Understand Access Point Image Upgrades for Remote Deployments

Contents

Introduction

This document describes methods for efficient Cisco AP image upgrades over WANs, addressing latency and reliability challenges.

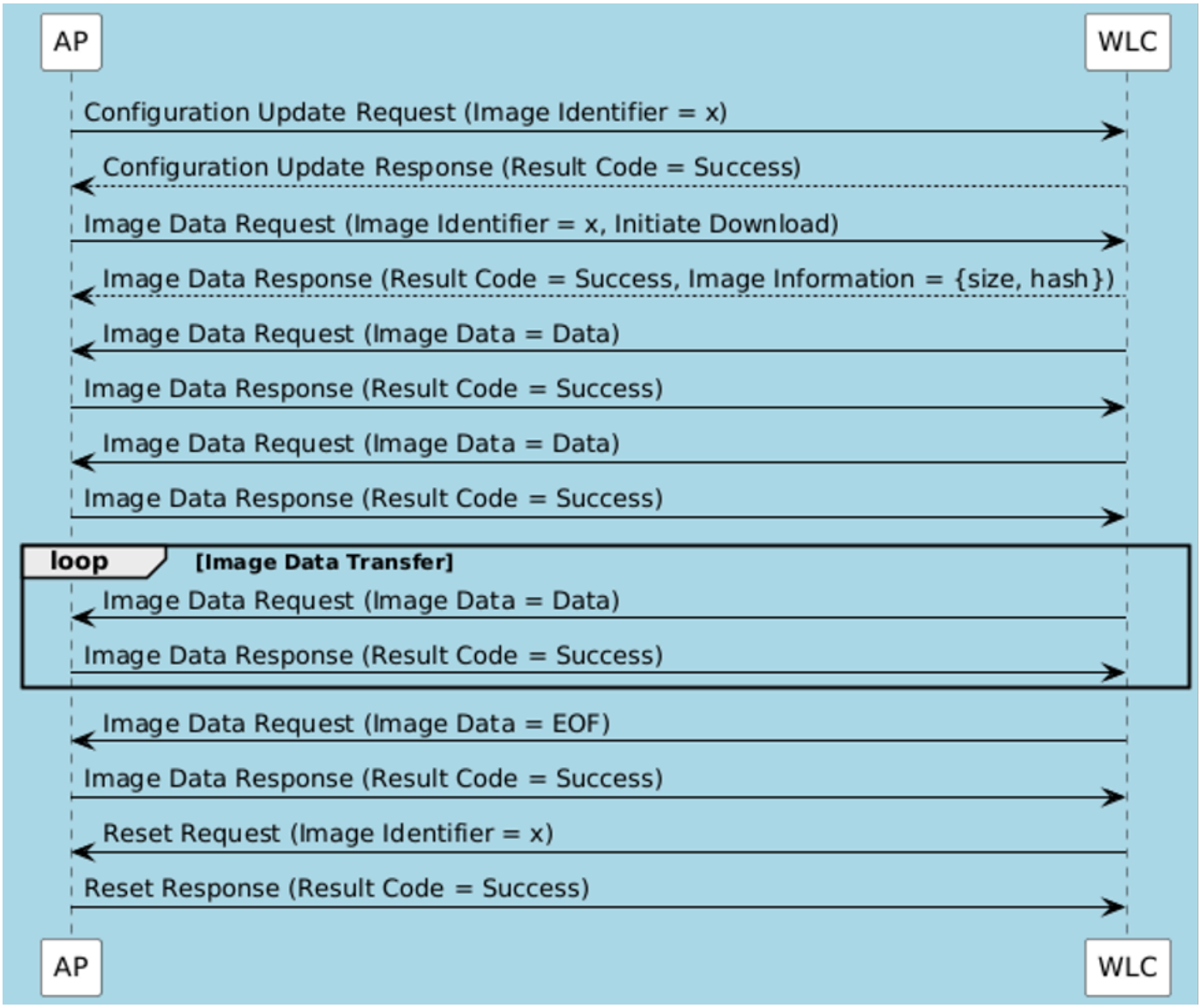
Cisco Access Point Image Upgrade Methods

Regular image upgrades are essential for Cisco Access Points (AP), but performing these over high-latency Wide Area Network (WAN) links to remote sites can be challenging. The standard CAPWAP image download method, while effective in local networks, can be slow and potentially less reliable over WANs. This section explores why this occurs and outlines alternative and enhanced methods designed for efficient remote upgrades.

The Challenge: Standard CAPWAP Image Download Over WAN

The fundamental process for AP image upgrade via CAPWAP is defined in RFC 5415, Section 9.1. This mechanism allows the Wireless LAN Controller (WLC) to serve the new AP image directly to the connected APs over the CAPWAP tunnel. For each Image Data Request message (RFC 5415, Section 9.1.1) containing a chunk of firmware data, the WLC waits for a corresponding Image Data Response acknowledgment (RFC 5415, Section 9.1.2) from the AP before sending the next chunk.

The image illustrates the image transfer process between the AP and WLC while the AP is in run state.

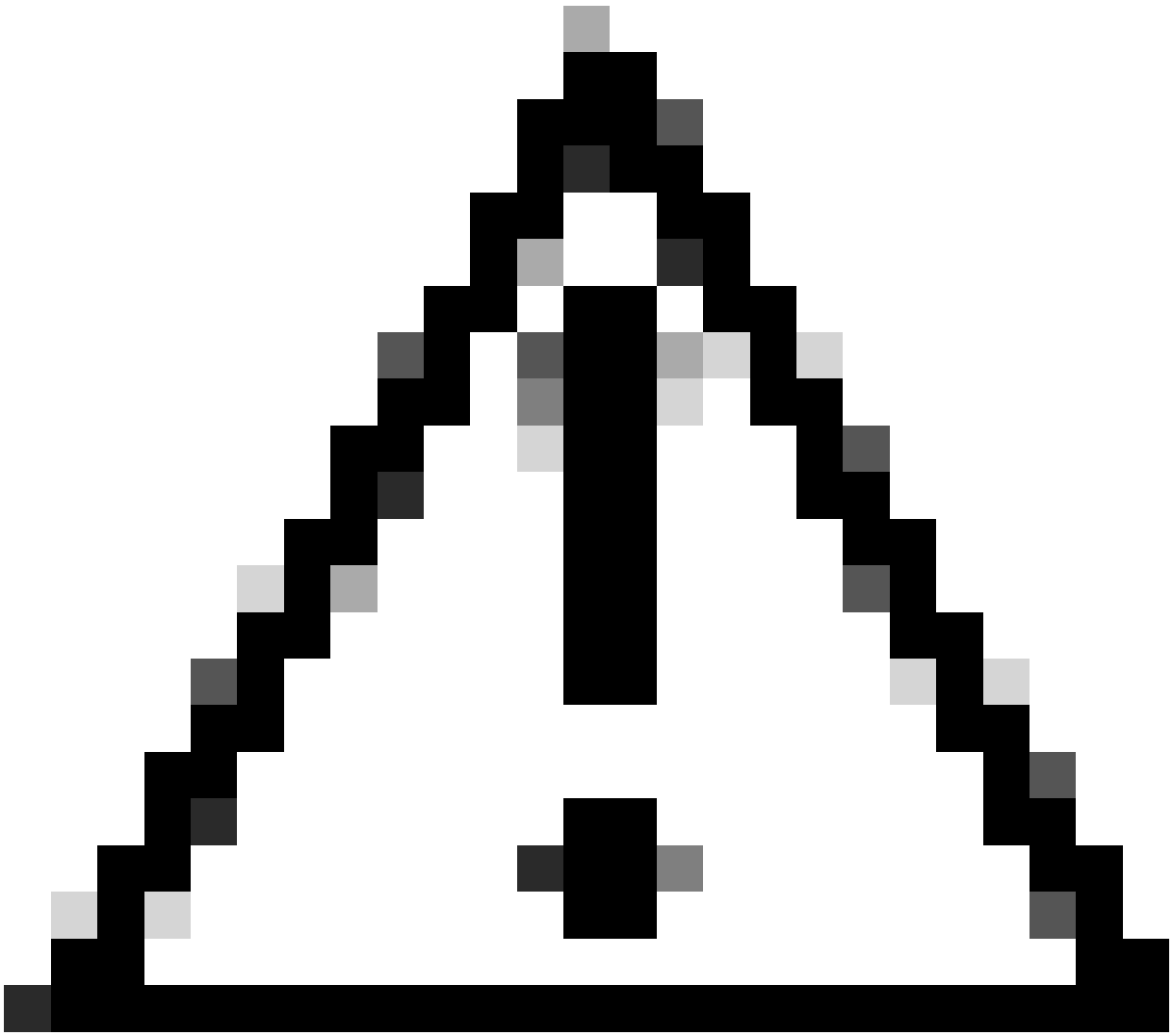


AP Image Transfer Process Flow

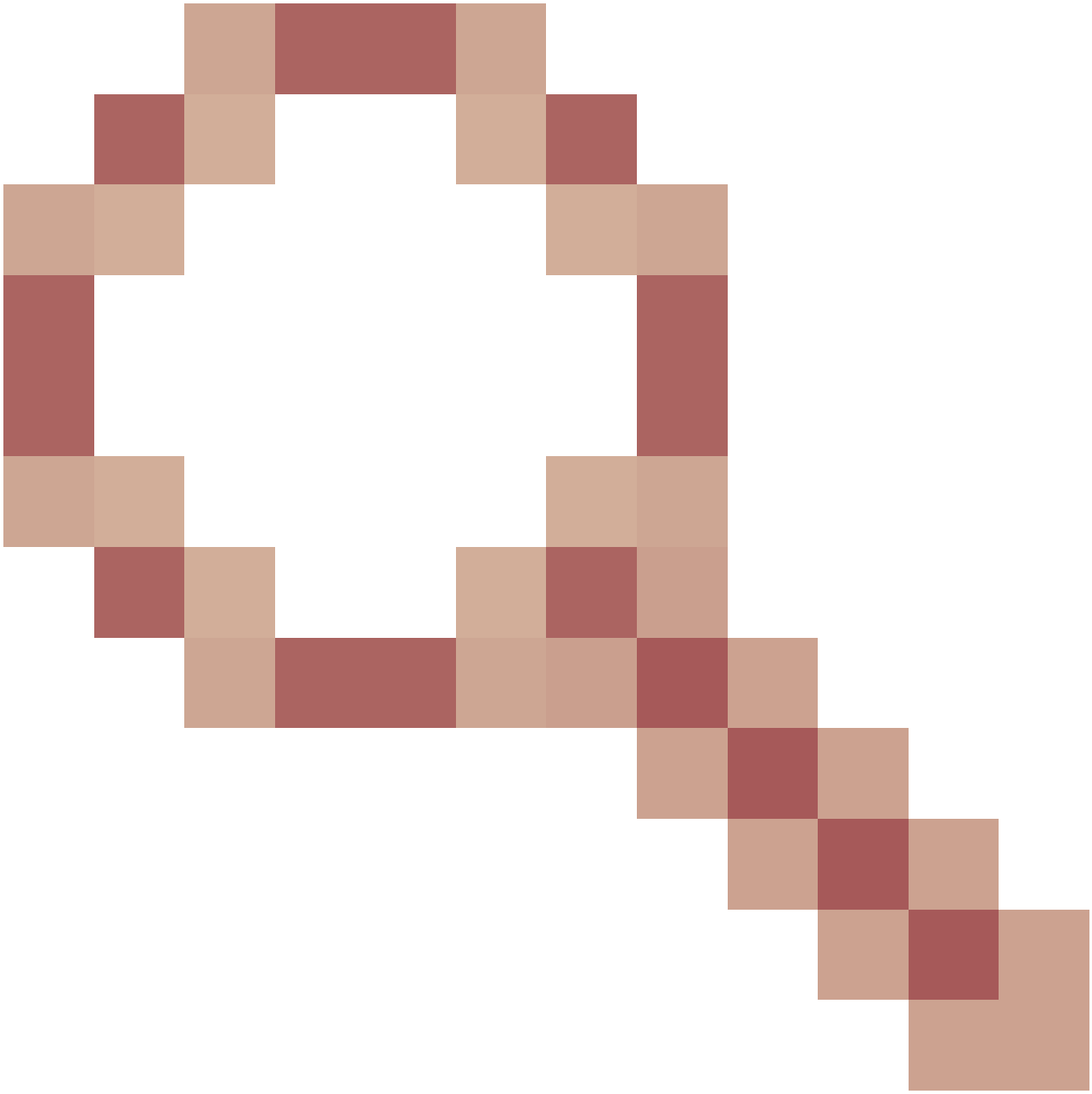
As observed, the WLC sends Image Data Request messages containing chunks of the firmware image data. The AP acknowledges receipt of these chunks by sending Image Data Response messages. This exchange continues until the entire image is transferred.

For each Image Data Request message, a corresponding Image Data Response message is expected as an acknowledgment. This means the AP must wait for each image packet to arrive, acknowledge it, and then wait for the next packet. This introduces slowness in image download in WAN environments.

Consider an example: If the Round Trip Time (RTT) between the AP and WLC is 100ms, this effectively limits the transfer rate to approximately 10 packets per second. If each packet size is 1000 Bytes, this translates to a maximum throughput of 10 KB/sec. If the AP image is 50MB, the theoretical minimum time to complete the transfer is approximately 5120 seconds. This illustrates that even if significant bandwidth is available, the CAPWAP image download can feel slow due to this stop-and-wait acknowledgment mechanism. This effect is less noticeable in local image transfers where the WLC and AP are part of the same campus network and latency is minimal.



Caution: A lossy WAN link can potentially lead to image corruption. See Cisco bug ID[CSCwf09053]



for more information on this.

To mitigate these limitations inherent in the standard CAPWAP control path transfer mechanism, particularly in high-latency or bandwidth-constrained WAN environments, three enhancements were introduced.

1. The CAPWAP Window enhancement improves the CAPWAP control path itself by implementing a multi-packet sliding window, allowing multiple data packets to be sent before requiring an acknowledgment, thereby increasing throughput over high-latency links within the CAPWAP framework.
2. Efficient Image Upgrade in FlexConnect Mode is an optimized method specifically designed for FlexConnect APs, which are frequently deployed in branch offices with limited WAN bandwidth. This method minimizes WAN load by distributing the image download task.
3. The Out-of-Band HTTPs-Based AP Image Download method addresses this by leveraging a separate, more efficient HTTPs protocol running on a dedicated webserver on the controller for the image transfer, moving it outside the restrictive CAPWAP control tunnel.

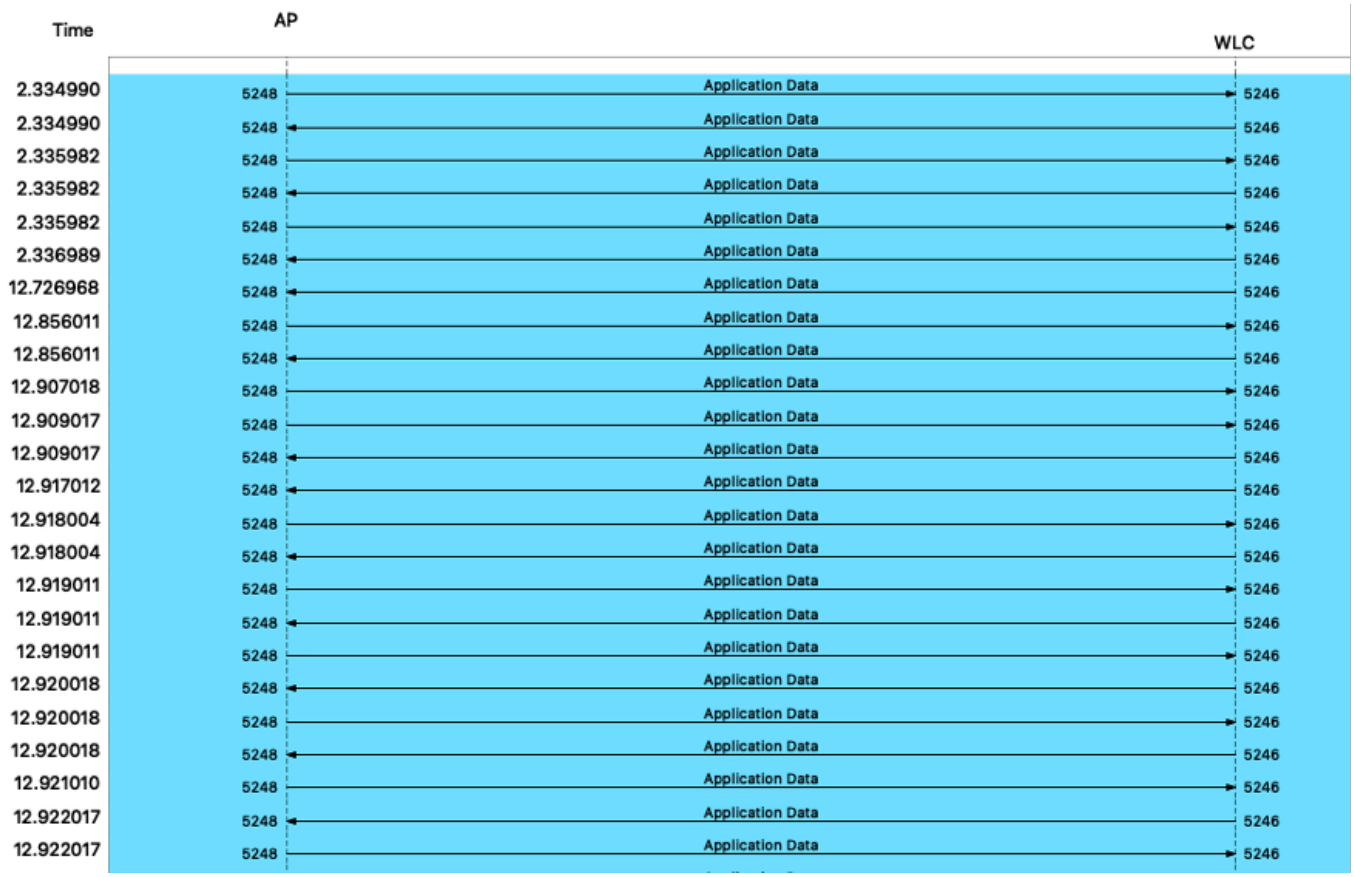
CAPWAP Image Download Window Enhancement

This feature enhances the speed of CAPWAP-based image downloads specifically for Office Extend Access Points (OEAP) or Teleworker APs. It addresses the limitation of the standard CAPWAP control channel having a single window, which requires acknowledgment for every packet before sending the next, slowing down transfers over high-latency links. This enhancement adds support for multiple sliding windows for control packets.

Impact of CAPWAP Window Size

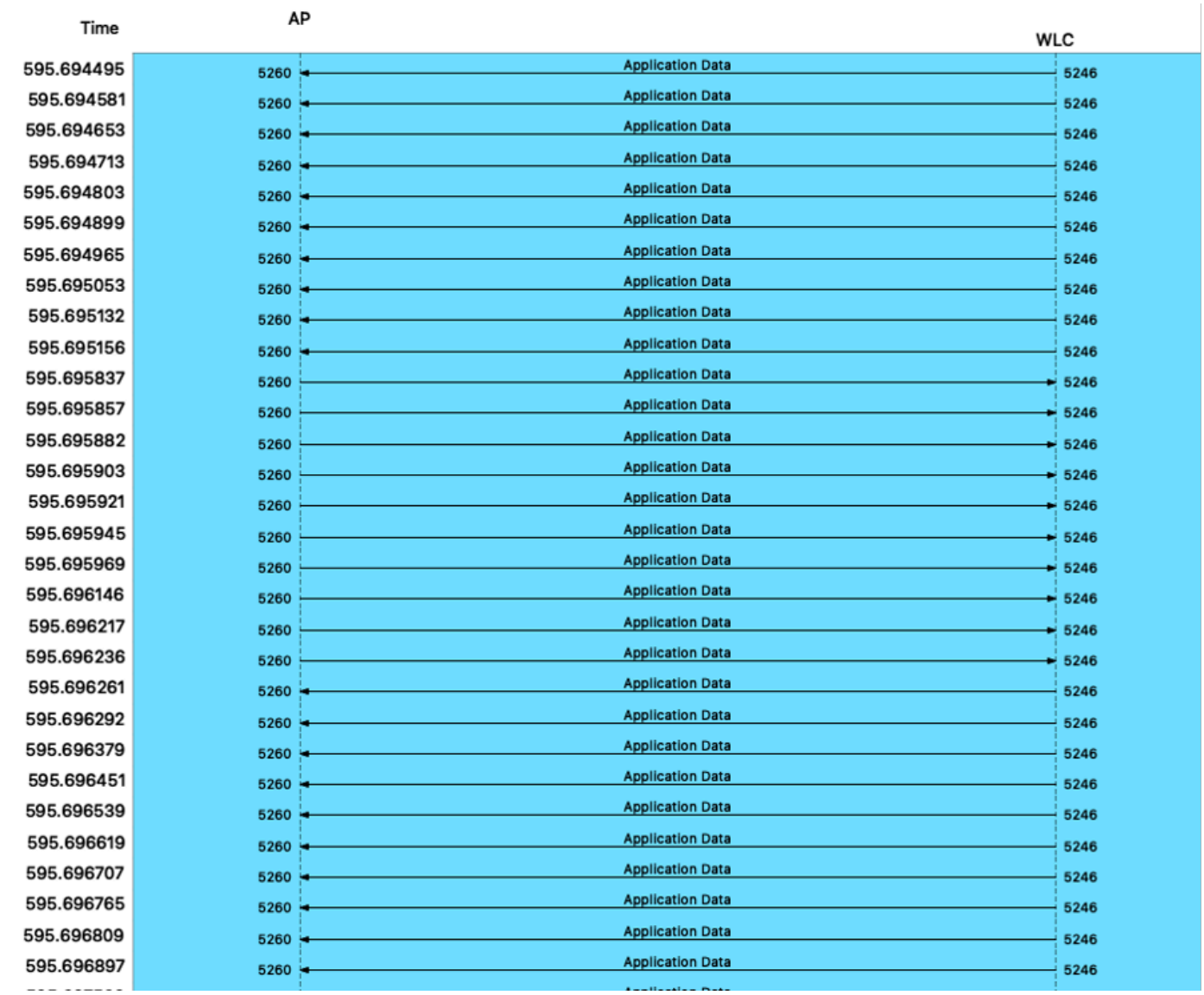
The efficiency of the CAPWAP image download process over the control channel is significantly influenced by the configured window size, especially across high-latency links.

With CAPWAP Window Size = 1 (Default/Standard): The packet flow exhibits a strict stop-and-wait behavior. For each Image Data Request packet sent by the WLC, the WLC pauses and waits for an Image Data Response acknowledgment from the AP before sending the next packet.



CAPWAP Image Upgrade Flow with Window Size 1

With CAPWAP Window Size = N (for example, 20): The packet flow demonstrates a sliding window mechanism. By allowing multiple packets to be in flight over the link before requiring an acknowledgment, the sliding window effectively masks the latency.



CAPWAP Image Upgrade Flow with Window Size 20

Process Overview

1. Configure an AP profile specifically for OEAP/Teleworker APs.
2. Set a CAPWAP window size greater than 1 within this profile.
3. Associate this AP profile to the OEAP/Teleworker APs.
4. During the AP join process, the configured window size is applied.
5. Subsequent CAPWAP image downloads utilize the larger window size, improving throughput.

Configuration (CLI)

Configure an **AP Profile** and set **CAPWAP** window size:

<#root>

```
configure terminal ap-profile capwap window size
  <- Between 3 to 20
end
```

Associate the AP profile to a site tag and apply to APs (similar to steps 2 and 3 in Efficient Image Upgrade, ensuring the correct ap-profile is linked via the site tag).

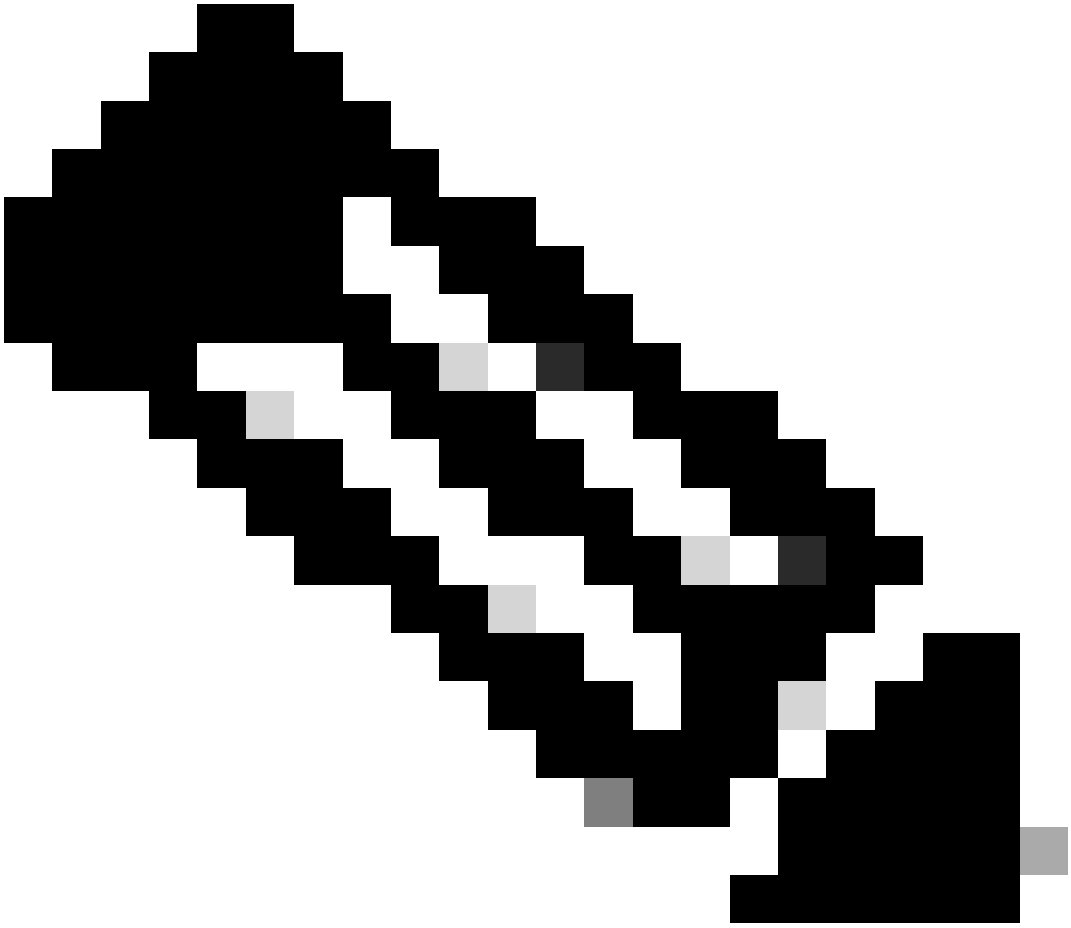
Verification (CLI)

<#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)
```

Restrictions/Considerations

- This enhancement is supported only on OEAP profiles.
- The window size gets updated on AP only during the AP join process.
- Predownload is not triggered if the latest upgrade image is already present on the AP.



Note: While primarily documented for OEAP, this enhancement has also been observed to function for regular FlexConnect APs. However, this has not been fully tested/ supported for FlexConnect deployments.

Efficient Image Upgrade in FlexConnect Mode

Efficient Image Upgrade is an optimized method specifically designed for FlexConnect APs, particularly useful in branch office deployments with limited WAN bandwidth. This method minimizes WAN load by designating a primary AP within a site tag to download the image from the controller, and then allowing other subordinate APs in the same site tag to download the image from the primary AP via TFTP. The primary AP is one AP per model per Site Tag.

Process Overview

1. A new AP image is staged on the WLC.
2. FlexConnect APs are assigned to a Site Tag configured for Efficient Image Upgrade.
3. The WLC selects one AP per model within the Site Tag as the primary AP.
4. The primary AP downloads the image from the WLC via the WAN link (typically via CAPWAP).

5. Once the primary AP has the image, subordinate APs in the same Site Tag download the image from the primary AP via TFTP over the local network.
6. At most, three subordinate APs can download simultaneously from a primary AP.
7. After download, APs reload to run the new image.

Benefits

- Reduces WAN bandwidth consumption by having only the primary AP download the image over the WAN.
- Leverages faster local network links (via TFTP) for image distribution to subordinate APs.

Configuration (CLI)

<#root>

```
Enable Predownload in Flex Profile:

configure terminal
wireless profile flex <flex-profile-name>
predownload

 <- Enables the Efficient Image Upgrade option.

end


Configure a Site Tag and Associate Flex Profile:

configure terminal
wireless tag site <site-name>
flex-profile <flex-profile-name>

<- 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 <ap-mac-address>

<- Use wired MAC address

policy-tag <policy-tag-name>
site-tag <site-tag-name>
rf-tag  <rf-tag-name>
end


Trigger Predownload to a Site Tag:

enable
ap image predownload site-tag <site-tag-name> start
```

Verification (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 <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
```

Restrictions/Considerations

- APs joined via a Site Tag must be at the same physical location for efficient local TFTP transfer.
- Uses TCP port 8443 for the listener service (also used for other functions like client debug bundles and Clean Air files). This port remains open even if the feature is disabled.
- Requires the WLC to be in install mode.

Out-of-Band HTTPs-Based AP Image Download

The OOB HTTPs-Based AP Image Download is an enhanced method introduced in Cisco IOS® XE Dublin 17.11.1 to improve AP image upgrade performance by transferring images outside the standard CAPWAP control path. A key advantage and safety net is its automatic fallback to standard in-band CAPWAP download if the HTTPs download fails.

The OOB HTTPs method leverages the standard TCP and the HTTPs for image transfer. Unlike the stop-and-wait mechanism of the CAPWAP control channel, TCP inherently uses a sliding window mechanism that allows for efficient bulk data transfer over high-latency links.

This method utilizes an webserver (nginx) running on the controller to serve AP images directly to the APs over HTTPs. This bypasses the limitations of CAPWAP control path for large file transfers, offering a potentially faster and more flexible download mechanism.

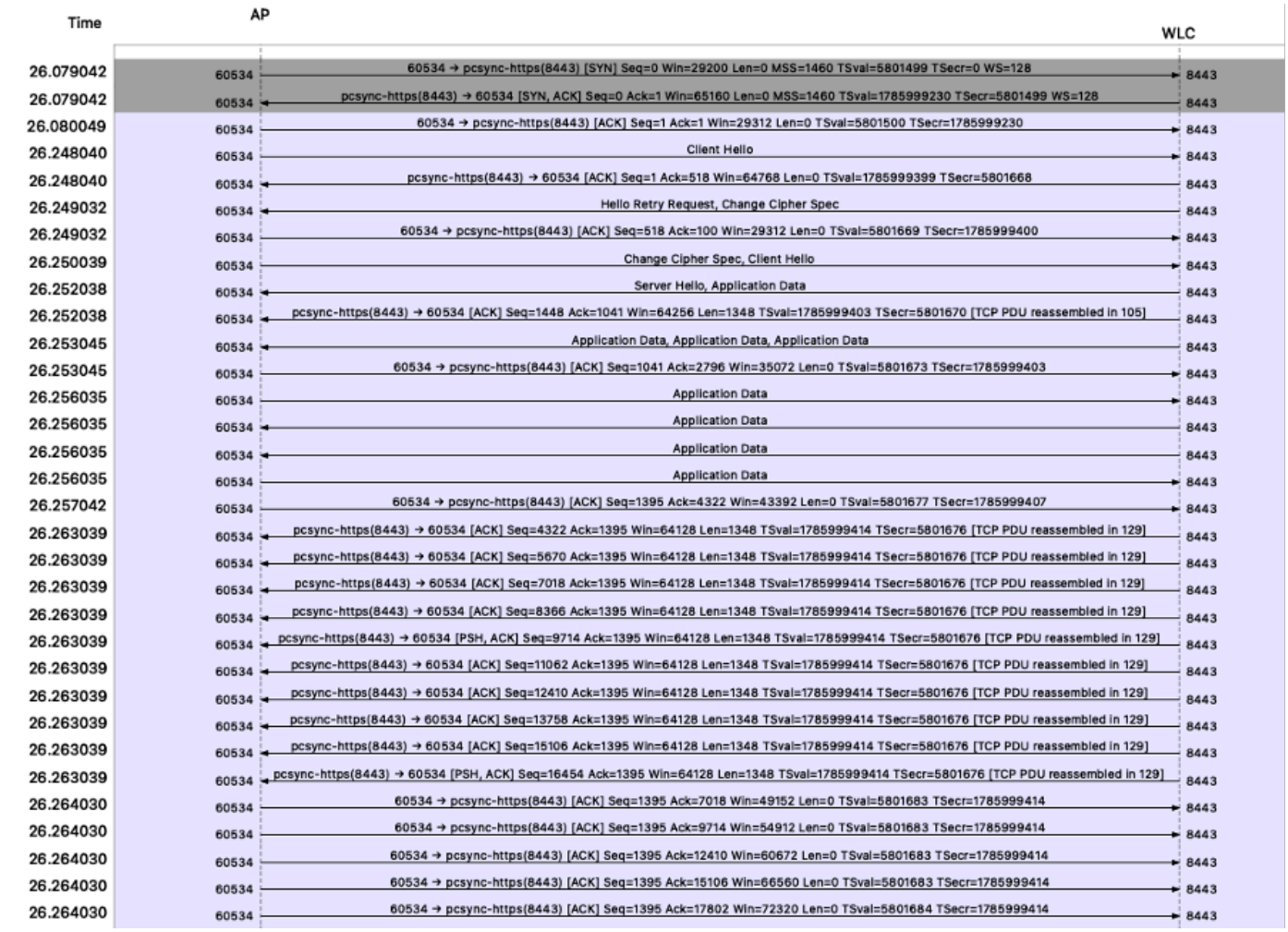
Use Case

This method is beneficial for accelerating AP image upgrades, particularly in large deployments or remote sites where the latency and bandwidth limitations of the CAPWAP control tunnel can make traditional in-band downloads time-consuming.

Process Overview

1. The new AP image is staged on the WLC.
2. The OOB HTTPs upgrade method is enabled and configured on the controller.
3. The AP, if it supports the OOB method, attempts to download the required image from the nginx webserver on the controller via HTTPs on the configured port.
4. If the HTTPs download is successful, the AP proceeds with the upgrade process.
5. If the HTTPs download fails, the AP automatically falls back to the standard in-band CAPWAP download method.

The packet capture shows the WLC acting as an HTTPs server and the AP as an HTTPs client initiating a standard TCP connection over port 8443 and file download.



HTTPS Based Image Upgrade Packet Flow

Configuration (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 <port_number>
end
```

Configuration (GUI)

1. Navigate to**Configuration > Wireless > Wireless Global**.

2. In the **AP Image Upgrade** section,**Enable HTTPs Method**.
3. (Optional)**Enter the values**in the HTTPs Port field.
4. Click **Apply to Device**.

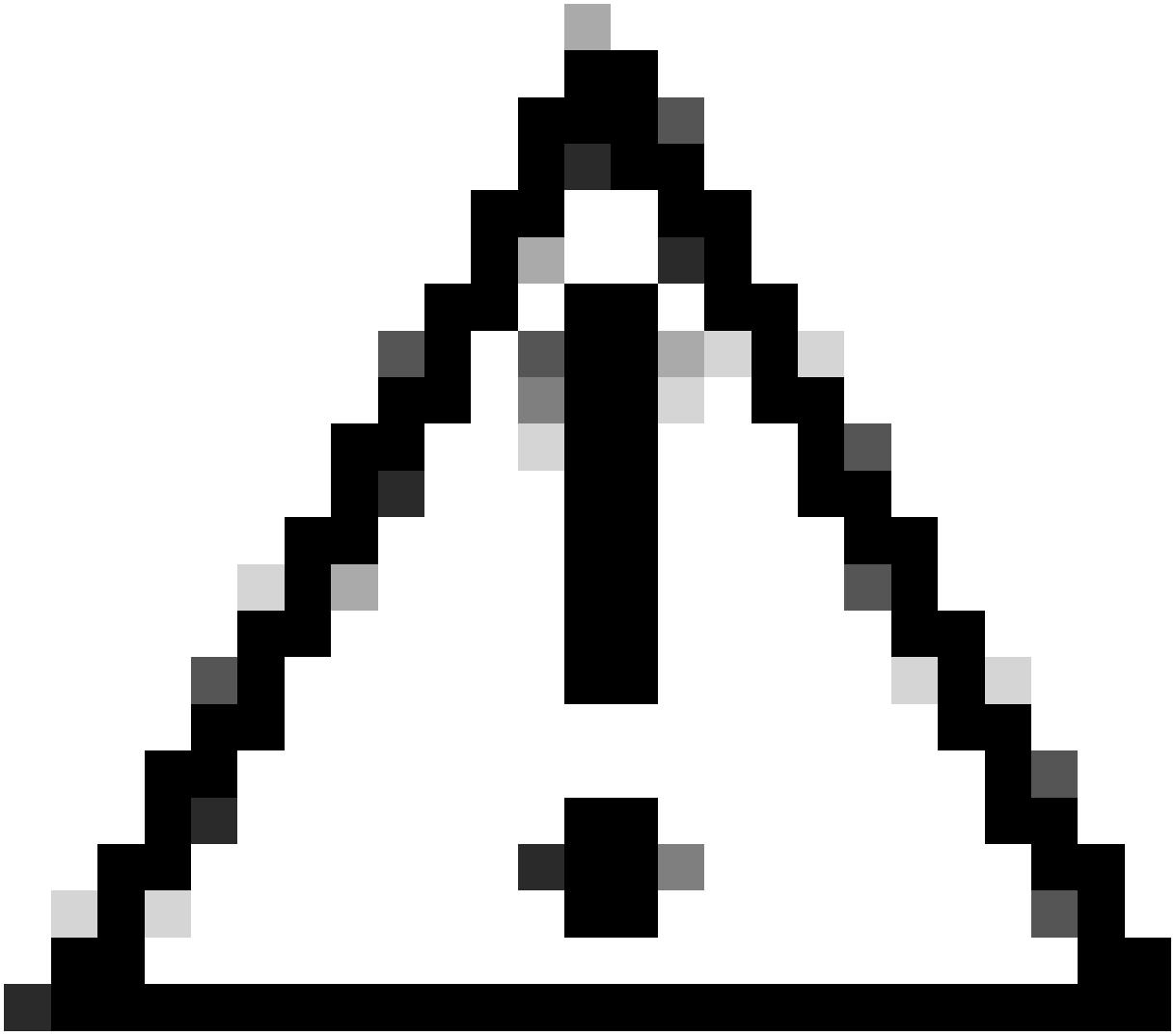
Verification (CLI)

<#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 <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
```

Restrictions/Considerations

- Requires Cisco IOS® XE Dublin 17.11.1 or later.
- Not supported on Cisco Embedded Wireless Controllers or Cisco Wave 1 Access Points.
- Requires global HTTPS configuration to be enabled on the controller.
- The nginx server must be running on the controller.
- The configured port must be reachable between the controller and APs.
- Upgrade can fail if the HTTPS server Trustpoint has a chain of CA certificates.
- Must be disabled (no ap upgrade method https) before downgrading to versions prior to Cisco IOS® XE 17.11.1.
- Port 443 is reserved. Avoid other standard/well-known ports.
- Default port 8443 conflict: If controller GUI HTTPS access also uses 8443, configure a different port for AP file transfer or GUI access.



Caution: It's important to be aware of security advisories related to file uploads, such as Cisco IOS XE Wireless Controller Software Arbitrary File Upload Vulnerability Always ensure your WLC software is up-to-date with the latest security patches.

Manual Individual AP Upgrade via TFTP/SFTP

This method involves directly accessing the AP CLI via console or SSH and initiating the image download from a TFTP or SFTP server. This is useful for troubleshooting specific APs, upgrading APs that are not currently joined to a controller, or to load a debug image provided by TAC.

Find the AP image:

This process actually loads the AP image directly onto the AP. In the case of WLC based upgrade, the WLC takes care of selecting the right image for the AP from the WLC image bundle. Here, manual selection is necessary.

The AP image version uses a different naming convention than the WLC image naming convention.

Navigate tothe link **Supported Access Points** in Cisco Catalyst 9800 Series Wireless Controller Software

Releases

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

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

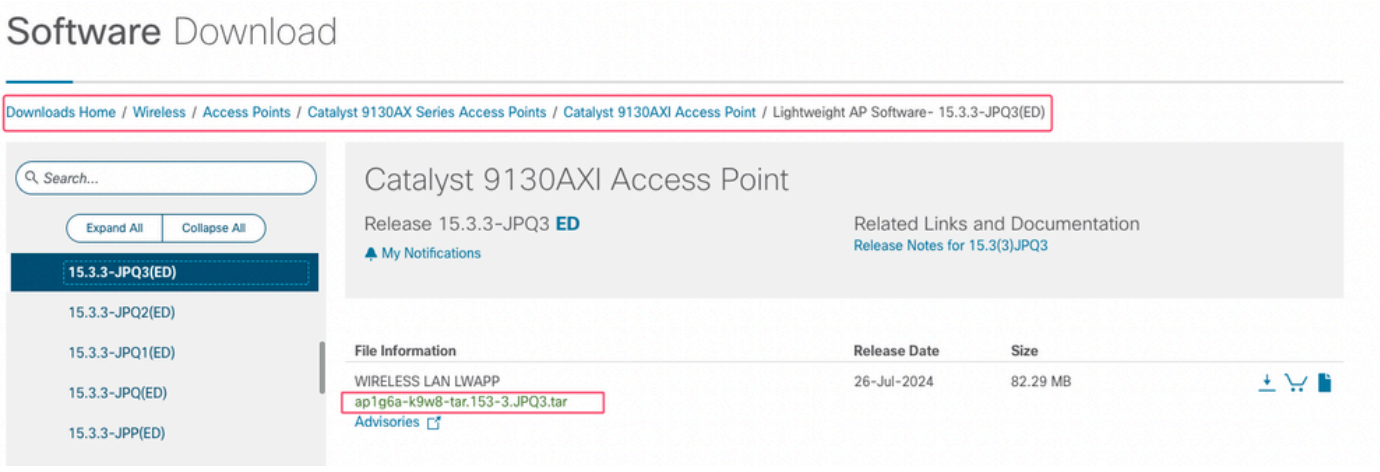
Wireless AP Compatibility Matrix

The first column describes the CCO image of the 9800 WLC. The third column lists the respective image version and the fourth column lists the supported access points for that version. Assume the need to install the AP image on AP 9130 for version 17.12.4. Checking the table shows the AP image name is15.3(3)JPQ3 and 9130 is listed as a supported model.

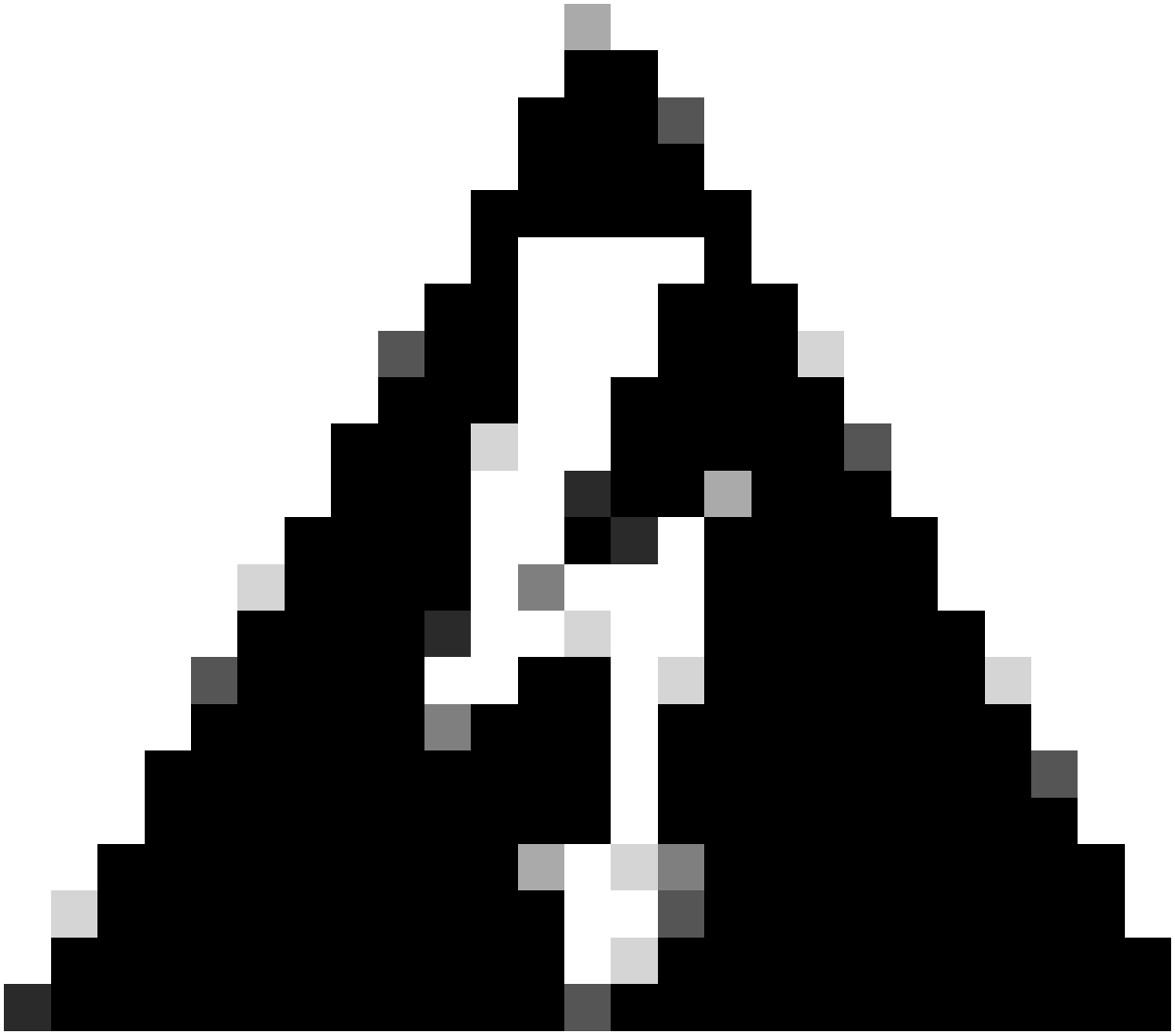
The next step is tonavigate to **software.cisco.com** and get the image from the AP download folder.

Downloads Home/ Wireless / Access Points / Catalyst 9130AX Series Access Points / Catalyst 9130AXI Access Point / Lightweight AP Software- 15.3.3-JPQ3(ED)

[Software Download - Catalyst 9130AXI Access Point]



AP Image Location



Warning: The download path differs based on the AP model and AP image version.

Process Overview

1. Stage the target AP image file(s) on an accessible TFTP or SFTP server.
2. Access the AP CLI (console or SSH).
3. Run the command **archive download-sw**, specifying the server and image file path.
4. The AP downloads the image.
5. After the download completes, restart the CAPWAP process or reload the AP for the new image to take effect.

Configuration (AP CLI)

<#root>

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

```
 <- Using TFTP:
```

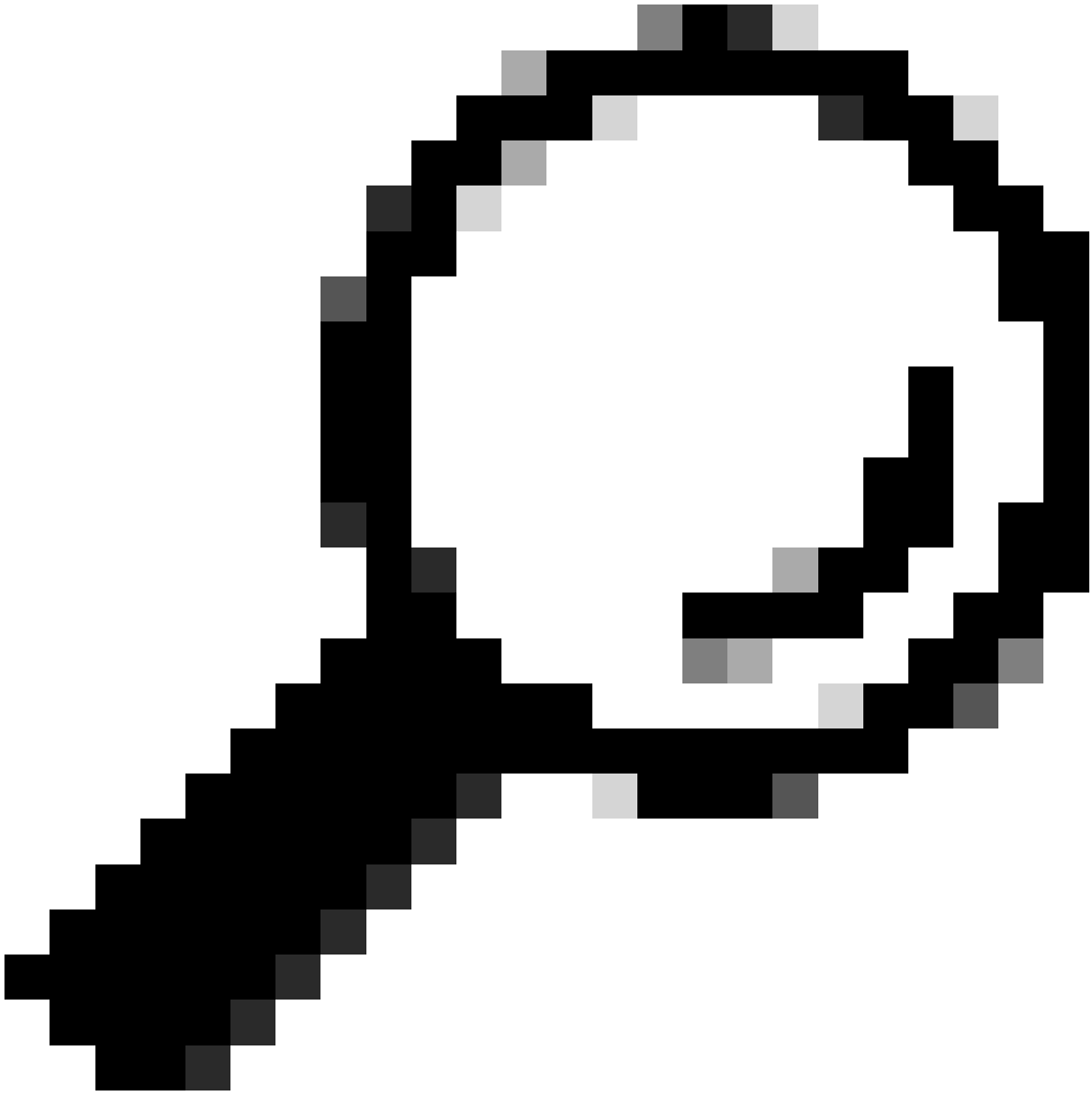
```
archive download-sw /no-reload sftp:/// Username: <SFTP_USER> Password: <SFTP_PASSWORD>
 <- Using SFTP:
reload
 <- Restart CAPWAP process after download:
```

Verification

- Monitor the TFTP/SFTP server logs to confirm the download.
- Observe the AP console for download progress and completion.
- After restart/reload, verify the new image version on the AP CLI or WLC.

Restrictions/Considerations

- Requires direct CLI access to each AP.
- Not scalable for upgrading a large number of APs individually (scripting is an option).
- TFTP performance is sensitive to latency; SFTP (using TCP) performs better over high-latency paths but requires interactive authentication (username/password).
- The/no-reloadoption prevents the AP from reloading immediately after download, allowing for manual control of the restart/reload timing.
- If migrating APs from AireOS to 9800, it is recommended to first upgrade the AP to a specific AireOS version (8.10.190.0 or higher) with fixes before joining the 9800.



Tip: WLAN Poller is a tool that can be used to create scripts to manually upgrade multiple APs. Find the WLAN Poller at this location. WLAN Poller

Which Method to Use Over Which One

- For OEAP or Teleworker APs over high-latency links:
  Enable the CAPWAP Image Download Time Enhancement. This is specifically designed to improve CAPWAP performance for these deployment types by using a sliding window, directly addressing the latency issue within the CAPWAP framework.
- For FlexConnect APs in branch offices with limited WAN bandwidth:
  Utilize the Efficient Image Upgrade in FlexConnect Mode. This method is highly recommended as it significantly reduces WAN load by using a primary AP for local distribution via TFTP, leveraging faster internal network speeds.
- For Local Mode APs (or FlexConnect/OEAP if the previously discussed methods are not applicable or sufficient) on supported platforms (Cisco IOS® XE 17.11.1+):

Consider the Out-of-Band HTTPs-Based AP Image Download. This method uses TCP/HTTPs for bulk transfer, which is more efficient over high-latency links than standard CAPWAP. It also provides a fallback to standard CAPWAP if the OOB transfer fails.

- For troubleshooting a single AP, upgrading an AP not joined to a WLC, or in emergency scenarios: Perform a Manual Individual AP Upgrade via TFTP/SFTP. This provides direct control over the upgrade process for a specific device but is not practical for large-scale deployments without automation. SFTP is generally preferred over TFTP for better performance over high-latency paths due to its use of TCP.
- Standard CAPWAP Upgrade: While the default, it is generally not recommended as the primary method for upgrading remote APs over high-latency WAN links due to its inherent stop-and-wait mechanism leading to slow transfers and potential reliability issues in older releases. Use the optimized methods described whenever possible for remote sites.

Choose the method that best aligns with your AP operating mode, network conditions, WLC software version, and the scale of your upgrade operation to ensure a smooth and efficient process for your remote APs.

Conclusion

While the standard CAPWAP image download method is suitable for local networks, remote AP deployments over WAN links benefit significantly from optimized upgrade techniques. Understanding the limitations of standard CAPWAP over high latency helps in choosing the right approach. The CAPWAP Image Download Time Enhancement improves performance for OEAP/Teleworker APs, Efficient Image Upgrade optimizes FlexConnect deployments by reducing WAN load, and Out-of-Band HTTPs offers a faster alternative for supported platforms. The manual TFTP/SFTP method remains a valuable tool for troubleshooting and specific scenarios.

References

Efficient Image Upgrade

Out-of-Band AP Image Download

AP Image Download Time Enhancement (OEAP or Teleworker Only)

Cisco Access Points Supported in Cisco Wireless Controller Platform Software Releases

WLAN Poller

Migrate from AireOS WLC to Catalyst 9800 with WLANPoller