

High Availability Using Patching and Rolling AP Upgrade on Cisco Catalyst 9800 Series Wireless Controllers



Contents

Overview.....	3
Platform support.....	3
Supported releases.....	3
Controller patching using Software Maintenance Updates (SMU).....	4
AP patching using an AP service pack.....	5
Rolling AP update infrastructure.....	5
Per-site AP service pack rollout.....	6
Per-AP-model service pack rollout.....	6
WebUI configuration.....	7
Upgrade and downgrade scenarios with APSP.....	11
CLI reference.....	13
N+1 rolling AP image upgrade.....	15
New AP model support using AP device pack.....	19
Upgrade and downgrade scenarios with APDP.....	21
WebUI configuration.....	22
CLI reference.....	24
Summary.....	24

Overview

Designing for high availability isn't limited to anticipating box failures and network events. It is also about providing high availability through the entire lifecycle of a deployment. A significant part of this lifecycle is the need for updates and upgrades on the network. This is where the power of Cisco IOS® XE comes in. Wireless controllers (WLCs) running Cisco IOS XE can now leverage capabilities that allow for timely fixes and updates to be made to the network. This helps contain the impact within an already released image, without the need to requalify a new release, and helps with faster resolution of critical, time-sensitive issues by providing fixes in a timely manner.

Cisco IOS XE Release 16.10 and later is infrastructure-ready to support the following features:

The diagram illustrates three key features supported by Cisco IOS XE Release 16.10 and later, each with a corresponding icon and a star icon indicating a new or enhanced feature.

- Controller updates:** Represented by a gear and circular arrows icon. Below the icon is the text "Controller updates", "Controller update or bug fixes", and a button labeled "SMU" with a star icon.
- PSIRTs, fixes on APs:** Represented by a red shield icon. Below the icon is the text "PSIRTs, fixes on APs", "AP update or bug fixes", and a button labeled "AP service pack" with a star icon.
- New AP model support:** Represented by four colored squares (green, blue, green, green) icon. Below the icon is the text "New AP model support", "Hot-patchable support for device pack", and a button labeled "AP device pack" with a star icon.

1. Controller fixes and updates using Software Maintenance Updates (SMUs)
 - Access Point (AP) fixes and updates using an AP Service Pack (APSP)
 - Support for new AP models using an AP Device Pack (APDP)

Platform support

Cisco® Catalyst® wireless platforms 9800-40, 9800-80, and 9800-CL.

802.11ac Wave 1 and Wave 2 access points: Cisco Aironet® 2802, 3802, 4800, and the 1800 1540, 1560, 1700, 2700, 3700, and 1570 Series.

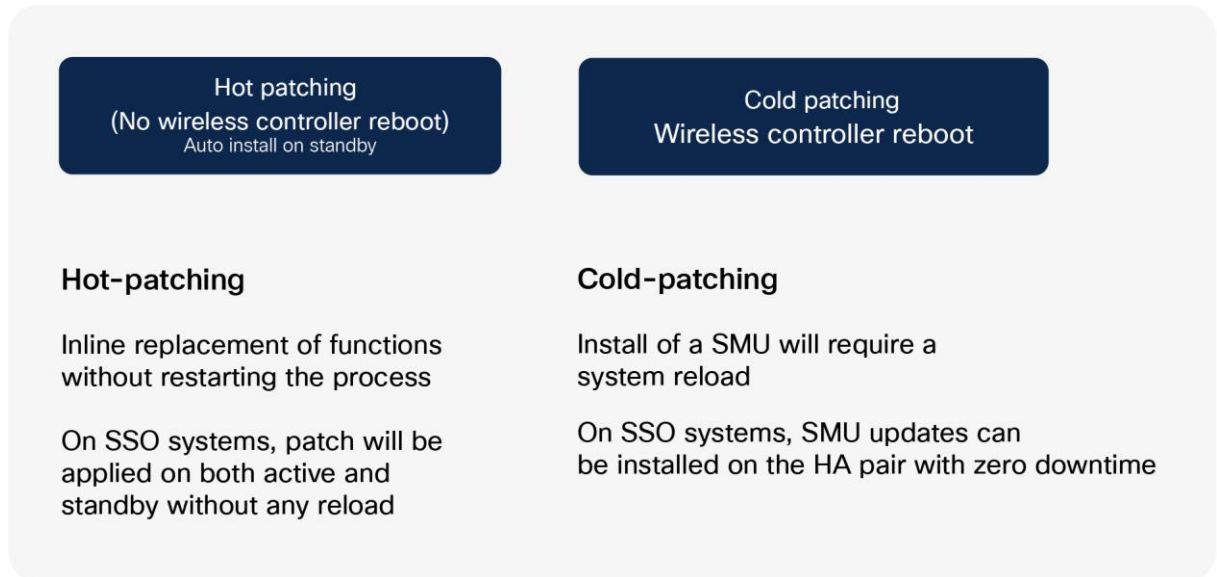
Supported releases

Cisco IOS XE Release 16.10 and later.

Controller patching using Software Maintenance Updates (SMU)

An SMU is a package that can be installed on a system to provide a patch fix or security resolution to an already released image. An SMU package is provided on a per-release and per-component basis and is specific to the platform.

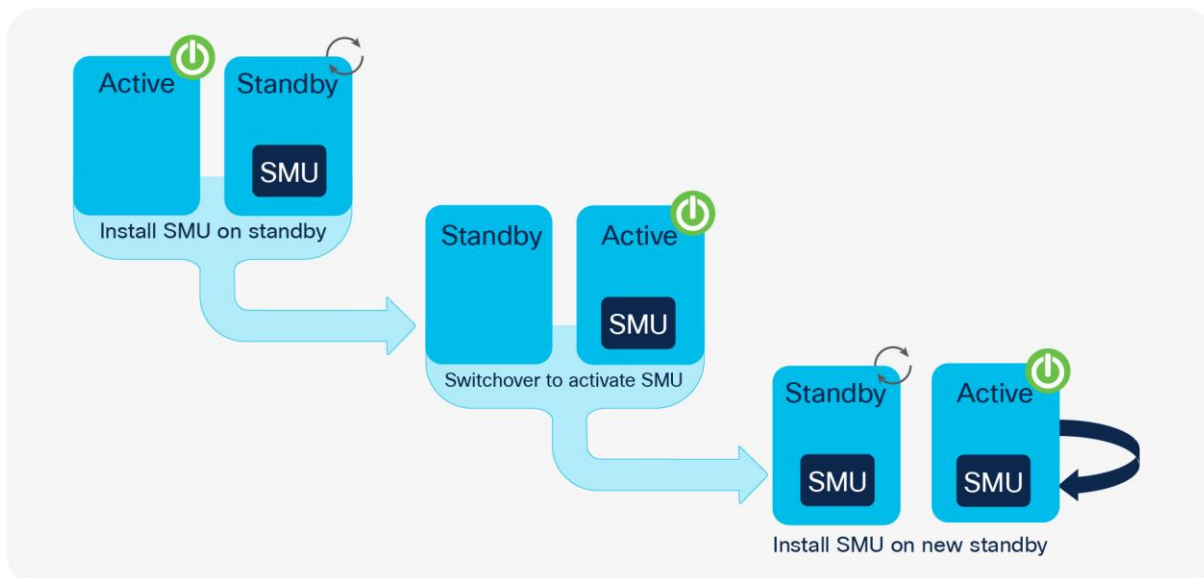
There are two types of SMUs – those that can be hot-patched and those that can only be cold-patched.



A hot patch does not need a system reload, which means the clients and APs will not be affected. When the controller is part of an HA pair, the SMU activation applies to both the active and hot-standby controllers.

A cold patch, on the other hand, requires a reload. However, since we are looking for a seamless, zero-downtime update, a Stateful Switchover (SSO) pair can be used to install a cold patch without bringing the network down. Figure 1 shows the process of installing a cold patch on an SSO pair.

Figure 1. Active-standby cold-patch activation



The system will install the SMU on the standby controller and reload the standby. The network is still running because the APs and clients are on the active controller. Once the standby is up, a switchover occurs, pushing all AP and client sessions to the new active controller (formerly the standby). At this point the SMU is installed on the new standby (which was the old active controller). Both controllers have now been updated with the SMU.

Note: SMUs are released only on long-lived MD releases, which means controller SMUs will be available starting with the first MD release, 16.12.

AP patching using an AP service pack

Rolling AP update infrastructure

The Cisco Catalyst 9800 Series supports rolling out critical AP bug fixes using an AP Service Pack (APSP). When APs need to be upgraded to the new image, the 9800 Series supports doing this in a staggered fashion, such that an appropriate number of APs are always up and running in the network and providing RF coverage to clients. This is referred to as a rolling AP upgrade.

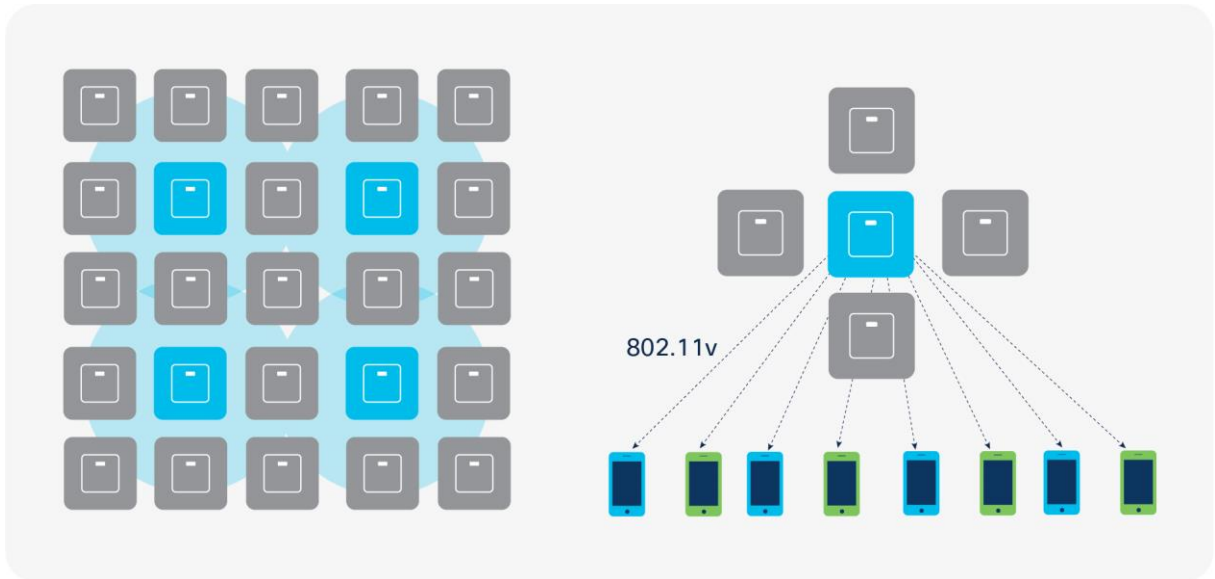
The AP service pack, which is for AP-specific fixes, will be independent of the SMU timeline and will be available on non-MD releases as well after Release 16.10.

Three main highlights to this feature are:

- Rolling updates are supported natively on the wireless controller using the UI or Command-Line Interface (CLI).
- Rolling updates support automatic candidate selection using the Radio Resource Management (RRM)-based AP neighbor information. The device auto-selects the candidate APs to be upgraded in each iteration based on a chosen percentage per iteration (5%, 15%, or 25%, with the default being 15%) and RRM AP neighbor information.

- Clients from candidate APs are actively steered away using 802.11v packets with the “dissociation imminent” field set to help ensure seamless network connectivity as APs are being upgraded. If clients do not honor this setting, they will be deauthenticated before AP reload.

Figure 2. Candidate AP selection and client steering



Release 16.11 provides the ability to apply an AP fix on a per-site and per-AP-model basis, which means that a pack can be selectively applied to a particular site and specific AP models that are affected by the fix.

Per-site AP service pack rollout

At the time of AP service pack activation, the user selects the sites where the AP service pack should be rolled out. All APs on these sites will be updated with the designated service pack, including any new APs that join the site after the filter is applied. This allows the user to control the propagation of a service pack in the network.

It should be noted that this enhancement allows for activating service packs on sites incrementally but requires that all sites be brought to the same service pack level before a new service pack can be rolled out to a subset of sites.

Per-AP-model service pack rollout

An AP service pack can also be built with a subset of AP images. These enable a predownload only to the affected AP models. Similarly, these service packs are activated only on the AP models affected, in conjunction with any site-based filters, as mentioned earlier.

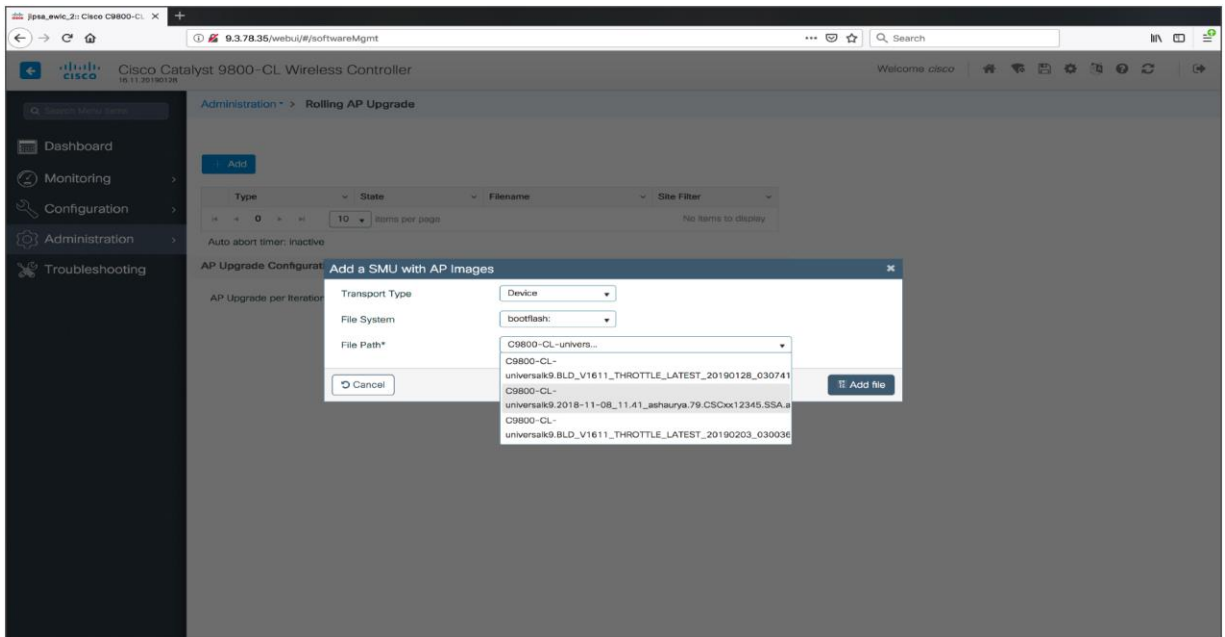
Again, it should be noted that if, for example, three model images were included in an APSP, all future APSPs in that release for any of these three AP images will contain all three of them. This helps subsequent service packs to supersede older ones.

These two capabilities work in conjunction with each other, meaning that you can select specific sites in a campus and then apply the fix to specific AP models within those sites, as designated by the service pack. This enables controlled propagation of the fix with minimal or no service disruption because the fix is predownloaded and rolled out only to affected AP models.

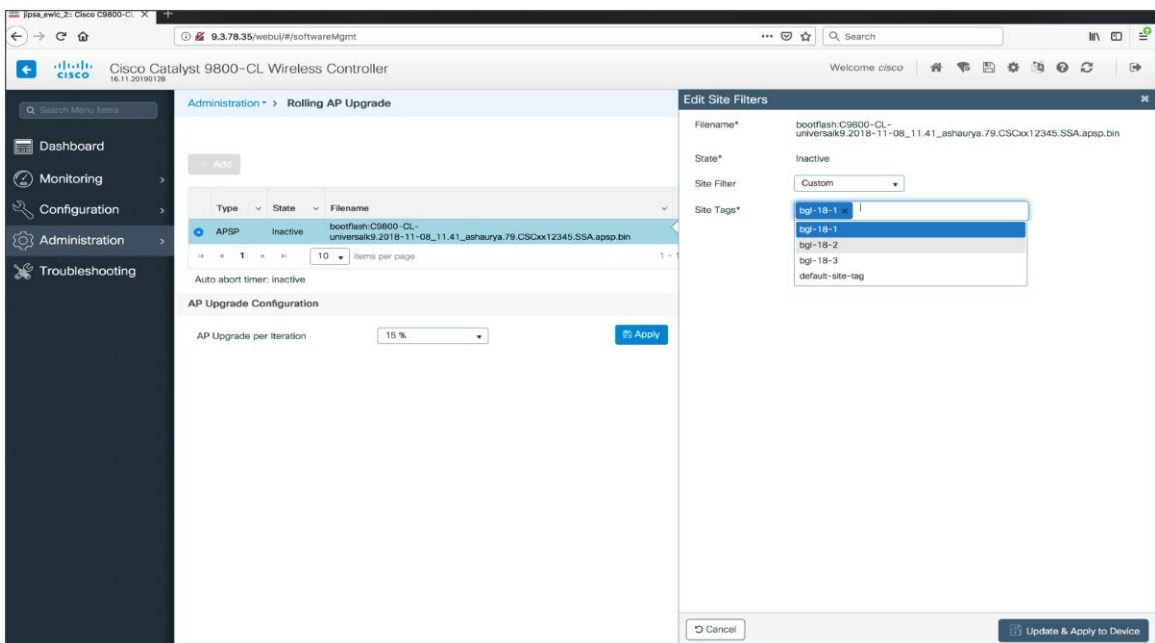
WebUI configuration

An AP service pack can be applied using a simple workflow on the controller UI. The steps that follow describe this process:

Step 1. Add the AP service pack under Administration > Rolling AP Upgrade.



Step 2. Select the site filters (optional) and AP upgrade per iteration percentage (the default is 15%). Click Update and Apply to Device.



Step 3. Monitor the progress under AP Predownload Statistics and AP Upgrade Statistics until the status of all APs is “Upgraded.”

There is an AP upgrade operation in progress. Please wait till it completes...

AP Upgrade Configuration

AP Upgrade per Iteration: 15%

AP Upgrade Statistics

Status: In Progress Percentage Complete: 0

Upgraded: 0 In Progress: 1 Remaining: 0

AP Predownload Statistics

Total number of APs: 2

Number of APs

- Initiated: 0
- Predownloading: 0
- Completed: 1
- Not Supported: 0
- Failed to Predownload: 0

AP Upgrade Configuration

AP Upgrade per Iteration: 15%

AP Upgrade Statistics

Status: In Progress Percentage Complete: 0

Upgraded: 0 In Progress: 1 Remaining: 0

AP Predownload Statistics

Total number of APs: 2

Number of APs

- Initiated: 0
- Predownloading: 0
- Completed: 1
- Not Supported: 0
- Failed to Predownload: 0

Site filters can be edited or cleared in order to propagate the AP service pack to other sites or all sites using the “All Sites” option, as shown below.

AP Upgrade Configuration

AP Upgrade per Iteration: 15%

AP Upgrade Statistics

Status: Complete Percentage Complete: 100

Upgraded: 1 In Progress: 0 Remaining: 0

AP Predownload Statistics

Total number of APs: 2

Number of APs

- Initiated: 0
- Predownloading: 0
- Completed: 1
- Not Supported: 0
- Failed to Predownload: 0

Edit Site Filters

Filename* bootflash:C9800-CL-universalk9.2018-11-08_11.41_ashaurya.79.CSCxx12345.SSA.apsp.bin

State* Activated and Uncommitted

Site Filter All Sites

Step 4. Commit the AP service pack by clicking the Commit button.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The main content area is titled "Administration > Rolling AP Upgrade". At the top, there are buttons for "+ Add" and "Commit". Below this is a table with columns for Type, State, Filename, and Site Filter. The table contains one entry: an APSP with State "Activated and Uncommitted" and Filename "bootflash:C9800-CL-universalk9.2018-11-08_11.41_ashaurya.79.CSCxx12345.SSA.apsp.bin". Below the table, there is an "AP Upgrade Configuration" section with a dropdown for "AP Upgrade per Iteration" set to "15%" and an "Apply" button. The "AP Upgrade Statistics" section shows "Status: Complete", "Percentage Complete: 100", "Upgraded: 1", "In Progress: 0", and "Remaining: 0". A table below lists the upgraded AP: "jpsa_2800L_2" with Ethernet MAC "70db.984e.2a40" and Status "Upgraded". On the right side, a terminal window displays the following log output:

```

Initiating INSTALL_PREPARE operation for activate
install_prepare: START Mon Feb 4 19:39:49 IST 2019
Prepare activate invoked with filename bootflash:C9800-CL-universalk9.2018-11-08_11.41_ashaurya.79.CSCxx12345.SSA.apsp.bin
Executing pre scripts....
install_prepare: Starting
Executing pre scripts done.
SUCCESS: install_prepare /bootflash/C9800-CL-universalk9.2018-11-08_11.41_ashaurya.79.CSCxx12345.SSA.apsp.bin Mon Feb 4 19:40:12 IST 2019
Initiating INSTALL_ACTIVATE operation for SMU file C9800-CL-universalk9.2018-11-08_11.41_ashaurya.79.CSCxx12345.SSA.apsp.bin
install_activate: START Mon Feb 4 19:40:58 IST 2019
install_activate: Activating SMU
Executing pre scripts....
Executing pre scripts done.
--- Starting SMU Activate operation ---
Performing SMU_ACTIVATE on all members
[1] SMU_ACTIVATE package(s) on chassis 1
[1] Finished SMU_ACTIVATE on chassis 1
Checking status of SMU_ACTIVATE on [1]
SMU_ACTIVATE: Passed on [1]
Finished SMU Activate operation

Executing post scripts....
Executing post scripts done.
Executing post scripts....
Executing post scripts done.
SUCCESS: install_activate /bootflash/C9800-CL-universalk9.2018-11-08_11.41_ashaurya.79.CSCxx12345.SSA.apsp.bin Mon Feb 4 19:41:35 IST 2019
  
```

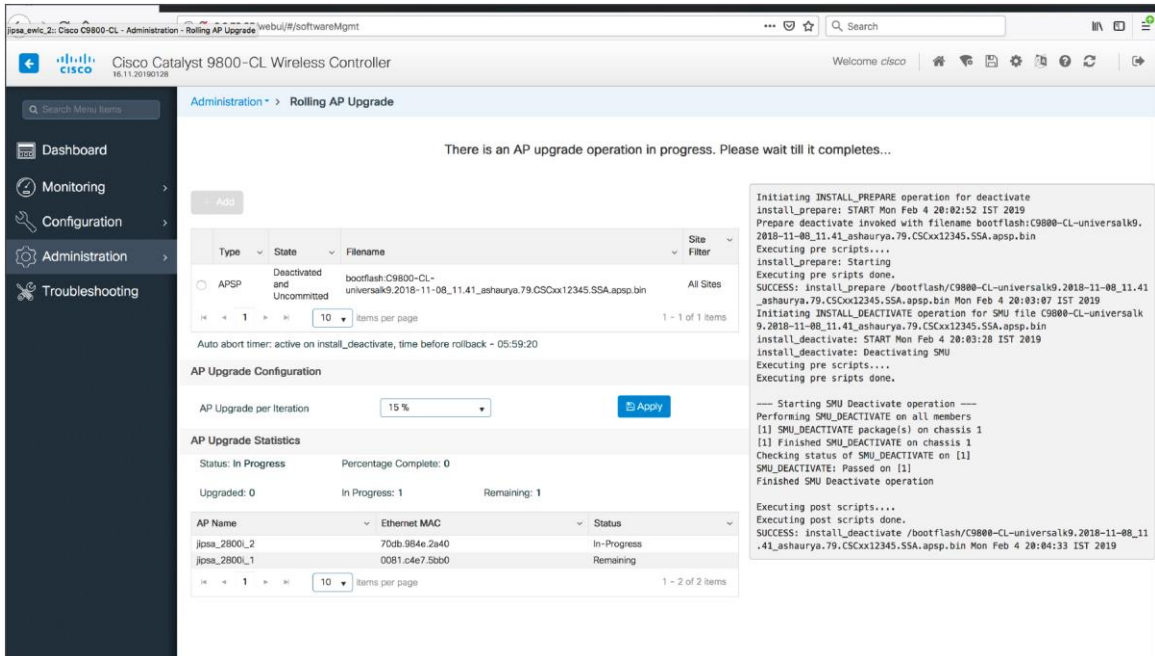
The AP service pack can be deactivated using the “Deactivate” option, which will deactivate the AP service pack from all sites where it was installed.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The main content area is titled "Administration > Rolling AP Upgrade". At the top, there are buttons for "+ Add" and "Deactivate". Below this is a table with columns for Type, State, Filename, and Site Filter. The table contains one entry: an APSP with State "Activated and Committed" and Filename "bootflash:C9800-CL-universalk9.2018-11-08_11.41_ashaurya.79.CSCxx12345.SSA.apsp.bin". Below the table, there is an "AP Upgrade Configuration" section with a dropdown for "AP Upgrade per Iteration" set to "15%" and an "Apply" button. The "AP Upgrade Statistics" section shows "Status: Complete", "Percentage Complete: 100", "Upgraded: 1", "In Progress: 0", and "Remaining: 0". A table below lists the upgraded AP: "jpsa_2800L_2" with Ethernet MAC "70db.984e.2a40" and Status "Upgraded". On the right side, a terminal window displays the following log output:

```

INSTALL_COMMIT OPERATION:
Initiating INSTALL_COMMIT operation
install_commit: START Mon Feb 4 19:59:37 IST 2019
install_commit: Committing SMU
Executing pre scripts....
install_commit:
Executing pre scripts done.
--- Starting SMU Commit operation ---
Performing SMU_COMMIT on all members
[1] Finished SMU_COMMIT package(s) on chassis 1
[1] Finished SMU_COMMIT on chassis 1
Checking status of SMU_COMMIT on [1]
SMU_COMMIT: Passed on [1]
Finished SMU Commit operation

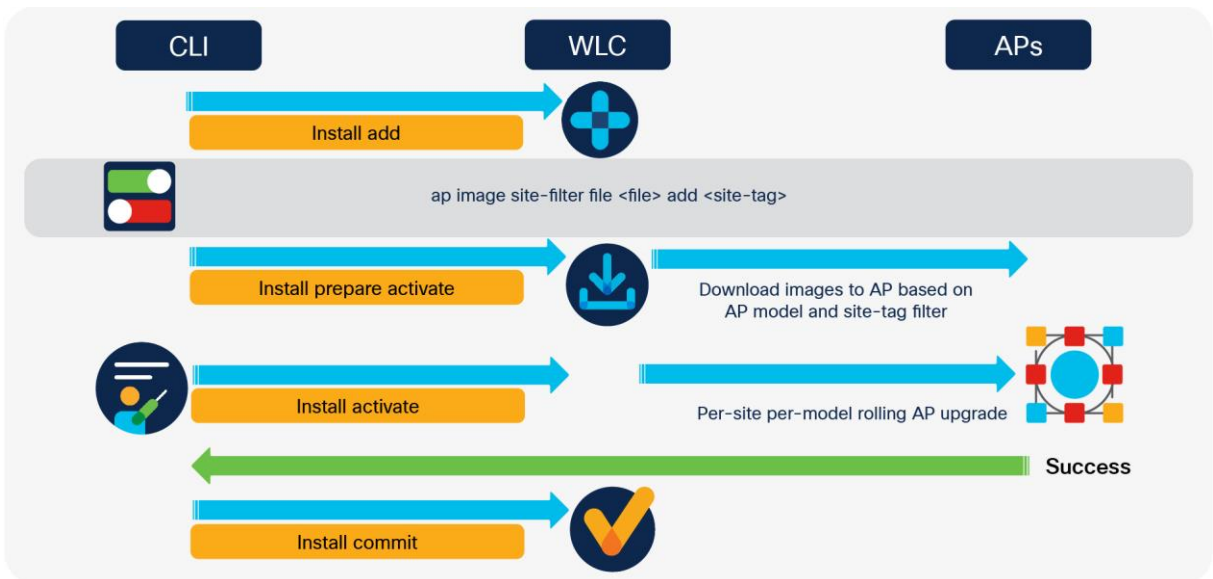
SUCCESS: install_commit /bootflash/C9800-CL-universalk9.2018-11-08_11.41_ashaurya.79.CSCxx12345.SSA.apsp.bin Mon Feb 4 19:59:58 IST 2019
  
```



The back-end/CLI workflow of successful APSP activation is shown below:

- Install add
- Install prepare activate
- Install activate
- Install commit

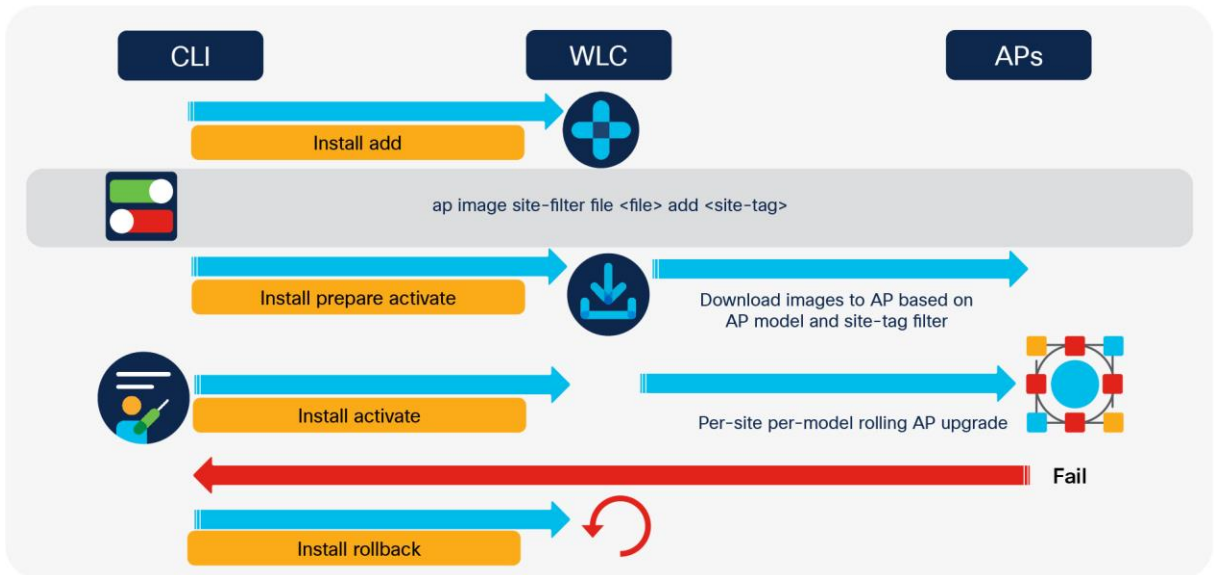
Figure 3. APSP successful installation workflow



In case of a failure, the service pack can be rolled back and the system will return to the last stable checkpoint:

- Install add
- Install prepare activate
- Install activate
- Install rollback

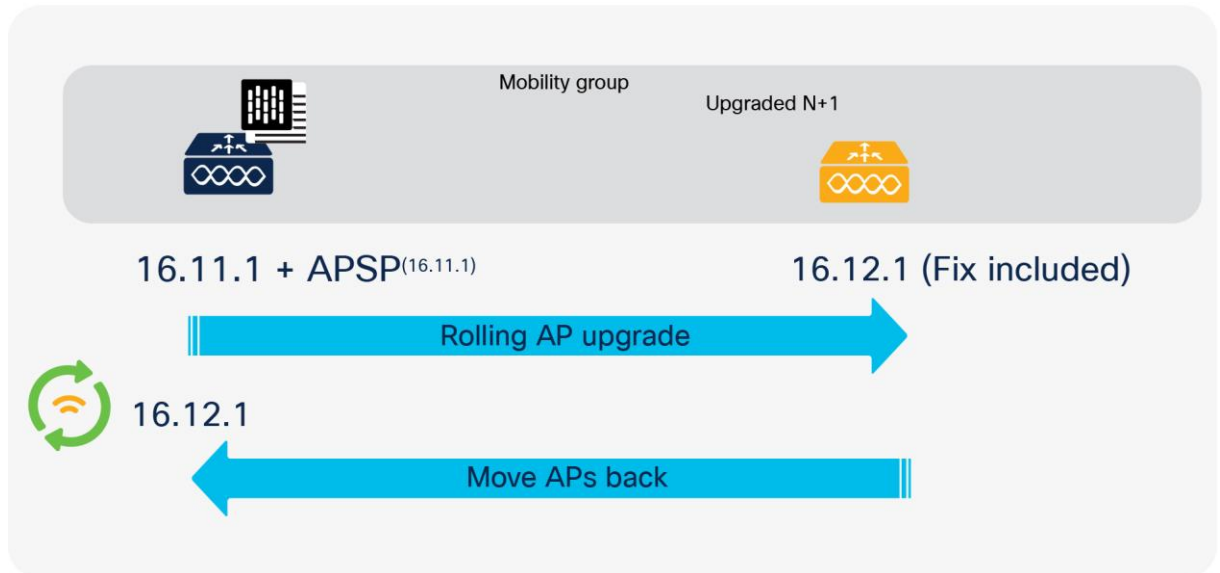
Figure 4. APSP installation failure workflow



Upgrade and downgrade scenarios with APSP

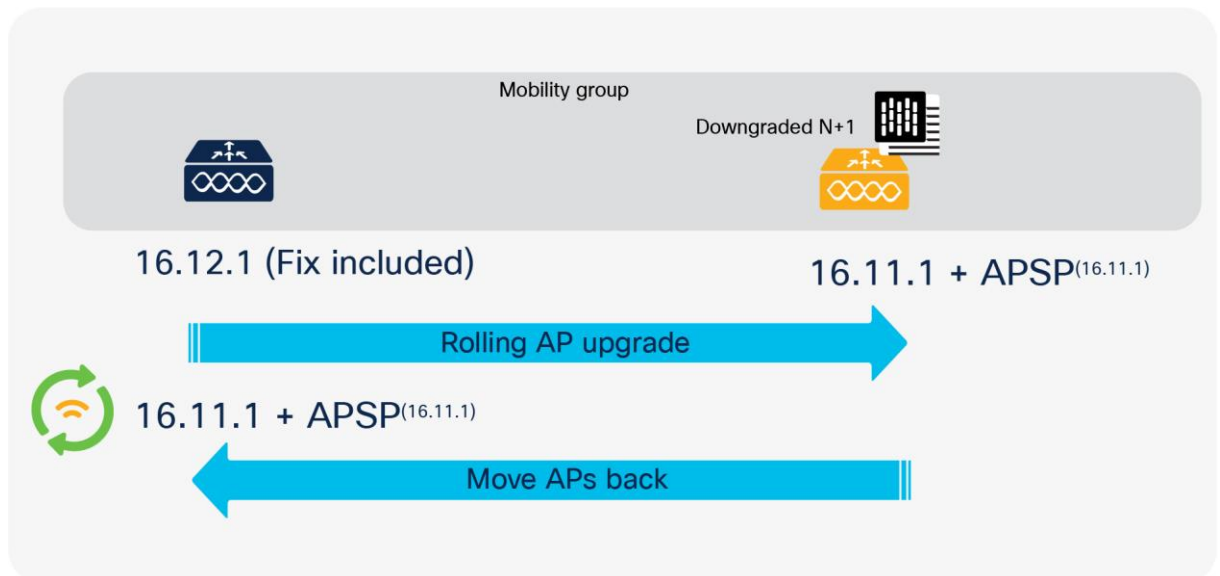
In an upgrade scenario, if upgrading to the next major or minor release, the fix should be integrated into the next release. The controller can be upgraded using the N+1 rolling upgrade process described in the next section. The target image is loaded on the N+1 controller, the APs are rolled over, the primary controller is upgraded, and the APs are rolled back. There is no service disruption, since an N+1 rolling AP upgrade is used.

Figure 5. Upgrade scenario with APSP



In the case of a downgrade, the N+1 controller is installed with the target downgrade image and the corresponding APSP. The APs are rolled over back to the N+1 controller, and the primary controller is reloaded with the downgraded image and the corresponding APSP. Any new APs that join part of the site where the fix is applicable will have the APSP pushed to them at the time of AP join, if they are the same model as the installed APSP.

Figure 6. Downgrade scenario with APSP



CLI reference

Activating an AP service pack

1. `install add file <file>`
Populates the predownload directory, persistent.
2. `ap image site-filter file <file> add <site-tag>`
Can be entered multiple times to set up a multisite filter.
3. `ap image site-filter file <file> remove <site-tag>`
Can be entered to remove a site filter.
4. `install activate prepare file <file>`
Does a predownload to some or all sites based on the filter.
5. `install activate file <file>`
Does a rolling AP upgrade to some or all sites based on the filter.
6. `install commit`

Adding a site filter

`ap image site-filter file <file> add <site-tag>`

Can be entered multiple times to set up a multisite filter.

`ap image site-filter file <file> apply`

Does a predownload and rolling AP upgrade to added sites based on the filter.

Removing a site filter

1. `ap image site-filter file <file> clear`

Does a predownload and rolling AP upgrade to all sites where it's not active.

Deactivating an AP service pack

1. `install deactivate prepare file <file>`
Informs wireless about imminent deactivation; wireless does a predownload to affected APs.
2. `install deactivate file <file>`
Does a rolling AP upgrade based on which AP models were present in the above file.

Please note that during deactivation if no APs in any sites are currently running the AP images from the APSP being deactivated, the above steps will be no-op in terms of predownload and rolling AP upgrade. Internal tables will be updated to remove that APSP.

Rolling back an AP service pack

1. install rollback to rollback_id1 prepare
Informs wireless about imminent rollback; wireless does a predownload to affected APs.
2. install rollback to rollback_id1
Does a rolling AP upgrade for all sites, based on which AP models are affected.

Please note that if some AP models were on the base image or a point before the rollback point, they will not be affected by the rollback.

Aborting activation of an AP service pack

1. install abort prepare
Informs wireless about an imminent abort; wireless does a predownload if needed.
2. install abort
If needed, does the abort by resetting APs in rolling fashion.

It is important to note here that “install abort prepare” must be followed up with an “install abort.”

If “install abort prepare” is called after “install deactivate file bootflash:abcd” was called but a rolling AP upgrade is still running, the rolling AP upgrade is stopped and the last upgrade report is marked as “abort prepped.” We know that the APs that completed the upgrade will need to be moved back to their last image when the “install abort” trigger comes, so these APs are asked to predownload the necessary image. The remaining APs are asked to predownload if their active image is not in the flash. This completes the “install abort prepare” handling. When the “install abort” trigger is received, we go through the report that was marked “abort prepped” and reset all the APs that were upgraded so that the abort is complete. After this, the user is free to enter any commands.

Show commands to verify functionality

show ap image site summary

```
c9800# show ap image site summary
```

```
Image name: apspl.bin
```

```
Site Tag           Prepared           Activated           Committed
```

```
-----  
BGL18              yes                ongoing             no  
BGL17              yes                ongoing             no
```

```
c9800#
```

```
show ap image file <APSP file name>
```

```
c9800# show ap image file apspl.bin
```

```
Image version: 16.10.1.25
```

```
AP image type: ap1g4, ap3g3
```

```
c9800#
```

The following show commands can be used to see the progress of a rolling AP upgrade:

```
show ap upgrade summary
show ap upgrade detailed <report-name>
```

N+1 rolling AP image upgrade

A zero-downtime network upgrade is a challenge for wireless networks. The reason is that these networks are made up of a set of interlocking devices, WLCs, and APs, which all need to be up to keep the network operational.

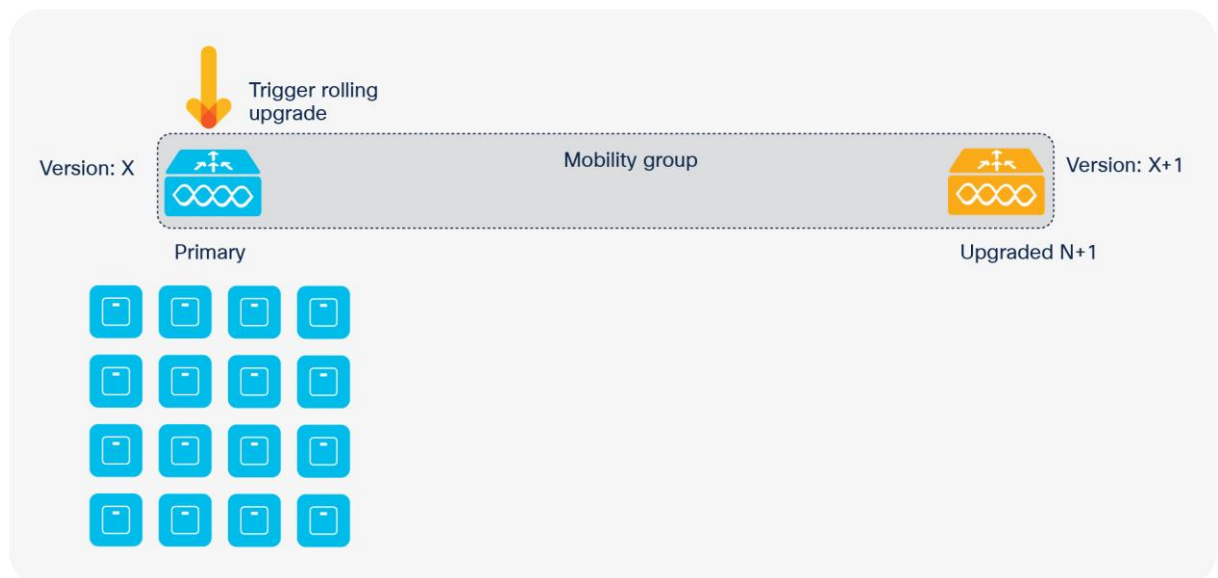
The advent of rolling AP upgrades opens up new possibilities for upgrading the controller code in a network using an N+1 controller, without bringing the network down. This can effectively achieve a zero-downtime network upgrade in an N+1 deployment.

The idea is to upgrade access points in a wireless network in a staggered manner, using the same rolling AP update infrastructure described earlier, such that an appropriate number of APs are always up and running in the network and providing RF coverage to clients.

The solution for an N+1 network upgrade using a rolling AP upgrade takes the form of three primitives that the administrator can use to achieve a zero-downtime upgrade. Orchestration and visualization capabilities are available on the wireless controller and will be available in Cisco DNA Center as well. The following steps describe the workflow for this solution.

1. The target version is installed on WLC2, and WLC2 is added to the same mobility group as WLC1. The target image is downloaded to WLC1, and associated APs are predownloaded with the image.

Figure 7. Image downloaded to primary WLC and AP predownloaded to APs



The user then triggers the exec command below, which moves all APs from a WLC (WLC1) to a mobility member (WLC2) whose identity (hostname and wireless management IP) is provided by the user.

ap image upgrade destination <WLC Name> <WLC IP>

This command will move APs to the specified destination WLC with a swap and reset command. It is assumed that the destination WLC is on the same version as the APs' backup image.

The device auto-selects the candidate APs to be upgraded in each iteration based on the chosen percentage of APs to be selected (5%, 15%, or 25%, with the default being 15%) and RRM AP neighbor information.

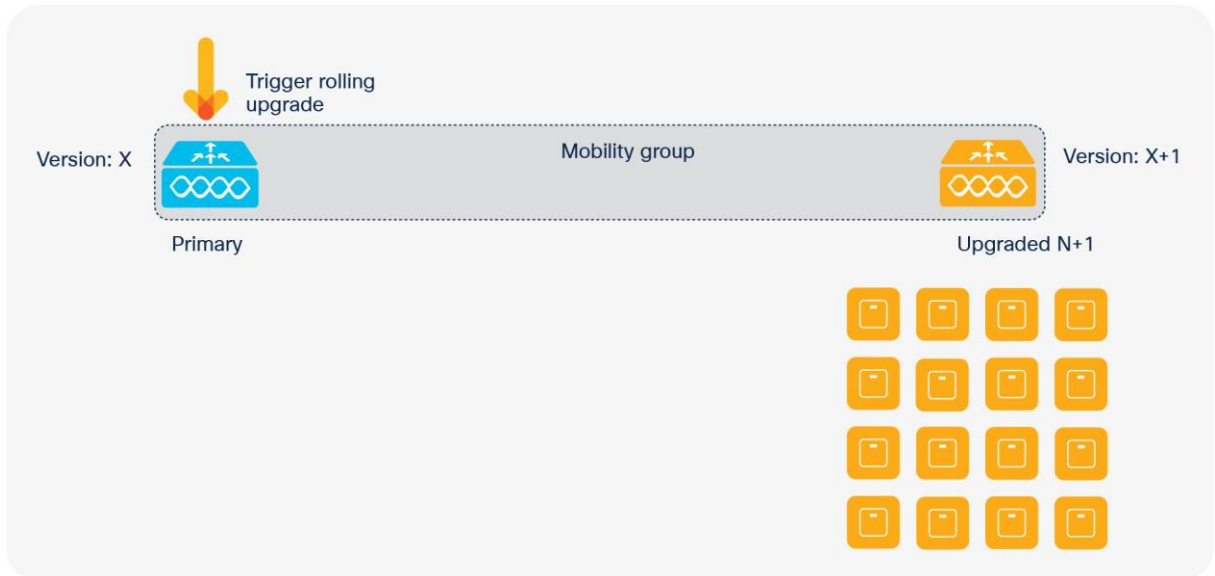
- For 25%, the expected number of iterations is about 5, and the upgrade will take about an hour.
- For 15%, the expected number of iterations is about 12, and the upgrade will take about two hours.
- For 5%, the expected number of some iterations is about 22, and the upgrade will take about four hours.

Figure 8. RRM-based candidate AP selection



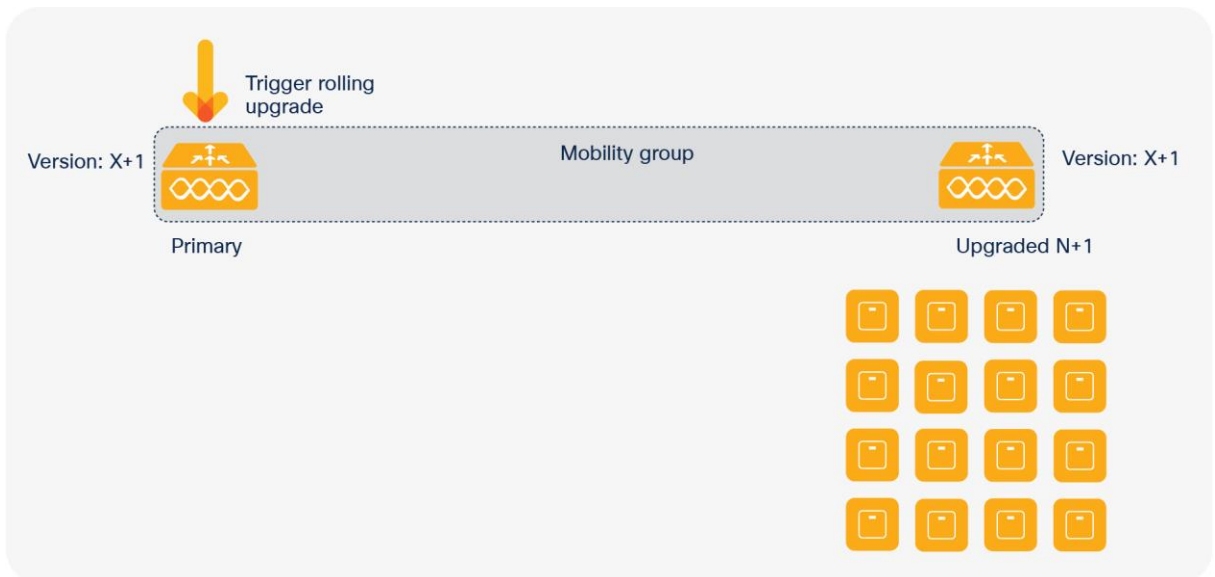
This exec command causes the APs to use WLC2 as their primary WLC. After this, the APs will be asked to swap and reset themselves using a rolling AP upgrade. As this AP upgrade happens, WLC2 will be informed about each iteration so that the upgrade report for this activity is available on both WLC1 and WLC2. The upgrade report created contains an indication that it is an AP move report and notes the source and destination.

Figure 9. Staggered rolling AP upgrade to N+1 WLC



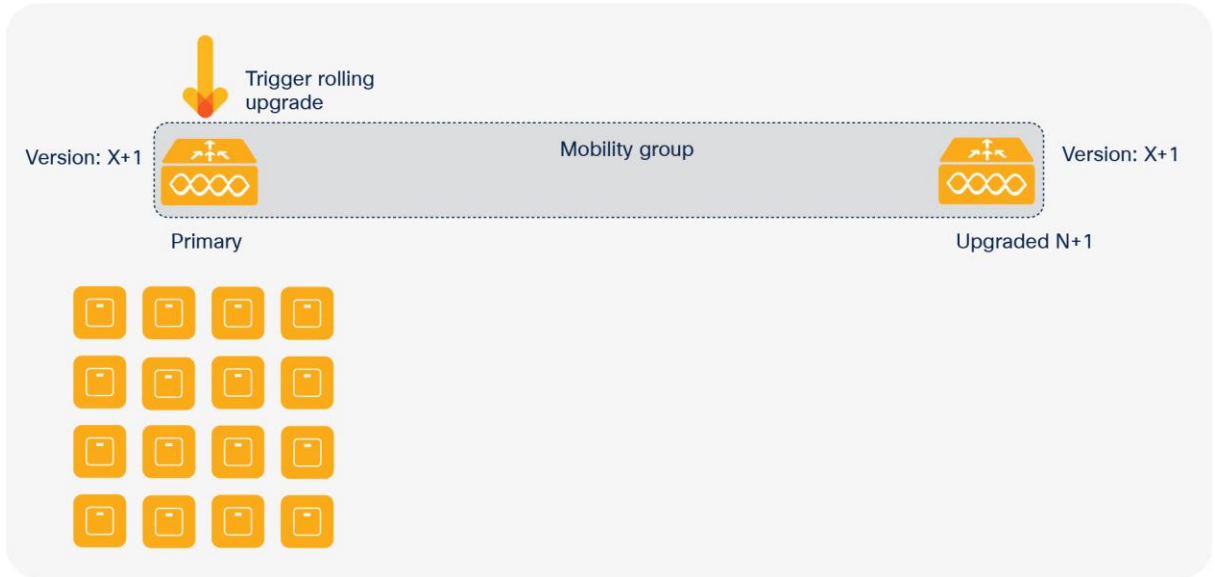
2. Once this move is complete, the image downloaded beforehand on WLC1 is activated with a reload to bring the WLC up with the new version.

Figure 10. Reload on primary WLC and upgrade to target image



3. After a reload of WLC1, once the mobility tunnel comes up, WLC2 will run a rolling AP upgrade to move the APs back to WLC1, using the same algorithm.

Figure 11. Optional fallback to primary WLC



The following command moves the APs contained in an upgrade report to another WLC without any version change. The command takes in a destination WLC identity (hostname and wireless management IP) and optionally a report name.

On this command trigger, if an upgrade report name was provided, we go to that report and go through the APs iteration by iteration. For each iteration we change the primary WLC to the provided WLC for APs in this iteration. If no upgrade report file name was provided, we run the rolling AP upgrade candidate selection process and come up with new iterations.

ap image move destination <WLC Name> <WLC IP> [<Upgrade Report Name>]

This command will move APs to the specified destination WLC without a swap and reset command. It is assumed that the destination WLC is on the same version as the current WLC.

Starting with Release 16.11, a single command sets the variables for the rolling AP upgrade. The user needs to trigger the “install activate” command manually to activate and reload WLC1 with the new image. After reload, the APs will move back to WLC1 automatically.

ap image upgrade destination <WLC Name> <WLC IP> [fallback]

The following show commands are provided to support this feature:

show ap upgrade summary

Displays all the upgrade report names.

show ap upgrade name <report-name>

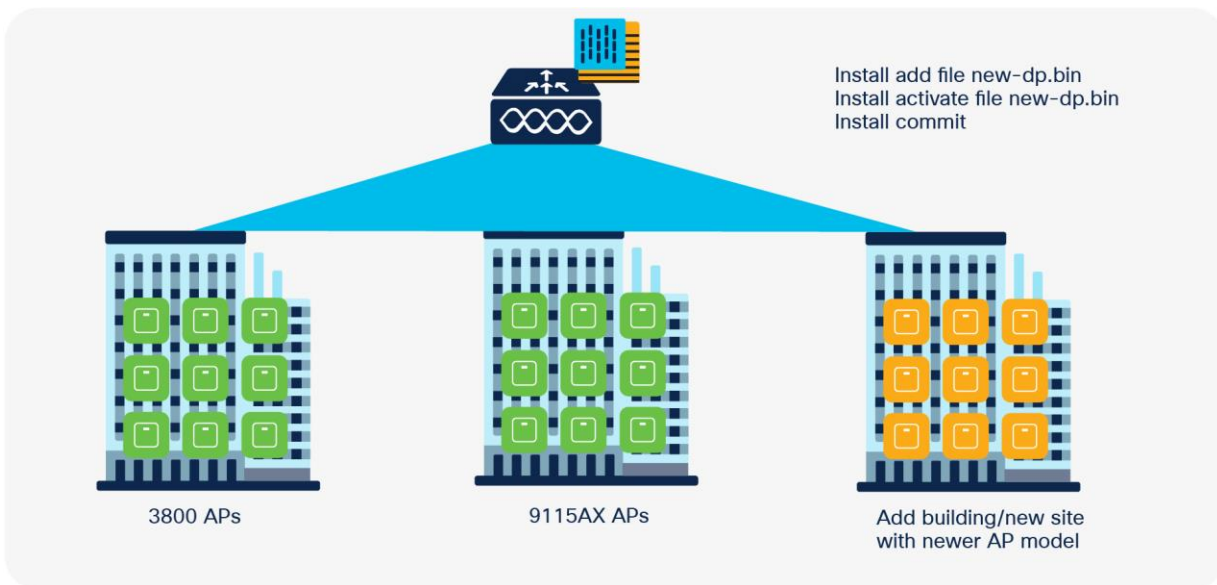
Displays AP upgrade information based on the upgrade report name.

New AP model support using AP device pack

Traditionally, when new AP hardware models are introduced, they are shipped with a corresponding WLC major software version. This means that the customer has to wait for a corresponding CCO version relative to the new AP model and has to upgrade the entire network. In Release 16.11, the wireless controller provides a way to introduce new AP models into customer networks using an AP Device Pack (APDP), without the customer having to move to a new WLC version. This allows faster deployment of the APs, confining the impact within the already validated image and effectively providing zero downtime for the controller, since it is a hot patch that does not require a reload on the controller.

Since this feature is platform independent, it is supported on all wireless platforms and all AP deployment modes (flex, local, and fabric).

Figure 12. APDP enables new AP models to join existing WLC code



Note: The new AP module will support only those capabilities that are supported in the base CCO version of the controller.

The workflow to install and activate an AP device pack is as follows.

Figure 13. APDP installation workflow



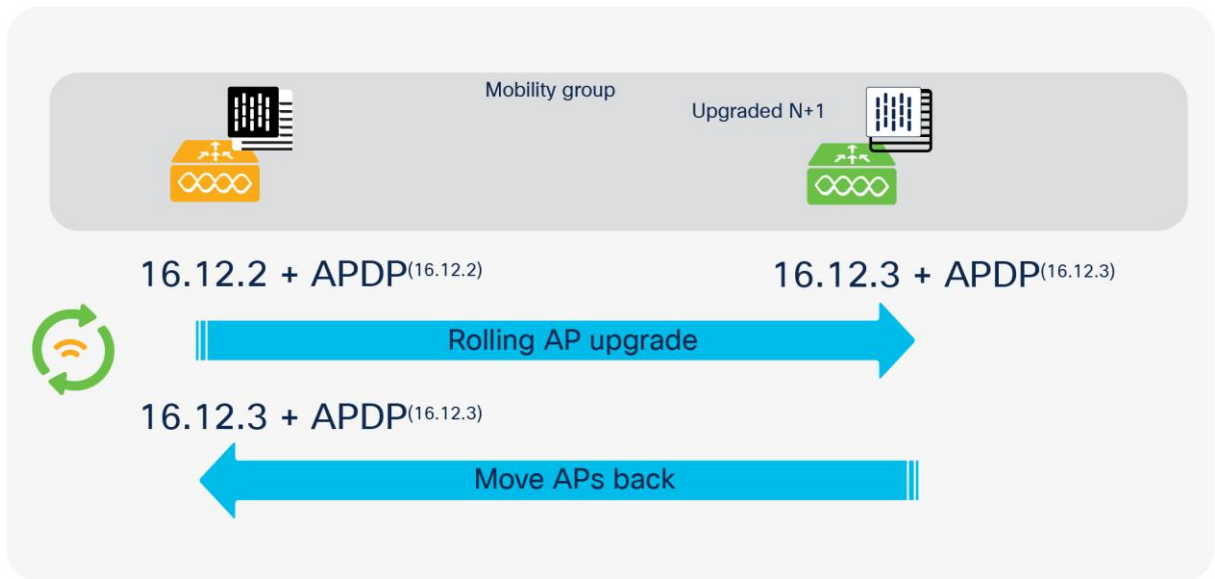
1. Add the APDP file using the “install add” command.
2. Use the “install activate” command for the APDP.
3. At this point, the WLC should be in a position to accept a new connection from the new AP model.

4. The “install commit” command will make this new AP software persistent.
 - Installation of APDP information is synced to the standby WLC in an HA system.
 - Bug fixes will be provided for a new AP introduced with the installation of an AP service pack.
 - The AP device pack will be supported up to the previous maintenance release. For example, if a new AP model is introduced in Release 16.14.1, the APDP will be supported in 16.12.x and 16.13.x.

Upgrade and downgrade scenarios with APDP

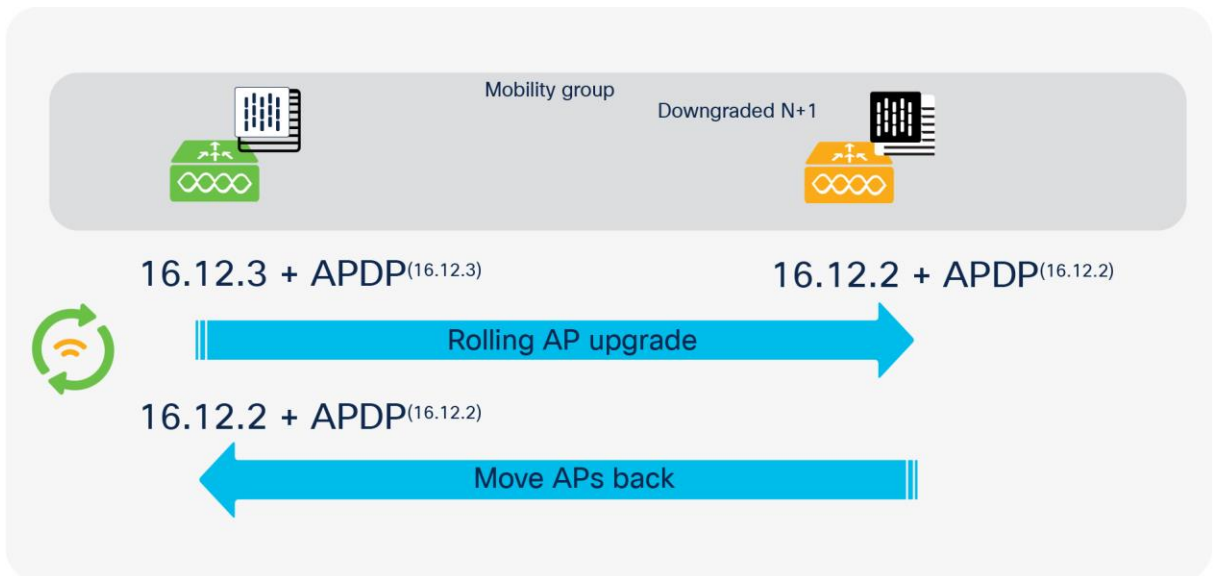
If the upgrade is to the next major release, support for the AP will be likely integrated into it. In the case of a maintenance release upgrade, an APDP pack corresponding to the image will be available and needs to be loaded on the N+1 controller. The APs are rolled over using the rolling AP upgrade process. The primary controller then needs to be reloaded with the new image and the corresponding APDP, and the APs are rolled back. No disruption occurs for existing or new model APs, since the device pack is always available.

Figure 14. Upgrade scenario with APDP



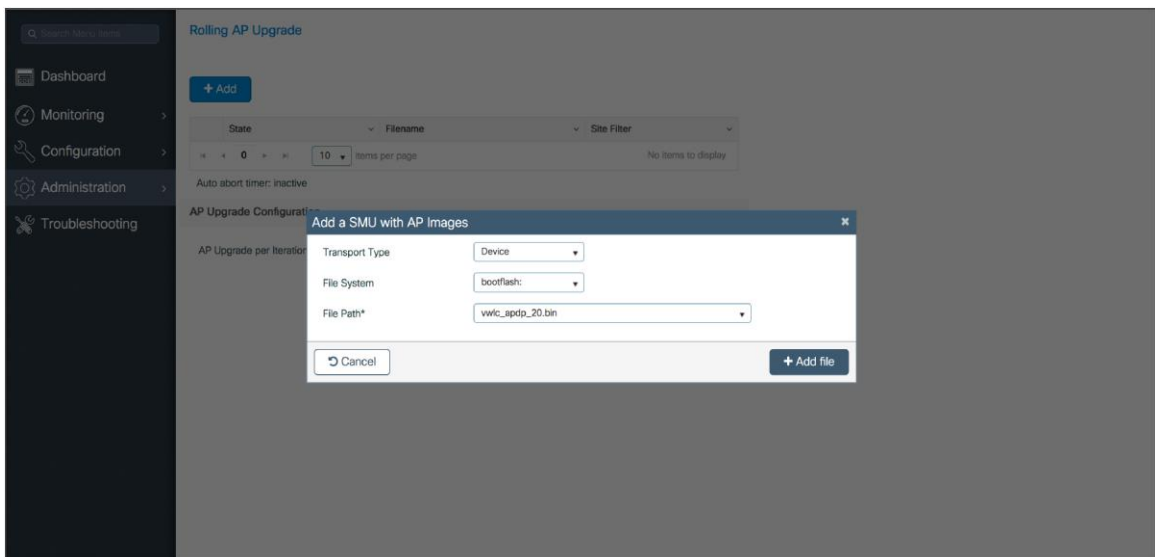
In the case of a downgrade, the N+1 controller is installed with the target downgrade image and the corresponding APDP. The APs are rolled over back to the N+1 controller, and the primary controller is reloaded with the downgraded image and the corresponding APDP.

Figure 15. Downgrade scenario with APDP



WebUI configuration

Step 1. AP device pack is downloaded to the controller under Administration > Rolling AP Upgrade.



Step 2. Click Activate to install the AP device pack on the controller as a hot patch.

The screenshot shows the 'Rolling AP Upgrade' configuration page. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area has a table with columns for State, Filename, and Site Filter. The table contains one entry: 'Inactive', 'bootflash:wlc_apdp_20.bin', and 'Not Configured'. Below the table, there is an 'AP Upgrade Configuration' section with a dropdown for 'AP Upgrade per iteration' set to '15%' and an 'Apply' button. On the right, a log panel displays the following text:

```

INSTALL ADD OPERATION:
--- Analyzing SMU file wlc_apdp_20.bin ---
SMU file wlc_apdp_20.bin has AP Images

Initiating INSTALL_ADD operation for SMU file wlc_apdp_20.bin
install_add: START Tue Feb 5 04:06:36 IST 2019
install_add: Adding SMU

--- Starting initial file syncing ---
Info: Finished copying bootflash:wlc_apdp_20.bin to the selected chassis
Finished initial file syncing

--- Starting SMU Add operation ---
Performing SMU_ADD on all members
[1] SMU_ADD package(s) on chassis 1
[1] Finished SMU_ADD on chassis 1
Checking status of SMU_ADD on [1]
SMU_ADD: Passed on [1]
Finished SMU Add operation

SUCCESS: install_add Tue Feb 5 04:07:02 IST 2019

```

Step 3. Monitor the logs on the right panel to verify that the APDP has been installed successfully. Once APs join the WLC, the APDP can be committed by clicking the Commit button.

The screenshot shows the 'Rolling AP Upgrade' configuration page after the 'Activate' step. The table now shows the state as 'Activated and Uncommitted' for the filename 'bootflash:wlc_apdp_20.bin' across 'All Sites'. The 'AP Upgrade Configuration' section remains the same. The log panel on the right displays the following text:

```

Initiating INSTALL_PREPARE operation for activate
install_prepare: START Tue Feb 5 04:08:14 IST 2019
Prepare activate invoked with filename bootflash:wlc_apdp_20.bin
Executing pre scripts....
install_prepare: Starting
Executing pre scripts done.
SUCCESS: install_prepare /bootflash/wlc_apdp_20.bin Tue Feb 5 04:08:32
IST 2019
Initiating INSTALL_ACTIVATE operation for SMU file wlc_apdp_20.bin
install_activate: START Tue Feb 5 04:08:49 IST 2019
install_activate: Activating SMU
Executing pre scripts....
Executing pre scripts done.

--- Starting SMU Activate operation ---
Performing SMU_ACTIVATE on all members
[1] SMU_ACTIVATE package(s) on chassis 1
[1] Finished SMU_ACTIVATE on chassis 1
Checking status of SMU_ACTIVATE on [1]
SMU_ACTIVATE: Passed on [1]
Finished SMU Activate operation

Executing post scripts....
Executing post scripts done.
Executing post scripts....
Executing post scripts done.
SUCCESS: install_activate /bootflash/wlc_apdp_20.bin Tue Feb 5 04:09:25
IST 2019

```

Rolling AP Upgrade

+ Add

State	Filename	Site Filter
Activated and Committed	bootflash:wlc_apdp_20.bin	All Sites

Auto abort timer: inactive

AP Upgrade Configuration

AP Upgrade per Iteration: 15% **Apply**

```

INSTALL COMMIT OPERATION:
Initiating INSTALL_COMMIT operation
install_commit: START Tue Feb 5 04:14:19 IST 2019
install_commit: Committing SMU
Executing pre scripts....
install_commit:
Executing pre scripts done.
--- Starting SMU Commit operation ---
Performing SMU_COMMIT on all members
[1] SMU_COMMIT package(s) on chassis 1
[1] Finished SMU_COMMIT on chassis 1
Checking status of SMU_COMMIT on [1]
SMU_COMMIT: Passed on [1]
Finished SMU Commit operation

SUCCESS: install_commit /bootflash/wlc_apdp_20.bin Tue Feb 5 04:14:32 I
ST 2019

```

CLI reference

The following install commands are provided to support this feature:

- `install add file < tftp/ftp/flash/disk:*.bin>`
- `install activate file <disk:*.bin>`
- `install commit`

If the user decides to deactivate an already installed APDP, the following install commands can be used:

- `install deactivate file <disk:*.bin>`
- `install commit`

Summary

Solutions described in this document enable controller and AP update operations on the network without causing a service disruption on the wireless network. The Cisco Catalyst 9800 Series controllers provide high availability across the lifecycle of deployment, from unplanned network events to planned upgrades in the network.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)