Cisco Vision Dynamic Signage Solution

Operation and Network Requirements

Version 1.2

February 2018

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco Systems, Inc.

www.cisco.com

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Google, Google Play, Android and certain other marks are trademarks of Google Inc.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Copyright © 2018 Cisco Systems, Inc. All rights reserved.

Contents

About this Guide

This document provides a detailed description of the Cisco Vision Dynamic Signage Solution components and what is required from the network to successfully deploy the solution.

Document Audience

This document is intended for Cisco engineers and product managers and Cisco partners. Additionally, technical sales and marketing people can use this document as a master reference guide when helping customers understand what components they need for implementing the solution.

Related Documents

Cisco Vision Documentation Page

- Cisco Vision Software Installation and Upgrade Guide
- Cisco Vision Administration Guide
- Cisco Vision Dynamic Signage Director Operations Guide

Borderless Campus Network Design Guide

Medianet Campus QoS Design 4.0

Cisco SAFE Reference Guide

SAFE - Network Foundation Protection

Cisco Design Zone (Top-Level Design Home Page)

Document History

Table 1. Revision History

Date	Revision	Comments
11/1017	1.0	Repackaging of Cisco Vision specific design components from the Connected Venue, Connected Venue Wi-Fi and Connected Stadium Video Headend Design Guides
1/16/18	1.1	Changed the Network Requirements chapter title to Solution Operation and Deployment Details Added new and updated a number of diagrams for clarity
2/13/18	1.2	Updated Multisite Deployment model diagrams to have a more consistent look. Technical content is unchanged. Added clarification concerning zone-based synchronization.

Cisco Vision Dynamic Signage Solution

Cisco Vision Dynamic Signage Component Overview

This section provides a brief overview of the components and operation of the Cisco Vision Dynamic Signage solution.

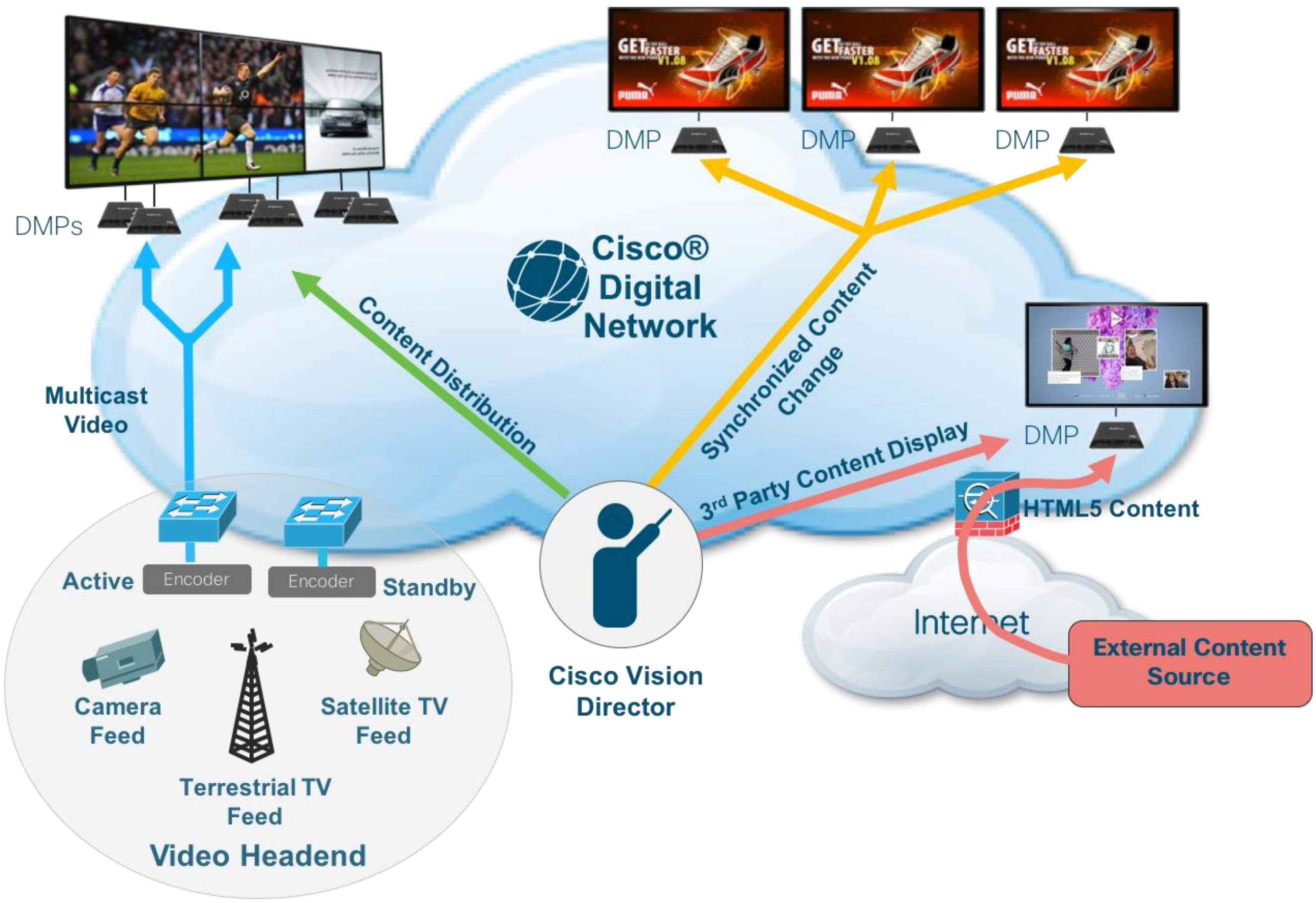
The Cisco Vision Dynamic Signage solution enables the integration and automated delivery of customized and dynamic content from multiple sources to different areas of the venue in standard definition (SD) to Ultra HD (4K). The solution is designed to enhance the visitor experience and to provide the venue with additional revenue streams through targeted advertising via engaging, moving, dynamically updating content.

Four major components that constitute a Cisco Vision Dynamic Signage solution:

- Cisco Vision Dynamic Signage Director for centralized content management and operations
- Digital Media Player for content playback
- Cisco Digital Network, the IP infrastructure foundation for content transport
- Video Headend for video aggregation and distribution

Note - Cisco Vision is the new name for StadiumVision since the product is now supported across other vertical markets outside of Sports.

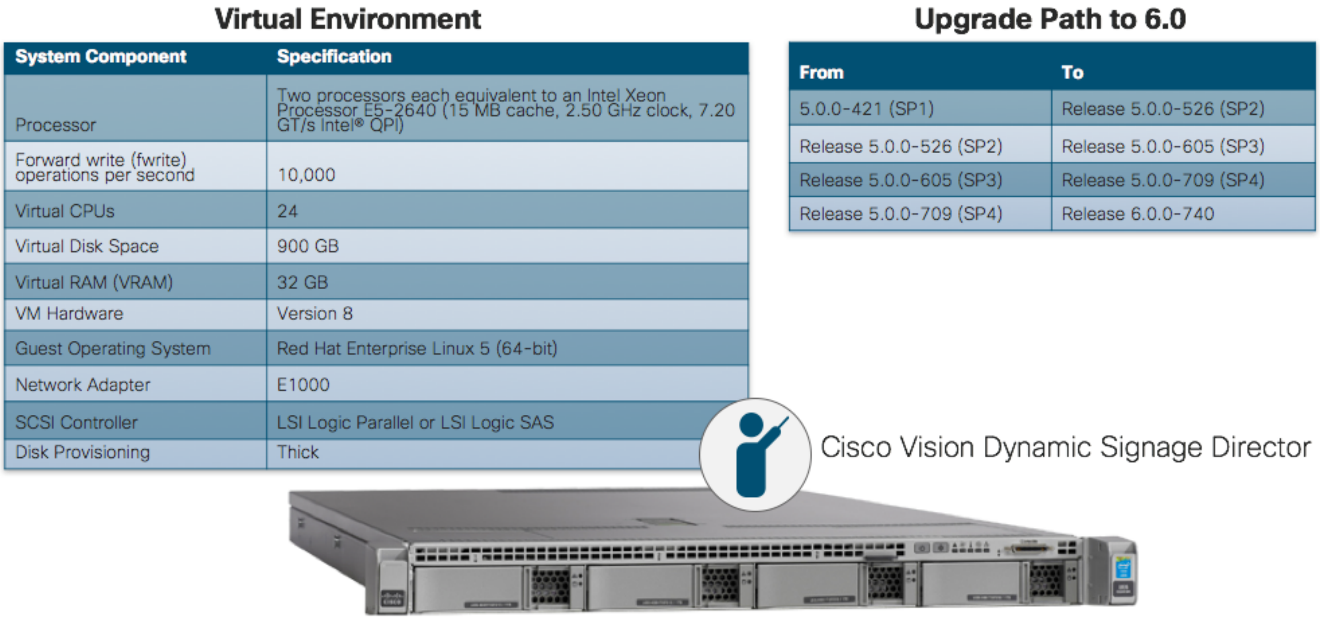
Figure 1 - Cisco Vision Dynamic Signage Components



Cisco Vision Dynamic Signage Director

Cisco Vision Dynamic Signage Director provides centralized management and operations of the Cisco Vision Dynamic Signage solution. It acts as a single point of control for managing all Digital Media Player (DMP) endpoints, for placing and delivering content (video, graphics, and external content), for defining unique display areas (zones and groups), as well as for the creation of entitlement areas (bars, restaurants, clubs, and suites). It also provides the interface to third-party applications and devices, score boards and statistics systems, external contact closure and IP triggering systems, and third-party touch panels (for local display control).

Figure 2 – Cisco Vision Dynamic Signage Director Overview



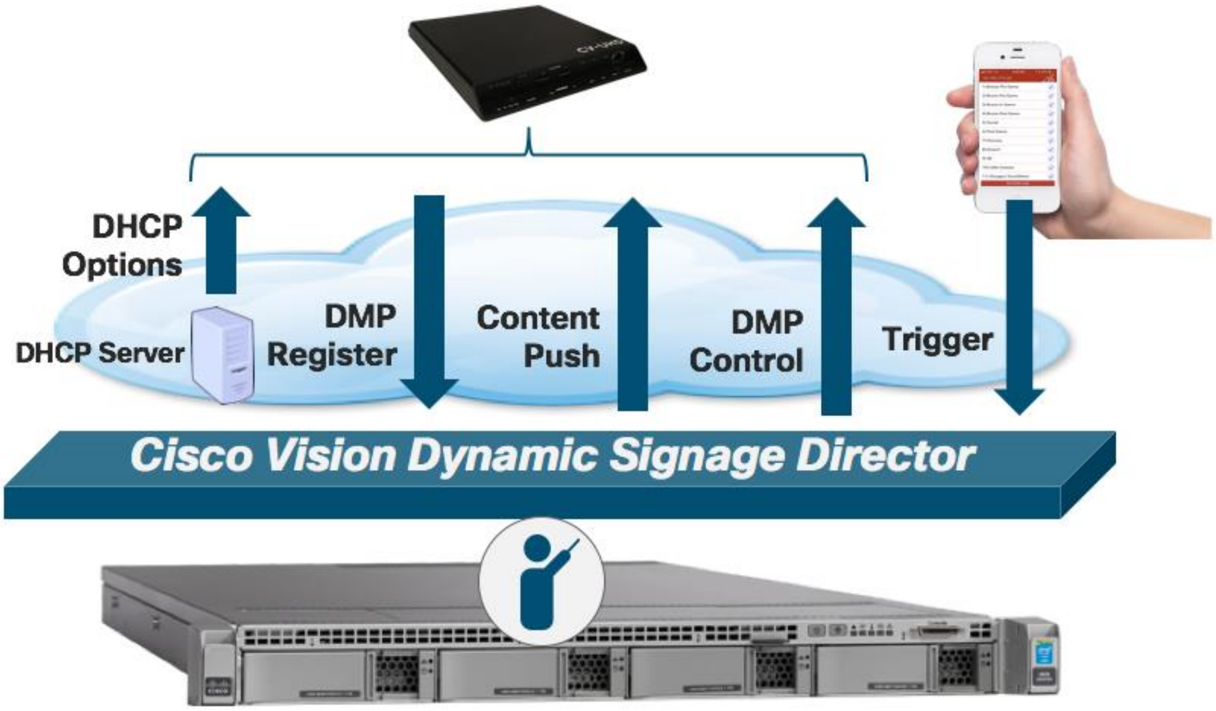
Virtual Environment

System Component	Specification
Processor	Two processors each equivalent to an Intel Xeon Processor E5-2640 (15 MB cache, 2.50 GHz clock, 7.20 GT/s Intel® QPI)
Forward write (fwrite) operations per second	10,000
Virtual CPUs	24
Virtual Disk Space	900 GB
Virtual RAM (VRAM)	32 GB
VM Hardware	Version 8
Guest Operating System	Red Hat Enterprise Linux 5 (64-bit)
Network Adapter	E1000
SCSI Controller	LSI Logic Parallel or LSI Logic SAS
Disk Provisioning	Thick

Upgrade Path to 6.0

From	To
5.0.0-421 (SP1)	Release 5.0.0-526 (SP2)
Release 5.0.0-526 (SP2)	Release 5.0.0-605 (SP3)
Release 5.0.0-605 (SP3)	Release 5.0.0-709 (SP4)
Release 5.0.0-709 (SP4)	Release 6.0.0-740

Figure 3 – Cisco Vision Dynamic Signage Director Functional Overview



Digital Media Player

The Digital Media Player (DMP) renders and displays static and dynamic content on each of the venue's connected displays. In addition to the support of 4K video resolution, the DMP can be powered by 802.3at Power over Ethernet, supports dual video regions, video wall and virtual ribbon-board synchronization, and the rendering of HTML5 content. The DMP also supports Live TV playback via the HDMI 2.0a input to play content from any broadcast channel — even protected HDCP content. The DMP is also available with built-in Wi-Fi, allowing you to deliver digital content to hard-to-reach displays, such as those on mobile kiosks.

Figure 4 - BRIGHTSIGN CV-UHD DMP For Cisco Vision

Table 1 - Digital Media Player Comparison Chart

Cisco Vision Dynamic Signage Feature	DMP-2K	SV-4K	CV-HD	CV-UHD
Wi-Fi Support	No	Yes	No	-WIFI Model
Power Over Ethernet or Local Power	PoE	PoE+	PoE	PoE+
HDMI out to Display	Yes	Yes	Yes	Yes
TV Control using RS-232 and IR Remote	DB9	DB9	TRS	TRS
TV Control using HDMI CEC	Yes	Yes	Yes	Yes
Audio Out and IR Out	Yes	Yes	Yes	Yes
Touchscreen Support	Yes	Yes	Yes	Yes
4K Local Video	No	Yes	No	Yes
2.1 AC3/AC3+ (Dolby Digital audio decode)	Yes	Yes	Yes	Yes
Auto-Registration	Yes	Yes	Yes	Yes
Dual Video Regions with Luma Key Support	Yes	Yes	No	Yes
HDMI-In as a Channel Source	No	Yes	No	Yes
HDMI-In Pass-Through for HDCP-compliant devices	No	Yes	No	Yes
Video Encoding as a Channel	No	Yes	No	Yes
Video Streaming through HDMI-Out	No	Yes	No	Yes
Encrypted Multicast Video Channels	Yes	Yes	Yes	Yes
Content Replacement	Yes	Yes	Yes	Yes
Content Synchronization	Yes	Yes	Yes	Yes

Figure 5 – CV-UHD Front Panel Overview

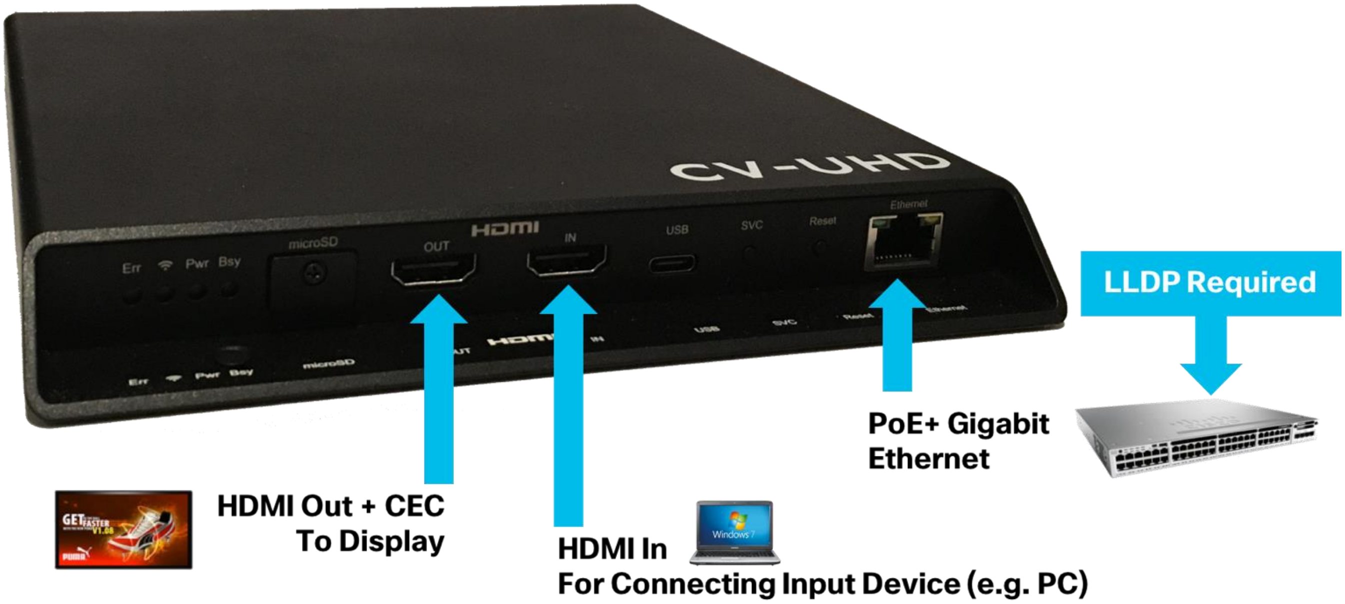
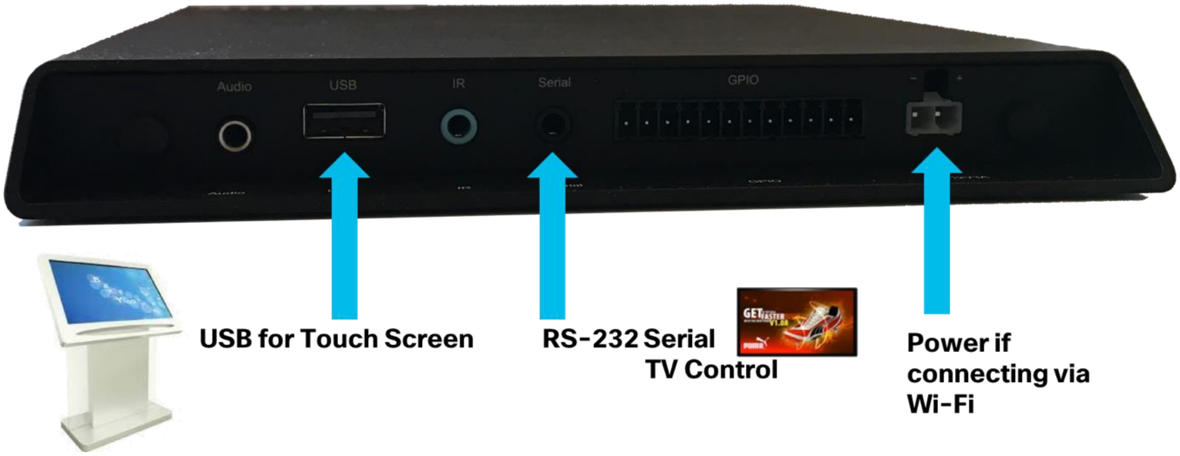


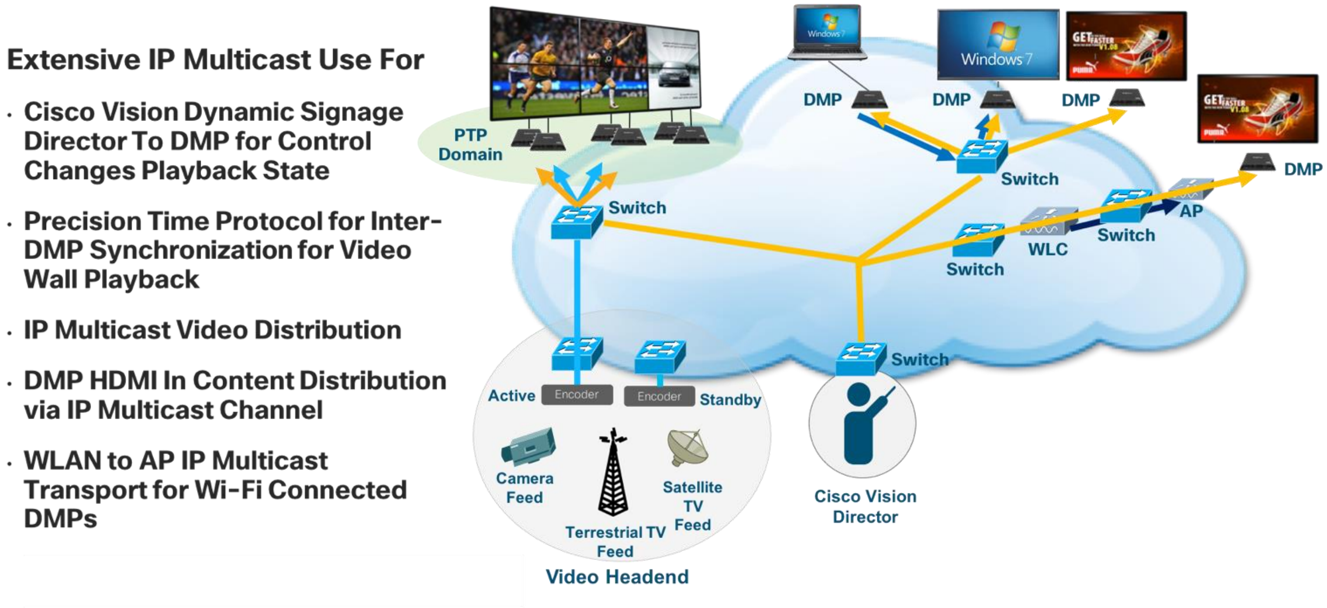
Figure 6 – CV-UHD Rear Panel Overview



Cisco Digital Network

Cisco's Digital Network is the foundational IP infrastructure that not only connects the video headend with the DMPs but typically interconnects all building IP endpoints to each other and to the outside world. The Cisco Vision Dynamic Signage solution requires a converged, highly scalable, secure digital network designed specifically for low latency and redundancy to bring together all forms of access, communications, entertainment and operations. This infrastructure is designed to enable the delivery of high-quality video, using advanced features of IP Multicast and quality of service (QoS). This network also acts as the foundation to enable other services within the venue, such as wireless communications, physical security, IP telephony, network audio and Point of Sales communications.

Figure 7 – Cisco Digital Network



Extensive IP Multicast Use For

- Cisco Vision Dynamic Signage Director To DMP for Control Changes Playback State
- Precision Time Protocol for Inter-DMP Synchronization for Video Wall Playback
- IP Multicast Video Distribution
- DMP HDMI In Content Distribution via IP Multicast Channel
- WLAN to AP IP Multicast Transport for Wi-Fi Connected DMPs

Video Headend

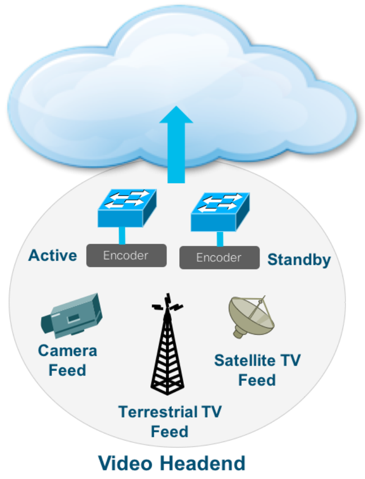
The headend is where video is received from various sources, such as in-house feeds (through the venue video control room), over-the-air channels (typically from local over-the-air broadcast networks), and broadcast channels from cable or satellite providers. It is responsible for placing the video feeds onto the IP network with minimal latency. Video feeds may be provided in Ultra HD, HD or SD resolution, and in encrypted or unencrypted formats.

The headend of the Cisco Vision Dynamic Signage solution is designed to accommodate all of these feeds and perform the necessary encoding, transcoding, and extracting to create H.264 (MPEG-4, Part 10), H.265 (HEVC), or legacy MPEG-1, MPEG-2 encoded streams. The headend then takes the processed streams, assigns a unique IP multicast address to each, and places it on the IP network to be joined by the digital media player (DMP) endpoints as a channel.

Figure 8 – Video Headend Overview

Video Headend is Used For

- **Aggregate & Organize Video Feeds from Various Sources**
  - **Local Camera Feeds**
  - **Terrestrial TV Feeds (i.e., Local Broadcast Channels)**
  - **Satellite Feeds (e.g., Direct TV)**
- **Encode the Feeds into IP Multicast Streams**
- **Distribute Those Streams to the Network**



Deployment Models

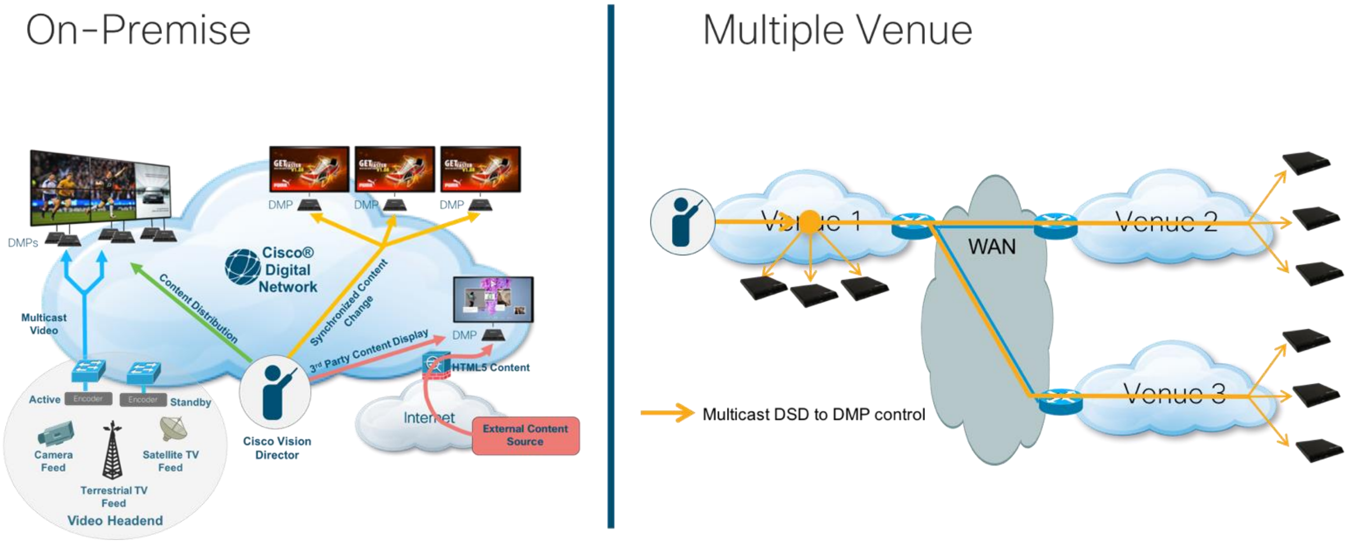
On-Premise

The On-Premise deployment model resembles an Enterprise client-server model with a server and its associated endpoints connected to an Enterprise campus network. The Cisco Vision Dynamic Signage Director server typically resides in the Data Center or in a Video Distribution service block (i.e., Video Headend) usually located near the broadcast room where all the various video input source feeds enter the venue.

Multiple Venue

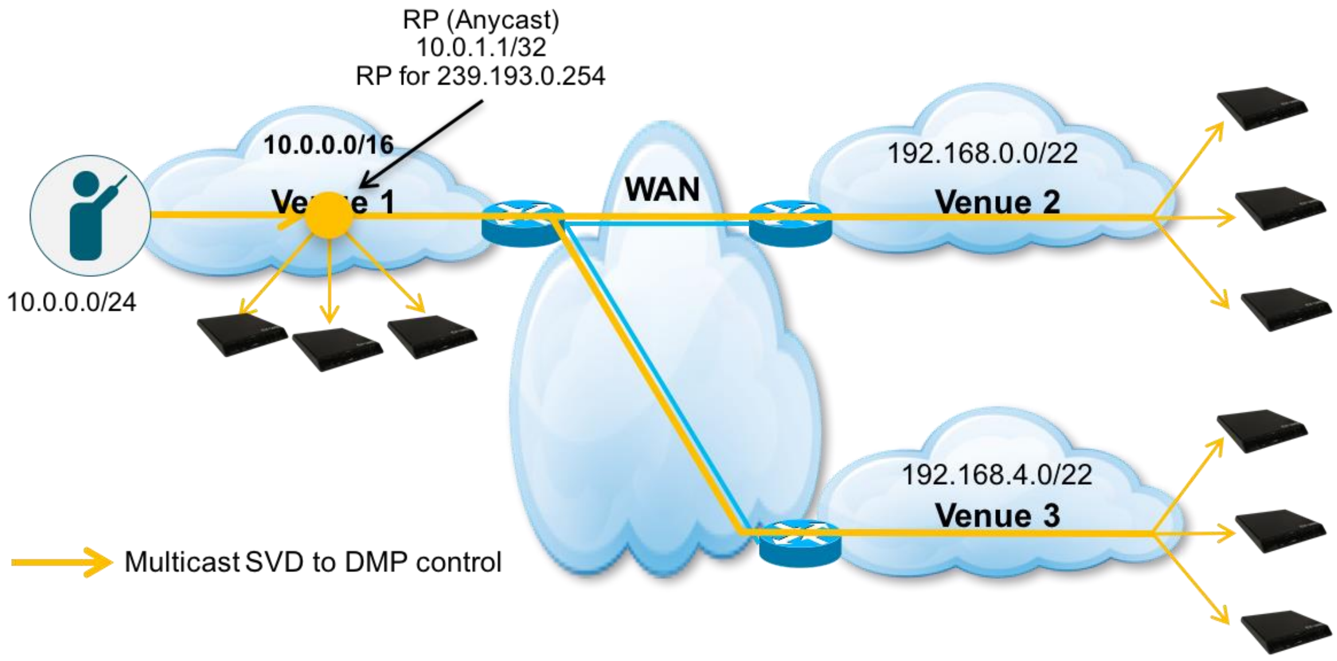
The Multiple Venue deployment model is one where the Dynamic Signage Director is located at a central location and DMPs are distributed locally and across a WAN to remote locations.

Figure 9 – Deployment Model Overview



This section describes how to configure the WAN. See the Configuring Dynamic Signage Director for Multiple Venue Support section in the Cisco Vision Dynamic Signage Director Server Administration Guide for more information.

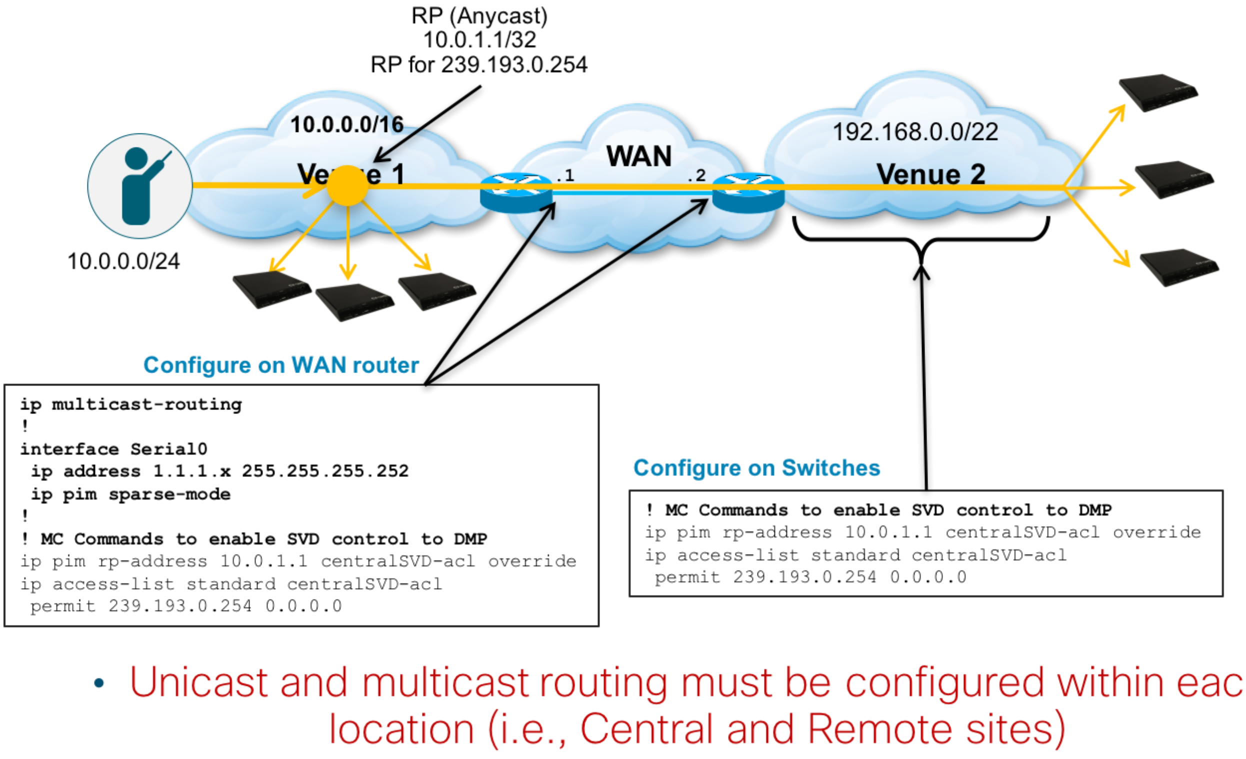
Figure 10 – Multiple Venue Deployment Model – Multicast Communication



The figure above shows the multicast communication between the Cisco Vision Dynamic Signage Director and the local and remote DMPs.

The figure below shows the commands required to enable multicast over a point-to-point WAN link and the additional commands required in the switches at the remote venue.

Figure 11 – Cisco Vision Dynamic Signage Director Multicast Routing over Point-to-Point WAN link



Configure on WAN router

```
ip multicast-routing
!
interface Serial0
 ip address 1.1.1.x 255.255.255.252
 ip pim sparse-mode
!
! MC Commands to enable SVD control to DMP
ip pim rp-address 10.0.1.1 centralSVD-acl override
ip access-list standard centralSVD-acl
 permit 239.193.0.254 0.0.0.0
```

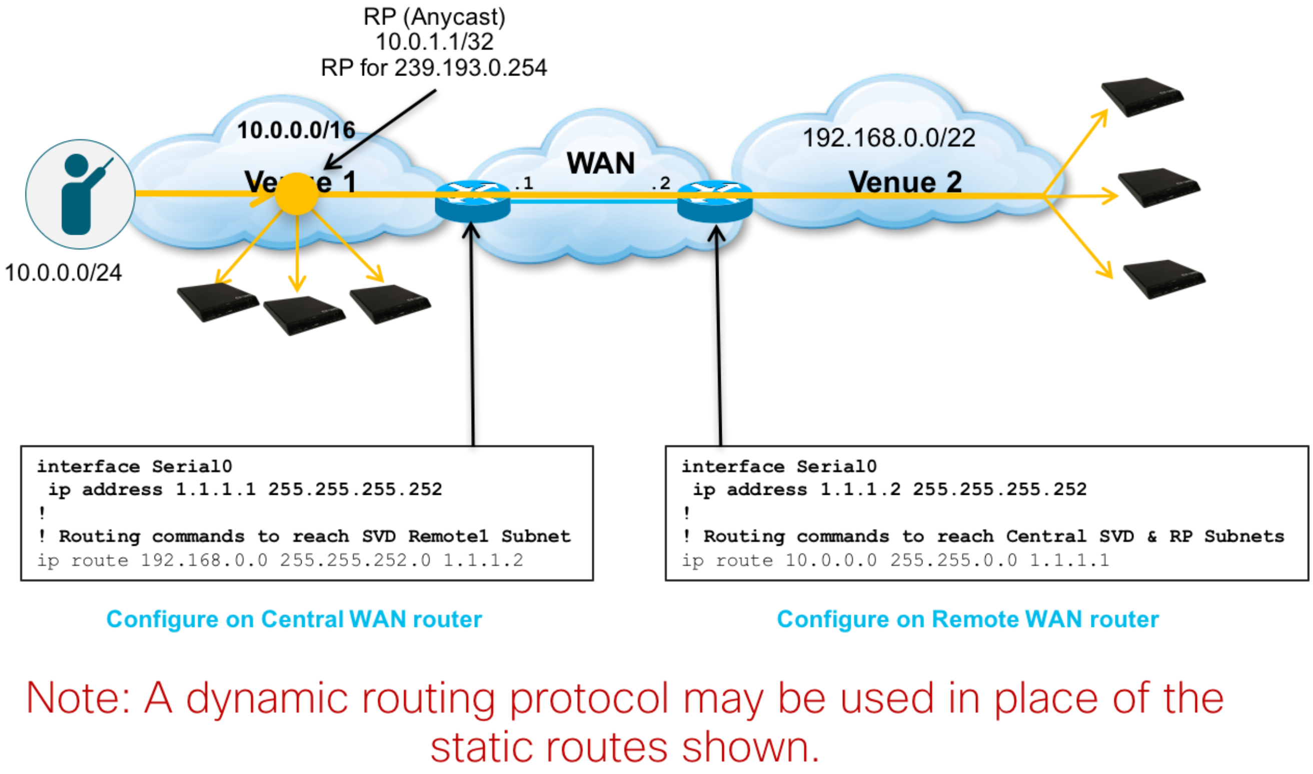
Configure on Switches

```
! MC Commands to enable SVD control to DMP
ip pim rp-address 10.0.1.1 centralSVD-acl override
ip access-list standard centralSVD-acl
 permit 239.193.0.254 0.0.0.0
```

- Unicast and multicast routing must be configured within each location (i.e., Central and Remote sites)

The figure below shows the specific commands to enable unicast routing between the central and remote DSD servers and between the remote venue and the central PIM Rendezvous Point (RP) that enables multicast routing.

Figure 12 - DSD Unicast Routing over Point-to-Point WAN Link



```
interface Serial0
 ip address 1.1.1.1 255.255.255.252
!
! Routing commands to reach SVD Remote1 Subnet
ip route 192.168.0.0 255.255.252.0 1.1.1.2
```

Configure on Central WAN router

```
interface Serial0
 ip address 1.1.1.2 255.255.255.252
!
! Routing commands to reach Central SVD & RP Subnets
ip route 10.0.0.0 255.255.0.0 1.1.1.1
```

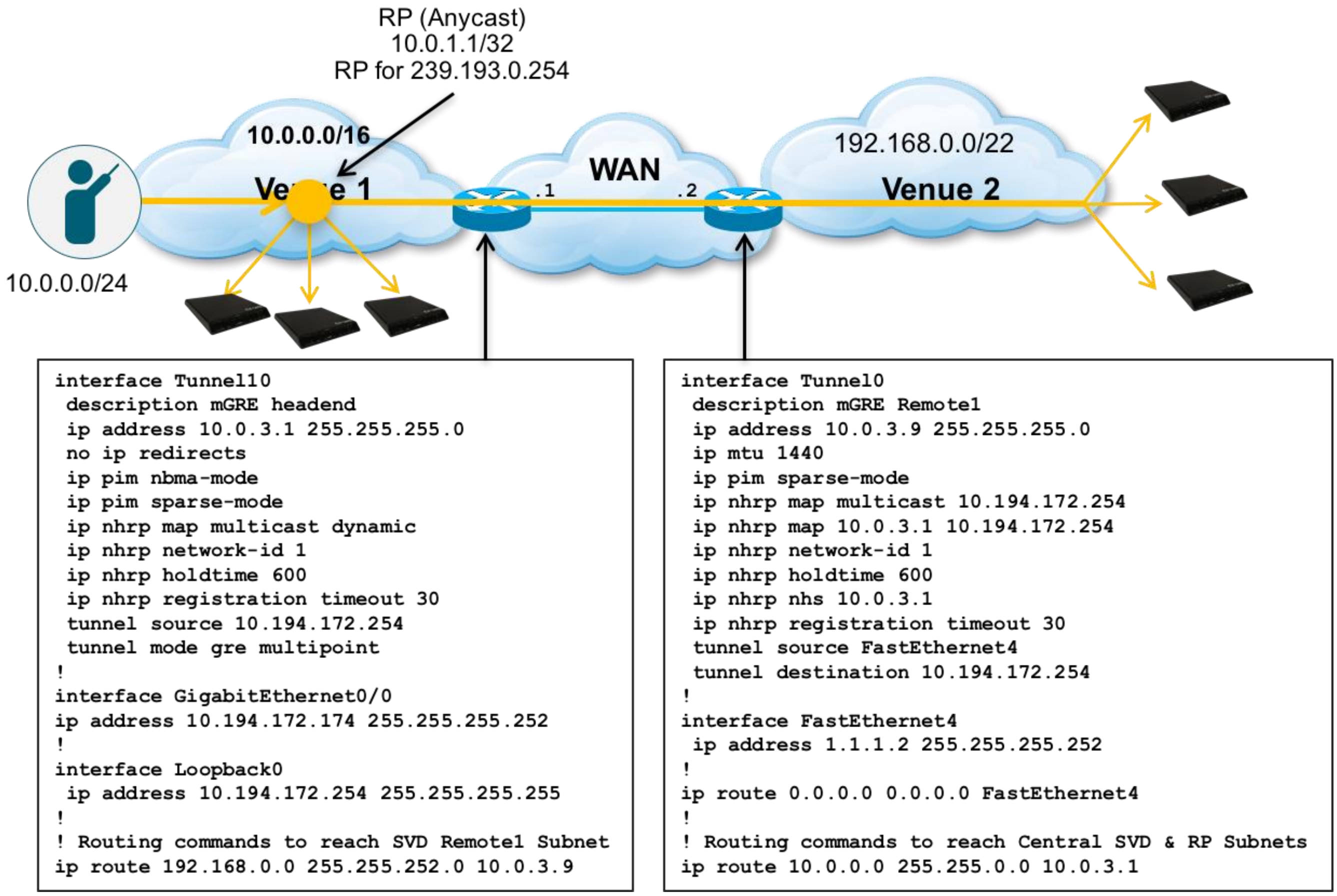
Configure on Remote WAN router

- Note: A dynamic routing protocol may be used in place of the static routes shown.

The figure below shows the commands used to enable both unicast and multicast routing over a routed WAN (e.g., private MPLS network). A Multipoint Generic Route Encapsulation (mGRE) tunnel is used to create a VPN across the WAN to enable multicast between the central and remote venues.

Note - A mGRE tunnel between the central and remote venue is not required if multicast is supported on the routed WAN. If the WAN is a public network (e.g., Internet), IPsec may be used for data privacy.

Figure 13 – DSD Multicast Routing over GRE tunnel



```
interface Tunnel10
 description mGRE headend
 ip address 10.0.3.1 255.255.255.0
 no ip redirects
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp holdtime 600
 ip nhrp registration timeout 30
 tunnel source 10.194.172.254
 tunnel mode gre multipoint
!
interface GigabitEthernet0/0
ip address 10.194.172.174 255.255.255.252
!
interface Loopback0
 ip address 10.194.172.254 255.255.255.255
!
! Routing commands to reach SVD Remote1 Subnet
ip route 192.168.0.0 255.255.252.0 10.0.3.9
```

```
interface Tunnel0
 description mGRE Remote1
 ip address 10.0.3.9 255.255.255.0
 ip mtu 1440
 ip pim sparse-mode
 ip nhrp map multicast 10.194.172.254
 ip nhrp map 10.0.3.1 10.194.172.254
 ip nhrp network-id 1
 ip nhrp holdtime 600
 ip nhrp nhs 10.0.3.1
 ip nhrp registration timeout 30
 tunnel source FastEthernet4
 tunnel destination 10.194.172.254
!
interface FastEthernet4
 ip address 1.1.1.2 255.255.255.252
!
ip route 0.0.0.0 0.0.0.0 FastEthernet4
!
! Routing commands to reach Central SVD & RP Subnets
ip route 10.0.0.0 255.255.0.0 10.0.3.1
```

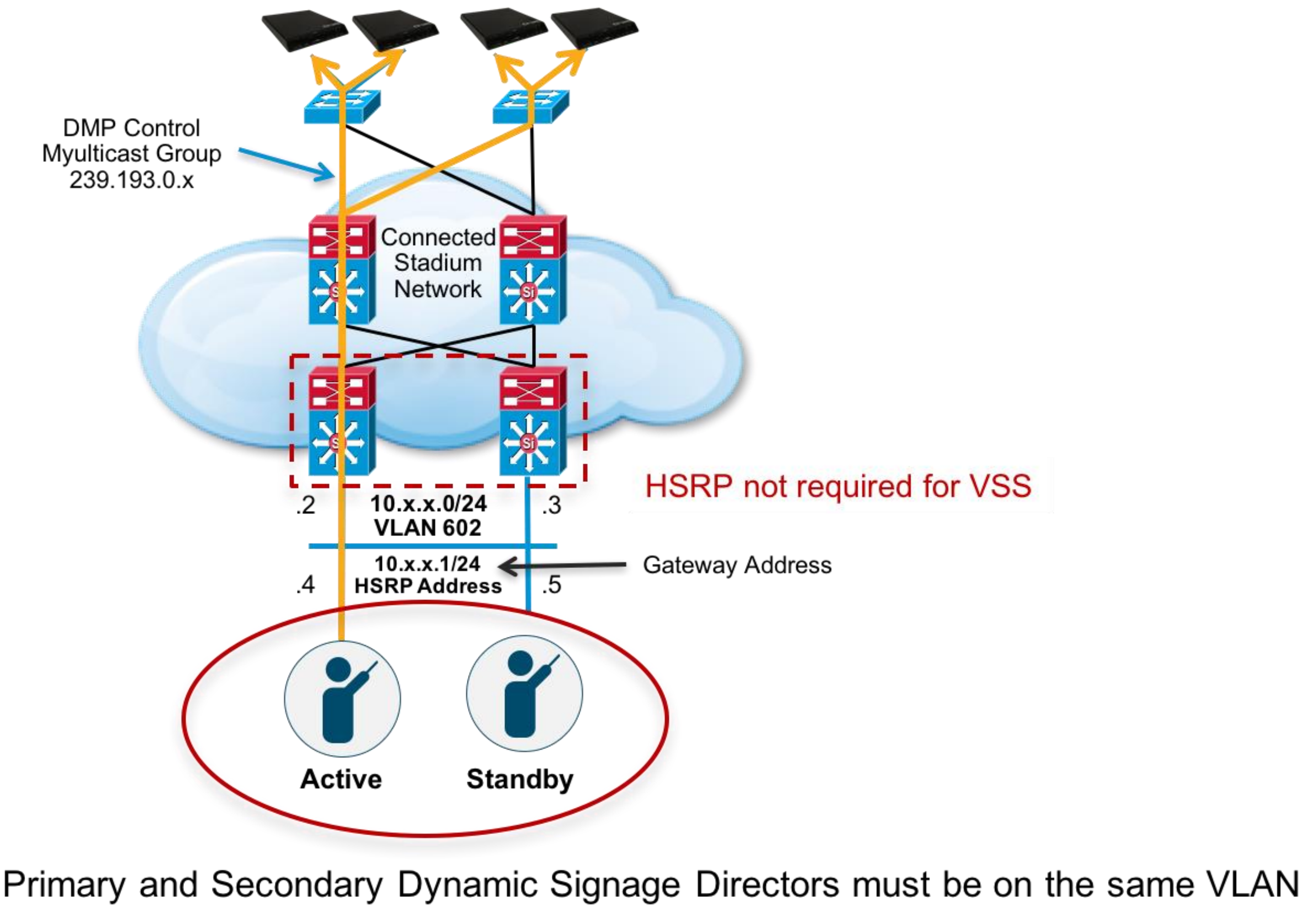
Solution Operation and Deployment Details

Connecting the Cisco Vision Dynamic Signage Director to the Network

For redundancy, Cisco Vision Dynamic Signage Director is installed on two bare metal or virtual servers, where one of the servers operates as the primary active server and the other server operates as a secondary backup server. If a failure occurs, you can configure the backup server to become the active server, but the failover process is not automatic.

Both servers must reside in the same VLAN and optimally connecting to their own switch as shown in the diagram below. HSRP should be configured to provide default gateway redundancy. Cisco Vision Dynamic Signage Director servers would typically be installed in the Data Center.

Figure 14 – Cisco Vision Server Configuration Overview



The primary and secondary servers are addressed as independent hosts with two different IP addresses on the same subnet.

The secondary server is only connected to the network to be made available as a backup to the primary should a failure occur. In addition, the secondary server can (and should) be configured to be backed up with data from the primary server on a scheduled basis so that it can be ready as a warm standby.

When the primary server fails, a manual process is used to restore the secondary server from a backup, shut down the primary server, change the secondary server's IP address to that of the primary and then to bring the secondary server into service.

Note - Although connecting servers to the Core switches is not typically recommended. There are instances where this may be done when Data Center switches are not used in the network. The main requirement is having the Layer 2 connection between the two switches where the Cisco Vision Dynamic Signage Directors are connected.

In addition, Cisco Vision Dynamic Signage Directors may be connected to a VDS switch but this allows the VDS switch as a single point of failure and is not a recommended connection scenario.
HSRP configuration information can be found at the following URL:

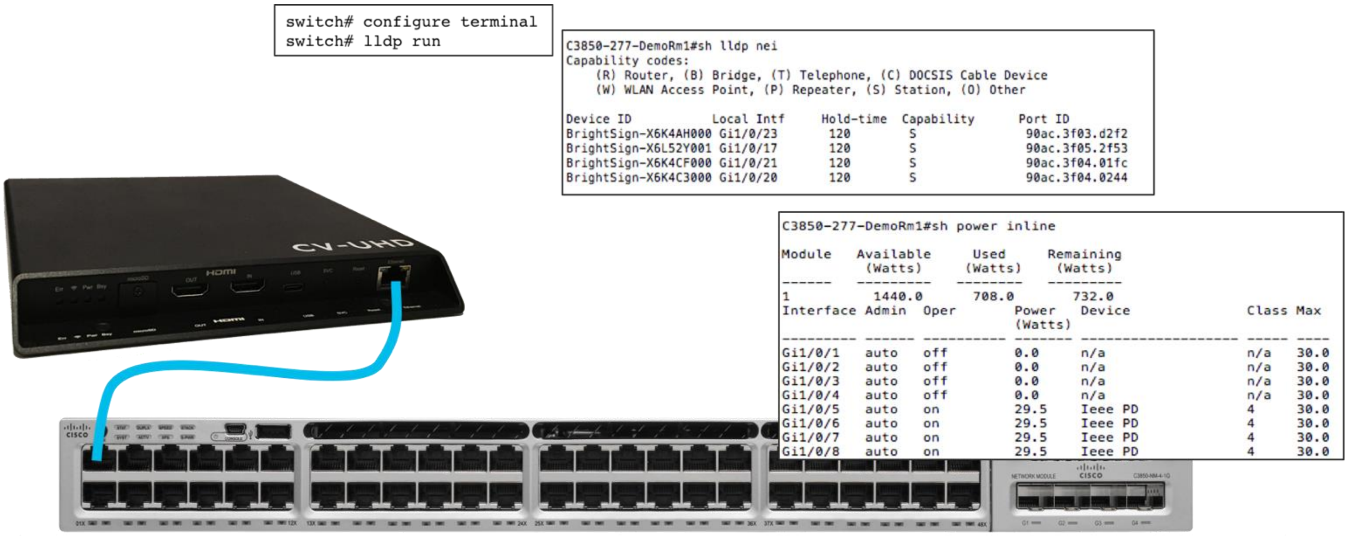
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swhsrp.html

Connecting the DMP to the Wired Network

802.3at Power over Ethernet

Access Layer switches should support the higher power IEEE 802.1at Power over Ethernet, also known as PoE+, which supports up to 30W per port. The newer 3700 Series Access Points and the Series 2 and Series 3 Digital Media Players will require 30 watts of power to take advantage of their new capabilities. The Access Layer switches should also always be equipped with the highest wattage power supplies and careful consideration must be made when choosing a switch model to ensure the switch can support the required number of PoE+ ports.

Figure 15 – The Roll of 802.3at Power over Ethernet and LLDP



```
switch# configure terminal
switch# lldp run
```

```
C3850-277-DemoRm1#sh lldp nei
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf     Hold-time  Capability      Port ID
BrightSign-X6K4AH000 Gi1/0/23       120        S               90ac.3f03.d2f2
BrightSign-X6L52Y001 Gi1/0/17       120        S               90ac.3f05.2f53
BrightSign-X6K4CF000 Gi1/0/21       120        S               90ac.3f04.01fc
BrightSign-X6K4C3000 Gi1/0/20       120        S               90ac.3f04.0244
```

```
C3850-277-DemoRm1#sh power inline

Module   Available     Used     Remaining
          (Watts)     (Watts)    (Watts)
------   ---------   --------   ---------
1          1440.0      708.0       732.0
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi1/0/1   auto   off        0.0     n/a                 n/a   30.0
Gi1/0/2   auto   off        0.0     n/a                 n/a   30.0
Gi1/0/3   auto   off        0.0     n/a                 n/a   30.0
Gi1/0/4   auto   off        0.0     n/a                 n/a   30.0
Gi1/0/5   auto   on         29.5    Ieee PD             4     30.0
Gi1/0/6   auto   on         29.5    Ieee PD             4     30.0
Gi1/0/7   auto   on         29.5    Ieee PD             4     30.0
Gi1/0/8   auto   on         29.5    Ieee PD             4     30.0
```

Note - DMPs require LLDP to fully power up. If LLDP is not enabled then DMPs may or may not power up and lead to an unstable condition. Use the command above to verify the CV-UHD DMPs negotiate 29.5 watts of power. CV-HD runs with 15W power.

The Role of LLDP

The Cisco Vision DMPs support standard Link Layer Discovery Protocol (LLDP). This capability allows the switch and DMP to learn about each other by exchanging LLDP messages and to negotiate 802.3at power over the Ethernet connection.

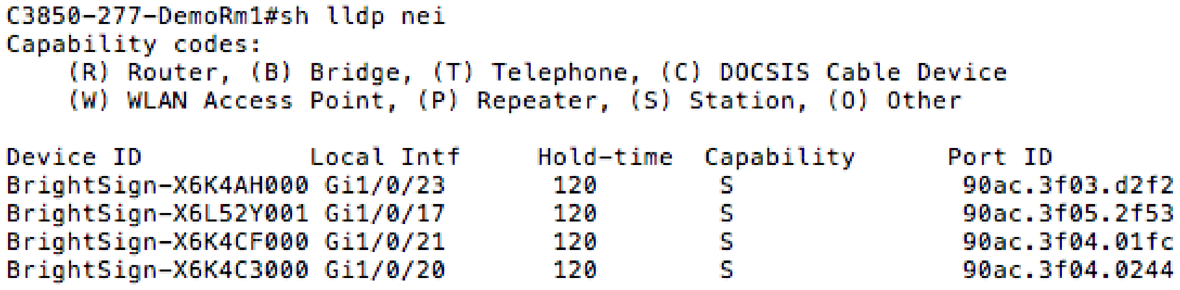
To configure LLDP on a Catalyst switch perform the following commands.

SUMMARY STEPS

```
switch# configure terminal

switch# lldp run

switch# interface interface-id

switch# lldp transmit

switch# lldp receive

switch# end

switch# show lldp
```

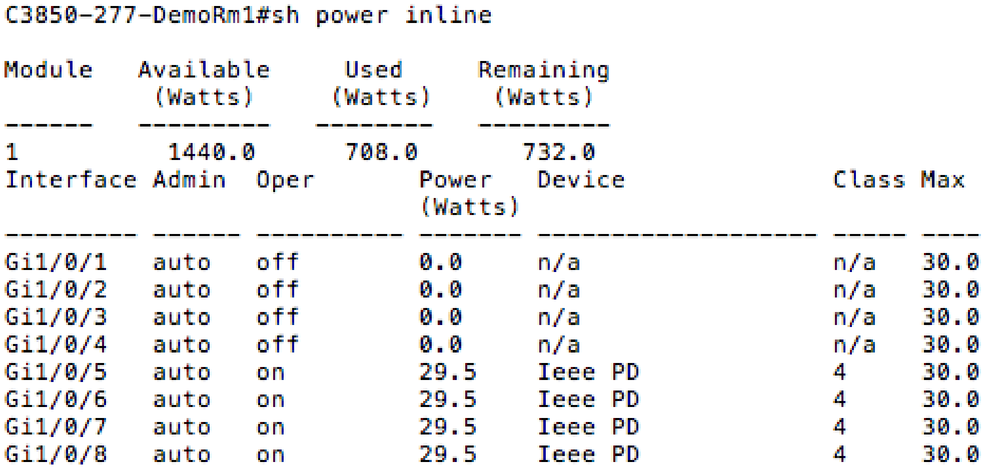
At the switch CLI and similar to the show cdp neighbor command, the show lldp neighbor command displays the DMPs that are connected to the switch. This information can be very useful when troubleshooting DMP issues.

Figure 16 – LLDP neighbor Information Display in Switch CLI Output



```
C3850-277-DemoRm1#sh lldp nei
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf     Hold-time  Capability      Port ID
BrightSign-X6K4AH000 Gi1/0/23       120        S               90ac.3f03.d2f2
BrightSign-X6L52Y001 Gi1/0/17       120        S               90ac.3f05.2f53
BrightSign-X6K4CF000 Gi1/0/21       120        S               90ac.3f04.01fc
BrightSign-X6K4C3000 Gi1/0/20       120        S               90ac.3f04.0244
```

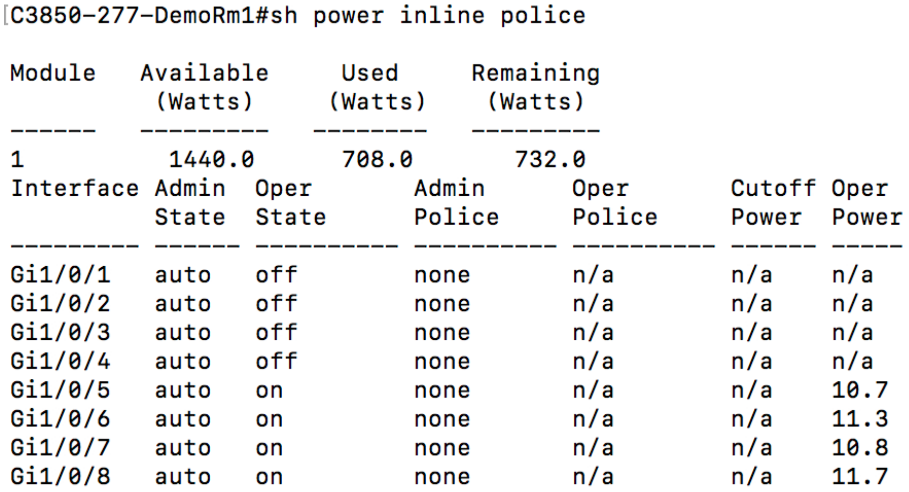
Figure 17 – Inline POE Power Display in Switch CLI Output



```
C3850-277-DemoRm1#sh power inline

Module   Available     Used     Remaining
          (Watts)     (Watts)    (Watts)
------   ---------   --------   ---------
1          1440.0      708.0      732.0
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi1/0/1   auto   off        0.0     n/a                 n/a   30.0
Gi1/0/2   auto   off        0.0     n/a                 n/a   30.0
Gi1/0/3   auto   off        0.0     n/a                 n/a   30.0
Gi1/0/4   auto   off        0.0     n/a                 n/a   30.0
Gi1/0/5   auto   on         29.5    Ieee PD             4     30.0
Gi1/0/6   auto   on         29.5    Ieee PD             4     30.0
Gi1/0/7   auto   on         29.5    Ieee PD             4     30.0
Gi1/0/8   auto   on         29.5    Ieee PD             4     30.0
```

Note - DMPs require LLDP to fully power up. If LLDP is not enabled then DMPs may or may not power up and lead to an unstable condition. Use the command above to verify the DMP negotiates 29.5 watts of power.

Figure 18 – Inline POE Power Police Display in Switch CLI Output

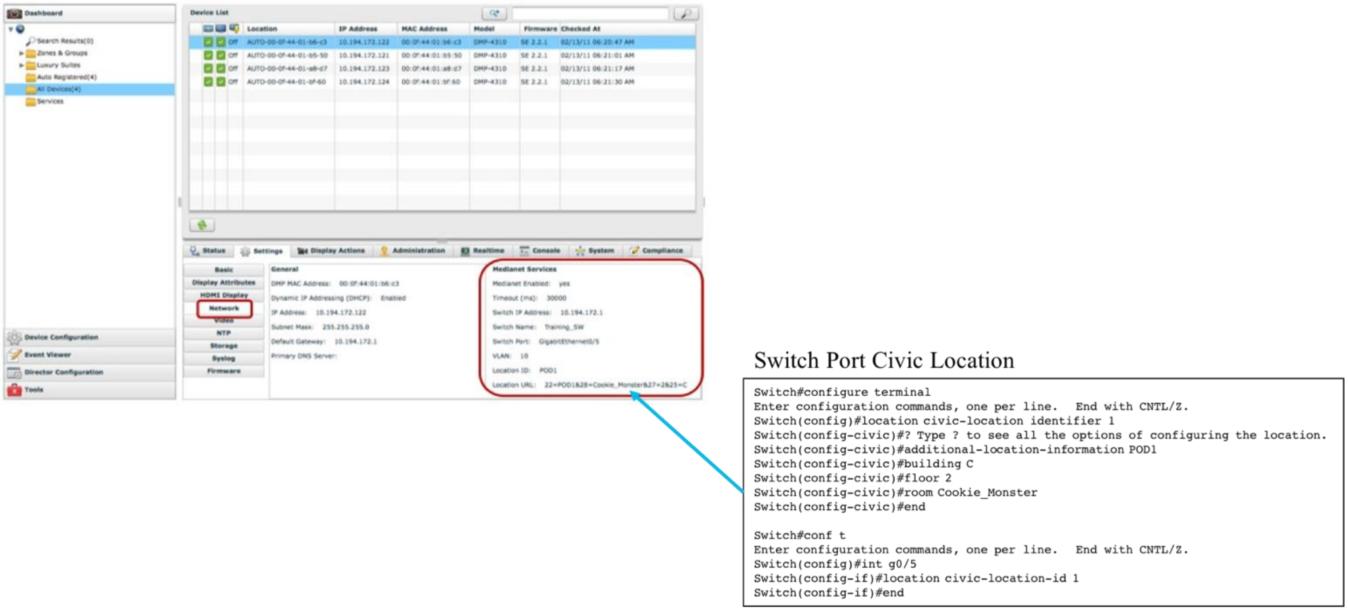


```
[C3850-277-DemoRm1#sh power inline police

Module   Available     Used     Remaining
          (Watts)     (Watts)    (Watts)
------   ---------   --------   ---------
1          1440.0      708.0      732.0
Interface Admin  Oper       Admin      Oper       Cutoff Oper
          State  State      Police     Police     Power  Power
--------- ------ ---------- ---------- ---------- ------ -----
Gi1/0/1   auto   off        none       n/a        n/a    n/a
Gi1/0/2   auto   off        none       n/a        n/a    n/a
Gi1/0/3   auto   off        none       n/a        n/a    n/a
Gi1/0/4   auto   off        none       n/a        n/a    n/a
Gi1/0/5   auto   on         none       n/a        n/a    10.7
Gi1/0/6   auto   on         none       n/a        n/a    11.3
Gi1/0/7   auto   on         none       n/a        n/a    10.8
Gi1/0/8   auto   on         none       n/a        n/a    11.7
```

Note *- To see the DMP's actual power consumption, the show power inline police command can be used. Notice that the actual consumed power is much less than the negotiated. The DMP will dynamically consume more power depending on the type of content displayed. This command can also be used to verify that switch power capacity is sufficient for supporting the number of connected DMPs.*

Cisco Vision Dynamic Signage Director uses LLDP information for populating the switch information in the Management Dashboard. This aids in troubleshooting.

Figure 19 – LLDP Information Display in Cisco Vision Dynamic Signage Director



Device List

			Location	IP Address	MAC Address	Model	Firmware	Checked At
✓	✓	Off	AUTO-00-0f-44-01-b6-c3	10.194.172.122	00:0f:44:01:b6:c3	DMP-4310	SE 2.2.1	02/13/11 06:20:47 AM
✓	✓	Off	AUTO-00-0f-44-01-b5-50	10.194.172.121	00:0f:44:01:b5:50	DMP-4310	SE 2.2.1	02/13/11 06:21:01 AM
✓	✓	Off	AUTO-00-0f-44-01-a8-d7	10.194.172.123	00:0f:44:01:a8:d7	DMP-4310	SE 2.2.1	02/13/11 06:21:17 AM
✓	✓	Off	AUTO-00-0f-44-01-bf-60	10.194.172.124	00:0f:44:01:bf:60	DMP-4310	SE 2.2.1	02/13/11 06:21:30 AM

General

DMP MAC Address: 00:0f:44:01:b6:c3
Dynamic IP Addressing (DHCP): Enabled
IP Address: 10.194.172.122
Subnet Mask: 255.255.255.0
Default Gateway: 10.194.172.1
Primary DNS Server:

Medianet Services

Medianet Enabled: yes
Timeout (ms): 30000
Switch IP Address: 10.194.172.1
Switch Name: Training_SW
Switch Port: GigabitEthernet0/5
VLAN: 10
Location ID: POD1
Location URL: 22=POD1&28=Cookie_Monster&27=2&25=C

Switch Port Civic Location

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#location civic-location identifier 1
Switch(config-civic)#? Type ? to see all the options of configuring the location.
Switch(config-civic)#additional-location-information POD1
Switch(config-civic)#building C
Switch(config-civic)#floor 2
Switch(config-civic)#room Cookie_Monster
Switch(config-civic)#end

Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int g0/5
Switch(config-if)#location civic-location-id 1
Switch(config-if)#end
```

The Role of Switch Port Civic Location

IOS civic location is a collection of labels that can be configured on each switch port, and then communicated to the DMP via LLDP. One use case for civic location is jack ID, hence allowing the DMP to learn what Ethernet jack it is connected to. The DMP reports any civic location information it learns back to Cisco Vision Dynamic Signage Director, where it can be retrieved and displayed by Cisco Vision Dynamic Signage Director as shown above.

The following example shows the civic location being configured and applied to interface gigabit Ethernet 0/5:

```
Switch#configure terminal

Enter configuration commands, one per line.    End with CNTL/Z.
```

```
Switch(config)#location civic-location identifier 1

Switch(config-civic)#? Type ? to see all the options of configuring the location.

Switch(config-civic)#additional-location-information POD1

Switch(config-civic)#building C Switch(config-civic)#floor 2 Switch(config-
civic)#room Cookie_Monster Switch(config-civic)#end


Switch#conf t

Enter configuration commands, one per line.     End with CNTL/Z.

Switch(config)#int g0/5

Switch(config-if)#location civic-location-id 1

Switch(config-if)#end
```

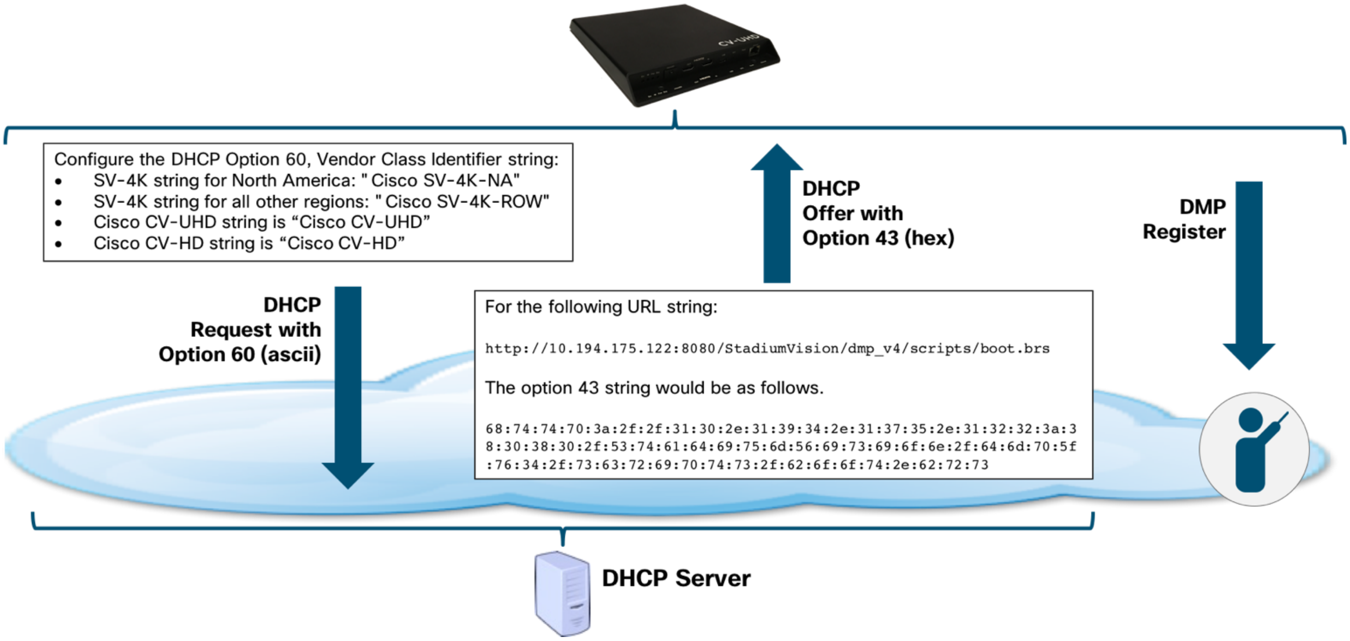
IOS civic location information can be viewed in the Management Dashboard and automatically link the DMP to its target Location in the Control Panel.

The Role of DHCP Options for DMP Auto-registration

The Cisco Digital Media Player (DMP) receives firmware and configuration from Cisco Vision Dynamic Signage Director. The DMP finds the Cisco Vision Dynamic Signage Director server through the use of DHCP options (specifically options 60 and 43). Option 60 is used to signal the digital media player that the option 43 content is meant for it to be received.

- If supporting a deployment with multiple DMP models (e.g., SV-4K, CV-UHD), you will need to configure an Option 60 string for each model.
- If the DHCP server is limited to a single Option 43 string per Option 60 per DHCP scope, then be sure to configure a separate VLAN & DHCP scope for each model of digital media player.

Figure 20 – DHCP and DMP Auto Registration



Configure the DHCP Option 60, Vendor Class Identifier string:

- SV-4K string for North America: " Cisco SV-4K-NA"
- SV-4K string for all other regions: " Cisco SV-4K-ROW"
- Cisco CV-UHD string is “Cisco CV-UHD”
- Cisco CV-HD string is “Cisco CV-HD”

For the following URL string:

```
http://10.194.175.122:8080/StadiumVision/dmp_v4/scripts/boot.brs
```

The option 43 string would be as follows.

```
68:74:74:70:3a:2f:2f:31:30:2e:31:39:34:2e:31:37:35:2e:31:32:32:3a:3
8:30:38:30:2f:53:74:61:64:69:75:6d:56:69:73:69:6f:6e:2f:64:6d:70:5f
:76:34:2f:73:63:72:69:70:74:73:2f:62:6f:6f:74:2e:62:72:73
```

The configuration steps are as follows:

1. Configure the DHCP Option 60, Vendor Class Identifier string:

    - SV-4K string for North America: "Cisco SV-4K-NA"
    - SV-4K string for all other regions: "Cisco SV-4K-ROW"
    - Cisco CV-UHD string is “Cisco CV-UHD”
    - Cisco CV-HD sting is “Cisco CV-HD”

2. Configure the converted DHCP Option 43, Vendor Specific Option URL:

Note - The option 43 string must be converted to TLV format for compatibility.

The DMP requires type-length-value (TLV) format for the data string. Specifically, the TLV format is constructed in the following manner:

- The string is built using hex values.
- The string begins with a two-character hex representation of the option 43 Type (an option 43 sub-option).
- The second two-character hex representation is the length of the information string, expressed in the number of ASCII characters of the string.
- Following the length value, the ascii string is typed out by using the two-character hex representation of each character in the string.
- The type designation is type 85 (decimal), expressed as type 55 (hex).

For the following URL string:

```
http://10.194.175.122:8080/StadiumVision/dmp_v4/scripts/boot.brs
```

The option 43 string would be as follows.

Hint: Use an ascii-to-hex conversion tool to simplify creating the hex string.

```
68:74:74:70:3a:2f:2f:31:30:2e:31:39:34:2e:31:37:35:2e:31:32:32:3a:38:30:38:30:2f:53:
74:61:64:69:75:6d:56:69:73:69:6f:6e:2f:64:6d:70:5f:76:34:2f:73:63:72:69:70:74:73:2f:
62:6f:6f:74:2e:62:72:73
```

Next, you place in front <decimal type code>:<decimal number of characters in the string>

Note - In Microsoft Word, you can carefully highlight the string and then click Tools>Word Count to get the number of characters in the string.

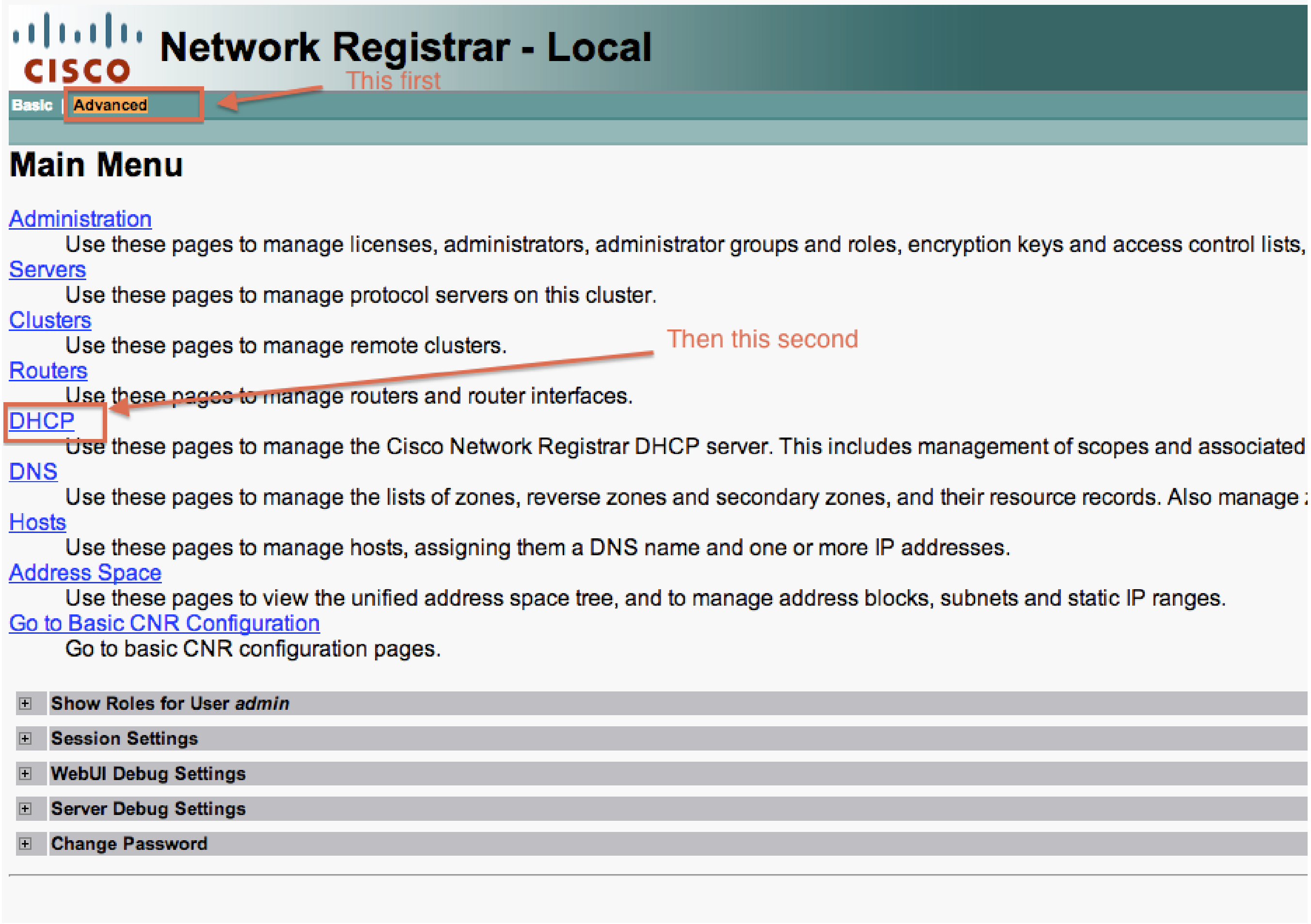
The type code is 55 in hex and in the above URL example, there's 64 characters in the string. Decimal 64 is equal to 40 in hex.

```
55:40:68:74:74:70:3a:2f:2f:31:30:2e:31:39:34:2e:31:37:35:2e:31:32:32:3a:38:30:38:30:
2f:53:74:61:64:69:75:6d:56:69:73:69:6f:6e:2f:64:6d:70:5f:76:34:2f:73:63:72:69:70:74:
73:2f:62:6f:6f:74:2e:62:72:73
```

Configuring DHCP Options in Cisco Network Registrar

1. Log in to CNR, select Advanced, then DHCP as shown below.

Figure 21 – Cisco Network Registrar Advanced Mode



Network Registrar - Local

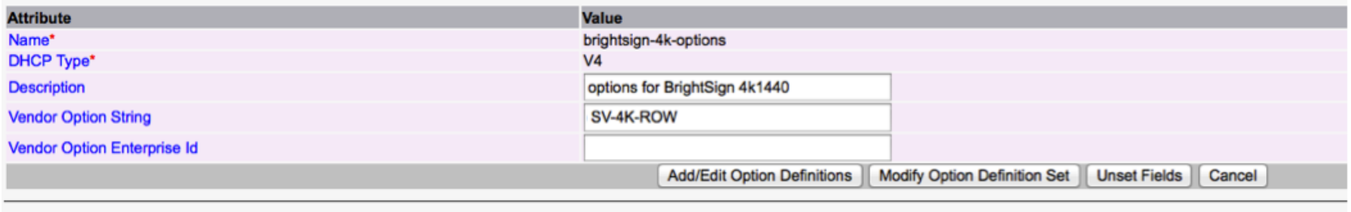
Main Menu

Administration
Use these pages to manage licenses, administrators, administrator groups and roles, encryption keys and access control lists,
Servers
Use these pages to manage protocol servers on this cluster.
Clusters
Use these pages to manage remote clusters.
Routers
Use these pages to manage routers and router interfaces.
DHCP
Use these pages to manage the Cisco Network Registrar DHCP server. This includes management of scopes and associated
DNS
Use these pages to manage the lists of zones, reverse zones and secondary zones, and their resource records. Also manage :
Hosts
Use these pages to manage hosts, assigning them a DNS name and one or more IP addresses.
Address Space
Use these pages to view the unified address space tree, and to manage address blocks, subnets and static IP ranges.
Go to Basic CNR Configuration
Go to basic CNR configuration pages.

2. Select the Options settings, then Add a New Option.

Attribute	Value	Comment
Name	SV-4K Options	could be anything
DHCP Type	V4	
Description	options for DMP	could be anything
Vendor Option String	Cisco SV-4K-NA	If DMP model is "NA"

Figure 22 – Cisco Network Registrar Vendor Option String



Attribute	Value
Name*	brightsign-4k-options
DHCP Type*	V4
Description	options for BrightSign 4k1440
Vendor Option String	SV-4K-ROW
Vendor Option Enterprise Id	

Note - You won't be able to create multiple options for same Vendor Option String.

3. Click Add Option Definition Set, then specify the option 43 value type you need.

4. Click the name you previously created, then Add/Edit Option Definitions.

5. On next display, click Add Option Definitions.

Number	43	
Name	brightsign-4k-option-43	could be anything
Description	option 43 items for DMP	could be anything
type	binary	
repeat	[0]	

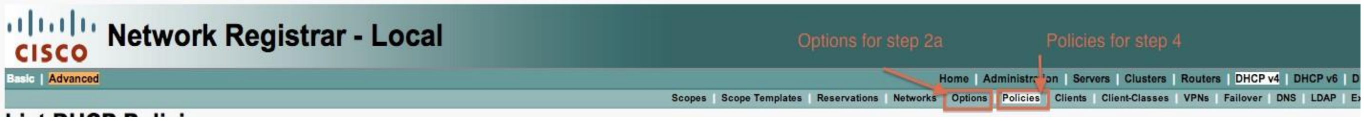
6. Click Add Option Definition.

7. Click Modify Option Definition Set.

Note - If you don't click Modify Option Definition Set here, it won't be saved.

8. Assign the new option to the right policies.

Figure 23 – Cisco Network Registrar Options and Policies



Network Registrar - Local
Options for step 2a
Policies for step 4
Basic | Advanced
Home | Administration | Servers | Clusters | Routers | DHCP v4 | DHCP v6 | D
Scopes | Scope Templates | Reservations | Networks | Options | Policies | Clients | Client-Classes | VPNs | Failover | DNS | LDAP | E

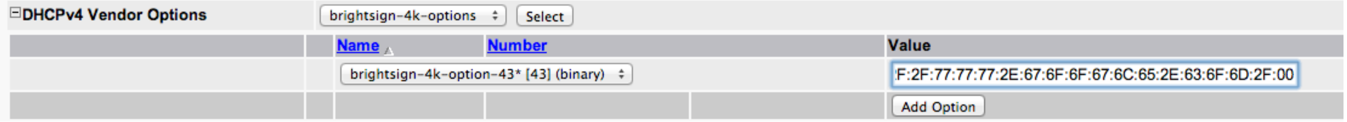
9. Click Policies in the upper menu (2nd level) and select a policy from the list.

10. Under DHCPv4 Vendor Options, select the appropriate name you created in the steps above, then click Select.

11. In the second dropdown, select the name you created.

12. Paste the option 43 binary field computed above into the "Value" field.

Figure 24 – Cisco Network Registrar DHCPv4 Vendor Options



DHCPv4 Vendor Options: brightsign-4k-options

Name: brightsign-4k-option-43* [43] (binary)

Value: F:2F:77:77:77:2E:67:6F:6F:67:6C:65:2E:63:6F:6D:2F:00

13. Click Add Option.

14. Click Modify Policy at the bottom of the display.

Note - If you don't click Modify Policy, your change will not be saved.

Configuring DHCP Options in Cisco Switch

Note - An IOS Switch is not recommended as a production DHCP server for a venue. This example is provided to allow for simple DHCP support for DMPs primarily used for testing and in a lab.

Note - If an IOS DHCP Server is used for IP address allocation for DMPs in a production network, we strongly recommend using database agents to maintain the DMP address bindings in case the switch is rebooted. See IP Addressing: DHCP Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) for more information.

In this example, a Cisco IOS DHCP is being used, which only supports a single pairing of options 60 and 43 within a single scope. This example only provides the procedure for the SV-4K media player.

Switch Configuration Example

```
! DHCP Database Agent CLI example

ip dhcp database ftp://user:password@172.16.4.253/router-dhcp write-delay 120

!

ip dhcp pool SV-4K

network 10.10.1.0 255.255.255.0

default-router 10.10.1.1

option 60 ascii Cisco SV-4K-NA

option 43 hex
5540.6874.7470.3A2F.2F31.302E.3139.342E.3137.352E.3132.323A.3830.3830.2F53.7461.6469
.756D.5669.7369.6F6E.2F64.6D70.5F76.342F.7363.7269.7074.732F.626F.6F74.2E62.7273
```

Note - Some IOS versions may require the text enclosed in quotes "Cisco SV-4K-ROW". If the IOS doesn't accept a leading quote in the string, then quotations are not needed.

Note - The periods in the option 43 string are automatically created by the IOS and ARE NOT TYPED when creating the ASCII string.

Troubleshooting DHCP

There are a few things to look for and tools to use when troubleshooting if DHCP is working properly.

1. If the DMP is not getting an IP address or looks like it's getting an IP address but you can't ping or login to the DMP's web interface then check the following.

    a. Verify you can reach the DHCP server by using ping.

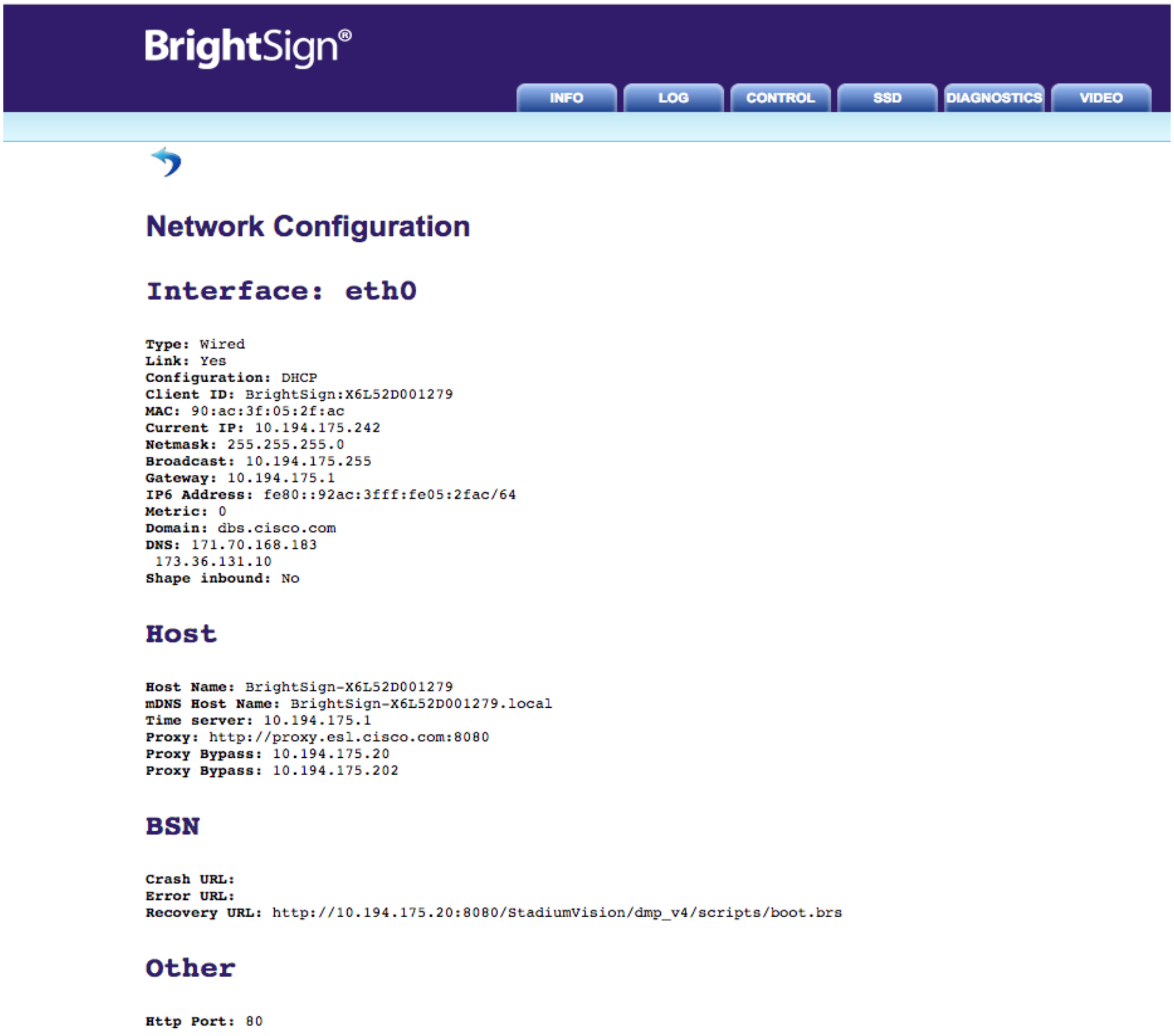
    b. Verify the DHCP server is configured to provide a default gateway.

    c. Verify the switch that provides the SVI (VLAN) interface has the ip helper-address (Catalyst) or ip dhcp relay (Nexus) commands configured.

2. If the DMP gets stuck at Network Recovery.

    a. Verify the DMP is using the correct Recovery URL retrieved during the DHCP process. Login to the DMP web UI and go to Diagnostics>Network Configuration.

Figure 25 – DMP Network Configuration Screen



Network Configuration

Interface: eth0

```
Type: Wired
Link: Yes
Configuration: DHCP
Client ID: BrightSign:X6L52D001279
MAC: 90:ac:3f:05:2f:ac
Current IP: 10.194.175.242
Netmask: 255.255.255.0
Broadcast: 10.194.175.255
Gateway: 10.194.175.1
IP6 Address: fe80::92ac:3fff:fe05:2fac/64
Metric: 0
Domain: dbs.cisco.com
DNS: 171.70.168.183
 173.36.131.10
Shape inbound: No
```

Host

```
Host Name: BrightSign-X6L52D001279
mDNS Host Name: BrightSign-X6L52D001279.local
Time server: 10.194.175.1
Proxy: http://proxy.esl.cisco.com:8080
Proxy Bypass: 10.194.175.20
Proxy Bypass: 10.194.175.202
```

BSN

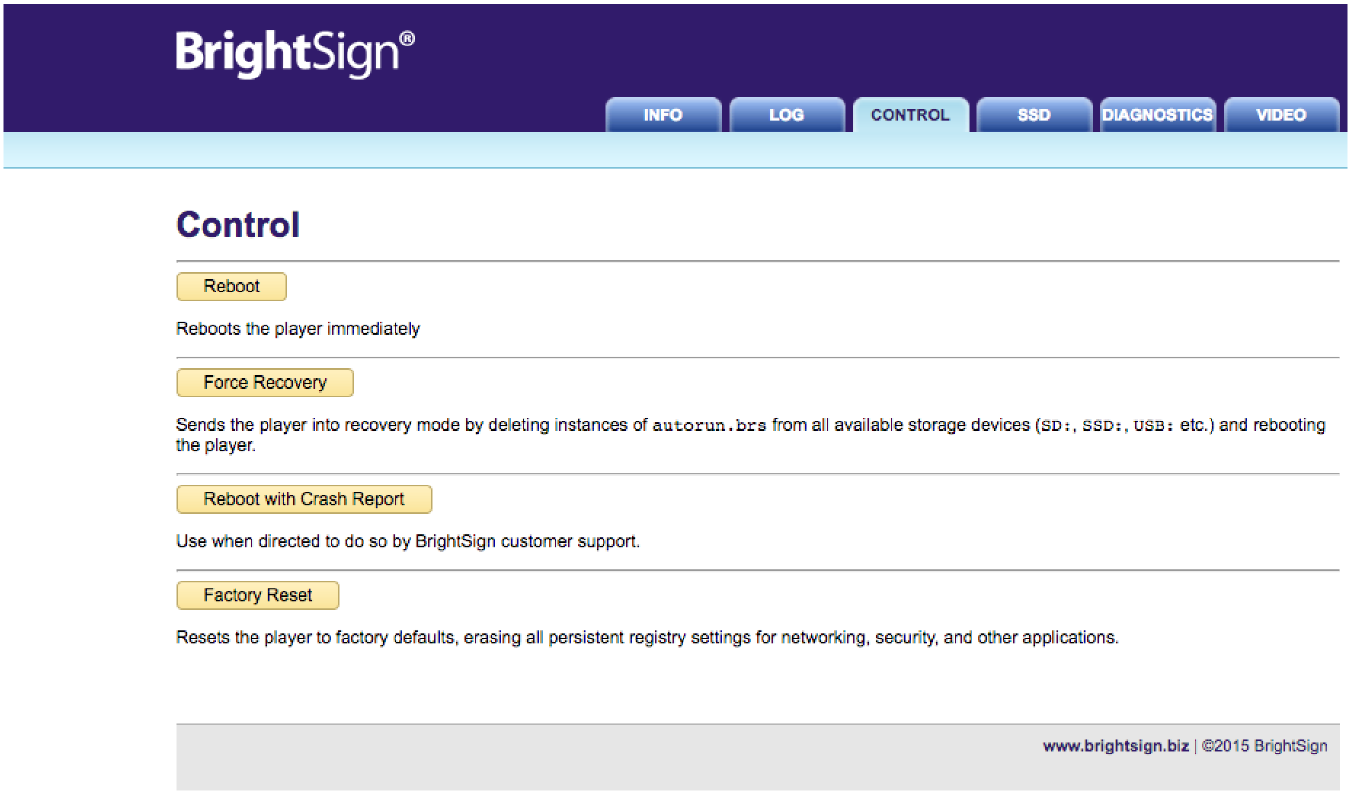
```
Crash URL:
Error URL:
Recovery URL: http://10.194.175.20:8080/StadiumVision/dmp_v4/scripts/boot.brs
```

Other

```
Http Port: 80
```

b. If the DMP appears to be getting an IP address, default gateway, and it's using the correct URL and is still not registering with Cisco Vision Dynamic Signage Director then do a Factory Reset via the DMP's web UI under the Control Tab.

Figure 26 – DMP Network Configuration Screen



Control

Reboots the player immediately

Sends the player into recovery mode by deleting instances of `autorun.brs` from all available storage devices (`SD:`, `SSD:`, `USB:` etc.) and rebooting the player.

Use when directed to do so by BrightSign customer support.

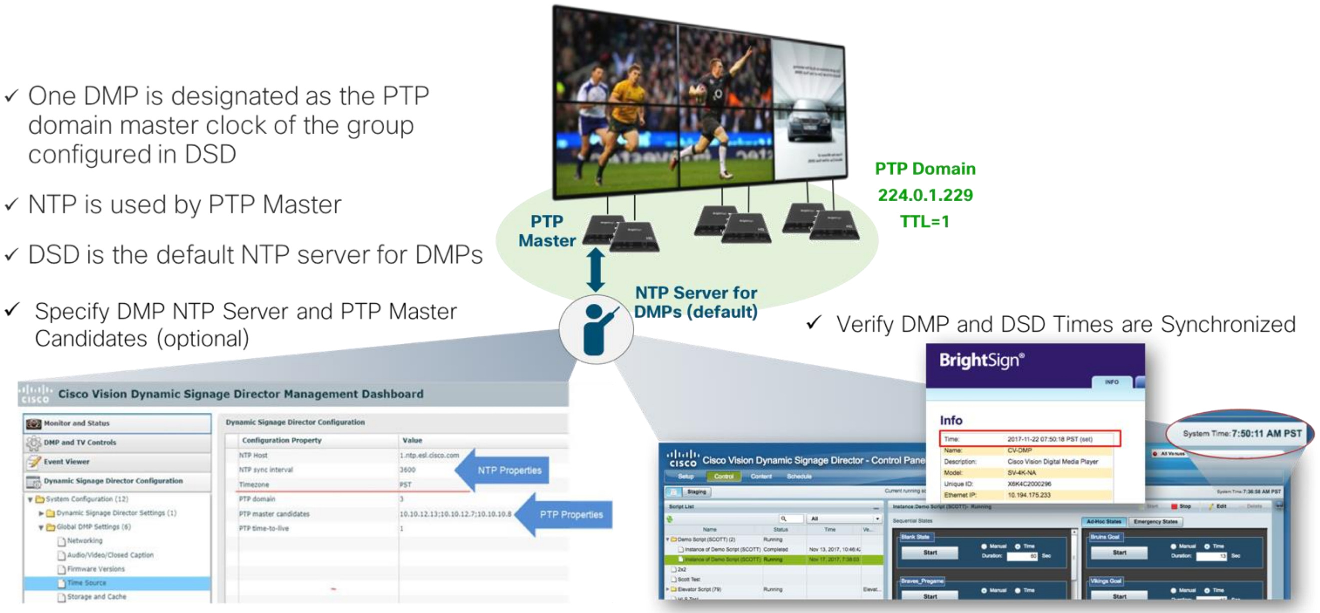
Resets the player to factory defaults, erasing all persistent registry settings for networking, security, and other applications.

www.brightsign.biz | ©2015 BrightSign

The Role of NTP and PTP for Synchronization

NTP provides reliable clocking for your Cisco Vision network and helps ensure synchronicity between redundant servers and between the Cisco Vision Dynamic Signage Director and the DMPs. The IEEE 1588 Precision Time Protocol (PTP) is used between DMPs.

Figure 27 – The Role of NTP and PTP for Synchronization



- ✓ One DMP is designated as the PTP domain master clock of the group configured in DSD
- ✓ NTP is used by PTP Master
- ✓ DSD is the default NTP server for DMPs
- ✓ Specify DMP NTP Server and PTP Master Candidates (optional)
- ✓ Verify DMP and DSD Times are Synchronized

PTP Domain
224.0.1.229
TTL=1
PTP Master
NTP Server for DMPs (default)
Cisco Vision Dynamic Signage Director Management Dashboard
Monitor and Status
DMP and TV Controls
Event Viewer
Dynamic Signage Director Configuration
System Configuration (12)
Dynamic Signage Director Settings (1)
Global DMP Settings (6)
Networking
Audio/Video/Closed Caption
Firmware Versions
Time Source
Storage and Cache
NTP Properties
PTP Properties
BrightSign®
INFO
Cisco Vision Dynamic Signage Director - Control Pane
System Time: 7:50:11 AM PST

Dynamic Signage Director Configuration

Configuration Property	Value
NTP Host	1.ntp.esl.cisco.com
NTP sync interval	3600
Timezone	PST
PTP domain	3
PTP master candidates	10.10.12.13;10.10.12.7;10.10.10.8
PTP time-to-live	1

Info

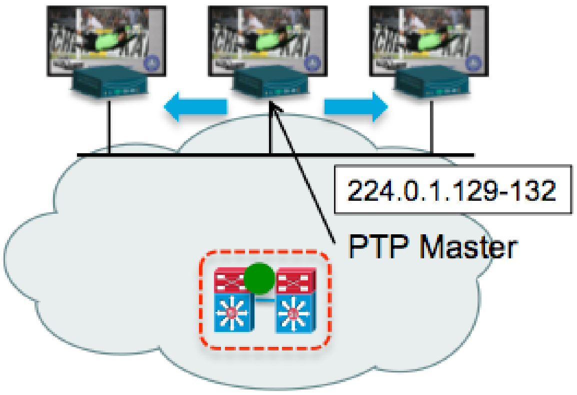
Time:	2017-11-22 07:50:18 PST (set)
Name:	CV-DMP
Description:	Cisco Vision Digital Media Player
Model:	SV-4K-NA
Unique ID:	X6K4C2000296
Ethernet IP:	10.194.175.233

Overview

The IEEE 1588 Precision Time Protocol (PTP) is a configurable synchronization option to synchronize clocks among Series 2 and 3 DMPS driving the display of time-critical content like for video walls.

Figure 28 – SV-4K PTP Synchronization

SV-4K PTP MC



Precision Time Protocol (PTP) is used to synchronize DMPs. The DMPs default of TTL = 1 restricts MC from propagating beyond the local VLAN.

When using PTP, one DMP is designated as the domain master clock. It will synchronize with a Network Time Protocol (NTP) reference clock and then act as the reference point for a set (also known as a domain) of slave DMP clocks. The protocol provides the means for slave DMPs to determine the path delay incurred from the master to themselves. This time delay is then incorporated in the slave's time to allow for highly precise time synchronization to the master DMP clock.

IEEE-1588 PTP uses multicast messages for communication with the following addresses

224.0.1.107

224.0.1.129 – Default Domain 0

224.0.1.130 – Alternate Domain 1

224.0.1.131 – Alternate Domain 2

224.0.1.132 – Alternate Domain 3

> **Note** - The DMPs use a TTL of 1 default, meaning PTP multicast is confined to the local subnet or VLAN. The TTL may be changed to greater than 1 to traverse a number of layer 3 hops. Careful consideration should be used when configuring TTL > 1 to traverse multiple hops due to the increased latency incurred. This may negatively affect synchronization. Also, the multicast routing in the network must be configured for the PTP group addresses mentioned above.

Configuring NTP on Cisco Vision Dynamic Signage Director Servers

Use the check-list below to understand the requirements and caveats for provisioning Cisco Vision Dynamic Signage Director servers and DMPs to use NTP and PTP for synchronization.

- Network Time Protocol (NTP) service is required in Cisco Vision Solution on the following devices:
  - Cisco Vision Dynamic Signage Director servers
  - Series 2 (SV-2K, SV-4K) and Series 3 (CV-HD, CV-UHD) that are the Precision Time Protocol (PTP) master device

- By default, both NTP and PTP services are automatically enabled for Series 2 and Series 3 media players.
- An NTP source also must be used to provide initial clocking to the devices that are elected PTP masters in the network.
- Only the DMP PTP masters derive a clock using NTP.
- The Cisco Vision Dynamic Signage Director server's default NTP source is a Red Hat Linux public pool. This setting may be changed to your preferred NTP source. A configuration change is performed in the Cisco Vision Dynamic Signage Director Management Dashboard and subsequently pushed to the DMPs upon reboot of both the server and then the DMPs.
- The Cisco Vision Dynamic Signage Director server is preconfigured as the NTP source for the DMPs.
- Do not use Cisco Vision Dynamic Signage Director as an NTP source for other devices in your network.
- If deploying Cisco Vision Dynamic Signage Director as a virtual machine, configure Director to use a reliable NTP server running on a bare metal server rather than a source from the local VM environment.

- Verify Cisco Vision Dynamic Signage Director and DMPs can reach the NTP source
- The DMP must not reference an NTP server pool. If the Cisco Vision Dynamic Signage Director server references an NTP server pool (the default) and you choose to not use the Director as the DMP's NTP source, then select a specific server from that same pool as the NTP server for the DMPs.
- Only IPv4 is supported for the NTP server address on the DMPs.
- The NTP server for the DMPs must not be a load-balanced server.
- The Cisco Vision Dynamic Signage Director network must be configured to allow bidirectional transmission of UDP messages on port 123 for NTP messages between the NTP source and DMPs.

Note - For a complete port reference for Cisco Vision Dynamic Signage Director servers, see the "Port Reference" module of the Cisco Vision Software Installation and Upgrade Guide: Dynamic Signage Director for your release.

Configuring the System Date and Time

When you install or upgrade the Cisco Vision Dynamic Signage Director, you need to configure the system date, time and time zone in the TUI.

Note - Although you can manually configure the system date and time on your servers when necessary, this should be avoided for your production network. NTP should be used.

Note - Cisco Vision Dynamic Signage Director servers is configured the following Red Hat Linux public pool of servers as the default NTP sources.

server 0.rhel.pool.ntp.org

server 1.rhel.pool.ntp.org

server 2.rhel.pool.ntp.org

If you choose to configure another NTP server. These server entries in the ntp.conf file must be commented out.

To set up the NTP source on Cisco Vision Dynamic Signage Director servers, complete the following steps:

1. From the TUI Main Menu, go to System Settings > Date and Time Settings > Setup NTP Source. A confirmation screen to Configure NTP and edit the ntp.conf file is displayed.
2. To open the ntp.conf file for edit, press any key. The ntp.conf file opens in the vi editor and the cursor is positioned at the end of the last configured NTP server line. If this is not the case, navigate to the server configuration section.
3. To enter INSERT line editing mode, type i. The vi editor changes to INSERT mode.
4. If you have a server that you prefer to use insert those servers and comment out the default servers.
5. To exit INSERT mode, press the Esc. key.
6. To save your changes, type: wq

The configuration is saved and the ntpd service is restarted. Verify that you see the "OK" confirmation that the ntpd has started.

7. To return to the Date and Time Settings menu, press any key.

Configuring the Time Zone

Configuring the time zone is required for the Cisco Vision Dynamic Signage Director server.

> **Note** - Although there is an option to set the time zone in the Venues interface of the Control Panel on the Cisco Vision Dynamic Signage Director server, this option is only informational and is used for proof-of-play reporting.

This section includes the following tasks:

- Finding the Time Zone Code for System Configuration (optional)
- Configuring the System Time Zone (required)

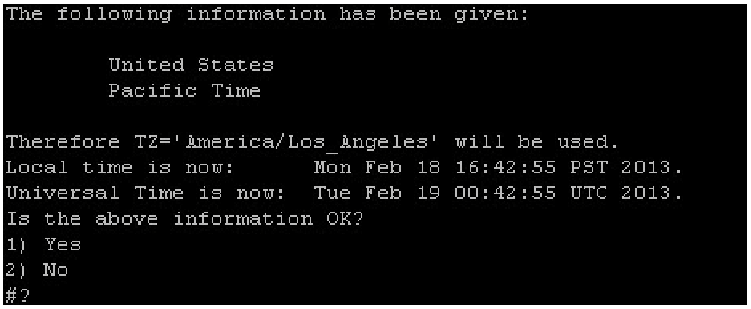
Finding the Time Zone Code for System Configuration (optional)

> **Note** - This task provides information only and does not actually configure the time zone.

To find the time zone code for system configuration, complete the following steps:

1. From the Date and Time Settings menu, do the following:
2. Select Change Timezone.
3. Type the number that corresponds to the applicable continent or ocean for the location of the server.
4. Type the number that corresponds to the country.
5. Type the number for the time zone (as applicable).
6. When the confirmation of the time zone information that you configured is displayed, type 1 (for Yes) to accept your settings, or 2 (for No) to cancel.

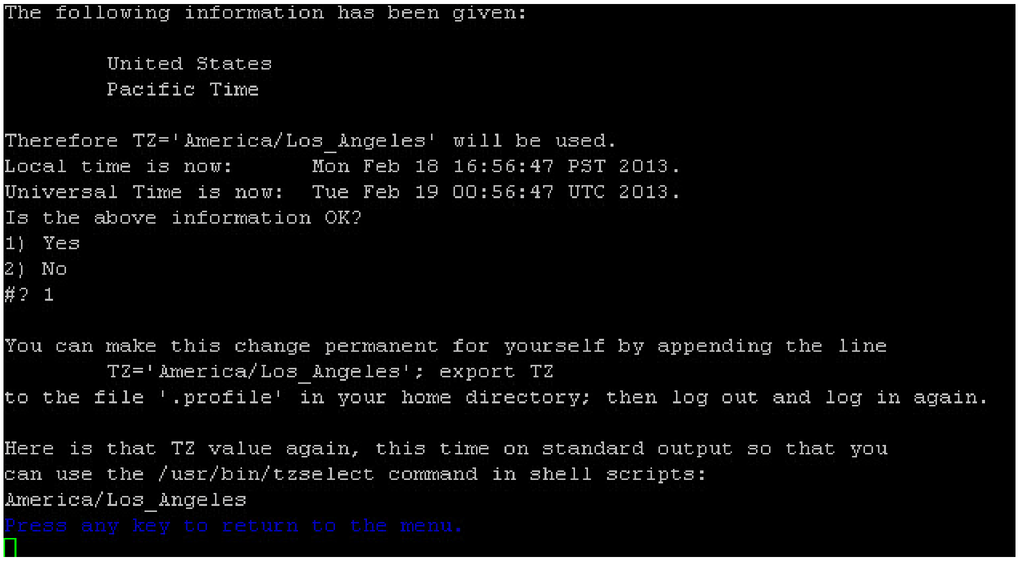
Figure 29 – Time Zone Confirmation Prompt



```
The following information has been given:

        United States
        Pacific Time

Therefore TZ='America/Los_Angeles' will be used.
Local time is now:      Mon Feb 18 16:42:55 PST 2013.
Universal Time is now:  Tue Feb 19 00:42:55 UTC 2013.
Is the above information OK?
1) Yes
2) No
#?
```

7. After confirming Yes at the prompt, copy the timezone string that is provided.

Figure 30 – Sample Time Zone Code



```
The following information has been given:

        United States
        Pacific Time

Therefore TZ='America/Los_Angeles' will be used.
Local time is now:      Mon Feb 18 16:56:47 PST 2013.
Universal Time is now:  Tue Feb 19 00:56:47 UTC 2013.
Is the above information OK?
1) Yes
2) No
#? 1

You can make this change permanent for yourself by appending the line
        TZ='America/Los_Angeles'; export TZ
to the file '.profile' in your home directory; then log out and log in again.

Here is that TZ value again, this time on standard output so that you
can use the /usr/bin/tzselect command in shell scripts:
America/Los_Angeles
Press any key to return to the menu.
```

8. Press any key to return to the Date and Time Settings menu.

9. Next, configure the system time zone using the appropriate code for the server location shown below.

Configuring the System Time Zone

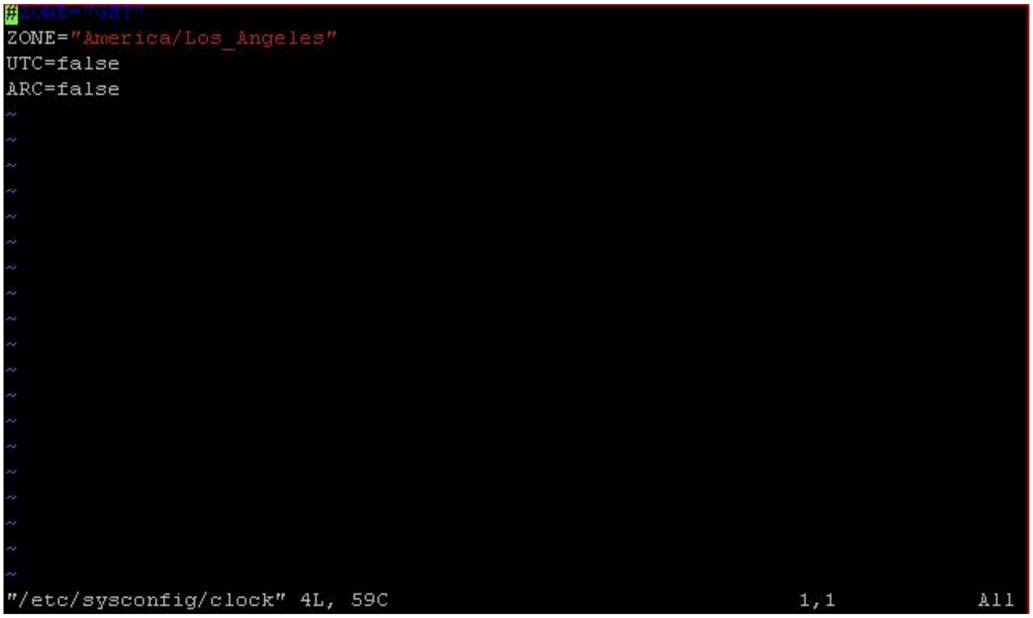
10. From the TUI Main Menu on the server, go to System Settings > Date and Time Settings > Change System Timezone.

11. At the prompt to edit the system clock file, press any key to continue.   The /etc/sysconfig/clock file is opened for editing.

12. Use the vi editor to specify your time zone. The diagram below shows an example using the entry for the "America/Los_Angeles" time zone.

Note - The quotation marks and underscore symbols are required.

Figure 31 – Editing the Clock File



```
#ZONE="GMT"
ZONE="America/Los_Angeles"
UTC=false
ARC=false
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/sysconfig/clock" 4L, 59C                                1,1           All
```

13. To exit INSERT mode, press the Esc. key.

14. To save your changes, type :wq!

    The configuration is saved and the ntpd service is restarted. Verify that you see the “OK” confirmation that the ntpd has started.

15. To return to the Date and Time Settings menu, press any key.

16. Restart the server to put the time zone changes into effect. Restarting the Cisco Vision Dynamic Signage Director Software

a. From the TUI Main Menu on the server, go to: Cisco Vision Server Administration > Restart Cisco Vision Dynamic Signage Director software.

b. When the prompt appears, press any key to return to the Server Administration menu.

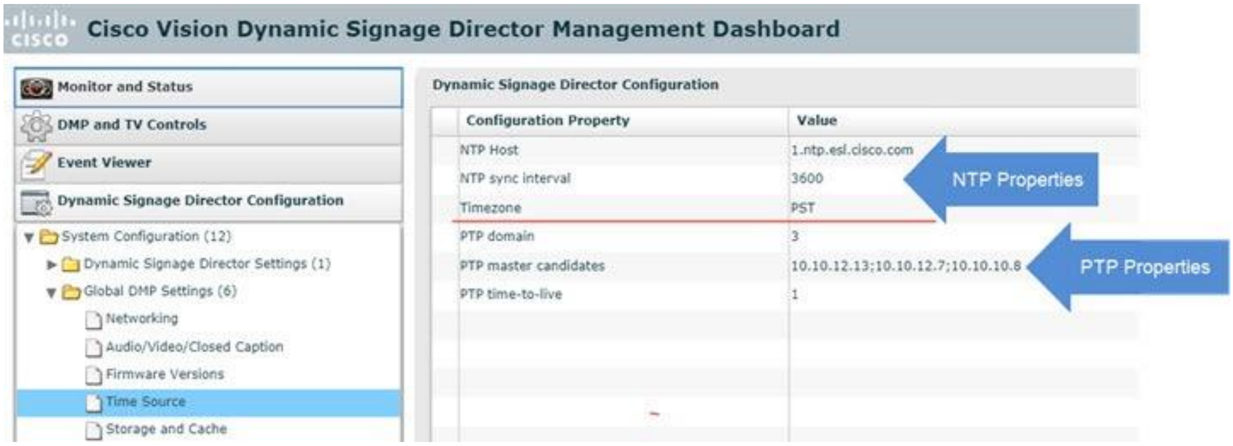
c. Return to the Main Menu and exit the TUI.

Configuring NTP and PTP on the Digital Media Players

To modify the standard NTP and PTP configuration on all Series 2 and Series 3 DMPs, complete the following steps:

1. Log into the Cisco Vision Dynamic Signage Director server as an administrator.
2. Go to the Management Dashboard.
3. Go to Dynamic Signage Director Configuration > System Configuration > Global DMP Settings > Time Source

Figure 32 – Global DMP Settings for NTP and PTP on the Series 2 and Series 3



Cisco Vision Dynamic Signage Director Management Dashboard
Monitor and Status
DMP and TV Controls
Event Viewer
Dynamic Signage Director Configuration
System Configuration (12)
Dynamic Signage Director Settings (1)
Global DMP Settings (6)
Networking
Audio/Video/Closed Caption
Firmware Versions
Time Source
Storage and Cache
Dynamic Signage Director Configuration
NTP Properties
PTP Properties

Configuration Property	Value
NTP Host	1.ntp.esl.cisco.com
NTP sync interval	3600
Timezone	PST
PTP domain	3
PTP master candidates	10.10.12.13;10.10.12.7;10.10.10.8
PTP time-to-live	1

4. (Optional) Change the global PTP properties as required for your network.

   For reference, the PTP domains are as follows:

   224.0.1.129 – Default Domain 0

   224.0.1.130 – Alternate Domain 1

   224.0.1.131 – Alternate Domain 2

   224.0.1.132 – Alternate Domain 3

Note - The PTP Domain may need to be changed if the Default Domain 0 is used by other applications (e.g., QSC network audio).

5. Optional) Change the global NTP properties as required for your environment.

Note - The default is the Director's IP address. If you change the NTP host, only put a single host entry.

6. Click the disk icon to Save changes.
7. Reboot the DMPs.

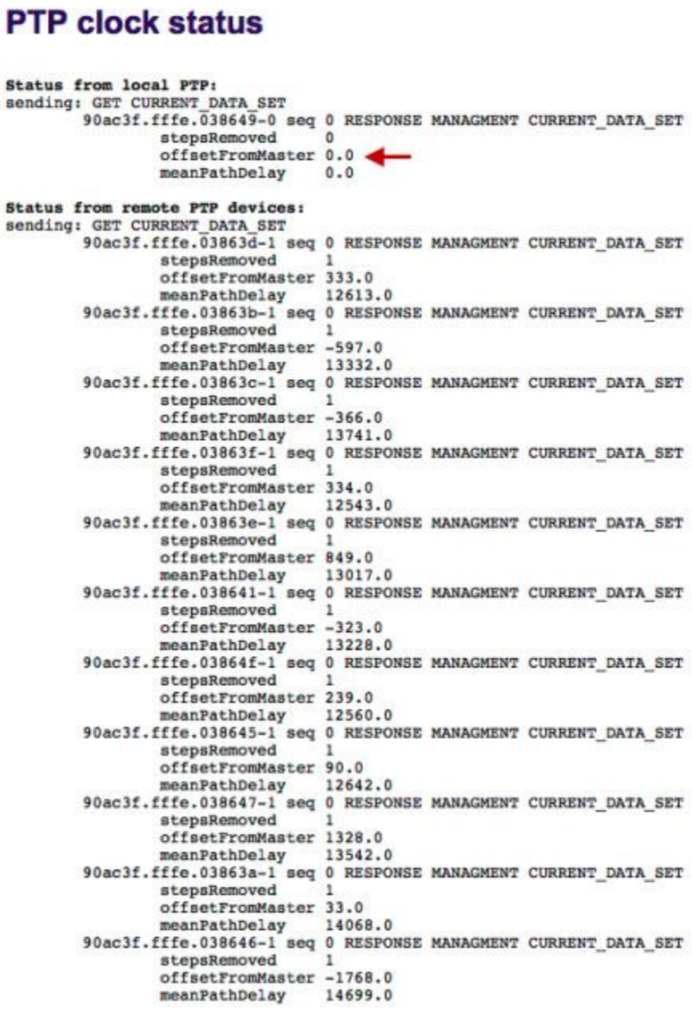
Verifying PTP Operation

This section describes how to verify the PTP configuration and also the operation of PTP for your Series 2 and Series 3 DMPs.

8. Open your browser and navigate to one of the DMPs: http://DMP-ip-address/ptp.html

9. Identify the PTP master by finding the unit that has an "offsetFromMaster" value of 0.0.

Figure 33 – Successful PTP Clock Operation

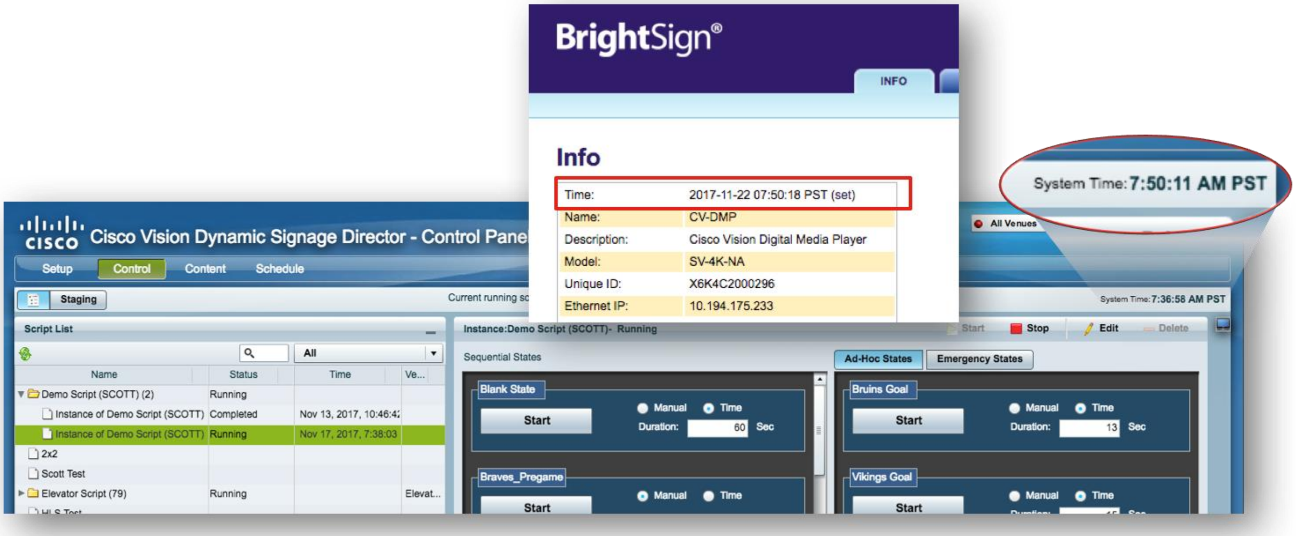


PTP clock status

```
Status from local PTP:
sending: GET CURRENT_DATA_SET
        90ac3f.fffe.038649-0 seq 0 RESPONSE MANAGMENT CURRENT_DATA_SET
                stepsRemoved     0
                offsetFromMaster 0.0
                meanPathDelay    0.0

Status from remote PTP devices:
sending: GET CURRENT_DATA_SET
        90ac3f.fffe.03863d-1 seq 0 RESPONSE MANAGMENT CURRENT_DATA_SET
                stepsRemoved     1
                offsetFromMaster 333.0
                meanPathDelay    12613.0
        90ac3f.fffe.03863b-1 seq 0 RESPONSE MANAGMENT CURRENT_DATA_SET
                stepsRemoved     1
                offsetFromMaster -597.0
                meanPathDelay    13332.0
        90ac3f.fffe.03863c-1 seq 0 RESPONSE MANAGMENT CURRENT_DATA_SET
                stepsRemoved     1
                offsetFromMaster -366.0
                meanPathDelay    13741.0
        90ac3f.fffe.03863f-1 seq 0 RESPONSE MANAGMENT CURRENT_DATA_SET
                stepsRemoved     1
                offsetFromMaster 334.0
                meanPathDelay    12543.0
        90ac3f.fffe.03863e-1 seq 0 RESPONSE MANAGMENT CURRENT_DATA_SET
                stepsRemoved     1
                offsetFromMaster 849.0
                meanPathDelay    13017.0
        90ac3f.fffe.038641-1 seq 0 RESPONSE MANAGMENT CURRENT_DATA_SET
                stepsRemoved     1
                offsetFromMaster -323.0
                meanPathDelay    13228.0
        90ac3f.fffe.03864f-1 seq 0 RESPONSE MANAGMENT CURRENT_DATA_SET
                stepsRemoved     1
                offsetFromMaster 239.0
                meanPathDelay    12560.0
        90ac3f.fffe.038645-1 seq 0 RESPONSE MANAGMENT CURRENT_DATA_SET
                stepsRemoved     1
                offsetFromMaster 90.0
                meanPathDelay    12642.0
        90ac3f.fffe.038647-1 seq 0 RESPONSE MANAGMENT CURRENT_DATA_SET
                stepsRemoved     1
                offsetFromMaster 1328.0
                meanPathDelay    13542.0
        90ac3f.fffe.03863a-1 seq 0 RESPONSE MANAGMENT CURRENT_DATA_SET
                stepsRemoved     1
                offsetFromMaster 33.0
                meanPathDelay    14068.0
        90ac3f.fffe.038646-1 seq 0 RESPONSE MANAGMENT CURRENT_DATA_SET
                stepsRemoved     1
                offsetFromMaster -1768.0
                meanPathDelay    14699.0
```

10. Verify the Cisco Vision Dynamic Signage Director's System Time matches that on the DMP. Go to the Event Management>Control Panel>Control and the DMP web UI Info Tab to verify the times match.

Figure 34 – Verify Cisco Vision Dynamic Signage Director and DMP Time



Info

Time:	2017-11-22 07:50:18 PST (set)
Name:	CV-DMP
Description:	Cisco Vision Digital Media Player
Model:	SV-4K-NA
Unique ID:	X6K4C2000296
Ethernet IP:	10.194.175.233

System Time: 7:50:11 AM PST

System Time: 7:36:58 AM PST

Script List

Name	Status	Time	Ve...
Demo Script (SCOTT) (2)	Running		
Instance of Demo Script (SCOTT)	Completed	Nov 13, 2017, 10:46:4:	
Instance of Demo Script (SCOTT)	Running	Nov 17, 2017, 7:38:03	
2x2			
Scott Test			
Elevator Script (79)	Running		Elevat...

Instance:Demo Script (SCOTT)- Running

Blank State — Duration: 60 Sec

Bruins Goal — Duration: 13 Sec

Switch Configuration Example

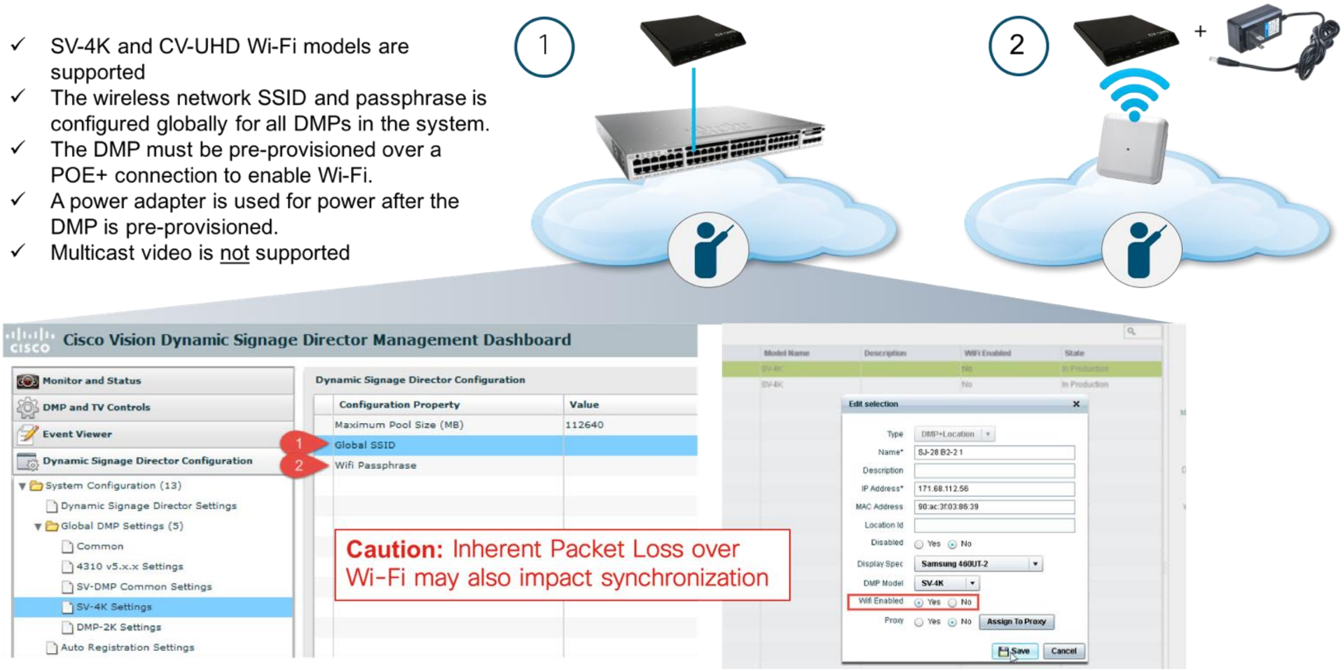
```
interface range GigabitEthernet1/0/x - y
 description SV-DMP Port
 switchport mode access
 switchport access vlan 110
 service-policy input CISCO-SV-DMP
!
ip access-list extended IEEE-1588
 remark PTP for DMPs and Audio Systems
 permit udp any host 224.0.1.129
 permit udp any host 224.0.1.130
 permit udp any host 224.0.1.131
 permit udp any host 224.0.1.132
!
ip access-list extended DMP-AS-A-VIDEO-SOURCE
 remark ACL used to mark a SV-4K sourced video stream
 permit udp <DMP Subnet/xx> host <239.193.20.x>
!
```

```
table-map policed-dscp
 map from 0 to 8
 map from 10 to 8
 map from 18 to 8
 map from 24 to 8
 map from 46 to 8
!
class-map match-any IEEE-1588
 match access-group name IEEE-1588
class-map match-any DMP-AS-A-VIDEO-SOURCE
 match access-group name DMP-AS-A-VIDEO-SOURCE
!
policy-map CISCO-SV-DMP
 class IEEE-1588
  set dscp ef
   police cir 1000000 bc 300000
   conform-action transmit
   exceed-action set-dscp-transmit dscp table policed-dscp
 class DMP-AS-A-VIDEO-SOURCE
  set dscp cs5
   police cir 25000000 bc 5000000
   conform-action transmit
   exceed-action set-dscp-transmit dscp table policed-dscp
 class class-default
  set dscp default
```

Connecting the DMP to the Wi-Fi Network

The DMP can be connected to the network via Wi-Fi if you need to deploy the DMPs in areas where there is no existing Ethernet cabling, where it is difficult to run cabling, or simply as an alternative to Ethernet network connectivity.

Figure 35 – Connecting the DMP to the Wi-Fi Network Overview



- ✓ SV-4K and CV-UHD Wi-Fi models are supported
- ✓ The wireless network SSID and passphrase is configured globally for all DMPs in the system.
- ✓ The DMP must be pre-provisioned over a POE+ connection to enable Wi-Fi.
- ✓ A power adapter is used for power after the DMP is pre-provisioned.
- ✓ Multicast video is not supported

Cisco Vision Dynamic Signage Director Management Dashboard

Dynamic Signage Director Configuration

	Configuration Property	Value
	Maximum Pool Size (MB)	112640
1	Global SSID	
2	Wifi Passphrase	

Caution: Inherent Packet Loss over Wi-Fi may also impact synchronization

Model Name	Description	WiFi Enabled	State
SV-4K		No	In Production
SV-4K		No	In Production

Edit selection

Type: DMP+Location
Name*: SJ-28 B2-2 1
Description:
IP Address*: 171.68.112.56
MAC Address: 90:ac:3f:03:86:39
Location Id:
Disabled: ○ Yes ● No
Display Spec: Samsung 460UT-2
DMP Model: SV-4K
Wifi Enabled: ● Yes ○ No
Proxy: ○ Yes ● No

Use the check-list below to understand the requirements and caveats for provisioning a DMP to use Wi-Fi

- SV-4K and CV-UHD Wi-Fi models are supported
- Wi-Fi connected DMPs are supported in Cisco Vision Dynamic Signage Director Release 5.0 or later.
- Support for the following Wi-Fi standards: 802.11a, 802.11b, or 802.11n.
- The wireless network SSID and passphrase is configured globally for all Wi-Fi-capable DMPs in the system.
- The SV-4K firmware automatically tries to connect with WEP (if the passphrase is of a suitable length), WPA1 or WPA2.
- A Wi-Fi access point must be configured to support multicast.
- The DMP must be pre-provisioned over a POE+ connection to enable Wi-Fi.
- An DMP power adapter is used for power after the DMP is pre-provisioned.
- Multicast video is not supported due to bandwidth limitations and inherent packet loss over a wireless network.
- Due to packet loss over Wi-Fi, TV on/off multicast control messages maybe lost TV control commands like TV power on or off may not consistently work as expected.
- If a data feed using multicast is dropped, the DMP continues to show old data or no data if the first message is lost.

Configuring the DMP in Cisco Vision Dynamic Signage Director

1. Log in to Cisco Dynamic Signage Director as an administrator.
2. From the Management Dashboard, go to: Dynamic Signage Director Configuration > System Configuration > Global DMP Settings > SV-4K Settings

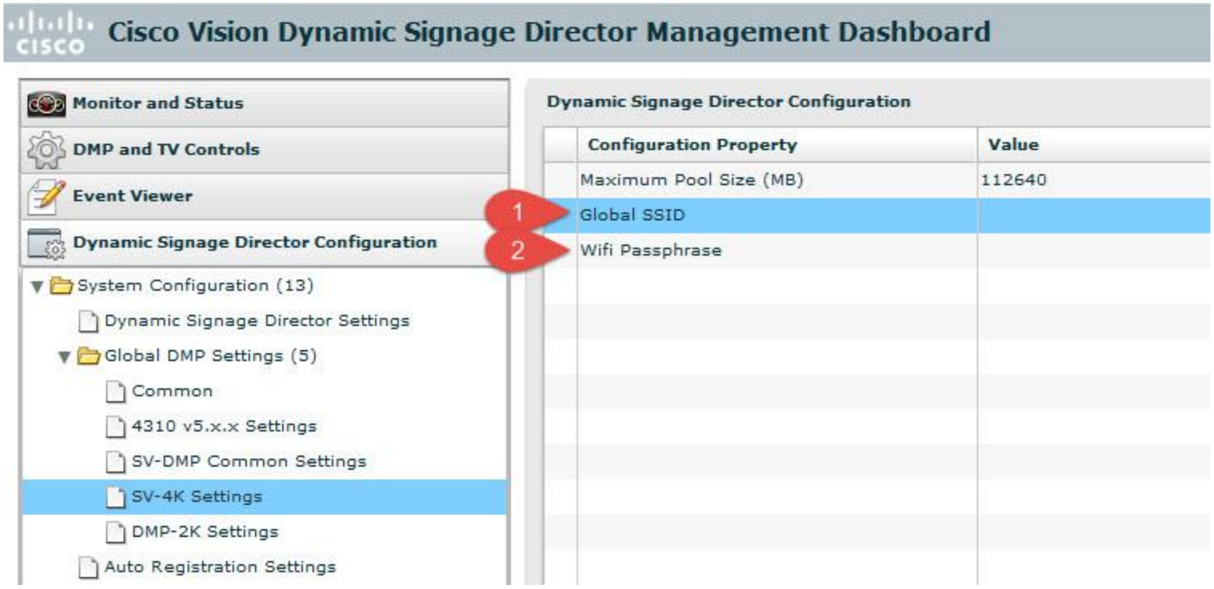
3. Specify the Global SSID and Wi-Fi Passphrase properties:

   a. Global SSID—Type the network SSID to be used by all SV-4Ks in the system that are using a Wi-Fi connection.

   b. Wi-Fi Passphrase—Type the WEP, WPA1, or WPA2 passphrase.

4. Save the configuration.

Figure 36 – SV-4K Wi-Fi Global SSID and Passphrase Configuration



Cisco Vision Dynamic Signage Director Management Dashboard

- Monitor and Status
- DMP and TV Controls
- Event Viewer
- Dynamic Signage Director Configuration
  - System Configuration (13)
    - Dynamic Signage Director Settings
    - Global DMP Settings (5)
      - Common
      - 4310 v5.x.x Settings
      - SV-DMP Common Settings
      - SV-4K Settings
      - DMP-2K Settings
    - Auto Registration Settings

Dynamic Signage Director Configuration

Configuration Property	Value
Maximum Pool Size (MB)	112640
Global SSID	
Wifi Passphrase	

5. Connect the SV-4K device using a hard-wired Ethernet PoE+ connection then do one of the following:

   a. If this is the initial setup of the DMP in Cisco Vision Dynamic Signage Director then provision the DMP according to the normal auto-registration process to download the required firmware and Wi-Fi credentials.

Note - These steps do not detail firmware configuration. Be sure that you have already specified the required firmware auto-registration settings for Cisco Vision Dynamic Signage Director.

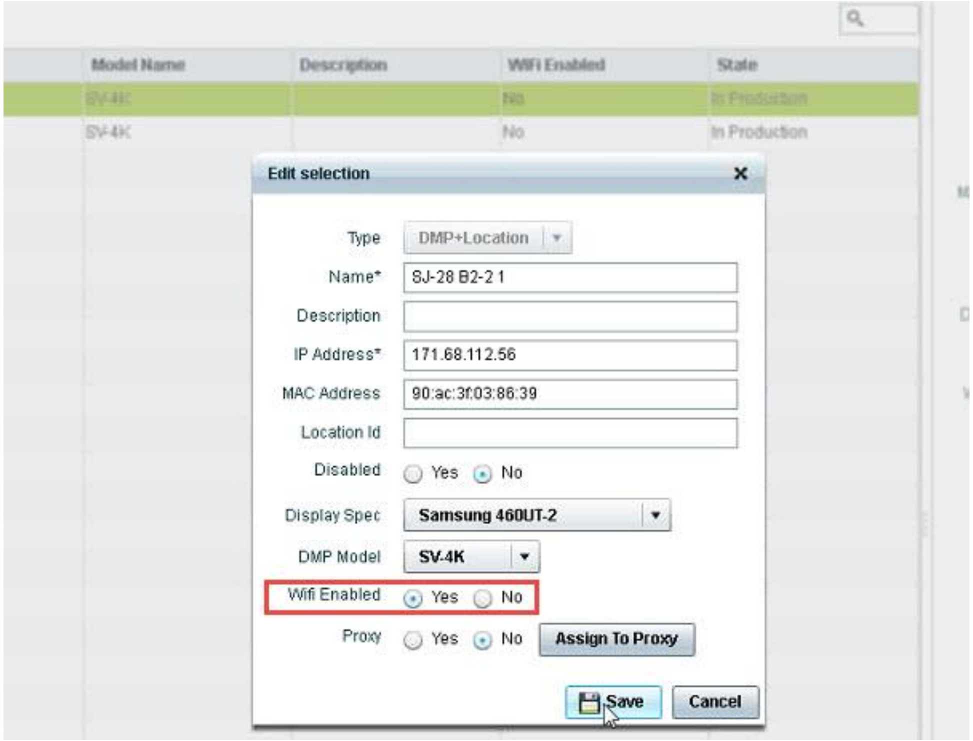
   b. If you have already provisioned the DMP for Cisco Vision Dynamic Signage Director Release 5.0 then reboot the DMP from the Management Dashboard.

6. Enable wireless connectivity on a per-DMP basis. Go to: Control Panel > Setup > Devices > DMP+Location

7. Select the DMPs that you want to configure.

8. Beside the "Wi-Fi Enabled" option, click Yes. Then, click Save.

Figure 37 – Wi-Fi Enabled Option Under SV-4K Device Settings



Model Name	Description	WiFi Enabled	State
SV-4K		No	In Production
SV-4K		No	In Production

Edit selection

Type: DMP+Location

Name*: SJ-28 B2-2 1

Description:

IP Address*: 171.68.112.56

MAC Address: 90:ac:3f:03:86:39

Location Id:

Disabled ○ Yes ● No

Display Spec: Samsung 460UT-2

DMP Model: SV-4K

Wifi Enabled ● Yes ○ No

Proxy ○ Yes ● No

9. Reboot the DMP from the Management Dashboard.

10. Verify Wi-Fi connectivity is successful when the Wi-Fi LED stays lit.

11. Remove the Ethernet cable and plug in the SV-4K power adapter and reboot the DMP.

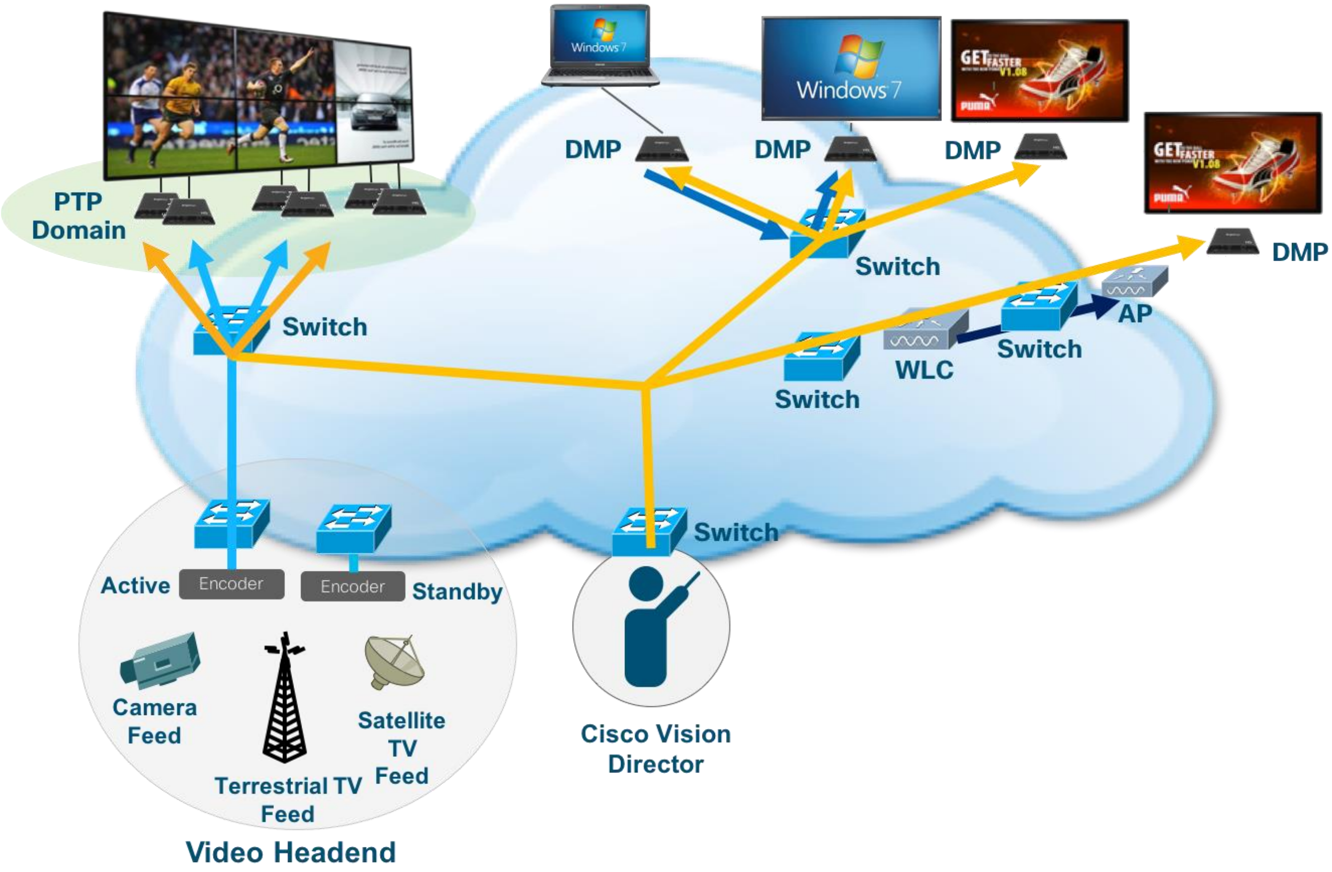
The Role of IP Multicast

Overview

Cisco Vision Dynamic Signage Solution uses IP multicast for the following functions:

- DMP control and Zone-based content synchronization
- Precision Time Protocol (PTP) for DMP-to-DMP synchronization
- Encode and Transmit IP Multicast - The Series 2 and Series 3 DMPs may take an HDMI input from an external device (e.g., laptop) and encode the input into an IP multicast stream to be transmitted on the network.
- Joining MC video channels multicast out from the Video Headend

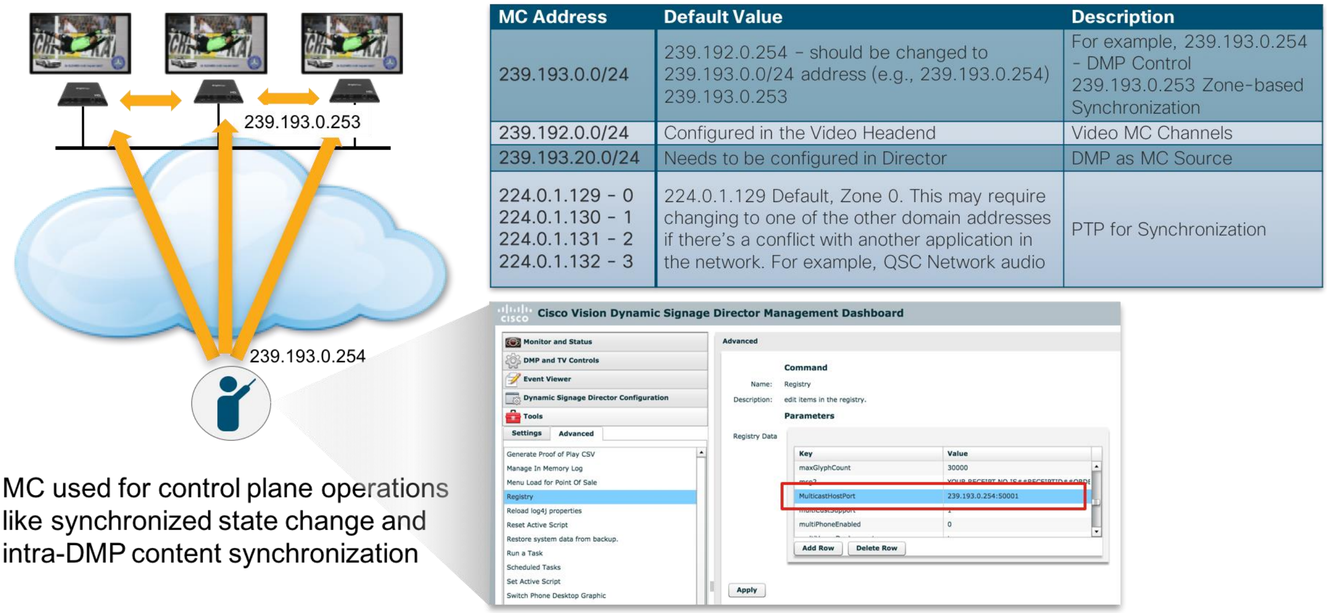
Figure 38 – IP Multicast Overview



Using IP Multicast for DMP Control and Content Synchronization

Cisco Vision Dynamic Signage Director uses IP multicast to send messages to control DMPs and synchronized content.

Figure 39 – Using IP Multicast for DMP Control and Content Synchronization Overview



MC used for control plane operations like synchronized state change and intra-DMP content synchronization

MC Address	Default Value	Description
239.193.0.0/24	239.192.0.254 – should be changed to 239.193.0.0/24 address (e.g., 239.193.0.254) 239.193.0.253	For example, 239.193.0.254 – DMP Control 239.193.0.253 Zone-based Synchronization
239.192.0.0/24	Configured in the Video Headend	Video MC Channels
239.193.20.0/24	Needs to be configured in Director	DMP as MC Source
224.0.1.129 – 0 224.0.1.130 – 1 224.0.1.131 – 2 224.0.1.132 – 3	224.0.1.129 Default, Zone 0. This may require changing to one of the other domain addresses if there's a conflict with another application in the network. For example, QSC Network audio	PTP for Synchronization

Cisco Vision Dynamic Signage Director Management Dashboard

Advanced

Command

Name: Registry

Description: edit items in the registry.

Parameters

Registry Data

Key	Value
maxGlyphCount	30000
MulticastHostPort	239.193.0.254:50001
multiPhoneEnabled	0

Table 2 - Multicast Addresses used by the Cisco Vision Solution

MC Address	Default Value	Description
239.193.0.0/24	239.192.0.254 – should be changed to 239.193.0.0/24 address (e.g., 239.193.0.254) 239.193.0.253	For example, 239.193.0.254 - DMP Control from Director 239.193.0.253 Zone-based Synchronization (TTL=1) between DMPs
239.192.0.0/24	Configured in the Video Headend	Video MC Channels
239.193.20.0/24	Needs to be configured in Director	DMP as MC Source
224.0.1.129 - 0 224.0.1.130 - 1 224.0.1.131 - 2 224.0.1.132 - 3	224.0.1.129 Default, Zone 0. This may require changing to one of the other domain addresses if there's a conflict with another application in the network. For example, QSC Network audio	PTP for Synchronization

Note - See the Cisco Vision Administration Guide for more detailed information.

1. From the Management Dashboard, select Tools > Advanced > Registry.
2. Scroll to the "MulticastHostPort" registry key in the Parameters list and confirm the entry for the registry.
3. Click on the value field and specify a multicast address in the range 239.193.0.0/24 and port number. For example, 239.193.0.254:50001

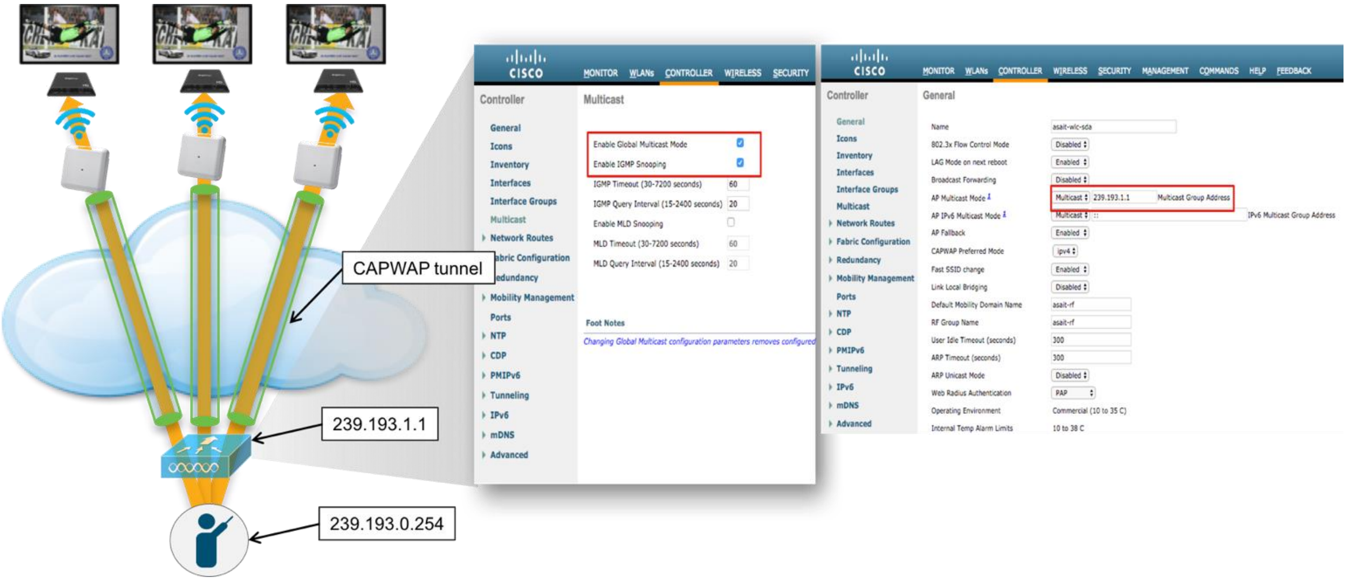
Note - Be sure to use the value that is configured in your network for transport of Cisco Vision Dynamic Signage Director control messages. Typically, the Multicast RP used for DMP control and synchronization is on the network's core switches.

4. Click Apply.

Configuring the Wi-Fi network for Multicast

Cisco's Enterprise wireless LAN architecture including WLAN controllers and Access Points support the transport of IP multicast. Below is an explanation of how it works.

Figure 40 – Configuring the Wi-Fi Network for Multicast Overview



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

Foot Notes

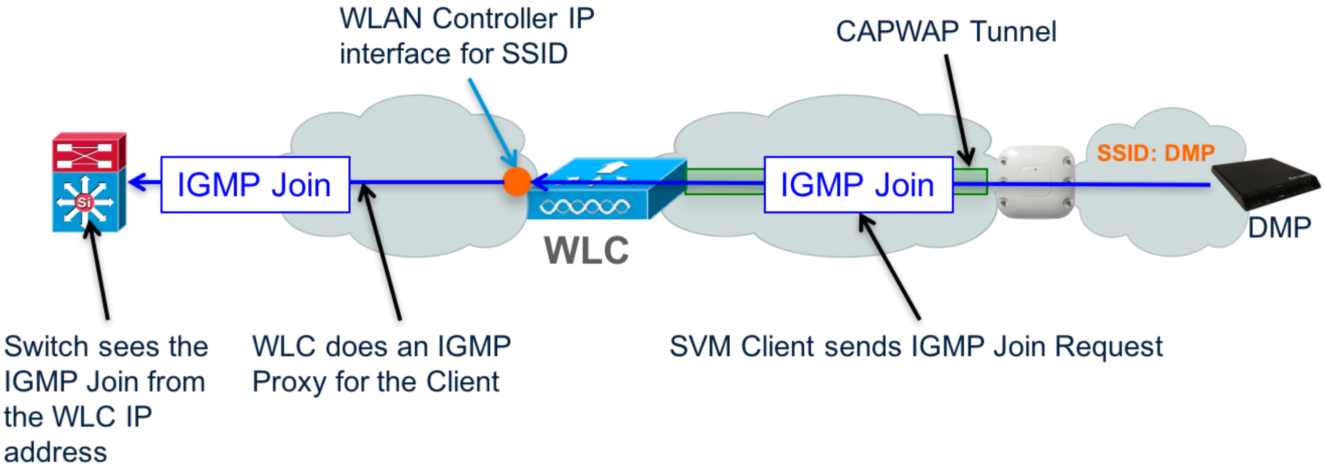
Changing Global Multicast configuration parameters removes configured

General

Name asait-wlc-sda
802.3x Flow Control Mode Disabled
LAG Mode on next reboot Enabled
Broadcast Forwarding Disabled
AP Multicast Mode Multicast 239.193.1.1 Multicast Group Address
AP IPv6 Multicast Mode Multicast :: IPv6 Multicast Group Address
AP Fallback Enabled
CAPWAP Preferred Mode ipv4
Fast SSID change Enabled
Link Local Bridging Disabled
Default Mobility Domain Name asait-rf
RF Group Name asait-rf
User Idle Timeout (seconds) 300
ARP Timeout (seconds) 300
ARP Unicast Mode Disabled
Web Radius Authentication PAP
Operating Environment Commercial (10 to 35 C)
Internal Temp Alarm Limits 10 to 38 C

Understanding How Multicast is Handled over Wi-Fi

Figure 41 – Multicast over Wi-Fi Overview


WLAN Controller IP interface for SSID
CAPWAP Tunnel
IGMP Join
IGMP Join
SSID: DMP
WLC
DMP
Switch sees the IGMP Join from the WLC IP address
WLC does an IGMP Proxy for the Client
SVM Client sends IGMP Join Request

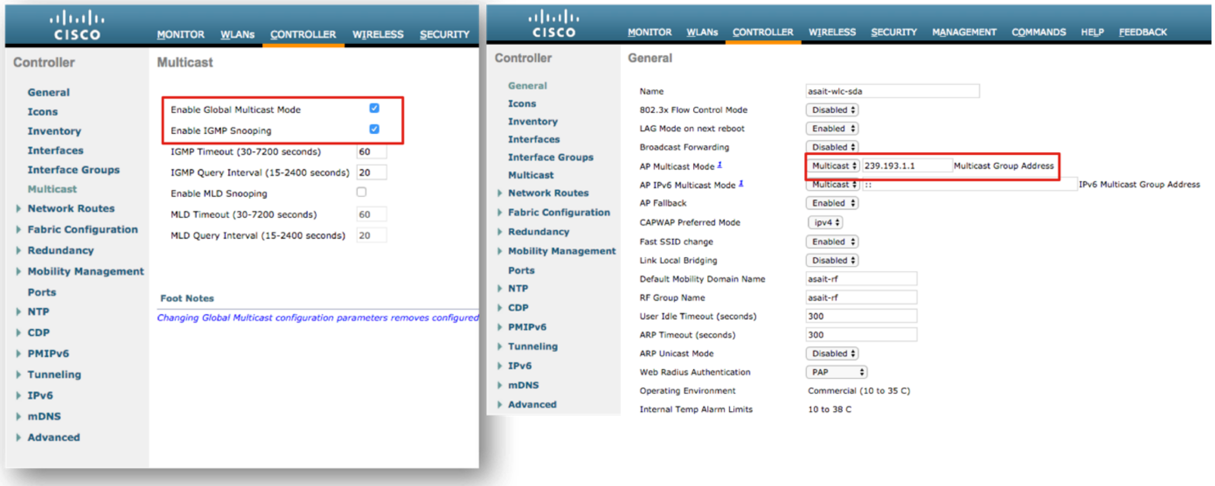
Configuring Multicast on the WLAN Controller

Note - Multicast is required to support DMP control traffic.

Note - It's not recommended to stream video over the Wi-Fi network.

Note - The WLAN Controller should use the Multicast RP on the core switches. Below shows an example using the 239.193.1.1 multicast address for the Controller. If there are multiple Controllers, each Controller would be assigned different multicast address.

Figure 42 – Cisco Wireless LAN Multicast Configuration



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

Foot Notes

Changing Global Multicast configuration parameters removes configured

General

Name asait-wlc-sda
802.3x Flow Control Mode Disabled
LAG Mode on next reboot Enabled
Broadcast Forwarding Disabled
AP Multicast Mode [1] Multicast 239.193.1.1 Multicast Group Address
AP IPv6 Multicast Mode [1] Multicast :: IPv6 Multicast Group Address
AP Fallback Enabled
CAPWAP Preferred Mode ipv4
Fast SSID change Enabled
Link Local Bridging Disabled
Default Mobility Domain Name asait-rf
RF Group Name asait-rf
User Idle Timeout (seconds) 300
ARP Timeout (seconds) 300
ARP Unicast Mode Disabled
Web Radius Authentication PAP
Operating Environment Commercial (10 to 35 C)
Internal Temp Alarm Limits 10 to 38 C

Using the DMP as an IP Multicast Source

In Release 4.1 and later releases, Cisco Vision Dynamic Signage Solution supports streaming video from a laptop or other supported device connected to the HDMI-In port on the SV-4K or CV-UHD media players to be played as a multicast-based channel over the wired Ethernet port.

Figure 43 – Using the DMP as an IP Multicast Source Overview

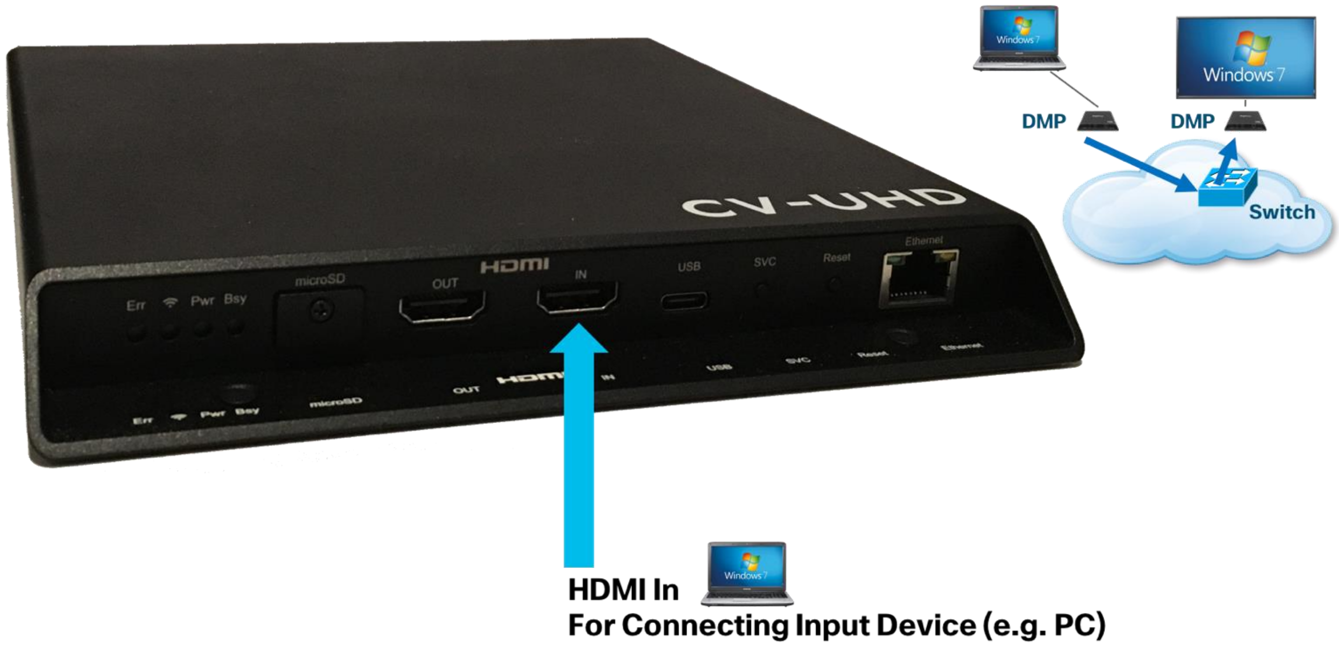
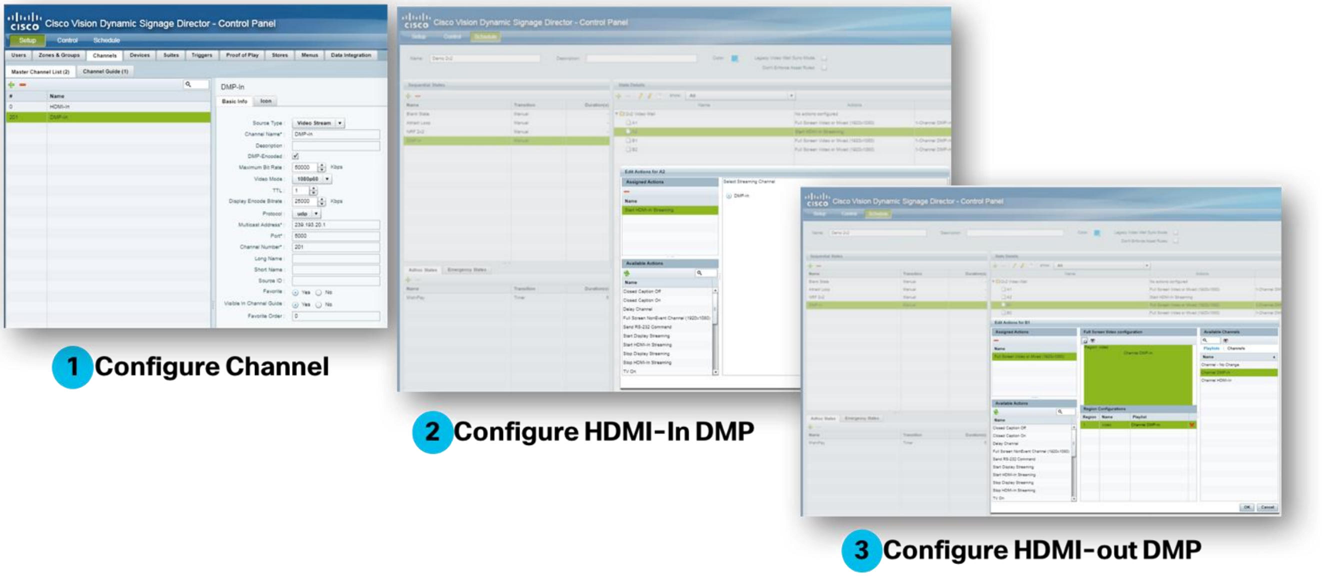


Figure 44 – Configuring Cisco Vision Dynamic Signage Director for Using the DMP as a Video Source



#	Name
0	HDMI-In
201	DMP-In

DMP-In

Source Type : Video Stream
Channel Name* : DMP-In
Description :
DMP-Encoded : ☑
Maximum Bit Rate : 50000 Kbps
Video Mode : 1080p60
TTL : 1
Display Encode Bitrate : 25000 Kbps
Protocol : udp
Multicast Address* : 239.193.20.1
Port* : 5000
Channel Number* : 201
Long Name :
Short Name :
Source ID :
Favorite : ● Yes ○ No
Visible In Channel Guide : ● Yes ○ No
Favorite Order : 0

The allowable multicast range to use for this feature is within the 239.193.20.0/24 range.

Note - On Cisco switches, IP Base only supports multicast stub routing. This means that the DMP-sourced multicast stream will not leave the local subnet. This type of multicast routing is indicative of the `ip pim passive command` configured on the subnet's Switch Virtual Interface (SVI).

Note - To stream DMP multicast IP Services must be installed in the DMP-connected switch and the SVI would be configured with the `ip pim sparse-mode` command.

Note - The Multicast RP used for this address range is located on the core switches.

Note - If you want to maintain privacy of channels, create a DMP-encoded channel per suite with a unique multicast address (from 239.193.20.0/24 range), and create a separate channel guide per suite. For example, if you have 10 suites—create 10 separate DMP-encoded channels with unique multicast addresses, create 10 different channel guides for each DMP-encoded channel, and assign each suite to a different channel guide.

For more information about configuring this feature, see the Cisco Vision Dynamic Signage Director Operations Guide.

Switch Configuration Example

```
! IP Base Catalyst Access Switch

ip multicast-routing distributed

!

interface TenGigabitEthernetx/0/z

 description ** Up Link **

 ip address 10.194.20.2 255.255.255.0

 ip pim sparse-mode

!

interface range GigabitEthernet1/0/x - y

 description SV-DMP Port

 switchport mode access

 switchport access vlan 10

 spanning-tree portfast

!

interface Vlan 10

 description SV-DMP VLAN

 ip address 10.194.10.1 255.255.255.0

 ip pim passive

!Commands to enable DMP control and DMP video

ip pim rp-address 10.0.0.1 anycast-grp-acl override

ip access-list standard anycast-grp-acl permit 239.193.0.0 0.0.255.255

!

!Commands to enable video multicast from the Video Headend

ip pim rp-address 10.1.1.1 prioritycast-grp-acl override
```

```
!
ip access-list standard prioritycast-grp-acl permit 239.192.0.0 0.0.0.255
!
service-policy input CISCO-SV-DMP
!
ip access-list extended IEEE-1588
 remark PTP for DMPs and Audio Systems
 permit udp any host 224.0.1.129
 permit udp any host 224.0.1.130
 permit udp any host 224.0.1.131
 permit udp any host 224.0.1.132
!
ip access-list extended DMP-AS-A-VIDEO-SOURCE
 remark ACL used to mark a SV-4K sourced video stream
 permit udp <DMP Subnet/xx> host <239.193.x.x>
!
table-map policed-dscp
 map from 0 to 8
 map from 10 to 8
 map from 18 to 8
 map from 24 to 8
 map from 46 to 8
!
class-map match-any IEEE-1588
 match access-group name IEEE-1588
class-map match-any DMP-AS-A-VIDEO-SOURCE
 match access-group name DMP-AS-A-VIDEO-SOURCE
!
policy-map CISCO-SV-DMP
 class IEEE-1588
```

```
  set dscp ef
   police cir 1000000 bc 300000
   conform-action transmit
   exceed-action set-dscp-transmit dscp table policed-dscp
 class DMP-AS-A-VIDEO-SOURCE
  set dscp cs5
   police cir 25000000 bc 5000000
   conform-action transmit
   exceed-action set-dscp-transmit dscp table policed-dscp
 class class-default
  set dscp default
```

Protocol Independent Multicast (PIM)

The IP Multicast design employs Protocol Independent Multicast (PIM) Sparse mode routing with Rendezvous Point (RP) redundancy.

1. Because PIM Sparse mode operates in an on-demand fashion, receivers must request a video stream using an IGMP join request.
2. This request is received by the receiver's local switch and is directed to a pre-configured Rendezvous Point (RP). The RP is where sources and receivers register and is how they find each other in the network.
3. Once registered, a tree is built to connect sources and receivers that the multicast stream will traverse.
4. Reverse Path Forwarding (RPF) using the network's unicast routing table is used to derive the shortest paths (or branches of the tree) between sources and receivers.

Below are the attributes of the Multicast network design.

- Uses PIM Sparse Mode multicast routing protocol
- Uses a set of Rendezvous Points (RP) on the Core switches for DMP control, synchronization and when the DMP acts as a video source
- Anycast RP & Multicast Source Discovery Protocol (MSDP) for RP redundancy on Core switches
- Anycast RP provides an active/active redundancy strategy
- Use ACLs and MC Boundaries to limit MC to their designated areas

Using Anycast for DMP Control

Anycast has the following attributes:

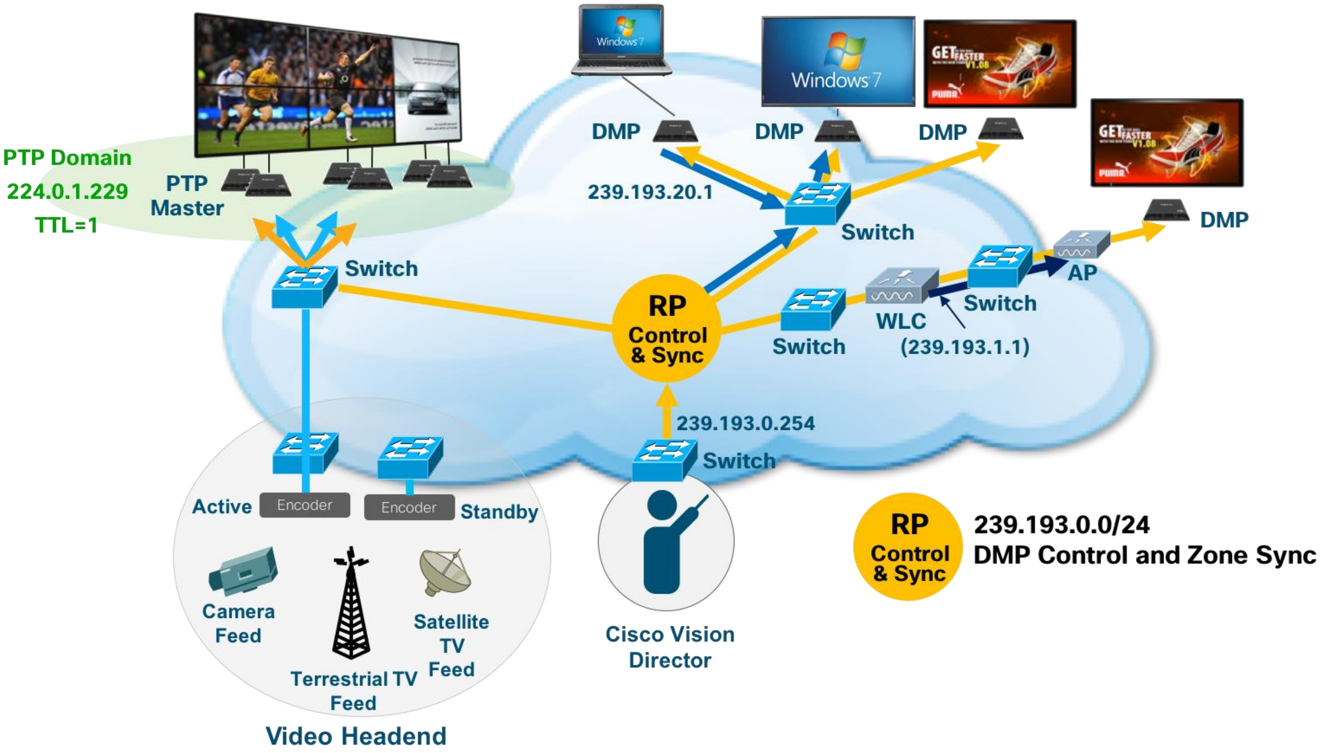
- Provides Source and RP Redundancy in an Active/Active redundancy model
- Sub-second failover
- Simple to implement. Sources can be anywhere in the network with no special IP addressing
- An RP is centrally configured with the same address and netmask on each of the Core switches
- Multicast Source Discovery Protocol (MSDP) is configured between the Nexus Core switches and their respective RPs to share source information

Note - MSDP is not required if using a Catalyst Virtual Switching Service (VSS) core.

Anycast

The Anycast strategy uses two or more RPs with the same IP address and mask and Multicast Source Discovery Protocol (MSDP) to distribute multicast source registration information among the RPs. This insures that each RP knows about all sources and can facilitate building an RP tree between the source and receiver.

Figure 45 – Anycast Overview



Operation and Configuration

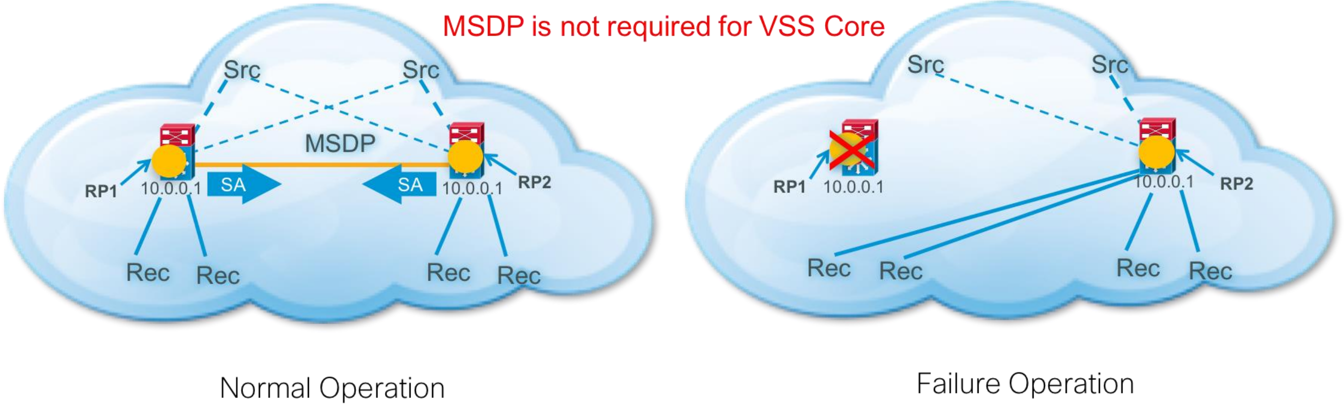
1. In Anycast RP, all the RPs are configured to be MSDP peers of each other.
2. When a multicast source (e.g., Cisco Vision Dynamic Signage Director) registers with one RP, a Source Advertisement (SA) message will be sent to the other RPs informing them that there is an active source for a particular multicast group.
3. The result is that each RP will know about the active sources in the area of the other RPs.
4. If any of the RPs were to fail, IP routing would converge.

5. New sources would register with the next closest RP.

6. Receivers would join toward the new RP and connectivity would be maintained.

Note - The RP is normally needed only to start new sessions with sources and receivers. The RP facilitates the shared tree so that sources and receivers can directly establish a multicast data flow. If a multicast data flow is already directly established between a source and the receiver, then an RP failure will not affect that session. Anycast RP ensures that new sessions with sources and receivers can begin at any time.

Figure 46 – Anycast in Action



- ✓ Sources register with the closest RP
- ✓ All RPs know about all sources via direct registration or Source Advertisement messages
- ✓ Receivers join MC groups using the closest RP
- ✓ Active/Active Redundancy

Switch Configuration Examples

Nexus 7000 Core Switch

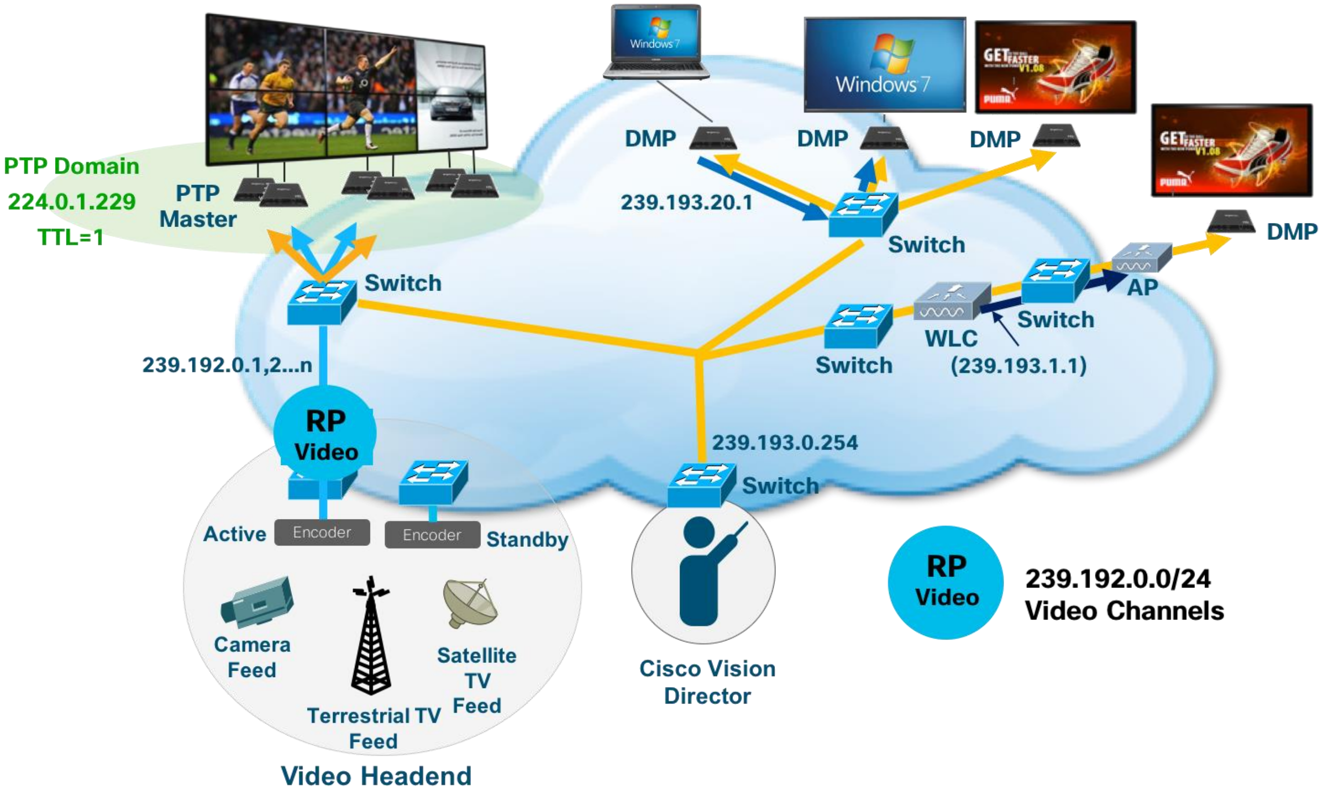
```
! Must be the same IP Address on both n7k routers

!

interface loopback0

 description Anycast RP

 ip address 10.0.0.1/32

 ip router eigrp 100

 ip pim sparse-mode

!

!The MSDP peer IP address will be different on each switch

interface loopback1

 description MSDP Peer
 ip address 10.2.2.1/32
 ip router eigrp 100
!
! Must be the same on both n7k routers with the exception of the MSDP peer IP addresses
feature msdp
ip msdp originator-id 10.2.2.1
ip msdp peer 10.2.2.2 connect-source 10.2.2.1
ip msdp reconnect-interval 1
ip msdp group-limit 800 source 0.0.0.0/0
ip msdp sa-limit 10.2.2.2 2000
!
ip pim rp-address 10.0.0.1 group-list 239.193.0.0/24
```

Catalyst Access Switch

```
ip pim rp-address 10.0.0.1 anycast-grp-acl override
ip access-list standard anycast-grp-acl permit 239.193.0.0 0.0.0.255
```

Using Prioritycast and DCM Active/Standby Redundancy

Figure 47 – Prioritycast RP Overview



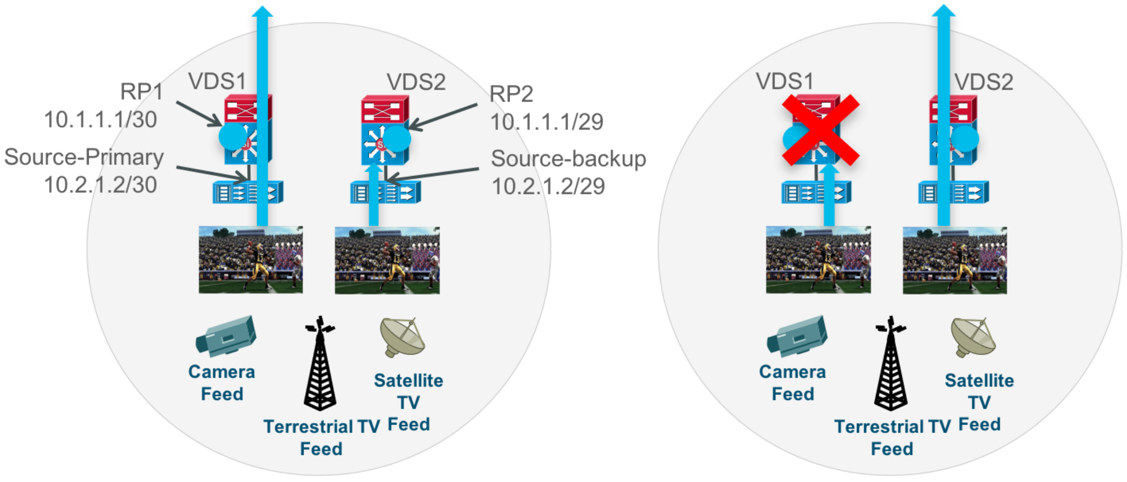
- Provides Source and RP Redundancy in an Active/Standby redundancy model
- Sub-second failover
- More Complex to implement. Redundant sources must use duplicate addressing with different masks
- Provides a single source stream on the network at a time to reduce the amount of traffic on the network and to avoid the video endpoints form arbitrating between two duplicate video streams
- Because the network controls what source traffic is allowed on the network, no vendor proprietary source sync protocol is required between sources to trigger the backup source to start streaming
- Prioritycast uses unicast routing mechanisms to have the network act as the arbiter of what source streams traverse the network and when. This is how the active/standby redundancy strategy is implemented.

Operation and Configuration

Below is a description of how this is accomplished.

1. Prioritycast uses duplicate multicast video sources, each source connected to a separate VDS switch
2. Each primary multicast source & Rendezvous Point (RP) and it's backup use identical IP addresses with differing network masks
3. The primary MC source & RP uses the longest network mask and therefore, is the active source & RP on the network
4. If the primary VDS switch or uplinks or primary MC video source Ethernet link fail, the network will converge and place the backup MC video source onto the network. The transition is transparent to the video receivers due to identical source IP addresses.

Figure 48 – Prioritycast in Action



Normal Operation

Failure Operation

- ✓ IP packets flow along the highest priority route (longest netmask)
- ✓ A network failure will direct IP packets along the next highest priority route via VDS2.
- ✓ Active/Standby Redundancy

Switch Configuration Example

Nexus 7000 Core Switch

```
feature pim
!
interface Ethernet1/4
  description VDS1 uplink1
  ip address 10.0.1.1/30
  ip router eigrp 1200
  ip pim sparse-mode
  no shutdown
!
interface Ethernet1/6
  description VDS2 uplink2
  ip address 10.0.3.1/30
  ip router eigrp 1200
  ip pim sparse-mode
  no shutdown
!
ip pim rp-address 10.1.1.1 group-list 239.192.0.0/24
```

VDS01 – Primary (Active)

```
interface Loopback1
description prioritycast-RP Primary address for Video IP Multicast
ip address 10.1.1.1 255.255.255.252
ip pim sparse-mode
!
ip pim rp-address 10.1.1.1 prioritycast-grp-acl override
!
ip access-list standard prioritycast-grp-acl permit 239.192.0.0 0.0.0.255
!
interface GigabitEthernetx/y
description Channel MMM, Primary Source 10.2.1.2
 ip address 10.2.1.1 255.255.255.252
 ip pim sparse-mode
!
interface GigabitEthernetx/y
 description Primary DCM Mgmt Port
 switchport access vlan 30
 ip address 192.168.30.1 255.255.255.248
!
interface TenGigabitEthernet0/x
 description ** Up Link to n7k-1
 ip address 10.0.1.2 255.255.255.252
 ip pim sparse-mode
!
```

```
interface TenGigabitEthernet0/x

 description ** Up Link to n7k-2

 ip address 10.0.2.2 255.255.255.252

 ip pim sparse-mode
```

VDS02 – Secondary (Standby)

```
interface Loopback1

 description prioritycast-RP Secondary address for Video IP Multicast

 ip address 10.1.1.1 255.255.255.248

 ip pim sparse-mode

!

ip pim rp-address 10.1.1.1 prioritycast-grp-acl override

!

ip access-list standard prioritycast-grp-acl permit 239.192.0.0 0.0.0.255

!

interface GigabitEthernetx/y

 description Channel MMM, Secondary Source 10.2.1.2

 ip address 10.2.1.1 255.255.255.248

 ip pim sparse-mode

!

interface GigabitEthernetx/y

 description Primary DCM Mgmt Port

 switchport access vlan 40

 ip address 192.168.40.2 255.255.255.248

!

interface TenGigabitEthernet0/x

 description ** Up Link to n7k

 ip pim sparse-mode
```

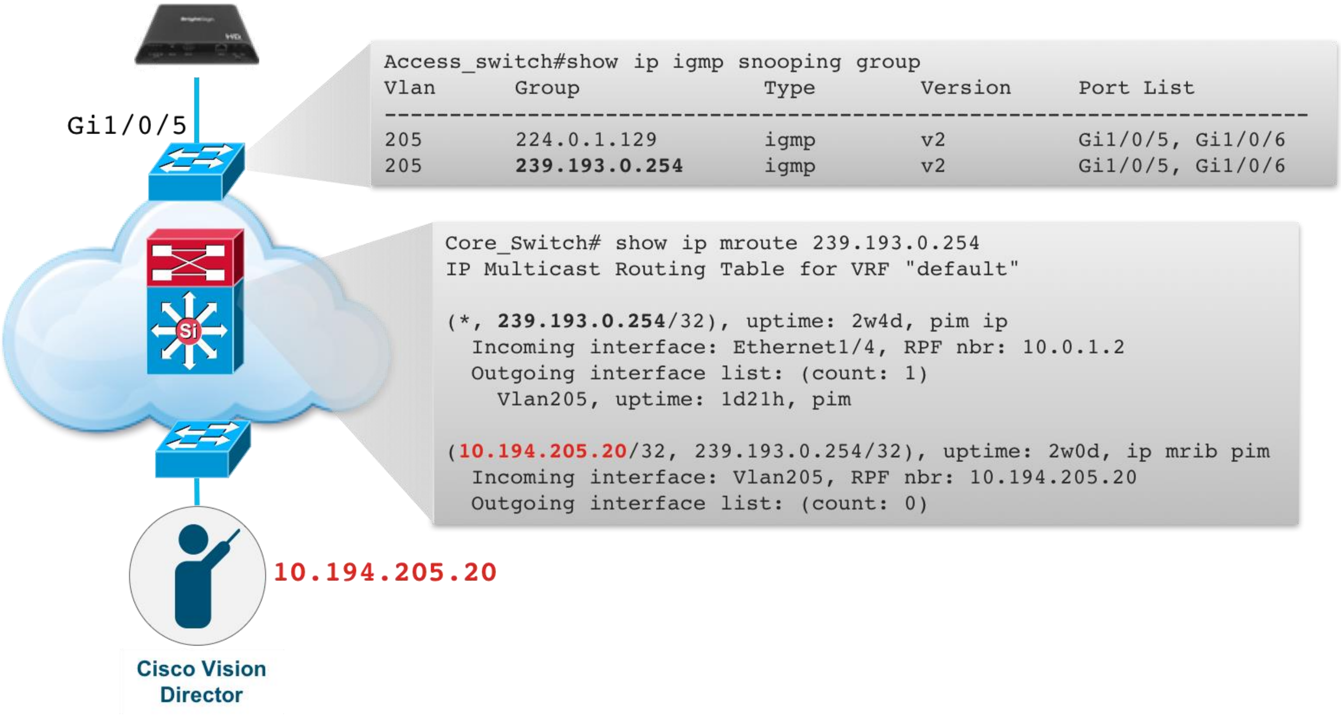
VDS Switch QoS Configuration

```
ip access-list extended DCM-DIRECTTV

 permit ip any 239.192.0.0 0.0.0.255

or

ip access-list extended DCM-DIRECTTV

   permit ip host <source DCM> any

!

class-map match-any DCM-DIRECTTV

 match access-group name DCM-DIRECTTV

!

policy-map POLICE-DCM

class DCM-DIRECTTV

  set dscp cs5

   police 4000000000 1000000 exceed-action drop

class class-default

 set dscp default

!

interface GigabitEthernetx/y

 description DCM output, Primary Source 10.2.1.2

 ip address 10.2.1.1 255.255.255.252

 service-policy input POLICE-DCM
```

Troubleshooting IP Multicast

Below are the basic requirements for multicast to work between the source and receiver and how to troubleshoot multicast issues.

Figure 49 – Troubleshooting IP Multicast in Cisco Switches



```
Access_switch#show ip igmp snooping group
Vlan        Group                  Type         Version        Port List
-------------------------------------------------------------------------
205         224.0.1.129            igmp         v2             Gi1/0/5, Gi1/0/6
205         239.193.0.254          igmp         v2             Gi1/0/5, Gi1/0/6
```

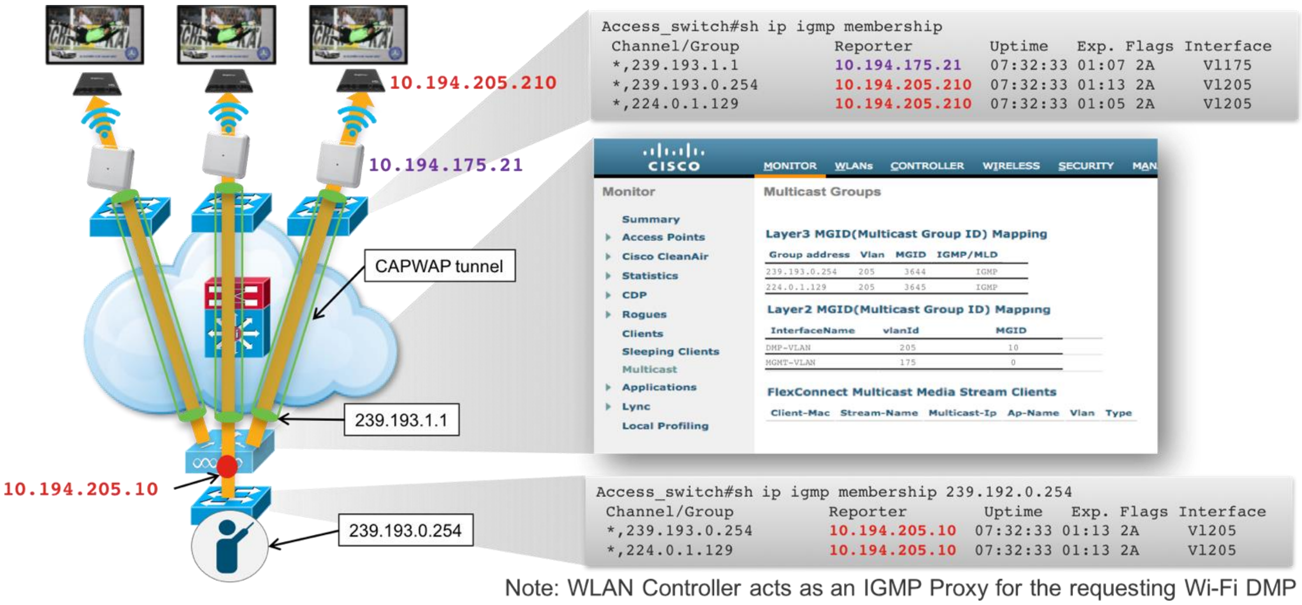
```
Core_Switch# show ip mroute 239.193.0.254
IP Multicast Routing Table for VRF "default"

(*, 239.193.0.254/32), uptime: 2w4d, pim ip
  Incoming interface: Ethernet1/4, RPF nbr: 10.0.1.2
  Outgoing interface list: (count: 1)
    Vlan205, uptime: 1d21h, pim

(10.194.205.20/32, 239.193.0.254/32), uptime: 2w0d, ip mrib pim
  Incoming interface: Vlan205, RPF nbr: 10.194.205.20
  Outgoing interface list: (count: 0)
```

- If the source and receiver are on the same subnet, then multicast routing (i.e., PIM) is not required.
- IGMP Snooping is enabled by default on Cisco switches and is used to direct multicast traffic within a VLAN to only the ports where devices request it via an IGMP join message. Use the ip igmp snooping group command on the DMP-connected switch to see what multicast groups the DMPs request from the network.
- Verify you see the multicast group requested is the one configured on the source. For example, after the DMP registers with the Cisco Vision Dynamic Signage Director, it will request the 239.193.0.253 (default for content synchronization, however it remains local to the DMP VLAN via TTL=1) and the 239.192.0.254 (default for DMP control).
- Another command that's useful for seeing what multicast groups a DMP or any receiver has requested is the show ip igmp membership command.

```
Access_switch#sh ip igmp membership

Flags: A  - aggregate, T - tracked

       L  - Local, S - static, V - virtual, R - Reported through v3

       I - v3lite, U - Urd, M - SSM (S,G) channel

       1,2,3 - The version of IGMP, the group is in

Channel/Group-Flags:
       / - Filtering entry (Exclude mode (S,G), Include mode (G))
Reporter:
       <mac-or-ip-address> - last reporter if group is not explicitly tracked
       <n>/<m>      - <n> reporter in include mode, <m> reporter in exclude

 Channel/Group                  Reporter        Uptime   Exp. Flags Interface
 *,239.192.0.15                 10.194.175.230  07:04:25 01:06 2A      Vl175
 *,239.192.0.6                  10.194.175.206  07:04:32 01:06 2A      Vl175
 *,239.192.0.254                10.194.175.234  07:04:33 01:04 2A      Vl175
 *,239.193.0.253                10.194.175.210  07:32:33 01:07 2A      Vl175
 *,239.192.0.254                10.194.175.204  07:32:33 01:13 2A      Vl175
 *,224.0.1.40                   10.194.175.8    13w3d    01:13 2LA     Vl175
 *,224.0.1.129                  10.194.175.239  07:32:33 01:05 2A      Vl175
```

- If the DMP is connected over Wi-Fi, the WLAN controller should show the multicast groups requested by the DMP via an IGMP join.

Figure 50 – Troubleshooting IP Multicast over Wi-Fi



```
Access_switch#sh ip igmp membership
 Channel/Group            Reporter        Uptime   Exp. Flags Interface
 *,239.193.1.1            10.194.175.21   07:32:33 01:07 2A      Vl175
 *,239.193.0.254          10.194.205.210  07:32:33 01:13 2A      Vl205
 *,224.0.1.129            10.194.205.210  07:32:33 01:05 2A      Vl205
```

Multicast Groups

Layer3 MGID(Multicast Group ID) Mapping

Group address	Vlan	MGID	IGMP/MLD
239.193.0.254	205	3644	IGMP
224.0.1.129	205	3645	IGMP

Layer2 MGID(Multicast Group ID) Mapping

InterfaceName	vlanId	MGID
DMP-VLAN	205	10
MGMT-VLAN	175	0

FlexConnect Multicast Media Stream Clients

Client-Mac	Stream-Name	Multicast-Ip	Ap-Name	Vlan	Type

```
Access_switch#sh ip igmp membership 239.192.0.254
 Channel/Group            Reporter        Uptime   Exp. Flags Interface
 *,239.193.0.254          10.194.205.10  07:32:33 01:13 2A      Vl205
 *,224.0.1.129            10.194.205.10  07:32:33 01:13 2A      Vl205
```

Note: WLAN Controller acts as an IGMP Proxy for the requesting Wi-Fi DMP

- Recall that the WLAN Controller acts as an IGMP proxy for the Wi-Fi connected DMPs so when looking at the switch that's connected to the WLAN Controller via the show ip igmp membership command, you will see the WLAN Controller's IP address as the reporter rather than the DMP's IP address.
- When there is no multicast router in the VLAN (or in other words, there's no PIM sparse-mode command on the VLAN interface) to originate the IGMP queries, you must configure an IGMP snooping querier to send membership queries.

Note - This command is usually only used for small single switch demo systems where the Cisco Vision Dynamic Signage Director and the DMPs are in the same VLAN.

```
Access_Switch#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

C3850-277-DemoRm1(config)#ip igmp snoop querier
```

- If multicast traffic must go between subnets, then a multicast routing protocol (e.g., PIM sparse-mode) is used.
- If PIM sparse-mode is used,
    - Verify a Rendezvous Point (RP) is configured on a loopback interface somewhere in the network (e.g., on core switches).
    - Each switch that has connected sources and receivers must have the ip pim sparse-mode command on all interfaces (including the RP loopback) between the source and receiver
    - Each switch that has connected sources and receivers must be configured with an ip pim rp command that points to the RP for the requested multicast group address.
    - Reachability is required between the source, RP, and receiver. Use the ping command between the source and RP and the source and receiver or vice versa. If ping works, you can use the mtrace command to see the path back to the source. If the multicast trace stalls, it's likely that the ip pim sparse-mode command is missing on the interface in the reverse path to the multicast source.

```
Core_Switch# mtrace ?

  WORD  IP address or hostname of source

Core_Switch# mtrace 10.194.175.20

Mtrace from 10.194.175.20 to 10.194.205.1 via group 0.0.0.0

Querying full reverse path...

  0  ? (10.194.205.1)

 -1  ? (10.194.205.2) PIM  [default]

Round trip time 6 ms; total ttl of 1 required.
```

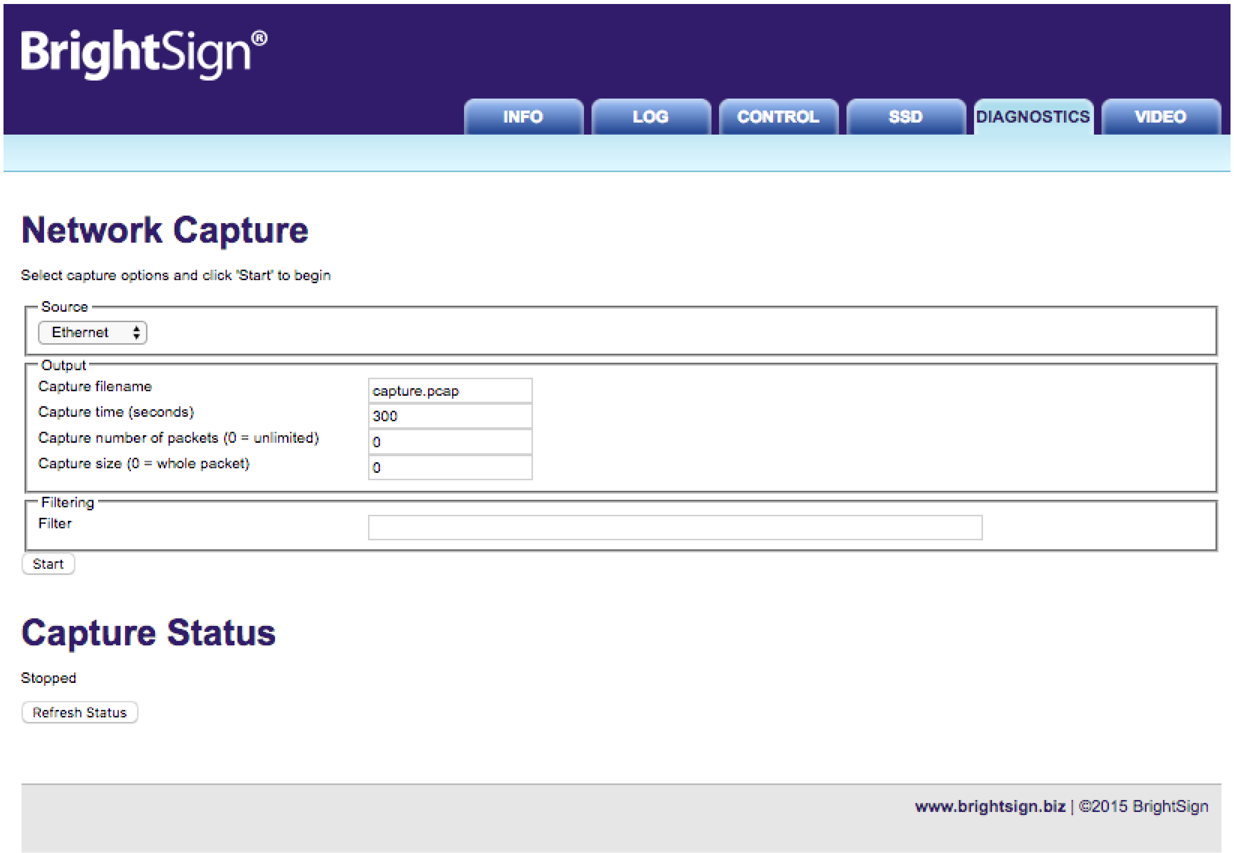
- Verify the multicast route between the source (Cisco Vision Dynamic Signage Director, 10.194.175.20) and receiver (DMP).

```
Core_Switch# show ip mroute 239.193.0.254

IP Multicast Routing Table for VRF "default"
```

```
(*, 239.193.0.254/32), uptime: 2w4d, pim ip

  Incoming interface: Ethernet1/4, RPF nbr: 10.0.1.2

  Outgoing interface list: (count: 1)

    Vlan175, uptime: 1d21h, pim


(10.194.175.20/32, 239.193.0.254/32), uptime: 2w0d, ip mrib pim

  Incoming interface: Vlan175, RPF nbr: 10.194.175.20

  Outgoing interface list: (count: 0)
```

- Another way to determine if multicast is routing, you can do a packet capture on the DMP via its web interface. Go to http://dmp_ipaddress Diagnostics>Network Packet Capture.

Figure 51 – DMP Network Packet Capture



Network Capture

Select capture options and click 'Start' to begin

Source
Ethernet

Output
Capture filename: capture.pcap
Capture time (seconds): 300
Capture number of packets (0 = unlimited): 0
Capture size (0 = whole packet): 0

Filtering
Filter:

Start

Capture Status

Stopped

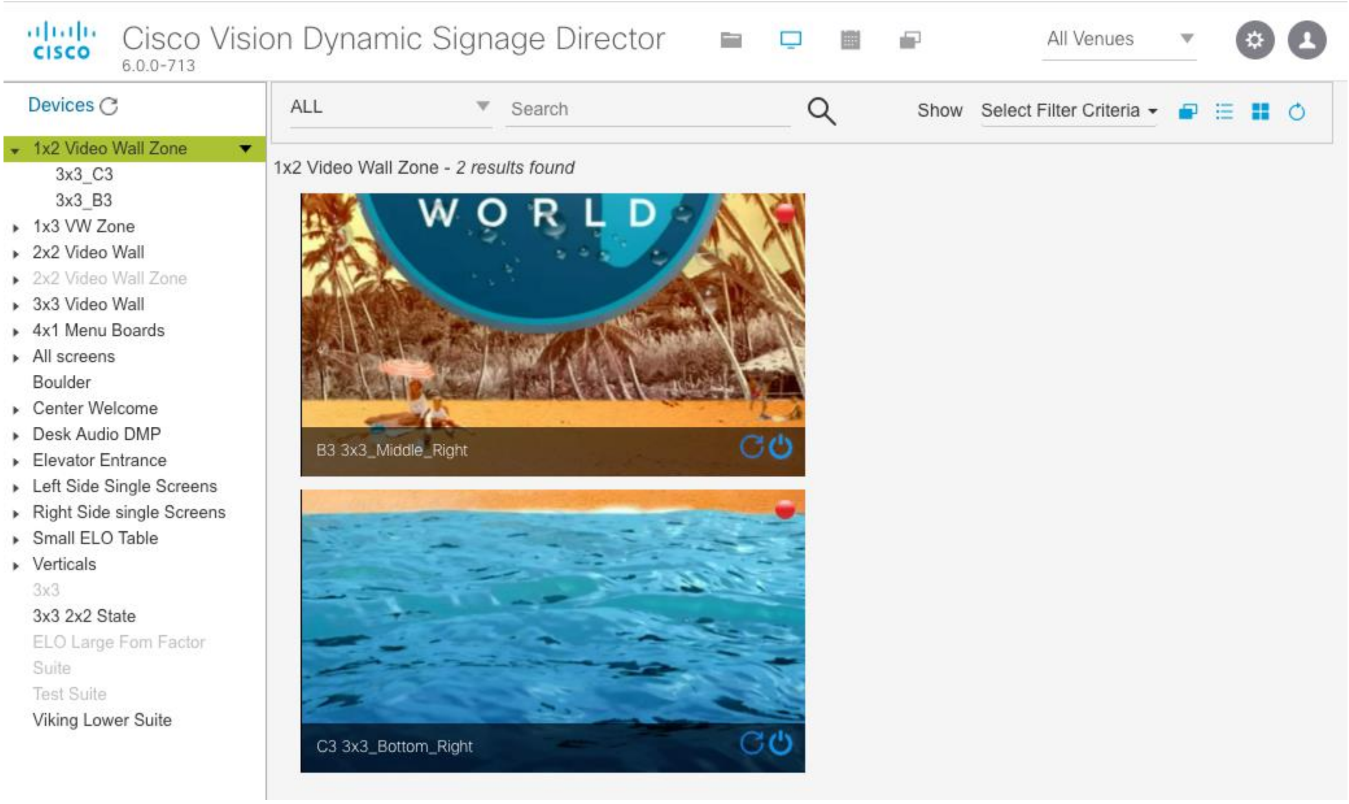
Refresh Status

www.brightsign.biz | ©2015 BrightSign

- Another packet capture option is using the monitor command on the Cisco switch.

- Once you start a script and choose a state, you can see if the correct content is running on the DMP from the Cisco Vision Dynamic Signage Director's Device Management screen.

Figure 52 – Cisco Vision Dynamic Signage Director's Device Management Screen



1x2 Video Wall Zone - *2 results found*