Wireless Converged Access Chromecast Configuration Example

Converged Access allow Wi-Fi networks to support wired connectivity and keep management of wired and wireless networks as simple as possible.

Note This document is an expansion of the Chromecast Deployment Guide. Refer to the Chromecast Deployment Guide for more details on Converged Access configuration on AireOS WLCs.

Prerequisites

- We recommend that you have basic knowledge on Cisco Catalyst 3850 Series, Cisco Catalyst 3650 Series, Cisco Catalyst 3560-CX Series, and Cisco 2960-CX Series Switches for Converged Access in Cisco IOS Release 3.6.x or later.

  Tip Refer to Converged Access Consolidated Quick Reference Templates for information about the latest available Release Notes for Converged Access Release 3.6.x or later

- Ensure that Switch Virtual Interfaces (SVIs) and DHCP pools or snooping are pre-configured.

Supported Platforms and Releases

The information in this document is based on the following:

- Cisco Catalyst 3650 Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 4500Sup8E Series Switches

Note The information in this document refers to devices in a specific lab environment. Descriptions of the devices are provided with default configuration values. If you are on a live network, you must understand the potential impact of all the commands.

Configuring Chromecast Support

Perform the following Global and WLAN configurations to launch Chromecast support on Cisco Catalyst 3850 Series, Cisco Catalyst 3650 Series, Cisco Catalyst 3560-CX Series, and Cisco 2960-CX Series Switches for Converged Access:

Configuring Wireless Mutlicast Globally

Perform the following tasks to configure wireless multicast globally:

Step 1 To enable the Multicast Support feature, use the **wireless multicast** command.

Step 2 To enable Internet Group Management Protocol (IGMP) snooping, use the i**p igmp snooping** and the **ip igmp snooping querier** commands.

Step 3 To set the mode of wireless Access point (AP) and Control and Provisioning of Wireless Access Points CAPWAP multicast to multicast-multicast, use the **ap capwap multicast** command.

```
Device# configure terminal
Device(config)# wireless multicast
Device(config)# ip igmp snooping
Device(config)# ip igmp snooping querier
Device(config)# ap capwap multicast <Multicast IP - 239.x.x.x>
```

Note Do not use multicast-unicast for AP CAPWAP multicast mode.

Step 4 To verify IGMP settings, use the **show ip igmp groups** command.

Step 5 To verify wireless multicast details, use the **show wireless multicast** and the **show wireless multicast group summary** commands.

Step 6 Tune the data rates for optimal performance.

Note The configuration and the data rates provided in the following examples must be tuned for optimal values as per the requirements.

The following is sample data rate configuration for 2.4 Ghz:

```
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_24M supported
ap dot11 24ghz rate RATE_36M supported
ap dot11 24ghz rate RATE_48M supported
ap dot11 24ghz rate RATE_54M supported
```

The following is the sample data rate configuration for 5 Ghz:

```
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 supported
ap dot11 5ghz rate RATE_36M supported
ap dot11 5ghz rate RATE_48M supported
ap dot11 5ghz rate RATE_54M supported
```

Note Use broadcast forwarding to enable IGMP snooping, if IGMP snooping cannot be enabled. Use the **wireless broadcast** command for broadcast forwarding. Alternatively, forward the broadcasts to a specific VLAN using the **wireless broadcast vlan** *VLAN ID* command.

Configuring WLAN

To configure the WLAN for Chromecast, perform the following steps:

Step 1 Enable the peer-to-peer blocking mode.

Step 2 Enable the support on multicast VLAN.

The following sample is an example for configuring WLAN using external RADIUS authentication, MAC-filter, and AAA-override:

```
aaa new-model
   !
   !
   aaa group server radius ISE
    server name ISE
   !
   aaa authentication dot1x ISE group ISE

   radius server ISE
    address ipv4 x.x.x.x auth-port 1645 acct-port 1646
    key XXXXX


dot1x system-auth-control

wlan Chromecast <WLAN ID> Chromecast
   aaa-override
   mac-filtering ISE¬
```

```
client vlan <VLAN ID>
no peer-blocking
ip multicast vlan <vlanid> // If using vlan select feature//
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security dot1x authentication-list ISE
session-timeout 1800
no shutdown
```

Note Depending on your WLAN security, choose the appropriate template.