Configuring Cisco SG Switches for Tesira Control and Dante

This article describes how to configure a Cisco SG small business series switch for use with Tesira and Dante. The examples given are for the SG350-28P model. The SG family contains several series of switches and the configuration process is similar.

Tesira Control traffic and Dante will operate using the out-of-box defaults of the switch. Tesira Control and Dante do not inherently require separation and can both exist in the same default VLAN. Separating Tesira Control and AV media into different VLANs is a best practice as the system increases in size.

Multicast traffic

Tesira and Dante use multicast traffic for peer discovery, hostname resolution, and clocking. Traffic is delivered to a multicast address and the switch sends it to all ports by default. This is also known as traffic flooding. This is not problematic for a small network with a limited number of devices. It does become an issue as more devices are actively transmitting on the network. IGMP Snooping provides a mechanism to constrain multicast traffic to specific ports. Devices join multicast groups and receive only the desired traffic. However, not all multicast address ranges are managed by IGMP and not all switches implement IGMP Snooping in the same manner.

Local-scope multicast addresses are defined in the range of 224.0.0.x. IGMP Snooping on Cisco SG Series switches does not register group joins on local-scope multicast addresses. The switch refers to this as unregistered multicast traffic and filters (drops) it by default. Tesira and Dante discovery mechanisms utilize local-scope addresses to communicate with other devices and Tesira expanders, such as the HD-1 dialer or EX-AEC. When IGMP Snooping and Bridge Filtering is enabled on SG switches to manage large quantities of traffic, Tesira devices will lose communication and discovery.

Careful configuration is required when mixing Control, Dante and other network streaming services such as video-over-IP devices or networked cameras.

Configuring the switch

The following configuration process is performed on the SG350-28P. The process is similar for other SG Series switches. Please refer to the Cisco documentation for specific details.
Connect to the switch

The Cisco SG switches have the Web UI enabled by default. Using the command line interface is beyond the scope of this article. Connect to the switch using the following default values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN Management IP</td>
<td>192.168.1.254 / 24</td>
</tr>
<tr>
<td>Username</td>
<td>cisco</td>
</tr>
<tr>
<td>Password</td>
<td>cisco</td>
</tr>
</tbody>
</table>

The default VLAN is configured to 192.168.1.254 with a subnet of /24 or 255.255.255.0. Any port on the switch will access the management IP since it is the default VLAN. Configure the connected computer to the same subnet and browse to [http://192.168.1.254/](http://192.168.1.254/) for the login page. If login in for the first time, the switch will require changing the password from the default. Follow Cisco's instructions to factory reset the switch in the event the password or management IP has been lost.

Once connected to the switch management page, switch the Display Mode from Basic to Advanced:

![Switch Management Page](image)

Remember to Save after applying any new values by clicking the flashing Save button at the top of the window.

Configure Multicast Management with IGMP Snooping

Enable Bridge Filtering on Multicast Properties

Enable the bridge filtering to activate the multicast management protocols on the switch.

1. Use the left navigation menu to open Multicast > Properties
2. Check enable on Bridge Multicast Filtering Status
3. Click Apply
Enable IPv4 IGMP Snooping

Enable IGMP snooping on the switch.

1. Navigate to Multicast > IPv4 Multicast Configuration > IGMP Snooping
2. Check enable for IGMP Snooping Status
3. Click Apply to change the setting

Edit IGMP Snooping Settings

Now edit the IGMP settings for VLAN 1. If multiple VLANs are configured, edit the appropriate Control or Dante VLAN number.

1. Keep the same IGMP Snooping settings page open
2. Select the radio button for the VLAN to edit
3. Click the Edit... button to open the edit window (Verify the browser did not block a pop-up window.)
4. Click Enable on IGMP Snooping Status
5. Click Enable on Immediate Leave
6. Click Enable on IGMP Querier Status
7. Click Apply and close the window

Note: Anecdotally, on some versions of SG300 firmware Tesira server-class devices and/or expanders can lose discovery at this point. Continue to the next section to modify how the switch filters (drops) or forwards multicast traffic.

**Configure Unregistered Multicast**

The switch by default will forward unregistered multicast traffic. Tesira utilizes unregistered multicast for device discovery. Enable forwarding on all the Tesira control and expander device ports. Enable filtering for all Dante ports. The following example shows Dante on ports 1-12 and Tesira control on ports 13-24. It may be configured in any manner required.

1. Navigate to Multicast > Unregistered Multicast
2. Enable Filtering on Dante device ports
3. Leave Forwarding enabled on Tesira device control ports
Tesira Control and Discovery will function properly after the ports have been configured to allow forwarding of registered traffic. Note that some Dante functions use unregistered local-scope multicast addresses. See the Dante network overview from Audinate for specific details. Certain monitoring or mDNS functionality may necessitate configuring all Dante ports to also use unregistered multicast Forwarding or manually configuring 224.0.0.x multicast groups show in the optional section below.

**Disable EEE**

Energy Efficiency Ethernet (EEE, a.k.a Green Ethernet) allows link states to enter low power mode for energy savings. While it works extremely well for business applications on computers, this often results in disruptions to AV device communication and network media clocking.

1. Navigate to Port Management > Green Ethernet > Properties
2. Uncheck Enable on 802.3 Energy Efficient Ethernet (EEE)
3. Click Apply

**Save Changes**

Any applied changes require saving to the startup configuration. Unsaved changes will be lost if the switch reboots or loses power. Click the flashing Save option to write changes to memory.
Optional configuration

In some cases, forwarding of unregistered multicast is not allowed on the network. This requires extra steps to manually configure multicast groups and statically assign ports to received that traffic. Blocking unregistered multicast and not configuring groups will cause Tesira and Dante automatic device discovery mechanisms to fail.

The following multicast address groups will need to be configured on the switch:

<table>
<thead>
<tr>
<th>Multicast Address</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.0.251</td>
<td>mDNS hostname resolution</td>
</tr>
<tr>
<td>224.0.0.252</td>
<td>Server-Class peer discovery</td>
</tr>
<tr>
<td>224.0.0.253</td>
<td>Sever-to-Remote device discovery</td>
</tr>
<tr>
<td>224.0.0.254</td>
<td>Remote-to-Server device discovery</td>
</tr>
</tbody>
</table>

Add multicast group addresses

1. Navigate to Multicast > IP Multicast Group Addresses
2. Click Add... to bring up the add window. (Verify the browser did not block a pop-up window.)
3. Check the correct VLAN ID is present.
4. Add the IP Multicast Group Address
5. Click Apply.
6. Repeat steps 1 - 5 for all multicast addresses used by Tesira in the table above.
Statically Assign Groups to Ports

The switch does not automatically understand which ports should receive traffic from a given Multicast Group. Every Tesira control port needs all the multicast groups assigned to it for discovery to operate. The following example shows Tesira control devices on ports 13-24. The switch may be configured in any manner.

1. After adding all the multicast IP address groups from the previous step, select the first IP address check box.
2. Click the Details... button. (Verify the browser did not block a pop-up window.)
3. Set the ports with Tesira control devices to Static. Forbidden or None will prevent delivery of traffic for the given address.
4. Click the Apply button and close the window.
5. Repeat the above steps for all the 224.0.0.x multicast addresses used by Tesira.
6. Save the configuration or else any changes are lost when the switch reboots.

Further reading

- Adding Dante to your Network (www.audinate.com) (PDF)
- Dante
- Tesira Network Infrastructure