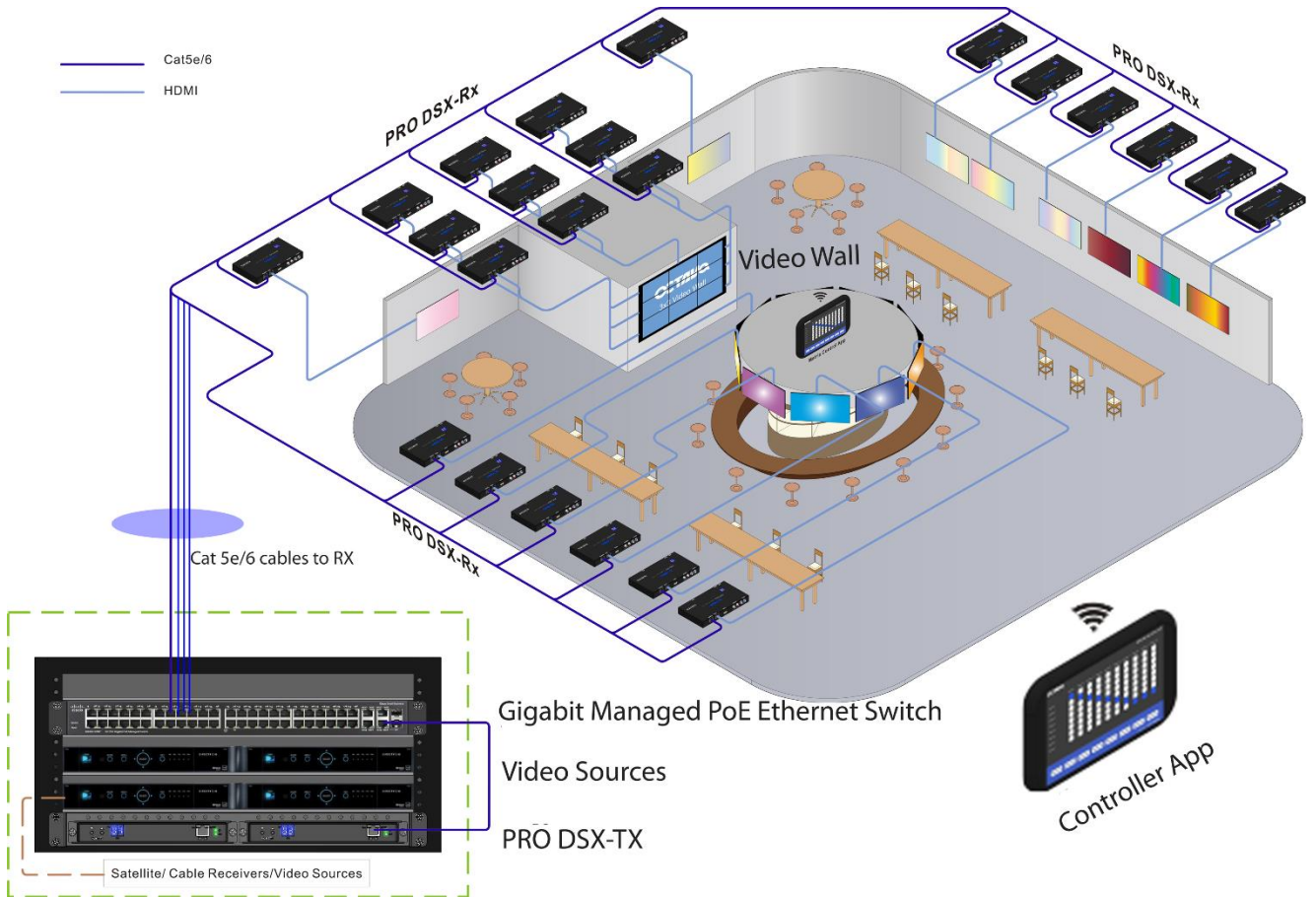


HDMI Over IP-PRO DSX Basic Network Switch Configuration For Cisco SG300/500 series

Revision: 1.2
Date: 8/29/18



System Application Diagram



Customizable Matrix Control App (available for iOS, and Android Devices)

HDMI Over IP-PRO DSX

Basic Network Switch Configuration for Cisco SG300/500 series

Introduction:

Scope: This guide provides a reference for configuring your network switch for use with the PRO DSX HDMI over IP Distribution System.

This configuration guide is based on the SG300 running firmware 1.4.1.3 or later. It is recommended that the firmware is up to date before continuing.

In this guide we will configure the network switch so some of the advanced features are enabled:

Jumbo frame : jumbo frames are Ethernet frames with more than 1500 bytes of payload.

Multicast Video: Multicast as compared to Unicast is a more efficient method of delivering video to multiple clients. Multicasting requires only 1 “channel/group” to be transmitted regardless of number of clients that will subscribe to the “channel/group”. Unicast would require 1 stream for each client , thus would increase the bandwidth requirement by N(number of clients).

IGMP (internet group management protocol): IGMP Querying/Snooping, optimizes network loading by ensuring that Multicast traffic is only forwarded to ports that are members of that Multicast group.

1. Connect a LAN cable directly from your PC to the “last” port of your SG-300-xx Ethernet switch.
For example, if you have a SG-300-28. Connect to the G28 port.



2. Login into the Cisco SG-300 per the instructions shown here. You may refer to the Cisco user manual as well.

Accessing and Managing Your Switch

Use the Web-Based Interface

To access the switch by using the web-based interface, you must know the IP address the switch is using. The switch uses the factory default IP address of **192.168.1.254** by default.

When the switch is using the factory default IP address, the System LED flashes continuously. When the switch is using a DHCP server-assigned IP address or an administrator has configured a static IP address, the System LED is on solid (DHCP is enabled by default).

NOTE If you are managing the switch through a network connection and the switch IP address is changed, either by a DHCP server or manually, your access to the switch will be lost. You must enter the new IP address the switch is using into your browser to use the *web-based interface*. If you are managing the switch through a console port connection, the link is retained.

To configure the switch through an IP network:



STEP 1 Power on the computer and the switch.

STEP 2 Set the IP configuration on your computer.

- a. If the switch is using the factory default IP address of **192.168.1.254**, you must choose an IP address for the computer in the range of 192.168.1.1—192.168.1.253 that is not already in use.
- b. If the IP address is assigned by a DHCP server, make sure the DHCP server is running and can be reached from the switch and the computer. It might be necessary to disconnect and reconnect the devices for them to discover their new IP addresses from the DHCP server.

NOTE Details on how to change the IP address on your computer depend upon the type of architecture and operating system you are using. Use the computer Help and Support functionality to search for “IP Addressing.”

STEP 3 Open a Web browser window. If you are prompted to install an Active-X plug-in when connecting to the device, follow the prompts to accept the plug-in.

STEP 4 Enter the switch IP address in the address bar and press **Enter**. For example, **http://192.168.1.254**.

The *Switch Login Page* displays.

STEP 5 Enter the default login information:

- Username is **cisco**
- Default password is **cisco** (passwords are case sensitive)

STEP 6 If this is the first time that you have logged on with the default username and password, the *Change Password Page* opens. The rules for constructing a new login and password are displayed on the page. Enter a new administrator password and click **Apply**.



CAUTION

Make sure that any configuration changes made are saved to the Startup configuration before exiting from the web-based interface by clicking on the **Save** icon. Exiting before you save your configuration will result in all current changes being lost the next time the switch is rebooted.

3. Check Firmware Version

Go to : **Status and Statics > System Summary**

The screenshot shows the configuration page for a Cisco SG300-10P 10-Port Gigabit PoE Managed Switch. The page is titled "SG300-10P 10-Port Gigabit PoE Managed Switch" and includes a language dropdown menu set to "English". The left sidebar shows a navigation menu with "System Summary" selected. The main content area is divided into two sections: "System Information" and "Software Information".

System Information		Software Information	
System Operational Mode:	L2 Mode	Firmware Version (Active Image):	1.4.1.3
System Description:	SG300-10P 10-Port Gigabit PoE Managed Switch	Firmware MD5 Checksum (Active Image):	e6e1243d05a6228d03bfb562616b78bb
System Location:	Edit	Firmware Version (Non-active):	1.3.5.58
System Contact:	Edit	Firmware MD5 Checksum (Non-active):	482fea5c6731bc9d2739cea78235720

4. Enable JUMBO Frame

Go to : Port Management > Port Settings. Enable JUMBO Frames

The screenshot shows the configuration page for a Cisco SG300-10P switch. The left sidebar contains a navigation menu with 'Port Management' expanded to 'Port Settings'. The main content area is titled 'Port Settings' and features a red-bordered box around the 'Jumbo Frames: Enable' option. Below this, there is a note: 'Jumbo frames configuration changes will take effect after saving the configuration and rebooting the switch.' and two buttons: 'Apply' and 'Cancel'.

Below the configuration area is a 'Port Setting Table' with the following data:

Entry No.	Port	Description	Port Type	Operational Status	Link Status SNMP Traps	Time Range		Port Speed	Duplex Mode	LAG	Protection State
						Name	State				
1	GE1		1000M-Copper	Down	Enabled						Unprotected

5. Enable Bridge Multicast Filter Status

Go to : Multicast> Properties. Enable Bridge Multicast Filter Status

The screenshot shows the configuration page for a Cisco SG300-10P switch. The left sidebar contains a navigation menu with the following items: Getting Started, Status and Statistics, Administration, Port Management, Smartport, VLAN Management, Spanning Tree, MAC Address Tables, Multicast (expanded), Properties (highlighted), MAC Group Address, IP Multicast Group Address, IPv4 Multicast Configuration, IPv6 Multicast Configuration, IGMP/MLD Snooping IP Multicast, Multicast Router Port, Forward All, and Unregistered Multicast. The main content area is titled 'Properties' and contains the following settings: 'Bridge Multicast Filtering Status' is checked and set to 'Enable' (this row is enclosed in a red box); 'VLAN ID' is set to '1'; 'Forwarding Method for IPv6' has three radio button options: 'MAC Group Address' (selected), 'IP Group Address', and 'Source Specific IP Group Address'; 'Forwarding Method for IPv4' also has three radio button options: 'MAC Group Address' (selected), 'IP Group Address', and 'Source Specific IP Group Address'. At the bottom of the configuration area are 'Apply' and 'Cancel' buttons.

6. Enable IGMP Snooping, IGMP Querier Status

Go to : Multicast> IPv4 Multicast Configuration> IGMP Snooping. Enable IGMP Snooping, IGMP Querier Status

The screenshot shows the configuration page for IGMP Snooping on a Cisco SG300-10P switch. The configuration is as follows:

- IGMP Snooping Status: Enable
- IGMP Querier Status: Enable

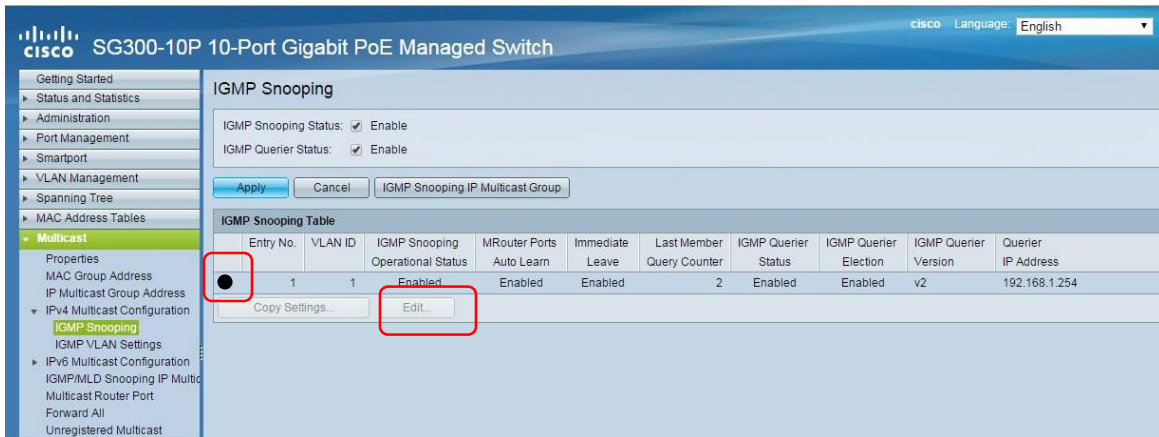
Buttons: Apply, Cancel, IGMP Snooping IP Multicast Group

Entry No.	VLAN ID	IGMP Snooping Operational Status	MRouter Ports Auto Learn	Immediate Leave	Last Member Query Counter	IGMP Querier Status	IGMP Querier Election	IGMP Querier Version	Querier IP Address
1	1	Enabled	Enabled	Enabled	2	Enabled	Enabled	v2	192.168.1.254

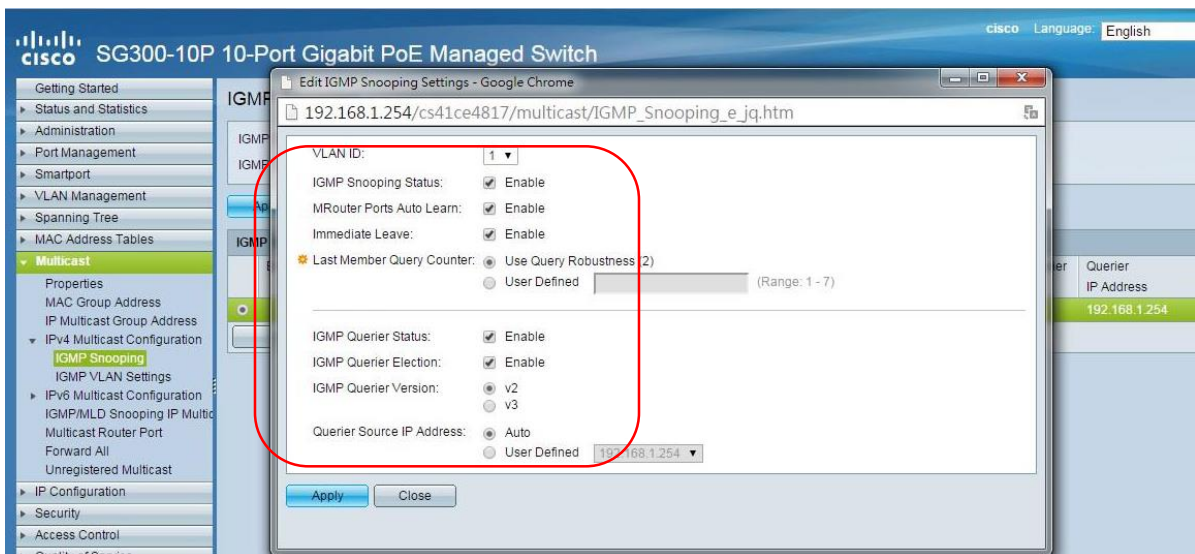
Buttons: Copy Settings..., Edit...

7. In **IGMP Snooping Table** SELECT the VLAN that the Octava PRO DSX will be connected to.

Then select **EDIT**



8. Configure the VLAN **IGMP SNOOPING** as shown below



9. Save , Apply



10. Reboot

reboot under **Administration>File Management > Reboot**

