Cisco Catalyst 3850 Switch

Deployment Guide

Contents

Preface ... **3**

Purpose ... 3
Audience ... 3
Conventions ... 3

Introduction ... **4**

Initializing the Cisco Catalyst 3850 Switch ... **4**

Console Setup ... 5
Using the USB Console Port ... 5
Using the RJ45 Port ... 5
Cisco IOS XE Software Bundle and Packages Overview ... 6
Booting Cisco IOS XE Software ... 7
Booting the Switch in Install Mode ... 7
Booting the Cisco Catalyst 3850 Switch in Bundle Mode ... 8
Updating Cisco IOS XE Software ... 8
Software Rollback ... 10
Software Clean ... 10
Migration to Install Mode from the Bootloader Prompt ... 14

Cisco Catalyst 3850 Switch Right-to-Use Licensing Model ... **16**

RTU License Types ... 16
Permanent RTU License ... 17
Image-Based License in a Stack ... 19
AP-Count License in a Stack ... 20
License Migration Between Switches ... 22
Evaluation RTU License ... 25
License Usage Monitoring ... 26
License Storage Management ... 27

Cisco Catalyst 3850 Switch Stacking ... **27**

Overview ... 27
Plug-and-Play Stack Deployment ... 29
Deploying Cisco Catalyst 3850 Switch StackWise-480 NSF and SSO ... 32
Converged Access with the Cisco Catalyst 3850 Switch ... 33
Distributed Functions Enable Converged Access ... 33
Logical Hierarchical Groupings of Roles ... 34
Converged Access Network Design with Cisco Catalyst 3850 Switch ... 35
Case Study: Configuring Converged Access with the Cisco Catalyst 3850 Switch ... 38
Configuring the Small Branch Deployment ... 38
Configuring the Large Branch or Medium Size Campus Deployment ... 40

Cisco Catalyst 3850 Switch Database Manager Template ... **42**

SDM Template Resources: VLAN and Advanced ... 42
SDM Template Configuration ... 43
Monitoring SDM Resources ... 44

Appendix A: List of Bootloader Commands ... **45**

Appendix B: Cisco Catalyst 3850 Switch Mobility Agent and Mobility Controller Configurations ... **46**

Preface

Purpose

The purpose of this guide is to explain the basic concepts and provide general procedures and commands to deploy Cisco® Catalyst® 3850 Switches. It does not provide detailed information about these commands.

Audience

This guide is for networking professionals who are responsible for designing, implementing, or administering a network that includes a standalone Cisco Catalyst 3850 Switch or a Cisco Catalyst 3850 Switch stack, referred to as the switch. Readers of this guide are expected to have prior experience working with the Cisco IOS® Software and familiarity with the concepts and terminology of local area networking, wireless local area networking, and Layer 2 and Layer 3 switching.

Conventions

This publication uses these conventions to convey instructions and information:

- Command names are in **boldface** text.
- System displays are in screen font.

Introduction

The next-generation Cisco Catalyst 3850 Switch meets the current and future demands of enterprise access-layer networks. As these networks incorporate ever more technologies, they must be secure, scalable, and resilient. The Cisco Catalyst 3850 Switch offers operational simplicity, scalability, and superb performance. The new Cisco StackWise-480 stack architecture delivers the industry’s best-in-class stack bandwidth and resiliency.

The Cisco Catalyst 3850 Switch supports the powerful next-generation Cisco IOS XE Software. The modular Cisco IOS XE Software architecture enables rich, scalable, and cost-effective integrated borderless networking services.

The Cisco Catalyst 3850 Switch is the first stackable access-layer switch that provides both wired and wireless services on a single Cisco IOS XE Software-based platform.

This guide describes the procedures required to deploy a Cisco Catalyst 3850 Switch:

1. Initializing the Cisco Catalyst 3850 Switch
2. Cisco Catalyst 3850 Switch right-to-use (RTU) licensing model
3. Cisco Catalyst 3850 Switch stacking
4. Converged access with the Cisco Catalyst 3850 Switch
5. Cisco Catalyst 3850 Switch Database Manager (SDM) template

Initializing the Cisco Catalyst 3850 Switch

- Console setup
- Cisco IOS XE Software bundle and packages overview
- Booting Cisco IOS XE Software
- Updating Cisco IOS XE Software
- Software rollback
- Software clean
- Boot loader upgrade
- Migration to installed mode

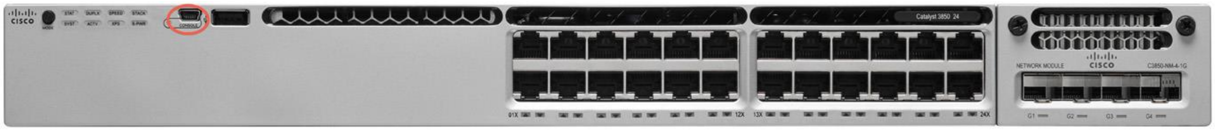
Console Setup

The Cisco Catalyst 3850 Switch (similar to the Cisco Catalyst 3750-X Switch) has two console ports: a USB mini console port in the front and an RJ45 console port in the rear. You can use either port (but not both) for input. However, both ports always display the switch output.

The default console port speed setting is 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

Using the USB Console Port

Figure 1. USB Console Port



The USB console port is the default management port and is supported in both install and boot loader modes.

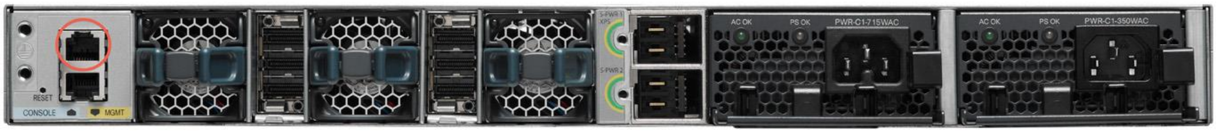
Before using the USB port, download the required driver to your PC from Cisco.com: http://software.cisco.com/download/release.html?mdfid=282979369&softwareid=282855122&release=3.1.

The USB console port has a configurable inactivity timer that automatically disables the port after a specified period from 1 to 240 minutes. Use this command to configure the inactivity timeout interval:

```
Switch(config-line)# usb-inactivity-timeout switch 1 ?
  <1-240>  Inactivity minutes before console reverts to RJ45
```

Using the RJ45 Port

Figure 2. RJ45 Console Port



To use the RJ45 port, you must configure precedence for it by using these commands:

```
Switch(config)# line con 0
Switch(config-line)# media-type rj45 switch 1
```

Configuring precedence for the RJ45 port enables it for input and disables input on the USB console port. However, switch output is always displayed on both ports.

Cisco IOS XE Software Bundle and Packages Overview

The Cisco Catalyst 3850 Switch uses Cisco IOS XE Software. Cisco IOS XE Software is delivered as a bundle that contains a set of packages. The Cisco IOS XE Software bundle uses this image name convention:

<platform_name>-<bundle_feature_set>.<key_ver>.<IOS-XE_version>.<IOS_image_version> .bin

Example: cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin

Explanation of bundle naming convention:

Image Name Element	Explanation	Example
platform_name	The name of the platform supported by the Cisco IOS XE Software bundle; **caa** represents converged access architecture	cat3k_caa
bundle_feature set	The feature set provided by the Cisco IOS XE Software bundle	universalk9
key_ver	A three-character string indicating that the Cisco IOS XE Software bundle (or the packages it contains, or both) is digitally signed	SPA
IOS_XE_version	The bundle's Cisco IOS XE Software release number	3.2.0SE
IOS_image_version	The Cisco IOS Software image version of the Cisco IOS Software package contained in the bundle	15.0(1)EX

The Cisco IOS XE Software bundle contains a set of packages and a provisioning file, called **packages.conf**, that is created automatically during the install process.

The **show version running** EXEC command displays the current running package(s) version:

```
Switch# show version running
Package: Base, version: 03.02.00SE, status: active
  File: cat3k_caa-base.SPA.03.02.00SE.pkg, on: Switch1
  Built: Wed Jan 09 21:59:52 PST 2013, by: gereddy

Package: Drivers, version: 03.02.00.SE, status: active
  File: cat3k_caa-drivers.SPA.03.02.00.SE.pkg, on: Switch1
  Built: Wed Jan 09 22:03:41 PST 2013, by: gereddy

Package: Infra, version: 03.02.00SE, status: active
  File: cat3k_caa-infra.SPA.03.02.00SE.pkg, on: Switch1
  Built: Wed Jan 09 22:00:56 PST 2013, by: gereddy

Package: IOS, version: 150-1.EX, status: active
  File: cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg, on: Switch1
  Built: Wed Jan 09 22:02:23 PST 2013, by: gereddy

Package: Platform, version: 03.02.00.SE, status: active
  File: cat3k_caa-platform.SPA.03.02.00.SE.pkg, on: Switch1
  Built: Wed Jan 09 22:01:46 PST 2013, by: gereddy

Package: WCM, version: 10.0.100.0, status: active
```

```
File: cat3k_caa-wcm.SPA.10.0.100.0.pkg, on: Switch1
Built: Wed Jan 09 22:03:05 PST 2013, by: gereddy
```

The Cisco IOS XE Software bundle includes these packages:

Package Name	File Name	Contents
Base	cat3k_caa-base.SPA.03.02.00SE.pkg	Kernel distribution
Drivers	cat3k_caa-drivers.SPA.03.02.00.SE.pkg	Platform drivers
Infra	cat3k_caa-infra.SPA.03.02.00SE.pkg	Infrastructure software, including system manager, installer, HA manager, and more
Cisco IOS Software	cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg	Cisco IOS Software image
Platform	cat3k_caa-platform.SPA.03.02.00.SE.pkg	Software not specific to the Cisco IOS Software platform and stack manager, platform manager, and more
WCM	cat3k_caa-wcm.SPA.10.0.100.0.pkg	Wireless controller software

Booting Cisco IOS XE Software

You can boot and run the Cisco IOS XE Software on the Cisco Catalyst 3850 Switch in either of two modes:

- Install mode (recommended mode of operation)
- Bundle mode

Booting the Switch in Install Mode

Cisco Catalyst 3850 Switches shipped to customers from manufacturing boot up in install mode. The Cisco Catalyst 3850 Switch is booted in install mode using a package provisioning file **packages.conf**. Do not modify this file.

In this example, the Cisco Catalyst 3850 Switch is configured to autoboot from the built-in flash memory:

```
Switch# show boot
BOOT variable = flash:packages.conf;
Manual Boot = no
Enable Break = no
```

The **show version** command output displays the Cisco Catalyst 3850 Switch mode of operation:

```
Switch# show ver | begin Switch Ports
Switch Ports Model              SW Version        SW Image              Mode
------ ----- -----              ----------        ----------            ----
     1 56    UA-C3850-48P       03.02.00SE        cat3k_caa-universalk9 INSTALL
Configuration register is 0x102
```

The packages and the provisioning file reside in the flash.

Note: Booting in install mode from a USB flash drive or using Trivial File Transfer Protocol (TFTP) is not supported.

Booting the Cisco Catalyst 3850 Switch in Bundle Mode

Booting a Cisco Catalyst 3850 Switch in bundle mode is just like booting a monolithic Cisco IOS Software image on a Cisco Catalyst 3750-X Switch.

This command boots the switch in bundle mode:

```
switch: boot flash:cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin
```

Note: Booting the switch in bundle mode consumes more memory than booting in install mode because the packages are extracted from the bundle and copied to the RAM.

You can boot the switch in bundle mode from the built-in flash memory, an external USB drive (usbflash0), or TFTP. Bundle mode is used to boot a Cisco Catalyst 3850 Switch from the boot loader prompt.

Updating Cisco IOS XE Software

When the switch is in install mode, you can install any new Cisco IOS XE Software bundle by using the **software Install** command.

Note: This command works only when the Cisco Catalyst 3850 Switch is booted in install mode.

Use the **show switch** command to check the status of the switch or switch stack. This example shows the status of a two-switch stack, where switch 2 is active:

```
Switch# show switch
Switch/Stack Mac Address : 2037.0653.cb00
                                                         H/W         Current
Switch#   Role          Mac Address          Priority    Version     State
-------------------------------------------------------------------------------
 1        Standby       2037.0653.fd80       1           P6A         Ready
*2        Active        2037.0653.cb00       1           P6A         Ready
```

This example shows the command syntax and the console log from a software install in a stack of two switches:

```
Switch# software install file flash: cat3k_caa-universalk9.SPA.03.02.00.SE.150-
1.EX.bin new
Preparing install operation ...
[2]: Copying software from active switch 2 to switch 1
[2]: Finished copying software to switch 1
[1 2]: Starting install operation
[1 2]: Expanding bundle flash: cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin
```

```
[1 2]: Copying package files
[1 2]: Package files copied
[1 2]: Finished expanding bundle flash: cat3k_caa-
universalk9.SPA.03.02.00.SE.150-1.EX.bin
[1 2]: Verifying and copying expanded package files to flash:
[1 2]: Verified and copied expanded package files to flash:
[1 2]: Starting compatibility checks
[1 2]: Finished compatibility checks
[1 2]: Starting application pre-installation processing
[1 2]: Finished application pre-installation processing
[1]: Old files list:
    Removed cat3k_caa-base.SSA.03.08.72.EMP2.pkg
    Removed cat3k_caa-drivers.SSA.03.08.72.EMP2.pkg
    Removed cat3k_caa-infra.SSA.03.08.72.EMP2.pkg
    Removed cat3k_caa-iosd-universalk9.SSA.150-8.72.EMP2.pkg
    Removed cat3k_caa-platform.SSA.03.08.72.EMP2.pkg
    Removed cat3k_caa-wcm.SSA.03.08.72.EMP2.pkg
[2]: Old files list:
    Removed cat3k_caa-base.SSA.03.08.72.EMP2.pkg
    Removed cat3k_caa-drivers.SSA.03.08.72.EMP2.pkg
    Removed cat3k_caa-infra.SSA.03.08.72.EMP2.pkg
    Removed cat3k_caa-iosd-universalk9.SSA.150-8.72.EMP2.pkg
    Removed cat3k_caa-platform.SSA.03.08.72.EMP2.pkg
    Removed cat3k_caa-wcm.SSA.03.08.72.EMP2.pkg
[1]: New files list:
    Added cat3k_caa-base.SPA.03.02.00SE.pkg
    Added cat3k_caa-drivers.SPA.03.02.00.SE.pkg
    Added cat3k_caa-infra.SPA.03.02.00SE.pkg
    Added cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg
    Added cat3k_caa-platform.SPA.03.02.00.SE.pkg
    Added cat3k_caa-wcm.SPA.10.0.100.0.pkg
[2]: New files list:
    Added cat3k_caa-base.SPA.03.02.00SE.pkg
    Added cat3k_caa-drivers.SPA.03.02.00.SE.pkg
    Added cat3k_caa-infra.SPA.03.02.00SE.pkg
    Added cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg
    Added cat3k_caa-platform.SPA.03.02.00.SE.pkg
    Added cat3k_caa-wcm.SPA.10.0.100.0.pkg
[1 2]: Creating pending provisioning file
[1 2]: Finished installing software.  New software will load on reboot.
[1 2]: Committing provisioning file
[1 2]: Do you want to proceed with reload? [yes/no]:y
```

Software Rollback

The **software rollback** command allows you to revert to an earlier Cisco IOS XE Software package after a software install. Software rollback is functional only when at least one rollback package with the file name packages.conf.00- is present. The rollback file is created automatically during the Cisco Catalyst 3850 Switch Cisco IOS XE Software image update process.

This example shows the flash directory of a switch with an available rollback package:

```
Switch# dir flash:
Directory of flash:/
15134  -rwx        1230   Oct 9 2012 12:52:15 +00:00  packages.conf.00-
15125  -rwx         556  Oct 10 2012 14:09:15 +00:00  vlan.dat

<Output Truncated>
```

To revert to an earlier software image, use the **software rollback** command with the rollback package name:

```
Switch1# software rollback provisioning-file flash:packages.conf00-
```

Software Clean

Flash space in a Cisco Catalyst 3850 Switch can be recovered safely by using the **software clean** command. This command deletes any redundant package files (.pkg), bundle files (.bin), or provisioning files (packages.conf*), without deleting the active .pkg and .conf file.

Do not use the **delete** command to remove unnecessary files from flash, because you might also delete the active .pkg or .conf files that are required for booting the switch.

Note: After you use the **software clean** command, the switch cannot revert to an earlier software image, because the required rollback files are deleted by this operation.

This example shows the results of the **software clean** command on a stack of two Cisco Catalyst 3850 Switches:

```
Switch# software clean
Preparing clean operation ...
[1 2]: Cleaning up unnecessary package files
[1 2]: No path specified, will use booted path flash:packages.conf
[1 2]: Cleaning flash:
[1]: Preparing packages list to delete ...
    cat3k_caa -base.SSA.03.08.79.EMP1.pkg
        File is in use, will not delete.
    cat3k_caa -drivers.SSA.03.08.79.EMP1.pkg
        File is in use, will not delete.
    cat3k_caa -infra.SSA.03.08.79.EMP1.pkg
```

```
File is in use, will not delete.
    cat3k_caa -iosd-universalk9.SSA.150-8.79.EMP1.pkg
        File is in use, will not delete.
    cat3k_caa -platform.SSA.03.08.79.EMP1.pkg
        File is in use, will not delete.
    cat3k_caa -wcm.SSA.03.08.79.EMP1.pkg
        File is in use, will not delete.
    packages.conf
        File is in use, will not delete.
[2]: Preparing packages list to delete ...
    cat3k_caa -base.SSA.03.08.79.EMP1.pkg
        File is in use, will not delete.
    cat3k_caa -drivers.SSA.03.08.79.EMP1.pkg
        File is in use, will not delete.
    cat3k_caa -infra.SSA.03.08.79.EMP1.pkg
        File is in use, will not delete.
    cat3k_caa -iosd-universalk9.SSA.150-8.79.EMP1.pkg
        File is in use, will not delete.
    cat3k_caa -platform.SSA.03.08.79.EMP1.pkg
        File is in use, will not delete.
    cat3850-wcm.SSA.03.08.79.EMP1.pkg
        File is in use, will not delete.
    packages.conf
        File is in use, will not delete.
[1]: Files that will be deleted:
    cat3k_caa-base.SSA.03.08.72.EMP2.pkg
    cat3k_caa-drivers.SSA.03.08.72.EMP2.pkg
    cat3k_caa-infra.SSA.03.08.72.EMP2.pkg
    cat3k_caa-iosd-universalk9.SSA.150-8.72.EMP2.pkg
    cat3k_caa-platform.SSA.03.08.72.EMP2.pkg
    cat3k_caa-universalk9.03.08.79.EMP1.bin
    cat3k_caa -wcm.SSA.03.08.72.EMP2.pkg
    packages.conf.01-
[2]: Files that will be deleted:
    cat3k_caa-base.SSA.03.08.72.EMP2.pkg
    cat3k_caa-drivers.SSA.03.08.72.EMP2.pkg
    cat3k_caa-infra.SSA.03.08.72.EMP2.pkg
    cat3k_caa-iosd-universalk9.SSA.150-8.72.EMP2.pkg
    cat3k_caa-platform.SSA.03.08.72.EMP2.pkg
cat3k_caa-universalk9.03.08.79.EMP1.bin
    cat3k_caa-wcm.SSA.03.08.72.EMP2.pkg
    packages.conf.00-
[1 2]: Do you want to proceed with the deletion? [yes/no]: yes
[1 2]: Clean up completed
```

Boot Loader Upgrade

The Cisco Catalyst 3850 Switch shipped from manufacturing is configured to autoboot Cisco IOS XE Software from the built-in flash and display the autoconfiguration dialog. In special circumstances a boot loader upgrade might be necessary for a Cisco IOS XE Software image upgrade.

These are the steps to upgrade a Cisco Catalyst 3850 Switch boot loader image:

Step 1. Enable manual boot and power cycle the switch.

Enter the **boot manual** command, along with the switch name or number:

```
Switch(config)# boot manual switch 1
Switch# wr mem
Building configuration...
Compressed configuration from 6503 bytes to 2335 bytes[OK]
Switch# reload
```

This is a sample of the switch display following a manual boot:

```
Booting...(use DDR clock 667 MHz)
Total memory size = 0x00000000 80000000
Initializing and Testing RAM
+++@@@@####...++@@++@@++@@++@@++@@++@@++@@++@@done.
Memory Test Pass!
Performing CPU BIST Test
CPU BIST Test Pass!
C3850 Boot Loader (C3850-HBOOT-M) Version 1.1, engineering software (P)
Compiled Wed Sep 12 16:56:12 PDT 2012 by johwang

<Output Truncated>

The system is not configured to boot automatically.  The
following command will finish loading the operating system
software:
    boot
switch:
```

There is a limited set of commands that are supported at the boot loader command prompt. Enter a question mark to view the available commands.

Note: Appendix A of this guide shows the complete list of boot loader commands.

Use the **version** boot loader command to display the current boot loader version:

```
switch: ver
C3850 Boot Loader (C3850-HBOOT-M) Version 1.1, engineering software (P)
Compiled Wed Sep 12 16:56:12 PDT 2012 by johwang
```

Step 2. Load the new boot loader image from a TFTP server.

This example shows how to establish TFTP connectivity to the switch from the boot loader prompt:

```
switch: IP_ADDR=10.1.104.130/255.255.255.0
switch: DEFAULT_ROUTER=10.1.104.1
switch: MANUAL_BOOT=yes
switch: ping 10.1.104.211
ping 10.1.104.211 with 32 bytes of data ...
Up 1000 Mbps Full duplex (port  0) (SGMII)
Host 10.1.104.211 is alive.
```

This example shows how to copy the boot loader image from TFTP:

```
switch: copy tftp://10.1.104.211/cat3850_loader.img.12Sep12.SSA bs:
Up 1000 Mbps Full duplex (port  0) (SGMII)
.................................................................................
.................................................................................
.................................................................................
............
File "tftp://10.1.104.211/switch/cat3850_loader.img.12Sep12.SSA" successfully
copied to "bs:"
```

Note: You can also copy the boot loader image from a USB flash drive.

Step 3. Reset the switch.

The reset command reloads the switch, and it starts up with the new boot loader image:

```
Switch: reset
```

To install the Cisco IOS XE Software, migrate from the boot loader prompt to the install mode.

Migration to Install Mode from the Bootloader Prompt

The Cisco IOS XE Software image for the Cisco Catalyst 3850 Switch is distributed as a bundle image. You cannot copy this bundle directly to the flash and then boot the switch. You must install the Cisco IOS XE Software bundle into the flash and then boot the switch from the installed software using the install mode. Perform this procedure if the Cisco IOS XE Software image that resides in the flash memory becomes corrupted.

Use the **ping** command to confirm TFTP connectivity from the boot loader prompt:

```
switch: ping 10.1.104.211
ping 10.1.104.211 with 32 bytes of data ...
Up 1000 Mbps Full duplex (port  0) (SGMII)
Host 10.1.104.211 is alive
```

Boot the switch from TFTP:

```
switch: boot tftp://10.1.104.211/switch/cat3k_caa-
universalk9.SPA.03.02.00.SE.150-1.EX.bin
Reading full image into memory....
<Output Truncated>
```

Use the **show version** command to display the software image version and the mode:

```
Switch# show version | begin Switch Ports
Switch Ports Model              SW Version        SW Image              Mode
------ ----- -----              ----------        ----------            ----
  1   56    WS-C3850-48P          03.02.00SE    cat3k_caa-universalk9  BUNDLE
```

The display shows bundle mode because the switch booted by loading the bundle either from TFTP or from a USB flash drive.

Copy the final bundle image to the flash either from the TFTP server or from a USB flash drive.

Use the **software expand** command to expand the bundle image in the flash:

```
Switch# software expand file flash: cat3k_caa-universalk9.SPA.03.02.00.SE.150-
1.EX.bin
Preparing expand operation ...
[1]: Expanding bundle flash: cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin
[1]: Copying package files
[1]: Package files copied
[1]: Finished expanding bundle flash: cat3k_caa-universalk9.SPA.03.02.00.SE.150-
1.EX.bin
```

Confirm that the bundle is expanded and packages.conf file is present in the flash memory:

```
Switch# dir flash:
Directory of flash:/
45351  -rwx        1218  Jan 18 2013 12:37:11 +00:00  packages.conf
45345  -rwx    74410468  Jan 18 2013 12:36:33 +00:00  cat3k_caa-
base.SPA.03.02.00SE.pkg
45346  -rwx     2773680  Jan 18 2013 12:36:33 +00:00  cat3k_caa-
drivers.SPA.03.02.00.SE.pkg
45347  -rwx    32478044  Jan 18 2013 12:36:39 +00:00  cat3k_caa-
infra.SPA.03.02.00SE.pkg
45348  -rwx    30393116  Jan 18 2013 12:36:46 +00:00  cat3k_caa-iosd-
universalk9.SPA.150-1.EX.pkg
45349  -rwx    18313952  Jan 18 2013 12:36:50 +00:00  cat3k_caa-
platform.SPA.03.02.00.SE.pkg
45350  -rwx    63402700  Jan 18 2013 12:37:09 +00:00  cat3k_caa-
wcm.SPA.10.0.100.0.pkg

<Output Truncated>
```

Reload the switch and boot with the newly created flash:packages.conf:

```
switch: boot flash:packages.conf
Getting rest of image
Reading full image into memory....done

<Output Truncated>

Switch# show version | begin Switch Ports
Switch   Ports    Model         SW Version        SW Image           Mode
------   -----    -----         ----------        ----------         ----
 1        56    WS-C3850-48P  03.02.00SE    cat3k_caa-universalk9   INSTALL
```

By default, when the **software expand** command is executed in the active switch of a switch stack, it is executed on all switches in the stack.

To autoload the installed image, perform these steps:

Use the **no boot manual** command to disable manual boot:

```
Switch(config)# no boot manual switch <#>
```

Use the **boot system** command to modify the boot command to boot from flash:

```
Switch(config)# boot system switch 3 flash:packages.conf
```

Use the **copy running-config startup-config** command to save the configuration:

```
Switch# copy running-config startup-config
```

Use the **show boot** command to verity that the switch is configured to boot from flash memory:

```
Switch# show boot
BOOT variable = flash:packages.conf;
Manual Boot = no
Enable Break = no
```

Cisco Catalyst 3850 Switch Right-to-Use Licensing Model

The Cisco Catalyst 3850 Switch right-to-use (RTU) is a trust-based licensing model designed to give customers the flexibility to upgrade, downgrade, or move the license for RMA purposes by using simple EXEC commands. The RTU licensing model allows customers to specify the desired image-based licensing level (LAN Base, IP Base, and IP Services) and AP-Count on the switch or switch stack through EXEC commands.

About the Cisco Catalyst 3850 Switch RTU license:

- The RTU license is purchased along with the Cisco Catalyst 3850 Switch (or separately) and is NOT tied to the unique device identifier (product ID + serial number) of a switch.
- When you purchase a switch, the license you specified in the purchase order is preinstalled.
- To upgrade the license, you can order an upgrade license and receive an electronic or printed license. After accepting the end-user license agreement (EULA), you enable the upgrade by using a simple CLI command.
- To transfer RTU licenses from one switch to another, deactivate the license on one switch and activate it on another.

RTU License Types

There are two main categories of Cisco Catalyst 3850 Switch RTU license: a permanent RTU license and a 90-day evaluation RTU license.

Permanent RTU License

This is a paid license that does not expire. You can activate permanent RTU licenses after you accept the EULA. The EULA assumes you have purchased the permanent license. There are two types of permanent RTU licenses:

- Image-based (or feature set) license
- Adder AP-Count license

Image-based license: This license is activated by Cisco before the switch is shipped and requires no customer configuration to enable it. Supported license levels include LAN Base, IP Base, and IP Services.

You can upgrade, disable, or move image-based licenses by using the **license right-to-use** command, either for individual switches or for all switches in a stack. Reload the switch or stack to activate the highest level license. For example, if you upgrade the license level from IP Base to IP Services, then the IP services license is activated by reloading the switch.

This command enables the ipservices license and accepts the EULA on all switches in the stack:

```
Switch1# license right-to-use activate ipservices all acceptEULA
% switch-1:stack-mgr:Reboot the switch to invoke the highest activated License
level
Switch1# show license right-to-use summary
  License Name    Type     Count   Period left
-----------------------------------------------
  ipbase       permanent   N/A      Lifetime
  apcount      base*        0       Lifetime
  apcount      adder       50       Lifetime

--------------------------------------------
License Level In Use: ipbase
License Level on Reboot: ipservices
Evaluation AP-Count: Disabled
Total AP Count Licenses: 0
AP Count Licenses In-use: 0
AP Count Licenses Remaining: 0    *AP base license is reserved for future use
```

Adder AP-Count license: The adder AP-Count license is an “add as you grow” license. You can add access point licenses as your network grows. You activate an adder AP-count license by using EXEC commands, and it is activated without a switch reload.

This example shows the license summary display for a switch with an activated adder AP-Count license:

```
Switch1# show license right-to-use summary
  License Name    Type     Count   Period left
-----------------------------------------------
  ipservices   permanent   N/A      Lifetime
  apcount      base        0        Lifetime
  apcount      adder       10       Lifetime
--------------------------------------------
License Level In Use: ipservices
License Level on Reboot: ipservices
Evaluation AP-Count: Disabled
Total AP Count Licenses: 10
AP Count Licenses In-use: 0
AP Count Licenses Remaining: 10

Switch1# license right-to-use activate apcount 25 slot 1 acceptEULA
Switch1#
%SMN_HBL_LICENSE-6-AP_ADD: 1 stack-mgr:  25 Adder AP Count Licenses are added

Switch1# show license right-to-use summary
  License Name    Type     Count   Period left
-----------------------------------------------
  ipservices   permanent   N/A      Lifetime
  apcount      base        0        Lifetime
  apcount      adder       35       Lifetime
--------------------------------------------
License Level In Use: ipservices
License Level on Reboot: ipservices
Evaluation AP-Count: Disabled
Total AP Count Licenses: 35
AP Count Licenses In-use: 0
AP Count Licenses Remaining: 25
```

This example shows the license summary display for a switch with a deactivated adder AP-Count license:

```
Switch1# license right-to-use deactivate apcount 25 slot 1
Switch1#
%SMN_HBL_LICENSE-6-AP_DEL: 1 stack-mgr:  25 Adder AP Count Licenses are removed
```

```
Switch1# show license right-to-use summary
  License Name    Type     Count   Period left
-----------------------------------------------
  ipservices   permanent   N/A      Lifetime
  apcount      base        0        Lifetime
  apcount      adder       10       Lifetime
--------------------------------------------
License Level In Use: ipservices
License Level on Reboot: ipservices
```

```
Evaluation AP-Count: Disabled
Total AP Count Licenses: 10
AP Count Licenses In-use: 0
AP Count Licenses Remaining: 10
```

Image-Based License in a Stack

In a Cisco Catalyst 3850 Switch stack, all switches **must be at the same image-based license (IP Services/IP Base/LAN Base) level**. The active switch license level is considered the reference, and the member switch licenses are compared to it. If there is a mismatch, the active switch displays a syslog message saying that the stack configuration was unsuccessful.

This is an example of the display on the active switch console:

```
%STACKMGR-1-STACK_LINK_CHANGE: 1 stack-mgr:  Stack port 1 on switch 1 is up
%SMN_HBL_LICENSE-6-LIC_INCOMPAT: 1 stack-mgr:  Switch 2 has an incompatible
license level. Activate a compatible level to get the switch to join the stack.
Switch1#show switch
Switch/Stack Mac Address : 2037.0653.fd80
                                             H/W   Current
Switch1#   Role    Mac Address     Priority Version  State
------------------------------------------------------------
*1       Active   2037.0653.fd80     15      P6A     Ready
 2       Member   2037.0653.cb00     1       0       Lic-Mismatch
 3       Member   0000.0000.0000     0       0       Provisioned
```

This message appears on the member switch console:

```
%IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-DISC_START: Switch 2 is
starting stack discovery
Switch 2 has a license mismatch with the stack. Only on activating a compatible
license will the switch join
```

This display shows the license mismatch with the active switch:

```
Switch1# show license right-to-use mismatch
 Slot#    License Name    Adder AP Count   Base AP Count
----------------------------------------------------------
 2         ipbase                50                0

Switch1# show license right-to-use summary
  License Name    Type      Count   Period left
-----------------------------------------------
  ipservices   permanent   N/A      Lifetime
  apcount      base        0        Lifetime
  apcount      adder       0       Lifetime
--------------------------------------------
License Level In Use: ipservices
License Level on Reboot: ipservices
Evaluation AP-Count: Disabled
Total AP Count Licenses: 0
AP Count Licenses In-use: 0
AP Count Licenses Remaining: 0
```

To enable the member switch to join the stack, change the license level of the member switch (switch 2) by activating the license from the active switch console:

```
Switch1# license right-to-use activate ipservices slot 2 acceptEULA
% switch-1:stack-mgr:Reboot the switch to invoke the highest activated License
level

%SMN_HBL_LICENSE-6-LIC_ACT: 1 stack-mgr:  ipservices License is activated
successfully on switch 2
Switch1#reload slot 2
Stack is in Half ring setup; Reloading a switch might cause stack split
Proceed with reload? [confirm]
```

After switch 2 reloads successfully, it joins the stack with the active switch.

```
Switch1# show switch
Switch/Stack Mac Address : 2037.0653.fd80 - Local Mac Address
Mac persistency wait time: Indefinite
                                            H/W   Current
Switch#   Role    Mac Address     Priority Version  State
------------------------------------------------------------
*1        Active   2037.0653.fd80     15      P6A     Ready
 2        Standby  2037.0653.cb00     14      P6A     Ready
 3        Member   0000.0000.0000     0       0       Provisioned
```

AP-Count License in a Stack

AP-Count license is available only with IP Base and IP Services licenses. A Cisco Catalyst 3850 Switch stack can support a maximum of 50 access points. An AP-Count license is required only if a Cisco Catalyst 3850 Switch is configured as both a mobility controller and a mobility agent. An AP-Count license is not needed if the Cisco Catalyst 3850 Switch is configured only as an mobility agent, which is the default configuration. For details on mobility agent, mobility controller, and other wireless and mobility-related entities, refer to the Cisco Catalyst 3850 Switch converged access section.

The total AP-Count license of a Cisco Catalyst 3850 Switch stack is equal to the sum of all the individual member AP-Count licenses, up to a maximum of 50 AP-Counts. The total AP-Count license of the stack is affected when stack members are added or removed:

- When new members are added to the stack, the total AP-Count license of the stack is automatically recalculated.
- When members are removed from the stack, the AP-Count license contributed by the removed switch is decremented from the total available AP-Count license in the stack.
- If more AP-Counts are connected than the available AP-Count license, a syslog warning message indicates this fact without disconnecting the excess connected AP-Counts until a stack reload.
- After the stack reload, the surplus AP-Count s are removed from the total AP-Count. The following examples explain the process.

Stack member addition example: A Cisco Catalyst 3850 Switch stack includes 3 switches, each with an AP-Count license that allows 10 AP-Counts, for a total of 30 supported AP-Counts. When a new Cisco Catalyst 3850 Switch (switch 4) is added to the stack with an AP-Count license allowing 25 AP-Counts, the stack supports a total of 50 AP-Counts because the total number of 55 access points (30+25) exceeds the stack limit.

Stack member removal example: In the preceding example, if switch 4 is removed from the stack, the AP-Count license remains at 50 AP-Counts until the stack is reloaded, if 50 AP-Counts are connected and active in the stack. After reload, the stack returns to its original value of 30 AP-Counts.

When the AP-Count for a stack exceeds 50, a syslog message appears in the active and member switches to indicate the excess AP-Count:

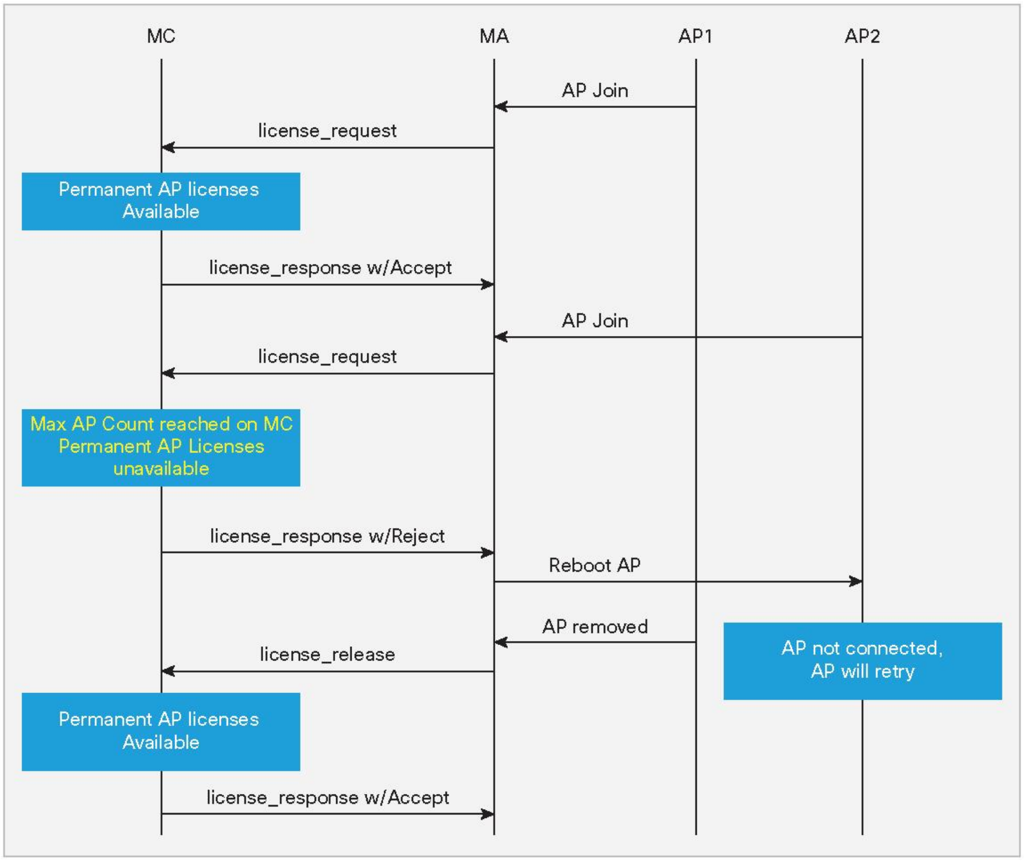
```
%IOSXE-1-PLATFORM: process stack-mgr: %SMN_HBL_LICENSE-1-EXCESS_AP_LIC: Total AP
Count Licenses available have exceeded the Maximum supported AP Count by 60


Switch1# show license right-to-use summary
  License Name    Type      Count    Period left
-----------------------------------------------
  ipservices    permanent   N/A       Lifetime
  apcount       base        0         Lifetime
  apcount       adder       110       Lifetime
--------------------------------------------
License Level In Use: ipservices
License Level on Reboot: ipservices
Evaluation AP-Count: Disabled
Total AP Count Licenses: 50
AP Count Licenses In-use: 0
AP Count Licenses Remaining: 50
```

By default the Cisco Catalyst 3850 Switch stack is configured as a mobility agent. In the wireless licensing model, a mobility agent is the access point count enforcement point. A mobility controller is the access point count management point. A Cisco Catalyst 3850 Switch stack can be configured as either a mobility controller or a mobility agent, or both, depending on the deployment requirement.

Figure 3 shows a typical licensing protocol interaction between an AP-Count, a mobility agent, and a mobility controller:

Figure 3. Licensing Protocol Call Flow


MC
MA
AP1
AP2
AP Join
license_request
Permanent AP licenses Available
license_response w/Accept
AP Join
license_request
Max AP Count reached on MC Permanent AP Licenses unavailable
license_response w/Reject
Reboot AP
AP removed
AP not connected, AP will retry
license_release
Permanent AP licenses Available
license_response w/Accept

In a large deployment, a Cisco Catalyst 3850 Switch stack is the mobility agent, and a 5760 wireless controller is the mobility controller. In a split mobility agent-mobility controller deployment, the AP-Count is managed at the mobility controller level.

License Migration Between Switches

You can easily migrate RTU licenses between Cisco Catalyst 3850 Switches. Both image-based and AP-Count licenses can be deactivated from one switch and activated on another switch. To deactivate a license, use the **license right-to-use deactivate** EXEC command. To activate a license, use the **license right-to-use activate** EXEC command.

These examples illustrate the process:

Example: Switch1 and Switch2 are nonstacked independent Cisco Catalyst 3850 Switches. To move the IP Services image-based license and 50 AP-Count license from Switch1 to Switch2:

Step 1. Verify the current licenses in Switch1:

```
Switch1# show license right-to-use summary
  License Name    Type     Count   Period left
-----------------------------------------------
  ipservices   permanent   N/A      Lifetime
  apcount      base        0        Lifetime
  apcount      adder       50       Lifetime
```

Step 2. Deactivate the image-based license and the AP-Count license from Switch1:

```
Switch1# license right-to-use deactivate ipservices slot 1
% switch-1:stack-mgr:Reboot the switch to invoke the highest activated License
level
Switch1#
%SMN_HBL_LICENSE-6-LIC_EULA_CLEAR: 1 stack-mgr:  EULA for ipservices License has
been cleared
%SMN_HBL_LICENSE-6-LIC_CHANGE: 1 stack-mgr:  Switch 1 Reboot License Level
changed from ipservices to lanbase, Reboot the switch to invoke the new license
level


Switch1# license right-to-use deactivate apcount 50 slot 1
Switch1#
%SMN_HBL_LICENSE-6-AP_DEL: 1 stack-mgr:  50 Adder AP Count Licenses are removed
```

Step 3. Reload Switch1 and verify that the licenses are cleared:

```
Switch1# show license right-to-use summary
  License Name    Type     Count   Period left
-----------------------------------------------
  lanbase      permanent   N/A      Lifetime
  apcount      base        0        Lifetime
  apcount      adder       0        Lifetime
--------------------------------------------
License Level In Use: lanbase
License Level on Reboot: lanbase
Evaluation AP-Count: Disabled
Total AP Count Licenses: 0
AP Count Licenses In-use: 0
AP Count Licenses Remaining: 0
```

Step 4. Enable the licenses in Switch 2:

```
Switch2# license right-to-use activate ipservices slot 2 acceptEULA
% switch-2:stack-mgr:Reboot the switch to invoke the highest activated License
level
Switch2#
%SMN_HBL_LICENSE-6-LIC_ACT: 2 stack-mgr:  ipservices License is activated
successfully on switch 2
%SMN_HBL_LICENSE-6-LIC_CHANGE: 2 stack-mgr:  Switch 2 Reboot License Level
changed from lanbase to ipservices, Reload the switch to invoke the new license
level
Switch2# license right-to-use activate apcount 50 slot 2 acceptEULA
Switch2#
%SMN_HBL_LICENSE-6-AP_ADD: 2 stack-mgr:  50 Adder AP Count Licenses are added
```

Step 5. Reload Switch 2 and confirm the active licenses:

```
Switch2# show license right-to-use summary
  License Name    Type     Count   Period left
-----------------------------------------------
  ipservices   permanent   N/A      Lifetime
  apcount      base        0        Lifetime
  apcount      adder       50       Lifetime

--------------------------------------------
License Level In Use: ipservices
License Level on Reboot: ipservices
Evaluation AP-Count: Disabled
Total AP Count Licenses: 50
AP Count Licenses In-use: 0
AP Count Licenses Remaining: 50
```

Evaluation RTU License

An evaluation license allows you to evaluate any license for 90 days free of charge. To activate an evaluation license, accept the EULA. The evaluation license EULA assumes that you will purchase a permanent license within 90 days; if you do not purchase a permanent license, the evaluation license is deactivated after 90 days. You receive a syslog message warning about deactivation 10 days before the evaluation license expires and another message 5 days before expiration. After the 90-day period expires, syslog messages appear every day until you reload the switch:

```
%SMN_HBL_LICENSE-1-EVAL_EXP: 1 stack-mgr:  Evaluation period of apcount eval
license expired 10 days ago. Purchase a permanent license.
%SMN_HBL_LICENSE-1-EVAL_EXP: 1 stack-mgr:  Evaluation period of apcount eval
license expired 11 days ago. Purchase a permanent license.
```

Note: You can activate a 90-day evaluation license only once on each Cisco Catalyst 3850 Switch. After the 90 days have expired, you cannot activate another 90-day evaluation license on the same switch.

Use these commands to enable an evaluation license:

```
Switch1# license right-to-use activate ipservices evaluation all acceptEULA
% Switch-1:stack-mgr:Reboot the switch to invoke the highest activated License
level
%SMN_HBL_LICENSE-6-LIC_ACT: 1 stack-mgr:  ipservices eval License is activated
successfully on switch 1
%SMN_HBL_LICENSE-6-LIC_CHANGE: 1 stack-mgr:  Switch 1 Reboot License Level
changed from ipbase to ipservices eval, Reboot the switch to invoke the new
license level
```

After a reload:

```
Switch1# show license right-to-use summary
License Name    Type     Count   Period left
-----------------------------------------------
  ipservices   evaluation  N/A      90
  apcount      base        0        Lifetime
  apcount      adder       0        Lifetime
--------------------------------------------
License Level In Use: ipbase
License Level on Reboot: ipservices eval
Evaluation AP-Count: Disabled
Total AP Count Licenses: 0
AP Count Licenses In-use: 0
AP Count Licenses Remaining: 0
```

Use these commands to deactivate an evaluation license:

```
Switch1# license right-to-use deactivate ipservices evaluation all
% switch-1:stack-mgr:Reboot the switch to invoke the highest activated License
level
Switch1#
%SMN_HBL_LICENSE-6-LIC_EULA_CLEAR: 1 stack-mgr:  EULA for ipservices eval License
has been cleared
%SMN_HBL_LICENSE-6-LIC_CHANGE: 1 stack-mgr:  Switch 1 Reboot License Level
changed from ipservices eval to ipbase, Reboot the switch to invoke the new
license level
```

Note: You must reload the switch to activate the correct license level.

License Usage Monitoring

The license usage record is maintained in the Cisco Catalyst 3850 Switch or switch stack for individual switches. The usage information is maintained from the initial boot and across reloads and includes the status of the EULA, in-use condition, and type of license. Deactivating a license resets the EULA status. The license information is updated daily for active in-use licenses and can be displayed by using the **show license right-to-use usage** command:

```
Switch1# show license right-to-use usage
 Slot#  License Name     Type     usage-duration(y:m:d)  In-Use  EULA
-----------------------------------------------------------------------
 1      ipservices     permanent     0 :0 :10               yes    yes
 1      ipservices     evaluation    0 :0 :0                no     no
 1      ipbase         permanent     0 :0 :0                no     yes
 1      ipbase         evaluation    0 :0 :0                no     yes
 1      lanbase        permanent*    0 :0 :3                no     yes
 1      apcount        evaluation    0 :0 :0                no     no
 1      apcount        base          0 :0 :0                no     no
 1      apcount        adder         0 :0 :9                yes    yes

 Slot#  License Name     Type     usage-duration(y:m:d)  In-Use  EULA
-----------------------------------------------------------------------
 2      ipservices     permanent     0 :0 :0                yes    yes
 2      ipservices     evaluation    0 :0 :0                no     no
 2      ipbase         permanent     0 :0 :0                no     yes
 2      ipbase         evaluation    0 :0 :0                no     no
 2      lanbase        permanent*    0 :0 :0                no     yes
 2      apcount        evaluation    0 :0 :0                no     no
 2      apcount        base          0 :0 :0                no     no
 2      apcount        adder         0 :0 :0                yes    yes
 Slot#  License Name     Type     usage-duration(y:m:d)  In-Use  EULA
----------------------------------------------------------------------
 3      ipservices     permanent    0 :0 :2              yes   yes
 3      ipservices     evaluation   0 :0 :0              no    no
 3      ipbase         permanent    0 :0 :0              no    no
 3      ipbase         evaluation   0 :0 :0              no    no
 3      lanbase        permanent*   0 :0 :0              no    yes
 3      apcount        evaluation   0 :0 :0              no    no
 3      apcount        base         0 :0 :0              no    no
 3      apcount        adder        0 :0 :2              yes   yes
* lanbase is the default license and hence lanbase evaluation license is not
applicable.
```

License Storage Management

The license information is stored in two hidden flash partitions: active and backup. The following information describes how the license information is stored and managed in the flash:

- Customer-ordered image-level license information is stored in the factory default license file, initially created by Cisco manufacturing.
- The license detail file maintains the license information for all the supported licenses, including license type, absolute usage, EULA acceptance status, and in-use state.
- License usage of the active licenses is updated once daily in the license detail file. The **license right-to-use activate** and **license right-to-use deactivate** commands also update the license detail file.
- A checksum is maintained and verified to prevent any tampering with the license files.
- Following activation, a license remains activated during reloads and image upgrades and downgrades.
- Erasing the configuration does not affect the license file because it is hidden in the flash.
- If the license file in the primary partition is corrupted or tampered with, the license file from the backup partition is used.
- If both the partitions are corrupted, Cisco can recreate the license files using the factory default files.

Cisco Catalyst 3850 Switch Stacking

Overview

Cisco Catalyst 3K switches define stacking architecture for enterprise networks to expand form factors, switching capacity, and redundancy in the wiring closet. Cisco StackWise® Plus is a proven and widely deployed cost-effective solution that delivers scale, performance, resiliency, and operational simplicity. To build the next-generation modular stack product, Cisco made significant changes to the StackWise Plus hardware and software architecture for the Cisco Catalyst 3850 Switch. The new Cisco Catalyst 3850 Switch is built upon high-speed next-generation Cisco application-specific integrated circuit (ASIC) technology and combined with the feature-rich and powerful Cisco IOS XE Software operating system.

The new StackWise-480 architecture allows you to build a high-speed stack ring with superior features and services scalability compared with StackWise Plus. The initial software version supports physically stacking up to four Cisco Catalyst 3850 Switches to form a stack ring. To accommodate varying port density requirements, the hardware can support both 48- and 24-port switches in a single stack ring. The Cisco Catalyst 3850 Switch deployed in stack mode is designed to deliver deterministic nonblocking switching performance to as many as 208 ports, including both wired and wireless network devices. The Cisco Catalyst 3850 Switch delivers uncompromised hardware-accelerated, rich integrated borderless network services and enterprise-class system resiliency. (See Figures 4 and 5).

Figure 4. Cisco Catalyst 3850 StackWise-480 Switch Stack Front View

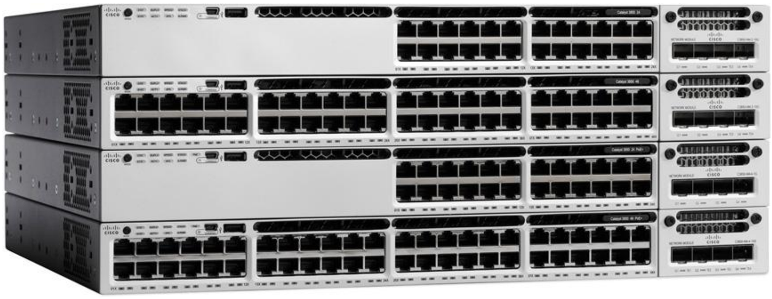
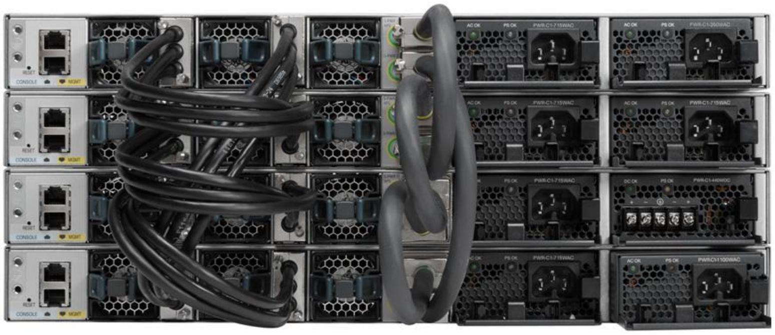


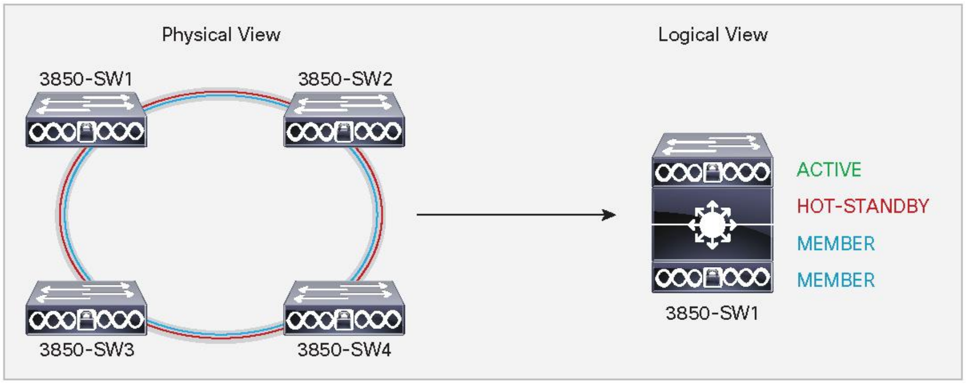
Figure 5. Cisco Catalyst 3850 StackWise-480 Switch Stack Rear View



The system architecture of the Cisco Catalyst 3850 Switch is designed to evolve as a solution engine that enables converged access infrastructure and rich integrated technologies with unparalleled application performance. This new Cisco switch delivers the simplified system operation tools that network administrators need to manage increasingly complex and feature-rich networks.

Cisco StackWise-480 provides a robust distributed forwarding architecture through each stack member switch and a unified, fully centralized control and management plane to simplify operation in a large-scale network design. One switch in a stack ring is elected to be the active switch. The active switch controls the management plane of the entire stack from both the network and user perspective. Figure 6 illustrates the physical versus logical view of a system in stack configuration mode.

Figure 6. Simplified Cisco Catalyst 3850 Switch Physical Versus Logical View



The system roles in the new resilient StackWise-480 architecture can be verified using the **show switch** EXEC command. The network administrator can check the current state of each member switch in the stack ring and identify the switch that is in hot-standby mode. The hot-standby switch assumes the active role when it detects a failure of the primary active switch.

This example shows the output of the **show switch** command used to display the switch roles in a configuration:

```
Switch#1# show switch
Switch/Stack Mac Address : 2037.06ce.0c00
Mac persistency wait time: Indefinite
                                                   H/W         Current
Switch#   Role     Mac Address     Priority        Version       State
-----------------------------------------------------------------------------
 1        Member   2037.06ce.0c40          1          P6A         Ready
*2        Active   2037.06ce.0c00         15          P6A         Ready
 3        Standby  2037.064d.2000         14          P6A         Ready
 4        Member   2037.06ce.0c80          1          P6A         Ready
```

Plug-and-Play Stack Deployment

Stack architecture allows network expansion when additional ports are required in the wiring closet. The hardware and software architecture of the Cisco Catalyst 3850 Switch allows you to insert new Cisco Catalyst 3850 Switches in a stack ring without major network disruption. The system and management operation, network configuration, and topologies remain transparent to the network, providing nonstop business communication during the upgrade.

This example shows the output of the **show switch stack-ports summary** command:

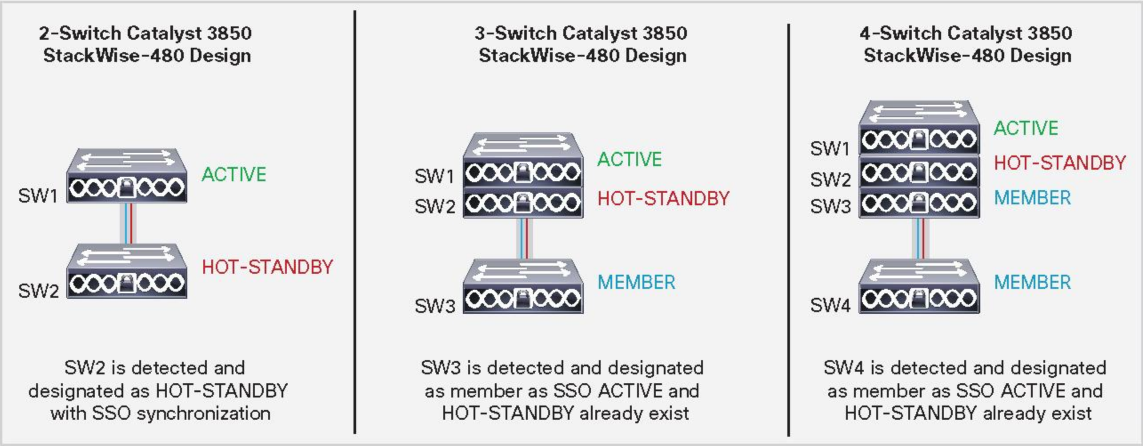
```
Switch1# show switch stack-ports summary
Sw#/Port#  Port Status  Neighbor  Cable Length   Link OK   Link Active   Sync OK
#Changes to LinkOK  In Loopback
----------------------------------------------------------------------------------
----------------------------------------------------------------------
```

```
1/1    OK        4     50cm     Yes     Yes      Yes     1        No
1/2    OK        2     50cm     Yes     Yes      Yes     1        No
2/1    OK        1     50cm     Yes     Yes      Yes     1        No
2/2    OK        3     50cm     Yes     Yes      Yes     1        No
3/1    OK        2     50cm     Yes     Yes      Yes     1        No
3/2    OK        4     50cm     Yes     Yes      Yes     1        No
4/1    OK        1     50cm     Yes     Yes      Yes     1        No
4/2    OK        3     50cm     Yes     Yes      Yes     1        No
```

The Cisco IOS XE Software high-availability framework is enabled by default on Cisco Catalyst 3850 Switches when they are deployed in StackWise-480 mode. The newly provisioned Cisco Catalyst 3850 Switch automatically discovers and dynamically joins the stack ring. The Cisco StackWise-480 technology features system-level N:1 high availability. Adding switches to and removing switches from a stack do not affect the active and hot standby roles already in effect in the stack.

To enable stateful switchover (SSO) resiliency in Cisco StackWise-480 mode, you must configure each switch with the same Cisco IOS XE Software version and license. Figure 7 illustrates system roles and operation of Cisco StackWise-480 when you add Cisco Catalyst 3850 Switches to a stack.

Figure 7. Plug-and-Play Cisco Catalyst 3850 Switch System Role Designation


2-Switch Catalyst 3850 StackWise-480 Design
SW1
ACTIVE
SW2
HOT-STANDBY
SW2 is detected and designated as HOT-STANDBY with SSO synchronization
3-Switch Catalyst 3850 StackWise-480 Design
SW1
ACTIVE
SW2
HOT-STANDBY
SW3
MEMBER
SW3 is detected and designated as member as SSO ACTIVE and HOT-STANDBY already exist
4-Switch Catalyst 3850 StackWise-480 Design
SW1
ACTIVE
SW2
HOT-STANDBY
SW3
MEMBER
SW4
MEMBER
SW4 is detected and designated as member as SSO ACTIVE and HOT-STANDBY already exist

The unique high-availability architecture in the Cisco StackWise-480 design enables distributed network services, such as flexible NetFlow, quality of service (QoS), and more, as well as providing system-level redundancy for all stack-member switches. During a complete stack reload, all switches participate in an election process to determine assignment of the active and standby roles. Several criteria, including switch priority and MAC addresses, are compared to elect the active and standby switches in the stack.

To assign the active and standby roles to specific switches, configure the default switch priority for all switches in the stack. You configure the priority once, usually during the initial configuration process, but you can change the configuration at any time. The configured switch priorities are immediately set in the boot loader configuration of each switch in the stack. This means the switch priority configuration cannot be verified from the startup or running configuration because it is programmed into different configuration components. The switch priority configuration in boot loader is parsed during the boot cycle, not read from the startup configuration stored in NVRAM.

To modify the default switch priority, use these EXEC commands:

```
Switch> enable
Switch# switch <number> priority 15
!Set priority 15 to elect switch in ACTIVE role

Switch# switch <number> priority 14
!Set priority 14 to elect switch in STANDBY role

Switch# switch <number> priority 13
!Set priority 13 to elect switch in next STANDBY role

Switch# switch <number> priority 12
!Set priority 12 to elect switch in next STANDBY role

To configure the switch number, use these commands

Switch> enable

Switch# switch <number> renumber <number>
!Statically renumber switch in stack ring
```

This example shows the priority of each switch and its role:

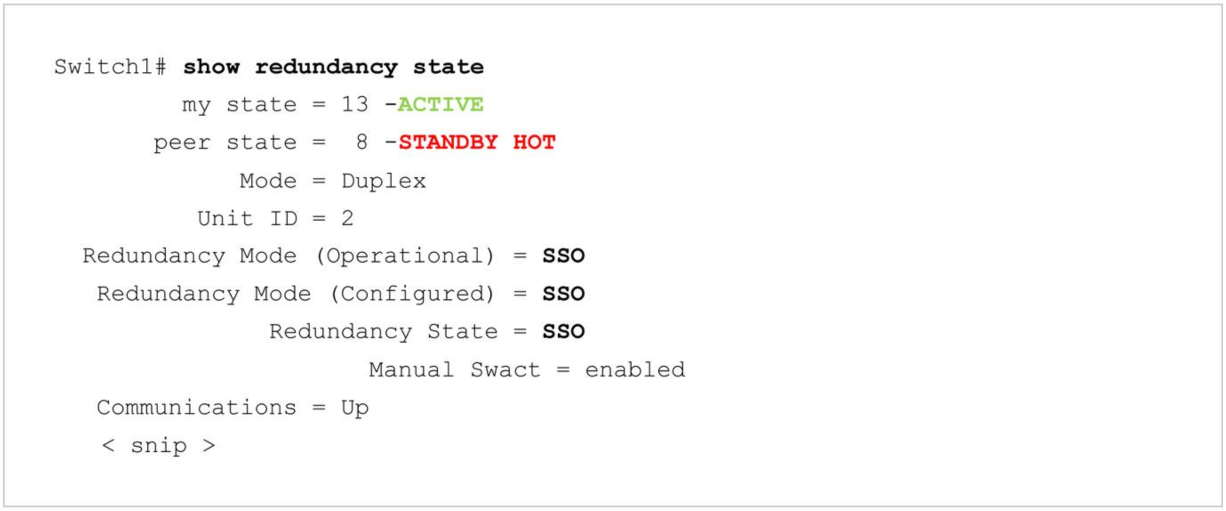
```
Switch1# show switch
Switch/Stack Mac Address : 2037.06ce.0c40
Mac persistency wait time: Indefinite
                                                      H/W         Current
Switch#   Role              Mac Address     Priority     Version      State
---------------------------------------------------------------------------
   1      Active       2037.06ce.0c40      15            P6A          Ready
  *2      Standby      2037.06ce.0c00      14            P6A          Ready
   3      Member       2037.064d.2000      13            P6A          Ready
   4      Member       2037.06ce.0c80      12            P6A          Ready
```

The Cisco Catalyst 3850 Switches support a wide range of Layer 2, Layer 3, and wireless stateful capabilities to provide nonstop network communication. In real time, the Cisco IOS XE Software running on the active switch synchronizes its protocol state machines, software forwarding tables, and system configuration to the Cisco IOS XE Software instance running on the standby switch. The other primary core services hosted by Cisco IOS XE Software are the integrated applications, such as the wireless control module (WCM). In Cisco StackWise-480 mode, the WCM is operational on the active Cisco Catalyst 3850 Switch that communicates with the locally attached Cisco wireless access points (WAPs), wireless clients, and distributed mobility peers to build a roaming network domain. The WCM on the standby switch is in hot-standby state as a Cisco IOS XE Software process. In real time, the active WCM performs the stateful synchronization of wireless protocols and control and provisioning of wireless access points (CAPWAP) tunnel information with the standby switch. If the active switch fails, the standby switch becomes the wireless controller by resynchronizing with the Cisco WAPs and mobility peers.

In the initial software release, the Cisco Catalyst 3850 Switch supports CAPWAP tunnels and Dynamic Transport Layer Security (DTLS), but not high availability for wireless clients. During a switchover, the new active WCM flushes the last-known wireless client and rebuilds the database and forwarding tables. As a result, the wireless client must restart communication with new wireless controller, using the same initial steps (such as 802.1X authentication, Dynamic Host Configuration Protocol [DHCP] request, and so on) to reconnect to the network.

Deploying Cisco Catalyst 3850 Switch StackWise-480 NSF and SSO

To maximize availability, the SSO capability is enabled by default when Cisco Catalyst 3850 Switches are deployed in Cisco StackWise-480 mode. No user configuration is required to enable SSO capability on a Cisco Catalyst 3850 Switch stack. You can verify that SSO is configured and operational by using the **show redundancy state** command. This is sample output showing SSO redundancy in a Cisco StackWise-480-based network design:



```
Switch1# show redundancy state
          my state = 13 -ACTIVE
        peer state =  8 -STANDBY HOT
              Mode = Duplex
           Unit ID = 2
  Redundancy Mode (Operational) = SSO
   Redundancy Mode (Configured) = SSO
               Redundancy State = SSO
                      Manual Swact = enabled
   Communications = Up
    < snip >
```

In stacking mode, the Cisco Catalyst 3850 active switch automatically performs SSO protocol synchronization with the standby switch. By default, the nonstop forwarding (NSF) subsystem in all the switches in a Cisco Catalyst 3850 Switch stack operates in NSF helper mode and supports nonstop data forwarding and graceful recovery during active to standby (Layer 3) switchover. Implementing NSF capability allows the remaining Cisco Catalyst 3850 Switches in the stack to continue forwarding data while the new active switch gracefully recovers the protocol state machines. To enable the graceful restart capability for supported protocols, you must manually enable graceful-restart capability under a routing instance. This sample configuration shows how to enable NSF capability for Enhanced Interior Gateway Routing Protocol (EIGRP):

```
Switch1(config)# router eigrp 100
Switch1(config-router)#nsf


Switch1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 100"
 < snip>
  EIGRP-IPv4 Protocol for AS(100)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
  EIGRP NSF enabled
     NSF signal timer is 20s
     NSF converge timer is 120s
    Router-ID: 10.125.100.16
< snip>
```

Converged Access with the Cisco Catalyst 3850 Switch

The Cisco Catalyst 3850 Switch can serve as an integrated wireless LAN controller for up to 50 directly attached Cisco access points and 2000 clients per stack. The Cisco Catalyst 3850 Switches can form the basis of a deployment that supports up to 250 Cisco access points and 16,000 clients. The converged access deployment mode builds on an existing Cisco Unified Wireless Network.

The converged access deployment is achieved by distributing some of the functions from the wireless LAN controllers (WLCs) to the Cisco Catalyst 3850 Switches in the access network. The access switches terminate the CAPWAP encapsulated wireless traffic locally and convert the wireless traffic into wired frames. This unifies wired and wireless traffic on the switch and makes it possible to apply the rich, intelligent wired services on wireless traffic.

This section explains the converged access deployment with the Cisco Catalyst 3850 Switches in detail. Before the details are explored, it is important to understand the functions that are distributed to the access switches.

Distributed Functions Enable Converged Access

There are three software functions (two required and one optional) that enable wireless services on WLC:

Mobility agent: The mobility agent manages CAPWAP tunnel terminations from access points and builds a database of client endpoints (mobile devices) that are served locally as well as roamed from an anchor WLC. The mobility agent also provides 802.1x authentication, proxy IGMP, and proxy ARP for locally served clients.

Mobility controller: The mobility controller provides a superset of the mobility agent software functions and manages mobility (roaming) for client stations that move from one WLC to another. The mobility controller provides guest access functionality by building an EtheroIP tunnel with the guest anchor controller in the DMZ. It also provides central management of the RF spectrum, such as rogue detection, dynamic channel assignment, transmission power on access points, coverage hole detection, and Cisco CleanAir® technology.

In addition, the mobility controller also builds a database of client stations across all the mobility agents. The mobility controller is responsible for caching the pairwise master key (PMK) of all clients on all the mobility agents; this enables fast roaming for the clients within its subdomain and mobility group.

The mobility controller controls a mobility subdomain. All the mobility agents in the subdomain form CAPWAP mobility tunnels to the mobility controller and report local and roamed client states to the mobility controller.

Because it performs these important functions, a mobility controller is a mandatory element in the converged access deployment. The mobility controller software function resides in the active member of a Cisco Catalyst 3850 Switch stack and can be assumed by the standby switch if the active switch fails. The active switch in a stack can host both the mobility controller function and the mobility agent function for all the locally connected Cisco access points.

By distributing these functions to the Cisco Catalyst 3850 Switches in the access network, the converged access network provides scalable, resilient, feature-rich wireless services along with wired services and features.

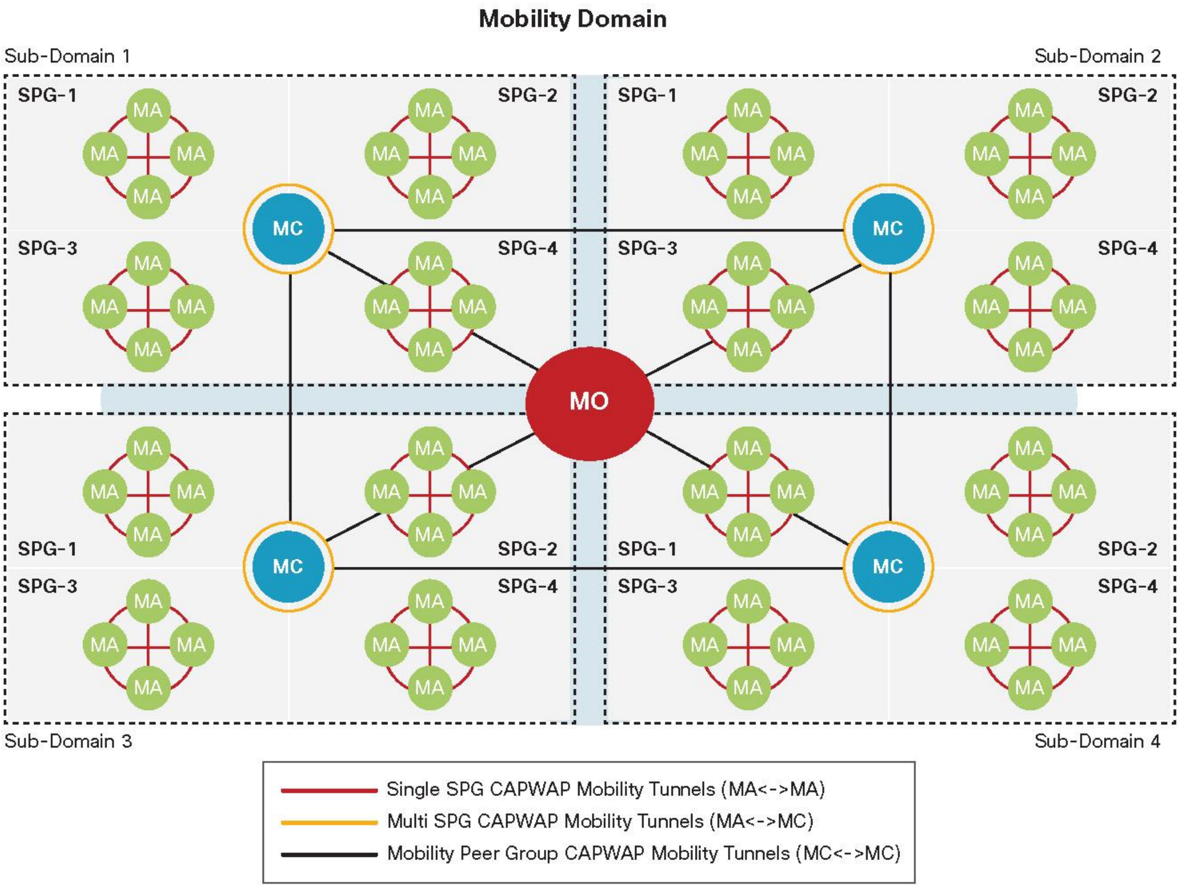
Mobility oracle: The mobility oracle is a software function that maintains client station visibility across the mobility controllers (mobility subdomains) in its mobility domain. The mobility oracle is an optional entity in the hierarchy of mobility agent-mobility controller-mobility oracle. The advantage of configuring a mobility oracle for a converged access deployment is that it scales and reduces control events for initial client joins and client roams, especially in a multi-mobility controller environment. This function cannot be hosted on the Cisco Catalyst 3850 Switch. It must be hosted on a Cisco 5508 WLC, WiSM2, or Cisco 5760 WLC with upgraded software. Typically, the mobility oracle is hosted on a controller appliance running the mobility controller function.

Logical Hierarchical Groupings of Roles

Mobility group: The Cisco Unified Wireless Network defines a mobility group as a logical group of mobility controllers that enable fast roaming for clients. In addition, the mobility group provides centralized RRM performed by a leader mobility controller that is either elected or statically configured.

Switch peer group: The converged access deployment defines a switch peer group (SPG) as a logical group of mobility agents within one mobility controller (or mobility subdomain). The main advantage of configuring SPGs is to restrict the roaming traffic to the switches within the SPG. When the mobility agents are configured in one SPG on the mobility controller, the software automatically forms full-mesh CAPWAP tunnels between the mobility agent switches. These CAPWAP tunnels can be formed in a multilayer network design (where the mobility agent switches are L2 adjacent) on a single VLAN or a routed access design (where the mobility agent switches are L3 adjacent). (See Figure 8).

Figure 8. Hierarchical Roles in Converged Access Deployment


Mobility Domain
Sub-Domain 1
Sub-Domain 2
Sub-Domain 3
Sub-Domain 4
SPG-1
SPG-2
SPG-3
SPG-4
MA
MC
MO
Single SPG CAPWAP Mobility Tunnels (MA<->MA)
Multi SPG CAPWAP Mobility Tunnels (MA<->MC)
Mobility Peer Group CAPWAP Mobility Tunnels (MC<->MC)

The SPGs should include the mobility agent switches that serve the domain where network users frequently roam. Intra-SPG roaming does not involve the mobility controller, whereas inter-SPG roaming requires traffic to traverse the mobility controller.

Converged Access Network Design with Cisco Catalyst 3850 Switch

Figure 9 shows a deployment suitable for a small branch office, with one Cisco Catalyst 3850 Switch serving as both mobility controller and mobility agent. This deployment supports up to 50 Cisco access points and 2000 clients.

Figure 9. Single Cisco Catalyst 3850 Switch Stack for Wired and Wireless in a Small Branch

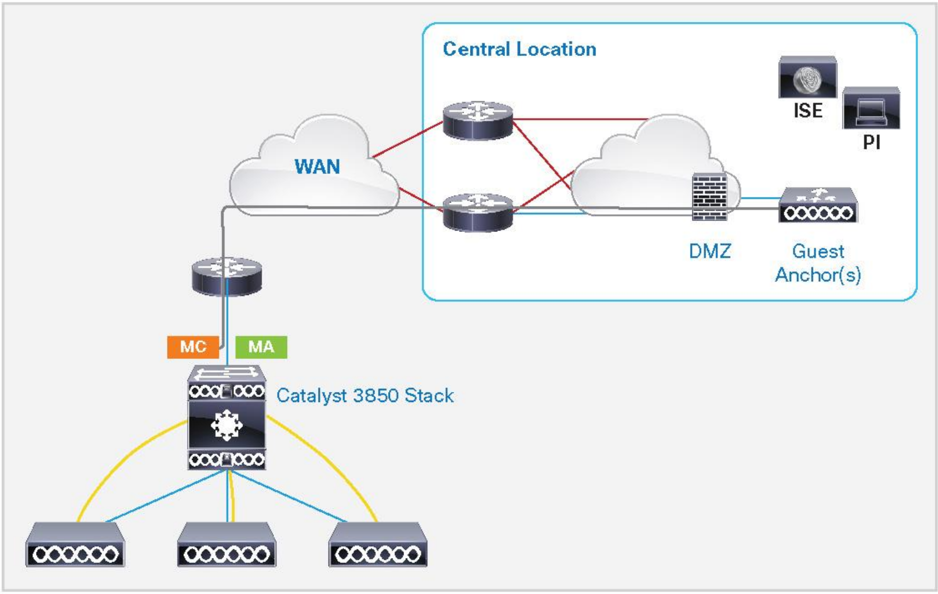


Figure 10 shows a deployment suitable for a medium to large branch office. The network includes one Cisco Catalyst 3850 Switch serving as a mobility controller, with additional Cisco Catalyst 3850 Switches serving as mobility agents. The mobility agents are configured in an SPG. This deployment supports up to 50 Cisco access points and 2000 clients.

Figure 10. Single Mobility Controller with Cisco Catalyst 3850 Switches for Wired and Wireless in Medium or Large Branch

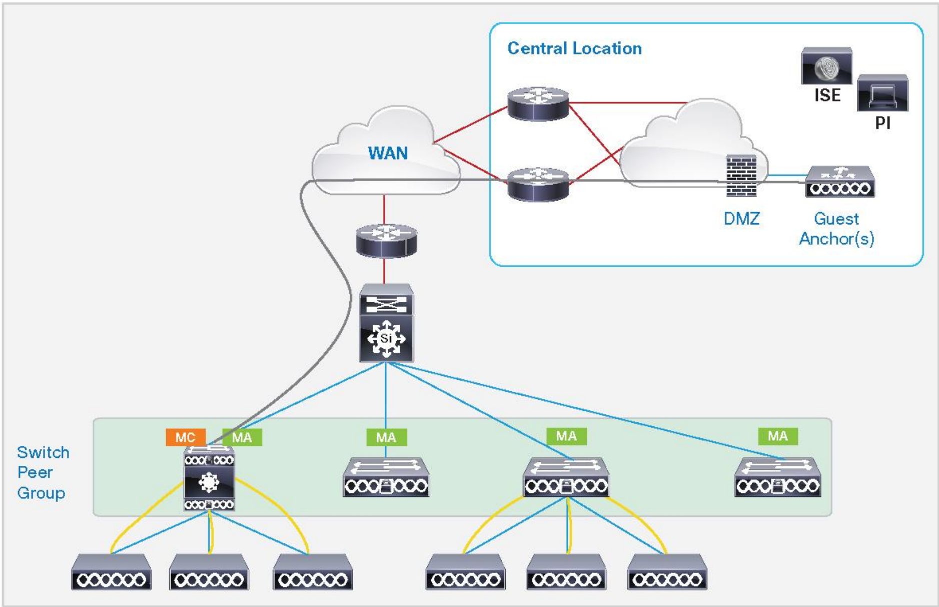


Figure 11 shows a medium size campus wireless deployment that can scale up to 250 Cisco access points and 16,000 clients. The network includes seven Cisco Catalyst 3850 Switches configured as mobility controllers (with additional switches operating as mobility agents in SPGs), all combined in a mobility group. Guest access is provided by guest anchor controllers in the DMZ.

Figure 11. Multiple Mobility Controllers with Cisco Catalyst 3850 Switches for Wired and Wireless in Medium or Large Campus

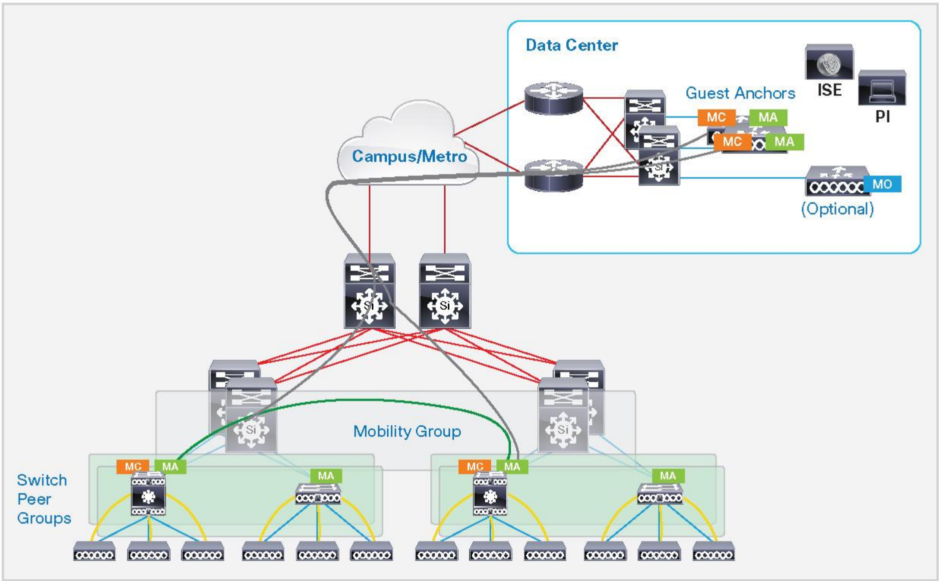
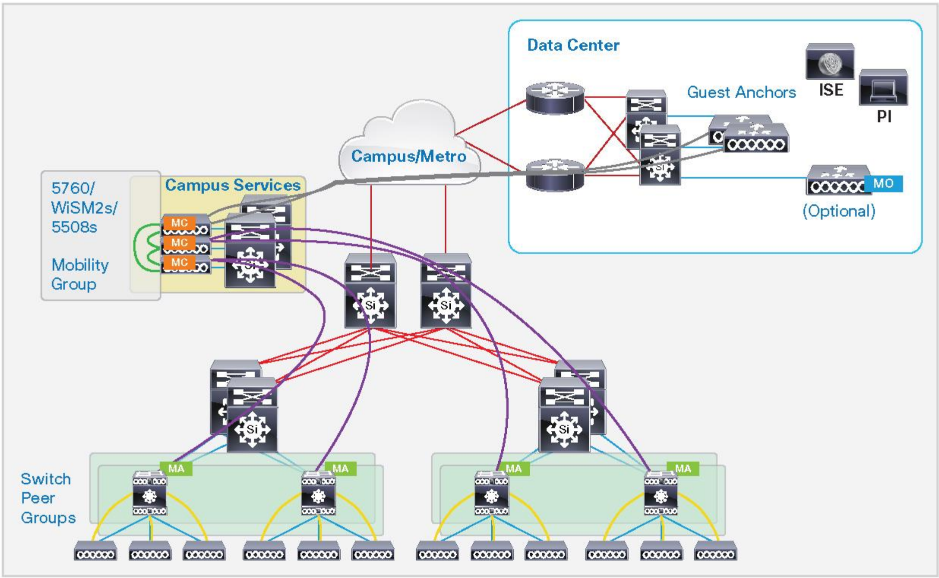


Figure 12 shows a large campus wireless deployment that can scale beyond 250 Cisco access points and 16,000 clients. In this deployment, Cisco Catalyst 3850 Switches are configured as as mobility agents and peered with a Cisco WLC (Cisco 5508 or WiSM2 Wireless LAN Controller with upgraded software, or a Cisco 5760 WLC) operating as a mobility controller.

Figure 12. Cisco 5508 or Cisco WiSM2 or Cisco 5760 Controller Appliances with Cisco Catalyst 3850 Switches for a Large Campus



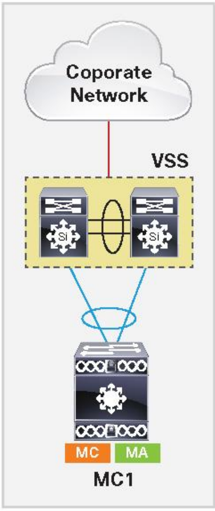
Case Study: Configuring Converged Access with the Cisco Catalyst 3850 Switch

This section explains how to configure the wireless services on the Cisco Catalyst 3850 Switch. The converged access deployment is explained using a case study that starts with a small branch that grows to a large branch or medium campus deployment.

Configuring the Small Branch Deployment

One Cisco Catalyst 3850 Switch forms the access layer. The distribution in this example is made of the Cisco Catalyst 4500E Supervisor 7-E systems in virtual switching system (VSS) configuration. It is a multilayer network design where the L3 switched virtual interfaces (SVIs) for L2 VLANs on the access are defined on the VSS system. The Cisco Catalyst 3850 Switch connects to the VSS through an L2 port channel configured as an 802.1Q trunk carrying all the VLANs. Three VLANs are used: VLAN 501 for wired clients, VLAN 500 for wireless clients, and VLAN 601 for switch and wireless management. The access points connect directly to the switch. (See Figure 13).

Figure 13. Cisco Catalyst 3850 Switch Mobility Controller and Mobility Agent



Use these commands to enable wireless termination on the Cisco Catalyst 3850 Switch:

```
MC1(config)# ap cdp
MC1(config)# wireless management interface vlan 601
MC1(config)# wireless mobility controller
%
Mobility role changed to Mobility Controller.
Please save config and reboot the whole stack.
```

The **ap cdp** command enables CDP process on the Cisco access points connected to the Cisco Catalyst 3850 Switch. The **wireless management interface** command is used to source the access point CAPWAP and other CAPWAP mobility tunnels. The **wireless mobility controller** command enables the switch to act as the mobility controller role for the converged access deployment. This command requires a reload of the switch. Save the configuration and reload the switch.

The next step is to configure service set identifiers (SSIDs), define wireless LAN (WLAN) on the switch, with corresponding VLAN used for wireless clients, the authentication and ciphers method, and the AAA server profile to use for this WLAN. In the following example, the name of the SSID is Cisco123, using the client VLAN 500 we defined for wireless clients, and enabling WPA, WPA2 with TKIP, using 802.1X authentication with the AAA server defined elsewhere in the configuration.

```
MC1(config)# wlan PROFILE 1 Cisco123
MC1(config-wlan)# aaa-override
MC1(config-wlan)# client association limit 2000
MC1(config-wlan)# client vlan 500
MC1(config-wlan)# security wpa wpa2 ciphers tkip
MC1(config-wlan)# security dot1x authentication-list ise
MC1(config-wlan)# no shutdown
```

To configure an open SSID, use the **no security wpa** command in the WLAN configuration.

To configure preshared key (PSK) security, use these commands:

```
MC1(config-wlan)# no security wpa akm dot1x
MC1(config-wlan)# security wpa akm psk set-key ascii 0 ciscoworks
```

This example shows output from the **show wireless mobility summary** command:

```
MC1# show wireless mobility summary
Mobility Controller Summary:
Mobility Role                                      : Mobility Controller
Mobility Protocol Port                             : 16666
Mobility Group Name                                : default
Controllers configured in the Mobility Domain:
IP                Public IP        Group Name       Multicast IP     Link Status
----------------------------------------------------------------------------
20.1.3.2          -                default                -          UP   : UP
```

This example shows output from the **show wlan summary** command:

```
MC1#show wlan summary
Number of WLANs: 1
WLAN Profile Name                SSID                            VLAN    Status
---------------------------------------------------------------------------
1    PROFILE                  Cisco123                          500       UP
```

This example shows output from the **show capwap summary** command:

```
MC1# show capwap summary
CAPWAP Tunnels General Statistics:
  Number of Capwap Data Tunnels       = 2
  Number of Capwap Mobility Tunnels   = 0
  Number of Capwap Multicast Tunnels  = 0
Name   APName                           Type PhyPortIf Mode      McastIf
------ -------------------------------- ---- --------- --------- -------
Ca5    3502E_G2/0/25_83A9               data Gi2/0/25  unicast    -
Ca4    3602I_G2/0/1_3A04                data Gi2/0/1   unicast    -
Name   SrcIP           SrcPort DestIP          DstPort DtlsEn MTU
------ --------------- ------- --------------- ------- ------ -----
Ca5    20.1.3.2        5247    20.1.3.54       63548   No     1657
Ca4    20.1.3.2        5247    20.1.3.53       58274   No     1657
```

The **show capwap summary** command output shows that two data CAPWAP tunnels are formed with the Cisco access points: Access point 3502E is connected to Gigabit Ethernet 2/0/25, and access point 3602I is connected to Gigabit Ethernet 2/0/1.

The switch and wireless management IP address is 20.1.3.2. This is the source IP address that the switch uses to form the data CAPWAP tunnels with the access points.

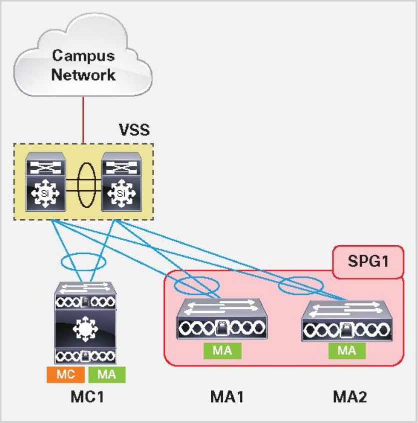
The access point IP addresses are the destination IP addresses: 20.1.3.54 on destination port 63584 and 20.1.3.53 on destination port 58274.

Configuring the Large Branch or Medium Size Campus Deployment

The single-switch network grows, and the network administrator needs to add more Cisco Catalyst 3850 Switches and expand wireless coverage to more endpoints and devices.

The existing Cisco Catalyst 3850 Switch remains the mobility controller. Additional Cisco Catalyst 3850 Switches are added and configured as mobility agents. The mobility agents can be configured in one switch peer group (SPG). (See Figure 14).

Figure 14. Cisco Catalyst 3850 Switch Mobility Controller and SPG



This example shows how to configure the SPG definitions and members on the mobility controller switch:

```
MC1(config)# wireless mobility controller peer-group SPG1
MC1(config)# wireless mobility controller peer-group SPG1 member ip 20.1.5.2
public-ip 20.1.5.2
MC1(config)# wireless mobility controller peer-group SPG1 member ip 20.1.7.2
public-ip 20.1.7.2
```

A switch peer group, SPG1, is defined on the mobility controller. The mobility agent switches included in SPG1 are configured with the switch and wireless management IP addresses 20.1.5.2 and 20.1.7.2.

On the mobility agent switches, configure the mobility controller, SSID, WLAN, and authentication methods. This example shows the configuration on the switch labeled MA1 in Figure 14:

```
MA1(config)# wireless mobility controller ip 20.1.3.2 public-ip 20.1.3.2
MA1(config)# wireless management interface Vlan602
MA1(config)# ap cdp
MA1(config)# wlan PROFILE 1 Cisco123
MA1(config-wlan)# aaa-override
MA1(config-wlan)# client association limit 2000
MA1(config-wlan)# client vlan 500
MA1(config-wlan)# security wpa wpa2 ciphers tkip
MA1(config-wlan)# security dot1x authentication-list ise
MA1(config-wlan)# no shutdown
```

The switch and wireless management IP address of the mobility controller switch is 20.1.3.2.

The switch and wireless management interface is VLAN 602.

The client VLAN that connects the mobility controller switch to the mobility agent switch is VLAN 500.

This example shows the configuration on the switch labeled MA2 in Figure 14:

```
MA2(config)# wireless mobility controller ip 20.1.3.2 public-ip 20.1.3.2
MA2(config)# wireless management interface Vlan603
MA2(config)# ap cdp
MA2(config)# wlan PROFILE 1 Cisco123
MA2(config-wlan)# aaa-override
MA2(config-wlan)# client association limit 2000
MA2(config-wlan)# client vlan 500
MA2(config-wlan)# security wpa wpa2 ciphers tkip
MA2(config-wlan)# security dot1x authentication-list ise
MA2(config-wlan)# no shutdown
```

The switch and wireless management IP address of the mobility controller switch is 20.1.3.2.

The switch and wireless management interface is VLAN 603.

The client VLAN that connects the mobility controller switch to the mobility agent switch is VLAN 500.

Note: The SPG definitions and the SPG membership are configured only on the mobility controller switch, and only the mobility controller definition is configured on the mobility agent switches. A complete configuration is in Appendix B.

The SPG membership defined on the mobility controller does not change depending on whether the access network between the mobility controller and mobility agent switches is Layer 2 or Layer 3.

Note: Advanced converged access configurations are described in the **Cisco Catalyst 3850 Switch Services Guide.**

Cisco Catalyst 3850 Switch Database Manager Template

Cisco Catalyst 3850 switch database manager (SDM) templates allow configuring the hardware resources based on the license level and features enabled in the switch. Two SDM templates are provided in the Cisco Catalyst 3850 Switch:

Advanced: This is the default template for all license levels. The advanced SDM template maximizes system resources for advanced features such as NetFlow, security access control, flow SPAN, multicast groups, and more.

VLAN: This template is available only in the LAN base license level and is enabled when the Cisco Catalyst 3850 Switch is deployed as a Layer 2 switch. Wireless features will not work with this SDM template configuration.

SDM Template Resources: VLAN and Advanced

Table 1 details the resource allocation for VLAN and advanced SDM templates. These resource allocations are based on L2 and IPv4 features. Because IPv6 features consume twice the ternary content addressable memory (TCAM) table size of IPv4 table entries, the switch supports half the number of TCAM table entries for IPv6.

Table 1. SDM Template Resource Allocation

Resource	Advanced Template	VLAN Template	Resource Explained
Number of VLANs	4094	4094	Maximum number of VLANs
Unicast MAC addresses	32768	32768	Maximum number of unicast MAC addresses
Overflow unicast MAC addresses	512	512	Used when the maximum unicast MAC address limit is reached
IGMP and multicast groups	8192	8192	Maximum number of IGMP and multicast groups
Overflow IGMP and multicast groups	512	512	Used when the maximum IGMP and multicast group limit is reached
Directly connected hosts	32768	32768	Maximum supported directly connected host routes
Indirect routes	8192	8192	Maximum supported indirect routes
Security access control entries	3072	3072	Maximum security ACEs
QoS access control entries	2816	3072	Maximum QoS ACEs
Policy-based routing ACEs	1280	0	Maximum PBR ACEs
NetFlow ACEs	1024	1024	Maximum NetFlow ACEs
Flow SPAN ACEs	256	256	Maximum SPAN ACEs
Tunnels	256	0	Maximum CAPWAP tunnels
Control plane entries	512	512	Internal software parameter

Resource	Advanced Template	VLAN Template	Resource Explained
Input NetFlow flows	8192	16384	Maximum ingress NetFlow flows
Output NetFlow flows	16384	8192	Maximum egress NetFlow flows

SDM Template Configuration

Use the **sdm prefer** configuration command to change the SDM template:

```
Switch(config)# sdm prefer ?
advanced  Advanced Template
vlan      Vlan Template

Switch(config)# sdm prefer vlan
Successfully set template id.
```

Reload the switch to activate the SDM template change.

Use the **show sdm prefer** command to confirm the current SDM template setting after the reload:

```
Switch# show sdm prefer
Showing SDM Template Info
This is the VLAN template for a typical Layer 2 network.
  Number of VLANs:                                      4094
  Unicast MAC addresses:                                32768
  Overflow Unicast MAC addresses:                       512
  IGMP and Multicast groups:                            8192
  Overflow IGMP and Multicast groups:                   512
  Directly connected hosts:                             32768
  Indirect routes:                                      8192
  Security Access Control Entries:                      3072
  QoS Access Control Entries:                           3072
  Policy Based Routing ACEs:                            0
  Netflow ACEs:                                         1024
  Input Microflow policer ACEs:                         0
  Output Microflow policer ACEs:                        0
  Flow SPAN ACEs:                                       256
  Tunnels:                                              0
  Control Plane Entries:                                512
  Input Netflow flows:                                  16384
  Output Netflow flows:                                 8192
```

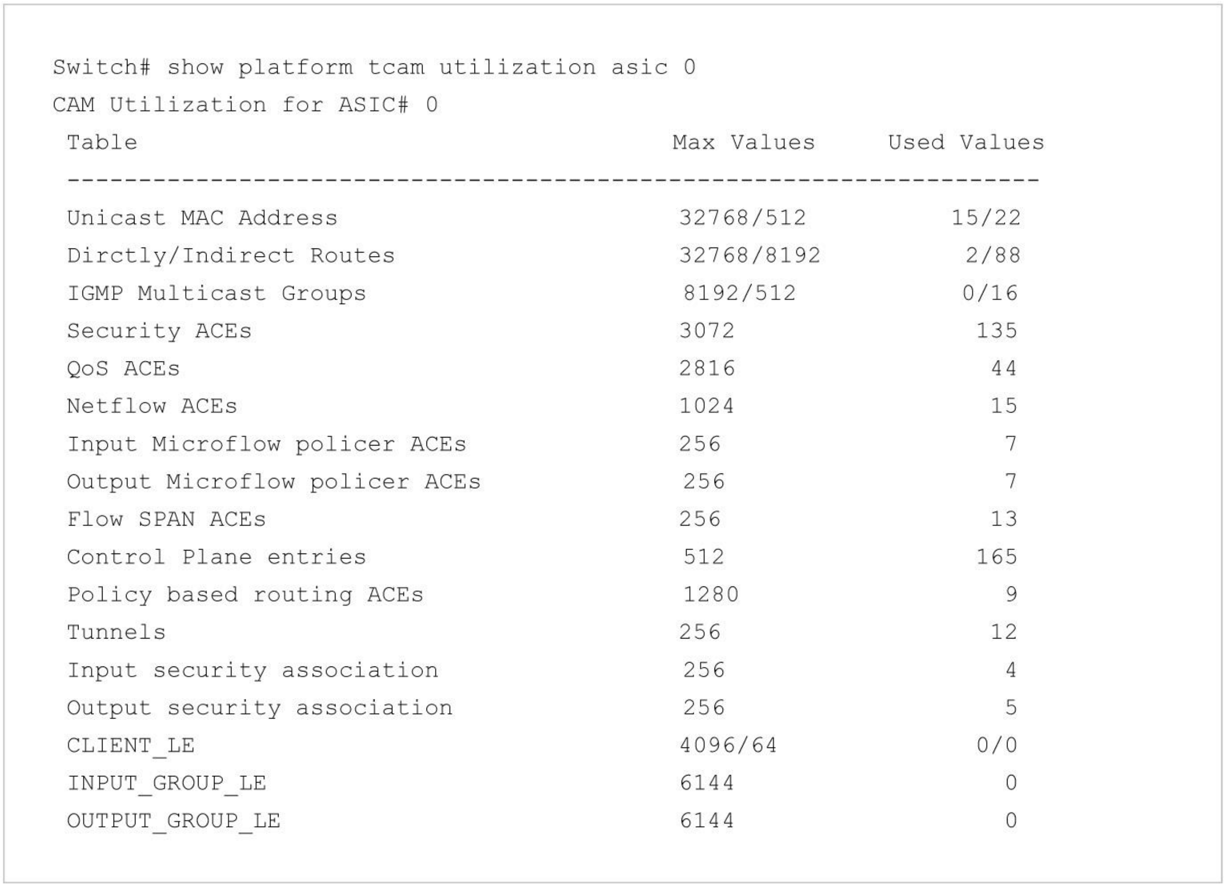
These numbers are typical for L2 and IPv4 features. For features such as IPv6 that consume double the entry size, only half as many entries can be created.

In a Cisco Catalyst 3850 Switch stack, an SDM template mismatch does NOT matter. As long as the license level matches, SDM mismatches are ignored, and all the stack switches use the active switch SDM template.

Monitoring SDM Resources

SDM template resources are crucial for normal operation of the Cisco Catalyst 3850 Switch. These resources are consumed based on the features/configuration and the traffic profile. Cisco recommends monitoring (for example, with Embedded Event Manager scripts) of TCAM resource utilization.

This example shows resource utilization for ASIC 0:



```
Switch# show platform tcam utilization asic 0
CAM Utilization for ASIC# 0
 Table                                     Max Values     Used Values
 --------------------------------------------------------------------
 Unicast MAC Address                        32768/512         15/22
 Dirctly/Indirect Routes                    32768/8192         2/88
 IGMP Multicast Groups                      8192/512           0/16
 Security ACEs                              3072                135
 QoS ACEs                                   2816                 44
 Netflow ACEs                               1024                 15
 Input Microflow policer ACEs               256                   7
 Output Microflow policer ACEs              256                   7
 Flow SPAN ACEs                             256                  13
 Control Plane entries                      512                 165
 Policy based routing ACEs                  1280                  9
 Tunnels                                    256                  12
 Input security association                 256                   4
 Output security association                256                   5
 CLIENT_LE                                  4096/64             0/0
 INPUT_GROUP_LE                             6144                  0
 OUTPUT_GROUP_LE                            6144                  0
```

Appendix A: List of Bootloader Commands

```
? -- Present list of available commands
         arp -- Show arp table or arp-resolve an address
        boot -- Load and boot an executable image
         cat -- Concatenate (type) file(s)
        copy -- Copy a file
      delete -- Delete file(s)
         dir -- List files in directories
emergency-install -- Initiate Disaster Recovery
  flash_init -- Initialize filesystem(s)
      format -- Format a filesystem
        fsck -- Check filesystem consistency
        help -- Present list of available commands
      memory -- Present memory heap utilization information
       mkdir -- Create dir(s)
        more -- Concatenate (display) file(s)
        ping -- Send ICMP ECHO_REQUEST packets to a network host
      rename -- Rename a file
       reset -- Reset the system
       rmdir -- Delete empty dir(s)
         set -- Set or display environment variables
   set_param -- Set system parameters in flash
        type -- Concatenate (type) file(s)
       unset -- Unset one or more environment variables
     version -- Display boot loader version
```

Appendix B: Cisco Catalyst 3850 Switch Mobility Agent and Mobility Controller Configurations

Cisco Catalyst 3850: Mobility Agent

```
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
service compress-config
!
hostname 3850-Access-MA
!
boot-start-marker
boot system switch all flash:packages.conf
boot-end-marker
!
username <removed> password 0 <removed>
aaa new-model
!
aaa authentication login no_auth none
aaa authentication dot1x default group radius
aaa authentication dot1x wireless group ise
aaa authorization network default group ise
aaa accounting network default start-stop group ise
!
aaa server radius dynamic-author
 client <IP> server-key <removed>
 auth-type any
!
aaa session-id common
switch 1 provision ws-c3850-48p
switch 2 provision ws-c3850-48p
switch 3 provision ws-c3850-48p
…
<snip>
…
dot1x system-auth-control
!
redundancy
 mode sso
!
vlan 500
```

Cisco Catalyst 3850: Mobility Agent

```
 name WIRELESS_CLIENT_VLAN
!
vlan 501
 name WIRED_CLIENT_VLAN
!
vlan 601
 name AP_MGMT_VLAN
!
interface Port-channel1
 description Connected to Distribution-Switch
 switchport mode trunk
…
<snip>
…
interface GigabitEthernet1/0/1
 description Connected to PC
 switchport access vlan 501
 switchport mode access
!
interface TenGigabitEthernet1/1/1
description Connected to Distribution-Switch
 switchport mode trunk
 load-interval 30
 channel-group 128 mode desirable
!
interface TenGigabitEthernet1/1/2
 description Connected to Distribution-Switch
 switchport mode trunk
 load-interval 30
 channel-group 128 mode desirable
!
interface GigabitEthernet2/0/1
 description Connection to 3500 Series AP
 switchport access vlan 601
 switchport mode access
 load-interval 30
!
…
<snip>
…
interface TenGigabitEthernet3/1/1
description Connected to Distribution-Switch
 switchport mode trunk
```

Cisco Catalyst 3850: Mobility Agent

```
 load-interval 30
 channel-group 128 mode desirable
!
interface TenGigabitEthernet1/1/2
 description Connected to Distribution-Switch
 switchport mode trunk
 load-interval 30
 channel-group 128 mode desirable
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan601
 description AP MGMT SVI
 ip address <IPADDR> <MASK>
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 <Gateway>
!
radius-server host <IP> key <removed>
radius-server retransmit 0
!
radius server ise
 address ipv4 <IP> auth-port 1812 acct-port 1813
 key <removed>
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 login authentication no_auth
 history size 254
 stopbits 1
 speed 115200
line aux 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 password cisco
```

Cisco Catalyst 3850: Mobility Agent

```
 logging synchronous
 login authentication no_auth
 length 0
 transport input all
line vty 5 15
!
wireless management interface Vlan601
!
wireless mobility controller ip <MC-VLAN602-IPADDR>
 public-ip <MC-VLAN602-IPADDR>
!
wlan <name> <ID> <SSID>
 aaa-override
 client vlan 500
 security wpa wpa2 ciphers tkip
 security dot1x authentication-list ise
 no shutdown
!
wireless rf-network <NAME>
!
wlan <name> <ID> <SSID>
 aaa-override
 client vlan 500
 security wpa wpa2 ciphers tkip
 security dot1x authentication-list ise
 no shutdown
!
ap cdp
ap dot11 24ghz rrm channel dca 1
ap dot11 24ghz rrm channel dca 6
ap dot11 24ghz rrm channel dca 11
ap dot11 5ghz rrm channel dca 36
ap dot11 5ghz rrm channel dca 40
ap dot11 5ghz rrm channel dca 44
ap dot11 5ghz rrm channel dca 48
ap dot11 5ghz rrm channel dca 52
ap dot11 5ghz rrm channel dca 56
ap dot11 5ghz rrm channel dca 60
ap dot11 5ghz rrm channel dca 64
ap dot11 5ghz rrm channel dca 149
ap dot11 5ghz rrm channel dca 153
ap dot11 5ghz rrm channel dca 157
ap dot11 5ghz rrm channel dca 161
```

Cisco Catalyst 3850: Mobility Agent

```
ap group default-group
end
```

Cisco Catalyst 3850: Mobility Controller

```
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
service compress-config
!
hostname 3850-Access-MC
!
boot-start-marker
boot system switch all flash:packages.conf
boot-end-marker
!
username <removed> password 0 <removed>
aaa new-model
!
aaa authentication login no_auth none
aaa authentication dot1x default group radius
aaa authentication dot1x wireless group ise
aaa authorization network default group ise
aaa accounting network default start-stop group ise
!
aaa server radius dynamic-author
 client <IP> server-key <removed>
 auth-type any
!
aaa session-id common
switch 1 provision ws-c3850-48p
switch 2 provision ws-c3850-48p
switch 3 provision ws-c3850-48p
…
<snip>
…
dot1x system-auth-control
!
```

Cisco Catalyst 3850: Mobility Controller

```
redundancy
 mode sso
!
vlan 502
 name WIRELESS_CLIENT_VLAN
!
vlan 503
 name WIRED_CLIENT_VLAN
!
vlan 602
 name AP_MGMT_VLAN
!
interface Port-channel1
description Connected to Distribution-Switch
switchport mode trunk
…
<snip>
…
interface GigabitEthernet1/0/1
 description Connected to PC
 switchport access vlan 503
 switchport mode access
!
interface TenGigabitEthernet1/1/1
description Connected to Distribution-Switch
 switchport mode trunk
 load-interval 30
 channel-group 128 mode desirable
!
interface TenGigabitEthernet1/1/2
 description Connected to Distribution-Switch
 switchport mode trunk
 load-interval 30
 channel-group 128 mode desirable
!
interface GigabitEthernet2/0/1
 description Connection to 3500 Series AP
 switchport access vlan 602
 switchport mode access
 load-interval 30
!
…
<snip>
```

Cisco Catalyst 3850: Mobility Controller

```
…
interface TenGigabitEthernet3/1/1
description Connected to Distribution-Switch
 switchport mode trunk
 load-interval 30
 channel-group 128 mode desirable
!
interface TenGigabitEthernet1/1/2
 description Connected to Distribution-Switch
 switchport mode trunk
 load-interval 30
 channel-group 128 mode desirable
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan602
 description AP MGMT SVI
 ip address 20.1.3.2 255.255.255.0
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 <Gateway>
!
radius-server host <IP> key <removed>
radius-server retransmit 0
!
radius server ise
 address ipv4 <IP> auth-port 1812 acct-port 1813
 key <removed>
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 login authentication no_auth
 history size 254
 stopbits 1
 speed 115200
line aux 0
 stopbits 1
```

Cisco Catalyst 3850: Mobility Controller

```
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 password cisco
 logging synchronous
 login authentication no_auth
 length 0
 transport input all
line vty 5 15
!
wireless management interface Vlan602
wireless mobility controller
wireless mobility controller peer-group SPG1
wireless mobility controller peer-group SPG1 member ip <MA-VLAN601-IPADDR>
 public-ip <MA-VLAN601-IPADDR>
!
wireless mobility controller peer-group SPG2
wireless mobility controller peer-group SPG2 member ip <MA-APMGMT-VLAN-IP>
public-ip <MA-APMGMT-VLAN-IP>
!
wireless mobility group member ip <MC-IPADDR>
public-ip <REMOTE-MC-IPADDR> group <PEER-GROUP-NAME>
wireless mobility group name <PEER-GROUP-NAME>
!
wireless rf-network <NAME>
!
wlan <name> <ID> <SSID>
 aaa-override
 client vlan 502
 security wpa wpa2 ciphers tkip
 security dot1x authentication-list ise
 no shutdown
!
ap cdp
ap dot11 24ghz rrm channel dca 1
ap dot11 24ghz rrm channel dca 6
ap dot11 24ghz rrm channel dca 11
ap dot11 5ghz rrm channel dca 36
ap dot11 5ghz rrm channel dca 40
ap dot11 5ghz rrm channel dca 44
ap dot11 5ghz rrm channel dca 48
ap dot11 5ghz rrm channel dca 52
ap dot11 5ghz rrm channel dca 56
```

Cisco Catalyst 3850: Mobility Controller

```
   ap dot11 5ghz rrm channel dca 60
   ap dot11 5ghz rrm channel dca 64
   ap dot11 5ghz rrm channel dca 149
   ap dot11 5ghz rrm channel dca 153
   ap dot11 5ghz rrm channel dca 157
   ap dot11 5ghz rrm channel dca 161
   ap group default-group
   end
```

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 **www.cisco.com/go/offices.**

Printed in USA C07-727067-00 03/13