



Appendix - Supporting Topics

This appendix contains the following sections:

- [LAN port functionality for different models, on page 1](#)
- [LED Color Indicators for Cisco Business Wireless APs, on page 1](#)
- [Primary AP Failover and Election Process, on page 4](#)
- [Pre-downloading an Image to an Access Point, on page 5](#)
- [Creating a Guest Network, on page 5](#)
- [Resetting a Device to Factory Default, on page 6](#)
- [SNMP Traps in CBW AP, on page 7](#)
- [Deployment and Troubleshooting Guidelines, on page 8](#)
- [Access Point Configuration Files, on page 12](#)

LAN port functionality for different models

Cisco Business AP Model	Type	Wired Ethernet Ports	AP Mode	Mesh Mode
CBW150AX	Primary Capable AP	1 (Uplink POE-PD)	NA	Ethernet Bridging
CBW151AXM	Mesh Extender	NONE	NA	NA

LED Color Indicators for Cisco Business Wireless APs

This chapter provides information on the LED behavior for Primary APs and Mesh Extenders. It also details the LED states during TFTP and HTTP upgrades.

LED behavior for Primary Capable Access Points

The Cisco access point has an LED indicator on the face of the unit for CBW150AX and CBW151AXM AP models.

After you have mounted the access point, connect and power up the Access Point. Observe the LED state to determine the device operation. The following table provides description for different states of the LED and their patterns on the AP device.

For normal Reload of Primary Capable APs, the LED states are as follows:

Table 1: LED behavior for Primary Capable Access Points

Stages of LED States	CBW150AX
Stage — 1 POE cable plug in	White Then blinking green
Stage — 2 Mode button pressed	Blinking blue (below 20 secs) Solid red (after 20 secs when kept pressed)
Stage — 3 Mode button released / Pressed for more than 60 seconds (Logs: Starting Image...)	Off
Note	The Mode Button functionality described in stages 1, 2, and 3 above are applicable for both Mesh Extenders and Primary Capable Access Points.
Stage — 4 Sequence of boot up (Logs: Linux version...)	Blinking green (normal boot) Off (if stages 2 and 3 occur)
Stage — 5 Sequence of boot up (Logs: 5g radio Domain...)	Blinking green Off (if stages 2 and 3 occur)
Stage — 6 Radio Init stage and waiting for Uplink IP config	Cycles through red, green, off
Stage — 7 IP assigned and Capwap Init (If a Primary AP exists in network, it moves to stage 8 else switchdriver process starts)	Cycles through green, red, off
Stage — 8 Capwap discovery to join state and image data response followed by image upgrade if version mismatch and reload (LED stages 1-7)	Cycles through green, red, off If image version mismatch occurs it will blink blue.
Stage — 9 Capwap setup, configure and run without clients connected (skip stage-8 if the image version is same)	Solid green
Stage — 10 At least one client connected	Solid blue

LED behavior for Mesh Extenders

Stages 1-6 in the following table is similar for both the Primary Capable AP (CBW150AX) and Mesh Extender (CBW151AXM). The different stages for mesh joining process is as follows:

Table 2: LED behavior for Mesh Extenders

Process	Mesh Extender CBW151AXM
Mesh Stage — 1 Starting mesh and searching for parent	Cycles through red, green, off
Mesh Stage — 2 IP assigned and CAPWAP Init	Cycles through green, red, off
Mesh Stage — 3 Mesh AP image data Note If the Mesh AP image version doesn't match the Primary AP version, the Mesh AP will begin to upgrade and then reload. Reload will cycle through Primary Capable stages 1-6, and then Mesh stages 1 - 2.	Blinking blue
Mesh Stage — 4 Mesh AP image data - Version match	Solid green
Mesh Stage — 5 Mesh AP joined Primary AP	Solid green
Stage — 6 At least one client connected	Solid blue

LED behavior during TFTP / HTTP Upgrade

When the AP or Mesh Extender starts to pre-download (TFTP or HTTP) the LED will begin blinking blue.

LED Display Settings

To enable, disable, or set the LED display to blink on an access point, do the following using the web UI:

-
- Step 1** Navigate to **Monitoring > Network Summary > Access Points**.
 - Step 2** Click on the access point the list that you want to enable/disable the LED.
 - Step 3** Click **Tools** from the menu list.
 - Step 4** Click **AP LED disable** to turn off the LED display. By default the LED is **ON**.
 - Step 5** To identify a particular access point from a group of access points placed together, click **Blink AP LED**.
-

Primary AP Failover and Election Process

Primary AP Redundancy for Failover

In a Cisco Business Wireless network, not all APs have the capability to work as a Primary AP. See [Supported Cisco Access Points](#) to know which AP models are capable of working as a Primary AP.

To enable a failover, your network must have two or more active APs with Primary AP capability. In the event of a failover, one of these other APs will automatically be elected as a Primary. The newly elected Primary will have the same IP and configuration as the original Primary. From an administrator perspective, there will be no difference between the original Primary and the newly elected Primary in case of a failover.



Note Clients that connect to the Primary AP will lose connectivity during a failover.

Primary AP Forced Failover

You can manually force any AP that has the capability, to become the Primary AP. This forced failover of the Primary AP to another Primary Capable AP of your choice can be performed using the Primary AP UI.

To perform a forced failover using the Primary AP UI:

1. Choose Navigate to **Wireless Settings > Access Points**.
2. In the **Access Points** window, click the **Edit** icon next to the AP you want to set as Primary.
The **Edit** window with the **General** tab is displayed.
3. Under the **General** tab, click **Make Me Primary AP** next to the **Operating Mode** field.



Note The **Make Me Primary** button is available only for the subordinate APs that are capable of participating in the Primary election process.

When you force the failover of the Primary to an AP of your choice using the UI, the current Primary AP reboots. The new AP takes over as the Primary AP with the IP address and configuration as the previous Primary. When the reboot is complete the previous Primary comes back online and joins the new Primary AP as a subordinate AP.



Note The forced failover causes downtime in the Cisco Business Wireless network. During this downtime, clients associated to wired uplink APs will not face any disruption in service and no new clients can be connected.

Primary AP Election Process

In a Cisco Business Wireless network, when the Primary AP shuts down, one of the other Primary Capable APs in this deployment is automatically designated as the Primary AP. The automatic selection of the Primary AP among the Primary-capable APs is an internal automatic Primary election process. This process is used to both detect the failure of the Primary AP and to designate the new Primary AP among the eligible APs.

This process is based on Virtual Router Redundancy Protocol (VRRP) that algorithmically determines the next Primary AP, based on the following parameters listed in the order of descending precedence:

- The AP configured as next-preferred Primary.
- The AP with the least load in terms of the number of associated clients.
- Among APs with a similar client load, the AP with the lowest MAC address.

Pre-downloading an Image to an Access Point

To minimize network outages, an upgrade software image is downloaded to the AP from the Primary AP without resetting the access point or losing network connectivity. This means that the upgrade image to the Primary AP is downloaded, and then the image is downloaded to all the Primary Capable APs and Mesh Extenders while the network is still up.

When the Primary AP reboots, the APs are disassociated and reboot. The Primary AP comes up first, followed by the APs, all with their upgraded images. Once the Primary AP responds to the discovery request sent by an AP with its discovery response packet, the AP sends a join request.

Creating a Guest Network

Login to the Primary AP Web UI, and navigate to **Wireless Settings > WLANs**.

Step 1 Click **Add new WLAN**.

Step 2 Set **Profile name** and **SSID** under the **General** tab.

Step 3 Under **WLAN Security** tab, enable **Guest Network** using the slider toggle button.

Step 4 Choose the type of web portal in the **Captive Portal** option. It can be either **Internal Splash Page** or **External Splash Page**.

Step 5 Choose one of the **Access Type** for Authentication.

For example, if you want your guests to use their Google/Facebook accounts for authenticating, use **Social Login** as the Access Type for your Guest WLAN.

Step 6 Choose the **ACL Name** if you want the guest to access or block few sites / IP.

Step 7 Click **Apply** to create the Guest WLAN.

Once the Guest connects to your Guest WLAN, it pop ups an **Authentication** page, and the network access is provided if successfully authenticated.

- Note**
- You can also export Guest information by navigating to **Monitoring > Network Summary > Guests** option.
 - The login page of the Guest WLAN can be configured in Web UI under **Wireless Settings > Guest WLAN** page. Refer to the section [Setting a Login Page for WLAN Guest Users](#).

Resetting a Device to Factory Default

To reset to factory default using the Mobile App:

- Select the ... **More** icon on the bottom right of the screen, then select **Reset to Factory Default**.

To clear the Primary AP configuration and reset the entire network, see [Clearing the Primary AP Configuration and Resetting to Factory Defaults](#).

To factory default a single AP, refer to the **Factory Default** section, under **Tools** in the [Viewing Access Point Details](#).

To reset the AP or Mesh extender to factory default using the **Mode button**, follow the steps below.

1. Remove or unplug the power to the device.
2. Press and hold the **Mode** button while re-applying power to the device.
3. Once the LED pattern changes to solid red, release the **Mode** button and allow the device to continue booting up.

The location of the **Mode** button on the CBW150AX and CBW151AXM models are shown below.

- **CBW150AX**: the mode button is located at the back of the device near the Ethernet port.



- **CBW151AXM**: the mode button is located at the side of the device near the Power button.



Note If the Mode button is pressed for over 60 seconds, the factory default reset is ignored. If the Mode button is pressed after the device boots up, it is ignored.

After a few seconds, the device LED will begin blinking blue for 20 seconds, and then switch to solid red.

SNMP Traps in CBW AP

You can configure the SNMP trap receiver in CBW UI and receive the SNMP traps. The SNMP Trap receiver can be configured using the Web UI by navigating to **Advanced > SNMP**. The following table lists the set of SNMP traps available in CBW AP and the instance at which these traps are triggered:

Table 3: SNMP Traps in CBW AP

Category	Trap Name	Purpose
System/Primary AP	Authentication Flag	Sending traps with invalid SNMP access.
	Multiple Users Flag	Sending of traps when multiple logins of Primary AP are active.
	configsave	Sending of traps when Primary AP save config called by UI/CLI.
	strong-pwd check	Sending of traps when Primary AP user credential's password policy is changed.
802.11 client	Excluded	Wireless client exclusion trap; If any client excluded by Primary AP, triggers this trap.
	Max Client Wrning Threshold	Triggers the trap when the system reaches 90% of max client associated with this Primary AP.
	Nac-Alert Traps	Sending of traps when the client joined on NAC enabled WLAN.
	WebAuthUserLogin	Guest user login on Guest WLAN.
	WebAuthUserLogout	Guest user logged out/client delete from Primary AP.
Cisco AP	AuthFailure	Access point authentication failure trap while Access point joining to the Primary AP it checks the mac filter. It is applicable in Mesh mode.
	Register	Access point join/disjoin from the Primary AP.
	InterfaceUp	Access point radio interface up/down trap.
	modeChange	Any operational mode change.
802.11 Security	WEP/WPA Decrypt Error	Sending traps if any wep/wpa decrypt error detected on any of the APs.
	IDS Signature attack detected	Sending traps if any IDS signature attack (Assoc, deauth flood) is detected by the Access point .

Category	Trap Name	Purpose
AAA	auth	Sending when an AAA authentication failure occurs for management user, net user, or MAC filter.
	servers	sending when no RADIUS servers are responding.
Rogue	Rogueap	Sending trap when detects the Rogue AP
Auto-RF Profiles(RRM)	Client/Channels Load,Noise, interference, coverage hole	Sending trap when failure or max threshold reached for the RRM measurements.
	Txpower	Send trap when Access points radio's tx power level changed.
	Channel	Send trap when Access points radio's channel changed.
Mesh	auth failure	Send trap when Mesh Extender's authentication is failed.
	child excluded parent	Sending trap if Mesh Extender excludes the parent node.
	parent change	Send trap if mesh extender changes the parent.
	child moved	Send trap if mesh extender moved from this parent.
	excessive parent change	Send trap if mesh extender change parent rapidly.
	onsetSnr	Send trap if parent SNR is poor (less than 12).
	abate SNR	Send trap if parent SNR is high (more than 60).
	excessive association	Send trap if mesh extender attempted too many association (10 count without success).
	excessive children	Send trap if any node has more than 20 mesh extenders (this will not hit for SMB customers).

Deployment and Troubleshooting Guidelines

This section provides details on deployment and troubleshooting issues.

Placing an AP/ Mesh Extender

Place the Mesh extenders in the line of sight of the Primary/Primary Capable AP or another Mesh Extender. Walls and other objects between the Mesh Extender and the Primary/Primary Capable AP or other Mesh Extenders may interfere or reduce connectivity.

Check the SSID signal strength of the Primary AP and place the Mesh Extender in a location that has enough signal strength.

The table below gives an approximate coverage area of CBW APs in the open space. The values can be reduced by a factor of 20-30% in case of office/home deployments and the APs could be placed apart at a computed distance.

AP	Meters	Feet
CBW150AX	15 to 18	50 to 60
CBW151AXM	15 to 18	50 to 60

Avoid placing the Mesh Extenders very close to each other and other Primary Capable APs.

Locate the Mesh Extenders where the Signal to Noise Ratio (SNR) value is good (more than 30).



Note Navigate to **Monitoring > Network Summary > Mesh Extender** to check the SNR value.

You can also identify the Nearest APs for each Mesh Extender by checking on **Nearest APs** field under **Monitoring > Access Points**. Select the Mesh Extender and then refer to the **General** section in the **Access Point View** page.

Setting Up Channel of Primary/Primary Capable APs

The Radio channel settings for Access Points and Mesh extenders default to Automatic. The channel settings for an Access Point or Mesh Extender can be changed in the Web UI by navigating to **Wireless Settings > Access Points**, and selecting the **Edit AP** action from the table. A pop-up window will have a tab for Radio 1 (2.4GHz) and Radio 2 (5GHz). For Mesh extenders, the backhaul radio channel is controlled by the Primary AP (by default 5GHz) and cannot be changed in the Mesh Extender window.

Following are some of the instances in which you would need to change the channel of Primary/Primary Capable APs for better performance.

By default, the APs in mesh deployment are configured with the mesh backhaul radio configured for channel number 36 and channel width as 80MHz in 5GHz radio.

- If additional Primary Capable APs are deployed to primarily provide additional capacity, then they should be deployed on a different channel than its neighboring Primary/ Primary Capable APs to minimize the co-channel interference.
- If many Rogue APs are present in the APs current channel, then change the channel of the Primary Capable APs. To view the Rogue APs, navigate to **Monitoring > Rogues > Access Points**.
- If Channel Utilization is high (greater than 75) and Interference is high in the serving channel, then change the channel in the AP. You can view the following error logs by navigating to **Advanced > Logging > Logs**.

Following is an example of a log displayed in the **Logs** window:

```
*RRM-DCLNT-5_0: Dec 25 16:51:34.543: %RRM-3-HIGHCHANNEL_UTIL: rrmLrad.c:7678
Interference is high on AP: APA453.0E1F.E480 [Level: 85] on Radio:
5Ghz(Radio2).Change Channel (Wireless->Access Points->Edit AP->Radio->Channel) to get
better/stable performance.
```

- Choose non-DFS channels (36-48, 149-165) for maximizing the coverage, as DFS channels (channel 52 - 144) will have low power level. To change the channel for the AP:

1. Navigate to **Wireless Settings > Access Points**.
2. Select the AP to edit in the channel.
3. Change the Channel under **Radio 2** in Mesh deployments.

In a Non-Mesh deployment:

1. Switch to Expert view.
2. Navigate to **Advanced > RF optimization > Select DCA channels > 5Ghz**.
3. Deselect the DFS channel numbers.



Note Nations apply their own RF emission regulations to the allowable channels, allowed users, and maximum power levels within the frequency ranges.

Recommendation on Mesh Hop Count

- Data Traffic: Maximum of 4 hops
- Voice Traffic: Maximum of 2 hops

Grouping Mesh Extenders using BGN name

You can deploy more than one Primary Capable AP in your network in the same sector (area), and can logically group the Mesh Extenders by configuring BGN string under **Wireless Settings > Access Points > Edit Access point > Mesh tab**. By default, the BGN value is set with first 10 characters of the configured SSID during initial setup. If BGN is configured, then Mesh Extenders will select the same BGN configured Parent. If there is no matched BGN configured parent, it will select any parent in the network and periodically disconnect and check for matched BGN parent.



Note This option is available in **Expert View** only.

Best practices for HTTP Image Upgrade

- Prefer a wired client to do the image upgrade, or a wireless client with a good connection score.
- Place the wireless client near the Primary AP and ensure it is connected while trying to upgrade image through HTTP image transfer method.
- Ensure your wireless client has high signal strength (greater than -65 dBm) and a good connection score (higher than 75%) to avoid any image download failures.
- If the image upgrade constantly fails, then use the **Cisco.com** mode for the Image upgrade.
- When uploading the images using HTTP method, you see a **Transfer fail** error on the Chrome browser, the self-signed certificate of Primary AP should be added in the **Trusted Root Authority**.

Adding Self-Signed certificate of Primary AP in Windows:

1. Navigate to the Primary AP UI using *https://ciscobusiness.cisco* or *https://<managementip>*, and click through the usual warnings for untrusted certificates.
2. In the address bar, right click on the **Not Secure** red warning triangle. Select **Certificate** to display the certificate.
3. In the pop-up window select the **Details** tab, and click **Copy to File** at the bottom right corner of the tab.
4. This launches the **Certificate Export Wizard**. Click **Next** at the bottom of the screen.
5. In the radio-button dialogue select the format. Leave the default **DER encoded binary X.509 (.CER)** and click **Next**.
6. Use **Browse** option to select a folder path to download the exported certificate. Click **Next** to export the certificate and then click **Finish**.
7. Click **OK** in the pop-up window to confirm the export was successful.
8. In the original **Certificate** pop-up window, click **OK** again.
9. Open the Chrome **Settings** page and click **Privacy and security** tab on the left navigation pane.
 - a. Click the **more** arrow to expand this section.
 - b. Choose the **Manage certificates** area.
10. In the pop-up **Certificates** window, select the **Trusted Root Certification Authorities** tab.
11. Click on the **Import** button to launch the **Certificate Import Wizard**.
12. Click **Next**.
13. Select **Browse** and use the explorer window to locate the certificate you exported in the earlier step.
14. Click **Next** and then **Finish**.
15. In the **Security Warning** pop-up window, click on **Yes**. You should see yet another pop-up letting you know that the import was successful.
16. Restart Chrome, and navigate to the Primary AP UI using *https://<managementip>*. You should see a closed padlock and **Secure** annotation to the left of the URL.

Adding Self-signed certificate of Primary AP in macOS:

Navigate to the Primary AP UI using *https://ciscobusiness.cisco* or *https://<managementip>*. Do the following in Chrome:

1. Navigate to **Developer Tools > Security tab**.
2. Click **View Certificate** to see the certificate.
3. Click and drag the image to your desktop.
4. Open the **Keychain Access** utility in OS X.
5. Select the **System** option on the left.
6. Click the **lock** icon on the upper-left to enable changes.
7. In the lower left corner of the screen select the **Certificates** option.

8. Drag the certificate you copied to the desktop into the list of certificates.
9. After the certificate is added to the **System** keychain, double-click to open it.
10. Expand the **Trust** section. For the first option, pick **Always Trust**.
11. Quit Chrome and all other browsers and navigate to the Primary AP UI using `https://<managementip>`. You should see the closed padlock and **Secure** annotation to the left of the URL.



Note Use `https://<managementip>` to access the Primary AP UI, if the self-signed certificate is added to your machine.

Resolving connection issues between CBW and CBD

- If the connection is based on a CBD probe, please ensure that the SNMP configuration in CBD and CBW are the same. To configure the SNMP details of the device on CBD, refer to *Managing Device Credentials* in the [Cisco Business Dashboard Administration Guide](#).
- If the connection between CBD and CBW is a direct management connection, ensure the following:
 - Verify if the credentials specified in **CBD Settings** page, is the same as created in CBD.
 - Verify if the correct certificate file is uploaded in CBW (in case CBD uses self-signed certificate).
 - Verify that the name or IP address configured for the Dashboard in CBW is listed in the **Subject-Alternative-Name** field of the dashboard's certificate
 - Check the system logs in the **logging** page.

Access Point Configuration Files

Description Status Table

Primary AP Primary Image	The default active image version of the Primary AP.
Primary AP Backup Image	The backup image version of the Primary AP.
AP Primary Image	The active image version of the access point.
AP Backup image	The backup image version of the access point.
Pre-download status	If the access point is going for an software update the corresponding pre-download status is displayed.
Pre-downloaded version	Version of the pre-downloaded image during software upgrade process.