

Inzicht in upgrades van het Access Point-image voor implementaties op afstand

Inhoud

[Inleiding](#)

[Cisco Access Point Image Upgrade Methods](#)

[De uitdaging: standaard CAPWAP-image downloaden via WAN](#)

[Verbetering van het downloadvenster voor CAPWAP-images](#)

[Procesoverzicht](#)

[Configuratie \(CLI\)](#)

[Verificatie \(CLI\)](#)

[Beperkingen/overwegingen](#)

[Efficiënte imageupgrade in FlexConnect-modus](#)

[Procesoverzicht](#)

[Voordelen](#)

[Configuratie \(CLI\)](#)

[Verificatie \(CLI\)](#)

[Beperkingen/overwegingen](#)

[Out-of-band HTTPs-gebaseerde AP Image Download](#)

[Use case](#)

[Procesoverzicht](#)

[Configuratie \(CLI\)](#)

[Configuratie \(GUI\)](#)

[Verificatie \(CLI\)](#)

[Beperkingen/overwegingen](#)

[Handmatige individuele AP-upgrade via TFTP/SFTP](#)

[Procesoverzicht](#)

[Configuratie \(AP CLI\)](#)

[Verificatie](#)

[Beperkingen/overwegingen](#)

[Welke methode te gebruiken over welke](#)

[Conclusie](#)

[Referenties](#)

Inleiding

In dit document worden methoden beschreven voor efficiënte upgrades van Cisco AP-images via WAN's, waarmee problemen op het gebied van latentie en betrouwbaarheid worden aangepakt.

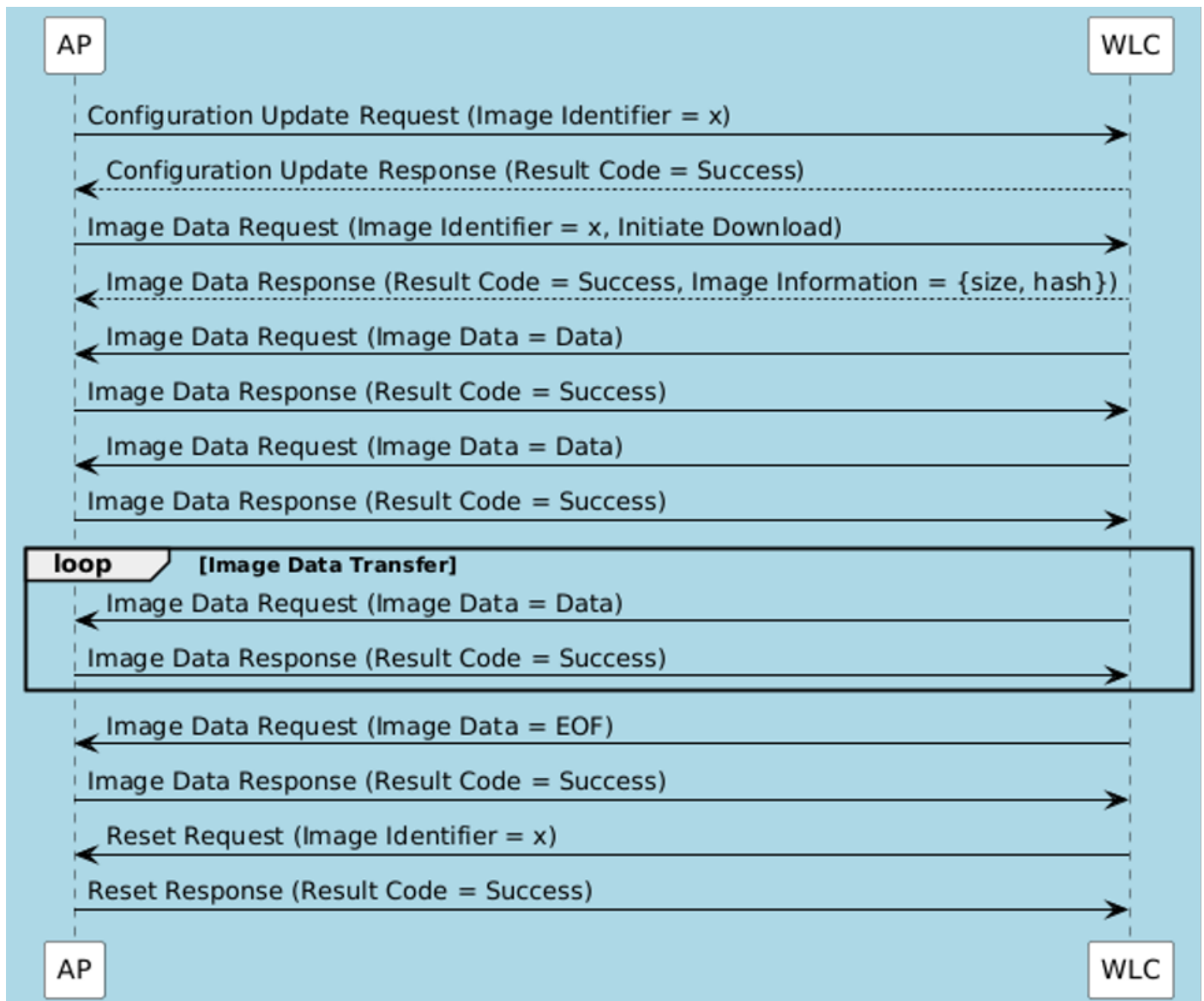
Cisco Access Point Image Upgrade Methods

Regelmatige image-upgrades zijn essentieel voor Cisco Access Points (AP), maar het kan een uitdaging zijn om deze over WAN-koppelingen (Wide Area Network) met hoge latentie naar externe locaties uit te voeren. De standaard CAPWAP-methode voor het downloaden van images is weliswaar effectief in lokale netwerken, maar kan traag en mogelijk minder betrouwbaar zijn via WAN's. In dit gedeelte wordt onderzocht waarom dit gebeurt en worden alternatieve en verbeterde methoden beschreven die zijn ontworpen voor efficiënte upgrades op afstand.

De uitdaging: standaard CAPWAP-image downloaden via WAN

Het fundamentele proces voor het upgraden van AP-images via CAPWAP is gedefinieerd in [RFC 5415](#), paragraaf 9.1. Met dit mechanisme kan de Wireless LAN Controller (WLC) het nieuwe AP-image rechtstreeks via de CAPWAP-tunnel aan de aangesloten AP's leveren. Voor elk Image Data Request-bericht (RFC 5415, sectie 9.1.1) dat een deel van de firmwaregegevens bevat, wacht de WLC op een overeenkomstige bevestiging van de Image Data Response (RFC 5415, sectie 9.1.2) van het toegangspunt voordat het volgende deel wordt verzonden.

De afbeelding illustreert het proces voor de overdracht van images tussen het toegangspunt en het WLC terwijl het toegangspunt in de uitvoeringsstand staat.



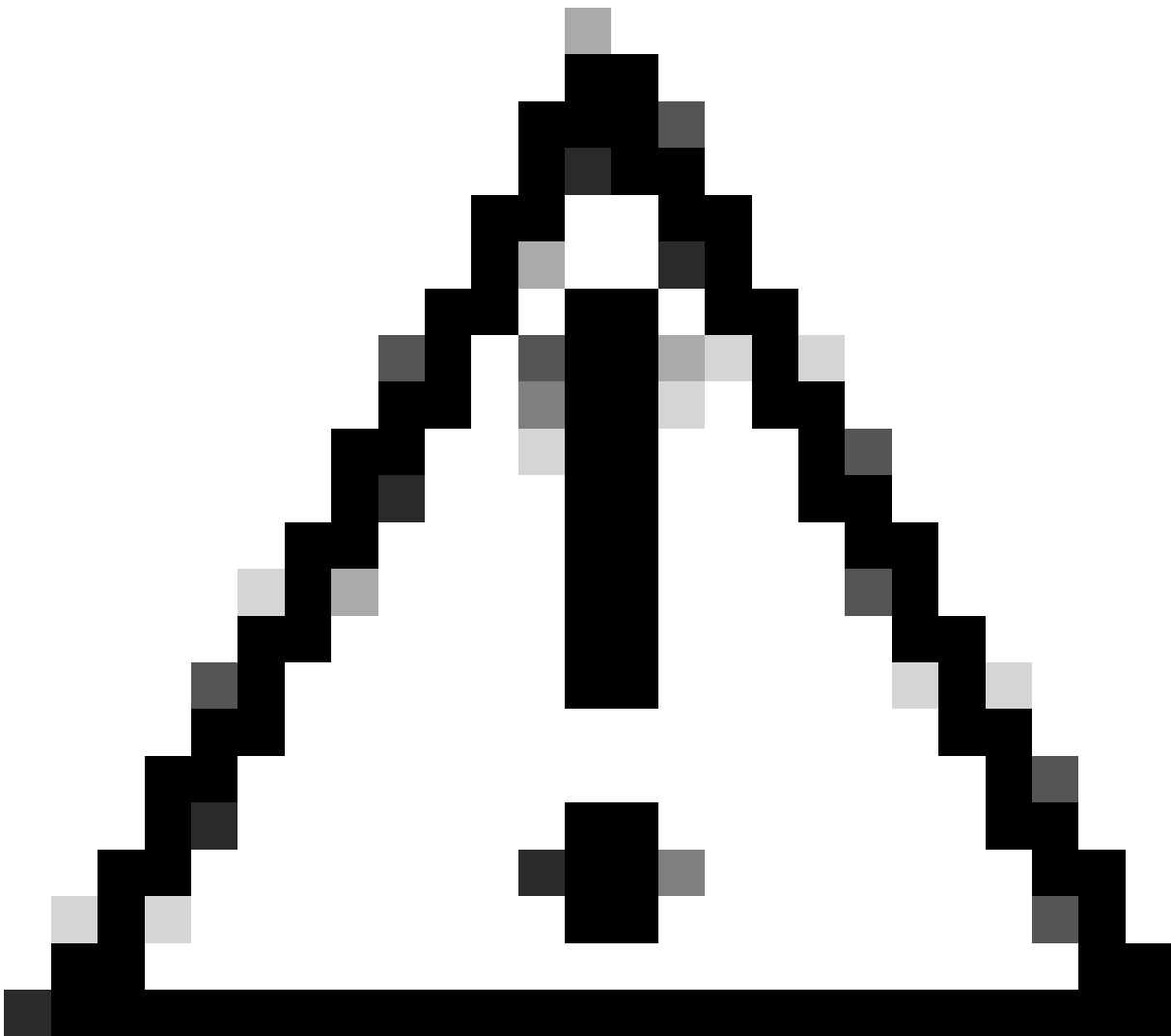
Processtroom voor overdracht van AP-images

Zoals opgemerkt, verzendt de WLC Image Data Request-berichten met stukjes van de firmware-afbeeldingsgegevens. De AP bevestigt de ontvangst van deze brokken door het verzenden van Image Data Response berichten. Deze uitwisseling gaat door totdat het hele beeld is overgebracht.

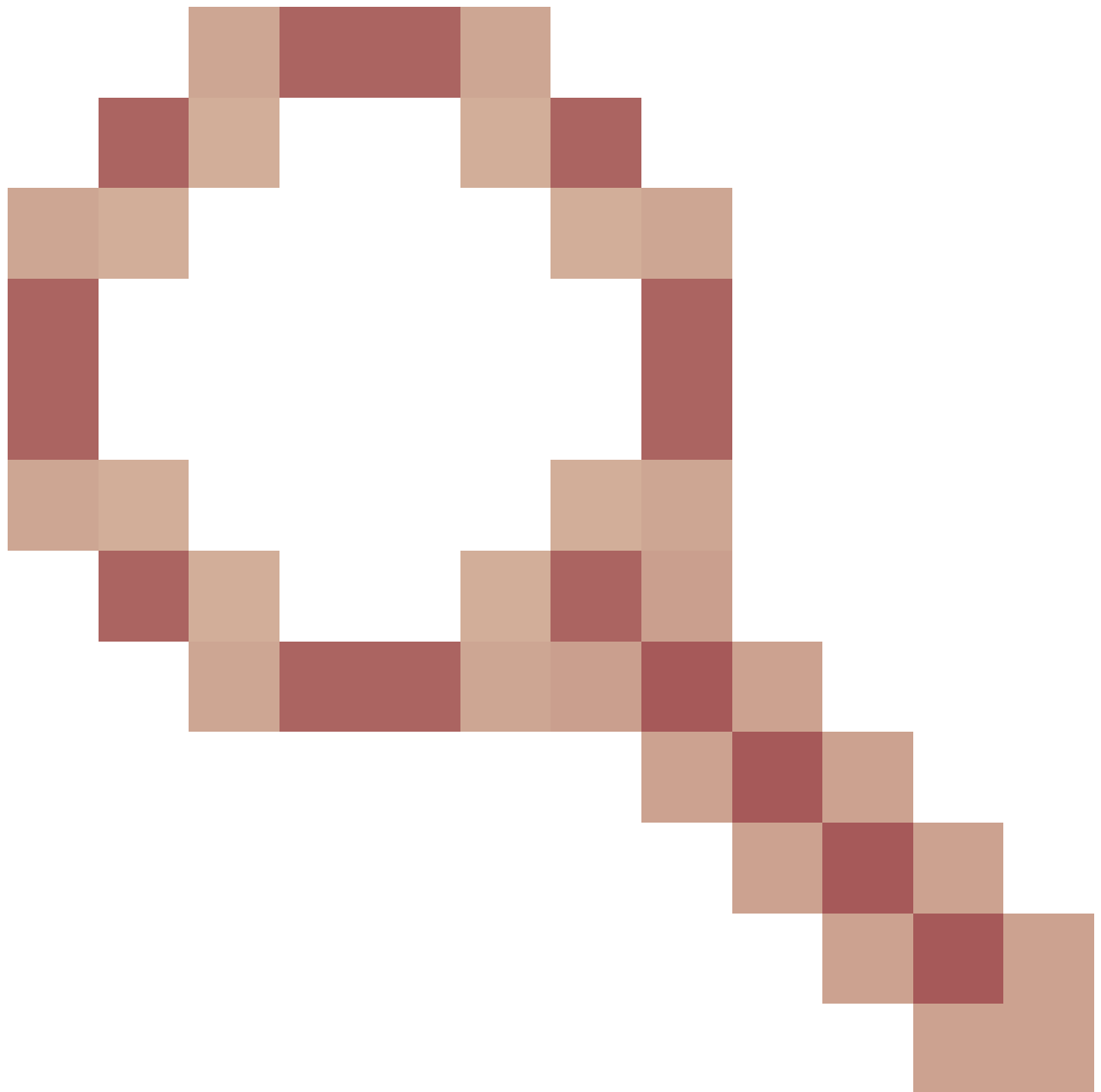
Voor elk Image Data Request-bericht wordt een corresponderend Image Data Response-bericht verwacht als bevestiging. Dit betekent dat het toegangspunt moet wachten tot elk afbeeldingspakket is aangekomen, het moet bevestigen en vervolgens moet wachten op het volgende pakket. Dit leidt tot traagheid bij het downloaden van afbeeldingen in WAN-omgevingen.

Neem een voorbeeld: als de RTT (Round Trip Time) tussen het toegangspunt en de WLC 100 ms is, beperkt dit de overdrachtssnelheid effectief tot ongeveer 10 pakketten per seconde. Als elke pakketgrootte 1000 bytes is, vertaalt dit zich in een maximale doorvoer van 10 KB / sec. Als het AP-image 50 MB is, bedraagt de theoretische minimumtijd voor het voltooien van de overdracht ongeveer 5120 seconden. Dit illustreert dat zelfs als er aanzienlijke bandbreedte beschikbaar is, de CAPWAP-imagedownload traag kan aanvoelen vanwege dit stop-and-wait-bevestigingsmechanisme. Dit effect is minder merkbaar bij lokale beeldoverdrachten waarbij de

WLC en AP deel uitmaken van hetzelfde campusnetwerk en de latentie minimaal is.



Let op: Een lossy WAN-link kan mogelijk leiden tot beeldbeschadiging. Zie Cisco-bug [IDCSCwf09053](https://tools.cisco.com/tsg/bugtools/bugsearch.do?bugid=IDCSCwf09053)



voor meer informatie hierover.

Om deze beperkingen te beperken die inherent zijn aan het standaard CAPWAP-besturingspad-overdrachtmechanisme, met name in WAN-omgevingen met hoge latentie of bandbreedte, werden drie verbeteringen geïntroduceerd.

1. De CAPWAP-vensterverbetering verbetert het CAPWAP-besturingspad zelf door een schuifvenster met meerdere pakketten te implementeren, waardoor meerdere gegevenspakketten kunnen worden verzonden voordat een bevestiging nodig is, waardoor de doorvoer over koppelingen met hoge latentie binnen het CAPWAP-framework wordt verhoogd.
2. Efficiënte imageupgrade in de FlexConnect-modus is een geoptimaliseerde methode die speciaal is ontworpen voor FlexConnect-toegangspunten, die vaak worden geïmplementeerd in filialen met een beperkte WAN-bandbreedte. Deze methode minimaliseert de WAN-belasting door de downloadtaak van het image te verdelen.

3. De Out-of-Band HTTPs-Based AP Image Download-methode pakt dit aan door gebruik te maken van een afzonderlijk, efficiënter HTTPs-protocol dat op een speciale webserver op de controller voor de beeldoverdracht wordt uitgevoerd en buiten de beperkende CAPWAP-besturingstunnel wordt verplaatst.

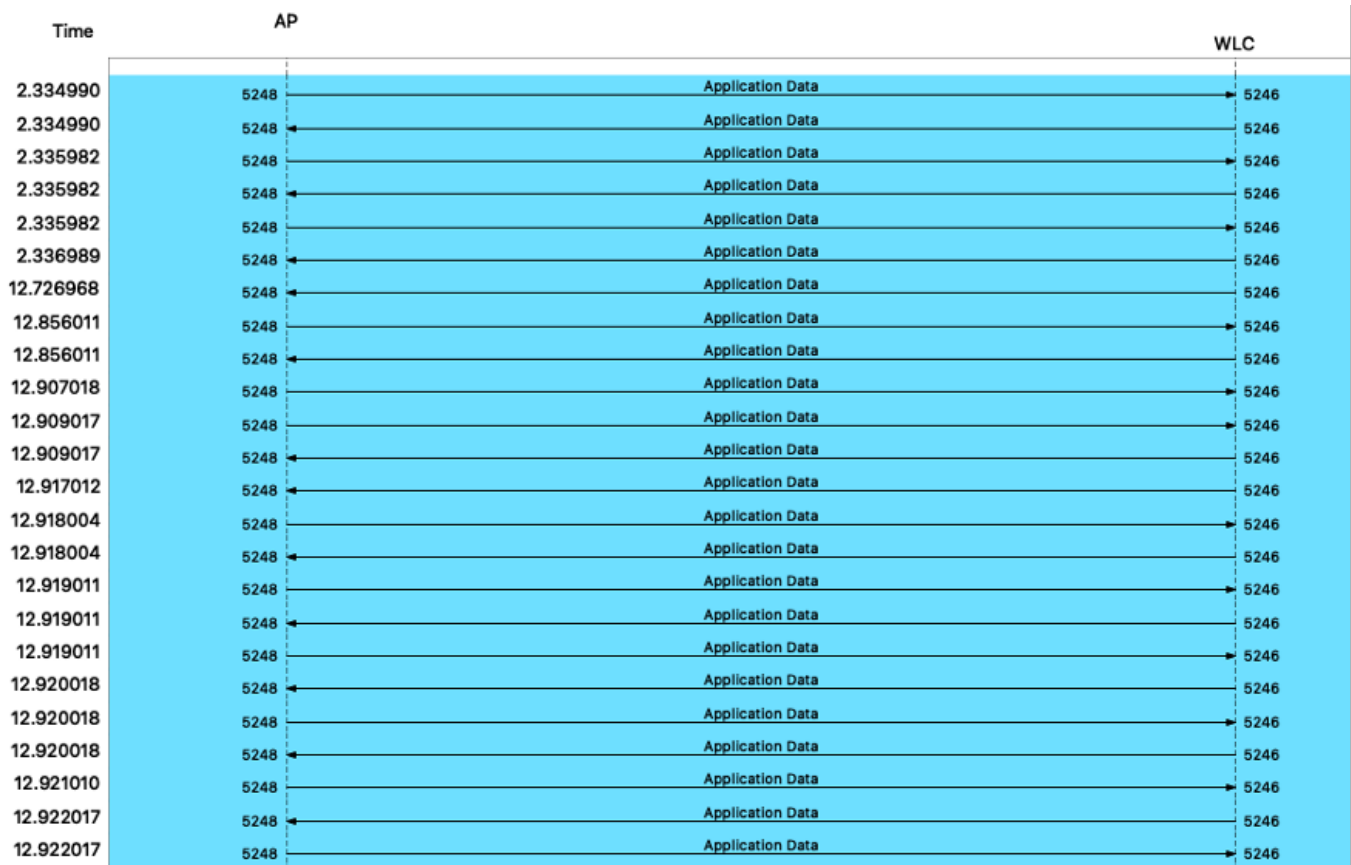
Verbetering van het downloadvenster voor CAPWAP-images

Deze functie verbetert de snelheid van het downloaden van op CAPWAP gebaseerde images, speciaal voor Office Extended Access Points (OEAP) of Teleworker AP's. Het behandelt de beperking van het standaard CAPWAP-controlekanaal met één venster, waarvoor erkenning voor elk pakket vereist is voordat het volgende wordt verzonden, waardoor overdrachten over koppelingen met hoge latentie worden vertraagd. Deze verbetering voegt ondersteuning toe voor meerdere schuifvensters voor besturingspakketten.

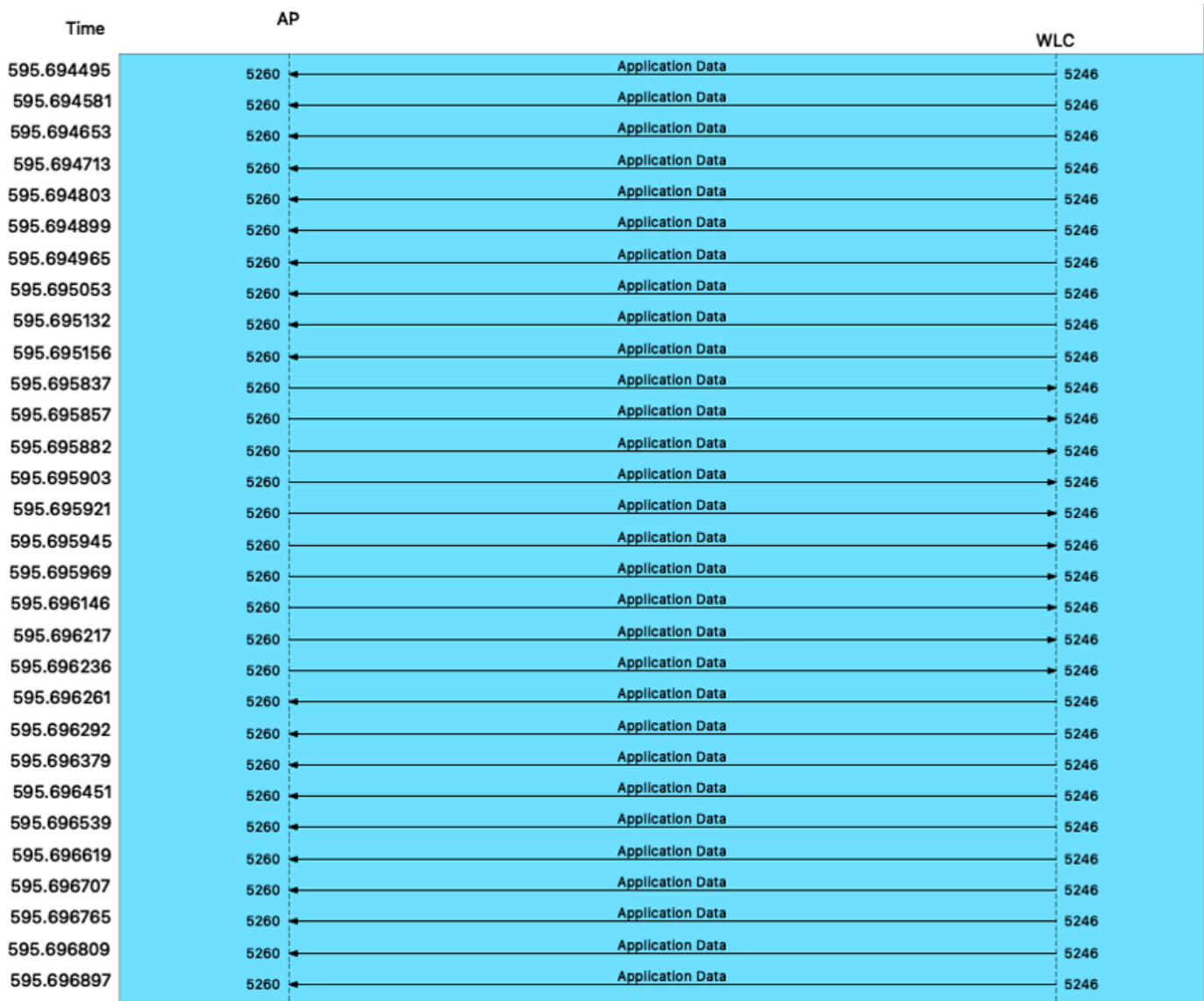
Impact van de grootte van het CAPWAP-venster

De efficiëntie van het downloaden van het CAPWAP-image via het controlekanaal wordt sterk beïnvloed door de geconfigureerde venstergrootte, met name bij koppelingen met hoge latentie.

Met CAPWAP Window Size = 1 (Standaard/Standaard): De pakketstroom vertoont een strikt stop-and-wait gedrag. Voor elk pakket Image Data Request dat door de WLC wordt verzonden, pauzeert de WLC en wacht op een bevestiging van de AP voor de reactie op de beeldgegevens voordat het volgende pakket wordt verzonden.



Met CAPWAP Window Size = N (bijvoorbeeld 20): De pakketstroom toont een schuifvenstermechanisme. Door toe te staan dat meerdere pakketten over de link vliegen voordat een bevestiging nodig is, maskeert het schuifvenster effectief de latentie.



Upgrade van CAPWAP-image met venstergrootte 20

Procesoverzicht

1. Configureer een AP-profiel specifiek voor OEAP/Teleworker AP's.
2. Stel binnen dit profiel een CAPWAP-venstergrootte in die groter is dan 1.
3. Koppel dit AP-profiel aan de OEAP/Teleworker AP's.
4. Tijdens het proces voor het aansluiten van het toegangspunt wordt de geconfigureerde venstergrootte toegepast.
5. Latere CAPWAP-imagedownloads maken gebruik van het grotere vensterformaat, waardoor de doorvoer wordt verbeterd.

Configuratie (CLI)

Configureer een AP-profiel en stel de grootte van het CAPWAP-venster in:

```
<#root>
```

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

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

```
end
```

Koppel het AP-profiel aan een sitetag en pas dit toe op AP's (vergelijkbaar met stap 2 en 3 in Efficiënte imageupgrade, waarbij wordt gewaarborgd dat het juiste AP-profiel via de sitetag wordt gekoppeld).

Verificatie (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)
```

Beperkingen/overwegingen

- Deze verbetering wordt alleen ondersteund op OEAP-profielen.
- De venstergrootte wordt alleen bijgewerkt op het toegangspunt tijdens het aanmeldingsproces van het toegangspunt.
- De predownload wordt niet geactiveerd als de laatste upgrade-image al op het toegangspunt aanwezig is.

Efficiënte imageupgrade in FlexConnect-modus

Efficiënte imageupgrade is een geoptimaliseerde methode die speciaal is ontworpen voor FlexConnect-toegangspunten en die met name nuttig is bij implementaties in filialen met beperkte WAN-bandbreedte. Deze methode minimaliseert de WAN-belasting door een primair toegangspunt binnen een sitetag aan te wijzen om de afbeelding van de controller te downloaden en vervolgens andere ondergeschikte toegangspunten in dezelfde sitetag toe te staan de afbeelding via TFTP van het primaire toegangspunt te downloaden. Het primaire toegangspunt is één toegangspunt per model per sitetag.

Procesoverzicht

1. Er wordt een nieuwe AP-afbeelding geënceneerd op de WLC.
2. FlexConnect-toegangspunten worden toegewezen aan een sitetag die is geconfigureerd voor een efficiënte imageupgrade.
3. De WLC selecteert één AP per model binnen de Site Tag als het primaire AP.
4. De primaire AP downloadt de afbeelding van de WLC via de WAN-link (meestal via CAPWAP).
5. Zodra het primaire toegangspunt het image heeft, downloaden ondergeschikte toegangspunten in dezelfde sitetag het image van het primaire toegangspunt via TFTP over het lokale netwerk.
6. Maximaal drie ondergeschikte toegangspunten kunnen gelijktijdig downloaden van een primair toegangspunt.
7. Na het downloaden worden de toegangspunten opnieuw geladen om het nieuwe image uit te voeren.

Voordelen

- Vermindert het WAN-bandbreedteverbruik doordat alleen het primaire toegangspunt het image via het WAN kan downloaden.
- Maakt gebruik van snellere lokale netwerkkoppelingen (via TFTP) voor de distributie van images naar ondergeschikte toegangspunten.

Configuratie (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
```

Verificatie (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
```

Beperkingen/overwegingen

- AP's die via een sitetag zijn aangesloten, moeten zich op dezelfde fysieke locatie bevinden voor een efficiënte lokale TFTP-overdracht.
- Gebruikt TCP-poort 8443 voor de listenerservice (ook gebruikt voor andere functies zoals bundels voor clientfoutopsporing en Clean Air-bestanden). Deze poort blijft open, zelfs als de functie is uitgeschakeld.
- De WLC moet in de installatiemodus staan.

Out-of-band HTTPs-gebaseerde AP Image Download

De OOB HTTPs-Based AP Image Download is een verbeterde methode die is geïntroduceerd in Cisco IOS® XE Dublin 17.11.1 om de prestaties van de AP-image-upgrade te verbeteren door afbeeldingen buiten het standaard CAPWAP-beheerpad te plaatsen.

De OOB HTTPs methode maakt gebruik van de standaard TCP en de HTTPs voor beeldoverdracht. In tegenstelling tot het stop-and-wait-mechanisme van het CAPWAP-besturingskanaal, maakt TCP inherent gebruik van een schuifvenstermechanisme dat een efficiënte overdracht van bulkgegevens over koppelingen met hoge latentie mogelijk maakt.

Deze methode maakt gebruik van een webserver (nginx) die op de controller wordt uitgevoerd om AP-afbeeldingen rechtstreeks via HTTP's aan de AP's te leveren. Dit omzeilt de beperkingen van het CAPWAP-besturingspad voor grote bestandsoverdrachten en biedt een potentieel sneller en flexibeler downloadmechanisme.

Use case

Deze methode is gunstig voor het versnellen van AP-image upgrades, met name in grote implementaties of externe sites waar de latentie en bandbreedte beperkingen van de CAPWAP control tunnel traditionele in-band downloads tijdrovend kan maken.

Procesoverzicht

1. De nieuwe AP-afbeelding wordt geënceneerd op de WLC.
2. De OOB HTTP-upgrademethode is ingeschakeld en geconfigureerd op de controller.
3. Als het toegangspunt de OOB-methode ondersteunt, probeert het de vereiste afbeelding te downloaden van de nginx-webserver op de controller via HTTP's op de geconfigureerde poort.
4. Als de HTTP-download succesvol is, gaat het toegangspunt verder met het upgradeproces.
5. Als de HTTP-download mislukt, valt het toegangspunt automatisch terug naar de standaard in-band CAPWAP-downloadmethode.

De pakketopname toont de WLC die fungeert als een HTTPs-server en de AP als een HTTPs-client die een standaard TCP-verbinding initieert via poort 8443 en het downloaden van bestanden.

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	60534 ← 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	60534 → Client Hello	8443
26.248040	60534 ← pcsync-https(8443) → 60534 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=1785999399 TSecr=5801668	8443
26.249032	60534 → 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	60534 → Change Cipher Spec, Client Hello	8443
26.252038	60534 → Server Hello, Application Data	8443
26.252038	60534 ← 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	60534 → 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	60534 → Application Data	8443
26.256035	60534 → Application Data	8443
26.256035	60534 → Application Data	8443
26.256035	60534 → 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	60534 ← 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	60534 ← 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	60534 ← 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	60534 ← 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	60534 ← 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	60534 ← 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	60534 ← 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	60534 ← 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	60534 ← 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	60534 ← 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

HTTPS-gebaseerde pakketstroom voor image-upgrade

Configuratie (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

Configuratie (GUI)

1. Ga naar Configuratie > Draadloos > Draadloos wereldwijd.
2. Schakel in het gedeelte AP Image Upgrade de HTTP-methode in.
3. (Optioneel) Voer de waarden in het veld HTTPs-poort in.
4. Klik op Toepassen op apparaat.

Verificatie (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 : Enabled")

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

Beperkingen/overwegingen

- Vereist Cisco IOS® XE Dublin 17.11.1 of hoger.
- Niet ondersteund op Cisco Embedded Wireless Controllers of Cisco Wave 1 Access Points.
- Hiervoor moet de globale HTTPS-configuratie op de controller zijn ingeschakeld.
- De nginx-server moet op de controller worden uitgevoerd.
- De geconfigureerde poort moet bereikbaar zijn tussen de controller en het toegangspunt.
- Upgrade kan mislukken als de HTTPS-server Trustpoint een keten van CA-certificaten heeft.
- Moet zijn uitgeschakeld (geen ap-upgrademethode https) voordat u een downgrade uitvoert naar versies vóór Cisco IOS® XE 17.11.1.
- Port 443 is gereserveerd. Vermijd andere standaard/bekende poorten.

- Standaardpoortconflict 8443: Als controller GUI HTTPS-toegang ook 8443 gebruikt, configureert u een andere poort voor AP-bestandsoverdracht of GUI-toegang.

Handmatige individuele AP-upgrade via TFTP/SFTP

Deze methode omvat het rechtstreeks benaderen van de AP CLI via console of SSH en het starten van het downloaden van de afbeelding van een TFTP- of SFTP-server. Dit is handig voor het oplossen van problemen met specifieke toegangspunten, het upgraden van toegangspunten die momenteel niet zijn gekoppeld aan een controller of het laden van een foutopsporingsafbeelding die wordt geleverd door TAC.

Zoek de AP-afbeelding:

Met dit proces wordt de AP-afbeelding rechtstreeks op het toegangspunt geladen. In het geval van een op WLC gebaseerde upgrade zorgt de WLC ervoor dat de juiste afbeelding voor het toegangspunt wordt geselecteerd uit de WLC-beeldbundel. Handmatige selectie is hierbij noodzakelijk.

De AP-afbeeldingsversie gebruikt een andere naamgevingsconventie dan de WLC-afbeeldingsnaamgevingsconventie.

Navigeer naar de link [Ondersteunde toegangspunten in Cisco Catalyst 9800 Series Wireless Controller Software Releases](#)

[Ondersteunde toegangspunten in Cisco Catalyst 9800 Series Wireless Controller-software releases](#)

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

Compatibiliteitsmatrix voor draadloze toegangspunten

De eerste kolom beschrijft de CCO-afbeelding van de 9800 WLC. In de derde kolom wordt de betreffende afbeeldingsversie weergegeven en in de vierde kolom worden de ondersteunde toegangspunten voor die versie weergegeven. Ga ervan uit dat het AP-image voor versie 17.17.1 op AP 9130 moet worden geïnstalleerd. Als u de tabel controleert, wordt de naam van de AP-afbeelding 15.3.(3)JPV en 9130 weergegeven als een ondersteund model.

De volgende stap is om naar software.cisco.com te navigeren en de afbeelding uit de map AP-download te halen.

Downloads Home / Draadloos / Toegangspunten Catalyst 9130AX-serie toegangspunten / Catalyst 9130AXI-toegangspunt / Lichtgewicht AP-software - 17.17.1(ED)

[Softwaredownload - Catalyst 9130AXI Access Point](#)

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		

Locatie AP-afbeelding



Waarschuwing: het downloadpad verschilt afhankelijk van het AP-model en de versie van het AP-image.

Procesoverzicht

1. Stage de doel-AP-afbeeldingsbestanden op een toegankelijke TFTP- of SFTP-server.
2. Toegang tot de AP CLI (console of SSH).
3. Voer de opdracht `archiefdownload-sw` uit, waarbij u het server- en imagebestandspad opgeeft.
4. Het toegangspunt downloadt de afbeelding.
5. Nadat de download is voltooid, start u het CAPWAP-proces opnieuw op of laadt u het toegangspunt opnieuw zodat het nieuwe image van kracht wordt.

Configuratie (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:

Verificatie

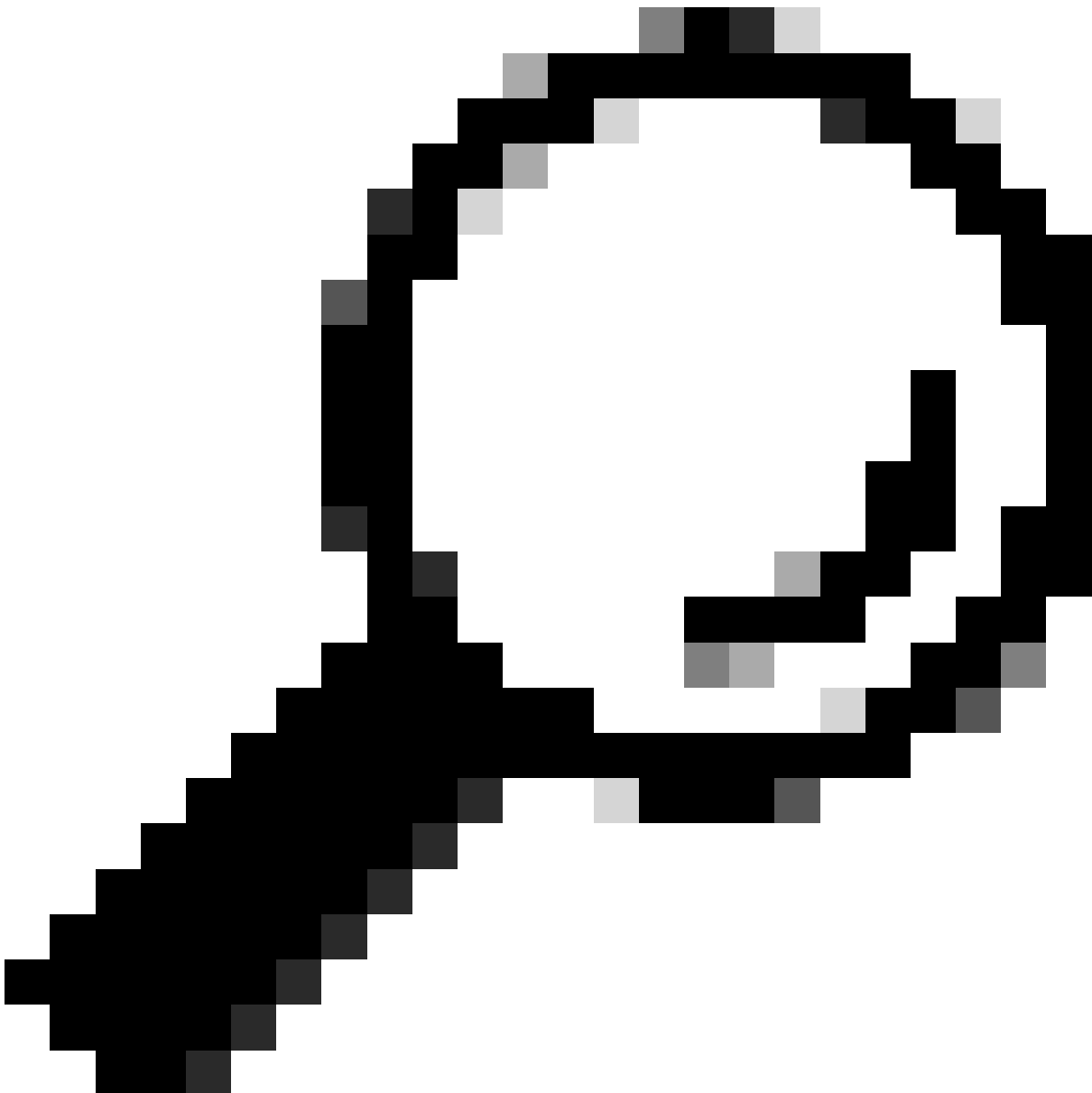
- Controleer de logbestanden van de TFTP/SFTP-server om de download te bevestigen.
- Observeer de AP-console voor de voortgang en voltooiing van het downloaden.
- Controleer na het opnieuw starten/laden de nieuwe versie van het image op de AP CLI of WLC.

Beperkingen/overwegingen

- Vereist directe CLI-toegang tot elk toegangspunt.
- Niet schaalbaar voor het afzonderlijk upgraden van een groot aantal toegangspunten

(scripting is een optie).

- TFTP-prestaties zijn gevoelig voor latentie; SFTP (met behulp van TCP) presteert beter over paden met hoge latentie, maar vereist interactieve verificatie (gebruikersnaam/wachtwoord).
 - De/no-reloadoptie voorkomt dat het toegangspunt onmiddellijk na het downloaden opnieuw wordt geladen, waardoor de timing van het opnieuw opstarten/opnieuw laden handmatig kan worden geregeld.
 - Als u toegangspunten van AireOS naar 9800 migreert, wordt aanbevolen om eerst het toegangspunt te upgraden naar een specifieke versie van AireOS (8.10.190.0 of hoger) met oplossingen voordat u zich bij de 9800 aansluit.
-



Tip: WLAN Poller is een tool die kan worden gebruikt om scripts te maken om handmatig meerdere toegangspunten te upgraden. Zoek de WLAN Poller op deze locatie. [WLAN-poller](#)

Welke methode te gebruiken over welke

- Voor OEAP- of Teleworker-toegangspunten via verbindingen met hoge latentie:
De verlenging van de downloadtijd van het CAPWAP-image inschakelen. Dit is specifiek ontworpen om de CAPWAP-prestaties voor deze implementatietypen te verbeteren door een schuifvenster te gebruiken waarmee het latentieprobleem direct wordt aangepakt binnen het CAPWAP-framework.
- Voor FlexConnect-toegangspunten in filialen met beperkte WAN-bandbreedte:
Gebruik de efficiënte imageupgrade in de FlexConnect-modus. Deze methode wordt sterk aanbevolen omdat de WAN-belasting aanzienlijk wordt verminderd door een primair toegangspunt te gebruiken voor lokale distributie via TFTP, waarbij gebruik wordt gemaakt van hogere interne netwerksnelheden.
- Voor toegangspunten in de lokale modus (of FlexConnect/OEAP als de eerder besproken methoden niet van toepassing of toereikend zijn) op ondersteunde platforms (Cisco IOS® XE 17.11.1+):
Overweeg de Out-of-Band HTTPs-gebaseerde AP Image Download. Deze methode maakt gebruik van TCP/HTTP's voor bulkoverdracht, wat efficiënter is via koppelingen met hoge latentie dan standaard CAPWAP. Het biedt ook een terugval naar standaard CAPWAP als de OOB-overdracht mislukt.
- Voor het oplossen van problemen met één toegangspunt, het upgraden van een toegangspunt dat niet is gekoppeld aan een WLC, of in noodscenario's:
Voer een handmatige individuele AP-upgrade uit via TFTP/SFTP. Dit biedt directe controle over het upgradeproces voor een specifiek apparaat, maar is niet praktisch voor grootschalige implementaties zonder automatisering. SFTP heeft over het algemeen de voorkeur boven TFTP voor betere prestaties over paden met hoge latentie vanwege het gebruik van TCP.
- Standaard CAPWAP-upgrade: hoewel de standaard is, wordt deze over het algemeen niet aanbevolen als de primaire methode voor het upgraden van externe toegangspunten via WAN-verbindingen met hoge latentie vanwege het inherente stop-en-wachtmechanisme dat leidt tot langzame overdrachten en potentiële betrouwbaarheidsproblemen in oudere releases. Gebruik waar mogelijk de beschreven geoptimaliseerde methoden voor externe locaties.

Kies de methode die het beste aansluit bij de besturingsmodus van uw toegangspunt, de netwerkomstandigheden, de WLC-softwareversie en de schaal van uw upgradebewerking om een soepel en efficiënt proces voor uw externe toegangspunten te garanderen.

Conclusie

Hoewel de standaard CAPWAP-methode voor het downloaden van images geschikt is voor lokale netwerken, profiteren externe AP-implementaties via WAN-koppelingen aanzienlijk van geoptimaliseerde upgradetechnieken. Inzicht in de beperkingen van standaard CAPWAP over hoge latentie helpt bij het kiezen van de juiste aanpak. De CAPWAP Image Download Time Enhancement verbetert de prestaties voor OEAP/Teleworker-toegangspunten, Efficient Image Upgrade optimaliseert FlexConnect-implementaties door de WAN-belasting te verminderen en

Out-of-Band HTTP's bieden een sneller alternatief voor ondersteunde platforms. De handmatige TFTP/SFTP-methode blijft een waardevol hulpmiddel voor het oplossen van problemen en specifieke scenario's.

Referenties

[Efficiënte imageupgrade](#)

[Out-of-band AP Image Download](#)

[AP Image Download Time Enhancement \(alleen OEAP of telewerker\)](#)

[Cisco-toegangspunten ondersteund in software releases van Cisco Wireless Controller-platform](#)

[WLAN-poller](#)

[Migreren van AireOS WLC naar Catalyst 9800 met WLANPoller](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.