Chromecast as mDNS Service in order to Cast Screen Configuration on WLC

Contents

Introduction

This document describes how to configure Chromecast devices to act as a Bonjour service provider. The use and administration of Chromecast devices on the networks is simplified by the support of Bonjour services. The **_googlecast._tcp.local.** service string allows Chromecast devices to act as any other Bonjour service provider. This service is used exclusively in order to cast the screen of a supported device to the screen where Chromecast is connected.

This document focuses on how to mirror from a computer that runs Google Chrome to a Chromecast device. For more information, see Cast a tab.

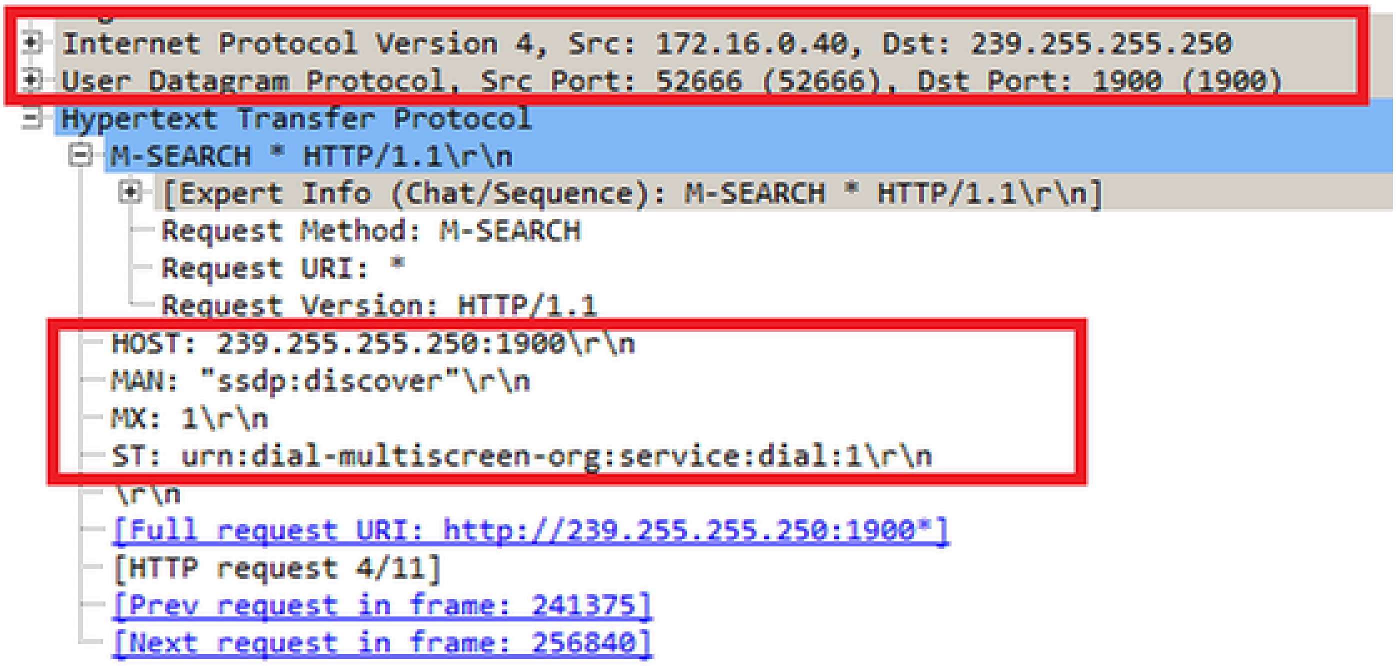
This document is focused in applications and end devices (like smartphones) that uses mDNS to discover Chromecast Devices. There will be some application or devices that will only try to look for Chromecast devices using Discovery and Launch (DIAL) service.

If our application and/or end device supports mDNS we can follow the Scenarios 1 to 3 but if our application only supports DIAL service then Chromecast device and the end device used to discover it must be on the same Virtual Local Area Network (VLAN) and in addition to that, Multicast forwarding needs to be enabled on the WLC. See Scenario 4 at the end of this document.

To verify if our device/application supports mDNS and/or DIAL we can make a packet capture and check the queries sent by our device/application.

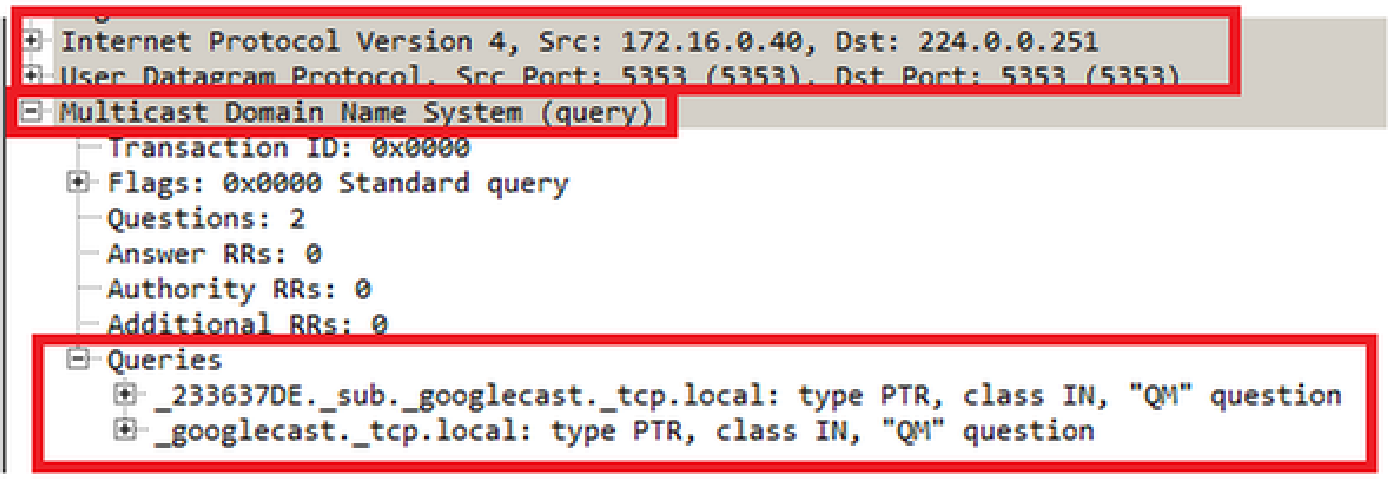
If we see queries sent only to 239.255.255.250 port UDP 1900 then our device/application only support DIAL service discovery, if we also see queries sent to 224.0.0.251 port UDP 5353 then our device/application also supports mDNS.

Example of DIAL querie:



```
+ Internet Protocol Version 4, Src: 172.16.0.40, Dst: 239.255.255.250
+ User Datagram Protocol, Src Port: 52666 (52666), Dst Port: 1900 (1900)
- Hypertext Transfer Protocol
  - M-SEARCH * HTTP/1.1\r\n
    + [Expert Info (Chat/Sequence): M-SEARCH * HTTP/1.1\r\n]
      Request Method: M-SEARCH
      Request URI: *
      Request Version: HTTP/1.1
    HOST: 239.255.255.250:1900\r\n
    MAN: "ssdp:discover"\r\n
    MX: 1\r\n
    ST: urn:dial-multiscreen-org:service:dial:1\r\n
    \r\n
    [Full request URI: http://239.255.255.250:1900*]
    [HTTP request 4/11]
    [Prev request in frame: 241375]
    [Next request in frame: 256840]
```

Example of mDNS querie:



```
+ Internet Protocol Version 4, Src: 172.16.0.40, Dst: 224.0.0.251
+ User Datagram Protocol, Src Port: 5353 (5353), Dst Port: 5353 (5353)
- Multicast Domain Name System (query)
    Transaction ID: 0x0000
  + Flags: 0x0000 Standard query
    Questions: 2
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  - Queries
    + _233637DE._sub._googlecast._tcp.local: type PTR, class IN, "QM" question
    + _googlecast._tcp.local: type PTR, class IN, "QM" question
```

Prerequisites

Requirements

Cisco recommends you have basic knowledge of Bonjour services over a Wireless LAN Controller (WLC). For more information, see Manage Bonjour Services for BYOD.

The Chromecast device must be able to make Domain Name System (DNS) queries to 8.8.8.8, otherwise it does not work.

Wireless clients that mirror screen-to-Chromecast do not need to have Internet access.

Components Used

The information in this document is based on these software and hardware versions:

- WLC 5508 version 8.0.110.0
- WLC 2504 version 8.0.110.0
- Chromecast version 27946
- Access Point (AP) 3700i in local mode
- Laptop that runs Google Chrome version 42.0.x

The information in this document was 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.

Configure

Configuration Scenarios

This section describes these four configuration scenarios:

1. Chromecast and wireless clients on the same Wireless LAN (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 Service Set Identifier (SSID))

Initial Configuration

For all of the scenarios except for scenario 4, add the service string used by Chromecast when you cast on a screen. This allows the WLC to recognize a Chromecast device.

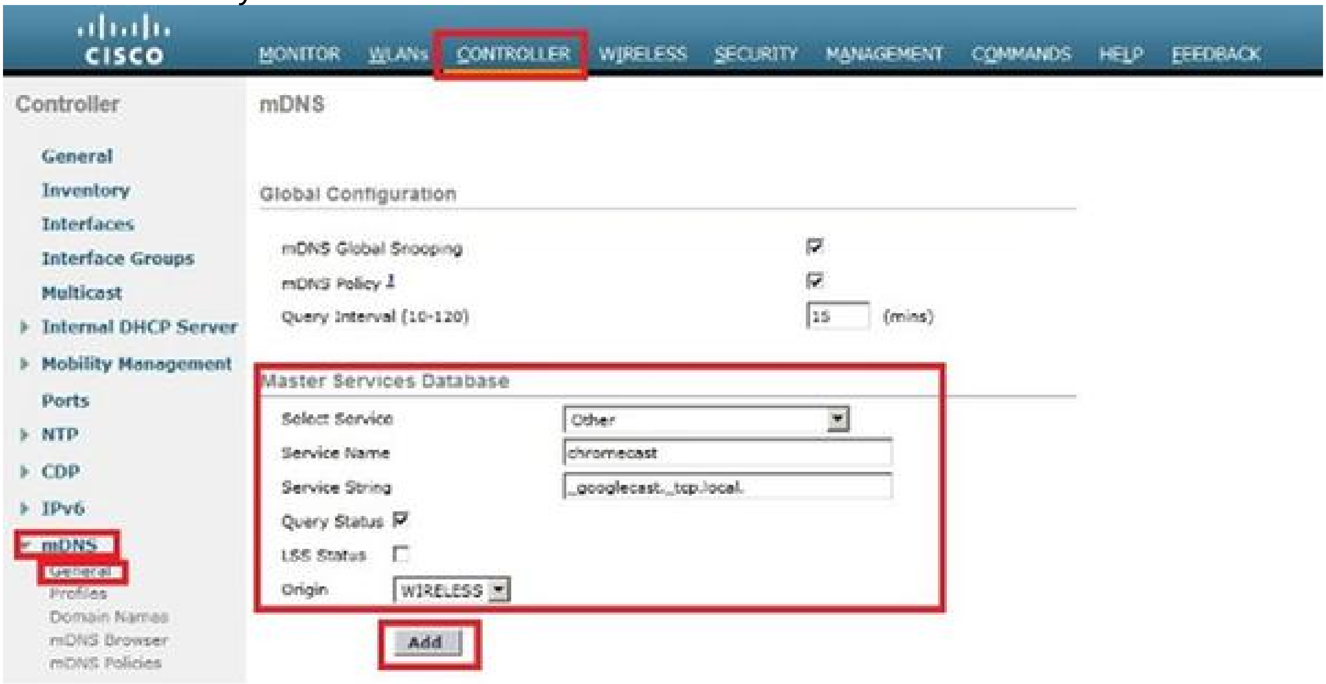
From the CLI:

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

Number of Services............................. 7
Mobility learning status ....................... Enabled
Service-Name  LSS  Origin  No SP  Service-string
------------------------------- ---- ---------- ----- ---------------
chromecast  No All 1 _googlecast._tcp.local.
```

From the GUI:

1. Choose **Controller** > **mDNS** > **General**. In the Master Services Database section of the mDNS window, choose these settings: For Select Service, choose **Other**.For Service name, enter **chromecast**.For Service String, enter **_googlecast._tcp.local.**.Check **Query Status**.For Origin, choose **Wireless**.

2. Click **Add** when you are done.



mDNS

Global Configuration

mDNS Global Snooping ☑

mDNS Policy ☑

Query Interval (10-120) 15 (mins)

Master Services Database

Select Service: Other

Service Name: chromecast

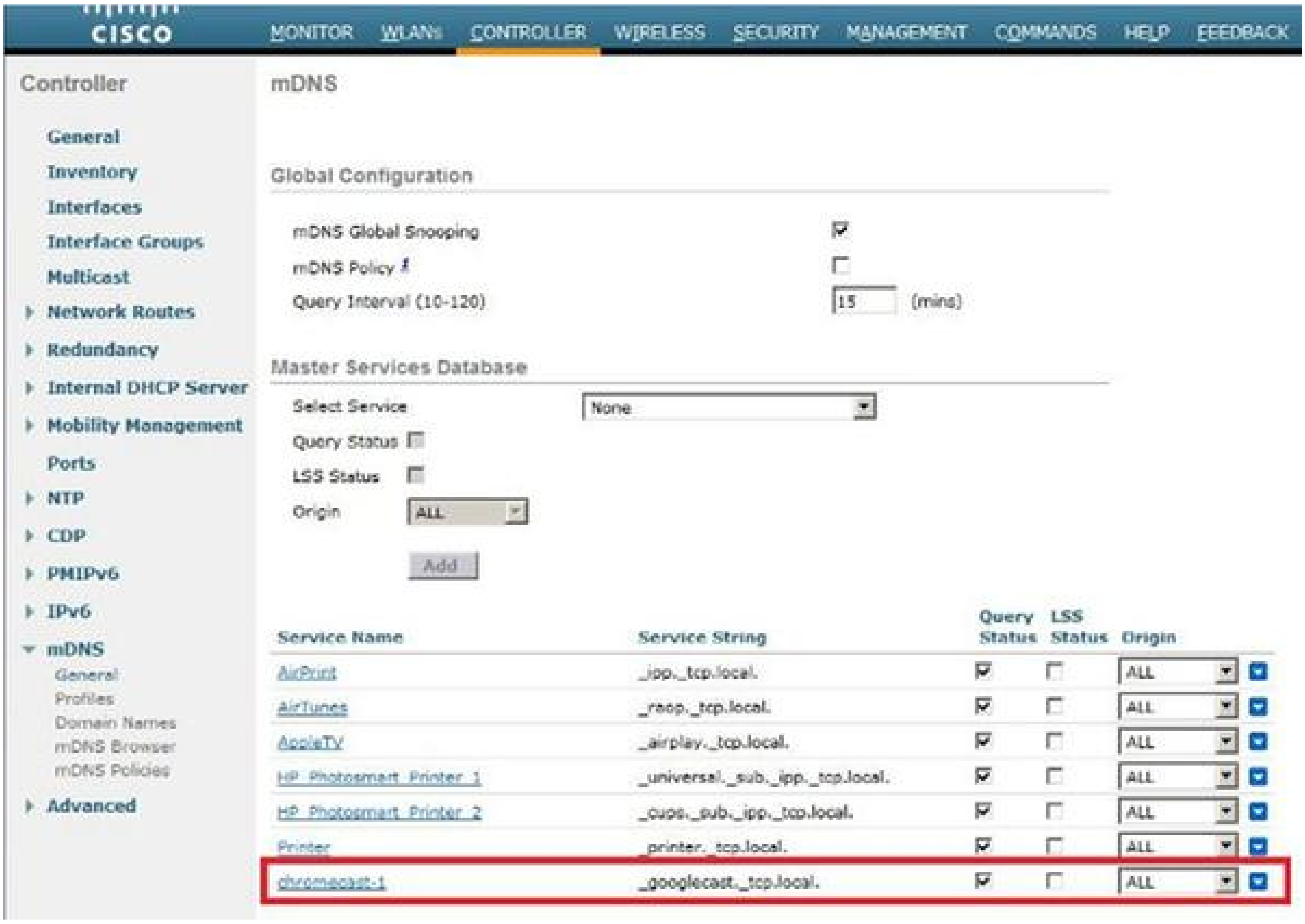
Service String: _googlecast._tcp.local.

Query Status ☑

LSS Status ☐

Origin: WIRELESS

The new Chromecast service appears in the multicast Domain Name System (mDNS) window:



mDNS

Global Configuration

mDNS Global Snooping ☑

mDNS Policy ☐

Query Interval (10-120) 15 (mins)

Master Services Database

Select Service: None

Query Status ☐

LSS Status ☐

Origin: ALL

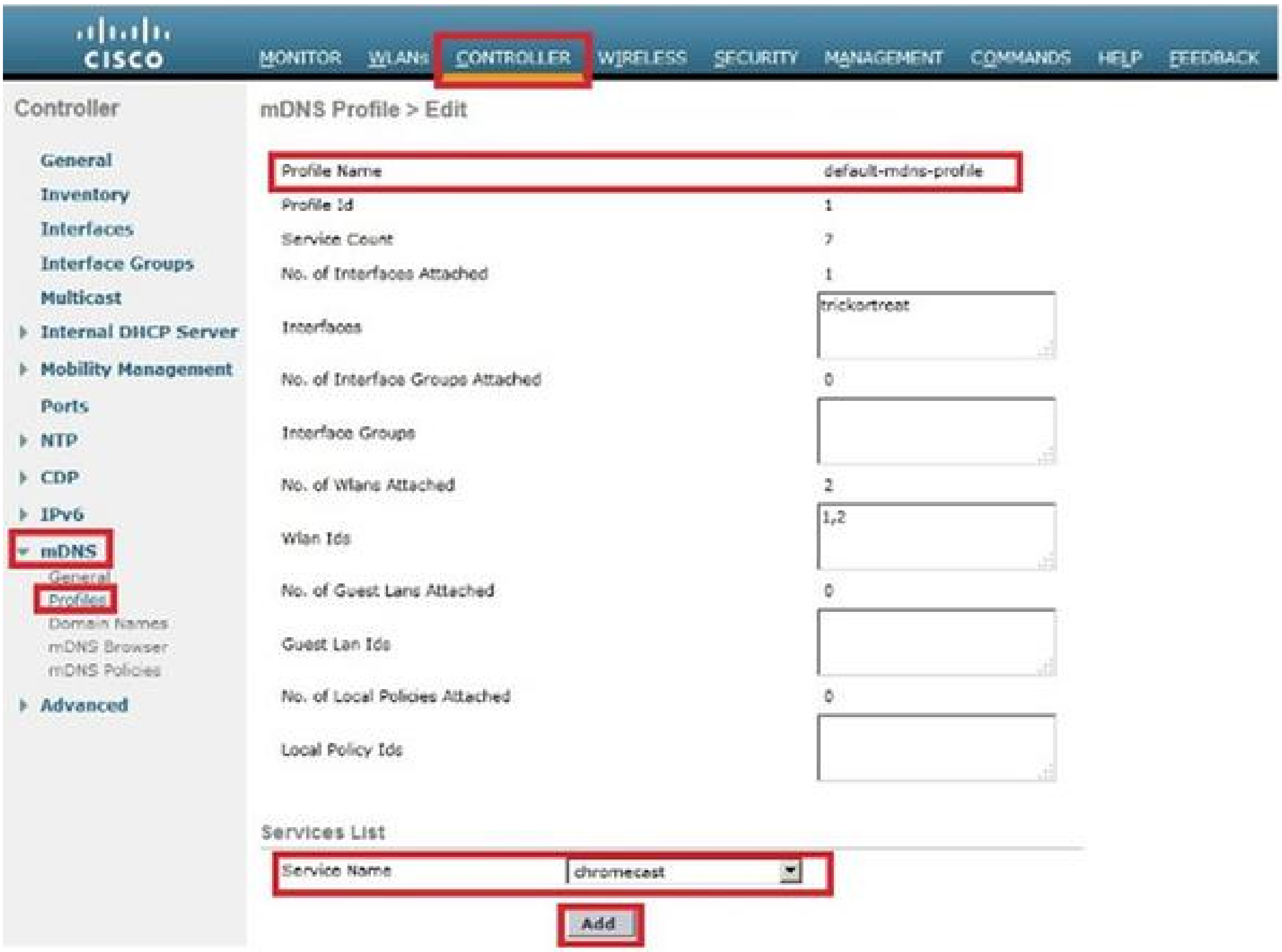
Service Name	Service String	Query Status	LSS Status	Origin
AirPrint	_ipp._tcp.local.	☑	☐	ALL
AirTunes	_raop._tcp.local.	☑	☐	ALL
AppleTV	_airplay._tcp.local.	☑	☐	ALL
HP_Photosmart_Printer_1	_universal._sub._ipp._tcp.local.	☑	☐	ALL
HP_Photosmart_Printer_2	_cups._sub._ipp._tcp.local.	☑	☐	ALL
Printer	_printer._tcp.local.	☑	☐	ALL
chromecast-1	_googlecast._tcp.local.	☑	☐	ALL

3. Add this service to the mDNS profile that is used on the WLAN. In this case the default profile is used. From the CLI:

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

>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` From the GUI, choose **Controller** > **mDNS** > **Profiles**. Verify the profile name in the Profile Name field and for Service Name, choose **chromecast** from the drop-down list. Click **Add** when you are
done.



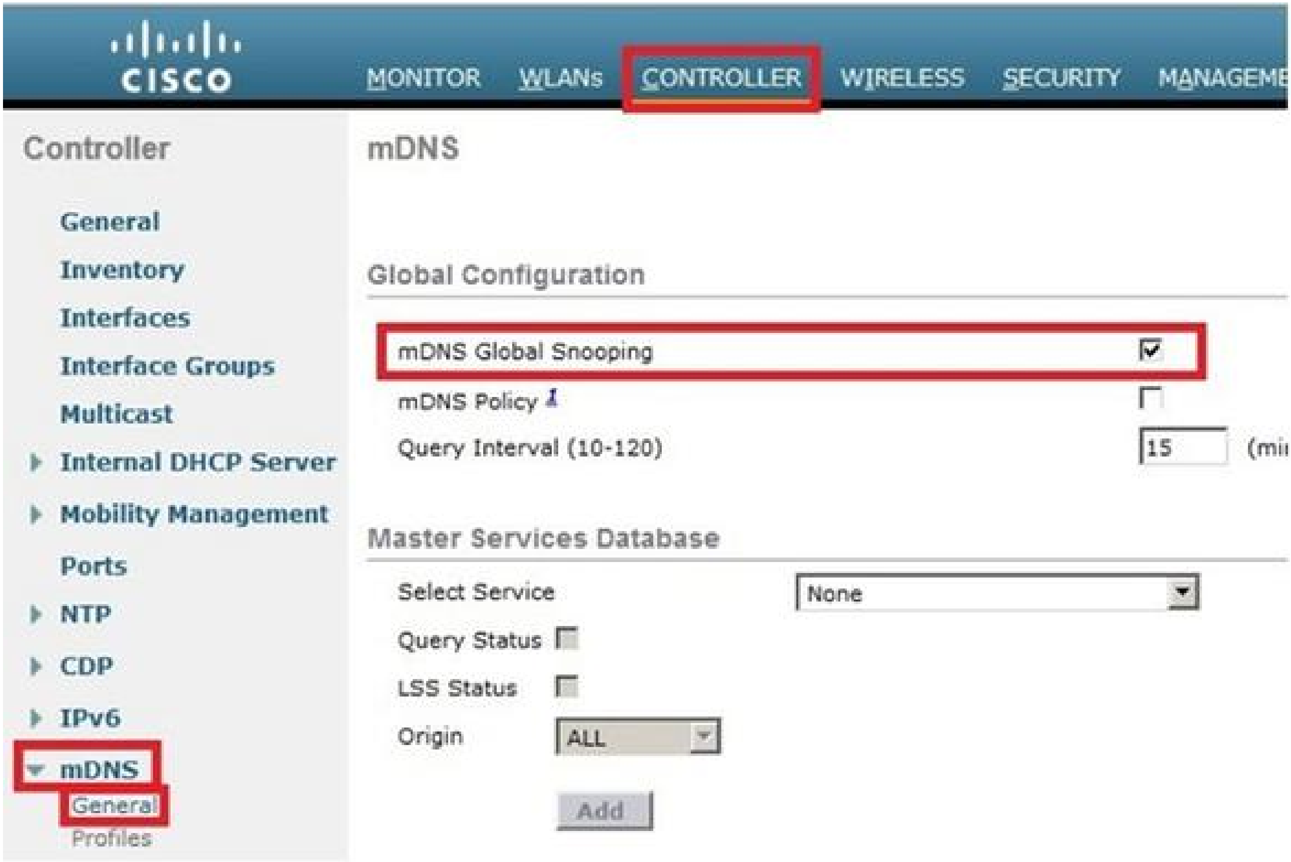
mDNS Profile > Edit

Profile Name	default-mdns-profile
Profile Id	1
Service Count	7
No. of Interfaces Attached	1
Interfaces	trickortreat
No. of Interface Groups Attached	0
Interface Groups	
No. of Wlans Attached	2
Wlan Ids	1,2
No. of Guest Lans Attached	0
Guest Lan Ids	
No. of Local Policies Attached	0
Local Policy Ids	

Services List

Service Name: chromecast

4. Enable mDNS snooping. Choose **Controller** > **mDNS** > **General** and check the **mDNS Global Snooping** checkbox.



mDNS

Global Configuration

mDNS Global Snooping ☑

mDNS Policy ☐

Query Interval (10-120) 15 (mi

Master Services Database

Select Service None

Query Status ☐

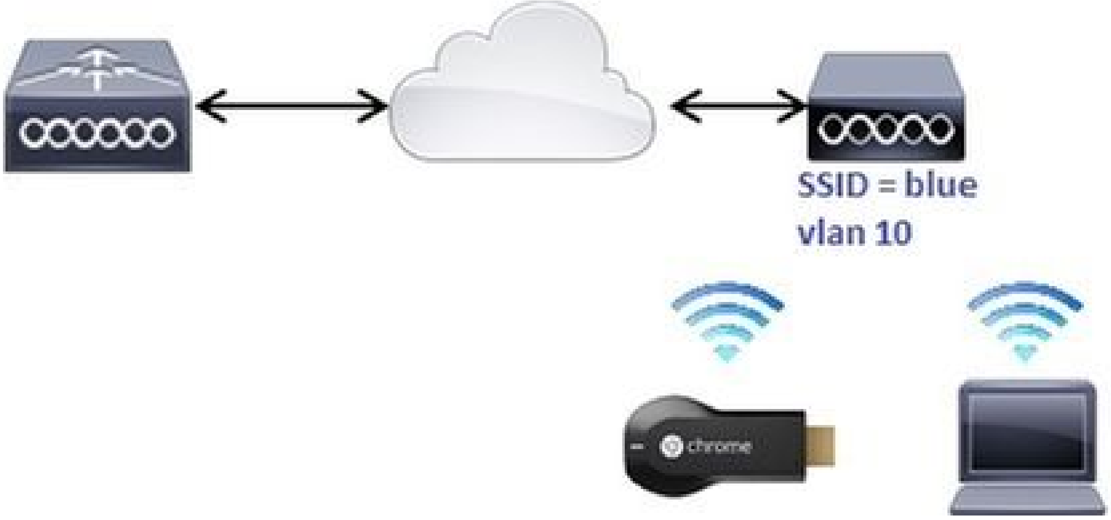
LSS Status ☐

Origin ALL

Chromecast and wireless client on same WLAN/VLAN

Network Diagram

This diagram shows Chromecast and wireless clients on the same WLAN and VLAN.

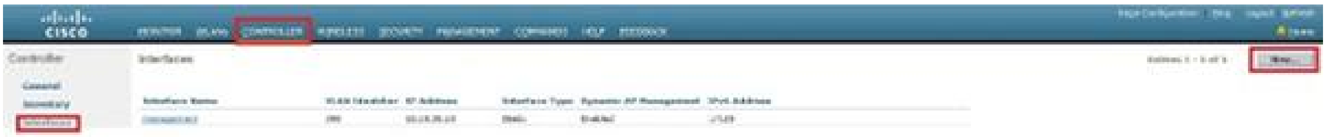


Configuration

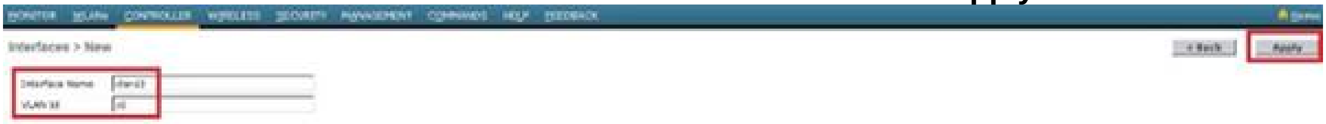
1. Create subinterface vlan 10. This interface has a Dynamic Host configuration Protocol (DHCP) server located on the same VLAN. From the CLI:

```
>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
```

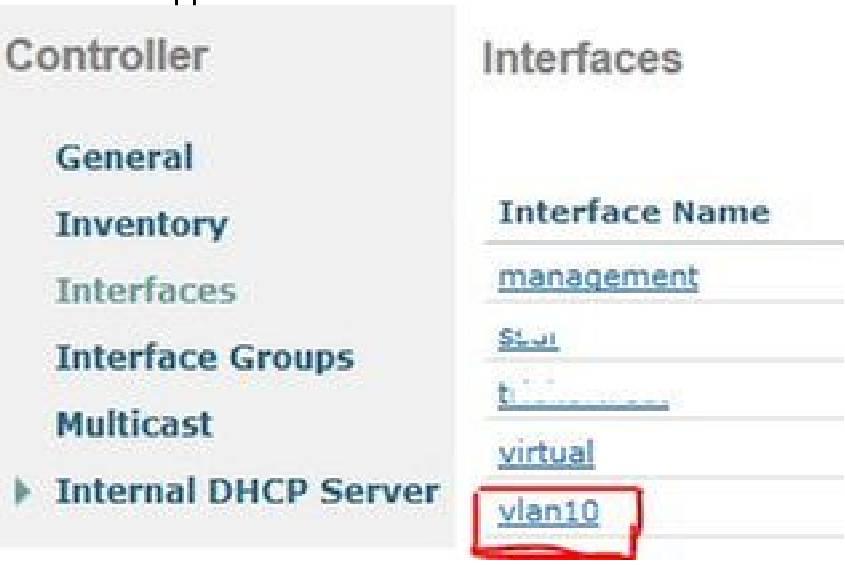
`>config interface dhcp dynamic-interface vlan10 proxy-mode disable` From the GUI:Choose **Controller** > **Interfaces** and click **New**.



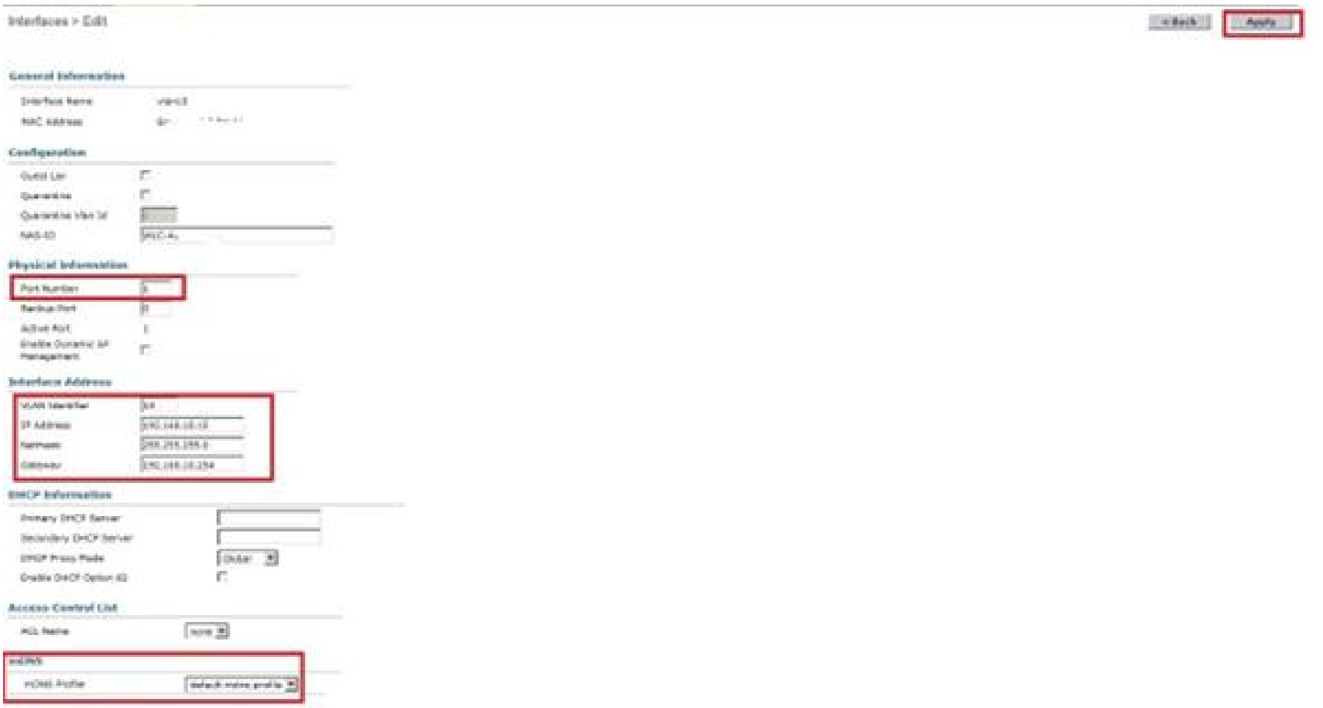
Enter the Interface Name and VLAN ID in the relevant fields. Click **Apply**.



The new interface appears on the screen. Click the new interface. In this example,



vlan10. In the Edit window, configure these fields: Port NumberVLAN IdentifierIP AddressNetmaskGatewaymDNS Profile

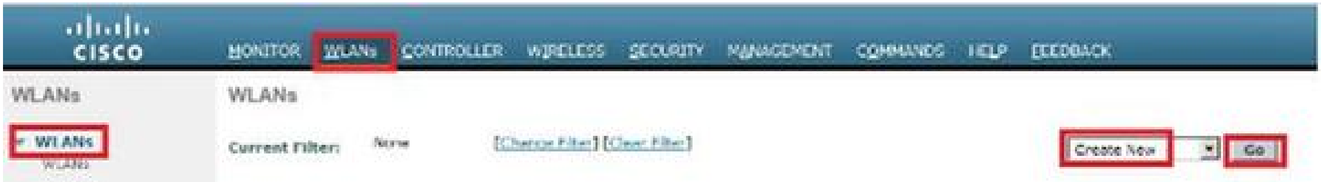


2. Create the WLAN with these settings: Security WPA2-PSK (password = cisco-chrome)Radio policy only 802.11gBy default mDNS snooping is enabled with default-profileMap it to vlan 10From the CLI:`>config wlan create 1 blue`

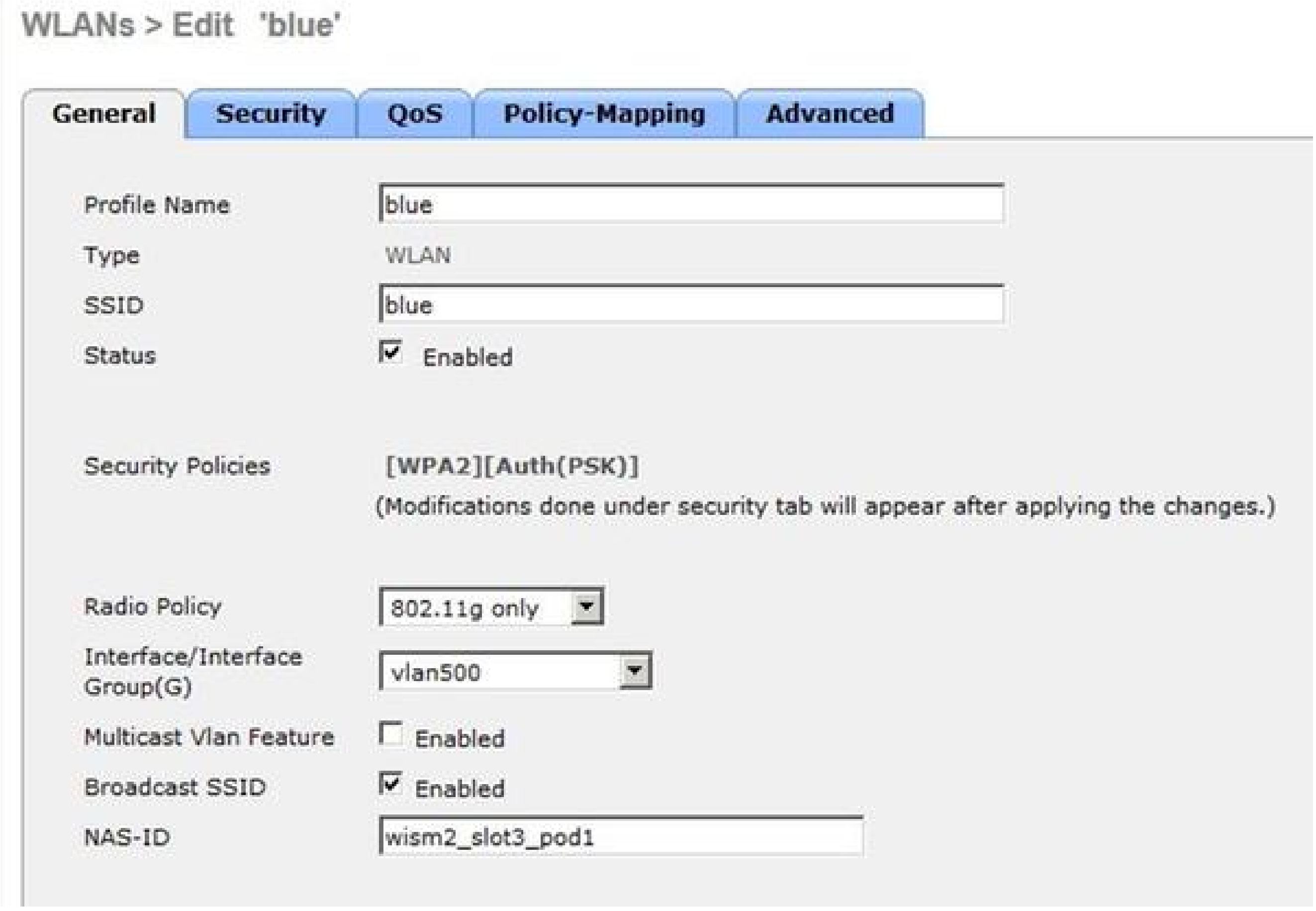
```
>config wlan security wpa akm 802.1x disable 1
>config wlan security wpa akm psk enable 1
>config wlan security wpa akm psk set-key ascii cisco-chrome 1
```

```
>config wlan interface 1 vlan10
>config wlan radio 1 802.11g-only

>config wlan ccx aironetIeSupport disable 1
>config wlan enable 1
```

From the GUI:Choose **WLANs** > **Create New** and click **Go**.



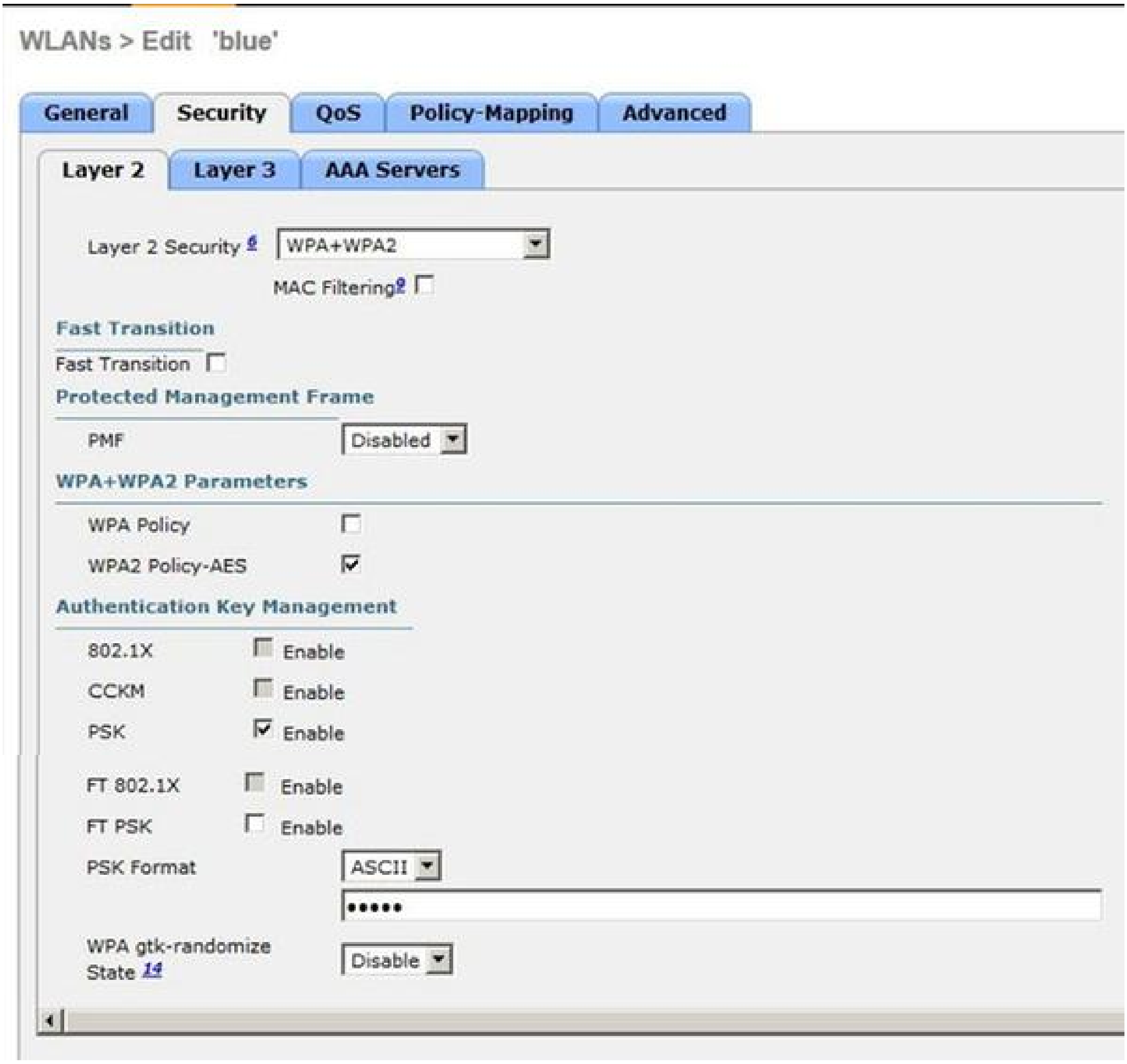
Click the General tab and enter the information in the relevant fields as this example shows:



WLANs > Edit 'blue'

Profile Name	blue
Type	WLAN
SSID	blue
Status	☑ Enabled
Security Policies	[WPA2][Auth(PSK)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	802.11g only
Interface/Interface Group(G)	vlan500
Multicast Vlan Feature	☐ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	wism2_slot3_pod1

Click the **Security** tab followed by the **Layer 2** tab. Configure the window as this example shows:



WLANs > Edit 'blue'

Layer 2 Security 6 WPA+WPA2

MAC Filtering 9 □

Fast Transition

Fast Transition □

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy □

WPA2 Policy-AES ☑

Authentication Key Management

802.1X □ Enable

CCKM □ Enable

PSK ☑ Enable

FT 802.1X □ Enable

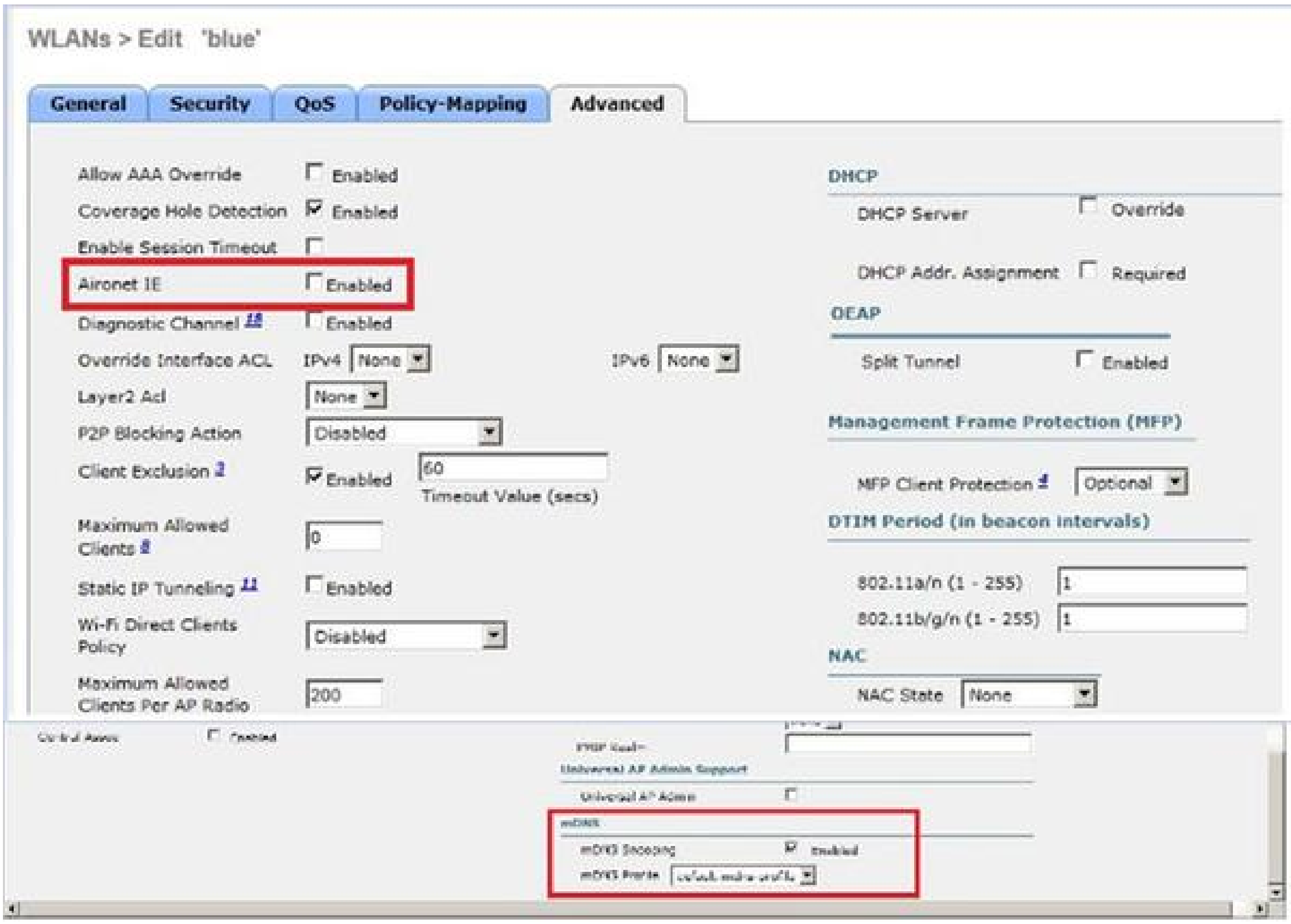
FT PSK □ Enable

PSK Format ASCII

•••••

WPA gtk-randomize State 14 Disable

Click the **Advanced** tab and ensure that **Aironet IE** is not enabled. Then check the checkbox to **Enable mDNS Snooping** and choose **default-mdns-profile** from the mDNS Profile drop-down list.



WLANs > Edit 'blue'

Allow AAA Override □ Enabled

Coverage Hole Detection ☑ Enabled

Enable Session Timeout □

Aironet IE □ Enabled

Diagnostic Channel □ Enabled

Override Interface ACL IPv4 None IPv6 None

Layer2 Acl None

P2P Blocking Action Disabled

Client Exclusion ☑ Enabled 60 Timeout Value (secs)

Maximum Allowed Clients 0

Static IP Tunneling □ Enabled

Wi-Fi Direct Clients Policy Disabled

Maximum Allowed Clients Per AP Radio 200

DHCP

DHCP Server □ Override

DHCP Addr. Assignment □ Required

OEAP

Split Tunnel □ Enabled

Management Frame Protection (MFP)

MFP Client Protection Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

802.11b/g/n (1 - 255) 1

NAC

NAC State None

Universal AP Admin Support

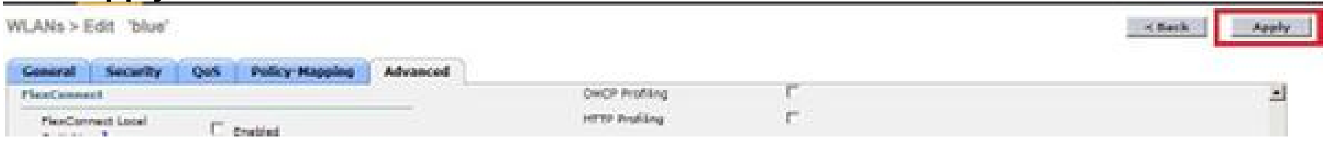
Universal AP Admin □

mDNS

mDNS Snooping ☑ Enabled

mDNS Profile default-mdns-profile

Click **Apply**.



WLANs > Edit 'blue'

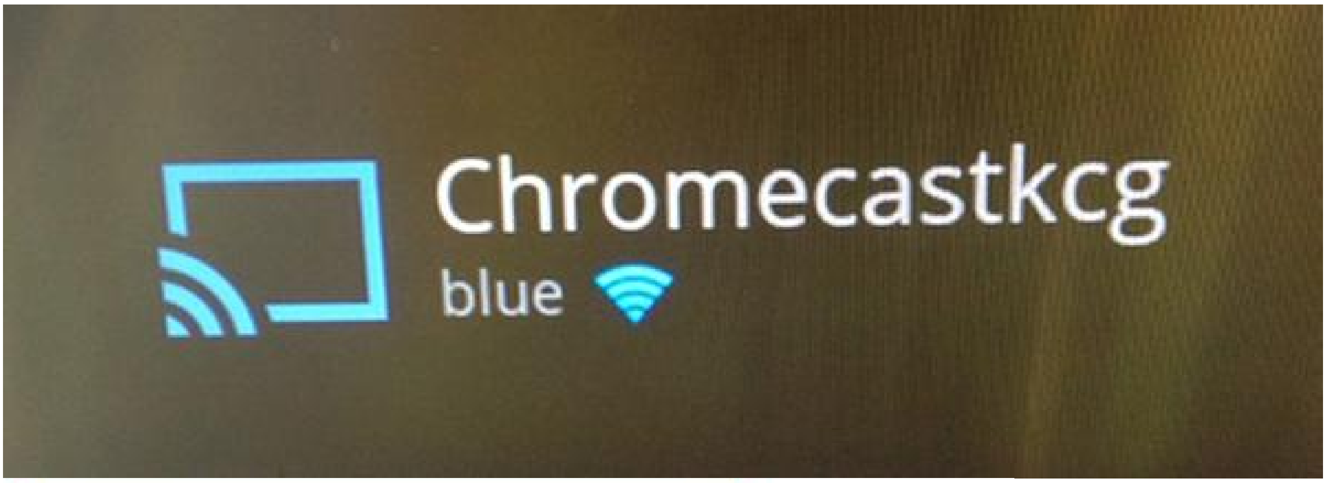
FlexConnect

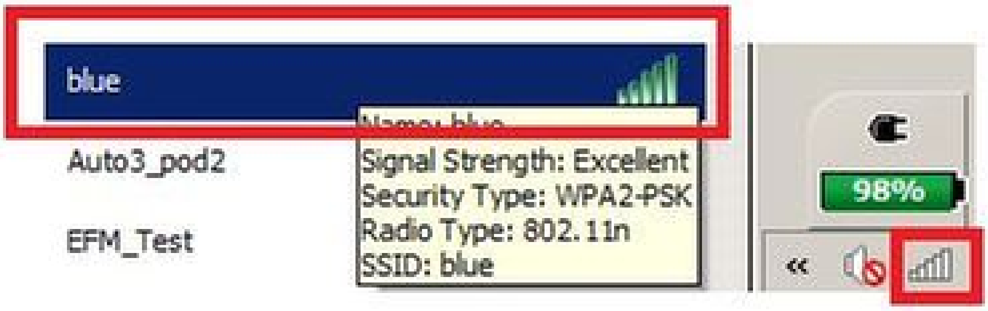
FlexConnect Local □ Enabled

DHCP Profiling □

HTTP Profiling □

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





Name: blue

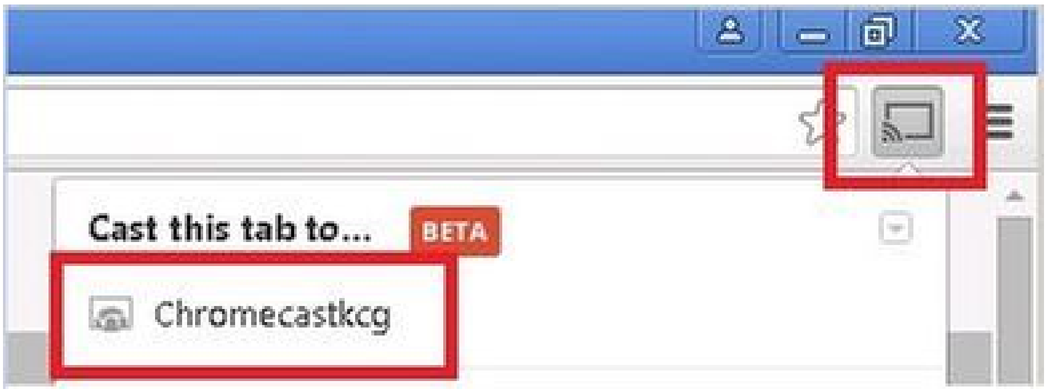
Signal Strength: Excellent

Security Type: WPA2-PSK

Radio Type: 802.11n

SSID: blue

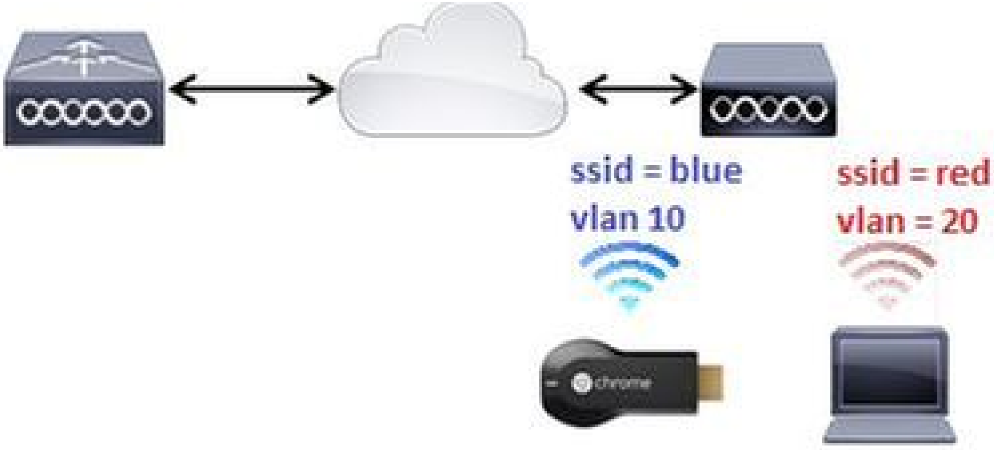
4. The Wireless client locates the Chromecast device and cast screen.



Chromecast and wireless client on different WLAN/VLAN

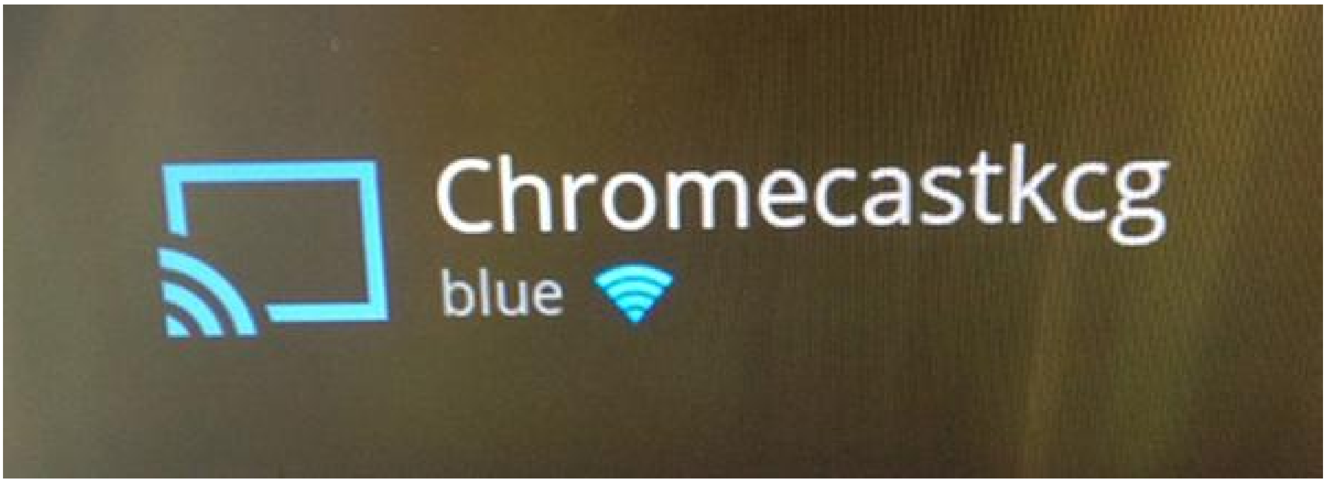
Network Diagram

This diagram shows Chromecast on WLAN A and wireless clients on WLAN B and different VLANs.

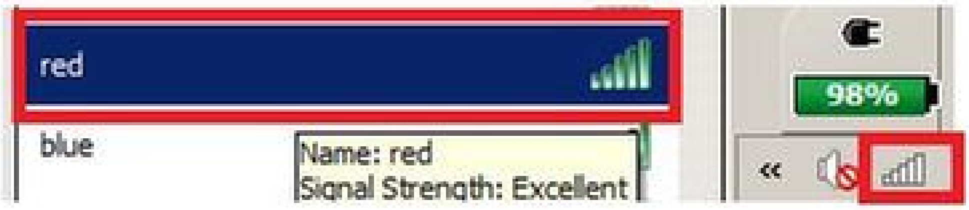


Configuration

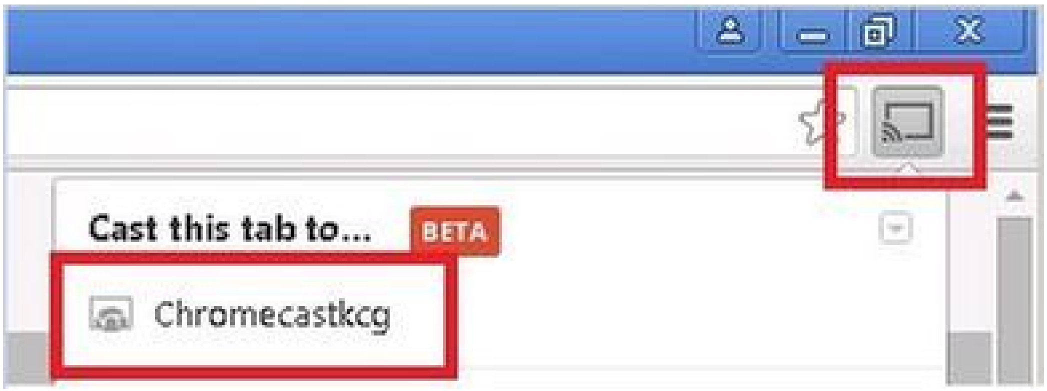
1. Add WLAN B for VLAN 20. See Steps 1 and 2 from Scenario 1 for more reference. `>config`
```
interface create vlan20 20
>config interface address dynamic-interface vlan10 192.168.20.15
255.255.255.0 192.168.20.254
>config interface port vlan20 1
>config interface mdns-profile vlan20 default-mdns-profile

>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.



4. The Wireless client can now cast a screen to the Chromecast device.



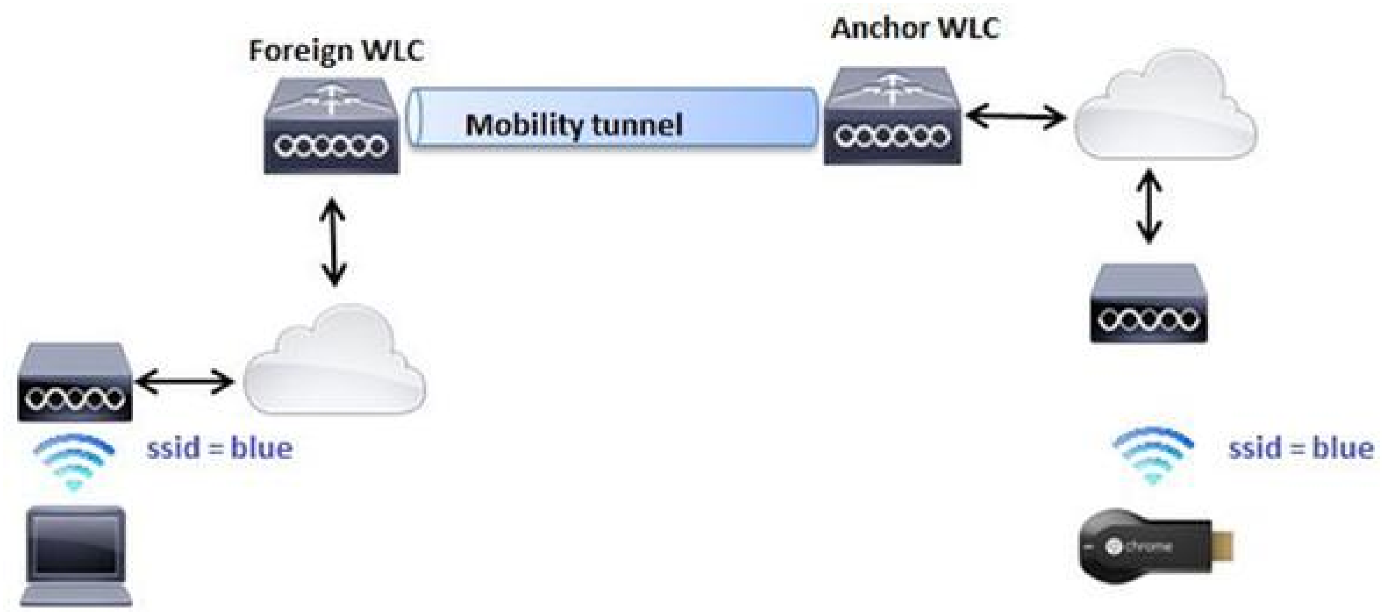
Note: Smartphones are not able to find Chromecast for management in this scenario. This scenario has only been tested for screen mirroring.

Note: This scenario only works when APs are in local mode. For APs in flexconnect - local switching, mirror only works if devices use the same VLAN (both Chromecast and laptop).

Foreing/Anchor scenario

Network Diagram

This diagram shows Chromecast on the anchor WLC and wireless clients on the foreign WLC.



Configuration

1. Create WLANs on both WLCs with identical settings. See Step 2 Scenario 1.
2. Create a mobility domain between both WLCs. From the 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


   (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
   ```

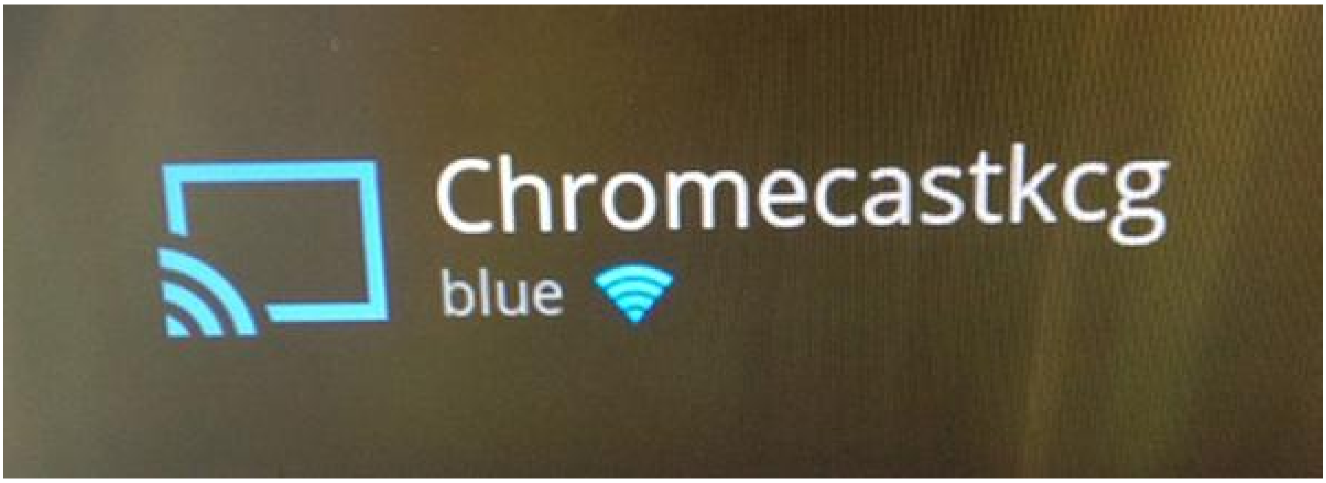
```
Mobility Protocol Port.......................... 16666
Default Mobility Domain......................... mb-anchor
Multicast Mode ................................. Disabled
Mobility Domain ID for 802.11r.................. 0x5313
Mobility Keepalive Interval..................... 10
Mobility Keepalive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

Controllers configured in the Mobility Group
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
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............... 2
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
bc:16:65:c2:aa:c0 10.88.244.87  mb-anchor  0.0.0.0  Up
```

3. Configure a WLAN that is anchored in order to anchor the WLC. From the CLI:

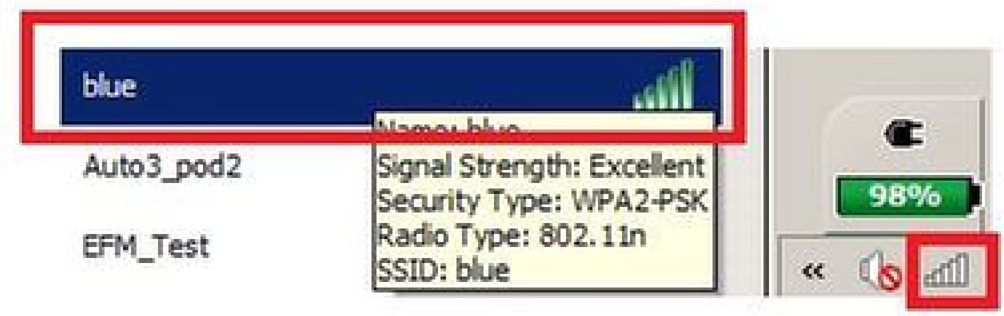
```
(WLC-Anchor) >config wlan disable 1
(WLC-Anchor) >config wlan mobility anchor add 1 10.88.244.87
(WLC-Anchor) >config wlan enable 1

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

For GUI instructions, see Configuring Mobility Groups (GUI).

4. Connect Chromecast to SSID blue on the anchor WLC.

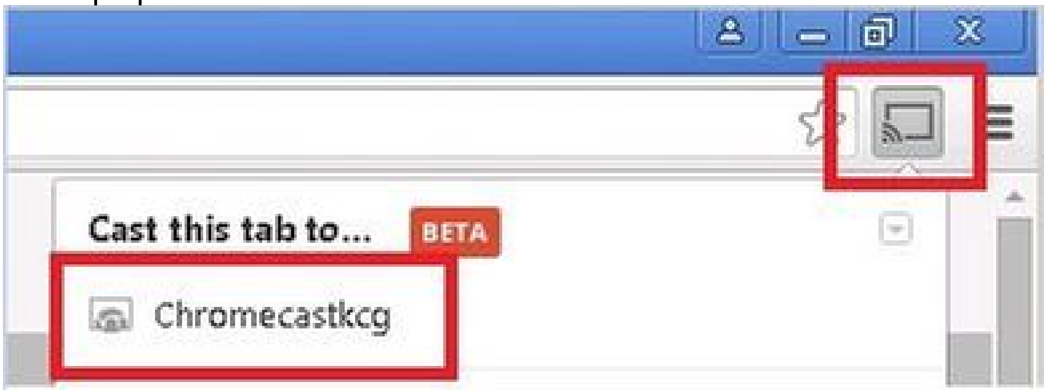


5. Connect a laptop to SSID blue on the foreign WLC.



Name: blue
Signal Strength: Excellent
Security Type: WPA2-PSK
Radio Type: 802.11n
SSID: blue

6. The laptop locates the Chromecast device for cast screen.



Using DIAL service

In order to discover Chromecast devices from smartphones/applications that only supports DIAL service we need to be sure that both of them are on the same vlan and multicast forwarding is enabled on the WLC. There are certain circumstances where they can be in different vlans. For more details check the next document Chromecast Deployment Guide, Release 7.6

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output.

1. Check that the Chromecast device and wireless clients are connected to the right WLAN.
```
>show client wlan 1

Number of Clients in WLAN........................ 1

MAC Address AP Name Status Auth Protocol Port Wired Mobility Role Device Type
----------------- ----------------- ------------- ---- ---------------- -----
80:d2:1d:4a:69:86 APe4c7.228a.4bf3 Associated Yes 802.11n(2.4 GHz) 1 No Local Unknown
00:f4:b9:0b:14:19 APe4c7.228a.4bf3 Associated Yes 802.11n(2.4 GHz) 1 No Local Unknown

chromecast mac address
wireless client mac address
```
2. Check that the Chromecast device is detected by the WLC. `>show mdns domain-name-ip summary`
```
Number of Domain Name-IP Entries................. 2

DomainName MAC Address IP Address Vlan Id Type TTL Time left
(sec) (sec)
-------------------- ---------------- ---------------- ------- ------ ------ ------
```

```
Chromecastkcg.local. 80:d2:1d:4a:69:86 192.168.10.66 10 Wireless 4725 4411


>show mdns service detailed chromecast

Service Name..................................... chromecast
Service String................................... _googlecast._tcp.local.
Service Id....................................... 8
Service query status............................. Enabled
Service LSS status............................... Disabled
Service learn origin............................. Wireless
Number of Profiles............................... 1
Profile.......................................... default-mdns-profile

Number of Service Providers ..................... 2
Number of priority MAC addresses ................ 0

ServiceProvider MAC Address AP Radio MAC Vlan Id Type TTL Time left
(sec) (sec)
-------------------- ---------------- ---------------- ------- ------
Chromecastkcg._googlecast._tcp.local. 80:D2:1D:4A:69:86 34:DB:FD:0B:9C:90
10 Wireless 4500 4410

Chromecast's name
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

The Output Interpreter Tool (registered customers only) supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output.

> **Note**: Refer to Important Information on Debug Commands before you use **debug** commands.

Enter the **debug mdns all enable** command in order to troubleshoot this configuration.