Managed Switch Tutorial

CISCO SG350-10p

Also shown: Internet Service from Cisco RV340

Guide Version:	0.985, August 2020
SG350 Firmware Version:	2.4.0.94

Copyright

Legal Notice and Disclaimer

Audinate retains ownership of all intellectual property in this document.

The information and materials presented in this document are provided as an information source only. While effort has been made to ensure the accuracy and completeness of the information, no guarantee is given, nor responsibility taken by Audinate for errors or omissions in the data.

Audinate is not liable for any loss or damage that may be suffered or incurred in any way as a result of acting on information in this document. The information is provided solely on the basis that readers will be responsible for making their own assessment, and are advised to verify all relevant representation, statements and information with their own professional advisers.

Software Licensing Notice

Audinate distributes products which are covered by Audinate license agreements and third-party license agreements.

For further information and to access copies of each of these licenses, please visit our website: www.audinate.com/software-licensing-notice

Contacts

Australia:

Audinate Pty Ltd
Level 7, 64 Kippax St
Surry Hills NSW 2010
AUSTRALIA

Tel. +61 2 8090 1000

Postal Address:

Audinate Pty Ltd
PO Box 855
Broadway NSW 2007
AUSTRALIA

info@audinate.com
www.audinate.com

North/South America:

Audinate, Inc
1200 NW Naito Parkway
Suite 630
Portland, OR 97209
USA

Tel. +1 503 224 2998

Europe, Middle East, Africa:

Audinate Ltd
Suite 104
Werks Central
15-17 Middle St
Brighton, BN1 1AL
United Kingdom

+44 (0) 1273 921695

Asia/Pacific:

Audinate Limited
Suite 1106-08
11/F Tai Yau Building
No 181 Johnston Road
Wanchai, Hong Kong

Tel. +(852)-3588 0030
+(852)-3588 0031

Fax +(852)-2975 8042

Contents

1. Preface 1

1.1. This a Tutorial, not a "Certified Switch Configuration" 1
1.2. What to Look for in a Managed Network Switch 1

2. Basic Switch Set-Up 1

2.1. Initialize the Switch 1
2.2. Log in to the Management Interface, Set an Admin Password 1
2.3. Advanced Mode 2
2.4. Update Firmware… If Desired 2
2.5. Save Configuration 4
2.6. Change the Management IP address 5
2.7. Switch Information: Location, Contact, Log-in Banner 7
2.8. Copy/Save Switch Configurations 8
2.9. Loading a Saved Configuration to the Switch 9

3. VLANs, Trunks, Link Aggregation Groups (LAGs) 10

3.1. Creating VLANs 11
3.2. Assigning a VLANs to Ports 12
3.3. Assigning Ports to a Link Aggregation Group (LAG) 16

4. Optimizing for Dante Audio-Video Traffic 18

4.1. Disable Energy Efficient Ethernet (EEE, Green Ethernet, 802.3az) 19
4.2. Quality of Service (QoS) 20
4.3. IGMP Snooping 24
4.4. Manually Forwarding Multicast Streams 29

5. Inter-VLAN Routing, DHCP 32

5.1. Reapply Lesson from Prior Chapter Switch Modifications 33
5.2. Add a DNS Server: 34
5.3. Assign Router IP Address in Each VLAN for Inter-VLAN routing 35
5.4. Assign DHCP Service in VLANs 1 and 2 36
5.5. Create a Static Route from the Switch to the Edge Router 38
5.6. Prepping the Edge Router (RV340) for this Exercise 39
5.7. Create the Static Route from the Router to the Switch 41
5.8. Connect the Router and Switch 41

6. Switch Utilities 42

6.1. CPU Utilization 42
6.2. Port Utilization 43

7. Credits and Acknowledgements 44
8. To Do for Final Version 44

1. Preface

1.1. This a Tutorial, not a "Certified Switch Configuration"

Audinate's Dante Certification Levels 2 and 3 discuss switch features for optimizing and segmenting network traffic. This tutorial is intended to give our industry hands-on experience making these settings in a real switch, using the Cisco SG350-series. This tutorial assumes the reader has passed at least Dante Certification Level 2. Sections will require knowledge from Dante Certification Level 3.

In reality, many Dante networks require no special switch configuration. Of course, these skills are helpful if, for example, your Dante network joins an enterprise network or spans multiple properties.

This tutorial should not be misconstrued as a formula to make a "Dante-Certified Switch Configuration". Just like other design processes, network design and switch configuration are a combination of science and artform. As you go through the guide, this should become apparent. Network administrators must weigh the needs of their system and devise a design that meets the need. Of course, the settings suggested will capitalize on capabilities built-in to Dante network packets.

If you have found this guide without attending the Dante Certification Program, you may find the program helpful – you can enroll at http://audinate.com/certify.

1.2. What to Look for in a Managed Network Switch

Different switches can be designed for various use cases. In this section, here are some core features to consider when looking at a switch. The SG350-10p does not meet all of these requirements – few switches do. The goal is to find the right balance of features for your use.

Physical Characteristics

Rack Mountable – In the AV market, most frequently switches will be going in a rack. So, something designed for rack rail mounting (instead of rack shelves) is helpful.

IEC Power Connections - An internal power supply further reduces the clutter of external transformers in "wall wart" or "camel hump" supplies. Some switches may offer redundant power connections – and either or both could be available on IEC connections or through external power supplies.

PoE Budget – There are various PoE specs that provide different voltages to devices. Most switches cannot provide that maximum voltage on every port simultaneously – the PoE budget describes the total voltage available to all ports at the same time.

Ambient Noise – Because switches are often designed to be placed in equipment closets and uptime is paramount, noisy fans are common. If the switch will be in a critical listening environment, it is worth seeking out switches that do not have fans. Generally, higher port count, speed over 1Gbit, PoE supplies and internal power supplies all generate heat that increase the likelihood of noticeable fans.

RJ45 and SFP Connectors – RJ45 should be familiar to anyone; SFP/SFP+ are discussed in Dante Certification program. It is helpful to have SFP slots, making the switch more versatile. For centre-of-the-star switches, it is helpful to have all-SFP versions of a switch like the Cisco SG350-10SFP.

Logical Features, Speed Considerations

Friendly User Interface – For those outside the IT profession, it may be advisable to look for a switch that is configured from a standard web browser or a graphic utility, rather than from a command-line interface.

EEE Disable – 802.3az, otherwise known as Energy Efficient Ethernet (EEE) or Green Ethernet, negatively impacts any media network. Most switches come with EEE enabled, but many can disable this feature.

Port Speed of 1Gbit or Better – Today, there is little point in buying switches below Gigabit speed for audio/video applications. 1Gbit ports are inexpensive, and sufficient for many uses.

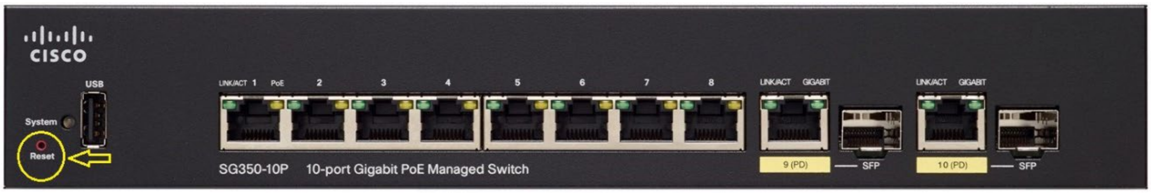
Since this guide focuses on the Cisco SG350-series, note that Cisco has a similar looking SF350-series. In these lines, the "SG" indicates SMB Gigabit. The "SF" indicates "SMB Fast Ethernet", or 100Mbit.

Trunk Port Speed – Some switches will offer higher speeds on a few ports, usually on the right side. For instance, you could have 1Gbit ports throughout the switch, but a few 10Gbit ports for faster uplink. This is more common as the port count grows, increasing demands on trunk lines.

Non-Blocking Switching Capacity – Most switches today have "non-blocking architecture", which means the switch will move as much traffic as the port speeds allow. This can be verified by looking in the specifications for "Switching Capacity", or a similar spec. This should be the sum of every port speed – doubled. The doubling of the number is to provide for full speed in and out of the port.

2. Basic Switch Set-Up

2.1. Initialize the Switch



If the switch is not factory-fresh, it is worth initializing the switch to start from a known baseline configuration. If during this tutorial you make a mistake to the saved configuration and wish to start over, you can always get your switch back to a known starting point with this process:

1) Ensure the switch is properly booted and running.

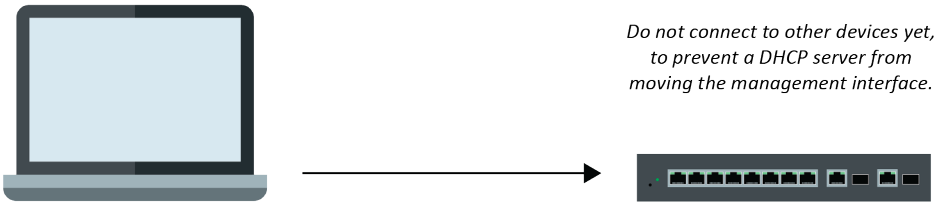
2) Insert a paperclip to firmly press and hold the reset button until the front panel lights flash (approximately 15-30 seconds).

Helpful Tips:

Pressing and releasing the reset button before the initialization process simply reboots the switch. The visual is similar, so this is confusing. If you suspect you lost your grip on the paperclip around the expected time for initializing, it is impossible to know which process just occurred unless you log in to the switch, knowing what changes to look for. When in doubt, initialize again.

Also, when we get to saving configurations, it is worth noting that the "factory configuration" can be overwritten, as described in Chapter 2.5 – Save Configuration. If the switch came from an existing installation and it is not restoring to the expected factory configuration, it is possible the factory configuration was overwritten. In that case, you'll need to find a factory default file to load that matches your switch's model and firmware.

2.2. Log in to the Management Interface, Set an Admin Password



Do not connect to other devices yet,
to prevent a DHCP server from
moving the management interface.

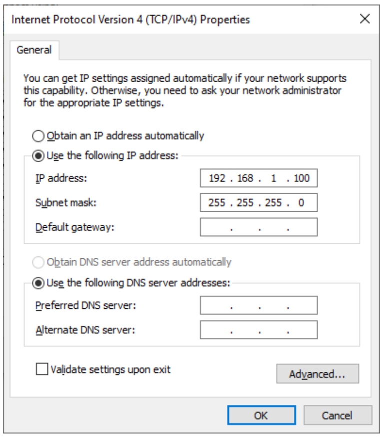
Set the computer to:

IP Address: 192.168. 1. 100
Subnet Mask: 255.255.255. 0

Use a web browser to log on to
the switch's management interface:

http://192.168.1.254/

Start with your computer and the network switch only. The SG350's management interface will follow a DHCP server if one is present, and that will take time to locate. In the absence of a DHCP server, the management interface will default to **192.162.1.254** /24.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

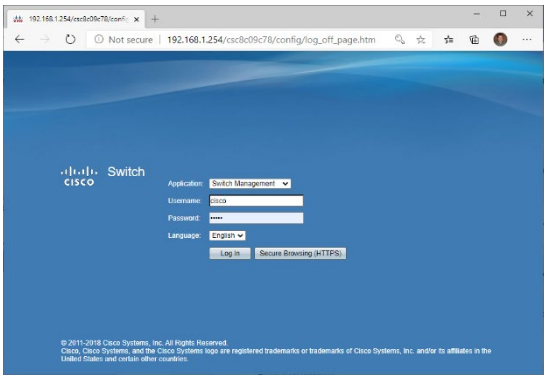
○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 1 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit



192.168.1.254/csc8c09c78/config/log_off_page.htm

Not secure

Application: Switch Management
Username: cisco
Password: •••••
Language: English

© 2011-2018 Cisco Systems, Inc. All Rights Reserved.
Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

1) Set your computer's network interface to a port that will connect to that IP address such as:

   IP Address: 192.168.1.100
   Subnet Mask: 255.255.255.0

2) Open a web browser and go to:

   http://192.168.1.254/

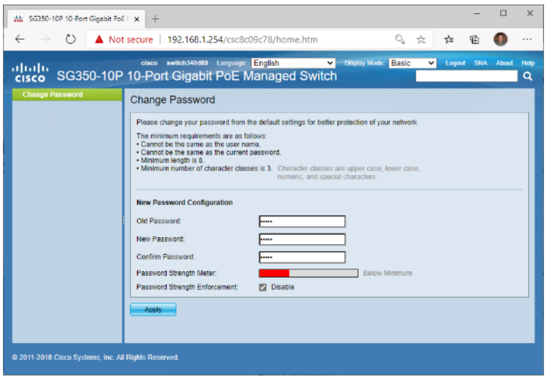
3) The default log-in credentials are:

   Username: cisco
   Password: cisco

Once you log in, the switch will probably ask you to establish new credentials for the Admin account. For this exercise, if you want to keep the password as the default "cisco", you can check

Password Strength Enforcement: ☑ Disable

and type the default "cisco" or some other simple password for the Admin account.



SG350-10P 10-Port Gigabit PoE

Not secure | 192.168.1.254/csc8c09c78/home.htm

cisco switch340d89 Language: English Display Mode: Basic Logout SNA About Help

cisco SG350-10P 10-Port Gigabit PoE Managed Switch

Change Password

Please change your password from the default settings for better protection of your network

The minimum requirements are as follows:
• Cannot be the same as the user name.
• Cannot be the same as the current password.
• Minimum length is 8.
• Minimum number of character classes is 3. Character classes are upper case, lower case, numeric, and special characters.

New Password Configuration

Old Password: •••••
New Password: •••••
Confirm Password: •••••
Password Strength Meter: Below Minimum
Password Strength Enforcement: ☑ Disable

© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

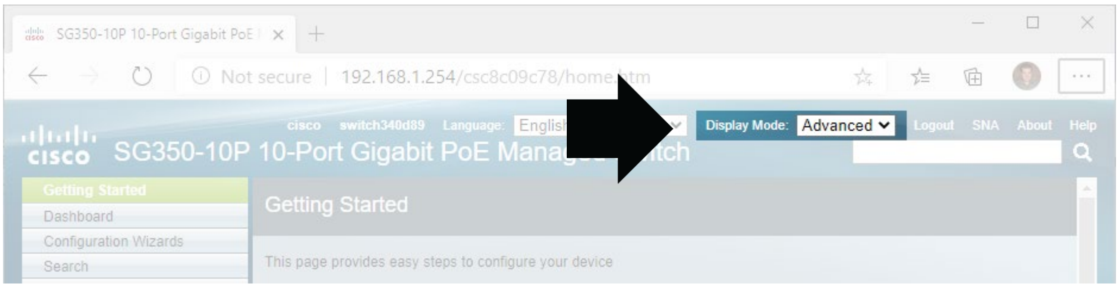
Helpful Tips:

It may take a managed network switch anywhere from one to three minutes to boot up. Until that finishes, the management interface may not be accessible or may be intermittent. Set a stopwatch on your cell phone or computer and make a note of how long it takes to log in to the management interface. That will help you plan your time on future reboot processes.

2.3. Advanced Mode

By default, the SG350 will begin in Basic mode. Many features this guide will cover requires "Advanced Mode" to see all settings. Rather than bounce between modes, we suggest you remain in Advanced Mode throughout this guide.

In the upper-right corner, switch your SG350 management interface to **Advanced Mode**.



Display Mode: Advanced

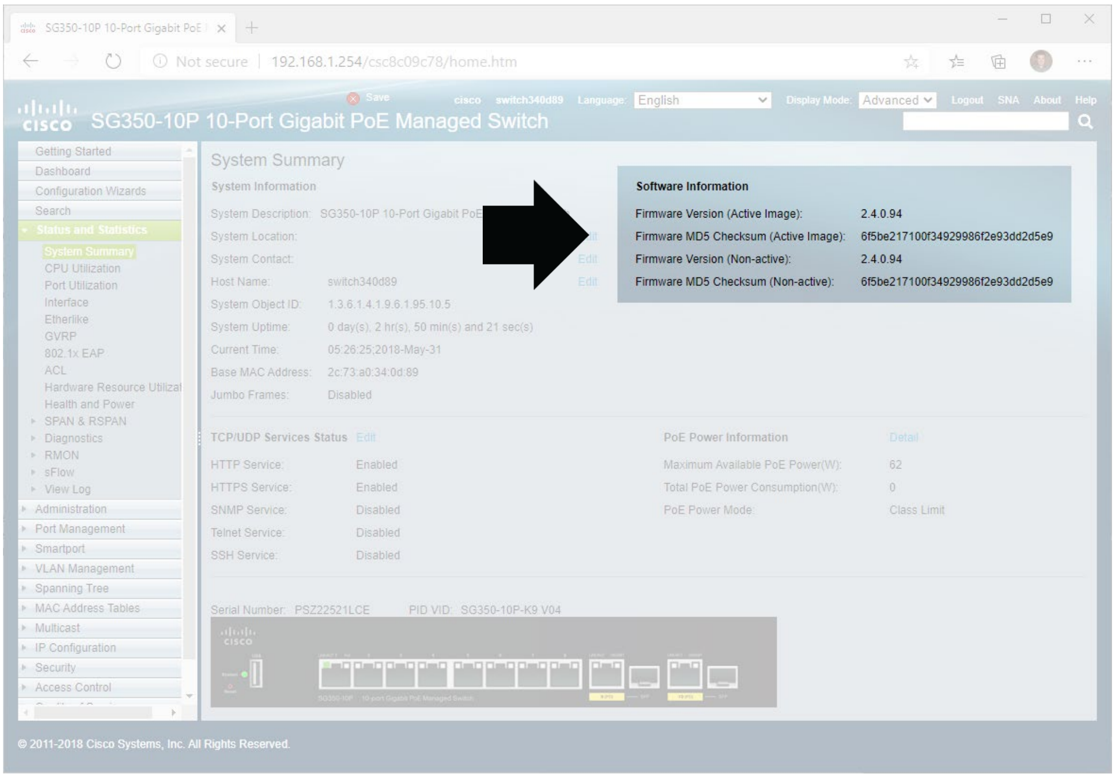
Getting Started

This page provides easy steps to configure your device

2.4. Update Firmware… If Desired

When first commissioning a system, it may be desirable to have all switches at the same firmware version. This allows you to export the configuration from one switch and copy it to another. Also, it ensures the management interface, options and behaviour are identical amongst your switches.

IT managers commonly keep their switches completely up to date to get all security patches. By contrast, audio-video professionals many subscribe to the old adage, "If it ain't broke, don't fix it." Updating may introduce a bug that matters. Which wisdom will win out likely depends on the level of exposure the switch will experience.



System Summary

System Information

System Description: SG350-10P 10-Port Gigabit PoE

System Location:

System Contact:

Host Name: switch340d89

System Object ID: 1.3.6.1.4.1.9.6.1.95.10.5

System Uptime: 0 day(s), 2 hr(s), 50 min(s) and 21 sec(s)

Current Time: 05:26:25;2018-May-31

Base MAC Address: 2c:73:a0:34:0d:89

Jumbo Frames: Disabled

Software Information

Firmware Version (Active Image): 2.4.0.94

Firmware MD5 Checksum (Active Image): 6f5be217100f34929986f2e93dd2d5e9

Firmware Version (Non-active): 2.4.0.94

Firmware MD5 Checksum (Non-active): 6f5be217100f34929986f2e93dd2d5e9

TCP/UDP Services Status

HTTP Service: Enabled

HTTPS Service: Enabled

SNMP Service: Disabled

Telnet Service: Disabled

SSH Service: Disabled

PoE Power Information

Maximum Available PoE Power(W): 62

Total PoE Power Consumption(W): 0

PoE Power Mode: Class Limit

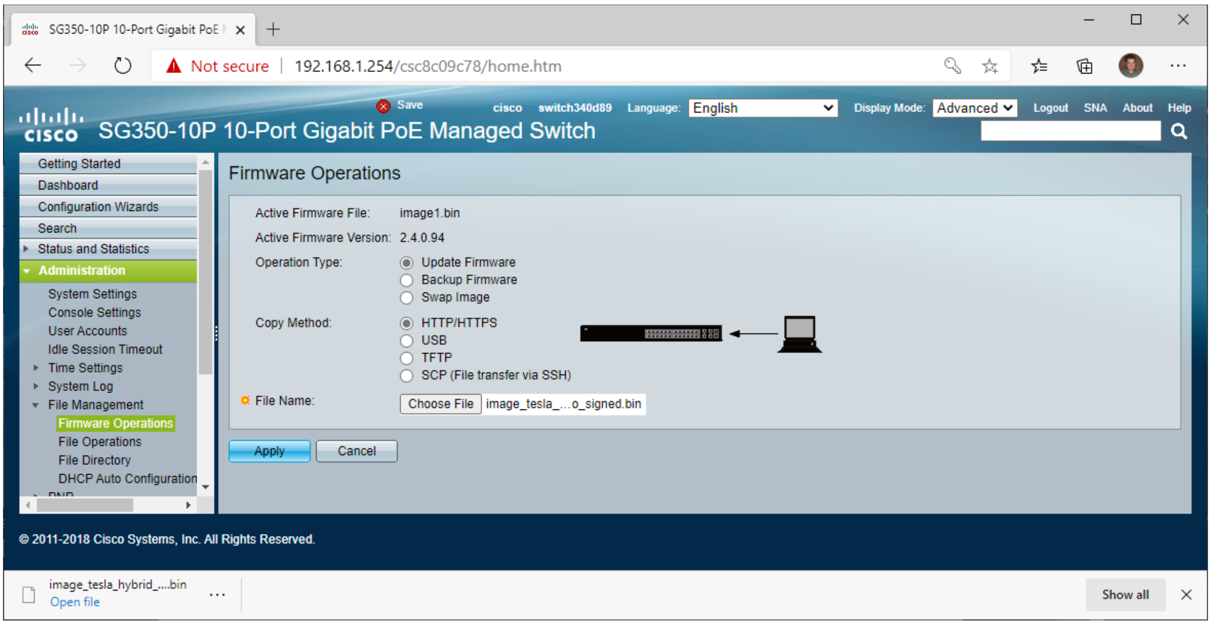
Serial Number: PSZ22521LCE PID VID: SG350-10P-K9 V04

© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

1) Go to **Status and Statistics** > **System Summary** to see the current firmware in your switch.

Compare this FW version to the latest versions on Cisco's web site. *This switch is popular enough that you can probably just search for "Cisco SG350 firmware download" and arrive at the appropriate web page.*

If a firmware update is desired….



Firmware Operations

Active Firmware File: image1.bin

Active Firmware Version: 2.4.0.94

Operation Type: ● Update Firmware ○ Backup Firmware ○ Swap Image

Copy Method: ● HTTP/HTTPS ○ USB ○ TFTP ○ SCP (File transfer via SSH)

File Name: Choose File image_tesla_...o_signed.bin

© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

2) Download the firmware file from Cisco's web site to your computer.

3) Open **Administration** > **File Management > Firmware Operations**.

   a. Click **Operation Type: Update Firmware**.

   b. Click **Choose File** and locate the firmware file on your computer.

   c. Click **Apply**.

   This process may take approximately 3 minutes. Once uploaded, we need to swap to the new firmware and reboot the machine.

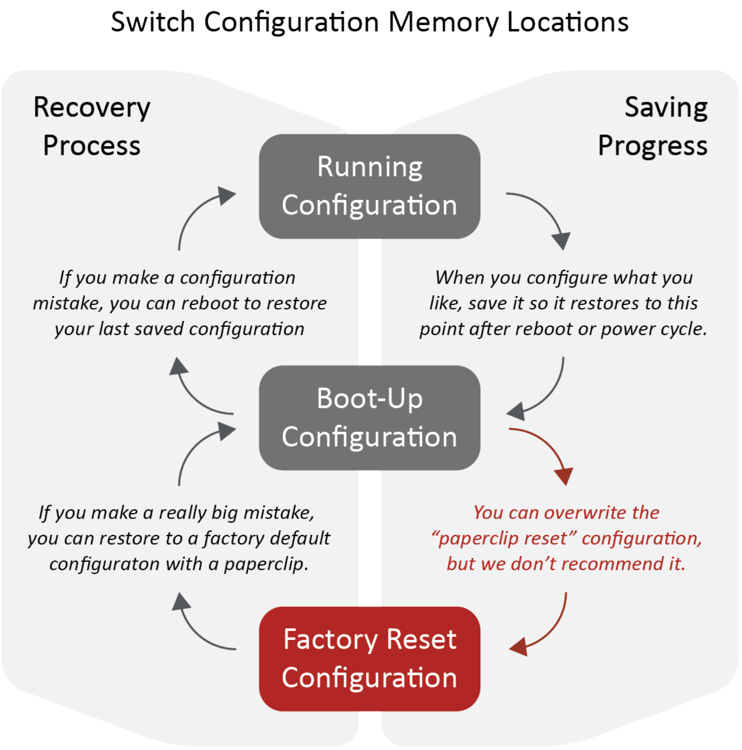
   d. Select the **Operation Type: Swap Image.**

   e. Select your new firmware version under **Active Image After Reboot**.

   f. Click **Apply.**

4) Do not reboot yet! We need to save your configuration before rebooting. Go on to section 2.5.

2.5. Save Configuration


Switch Configuration Memory Locations
Recovery Process
Saving Progress
Running Configuration
Boot-Up Configuration
Factory Reset Configuration
If you make a configuration mistake, you can reboot to restore your last saved configuration
When you configure what you like, save it so it restores to this point after reboot or power cycle.
If you make a really big mistake, you can restore to a factory default configuraton with a paperclip.
You can overwrite the "paperclip reset" configuration, but we don't recommend it.

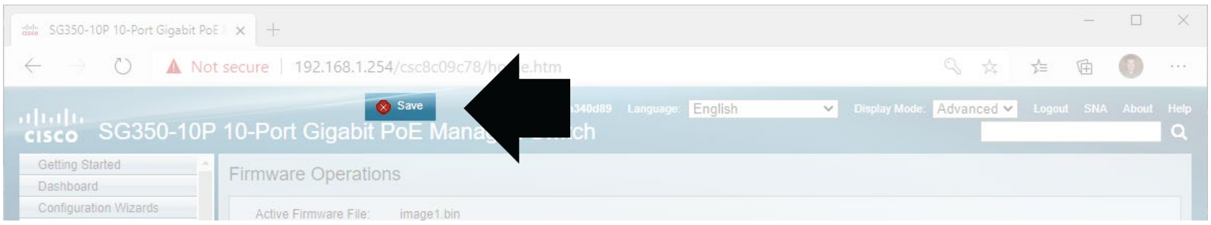
The SG350 has three configuration memory locations. The first two are easy to understand if you think about a Microsoft Word document.

When changes are made to a Word doc, the change only exists in the computer's memory. If the user quits Word without saving, the changes to the document are lost. Next time they open the document, they'll get the last saved version.

The switch works the same way. Changes are stored in memory (Running Configuration) and many changes are acted upon immediately. However, if the switch reboots without saving the configuration, it restores to the last saved version (Boot-up Configuration). This can be a simple way to recover from a complex configuration mistake, especially if you save configuration periodically; it acts like a restore point.

The third memory location is the configuration that will be loaded when the switch is initialized. The SG350-series does allow you to overwrite this position, but it is generally not recommended. A rental house might use this to bring the switch to a known configuration, but there may not be many good reasons for a user to override this area.

Anytime a change is made to the running switch configuration, the web interface will show a blinking “Save” icon at the top of the screen.


SG350-10P 10-Port Gigabit PoE
Not secure
192.168.1.254/csc8c09c78/home.htm
Save
SG350-10P 10-Port Gigabit PoE Managed Switch
Language: English
Display Mode: Advanced
Logout SNA About Help
Getting Started
Dashboard
Configuration Wizards
Firmware Operations
Active Firmware File: image1.bin

To save the Running Configuration to the Boot-Up Configuration, click **Save** at the top of the screen.

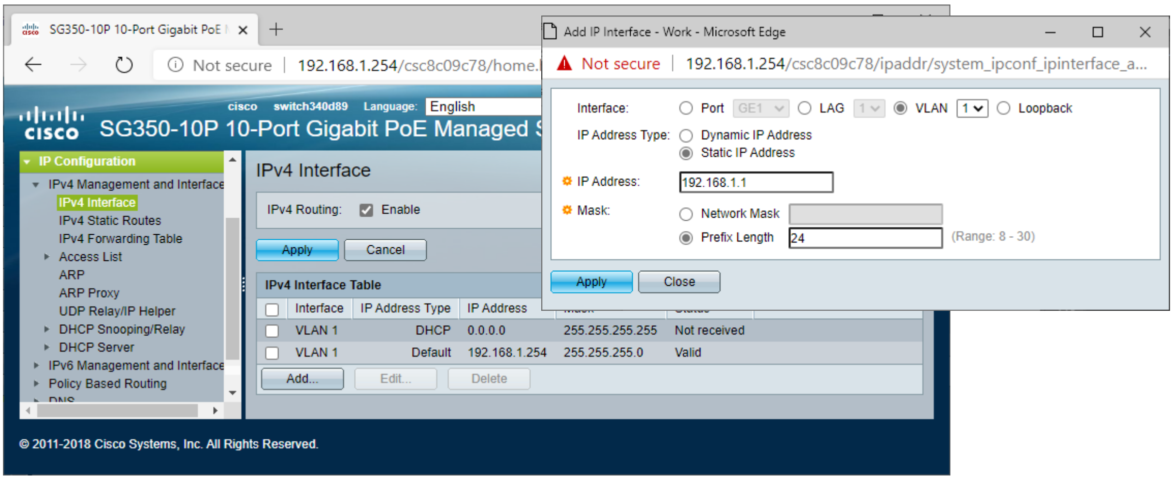
To negate your changes and restore to your Boot-Up Configuration, go to **Administration** > **Reboot**. (and follow on-screen confirmations) or simply interrupt power.

If you need to reboot to take advantage of newly installed firmware, now is the time to do that.

2.6. Change the Management IP address

Chances are, you’ll want to set the IP address of the management interface to a known address that works in your network scheme. If you will also be implementing inter-VLAN routing on this switch (covered in Chapter 5), this address will also be the router address from the management VLAN. So, in our example, our IP address will end in “.1” so it is ready to be the routing address – but you can adapt this if needed.

IT departments will often create a special VLAN for switch management, keeping it separate from the people on their network. But for this exercise, we’ll let the Dante VLAN also have access to the switch configuration screens.


SG350-10P 10-Port Gigabit PoE
Not secure
192.168.1.254/csc8c09c78/home.
cisco switch340d89 Language: English
SG350-10P 10-Port Gigabit PoE Managed S
IP Configuration
IPv4 Management and Interface
IPv4 Interface
IPv4 Static Routes
IPv4 Forwarding Table
Access List
ARP
ARP Proxy
UDP Relay/IP Helper
DHCP Snooping/Relay
DHCP Server
IPv6 Management and Interface
Policy Based Routing
DNS
Apply
Cancel
Add...
Edit...
Delete
© 2011-2018 Cisco Systems, Inc. All Rights Reserved.
Add IP Interface - Work - Microsoft Edge
Not secure
192.168.1.254/csc8c09c78/ipaddr/system_ipconf_ipinterface_a...
Apply
Close

IPv4 Interface

IPv4 Routing: ☑ Enable

IPv4 Interface Table

□	Interface	IP Address Type	IP Address		
□	VLAN 1	DHCP	0.0.0.0	255.255.255.255	Not received
□	VLAN 1	Default	192.168.1.254	255.255.255.0	Valid

Interface: ○ Port GE1 ○ LAG 1 ● VLAN 1 ○ Loopback

IP Address Type: ○ Dynamic IP Address ● Static IP Address

IP Address: 192.168.1.1

Mask: ○ Network Mask ● Prefix Length 24 (Range: 8 - 30)

1) Open **IP Configuration** > **IPv4 Management and Interface** > **IPv4 Interface**.

We will see the switch has two options – DHCP and the default address currently.

2) Click **Add…** to create your new management interface.

Note: In older firmware, you click ***Edit…*** *to change the default address. The newer firmware doesn’t appear to allow editing – you have to delete and recreate interfaces. At initial set-up, the interface added here will replace the default addresses.*

3) Set this as a **Static IP Address** at **192.168.1.1**.

4) Enter the **Subnet Mask** as a prefix of 24-bits (or spell it out as a mast of 255.255.255.0.)

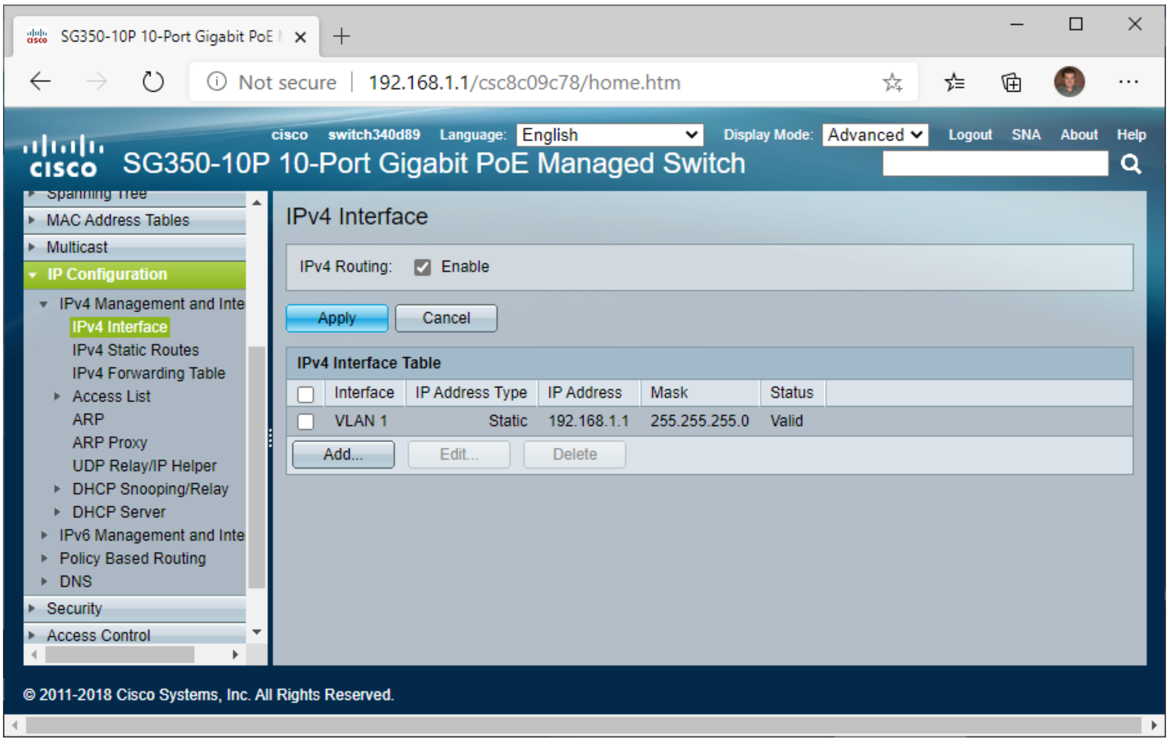
5) Click **Apply**.

   At this point, the management IP address has moved. We'll need to log back in at the new address. If you're address was in a new subnet, remember to change your computer's IP address.

6) Log back into the switch at 192.168.1.1 and enter your credentials.

7) Open **IP Configuration** > **IPv4 Management and Interface** > **IPv4 Interface**.

   We should just see one management IP address, now.



IPv4 Interface

IPv4 Routing: ☑ Enable

IPv4 Interface Table

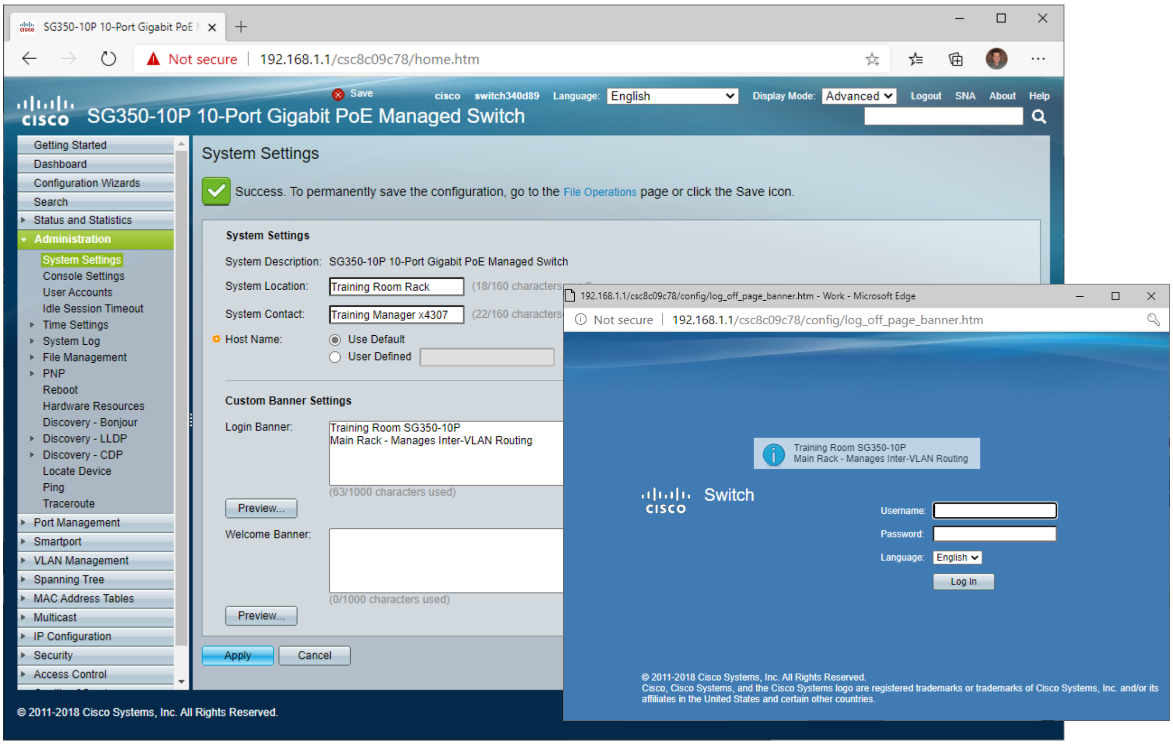
□	Interface	IP Address Type	IP Address	Mask	Status
□	VLAN 1	Static	192.168.1.1	255.255.255.0	Valid

Reminder:
Now is a good time to save.

2.7. Switch Information: Location, Contact, Log-in Banner

If there are multiple switches in the network, it can be helpful to label the switch according to its location. On the physical switch, console tape or a labeller can be used on the front or back panels to document the management IP address and/or notes about the configuration. But when you log in, it is also nice confirmation to know which switch you are in or who to contact for support.

The System Location and System Contact field will remain in the set-up screens. If you want to hide this information from prying eyes, this is where to go. If you want information to be visible at the log-in screen, use the Login Banner feature.



System Settings

Success. To permanently save the configuration, go to the File Operations page or click the Save icon.

System Settings

System Description: SG350-10P 10-Port Gigabit PoE Managed Switch

System Location: Training Room Rack (18/160 characters

System Contact: Training Manager x4307 (22/160 characters

Host Name: ● Use Default ○ User Defined

Custom Banner Settings

Login Banner: Training Room SG350-10P
Main Rack - Manages Inter-VLAN Routing
(63/1000 characters used)

Welcome Banner:
(0/1000 characters used)

Training Room SG350-10P
Main Rack - Manages Inter-VLAN Routing

Username:
Password:
Language: English

© 2011-2018 Cisco Systems, Inc. All Rights Reserved.
Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

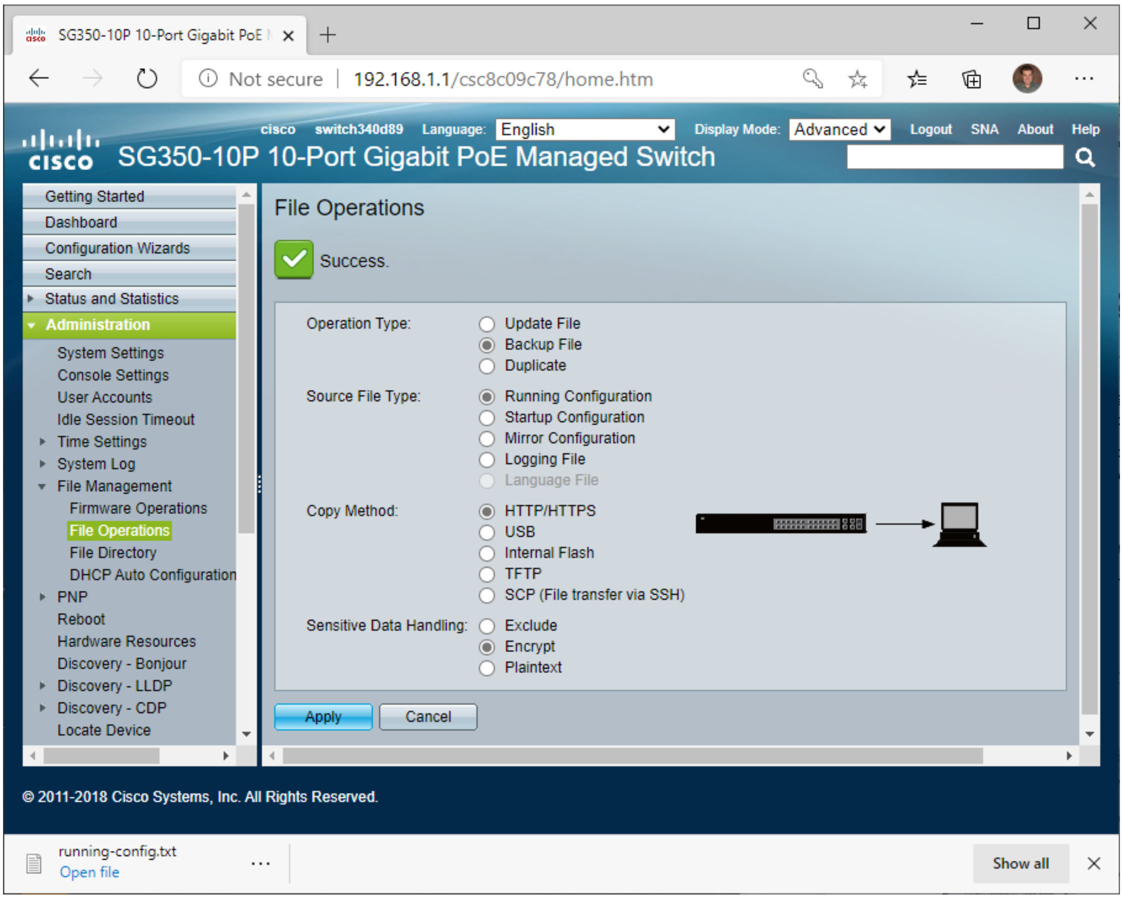
1) Open **Administration** > **System Settings.**

2) Edit the fields as desired and click **Apply** to confirm the new settings.

3) Click **Preview** to see what your Log-In Banner will look like.

Reminder:
Now is a good time to save.

2.8. Copy/Save Switch Configurations



File Operations

✓ Success.

Operation Type: ○ Update File ● Backup File ○ Duplicate

Source File Type: ● Running Configuration ○ Startup Configuration ○ Mirror Configuration ○ Logging File ○ Language File

Copy Method: ● HTTP/HTTPS ○ USB ○ Internal Flash ○ TFTP ○ SCP (File transfer via SSH)

Sensitive Data Handling: ○ Exclude ● Encrypt ○ Plaintext

1) Open **Administration** > **File Management** > **File Operations**

   a. Under **File Operation**, select **Backup File**.

      This instructs the switch to save the configuration (rather than load it). In the picture, you'll notice the arrow from the switch to the computer, indicating the direction of the data flow.

   b. Select the **Source File Type** (probably the **Running Configuration**)

   c. Select the Copy Method (probably **HTTP/HTTPS**)

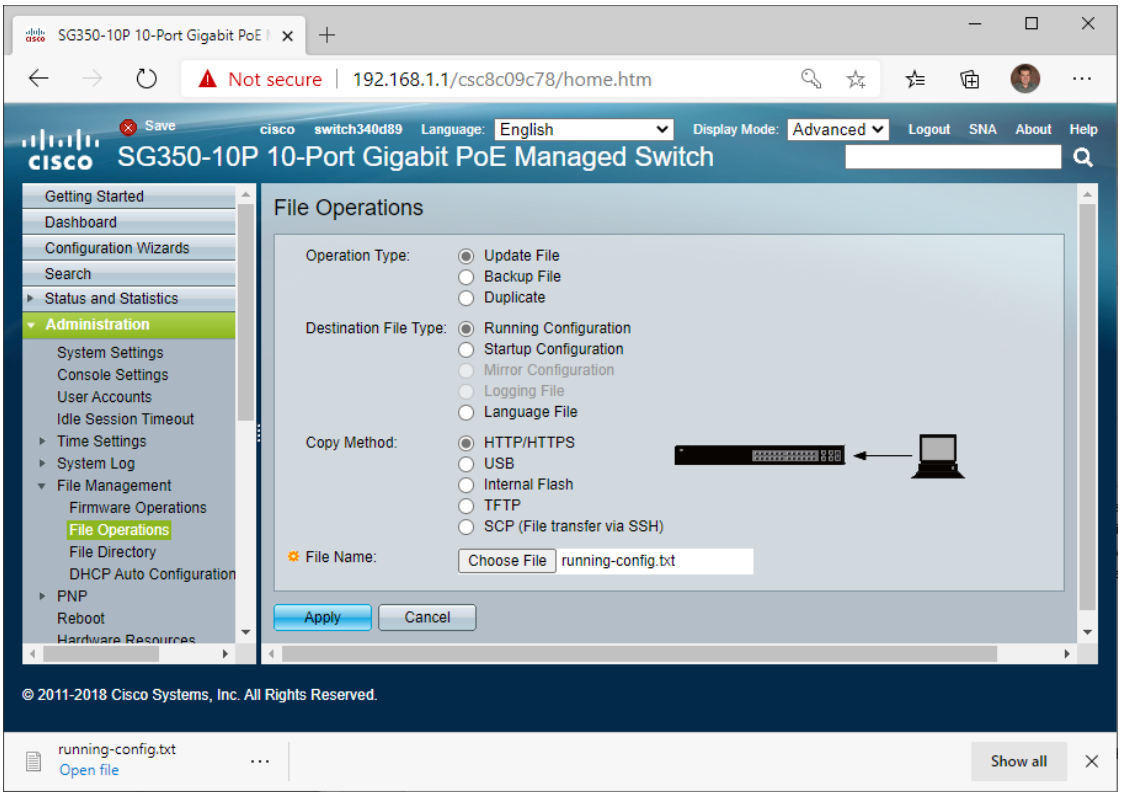
   d. Select Sensitive Data Handling (probably **Encrypt** or **Plain Text**)

   e. Click **Apply**.

The file will download to your machine as a .txt text file.

2.9. Loading a Saved Configuration to the Switch

When loading configuration files, Cisco suggests they must come from the same model and same firmware switch. Also, be aware that the file will contain the management IP address of the switch. So, if you have multiples of the same model switch, you can use this to duplicate the settings. However, you will want to keep it separate when loading so you can change the management IP address before attaching the switch to the main network.



File Operations

Operation Type: ● Update File ○ Backup File ○ Duplicate

Destination File Type: ● Running Configuration ○ Startup Configuration ○ Mirror Configuration ○ Logging File ○ Language File

Copy Method: ● HTTP/HTTPS ○ USB ○ Internal Flash ○ TFTP ○ SCP (File transfer via SSH)

File Name: Choose File running-config.txt

1) Open **Administration** > **File Management** > **File Operation.**

   a. Under **File Operation**, select **Update File**.

      This instructs the switch to load the configuration in (rather than save it. Notice the arrow from the computer to the switch, indicating the direction of the data flow.

   b. Select the **Source File Type** (probably the **Start-up Configuration**).

   c. Select the Copy Method (probably **HTTP/HTTPS**).

   d. Locate the configuration file on your computer.

   e. Click **Apply**.

Once the configuration loads, it should reboot. Remember, when you log back in, you'll need to log in to the management IP address in the configuration file.

3. VLANs, Trunks, Link Aggregation Groups (LAGs)

To succeed in this chapter, the reader needs to have a firm grasp on the concepts taught in Audinate's Dante Certification Level 2, 2021 Edition. For information about this training program, go to https://audinate.com/certify

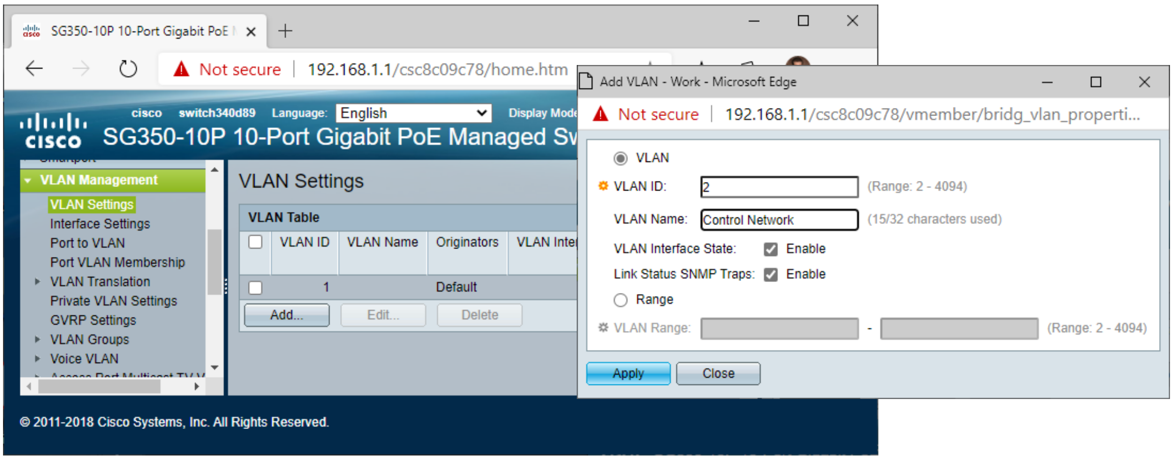
Switch Example Design (Chapter 3)

Port:	1	2	3	4	5	6	7	8	9	10
VLAN/Tagged "U" is untagged "T" is tagged	1 - U (Dante)					2 - U (Control)			1 - U (Dante) 2 - T (Control)	
Type	Access								Trunk	
Special									LAG #1	

In this chapter, the instructions show how to break a switch in to VLANs, establish a trunk line to carry multiple VLANs, and how to create a Link Aggregation Group (LAG) across multiple ports. In this case, the LAG will be used on the trunk lines to provide more bandwidth from this switch to another.

3.1. Creating VLANs

IT Professionals will often break the network in to multiple VLANs, organizing devices by functional groups, physical location or other means. It not uncommon for IT departments to limit the size of a VLAN to 250-500 devices to minimize the amount of network chatter from multicast and broadcast messages from various services on the network ports.


SG350-10P 10-Port Gigabit PoE
Not secure
192.168.1.1/csc8c09c78/home.htm
cisco switch340d89 Language: English Display Mode
SG350-10P 10-Port Gigabit PoE Managed Sw
VLAN Management
VLAN Settings
Interface Settings
Port to VLAN
Port VLAN Membership
VLAN Translation
Private VLAN Settings
GVRP Settings
VLAN Groups
Voice VLAN
Add...
Edit...
Delete
© 2011-2018 Cisco Systems, Inc. All Rights Reserved.
Add VLAN - Work - Microsoft Edge
Not secure
192.168.1.1/csc8c09c78/vmember/bridg_vlan_properti...
Apply
Close

VLAN Settings

VLAN Table

☐	VLAN ID	VLAN Name	Originators	VLAN Inte
☐	1		Default	

● VLAN

VLAN ID: 2 (Range: 2 - 4094)

VLAN Name: Control Network (15/32 characters used)

VLAN Interface State: ☑ Enable

Link Status SNMP Traps: ☑ Enable

○ Range

VLAN Range: - (Range: 2 - 4094)

To create the second VLAN:

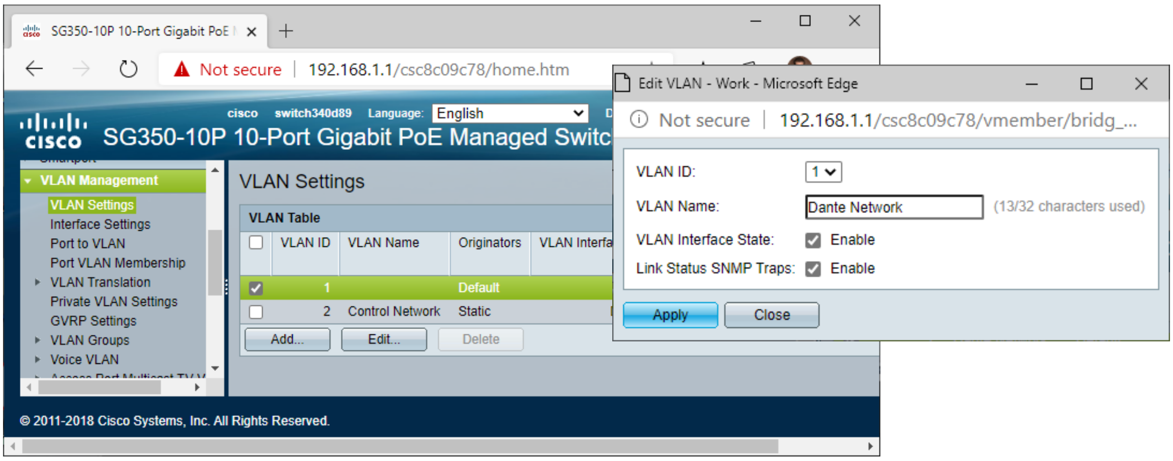
1) Open **VLAN Management > VLAN Settings**

   a. Click **Add…**

   b. Assign a **VLAN ID**

   c. Enter the **VLAN Name** for your documentation. In this example, use **Control Network**.

   d. Click **Apply.**


SG350-10P 10-Port Gigabit PoE
Not secure
192.168.1.1/csc8c09c78/home.htm
cisco switch340d89 Language: English
SG350-10P 10-Port Gigabit PoE Managed Switc
VLAN Management
VLAN Settings
Interface Settings
Port to VLAN
Port VLAN Membership
VLAN Translation
Private VLAN Settings
GVRP Settings
VLAN Groups
Voice VLAN
Add...
Edit...
Delete
© 2011-2018 Cisco Systems, Inc. All Rights Reserved.
Edit VLAN - Work - Microsoft Edge
Not secure
192.168.1.1/csc8c09c78/vmember/bridg_...
Apply
Close

VLAN Settings

VLAN Table

☐	VLAN ID	VLAN Name	Originators	VLAN Interfa
☑	1		Default	
☐	2	Control Network	Static	

VLAN ID: 1

VLAN Name: Dante Network (13/32 characters used)

VLAN Interface State: ☑ Enable

Link Status SNMP Traps: ☑ Enable

To name the first VLAN:

2) Check the box for the first VLAN.

   a. Enter the **VLAN Name**. In this example, use **Dante Network**.

   b. Click **Apply**.

3.2. Assigning Ports to VLANs

Once all VLANs are created, each port must know what VLAN(s) it belongs to. Here are two modes:

Ports 1-8: Access, Untagged – Ports 1-8 are expecting Dante devices, computers, printers, etc. These should be set to Access. They will only belong to one VLAN, and the packets should remain untagged.

Ports 9-10: Trunk, One VLAN Untagged and all other VLANs Tagged – Ports 9-10 will be set to "Trunk" so they can transport multiple VLANs. In this situation, one VLAN (usually the maintenance VLAN) can remain untagged, but the rest should be tagged.

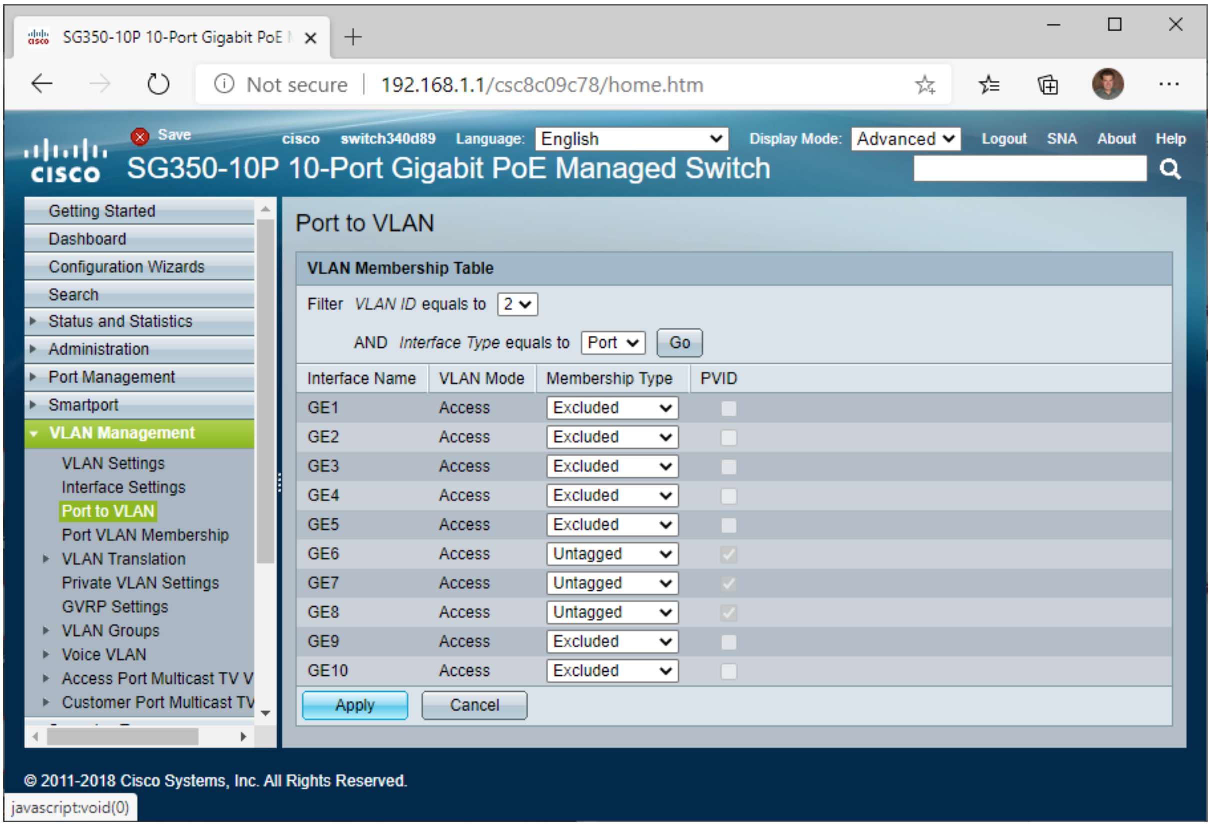
Tagged means an 802.1Q tag is added to each packet. When a device transmits multiple VLANs on the same cable, the receiver knows which VLAN the port belongs to by looking at the tag. Before it moves the packet to other ports, the 802.1Q tag will be removed so it is untagged traffic again.

On a trunk line, it is common practice to leave one VLAN untagged - this is commonly used for the switch configuration VLAN. This allows a technician to plug their laptop directly to any trunk port and access the configuration screen. Because data from the other VLANs will be tagged, it will be ignored by the laptop.

ℹ **Make sure your computer is plugged in to a port that will remain in the VLAN with the switch management interface.** In this example, that would be ports 1-5. If you assign the port your computer is using to a VLAN that does not have access to the management port, you can simply move your connection and log back in. *If you didn't think about this and forgot to leave one port with access to the switch management screen, you can reboot your switch and be restored to your last saved configuration.*

Assigning VLANs to Access Ports

In the example, ports 1-5 are already set properly. Only ports 6-8 need to be re-assigned.



Port to VLAN

VLAN Membership Table

Filter *VLAN ID* equals to 2

AND *Interface Type* equals to Port Go

Interface Name	VLAN Mode	Membership Type	PVID
GE1	Access	Excluded	☐
GE2	Access	Excluded	☐
GE3	Access	Excluded	☐
GE4	Access	Excluded	☐
GE5	Access	Excluded	☐
GE6	Access	Untagged	☑
GE7	Access	Untagged	☑
GE8	Access	Untagged	☑
GE9	Access	Excluded	☐
GE10	Access	Excluded	☐

Apply Cancel

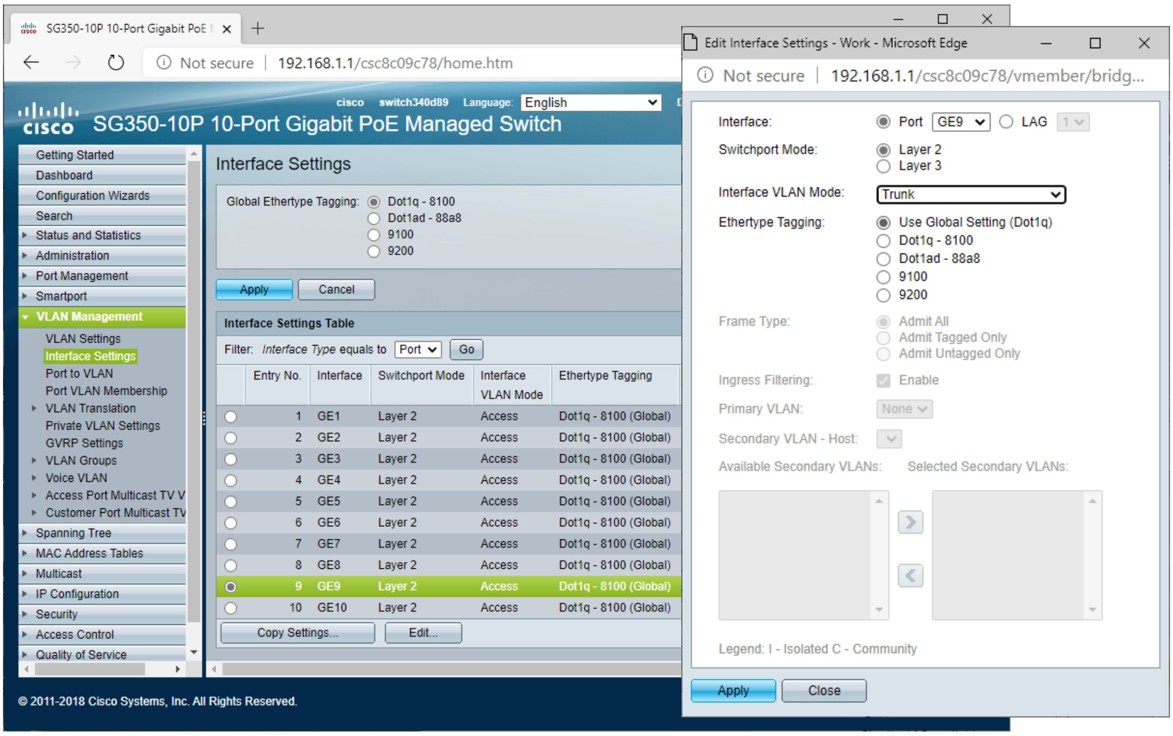
1) Open **VLAN Management** and select **Port to VLAN**.

   a. At the top, select VLAN ID equals 2, and click **Go**.

   b. On GE6, GE7 and GE8, set the Membership Type to **Untagged**.

2) Click **Apply**.

Assigning Ports as Trunk with Multiple VLANs


SG350-10P 10-Port Gigabit PoE
Not secure | 192.168.1.1/csc8c09c78/home.htm
cisco switch340d89 Language: English
SG350-10P 10-Port Gigabit PoE Managed Switch
Getting Started
Dashboard
Configuration Wizards
Search
Status and Statistics
Administration
Port Management
Smartport
VLAN Management
VLAN Settings
Interface Settings
Port to VLAN
Port VLAN Membership
VLAN Translation
Private VLAN Settings
GVRP Settings
VLAN Groups
Voice VLAN
Access Port Multicast TV V
Customer Port Multicast TV
Spanning Tree
MAC Address Tables
Multicast
IP Configuration
Security
Access Control
Quality of Service
© 2011-2018 Cisco Systems, Inc. All Rights Reserved.
Edit Interface Settings - Work - Microsoft Edge
Not secure | 192.168.1.1/csc8c09c78/vmember/bridg...

Interface Settings

Global Ethertype Tagging: ● Dot1q - 8100 ○ Dot1ad - 88a8 ○ 9100 ○ 9200

Apply Cancel

Interface Settings Table

Filter: *Interface Type* equals to Port Go

	Entry No.	Interface	Switchport Mode	Interface VLAN Mode	Ethertype Tagging
○	1	GE1	Layer 2	Access	Dot1q - 8100 (Global)
○	2	GE2	Layer 2	Access	Dot1q - 8100 (Global)
○	3	GE3	Layer 2	Access	Dot1q - 8100 (Global)
○	4	GE4	Layer 2	Access	Dot1q - 8100 (Global)
○	5	GE5	Layer 2	Access	Dot1q - 8100 (Global)
○	6	GE6	Layer 2	Access	Dot1q - 8100 (Global)
○	7	GE7	Layer 2	Access	Dot1q - 8100 (Global)
○	8	GE8	Layer 2	Access	Dot1q - 8100 (Global)
●	9	GE9	Layer 2	Access	Dot1q - 8100 (Global)
○	10	GE10	Layer 2	Access	Dot1q - 8100 (Global)

Copy Settings... Edit...

Interface: ● Port GE9 ○ LAG 1

Switchport Mode: ● Layer 2 ○ Layer 3

Interface VLAN Mode: Trunk

Ethertype Tagging: ● Use Global Setting (Dot1q) ○ Dot1q - 8100 ○ Dot1ad - 88a8 ○ 9100 ○ 9200

Frame Type: ● Admit All ○ Admit Tagged Only ○ Admit Untagged Only

Ingress Filtering: ☑ Enable

Primary VLAN: None

Secondary VLAN - Host:

Available Secondary VLANs: Selected Secondary VLANs:

Legend: I - Isolated C - Community

Apply Close

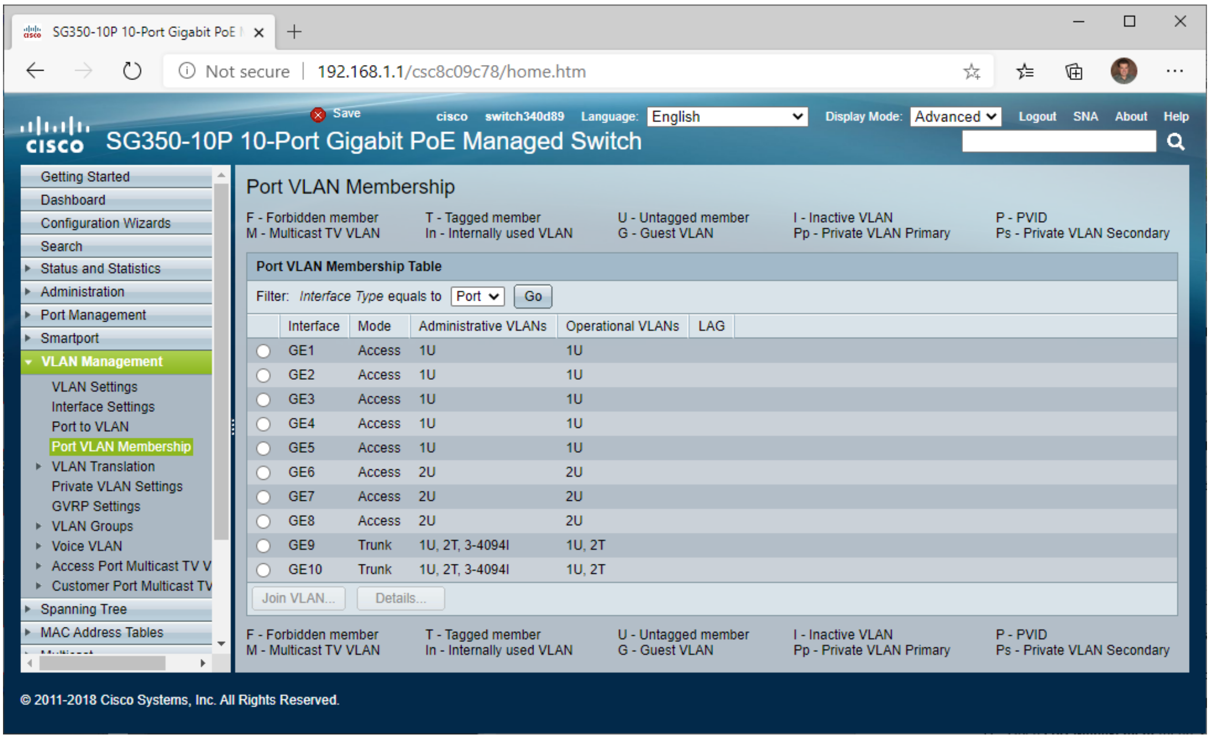
1) Open **VLAN Management** and open **Interface Settings**.

2) Select the radio button for the first trunk line (port 9), and click **Edit…**

   a. Select **Interface to VLAN Mode** as **Trunk**.

3) Click **Apply**.

4) *Use the drop-down menu in this pop-up window to assign port 10 as trunk.*



Port VLAN Membership

F - Forbidden member
M - Multicast TV VLAN
T - Tagged member
In - Internally used VLAN
U - Untagged member
G - Guest VLAN
I - Inactive VLAN
Pp - Private VLAN Primary
P - PVID
Ps - Private VLAN Secondary

Port VLAN Membership Table

Filter: *Interface Type* equals to Port Go

	Interface	Mode	Administrative VLANs	Operational VLANs	LAG
○	GE1	Access	1U	1U	
○	GE2	Access	1U	1U	
○	GE3	Access	1U	1U	
○	GE4	Access	1U	1U	
○	GE5	Access	1U	1U	
○	GE6	Access	2U	2U	
○	GE7	Access	2U	2U	
○	GE8	Access	2U	2U	
○	GE9	Trunk	1U, 2T, 3-4094I	1U, 2T	
○	GE10	Trunk	1U, 2T, 3-4094I	1U, 2T	

F - Forbidden member
M - Multicast TV VLAN
T - Tagged member
In - Internally used VLAN
U - Untagged member
G - Guest VLAN
I - Inactive VLAN
Pp - Private VLAN Primary
P - PVID
Ps - Private VLAN Secondary

To confirm the VLAN assignments assignment as Trunk, go to:

VLAN Management > **Port VLAN Membership.**

Here, the switch will show the VLAN assignments, as well as which ports are set for trunk or access status.

In this case, the switch is automatically assigning all VLANs to the trunk line. If you ever needed to change that routing, you can go back to VLAN Management > Port to VLAN. There, you can select which VLANs are tagged, untagged in the trunk line as well as VLANs excluded from the trunk line.

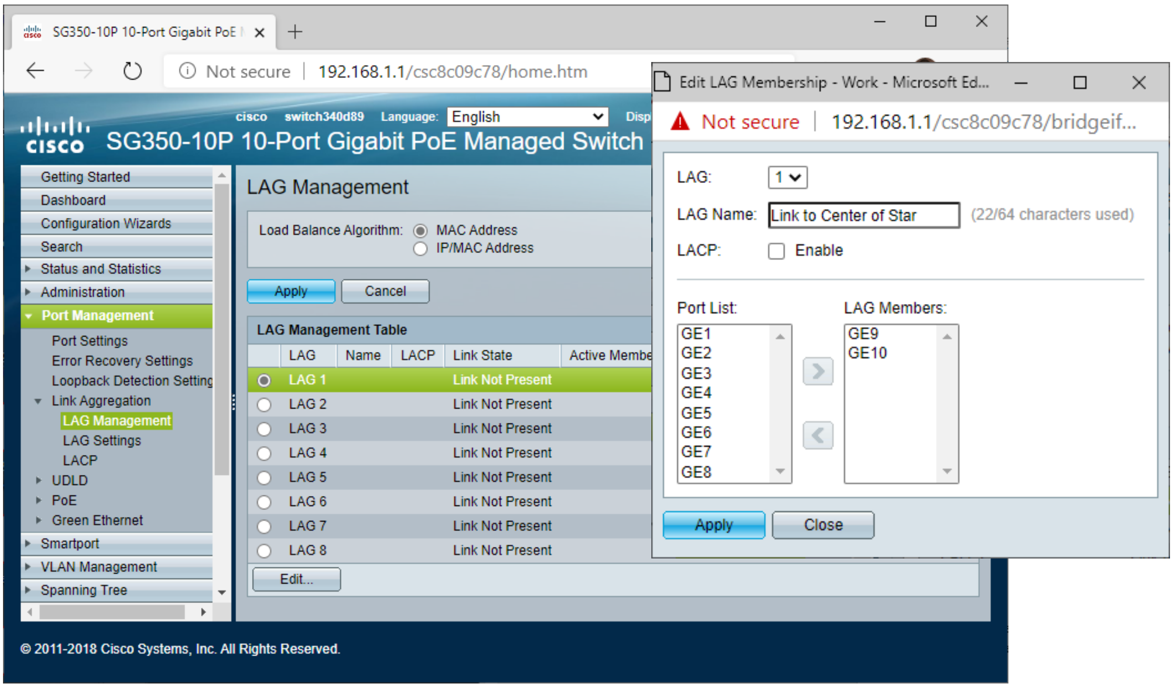
3.3. Assigning Ports to a Link Aggregation Group (LAG)

LAG Port Membership

A Link Aggregation Group (LAG) allows multiple cables to make the same connection between switches. This is usually done to allow more bandwidth between two switches.

Some will position LAGs as a form of redundancy, a bit like Spanning Tree Protocols can do. The difference being that LAGs will use the additional bandwidth of the "redundant" cable, where STP won't – that can be good or bad.

However, it should be understood that both STP and LAGs do not recover quickly. Dante Redundant networks provide seamless audio through network hits. STP and LAGs may take 60 seconds to recover from a problem. So, in live production, broadcast and other mission critical environments, this performance differences should be considered in network design. (Obviously, it is possible to STP or LAGs on Dante networks set up redundantly, but this returns to the discussion of, "How much redundancy do you want?"


SG350-10P 10-Port Gigabit PoE
Not secure | 192.168.1.1/csc8c09c78/home.htm
cisco switch340d89 Language: English
SG350-10P 10-Port Gigabit PoE Managed Switch
Getting Started
Dashboard
Configuration Wizards
Search
Status and Statistics
Administration
Port Management
Port Settings
Error Recovery Settings
Loopback Detection Setting
Link Aggregation
LAG Management
LAG Settings
LACP
UDLD
PoE
Green Ethernet
Smartport
VLAN Management
Spanning Tree
Apply
Cancel
Edit...
© 2011-2018 Cisco Systems, Inc. All Rights Reserved.
Edit LAG Membership - Work - Microsoft Ed...
Not secure | 192.168.1.1/csc8c09c78/bridgeif...
Apply
Close

LAG Management

Load Balance Algorithm: ● MAC Address ○ IP/MAC Address

LAG Management Table

	LAG	Name	LACP	Link State	Active Membe
●	LAG 1			Link Not Present	
○	LAG 2			Link Not Present	
○	LAG 3			Link Not Present	
○	LAG 4			Link Not Present	
○	LAG 5			Link Not Present	
○	LAG 6			Link Not Present	
○	LAG 7			Link Not Present	
○	LAG 8			Link Not Present	

LAG: 1

LAG Name: Link to Center of Star (22/64 characters used)

LACP: □ Enable

Port List:	LAG Members:
GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8	GE9 GE10

1) Open **Port Management** menu, **Link Aggregation** and select the **LAG Management**.

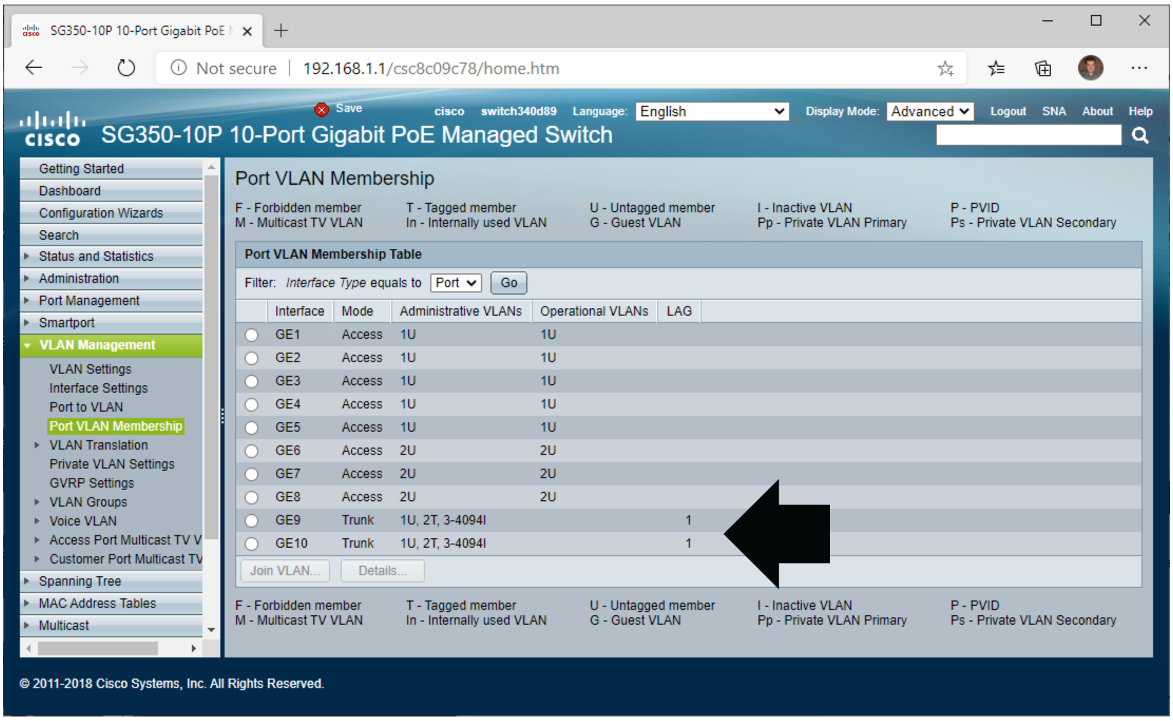
   a. Select the radio button for an available LAG (i.e.: LAG1) and click **Edit.**

   b. In the port list, select GE9 and click the right arrow to make it a LAG member.

   c. Repeat "Step 1b" for GE10.

2) Click **Apply**.

Verifying LAG Configuration



Port VLAN Membership

F - Forbidden member
M - Multicast TV VLAN
T - Tagged member
In - Internally used VLAN
U - Untagged member
G - Guest VLAN
I - Inactive VLAN
Pp - Private VLAN Primary
P - PVID
Ps - Private VLAN Secondary

Port VLAN Membership Table

Filter: *Interface Type* equals to Port Go

	Interface	Mode	Administrative VLANs	Operational VLANs	LAG
○	GE1	Access	1U	1U	
○	GE2	Access	1U	1U	
○	GE3	Access	1U	1U	
○	GE4	Access	1U	1U	
○	GE5	Access	1U	1U	
○	GE6	Access	2U	2U	
○	GE7	Access	2U	2U	
○	GE8	Access	2U	2U	
○	GE9	Trunk	1U, 2T, 3-4094I		1
○	GE10	Trunk	1U, 2T, 3-4094I		1

Join VLAN... Details...

F - Forbidden member
M - Multicast TV VLAN
T - Tagged member
In - Internally used VLAN
U - Untagged member
G - Guest VLAN
I - Inactive VLAN
Pp - Private VLAN Primary
P - PVID
Ps - Private VLAN Secondary

To confirm assignment to the LAG, return to **VLAN Management** and select **Port VLAN Membership.**

Give the LAG a suitable name and select the ports to join this LAG. Normally the **last ports** are used as they have optional fibre modules. Press **Apply** to confirm.

4. Optimizing for Dante Audio-Video Traffic

To succeed in this chapter, the reader needs to have a firm grasp on the concepts taught in Audinate's Dante Certification Level 2, 2021 Edition. For information about the Dante Certified Training Program, go to https://audinate.com/certify

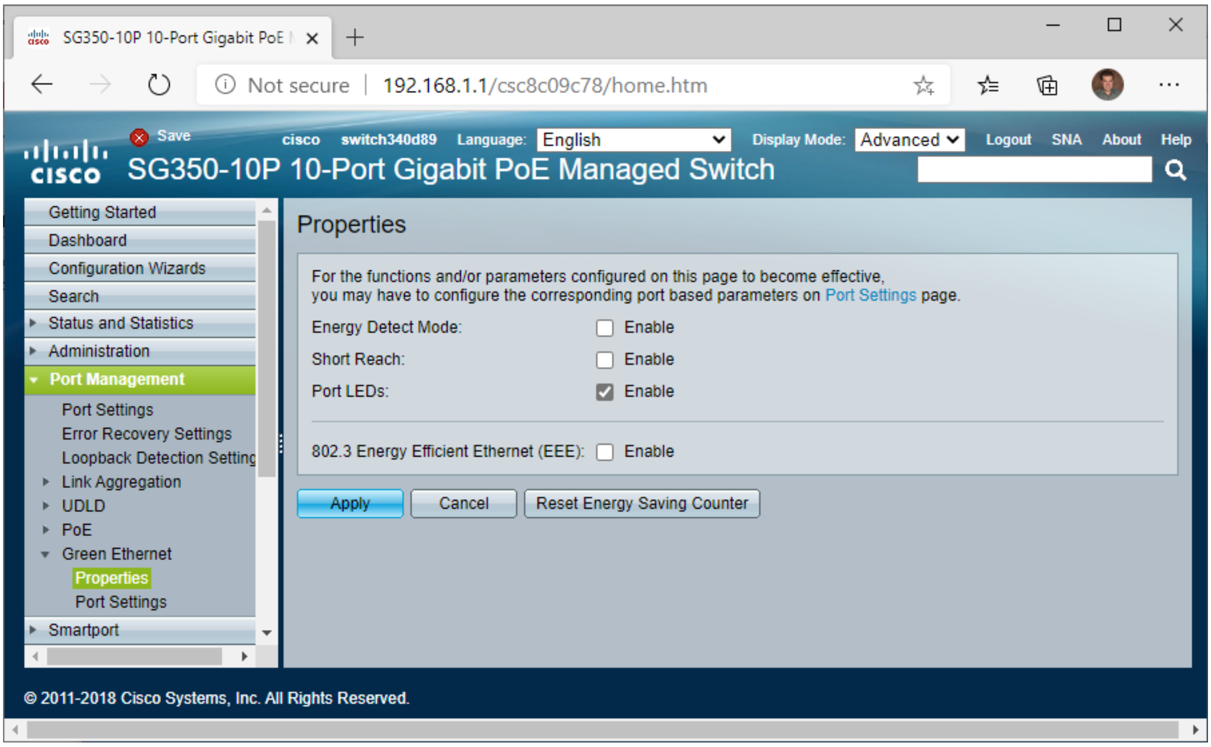
Switch Example Design

Port:	1	2	3	4	5	6	7	8	9	10
VLAN/Tagged "U" is untagged "T" is tagged	1 - U (Dante)					2 - U (Control)			1 - U (Dante) 2 - T (Control)	
Type	Access								Trunk	
Special	Forward All Multicast	Manual Forward Multicast							LAG #1	

In this chapter, the instructions show how to disable Energy Efficient Ethernet (EEE), establish Quality of Service (QoS) and engage IGMP snooping v3. Because some devices may have challenges with IGMP snooping instructions are also offered on how to manually override IGMP snooping on some ports in bulk or on specific streams.

4.1. Disable Energy Efficient Ethernet (EEE, Green Ethernet, 802.3az)

Like most switches, the SG350 defaults with Energy Efficient Ethernet (EEE) activated. While it is noble to save energy "one microwatt at a time", this feature is known to interrupt traffic and skew clock synchronization. Disabling this feature is always recommended for critical live performance systems.


SG350-10P 10-Port Gigabit PoE
Not secure | 192.168.1.1/csc8c09c78/home.htm
Save
cisco switch340d89 Language: English Display Mode: Advanced Logout SNA About Help
SG350-10P 10-Port Gigabit PoE Managed Switch
Getting Started
Dashboard
Configuration Wizards
Search
Status and Statistics
Administration
Port Management
Port Settings
Error Recovery Settings
Loopback Detection Setting
Link Aggregation
UDLD
PoE
Green Ethernet
Properties
Port Settings
Smartport
Apply
Cancel
Reset Energy Saving Counter
© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

Properties

For the functions and/or parameters configured on this page to become effective, you may have to configure the corresponding port based parameters on Port Settings page.

Energy Detect Mode: □ Enable

Short Reach: □ Enable

Port LEDs: ☑ Enable

802.3 Energy Efficient Ethernet (EEE): □ Enable

1) Open **Port Management** > **Green Ethernet** > **Properties.**

2) Uncheck any boxes for

   a. Energy Detect Mode
   b. Short Reach
   c. 802.3 Energy Efficient Ethernet (EEE)

3) Click **Apply** to confirm.

   When you click apply, you may lose connection with the switch for a period of time, say 15-30 seconds. Refresh your screen to reload.

4.2. Quality of Service (QoS)

What is QoS and When it is Helpful?

Quality of Service (QoS) allows us to prioritize some traffic over others. There are three main times this becomes a consideration for Dante networks:

1) Converged Networks (Networks that carry multiple traffic types, like audio and internet service)
2) Saturated Networks (Critical Audio Paths reach or exceed 70% of bandwidth capacity)
3) 100Mbit Devices (In this case, QoS will improve clocking stability)

It is important to realize that QoS Is not magic – it does not create more bandwidth. So, if your network is saturating, it may be time to get faster links. This is more effective. This is where you might consider a 1Gbit switch with 10Gbit uplink ports or arranging trunk lines in LAGs to handle the capacity.

Note – on the SG350, QoS settings will apply across all VLANs. Not only is the QoS engage switch common to all VLANs, but the priorities will be identical on all VLANs.

Dante QoS Values, Understanding QoS Queues

On the SG350, the DSCP values are shown with the DSCP label and Decimal Value, so we've greyed out the hex and binary values.

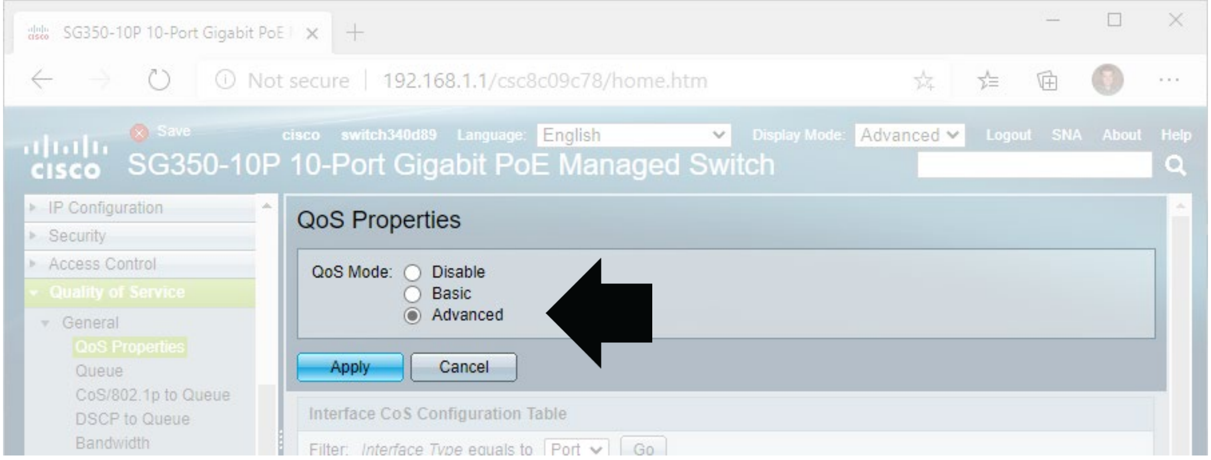
Dante DSCP Classes

Type	Priority	DSCP Label	Decimal	Hex	Binary
Clocking (PTP)	High	CS7	56	0x38	111000
Dante Audio	Medium	EF	46	0x2E	101110
Control	Low	CS1	8	0x08	001000

DSCP values on the packets will range from 0-63. This simply represents a "class" of data. The SG350 switch will read these values and place the packets in one of eight QoS priority queues as we decide. *(Note - the SG300 has 4 queues.)* So, the DSCP value is not the priority level – itself - higher DSCP values could be higher or lower priority – it all depends on the matrix you assign.

When we think of our "first priority", we think of an order of tasks. So, the first priority is the first step, or the highest priority. In QoS, it is inverted. The highest value is the highest priority. So, if there are 8 QoS Queues, then Queue 8 is the highest priority. It is common for people to misunderstand this and set up QoS completely backwards. Don't make that mistake!

Setting QoS for Dante


SG350-10P 10-Port Gigabit PoE
Not secure | 192.168.1.1/csc8c09c78/home.htm
Save
cisco switch340d89 Language: English Display Mode: Advanced Logout SNA About Help
cisco SG350-10P 10-Port Gigabit PoE Managed Switch
IP Configuration
Security
Access Control
Quality of Service
General
QoS Properties
Queue
CoS/802.1p to Queue
DSCP to Queue
Bandwidth

QoS Properties

QoS Mode: ○ Disable
○ Basic
● Advanced

Apply Cancel

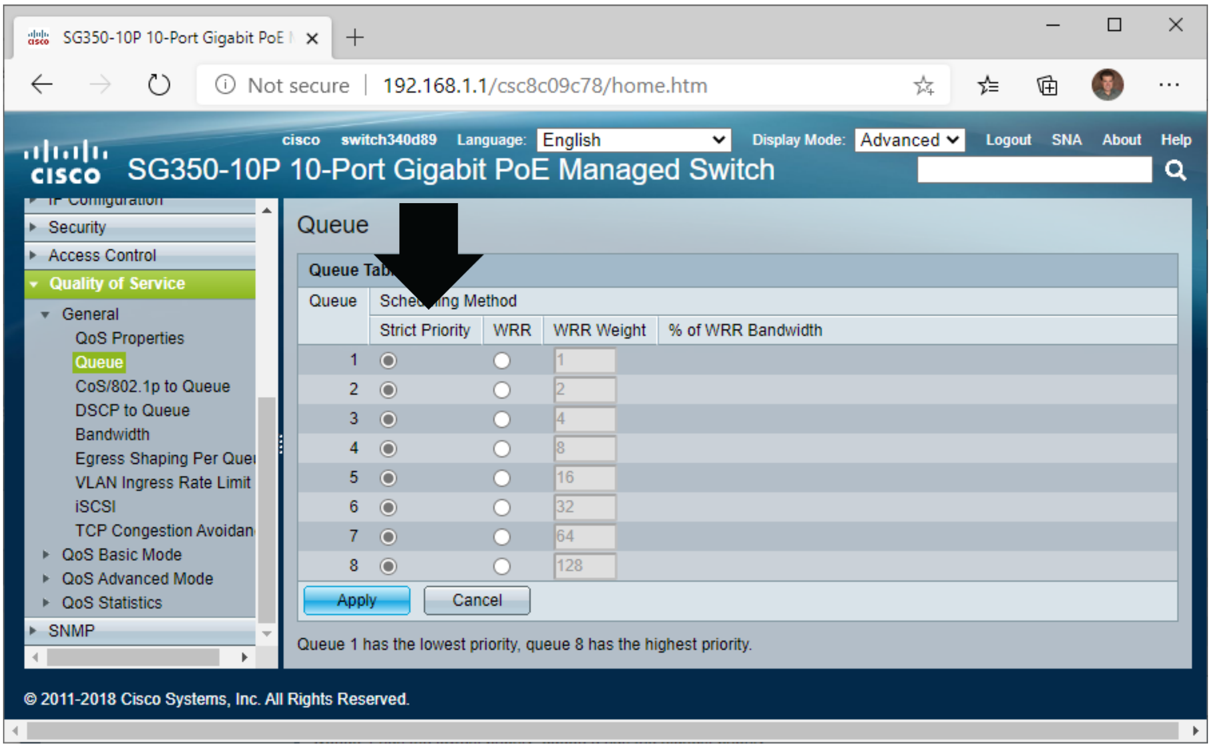
Interface CoS Configuration Table

Filter: *Interface Type* equals to Port Go

1) Go to **Quality of Service** > **General > QoS Properties**.

   a. Select the Advanced radio button for QoS Mode.

   b. Click **Apply**.



Queue

Queue Table

Queue	Scheduling Method			
	Strict Priority	WRR	WRR Weight	% of WRR Bandwidth
1	●	○	1	
2	●	○	2	
3	●	○	4	
4	●	○	8	
5	●	○	16	
6	●	○	32	
7	●	○	64	
8	●	○	128	

Apply Cancel

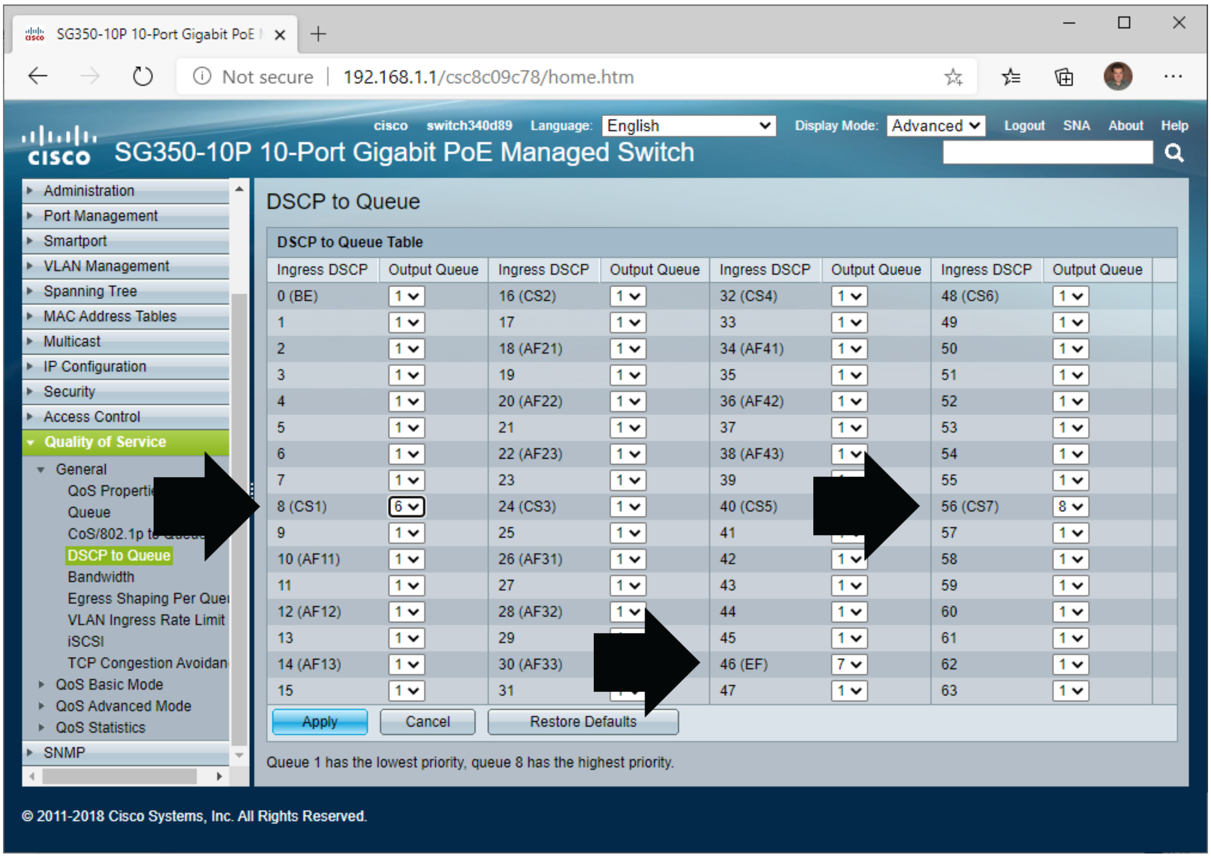
Queue 1 has the lowest priority, queue 8 has the highest priority.

© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

2) Go to **Quality of Service** > **General > Queue**.

   a. Ensure all queues are set to Strict Priority.

   b. If any changes were made, click **Apply.**



DSCP to Queue

DSCP to Queue Table

Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue
0 (BE)	1	16 (CS2)	1	32 (CS4)	1	48 (CS6)	1
1	1	17	1	33	1	49	1
2	1	18 (AF21)	1	34 (AF41)	1	50	1
3	1	19	1	35	1	51	1
4	1	20 (AF22)	1	36 (AF42)	1	52	1
5	1	21	1	37	1	53	1
6	1	22 (AF23)	1	38 (AF43)	1	54	1
7	1	23	1	39		55	1
8 (CS1)	6	24 (CS3)	1	40 (CS5)		56 (CS7)	8
9	1	25	1	41		57	1
10 (AF11)	1	26 (AF31)	1	42	1	58	1
11	1	27	1	43	1	59	1
12 (AF12)	1	28 (AF32)	1	44	1	60	1
13	1	29		45	1	61	1
14 (AF13)	1	30 (AF33)		46 (EF)	7	62	1
15	1	31		47	1	63	1

Queue 1 has the lowest priority, queue 8 has the highest priority.

3) Go to **Quality of Service** > **General > DSCP to Queue**.

a. Set all DSCP values to queue 1 (or some value below 6), for now.

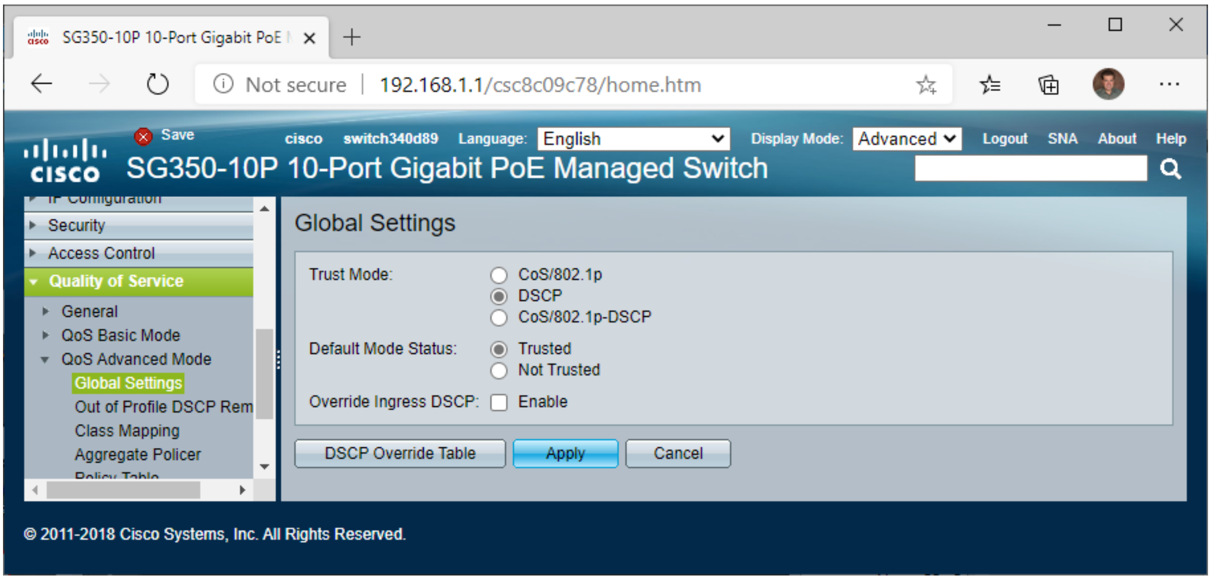
SG350 and SG300 Tip: Click on the dropdown menu for DSCP value 0 and press 1 on the keyboard. Then, alternate between pressing Tab and 1 on the keyboard to quickly advance through all DSCP values. Then, go back to elevate the few DCSP values as needed in the next steps.

b. Set DSCP value of **56 (SC7)** to enter queue **8**.

c. Set DSCP value of **46 (EF)** to enter queue **7**.

d. Set DSCP value of **8 (CS1)** to enter queue **6**.

e. Click **Apply** to confirm



Global Settings

Trust Mode: ○ CoS/802.1p ● DSCP ○ CoS/802.1p-DSCP

Default Mode Status: ● Trusted ○ Not Trusted

Override Ingress DSCP: □ Enable

4) Go to **Quality of Service** > **QoS Advanced Mode > Global Settings**.

   a. Set Trust Mode to DSCP.

   b. Set Default Mode Status to Trusted.

   c. Leave Ingress DSCP should be unchecked.

   d. Click **Apply** to confirm.

Reminder:
Now is a good time to save.

4.3. IGMP Snooping

Without IGMP snooping, any multicast packet will be delivered to every port in your LAN (or VLAN). By engaging IGMP snooping, you can ask the switch to only send multicast to the devices that request it.

Dante networks certainly use multicast for discovery and clocking, but this is a very low data load. It may be under 20Kbps, on a small network… or 0.002% of a 1Gbit port's capacity. Dante audio and video are unicast by default. When flows are flipped to multicast to create a traffic build-up, then IGMP snooping becomes valuable.

When considering what is "a lot" of multicast, think in terms of the slowest port in that LAN. Like QoS, the presence of 100Mbit or even 10Mbit ports will increase IGMP snooping's benefit.

To gauge your multicast traffic, Dante Controller estimates the amount of multicast traffic generated by Dante audio and video flows at the bottom of the screen. This number does not account for multicast traffic from other systems… it is just a calculation of Dante's impact.

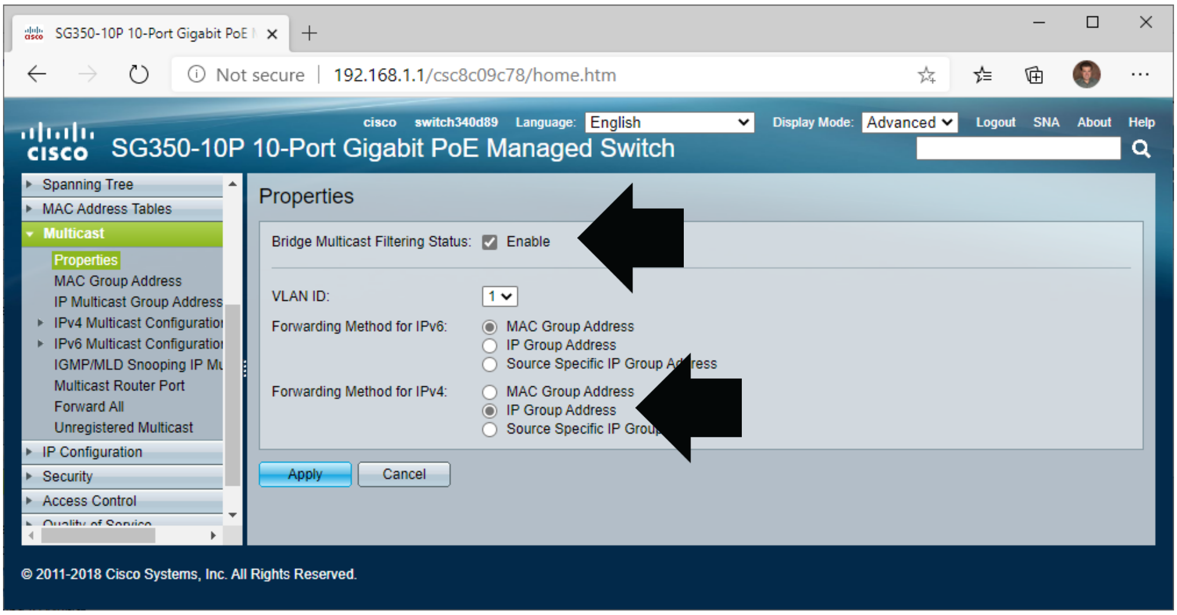
It is also possible to look in Dante Controller > Device Info tab and see how much traffic is being received at each port on the Dante primary (and if applicable) secondary network.

For those who worked on older Cisco SG300 switches, this process is not many steps longer than it was before. However, this will get you through the process.

On the SG350-series, IGMP snooping can be enabled on a per-VLAN basis. This is not true of all network switches – some only offer a global switch for all VLANs. In this example, we only need to turn on IGMP snooping on VLAN 1.

> **Mac OS-X machines running Dante Virtual Soundcard (DVS)** will likely lose clock and mute when IGMP snooping is engaged on many switch manufacturers. The Mac OS and many switch configurations do not refresh the Time-To-Live for multicast subscriptions, and thus the clock falls silent. You'll know this is the case if Dante Controller shows "Listening" status. To address this, after multicast is set up, continue to the next section on manually forwarding multicast streams.

Set IGMP Snooping based on IP Group Address



Properties

Bridge Multicast Filtering Status: ☑ Enable

VLAN ID: 1

Forwarding Method for IPv6: ● MAC Group Address ○ IP Group Address ○ Source Specific IP Group Address

Forwarding Method for IPv4: ○ MAC Group Address ● IP Group Address ○ Source Specific IP Group

1) Open **Multicast > Properties.**

   a. Check the box for **Bridge Multicast Filtering Status.**

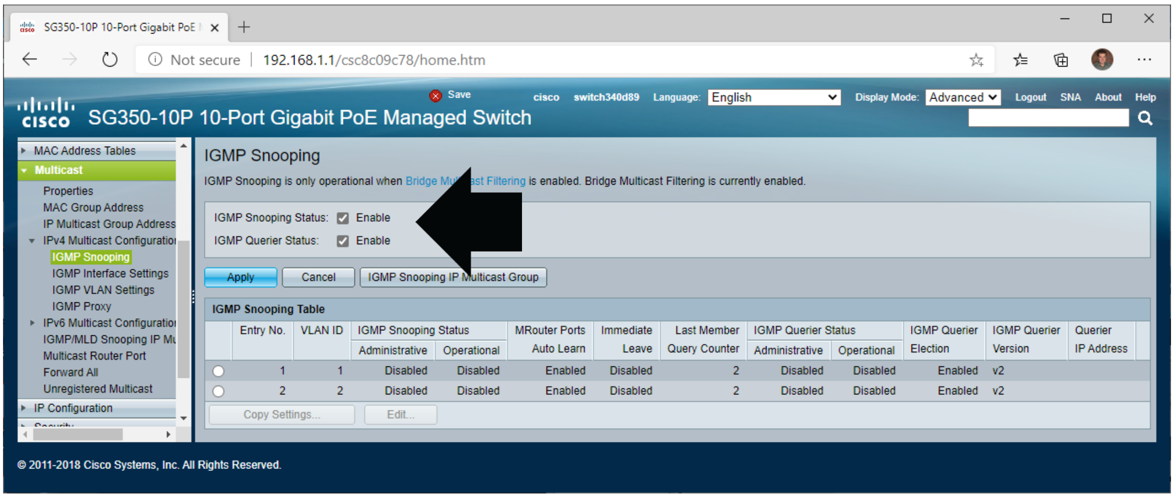
   b. Select the VLAN ID on which you would like to engage IDMP Snooping. *If there are no VLANs, use VLAN ID 1.*

   c. Under **Forwarding Method for IPv4**, select the radio button for **IP Group Address**.

   d. Click **Apply**.

2) *If you create more VLANs, you will need to repeat this process on each VLAN you would like to have IGMP Snooping engaged on.*

Engage IGMP Snooping (and Choose One Switch as Querier)


SG350-10P 10-Port Gigabit PoE
Not secure | 192.168.1.1/csc8c09c78/home.htm
Save
cisco switch340d89 Language: English
Display Mode: Advanced
Logout SNA About Help
cisco SG350-10P 10-Port Gigabit PoE Managed Switch
MAC Address Tables
Multicast
Properties
MAC Group Address
IP Multicast Group Address
IPv4 Multicast Configuratio
IGMP Snooping
IGMP Interface Settings
IGMP VLAN Settings
IGMP Proxy
IPv6 Multicast Configuratio
IGMP/MLD Snooping IP Mu
Multicast Router Port
Forward All
Unregistered Multicast
IP Configuration
Apply
Cancel
IGMP Snooping IP Multicast Group
Copy Settings...
Edit...
© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

IGMP Snooping

IGMP Snooping is only operational when Bridge Mu ast Filtering is enabled. Bridge Multicast Filtering is currently enabled.

IGMP Snooping Status: ☑ Enable

IGMP Querier Status: ☑ Enable

IGMP Snooping Table

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

1) Go to **Multicast** > **IPv4 Multicast Configuration** > **IGMP Snooping**.

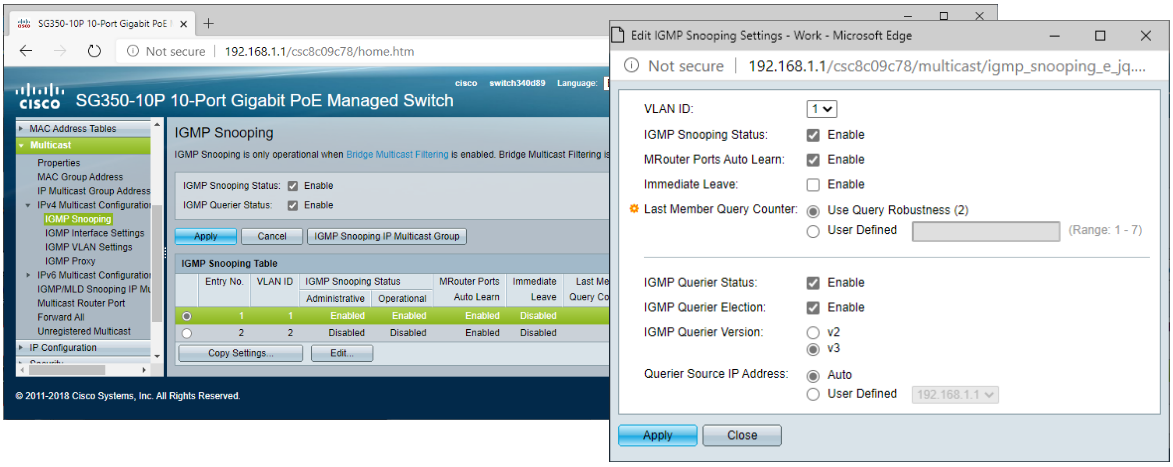
   a. Check the box for **IGMP Snooping Status** for all switches in the network.

   b. Check the box for **IGMP Querier Status** on one switch in the network.

   Note: If you have primary and secondary on isolated switches, then you have two networks. If you want IGMP snooping on both networks, you should have one querier on the primary, and one on the secondary.

   c. Click **Apply**.

Edit IGMP Snooping Parameters for Dante VLANs, Part 1


SG350-10P 10-Port Gigabit PoE
Not secure | 192.168.1.1/csc8c09c78/home.htm
cisco switch340d89 Language:
cisco SG350-10P 10-Port Gigabit PoE Managed Switch
MAC Address Tables
Multicast
Properties
MAC Group Address
IP Multicast Group Address
IPv4 Multicast Configuration
IGMP Snooping
IGMP Interface Settings
IGMP VLAN Settings
IGMP Proxy
IPv6 Multicast Configuration
IGMP/MLD Snooping IP Mu
Multicast Router Port
Forward All
Unregistered Multicast
IP Configuration
Apply
Cancel
IGMP Snooping IP Multicast Group
Copy Settings...
Edit...
© 2011-2018 Cisco Systems, Inc. All Rights Reserved.
Edit IGMP Snooping Settings - Work - Microsoft Edge
Not secure | 192.168.1.1/csc8c09c78/multicast/igmp_snooping_e_jq....
Apply
Close

IGMP Snooping

IGMP Snooping is only operational when Bridge Multicast Filtering is enabled. Bridge Multicast Filtering is

IGMP Snooping Status: ☑ Enable

IGMP Querier Status: ☑ Enable

IGMP Snooping Table

	Entry No.	VLAN ID	IGMP Snooping Status		MRouter Ports Auto Learn	Immediate Leave	Last Me Query Co
			Administrative	Operational			
●	1	1	Enabled	Enabled	Enabled	Disabled	
○	2	2	Disabled	Disabled	Enabled	Disabled	

VLAN ID: 1

IGMP Snooping Status: ☑ Enable

MRouter Ports Auto Learn: ☑ Enable

Immediate Leave: □ Enable

Last Member Query Counter: ● Use Query Robustness (2)
○ User Defined (Range: 1 - 7)

IGMP Querier Status: ☑ Enable

IGMP Querier Election: ☑ Enable

IGMP Querier Version: ○ v2
● v3

Querier Source IP Address: ● Auto
○ User Defined 192.168.1.1

1) While still in **Multicast** > **IPv4 Multicast Configuration** > **IGMP Snooping**.

2) Check the box to select a the VLAN with Dante traffic, and click **Edit**.

3) In the top section, set

a. VLAN ID: *Select the VLAN you wish to affect. If there are no VLANs, use ID 1.*

b. IGMP Snooping Status: ☑ Enabled

c. MRouter Ports Auto Learn: ☑ Enabled

d. Immediate Leave: □ Enabled

e. Last member Query Counter: ⦿ Use Query Robustness (2)
○ User Defined

4) If this switch will not be the IGMP Querier in the network, uncheck the IGMP Querier Status box; the rest will grey out (and won't matter). However, in a single switch exercise this switch will be the querier, so make the following settings:

a. IGMP Querier Status: ☑ Enabled

b. IGMP Querier Election: ☑ Enabled

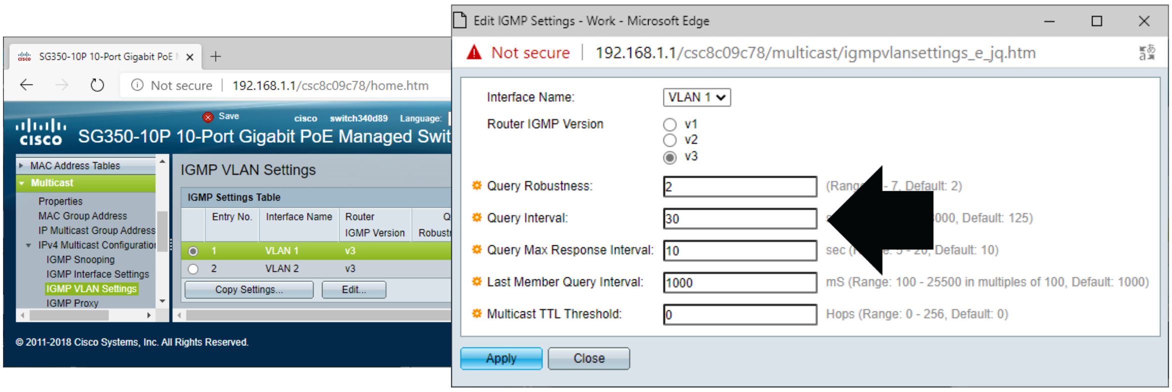
c. IGMP Querier Version: ○ v2
⦿ v3

d. Querier Source IP Address: ⦿ Auto
○ User Defined

5) Click **Apply** to Confirm

6) *Repeat for each VLAN you wish to have IGMP snooping managing Dante multicast traffic.*

Edit IGMP Snooping Parameters for Dante VLANs, Part 2


SG350-10P 10-Port Gigabit PoE
Not secure | 192.168.1.1/csc8c09c78/home.htm
Save
cisco
switch340d89
Language:
cisco
SG350-10P 10-Port Gigabit PoE Managed Swit
MAC Address Tables
Multicast
Properties
MAC Group Address
IP Multicast Group Address
IPv4 Multicast Configuratio
IGMP Snooping
IGMP Interface Settings
IGMP VLAN Settings
IGMP Proxy
IGMP VLAN Settings
Copy Settings...
Edit...
© 2011-2018 Cisco Systems, Inc. All Rights Reserved.
Edit IGMP Settings - Work - Microsoft Edge
Not secure | 192.168.1.1/csc8c09c78/multicast/igmpvlansettings_e_jq.htm
Apply
Close

IGMP Settings Table

	Entry No.	Interface Name	Router IGMP Version	Q Robust
●	1	VLAN 1	v3	
○	2	VLAN 2	v3	

Interface Name: VLAN 1

Router IGMP Version: ○ v1 ○ v2 ● v3

Query Robustness: 2 (Rang - 7, Default: 2)

Query Interval: 30 000, Default: 125)

Query Max Response Interval: 10 sec (e: 5 - 20, Default: 10)

Last Member Query Interval: 1000 mS (Range: 100 - 25500 in multiples of 100, Default: 1000)

Multicast TTL Threshold: 0 Hops (Range: 0 - 256, Default: 0)

1) Open **Multicast** > **IPv4 Multicast Configuration** > **IGMP VLAN Settings**.

2) Check the box to select a the VLAN with Dante traffic, and click **Edit**.

3) Select the VLAN which has Dante. *If there are no VLANs, use ID 1.*

4) Make the following settings: *The query Interval should be the only non-default setting.*

IGMP Querier Version:	○ v1 ○ v2 ⦿ v3	
Query Robustness:	2	(Range 1-7, Default 2)
Query Interval:	30	sec (Range: 30-18000, Default 125)
Query Max Response Interval:	10	sec (Range: 5-20, Default 10)
Last Member Query Interval:	1000	mS (Range: 100-25500 in multiples of 100. Default 1000)
Multicast TTL Threshold:	0	Hops (Range: 0- 256, Default 0)

5) Click **Apply** to confirm.

6) Repeat for each VLAN you wish to have IGMP snooping managing Dante multicast traffic.

Helpful Tips:

Dante can operate using IGMP snooping v2 or v3. There are other audio devices on the market that do not support IGMP snooping v3. If you need to downgrade to v2, Dante can adapt to that.

For those in live production environments, communication for IP-based lighting systems like Art-Net or ETCNet is largely multicast and their manufacturers usually prefer IGMP Snooping to be off. So, if that traffic will exist on the same network switches, it is wise to put it on a separate VLAN and leave IGMP snooping off for the lighting VLAN (assuming the switch supports this capability).

Reminder:
Now is a good time to save.

4.4. Manually Forwarding Multicast Streams

Some devices do not operate properly with IGMP snooping. The Mac OS platform with Dante Virtual Soundcard (DVS) is an example where conflicts arise. When the design calls for IGMP snooping and yet some critical devices will not work correctly, here are two ways to manually manage multicast traffic:

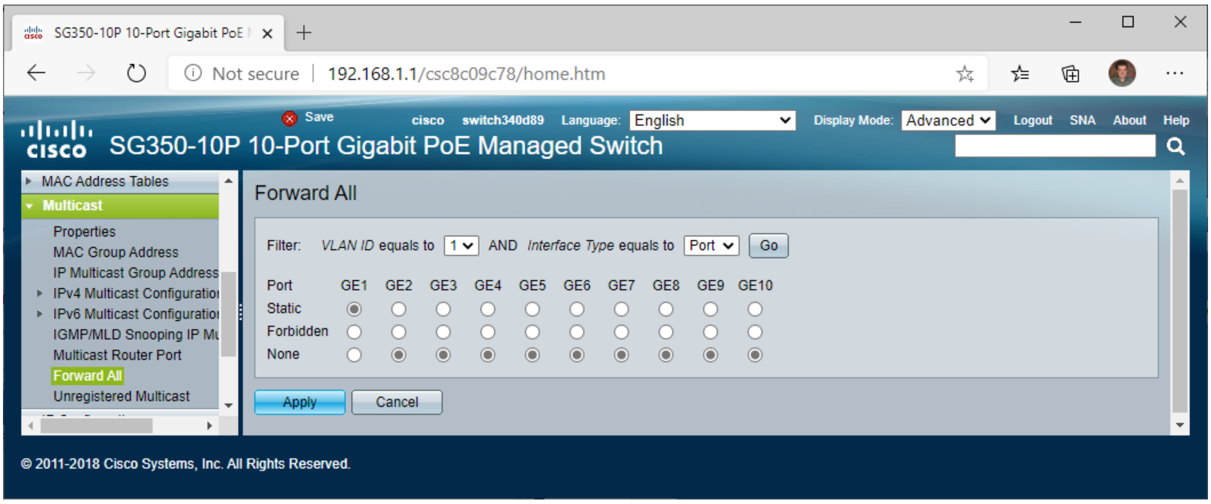
Forward All Multicast does what it sounds like – it forwards all multicast traffic to a particular port. This is the functional equivalent of disabling IGMP snooping for a single port. If the devices in question can handle the full multicast load (especially if it will be requesting most, if not all multicast traffic anyway), this can be a crude, but simple way to solve the issue. *For instance, if a Mac OS-X machine has a 1Gbit port and there is 200Mbit of multicast traffic on the network, this may be an acceptable, especially for a recording DAW.*

Manually Forwarding Multicast also does what it sounds like. If the required streams are known, the switch can be manually instructed to send specific multicast streams to a port. This is more precise than Forward All Multicast, not only alleviating unnecessary bandwidth on a particular port, but also on the trunk lines between switches carrying the unnecessary data in this direction. However, if the mix of streams changes over time, this may need manual reconfiguration. *This may be preferable for a machine that is only struggling with clocking data and does not need the other streams. An example might be a DAW that is simply playing backing tracks or running virtual instruments for a live stage show.*

Helpful Tips:

When configuring ports in this way for a Mac OS-X machine, it is helpful to indicate this on the physical port itself. Add an Apple logo, or a simple label to indicate this port has a custom adaptation for that computer. This is especially helpful for laptops that come and go.

Option 1: Forward All Multicast for a Port


SG350-10P 10-Port Gigabit PoE
Not secure
192.168.1.1/csc8c09c78/home.htm
Save
cisco
switch340d89
Language: English
Display Mode: Advanced
Logout
SNA
About
Help
SG350-10P 10-Port Gigabit PoE Managed Switch
MAC Address Tables
Multicast
Properties
MAC Group Address
IP Multicast Group Address
IPv4 Multicast Configuratio
IPv6 Multicast Configuratio
IGMP/MLD Snooping IP Mu
Multicast Router Port
Forward All
Unregistered Multicast
Apply
Cancel
© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

Forward All

Filter: *VLAN ID* equals to 1 AND *Interface Type* equals to Port Go

Port	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10
Static	●	○	○	○	○	○	○	○	○	○
Forbidden	○	○	○	○	○	○	○	○	○	○
None	○	●	●	●	●	●	●	●	●	●

1) Go to **Multicast** > **Forward All**.

   a. Choose the appropriate VLAN. If changed, click **Go**. *If there are no VLANs, use ID 1.*

   b. Select the **Static** radio button for the desired ports. *In the above example, we target port 1.*

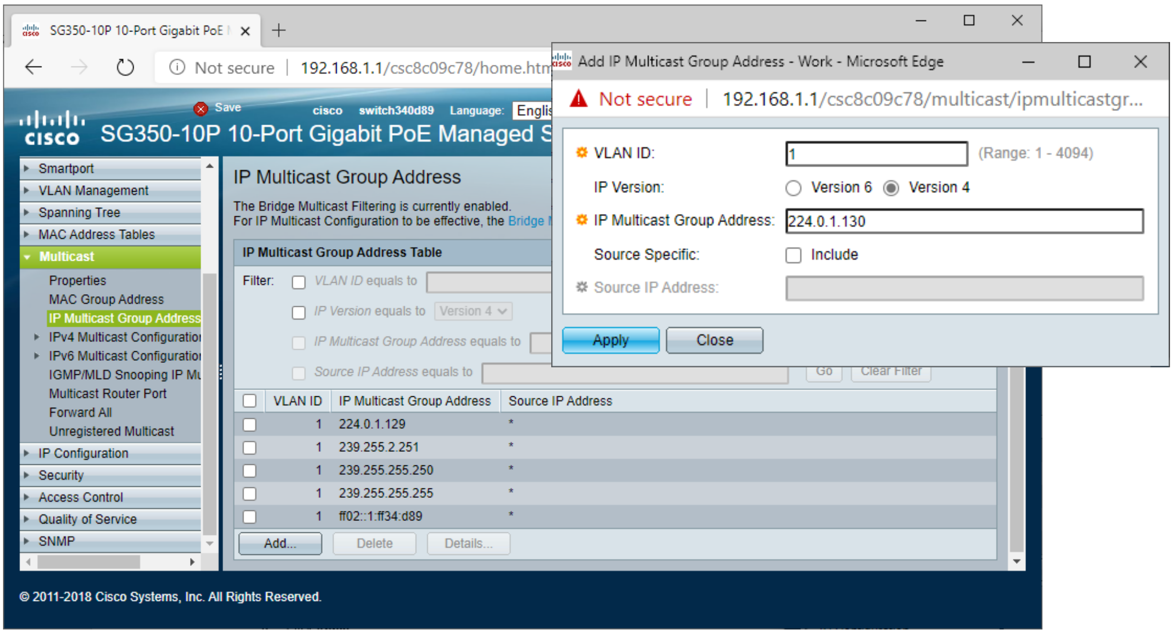
2) Click **Apply**.

Option 2: Manually Forwarding Individual Multicast Streams for a Port

Rather than forward every multicast stream, thereby defeating IGMP Snooping on a port, it is also possible to selectively (manually) forward the streams needed for a device. The SG350 does not appear to offer access down to the multicast stream port level, it simply sends anything from any port on a multicast IP.

Core Dante Multicast Group Addresses

Type	Multicast Stream IP/Port
Dante Discovery (mDNS)	224.0.0.251 :5353
Dante Clocking (PTP)	224.0.1.129 - 224.0.1.132, ports 319 - 320
Dante Monitoring	224.0.0.320– 224.0.0.232, ports 8700 - 8706


SG350-10P 10-Port Gigabit PoE
Not secure | 192.168.1.1/csc8c09c78/home.htm
Save
cisco switch340d89 Language: English
cisco SG350-10P 10-Port Gigabit PoE Managed S
Smartport
VLAN Management
Spanning Tree
MAC Address Tables
Multicast
Properties
MAC Group Address
IP Multicast Group Address
IPv4 Multicast Configuration
IPv6 Multicast Configuration
IGMP/MLD Snooping IP Mu
Multicast Router Port
Forward All
Unregistered Multicast
IP Configuration
Security
Access Control
Quality of Service
SNMP
Add IP Multicast Group Address - Work - Microsoft Edge
Not secure | 192.168.1.1/csc8c09c78/multicast/ipmulticastgr...
Go
Clear Filter
Add...
Delete
Details...
Apply
Close
© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

IP Multicast Group Address

The Bridge Multicast Filtering is currently enabled.
For IP Multicast Configuration to be effective, the Bridge M

IP Multicast Group Address Table

Filter: □ VLAN ID equals to
□ IP Version equals to Version 4
□ IP Multicast Group Address equals to
□ Source IP Address equals to

□	VLAN ID	IP Multicast Group Address	Source IP Address
□	1	224.0.1.129	*
□	1	239.255.2.251	*
□	1	239.255.255.250	*
□	1	239.255.255.255	*
□	1	ff02::1:ff34:d89	*

VLAN ID: 1 (Range: 1 - 4094)

IP Version: ○ Version 6 ● Version 4

IP Multicast Group Address: 224.0.1.130

Source Specific: □ Include

Source IP Address:

1) Go to **Multicast** > **IP Multicast Group Addresses**.

   The table will show streams it already sees existing on the network.

2) If the stream you want is not listed in the table, click **Add…** to list a new Multicast Group Address:

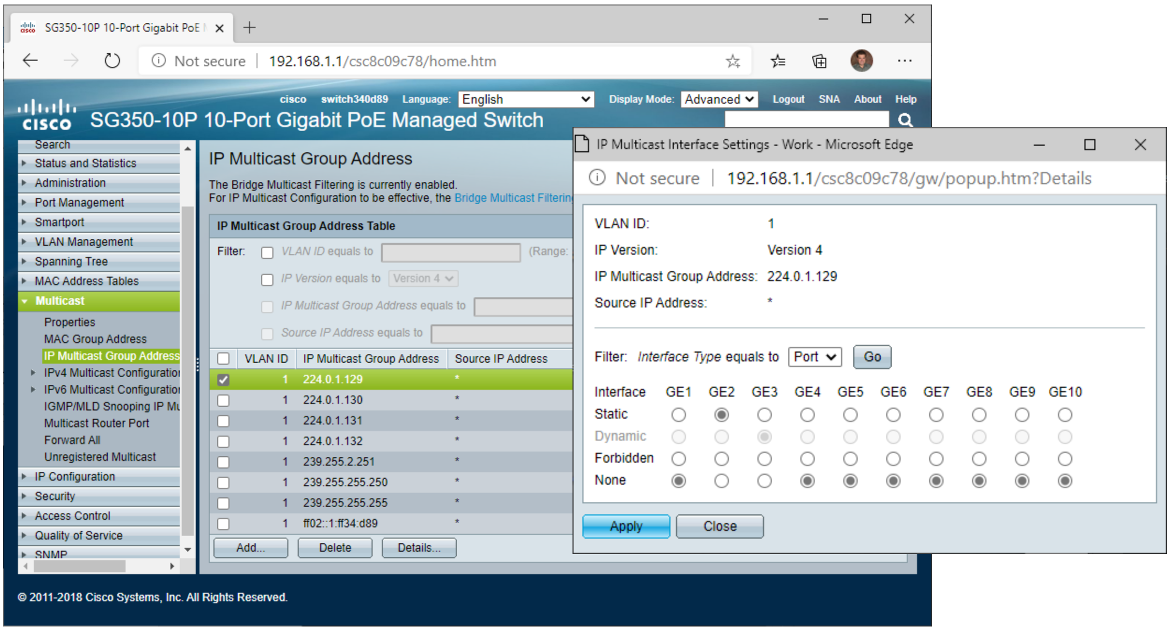
   a. Choose the **VLAN** on which you want to forward a stream. *If there are no VLANs, use ID 1.*

   b. Ensure **IP Version** radio button for **Version 4** is selected.

   c. Enter the **IP Multicast Group address**.

   d. Click **Apply**.

   e. Repeat this for each Multicast Group Address you'd like to add, then close the pop-up.



SG350-10P 10-Port Gigabit PoE
Not secure | 192.168.1.1/csc8c09c78/home.htm
cisco switch340d89 Language: English Display Mode: Advanced Logout SNA About Help
SG350-10P 10-Port Gigabit PoE Managed Switch
Search
Status and Statistics
Administration
Port Management
Smartport
VLAN Management
Spanning Tree
MAC Address Tables
Multicast
Properties
MAC Group Address
IP Multicast Group Address
IPv4 Multicast Configuration
IPv6 Multicast Configuration
IGMP/MLD Snooping IP Mu
Multicast Router Port
Forward All
Unregistered Multicast
IP Configuration
Security
Access Control
Quality of Service
SNMP
© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

IP Multicast Group Address

The Bridge Multicast Filtering is currently enabled.
For IP Multicast Configuration to be effective, the Bridge Multicast Filtering

IP Multicast Group Address Table

Filter: □ VLAN ID equals to (Range:
□ IP Version equals to Version 4
□ IP Multicast Group Address equals to
□ Source IP Address equals to

□	VLAN ID	IP Multicast Group Address	Source IP Address
☑	1	224.0.1.129	*
□	1	224.0.1.130	*
□	1	224.0.1.131	*
□	1	224.0.1.132	*
□	1	239.255.2.251	*
□	1	239.255.255.250	*
□	1	239.255.255.255	*
□	1	ff02::1:ff34:d89	*

Add... Delete Details...

IP Multicast Interface Settings - Work - Microsoft Edge

Not secure | 192.168.1.1/csc8c09c78/gw/popup.htm?Details

VLAN ID: 1
IP Version: Version 4
IP Multicast Group Address: 224.0.1.129
Source IP Address: *

Filter: *Interface Type* equals to Port Go

Interface	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10
Static	○	●	○	○	○	○	○	○	○	○
Dynamic	○	○	●	○	○	○	○	○	○	○
Forbidden	○	○	○	○	○	○	○	○	○	○
None	●	○	○	●	●	●	●	●	●	●

Apply Close

3) Select a Multicast Group Address to Manually route, and click **Details…**

a. For ports to receive this stream manually as **Static**. Leave others on **None**.

4) Click **Apply**.

Reminder:
Now is a good time to save.

5. Inter-VLAN Routing, DHCP

To succeed in this chapter, the reader needs to have a firm grasp on the concepts taught in Audinate's Dante Certification Level 3, 2021 Edition. DHCP service, while a very simple concept, is included in this chapter because the DHCP service intertwines with Inter-VLAN routing. It seemed logical to keep the two together in this section. For information about the Dante Certified Training Program, go to https://audinate.com/certify

Switch Example Design

Port:	1	2	3	4	5	6	7	8	9	10
VLAN/Tagged "U" is untagged "T" is tagged	1 - U Dante Subnet 1					2 - U Dante Subnet 2		9 - U Internet	1 - U (Dante 1) 2 - T (Dante 2)	
Type	Access					Access		Access	Trunk	
Special	Forward All Multicast	Manual Forward Multicast							LAG #1	

This chapter will build upon the configuration from the prior chapter, with some minor modifications.

VLAN 2 will be converted to another Dante VLAN. Inter-VLAN routing will be engaged. If a Dante Domain Manager server is available, we will set it in VLAN 1 on port 5 at 192.168.1.2. This will allow devices to work together across subnets, complete with discovery (once recognized by Dante Domain Manager), as well as clocking, audio routing and control.

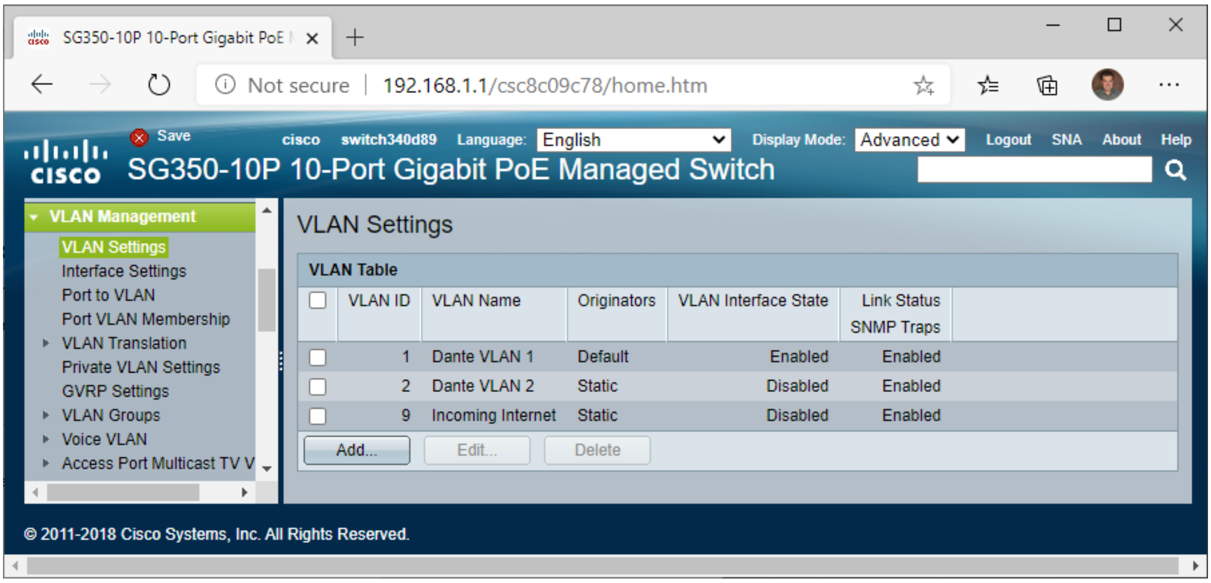
VLAN 9 will be added to bring in internet service from an edge router. The edge router will require a static route to this "next hop router". As such, this will not likely work with a standard home cable modem or DSL router. In the example, we will use a Cisco RV340 SMB router, which can bridge the gap even in a home setting.

The subnets and static IPs assigned will be as follows:

Exercise VLANs, Subnet Assignments and Static IPs

VLAN	Subnet	Static IPs	
1 - Dante Subnet 1	192.168.1.0 /24	192.168.1.1 192.168.1.2	Router, Switch Management Address Dante Domain Manager Server
2 - Dante Subnet 2	192.168.2.0 /24	192.168.2.1	Router
9 – Internet	192.168.0.0 /24	192.168.0.1 192.168.0.2	Internet Router Local InterVLAN Router on this switch

5.1. Reapply Lesson from Prior Chapter Switch Modifications


SG350-10P 10-Port Gigabit PoE
Not secure | 192.168.1.1/csc8c09c78/home.htm
Save
cisco switch340d89 Language: English Display Mode: Advanced Logout SNA About Help
SG350-10P 10-Port Gigabit PoE Managed Switch
VLAN Management
VLAN Settings
Interface Settings
Port to VLAN
Port VLAN Membership
VLAN Translation
Private VLAN Settings
GVRP Settings
VLAN Groups
Voice VLAN
Access Port Multicast TV V
Add...
Edit...
Delete
© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

VLAN Settings

VLAN Table

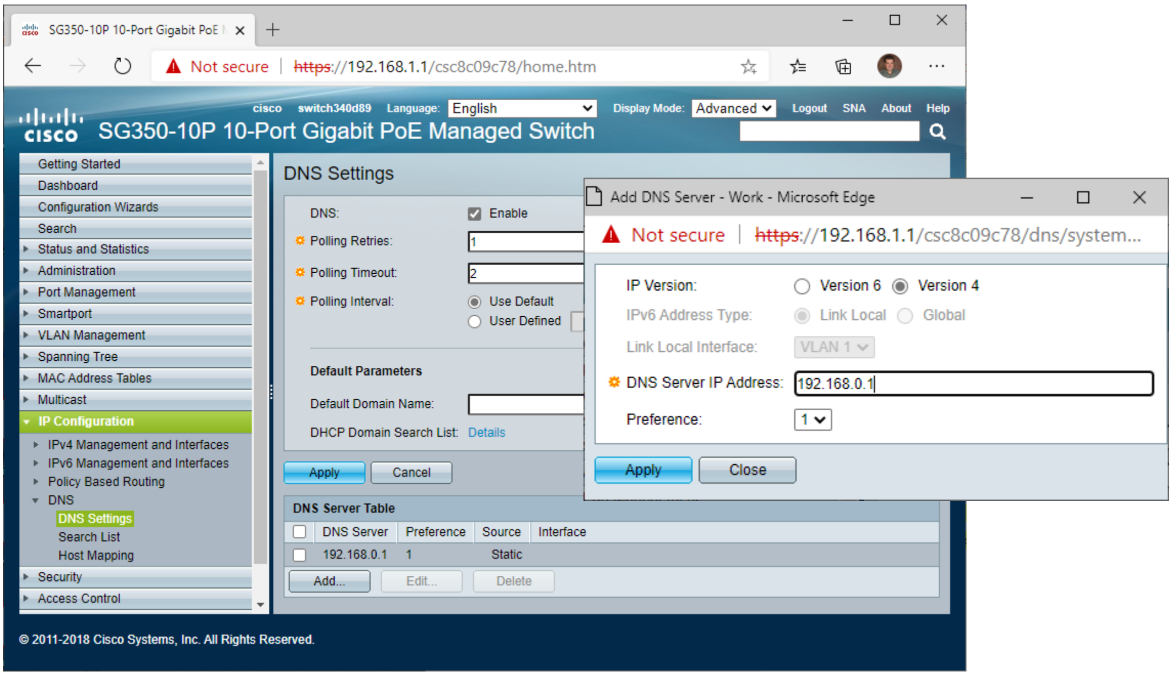
□	VLAN ID	VLAN Name	Originators	VLAN Interface State	Link Status SNMP Traps
□	1	Dante VLAN 1	Default	Enabled	Enabled
□	2	Dante VLAN 2	Static	Disabled	Enabled
□	9	Incoming Internet	Static	Disabled	Enabled

If desired, revisit section 4.3 for instructions on setting IGMP Snooping on VLAN 2.

If you have a router capable of static routes, revisit section 3.1 to 3.2 for instructions on creating VLAN 9 to accept the incoming internet service and assign it to port 8.

5.2. Add a DNS Server:

DNS server converts domain names (like www.audinate.com) to IP addresses. This exercise offers the option of bringing in internet service, and DNS will be critical to making that useful. DNS servers can also be set up to service local addresses. In this example, we simply use the main router's reflection to the ISP.



DNS Settings

DNS: ☑ Enable

Polling Retries: 1

Polling Timeout: 2

Polling Interval: ● Use Default ○ User Defined

Default Parameters

Default Domain Name:

DHCP Domain Search List: Details

DNS Server Table

□	DNS Server	Preference	Source	Interface
□	192.168.0.1	1	Static	

Add DNS Server

IP Version: ○ Version 6 ● Version 4

IPv6 Address Type: ● Link Local ○ Global

Link Local Interface: VLAN 1

DNS Server IP Address: 192.168.0.1

Preference: 1

1) Go to **IP Configuration** > **DNS** > **DNS Settings**

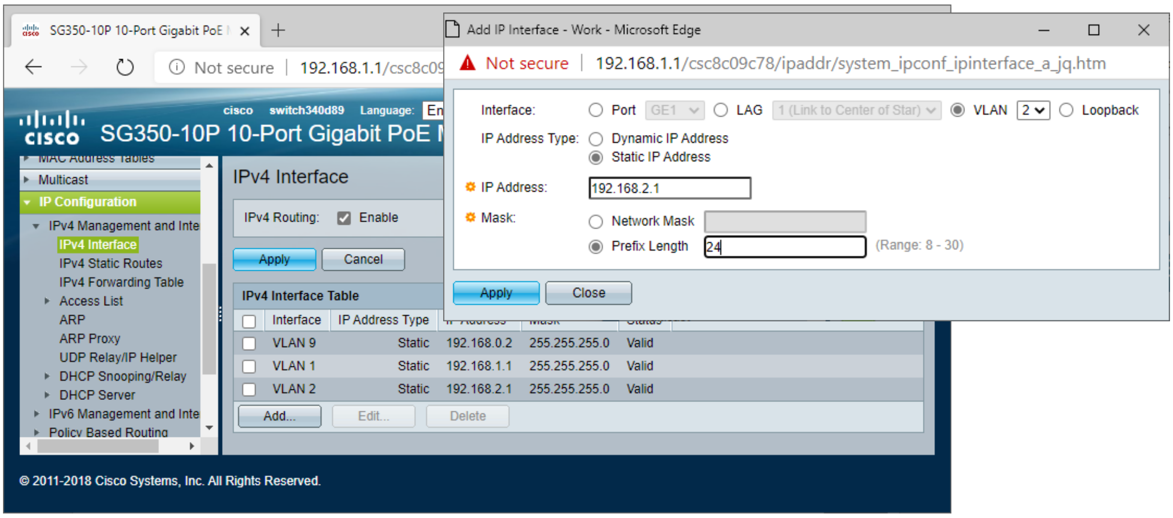
   a. Under **DNS Server Table**, click **Add…**

   b. Add the **DNS Server's IP Address**. In this example, that is **192.168.0.1**.

   c. Click **Apply**.

Reminder:
Now is a good time to save.

5.3. Assign Router IP Address in Each VLAN for Inter-VLAN routing


SG350-10P 10-Port Gigabit PoE
Not secure | 192.168.1.1/csc8c09
cisco switch340d89 Language: En
SG350-10P 10-Port Gigabit PoE
MAC Address Tables
Multicast
IP Configuration
IPv4 Management and Inte
IPv4 Interface
IPv4 Static Routes
IPv4 Forwarding Table
Access List
ARP
ARP Proxy
UDP Relay/IP Helper
DHCP Snooping/Relay
DHCP Server
IPv6 Management and Inte
Policy Based Routing
Apply
Cancel
Add...
Edit...
Delete
© 2011-2018 Cisco Systems, Inc. All Rights Reserved.
Add IP Interface - Work - Microsoft Edge
Not secure | 192.168.1.1/csc8c09c78/ipaddr/system_ipconf_ipinterface_a_jq.htm
Apply
Close

IPv4 Interface

IPv4 Routing: ☑ Enable

IPv4 Interface Table

□	Interface	IP Address Type			
□	VLAN 9	Static	192.168.0.2	255.255.255.0	Valid
□	VLAN 1	Static	192.168.1.1	255.255.255.0	Valid
□	VLAN 2	Static	192.168.2.1	255.255.255.0	Valid

Interface: ○ Port GE1 ○ LAG 1 (Link to Center of Star) ● VLAN 2 ○ Loopback

IP Address Type: ○ Dynamic IP Address ● Static IP Address

IP Address: 192.168.2.1

Mask: ○ Network Mask ● Prefix Length 24 (Range: 8 - 30)

1) Open the **IP Configuration** menu, **IPv4 Management and Interface**, and select **IPv4 Interface.**

2) Click **Add…**

   a. Ensure **VLAN 1** is selected at the top.

   b. Select the radio button for **IP Address type** as **Static IP Address.**

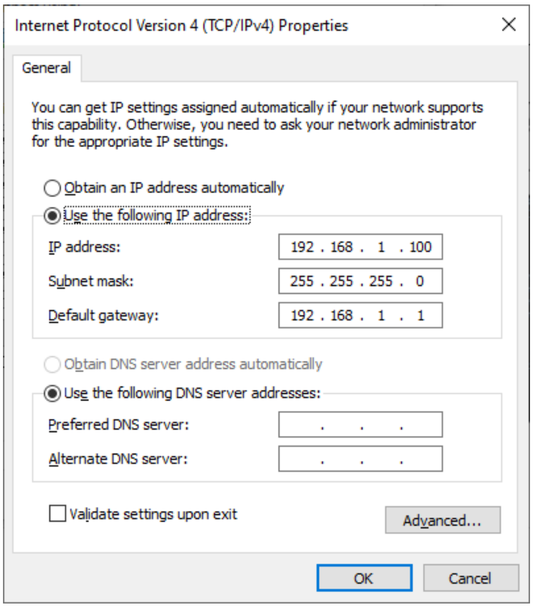
   c. Type in an address of **192.168.1.1.**

   d. Select a **Network Mask** of **255.255.255.0** *or choose a prefix length of 24 – it is the same result*.

   e. Click **Apply**.

3) Repeat this process for VLAN 2, adding a router address of **192.168.2.1.**

4) If you are adding the internet feed, repeat this process for VLAN 9, adding a router at 192.168.0.2. This switch's router will end in dot-2, the edge router will end in dot-1.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

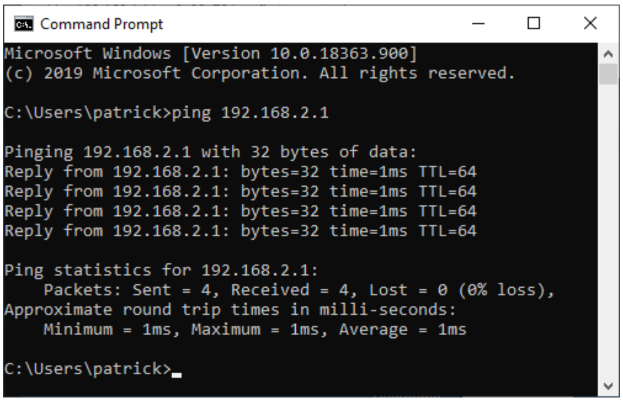
IP address: 192 . 168 . 1 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

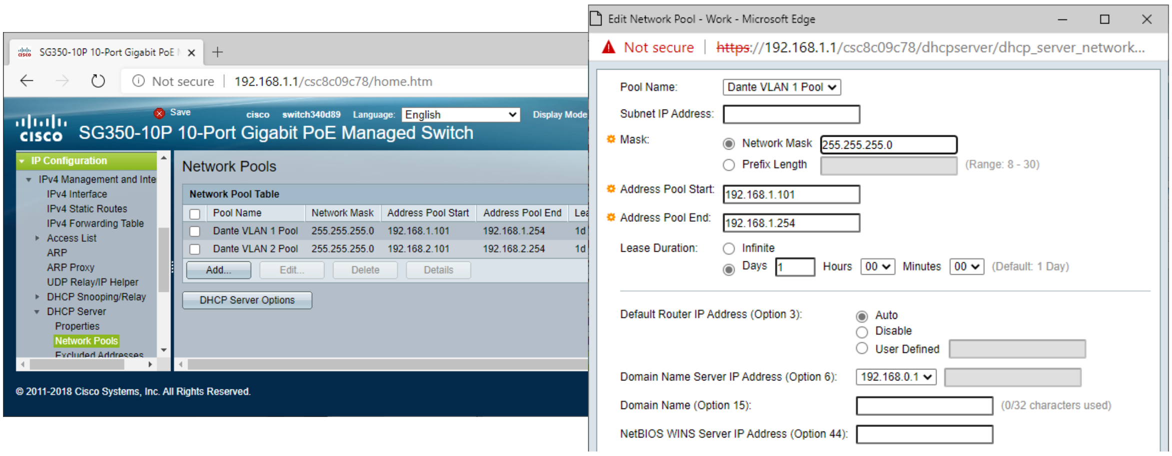
□ Validate settings upon exit

If your computer is still set up in static IP with no gateway, add a gateway, now. With that in place, we should be able to ping the addresses of the routers. If you have other devices on the network, you can ping them as well.



```
Microsoft Windows [Version 10.0.18363.900]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\patrick>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=1ms TTL=64
Reply from 192.168.2.1: bytes=32 time=1ms TTL=64
Reply from 192.168.2.1: bytes=32 time=1ms TTL=64
Reply from 192.168.2.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\patrick>_
```

5.4. Assign DHCP Service in VLANs 1 and 2


SG350-10P 10-Port Gigabit PoE
Not secure | 192.168.1.1/csc8c09c78/home.htm
Save
cisco
switch340d89
Language: English
Display Mode
cisco
SG350-10P 10-Port Gigabit PoE Managed Switch
IP Configuration
IPv4 Management and Inte
IPv4 Interface
IPv4 Static Routes
IPv4 Forwarding Table
Access List
ARP
ARP Proxy
UDP Relay/IP Helper
DHCP Snooping/Relay
DHCP Server
Properties
Network Pools
Excluded Addresses
© 2011-2018 Cisco Systems, Inc. All Rights Reserved.
Edit Network Pool - Work - Microsoft Edge
Not secure | ~~https~~://192.168.1.1/csc8c09c78/dhcpserver/dhcp_server_network...

Network Pools

Network Pool Table

□	Pool Name	Network Mask	Address Pool Start	Address Pool End	Lea
□	Dante VLAN 1 Pool	255.255.255.0	192.168.1.101	192.168.1.254	1d
□	Dante VLAN 2 Pool	255.255.255.0	192.168.2.101	192.168.2.254	1d

Add... | Edit... | Delete | Details

DHCP Server Options

Pool Name: Dante VLAN 1 Pool

Subnet IP Address:

Mask: ● Network Mask 255.255.255.0 ○ Prefix Length (Range: 8 - 30)

Address Pool Start: 192.168.1.101

Address Pool End: 192.168.1.254

Lease Duration: ○ Infinite ● Days 1 Hours 00 Minutes 00 (Default: 1 Day)

Default Router IP Address (Option 3): ● Auto ○ Disable ○ User Defined

Domain Name Server IP Address (Option 6): 192.168.0.1

Domain Name (Option 15): (0/32 characters used)

NetBIOS WINS Server IP Address (Option 44):

1) Open **IP Configuration > IPv4 Management and Interface, DHCP Server**, **Network Pools**

2) Click **Add…** and make the settings for the first address pool as follows:

Pool Name:	Dante VLAN 1 Pool
Subnet IP Address:	192.168.1.0
Mask:	○ Network Mask
	⦿ Prefix Length: 24
Address Pool Start:	192.168.1.101
Address Pool End:	192.168.1.254
Domain Name Server IP Address (Option 6):	192.168.0.1

Leave the rest of the settings alone

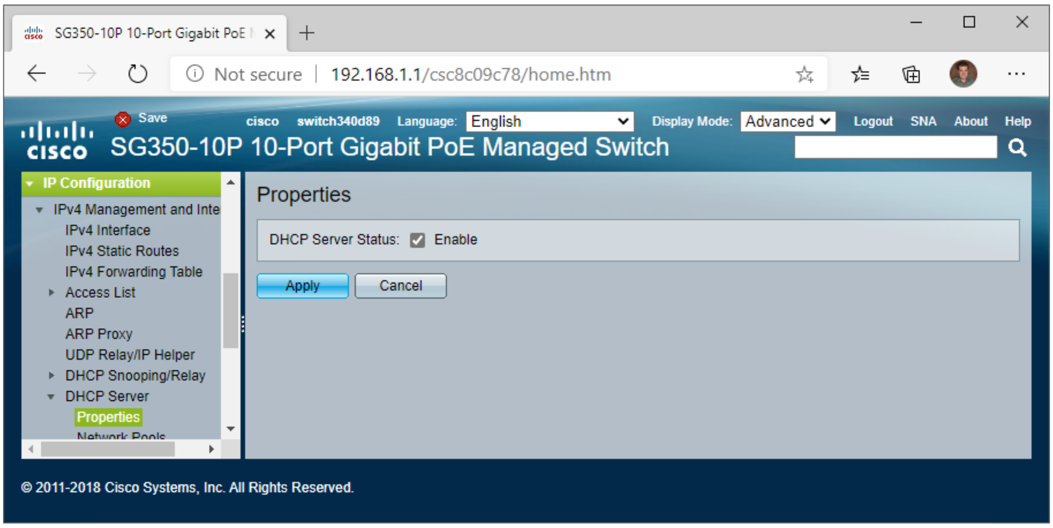
3) Click Apply.

4) Make the settings for the next address pool as follows:

Pool Name:	Dante VLAN 2 Pool
Subnet IP Address:	192.168.2.0
Mask:	○ Network Mask
	⦿ Prefix Length: 24
Address Pool Start:	192.168.2.101
Address Pool End:	192.168.2.254
Domain Name Server IP Address (Option 6):	192.168.0.1

Leave the rest of the settings alone

5) Click **Apply**.



Properties

DHCP Server Status: ☑ Enable

6) Open **IP Configuration** > **IPv4 Management and Interface > DHCP Server** > **Properties**

   a. Check DHCP Server Status: ☑ Enable

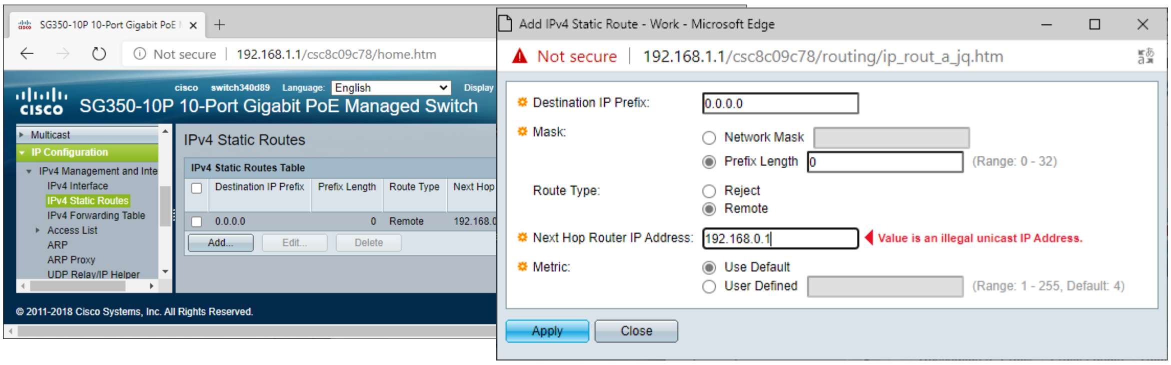
   b. Click **Apply.**

At this point, your computer controlling this should be able to receive an address by DHCP from the switch. Go into the network configuration and set it to DHCP.

Reminder:
Now is a good time to save.

5.5. Create a Static Route from the Switch to the Edge Router

The prior sections set up the SG350 for Inter-VLAN routing. In order to link the SG350 to another router, we need to give the switch instructions on how to find this. In this example, we will set up a static route for the switch's internal router.



Add IPv4 Static Route - Work - Microsoft Edge

Not secure | 192.168.1.1/csc8c09c78/routing/ip_rout_a_jq.htm

Destination IP Prefix: 0.0.0.0

Mask: ○ Network Mask ● Prefix Length 0 (Range: 0 - 32)

Route Type: ○ Reject ● Remote

Next Hop Router IP Address: 192.168.0.1 Value is an illegal unicast IP Address.

Metric: ● Use Default ○ User Defined (Range: 1 - 255, Default: 4)

Apply Close

IPv4 Static Routes Table

☐	Destination IP Prefix	Prefix Length	Route Type	Next Hop
☐	0.0.0.0	0	Remote	192.168.0

SG350-10P 10-Port Gigabit PoE
Not secure | 192.168.1.1/csc8c09c78/home.htm
cisco switch340d89 Language: English Display
SG350-10P 10-Port Gigabit PoE Managed Switch
Multicast
IP Configuration
IPv4 Management and Inte
IPv4 Interface
IPv4 Static Routes
IPv4 Forwarding Table
Access List
ARP
ARP Proxy
UDP Relay/IP Helper
IPv4 Static Routes
Add...
Edit...
Delete
© 2011-2018 Cisco Systems, Inc. All Rights Reserved.

1) Open the **IP Configuration** menu, **IPv4 Management and Interface**, and select **IPv4 Static Routes.**

   a. Click **Add…**

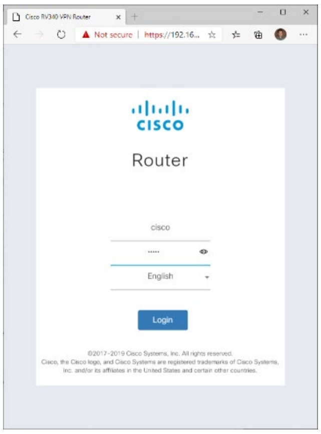
   b. Destination IP Prefix: 0.0.0.0 *All IP addresses…*

   c. Mask: Network Mask: 0.0.0.0 *… that are not local…*

   d. Next Hop Router IP Address: 192.168.0.1 *… should go to this router IP (on another device).*

   e. Click **Apply**.

5.6. Prepping the Edge Router (RV340) for this Exercise



For our example, this will take the RV340 Cisco switch and do the minimal set-up to make this work. Here, we will put it in the right subnet, then make the static route to the "next hop" at our SG350 switch.

1) Connect directly to a LAN port on the router.

2) Log in to the router.

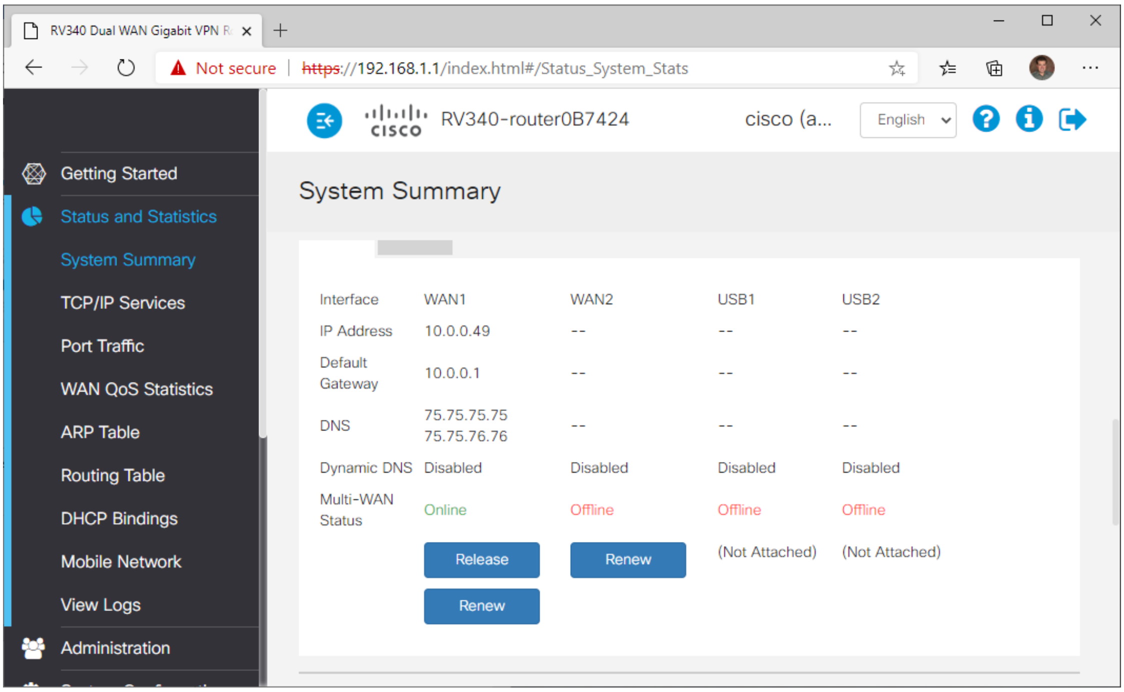
   a. Default is 192.168.1.1)

   b. Default username/password is cisco/cisco again.

3) Update the Admin password.

   The router will allow you to require a minimum password strength. If you want to keep it simple for the exercise, uncheck enforcement and set it to cisco/cisco again.

   Once the password is entered, you'll have to log back in again.



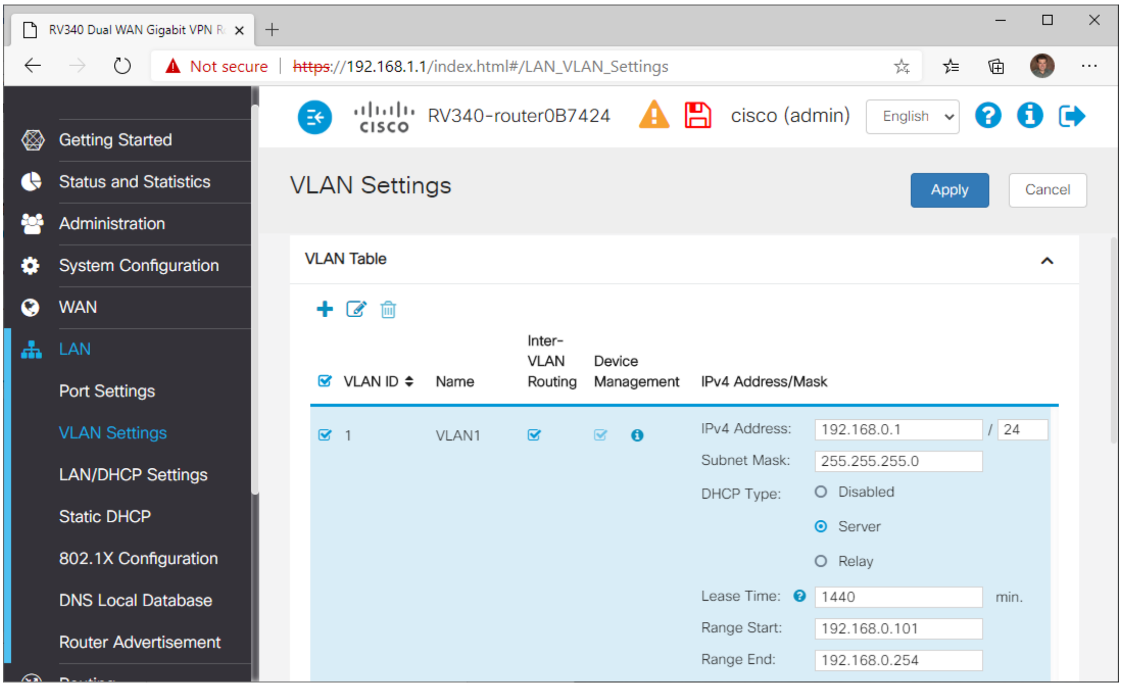
System Summary

Interface	WAN1	WAN2	USB1	USB2
IP Address	10.0.0.49	--	--	--
Default Gateway	10.0.0.1	--	--	--
DNS	75.75.75.75 75.75.76.76	--	--	--
Dynamic DNS	Disabled	Disabled	Disabled	Disabled
Multi-WAN Status	Online	Offline	Offline	Offline
	Release Renew	Renew	(Not Attached)	(Not Attached)

4) Use the initial set-up wizard to get some basic settings for the WAN port in.

   Hopefully, your ISP is not putting your WAN port in a subnet you used on the LAN (192.168.0-2.x). Routers should not see the same subnet on two different legs. If there is a conflict of subnets, you will need to change any duplicates, so each section has a unique address.

   *In our example, if we scroll down the page at **Status and Statistics** > **System Summary**, our WAN port received an address of 10.0.0.49 /24, which does not conflict.*



VLAN Settings

VLAN Table

☑ VLAN ID	Name	Inter-VLAN Routing	Device Management	IPv4 Address/Mask
☑ 1	VLAN1	☑	☑	IPv4 Address: 192.168.0.1 / 24 Subnet Mask: 255.255.255.0 DHCP Type: ○ Disabled ● Server ○ Relay Lease Time: 1440 min. Range Start: 192.168.0.101 Range End: 192.168.0.254

5) Change the router to operate in the 192.168.0.0/24 subnet. *Default is 192.168.1.0 /24.*

   a. Go to **LAN** > **VLAN Settings**.

   b. Check the box for VLAN 1 and click on ✎ icon to edit.

   c. Change the IPv4 Address to 192.168.0.1. This will be the router address.

   d. Set the **DHCP Range** as desired. In the example, it is set to **.101** to **.254.**

   e. Click **Apply**.

6) Assuming the subnet was changed, log back into the router at 192.168.0.1.

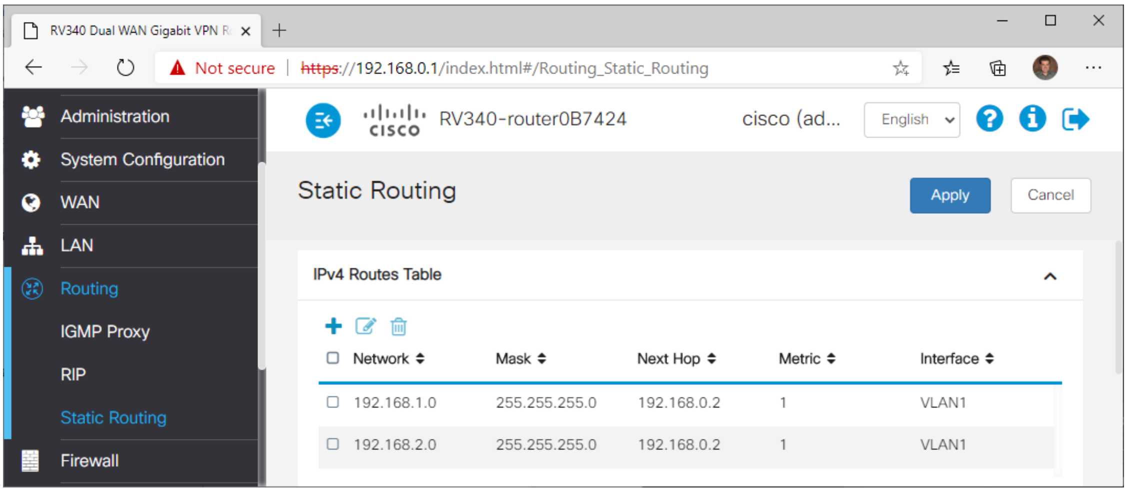
   Remember that your computer may need to reset IP address to be in the same subnet, as well.

7) Press the 💾 icon to save your router configuration.

   a. The page will likely default to copy the Running Config to the Start-up Config.

   b. Click **Apply**.

5.7. Create the Static Route from the Router to the Switch



□ Network	Mask	Next Hop	Metric	Interface
□ 192.168.1.0	255.255.255.0	192.168.0.2	1	VLAN1
□ 192.168.2.0	255.255.255.0	192.168.0.2	1	VLAN1

8) Make static routes for the subnets that are managed in the SG350.

   a. Go to **Routing** > **Static Route**.

   b. Under IPv4 Routes Table, click on ✚ icon to add a route.

      i. Set **Network** as **192.168.1.0.**

      ii. Leave **Mask** as **255.255.255.0.**

      iii. Set **Next Hop** as **192.168.0.2.** *This is the path to the router in the SG350.*

      iv. Set the **Interface** to **VLAN1**.

   c. Repeat - click on ✚ icon to add another route.

      i. Set **Network** as **192.168.2.0.**

      ii. Leave **Mask** as **255.255.255.0.**

      iii. Set **Next Hop** as **192.168.0.2.** *This is the path to the router in the SG350.*

      iv. Set the **Interface** to **VLAN1**.

   d. Click **Apply**.

9) Press the 💾 icon to save your router configuration.

   a. The page will likely default to copy the Running Config to the Start-up Config.

   b. Click **Apply**.

5.8. Connect the Router and Switch

If your configuration followed ours, connect port 8 of the SG350 switch to any LAN port on the RV340 router. Of course, also make sure a WAN port on the router is connected to the incoming internet service.

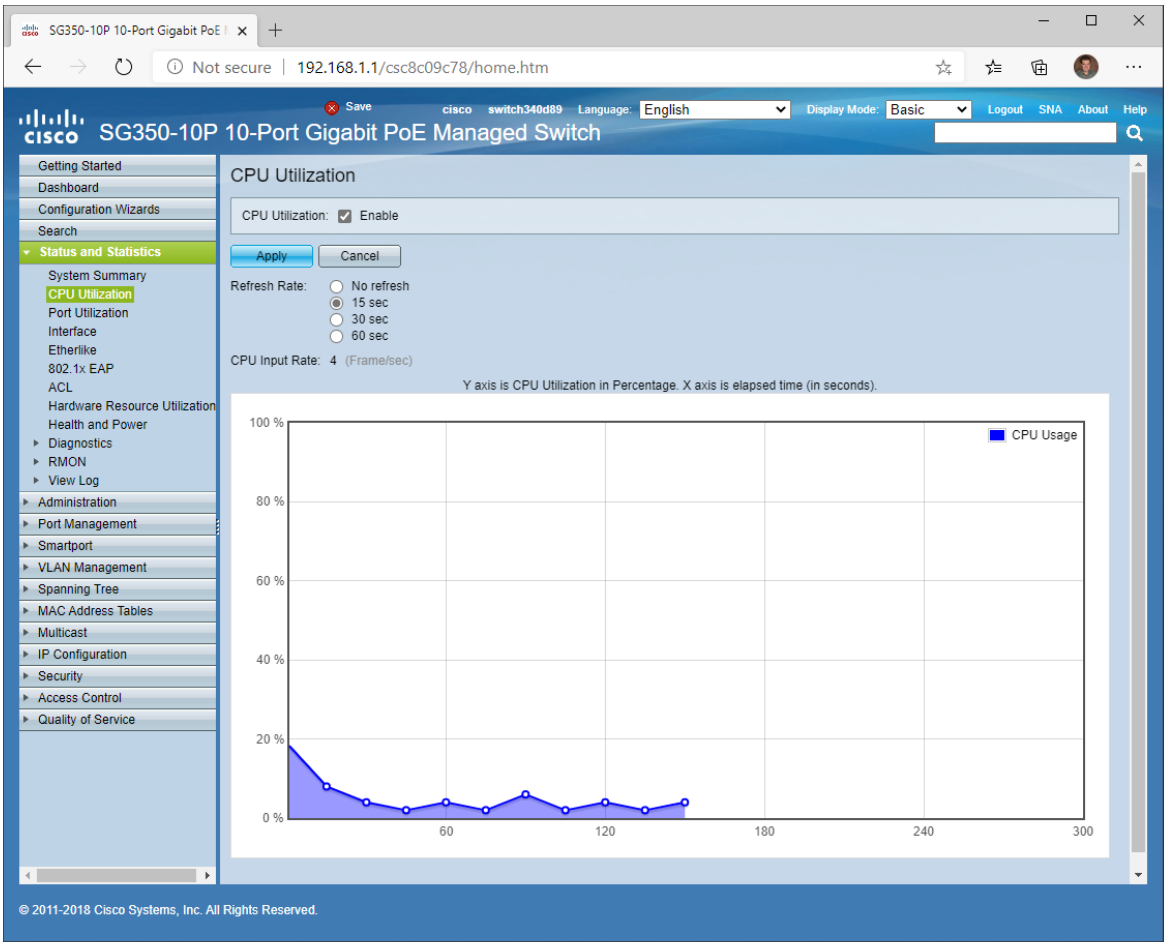
Now, you can plug in to any port on the router or switch, and have routed connectivity on the LAN, and to the internet! Congratulations!

6. Switch Utilities

The SG350-series switch has some utilities built-in that are easy to understand, and useful when commissioning a system. This section will include a few of them.

6.1. CPU Utilization

A CPU Utilization Meter is available on most managed switches. It will help determine how heavily the CPU is taxed to manage your switching traffic – this is useful to determine the impact of features like IGMP Snooping (for managing multicast traffic) can significantly impact the CPU. The demands of Dante audio and video traffic are fairly consistent, and so a test duration of just a few minutes can be quite revealing.



CPU Utilization

CPU Utilization: ☑ Enable

Refresh Rate: ○ No refresh ● 15 sec ○ 30 sec ○ 60 sec

CPU Input Rate: 4 (Frame/sec)

Y axis is CPU Utilization in Percentage. X axis is elapsed time (in seconds).

To view this utility:

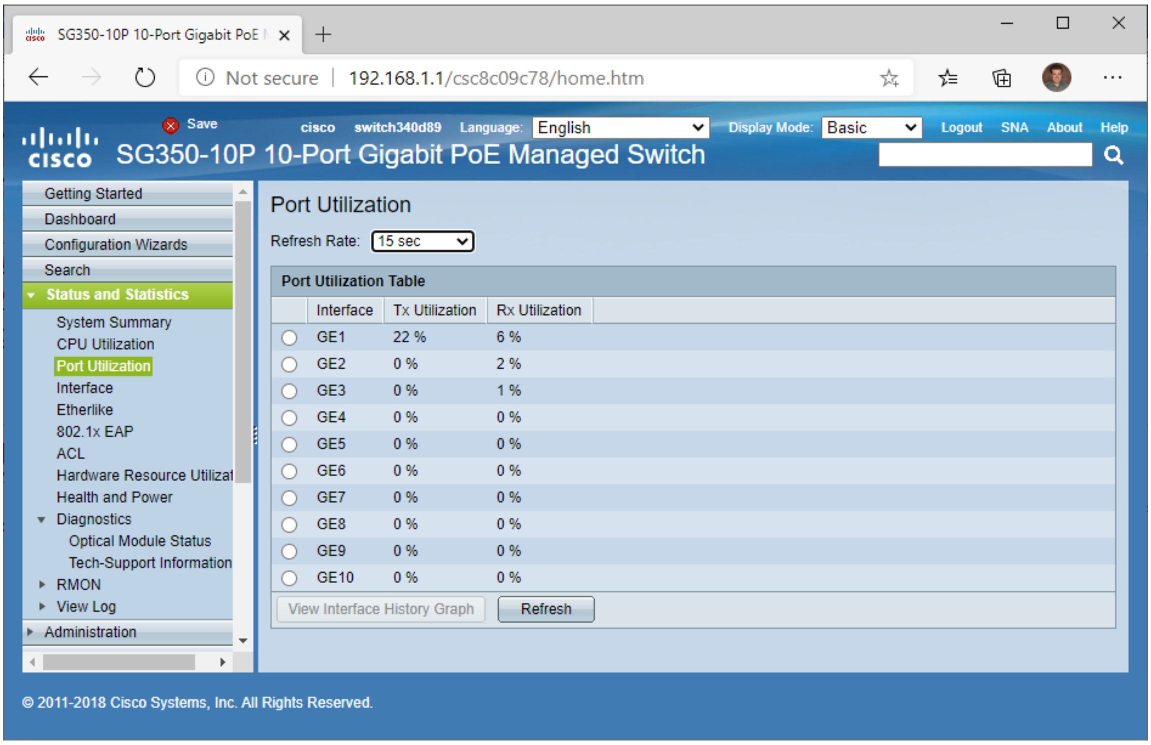
1) Go to **Status and Statistics** > **CPU Utilization**

2) Choose a **Refresh Rate** – perhaps 15 seconds would provide more detailed information quickly.

The switch does not store a history, and the first data point will show up at the end of the first refresh interval. So, if 15 seconds is chosen, no data will appear for 15 seconds, then another datapoint will appear every 15 seconds thereafter.

6.2. Port Utilization

While Dante Controller can show you how much data is flowing in and out of each Dante device, managed switches can typically show you the amount of data on any port – including the more likely bottleneck of trunk lines between switches.



Language: English

Display Mode: Basic

Port Utilization

Refresh Rate: 15 sec

Port Utilization Table

	Interface	Tx Utilization	Rx Utilization
○	GE1	22 %	6 %
○	GE2	0 %	2 %
○	GE3	0 %	1 %
○	GE4	0 %	0 %
○	GE5	0 %	0 %
○	GE6	0 %	0 %
○	GE7	0 %	0 %
○	GE8	0 %	0 %
○	GE9	0 %	0 %
○	GE10	0 %	0 %

To view this utility

1) Go to **Status and Statistics** > **Port Utilization**

2) Choose a **Refresh Rate** if you would like to get updates over time.

If your network is converged with other systems that are not consistent in bandwidth demands, it may be helpful to pull a chart on a particular port to gain an understanding of the changing traffic load.

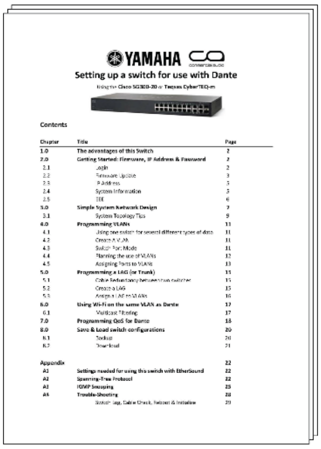
7. Credits and Acknowledgements

Previous Generations of Guides

In 2013, Yamaha and Audinate developed a guide to the Cisco SG300. Many in the audio industry were introduced to managed switches through this document.

The fact that the SG300 used a web browser for configuration (rather than command line) allowed most to adapt to this switch quickly. In installations, Cisco was an acceptable brand for IT professionals – another plus. And so, the SG300 became a popular model, indeed.

Other manufacturers often added instructions for tweaks that their products would need, and they used this as a base model. Even as Dante Certification Training came in to play, many students appreciated these guides as a chance to get hands on experience and gain an immersive perspective on networking.



YAMAHA

Setting up a switch for use with Dante

Using the Cisco SG300-20 or Teqsas CyberTEQ-m

Contents

Chapter	Title	Page
1.0	**The advantages of this Switch**	2
2.0	**Getting Started: Firmware, IP Address & Password**	2
2.1	Login	2
2.2	Firmware Update	3
2.3	IP Address	3
2.4	System Information	3
2.5	EEE	6
3.0	**Simple System Network Design**	7
3.1	System Topology Tips	9
4.0	**Programming VLANs**	11
4.1	Using one switch for several different types of data	11
4.2	Create A VLAN	11
4.3	Switch Port Mode	11
4.4	Planning the use of VLANs	12
4.5	Assigning Ports to VLANs	13
5.0	**Programming a LAG (or Trunk)**	15
5.1	Cable Redundancy between two switches	15
5.2	Create a LAG	15
5.3	Assign a LAG to VLANs	16
6.0	**Using Wi-Fi on the same VLAN as Dante**	17
6.1	Multicast Filtering	17
7.0	**Programming QoS for Dante**	18
8.0	**Save & Load switch configurations**	20
8.1	Backup	20
8.2	Download	21
Appendix		22
A1	**Settings needed for using this switch with EtherSound**	22
A2	**Spanning-Tree Protocol**	22
A3	**IGMP Snooping**	25
A4	**Trouble-Shooting**	28
	Switch Log, Cable Check, Reboot & Initialize	29

We would like to recognize the contributions of many guides that came before this one. While we wrote this version from scratch (and for the successor model SG350), many of us writing this guide learned from and took inspiration from the preceding guides. Thank you to all who made them (and this one) possible.

Chris Ware - Kieran Walsh - Andy Cooper - Steve Seable - Patrick Killianey - Kathryn Taub - Augusto Marcondes

Images

The floppy disk icon is royalty free image, from the following archive:

http://icons.iconarchive.com/icons/oxygen-icons.org/oxygen/256/Actions-document-save-icon.png

8. To Do for Final Version

Verify formatting instruction steps consistent for indents, phrasing, periods at end, etc. – **DONE by Gus on 24th August**

Credits and Acknowledgements approved by those mentioned.

Screen shots of Dante Controller before/after IGMP Snooping implementation.

Screen shots of Layer 3 Routing – showing what it looks like to have domains across subnets.