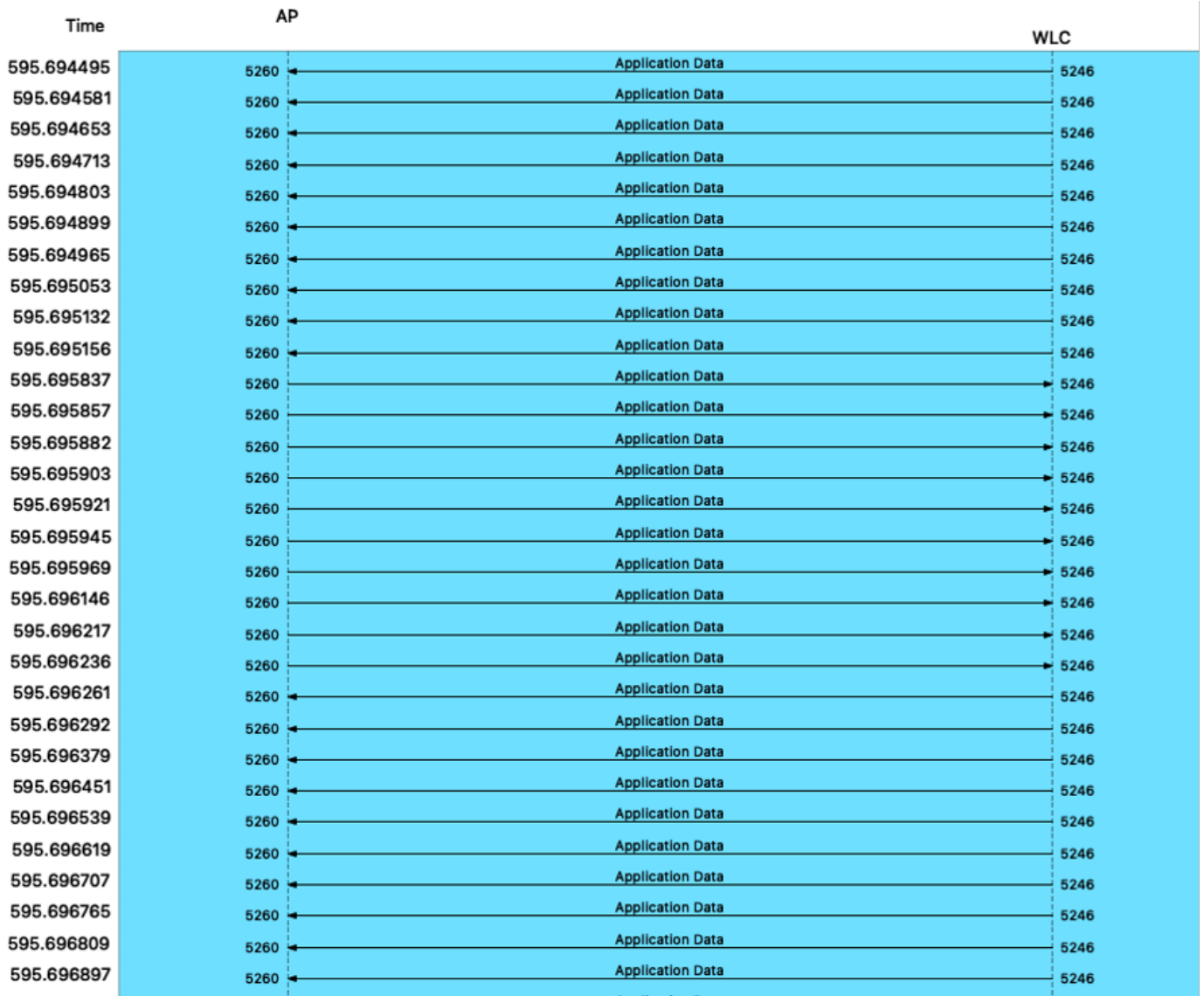
CAPWAP影像下載過程通過控制通道上的效率受配置的視窗大小影響顯著，尤其是在高延遲鏈路上。

CAPWAP視窗大小= 1 (預設/標準)：資料包流表現出嚴格的停止和等待行為。對於WLC傳送的每個影像資料請求資料包，WLC會暫停並等待來自AP的影像資料響應確認，然後再傳送下一個資料包。



視窗大小為1的CAPWAP映像升級流程

在CAPWAP視窗大小= N (例如，20) 的情況下：資料包流演示了滑動視窗機制。通過在要求確認之前允許多個資料包在鏈路上傳輸，滑動視窗有效地遮蔽了延遲。



視窗大小為20的CAPWAP映像升級流程

流程概述

1. 專門為OEAP/遠端工作人員AP配置AP配置檔案。
2. 在此配置檔案中將CAPWAP視窗大小設定為大於1。
3. 將此AP配置檔案關聯到OEAP/遠端工作人員AP。
4. 在AP加入過程中，將應用配置的視窗大小。
5. 後續的CAPWAP映像下載會利用更大的視窗大小，從而提高吞吐量。

組態(CLI)

配置AP配置檔案並設定CAPWAP窗口大小：

```
<#root>
```

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

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

end

將AP配置檔案與站點標籤關聯並應用到AP（類似於高效映像升級中的步驟2和3，確保通過站點標籤連結正確的ap配置檔案）。

驗證(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 Active)

show ap config general

| in indo <- View AP configuration details(Shows Capwap Active Window Size)

限制/注意事項

- 此增強功能僅在OEAP配置檔案中受支援。
- 僅在AP加入過程中在AP上更新視窗大小。
- 如果AP上已存在最新的升級映像，則不會觸發預下載。

FlexConnect模式下的高效映像升級

高效映像升級是專門針對FlexConnect AP設計的最佳化方法，尤其適用於廣域網頻寬有限的分支機構部署。此方法通過在站點標籤內指定主AP從控制器下載映像，然後允許同一站點標籤中的其他從屬AP通過TFTP從主AP下載映像，從而將WAN負載降至最低。主AP是每個站點標籤的每個型號一個AP。

流程概述

1. 新的AP映像暫存在WLC上。
2. FlexConnect AP分配給為高效映像升級配置的站點標籤。
3. WLC在站點標籤內為每個型號選擇一個AP作為主AP。
4. 主AP通過WAN鏈路（通常通過CAPWAP）從WLC下載映像。
5. 主AP獲得映像後，位於同一站點標籤中的從屬AP會通過TFTP通過本地網路從主AP下載映像。
6. 最多可以從一個主AP同時下載三個從屬AP。
7. 下載後，AP將重新載入以運行新映像。

優勢

- 通過僅讓主AP通過WAN下載映像來降低WAN頻寬消耗。
- 利用更快的本地網路鏈路 (通過TFTP) 將映像分發到下屬AP。

組態(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

驗證(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/注意事項

- 通過站點標籤加入的AP必須位於同一物理位置，以便進行有效的本地TFTP傳輸。
- 將TCP埠8443用於偵聽程式服務（也用於客戶端調試捆綁包和Clean Air檔案等其他功能）。即使停用該功能，此連線埠仍會保持開放狀態。
- 需要WLC處於安裝模式。

帶外HTTPs型AP映像下載

基於OOB HTTPs的AP映像下載是Cisco IOS® XE Dublin 17.11.1中引入的增強方法，用於通過將映像傳輸到標準CAPWAP控制路徑之外來提高AP映像升級效能。

OOB HTTPs方法利用標準TCP和HTTPs進行映像傳輸。與CAPWAP控制通道的停止和等待機制不同，TCP本身使用滑動視窗機制，允許通過高延遲鏈路進行有效的批次資料傳輸。

此方法利用在控制器上運行的Web伺服器(nginx)，以透過HTTPs直接將存取點映像提供到存取點。這繞過了用於大型檔案傳輸的CAPWAP控制路徑的限制，提供了可能更快、更靈活的下載機制。

使用案例

此方法有利於加速AP映像升級，尤其是在大型部署或遠端站點，在這些站點中，CAPWAP控制隧道的延遲和頻寬限制可能使得傳統的帶內下載非常耗時。

流程概述

1. 新的AP映像WLC上暫存。

2. 控制器上啟用並配置了OOB HTTPs升級方法。
3. AP (如果支援OOB方法) 會嘗試通過已配置埠上的HTTP從控制器上的nginx Web伺服器下載所需的映像。
4. 如果HTTPs下載成功，AP將繼續執行升級過程。
5. 如果HTTPs下載失敗，AP將自動回退到標準的帶內CAPWAP下載方法。

資料包捕獲顯示WLC充當HTTPs伺服器，AP充當HTTPs客戶端，通過埠8443和檔案下載啟動標準TCP連線。

Time	AP	WLC
26.079042	60534 → pcsync-https(8443) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 TSval=5801499 TSecr=0 WS=128	8443
26.079042	pcsync-https(8443) → 60534 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 TSval=1785999230 TSecr=5801499 WS=128	8443
26.080049	60534 → pcsync-https(8443) [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=5801500 TSecr=1785999230	8443
26.248040	Client Hello	8443
26.248040	pcsync-https(8443) → 60534 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=1785999399 TSecr=5801668	8443
26.249032	Hello Retry Request, Change Cipher Spec	8443
26.249032	60534 → pcsync-https(8443) [ACK] Seq=518 Ack=100 Win=29312 Len=0 TSval=5801669 TSecr=1785999400	8443
26.250039	Change Cipher Spec, Client Hello	8443
26.252038	Server Hello, Application Data	8443
26.252038	pcsync-https(8443) → 60534 [ACK] Seq=1448 Ack=1041 Win=64256 Len=1348 TSval=1785999403 TSecr=5801670 [TCP PDU reassembled in 105]	8443
26.253045	Application Data, Application Data, Application Data	8443
26.253045	60534 → pcsync-https(8443) [ACK] Seq=1041 Ack=2796 Win=35072 Len=0 TSval=5801673 TSecr=1785999403	8443
26.256035	Application Data	8443
26.256035	Application Data	8443
26.256035	Application Data	8443
26.256035	Application Data	8443
26.257042	60534 → pcsync-https(8443) [ACK] Seq=1395 Ack=4322 Win=43392 Len=0 TSval=5801677 TSecr=1785999407	8443
26.263039	pcsync-https(8443) → 60534 [ACK] Seq=4322 Ack=1395 Win=64128 Len=1348 TSval=1785999414 TSecr=5801676 [TCP PDU reassembled in 129]	8443
26.263039	pcsync-https(8443) → 60534 [ACK] Seq=5670 Ack=1395 Win=64128 Len=1348 TSval=1785999414 TSecr=5801676 [TCP PDU reassembled in 129]	8443
26.263039	pcsync-https(8443) → 60534 [ACK] Seq=7018 Ack=1395 Win=64128 Len=1348 TSval=1785999414 TSecr=5801676 [TCP PDU reassembled in 129]	8443
26.263039	pcsync-https(8443) → 60534 [ACK] Seq=8366 Ack=1395 Win=64128 Len=1348 TSval=1785999414 TSecr=5801676 [TCP PDU reassembled in 129]	8443
26.263039	pcsync-https(8443) → 60534 [PSH, ACK] Seq=9714 Ack=1395 Win=64128 Len=1348 TSval=1785999414 TSecr=5801676 [TCP PDU reassembled in 129]	8443
26.263039	pcsync-https(8443) → 60534 [ACK] Seq=11062 Ack=1395 Win=64128 Len=1348 TSval=1785999414 TSecr=5801676 [TCP PDU reassembled in 129]	8443
26.263039	pcsync-https(8443) → 60534 [ACK] Seq=12410 Ack=1395 Win=64128 Len=1348 TSval=1785999414 TSecr=5801676 [TCP PDU reassembled in 129]	8443
26.263039	pcsync-https(8443) → 60534 [ACK] Seq=13758 Ack=1395 Win=64128 Len=1348 TSval=1785999414 TSecr=5801676 [TCP PDU reassembled in 129]	8443
26.263039	pcsync-https(8443) → 60534 [ACK] Seq=15106 Ack=1395 Win=64128 Len=1348 TSval=1785999414 TSecr=5801676 [TCP PDU reassembled in 129]	8443
26.263039	pcsync-https(8443) → 60534 [PSH, ACK] Seq=16454 Ack=1395 Win=64128 Len=1348 TSval=1785999414 TSecr=5801676 [TCP PDU reassembled in 129]	8443
26.264030	60534 → pcsync-https(8443) [ACK] Seq=1395 Ack=7018 Win=49152 Len=0 TSval=5801683 TSecr=1785999414	8443
26.264030	60534 → pcsync-https(8443) [ACK] Seq=1395 Ack=9714 Win=54912 Len=0 TSval=5801683 TSecr=1785999414	8443
26.264030	60534 → pcsync-https(8443) [ACK] Seq=1395 Ack=12410 Win=60672 Len=0 TSval=5801683 TSecr=1785999414	8443
26.264030	60534 → pcsync-https(8443) [ACK] Seq=1395 Ack=15106 Win=66560 Len=0 TSval=5801683 TSecr=1785999414	8443
26.264030	60534 → pcsync-https(8443) [ACK] Seq=1395 Ack=17802 Win=72320 Len=0 TSval=5801684 TSecr=1785999414	8443

基於HTTPS的映像升級封包流量

組態(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

組態(GUI)

1. 導覽至Configuration > Wireless > Wireless Global。
2. 在「AP Image Upgrade」部分中，啟用HTTPS方法。
3. (可選) 在「HTTPS埠」欄位中輸入值。
4. 按一下Apply to Device。

驗證(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/注意事項

- 需要Cisco IOS® XE Dublin 17.11.1或更高版本。
- 思科嵌入式無線控制器或Cisco Wave 1接入點不支援。
- 需要在控制器上啟用全域性HTTPS配置。
- Nginx伺服器必須在控制器上運行。
- 控制器和AP之間必須可以訪問已配置的埠。
- 如果HTTPS伺服器信任點具有CA證書鏈，升級可能失敗。
- 在降級到Cisco IOS® XE 17.11.1之前的版本之前必須禁用（無ap升級方法https）。
- 保留埠443。避免使用其他標準/公認埠。
- 預設埠8443衝突：如果控制器GUI HTTPS訪問也使用8443，請為AP檔案傳輸或GUI訪問配置不同的埠。

通過TFTP/SFTP手動升級各個AP

此方法包括通過控制檯或SSH直接訪問AP CLI並從TFTP或SFTP伺服器啟動映像下載。這適用於疑難排解特定AP、升級目前未加入控制器的AP，或載入由TAC提供的偵錯映像。

查詢AP映像：

此過程實際上會將AP映像直接載入到AP。在基於WLC的升級中，WLC會負責從WLC映像套件中選擇正確的AP映像。在這裡，需要手動選擇。

AP映像版本使用的命名約定與WLC映像命名約定不同。

導覽至Cisco Catalyst 9800系列無線控制器軟體版本中的支援存取點連結

[Cisco Catalyst 9800系列無線控制器軟體版本中支援的接入點](#)

Supported Access Points in Cisco Catalyst 9800 Series Wireless Controller Software Releases

Table 5. Cisco Catalyst 9800 Wireless Controller and Supported Access Points

IOS XE Release	Access Point Image Version Number	Access Point Release	Supported Access Points
Cisco IOS XE 17.17.1	17.17.0.87	15.3(3)JPV	Cisco Wireless Wi-Fi 7 APs: 9176 (I/D1), 9178I, 9172(I/H) Cisco Catalyst Wi-Fi 6E APs: 9136 (I), 9162 (I), 9164 (I), 9166 (I/D1) Cisco Catalyst Wi-Fi 6 APs: 9105AX (I/W), 9115AX (I/E), 9117AX (I), 9120AX (I/E/P), 9130AX (I/E) Cisco Aironet APs: 1815 (I/W/M/T), 1830 (I), 1840 (I), 1852 (I/E), 1800I, 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 9163 (E) Series Access Points, Cisco Catalyst Industrial Wireless 9167 (I/E) Heavy Duty Access Points, Cisco Catalyst IW9165D Heavy Duty Access Points, Cisco Catalyst IW9165E Rugged Access Points Sensors: Cisco Aironet 1800s Active Sensor Pluggable Modules: Wi-Fi 6 Pluggable Module for Industrial Routers

無線AP相容性矩陣

第一列說明9800 WLC的CCO映像。第三列列出相應的影象版本，第四列列出該版本支援的接入點。假設需要在AP 9130上為版本17.17.1安裝AP映像。檢查表後顯示AP映像名稱為15.3。(3)JPV和9130被列為受支援的型號。

下一步是導航至software.cisco.com，然後從AP下載資料夾獲取映像。

下載家庭/無線/接入點Catalyst 9130AX系列接入點/Catalyst 9130AXI接入點/輕量AP軟體 — 17.17.1(ED)

[軟體下載 — Catalyst 9130AXI存取點](#)

Software Download

Downloads Home / Wireless / Access Points / Catalyst 9130AX Series Access Points / Catalyst 9130AXI Access Point / Lightweight AP Software- 17.17.1(ED)

Search...

Expand All Collapse All

Latest Release

17.15.3(ED)

15.3.3-JPQ4(MD)

17.17.1(ED)

17.16.1(ED)

Catalyst 9130AXI Access Point

Release 17.17.1 ED

[My Notifications](#)

Related Links and Documentation

- No related links or documentation -

File Information	Release Date	Size
WIRELESS LAN LWAPP	27-Mar-2025	89.49 MB
ap1g6a-k9w8-tar.17_17_0_87.tar		
Advisories		

AP映像位置



警告：下載路徑因AP型號和AP映像版本而異。

流程概述

1. 將目標AP映像檔案存放到可訪問的TFTP或SFTP伺服器上。
2. 訪問AP CLI (控制檯或SSH) 。
3. 運行命令archive download-sw , 指定伺服器和映像檔案路徑。
4. AP下載映像。
5. 下載完成後，重新啟動CAPWAP進程或重新載入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
```

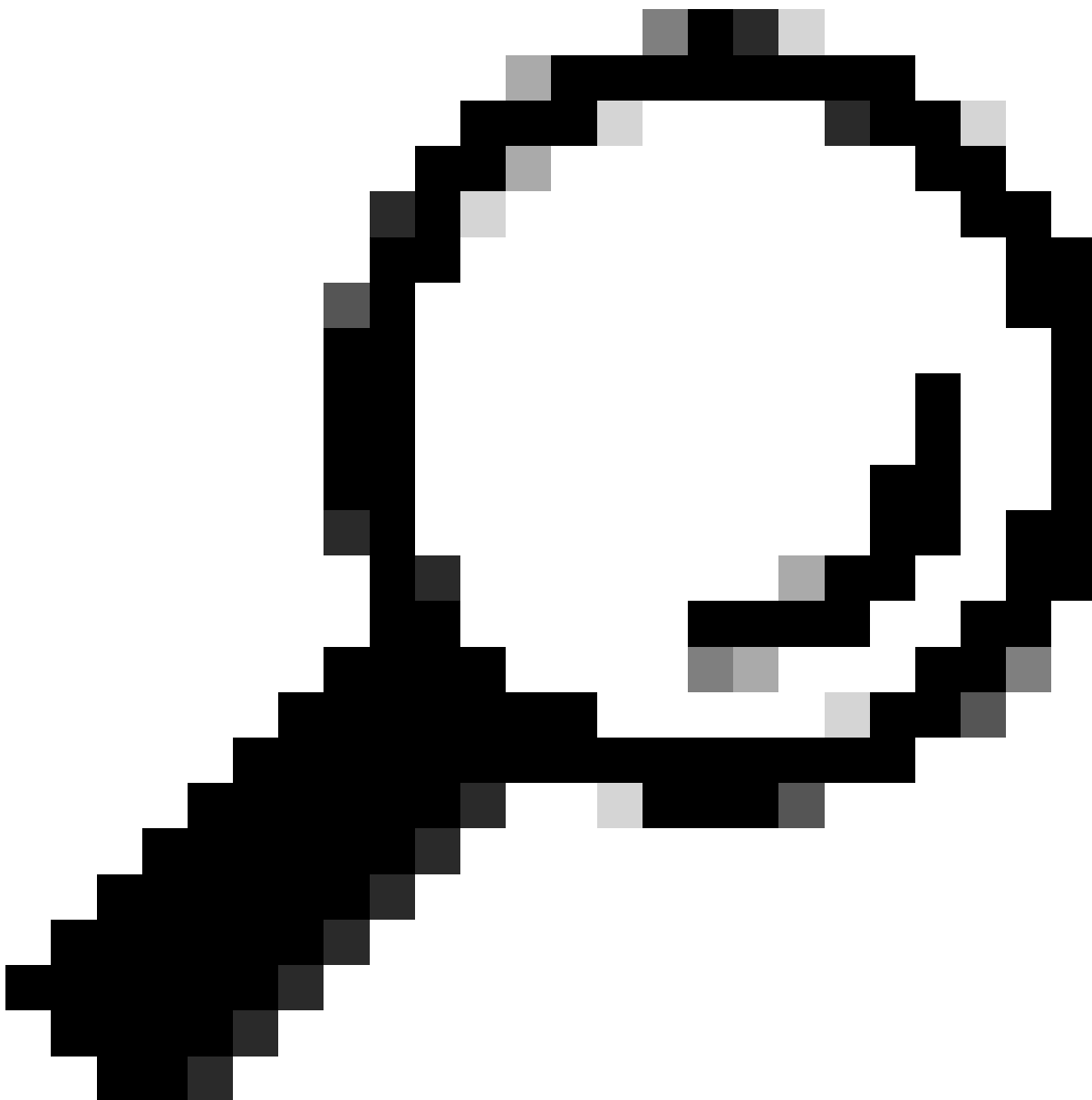
<- Restart CAPWAP process after download:

驗證

- 監控TFTP/SFTP伺服器日誌以確認下載。
- 觀察AP控制檯下載進度和完成情況。
- 重新啟動/重新載入後，在AP CLI或WLC上驗證新的映像版本。

限制/注意事項

- 需要對每個AP進行直接CLI訪問。
- 不可擴展，無法單獨升級大量AP (指令碼是一個選項) 。
- TFTP效能對延遲敏感；SFTP (使用TCP) 在高延遲路徑上效能更佳，但需要互動式身份驗證 (使用者名稱/密碼) 。
- The/no-reloadage可防止AP在下載後立即重新載入，從而允許手動控制重新啟動/重新載入計時。
- 如果將AP從AireOS遷移到9800，建議在加入9800之前，首先將AP升級到具有修復功能的特定AireOS版本 (8.10.190.0或更高版本) 。



提示：WLAN Poller是一種工具，可用於建立手動升級多個AP的指令碼。在此位置找到WLAN輪詢器。[WLAN輪詢器](#)

使用哪種方法

- 對於使用高延遲鏈路的OEAP或遠端工作人員AP：
啟用CAPWAP映像下載時間增強功能。這是專門為通過使用滑動視窗來提高CAPWAP效能而設計的，它直接解決了CAPWAP框架中的延遲問題。
- 對於廣域網頻寬有限的分支機構中的FlexConnect AP：
在FlexConnect模式下利用高效的映像升級。強烈建議使用此方法，因為它通過使用主AP通過TFTP進行本地分發，利用更快的內部網路速度，從而顯著減少了WAN負載。
- 對於受支援平台(Cisco IOS® XE 17.11.1+)上的本地模式AP（或者，如果前面討論的方法不適用或不足，則為FlexConnect/OEAP）：

考慮帶外基於HTTPs的AP映像下載。此方法使用TCP/HTTP進行批次傳輸，與標準CAPWAP相比，該方法在高延遲鏈路上的效率更高。如果OOB傳輸失敗，它還提供回退到標準CAPWAP。

- 若要對單個AP進行故障排除，請升級未加入WLC的AP，或者在緊急情況下升級：通過TFTP/SFTP執行手動單個AP升級。這樣可直接控制特定裝置的升級過程，但不適用於沒有自動化的大規模部署。由於使用TCP，SFTP通常優先於TFTP，因此其效能優於高延遲路徑。
- 標準CAPWAP升級：雖然是預設配置，但通常不建議將其作為通過高延遲WAN鏈路升級遠端AP的主要方法，因為其固有的停止和等待機制會導致傳輸速度緩慢，並且舊版本中可能存在可靠性問題。儘可能對遠端站點使用所述的最佳化方法。

選擇最符合您存取點作業模式、網路條件、WLC軟體版本和升級作業規模的方法，以確保您的遠端AP的流程順暢且高效。

結論

雖然標準CAPWAP映像下載方法適用於本地網路，但通過廣域網鏈路進行遠端AP部署可顯著受益於最佳化的升級技術。瞭解標準CAPWAP對高延遲的限制有助於選擇正確的方法。CAPWAP映像下載時間增強功能提高了OEAP/遠端工作人員AP的效能，高效映像升級通過減少WAN負載來最佳化FlexConnect部署，帶外HTTP為受支援的平台提供了更快的替代方案。手動TFTP/SFTP方法依然是故障排除和特定場景的重要工具。

參考資料

[高效映像升級](#)

[帶外AP映像下載](#)

[AP映像下載時間增強 \(僅限OEAP或遠端工作人員 \)](#)

[思科無線控制器平台軟體版本支援的思科接入點](#)

[WLAN輪詢器](#)

[使用WLANoller從AireOS WLC遷移到Catalyst 9800](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。