Chromecast Deployment Guide, Release 7.6

First Published: March, 2014

Introduction

This document provides information on the theory of operation and configuration for the Cisco Unified Wireless LAN solution as it pertains to supporting Multicast applications for devices such as Google Chromecast.

Prerequisite

Components Used

The below implementation was tested using AireOS code version 7.6.100.0 with a 5508 Wireless LAN Controller and 3702 Aironet AP.

This document is not restricted to specific software and hardware versions.

The information in this document is created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

What is Chromecast?

Chromecast is a digital media player developed by Google. The device, a HDMI dongle, plays audio/video content on a high-definition screen by directly streaming it via Wi-Fi from the Internet or a local network. Users select the media to play by using Chromecast enabled mobile/Web applications, or through a feature called “tab casting” that can mirror most Google Chrome browser content running on the device (MAC OSX and Windows).
Chromecast uses a simple multicast protocol for Discovery and Launch that enables users to mirror their devices on a second screen.

The Chromecast devices operate on DIAL protocol. The DIAL Service Discovery enables a client to discover DIAL Server (Chromecast) on its local network, and obtain access to those services. This is achieved by using a new search target within the SSDP defined by uPNP.

1. (Service Discovery Request)
   239.255.255.250

1. (Response with IP address of service)
The clients that wish to discover Chromecast servers send a request over UDP to IP address 239.255.255.250 and UDP port number 1900. See Chromecast Packet Level Details for more information.

Problem Statement

The multicast address used by the Chromecast discovery packets has a TTL (Time To Live) set to 1. Routers cannot use multicast routing to redirect traffic across L2 subnets because this results in only link local discovery of Chromecast, which might not be ideal for larger networks.

This document provides information on deploying Chromecast over large networks with single, as well as multiple VLANs.

Wi-Fi Considerations

Chromecast devices have a single radio and work on the 2.4 GHz band. So, you need to make sure the SSID that the Chromecast devices is connected to is broadcasted on the 11b radio.
From a security standpoint, Chromecast devices do not support 802.1x, so Cisco recommends you to create a separate SSID for Chromecast that supports WPA2 PSK (Pre-Shared Key).

Firewall Considerations

Chromecast discovery packets rely on the DIAL protocol operating at UDP port 1900 and send the requests to the address 239.255.255.250. Ensure that no firewall blocks connectivity between the Chromecast device and wireless client.

Deployment Considerations

The following sections describe the steps for configuring the wireless LAN controller to enable Chromecast support on a Cisco Wireless network.

Deploying Chromecast using MDNS Bonjour Services

The use and administration of Chromecast devices on the networks has been simplified by the support of Bonjour services. By using the service string "._googlecast._tcp.local.", Chromecast devices can act as any other Bonjour service provider. This service is used exclusively for casting the screen of a supported device to the screen where Chromecast is connected.
This section explains the configurations performed for the following scenarios:

1. Chromecast and wireless clients on the same WLAN and same VLAN
2. Chromecast on WLAN A and wireless clients on WLAN B, different VLANs
3. Chromecast on anchor WLC and wireless clients on foreign WLC
4. Chromecast and wireless clients on different VLANs (same SSID)

**Initial Configuration**

For any of the previous scenarios except scenario 4 (Chromecast and wireless clients on different VLANs (same SSID)), you must add the service string used by Chromecast when casting a screen. This allows the WLC to recognize the Chromecast device.

**CLI**

```bash
>config mdns service create chromecast _googlecast._tcp.local. origin wireless lss disable query enable
>show mdns service summary
```

**GUI**

[Diagram of the GUI interface for adding a service string]
Now, you can add this service to the mDNS profile that is used on the WLAN. In this case, the default profile is used:

**CLI**

`>config mdns profile service add default-mdns-profile chromecast`

`>show mdns profile detailed default-mdns-profile`

- **Profile Name**: default-mdns-profile
- **Profile Id**: 1
- **No of Services**: 7
- **Services**: AirPrint, AirTunes, AppleTV, HP_Photosmart_Printer_1, HP_Photosmart_Printer_2, Printer, chromecast

**GUI**
Deployment Considerations

Ensure that the following settings are enabled globally on WLC:

- Multicast
- IGMP snooping
- mDNS snooping

**CLI**

To check the status of Multicast, IGMP snooping, and mDNS snooping on the CLI, run the following command:

```shell
>show network summary
```

```
Ethernet Multicast Forwarding............ Enable
IGMP snooping.......................... Enabled
mDNS snooping............................ Enabled
```

To enable the settings on the CLI, run the following commands:

```shell
>config network multicast global enable
>config network multicast igmp snooping enable
>config mdns snooping enable
```

**GUI**

To enable the settings on the GUI, refer to the following screenshots.
Scenario 1: Chromecast and Wireless Clients on the Same WLAN and Same VLAN

Network Diagram
Configurations

1. Create subinterface vlan 10 (This interface has a DHCP server located on the same VLAN)
   
   **CLI**
   
   > config interface create vlan10 10
   > config interface address dynamic-interface vlan10 192.168.10.15 255.255.255.0 192.168.10.254
   > config interface port vlan10 1
   > config interface mdns-profile vlan10 default-mdns-profile
   > config interface dhcp dynamic-interface vlan10 proxy-mode disable

   **GUI**
2. Create the WLAN.
   - Security WPA2-PSK (password = cisco-chrome)
   - Radio policy only 802.11g
   - By default mDNS snooping is enabled with default-profile
   - Map it to vlan 10

CLI
Deployment Considerations

>config wlan create 1 blue
>config wlan security wpa akm 802.1x disable 1
>config wlan security wpa akm psk enable 1
>config wlan security wpa akm psk set-key ascii cisco-chrome 1
>config wlan interface 1 vlan10
>config wlan radio 1 802.11g-only
>config wlan ccx aironetIeSupport disable 1
>config wlan enable 1

GUI
3. Connect the Chromecast and wireless client to the WLAN.

The wireless client locates the Chromecast device and cast screen.
Scenario 2: Chromecast on WLAN A and Wireless Clients on WLAN B, Different VLANs

Network Diagram

Configurations

1. Add WLAN B for VLAN 20 (See step 1 and 2 from scenario 1 for more reference)
   
   >config interface create vlan20 20
   
   >config interface address dynamic-interface vlan10 192.168.20.15 255.255.255.0 192.168.20.254
   
   >config interface port vlan20 1
   
   >config interface mdns-profile vlan20 default-mdns-profile
   
   >config interface dhcp dynamic-interface vlan20 proxy-mode disable
   
   >config wlan create 2 red
   
   >config wlan security wpa akm 802.1x disable 2
   
   >config wlan security wpa akm psk enable 2
   
   >config wlan security wpa akm psk set-key ascii cisco-chrome 2
   
   >config wlan interface 2 vlan20
   
   >config wlan radio 2 802.11g-only
   
   >config wlan ccx aironetIeSupport disable 2
   
   >config wlan enable 2

2. Connect Chromecast to SSID blue.
3. Connect the wireless client to SSID red.

The wireless client should be able to cast screen to the Chromecast device.

---

**Note**  The smartphones would not be able to find Chromecast for management for this scenario. This scenario is tested only for screen mirroring.

**Note**  This scenario will only work when having APs in local mode. For APs in FlexConnect – local switching, mirror will only work if devices are using the same VLAN (both Chromecast and laptop).
Scenario 3: Chromecast on Anchor WLC and Wireless Clients on Foreign WLC

Network Diagram

Configurations

1. Create WLANs on both WLCs with exact same settings (see Step 2 in Scenario 1).
2. Create mobility domain between both WLCs.

CLI:

(WLC-Anchor) >show mobility summary

Mobility Protocol Port........................... 16666
Default Mobility Domain........................ mb-anchor
Multicast Mode .................................. Disabled
Mobility Domain ID for 802.11r................... 0x5313
Mobility Keepalive Interval...................... 10
Mobility Keepalive Count......................... 3
Mobility Group Members Configured.............. 1
Mobility Control Message DSCP Value.............. 0

Controllers configured in the Mobility Group
MAC Address      IP Address      Group Name     Multicast IP     Status
bc:16:65:c2:aa:c0 10.88.244.87    mb-anchor      0.0.0.0          Up

(WLC-Foreign) >show mobility summary

Mobility Protocol Port........................... 16666
Default Mobility Domain......................... mb-foreign
Multicast Mode .................................. Disabled
Mobility Domain ID for 802.11r................... 0x25f5
Mobility Keepalive Interval...................... 10
Mobility Keepalive Count......................... 3
Mobility Group Members Configured.............. 1
Mobility Control Message DSCP Value.............. 0

Controllers configured in the Mobility Group
MAC Address      IP Address      Group Name     Multicast IP     Status
6c:20:56:b8:ba:40 10.10.30.10      mb-foreign      0.0.0.0          Up
Deployment Considerations

**REVIEW DRAFT—CISCO CONFIDENTIAL**

(WLC-Anchor) >config mobility group member add 6c:20:56:b8:ba:40 10.10.30.10 mb-foreign

(WLC-Foreign) >config mobility group member add bc:16:65:c2:aa:c0 10.88.244.87 mb-anchor

(WLC-Anchor) >show mobility summary

Mobility Protocol Port...................... 16666
Default Mobility Domain.................. mb-anchor
Multicast Mode ......................... Disabled
Mobility Domain ID for 802.11r........ 0x5313
Mobility Keepalive Interval............... 10
Mobility Keepalive Count............... 3
Mobility Group Members Configured........ 2
Mobility Control Message DSCP Value...... 0

Controllers configured in the Mobility Group

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>Group Name</th>
<th>Multicast IP</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>6c:20:56:b8:ba:40</td>
<td>10.10.30.10</td>
<td>mb-foreign</td>
<td>0.0.0.0</td>
<td>Up</td>
</tr>
<tr>
<td>bc:16:65:c2:aa:c0</td>
<td>10.88.244.87</td>
<td>mb-anchor</td>
<td>0.0.0.0</td>
<td>Up</td>
</tr>
</tbody>
</table>

(WLC-Foreign) >show mobility summary

Mobility Protocol Port...................... 16666
Default Mobility Domain.................. mb-foreign
Multicast Mode ......................... Disabled
Mobility Domain ID for 802.11r........ 0x25f5
Mobility Keepalive Interval............... 10
Mobility Keepalive Count............... 3
Mobility Group Members Configured........ 2
Mobility Control Message DSCP Value...... 0

Controllers configured in the Mobility Group

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>Group Name</th>
<th>Multicast IP</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>6c:20:56:b8:ba:40</td>
<td>10.10.30.10</td>
<td>mb-foreign</td>
<td>0.0.0.0</td>
<td>Up</td>
</tr>
<tr>
<td>bc:16:65:c2:aa:c0</td>
<td>10.88.244.87</td>
<td>mb-anchor</td>
<td>0.0.0.0</td>
<td>Up</td>
</tr>
</tbody>
</table>

3. Configure WLAN to be anchored to anchor WLC:

(WLC-Anchor) >config wlan disable 1

(WLC-Anchor) >config wlan mobility anchor add 1 10.88.244.87

(WLC-Anchor) >config wlan enable 1

(WLC-Foreign) >config wlan disable 1

(WLC-Foreign) >config wlan mobility anchor add 1 10.88.244.87

(WLC-Foreign) >config wlan enable 1

GUI:

Refer to

4. Connect Chromecast to SSID blue on anchor WLC.
5. Connect the laptop to SSID blue on foreign WLC.

The laptop locates the Chromecast device for cast screen.

Scenario 4: Chromecast and wireless clients on different VLANs (same SSID)

If there is a need to manage Chromecast devices from smartphones on a different VLANs, refer to the following link:

http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/7-6/chromecastDG76/ChromecastDG76.html#pgfId-46574

Deploying Chromecast Devices and Users on a Single VLAN

When deploying Chromecast over network, it is important that both the client and Chromecast device offering the service are on the same VLAN. For the wireless network, this means ensuring each client user is on the same back-end interface in the controller.

For a large-scale deployment, using a single VLAN may be impossible. For information about how to have clients on one VLAN while the Chromecast devices are on another, see Chromecast using VLAN Select and AAA Override section.

Enabling Multicast Support

From the Controller tab, choose the Multicast link on the left-hand menu. Enable Global Multicast Mode and IGMP Snooping. Multicast and snooping mechanisms are outside the scope of this document. For more background information on these topics, see IP Multicast Technology Overview.
Configuring the Multicast Distribution Mode to Access Points

The Cisco Unified Wireless Network (CUWN) supports two methods of multicast distribution to access points (APs) associated with the controller. In both the modes, the original multicast packet from the wired network is encapsulated inside a Layer 3 CAPWAP packet sent via either CAPWAP Unicast or Multicast to the AP. Since the traffic is CAPWAP encapsulated, APs do not have to be on the same VLAN as the client Chromecast traffic.

The two methods of Multicast distribution are compared here:

<table>
<thead>
<tr>
<th>“Multicast-Unicast” Mode</th>
<th>“Multicast-Multicast” Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAPWAP</td>
<td>CAPWAP</td>
</tr>
<tr>
<td>239.255.255.250</td>
<td>239.255.255.250</td>
</tr>
</tbody>
</table>

Multicast-Multicast Distribution Mode

Multicast-multicast mode is the recommended option for scalability and wired bandwidth efficiency reasons.

**Note**

Multicast-multicast mode is required for the 2500-Series Wireless LAN Controller.

Go to the **Controller** tab on the General page and ensure that the AP Multicast Mode is configured to use **Multicast** mode and that a valid group address is configured. The group address is an IPv4 multicast group and is recommended to be in the 239.x.x.x-239.255.255.255 range which is scoped for private multicast applications. Do not use the 224.x.x.x, 239.0.0.x, or the 239.128.0.x address ranges for the multicast group address. Addresses in these ranges overlap with the link local MAC addresses and flood all switch ports, even with IGMP snooping enabled.
Multicast-Unicast Distribution Mode

If the wired network is not properly configured to deliver the CAPWAP multicast between the controller and AP or FlexConnect mode, and APs is used for centrally switched WLANs supporting multicast, then unicast-multicast mode is required.

Go to the Controller tab on the General page and ensure that the AP Multicast Mode is configured to use Unicast mode.
Verifying whether Chromecast is Snooped

In order to verify that Chromecast is being forwarded correctly, browse to the Monitor tab and click the Multicast left-hand menu. The address of 239.255.255.250 should be visible from the list. Click the MGID number in order to view the clients which have joined the multicast group.
Known Caveat

Description

Google Chromecast can use a supplemental feature called screencast. This feature allows the client to cast its screen to the HDMI output display/TV.

Here is Google screencast guide from Google:
https://support.google.com/chromecast/answer/6059461?hl=en

This screencast requires mdns to be configured on the WLC because it uses the following mdns query: 224.0.0.251 MDNS PTR _googlecast._tcp.local.

Symptom

Chromecast/Screencast feature depends on mDNS query of 224.0.0.251 MDNS PTR _googlecast._tcp.local.

Needs to be documented in the WLC Chromecast guide.

Conditions

WLC or NGWC implementing Chromecast and its Screencast function.
**Deployment Considerations**

**Workaround**

Configure mDNS filter.

**Tune Multicast Data Rates**

Multicast applications, such as Chromecast, require special consideration when being deployed over a wireless network because a multicast in 802.11 is sent out as a broadcast so that all clients can hear it. The actual data rate used by the AP in order to transmit the Chromecast frames is the highest mandatory rate configured within that band. For 2.4 GHz, the default rate is 11 Mbps.

In order to optimize the delivery of these frames, it is important to tune the 802.11 data rates within the controller to allow multicast to be delivered at the highest rate that the coverage model of the network can support. For networks with a low density of APs, it may be necessary to keep the data rates at the default. For a network that does not have any requirement to support 802.11b clients, tuning the data rate to 12 Mbps mandatory and lower rates disabled will help to reduce multicast airtime utilization. This is configured under the Wireless tab and the 802.11b/g/n > Network menu.
Ensuring Peer-to-Peer Blocking is Disabled

Peer-to-peer blocking is configured on a per-WLAN basis and prevents clients on the wireless network from communicating with one another. By default, peer-to-peer blocking is disabled for new WLANs. But, if enabled, can cause issues for services such as Chromecast on the wireless network. Any Chromecast service that relies on communication between wireless clients can be broken by peer-to-peer blocking.

Under the WLANs tab > Advanced section of the WLAN configuration, make sure P2P Blocking Action is set to Disabled.
Blocking Chromecast

In some cases, it is desirable to filter out Chromecast in order to prevent discovery between two nodes while still enabling other multicast applications.

Complete these steps:

**Step 1** Create ACLs on the wireless LAN controller in order to filter out Chromecast discovery traffic.

For AireOS WLC Version 7.2 or Lower

Choose **Controller** tab > **Interfaces** on the left-hand menu in order to apply the ACL. The ACL Name should be changed to the ACL created in Step 1.
For AireOs WLC Version 7.2 or higher
Apply the IPv4 and IPv6 ACL in order to filter out Chromecast traffic before it can be forwarded to other clients.
Chromecast Application

Clients with Chromecast extension installed on their Chrome browser can display the entire browser and screen by using a Chromecast device. Once the client discovers the Chromecast device using SSDP, the subsequent connections between the wireless client and Chromecast device to mirror the display use TCP based unicast messages.

Complete the following steps to install Chromecast extension:

**Step 1**  
Visit the store for chrome extension at:  
https://chrome.google.com/webstore/search-extensions/googlecast

**Step 2**  
Install the GoogleCast Extension:  
For more information on installing chrome extension visit:  
https://support.google.com/chrome/answer/167997?hl=en

**Step 3**  
Notice the Googlecast tab at the top right corner of the chrome browser on installing the extension.
Step 4  Make sure that the Computer is connected to the client wireless network. Click the browser to find the Chromecast device in your network and mirror your browser.
Chromecast using VLAN Select and AAA Override

The limitation of using Chromecast on a single VLAN is difficulty to scale for large campus networks such as a university or an enterprise. If a large subnet is created for all wireless clients, the multicast messages quickly consume up valuable airtime across the network. You can use the VLAN Select feature to assign clients to an array of VLANs on the back-end, essentially breaking up the multicast domain. An option of the VLAN Select feature is the Multicast VLAN, which allows you to select a specific interface for downstream multicast traffic.

For more information on VLAN Select, see the VLAN Select and Multicast Optimization Features Deployment Guide.

Using VLAN Select with the multicast VLAN feature allows a separate subnet to be used for Chromecast devices, while still enabling Chromecast for use by a specific set of clients on a different VLAN. The specific set of clients can be assigned to a VLAN using AAA override.

For example, consider a University campus with Chromecast devices installed in each classroom. The administrator wants to design a policy to provide Chromecast access to only the teachers, and avoid the students from getting access to the Chromecast devices.

Complete the steps:
Step 1  Go to the Controller tab > Interfaces on the left-hand menu. Create the necessary interfaces for the client VLANs (student and teacher in this example) and also an interface for the Chromecast subnet (chromecast_device in this example).

Step 2  (Optional: This can be achieved using a single interface as well). Go to the Controller tab > Interface Groups on the left-hand menu. Create a new interface group, and add the previously created client interfaces (teacher and student, in this example).

Step 3  (Optional: This can be achieved using a single interface as well, e.g. student). Go to the WLANs tab, and create the client SSID. Select the interface group created in Step 2.
Step 4  Enable AAA Override for the Client SSID, to ensure that the client who need Chromecast access is assigned to the Teacher VLAN.
Step 5  On the back-end radius server, assign the correct VLAN by user role. Following is an example of configuring the Cisco ISE (Identity Services Engine) to assign VLAN 40 to a teacher. Follow the same procedure to assign a separate VLAN to the student by accessing a back-end user database (e.g. Active Directory).

![Cisco Identity Services Engine](image)

Step 6  Create a new SSID for the Chromecast devices. The security policy should be WPA2-PSK, and the interface should be the chromecast_device VLAN created in Step 1. It is also advisable to configure the WLAN radio policy to **802.11b/g only**. Enable the Multicast VLAN feature and select **Teacher** as the multicast interface created in Step 1.
Verifying VLAN Select and AAA Override with Chromecast

Complete the steps:

**Step 1** Visit the store for chrome extension at:
https://chrome.google.com/webstore/search-extensions/googlecast.

**Step 2** Install the GoogleCast Extension:
For more information on installing chrome extension visit:
https://support.google.com/chrome/answer/167997?hl=en

**Step 3** Notice the Googlecast tab at the top right corner of the chrome browser on installing the extension:
Step 4  Make sure that the Computer is connected to the client wireless network and gets an IP address from the Teacher VLAN. Click the googlecast tab on the teacher user computer, and you should be able to discover the Chromecast device.

Step 5  Make sure that the Computer is connected to the client wireless network and gets an IP address from the Student VLAN. Click the Googlecast tab on the student user computer, and the Chromecast device should not be discovered.
Chromecast Packet Level Details

The Chromecast devices operate on DIAL protocol. The DIAL service discovery enables a client to discover the DIAL Server (Chromecast) on its local network, and obtain access to DIAL services. This is achieved by using a new search target within the SSDP defined by uPNP.

1. Service Discovery Request:

239.255.255.250

1. (Response with IP address of service)

1. Service Discovery Request:
The clients that wish to discover Chromecast servers send a request over UDP to the IP address 239.255.255.250 and UDP port number 1900. Included in the multicast packet is the Search Target predefined by the DIAL specification:


The TTL on the multicast packet set to 1 ensures that the packet is not routed across subnets.

2. **Service Discovery Response:**

A Chromecast device receiving the request with the Search Target responds by sending a unicast UDP packet to the client. The UDP packet contains the LOCATION header, which has an absolute http URL for the uPnP description of the Chromecast device. The UDP packet also contains the Search Target sent in the request packet.
Chapter 1  Chromecast Deployment Guide, Release 7.6

### Chromecast Packet Level Details

3. The subsequent connections are TCP based unicast packets, which are explained in detail at: http://www.dial-multiscreen.org/dial-protocol-specification