Converged Wired and Wireless Access

This workflow explains how to enable the converged access functionality of the switch, and explains how the switch can operate as the wireless mobility controller (MC) as well as the wireless mobility anchor (MA) in a small branch deployment.

Wired and wireless features that are enabled in the same platform is referred to as *converged access*. The wired plus wireless features are bundled into a single Cisco IOS Software image, which reduces the number of software images that users have to qualify and certify before enabling them in their network.

Converged access improves wireless bandwidth across the network and the scale of wireless deployment. For example, a 48-port Catalyst 3850 switch provides 40 Gbps of wireless throughput. This wireless capacity increases with the number of members in the stack. This ensures that the network will scale with current wireless bandwidth requirements, as dictated by IEEE 802.11n-based access points and with future wireless standards such as IEEE 802.11ac.

Prerequisites

Complete the following tasks before proceeding with wireless configuration:

- Switch stack must function in Stateful Switchover (SSO) mode.
- Interface configuration is completed, as explained in the "Access Interface Connectivity" workflow.
- Lightweight access points are used.
- NTP configuration should be present and operational, as explained in the "Global System Configuration" workflow.
- A wireless site survey should be completed. The site survey identifies the proper placement of wireless access points for the best coverage. For detailed information about the site survey process and the tool to use, see the *Wireless Site Survey FAQ*.
- Complete the QoS workflow.

Restrictions

- AP-count licenses are supported only on IP Base and IP Services licenses. See the *Cisco Catalyst 3850 Switch Right-to-Use Licensing Model*.

- A Catalyst 3850 switch stack can support a maximum of 50 access points.
- A Cisco Catalyst 3650 stack can support a maximum of 25 access points.
- WLAN cannot use client VLAN 0.

Identify Configuration Values

We recommend that you identify certain switch configuration values in advance so that you are ready to proceed with this section without interruption. As you follow the configuration sequence, replace the values in column B with your values in column C.

Note This workflow contains two separate IP subnets that contain VLANs used for access points and wireless clients. The access points are on VLAN 12, and use IP subnet 192.168.12.x. The wireless clients are on VLAN 200, and use IP subnet 192.168.13.x.

Note In the configuration examples, you must replace the blue italicized example values with your own values.

Table 10 Wireless LAN Controller Values

A. Value Name	B. Example Value Names	C. Your Value
Number of access point count licenses and slots	*10/1, 15/2*	
Management VLAN	*wireless-management-vlan*	
Management VLAN access point and description	*Wireless VLAN* *Wireless Management VLAN Interface*	
IP address for VLAN interface managing access points	*192.168.12.2 255.255.255.0*	
Access point pool	*APVlan10-Pool*	
Access point client pool	*192.168.12.0 255.255.255.0*	
Default router for client	*10.1.1.1*	
excluded address	*192.168.12.1*	
Wireless management interface	*vlan12*	
Access interface	*GigabitEthernet1/0/3*	
Description	*Lightweight Access Point*	
WLAN interface for client VLAN	*200*	
WLAN profile and ID	*Wireless_Client*	
Wireless client VLAN IP address	*192.168.13.2 255.255.254.0*	
WLAN for easy-RADIUS and ID	*OPEN_WLAN 1 open_wlan*	
RADIUS server	*AuthServer*	

Table 10 Wireless LAN Controller Values

A. Value Name	B. Example Value Names	C. Your Value
IPv4 address for RADIUS	***192.168.254.14***	
Auth-port	***1645***	
Acct-port	***1646***	
AAA group	***RADIUS-GROUP***	
RADIUS server dead-criteria time/tries	***10/3***	
RADIUS server deadtime	***1***	
WLAN with WPA2 and IEEE 802.1x enabled	***Secure_WLAN1 CISCO_WLAN***	
Input service policy	***wlan-Guest-Client-Input-Policy***	
Output service policy	***wlan-Guest-SSID-Output-Policy***	

Note Configuration examples begin in global configuration mode, unless noted otherwise.

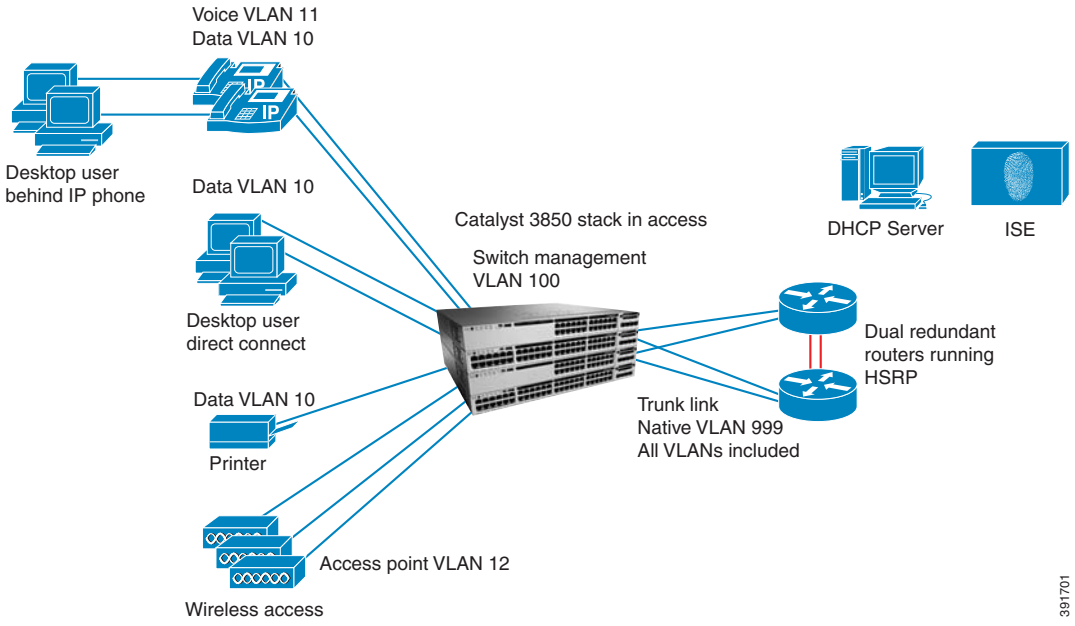
LAN Access Switch Topology with Wireless Connectivity

This topology shows the switch stack connected to multiple routers. The most common deployment of converged access is in a branch scenario, but this workflow also applies to a campus deployment.

The switch is stacked and acts as both the MC and MA. In a single stack converged access deployment, the switch can support up to 50 directly connected access points. For converged access, at least one lightweight access point is required. A maximum of 50 access points can be supported by a switch stack.

We recommend that you distribute the access points equally across the stack to achieve reliability during switchover scenarios preventing connectivity loss to access points connected to a member or standby switch.

Figure 13 LAN Access Switch Topology with Wireless Connectivity



Enable the Switch as a Wireless Controller

- Install Access Point Licenses on the Switch
- Configure a Wireless Management VLAN
- Configure Service Connectivity
- Enable Wireless Controller Functionality
- Change a Switch to Run in Mobility Controller Mode
- Enable the Access Point Connections

Install Access Point Licenses on the Switch

For ease of use, an evaluation license is preinstalled on your switch, but you are required to accept the End-User-License Agreement (EULA) before the 90-day period expires.

The IP Base and IP Services image-based licenses support wireless functionality. The minimum license level for wireless functionality is IP Base.

The total AP-count license of a switch stack is equal to the sum of all the individual member AP-count licenses, up to a maximum of 50 AP-count licenses.

The total AP-count license of the stack is affected when stack members are added or removed:

- When a new member is added to the stack that has an existing AP-count license, then the total available AP-count license for the switch stack is automatically recalculated.
- When members are removed from the stack, the total AP-count license is decremented from the total available AP-count license in the stack.

- If more access points are connected that exceed the total number of accepted AP-count licenses, a syslog warning message is sent without disconnecting the newly connected access points until a stack reload.
- After a stack reload, the newly connected access points are removed from the total access point count.

You can activate permanent RTU licenses after you accept the EULA. The EULA assumes you have purchased the permanent license. Use AP-count adder type licenses to activate access point licenses. 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.

Step 1 Activate a permanent access point license and accept the EULA.

Access point licenses are configured for permanent or for evaluation purposes. To prevent disruptions in operation, the switch does not change licenses when an evaluation license expires. You get a warning that your evaluation license will expire and you must disable the evaluation license and purchase a permanent one.

We recommend that you purchase and activate a permanent license and accept the EULA to avoid an untimely expiration.

The following examples activate 10 access point licenses on member 1 and 15 on member 2.

```
license right-to-use activate apcount 10 slot 1 acceptEULA
license right-to-use activate apcount 15 slot 2 acceptEULA
```

For more information about RTU licenses, see the "Configuring Right-To-Use Licenses" chapter in the *System Management Configuration Guide, Cisco IOS SE Release 3E*.

Verify AP-Count License Installation

Step 2 Verify the allocation of the access point licenses on the switch.

The following example shows two members in the stack:

```
show license right-to-use

Slot#  License name   Type     Count   Period left
--------------------------------------------------------
1      ipbase       permanent     N/A   Lifetime
1      lanbase      permanent     N/A   Lifetime
1      apcount      adder         10    Lifetime
License Level on Reboot: ipbase
  Slot#  License name   Type     Count   Period left
--------------------------------------------------------
2      ipbase       permanent     N/A   Lifetime
2      lanbase      permanent     N/A   Lifetime
2      apcount      adder         15    Lifetime
License Level on Reboot: ipbase
```

Step 3 Verify the RTU license summary details.

The example shows that a permanent IP Services license is installed and is available upon switch reboot: Five AP-count licenses are in use.

```
show license right-to-use summary

  License Name    Type     Count   Period left
------------------------------------------------
  ipservices   permanent   N/A      Lifetime
  apcount      base        0       Lifetime
  apcount      adder       25      Lifetime

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

License Level In Use: ipservices
License Level on Reboot: ipservices
Evaluation AP-Count: Disabled
Total AP Count Licenses: 25
AP Count Licenses In-use: 5
AP Count Licenses Remaining: 20
```

Configure a Wireless Management VLAN

Step 4 Configure the VLAN and SVI and assign it an IP address.

A wireless management VLAN is used for access point CAPWAP and other CAWAP mobility tunnels. The creation of a wireless management VLAN is mandatory. First, configure the VLAN in hardware and then create the SVI and assign it to an IP address. (See the "Create a Management VLAN in Hardware" section in the Initial Switch Configuration workflow.)

```
! To activate the VLAN in the database if it does not exist.
interface vlan 12
  name Wireless VLAN
  description Wireless Management VLAN Interface
  ip address 192.168.12.2 255.255.255.0
  no shutdown
  end
```

Configure Service Connectivity

Step 5 Create a name for the server address pool and specify the subnet network number and mask of the address pool client, and the default router for the client.

If you want the switch to receive IP address information you must configure the server with the IP address and subnet mask of the client and a router IP address to provide a default gateway for the switch. The server uses the DNS server to resolve the TFTP server name to an IP address, but configuration of the DNS server IP address is optional.

In small branch deployments in which the MC and MA are combined, we recommend using the switch as the server for the lightweight access points. In this deployment, the switch operates in Layer 2 mode, and the upstream router provides all routing functions.

We recommend that you exclude the IP address already used for the default router and the in-use wireless management SVI address to prevent an upstream router from allocating this IP address to an access point.

```
ip  pool APVlan10-Pool
network 192.168.12.0 255.255.255.0
default-router 192.168.12.1
ip  excluded-address 192.168.12.1 192.168.12.2
```

Enable Wireless Controller Functionality

Step 6 Configure an SVI (rather than a physical interface) as the management VLAN.

The **wireless management interface** command is used to source the access point CAPWAP and other CAPWAP mobility tunnels.

An SVI must be configured with an IP address before enabling the wireless controller.

```
wireless management interface vlan12
```

Change a Switch to Run in Mobility Controller Mode

Step 7 Enable the switch as an MC before the AP-count license installation.

In the wireless licensing model, the MA is the access point enforcer and the MC is the gatekeeper of the access points. The MC allows an access point to join the switch or not. The default role of the switch after boot up is an MA.

It is mandatory to save the configuration and reload the switch for the MC role to take effect.

```
wireless mobility controller
%
Mobility role changed to Mobility Controller. Please save config and
reboot the whole stack.
end
write memory
reload
proceed with reload? [confirm] y
```

Step 8 After the switch reboots, verify that the role of the switch has changed to Mobility Controller.

```
show wireless mobility summary

Mobility Controller Summary:

Mobility Role                                   : Mobility Controller
Mobility Protocol Port                          : 16666
Mobility Group Name                             : default
Mobility Oracle IP Address                      : 0.0.0.0
DTLS Mode                                       : Enabled
Mobility Domain ID for 802.11r                  : 0xac34
Mobility Keepalive Interval                     : 10
Mobility Keepalive Count                        : 3
Mobility Control Message DSCP Value             : 48
Mobility Domain Member Count                    : 3

Link Status is Control Link Status : Data Link Status

Controllers configured in the Mobility Domain:

IP              Public IP   Group Name    Multicast IP    Link Status
------------------------------------------------------------------------------
192.168.102.210   -N/A     default        0.0.0.0        UP   :  UP
```

Enable the Access Point Connections

Step 9 Connect the access points directly to the switch ports to complete installation.

It is mandatory that the access point connection port be configured as an access port. The access point does not register if the port is configured as a trunk.

Note The access VLAN on the switch port should be the same as the wireless management VLAN configured in Step 4 in this workflow.

```
interface GigabitEthernet1/0/3
  description Lightweight Access Point
  switchport host
  switchport access vlan 12
  switchport port-security maximum 11
  switchport port-security
  switchport port-security aging time 2
  switchport port-security aging type inactivity
  switchport port-security violation restrict
  ip  snooping limit rate 100
  switchport block unicast
  storm-control broadcast level pps 1k
  storm-control multicast level pps 2k
  storm-control action trap
```

Enable a Client VLAN

Step 10 Configure an external server to allocate IP addresses for clients. Define a client VLAN and activate the VLAN in the database.

Every WLAN profile must be associated with a client VLAN.

```
!Activate the client VLAN in the VLAN database.
!Configure VLAN 200 if not already configured.
!
vlan 200
name Wireless_Client
end
!
interface vlan 200
  description Client VLAN
  ip address 192.168.13.2 255.255.254.0
  no shutdown
  end
```

Provisioning a Small Branch WLAN

- Provision in Easy-RADIUS—Easiest to configure and does not rely on outside services.
- Provision in Secure Mode—End-users are authenticated by the external RADIUS server or ISE.
- Manage Radio Frequency and Channel Settings

We highly recommend that secure mode be provisioned for security concerns. However, both WLAN modes can co-exist if the network design requires it. For example, you can provision both WLANs on a single switch with each WLAN having its own purpose in the network.

Note If your network does not permit open access for any wireless device, proceed to the "Provision in Secure Mode" section and provision your wireless network in secure mode.

Note Guest Access network deployment is beyond the scope of this document. For detailed information, see the "Configuring Wireless Guest Access" chapter in the *Security Configuration Guide, Cisco IOS XE Release 3E, (Catalyst 3850 Switches)*.

Provision in Easy-RADIUS

Easy-RADIUS allows access to the network without authentication and is not secure.

- Disable Authentication to Enable Easy-RADIUS
- Configure QoS to Secure the WLAN
- Verify Client Connectivity in RADIUS

Note If your network does not permit open access for any wireless device, proceed to the "Provision in Secure Mode" section and provision your wireless network in secure mode.

Disable Authentication to Enable Easy-RADIUS

Step 1 To provision in easy-RADIUS, use the **no security** EXEC commands to disable authentication for a WLAN.

By default, the WLAN is enabled for security with Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2). To make the WLAN open, use the **no security wpa wpa2** command.

```
wlan OPEN_WLAN 1 open_wlan
client vlan 200
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
no shutdown
```

Note By default, the broadcast SSID is enabled, and the WLAN/SSID information is sent in the beacons. The **no broadcast-ssid** command can be used to hide the SSID from being broadcast or made visible to end clients. When the SSID broadcast is disabled, the end-users will still be able to connect to the SSID by explicitly entering the SSID information manually in the wireless client network properties.

Configure QoS to Secure the WLAN

Step 2 Configure a service policy on the ingress direction to properly classify traffic.

All ingress traffic is classified the same as wired traffic. On egress, the secure WLAN is given the majority of the available bandwidth.

QoS configuration for a secure WLAN assumes that there is another WLAN with lower priority, such as a guest or open WLAN. The end users on a secure WLAN should not be impacted by non-critical traffic on other WLANs.

All WLANs share the default port_child_policy egress service policy. This policy is configured by default and does not need to be explicitly configured on a WLAN.

```
wlan secure_WLAN 2 CISCO_WLAN
shutdown
service-policy client input wlan-Entr-Client-Input-Policy
service-policy output wlan-Entr-SSID-Output-policy
no shutdown
exit
```

Verify Client Connectivity in RADIUS

Step 3 Associate clients and verify connectivity

Clients are associated to the WLAN end device by choosing the appropriate SSID.

Client connectivity can be verified by using wireless **show** commands that display state and authentication information.

```
pol-edu-3850-mc-12#show wireless client summary
Number of Local Clients : 2


MAC Address    AP Name                           WLAN State
Protocol
-------------------------------------------------------------------------------
-----
0000.3a40.0001 pol-edu-tsim-40-6              4    UP               11a
0000.3a40.0002 pol-edu-tsim-40-1              4    UP               11a

pol-edu-3850-mc-12#show wcdb database all
        Total Number of Wireless Clients = 2
                Clients Waiting to Join   = 0
                Local Clients             = 2
                Anchor Clients            = 0
                Foreign Clients           = 0
                MTE Clients               = 0

Mac Address    VlanId IPv4 Address      Src If             Mob
-------------- ------ --------------- ------------------ -------
0000.3a40.0001    340 153.40.125.100  0x00000000800000E2 LOCAL
0000.3a40.0002    340 153.40.125.101  0x00000000800000A1 LOCAL
```

```
!
!Look for client open auth state.

pol-edu-3850-mc-12#show access-session mac 0000.3a40.0001 details
            Interface:  Capwap33
          MAC Address:  0000.3a40.0001
         IPv6 Address:  fe80::200:3aff:fe40:1
         IPv4 Address:  153.40.125.100
            User-Name:  cisco
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  000000000000002D000B81FD
      Acct Session ID:  Unknown
               Handle:  0xe9000023
       Current Policy:  (No Policy)
           Blocked On:


Server Policies:
           Vlan Group: Name: 340, Vlan: 340


Method status list:
       Method           State
        dot1x           Authc Success

!
```

Provision in Secure Mode

Secure mode allows secure wireless connectivity. End users are authenticated by an external RADIUS server or ISE. Provision in secure mode if your network does not permit open access for any wireless device.

- Enable the AAA RADIUS Server
- Configure the WLAN with IEEE 802.1x Authentication
- Configure QoS Service Policies for an Open WLAN
- DHCP Snooping

Enable the AAA RADIUS Server

The configuration of the RADIUS server is dependent on the RADIUS service that you choose.

Step 1 Enable the AAA RADIUS server.

You must match the following configuration with an equivalent configuration on the RADIUS server.

```
aaa new-model
aaa session-id common
aaa authentication dot1x default group RADIUS
aaa authorization network default group RADIUS
aaa accounting dot1x default start-stop group RADIUS
!
! Enable 802.1X authentication globally on the switch
!
dot1x system-auth-control
! Radius Server definition (adds ISE to the Radius Group)
!
RADIUS server AuthServer
  address ipv4 192.168.254.14 auth-port 1645 acct-port 1646
  key cisco123
!
!
aaa group server RADIUS RADIUS-GROUP
server name AuthServer
```

Configure the WLAN with IEEE 802.1x Authentication

Step 2 Create a WLAN with WPA2 and IEEE 802.1x enabled.

Although the controller and access points support WLAN with SSID using WPA and WPA2 simultaneously, some wireless client drivers cannot support complex SSID settings.

Whenever possible, we recommend only WPA2 be configured with Advanced Encryption Standard (AES).

```
wlan Secure_WLAN1 CISCO_WLAN
client vlan 200
no shutdown
```

Note WPA2 with AES encryption and IEEE 802.1x key management are enabled by default on the WLAN for the switch so you do not need to explicitly configure these security settings.

Configure QoS Service Policies for an Open WLAN

Step 3 Configure service policies for ingress and egress traffic for an open WLAN.

All ingress traffic is classified the same as wired traffic, but egress traffic is allocated only 30% of the available bandwidth.

When configuring QoS for an open WLAN, a low priority WLAN should be created for guest usage. The end users on an open WLAN are restricted and should not impact business-critical traffic on secure enterprise WLANs.

All WLANs share the port_child_policy egress policy. The policy is configured by default and is not explicitly configured on a WLAN.

```
wlan OPEN_WLAN 1 open_wlan
shutdown
service-policy client input wlan-Guest-Client-Input-Policy
service-policy output wlan-Guest-SSID-Output-Policy
no shutdown
exit
```

DHCP Snooping

Step 4 DHCP snooping configuration is required on the controller for proper client join functionality. DHCP snooping needs to be enabled on each client VLAN including the override VLAN if override is applied on the WLAN.

```
ip dhcp snooping
ip dhcp snooping vlan 100
```

Enable bootp-broadcast command. It is needed for clients that send the DHCP messages with broadcast addresses and broadcast bit is set in the DHCP message.

```
ip dhcp snooping wireless bootp-broadcast enable
```

On the interface:

Note If upstream is via a port channel, the trust Config should be on the port channel interface as well.

```
interface TenGigabitEthernet1/0/1
switchport trunk allowed vlan 100
switchport mode trunk
ip dhcp snooping trust
```

Note DHCP snooping should be configured on the Guest Anchor controller for guest access similar to the Config above.

To allow ingress and egress traffic on the network, the -required option in the WLAN settings forces clients to perform an address request and renew operation each time an association is made with the WLAN. This option allows strict control of used IP addresses.

Manage Radio Frequency and Channel Settings

Radio Resource Management (RRM), also known as Auto-RF, helps with channel and power setting management, but Auto-RF cannot correct for a poor radio frequency design.

- Disable Low Data Rates
- Enable Clean Air
- Enable Dynamic Channel Assignment
- Associate WLAN Clients
- Verify WLAN Client Connectivity

For any wireless deployment, we recommend a site survey to ensure a proper quality service design for your wireless clients.

Disable Low Data Rates

Step 1 Disable the 5-Ghz and 2.4-Ghz networks to successfully modify wireless spectrum rates.

In a well-designed wireless network with good radio frequency coverage, lower data rates can be disabled. Low data rates consume the most airtime.

Limiting the number of supported data rates allows clients to down-shift faster when retransmitting. Wireless clients try to send at the fastest data rate. If the transmitted frame is unsuccessful, the wireless client will retransmit at the next lowest available data rate. The removal of some supported data rates means that clients that need to retransmit a frame directly down-shift several data rates, which increases the chance for the frame to go through at the second attempt. IEEE 802.11b-only devices no longer need to be accommodated. Disable speeds used by IEEE 802.11b-only devices.

```
!Shutdown 5ghz network.
!
ap dot11 5ghz shutdown
!
!Enable 802.11n and 802.11ac for the 5Ghz spectrum.
!
ap dot11 5ghz dot11n
ap dot11 5ghz rate RATE_6M disable
ap dot11 5ghz rate RATE_9M disable
ap dot11 5ghz rate RATE_12M mandatory
ap dot11 5ghz rate RATE_18M supported
ap dot11 5ghz rate RATE_24M mandatory
ap dot11 5ghz rate RATE_36M supported
ap dot11 5ghz rate RATE_48M supported
ap dot11 5ghz rate RATE_54M supported
no ap dot11 5ghz shutdown
!
!Shutdown 2.4Ghz network
!
ap dot11 24ghz shutdown
!
```

Step 2 Enable wireless spectrums.

The lightweight access points support two wireless spectrums: 5 Ghz and 2.4 Ghz. You must enable and disable speeds in each spectrum, but the speeds do not have to match.

- Enable IEEE 802.11n and IEEE 802.11ac for the 5-Ghz spectrum.
- Enable IEEE 802.11n and IEEE 802.11g for the 2.4-Ghz spectrum.

Note Beacons are sent at the lowest mandatory rate that define the cell size.

When deploying the switch in converged access mode as a hotspot, the lowest data rate should be enabled to increase coverage gain versus speed. In addition, the recommended data rates are to be used in a wireless network with good radio frequency coverage. Data rates are contingent upon the nature of your radio frequency deployment.

```
!Enable 802.11n and 802.11g for the 2.4Ghz spectrum.
!
ap dot11 24ghz dot11g
ap dot11 24ghz dot11n
ap dot11 24ghz rate RATE_24M mandatory
ap dot11 24ghz rate RATE_1M disable
ap dot11 24ghz rate RATE_2M disable
ap dot11 24ghz rate RATE_5_5M disable
ap dot11 24ghz rate RATE_6M disable
ap dot11 24ghz rate RATE_9M disable
ap dot11 24ghz rate RATE_11M disable
ap dot11 24ghz rate RATE_12M mandatory
ap dot11 24ghz rate RATE_18M supported
ap dot11 24ghz rate RATE_36M supported
ap dot11 24ghz rate RATE_48M supported
ap dot11 24ghz rate RATE_54M supported
no ap dot11 24ghz shutdown
```

Enable Clean Air

Step 3 Enable Clean Air on the switch and on devices that are common in your deployment environment.

The switch detects and reduces radio frequency interference when Clean Air is enabled. Some sources of interference are jammers, microwave ovens, and bluetooth devices.

```
ap dot11 24ghz cleanair
ap dot11 5ghz cleanair
ap dot11 24ghz cleanair device jammer
ap dot11 24ghz cleanair device cont-tx
ap dot11 24ghz cleanair device dect-like
ap dot11 24ghz cleanair device mw-oven
ap dot11 24ghz cleanair device video
!
ap dot11 5ghz cleanair device jammer
ap dot11 5ghz cleanair device cont-tx
ap dot11 5ghz cleanair device dect-like
ap dot11 5ghz cleanair device video
```

Step 4 Verify that Clean Air is enabled on devices.

```
show ap dot11 24ghz cleanair config
show ap dot11 5ghz cleanair config
```

Enable Dynamic Channel Assignment

Step 5 Make sure that the wireless 2.4-Ghz and 5-Ghz networks are shut down, as described in the "Disable Low Data Rates" section.

Step 6 Enable Dynamic Channel Assignment (DCA) on both the 2.4-Ghz and 5-Ghz wireless spectrums to optimize channel assignments on radios for interference-free operation. For the 5-Ghz spectrum, enable channel bonding to increase throughput.

DCA uses over-the-air metrics reported by each radio on every possible channel and provides a solution that maximizes channel bandwidth and minimizes radio frequency interference from all sources: self (signal), other networks (foreign interference), and noise (everything else).

```
ap dot11 24ghz rrm channel dca global auto
ap dot11 5ghz  rrm channel dca global auto

ap dot11 5ghz shutdown
ap dot11 5ghz rrm channel dca chan-width 80
no ap dot11 5ghz shutdown
```

Associate WLAN Clients

Step 7

Association of WLAN clients is done on the end-client device by choosing the appropriate SSID and supplying the required credentials for authentication. Client connectivity depends on the type of device used which can be verified by looking at the wireless network interface details.

Verify WLAN Client Connectivity

Step 8 Verify client connectivity.

```
show authentication sessions mac ec55.f9c6.266b detail
            Interface:  Capwap4
               IIF-ID:  0x5062800000033A0
          MAC Address:  ec55.f9c6.266b
         IPv6 Address:  Unknown
         IPv4 Address:  121.1.0.253
            User-Name:  Employee1
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  64010101539f285900003353
      Acct Session ID:  Unknown
               Handle:  0xDB000467
       Current Policy:  (No Policy)

 Server Policies (priority 100)

Method status list:
       Method           State
       dot1x            Authc Success
```

```
show wcb database all
!Need to look for the output of 'AUTH' equals to 'RUN'.
!
   Total Number of Wireless Clients = 1
      Clients Waiting to Join   = 0
      Local Clients             = 1
      Anchor Clients            = 0
      Foreign Clients           = 0
      MTE Clients               = 0

Mac Address    VlanId IP Address      Src If             Auth     Mob
-------------- ------ --------------- ------------------ -------- -------
ec55.f9c6.266b    200 121.1.0.253     0x006B2F4000002844 RUN      LOCAL
```

Show Running Configuration for Wireless LAN Converged Access

Step 1 Enter the **show running-configuration** command to display the wireless configuration settings for the switch.

```
show running configuration

ip arp inspection vlan 10-11,100
!
ip device tracking
ip  snooping vlan 10-13,100,200
no ip  snooping information option
ip  snooping wireless bootp-broadcast enable
!
! the default router for subnet 192.168.12.x /24 is the upstream router
! 192.168.12.2 is the layer 3 address of the 3850 vlan interface on vlan 12
!
ip  excluded-address 192.168.12.1
ip  excluded-address 192.168.12.2
!
!
!Access Point IP  pool defined locally on the 3850
!
ip  pool APVlan12-pool
network 192.168.12.0 255.255.255.0
default-router 192.168.12.1
!
! Vlan 200 for wireless clients, and the subnet 192.168.13.x /23
!  the  server is external to the 3850.
vlan 200
 name Wireless_Client
!
<snip>
!
! remember to exclude 192.168.13.2 on the  server. Its statically defined
on the vlan 200 intf
interface Vlan200
description wireless Clients
ip address 192.168.13.2 255.255.255.0
!
wireless mobility controller
wireless management interface Vlan12
!
! this is copied from the “show run” output.
wlan OPEN_WLAN 1 WiFi_Open
client vlan 200
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
no shutdown
!
```

(Continued)

```
! Radio Resource management features
ap dot11 24ghz shutdown
ap dot11 24ghz cleanair
ap dot11 24ghz rate RATE_1M disable
ap dot11 24ghz rate RATE_2M disable
ap dot11 24ghz rate RATE_5_5M disable
ap dot11 24ghz rate RATE_6M disable
ap dot11 24ghz rate RATE_9M disable
ap dot11 24ghz rate RATE_11M disable
ap dot11 24ghz rate RATE_12M supported
ap dot11 24ghz rate RATE_18M supported
ap dot11 24ghz rate RATE_24M mandatory
ap dot11 24ghz rate RATE_36M supported
ap dot11 24ghz rate RATE_48M supported
ap dot11 24ghz rate RATE_54M supported
no ap dot11 24ghz shutdown
!
ap dot11 5ghz shutdown
ap dot11 5ghz rrm channel dca chan-width 80
ap dot11 5ghz cleanair
ap dot11 5ghz rate RATE_6M disable
ap dot11 5ghz rate RATE_9M disable
ap dot11 5ghz rate RATE_12M disable
ap dot11 5ghz rate RATE_18M disable
ap dot11 5ghz rate RATE_24M mandatory
ap dot11 5ghz rate RATE_36M supported
ap dot11 5ghz rate RATE_48M supported
ap dot11 5ghz rate RATE_54M supported
no ap dot11 5ghz shutdown
ap group default-group
end
```