

リモート導入用のアクセスポイントイメージアップグレードについて

内容

[はじめに](#)

[Ciscoアクセスポイントイメージアップグレード方式](#)

[課題：WAN経由での標準的なCAPWAPイメージのダウンロード](#)

[CAPWAPイメージダウンロードウィンドウの機能拡張](#)

[プロセスの概要](#)

[設定\(CLI\)](#)

[検証\(CLI\)](#)

[制限事項/考慮事項](#)

[FlexConnectモードでの効率的なイメージアップグレード](#)

[プロセスの概要](#)

[利点](#)

[設定\(CLI\)](#)

[検証\(CLI\)](#)

[制限事項/考慮事項](#)

[アウトオブバンドHTTPSベースのAPイメージのダウンロード](#)

[使用例](#)

[プロセスの概要](#)

[設定\(CLI\)](#)

[設定\(GUI\)](#)

[検証\(CLI\)](#)

[制限事項/考慮事項](#)

[TFTP/SFTPによる個々のAPの手動アップグレード](#)

[プロセスの概要](#)

[設定\(AP CLI\)](#)

[検証](#)

[制限事項/考慮事項](#)

[使用する方式](#)

[結論](#)

[参考資料](#)

はじめに

このドキュメントでは、WAN経由でCisco APイメージを効率的にアップグレードし、遅延と信頼性の課題に対処する方法について説明します。

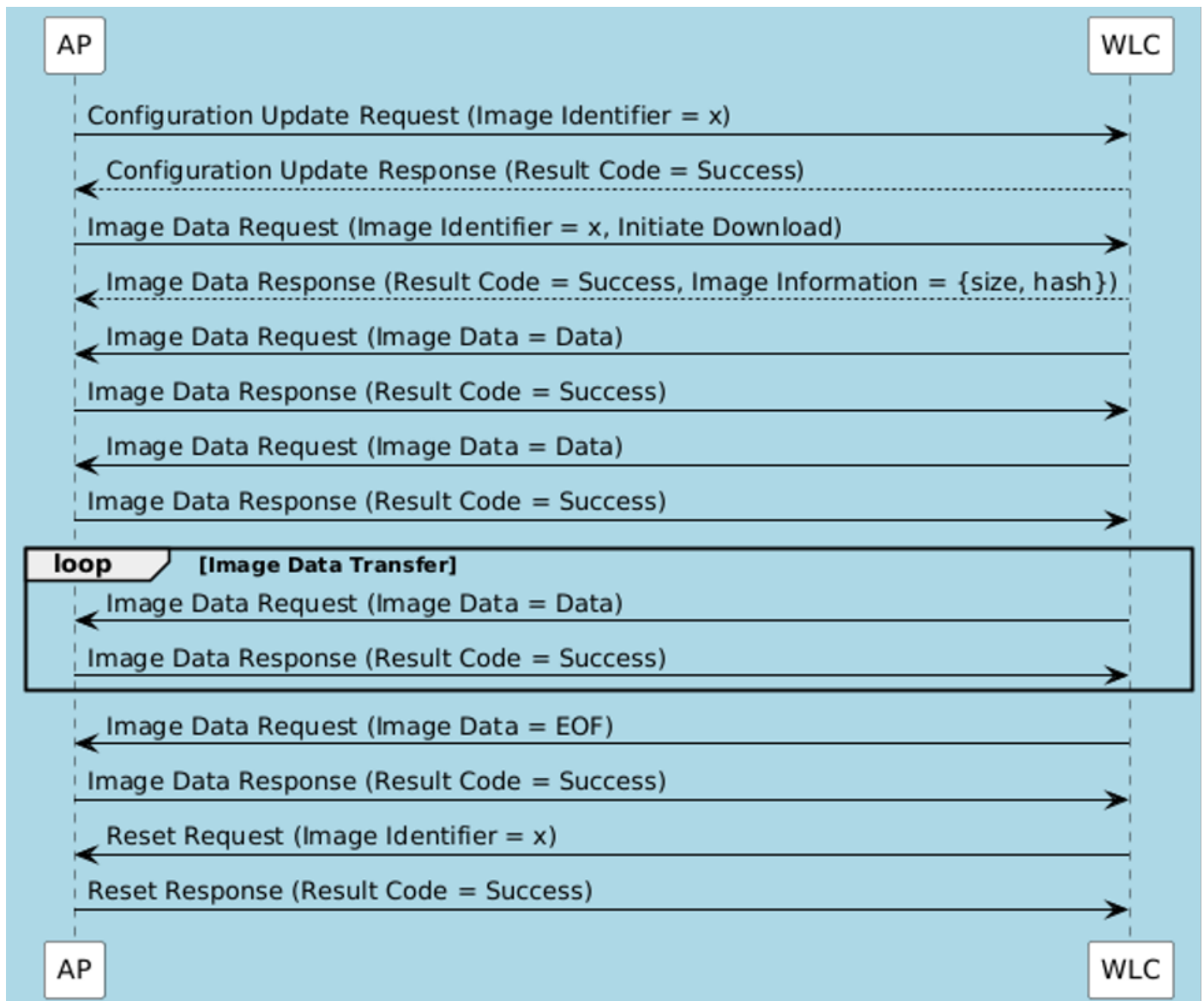
Ciscoアクセスポイントイメージアップグレード方式

シスコのアクセスポイント(AP)では定期的なイメージアップグレードが不可欠ですが、このようなアップグレードを高遅延のワイドエリアネットワーク(WAN)リンク経由でリモートサイトに対して実行するのは困難な場合があります。標準のCAPWAPイメージダウンロード方式は、ローカルネットワークでは効果的ですが、低速で、WAN経由での信頼性が低い可能性があります。このセクションでは、この問題が発生する理由を説明し、効率的なリモートアップグレードのために設計された代替および強化された方法の概要を示します。

課題：WAN経由での標準的なCAPWAPイメージのダウンロード

CAPWAPによるAPイメージのアップグレードの基本的なプロセスは、[RFC 5415](#)のセクション9.1で定義されています。このメカニズムにより、ワイヤレスLANコントローラ(WLC)は、CAPWAPトンネルを介して、接続されたAPに新しいAPイメージを直接提供できます。ファームウェアデータのチャンクを含むImage Data Request (RFC 5415、セクション9.1.1) ごとに、WLCは、次のチャンクを送信する前に、APからの対応するImage Data Response Acknowledgment (RFC 5415、セクション9.1.2) を待機します。

次の図は、APがrun状態の間のAPとWLCの間のイメージ転送プロセスを示しています。

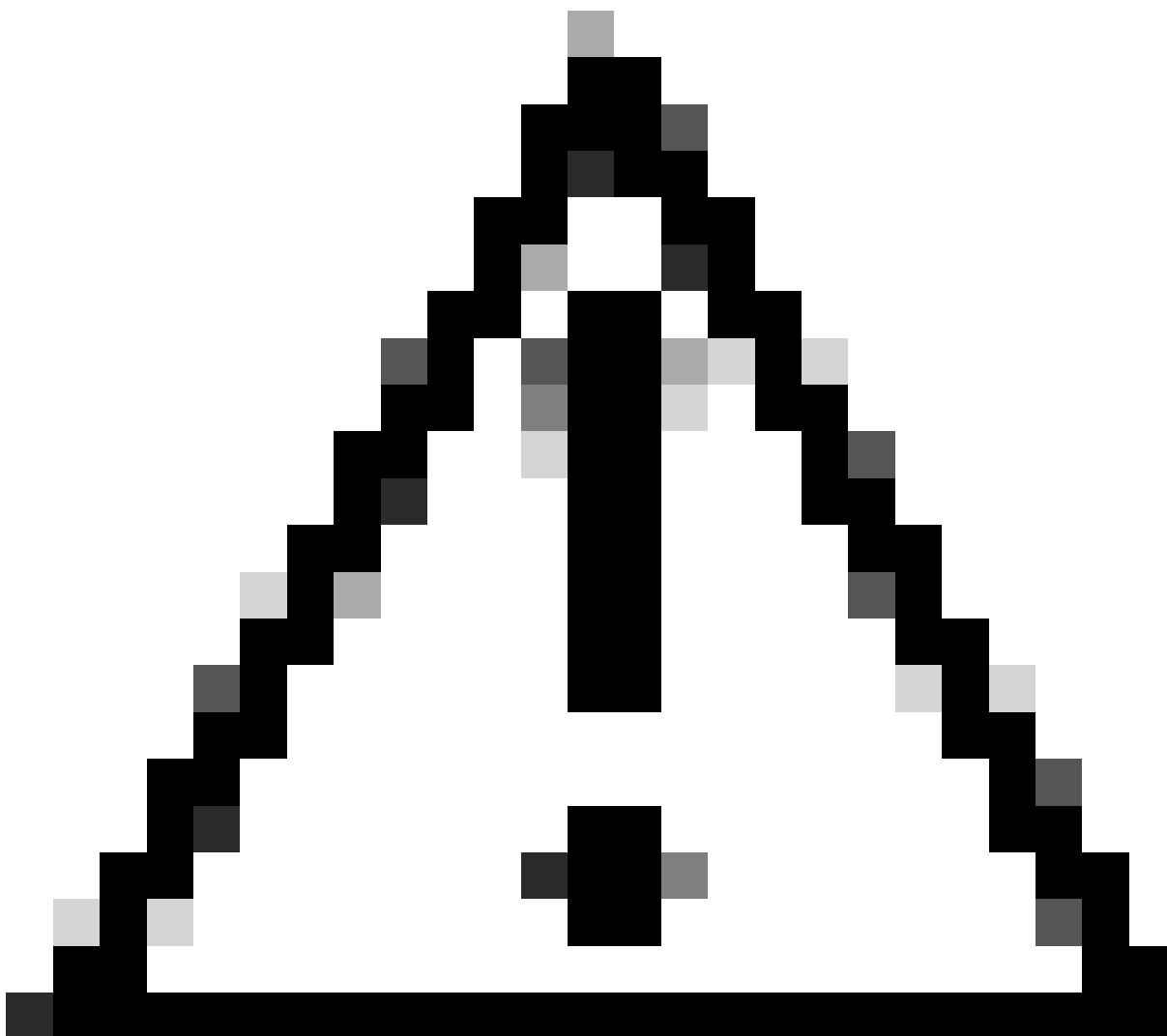


APイメージ転送のプロセスフロー

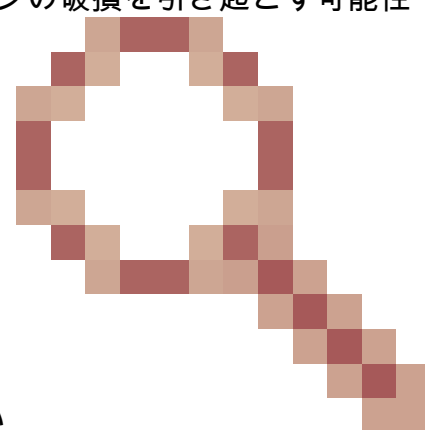
観察されたように、WLCはファームウェアイメージデータのチャンクを含むイメージデータ要求メッセージを送信します。APは、Image Data Response(IDR)メッセージを送信して、これらのチャンクの受信を確認応答します。この交換は、イメージ全体が転送されるまで続きます。

各画像データ要求メッセージに対して、対応する画像データ応答メッセージが確認応答として期待されます。つまり、APは各イメージパケットが到着するのを待ち、確認応答を行い、次のパケットを待つ必要があります。これにより、WAN環境でのイメージダウンロードの速度が低下します。

たとえば、APとWLCの間のラウンドトリップ時間(RTT)が100ミリ秒の場合、これによって転送レートが実質的に1秒あたり約10パケットに制限されます。各パケットサイズが1000バイトの場合、最大スループットは10 KB/秒になります。APイメージが50MBの場合、転送を完了するための理論上の最小時間は約5120秒です。このことは、たとえ十分な帯域幅が使用可能であっても、このSTOP-AND-WAIT確認応答メカニズムのためにCAPWAPイメージのダウンロードが遅いと感じる場合があることを示しています。この影響は、WLCとAPが同じキャンパスネットワークの一部であり、遅延が最小限であるローカルイメージ転送では目立ちません。



注意：パケット損失の起こりやすいWANリンクは、イメージの破損を引き起こす可能性



があります。Cisco Bug [IDCSCwf09053](#)を参照してください
を参照してください。

特に高遅延または帯域幅に制約のあるWAN環境において、標準のCAPWAP制御パス転送メカニズムに内在するこれらの制限を緩和するために、3つの機能拡張が導入されました。

1. CAPWAPウィンドウ拡張機能は、マルチパケットスライディングウィンドウを実装するこ

とで、CAPWAP制御パス自体を改善します。これにより、確認応答が必要になる前に複数のデータパケットを送信できるようになり、CAPWAPフレームワーク内の高遅延リンクのスループットが向上します。

2. FlexConnectモードでのEfficient Image Upgradeは、WAN帯域幅が限られているブランチオフィスで頻繁に導入されるFlexConnect AP用に設計された最適化方式です。この方法では、イメージのダウンロードタスクを配布することにより、WANの負荷を最小限に抑えます。
3. アウトオブバンドHTTPsベースのAPイメージのダウンロード方式では、イメージ転送のためにコントローラ上の専用Webサーバで実行される、独立した、より効率的なHTTPsプロトコルを活用し、限定的なCAPWAP制御トンネルの外部に移動させることで、この問題に対処しています。

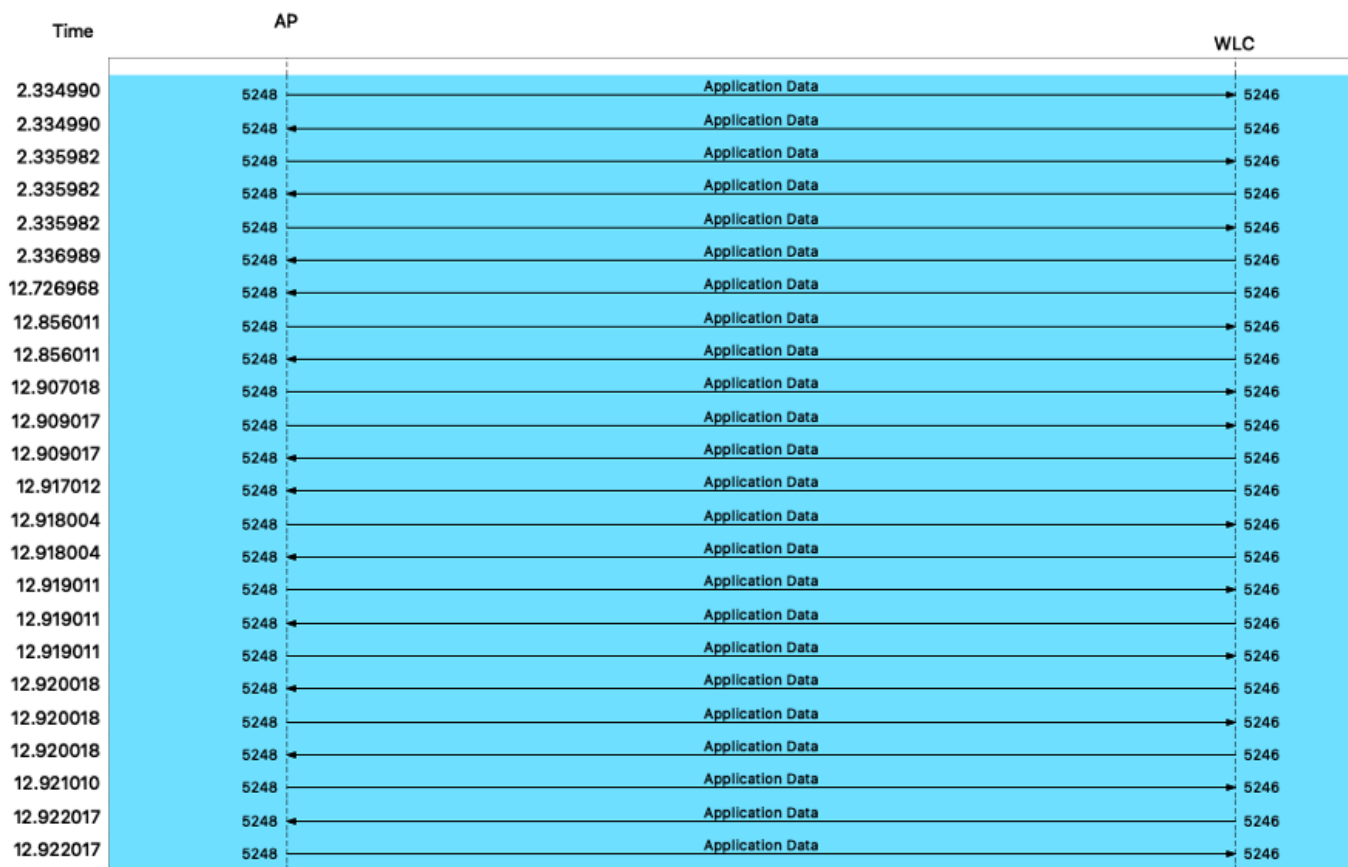
CAPWAPイメージダウンロードウィンドウの機能拡張

この機能により、Office Extend Access Points(OEAP)またはテレワーカーAP専用のCAPWAPベースのイメージダウンロードの速度が向上します。これは、単一のウィンドウを持つ標準のCAPWAP制御チャネルの制限に対処するもので、次のパケットを送信する前にすべてのパケットに対して確認応答が必要になるため、高遅延リンクでの転送が遅くなります。この機能拡張により、制御パケットに対する複数のスライディングウィンドウのサポートが追加されました。

CAPWAPウィンドウサイズの影響

制御チャネルでのCAPWAPイメージダウンロードプロセスの効率は、設定されたウィンドウサイズ (特に高遅延リンク間) によって大きく影響されます。

CAPWAPウィンドウサイズ= 1 (デフォルト/標準) : パケットフローは厳密なstop-and-wait動作を示します。WLCから送信されたImage Data Request(MDRQ)パケットごとに、WLCは一時停止し、APからのImage Data Response確認応答を待機してから、次のパケットを送信します。



ウィンドウサイズ1のCAPWAPイメージアップグレードフロー

CAPWAPウィンドウサイズ= N (たとえば20) : パケットフローはスライディングウィンドウメカニズムを示します。確認応答を要求する前に複数のパケットがリンク上を通過できるようにすることで、スライディングウィンドウは遅延を効果的にマスクします。

Time	AP	WLC
595.694495	5260 ←	Application Data → 5246
595.694581	5260 ←	Application Data → 5246
595.694653	5260 ←	Application Data → 5246
595.694713	5260 ←	Application Data → 5246
595.694803	5260 ←	Application Data → 5246
595.694899	5260 ←	Application Data → 5246
595.694965	5260 ←	Application Data → 5246
595.695053	5260 ←	Application Data → 5246
595.695132	5260 ←	Application Data → 5246
595.695156	5260 ←	Application Data → 5246
595.695837	5260 ←	Application Data → 5246
595.695857	5260 ←	Application Data → 5246
595.695882	5260 ←	Application Data → 5246
595.695903	5260 ←	Application Data → 5246
595.695921	5260 ←	Application Data → 5246
595.695945	5260 ←	Application Data → 5246
595.695969	5260 ←	Application Data → 5246
595.696146	5260 ←	Application Data → 5246
595.696217	5260 ←	Application Data → 5246
595.696236	5260 ←	Application Data → 5246
595.696261	5260 ←	Application Data → 5246
595.696292	5260 ←	Application Data → 5246
595.696379	5260 ←	Application Data → 5246
595.696451	5260 ←	Application Data → 5246
595.696539	5260 ←	Application Data → 5246
595.696619	5260 ←	Application Data → 5246
595.696707	5260 ←	Application Data → 5246
595.696765	5260 ←	Application Data → 5246
595.696809	5260 ←	Application Data → 5246
595.696897	5260 ←	Application Data → 5246

ウィンドウサイズが20のCAPWAPイメージアップグレードフロー

プロセスの概要

1. OEAP/テレワーカーAP専用のAPプロファイルを設定します。
2. このプロファイル内でCAPWAPウィンドウサイズを1より大きく設定します。
3. このAPプロファイルをOEAP/テレワーカーAPに関連付けます。
4. APの加入プロセス中に、設定されたウィンドウサイズが適用されます。
5. 以降のCAPWAPイメージのダウンロードでは、より大きなウィンドウサイズが使用され、スループットが向上します。

設定(CLI)

APプロファイルを設定し、CAPWAPウィンドウサイズを設定します。

<#root>

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

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

```
end
```

APプロファイルをサイトタグに関連付け、APに適用します (「効率的なイメージアップグレード」のステップ2および3と同様に、正しいAPプロファイルがサイトタグを介してリンクされていることを確認します)。

検証(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)
```

制限事項/考慮事項

- この拡張機能は、OEAPプロファイルでのみサポートされます。
- ウィンドウサイズは、AP加入プロセス中にのみAPで更新されます。
- 最新のアップグレードイメージがAPにすでに存在している場合、プレダウロードはトリガーされません。

FlexConnectモードでの効率的なイメージアップグレード

Efficient Image Upgradeは、FlexConnect AP用に設計された最適化方式で、特にWAN帯域幅に制限のあるブランチオフィスへの導入に役立ちます。この方法では、サイトタグ内のプライマリAPを指定してコントローラからイメージをダウンロードした後、同じサイトタグ内の他の下位APがTFTPを介してプライマリAPからイメージをダウンロードできるようにすることで、WANの負荷を最小限に抑えます。プライマリAPは、サイトタグごとのモデルごとに1つのAPです。

プロセスの概要

1. 新しいAPイメージがWLCでステージングされます。
2. FlexConnect APは、効率的なイメージアップグレードのために設定されたサイトタグに割り当てられます。
3. WLCは、サイトタグ内のモデルごとに1つのAPをプライマリAPとして選択します。
4. プライマリAPは、WANリンク経由 (通常はCAPWAP経由) でWLCからイメージをダウン

ロードします。

5. プライマリAPにイメージが割り当てられると、同じサイトタグ内の下位APは、ローカルネットワーク経由でTFTPを使用してプライマリAPからイメージをダウンロードします。
6. 最大3つの下位APがプライマリAPから同時にダウンロードできます。
7. ダウンロード後、APは新しいイメージを実行するためにリロードします。

利点

- プライマリAPのみがWAN経由でイメージをダウンロードするようにすることで、WANの帯域幅使用量を削減します。
- 下位のAPへのイメージ配信に、より高速なローカルネットワークリンク（TFTP経由）を利用します。

設定(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
```

検証(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

制限事項/考慮事項

- サイトタグを使用して参加するAPは、効率的なローカルTFTP転送のために物理的に同じ場所に配置する必要があります。
- リスナーサービスにTCPポート8443を使用します (クライアントデバッグバンドルやClean Airファイルなどの他の機能にも使用されます)。 このポートは、機能が無効になっても開いたままになります。
- WLCがインストールモードである必要があります。

アウトオブバンドHTTPsベースのAPイメージのダウンロード

OOB HTTPsベースAPイメージのダウンロードは、標準のCAPWAP制御パスの外部にイメージを転送することによってAPイメージのアップグレードパフォーマンスを向上させるために、Cisco IOS® XE Dublin 17.11.1で導入された拡張方式です。

OOB HTTPs方式では、標準TCPとHTTPを使用してイメージを転送します。CAPWAP制御チャネルのstop-and-waitメカニズムとは異なり、TCPでは本質的にスライディングウィンドウメカニズムが使用され、高遅延リンク上での効率的なバルクデータ転送が可能になります。

この方式では、コントローラ上で実行されているWebサーバ(nginx)を使用して、HTTP経由でAPにAPイメージを直接提供します。これにより、大容量ファイルの転送に関するCAPWAP制御パスの制限が回避され、より高速で柔軟なダウンロードメカニズムが提供されます。

使用例

この方法は、APイメージのアップグレードを高速化する場合に有効です。特に、CAPWAP制御トンネルの遅延と帯域幅の制限により、従来のインバンドダウンロードに時間がかかる可能性がある、大規模な展開やリモートサイトで有効です。

プロセスの概要

1. 新しいAPイメージがWLCでステージングされます。
2. OOB HTTPsアップグレード方式は、コントローラで有効にされ、設定されます。
3. APは、OOB方式をサポートする場合、設定されたポート上のHTTPを介して、コントローラ上のnginx Webサーバから必要なイメージをダウンロードしようとします。
4. HTTPのダウンロードが成功すると、APではアップグレードプロセスが続行されます。
5. HTTPのダウンロードが失敗すると、APは自動的に標準のインバンドCAPWAPダウンロード方式にフォールバックします。

パケットキャプチャは、WLCがHTTPsサーバとして機能し、APがHTTPsクライアントとして機能して、ポート8443経由の標準TCP接続とファイルのダウンロードを開始していることを示しています。

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ベースのイメージアップグレードパケットフロー

設定(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

設定(GUI)

1. Configuration > Wireless > Wireless Globalの順に移動します。
2. APイメージアップグレードセクションで、HTTPSメソッドを有効にします。
3. (オプション) HTTPS Portフィールドに値を入力します。
4. Apply to Deviceをクリックします。

検証(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

制限事項/考慮事項

- Cisco IOS® XEダブリン17.11.1以降が必要。
- Cisco Embedded Wireless ControllerまたはCisco Wave 1アクセスポイントではサポートされません。
- コントローラでグローバルHTTPS設定を有効にする必要があります。
- nginxサーバがコントローラ上で実行されている必要があります。
- 設定されたポートは、コントローラとAPの間に到達可能である必要があります。
- HTTPSサーバのトラストポイントにCA証明書のチェーンがある場合、アップグレードが失敗する可能性があります。
- Cisco IOS® XE 17.11.1より前のバージョンにダウングレードする前に、無効にする必要が

あります (APアップグレード方式httpsなし)。

- ポート443は予約済みです。他の標準ポートや既知のポートは使用しないでください。
- デフォルトポート8443の競合：コントローラのGUI HTTPSアクセスも8443を使用する場合、APファイル転送またはGUIアクセス用に別のポートを設定します。

TFTP/SFTPによる個々のAPの手動アップグレード

この方法では、コンソールまたはSSH経由でAP CLIに直接アクセスし、TFTPまたはSFTPサーバからイメージのダウンロードを開始します。これは、特定のAPのトラブルシューティング、現在コントローラに加入していないAPのアップグレード、またはTACが提供するデバッグイメージのロードに役立ちます。

APイメージを検索します。

このプロセスは、実際にはAPイメージをAPに直接ロードします。WLCベースのアップグレードの場合、WLCはWLCイメージバンドルからAPに適したイメージを選択します。ここでは、手動で選択する必要があります。

APイメージのバージョンでは、WLCイメージの命名規則とは異なる命名規則が使用されます。

Cisco Catalyst 9800シリーズWireless Controllerソフトウェアリリースのリンクサポート対象アクセスポイントに移動します

[Cisco Catalyst 9800シリーズワイヤレスコントローラソフトウェアリリースでサポートされているアクセスポイント](#)

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

ワイヤレスAPの互換性マトリクス

最初の列では、9800 WLCのCCOイメージについて説明します。3列目には対応するイメージバージョンが、4列目にはそのバージョンでサポートされるアクセスポイントが表示されます。バージョン17.17.1のAP 9130にAPイメージをインストールする必要があると仮定します。表を確認すると、APイメージ名が15.3であることがわかります。(3)JPVおよび9130はサポート対象モデルとしてリストされています。

次の手順では、software.cisco.comに移動し、APダウンロードフォルダからイメージを取得します。

Downloads Home / Wireless / Access Points Catalyst 9130AXシリーズアクセスポイント / Catalyst 9130AXIアクセスポイント / Lightweight APソフトウェア – 17.17.1(ED)

[ソフトウェアダウンロード – Catalyst 9130AXIアクセスポイント](#)

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イメージロケーション



警告：ダウンロードパスは、APモデルとAPイメージのバージョンによって異なります。

プロセスの概要

1. アクセス可能なTFTPまたはSFTPサーバにターゲットAPイメージファイルをステージングします。
2. APのCLI (コンソールまたはSSH) にアクセスします。
3. archive download-swコマンドを実行して、サーバとイメージファイルのパスを指定します。
4. APがイメージをダウンロードします。
5. ダウンロードが完了したら、CAPWAPプロセスを再起動するか、APをリロードして新しいイメージを有効にします。

設定(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:

検証

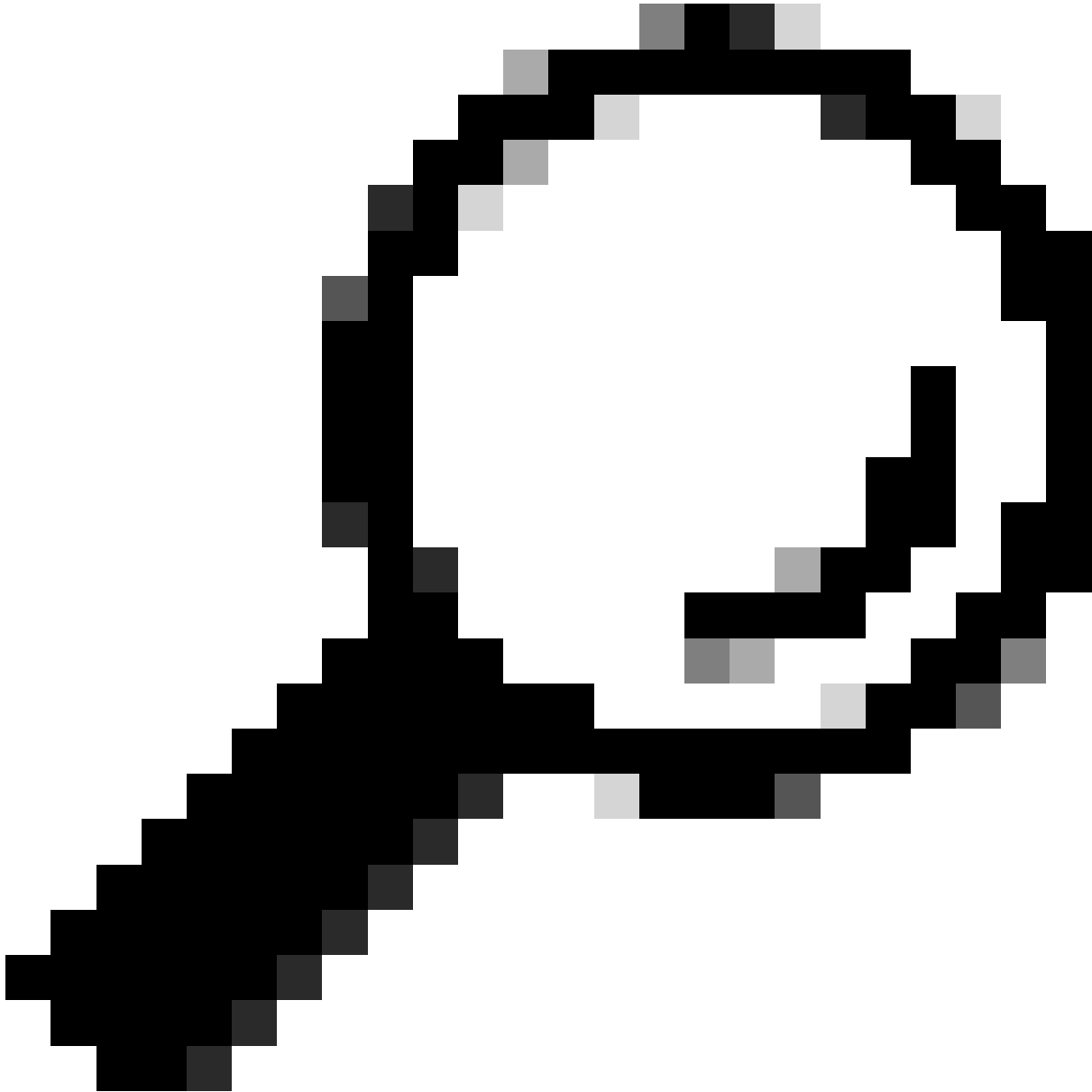
- TFTP/SFTPサーバのログを監視して、ダウンロードを確認します。
- APコンソールで、ダウンロードの進行状況と完了を確認します。
- 再起動/リロード後、AP CLIまたはWLCで新しいイメージのバージョンを確認します。

制限事項/考慮事項

- 各APへの直接CLIアクセスが必要。
- 多数のAPを個別にアップグレードする拡張性がない (スクリプトはオプション) 。
- TFTPのパフォーマンスは遅延の影響を受けやすい。SFTP (TCPを使用) は高遅延パスよりもパフォーマンスが高いが、インタラクティブ認証 (ユーザ名/パスワード) が必要。
- /no-reloadoptionを指定すると、ダウンロード直後のAPのリロードが防止され、再起動/リロ

ードタイミングを手動で制御できます。

- APをAireOSから9800に移行する場合、9800に参加する前に、修正を含む特定のAireOSバージョン (8.10.190.0以降) にAPをアップグレードすることをお勧めします。



ヒント:WLAN Pollerは、複数のAPを手動でアップグレードするスクリプトを作成するために使用できるツールです。この場所でWLANポーラーを見つけます。[WLANポーラー](#)

使用する方式

- 高遅延リンク上のOEAPまたはテレワーカーAPの場合：
CAPWAPイメージダウンロード時間機能拡張を有効にします。これは、スライディングウィンドウを使用してCAPWAPフレームワーク内の遅延の問題に直接対処することで、これらの導入タイプのCAPWAPパフォーマンスを向上させることを目的としています。

- WAN帯域幅が制限されたブランチオフィスのFlexConnect APの場合：
FlexConnectモードで効率的なイメージアップグレードを利用します。この方法は、TFTP経由でローカル配信にプライマリAPを使用して内部ネットワークの速度を高速化することでWANの負荷を大幅に軽減するため、強く推奨されます。
- ローカルモードAP（または、前述の方式が適用されないか十分でない場合はFlexConnect/OEAP）の場合、サポートされているプラットフォーム(Cisco IOS® XE 17.11.1+)で次の手順を実行します。
アウトオブバンドHTTPsベースのAPイメージのダウンロードを検討してください。この方式では、バルク転送にTCP/HTTPを使用します。これは、標準のCAPWAPよりも高遅延リンク上で効率的です。また、OOB転送が失敗した場合の標準CAPWAPへのフォールバックも提供します。
- 単一APのトラブルシューティング、WLCに加入していないAPのアップグレード、または緊急時のシナリオ：
TFTP/SFTP経由で個々のAPの手動アップグレードを実行する。これにより、特定のデバイスのアップグレードプロセスを直接制御できますが、自動化されていない大規模な導入には実用的ではありません。SFTPはTCPを使用するため、高遅延パスよりもパフォーマンスが優れているため、一般にTFTPよりもSFTPの方が優先されます。
- 標準のCAPWAPアップグレード：デフォルトの方法ですが、一般的には、高遅延WANリンク経由でリモートAPをアップグレードするための主要な方法としてはお勧めできません。これは、以前のリリースでは転送が遅くなり、信頼性の問題が発生する可能性があるという、停止して待機するメカニズムが備わっていることが原因です。リモートサイトについては、可能な限り次に示す最適化された方法を使用してください。

APの動作モード、ネットワークの状態、WLCソフトウェアのバージョン、およびアップグレード操作の規模に最も適した方法を選択して、リモートAPの円滑かつ効率的なプロセスを保証します。

結論

標準のCAPWAPイメージのダウンロード方式はローカルネットワークに適していますが、WANリンク経由のリモートAP展開では、最適化されたアップグレード技術により大きなメリットが得られます。高遅延に対する標準CAPWAPの制限を理解することは、適切なアプローチの選択に役立ちます。CAPWAPイメージダウンロード時間機能拡張は、OEAP/テレワーカーAPのパフォーマンスを向上させ、効率的なイメージアップグレードは、WANの負荷を軽減することでFlexConnectの導入を最適化し、アウトオブバンドHTTPは、サポートされているプラットフォーム向けにより高速な代替を提供します。手動のTFTP/SFTP方式は、トラブルシューティングや特定のシナリオに役立つツールです。

参考資料

[効率的なイメージアップグレード](#)

[アウトオブバンドAPイメージのダウンロード](#)

[APイメージのダウンロード時間の改善 \(OEAPまたはテレワーカーのみ\)](#)

[Cisco Wireless Controllerプラットフォームソフトウェアリリースでサポートされているシスコ
アクセスポイント](#)

[WLANポーラー](#)

[AireOS WLCからWLANPollerを使用したCatalyst 9800への移行](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。