CHAPTER 1

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

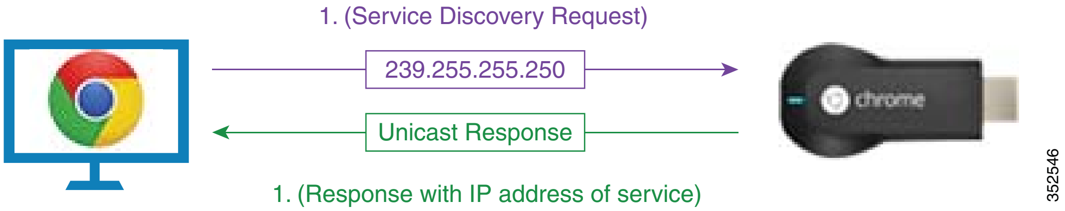
Refer to Cisco Technical Tips Conventions for more information on document conventions.

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.

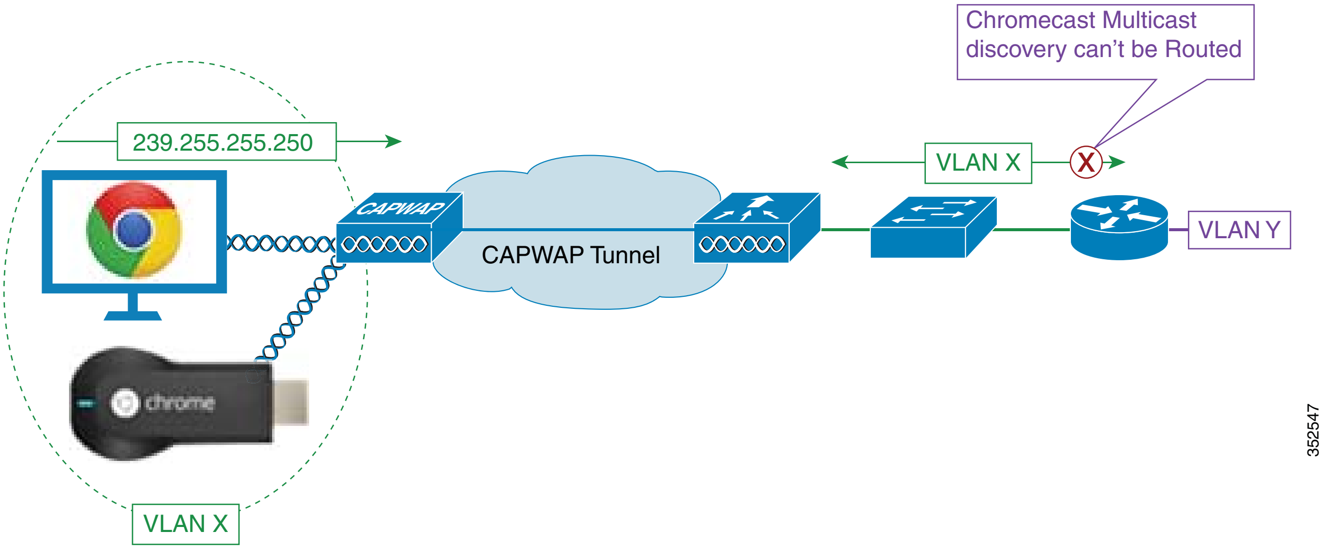
The Chromecast devices operate on DIAL protocol. The DIAL Service Discovery enables a client to discover DIAL Server (Chromecast) on its local network, and obtain access to those services. This is achieved by using a new search target within the SSDP defined by uPNP.


1. (Service Discovery Request)
239.255.255.250
Unicast Response
1. (Response with IP address of service)
chrome
352546

The clients that wishes 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.

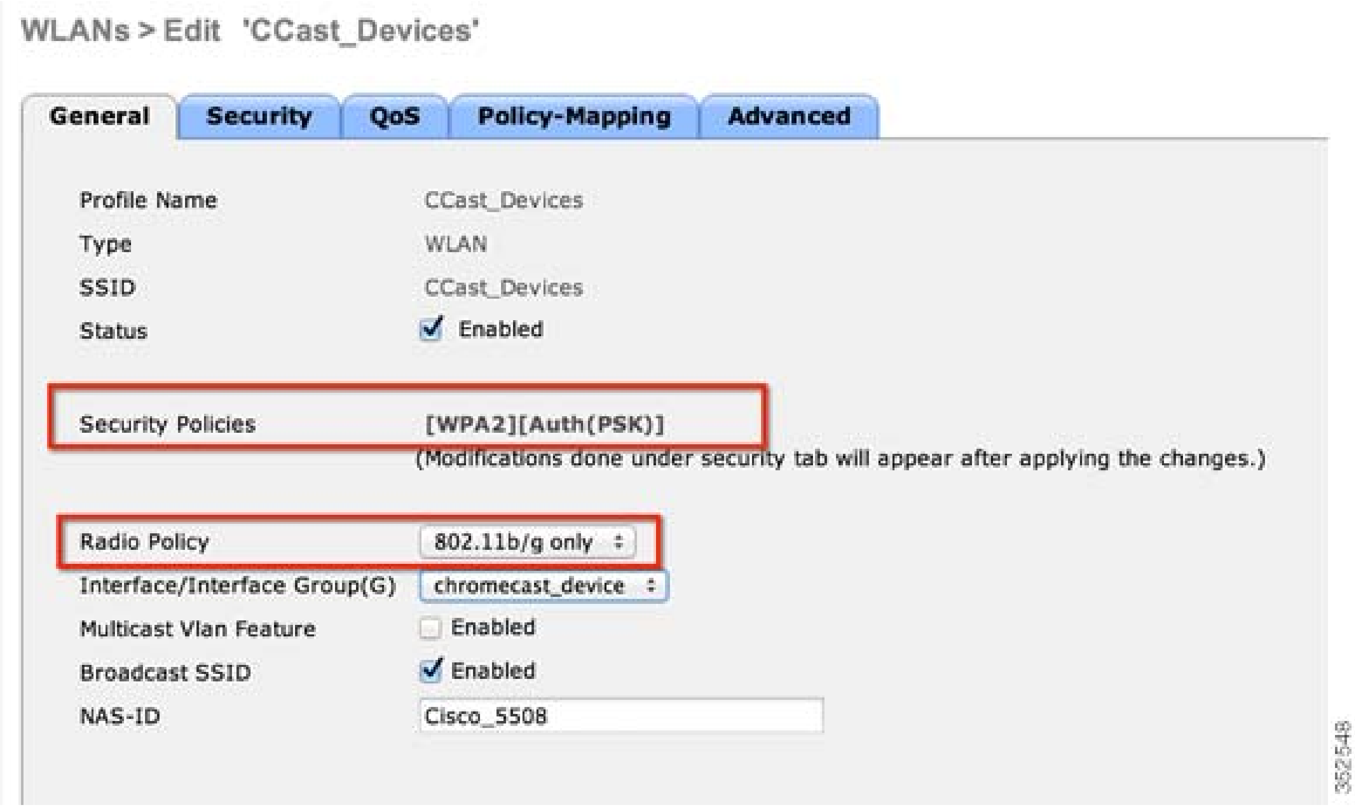


This document provides information on deploying Chromecast over large networks with single, as well as multiple VLANs.

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).



WLANs > Edit 'CCast_Devices'

Profile Name CCast_Devices
Type WLAN
SSID CCast_Devices
Status ☑ Enabled

Security Policies [WPA2][Auth(PSK)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy 802.11b/g only
Interface/Interface Group(G) chromecast_device
Multicast Vlan Feature □ Enabled
Broadcast SSID ☑ Enabled
NAS-ID Cisco_5508

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.

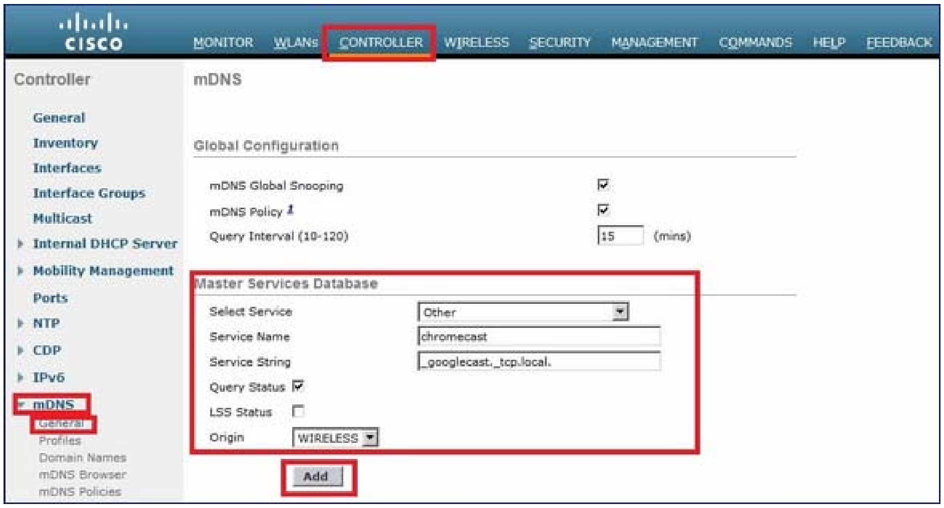
CLI

>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.
```

GUI



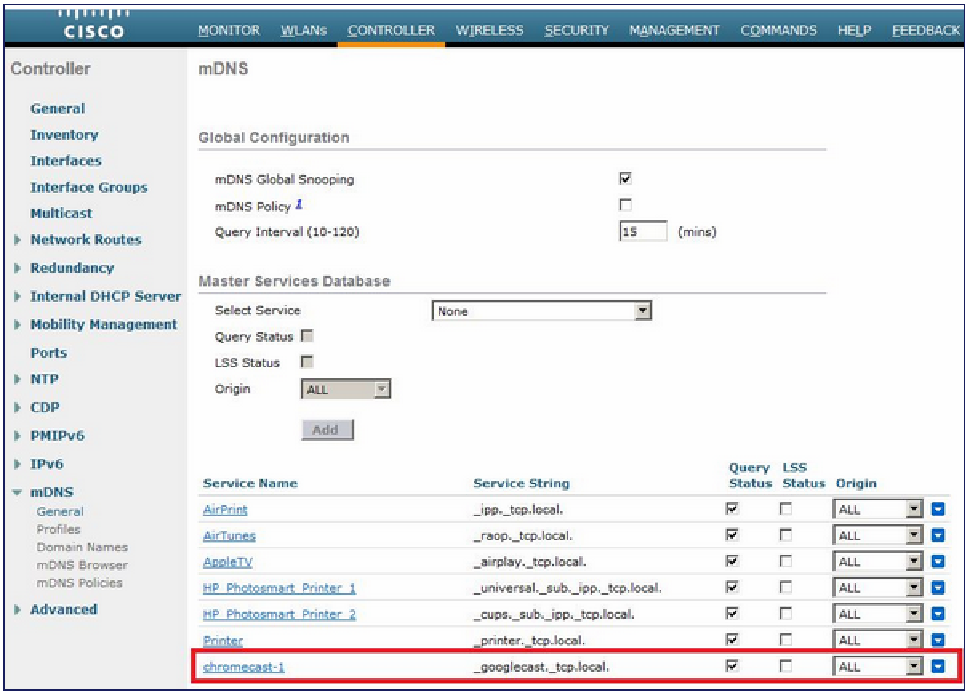
mDNS

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



mDNS

Global Configuration

mDNS Global Snooping ☑

mDNS Policy 1 □

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

Now, you can add this service to the mDNS profile that is used on the WLAN. In this case, the default profile is used:

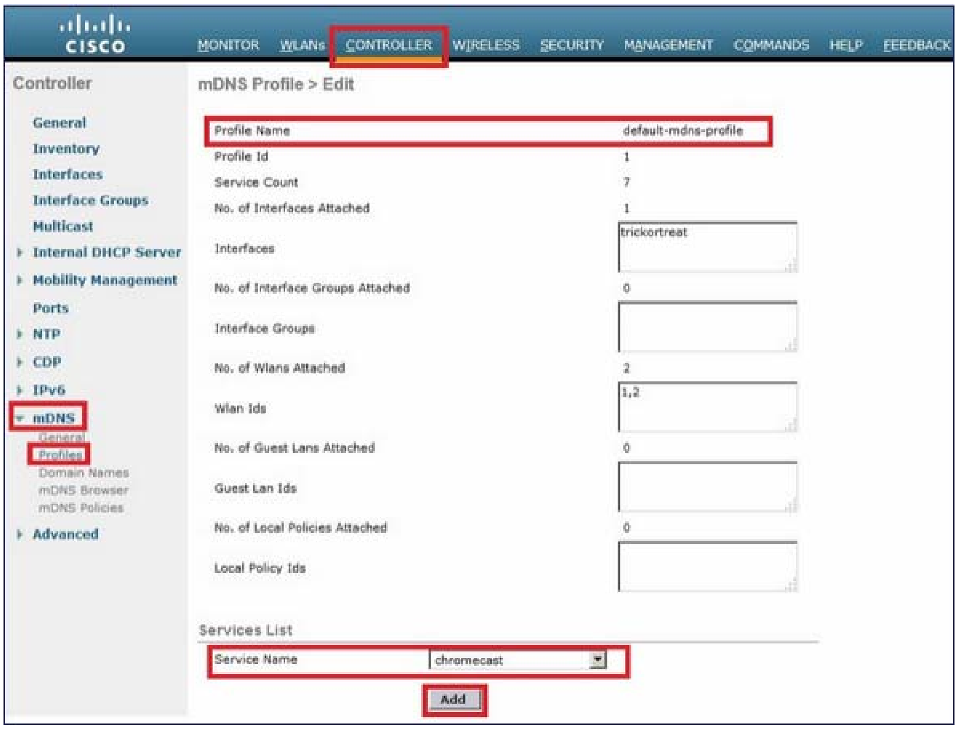
CLI

>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



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

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:

>show network summary

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

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

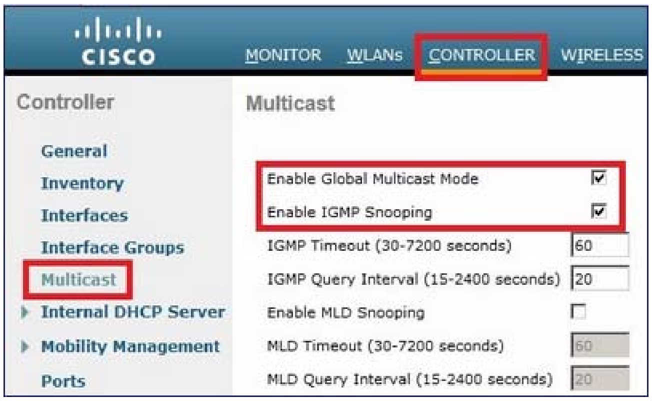
>config network multicast global enable

>config network multicast igmp snooping enable

>config mdns snooping enable

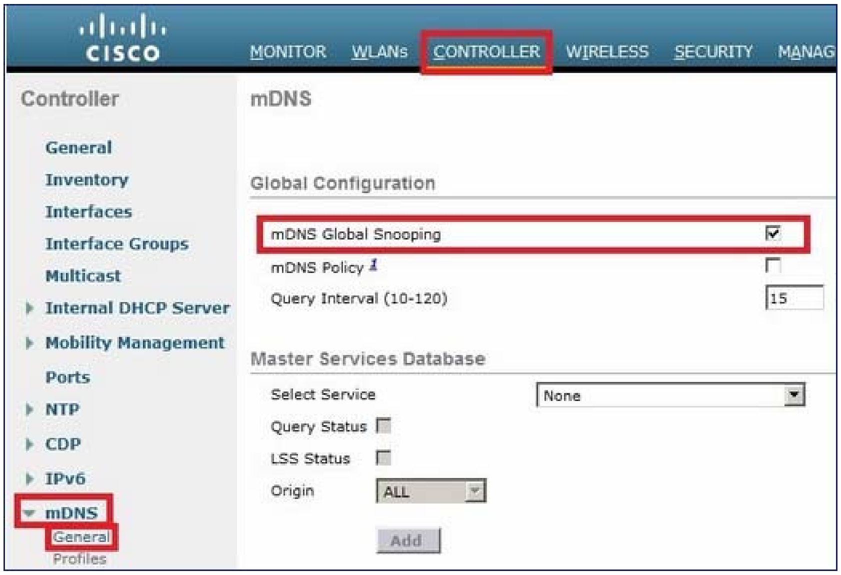
GUI

To enable the settings on the GUI, refer to the following screenshots.



Multicast

Enable Global Multicast Mode	☑
Enable IGMP Snooping	☑
IGMP Timeout (30-7200 seconds)	60
IGMP Query Interval (15-2400 seconds)	20
Enable MLD Snooping	□
MLD Timeout (30-7200 seconds)	60
MLD Query Interval (15-2400 seconds)	20



mDNS

Global Configuration

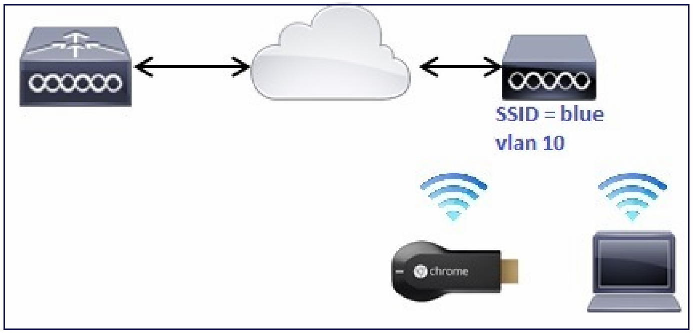
mDNS Global Snooping	☑
mDNS Policy	□
Query Interval (10-120)	15

Master Services Database

Select Service	None
Query Status	□
LSS Status	□
Origin	ALL

Scenario 1: Chromecast and Wireless Clients on the Same WLAN and Same VLAN

Network Diagram



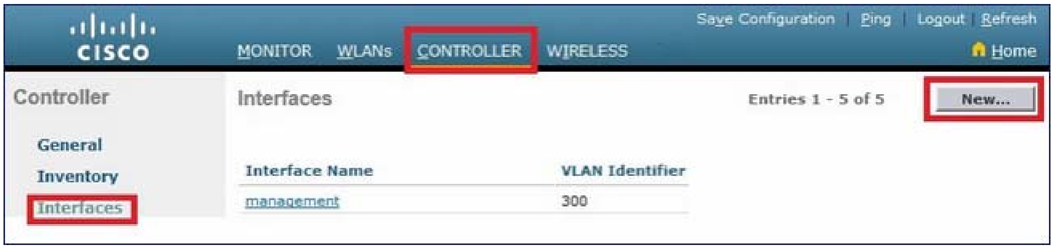
Configurations

1. Create subinterface vlan 10 (This interface has a DHCP server located on the same VLAN)

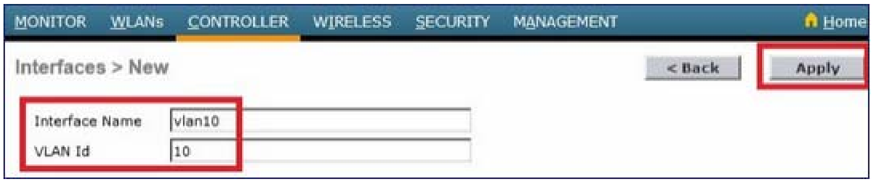
CLI

```
>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

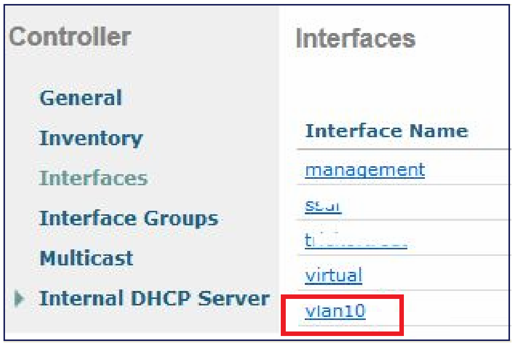


Interface Name	VLAN Identifier
management	300

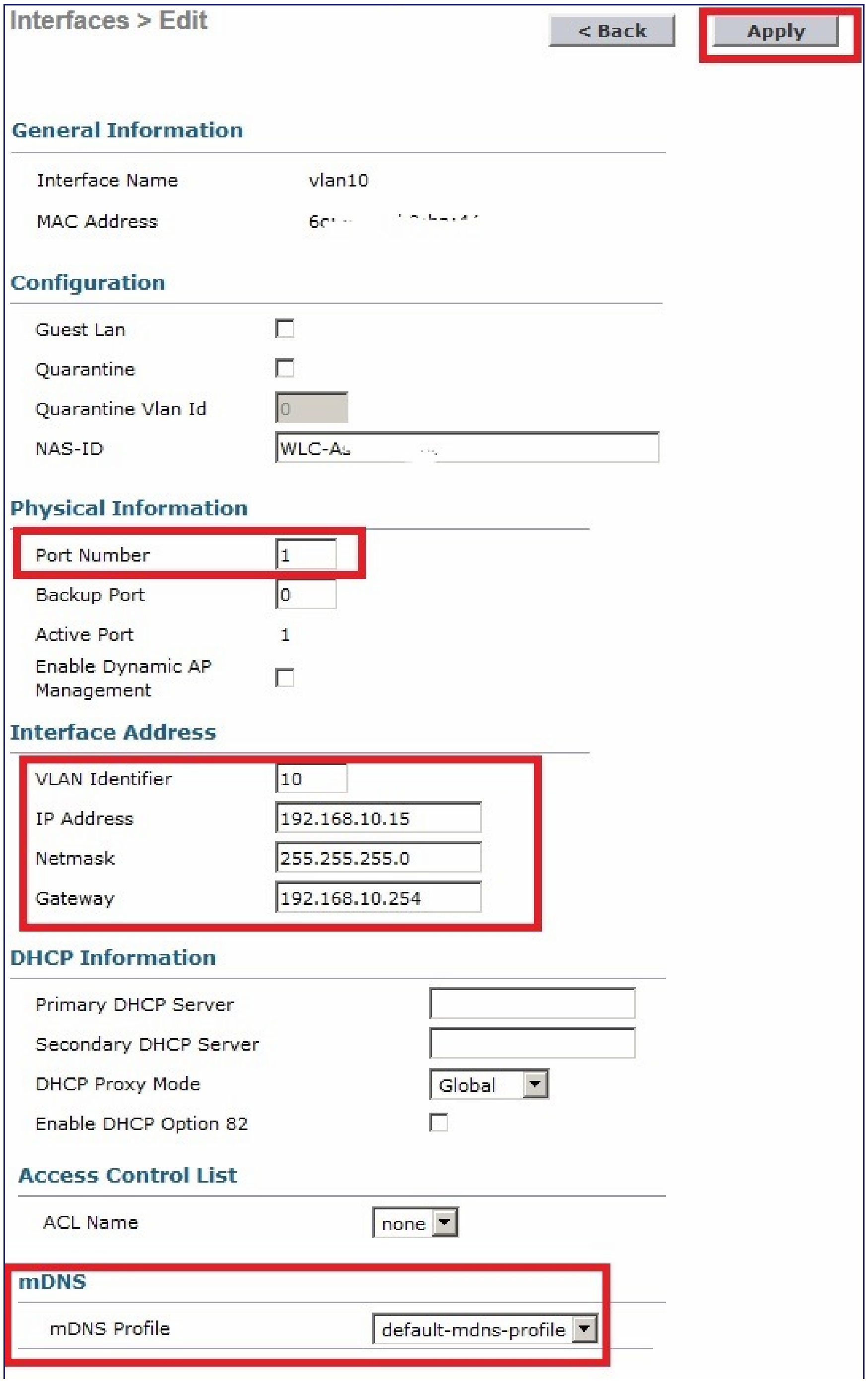


Interface Name: vlan10

VLAN Id: 10



Interface Name
management
[illegible]
[illegible]
virtual
vlan10



Interfaces > Edit

General Information

Interface Name vlan10

MAC Address 6c

Configuration

Guest Lan □

Quarantine □

Quarantine Vlan Id 0

NAS-ID WLC-A

Physical Information

Port Number 1

Backup Port 0

Active Port 1

Enable Dynamic AP Management □

Interface Address

VLAN Identifier 10

IP Address 192.168.10.15

Netmask 255.255.255.0

Gateway 192.168.10.254

DHCP Information

Primary DHCP Server

Secondary DHCP Server

DHCP Proxy Mode Global

Enable DHCP Option 82 □

Access Control List

ACL Name none

mDNS

mDNS Profile default-mdns-profile

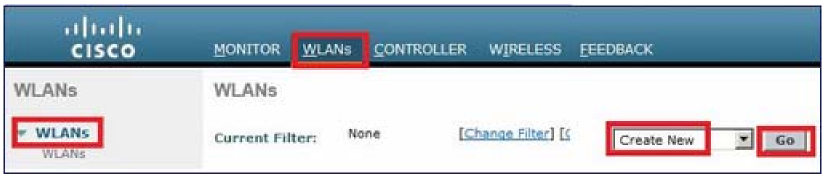
2. Create the WLAN.

- 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

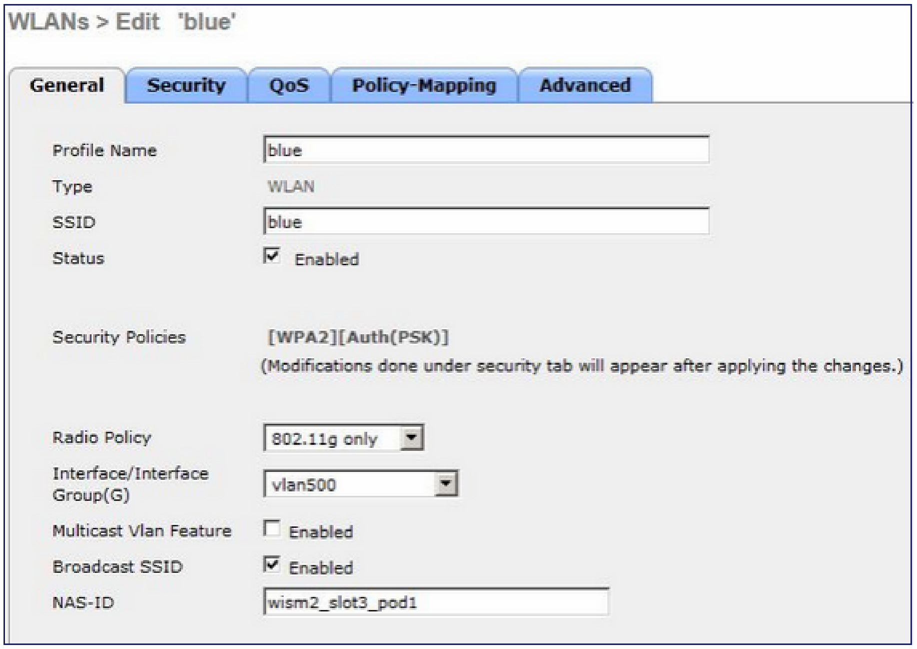
CLI

```
>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

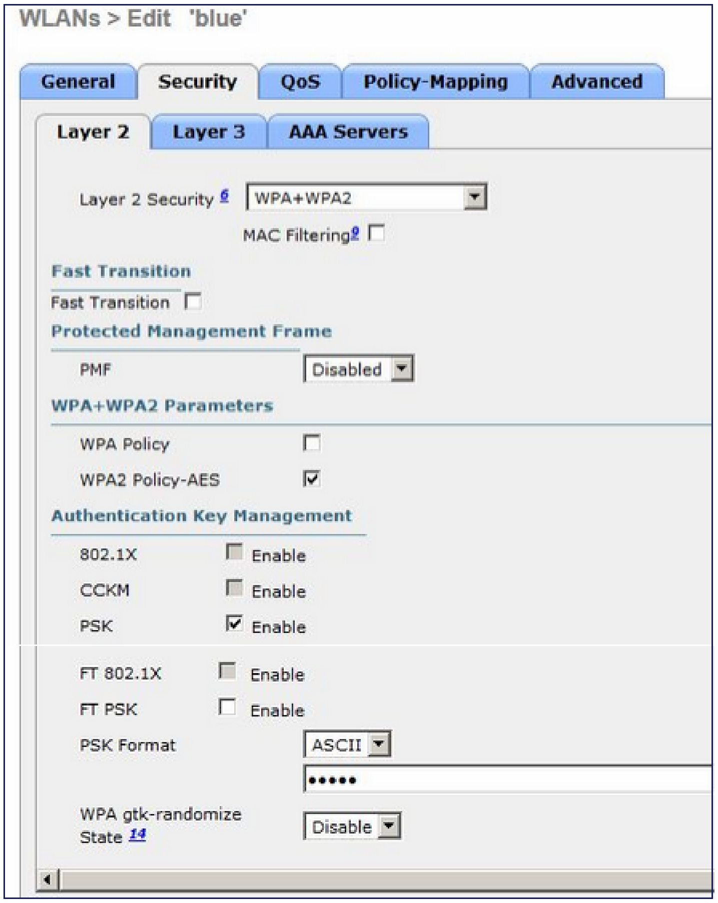


Current Filter: None



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



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

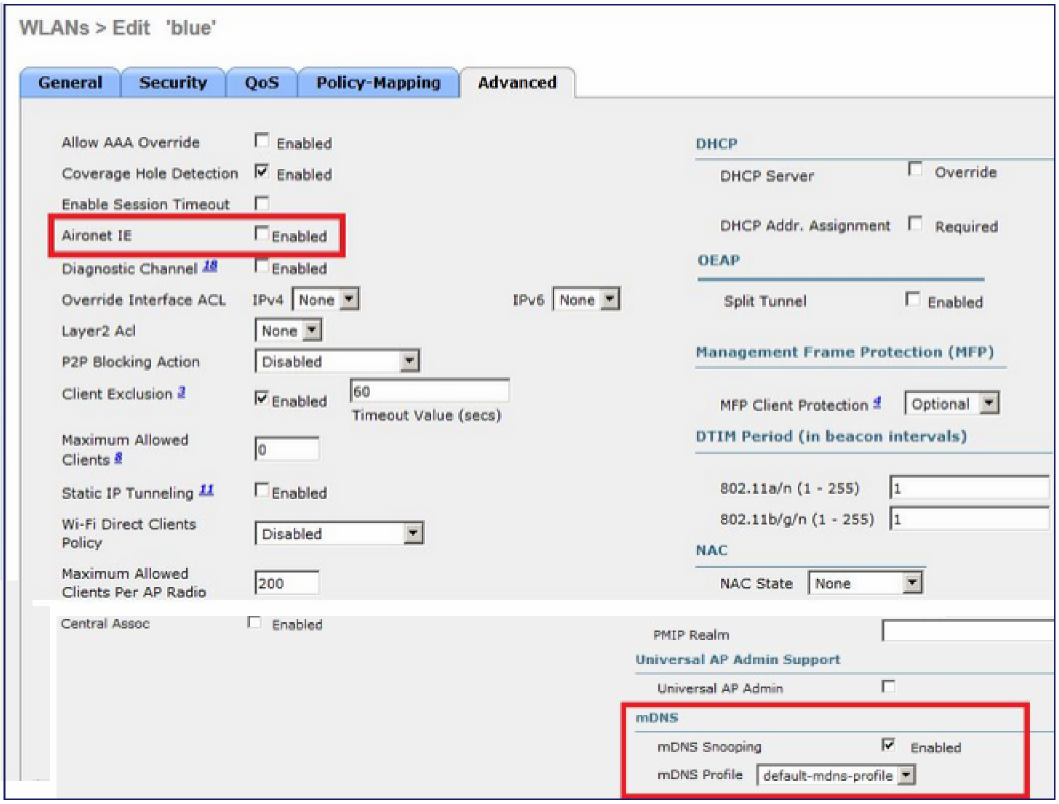
FT 802.1X □ Enable

FT PSK □ Enable

PSK Format ASCII

•••••

WPA gtk-randomize State [14] Disable



WLANs > Edit 'blue'

Allow AAA Override □ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout □
Aironet IE □ Enabled
Diagnostic Channel 18 □ Enabled
Override Interface ACL IPv4 None IPv6 None
Layer2 Acl None
P2P Blocking Action Disabled
Client Exclusion 3 ☑ Enabled 60 Timeout Value (secs)
Maximum Allowed Clients 8 0
Static IP Tunneling 11 □ Enabled
Wi-Fi Direct Clients Policy Disabled
Maximum Allowed Clients Per AP Radio 200
Central Assoc □ Enabled

DHCP
DHCP Server □ Override
DHCP Addr. Assignment □ Required

OEAP
Split Tunnel □ Enabled

Management Frame Protection (MFP)
MFP Client Protection 4 Optional

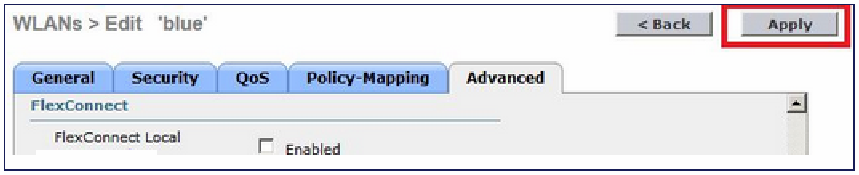
DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
NAC State None

PMIP Realm

Universal AP Admin Support
Universal AP Admin □

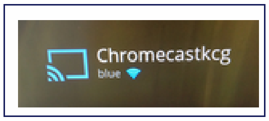
mDNS
mDNS Snooping ☑ Enabled
mDNS Profile default-mdns-profile

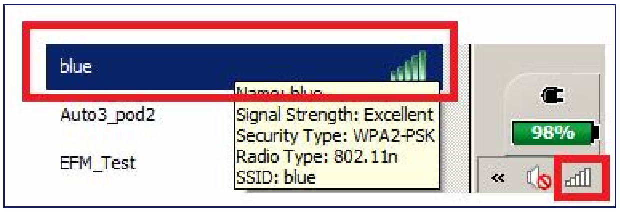


WLANs > Edit 'blue'

FlexConnect
FlexConnect Local □ Enabled

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

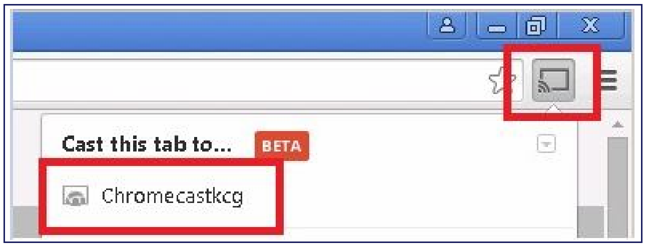




blue
Auto3_pod2
EFM_Test

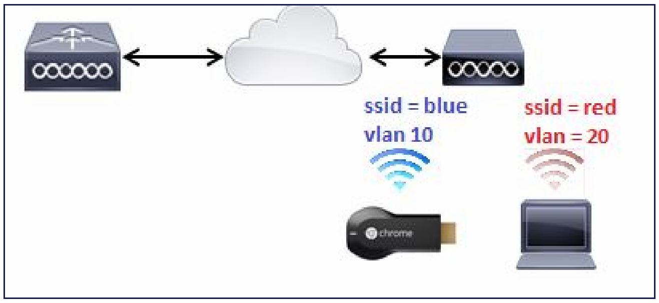
Name: blue
Signal Strength: Excellent
Security Type: WPA2-PSK
Radio Type: 802.11n
SSID: blue

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



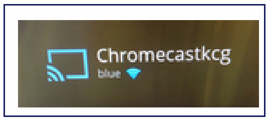
Configurations

1. Add WLAN B for VLAN 20 (See step 1 and 2 from scenario 1 for more reference)

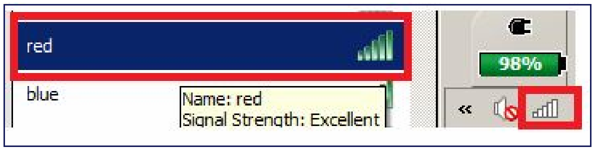
```
>config interface create vlan20 20
>config interface address dynamic-interface vlan10 192.168.20.15 255.255.255.0 192.168.20.254
>config interface port vlan20 1
>config interface mdns-profile vlan20 default-mdns-profile
>config interface dhcp dynamic-interface vlan20 proxy-mode disable

>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
```

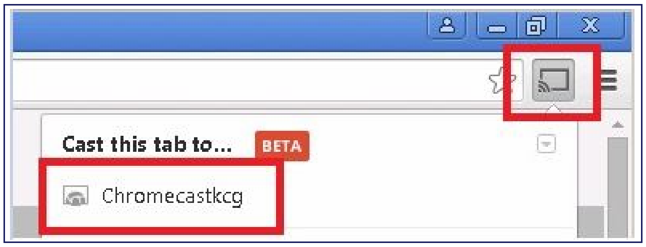
2. Connect Chromecast to SSID blue.



3. Connect the wireless client to SSID red.



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

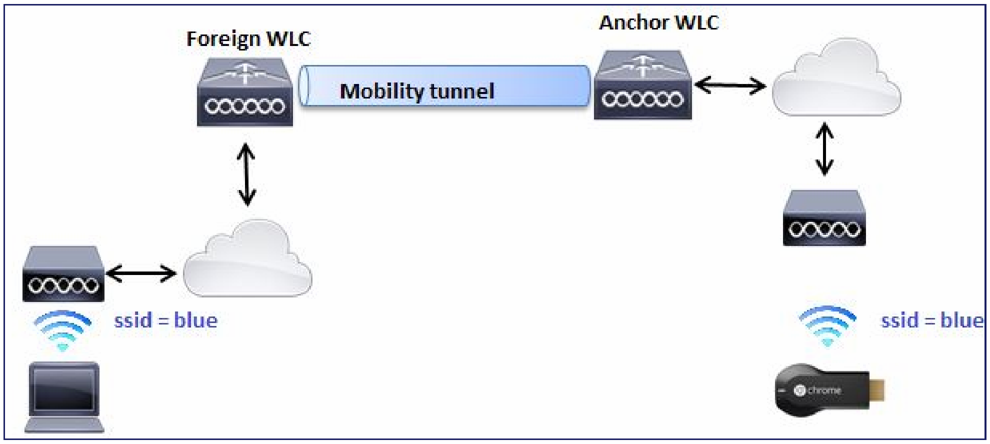


Note The smartphones would not be able to find Chromecast for management for this scenario. This scenario is tested only for screen mirroring.

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
```

```
(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 WLAN to be anchored to anchor WLC:

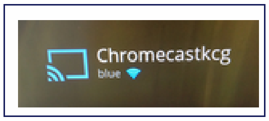
```
(WLC-Anchor) >config wlan disable 1
(WLC-Anchor) >config wlan mobility anchor add 1 10.88.244.87
(WLC-Anchor) >config wlan enable 1


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

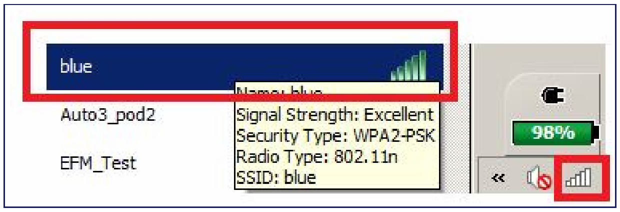
GUI:

Refer to http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80/b_cg80_chapter_010001101.html#ID270

4. Connect Chromecast to SSID blue on anchor WLC.

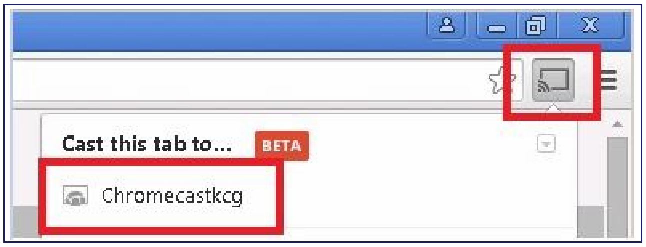


5. Connect the laptop to SSID blue on foreign WLC.



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

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 smarphones 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.

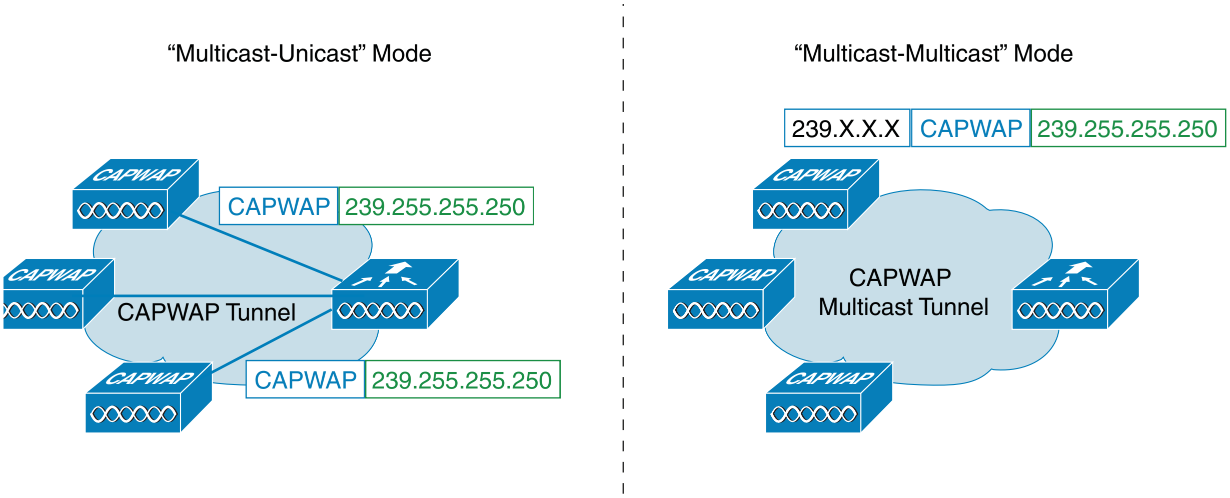
Enabling Multicast Support

From the **Controller** tab, choose the **Multicast** link on the left-hand menu. Enable G**lobal 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:

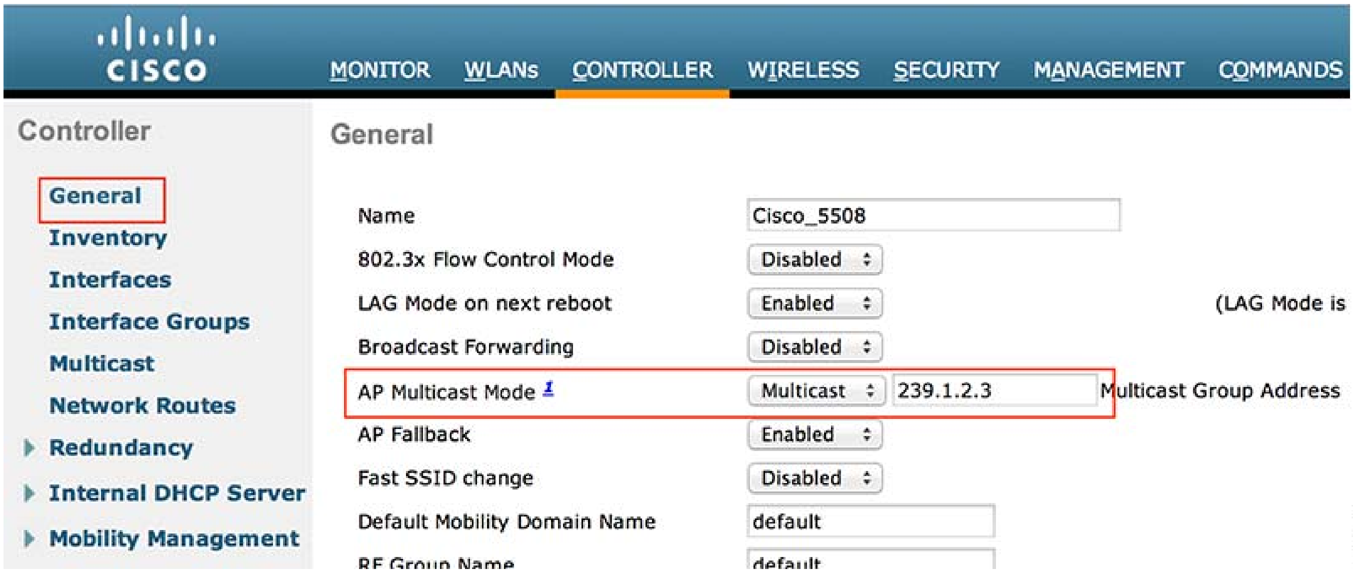


Multicast-Multicast Distribution Mode

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.



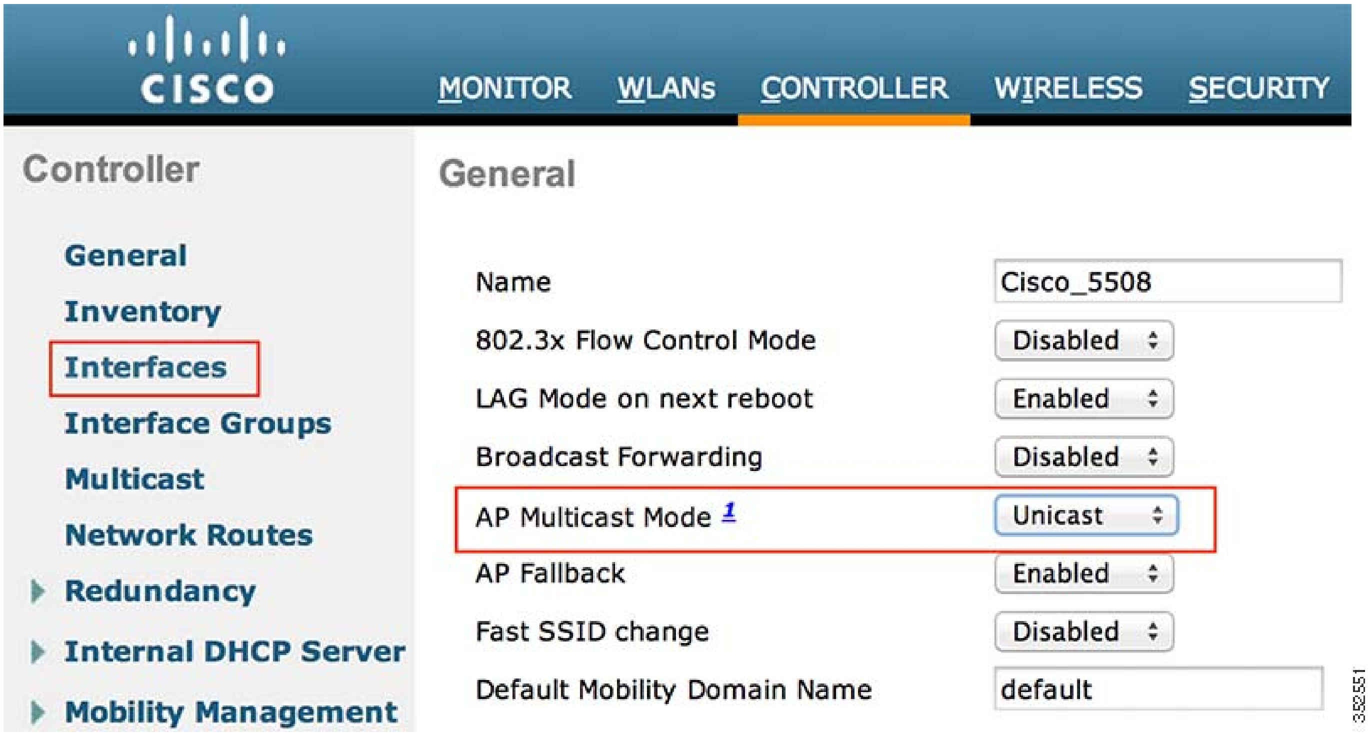
General

Name	Cisco_5508	
802.3x Flow Control Mode	Disabled	
LAG Mode on next reboot	Enabled	(LAG Mode is
Broadcast Forwarding	Disabled	
AP Multicast Mode 1	Multicast 239.1.2.3	Multicast Group Address
AP Fallback	Enabled	
Fast SSID change	Disabled	
Default Mobility Domain Name	default	
RF Group Name	default	

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.

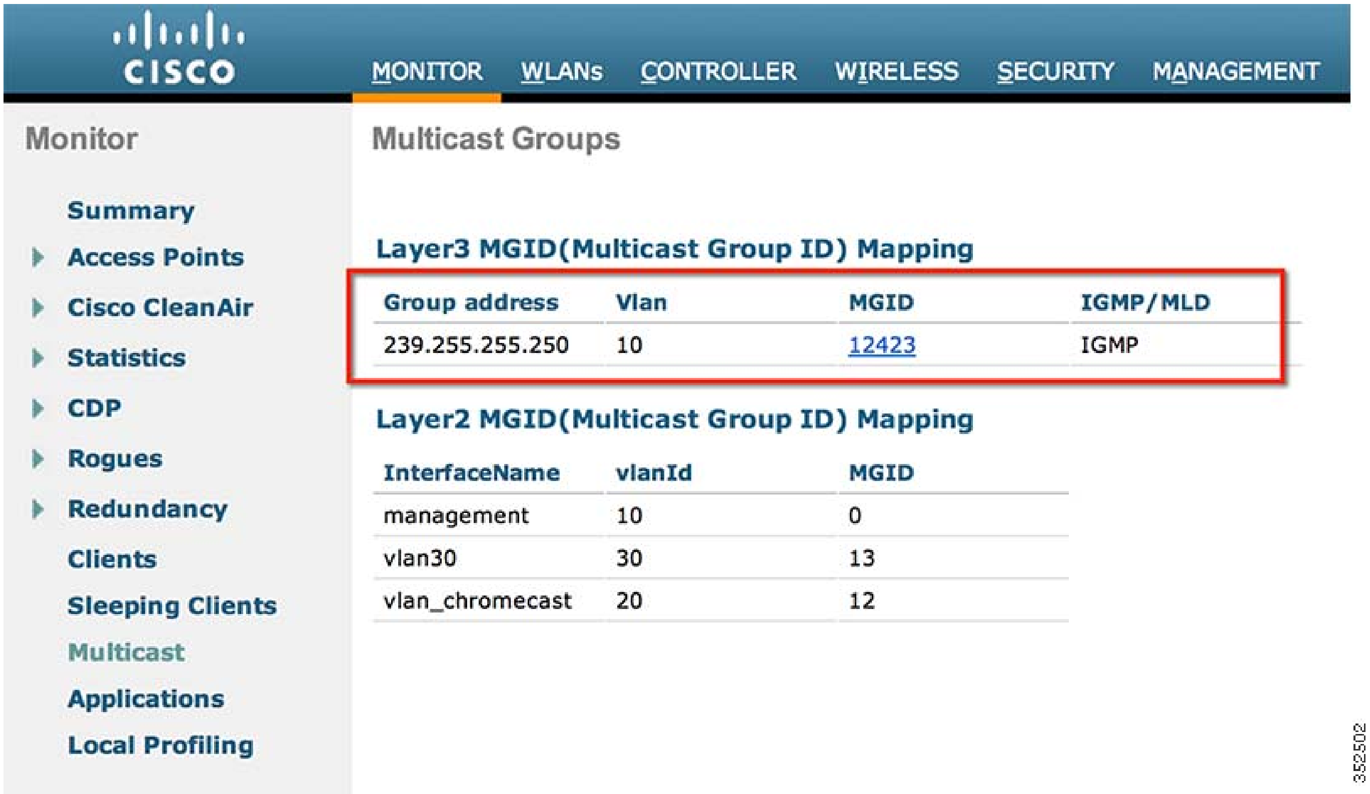


General

Name	Cisco_5508
802.3x Flow Control Mode	Disabled
LAG Mode on next reboot	Enabled
Broadcast Forwarding	Disabled
AP Multicast Mode [1]	Unicast
AP Fallback	Enabled
Fast SSID change	Disabled
Default Mobility Domain Name	default

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.



Multicast Groups

Layer3 MGID(Multicast Group ID) Mapping

Group address	Vlan	MGID	IGMP/MLD
239.255.255.250	10	12423	IGMP

Layer2 MGID(Multicast Group ID) Mapping

InterfaceName	vlanId	MGID
management	10	0
vlan30	30	13
vlan_chromecast	20	12

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 Chromecst guide.

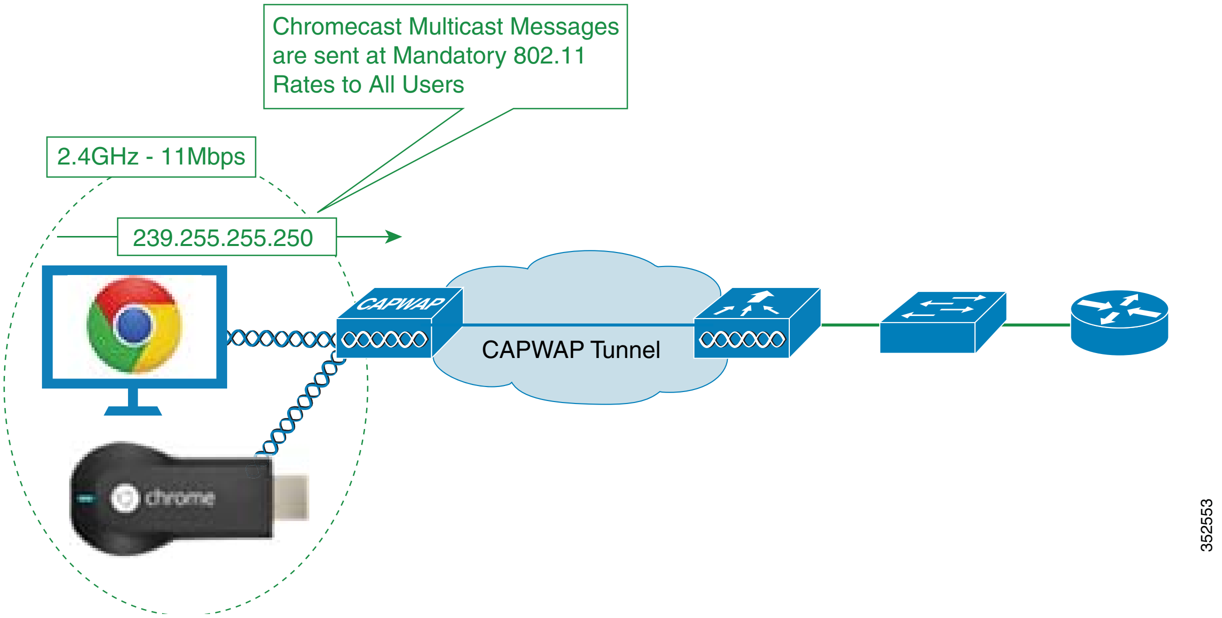
Conditions

WLC or NGWC implementing Chromecast and its Screencast function.

Workaround

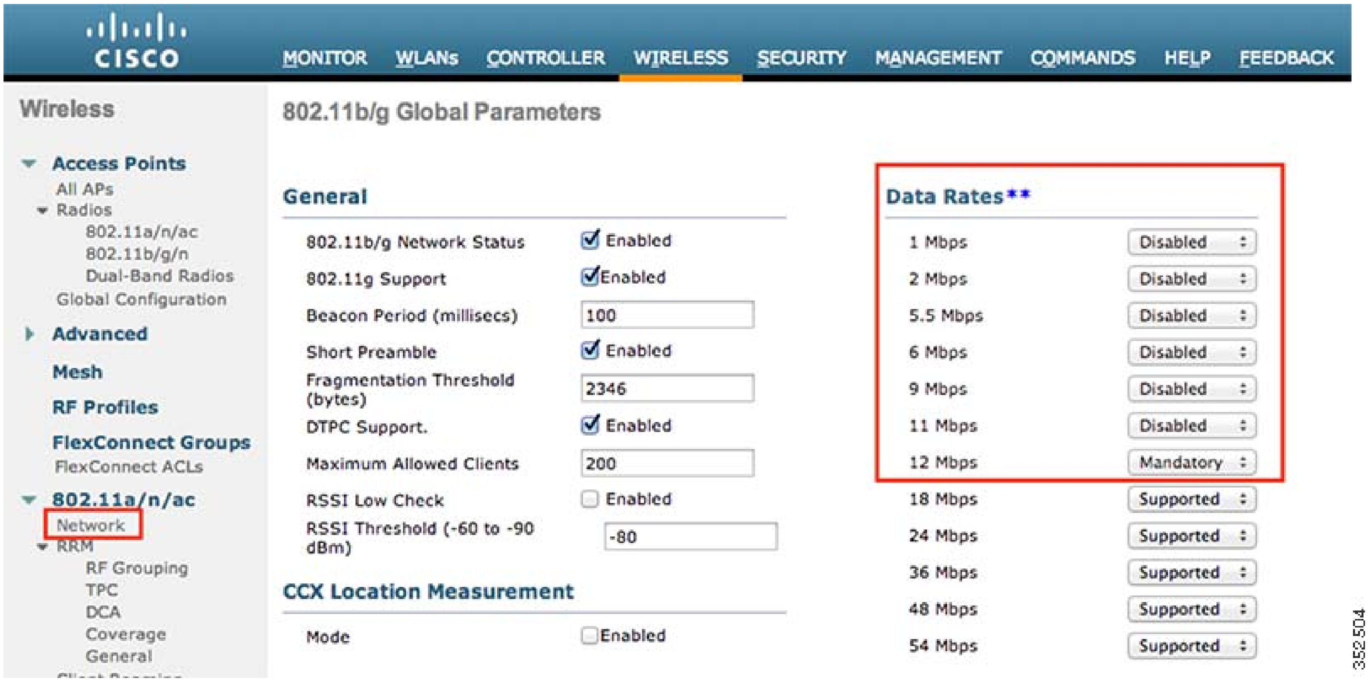
Configure mDNS filter.

Tune Multicast Data Rates


Chromecast Multicast Messages are sent at Mandatory 802.11 Rates to All Users
2.4GHz - 11Mbps
239.255.255.250
CAPWAP
CAPWAP Tunnel
chrome
352553

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.



802.11b/g Global Parameters

General

802.11b/g Network Status	☑ Enabled
802.11g Support	☑ Enabled
Beacon Period (millisecs)	100
Short Preamble	☑ Enabled
Fragmentation Threshold (bytes)	2346
DTPC Support.	☑ Enabled
Maximum Allowed Clients	200
RSSI Low Check	□ Enabled
RSSI Threshold (-60 to -90 dBm)	-80

CCX Location Measurement

Mode	□ Enabled

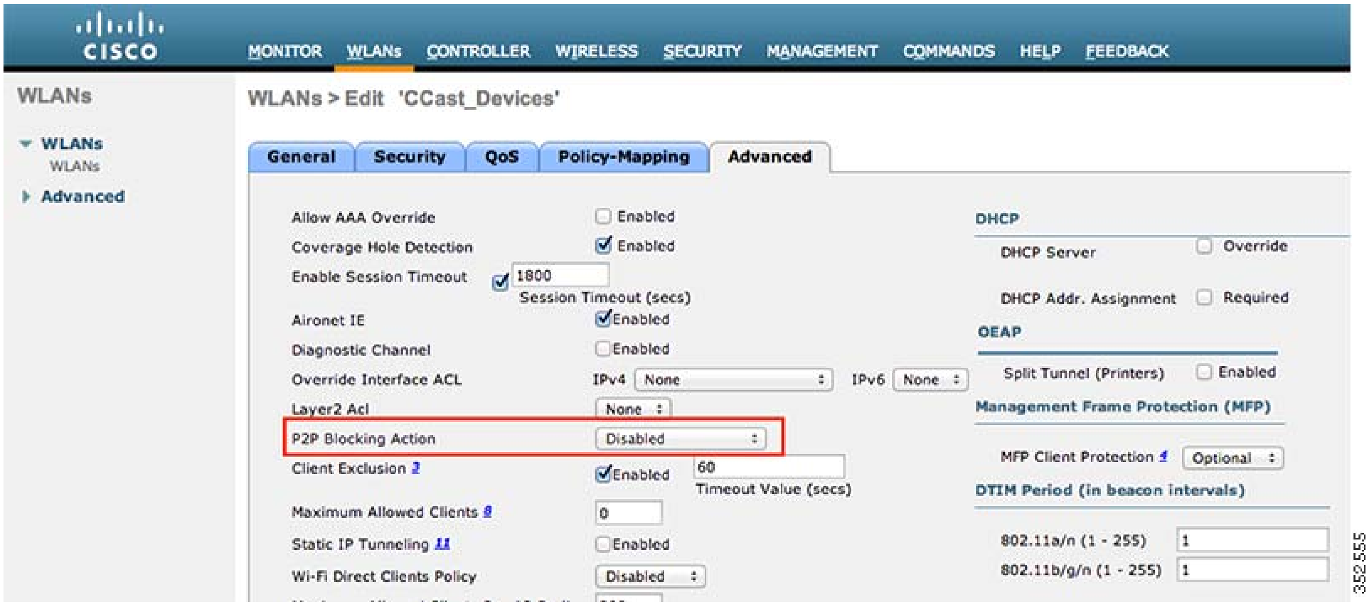
Data Rates**

1 Mbps	Disabled
2 Mbps	Disabled
5.5 Mbps	Disabled
6 Mbps	Disabled
9 Mbps	Disabled
11 Mbps	Disabled
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Supported
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

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.**



WLANs > Edit 'CCast_Devices'

Allow AAA Override □ Enabled

Coverage Hole Detection ☑ Enabled

Enable Session Timeout ☑ 1800 Session Timeout (secs)

Aironet IE ☑ Enabled

Diagnostic Channel □ Enabled

Override Interface ACL IPv4 None IPv6 None

Layer2 Acl None

P2P Blocking Action Disabled

Client Exclusion 3 ☑ Enabled 60 Timeout Value (secs)

Maximum Allowed Clients 8 0

Static IP Tunneling 11 □ Enabled

Wi-Fi Direct Clients Policy Disabled

DHCP

DHCP Server □ Override

DHCP Addr. Assignment □ Required

OEAP

Split Tunnel (Printers) □ Enabled

Management Frame Protection (MFP)

MFP Client Protection 4 Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

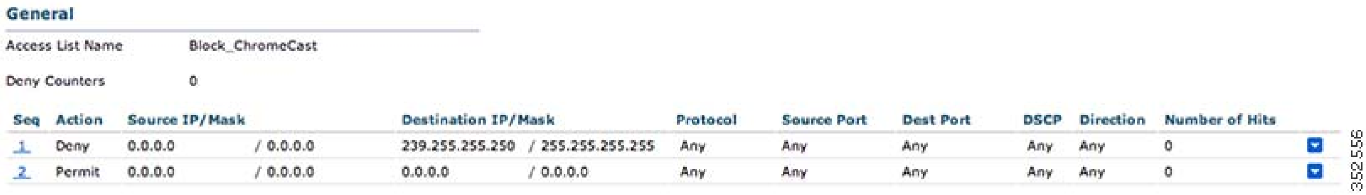
802.11b/g/n (1 - 255) 1

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.



General

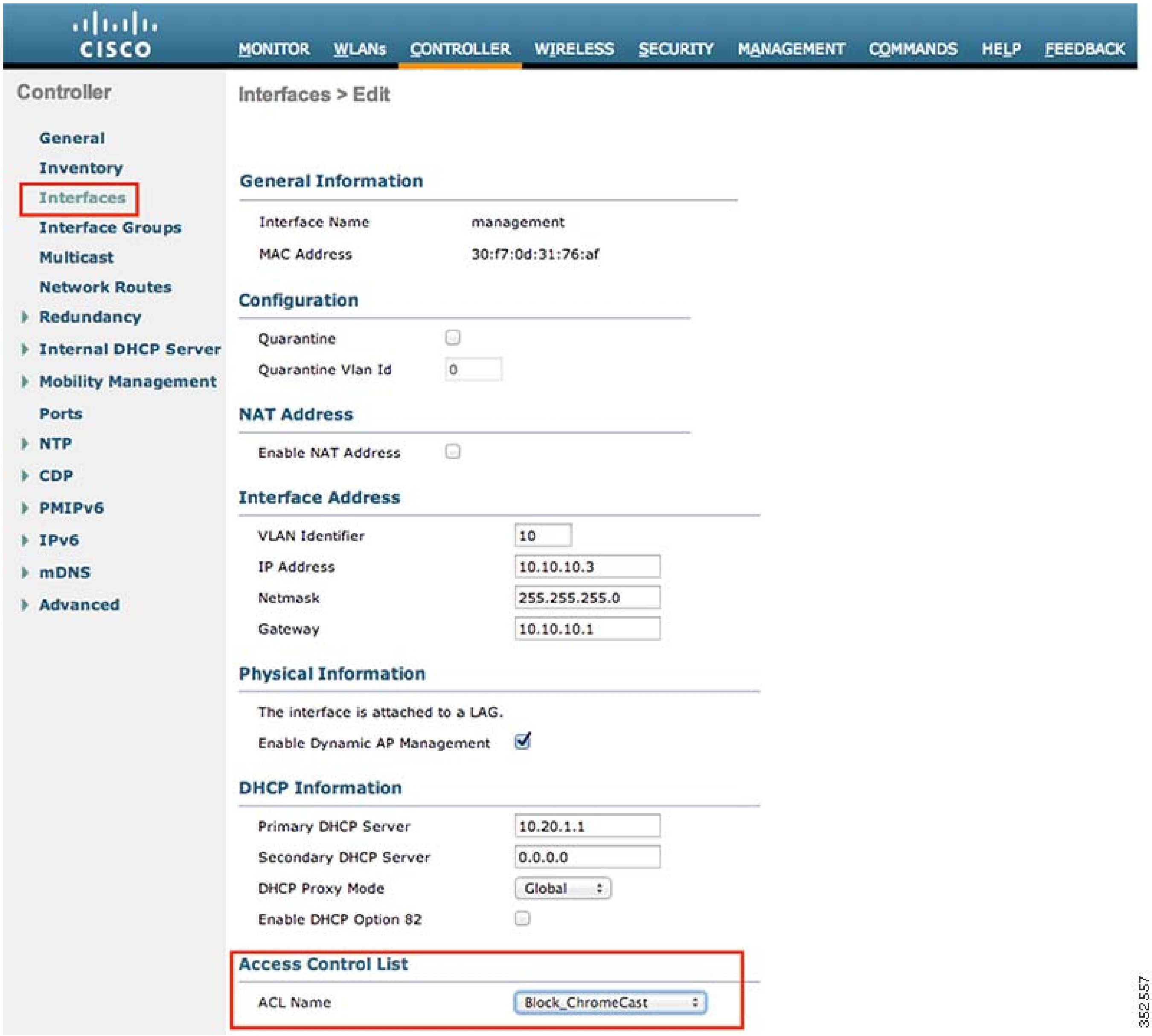
Access List Name Block_ChromeCast

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Deny	0.0.0.0 / 0.0.0.0	239.255.255.250 / 255.255.255.255	Any	Any	Any	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

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.



Interfaces > Edit

General Information

Interface Name management
MAC Address 30:f7:0d:31:76:af

Configuration

Quarantine □
Quarantine Vlan Id 0

NAT Address

Enable NAT Address □

Interface Address

VLAN Identifier 10
IP Address 10.10.10.3
Netmask 255.255.255.0
Gateway 10.10.10.1

Physical Information

The interface is attached to a LAG.
Enable Dynamic AP Management ☑

DHCP Information

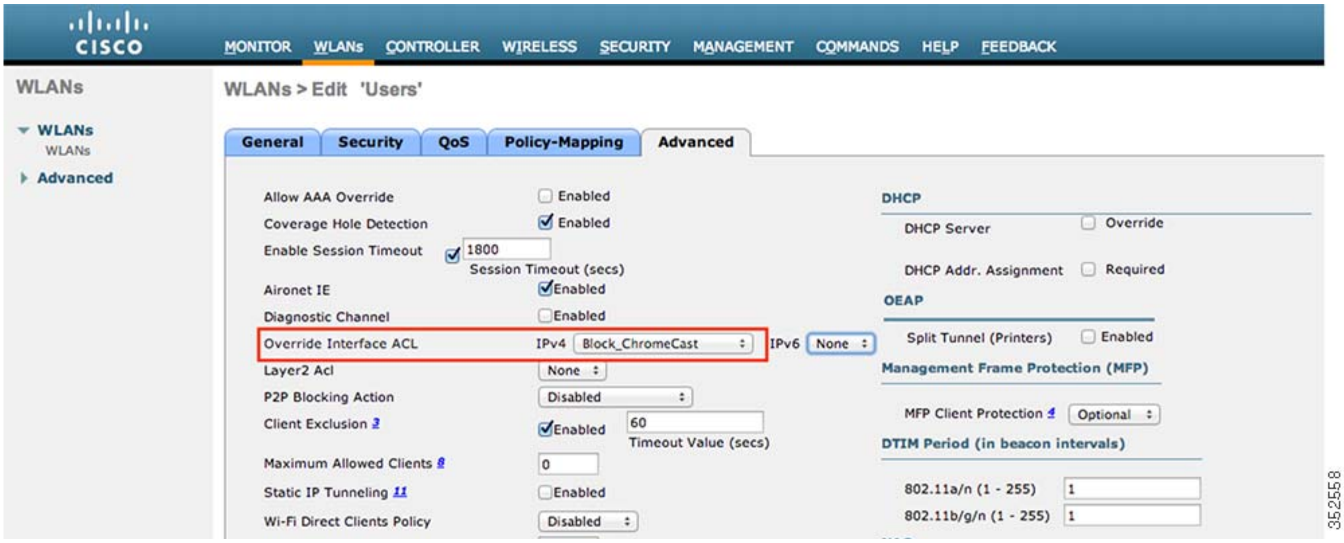
Primary DHCP Server 10.20.1.1
Secondary DHCP Server 0.0.0.0
DHCP Proxy Mode Global
Enable DHCP Option 82 □

Access Control List

ACL Name Block_ChromeCast

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.


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
General Security QoS Policy-Mapping Advanced
352558

WLANs > Edit 'Users'

Allow AAA Override	□ Enabled
Coverage Hole Detection	☑ Enabled
Enable Session Timeout	☑ 1800 Session Timeout (secs)
Aironet IE	☑Enabled
Diagnostic Channel	□Enabled
Override Interface ACL	IPv4 Block_ChromeCast IPv6 None
Layer2 Acl	None
P2P Blocking Action	Disabled
Client Exclusion 3	☑Enabled 60 Timeout Value (secs)
Maximum Allowed Clients 8	0
Static IP Tunneling 11	□Enabled
Wi-Fi Direct Clients Policy	Disabled

DHCP

DHCP Server	□ Override
DHCP Addr. Assignment	□ Required

OEAP

Split Tunnel (Printers)	□ Enabled

Management Frame Protection (MFP)

MFP Client Protection 4	Optional

DTIM Period (in beacon intervals)

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

Chromecast Application

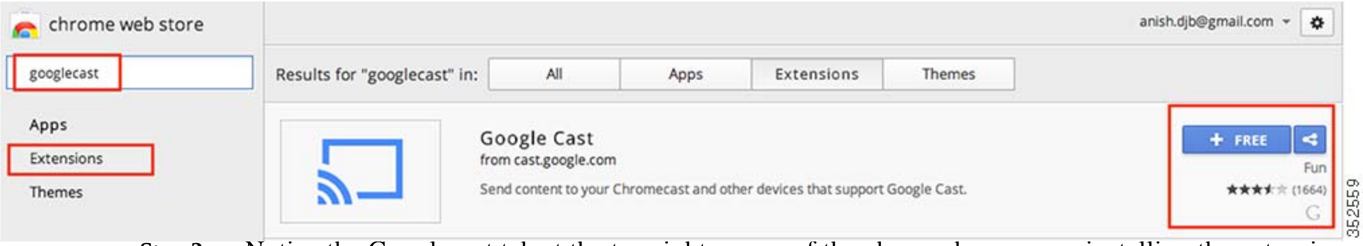
Clients with Chromecast extension installed on their Chrome browser can display the entire browser and screen by using a Chromecast device. Once the client discovers the Chromecast device using SSDP, the subsequent connections between the wireless client and Chromecast device to mirror the display use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

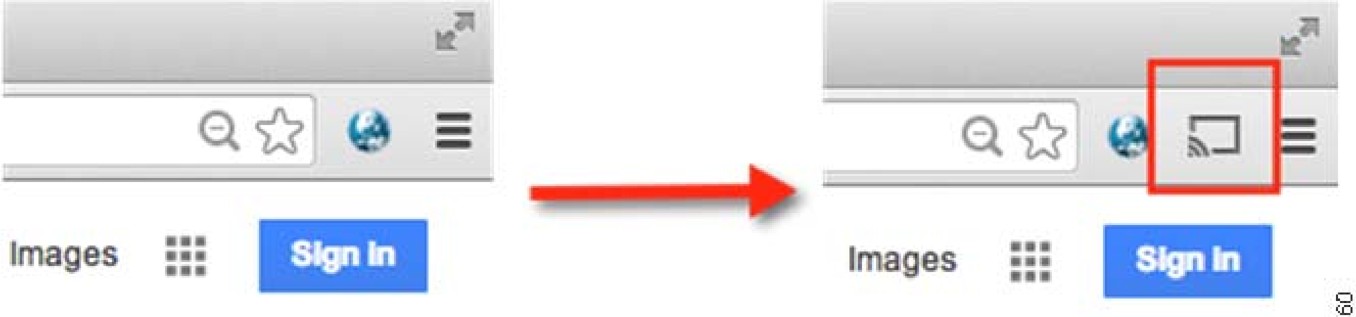
Step 2 Install the GoogleCast Extension:

For more information on installing chrome extension visit: https://support.google.com/chrome/answer/167997?hl=en



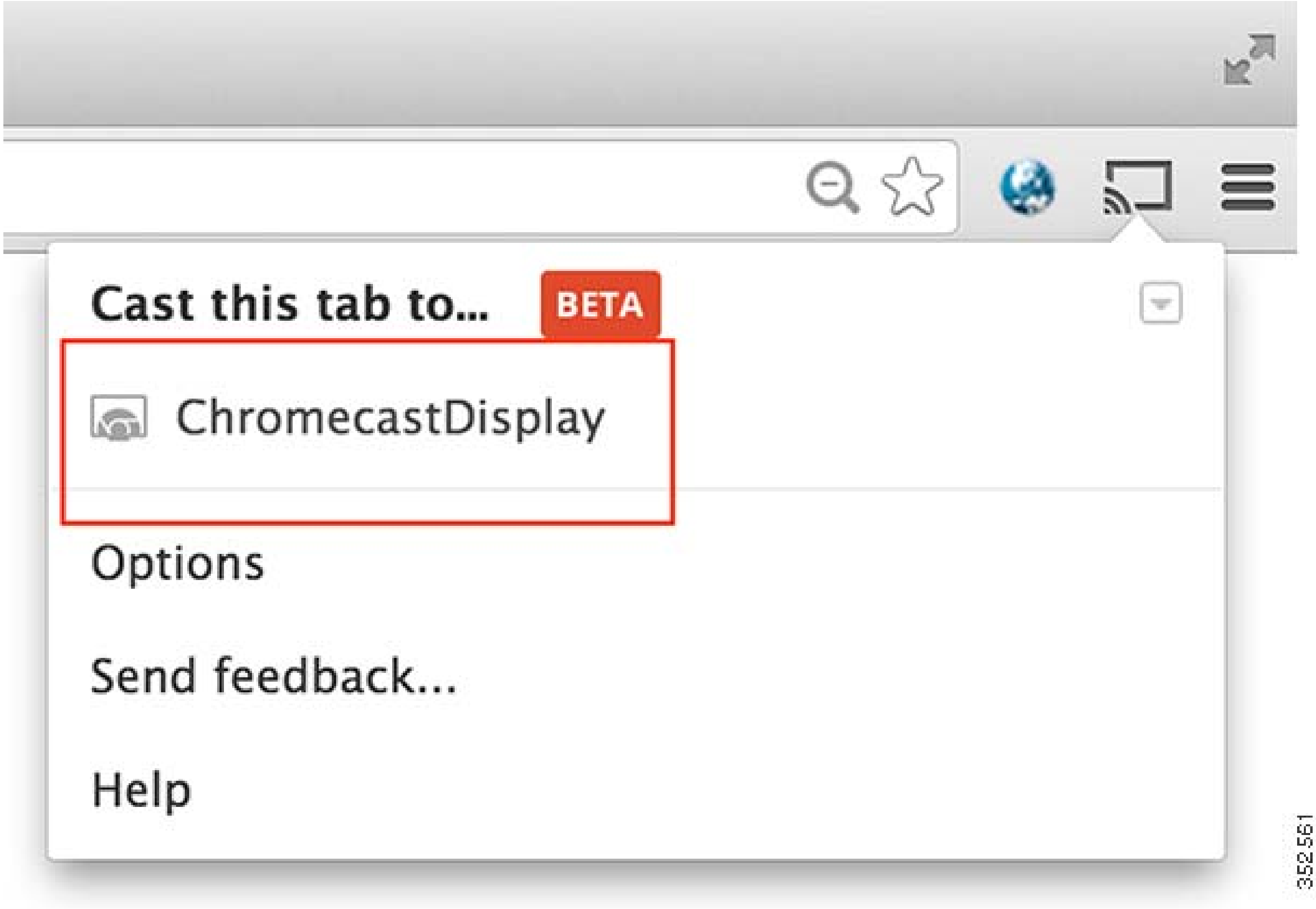
Google Cast
from cast.google.com
Send content to your Chromecast and other devices that support Google Cast.

Step 3 Notice the Googlecast tab at the top right corner of the chrome browser on installing the extension:



352560

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.



352561

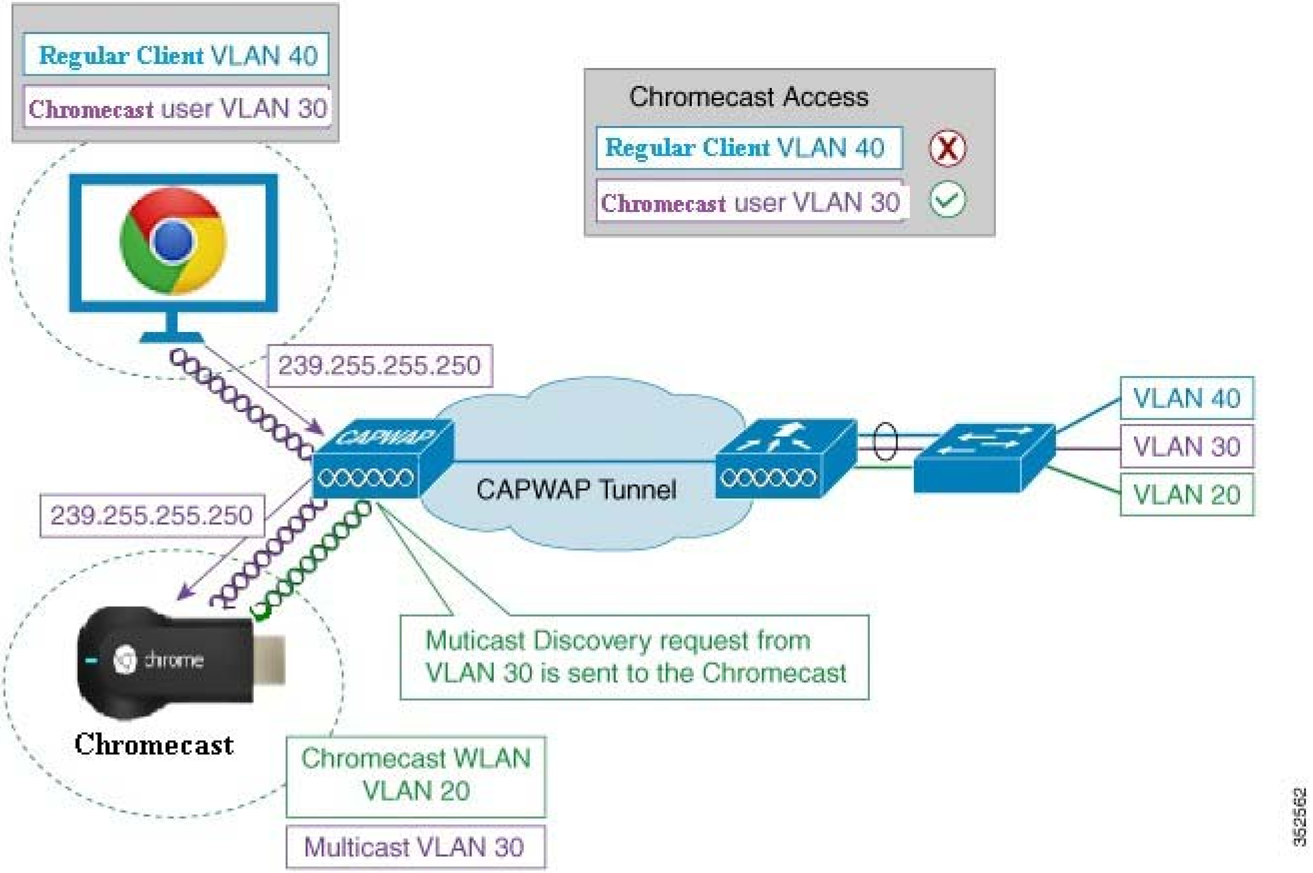
Chromecast using VLAN Select and AAA Override

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.

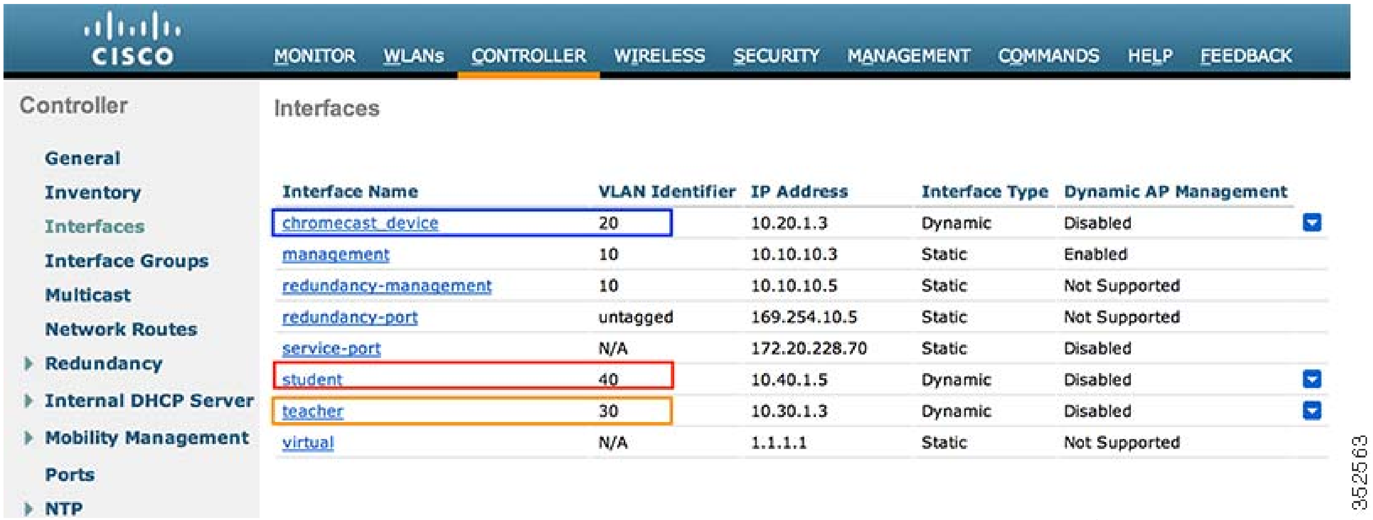
Using VLAN Select with the multicast VLAN feature allows a separate subnet to be used for Chromecast devices, while still enabling Chromecast for use by a specific set of clients on a different VLAN. The specific set of clients can be assigned to a VLAN using AAA override.

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:

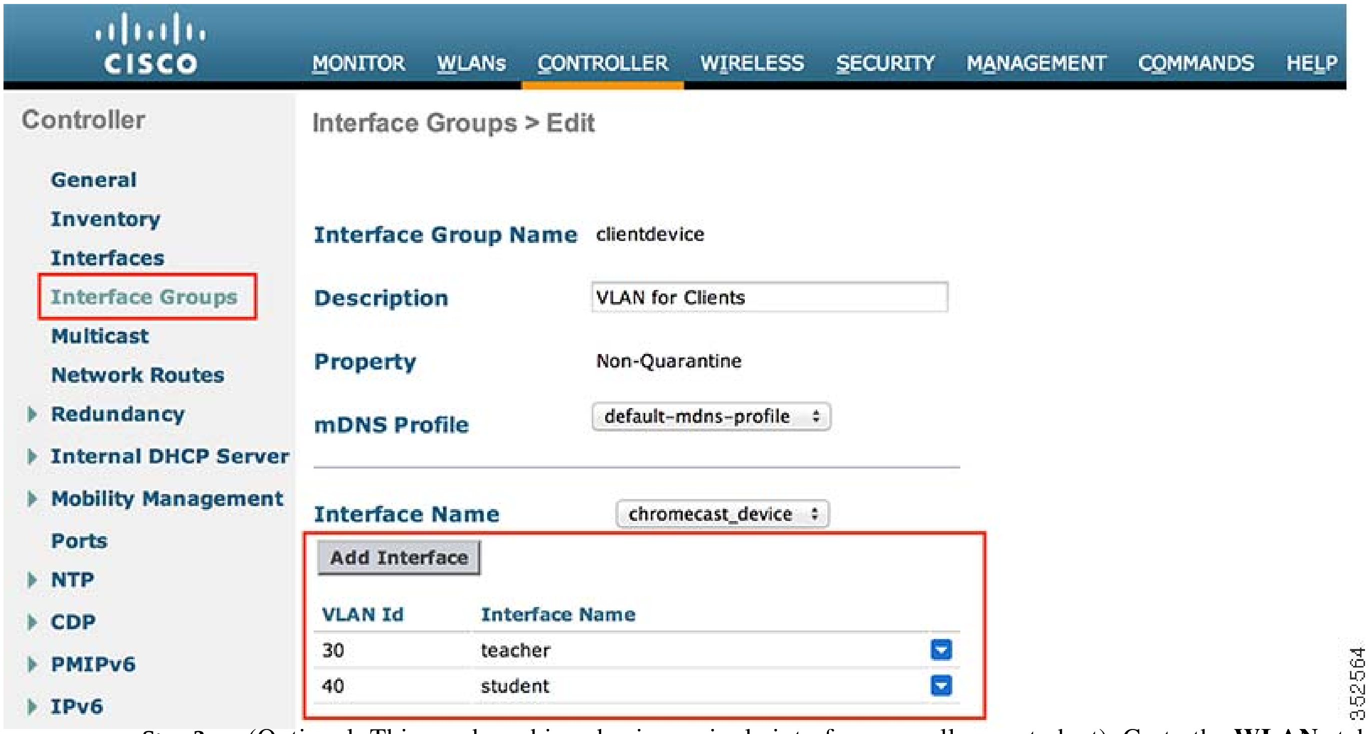
Step 1 Go to the **Controller** tab > **Interfaces** on the left-hand menu. Create the necessary interfaces for the client VLANs (student and teacher in this example) and also an interface for the Chromecast subnet (chromecast_device in this example).



Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
chromecast_device	20	10.20.1.3	Dynamic	Disabled
management	10	10.10.10.3	Static	Enabled
redundancy-management	10	10.10.10.5	Static	Not Supported
redundancy-port	untagged	169.254.10.5	Static	Not Supported
service-port	N/A	172.20.228.70	Static	Disabled
student	40	10.40.1.5	Dynamic	Disabled
teacher	30	10.30.1.3	Dynamic	Disabled
virtual	N/A	1.1.1.1	Static	Not Supported

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).



Interface Groups > Edit

Interface Group Name clientdevice

Description VLAN for Clients

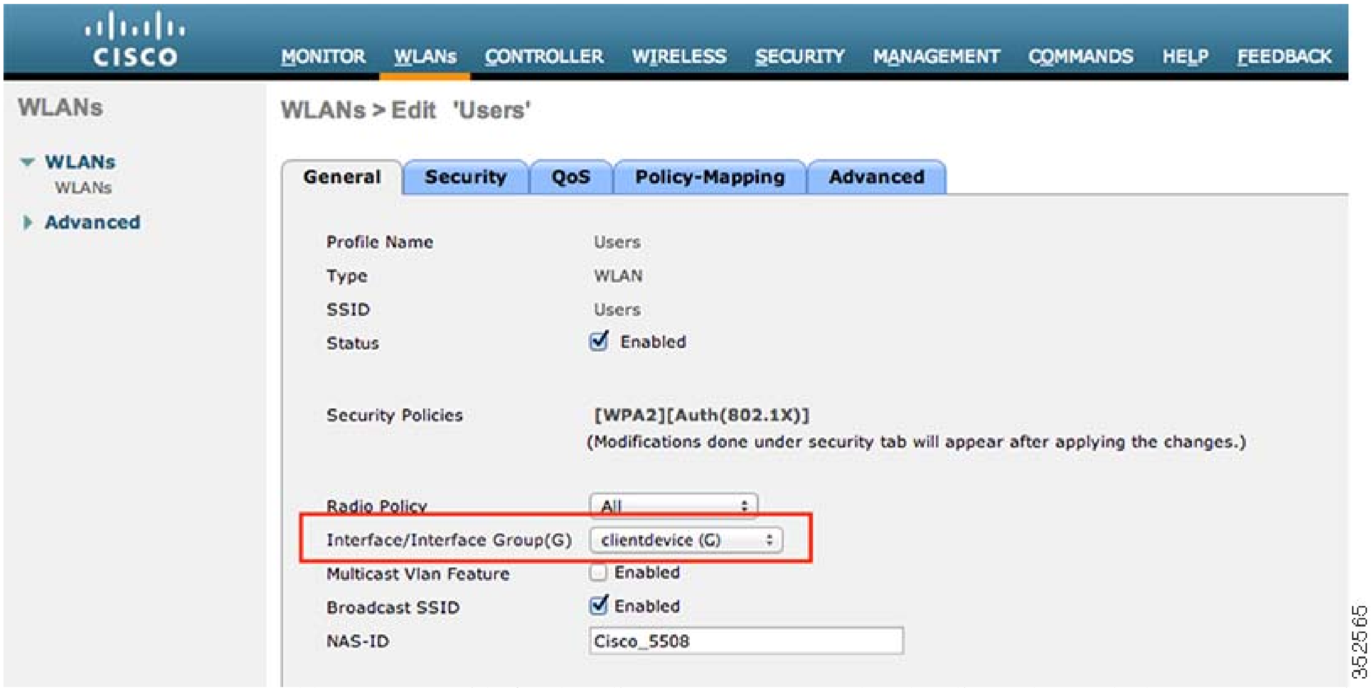
Property Non-Quarantine

mDNS Profile default-mdns-profile

Interface Name chromecast_device

VLAN Id	Interface Name
30	teacher
40	student

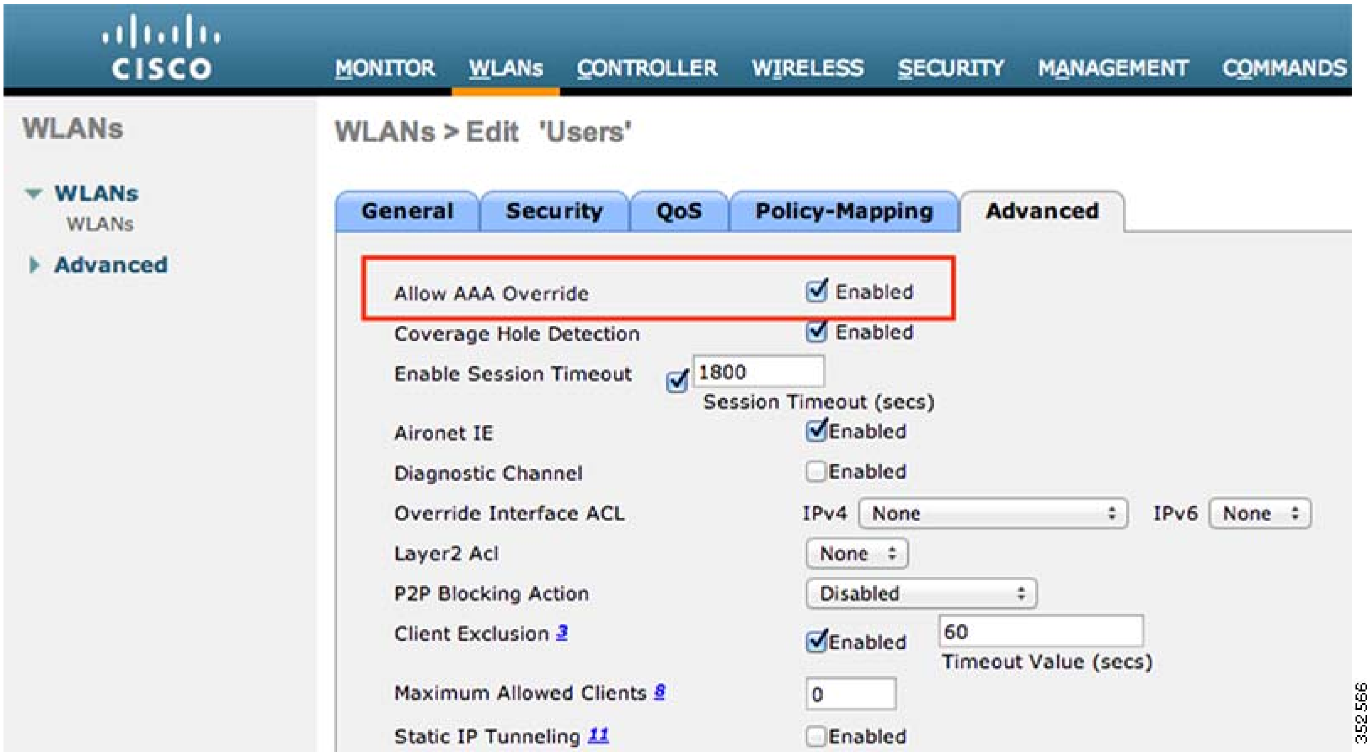
Step 3 (Optional: This can be achieved using a single interface as well, e.g. student). Go to the **WLANs** tab, and create the client SSID. Select the interface group created in Step 2.



WLANs > Edit 'Users'

Profile Name	Users
Type	WLAN
SSID	Users
Status	☑ Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	clientdevice (G)
Multicast Vlan Feature	□ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	Cisco_5508

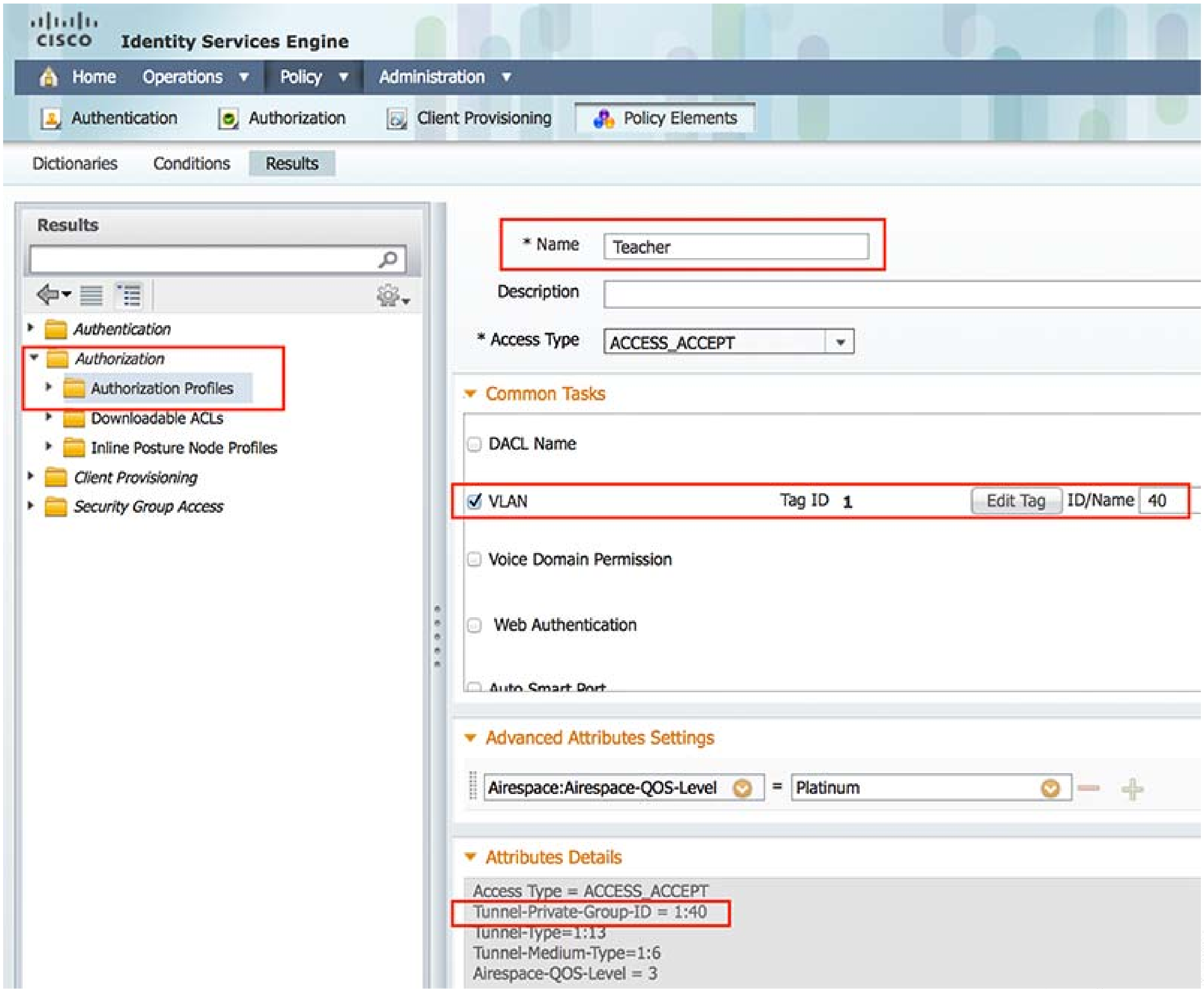
Step 4 Enable AAA Override for the Client SSID, to ensure that the client who need Chromecast access is assigned to the Teacher VLAN.



WLANs > Edit 'Users'

Allow AAA Override	☑ Enabled
Coverage Hole Detection	☑ Enabled
Enable Session Timeout	☑ 1800 Session Timeout (secs)
Aironet IE	☑Enabled
Diagnostic Channel	□Enabled
Override Interface ACL	IPv4 None IPv6 None
Layer2 Acl	None
P2P Blocking Action	Disabled
Client Exclusion 3	☑Enabled 60 Timeout Value (secs)
Maximum Allowed Clients 8	0
Static IP Tunneling 11	□Enabled

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)



* Name: Teacher

Description:

* Access Type: ACCESS_ACCEPT

Common Tasks

□ DACL Name

☑ VLAN Tag ID 1 ID/Name 40

□ Voice Domain Permission

□ Web Authentication

□ Auto Smart Port

Advanced Attributes Settings

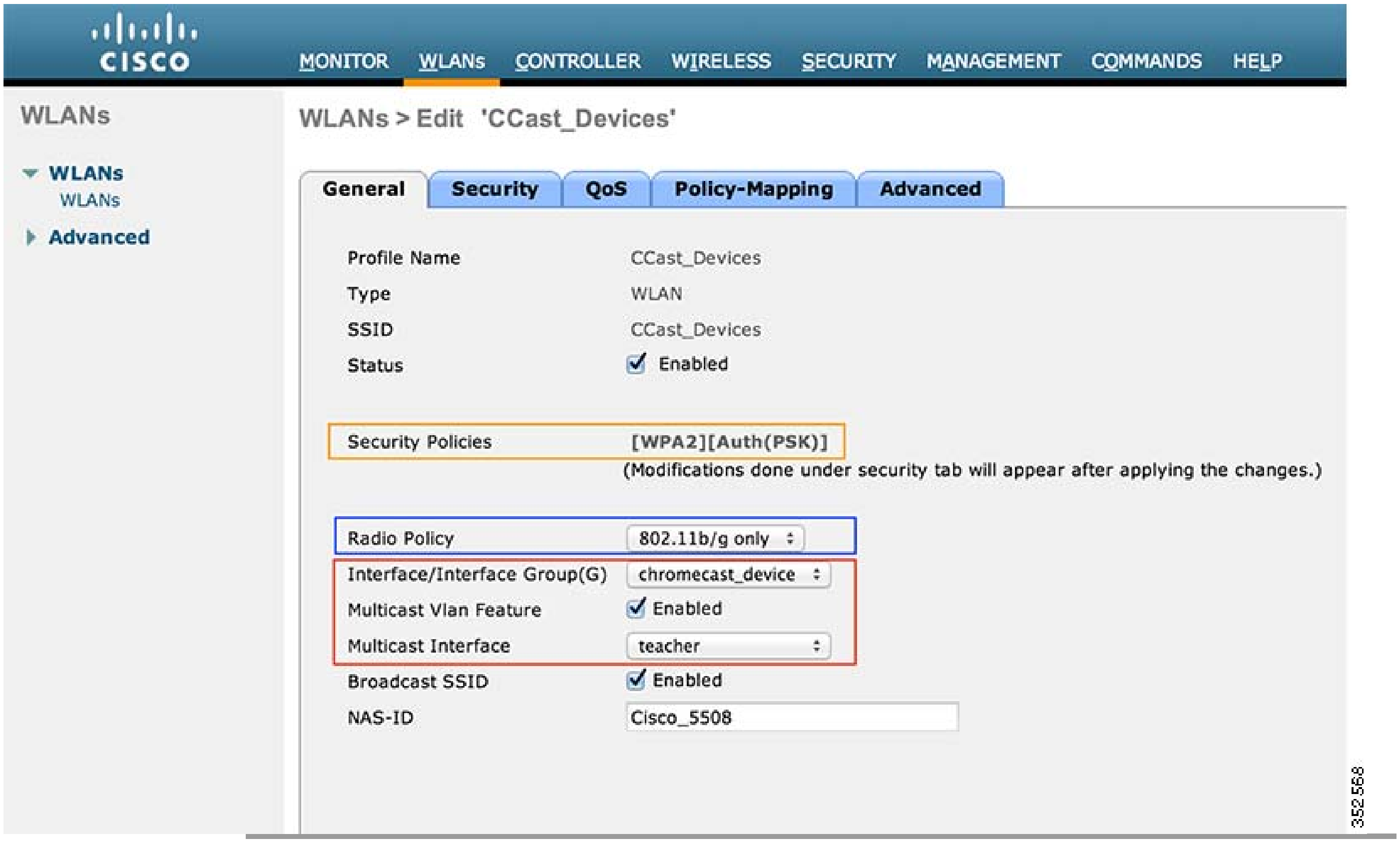
Airespace:Airespace-QOS-Level = Platinum

Attributes Details

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:40
Tunnel-Type=1:13
Tunnel-Medium-Type=1:6
Airespace-QOS-Level = 3

352567

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.



WLANs > Edit 'CCast_Devices'

Profile Name CCast_Devices
Type WLAN
SSID CCast_Devices
Status ☑ Enabled

Security Policies [WPA2][Auth(PSK)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy 802.11b/g only
Interface/Interface Group(G) chromecast_device
Multicast Vlan Feature ☑ Enabled
Multicast Interface teacher
Broadcast SSID ☑ Enabled
NAS-ID Cisco_5508

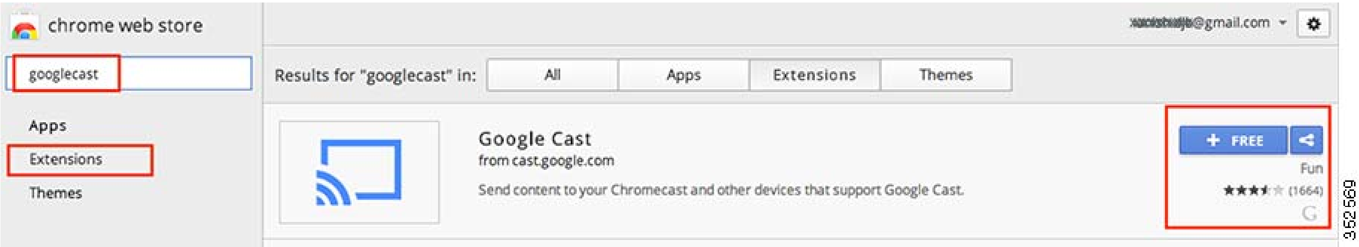
Verifying VLAN Select and AAA Override with Chromecast

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



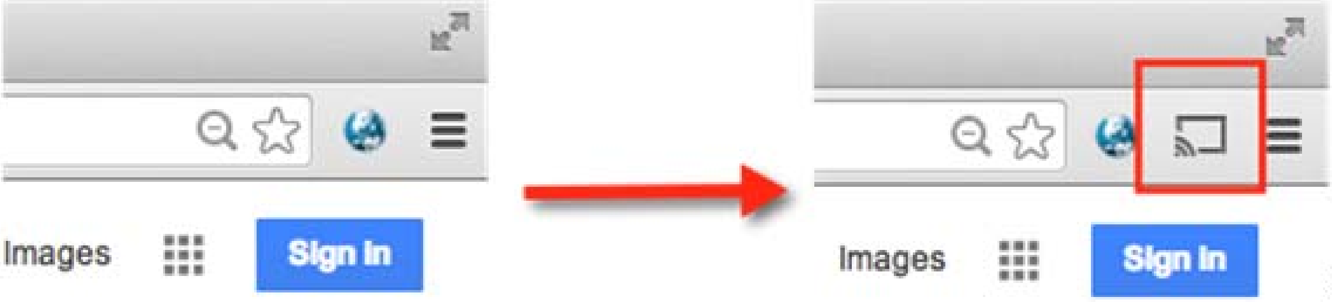
[redacted]@gmail.com

googlecast

Results for "googlecast" in:

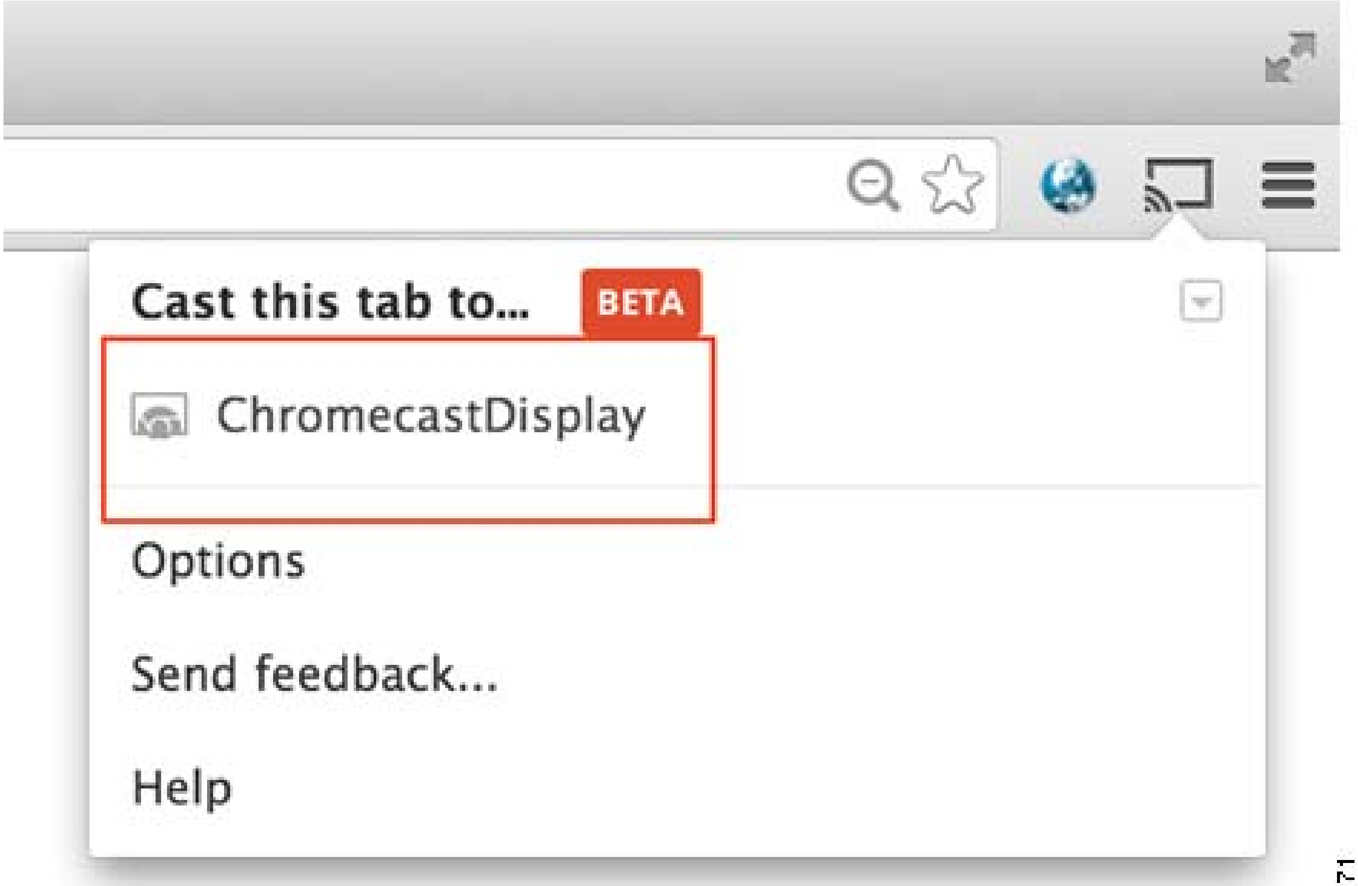
Google Cast
from cast.google.com
Send content to your Chromecast and other devices that support Google Cast.

Step 3 Notice the Googlecast tab at the top right corner of the chrome browser on installing the extension:



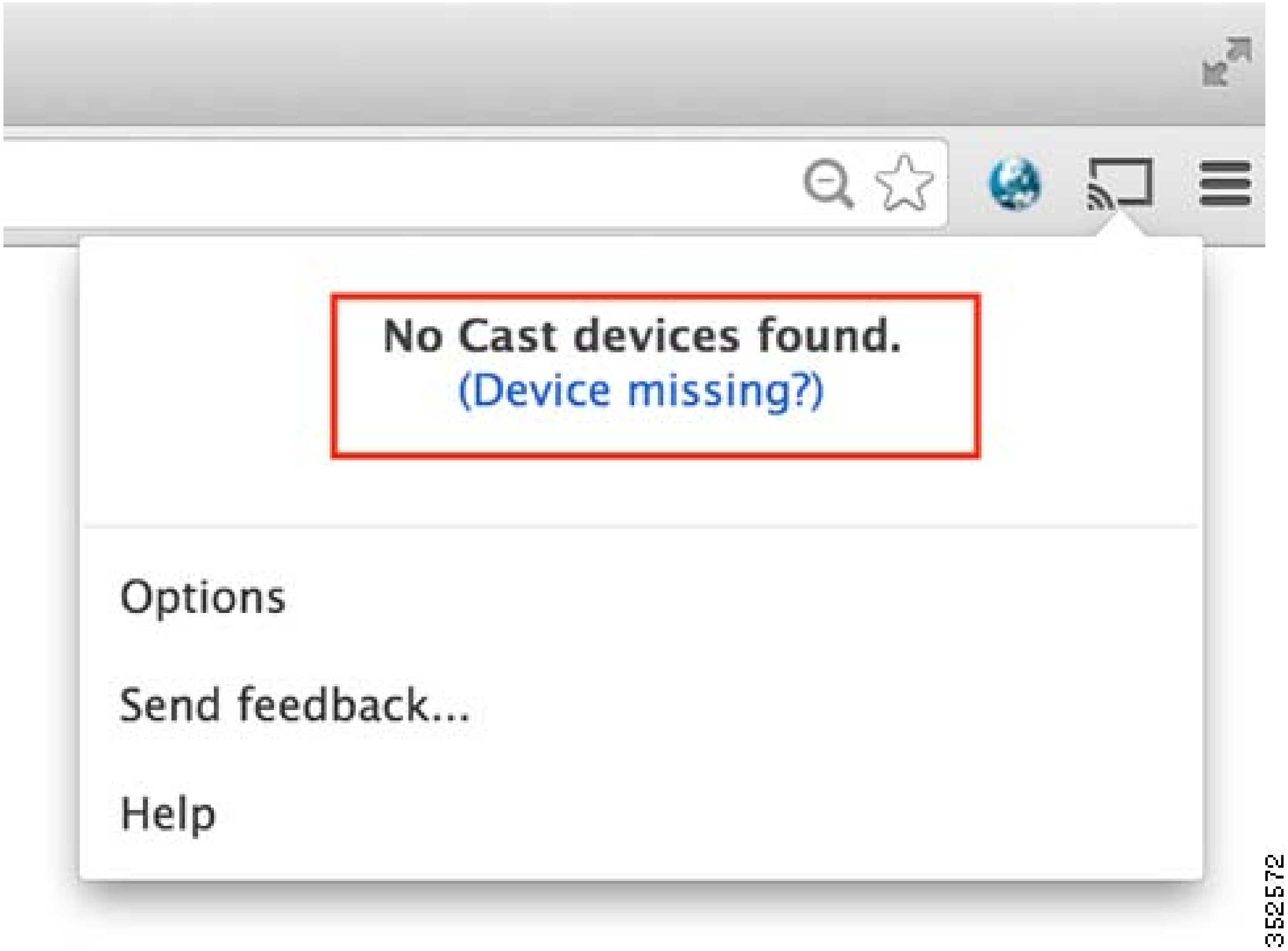
352570

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.



352571

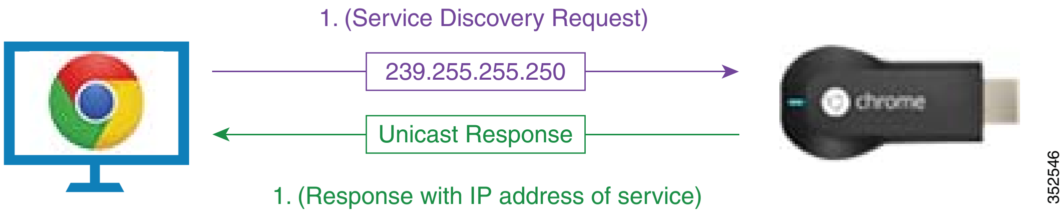
Step 5 Make sure that the Computer is connected to the client wireless network and gets an IP address from the Student VLAN. Click the Googlecast tab on the student user computer, and the Chromecast device should not be discovered.



No Cast devices found.
(Device missing?)

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.



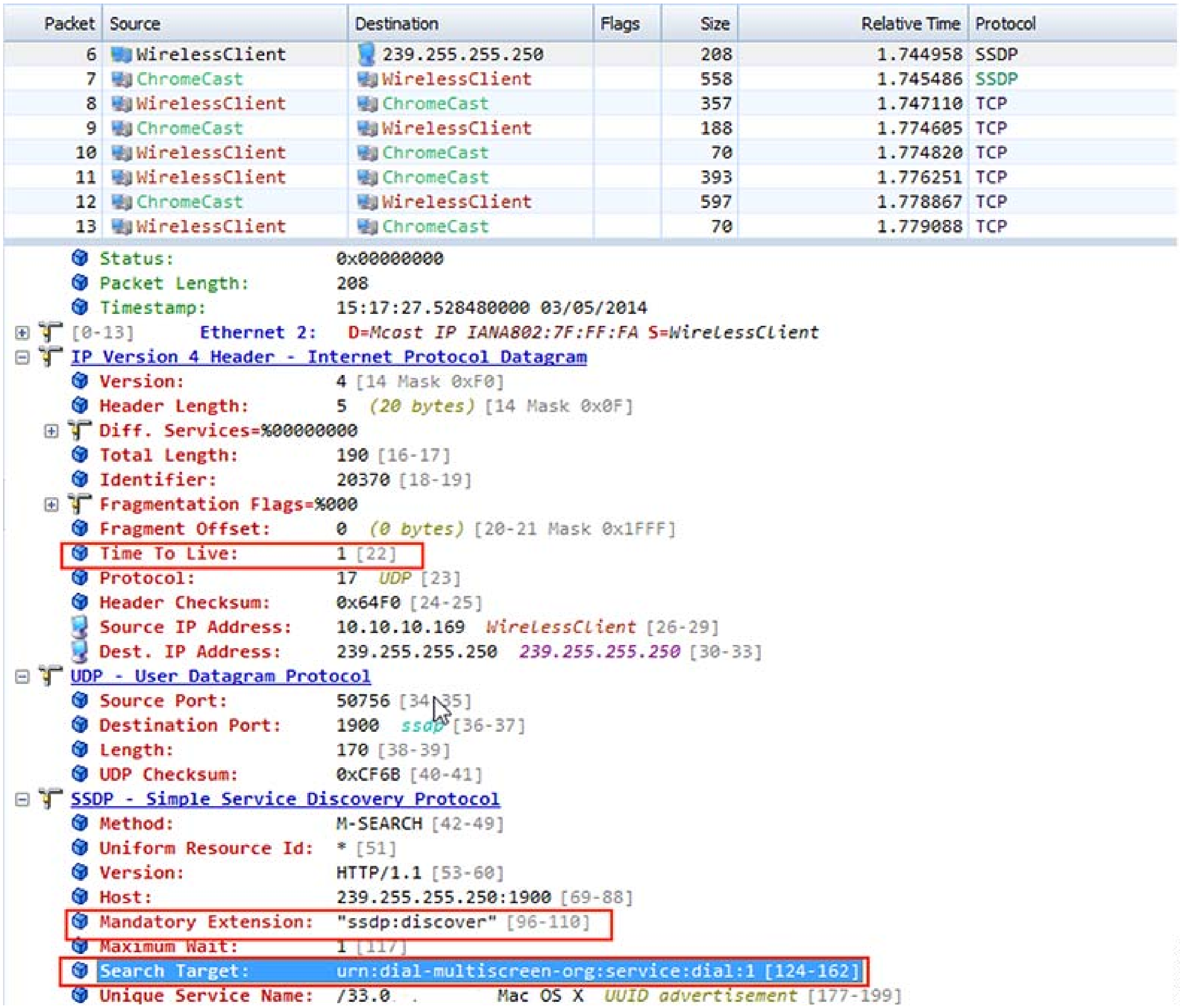
1. (Service Discovery Request)
239.255.255.250
Unicast Response
1. (Response with IP address of service)
chrome
352546

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:

urn:dial-multiscreen-org:service:dial:1.

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



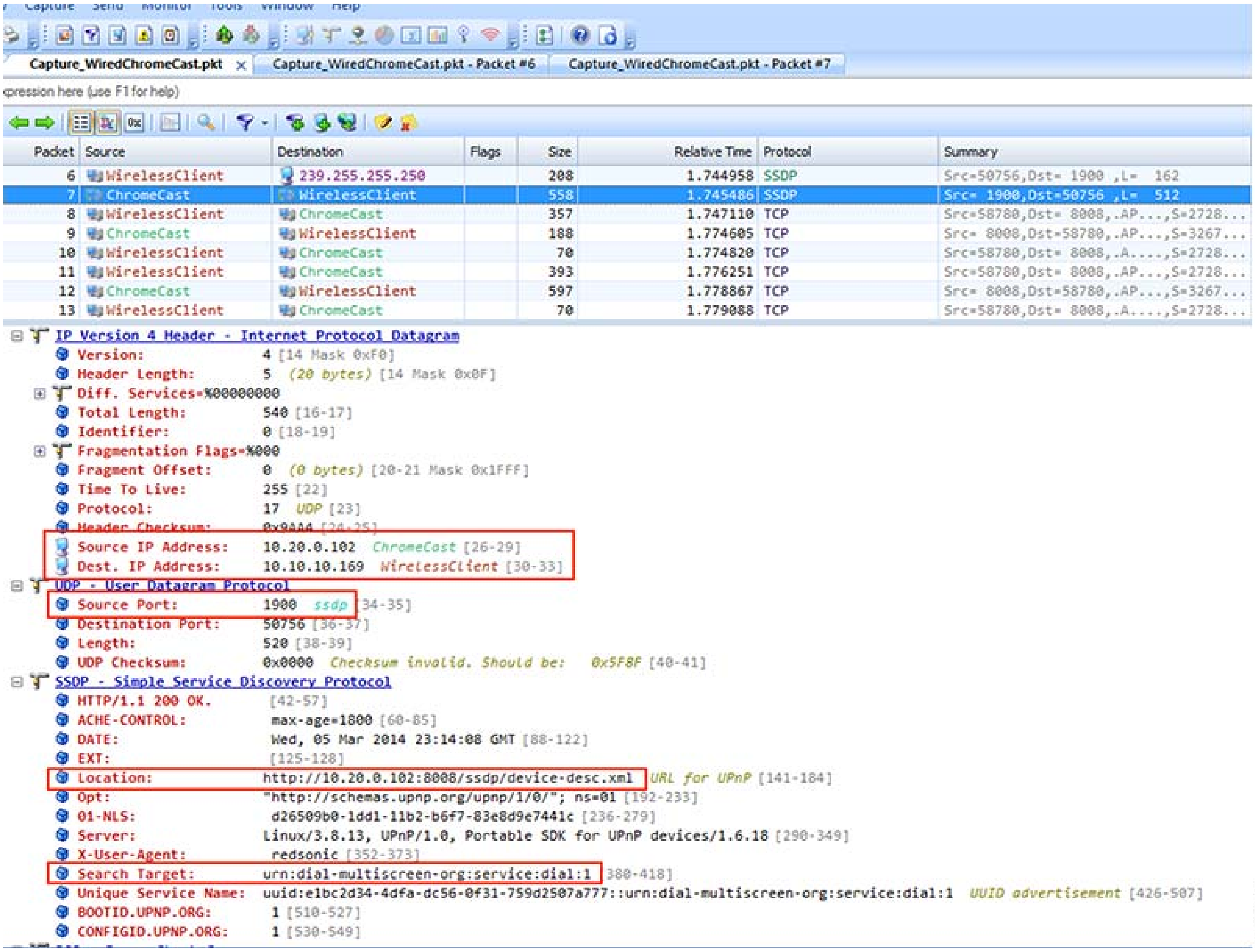
Packet	Source	Destination	Flags	Size	Relative Time	Protocol
6	WirelessClient	239.255.255.250		208	1.744958	SSDP
7	ChromeCast	WirelessClient		558	1.745486	SSDP
8	WirelessClient	ChromeCast		357	1.747110	TCP
9	ChromeCast	WirelessClient		188	1.774605	TCP
10	WirelessClient	ChromeCast		70	1.774820	TCP
11	WirelessClient	ChromeCast		393	1.776251	TCP
12	ChromeCast	WirelessClient		597	1.778867	TCP
13	WirelessClient	ChromeCast		70	1.779088	TCP

```
    Status:                 0x00000000
    Packet Length:          208
    Timestamp:              15:17:27.528480000 03/05/2014
⊞ [0-13]      Ethernet 2:   D=Mcast IP IANA802:7F:FF:FA S=WirelessClient
⊟ IP Version 4 Header - Internet Protocol Datagram
    Version:                4 [14 Mask 0xF0]
    Header Length:          5  (20 bytes) [14 Mask 0x0F]
  ⊞ Diff. Services=%00000000
    Total Length:           190 [16-17]
    Identifier:             20370 [18-19]
  ⊞ Fragmentation Flags=%000
    Fragment Offset:        0  (0 bytes) [20-21 Mask 0x1FFF]
    Time To Live:           1 [22]
    Protocol:               17  UDP [23]
    Header Checksum:        0x64F0 [24-25]
    Source IP Address:      10.10.10.169  WirelessClient [26-29]
    Dest. IP Address:       239.255.255.250  239.255.255.250 [30-33]
⊟ UDP - User Datagram Protocol
    Source Port:            50756 [34-35]
    Destination Port:       1900  ssdp [36-37]
    Length:                 170 [38-39]
    UDP Checksum:           0xCF6B [40-41]
⊟ SSDP - Simple Service Discovery Protocol
    Method:                 M-SEARCH [42-49]
    Uniform Resource Id:    * [51]
    Version:                HTTP/1.1 [53-60]
    Host:                   239.255.255.250:1900 [69-88]
    Mandatory Extension:    "ssdp:discover" [96-110]
    Maximum Wait:           1 [117]
    Search Target:          urn:dial-multiscreen-org:service:dial:1 [124-162]
    Unique Service Name:    /33.0 .          Mac OS X  UUID advertisement [177-199]
```

352573

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.

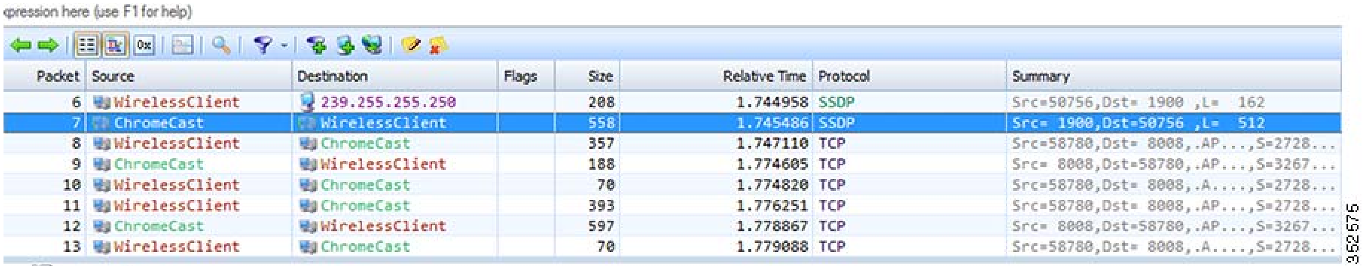

Capture_WiredChromeCast.pkt
Capture_WiredChromeCast.pkt - Packet #6
Capture_WiredChromeCast.pkt - Packet #7
xpression here (use F1 for help)

Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary
6	WirelessClient	239.255.255.250		208	1.744958	SSDP	Src=50756,Dst= 1900 ,L= 162
7	ChromeCast	WirelessClient		558	1.745486	SSDP	Src= 1900,Dst=50756 ,L= 512
8	WirelessClient	ChromeCast		357	1.747110	TCP	Src=58780,Dst= 8008,.AP...,S=2728...
9	ChromeCast	WirelessClient		188	1.774605	TCP	Src= 8008,Dst=58780,.AP...,S=3267...
10	WirelessClient	ChromeCast		70	1.774820	TCP	Src=58780,Dst= 8008,.A....,S=2728...
11	WirelessClient	ChromeCast		393	1.776251	TCP	Src=58780,Dst= 8008,.AP...,S=2728...
12	ChromeCast	WirelessClient		597	1.778867	TCP	Src= 8008,Dst=58780,.AP...,S=3267...
13	WirelessClient	ChromeCast		70	1.779088	TCP	Src=58780,Dst= 8008,.A....,S=2728...

```
⊟ IP Version 4 Header - Internet Protocol Datagram
    Version:               4 [14 Mask 0xF0]
    Header Length:         5  (20 bytes) [14 Mask 0x0F]
  ⊞ Diff. Services=%00000000
    Total Length:          540 [16-17]
    Identifier:            0 [18-19]
  ⊞ Fragmentation Flags=%000
    Fragment Offset:       0  (0 bytes) [20-21 Mask 0x1FFF]
    Time To Live:          255 [22]
    Protocol:              17  UDP [23]
    Header Checksum:       0x9AA4 [24-25]
    Source IP Address:     10.20.0.102  ChromeCast [26-29]
    Dest. IP Address:      10.10.10.169  WirelessClient [30-33]
⊟ UDP - User Datagram Protocol
    Source Port:           1900  ssdp [34-35]
    Destination Port:      50756 [36-37]
    Length:                520 [38-39]
    UDP Checksum:          0x0000  Checksum invalid. Should be:   0x5F8F [40-41]
⊟ SSDP - Simple Service Discovery Protocol
    HTTP/1.1 200 OK.        [42-57]
    ACHE-CONTROL:           max-age=1800 [60-85]
    DATE:                   Wed, 05 Mar 2014 23:14:08 GMT [88-122]
    EXT:                    [125-128]
    Location:              http://10.20.0.102:8008/ssdp/device-desc.xml URL for UPnP [141-184]
    Opt:                   "http://schemas.upnp.org/upnp/1/0/"; ns=01 [192-233]
    01-NLS:                 d26509b0-1dd1-11b2-b6f7-83e8d9e7441c [236-279]
    Server:                Linux/3.8.13, UPnP/1.0, Portable SDK for UPnP devices/1.6.18 [290-349]
    X-User-Agent:           redsonic [352-373]
    Search Target:         urn:dial-multiscreen-org:service:dial:1 380-418]
    Unique Service Name:   uuid:e1bc2d34-4dfa-dc56-0f31-759d2507a777::urn:dial-multiscreen-org:service:dial:1  UUID advertisement [426-507]
    BOOTID.UPNP.ORG:        1 [510-527]
    CONFIGID.UPNP.ORG:      1 [530-549]
```

352574

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



Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary
6	WirelessClient	239.255.255.250		208	1.744958	SSDP	Src=50756,Dst= 1900 ,L= 162
7	ChromeCast	WirelessClient		558	1.745486	SSDP	Src= 1900,Dst=50756 ,L= 512
8	WirelessClient	ChromeCast		357	1.747110	TCP	Src=58780,Dst= 8008,.AP...,S=2728...
9	ChromeCast	WirelessClient		188	1.774605	TCP	Src= 8008,Dst=58780,.AP...,S=3267...
10	WirelessClient	ChromeCast		70	1.774820	TCP	Src=58780,Dst= 8008,.A....,S=2728...
11	WirelessClient	ChromeCast		393	1.776251	TCP	Src=58780,Dst= 8008,.AP...,S=2728...
12	ChromeCast	WirelessClient		597	1.778867	TCP	Src= 8008,Dst=58780,.AP...,S=3267...
13	WirelessClient	ChromeCast		70	1.779088	TCP	Src=58780,Dst= 8008,.A....,S=2728...

352575