



The bridge to possible

Why You Shouldn't Fear Upgrading Your ACI Fabric

The Handbook!

Takuya Kishida - Technical Leader, Technical Marketing Engineering

Joey Ristaino - Technical Leader, Technical Marketing Engineering

BRKDCN-2910

CISCO *Live!*

#CiscoLive

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

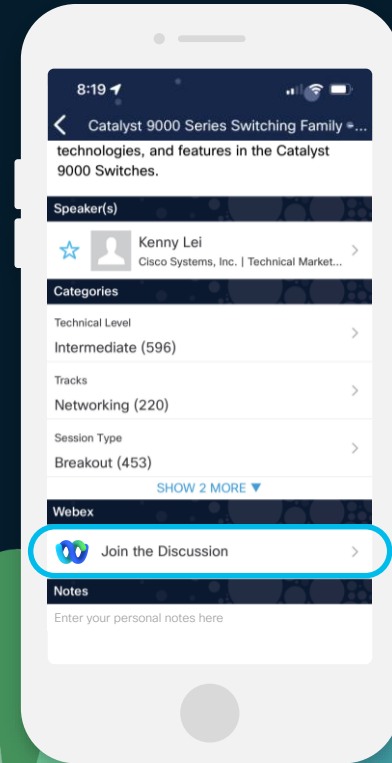
How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 7, 2024.

CISCO *Live!*

<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKDCN-2910>

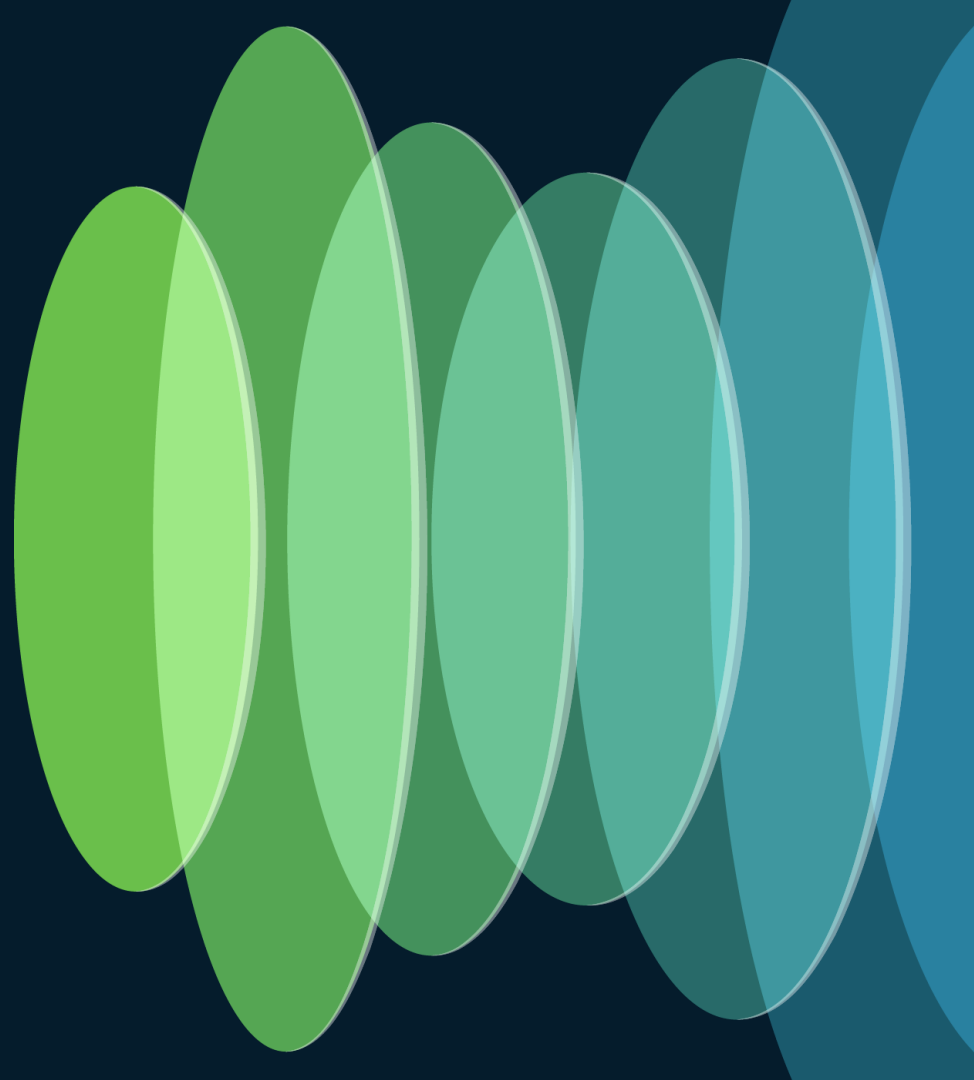




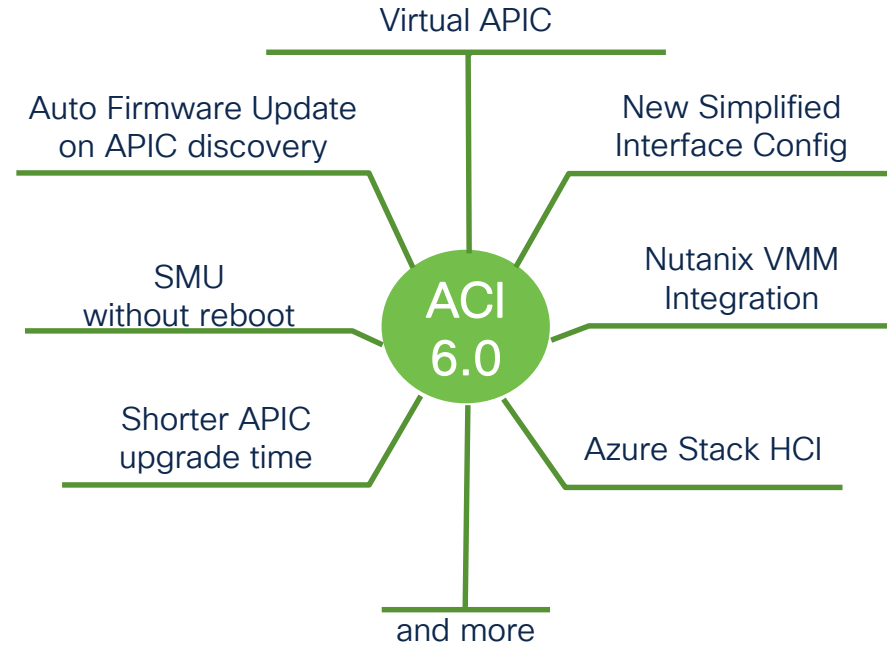
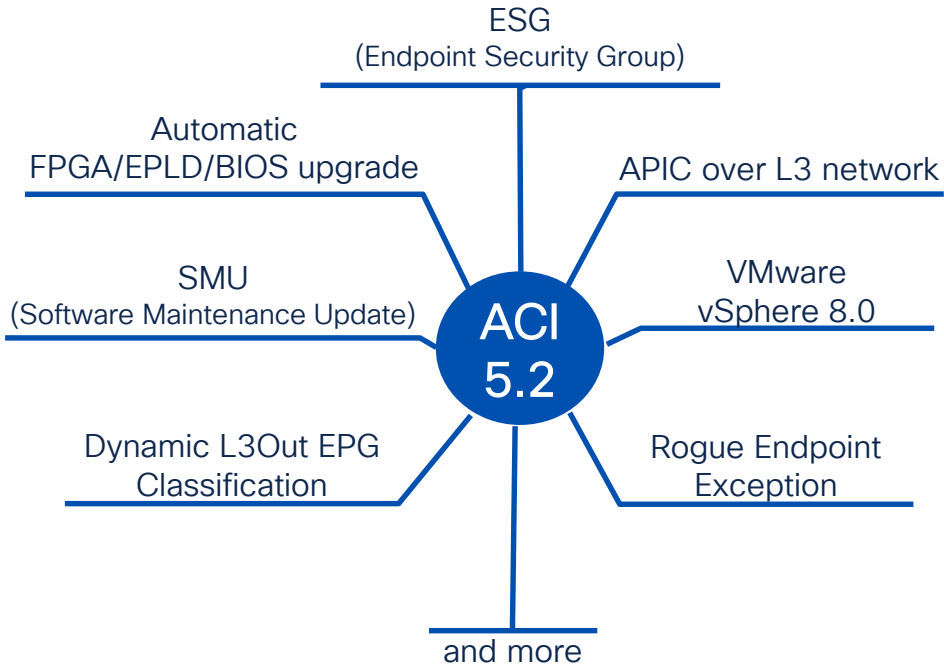
Agenda

- Why Upgrade?
- Upgrade Architecture
 - ACI Firmware Upgrade Types
 - Upgrade Architecture – APIC
 - Upgrade Architecture – Switches
 - (Bonus) Upgrade Enhancements
- Best Practices
 - Best Practices Workflow Review
 - Best Practices Configurations
 - “Pre-Upgrade Checklist” Review and Execution
 - “Do’s and Don’ts”

Why Upgrade?



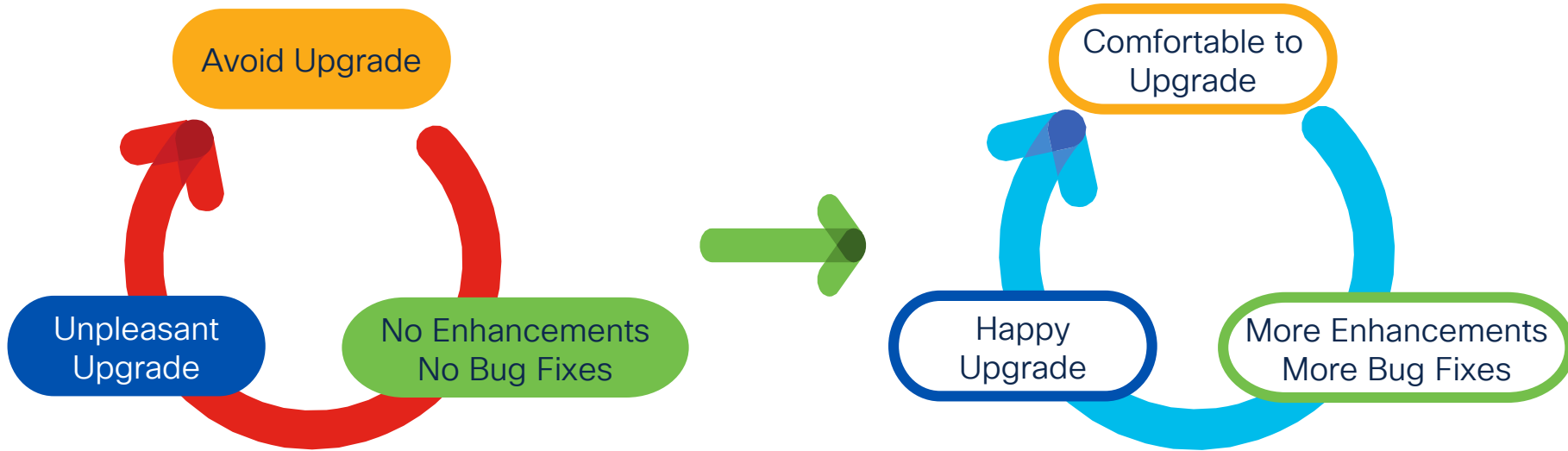
New features, new use cases, new possibilities



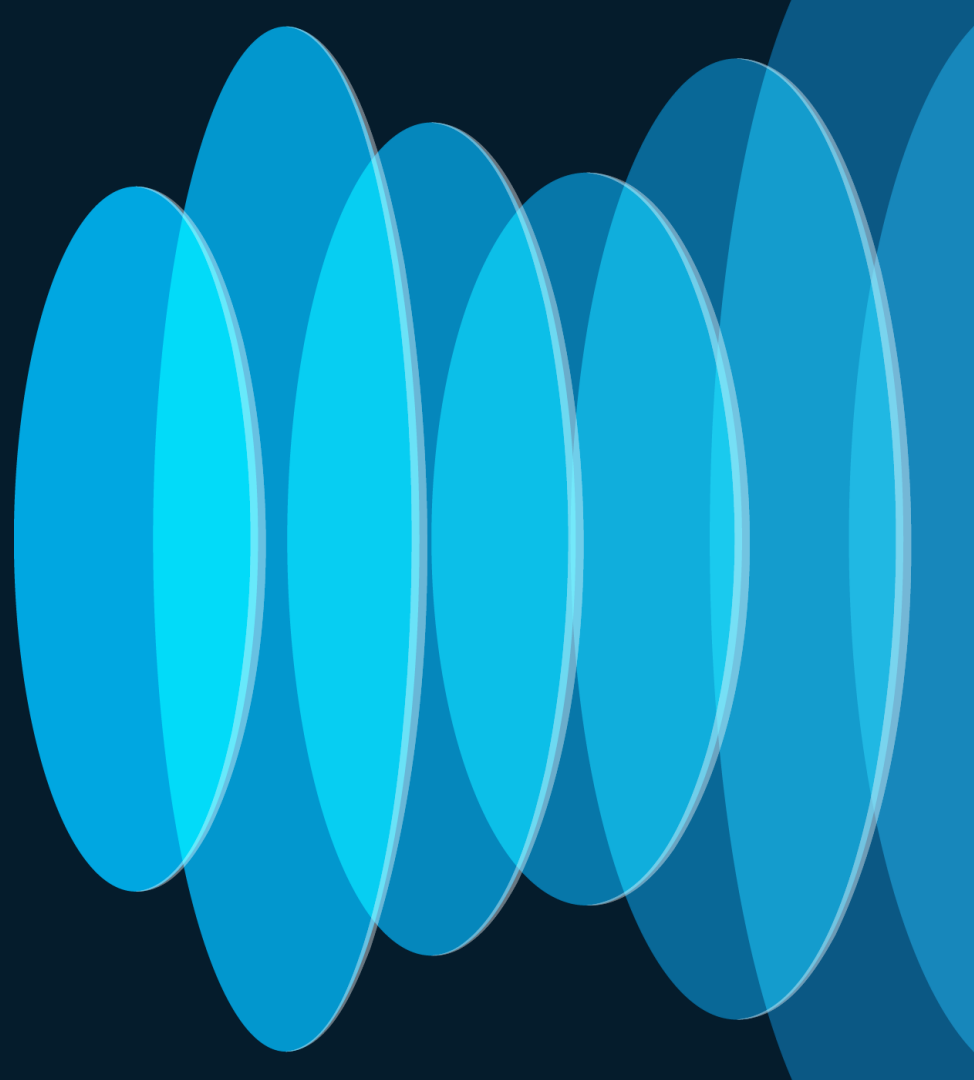
And more with NDI (Nexus Dashboard Insight) for ACI 4.2(5) or newer

Get out of the vicious cycle

By knowing the upgrade architecture and best practices



ACI Firmware Upgrade Types





ACI Firmware Upgrade Types



ACI Firmware Upgrade Types (Regular)

 Regular Upgrade

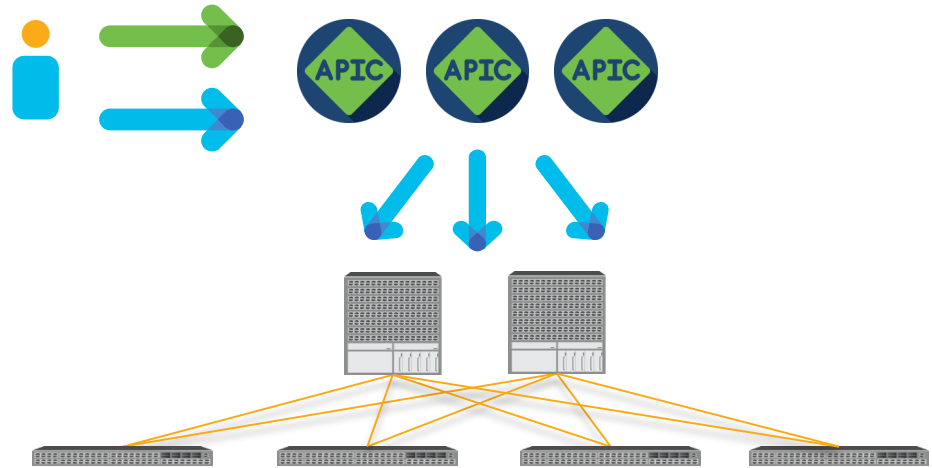
 Software Maintenance Upgrade (SMU)

 EPLD/FPGA Upgrade (Only Switches)

Base OS firmware upgrade

In principle, all APICs and switches should be on the same version

- 1 APIC Upgrade
- 2 Switch Upgrade (through APIC)



Different versions in the same fabric??



In principle, this should be avoided.

What if I cannot finish upgrades in a single upgrade window?

- Available options

APIC firmware

- All APICs must be on the same version

Switch firmware

- Switches can be on different versions
with limited operations.



Create, update and delete **BDs, EPGs, contracts, L3Outs, VMM domains, Access Policies**



Collect **configuration backups, techsupports**, or troubleshoot with **SPAN**



Physical operations such as enabling disabling **interfaces, replacing a node**


See Upgrade Guide for the complete list:

<https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/all/apic-installation-aci-upgrade-downgrade/Cisco-APIC-Installation-ACI-Upgrade-Downgrade-Guide/m-operations-allowed-during-mixed-versions-on-cisco-aci-switches.html>


ACI Firmware Upgrade Types (SMU)

5.2(1)

NEW

 Regular Upgrade

 Software Maintenance Upgrade (SMU)

 EPLD/FPGA Upgrade
(Only Switches)

A patch for a specific defect

No need to upgrade the entire fabric. You can apply it only to APICs or affected switch nodes

1

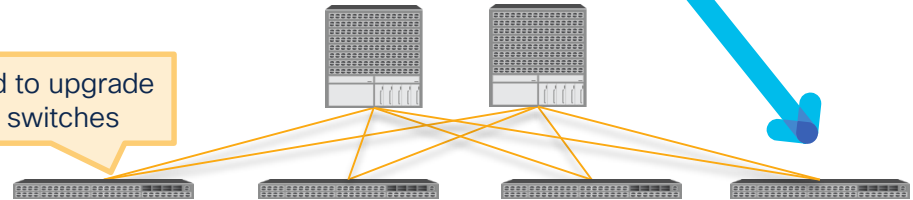
SMU for all APICs

2


SMU for specific switches (through APIC)




No need to upgrade other switches



ACI Firmware Upgrade Types (EPLD/FPGA)

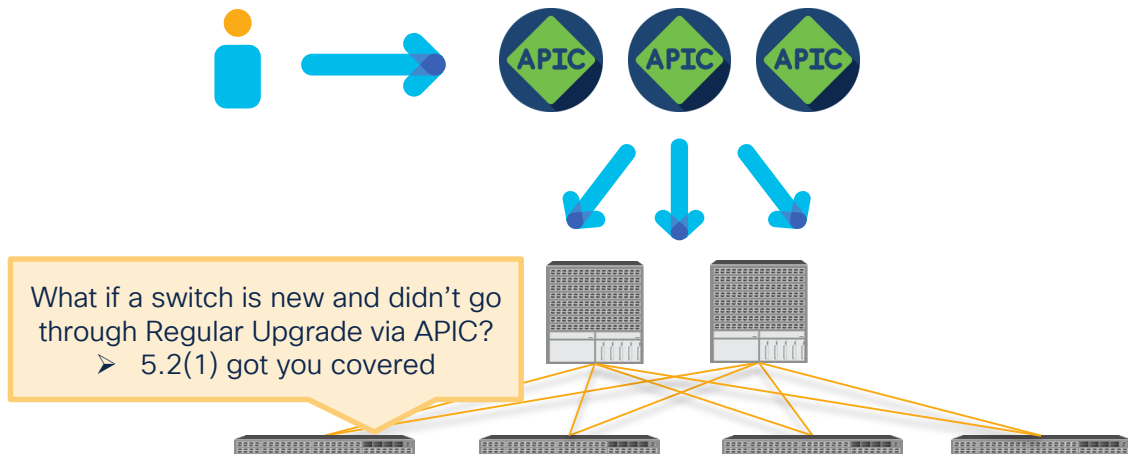
 Regular Upgrade

 Software Maintenance Upgrade (SMU)

 EPLD/FPGA Upgrade (Only Switches)

Hardware related firmware

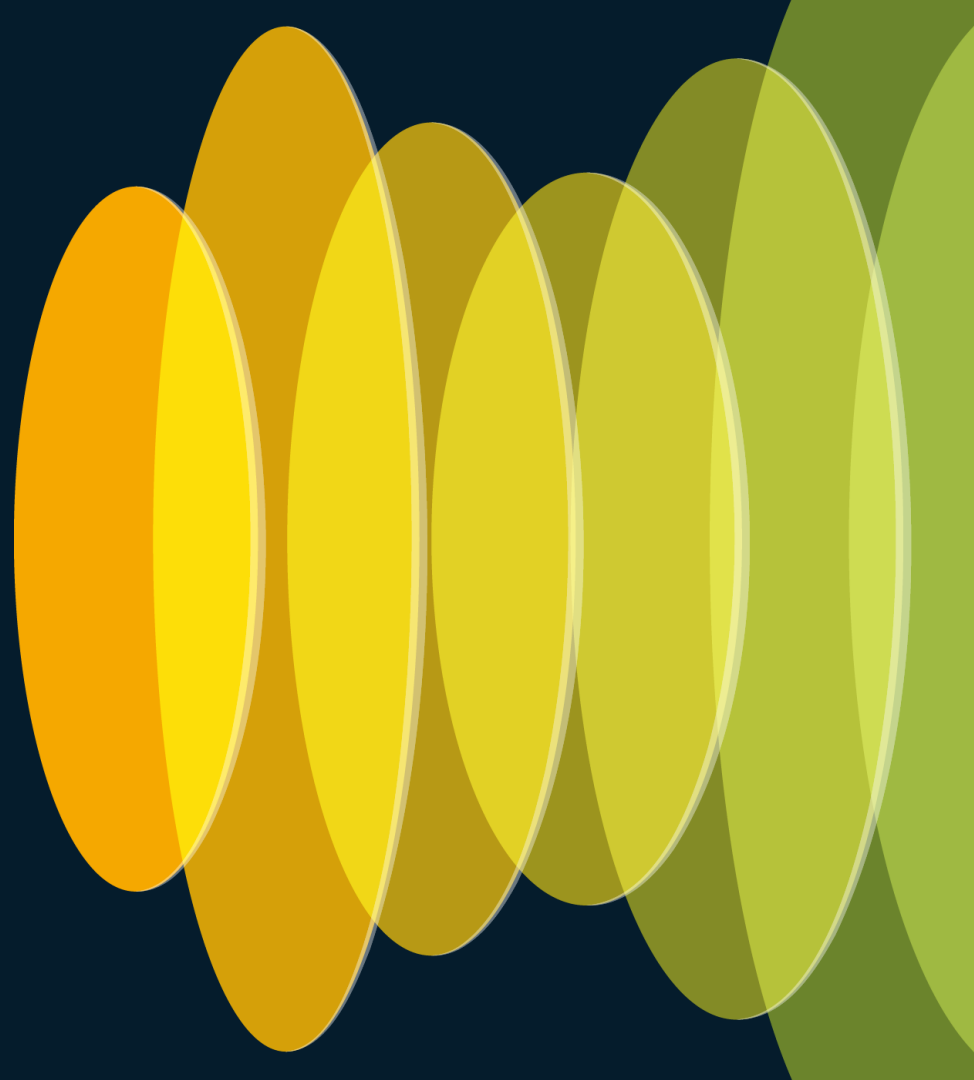
Each ACI switch version has the desired EPLD/FPGA version.
Automatically upgraded via Regular Upgrade through APIC.
➤ No user configurations



APIC Upgrade Architecture

Note: for 4.0 or newer APICs

CISCO *Live!*



APIC Upgrade Architecture

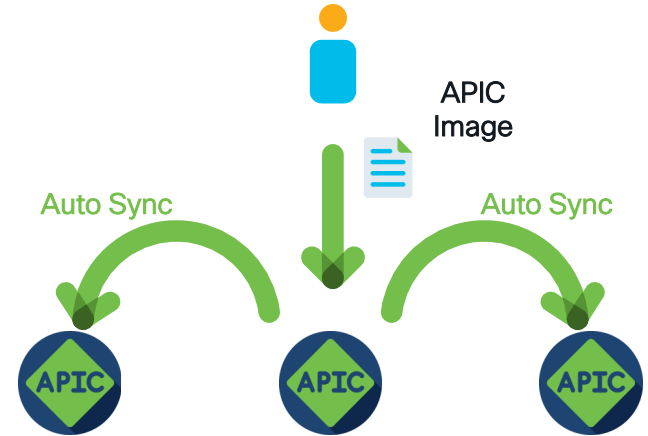
Image Upload

- A user uploads the APIC image on one of APICs
- After md5sum check, the image is copied to other APICs

Trigger

Install

Data Conversion
&
Reboot



APIC Upgrade Architecture

Image Upload

Trigger

- Set the target version on all APICs
- APIC1 informs shards on all APICs of upgrades

Install

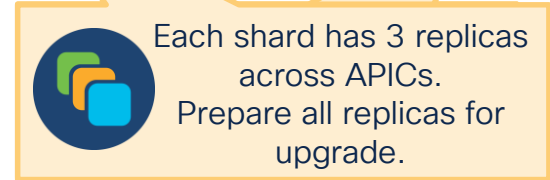
Data Conversion
&
Reboot

No disruptive operations from this point.
(details in later slides)

Estimated Time

A few min.

Prepare all shards for upgrade



APIC Upgrade Architecture

Image Upload

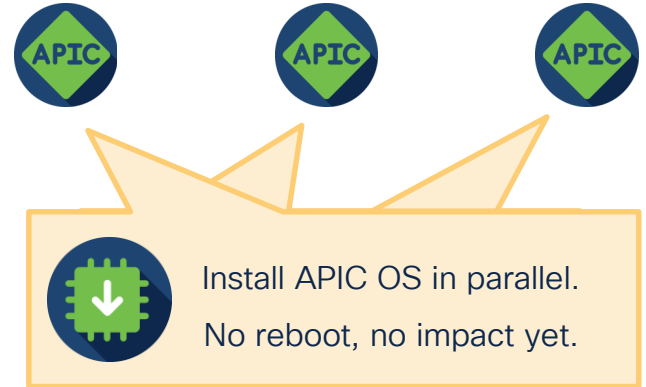
Trigger

Install

- Install APIC OS in a backup partition
- All APICs perform this in parallel

Data Conversion
&
Reboot

Estimated Time
A few min.



APIC Upgrade Architecture

Image Upload

Trigger

Install

**Data Conversion
&
Reboot**

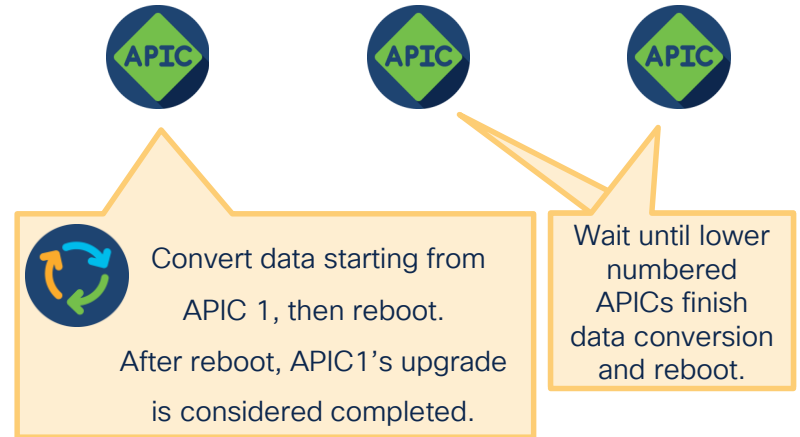
- Convert user configurations and data to the target version format
- Conversion happens one APIC at a time

6.0(3) or newer requires significantly less time due to an internal enhancement in data conversion

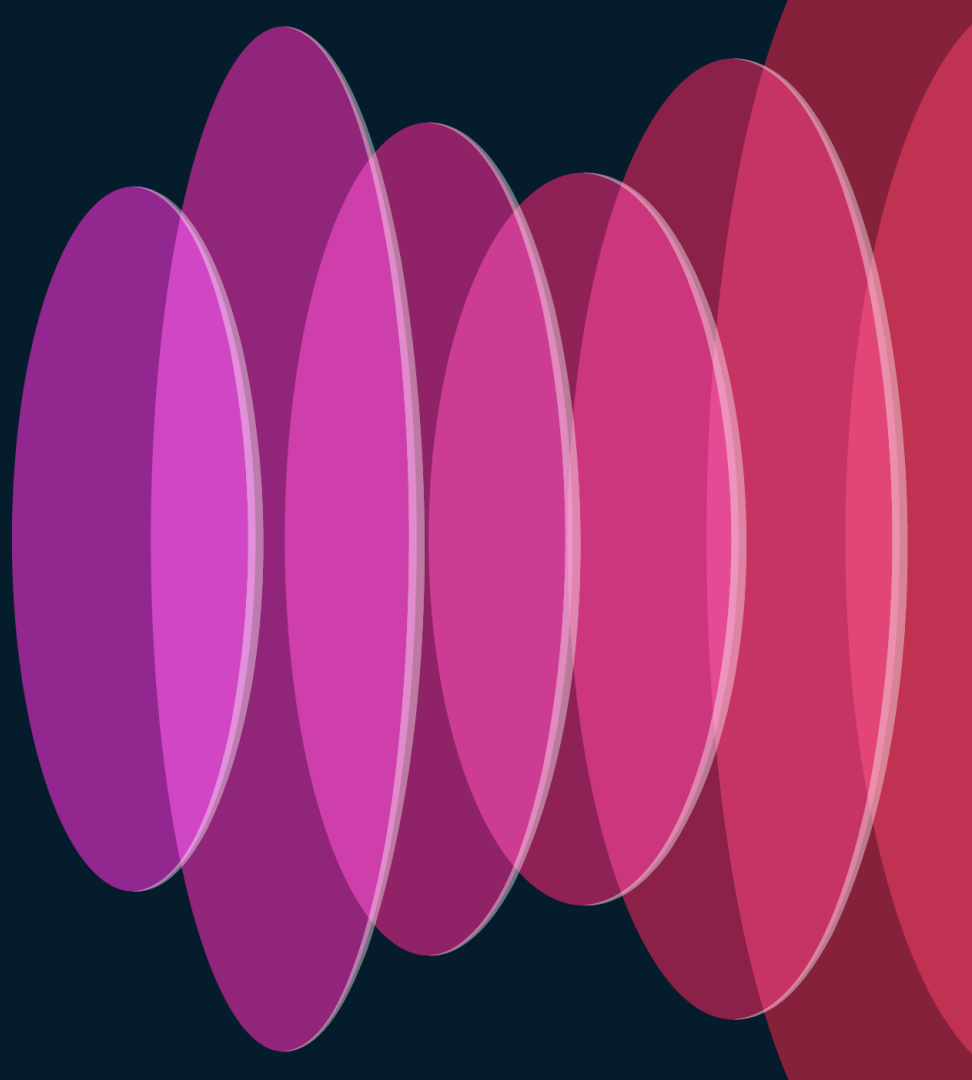
NEW

Estimated Time

Depends on the size of data.
A fair estimation would be 40 min per APIC
(potentially more or less)



ACI Switch Upgrade Architecture



ACI Switch Upgrade Flow

Image Download

- The switch downloads the image from APIC
- The download is via infra TEP

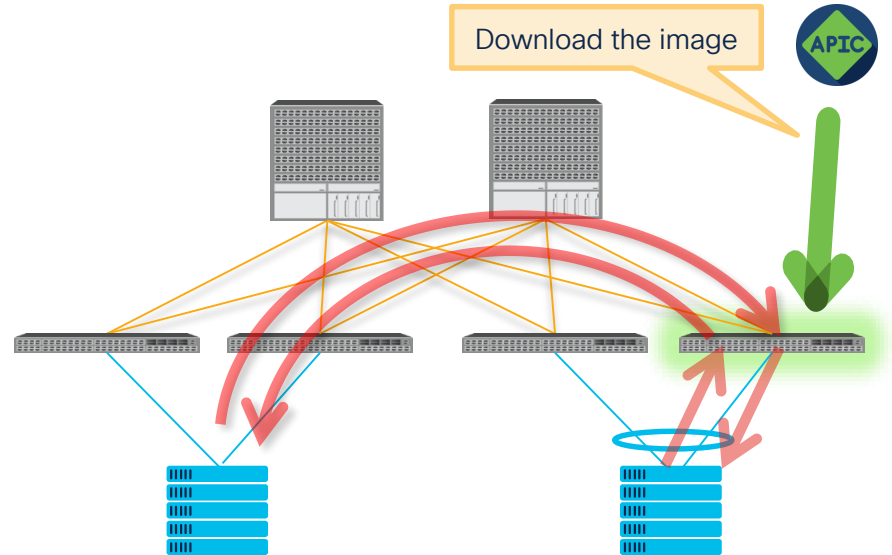
Queuing

Preparation

Reboot

Boot Up

No Traffic Impact



ACI Switch Upgrade Flow

Image
Download

Queuing

- The switch receives approval from APIC
- Controls switches that are upgraded in parallel

Preparation

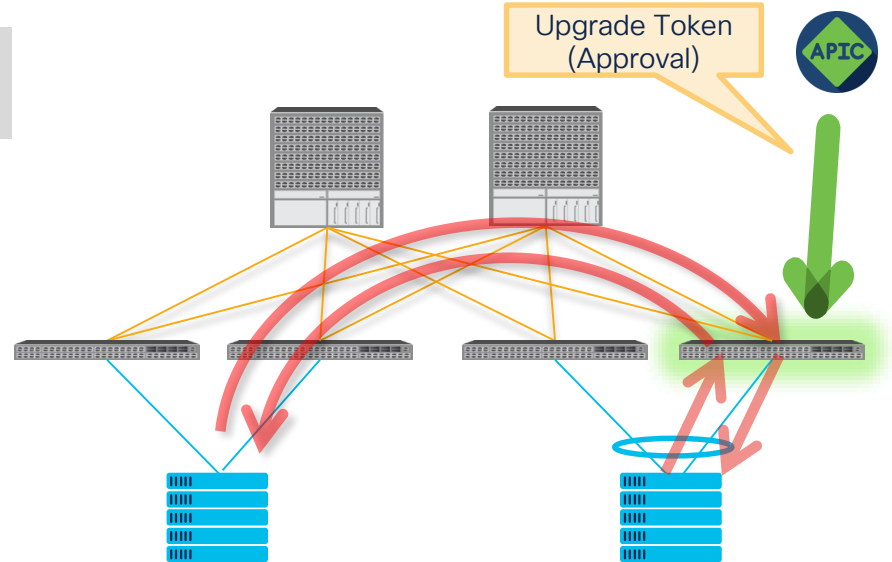
Since APIC 4.1(1)

- One leaf at a time in each vPC pair
- Not all spines in each pod if graceful option is used

Reboot

Boot Up

No Traffic Impact



ACI Switch Upgrade Flow

Image
Download

Queuing

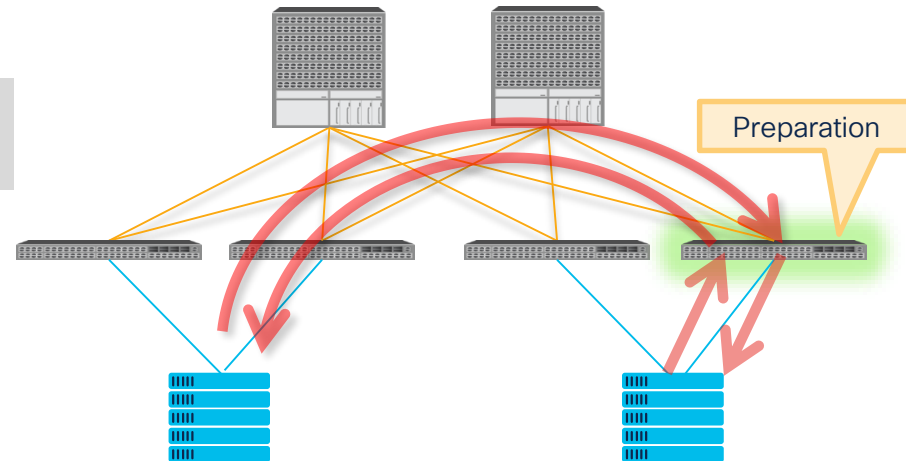
Preparation

- The switch extracts the image.
- The switch sets the boot var and so on.

Reboot

Boot Up

No Traffic Impact



ACI Switch Upgrade Flow

Image
Download

Queuing

Preparation

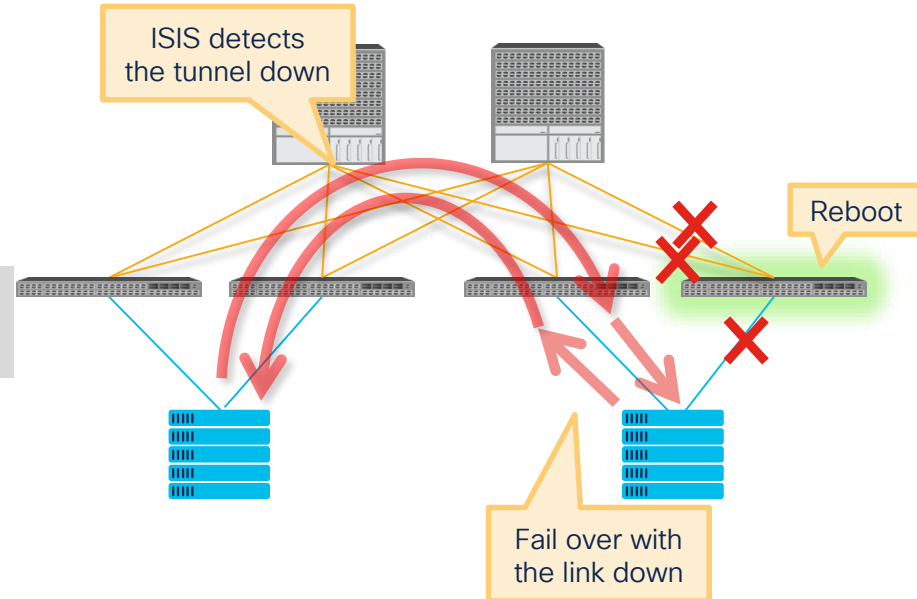
Reboot

- Wipe the config and reboot (i.e. clean reboot)
- Traffic failover relies on link failure

Boot Up

- Depends on other conditions such as:
- Link failure detection time on external devices
 - Routing protocol and so on

**< 100 msec Traffic Impact
in the best case**



ACI Switch Upgrade Flow

Image
Download

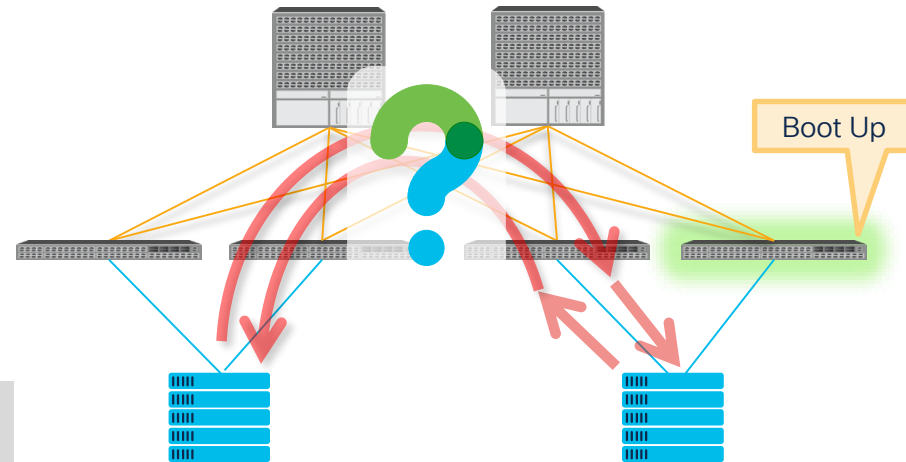
Queuing

Preparation

Reboot

Boot Up

- Various traffic flow optimizations
- (Continue to next slides)



ACI Switch Upgrade Flow (Boot Up Sequence)

Boot Up

· Various traffic flow optimizations

01

- Bring up fabric links
- Bring up APIC connected down links
- Admin down other down links

02

03

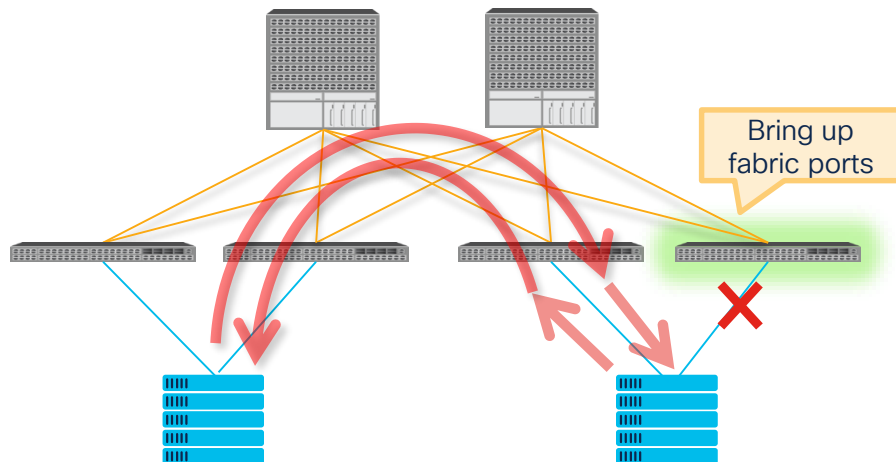
04

05

06

07

No Traffic Flow Change



ACI Switch Upgrade Flow (Boot Up Sequence)

Boot Up

· Various traffic flow optimizations

01

- Bring up fabric links
- Bring up APIC connected down links
- Admin down other down links

02

- An APIC discovers the switch via DHCP/LLDP
- The same TEP IP is assigned

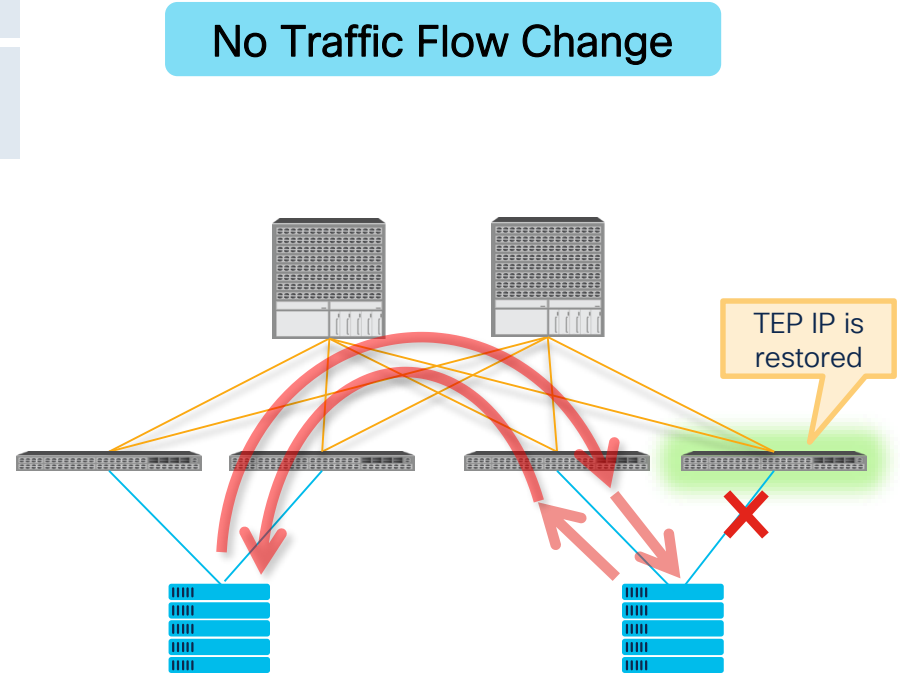
03

04

05

06

07



ACI Switch Upgrade Flow (Boot Up Sequence)

Boot Up

· Various traffic flow optimizations

01

- Bring up fabric links
- Bring up APIC connected down links
- Admin down other down links

02

- An APIC discovers the switch via DHCP/LLDP
- The same TEP IP is assigned

03

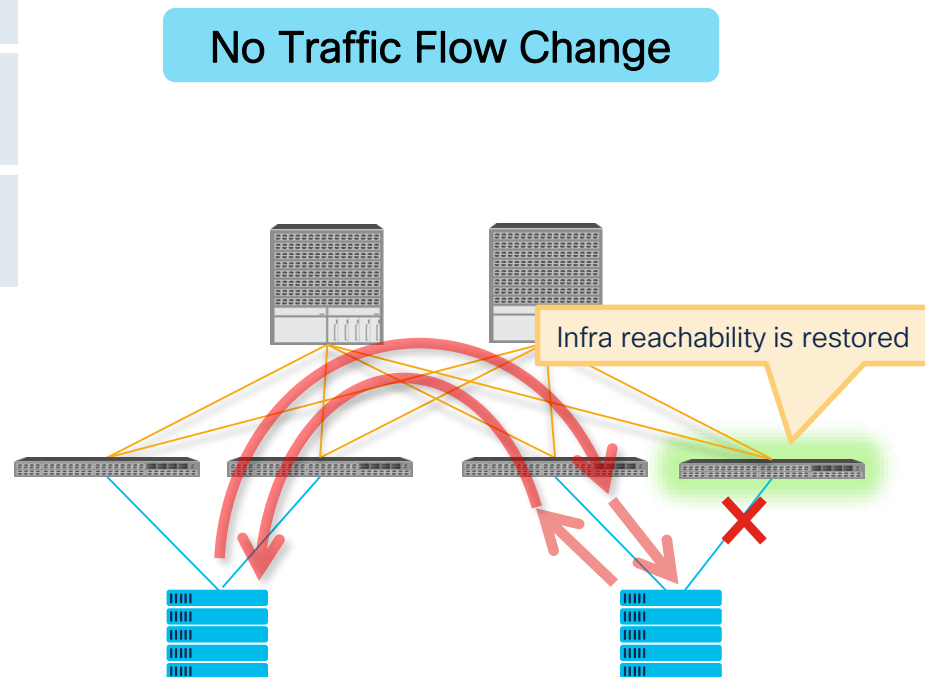
- ISIS overload mode is activated
 - ✓ ISIS advertises the TEP IP with a large metric
 - ✓ ISIS does not advertise BD mcast groups to join

04

05

06

07



ACI Switch Upgrade Flow (Boot Up Sequence)

Boot Up

· Various traffic flow optimizations

01

- Bring up fabric links
- Bring up APIC connected down links
- Admin down other down links

02

- An APIC discovers the switch via DHCP/LLDP
- The same TEP IP is assigned

03

- ISIS overload mode is activated
 - ✓ ISIS advertises the TEP IP with a large metric
 - ✓ ISIS does not advertise BD mcast groups to join

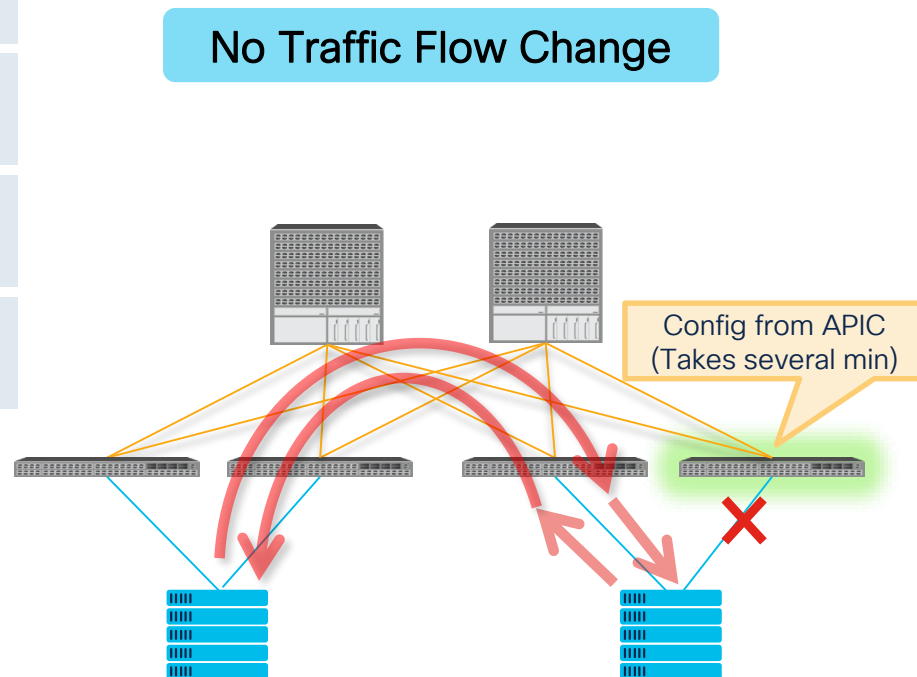
04

- Starts downloading configurations from an APIC

05

06

07



ACI Switch Upgrade Flow (Boot Up Sequence)

Boot Up

· Various traffic flow optimizations

01

- Bring up fabric links
- Bring up APIC connected down links
- Admin down other down links

02

- An APIC discovers the switch via DHCP/LLDP
- The same TEP IP is assigned

03

- ISIS overload mode is activated
 - ✓ ISIS advertises the TEP IP with a large metric
 - ✓ ISIS does not advertise BD mcast groups to join

04

- Starts downloading configurations from an APIC

05

- ISIS multicast overload mode completes (i.e. flood)
- vPC peer is established at the same time

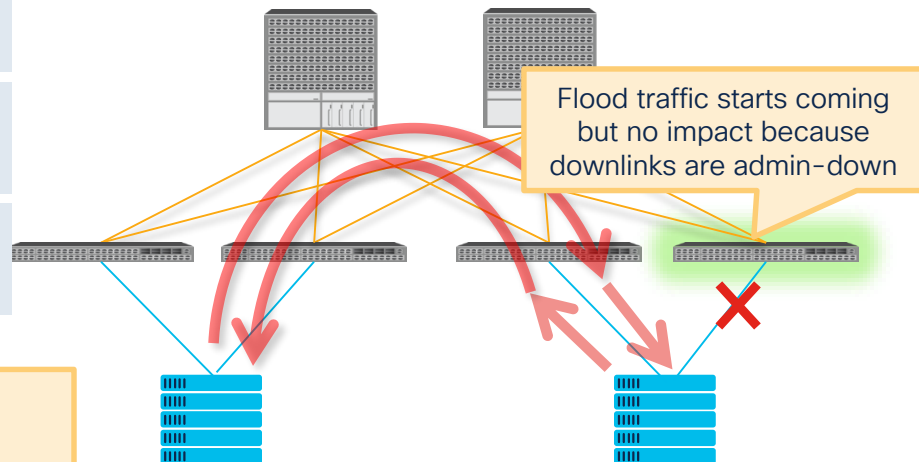
06

ISIS multicast overload timer

- Leaf nodes – Fixed 1min
- Spine nodes – When FTAG tree is created (Fixed 1 min prior to Switch 14.2(1))

07

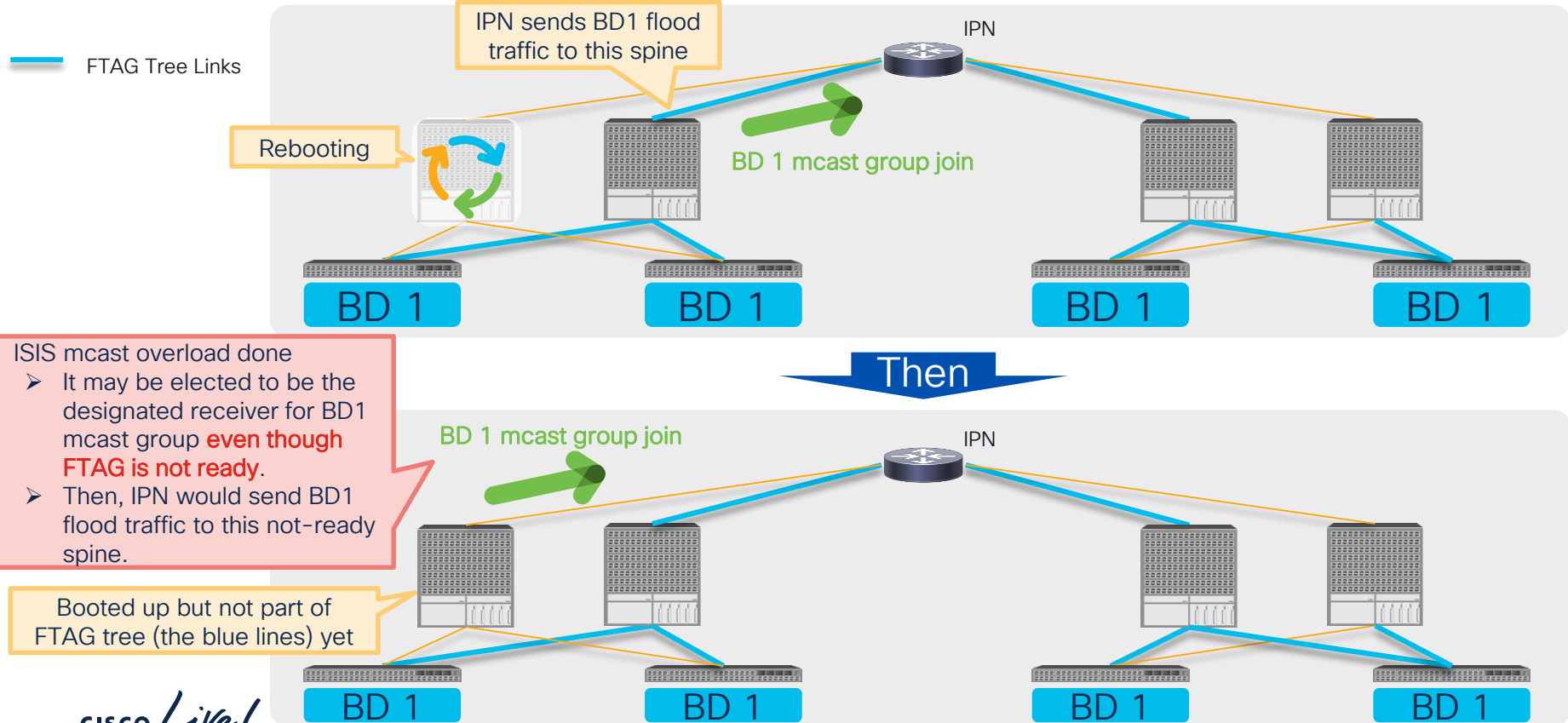
No Traffic Flow Change



Spine ISIS multicast overload timer (CSCvp79708)



Why not a fixed 1 min?



ACI Switch Upgrade Flow (Boot Up Sequence)

Boot Up

· Various traffic flow optimizations

01

- Bring up fabric links
- Bring up APIC connected down links
- Admin down other down links

02

- An APIC discovers the switch via DHCP/LLDP
- The same TEP IP is assigned

03

- ISIS overload mode is activated
 - ✓ ISIS advertises the TEP IP with a large metric
 - ✓ ISIS does not advertise BD mcast groups to join

04

- Starts downloading configurations from an APIC

05

- ISIS multicast overload mode completes (i.e. flood)
- vPC peer is established at the same time

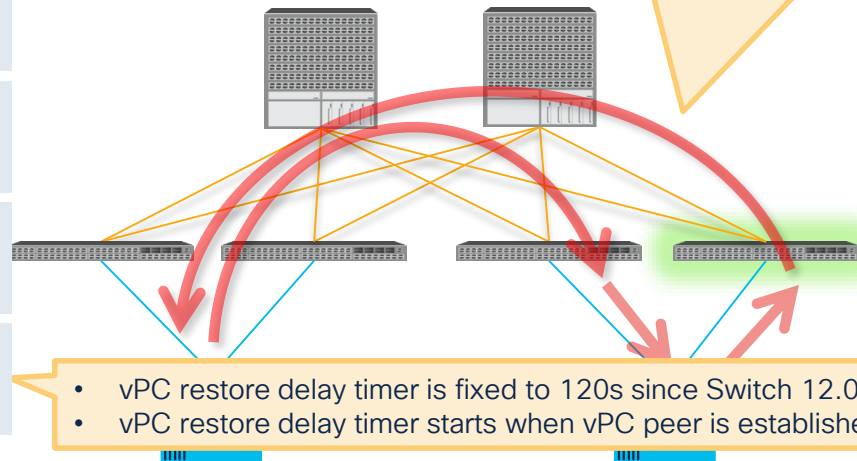
06

- Full configuration has been downloaded
 - ✓ Bring up access links (downlinks)
 - ✓ and vPC ports after vPC restore delay timer expires

07

Ready to receive traffic

- VLANs are deployed
 - For VMM, depends on Resolution Immediacy
- Contracts are deployed
 - Depends on Deployment Immediacy
- Spine-Proxy is ready
- Flood handling (FTAG) is ready



ACI Switch Upgrade Flow (Boot Up Sequence)

Boot Up

· Various traffic flow optimizations

01

- Bring up fabric links
- Bring up APIC connected down links
- Admin down other down links

02

- An APIC discovers the switch via DHCP/LLDP
- The same TEP IP is assigned

03

- ISIS overload mode is activated
 - ✓ ISIS advertises the TEP IP with a large metric
 - ✓ ISIS does not advertise BD mcast groups to join

04

- Starts downloading configurations from an APIC

05

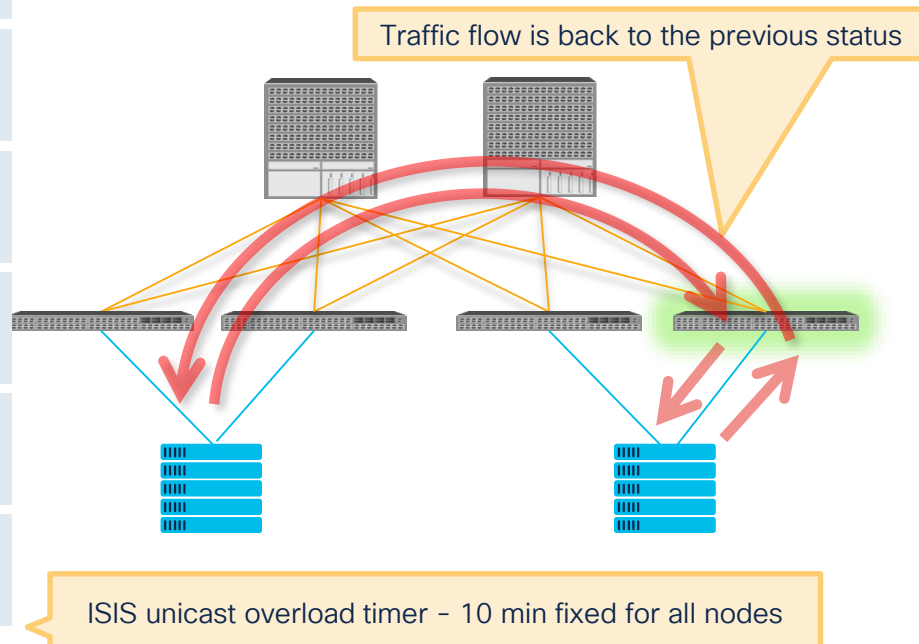
- ISIS multicast overload mode completes (i.e. flood)
- vPC peer is established at the same time

06

- Full configuration has been downloaded
 - ✓ Bring up access links (downlinks)
 - ✓ and vPC ports after vPC restore delay timer expires

07

- ISIS unicast overload mode completes
 - ✓ The TEP IP is advertised with a normal metric



ACI Switch Upgrade with Graceful Option (a.k.a. Graceful Upgrade)

ACI Switch Upgrade with graceful option

Image
Download

Scheduler

Preparation

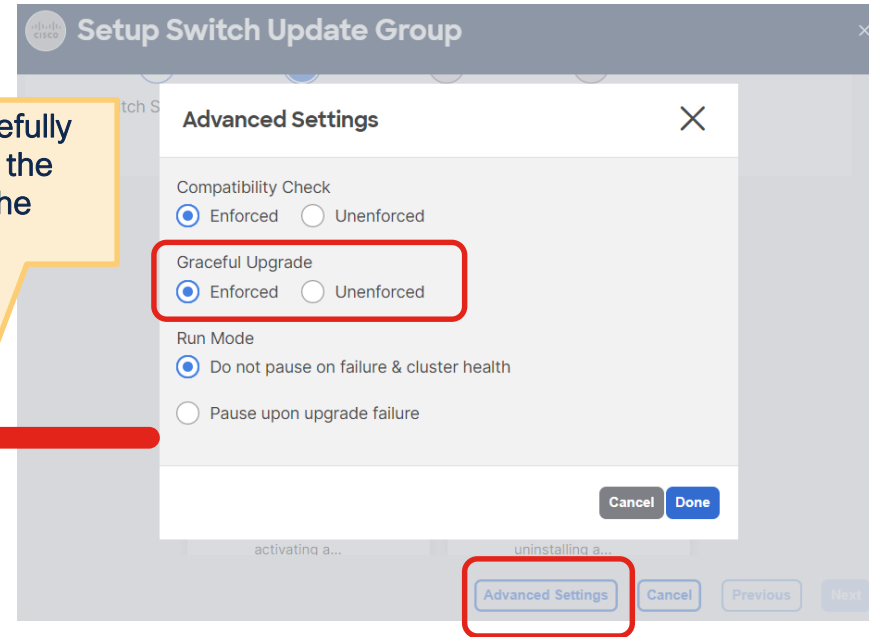
Reboot

- Wipe the config and reboot (i.e. clean reboot)
- ~~Traffic failover relies on link failure~~

Boot Up

The rest is the same as without graceful option.

Graceful Option is to gracefully isolate the switch before the switch goes down for the upgrade



ACI Switch Upgrade with graceful option

Image Download

Scheduler

Preparation

Reboot

- Wipe the config and reboot (i.e. clean reboot)
- ~~Traffic failover relies on link failure~~

Boot Up

The rest is the same as without graceful option.

Graceful Option is to gracefully isolate the switch before the switch goes down for the upgrade

Older APIC GUI

Schedule Node Upgrade

Group Type: Switch vPod

Upgrade Group: Existing New

Upgrade Group Name:

Manual Silent Roll Package Upgrade:

Target Firmware Version:

Ignore Compatibility Check:

Graceful Maintenance:

Run Mode: Do not pause on failure and do not wait on cl

Upgrade Start Time: Now Download Image Now and Schedu

Enhanced reboot sequence with graceful option

- Graceful option **disabled**

Reboot

1. Wipe the config and reboot (i.e. clean reboot)
2. Traffic failover relies on user configured link failure mechanism

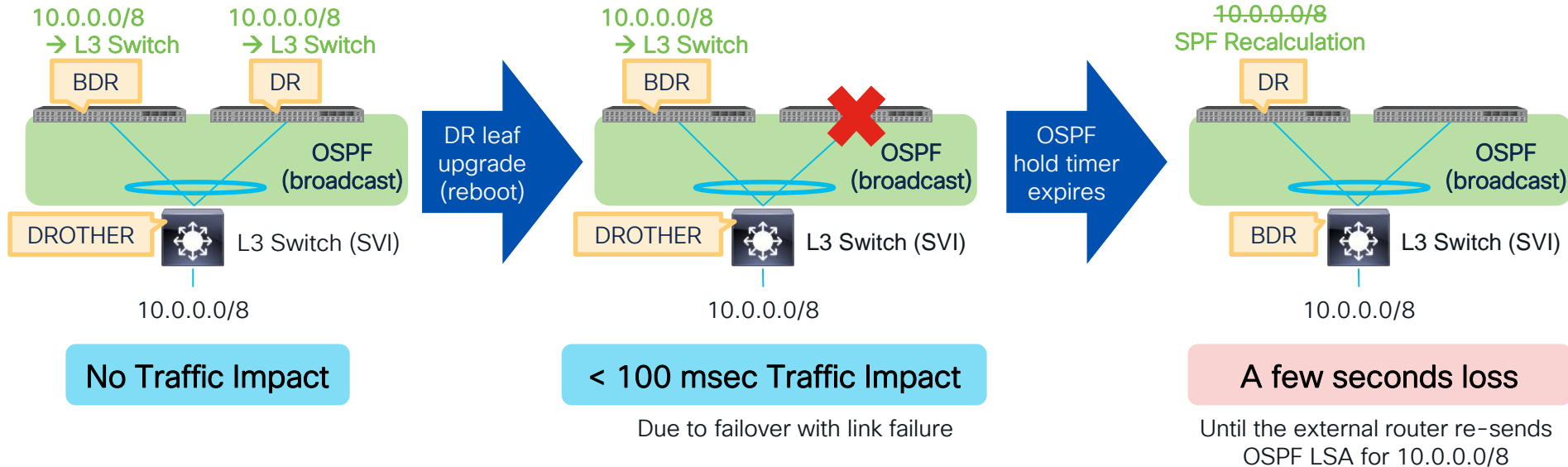
- Graceful option **enabled**

Reboot

1. Put the switch into MMode (Maintenance Mode)
 1. ISIS Overload Mode enabled
 2. Graceful Shutdown on Routing Protocols
 - ✓ Leaf - BGP, EIGRP, OSPF for L3Out
 - ✓ Spine - BGP, OSPF for IPN, GOLF
 3. vPC informs its peer that this switch is going down
 4. LACP sends PDUs with aggregation bit zero (starting from 3.1(2))
 - External devices can exclude the link from the port-channel before the link physically goes down.
 5. Shutdown front panel ports
 - ✓ Leaf - all down links including APIC connected links
2. Wipe the config and reboot (i.e. clean reboot)

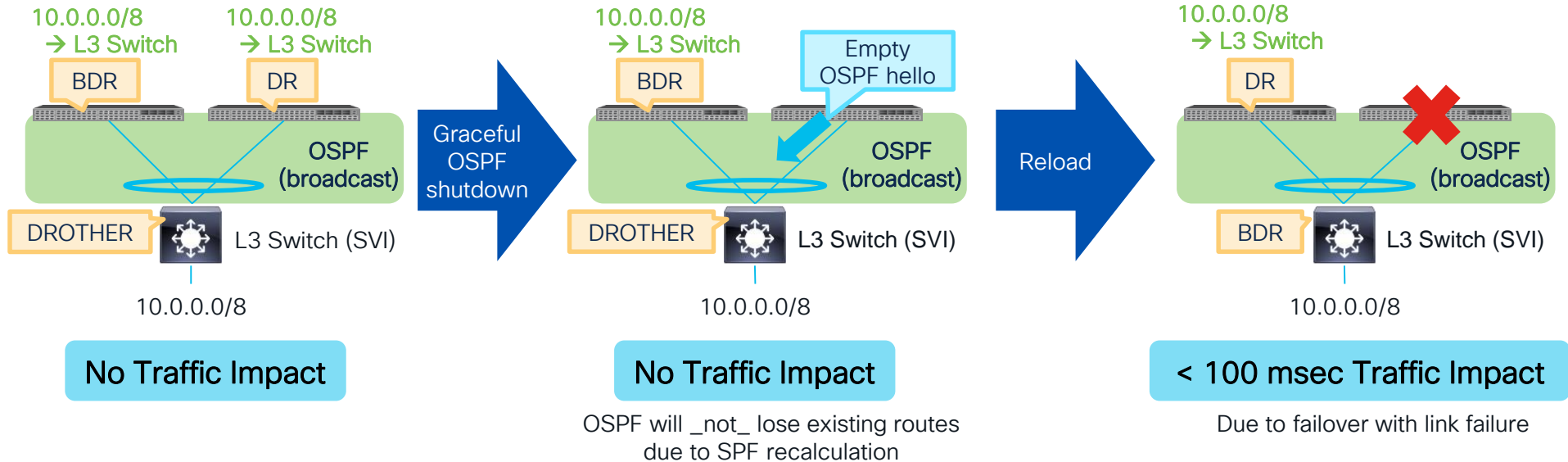
Traffic Disruption without Graceful Upgrade

- OSPF DR reboot example



With Graceful Upgrade

- OSPF DR reboot example



GIR and Graceful Upgrade in ACI



Both GIR (Graceful Insertion and Removal) and Graceful Upgrade put the switch in MMode (Maintenance Mode) to isolate the switch from the fabric.

However, the use case for these two features are completely different.

GIR (Graceful Insertion and Removal)

Use Case:

- To isolate a switch for further debugging
- To quickly restore service by isolating a malfunctioning switch

Difference:

- It is not supported to upgrade a switch in MMode via GIR

Serial Number	Model	Pod ID
FDO230...	N9K-C93106V...	1
FDO230...	N9K-C93106V...	
FDO232...	N9K-C93106V...	
FDO232...	N9K-C93106V...	
FDO232...	N9K-C93106V...	
FDO232...	N9K-C93106V...	
FDO232...	N9K-C93106V...	

An upgrade with the graceful option

Use Case:

- To upgrade a switch after isolating the switch

Difference:

- The switch will communicate to APIC and perform an upgrade immediately after the switch was put into MMode.

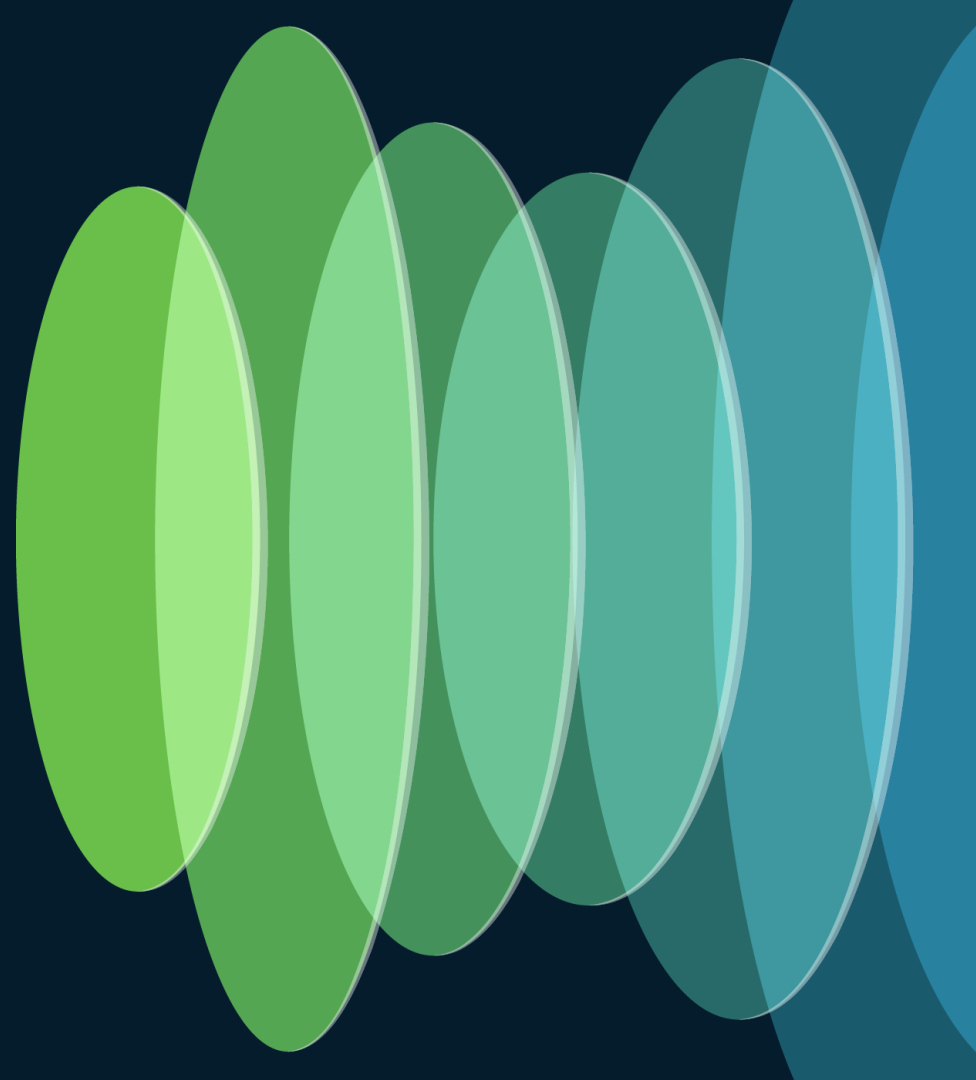
Advanced Settings

Compatibility Check
 Enforced Unenforced

Graceful Upgrade
 Enforced Unenforced

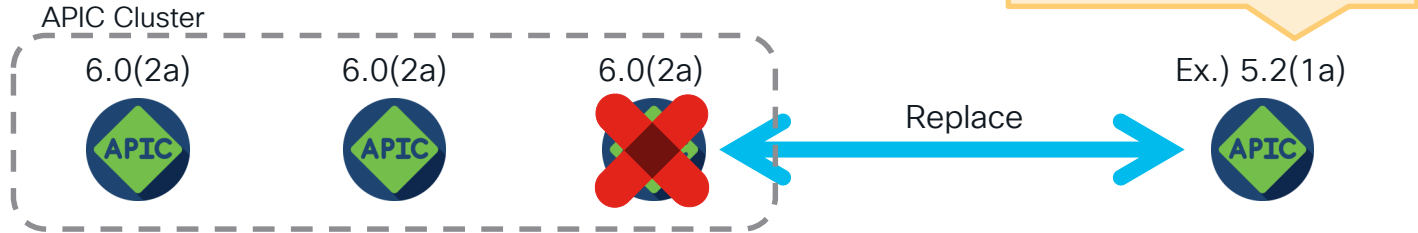
Run Mode

Auto Firmware Update



Auto Firmware Update for APIC

Use Case 1: APIC Replacement



Use Case 2: Cluster Expansion



Auto Firmware Update for Switches

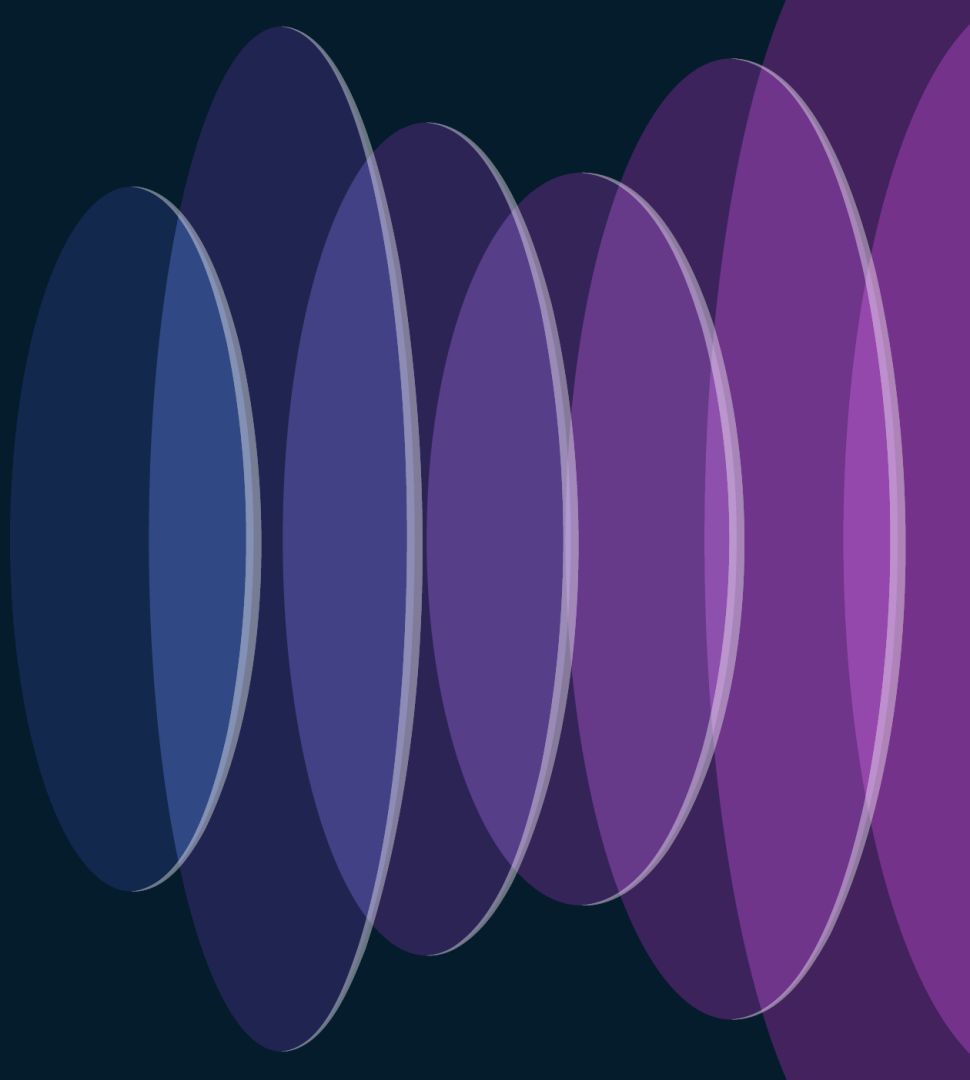
Enforcing Version Consistency

The screenshot shows the 'Fabric Membership' configuration page. At the top, there are tabs for 'Registered Nodes', 'Nodes Pending Registration', 'Unreachable Nodes', 'Unmanaged Fabric Nodes', and 'Auto Firmware Update'. The 'Auto Firmware Update' tab is selected. Below the tabs, there is a blue information box with a warning icon. The text inside the box reads: 'When Auto Firmware Update on Switch Discovery is enabled, APIC automatically updates the switch firmware for the following scenarios:'. Below this, there is a bulleted list: '• A new switch discovery with a new node ID.', '• A switch replacement with an existing node ID.', and '• An initialization and rediscovering of an existing node.'. Below the list, there is a paragraph: 'If the new switch's node ID is already part of a firmware update group under Admin > Firmware, such as a replacement scenario, the new switch is updated to the target version specified by the update group. Otherwise, it is updated to Default Firmware Version specified by Auto Firmware Update on Switch Discovery.'. Below the information box, there is a green-bordered box containing the configuration options: 'Auto Firmware Update on Switch Discovery: ' and 'Default Firmware Version: n9000-15.2(7f)'. The 'Default Firmware Version' is shown in a dropdown menu.

Fabric > Inventory > Fabric Membership > Auto Firmware Update >=5.1(1)







Admin > Firmware > Infrastructure > Nodes > Enforce Bootscript Version Validation < 5.1(1)

32-bit/64-bit Switch Images



32-bit/64-bit switch images

<https://software.cisco.com>

Cisco Nexus 9000 Series ACI Mode Switch Software 64-bit Release 16.0(2h) aci-n9000-dk9.16.0.2h-cs_64.bin Advisories	01-Mar-2023	2007.44 MB	  
Cisco Nexus 9000 Series ACI Mode Switch Software 32-bit Release 16.0(2h) aci-n9000-dk9.16.0.2h.bin Advisories	01-Mar-2023	1893.29 MB	  

Why?

Scalability

To utilize the most of what the switch hardware has to offer.

Example: Forwarding Scale Profile such as Max LPM profile requires 32 GB memory / 64-bit image.

Which Image?

APIC picks the right one for you

6.0(3) or newer:

Total memory is 24GB or less: 32 bit

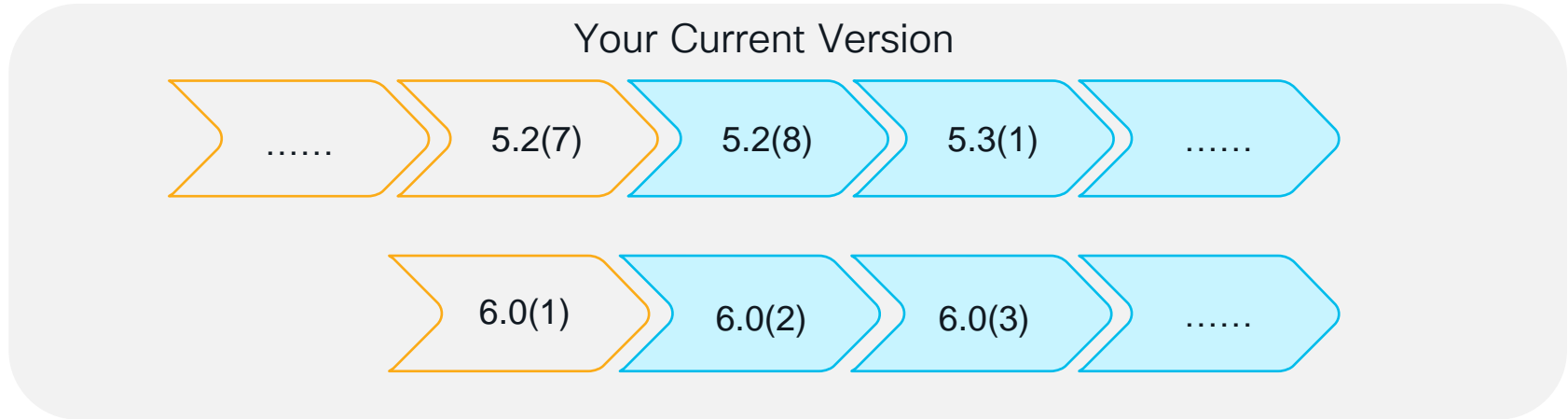
Otherwise: 64 bit

6.0(2):

Fixed per switch model

Upgrade Procedure

When do you upload 64-bit switch images to APICs?



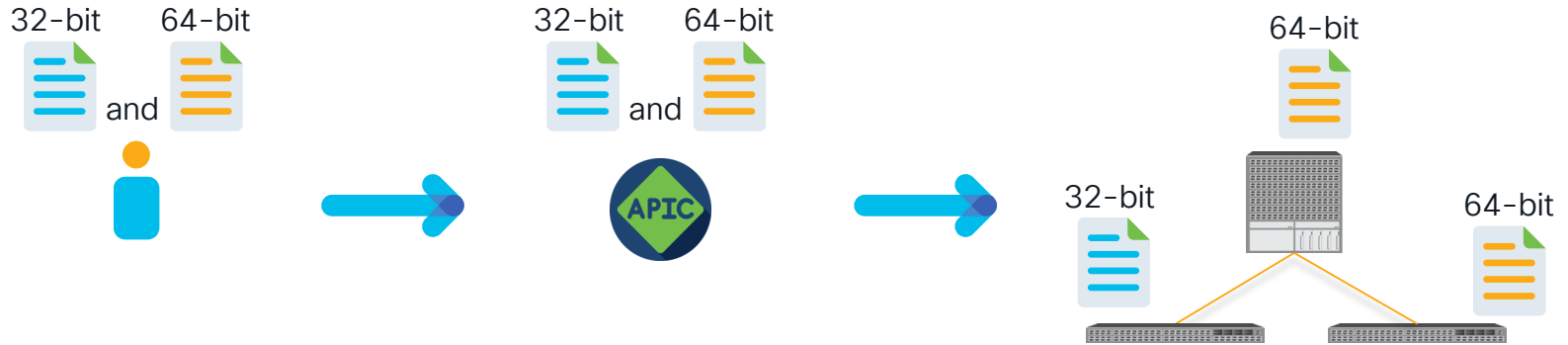
Do not upload the 64-bit image until APICs are upgraded to the [blue versions](#)



Upload the 64-bit image before APICs are upgraded

Upgrade Procedure

Always upload both 32-bit and 64-bit switch images on APICs



Upgrade and Reload

There may be 2 reloads when a switch uses a 64-bit image for the first time

1 APIC picks 32 or 64

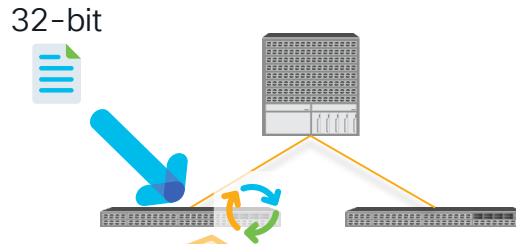
32-bit or 64-bit



APIC checks its internal catalog for the memory options for each switch model.

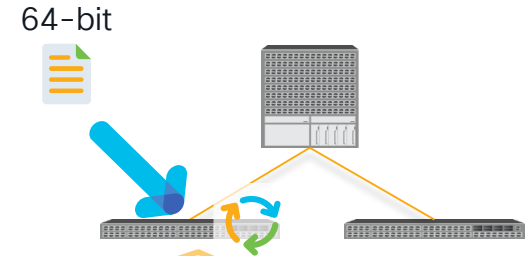
If the switch model can have 24GB or less memory, APIC loads 32-bit image first.

2 Switch Upgrade



Switches upgrade with whichever the image passed by APICs

3 Switch Upgrade Again



Automatically upgrade again with 64-bit with the conditions below:

- The switch has 32GB or more memory
- The switch is running a 32-bit image of 6.0(3) or later

If the switch is already running 64-bit, the next upgrade will use 64-bit directly. No more 2 reloads.



Memory Options

Switch models that can have 24GB or less memory

Product ID	Possible Memory Size
N9K-C9332C	16GB
N9K-C93180LC-EX	24GB
N9K-C93180YC-EX	24GB
N9K-C93108TC-EX	24GB
N9K-C93180YC-FX	24GB or 32GB
N9K-C93108TC-FX	24GB
N9K-C9348GC-FXP	24GB

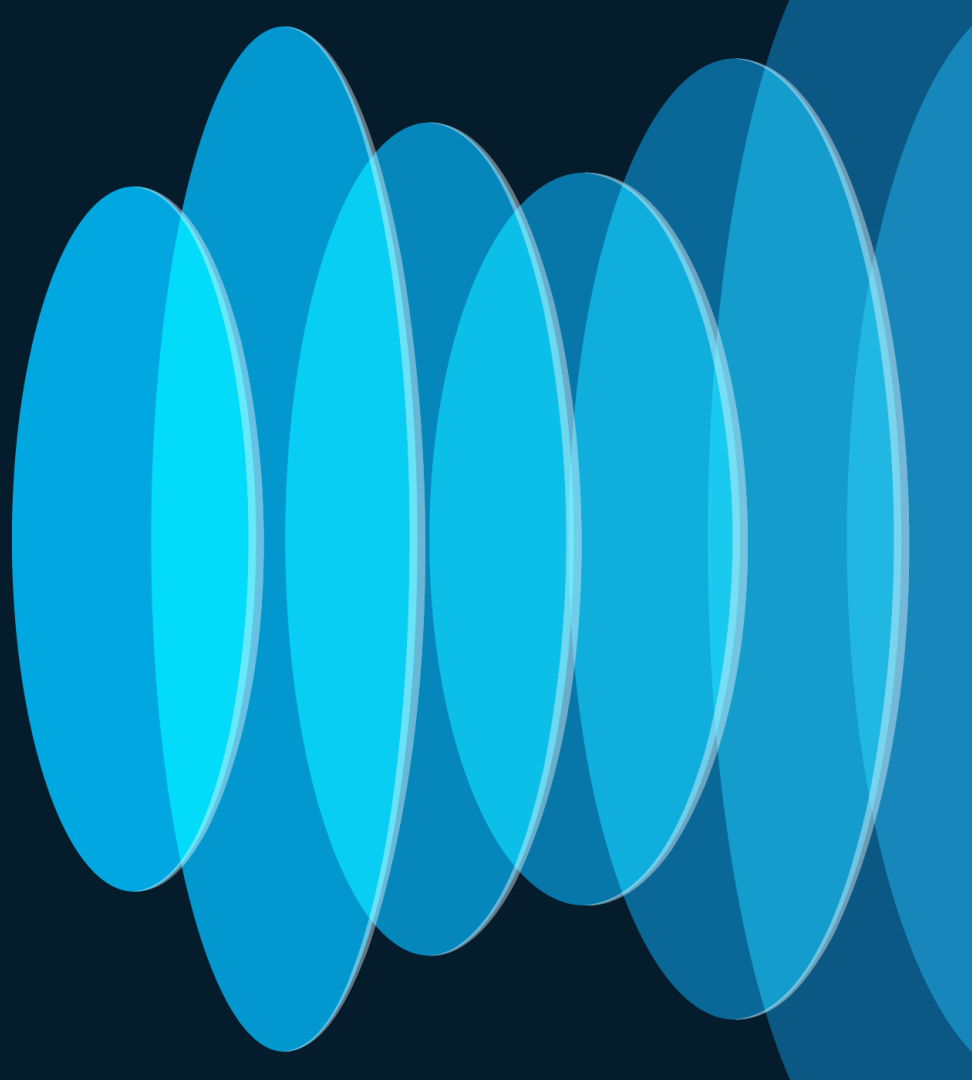
Product ID	Possible Memory Size
N9K-C9336C-FX2	24GB
N9K-C9336C-FX2-E	24GB
N9K-C93216TC-FX2	16GB or 24GB
N9K-C93240YC-FX2	16GB or 24GB
N9K-C93360YC-FX2	16GB or 24GB
N9K-C93180YC-FX3	16GB or 32GB
N9K-C93180YC-FX3H	16GB or 32GB
N9K-C93108TC-FX3H	16GB or 32GB
N9K-C93108TC-FX3P	16GB or 32GB
N9K-C9364C-GX	16GB or 32GB

These switches may reload twice





Note:

This list is based on the internal catalog on APIC running 6.0(5). Subject to change.

Upgrade Enhancements



ACI Upgrade Enhancement Quick Summary

		Supported APIC versions 	4.1(1)	4.2(1)	4.2(5)	5.2(1)	5.2(3)	6.0(2)	6.0(3)	Switch version requirements
Upgrade Time Optimization 	Switch Image Pre-download	✓	✓	✓	✓	✓	✓	✓	✓	14.1(1) or later
	Multi-Pod Parallel Switch Upgrade			✓	✓	✓	✓	✓	✓	No requirements
	Unlimited Parallel Switch Upgrade By Default			✓	✓	✓	✓	✓	✓	No requirements
Visibility 	Faster APIC Data Conversion								✓	N/A
	APIC Detailed Install Stage			✓	✓	✓	✓	✓	✓	N/A
	Switch Image Download Progress			✓	✓	✓	✓	✓	✓	14.5(1) or later
Operation Optimization 	Built-in Pre-Upgrade Validation		✓	✓	✓	✓	✓	✓	✓	No requirements
	Pre-Upgrade Validator App					✓	✓	✓	✓	No requirements
	SMU Support					✓	✓	✓	✓	15.2(1) or later
	Auto EPLD/FPGA upgrade					✓	✓	✓	✓	15.2(1) or later
	NXOS to ACI auto conversion via POAP						✓	✓	✓	15.2(3) or later
	Auto Firmware Update for APIC							✓	✓	N/A
	Auto Firmware Update for switches		✓	✓	✓	✓	✓	✓	✓	No requirements



Upgrade Time Reduction



Switch Image Download
from APIC to switches



Upgrade multiple
pods/switches in parallel

Switch Image Pre-Download with a scheduler 4.1(1)



Schedule Node Upgrade

Group Type: **Switch** vPod

Upgrade Group: Existing **New**

Upgrade Group Name: TMP

Target

Graceful Maintenance:

Run Mode: Do not pause on do not wait on cluster health **Pause upon upgrade failure**

Upgrade Start Time: **Now** Download Image Now and Schedule Upgrade for Later

Scheduler: TMP

All Nodes

ID	Name	Role	Model	Current Firmware	Status
Pod1/1001	F1-P1-Spine-1001	spine	N9K-C9332C	n9000-15.0(1a)	Not Scheduled

New label in ACI 14.2(5).
The functionality of pre-download has been the same since ACI 4.1. Prior to 14.2(5), it was labeled as "Schedule for Later" with the same functionality..

Long time ahead

Name	Date
TMP	2025-05-05T00:00:00.000...

1. Schedule for a long time ahead just to trigger pre-download of a switch image.
2. During the actual maintenance window, come back to this same window (maintenance group) and select "Now" to trigger the upgrade on demand. Switches don't need to re-download images and can proceed with the upgrade immediately.



Switch Image Download Progress

4.2(5)



Firmware

Summary **Infrastructure** Images Faults History

Controllers **Nodes**

Enforce Bootscript Version Validation:
Default Firmware Version:

New in ACI 4.2(5), download progress (switches need to be 14.2(5) for this functionality)

ID	Name	Role	Model	Current Firmware	Upgrade Group	Download Progress	Status	Upgrade Progress
Pod1/1001	f2-spine1	spine	N9K-C9332C	n9000-15.0(0.128)	ALL Target FW: n9000-15.0(0.139b)		30% Firmware upgrade queued with group ALL to...	
Pod1/1002	f2-spine2	spine	N9K-C9332C	n9000-15.0(0.128)	ALL Target FW: n9000-15.0(0.139b)		30% Firmware upgrade queued with group ALL to...	
Pod1/101	f2-leaf1	leaf	N9K-C93180YC-FX	n9000-15.0(0.128)	ALL Target FW: n9000-15.0(0.139b)		30% Firmware upgrade queued with group ALL to...	
Pod1/102	f2-leaf2	leaf	N9K-C93180YC-FX	n9000-15.0(0.128)	ALL Target FW: n9000-15.0(0.139b)		30% Firmware upgrade queued with group ALL to...	
Pod1/103	f2-leaf3	leaf	N9K-C93240YC-FX2	n9000-15.0(0.128)	ALL Target FW: n9000-15.0(0.139b)		30% Firmware upgrade queued with group ALL to...	
Pod1/104	f2-leaf4	leaf	N9K-C93240YC-FX2	n9000-15.0(0.128)	ALL Target FW: n9000-15.0(0.139b)		30% Firmware upgrade queued with group ALL to...	

- All switches (regardless of pods or vPC) in the update group download the switch image from APICs in parallel. During this period, the Upgrade Progress remains 0 %.
- **With the new Download Progress bar, users can see whether switches finished the download and ready to upgrade.**
- If it was triggered with a scheduler, all switches wait after they completed their download.
- If it was triggered with “Upgrade Now”, each switch proceed with the upgrade as soon as it has completed its download.

Switch Image Pre-Download (built-in)

5.1(1)



Update Settings

Name: ODD Target Version: n9000-16.0(1.363)

Selected Switches To Update

3

- Leafs 2
- Spines 1

Selected Switches To Update

Filter by attributes

Pod	ID	Name	Role	Model	Version	Last Update
1	101	f2-leaf1	Leaf	N9K-C93180YC-FX	n9000	
2	103	f2-leaf3	Leaf	N9K-C93240YC-FX	n9000	
1	1001	f2-spine1	Spine	N9K-C9332C	n9000	

10 Rows Page 1 of 1 <<< 1-3 of 3 >>>

Cancel Previous **Begin Download**

Pre-Download is built-in

Installation will not start until you manually trigger installation after the download has completed.

Switch Image Download Progress

5.1(1)



Update Details

Target Version
n9000-16.0(1.363)

Switches by Role

- Leaves: 2
- Spines: 1

Switch Reboot Required ⓘ
Not Applicable

Overall Status
Downloading

Status Breakdown

- Failed: 0
- Decommissioned: 0
- Unreachable: 0
- Downloading: 3
- Other: 0

3

Switches

Filter by attributes

Pod	Switch ID	Name	Role	Model	Last Update	Current Version	SMU Version	Status
1	1001	f2-spine1	spine	N9K-C9332C	2023-01-25T1	n9000-16.0(1.	-	Downloading (30%)
1	101	f2-leaf1	leaf	N9K-C93180Y	2023-01-25T1	n9000-16.0(1.	-	Downloading (20%)

20 Rows

Page 1 of 1 << 1-3 of 3 >>

Progress of each step (download and install)

Switch Image Download Progress

(APIC 4.2(5), Switch 14.2(4))



Firmware

Summary Infrastructure Images Faults History

Controllers Nodes

Enforce Bootscript Version Validation:

Remain empty

ID	Name	Role	Model	Current Firmware	Upgrade Group	Download Progress	Status	Upgrade Progress
Pod1/1001	F3-P1-Spine-1001	spine	N9K-C9364C	n9000-14.2(4i)	ALL Target FW: n9000-15.0(1i)		Firmware upgrade queued with group ALL t...	0%
Pod1/1002	F3-P1-Spine-1002	spine	N9K-C9364C	n9000-14.2(4i)	ALL Target FW: n9000-15.0(1i)		Firmware upgrade queued with group ALL t...	0%
Pod1/101	F3-P1-Leaf-101	leaf	N9K-C93180YC-EX	n9000-14.2(4i)	ALL Target FW: n9000-15.0(1i)		Firmware upgrade queued with group ALL t...	0%
Pod1/111	F3-P1-RL-111	leaf	N9K-C9336C-FX2	n9000-14.2(4i)	ALL Target FW: n9000-15.0(1i)		Firmware upgrade queued with group ALL t...	0%
Pod2/2001	F3-P2-Spine-2001	spine	N9K-C9504	n9000-14.2(4i)	ALL Target FW: n9000-15.0(1i)		Firmware upgrade queued with group ALL t...	0%
Pod2/2002	F3-P2-Spine-2002	spine	N9K-C9504	n9000-14.2(4i)	ALL Target FW: n9000-15.0(1i)		Firmware upgrade queued with group ALL t...	0%
Pod2/201	F3-P2-Leaf-201	leaf	N9K-C93180YC-EX	n9000-14.2(4i)	ALL Target FW: n9000-15.0(1i)		Firmware upgrade queued with group ALL t...	0%
Pod2/202	F3-P2-Leaf-202	leaf	N9K-C93180YC-EX	n9000-14.2(4i)	ALL Target FW: n9000-15.0(1i)		Firmware upgrade queued with group ALL t...	0%
Pod2/211	F3-P2-RL-211	leaf	N9K-C93180YC-EX	n9000-14.2(4i)	ALL Target FW: n9000-15.0(1i)		Firmware upgrade queued with group ALL t...	0%
Pod2/212	F3-P2-RL-212	leaf					unknown	

Download Progress will not be displayed when switches are older than 14.2(5) even if APIC is 4.2(5) or later

Upgrade multiple pods/switches in parallel



Summary Infrastructure Images Faults History

Controllers Nodes

Enforce Bootscript Version Validation:

One pod at a time

Upgrade Progress

Pod ID	Progress	Percentage
Pod1/101	<div style="width: 60%;"></div>	60%
Pod1/111	<div style="width: 60%;"></div>	60%
Pod2/201	<div style="width: 0%;"></div>	0%
Pod2/211	<div style="width: 0%;"></div>	0%
Pod1/1001	<div style="width: 60%;"></div>	60%
Pod2/2001	<div style="width: 0%;"></div>	0%
Pod2/202	<div style="width: 0%;"></div>	0%
Pod2/212	<div style="width: 0%;"></div>	0%

ID	Name	Role	Model	Current Firmware	Upgrade Group	Status	Upgrade Progress
Pod1/101	F3-P1-Leaf-101	leaf	N9K-C93180YC-EX	n9000-14.1(2g)	ODD Target FW: n9000-14.1(2x)	Firmware upgrade in progress with group ODD to desired version n9000-14.1(2x)	<div style="width: 60%;"></div> 60%
Pod1/111	F3-P1-RL-111	leaf	N9K-C9336C-FX2	n9000-14.1(2g)	ODD Target FW: n9000-14.1(2x)	Firmware upgrade in progress with group ODD to desired version n9000-14.1(2x)	<div style="width: 60%;"></div> 60%
Pod2/201	F3-P2-Leaf-201	leaf	N9K-C93180YC-EX	n9000-14.1(2g)	ODD Target FW: n9000-14.1(2x)	Firmware upgrade queued with group ODD to desired version n9000-14.1(2x)	<div style="width: 0%;"></div> 0%
Pod2/211	F3-P2-RL-211	leaf	N9K-C93180YC-EX	n9000-14.1(2g)	ODD Target FW: n9000-14.1(2x)	Firmware upgrade queued with group ODD to desired version n9000-14.1(2x)	<div style="width: 0%;"></div> 0%
Pod1/1001	F3-P1-Spine-1001	spine	N9K-C9364C	n9000-14.1(2g)	ODD Target FW: n9000-14.1(2x)	Firmware upgrade in progress with group ODD to desired version n9000-14.1(2x)	<div style="width: 60%;"></div> 60%
Pod2/2001	F3-P2-Spine-2001	spine	N9K-C9504	n9000-14.1(2g)	ODD Target FW: n9000-14.1(2x)	Firmware upgrade queued with group ODD to desired version n9000-14.1(2x)	<div style="width: 0%;"></div> 0%
Pod2/202	F3-P2-Leaf-202	leaf	N9K-C93180YC-EX	n9000-14.1(2g)		Not Scheduled	<div style="width: 0%;"></div> 0%
Pod2/212	F3-P2-RL-212	leaf	N9K-C93180YC-EX	n9000-14.1(2g)		Not Scheduled	<div style="width: 0%;"></div> 0%

When the actual upgrade starts, APICs allow each switch to upgrade based on the following rules;

- One Pod at a time (14.2(5) has an update)
- When triggered with “Upgrade Now”, 20 switches at a time (14.2(5) has an update)
- When a vPC pair leaf nodes are in the same group, only one of the pair at a time



Unlimited Parallel Upgrade

4.2(5)



All pods at once

Firmware

Summary Infrastructure Images Faults History

Controllers Nodes

Enforce Bootscript Version Validation:

ID	Name	Role	Model	Current Firmware	Upgrade Group	Download Progress	Status	Upgrade Progress
Pod1/1001	F3-P1-Spine-1001	spine	N9K-C9364C	n9000-14.2(4i)	ALL Target FW: n9000-15.0(1i)		Firmware upgrade in progress with group A...	45%
Pod1/1002	F3-P1-Spine-1002	spine	N9K-C9364C	n9000-14.2(4i)	ALL Target FW: n9000-15.0(1i)		Firmware upgrade in progress with group A...	45%
Pod1/101	F3-P1-Leaf-101	leaf	N9K-C93180YC-EX	n9000-14.2(4i)	ALL Target FW: n9000-15.0(1i)		Firmware upgrade in progress with group A...	45%
Pod1/111	F3-P1-RL-111	leaf	N9K-C9336C-FX2	n9000-14.2(4i)	ALL Target FW: n9000-15.0(1i)		Firmware upgrade in progress with group A...	45%
Pod2/2001	F3-P2-Spine-2001	spine	N9K-C9504	n9000-14.2(4i)	ALL Target FW: n9000-15.0(1i)		Firmware upgrade in progress with group A...	45%
Pod2/2002	F3-P2-Spine-2002	spine	N9K-C9504	n9000-14.2(4i)	ALL Target FW: n9000-15.0(1i)		Firmware upgrade in progress with group A...	45%
Pod2/201	F3-P2-Leaf-201	leaf	N9K-C93180YC-EX	n9000-14.2(4i)	ALL Target FW: n9000-15.0(1i)		Firmware upgrade in progress with group A...	45%
Pod2/202	F3-P2-Leaf-202	leaf	N9K-C93180YC-EX	n9000-14.2(4i)	ALL Target FW: n9000-15.0(1i)		Firmware upgrade in progress with group A...	45%
Pod2/211	F3-P2-RL-211	leaf	N9K-C93180YC-EX	n9000-14.2(4i)	ALL Target FW: n9000-15.0(1i)		Firmware upgrade in progress with group A...	45%
Pod2/212	F3-P2-RL-212	leaf					unknown	

- From APIC 14.2(5) or later, any switches in any pods can be upgraded in parallel
- “Upgrade Now” is no longer limited to 20 switches at a time





Agenda

- Upgrade Architecture
 - ACI Firmware Upgrade Types
 - Upgrade Architecture – APIC
 - Upgrade Architecture – Switches
 - (Bonus) Upgrade Enhancements
- Best Practices
 - Best Practices Workflow Review
 - Best Practices Configurations
 - “Pre-Upgrade Validation” Review and Execution
 - “Do’s and Don’ts”

Recommended Guides

Cisco ACI Upgrade Checklist – Important Starting Point



ACI Upgrade Checklist:

<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/Cisco-ACI-Upgrade-Checklist.html>

Detailed Upgrade Guide (the basis for this presentation)

<https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/all/apic-installation-aci-upgrade-downgrade/Cisco-APIC-Installation-ACI-Upgrade-Downgrade-Guide.html>

Cisco ACI Upgrade Checklist

	Task
<input type="checkbox"/>	Pick your target APIC and ACI switch versions. <ul style="list-style-type: none"> Both APICs and ACI switches must be upgraded to the same version. APIC and ACI switch versions that are compatible to each other are described in the form of x.y(z) and 1x.y(z). For instance, APIC version 5.2(1g) corresponds to ACI switch version 15.2(1g). Check the Release Notes (APIC and ACI switches) for the target version for any open caveats or defects.
<input type="checkbox"/>	See the APIC Upgrade/Downgrade Support Matrix for the supported upgrade paths from your current version. <ul style="list-style-type: none"> If your current version and the target version are too far apart, you might need to upgrade both your APICs and switches to an intermediate version suggested in the APIC Upgrade/Downgrade Support Matrix first. See Multistep Upgrades in the Cisco APIC Installation and ACI Upgrade and Downgrade Guide for more information. The APIC Upgrade/Downgrade Support Matrix also shows you which CIMC version you need to use for your target APIC version.
<input type="checkbox"/>	Review the ACI upgrade architecture. See ACI Upgrade Architecture in the Cisco APIC Installation and ACI Upgrade and Downgrade Guide to understand what you should expect along with what you must not perform.
<input type="checkbox"/>	Export your configuration for backup. See the Cisco ACI Configuration Files: Import and Export document for details. Ensure that AES encryption is enabled.
<input type="checkbox"/>	Disable all App Center apps on the APICs. See Guidelines for App Center Apps in the Cisco APIC Installation and ACI Upgrade and Downgrade Guide for details.
<input type="checkbox"/>	Download both APIC and ACI switch firmware to your APICs. See the Downloading APIC and Switch Images on APICs section in the Cisco APIC Installation and ACI Upgrade and Downgrade Guide for each release for details: <ul style="list-style-type: none"> Releases prior to 4.x: Downloading APIC and Switch Images on APICs Releases 4.x or 5.0: Downloading APIC and Switch Images on APICs Release 5.1 or later: Downloading APIC and Switch Images on APICs
<input type="checkbox"/>	Download ACI switch firmware from your APICs to each switch. Starting from switch release 14.1(1), switches can download the image from APICs prior to the upgrade. See Rule 5 – Save time by downloading switch images beforehand in the Cisco APIC Installation and ACI Upgrade and Downgrade Guide for details.
<input type="checkbox"/>	Perform pre-upgrade validations. See Pre-Upgrade Checklists in the Cisco APIC Installation and ACI Upgrade and Downgrade Guide for details.
<input type="checkbox"/>	Upgrade CIMC on your APICs if suggested so by the Support Matrix. See Upgrading the CIMC Software in the Cisco APIC Installation and ACI Upgrade and Downgrade Guide for details.
<input type="checkbox"/>	Upgrade APICs. See the Upgrading the Cisco APIC section in the Cisco APIC Installation and ACI Upgrade and Downgrade Guide for each release for details: <ul style="list-style-type: none"> Releases prior to 4.x: Upgrading the Cisco APIC from Releases Prior to Release 4.x Releases 4.x or 5.0: Upgrading the Cisco APIC From Releases 4.x or 5.0 Release 5.1 or later: Upgrading the Cisco APIC From Releases 5.1x or Later

ACI Firmware Upgrade Best Practice Checklist

- ✓ Determine Desired Software and Check Support Matrix
- ✓ Review and Implement Best Practice Configurations
- ✓ Discover and Clear any issues raised from “pre-upgrade validations”
- ✓ Review Upgrade Architecture and “do’s and don’ts”

ACI Software Life Cycle

1

Cisco Recommended Software Releases

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/recommended-release/b_Recommended_Cisco_ACI_Releases.html

2

Cisco ACI Release Notes

<https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>

3

Cisco ACI Upgrade/Downgrade Support Matrix

<https://www.cisco.com/c/dam/en/us/td/docs/Website/datacenter/apicmatrix/index.html>

4



APIC Upgrade/Downgrade Support Matrix

This page provides Cisco APIC software upgrade and downgrade information based on current and target releases. The provided upgrade paths have been tested and validated by Cisco, Cisco partners, or both.

For an overview of the entire fabric upgrade process, including relevant reference and procedure documents, see the [Cisco ACI Upgrade Checklist](#).

For feedback on this tool, send email to apic-docfeedback@cisco.com.

I am upgrading... I am downgrading...

From release

To release

Current release: 3.2(10)

Target release: 4.2(7) [[↗](#)]

Recommended path: Direct path from Current Release. [[Show All](#)]

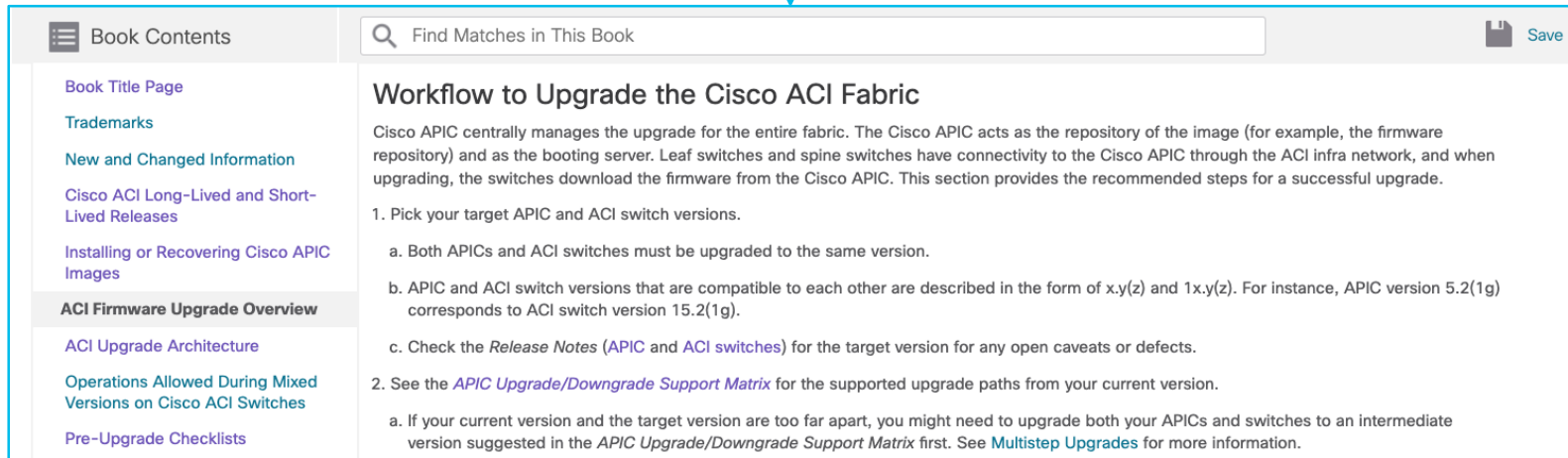
Determines if Multi-Step Upgrade is Required

ACI Upgrade Overview

5

Review the ACI Upgrade/Downgrade Guide!

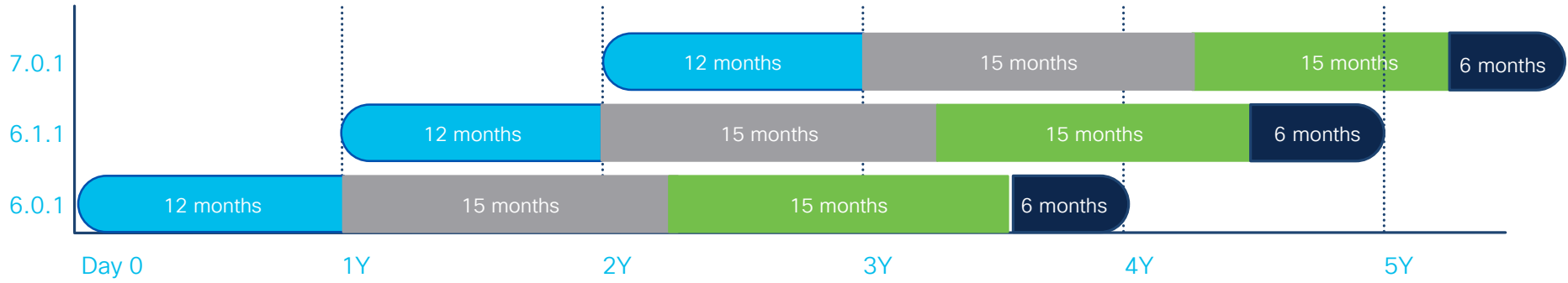
https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/all/apic-installation-aci-upgrade-downgrade/Cisco-APIC-Installation-ACI-Upgrade-Downgrade-Guide/m-aci-firmware-upgrade-overview.html#id_48185



The screenshot shows a web interface for a Cisco document. On the left is a navigation menu with items like 'Book Contents', 'Book Title Page', 'Trademarks', 'New and Changed Information', 'Cisco ACI Long-Lived and Short-Lived Releases', 'Installing or Recovering Cisco APIC Images', 'ACI Firmware Upgrade Overview' (highlighted), 'ACI Upgrade Architecture', 'Operations Allowed During Mixed Versions on Cisco ACI Switches', and 'Pre-Upgrade Checklists'. The main content area has a search bar at the top with the text 'Find Matches in This Book' and a 'Save' button. Below the search bar is the title 'Workflow to Upgrade the Cisco ACI Fabric'. The text describes the role of the Cisco APIC in managing upgrades and lists two main steps: 1. Pick your target APIC and ACI switch versions, and 2. See the APIC Upgrade/Downgrade Support Matrix for supported upgrade paths. Step 1 includes sub-points about version compatibility and checking release notes. Step 2 includes a note about upgrading to an intermediate version if the target is too far away.

New Release Cadence

Key objectives | Predictable software release cadence | Reach maintenance mode quickly



Legend

- Development cycle
- Maintenance cycle
- Extended support with PSIRT fixes
- TAC support

No short-lived and long-lived release tags | Three feature releases from FCS date, including FCS release | Fourth release is a maintenance release (MR), target for golden star | Hardware lifecycle is defined by multiple release and not tied to a single release | Total release lifecycle of four years

CIMC Version Compatibility

6

Option 1: Support Matrix <https://www.cisco.com/c/dam/en/us/td/docs/Website/datacenter/apicmatrix/index.html>

APIC Software Upgrade/Downgrade Support Matrix

This page provides Cisco APIC software upgrade and downgrade information based on current and target releases. The provided upgrade paths have been tested and validated by Cisco, Cisco partners, or both.

For an overview of the entire fabric upgrade process, including relevant reference and procedure documents, see the [Cisco ACI Upgrade Checklist](#).

For feedback on this tool, send email to apic-docfeedback@cisco.com.

I am upgrading... I am downgrading...

From release

To release



Recommended software for target release:

This is a list of **recommended** releases, not the only supported releases for your target APIC release. Check the specific software's *Release Notes* and documentation for other release versions supported for your target APIC release.

- Cisco NX-OS ACI-mode version: 15.2(7)
- Cisco Nexus Dashboard Orchestrator: 3.7(2g)
- Cisco ACI Virtual Edge version: 3.2(4b)
- Cisco IMC version: UCS C220/C240 M5 (APIC-L3/M3): 4.1(3f); UCS C220/C240 M4 (APIC-L2/M2): 4.1(2g); UCS C220/C240 M3 (APIC-L1/M1): 3.0(4l)
- Canonical version: Ussuri

Option 2: APIC Release Note <https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>

Release Notes

Cisco APIC Release Notes

- [Cisco Application Policy Infrastructure Controller Release Notes, Release 6.0\(2\)](#)
- [Cisco Application Policy Infrastructure Controller Release Notes, Release 6.0\(1\)](#)
- [Cisco Application Policy Infrastructure Controller Release Notes, Release 5.2\(7\)](#)
- [Cisco Application Policy Infrastructure Controller Release Notes, Release 5.2\(6\)](#)



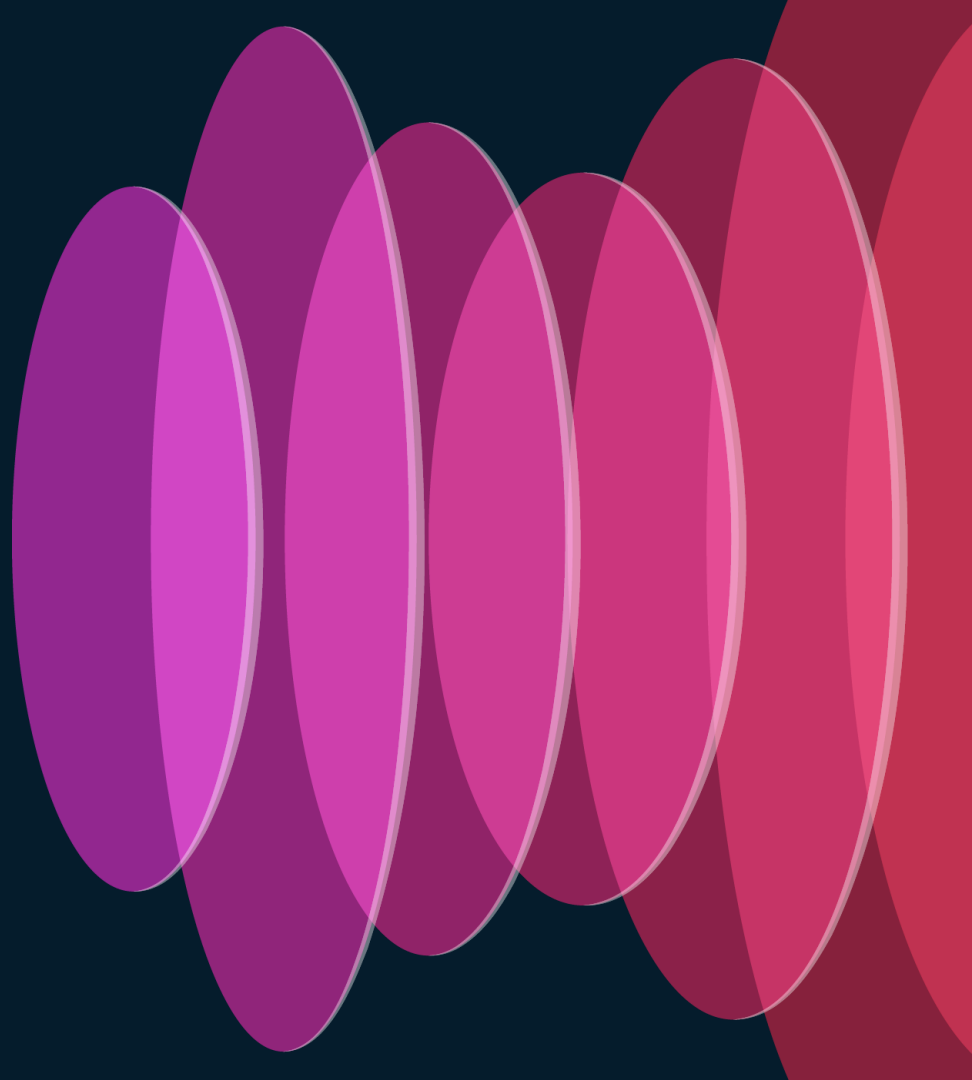
CIMC HUU ISO

- 4.2(3b) CIMC HUU ISO (recommended) for UCS C220/C240 M5 (APIC-L3/M3)
- 4.2(2a) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)
- 4.1(3f) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)
- 4.1(3d) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)
- 4.1(3c) CIMC HUU ISO for UCS C220/C240 M5 (APIC-L3/M3)
- 4.1(2k) CIMC HUU ISO (recommended) for UCS C220/C240 M4 (APIC-L2/M2)

ACI Firmware Upgrade Best Practice Checklist

- ✓ Determine Desired Software and Check Support Matrix
- ✓ Review and Implement Best Practice Configurations
- ✓ Discover and Clear any issues raised from “pre-upgrade validations”
- ✓ Review Upgrade Architecture and “do’s and don’ts”

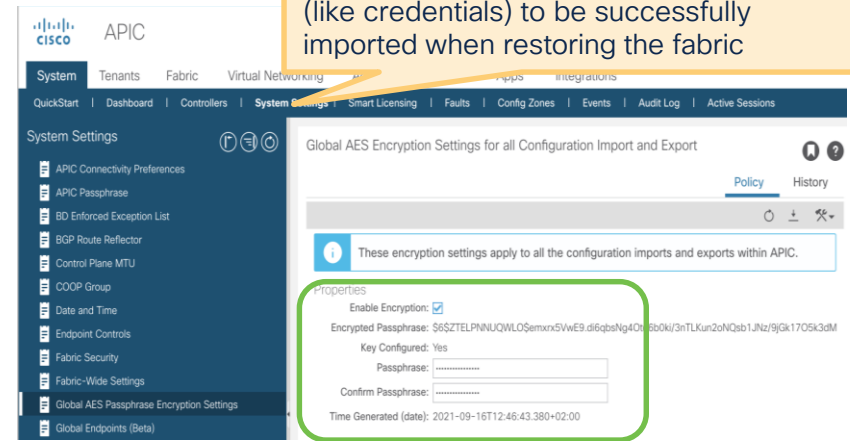
Back Up Configuration



Back Up Configuration with AES File Encryption

- The AES passphrase that generates the encryption keys cannot be recovered or read by an ACI administrator or any other user. The AES passphrase is not stored. **Copy your passphrase somewhere safe!**
- Setup automatic backups on a scheduler to maintain a consist and up to date backup at all times. **Always export it to a remote location.**
- In case of upgrade failure, AES backup can be used to **recover the system non-disruptively** as worst case scenario.

Setting Global AES Encryption allows all the secure properties of the configuration (like credentials) to be successfully imported when restoring the fabric



APIC

System Tenants Fabric Virtual Networking Apps Integrations

QuickStart | Dashboard | Controllers | System Settings | Smart Licensing | Faults | Config Zones | Events | Audit Log | Active Sessions

System Settings

Global AES Encryption Settings for all Configuration Import and Export

Policy History

These encryption settings apply to all the configuration imports and exports within APIC.

Properties

Enable Encryption:

Encrypted Passphrase: \$6\$ZTELPINUQWLO\$emrx5VwE9.dI6qbsNg40sBb0ki/3nTLKun2oNQsb1.Niz/9JGk1705k3dM

Key Configured: Yes

Passphrase:

Confirm Passphrase:

Time Generated (date): 2021-09-16T12:46:43.380+02:00

Pre ACI v4.0.1 Setting Location:

Admin > AAA > AES Encryption Passphrase and Keys for Config Export (and Import)

ACI v4.0.1 and later Location:

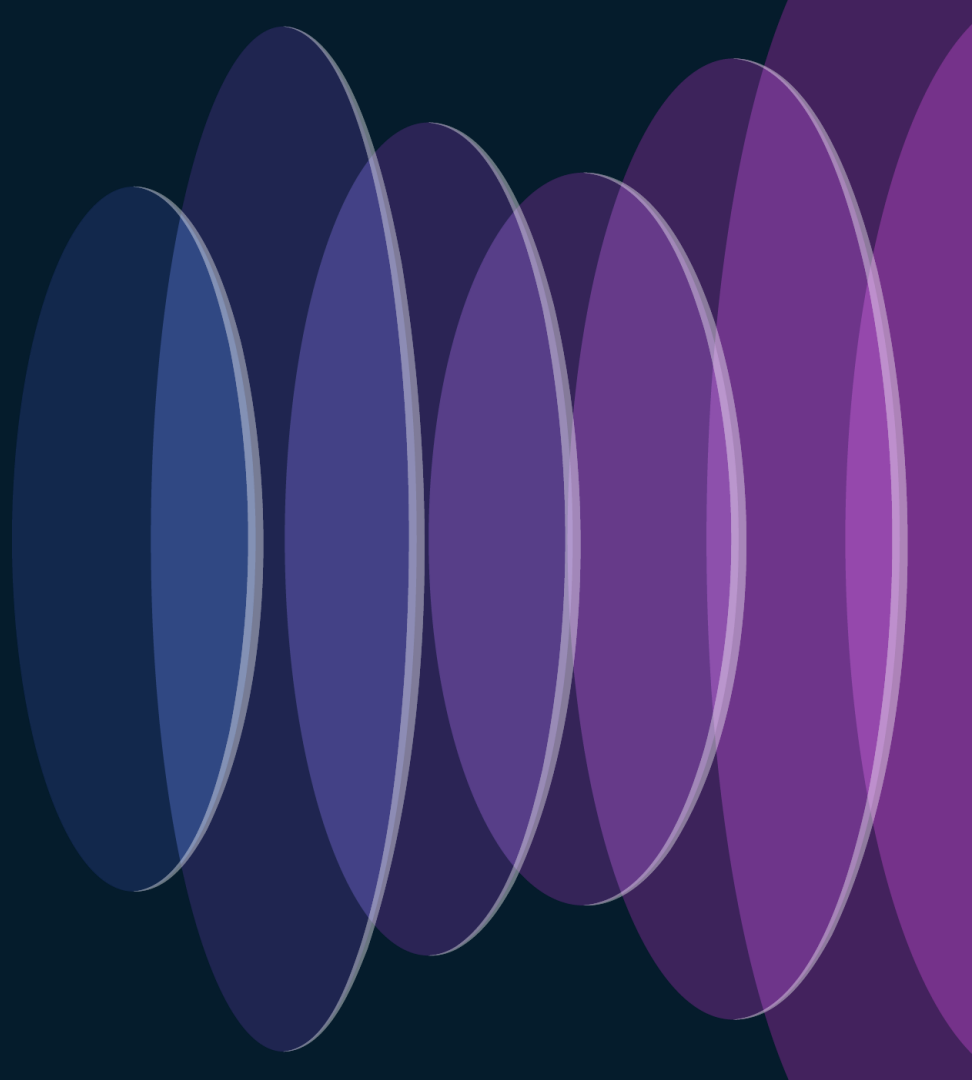
System > System Settings > Global AES Passphrase Encryption Settings

Technote For Import/Export:

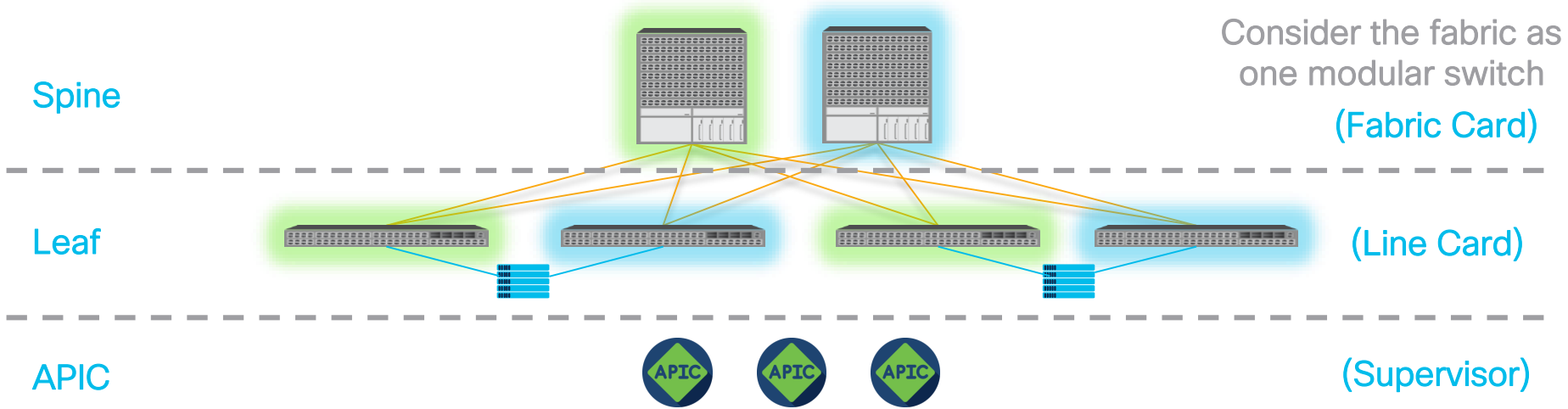
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b_KB_Using_Import_Export_to_Recover_Config_States.html

CISCO Live!

Switch Upgrade Groups



ACI Firmware Upgrade Best Practice 101



ACI is a solution to manage multiple switches as if it's one huge switch

- APIC (i.e. SUP of the fabric) can be upgraded non-disruptively.
- Each switch (i.e. modules of the fabric) can intelligently choose appropriate switch nodes for non-disruptive traffic flow

Always keep hardware redundancy to achieve zero-to-minimum traffic disruption

1. Upgrade **Green** switch groups
2. Upgrade **Blue** switch groups

Switch Upgrade Advanced Options

Upgrade Group

- Name
- Node ID List
- Target Firmware Version
- Scheduler
- Ignore Compatibility Check
- Graceful option
- Run Mode

Rule of Thumb

Change defaults only when you must.

- **Compatibility Check** (default: Enforced)
Only unenforce in a lab where you would like to ignore the supported upgrade path.
- **Graceful Upgrade** (default: Unenforced)
Only enforce when sub-100ms routing protocol convergence is required.
Never enforce this when hardware redundancy is lacking. (single spine/leaf pod)
- **Run Mode** (default < 5.1: pause upon upgrade failure
(default >= 5.1: don't pause upon upgrade failure)
By default, APIC scheduler will stop putting new switches into queue if
 - a) APIC cluster is not fully-fit
 - b) The upgrade of previous switches in the same upgrade group failed.Ex.) You have 20 leaves in a group. If 1 fails, it will pause all remaining switches that are still queued. If other 19 leaves already started upgrade procedure, those will not be paused.

Later Releases, ie: 5.2

Edit > Version Selection > Advanced Settings

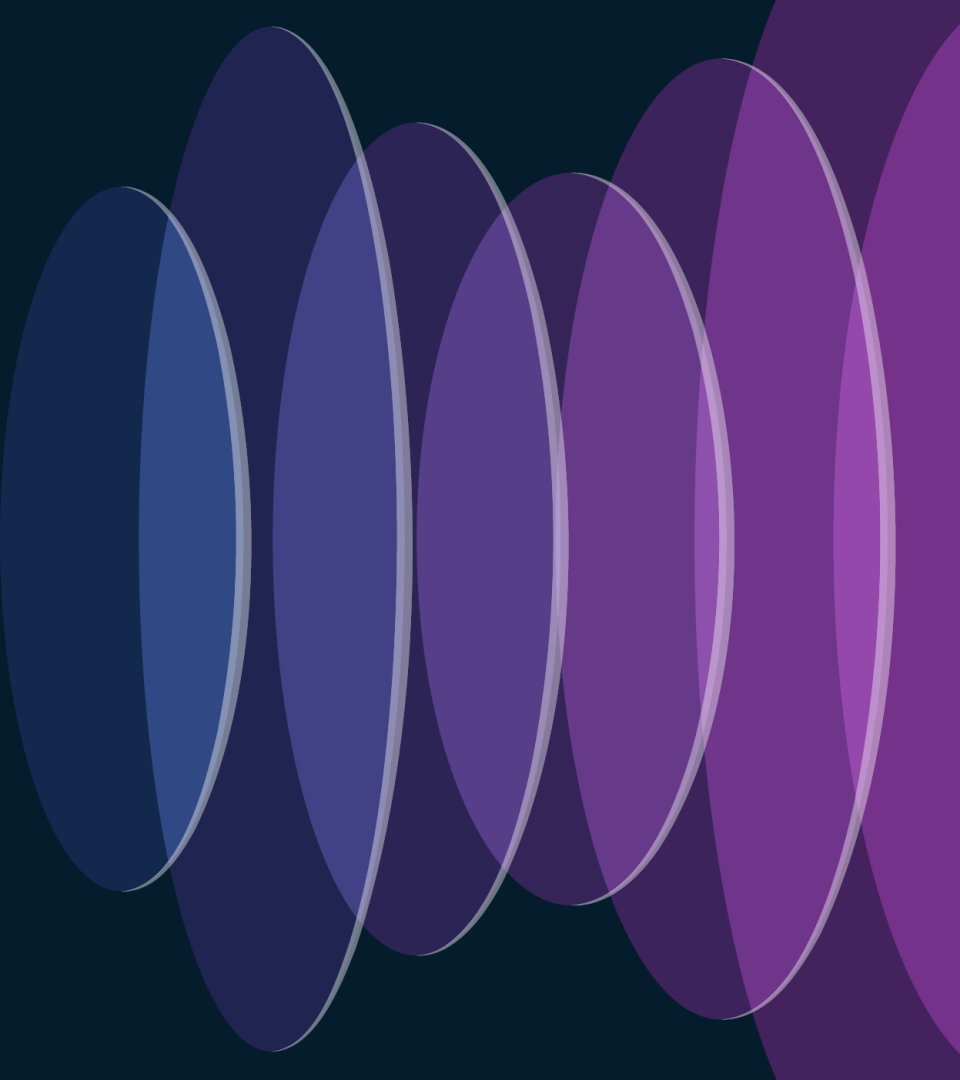
Advanced Settings

Compatibility Check
 Enforced Unenforced

Graceful Upgrade
 Enforced Unenforced

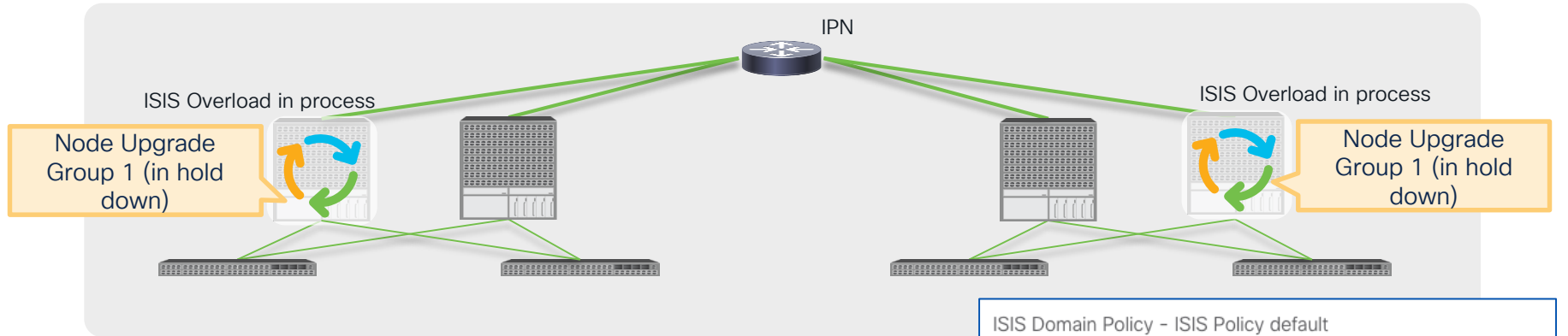
Run Mode
 Do not pause on failure & cluster health Pause upon upgrade failure

IS-IS Metric Policy for Multi-Pod and Multi-Site

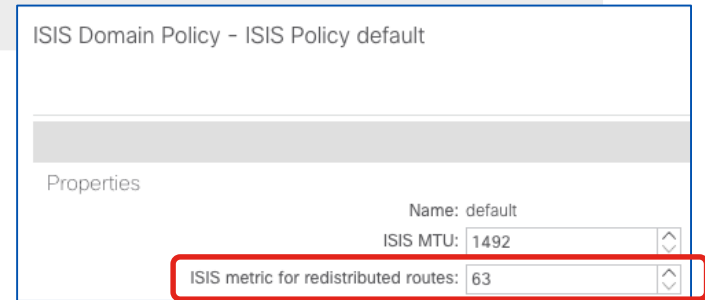


Helpful Tips for Multi-Pod / Multi-Site

ISIS Metric Policy Configuration



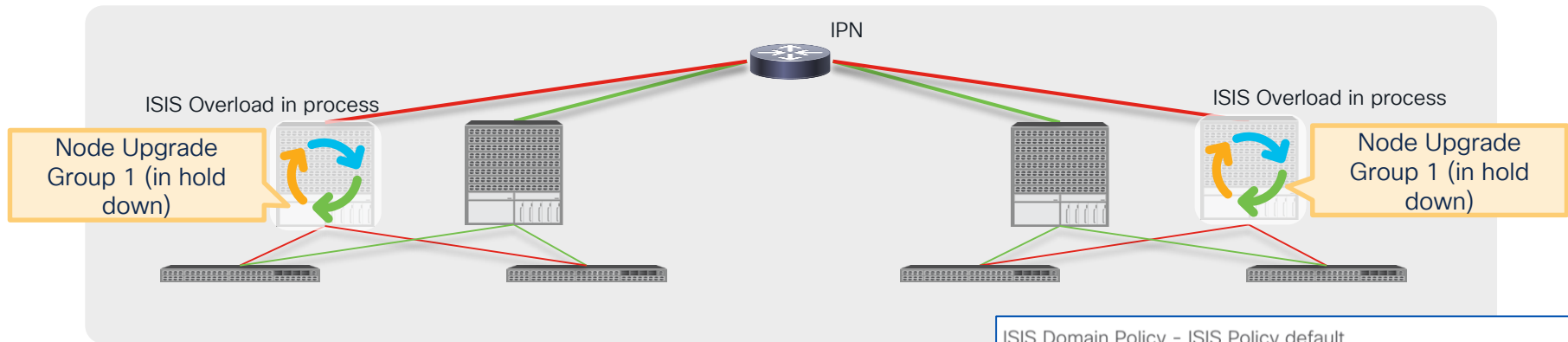
- Default fabric wide IS-IS metric is set at 63 (max value)
- During upgrade, spines set the overload mode while policy is being downloaded.
- If fabric-wide value is already at max, the overload functionality is ineffective.
- This can create unexpected traffic interruption if leaf sends traffic to a spine which is not fully upgraded.



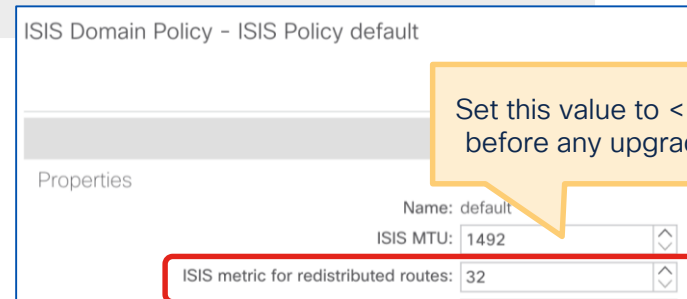
Settings > ISIS Policy (Default Config)

Helpful Tips for Multi-Pod / Multi-Site

ISIS Metric Policy Configuration



- By Lowering the Value, Remote POD TEP Routes will be preferred through the remaining spines in each POD.
- Once Overload is completed, the spine which was upgraded will advertise these routes using the metric configured.
- This results in ECMP between all spines after the upgrade has completed.

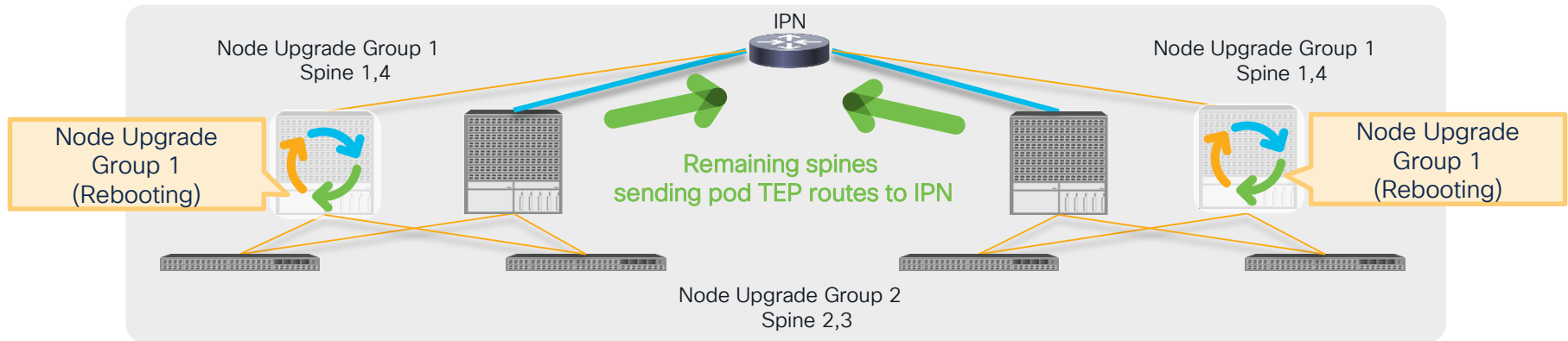


Settings > ISIS Policy

Helpful Tips for Multi-Pod / Multi-Site



Verify Spines are Exchanging Routes to the IPN after upgrade



- When Node Upgrade Group 1 finishes, Spines may show as “completed” in upgrade UI but routes towards IPN/ISN may still be in hold down period (up to 10 min)
- Before starting Spine Node Upgrade Group 2, verify that TEP routes of pods / sites are being sent / received from newly upgraded spines in Group 1

Helpful Tips for Multi-Pod / Multi-Site

Verify Spines are Exchanging Routes to the IPN after upgrade



System Tenants **Fabric** Virtual Networking L4-L7 Service: System Tenants **Fabric** Virtual Networking L4-L7 Services Admin Operations Apps Integrations

Inventory | Fabric Policies | Access Policies

Inventory

- Quick Start
- Topology
- Pod 1
 - s1-pod1-leaf101 (Node-101)
 - s1-pod1-leaf102 (Node-102)
 - s1-pod1-leaf103 (Node-103)
 - s1-pod1-leaf104 (Node-104)
 - s1-pod1-spine201 (Node-201)
 - Chassis
 - Interfaces
 - Protocols
 - BGP
 - COOP
 - IPV4
 - IPV6
 - ISIS
 - LLDP
 - OSPF
 - OSPF for VRF-overlay-1
 - Areas
 - Interfaces
 - Routes

Pod Fabric Setup Policy

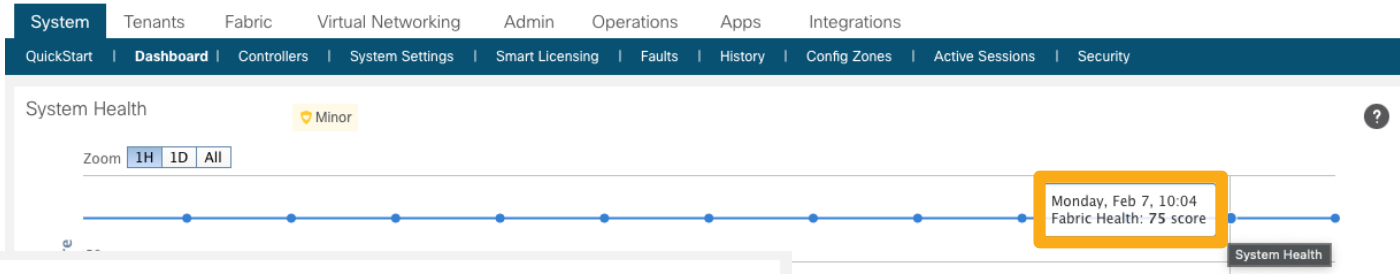
Pod ID	TEP Pool	Admin Distance
1	10.0.0.0/16	110
2	14.0.0.0/16	110

Route	Flags	Unicast Cost	Next Hop	Interface	Admin Distance
Route 20.0.0.37/32	in-rib,v4	3	20.0.0.37/32	intra backbone in-rib,v4	110
Route 20.0.0.36/32	in-rib,v4	3	20.0.0.36/32	intra backbone in-rib,v4	110
Route 20.0.0.1/32	in-rib,v4	20	20.0.0.1/32	ext2 backbone in-rib,v4	110
Route 20.0.0.0/16	in-rib,v4	20	20.0.0.0/16	ext2 backbone in-rib,v4	110
Route 2.2.2.2/32	direct,v4	1	2.2.2.2/32	intra backbone direct,v4	110
Route 172.16.22.230/32	v4	20	172.16.22.230/32	ext2 backbone v4	110
Route 172.16.22.229/32	v4	20	172.16.22.229/32	ext2 backbone v4	110
Route 172.16.22.225/32	v4	20	172.16.22.225/32	ext2 backbone v4	110
Route 172.16.22.0/24	v4	20	172.16.22.0/24	ext2 backbone v4	110
Route 14.0.240.32/32	in-rib,v4	3	14.0.240.32/32	intra backbone in-rib,v4	110
Route 14.0.0.35/32	in-rib,v4	20	14.0.0.35/32	ext2 backbone in-rib,v4	110
Route 14.0.0.34/32	in-rib,v4	20	14.0.0.34/32	ext2 backbone in-rib,v4	110
Route 14.0.0.33/32	in-rib,v4	20	14.0.0.33/32	ext2 backbone in-rib,v4	110
Route 14.0.0.0/16	in-rib,v4	20	14.0.0.0/16	ext2 backbone in-rib,v4	110
Route 10.255.6.201/32	in-rib,v4	3	10.255.6.201/32	intra backbone in-rib,v4	110

ACI Firmware Upgrade Best Practice Checklist

- ✓ Determine Desired Software and Check Support Matrix
- ✓ Review and Implement Best Practice Configurations
- ✓ Discover and Clear any issues raised from “pre-upgrade validations”
- ✓ Review Upgrade Architecture and “do’s and don’ts”

Does your fabric look like this?



Fault Counts by Domain

Hide Acknowledged Faults

Hide Delegated Faults

SYSTEM WIDE	164	1858	31173	6205
Access	145	1789	5	82
External	0	0	0	4995
Framework	0	2	0	0
Infra	19	62	1270	1126
Management	0	4	5	0
Security	0	0	214	0
Tenant	0	1	29679	2
Apps	0	0	0	0

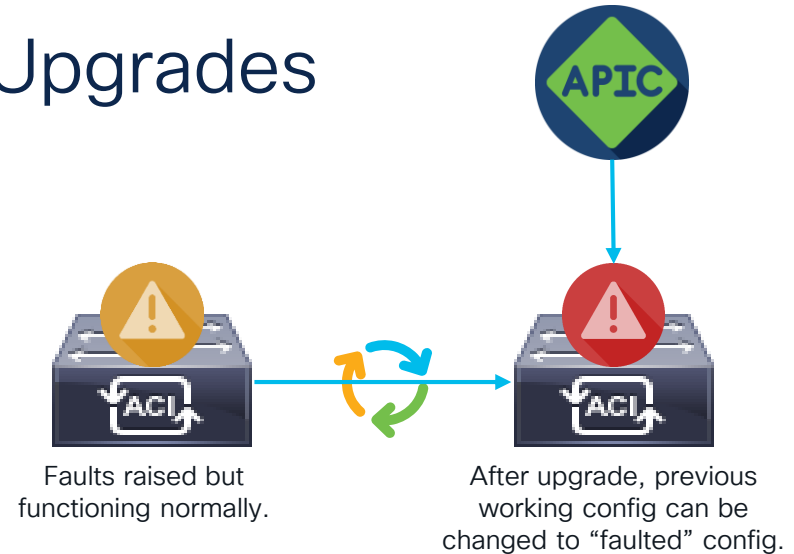
Tenants with Health ≤ 99

Name Health Score

scale_vpc20	Warning
scale_vpc30	Warning
scale_vpc40	Warning
scale_vpc50	Warning
Tenant_1	Critical
Tenant_10	Critical
Tenant_100	Critical
Tenant_101	Critical

Faults, and the Impact on Upgrades

- Faults can be raised if there is an overlap, or invalid config.
- After an upgrade the switch requests it's configuration "fresh" from APIC. This is the "stateless" behavior of ACI.
- If Logical Config (APIC) has conflicts, the "faulted" config can get pushed before the previously working config.

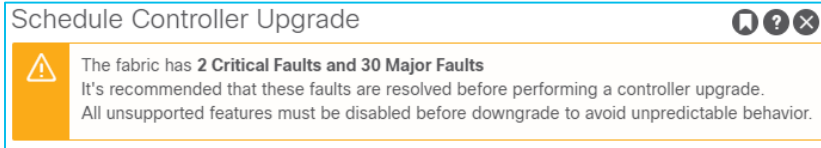


L2 Port Config (F0467 port-configured-as-13)
L3 Port Config (F0467 port-configured-as-12)
Config On APIC Connected Port (F0467 port-configured-for-apic)
etc . . .

Pre-Upgrade Validation

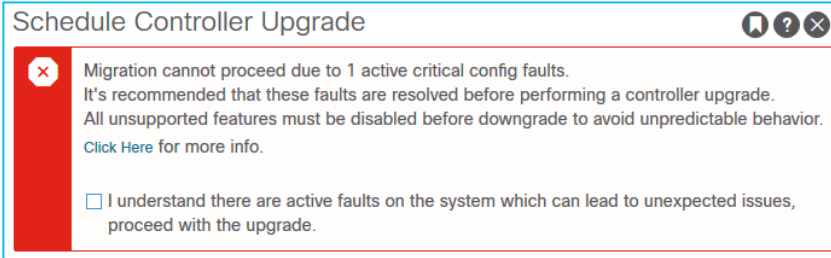
3.2 - continuing 

APIC 3.2, 4.0, 4.1



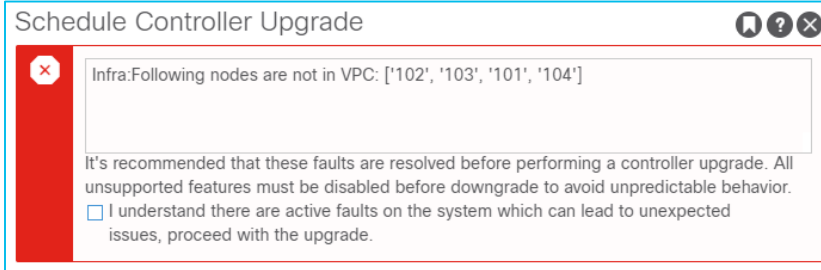
Screenshot of a warning message titled "Schedule Controller Upgrade". The message contains an orange warning icon and text: "The fabric has 2 Critical Faults and 30 Major Faults. It's recommended that these faults are resolved before performing a controller upgrade. All unsupported features must be disabled before downgrade to avoid unpredictable behavior."

APIC 4.2(1) - 4.2(3)



Screenshot of a warning message titled "Schedule Controller Upgrade". The message contains a red error icon and text: "Migration cannot proceed due to 1 active critical config faults. It's recommended that these faults are resolved before performing a controller upgrade. All unsupported features must be disabled before downgrade to avoid unpredictable behavior. Click Here for more info." Below the text is a checkbox: " I understand there are active faults on the system which can lead to unexpected issues, proceed with the upgrade."

APIC 4.2(4)

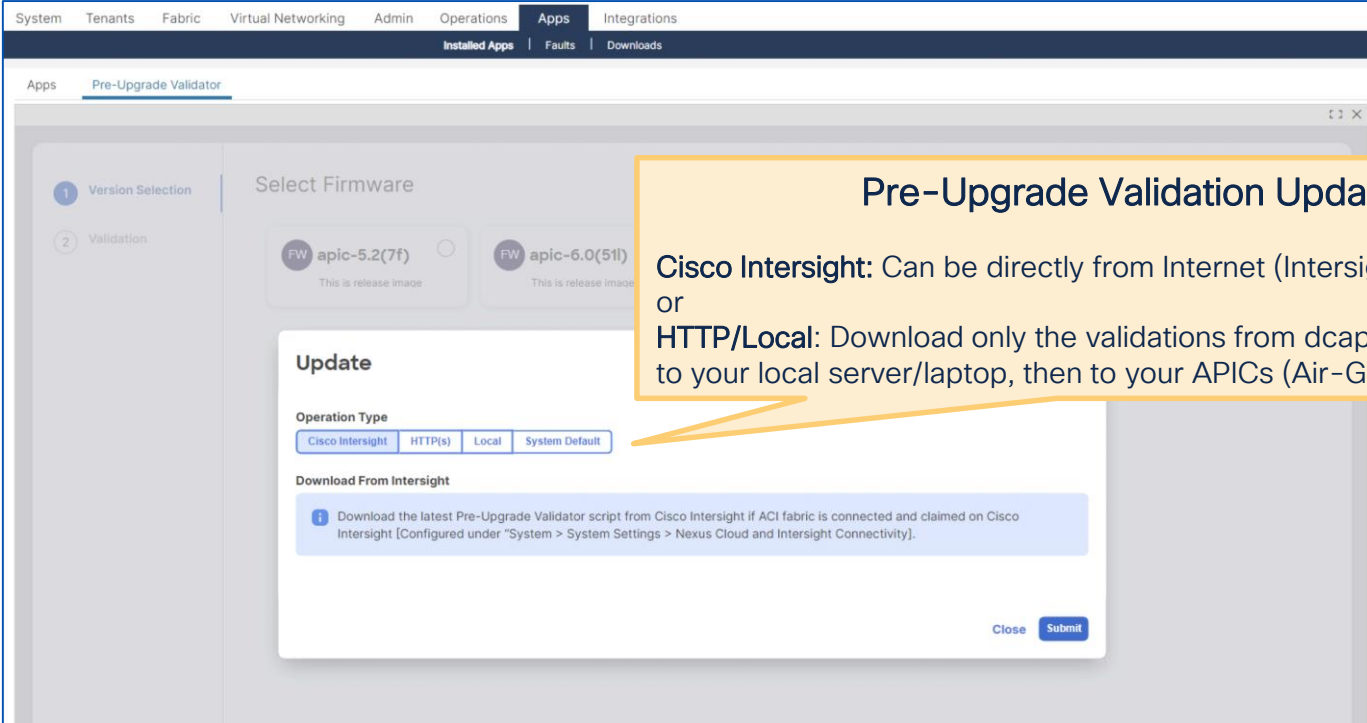


Screenshot of a warning message titled "Schedule Controller Upgrade". The message contains a red error icon and text: "Infra:Following nodes are not in VPC: ['102', '103', '101', '104']". Below this is a text box containing the same text. Further down, it says: "It's recommended that these faults are resolved before performing a controller upgrade. All unsupported features must be disabled before downgrade to avoid unpredictable behavior." At the bottom is a checkbox: " I understand there are active faults on the system which can lead to unexpected issues, proceed with the upgrade."

- Prior to 4.2, the APIC upgrade simply warned about the number of all critical and major faults
- On 4.2(1) - 4.2(3), the APIC upgrade warned about
 - ✓ config related critical faults
 - ✓ some specific faults that are known to cause issues during upgrades.
- On 4.2(4), the APIC upgrade warns about
 - ✓ config related critical faults
 - ✓ some specific faults that are known to cause issues during upgrades
 - ✓ A few nonoptimal configurations that may disrupt traffic during the upgrade.
- Additional validation items are being added on each release.

Pre-Upgrade Validation (AppCenter App)

What happens if Cisco adds additional checks?



The screenshot shows the Cisco AppCenter interface for the Pre-Upgrade Validator. The main window is titled "Pre-Upgrade Validator" and has a sidebar with "Version Selection" and "Validation" steps. The main content area is titled "Select Firmware" and shows two firmware options: "FW apic-5.2(7f)" and "FW apic-6.0(51I)". A modal window titled "Update" is open, showing "Operation Type" with buttons for "Cisco Intersight", "HTTP(s)", "Local", and "System Default". Below this, there is a section "Download From Intersight" with an information icon and a message: "Download the latest Pre-Upgrade Validator script from Cisco Intersight if ACI fabric is connected and claimed on Cisco Intersight [Configured under 'System > System Settings > Nexus Cloud and Intersight Connectivity]". The modal has "Close" and "Submit" buttons.

Pre-Upgrade Validation Updates

Cisco Intersight: Can be directly from Internet (Intersight)
or
HTTP/Local: Download only the validations from dcappcenter.cisco.com to your local server/laptop, then to your APICs (Air-Gapped)

<https://dcappcenter.cisco.com/pre-upgrade-validator.html>

Supported on 5.2. Pre-packaged in APIC in 6.0(2) and later

Pre-Upgrade Validation – Script

<https://github.com/datacenter/ACI-Pre-Upgrade-Validation-Script>

```
[Check 1/36] APIC Target version image and MD5 hash...
Checking f2-apic1.....

[Check 2/36] Target version compatibility...
[Check 3/36] Gen 1 switch compatibility...
[Check 4/36] Remote Leaf Compatibility... No Remote Leaf Found
[Check 5/36] APIC CIMC Compatibility...
[Check 6/36] APIC Cluster is Fully-Fit...
[Check 7/36] Switches are all in Active state...
[Check 8/36] NTP Status...
[Check 9/36] Firmware/Maintenance Groups when crossing 4.0 Release... Versions not applicable
[Check 10/36] Features that need to be Disabled prior to Upgrade...
  Feature      Name           Status  Recommended Action
  -----
App Center    Policy Viewer  active  Disable the app
Config Zone   test           Locked  Change the status to "Open" or remove the zone

[Check 11/36] Switch Upgrade Group Guidelines... No upgrade groups found!
[Check 12/36] APIC Disk Space Usage (F1527, F1528, F1529 equipment-full)...
[Check 13/36] Switch Node /bootflash usage... all below 50%
[Check 14/36] Standby APIC Disk Space Usage... No standby APIC found
[Check 15/36] APIC SSD Health (F2731 equipment-wearout)...
[Check 16/36] Switch SSD Health (F3073, F3074 equipment-flash-warning)...
[Check 17/36] Config On APIC Connected Port (F0467 port-configured-for-apic)...
[Check 18/36] L3 Port Config (F0467 port-configured-as-l2)...
[Check 19/36] L2 Port Config (F0467 port-configured-as-l3)...
[Check 20/36] L3Out Subnets (F0467 prefix-entry-already-in-use)...
[Check 21/36] BD Subnets (F1425 subnet-overlap)...
[Check 22/36] BD Subnets (F0469 duplicate-subnets-within-ctx)...
[Check 23/36] VMM Domain Controller Status...
[Check 24/36] VMM Domain LLDP/CDP Adjacency Status... No LLDP/CDP Adjacency Failed Faults Found
```

The goal of the script

To be able to apply the latest validations on any APIC versions via a script

Why the script may be a better choice?:

- Supports older versions – available for everyone!
- Always has the latest checks
- With Github account, you can submit issues or features directly



Both app and script are fully supported by TAC

Pre-Upgrade Validation Script

```
admin@apic1:techsupport> python aci-preupgrade-validation-script.py  
==== 2024-05-28T08:45:58-0500 ====
```

```
Enter username for APIC login      : admin  
Enter password for corresponding User :
```

User Enters Credentials

Checks that require login leverage this input

```
Checking current APIC version (switch nodes are assumed to be on the same version)...3.2(10e)
```

```
Gathering APIC Versions from Firmware Repository...
```

```
[1]: aci-apic-dk9.5.2.7g.bin
```

User Selects Target Version

Checks that require target version leverage this input.

```
What is the Target Version?      : 1
```

```
You have chosen version "aci-apic-dk9.5.2.7g.bin"  
[Check 1/64] APIC Target version image and MD5 hash...  
Checking fab3-apic1.....
```

```
[Check 2/64] Target version compatibility...  
[Check 3/64] Gen 1 switch compatibility...
```

```
. . .  
. . .  
. . .  
. . .  
. . .
```

Failure Details are Provided

Issue should be corrected (Script Re-Run to validate) before performing upgrade.

```
[Check 19/64] L2 Port Config (F0467 port-configured-as-l3)...
```

Fault	Pod	Node	Tenant	AP	EPG	Port	Recommended Action
-------	-----	------	--------	----	-----	------	--------------------

----	---	----	-----	--	---	----	-----
------	-----	------	-------	----	-----	------	-------

F0467	pod-1	node-101	jr	ap1	epg1	eth1/6	Resolve the conflict by removing this config or other configs using this port as L3
-------	-------	----------	----	-----	------	--------	---

FAIL - OUTAGE WARNING!!

DONE
PASS
PASS
PASS

Pre-Upgrade Validation Script

```
[Check 59/64] fvUplinkOrderCont with blank active uplinks definition... PASS
[Check 60/64] CoS 3 with Dynamic Packet Prioritization... PASS
[Check 61/64] N9K-C93108TC-FX3P/FX3H Interface Down... PASS
[Check 62/64] Invalid FEX Relation Source... PASS
[Check 63/64] LLDP Custom Interface Description Defect... PASS
[Check 64/64] Route-map Community Match Defect... PASS
```

=== Summary Result ===

```
PASS : 55
FAIL - OUTAGE WARNING!! : 4
FAIL - UPGRADE FAILURE!! : 2
MANUAL CHECK REQUIRED : 1
N/A : 2
ERROR !! : 0
TOTAL : 64
```

Summary is Provided

All "FAIL" Categories need remediation.
Detailed Recommendations to Remediate are
in the Upgrade Guide!

Log Bundle is Created

Upload this to any TAC Case if Necessary.

Pre-Upgrade Check Complete.

Next Steps: Address all checks flagged as FAIL, ERROR or MANUAL CHECK REQUIRED

Result output and debug info saved to below bundle for later reference.

Attach this bundle to Cisco TAC SRs opened to address the flagged checks.

Result Bundle: /data/techsupport/Scripts/pre-upgrade/preupgrade_validator_2024-05-28T08-45-58-0500.tgz

Pre-Upgrade Validation – Script Documentation

[Read the Docs!](#)

ACI Pre-Upgrade Validation Script

Getting Started

The script (`aci-preupgrade-validation-script.py`) needs to be run on one of your Cisco APICs via SSH session.

Cisco APIC is a linux appliance. You can download the script and copy it over to an APIC just as you do for a regular linux machine.

In case you are wondering how to do this, here are some examples.

Note

/data/techsupport is an ideal location to place the script on your APIC

1. Download the script (`aci-preupgrade-validation-script.py`)

Option1: git clone

```
On your local machine
git clone git@github.com:datacenter/ACI-Pre-Upgrade-Validation-Script.git
```

Option2: via browser

Download the script from here: [aci-preupgrade-validation-script.py](#)

2. Copy the script to an APIC

Option1: SCP, SFTP, etc.

```
On your local machine
scp aci-preupgrade-validation-script.py admin@apic IP>:/data/techsupport
```

Option2: SSH and copy/paste via `cat`

Validation Reference

L2/L3 Port Config

This is another type of the F0467 fault code family that you should check before an upgrade. This fault alerts that an interface configured under a Layer3 Out (L3Out) has failed because the port that the policy is deployed for is operating in the opposite mode. For example, you might have configured a routed sub-interface under an L3Out, making the port an L3 port. However, there is already L2 policy on that port. A port in ACI can either be L2 or L3, but not both, just like a port on any layer 3 switches that can be either **switchport (L2)** or **no switchport (L3)**, so this policy fails in this situation. The same rule applies if a port is already an L3 port, but you deploy L2 config onto it. After an upgrade, it's possible that the previously working configuration will break if this faulty policy is deployed first after the switch reloads.

It is critical that you resolve these issues before the upgrade to prevent any issues. The interface that the fault is raised on should either be corrected or deleted in order to clear the fault. You can run the moquery below on the CLI of any Cisco APIC to check if these faults exist on the system. The faults are visible within the GUI as well.

Fault Example (F0467: port-configured-as-l2)

The following fault shows an example of the configuration from L3Out OSPF under tenant jtr has failed on node 101 eth1/7 because the same port is already configured as L2 by other components, such as EPSs or other L3Outs using the same port as SVI. It implies that, in this case, L3Out OSPF is trying to use node 101 eth1/7 as a routed port or routed sub-interface (L3) as opposed to SVI (L2).

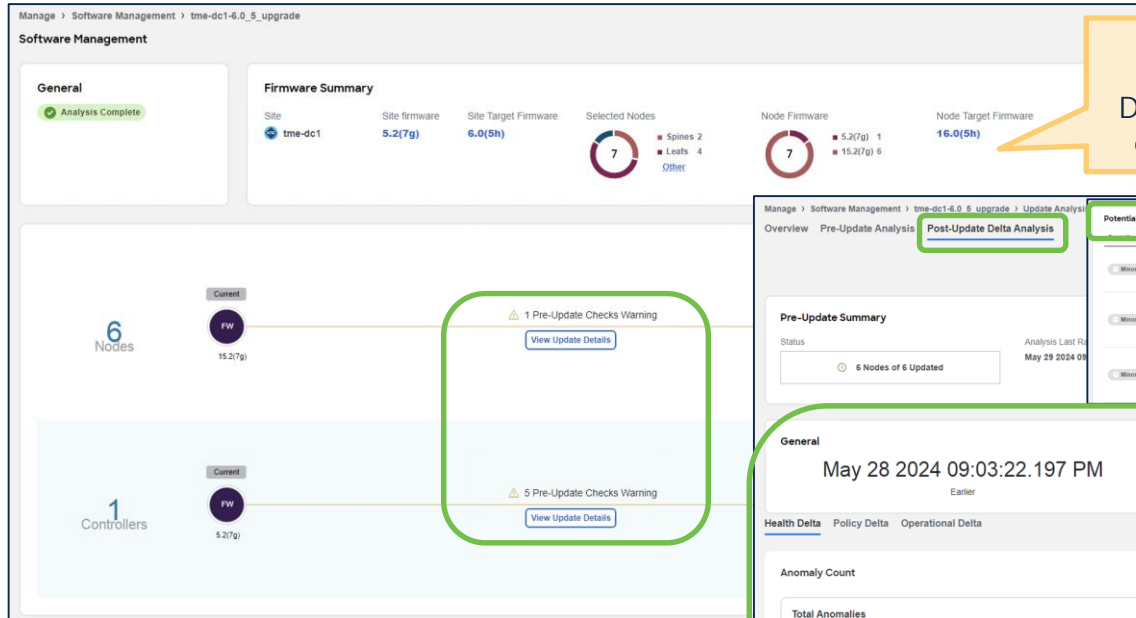
```
admin@apic1:~$ moquery -c faultDelegate -x 'query-target-filter=word(faultInst.changeSet,"port-con
Total Objects shown: 1

# fault.Delegate
affected      : resPolCnt/rtdOutCnt/rtdOutDef-[uni/tn-jtr/out-OSPF]/node-101/stpshatt-[eth1/7].
code         : F0467
ack         : no
cause       : configuration-failed
changeSet   : configObj:port-configured-as-l2, configSt:failed-to-apply, temporaryError:no
childAction
created     : 2021-06-23T12:17:54.775-04:00
descr      : Fault delegate: Configuration failed for uni/tn-jtr/out-OSPF node 101 eth1/7 due
dn         : uni/tn-jtr/out-OSPF/Fd-[resPolCnt/rtdOutCnt/rtdOutDef-[uni/tn-jtr/out-OSPF]/node
domain     : tenant
highestSeverity : minor
lastTransition : 2021-06-23T12:20:09.780-04:00
lc         : raised
modTs      : never
occur      : 1
origSeverity : minor
prevSeverity : minor
rn         : fd-[resPolCnt/rtdOutCnt/rtdOutDef-[uni/tn-jtr/out-OSPF]/node-101/stpshatt-[eth
rule        : fv-m-issues-config-failed
severity    : minor
status     :
subject    : management
type       : config
```

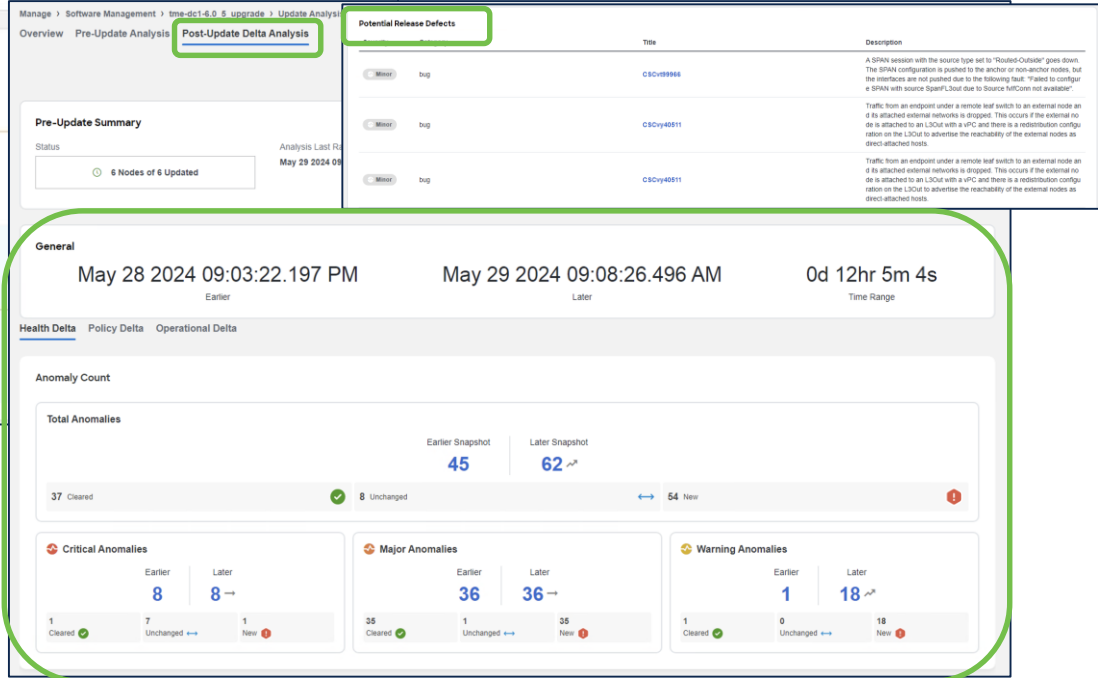
Table of contents

- Compatibility (Target ACI Version)
- Compatibility (CIMC Version)
- Compatibility (Switch Hardware)
- Compatibility (Switch Hardware - gen1)
- Compatibility (Remote Leaf Switch)
- APIC Target version image and MD5 hash
- APIC Cluster is Fully Fit
- Switches are all in Active state
- NTP Status
- Firmware/Maintenance Groups when crossing 4.0 Release
- Features that need to be disabled prior to Upgrade
- Switch Upgrade Group Guidelines
- Intersight Device Connector upgrade status
- Mini ACI Upgrade to 6.0(2) or later
- Fault Check Details
 - APIC Disk Space Usage
 - Standby APIC Disk Space Usage
 - Switch Node/Bootflash usage
 - APIC SSD Health
 - Switch SSD Health
 - Config On APIC Connected Port
 - L2/L3 Port Config
 - Access (Untagged) Port Config
 - Encap Already in Use
 - L3Out Subnets
 - BD Subnets
 - VMM Domain Controller Status

Nexus Dashboard Insights (Optional)



Benefit of Nexus Insights
Does both a pre-check and a post-check to alert on effects and changes in the upgrade window



- Pre-Update Verifications and Alerting
- Detailed list of bugs addressed in the upgrade
- Post-upgrade Delta analysis of Anomalies, Edits and Operations changes in the upgrade process

ACI Firmware Upgrade Best Practice Checklist



Determine Desired Software and Check Support Matrix



Review and Implement Best Practice Configurations



Discover and Clear any issues raised from “pre-upgrade validations”



Review Upgrade Architecture and “Do’s and Don’ts”

Do's and Don'ts

If at any point in time you believe the upgrade/downgrade has either stalled or failed, follow the guidelines below:

- Do View the APIC Faults and Installer Logs.
- Do Collect the Tech Support Files.
- Do Contact Cisco TAC if Needed.



```
admin@apic1:logs> pwd
/firmware/logs
admin@apic1:logs> ls -l
2021-04-15T07:42:57-50
2021-05-28T10:18:33-50
admin@apic1:logs> ls -l ./2021-05-28T10:18:33-50
atom_installer.log
insieme_4x_installer.log
```

```
leaf101# pwd
/mnt/pss
leaf102# ls installer_detail.log
installer_detail.log
```



```
admin@apic1:~> techsupport local
```



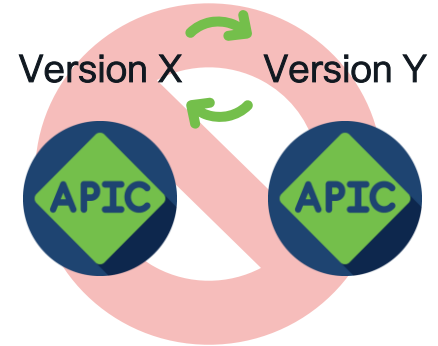
Do's and Don'ts

If at any point in time you believe the upgrade/downgrade has either stalled or failed, it is critical that you do not take any of the actions listed below:

Don't reload any APIC in the cluster manually.

Don't decommission any APIC in the cluster.

Don't change the firmware target version back to the original version.





Final Tip

You've read the "Do's and Don'ts"...

When in Doubt,
Contact Cisco Support



With Proper Backups, Recovery is Always an Option

ACI Firmware Upgrade Best Practice Checklist



Determine Desired Software and Check Support Matrix



Review and Implement Best Practice Configurations



Discover and Clear any issues raised from “pre-upgrade validations”



Review Upgrade Architecture and “do’s and don’ts”

Key points to remember

- Always make sure you are performing a supported upgrade.
- Best Practice Configuration and Backups are Critical to Success
- ACI Pre-Upgrade Validations will prevent known issues from impacting the upgrade.
- Never perform a disruptive procedure during an upgrade without help from Cisco.

Reference

- Cisco APIC Installation and ACI Upgrade and Downgrade Guide
<https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/all/apic-installation-aci-upgrade-downgrade/Cisco-APIC-Installation-ACI-Upgrade-Downgrade-Guide.html>
- Cisco ACI Upgrade Checklist
<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/Cisco-ACI-Upgrade-Checklist.html>
- Cisco APIC Release Notes
<https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>
- Release Notes for Cisco Nexus 9000 Series Switches in ACI Mode
<https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html>
- Getting Started Guide (NX-OS to ACI POAP Auto-conversion)
<https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/5x/getting-started/cisco-apic-getting-started-guide-52x/fabric-initialization-52x.html#d5018e3247a1635>

Reference

- Cisco APIC Installation and ACI Upgrade / Downgrade Guide
<https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/all/apic-installation-aci-upgrade-downgrade/Cisco-APIC-Installation-ACI-Upgrade-Downgrade-Guide.html>
- Cisco ACI Upgrade Checklist
<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/Cisco-ACI-Upgrade-Checklist.html>
- Cisco APIC Release Notes
<https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>
- Release Notes for Cisco Nexus 9000 Series Switches in ACI Mode
<https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html>
- Cisco ACI Upgrade Matrix
<https://www.cisco.com/c/dam/en/us/td/docs/Website/datacenter/apic/matrix/index.html>
- Pre-Upgrade Validation Script
<https://github.com/datacenter/ACI-Pre-Upgrade-Validation-Script>
- Pre-Upgrade Validation Script Documentation
<https://datacenter.github.io/ACI-Pre-Upgrade-Validation-Script/>

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.



Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.



Level up and earn **exclusive prizes!**



Complete your surveys in the **Cisco Live mobile app.**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive