Configuring the Cisco StadiumVision Director Server System Settings

First Published: March 20, 2015
Revised: May 1, 2015

This document is intended for Cisco StadiumVision Director administrators and describes how to configure the initial setup of the Cisco StadiumVision Director server.

Contents

- Prerequisites for Configuring Cisco StadiumVision Director Server System Settings, page 13
- How to Configure Cisco StadiumVision Director Server System Settings, page 14
- What To Do Next, page 45

Prerequisites for Configuring Cisco StadiumVision Director Server System Settings

Before you configure Cisco StadiumVision Director servers, be sure that the following requirements are met:

- The Cisco StadiumVision Director server hardware and software is installed. For more information, see the *Cisco StadiumVision Director Software Installation and Upgrade Guide, Release 4.0*.
- The Cisco StadiumVision Director Server is installed and you know the IP address.
- You have a supported browser version for Cisco StadiumVision Director. For more information about the latest supported browsers, see the *Cisco StadiumVision Release Notes for Release 4.0*.

- You have the network information required to configure the Ethernet connection on the Cisco StadiumVision Director Remote server, such as:
  - IP address (IPv4 only) and network mask

    Note The Cisco StadiumVision Director Remote server should be configured with a static IP address or a non-expiring DHCP lease. In addition, DHCP Server Option 43 should be set up to point to the primary server's URL for auto-registration to work.

  - Default gateway address
  - DNS server address
  - Hostname
- You have either physical console access or an SSH client such as PuTTY to log into the Cisco StadiumVision Director server.
- You know the installer account credentials on the Cisco StadiumVision Director server.
- You understand how to use the Text Utility Interface (TUI). For more information, see the "Cisco StadiumVision Director Server Text Utility Interface" module on page 121. For simplicity in these tasks, the instruction to "select" a particular menu item implies that you type the character that corresponds to the menu option and press **Enter**.
- For NTP configuration requirements, see the "Prerequisites for Configuring NTP on Cisco StadiumVision Director Servers and DMPs" section on page 21.
- For multicast configuration requirements, see the "Prerequisites for Configuring Multicast Ports in Cisco StadiumVision Director" section on page 42.

How to Configure Cisco StadiumVision Director Server System Settings

This section includes the following tasks:

- Completing Initial Configuration of System Settings After a Full ISO Installation, page 14 (required)
- Configuring the Cisco StadiumVision Director Server Network Interface, page 15 (as required)
- Editing the Hosts File, page 18 (as required)
- Restarting the Network Service on the Server, page 19 (as required)
- Generating the SSL Certificate, page 19 (as required)
- Configuring NTP on Cisco StadiumVision Servers and DMPs, page 20 (required)
- Configuring Multicast Ports for Cisco StadiumVision Director, page 38 (required)

Completing Initial Configuration of System Settings After a Full ISO Installation

When you install a full ISO on a Platform 3 server, you configure certain network settings in the Linux interface as part of the ISO installation such as the server IP address and DNS configuration.

As long as the network configuration is successfully completed as part of the installation, then the only remaining system configuration is to set the date and time options on the server and restart the Cisco StadiumVision Director software.

For detailed information about how to configure the date and time options, see the "Configuring NTP on Cisco StadiumVision Servers and DMPs" section on page 20.

Note If for some reason you were unable to complete the Linux network configuration as part of the ISO installation, then you need to complete all of the tasks in this module.

Configuring the Cisco StadiumVision Director Server Network Interface

Note If for some reason you were unable to complete the Linux network configuration as part of the full ISO installation, then complete this task.

This task describes how to access the Linux menus from the TUI to configure the Cisco StadiumVision Director server network interface.

To configure the Cisco StadiumVision Director server network interface, complete the following steps:

Step 1 Log into the TUI as installer on the server using a directly-connected console or SSH client.

The TUI Main Menu is displayed.

Step 2 From the Main Menu, go to **System Settings > Network Settings > Setup Network Information**.

Tip To navigate through the TUI menus you must type the character that corresponds to the menu area where you want to go (a, b, c, and so on) and press **Enter**.

To return to other menus, you must back out of the hierarchy of menus using one of the indicated keys to return you to prior menus.

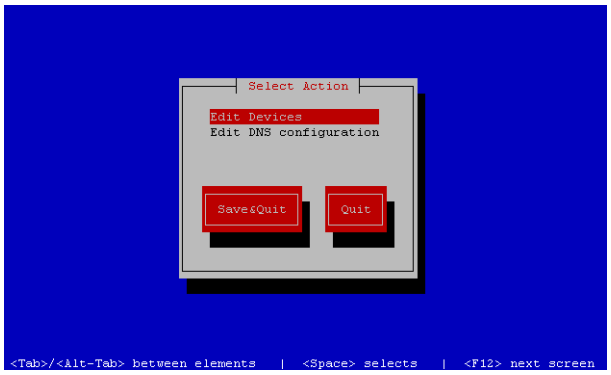
Step 3 At the Configure Network confirmation screen, press any key to continue to enter the Linux network configuration interface.

The Select Action Linux screen is displayed with the **Edit Devices** option selected.

Tip If you notice what appears to be stray characters in the Linux interface, verify that your SSH client is using the UTF-8 character set translation.

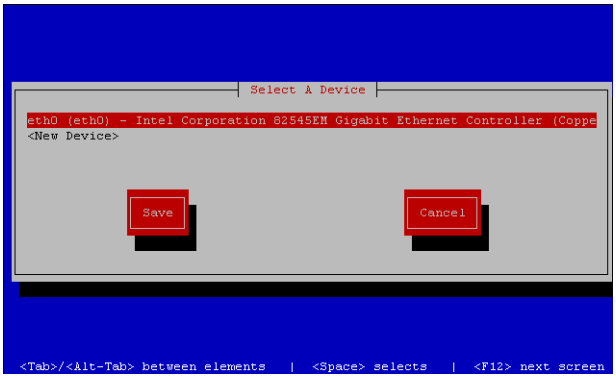
Step 4 In the Select Action screen, select **Edit Devices** and press **Enter**.

Figure 1 Select Action Screen



Step 5 In the Select a Device screen, select **eth0** and press **Enter**.

Figure 2 Select a Device Screen

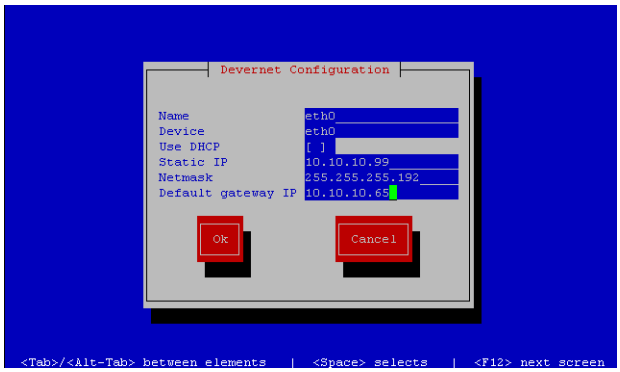


The Ethernet Configuration screen is displayed.

Note The Linux screen is mislabeled “Devernet Configuration.”

Step 6 In the Ethernet Configuration screen (Figure 3), do the following:

Figure 3 Devernet Configuration Screen



a. Press the Tab key until the cursor is positioned on the Static IP address line.

b. Press the backspace key to go to the beginning of the line and type in the IPv4 address of the Cisco StadiumVision Director Server.

Note This should be a different IP address than what you configured for the CIMC interface.

c. Press the tab key to go to the Netmask line. Type the network mask for the IPv4 address.

d. (Optional) In the Default gateway IP line, type the address of the default gateway of your network.

Step 7 When configuration of all options is complete, press the Tab key until the **Ok** button is selected and press **Enter**.

You return to the Select a Device screen.

Step 8 Press the Tab key until the **Save** button is highlighted and press **Enter**.

You return to the Select Action screen.

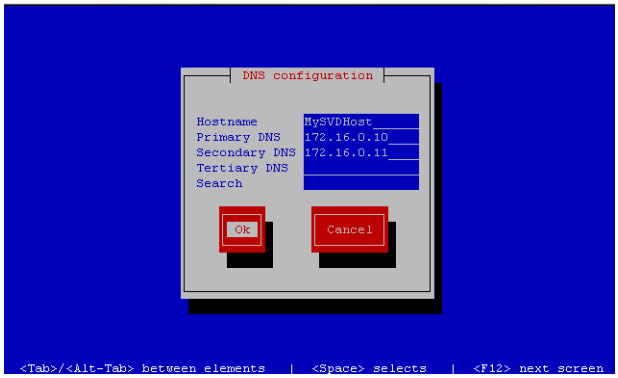
Step 9 Press the down arrow key to select the **Edit DNS configuration** option and press **Enter**.

The DNS configuration screen is displayed.

Step 10 In the DNS configuration screen (Figure 4), select and configure the Hostname and one or more DNS Server IP addresses.

Note Do not use hostnames that contain periods "." within the name.

Figure 4 DNS Configuration Screen



Step 11 Press the Tab key until the **Ok** button is selected and press **Enter**.

You return to the Select Action screen.

Step 12 In the Select Action screen, press the Tab key until the **Save&Quit** button is selected and press **Enter**.

You return to the TUI Configure Network menu.

Editing the Hosts File

Note If for some reason you were unable to complete the Linux network configuration as part of the full ISO installation, then complete this task.

Before you begin, be sure that you know how to use the vi editor. For more information, see the "Cisco StadiumVision Director Server Text Utility Interface" module on page 121.

To edit the hosts file, complete the following steps:

Step 1 From the TUI Network Settings menu, select the **Edit hosts file** option.

Step 2 At the confirmation prompt, press any key to open the /etc/hosts file for editing.

Step 3 Change the line with IP address "10.10.10.10" to a comment (insert a # character at the beginning of the line) as shown in the following example:

```
#10.10.10.10
```

Step 4 Change the line for the IPv6 localhost entry "::1" to a comment as shown in the following example:

```
#::1
```

Step 5 Add a line for the server IP address and hostname as shown in the following example, where *x.x.x.x* is the IPv4 address of the Cisco StadiumVision Director server, and *hostname* is the name to identify the server:

```
x.x.x.x hostname
```

Note Do not use hostnames that contain periods "." within the name.

Step 6 Press **Esc** to enter vi command mode.

Step 7 Save the changes to the file by typing the following command:

```
:wq
```

Step 8 Press any key to return to the Network Settings menu.

Restarting the Network Service on the Server

Note If for some reason you were unable to complete the Linux network configuration as part of the full ISO installation, then complete this task.

After you complete the network configuration on the Cisco StadiumVision Director server, restart the network service to apply the network configuration.

Step 1 Log into the TUI as installer on the server using a directly-connected console or SSH client.

The TUI Main Menu is displayed.

Step 2 From the Main Menu, go to **Services Control > Networking > Restart networking**.

The network interface eth0 is restarted.

Step 3 Confirm that the command completed successfully.

Step 4 Press any key to return to the Networking menu.

Step 5 Return to the Main Menu.

Generating the SSL Certificate

Note If for some reason you were unable to complete the Linux network configuration as part of the full ISO installation, then complete this task.

To generate the SSL certificate, complete the following steps:

Step 1 From the Main Menu, go to **System Settings > Network Settings**.

Step 2 Select the **Generate certificate file** option.

Step 3 When the confirmation warning prompt appears, type **Y** to continue and generate a new SSL certificate.

To cancel without generating a new certificate, type **N**.

Step 4 Press any key to return to the Network Settings menu.

Configuring NTP on Cisco StadiumVision Servers and DMPs

Network Time Protocol (NTP) service is required in Cisco StadiumVision Director on the following devices:

- Cisco StadiumVision Director servers
- Cisco StadiumVision Director Remote servers
- Cisco DMP 4310Gs
- SV-4K Precision Time Protocol (PTP) master device

NTP provides reliable clocking for your Cisco StadiumVision network. NTP helps ensure synchronicity between redundant servers and the Cisco StadiumVision Director remote servers, and optimizes playlist synchronization on the Cisco DMP 4310Gs.

Note For optimized synchronization on the SV-4K media players, PTP is used. Only the SV-4K PTP masters derive a clock using NTP.

You should verify the NTP configuration for your Cisco StadiumVision servers, since the default NTP source is a Red Hat Linux public pool and might not be the NTP server source that you want to use for your venue.

Configuration of the DMP NTP source is done within the Cisco StadiumVision Director Management Dashboard. As a best practice, the Cisco StadiumVision Director server is already set as the NTP host by default for both the Cisco DMP 4310G and SV-4K media players. This does not need to be changed unless the venue requires a different NTP source.

Caution The Cisco StadiumVision Director server is itself enabled as an NTP host to provide timing to the *Cisco DMPs and SV-4Ks only*. You also can use the Cisco StadiumVision Director server as the NTP host for your remote servers. Do not use Cisco StadiumVision Director as an NTP host for other devices in your network.

This section includes the following tasks:

- Prerequisites for Configuring NTP on Cisco StadiumVision Director Servers and DMPs, page 21 (required)
- Configuring the System Date and Time Using NTP on Cisco StadiumVision Servers, page 22 (required)
- Configuring NTP on the Cisco DMP 4310G, page 26 (required)
- Configuring NTP and PTP on the SV-4K Media Players, page 33 (required)

Prerequisites for Configuring NTP on Cisco StadiumVision Director Servers and DMPs

Caution If you are running Cisco StadiumVision Director on a virtual server, then you should reference a reliable NTP server running on a bare metal server, rather than relying on a clock from a VM environment that can drift and is not accurate.

Before configuring NTP on Cisco StadiumVision Director Servers and DMPs, be sure that the following requirements are met:

- You understand how to use vi editor commands.
- You understand the NTP host requirements for your Cisco StadiumVision servers:
  - If you do not want to use the default public pool of NTP servers for the Cisco StadiumVision servers, you have the IP address or DNS name of the NTP host for your network.
  - If you plan to use a public pool of NTP servers, be sure that the servers are reachable from the Cisco StadiumVision network. By default, the ntp.conf file on Cisco StadiumVision Director servers has configured the following Red Hat Linux public pool of servers:

    server 0.rhel.pool.ntp.org
    server 1.rhel.pool.ntp.org
    server 2.rhel.pool.ntp.org

Tip For more information about using NTP pool servers see the Network Time Protocol website at:

http://support.ntp.org/bin/view/Servers/NTPPoolServers

- If you plan to change the default best practice of using the Cisco StadiumVision Director server as the NTP source for DMPs, be sure that the following requirements are met:
  - You have configured the NTP host for the Cisco StadiumVision Director server first.
  - You have upgraded the DMP firmware.

    For more information about how to upgrade the DMP firmware, see the *Cisco StadiumVision Director Software Installation and Upgrade Guide* for your release.
  - For optimal synchronization, use the same NTP server that is configured for the Cisco StadiumVision Director server. However, it is not required.
  - The DMP must not reference an NTP server pool. If the Cisco StadiumVision Director server references an NTP server pool (the default), 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 StadiumVision network is configured to allow bidirectional transmission of UDP messages on port 123 for NTP messages.

  UDP port 123 is used for communication between the Cisco StadiumVision servers and NTP hosts, and the DMPs and NTP host (by default, this is the Cisco StadiumVision Director server).

  For a complete port reference for Cisco StadiumVision Director servers, see the “Port Reference” module of the *Cisco StadiumVision Director Software Installation and Upgrade Guide* for your release.

Configuring the System Date and Time Using NTP on Cisco StadiumVision Servers

When you install or upgrade the Cisco StadiumVision Director or Cisco StadiumVision Director Remote servers, you need to configure the system date and time in the TUI. You also need to configure the time zone.

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

- Setting Up the NTP Source on Cisco StadiumVision Servers, page 22 (required)
- Configuring the Time Zone, page 23 (required)
- Restarting the Cisco StadiumVision Software, page 25 (required)
- Configuring the Date and Time Manually, page 26 (if necessary)

Setting Up the NTP Source on Cisco StadiumVision Servers

Note Complete this task only if you do not want to use the default public pool of servers.

Standard NTP server configuration uses the word "server" followed by the Domain Name System (DNS) name or IP address of an NTP server. By default, the ntp.conf file on Cisco StadiumVision Director servers has configured the following Red Hat Linux public pool of servers:

```
server 0.rhel.pool.ntp.org
server 1.rhel.pool.ntp.org
server 2.rhel.pool.ntp.org
```

For these servers to be used as a reference clock, they must be reachable from the Cisco StadiumVision network.

If you want to use your own server, be sure to add it and comment out these default pool servers in the ntp.conf file. Otherwise, you do not need to do any further editing of the ntp.conf file in this task.

To set up the NTP host on Cisco StadiumVision servers, complete the following steps:

Step 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.

Step 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.

Step 3 To enter INSERT line editing mode, type **i**.

The vi editor changes to INSERT mode.

Step 4 If you have a server that you want to use as the reference clock source at your site, do the following:

- Add a line and type "**server** *ip-address*" or "**server** *dns-name*," where *ip-address* or *dns-name* is replaced by the IP address or name of the NTP server that you want to configure.
- Go to the lines where the pool servers are configured and add a "#" sign in front to comment them out of the configuration as shown below:

```
#server 0.rhel.pool.ntp.org
```

```
#server 1.rhel.pool.ntp.org
#server 2.rhel.pool.ntp.org
```

Step 5 To exit INSERT mode and return to vi command mode, press **Esc**.

Step 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.

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

Configuring the Time Zone

Configuring the time zone is required for both the Cisco StadiumVision Director and Cisco StadiumVision Director Remote servers.

Note Although there is an option to set the time zone in the Venues interface of the Control Panel on the Cisco StadiumVision Director server, this option is informational only and is also used for proof-of-play reporting. The actual time zone for the venue is configured from the TUI on the remote server.

This section includes the following tasks:

- Finding the Time Zone Code for System Configuration, page 23 (optional)
- Configuring the System Time Zone, page 24 (required)

Finding the Time Zone Code for System Configuration

Use this task if you need to find out the time zone code to configure the server's time zone information.

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:

Step 1 From the Date and Time Settings menu, do the following:

a. Select **Change Timezone**.

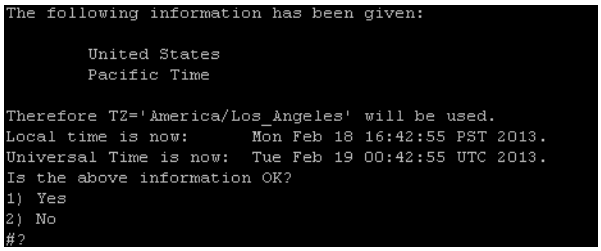
b. Type the number that corresponds to the applicable continent or ocean for the location of the remote server.

c. Type the number that corresponds to the country.

d. Type the number for the time zone (as applicable).

e. 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 5).

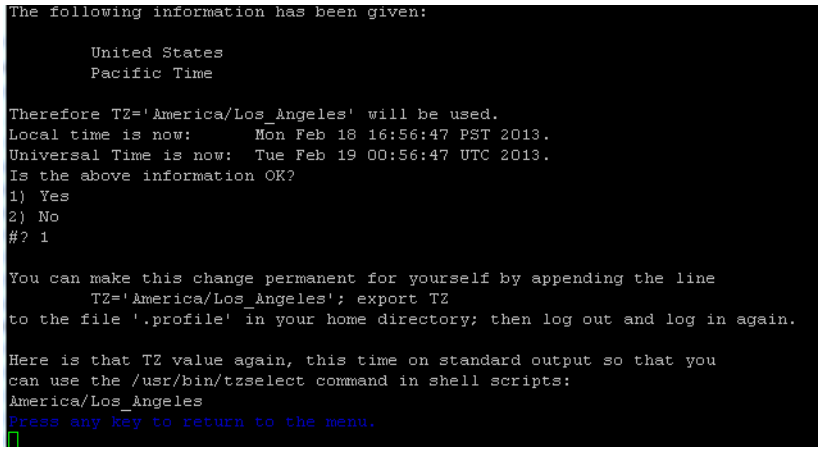
Figure 5 Time Zone Confirmation Prompt



f. After confirming Yes at the prompt, note the time zone string that is provided.

Figure 6 shows a sample time zone code for America/Los_Angeles.

Figure 6 Sample Time Zone Code



Step 2 Press any key to return to the Date and Time Settings menu.

Step 3 Configure the system time zone using the appropriate code for the server location. See the "Configuring the System Time Zone" section on page 24.

Configuring the System Time Zone

Prerequisites

Before you configure the system time zone, you should know the following information:

- How to use vi editor commands.
- The time zone code for the server location. If you need to look up the time zone code, see the "Finding the Time Zone Code for System Configuration" section on page 23.

Procedure

To configure the system time zone so that it persists after restart of the server, complete the following steps:

Step 1 From the TUI Main Menu on the server, go to **System Settings > Date and Time Settings > Change System Timezone**.

Step 2 At the prompt to edit the system clock file, press any key to continue.

The /etc/sysconfig/clock file is opened for editing.

Step 3 Use the vi editor to specify your time zone. Figure 7 shows an entry for the **"America/Los_Angeles"** time zone code.

Tip The quotation marks and underscore symbols are required.

Figure 7 Editing the Clock File

Step 4 To exit INSERT mode and return to vi command mode, press **Esc**.

Step 5 To save your changes, type **:wq!**.

Step 6 At the prompt, press any key to return to the Date and Time Settings menu.

Step 7 Restart the server to put the time zone changes into effect.

Restarting the Cisco StadiumVision Software

After you configure an NTP server and time zone in the TUI on the server, you must restart the software on the Cisco StadiumVision Director or Cisco StadiumVision Director Remote server.

To restart the Cisco StadiumVision software, complete the following steps:

Step 1 From the TUI Main Menu on the server, do one of the following according to the server that you need to restart:

- Go to **StadiumVision Server Administration > Restart StadiumVision software**.
- Go to **StadiumVision Remote Server Administration > Restart StadiumVision Remote software**.

Cisco StadiumVision Remote distribution is stopped and restarted.

Step 2 When the prompt appears, press any key to return to the Server Administration menu.

Step 3 Return to the Main Menu and exit the TUI.

Configuring the Date and Time Manually

Note This task is provided as a precaution if you should find it necessary to manually set the system date and time. Manual date and time configuration should be avoided on a production system and NTP service used instead.

To configure the date and time manually, complete the following steps:

Step 1 From the TUI Main Menu on the server, go to **System Settings > Date and Time Settings > Change Date and Time**.

Step 2 At the confirmation prompt, type **Y** to continue.

Step 3 Type the new date and time in the format: MMDDhhmm[[CC] YY] [.ss], where:

- MMDDhhmm is required (MM is month, DD is day, hh is hour, and mm is minutes).
- CC is the century (first 2 digits of the year) and is optional for use with YY. For example “20” in the year 2013.
- YY is the last 2 digits of the year and is optional. For example “13” in the year 2013.
- .ss is seconds and is optional.

Step 4 Press any key to return to the Date and Time Settings menu.

Configuring NTP on the Cisco DMP 4310G

In Release 3.2 and later releases, you must configure NTP on the Cisco StadiumVision Director server *and* the Cisco DMP 4310Gs. Granules are no longer used in Cisco StadiumVision Director for timing with the DMPs.

Through default MIB settings on the DMPs, the following values are preset and should not be modified:

- Time zone—Etc/UTC Coordinated Universal Time.
- Daylight Savings Time—Off.

Generally, the only values that you might consider changing are the NTP host and the sync interval. These values can be configured both globally and for selected DMPs.

This section includes the following tasks:

- Applying the Standard NTP Configuration on All Cisco DMP 4310Gs in the System, page 27 (recommended)
- Modifying the Standard NTP Configuration Globally on all Cisco DMP 4310Gs, page 27 (optional)
- Modifying the Standard NTP Configuration on Selected Cisco DMP 4310Gs in the System, page 29 (optional)

- Verifying Time Synchronization on the Cisco DMP 4310G, page 31 (recommended)

Applying the Standard NTP Configuration on All Cisco DMP 4310Gs in the System

The NTP service is automatically enabled for Cisco DMP 4310Gs, and uses the Cisco StadiumVision Director server as the host. If you do not plan to change the NTP host, then you can simply run the **Global DMP Settings** command to apply the standard configuration on all DMPs in the system.

To apply the standard NTP configuration on all Cisco DMP 4310Gs, complete the following steps:

Step 1 Log into the Cisco StadiumVision Director server as an administrator.

Step 2 Go to the **Management Dashboard**.

Step 3 Go to **DMP and TV Controls > Global Settings > Global DMP Settings**.

Step 4 Select All Devices and click the Play (>) icon to run the command.

All global MIB settings, including the new NTP settings, are sent to all DMPs.

Modifying the Standard NTP Configuration Globally on all Cisco DMP 4310Gs

Table 1 provides information about all of the global DMP NTP properties that can be specified in the Management Dashboard to control NTP service on all Cisco DMP 4310Gs.

Table 1 Global DMP 4310 v5.x.x.x Settings—NTP Property Values

Property (Registry Key)	Description	Values
NTP (Globaldmpsetting.common.deploy.init.startService_ntpc)	Enables or disables running of the NTP service on the DMP.	• **yes**—(Default) Enables NTP service to support playlist synchronization across DMPs. • **no**—Disables NTP service. • **Ignore**—
NTP Host (Globaldmpsetting.common.deploy.hostname)	IPv4 address of the NTP server.	Default—IP address of the Cisco StadiumVision Director server.

Table 1 Global DMP 4310 v5.x.x.x Settings—NTP Property Values (continued)

Property (Registry Key)	Description	Values
NTP sync interval (Globaldmpsetting.common.deploy.ntpc.interval)	Number of seconds that the DMP waits before trying to sync time with the configured NTP host. The DMP clock drifts, so setting the NTP sync interval too high can cause observable deterioration of synchronization over time. Playlist synchronization improves when the DMP updates its clock.	**40** (Default) **Note** Do not specify a value less than 40 due to a known problem in the DMP 4310G.
NTP status (Globaldmpsetting.common.info.ntpc.status)	Expected NTP status from the DMP for DMP compliance checking.	• **Synchronized to server** *svd-ip* **at stratum** *n*—Uses the IP address of the Cisco StadiumVision Director server and its NTP stratum level. **Note** If you change the NTP Host, you need to change keep this string but change the *svd-ip* and *n* arguments to reflect the corresponding values for that new host. • **$svd_ignore**—(Default) Skips this field during DMP compliance testing.

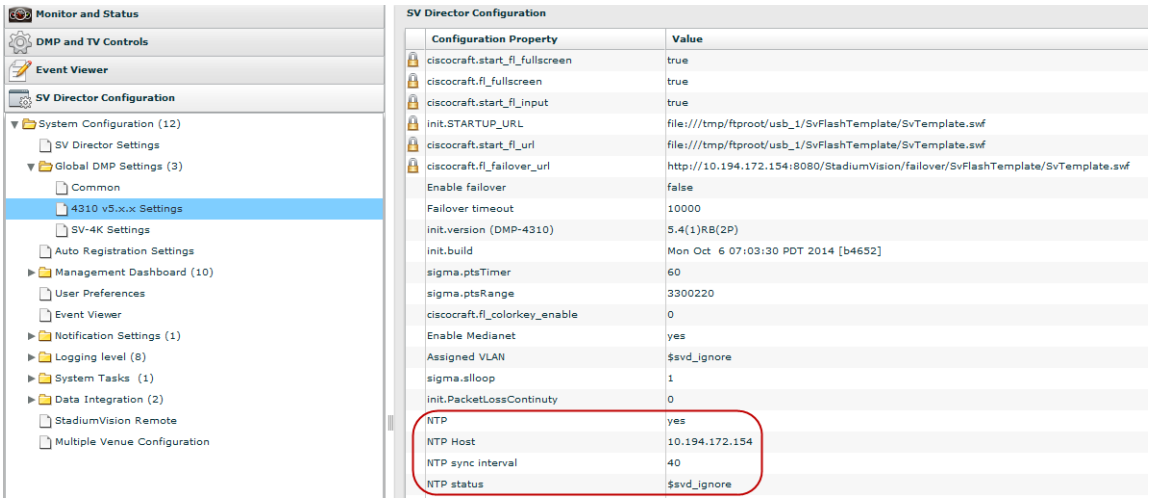
To modify the standard NTP configuration globally on all Cisco DMP 4310Gs, complete the following steps:

Step 1 Log into the Cisco StadiumVision Director server as an administrator.

Step 2 Go to the **Management Dashboard**.

Step 3 Click **SV Director Configuration > System Configuration > Global DMP Settings > Common** (Figure 8).

Figure 8 Global DMP Settings for NTP for the Cisco DMP 4310G



Step 4 To change the NTP Host, type the IPv4 address of the NTP server that you want the DMPs to reference.

Step 5 (Optional) In the NTP status property, change the IP address and stratum number according to the new NTP host.

Note To skip this field when performing DMP compliance checking, use the **$svd_ignore** value.

Step 6 (Optional) Change other global NTP properties as required for your environment. Refer to Table 1.

Step 7 Click the disk icon to Save changes (Figure 9).

Figure 9 Save Changes Icon

Step 8 Go to **DMP and TV Controls > Global Settings > Global DMP Settings**.

Step 9 Select All Devices and click the Play (>) icon to run the command.

All global MIB settings, including the new NTP settings, are sent to all DMPs.

Modifying the Standard NTP Configuration on Selected Cisco DMP 4310Gs in the System

Table 2 describes all of the NTP MIBs and their default values.

Note Under normal operation, only the ntpc.hostname and ntpc.interval MIBs should be modified.

Table 2 Cisco DMP 4310G NTP MIB Descriptions and Settings

MIB	Description	Required?	Values
init.startService_ntpc	NTP service on the DMP. **Note** Avoid modifying this MIB.	Yes	• **yes**—(Default) Enables NTP service to support playlist synchronization across DMPs. • **no**—Disables NTP service.
ntpc.dst	Daylight savings time parameter of the NTP service. **Note** Avoid modifying this MIB.	Yes	• **on**—(Default). • **off**—(Required).
ntpc.timezone	Time zone parameter of the NTP service. **Note** Avoid modifying this MIB.	Yes	**Etc/UTC**—(Default). Coordinated Universal Time. **Note** The Etc/UTC value is case sensitive and must be typed as shown.
ntpc.hostname	NTP server address (IPv4 format only).	Yes, when DMP NTP service is enabled.	• No value—(Default). • IPv4 address—(Required).
ntpc.interval	Number of seconds that the DMP waits before trying to sync time with the configured NTP host. The DMP clock drifts, so setting the NTP sync interval too high can cause observable deterioration of synchronization over time. Playlist synchronization improves when the DMP updates its clock.	Yes	**40** (Default) **Note** Do not specify a value less than 40 due to a known problem in the DMP 4310G.

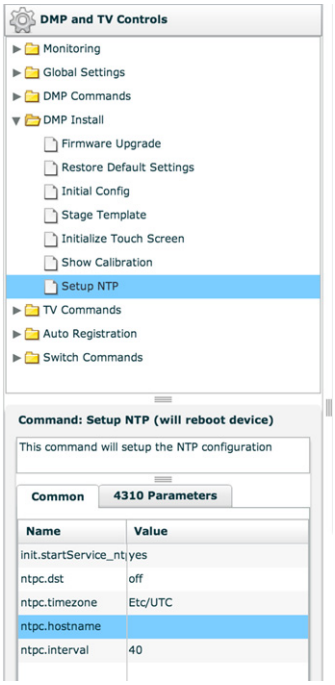
To modify the standard NTP configuration on selected Cisco DMP 4310Gs, complete the following steps:

Step 1 Log into the Cisco StadiumVision Director server as an administrator.

Step 2 Go to the **Management Dashboard**.

Step 3 Click **DMP and TV Controls > DMP Install > Setup NTP** (Figure 10).

Figure 10 DMP and TV Controls Setup NTP MIBs



Step 4 From the Common tab in the Command:Setup NTP section, specify the values of the NTP MIB variables according to the recommended and required values in In the Select Devices panel, select the DMPs where you want to setup the NTP service.

Step 5 Click the Play button to set the MIB values on the selected devices.

Verifying Time Synchronization on the Cisco DMP 4310G

You can find DMPs that are having problems synchronizing with the NTP server using the DMP compliance check in the Management Dashboard.

Before you can run a valid DMP compliance check for the DMP synchronization status, the "**Synchronized to server** *svd-ip* **at stratum** *n*" value of the NTP status global DMP properties must reflect the IP address of your NTP host and its stratum level.

Note Outside of Cisco StadiumVision Director, if you know the DMP IP address, you can find a single DMP's NTP status using a web browser and going to either of the following URLs:

http://*dmpIpAddress*

https://dmpIpAddress*/get_param?p=

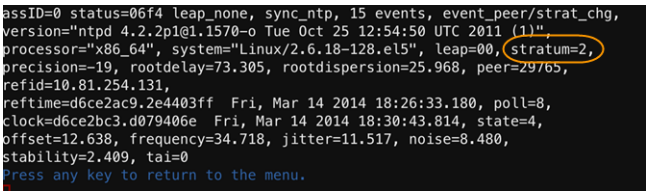
Find "ntpc.status". A sample line depicting unsuccessful time synchronization is:
ntpc.status T_STRING Not Synchronized

To verify time synchronization on the Cisco DMP 4310G, complete the following steps:

Step 1 Do one of the following to find and confirm the stratum level for the NTP host:

- If you are using the Cisco StadiumVision Director server as the NTP host:
  - Log into the TUI and go to **Troubleshooting > NTP > Local clock state** (Figure 11).

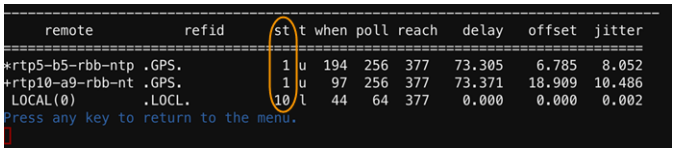
Figure 11 Stratum Field in Local Clock State TUI Output



Tip Alternatively, you can run a DMP **Get Status** command on one of the DMPs from the Management Dashboard and find the value reported in it ntpc.status MIB value.

- If you are using an NTP host other than the Cisco StadiumVision Director server:
  - Log into the TUI and go to **Troubleshooting > NTP > Show configured peers and clients**. Find the configured NTP host in the "refid" field and its corresponding stratum level under the "st" column.

Figure 12 Stratum Field in Show Configured Peers and Clients Output



Step 2 Go to the **Management Dashboard** and do the following:

- In the NTP status property, type the value to "**Synchronized to server** *svd-ip* **at stratum** *n*" and be sure that the IP address is set to your NTP host and the stratum level matches the level that you confirmed in Step 1.
- Run the **Global DMP settings** command to apply the configuration to all DMPs.

See the "Modifying the Standard NTP Configuration Globally on all Cisco DMP 4310Gs" section on page 27 for more information.

Step 3 Go to the **Management Dashboard**.

Step 4 Click **DMP and TV Controls > Monitoring > Get Status**.

Step 5 At the bottom of the screen, go to **Status > Compliance**.

Step 6 Find ntpc.status MIB and look for information about the synchronization status, such as "Not synchronized."

If your DMPs are not synchronized, see the "What To Do Next" section on page 33.

What To Do Next

If you find that DMPs are not synchronized:

- Confirm that you have met the requirements described in the "Prerequisites for Configuring NTP on Cisco StadiumVision Director Servers and DMPs" section on page 21.
- Verify your NTP host configuration to be sure that the proper IP address is configured.
- Verify reachability of the NTP server from the DMPs in your Cisco StadiumVision network.

For more information about other NTP troubleshooting on your network, refer to the following URL:

http://doc.ntp.org/3-5.93e/debug.html

Note After you verify DMP NTP synchronization, be sure to reset the NTP status field back to $svd_ignore because the stratum value can change.

Configuring NTP and PTP on the SV-4K Media Players

By default, both NTP and PTP services are automatically enabled for SV-4K media players. The SV-4K media players use PTP to achieve optimal synchronization. However, an NTP source also must be used to provide initial clocking to the SV-4K devices that are elected PTP masters in the network.

This section provides information about the default settings and how to modify them. It includes the following tasks:

- Restrictions for NTP and PTP on the SV-4K Media Players, page 33
- Guidelines for NTP and PTP on the SV-4K Media Players, page 34
- Modifying the Standard NTP and PTP Configuration on All SV-4Ks in the System, page 35 (optional)
- Verifying PTP Operation for the SV-4K Media Player, page 37

Restrictions for NTP and PTP on the SV-4K Media Players

Before you configure PTP on the SV-4K media players, consider the following restrictions:

- PTP messages will not cross VLANs. Therefore, PTP master candidates need to be identified for each VLAN and configured in the Management Dashboard.

  Note For ease of configuration for venues with multiple VLANs, the system is configured by default to list all SV-4K devices as eligible PTP master candidates. However, be aware that although this simplifies configuration, the time that it takes for the SV-4Ks to arbitrate a master SV-4K device in each network will vary, and depends on the number of eligible devices in each network.

- Content synchronization for video playback on the SV-4K media player relies on precise time across DMPs using PTP. The behavior is similar to content synchronization on the Cisco DMP 4310G. If SV-4K devices are playing video and one of the devices reboots, the rebooting unit will restart video playback from the beginning and will only synchronize with the other players when the next item in the playlist is rendered.

If SV-4Ks are participating in zone-based content synchronization for video walls, with some enhanced synchronization capability, the rebooting unit will synchronize with the current item being played by the device leader in the video wall. For more information, see the "Working with Video Walls" section of the *Cisco StadiumVision Director Operations Guide, Release 4.0*.

Guidelines for NTP and PTP on the SV-4K Media Players

Before you configure NTP and PTP on the SV-4K media players, consider the following guidelines:

- For new installations of Cisco StadiumVision Director Release 4.0, PTP is the default time source for the SV-4K media players, with NTP as the default time source for the elected SV-4K PTP master.

NTP Guidelines

- Each SV-4K media player designated as PTP master (per VLAN) will use NTP as its time source. The other SV-4K devices in the network operate using a PTP reference clock from the elected PTP master.
- When PTP is disabled (not recommended), all SV-4K players use NTP to set their local clock.

Note For synchronized video playback, NTP alone cannot be relied upon for SV-4K devices and PTP must be used.

- The default NTP synchronization interval with the host time server is one hour and is configurable.
- An NTP source must be configured in Cisco StadiumVision Director. By default, the Cisco StadiumVision Director server is configured as the SV-4K NTP host (just as with the Cisco DMP 4310G).

PTP Guidelines

- PTP version 2 is supported only for the SV-4K media players and applies globally to all devices in the Cisco StadiumVision Director network when configured.
- PTP configuration includes a PTP domain and a set of master candidates:
  - PTP domain—Default is 0.

    Be sure that this domain does not conflict with any other PTP domain (and multicast addressing) in use in your network, and revise as needed. See Table 3 for more information.
  - PTP master candidates—Default is *.

    This specifies that all SV-4K devices in the network are eligible as master candidates and will go through arbitration to designate a master for their respective subnets.
- If you revise the default PTP master candidates configuration, you must configure one or more SV-4K devices as master candidates in a semicolon-separated list of IP addresses for each VLAN.

  A minimum of two master candidates per network is recommended.
- If there is an in-house PTP master for your network, leave the "PTP master candidates" property value blank. However, this configuration is only supported for venues without multiple subnets.

Modifying the Standard NTP and PTP Configuration on All SV-4Ks in the System

By default the NTP and PTP services are automatically enabled and configured for SV-4K media players. Use this task if you need to modify the default settings described in Table 3 and Table 4.

Table 3 Global SV-4K Settings—PTP Property Values

Property (Registry Key)	Description	Values
PTP domain (Globaldmpsetting.sv4k.init.ptp.domain)	Domain number for the SV-4K PTP network, which defines the multicast address for PTP communication.	For IEEE-1588 PTP, possible values are: • **0**—(Default) 224.0.1.129 • **1**—224.0.1.130 • **2**—224.0.1.131 • **3**—224.0.1.132
PTP master candidates (Globaldmpsetting.sv4k.init.ptp.master.host)	Eligible SV-4K devices for master candidate selection.	Possible values are: • ***—(Default). Wildcard pattern that specifies all SV-4K devices in the network as eligible PTP master candidates. • Semicolon-separated IPv4 addresses of SV-4K devices for each subnet. **Example:** 10.0.0.3;10.0.0.4;192.168.0.5;192.168.0.6 • blank—Specifies that a PTP master source external to Cisco StadiumVision Director is used. This configuration is only valid for a venue without SV-4K devices in multiple subnets.

Table 4 Global SV-4K Settings—NTP Property Values

Property (Registry Key)	Description	Values
NTP Host (Globaldmpsetting.sv4k.deploy.ntpc.hostname)	IPv4 address of the NTP server.	Default—IP address of the Cisco StadiumVision Director server.
NTP sync interval (Globaldmpsetting.sv4k.deploy.ntpc.interval)	Number of seconds that the SV-4K waits before trying to synchronize its time with the configured NTP host.	**3600** (Default)
Timezone (Globaldmpsetting.sv4k.deploy.ntpc.timezone)	Code for the timezone to be used.	**GMT** (Default)

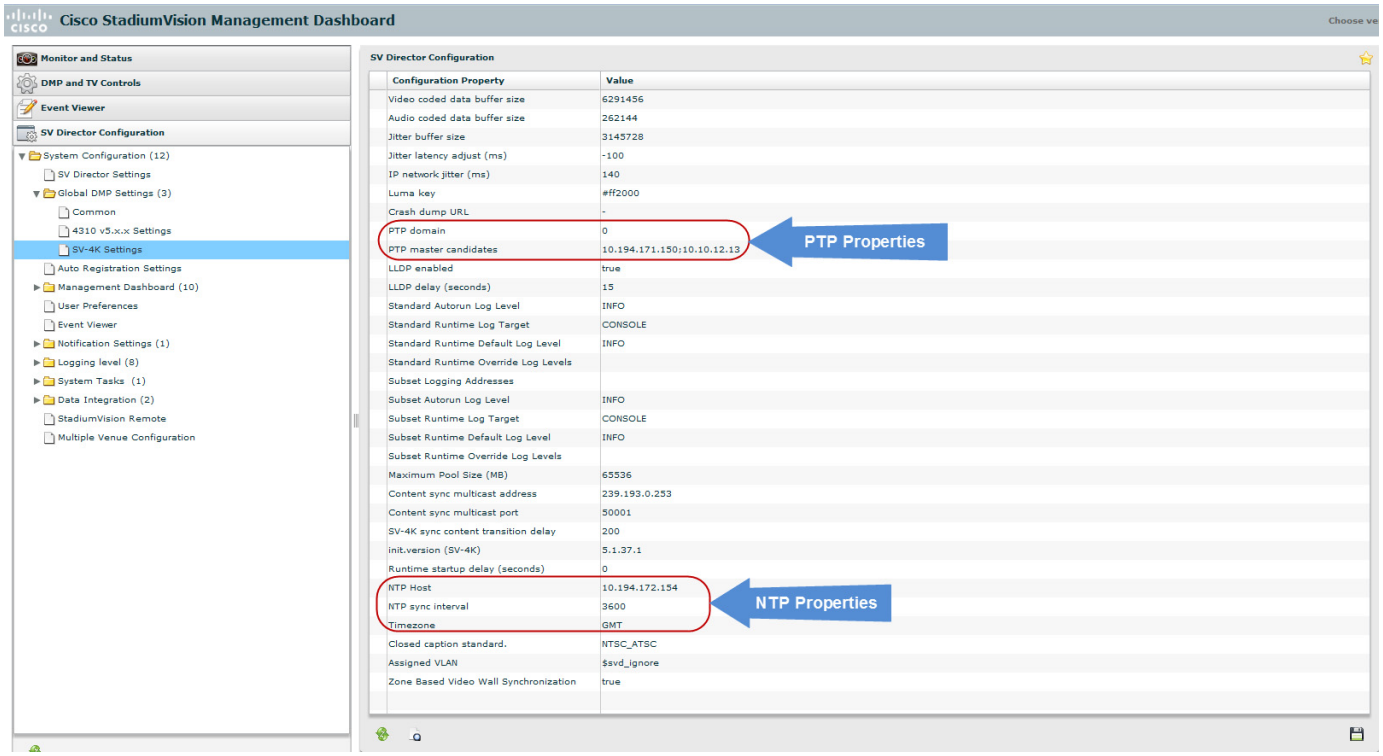
To modify the standard NTP and PTP configuration on all SV-4Ks, complete the following steps:

Step 1 Log into the Cisco StadiumVision Director server as an administrator.

Step 2 Go to the **Management Dashboard**.

Step 3 Go to **SV Director Configuration > System Configuration > Global DMP Settings > SV-4K Settings** (Figure 13).

Figure 13 Global DMP Settings for NTP and PTP on the SV-4K



Step 4 (Optional) Change the global PTP properties as required for your network. Refer to Table 3.

Step 5 (Optional) Change the global NTP properties as required for your environment. Refer to Table 4.

Step 6 Click the disk icon to Save changes.

Step 7 Reboot the SV-4K devices.

Verifying PTP Operation for the SV-4K Media Player

This section describes how to verify the PTP configuration and also the operation of PTP for your SV-4K devices.

To verify the PTP operation for the SV-4K media player, complete the following steps:

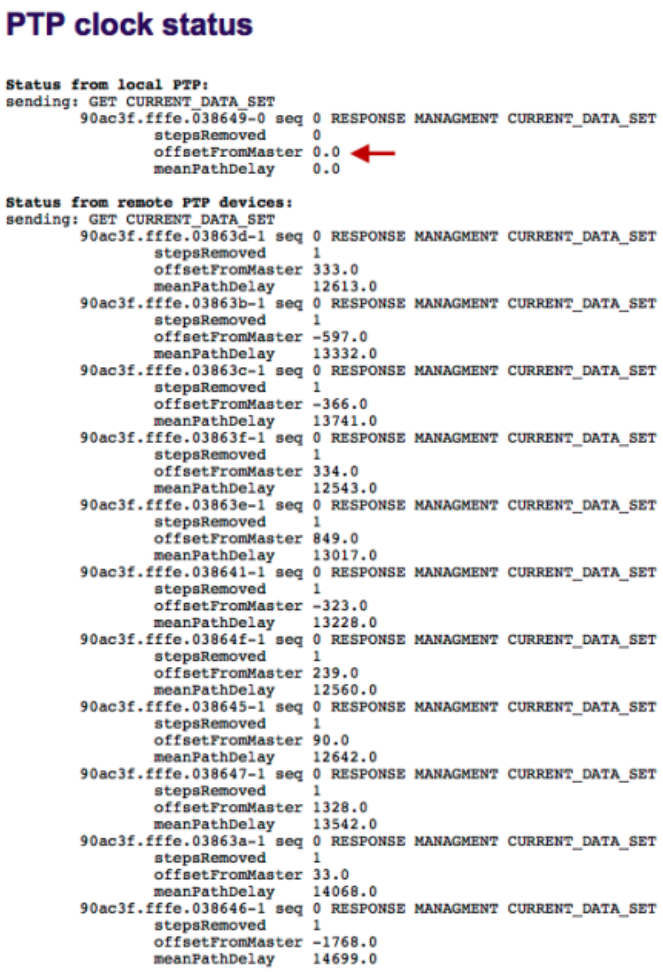
Step 1 Open your browser and navigate to one of the DMPs:

http://*sv4k-ip-address***/ptp.html**

Step 2 Identify the PTP master by finding the unit that has an "offsetFromMaster" value of 0.0.

Figure 14 highlights the PTP master and shows a network where PTP is operating successfully with 12 SV-4K members.

Figure 14 Successful PTP Clock Operation



Configuring Multicast Ports for Cisco StadiumVision Director

This section includes the following topics:

- Information about Multicast Support in Cisco StadiumVision Director, page 38
- Prerequisites for Configuring Multicast Ports in Cisco StadiumVision Director, page 42
- How to Configure Multicast Ports in Cisco StadiumVision Director, page 42

Information about Multicast Support in Cisco StadiumVision Director

This section includes the following topics:

- Per-Script Multicast Optimization, page 39
- Multicast Registry Keys in Cisco StadiumVision Director, page 40

Per-Script Multicast Optimization

In Cisco StadiumVision Director Release 3.2 and later releases, the original Multicast Optimization introduced in Release 3.1 is replaced by Per-Script Multicast Optimization (for up to 20 different scripts) to reduce the number of multicast messages that each DMP must process.

Per-Script Multicast Optimization is designed to reduce the load on DMPs when the following conditions are present in Cisco StadiumVision Director:

- More than one event script is run simultaneously in a venue.

  The scripts can be running across multiple venues, scripts running in a single venue, or running in systems without Cisco StadiumVision Director Remote servers.

- The External Content Integration feature is used, which sends multiple messages to the DMPs in a script.

Table 5 provides a summary of the two different multicast optimization features supported in Cisco StadiumVision Director.

Table 5 Summary of Multicast Optimization Features in Cisco StadiumVision Director

Feature Name	Release	Scope	Remote Servers Required	Default
Multicast Optimization[1]	3.1 only	Per Site	Yes	Automatic when multi-venue support is enabled.
Per-Script Multicast Optimization	3.2 and later	Per Script (20 maximum)[2]	No	Disabled.

1. For information about per-site multicast optimization in Cisco StadiumVision Director Release 3.1, see the "Multicast Optimization for Remote Venues" topic in the "Configuring Cisco StadiumVision Director for Multiple Venue Support" module of the *Cisco StadiumVision Director Server Administration Guide, Release 3.1*.
2. If you are running more than 20 scripts, then the first 20 scripts operate using per-script multicast channels, and the additional scripts are run over the global multicast host port.

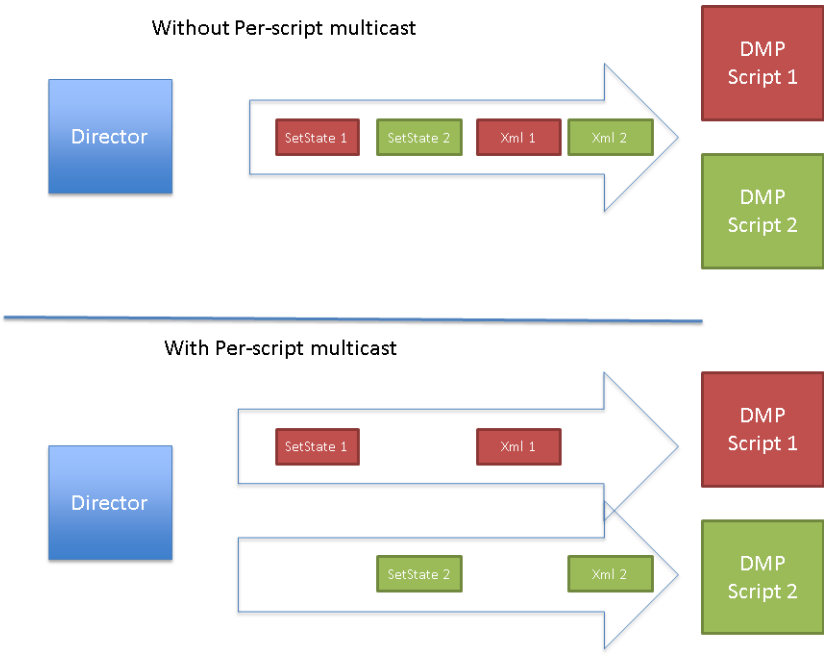
Benefits of Per-Script Multicast

In releases of Cisco StadiumVision Director 3.1 and earlier, the server uses a single multicast channel for all DMPs. In Release 3.2 and later, you can configure multiple multicast channels, over which the server sends only the multicast messages needed for a particular event script for up to 20 scripts.

If you are running more than 20 scripts, then the first 20 scripts operate using per-script multicast channels, and the additional scripts are run over the global multicast host port.

Figure 15 shows this message separation. Each DMP goes from seeing four packets to seeing two. More importantly, each DMP now only has to process one XML payload, which is important when the XML payloads are sizeable.

Figure 15 Multicast Messaging With and Without Per-Script Multicast Optimization



All DMPs, including those associated with a Cisco StadiumVision Director Remote server, listen on these per-script multicast channels.

For messages that apply to multiple event scripts, the message is duplicated and sent to each multicast channel. Therefore, this feature can increase the load on Cisco StadiumVision Director and Cisco StadiumVision Director Remote servers (increasing the number of messages sent and copying of messages) as a tradeoff for reducing the number of messages seen and processed by DMPs. However, this load is expected to be negligible.

Multicast Registry Keys in Cisco StadiumVision Director

Cisco StadiumVision Director uses multicast messages for DMP control-plane operation. Cisco Connected Stadium network design assigns the following multicast group addresses for use by Cisco StadiumVision Director:

- 239.193.0.0/24—For control communication
- 239.192.0.0/24—For video communication (This network should be avoided for the multicast configuration described in this module.)

Multicast addressing is configured using registry keys from the Cisco StadiumVision Director Management Dashboard.

Table 6 describes the registry keys in Cisco StadiumVision Director that control the multicast configuration.

Note The default PTP domain 0 uses multicast address 224.0.1.129. For more information, see Table 3 on page 35.

Table 6 Multicast Registry Keys in Cisco StadiumVision Director

Registry Key	Default Value	Description
Globaldmpsetting.sv4k.init.dmpsync .multicast.address	239.193.0.153	Sets the global multicast address used for zone-based synchronization on the SV-4K.
Globaldmpsetting.sv4k.init.dmpsync .multicast.port	50001 **Note** The system automatically uses an additional port based on this default (default + 1) for secondary video. In the case of the 50001 default, 50002 is also reserved for secondary video use.	Sets the default port for the primary video for zone-based synchronization multicast address on the SV-4K.
MulticastHostPort	239.192.0.254:50001 **Caution** This default multicast address should be changed after installation to use the **239.193**.0.0/24 address range, or the network that is configured in your Cisco Connected Stadium network for Cisco StadiumVision control.	Sets the global multicast address and port for Cisco StadiumVision Director.
transport.dynamic.enable	• False (for upgraded servers). Per-Script Multicast Optimization is disabled and the Cisco StadiumVision Director server sends all communication over the MulticastHostPort address directly to all DMPs and Cisco StadiumVision Director Remote servers, including all remote DMPs. • True (for new installations)	Enables and disables Per-Script Multicast optimization.
transport.dynamic.send_range	50080-50099 If the MulticastHostPort registry key is 239.193.0.254:50001, then 239.193.0.254:50080–239.193.0.254:50099 is used as the range of Global hostports for the running scripts.	Specifies the range of ports for Per-Script Multicast Optimization. These ports are used with the network specified in the MulticastHostPort registry key, to define a range of additional global hostports to be assigned for running scripts.

Prerequisites for Configuring Multicast Ports in Cisco StadiumVision Director

Before you configure multicast ports, be sure that the following requirements are met:

- Be sure that you understand the multicast addressing in use for all areas of your Cisco StadiumVision network, including Cisco Connected Stadium and Cisco StadiumVision Mobile networks. Confirm that there are not any multicast address/port overlaps.

Caution Because of the large number of ports that per-script multicast configuration requires, and the possibility for hard-to-diagnose failures if video is routed to a DMP's control channel (which can occur when the port numbers are the same and even if the group/host portion is different), it is critical to verify that the port ranges you plan to use are not used by any other source of multicast in the network.

  - For a summary of all of the input and output ports in use by Cisco StadiumVision Director and Cisco StadiumVision Director Remote, see the "Appendix B: Port Reference" module in the *Cisco StadiumVision Director Software Installation and Upgrade Guide, Release 4.0*.
  - For more information about the recommended multicast addressing for the Cisco Connected Stadium network, see the *Cisco Connected Stadium Design Guide* available from your Cisco Systems representative.
- The network is properly configured to route the global multicast host port to be visible for all DMPs in the Cisco StadiumVision network, including those at remote venues and associated to venues in a multi-venue environment.

How to Configure Multicast Ports in Cisco StadiumVision Director

This section includes the following tasks:

- Configuring the Global Multicast Host Port in Cisco StadiumVision Director, page 42 (required)
- Configuring Per-Script Multicast in Cisco StadiumVision Director, page 43 (recommended)
- Configuring Multicast Support for Zone-Based Content Synchronization for the SV-4K, page 44 (optional)

Configuring the Global Multicast Host Port in Cisco StadiumVision Director

The global multicast host port is used by Cisco StadiumVision Director to send messages to DMPs when they are not part of a script, when per-script multicast is disabled, or when the number of scripts running exceeds to configured maximum of per-script multicast ports.

It is configured in the "MulticastHostPort" registry key in the Management Dashboard.

Note The default value currently uses the address 239.192.0.254:50001 and should be changed to a network address in the range 239.193.0.0/24.

To verify or configure the multicast addressing for Cisco StadiumVision Director, complete the following steps:

Step 1 From the Management Dashboard, select **Tools** > **Advanced** > **Registry**.

Step 2 Scroll to the "MulticastHostPort" registry key in the Parameters list and confirm the entry for the registry.

Step 3 Click on the value field and specify a multicast address in the range 239.193.0.0/24 and port number.

Note Be sure to use the value that is configured in your Cisco Connected Stadium network for Cisco StadiumVision Director control messages and include the **:***port*. The recommended default is **:50001**.

Step 4 Click **Apply**.

Configuring Per-Script Multicast in Cisco StadiumVision Director

By default, Per-Script Multicast Optimization is disabled and the Cisco StadiumVision Director server sends all communication over the MulticastHostPort address directly to all DMPs and Cisco StadiumVision Director Remote servers, including all remote DMPs.

To configure per-script multicast, complete the following steps:

Step 1 From the Management Dashboard, select **Tools > Advanced > Registry**.

Step 2 To enable per-script multicast, change the values of the following registry keys:

- **transport.dynamic.enable**—Specify a value of **true**.
- **transport.dynamic.send_range**—(As Required) Change the range of ports to comply with your network configuration. The default is 50080-50099.

Note Be sure that these ports do not overlap with other multicast ports in use on your network.

Step 3 Click **Apply**.

Step 4 Reload the Flash template on all DMPs:

a. From the DMP and TV Controls dashboard drawer, navigate to and select the following command: **DMP and TV Controls > DMP Install > Stage Template**.

b. Select all of the DMP devices where the command should be applied.

c. Click the Play button to run the command on the selected devices.

Step 5 To verify the configuration:

a. Start and stop event scripts and change states.

b. Verify that the multicast port that the DMP is listening on is one of the per-script ports (50080-50099 by default), rather than the global multicast hostport (50001).

If the scripts do not sart and stop, see the "Troubleshooting Per-Script Multicast Configuration" section on page 43.

Troubleshooting Per-Script Multicast Configuration

This section includes information about troubleshooting the following behaviors when per-script multicast optimization is enabled:

- Scripts Unable to Start or Stop, page 44

- DMPs Rebooting, page 44

Scripts Unable to Start or Stop

Verify that the multicast packets are reaching the DMPs using any or all of the following methods:

- Look at the sv_msg_mcast_trace.log available from the Troubleshooting menu of the TUI for Cisco StadiumVision Director in the Control logs.
- Use a packet sniffer device at Cisco StadiumVision Director and/or at the DMP.
- Inspect the multicast configuration of the Cisco Connected Stadium switch by turning on debug for multicast group subscriptions.

Tip It is valuable to know the multicast group/port that a specific DMP should be listening on. This can be validated using the dmpconfig debug feature, by going to the URL:

http://svd-ip:8080/StadiumVision/dmpconfig/000000000000?ipaddr=x.x.x.x, where

x.x.x.x is the IP address of the DMP to be debugged.

In the XML output provided, you will see the multicast IP address and port in use.

DMPs Rebooting

DMPs rebooting or becoming unresponsive while per-script multicast is enabled is most likely due to some multicast video port overlap with the ports used for multicast control.

To diagnose this condition:

- Inspect all multicast port numbers in the configuration to investigate any multicast group/port overlaps.
- Using a packet sniffer, inspect network traffic on a separate box and via port span rather than on a DMP.

Configuring Multicast Support for Zone-Based Content Synchronization for the SV-4K

Zone-based content synchronization provides enhanced recovery for video walls if an SV-4K reboots during the running of a playlist. It is intended for dedicated video walls running video content of longer duration (> 15 minutes).

The default multicast address and ports are automatically configured to support zone-based content synchronization for the SV-4K upon installation of the Cisco StadiumVision Director software; however, the feature is not enabled by default.

Use this task to change the default multicast values as needed, when you assess your system-wide multicast addressing needs.

Note By default, zone-based content synchronization is not enabled for the SV-4K. For more information, see the “Working with Video Walls” section of the *Cisco StadiumVision Director Operations Guide*.

To configure multicast support for zone-based content synchronization for the SV-4K, complete the following steps:

Step 1 From the Management Dashboard, go to **SV Director Configuration > System Configuration > Global DMP Settings > SV-4K Settings**.

Step 2 Verify that the following default values for the following properties are compatible for your network, and change as required:

- **Content sync multicast address**—239.193.0.253
- **Content sync multicast port**—50001

Step 3 Save your changes.

What To Do Next

After you have configured the system settings for your Cisco StadiumVision Director servers, be sure to do the following:

- Configure the backup environment between your primary and secondary servers. For more information, see the "Backing Up and Restoring Cisco StadiumVision Director Servers" module on page 89.
- If you are configuring Cisco StadiumVision Director Remote servers:

  The centralized Cisco StadiumVision Director server is configured by default to use a global account for communication with all Cisco StadiumVision Director Remote servers to support monitoring of venues from the Management Dashboard. Using the default configuration, you can specify a common password to be used by all Cisco StadiumVision Director Remote servers.

  You can change the default configuration and specify a unique password for each remote server. To do this, you must modify the global credential on the Cisco StadiumVision Director server, and then configure a password in the Venues interface from the Control Panel on the Cisco StadiumVision Director server.

  Whether you are using a common or unique password, the remote server must be configured to use the same password that is configured on the Cisco StadiumVision Director server for that venue.

  For more information about configuring Cisco StadiumVision Director to support remote servers and multiple venue support, see the following modules:

  - "Configuring Cisco StadiumVision Director Remote Servers" module on page 47.
  - "Configuring Cisco StadiumVision Director for Multiple Venue Support" module on page 57.