Managed Switch Tutorial

CISCO CBS350-8FP-2G

Also shown: "Next Hop Router" for Internet Service linking through Cisco RV340 Router

Guide Version: v1.00, September 2022

Firmware Version: 3.2.0.84 (used on CBS350-8FP-2G)

Copyright

Legal Notice and Disclaimer

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
Future Business Centre
Kings Hedges Rd
Cambridge CB4 2HY
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. This a Tutorial, not a "Certified Switch Configuration"

This tutorial is intended to give our industry hands-on experience making these settings in a real switch, using the Cisco CBS350-series. This tutorial assumes the reader has passed at least Dante Certification Level 2. The last sections may require knowledge from Dante Certification Level 3.

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

In reality, many Dante networks require no special switch configuration. Of course, the skills learned in Dante Certification are helpful as your network grows in size, joins an enterprise network or spans multiple properties. The skills have less to do with operating Dante – it is all about having perspective on the network you are joining and knowing how to work with IT professionals.

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.

1.2. What to Look for in a Managed Network Switch

Categories: Unmanaged, SOHO, SMB, Enterprise

There are a few common categories of networking hardware, intended to represent a use case and thus a typical feature set. This usually defines a range of expectations around traffic management, performance, uptime, and price sensitivity.

Unmanaged/Residential – These products are great for plug-and-play networks at home, providing large port capacities at low cost that can be set up by non-technical people. Ports are more likely to be "oversubscribed", meaning the switch could run some ports at full speed but not all ports at full speed simultaneously. Customers in this category are price aware and as such they accept the need to restart their home router or switches.

SOHO (Small Office/Home Office). These are designed for professionals working at home or in a small office, perhaps 10-20 people. Product reliability takes a step up; these customers know the cost of downtime and are willing to spend a bit more on the equipment to prevent problems. Basic traffic controls start to appear, especially those around VPN, VoIP and VLANs for a separate guest Wi-Fi SSID.

SMB (Small and Medium Business). Products move away from table-top designs, favoring rackmount chassis for routers and switches, or ceiling/wall-mount hardware for Wi-Fi access points. Products more commonly are built with "non-blocking architecture", meaning you can use of all ports at maximum speed, simultaneously. A wider array of traffic management features is found on these products, including QoS, IGMP Snooping, ACLs, and Layer 3 operations. SMB products often act as the core for a medium-sized office or on the periphery of an Enterprise core network.

Enterprise – These products are intended for deployment by networking professionals. The web configuration interfaces are usually not found, in favor of a command line interface that can be readily deployed across the whole range of products. These products will push the boundaries of performance and uptime with redundant hardware (especially power supplies) and isolated self-monitoring routines to report any issues and allow for remote-restart capabilities.

In Audinate's training program, we often suggest technicians have a known-good unmanaged switch available for simple troubleshooting. Because unmanaged switches won't block Dante traffic, they can be a good arbiter in determining whether the fault lies in the main network or if it is in the Dante device configuration.

Unmanaged switches may also be useful in simple, low-cost conference room designs. In more mission critical networks, it is commonly accepted that SMB switches are an affordable starting point.

Physical Characteristics

Rack Mountable – In the AV market, switches often go in a rack. It is helpful to avoid rack shelves.

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. While these can protect against the failure of an internal power supply, it is also wise to connect these separate inputs from different breakers or to include at least one UPS.

PoE Budget – There are several PoE specifications, each subsequent version added more power to the end device. Most switches cannot provide that total voltage on every port simultaneously; the PoE budget describes the total voltage available to all ports at the same time.

Year Ratified	PoE Standard	Descriptor	Informal Name	Port-Supplied Power
2003	**802.3af**	**Type 1**	**PoE**	**15W**
2009	**802.3at**	**Type 2**	**PoE+**	**30W**
2018	**802.3bt**	**Type 3**	**PoE++**	**60W**
		Type 4		**100W**

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. SFP tends to support up to 1Gbps, SFP+ supports higher rates. SFP slots make the switch more versatile, should fiber-optic links be required at a future date. For centre-of-the-star switches, it is helpful to have all-SFP versions of a switch like the Cisco CBS350-8S-E-2G.

Management Connections – The interface for a managed switch can typically be accessed through the network. However, if a problem arises and there are no free ports on the unit, a technician may wish to plug directly into the switch. If all network ports are occupied, the technician would have to remove something.

To avoid this, managed switches typically offered a "console port" using a serial (RS232) connection. As serial ports became rare, USB began to appear. And today, we start to see Out of Band (OOB) ports.

And OOB port is a standard Ethernet port link that is not part of the switching network. (It is outside of the normal network traffic bandwidth). The OOB port only provides a link to the management interface. Often, it will not have a DHCP server, instead expecting a Link Local 169.254.0.0 /16 address.

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. These are more commonly found on SMB switches and below.

EEE Disable – 802.3az, otherwise known as Energy Efficient Ethernet (EEE) or Green Ethernet, negatively impacts all real-time systems. Today, most switches come with EEE enabled, but it can be disabled on most managed switches. Some SOHO and unmanaged switches will offer the ability to disable this, as well.

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.

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. If you need multiple locations with 10Gbps ports, you may also need to consider a switch with 10Gbps ports throughout to act as the "center-of-the-star" that all switches connect through.

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.

1.3. CBS350-Series Naming Conventions

On the CBS350-series, there are some naming conventions, as best we can discern. We can use the CBS350-8P-E-2G for example, but we will also show other naming indicators. We'll highlight the ones that apply to our example:

- 8 represents the number of device ports. 1Gbps speed is assumed, unless otherwise indicated.

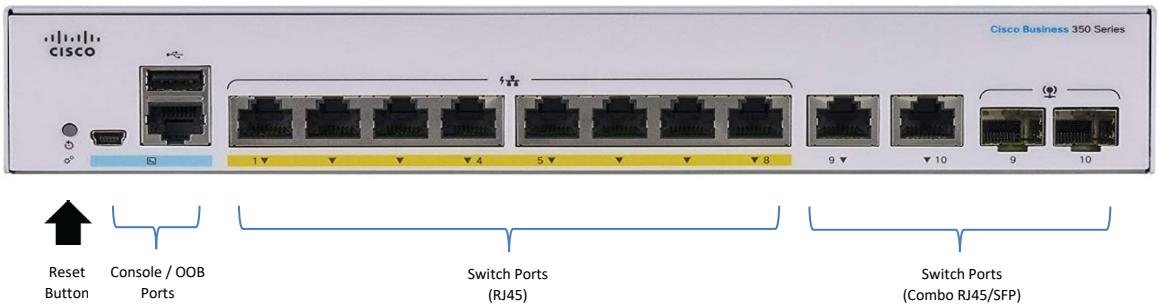
- T means the ports are RJ45 with no PoE functionality.
- M means the ports are RJ45 with multi-gigabit speed, up to 2.5Gbps.
- MG means the ports are RJ45 with a mix of 1Gbps and 2.5Gbps speeds.
- X means the ports are RJ45 with 10Gbps speed.
- S means the ports are SFP slots.
- P means the ports are RJ45 with PoE+ capabilities with a moderate PoE budget.
- FP means the ports are RJ45 with PoE+ capabilities with a larger PoE budget.

- E means the device has an external power supply. This is left out if the device has an internal supply. *At the time this document is published, the 8-port switch is the only one available with an external power supply, and it is also available in an internal supply version for a higher price.*

- 2 means there are two additional ports visualized as a trunk line. These could be combo RJ45/SFP or SFP only.

- G means the additional ports are Gigabit.
- X means the additional ports are higher bandwidth – likely 10 Gigabit.

2. Basic Switch Set-Up



2.1. Initialize the Switch

Before programming any network switch from scratch, it is wise to initialize it just to be sure you are working 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:

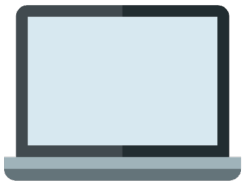
1) Ensure the switch is properly booted and running. (Boot-up may take a few minutes.)

2) 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 switch's visual indicators will behave the same way whether you reboot or initialize the switch, and this can be confusing. If you suspect you lost your grip on the paperclip, wait for the switch to finish rebooting and repeat the initialization process, just to be sure.

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



Set the computer to:

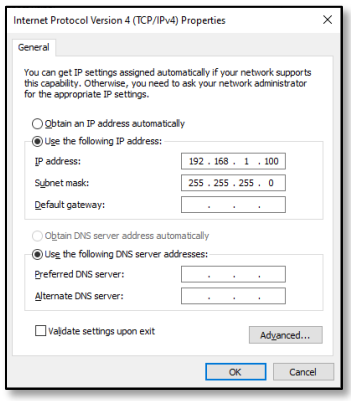
IP Address: 192.168. 1. 100
Subnet Mask: 255.255.255. 0

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

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 CBS350's management interface will follow a DHCP server if one is present, and that may take time to locate. In the absence of a DHCP server, the management interface will default to **192.162.1.254** /24.



1) Connect your computer to a switch port. For this example, port 5.

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

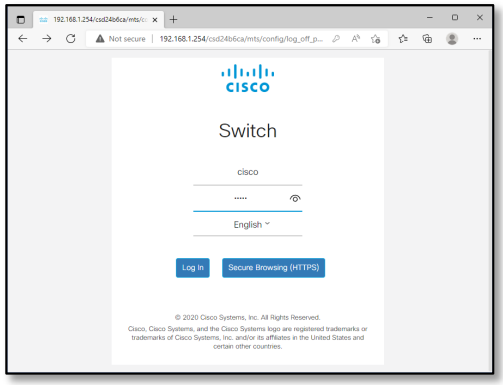
   IP Address: 192.168.1.100
   Subnet Mask: 255.255.255.0

3) Open a web browser and go to:

   http://192.168.1.254/

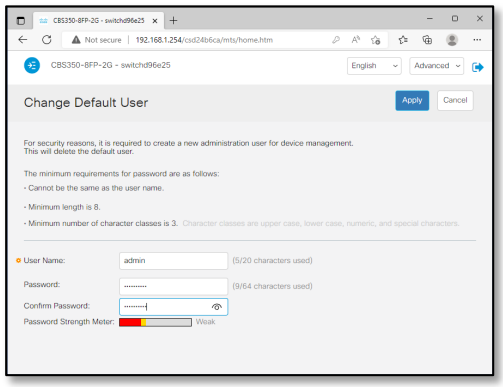
4) The default log-in credentials are:

   Username: cisco
   Password: cisco



Once you log in, the switch will probably ask you to establish new credentials for the admin account.

You will be required to create a new Username and Password.



Helpful Tips:

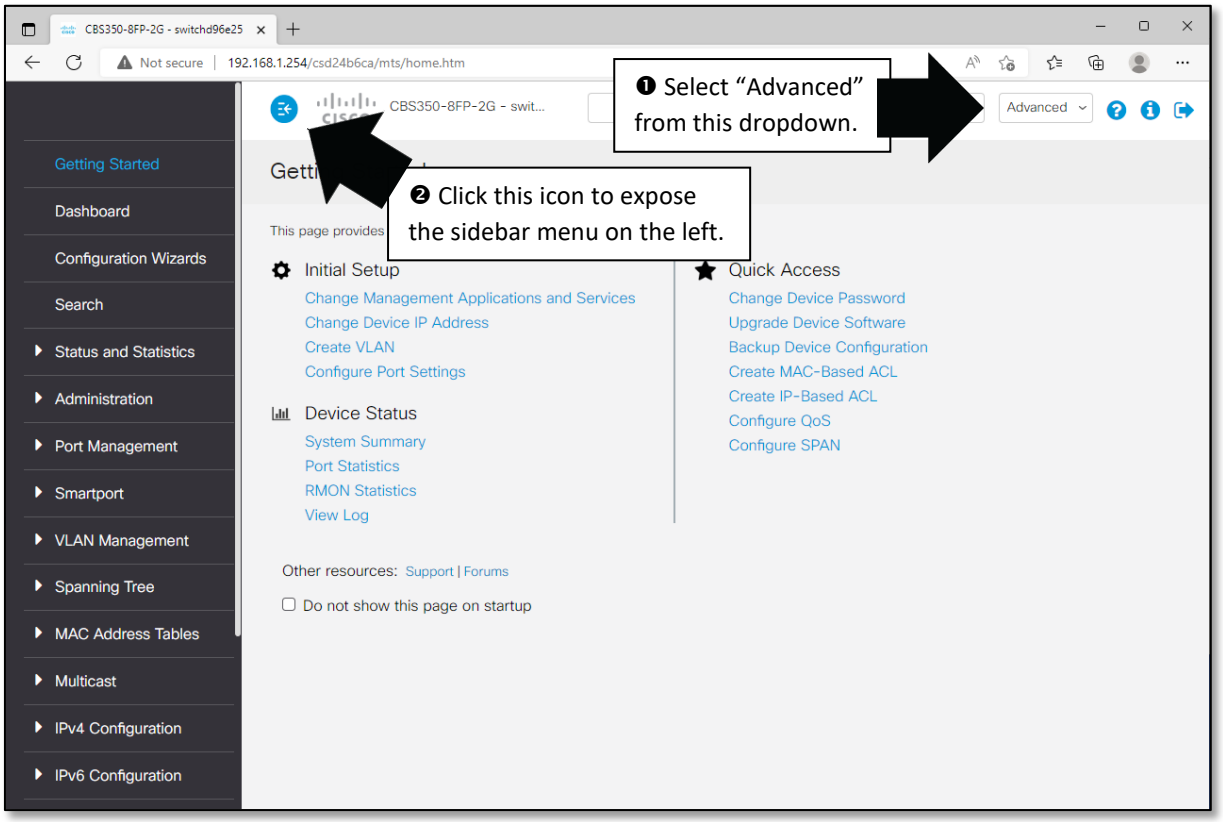
It may take a managed network switch anywhere from one to four minutes to boot up. The management interface will not be accessible until (or may be intermittent) until it finishes booting. Set a stopwatch on your cell phone or computer and make a note of how long it takes to log in to the management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

2.3. Advanced Mode

By default, the CBS350 will begin in Basic mode, and the menu bar will be hidden. Many features this guide require the menus in "Advanced Mode" to see all settings. To make sure they are accessible, let's set your menu to look like ours:

1) In the upper-right corner, select the dropdown menu that says "Basic" and set it to "**Advanced**"

2) Click the blue menu icon in the upper left to expose the left menu bar. We want that menu exposed.



2.4. Symbols

Here are some symbols you will encounter in the menus, and how we will refer to them:

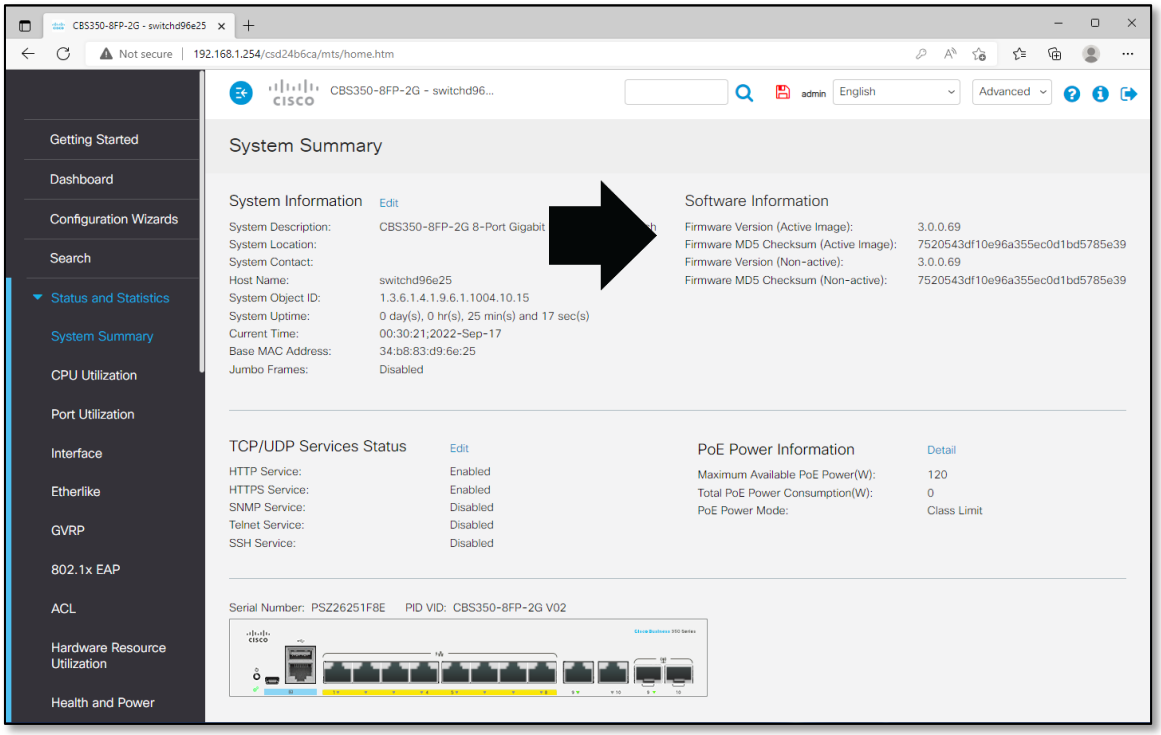
+ Add or New Edit Save

2.5. 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 new bug or require reprogramming, which in turn creates a troubleshooting process. Which wisdom will win out in your situation likely depends on the switch's level of exposure to the outside world.

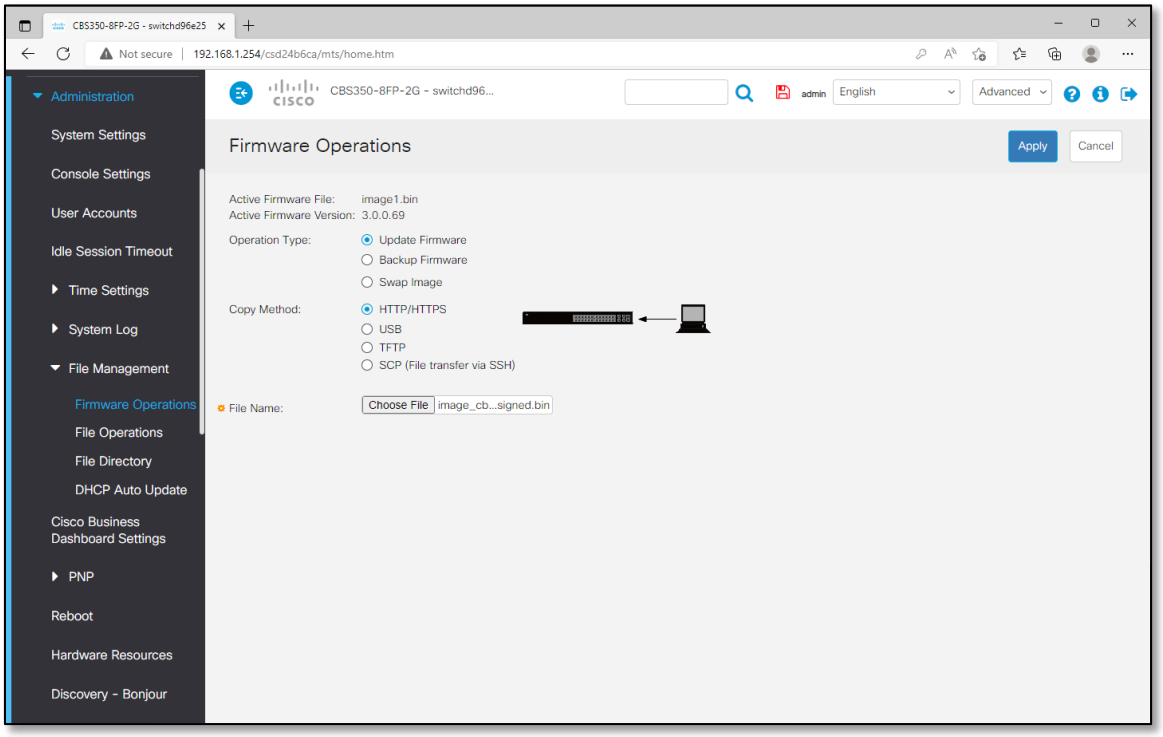
To check the firmware on your switch and update it (if necessary):



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. *If you ask your favorite search engine for "Cisco CBS350 firmware download", it may offer a link to the switch model resource page.*

If a firmware update is desired….



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! Click the blinking icon at the top to save the changes you've made so far.

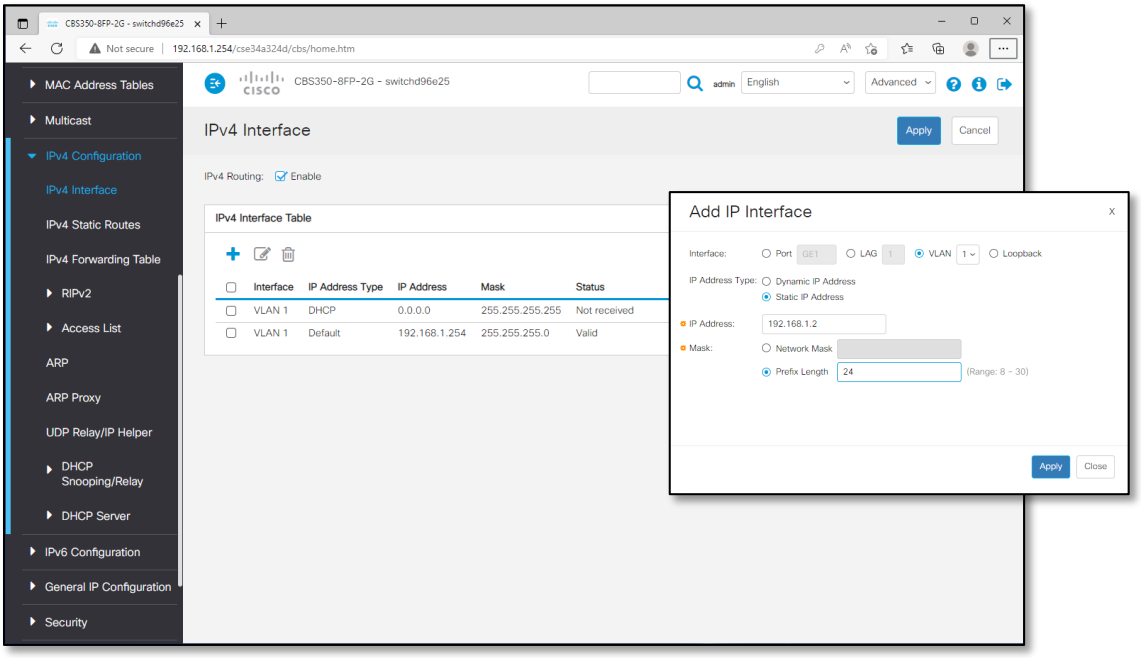
5) Open **Administration** > **Reboot**.

    a. Click **Reboot** in the upper right.

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. In our example, we will assume a single VLAN with a hardware router at 192.168.1.1. We'll set this switch to 192.168.1.2. You can adapt this to your network as desired.

IT departments will often create a special VLAN for management of network devices, keeping those interfaces away from the people on their network. But for this exercise, we'll let the Dante VLAN also have access to the switch configuration screens.



1) Open **IPv4 Configuration** > **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.

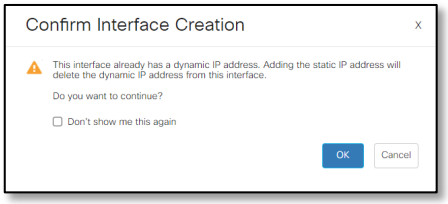
   This firmware doesn't appear to allow editing of the management interface. When we create this new address in the same subnet as the old one, the old one will be automatically removed in Step 5. If you are creating a management interface in a new subnet, you decide to keep ore remove the old one.

3) Set this as a **Static IP Address** at **192.168.1.2**.

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

5) Click **Apply**.

   The switch will pop-up a dialog box saying the prior dynamic address will be removed when this is added. Click **OK** *through that. The switch will now be taking a new management IP address, so we'll need to log-in to the management screen again.*

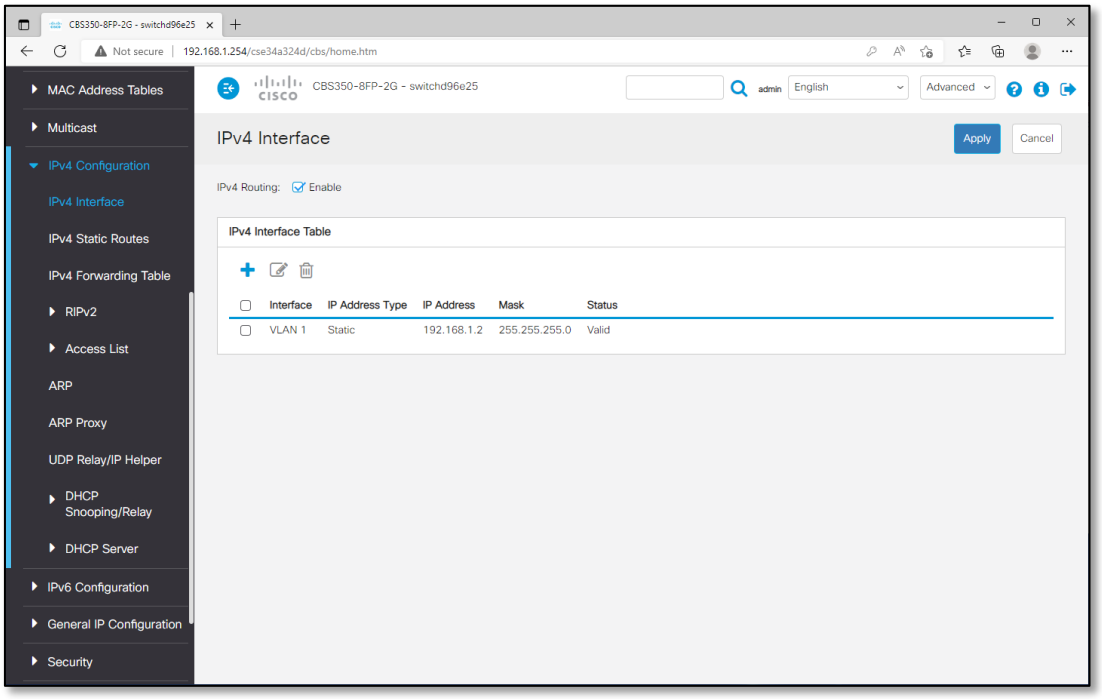


6) Log in to the switch at the new IP address (192.168.1.2) and enter your credentials.

   Remember – if you changed the subnet of the management interface, you now need to change your computer's IP configuration to connect locally.

7) Open **IPv4 Configuration** > **IPv4 Interface**.

   You should now see one management IP address at the designed address.

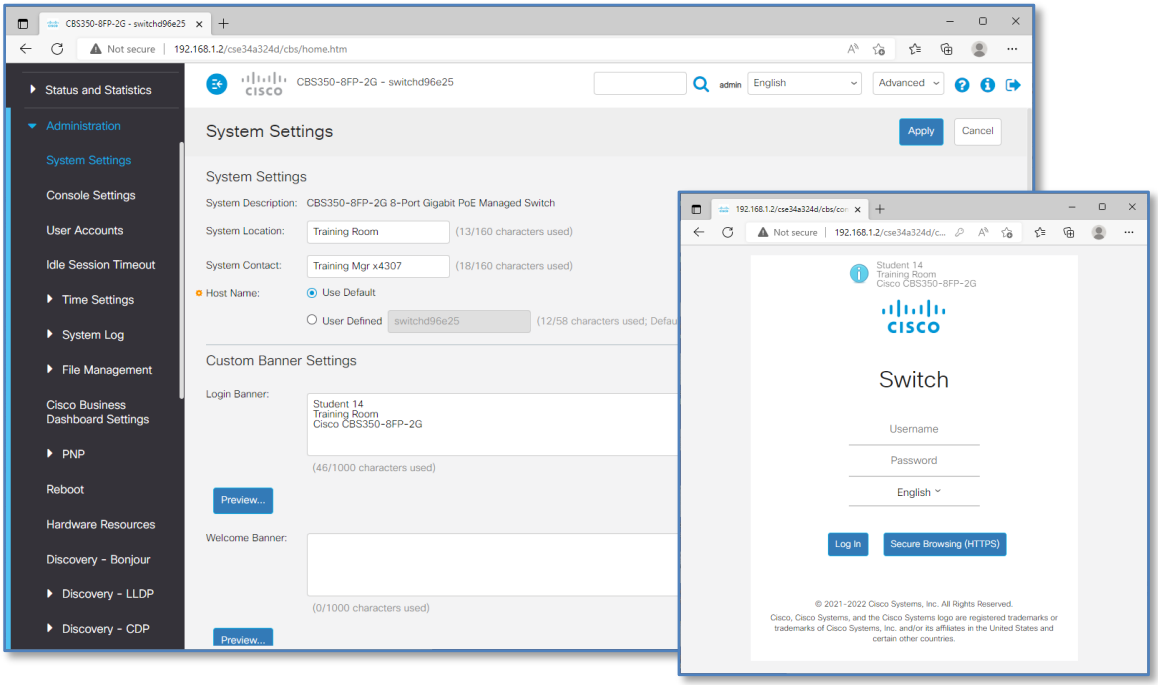


Reminder:
Now is a good time to save.

2.7. Switch Information Fields: 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 and/or back panels to document the management IP address and any notes about the configuration. But when you log in, it is also nice to have the log-in screen confirm which switch you are in and who to contact for changes and support.

The System Location and System Contact field will only be seen in the set-up screens. So if you want to hide this information from prying eyes, this is where to put that information. If you want to identify the switch at the log-in screen, use the Login Banner feature as shown, here:



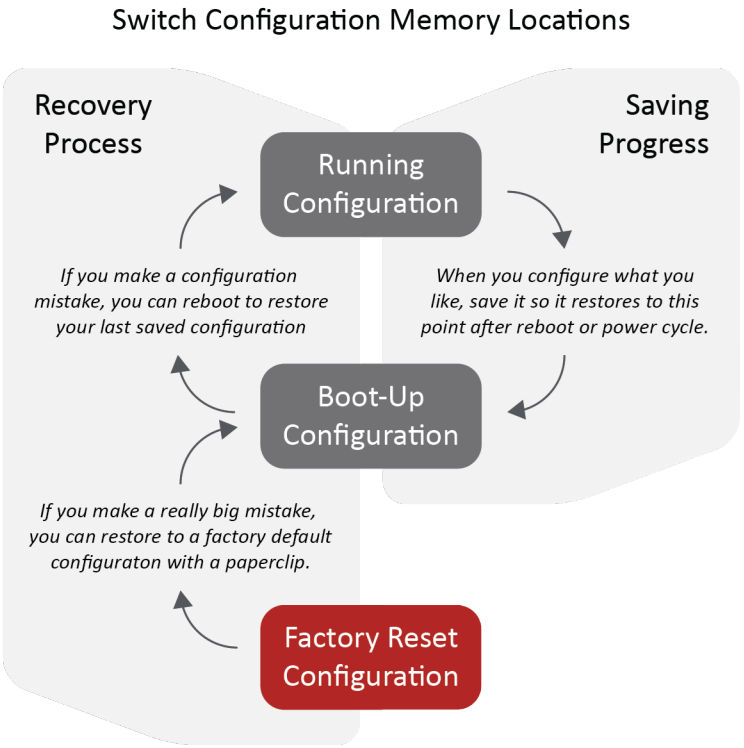
1) Open **Administration** > **System Settings.**
2) Edit the fields as desired and click **Apply** to confirm the new settings.
3) Click **Preview** to see what your Log-In Banner will look like.

Reminder:
Now is a good time to save.

2.8. Stored Configurations: Running, Boot-Up and Factory Reset

Most managed switches have three switch configuration memory locations:

- Running Configuration
- Boot-up Configuration
- Factory Reset Configuration



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 the document is opened, the user sees the last saved version.

Managed switches work the same way. Any management changes made are stored in memory (Running Configuration). 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. Effectively, this is like a restore point.

Of course, most people have used a paperclip to restore the Factory Reset configuration. What you're really doing is loading a configuration from a protected memory location to the Boot-up Configuration. When the switch reboots, that configuration will be loaded in to running configuration.

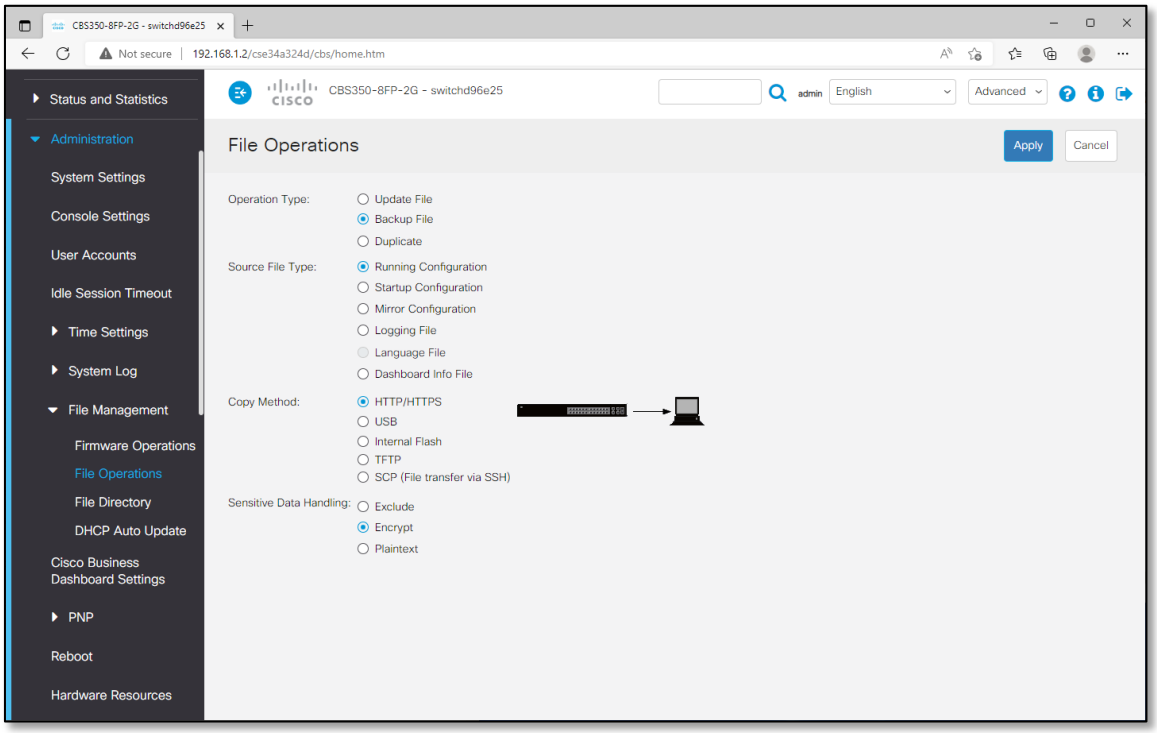
The blinking diskette icon is your indication that changes have been made but not saved. As we know:

- To save the running configuration to boot-up configuration, click the flashing diskette icon.
- To reboot the machine (and go back to your boot-up configuration, go to **Administration** > **Reboot**

2.9. Exporting/Saving Switch Configurations

Managed switches offer the ability to export their configuration to a file. This is commonly used to create a back-up of the configuration. This can also be used to copy configurations from one switch to another, though this will require changes to features that should be unique per switch, such as the management IP address, log-in banner information, and so on. This can be done in a simple text editor.

To export the settings of a switch:



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

2) Under **File Operation**, select **Backup File**.

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

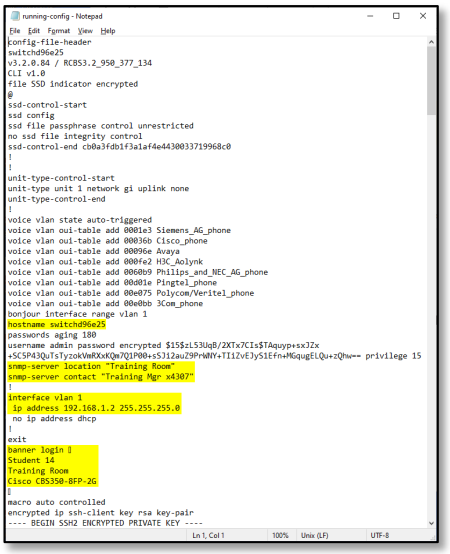
3) Under **Source File Type,** select **Running Configuration.**

4) Under **Copy Method,** select **HTTP/HTTPS.**

5) Under **Sensitive Data Handling**, choose **Encrypt.**

6) Click **Apply**.

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

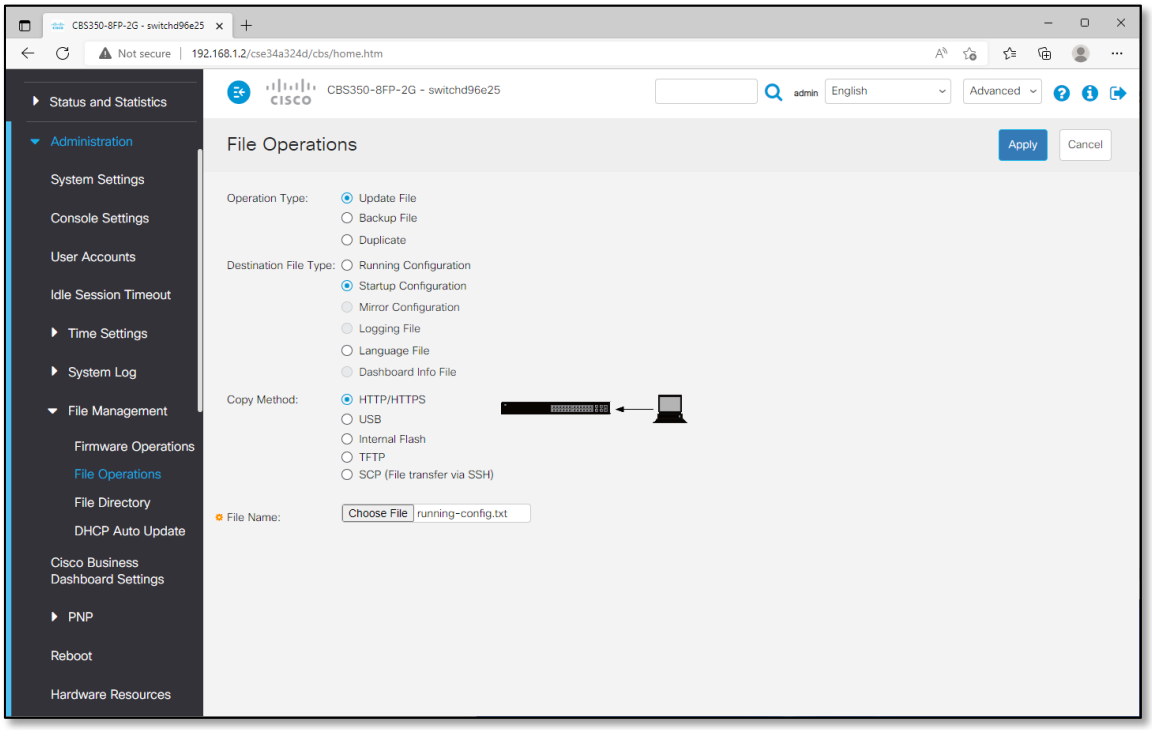


At right, is an example of a configuration file opened in a standard text editor. We've highlighted sections that you may want to customize before loading to another computer. If you do this, be careful not to change the formatting of the file.

2.10. 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, host name, and other information that should likely be unique. If you choose to use this feature to duplicate settings from one switch to the next, be sure to edit those before copying the information in, or keep the switch isolated from the main network until you can make those data fields unique.

To load a configuration from a file on your computer:



1) Open **Administration** > **File Management** > **File Operation.**
2) Under **File Operation**, select **Update File**.

   This instructs the switch to load the configuration (rather than save it). In the picture, notice the arrow from the computer to the switch, indicating the data flow direction.
3) Under **Source File Type,** select **Start-up Configuration**.
4) Under **Copy Method,** select **HTTP/HTTPS**.
5) Click **Choose File** and locate the configuration file on your computer.
6) 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 with the credentials from the configuration file.

Reminder:
Now is a good time to save.

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, Second Edition. To sign up for this free, on-demand training program, go to https://audinate.com/certify.

Switch Example Design (Chapter 3)

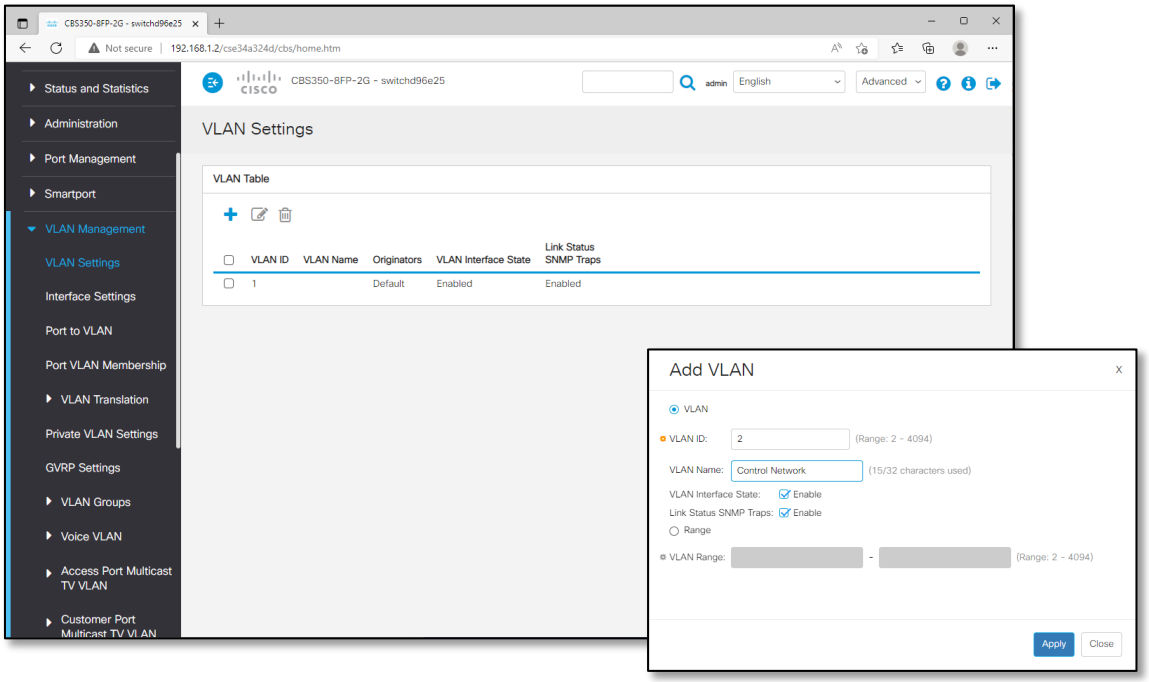
Port:	1	2	3	4	5	6	7	8	9	10
VLAN/Tagged "U" is untagged "T" is tagged	1 - U (Dante)					2 - U (Control)			1 - U (Dante) 2 - T (Control)	
Type	Access								Trunk	
Special									LAG #1	

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 the next switch.

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 is common for IT departments to limit the size of a VLAN to a 24-bit subnet, maybe even smaller.

In Dante Certification Level 2, we discuss how a 24-bit subnet will lead to a local network with 254 available IP addresses. In Dante Certification Level 3, Second Edition, we discuss how this minimizes network chatter from multicast and broadcast messages from various network services.



To create the second VLAN:

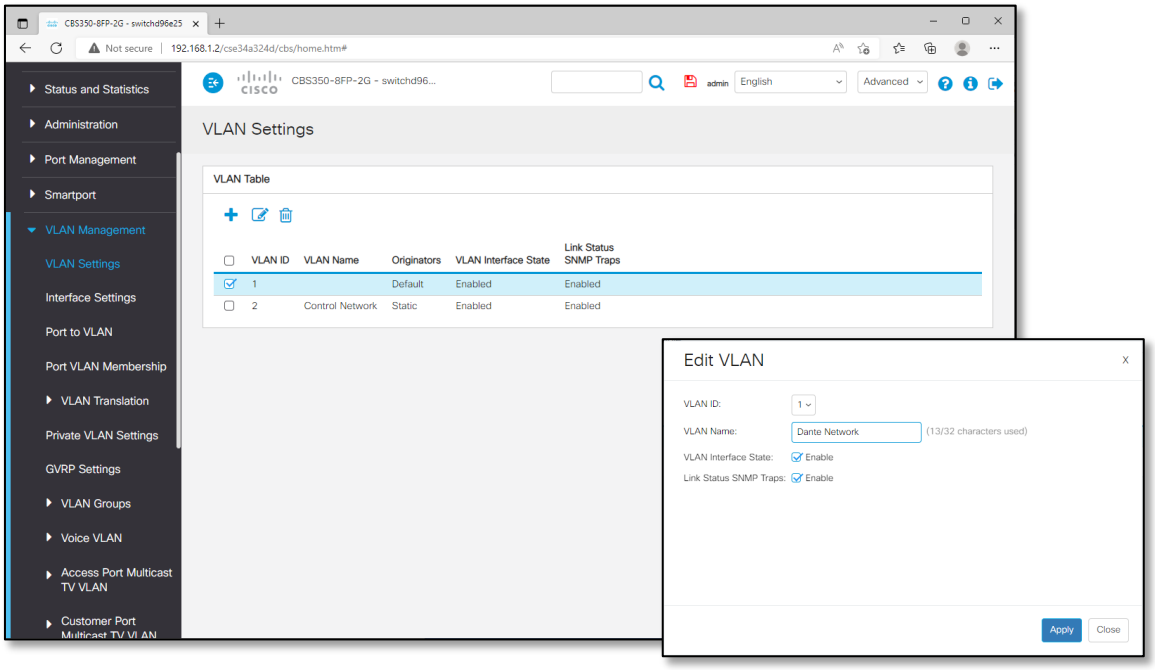
1) Open **VLAN Management > VLAN Settings**

   a. Click the ✚ icon to add a new VLAN.

   b. Enter a **VLAN ID**. In this example, make it VLAN 2.

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

   d. Click **Apply.**

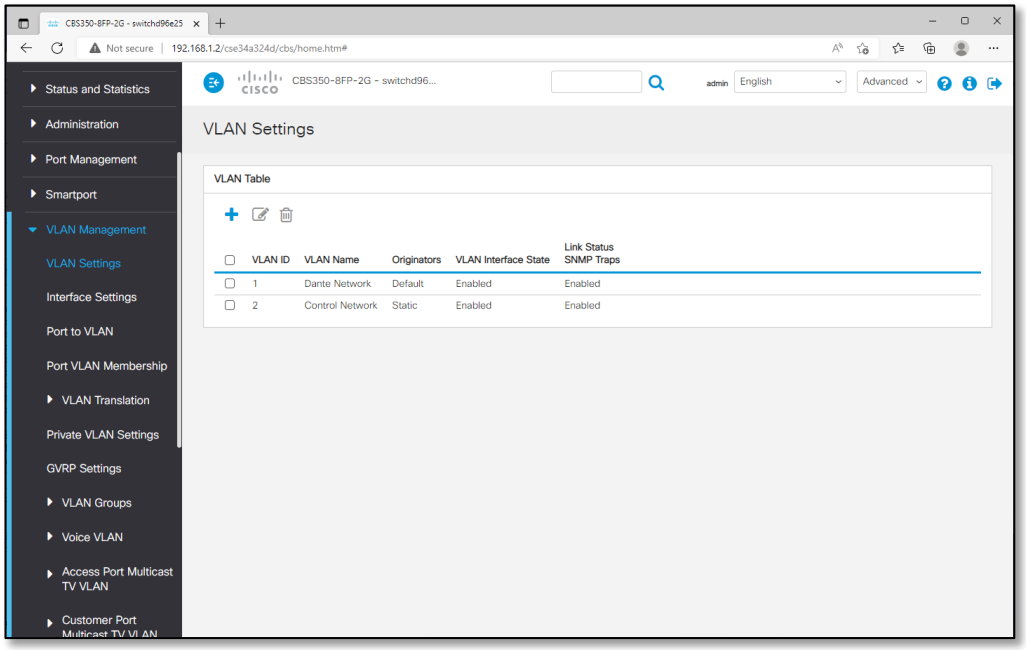


To go back and add a name the first VLAN:

2) Check the box for the first VLAN and click the icon to edit.

   a. Update 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 be assigned to VLAN(s). There are two modes:

Ports 1-8: Access, Untagged – "Access" means the port will have direct access to a single VLAN, with no 802.1Q tags. This is appropriate for network endpoints like Dante devices, computers, printers, etc.

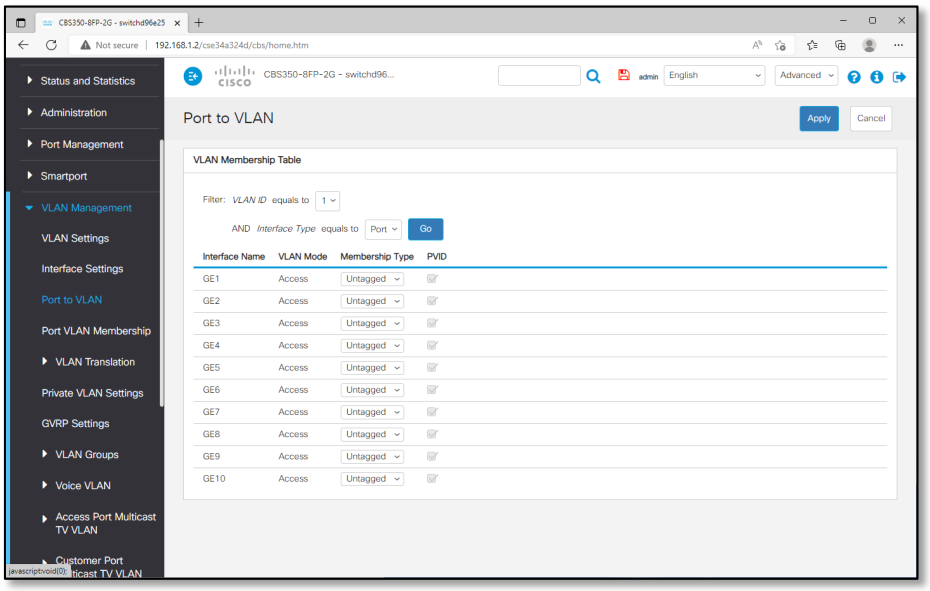
Ports 9-10: Trunk, One VLAN Untagged and all other VLANs Tagged – "Trunk" means the port can transport multiple VLANs. In this situation, one VLAN (usually the maintenance VLAN) can remain untagged, but the rest will need to be tagged.

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.

- **Make sure your computer is plugged in to a port that will remain in the VLAN with the switch management interface.** In this example, this 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 to VLAN 1, as desired. We need to assign ports 6-8 to VLAN 2.



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

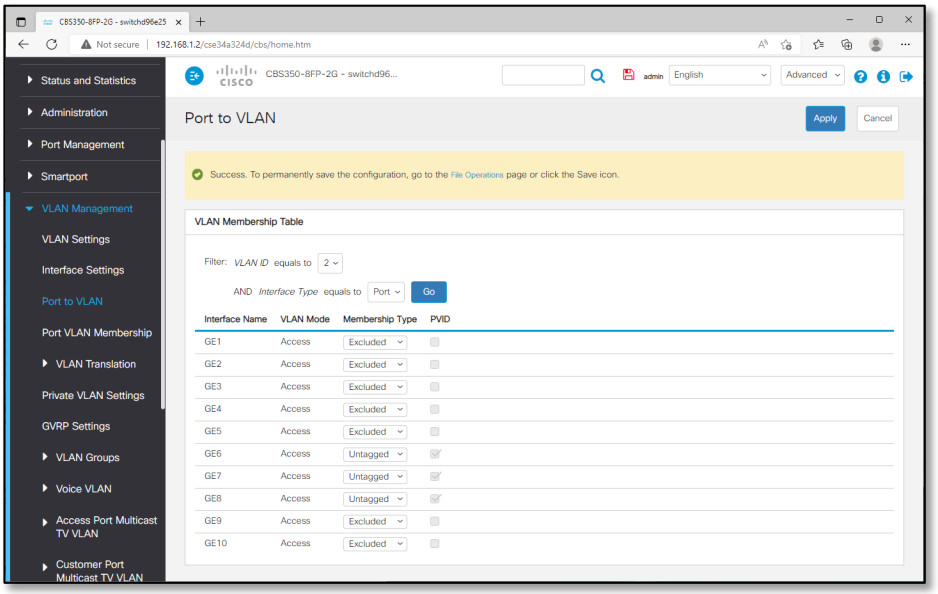
   All ports are showing their membership *for VLAN 1: "Untagged".*

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

      The list below will update. All ports are showing their membership for VLAN 2: "Excluded"

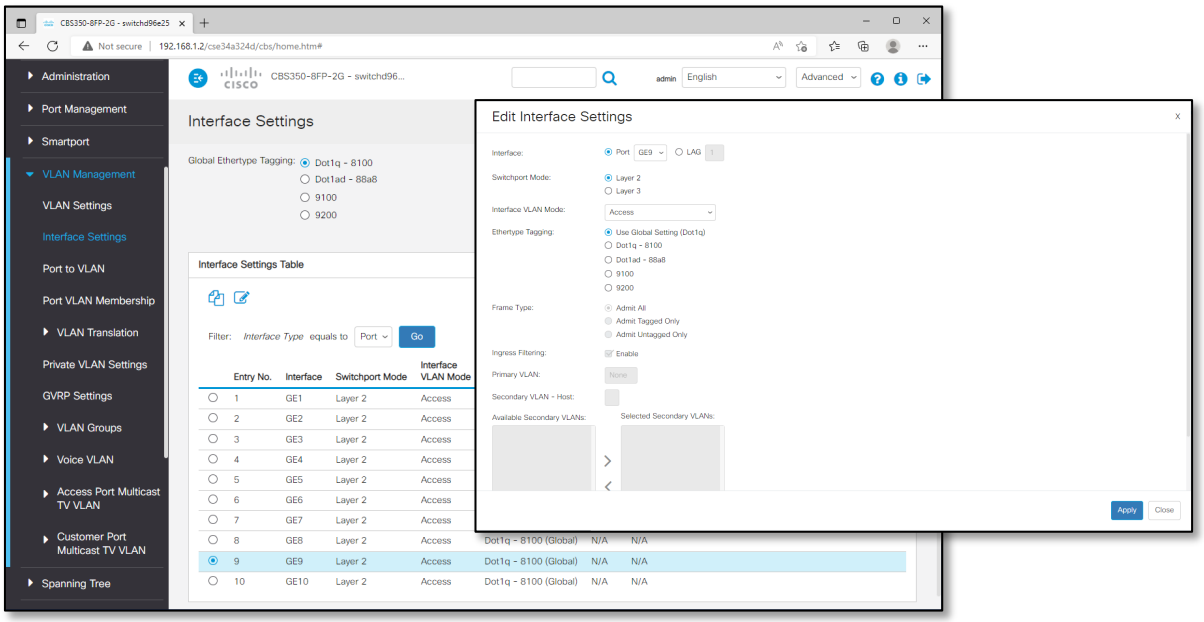
   b. On GE6, GE7 and GE8, set the Membership Type to **Untagged**.

2) Click **Apply**. *When complete, your screen should look like the image below:*

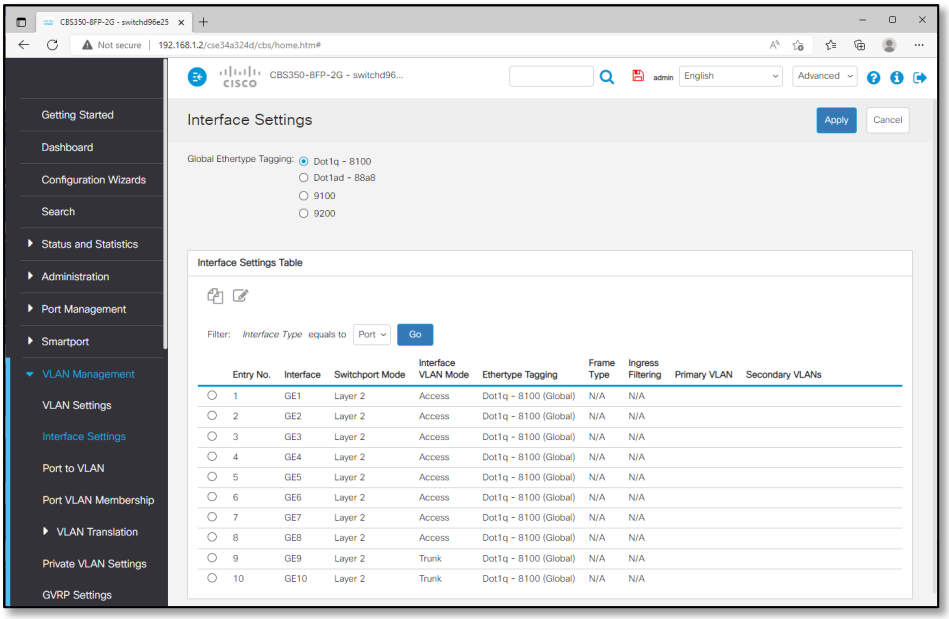


Assigning Ports as Trunk with Multiple VLANs

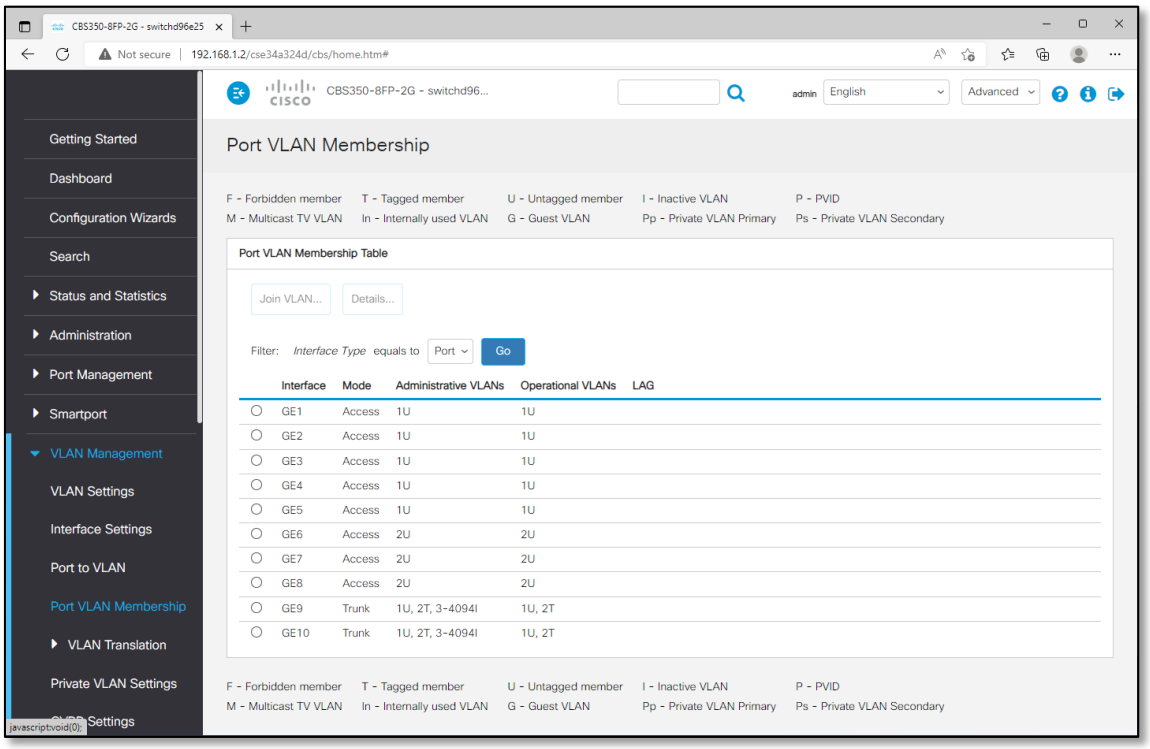
In our example, we want to set ports 9-10 as trunk lines carrying VLANs 1 and 2. To do that:



1) Open **VLAN Management** and open **Interface Settings**.
2) Select the radio button for the first trunk line (port 9) and click the icon to edit.
    a. Select **Interface to VLAN Mode** as **Trunk**.
3) Click **Apply**.
4) Repeat the process for port 10. *When complete, your screen should look like the image below:*



Confirming Trunk Assignments



To confirm all VLAN and Access/Trunk assignments:

1) Open **VLAN Management** > **Port VLAN Memberships**.

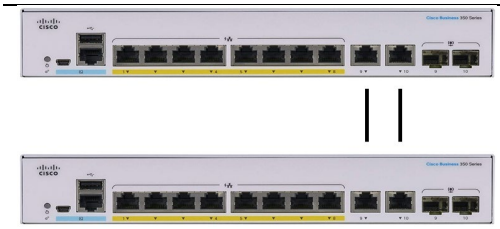
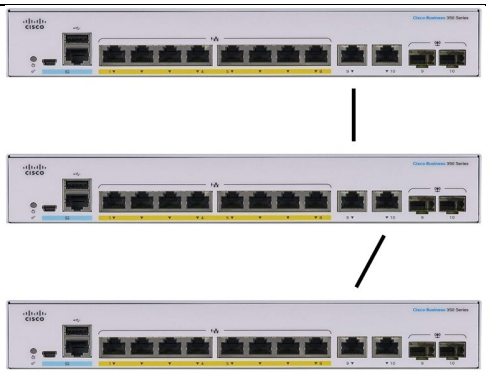
   There is a key at the top and bottom, shows the letter codes for each port assignment. (The key at top and bottom is helpful when the switch has larger port counts.) In this display, we can see:

   - Ports 1-5 are on VLAN 1, untagged.
   - Ports 6-8 are on VLAN 2, untagged.
   - Ports 9-10 are trunk lines carrying VLAN 1 untagged, and VLAN 2 tagged.

   Ignore the third VLAN – that is likely an automatic feature in Cisco. It shows "I" for inactive and should remain that way.

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

A Link Aggregation Group (LAG) bundles multiple connections between switches for more bandwidth without creating a broadcast storm. With this setting made, the switches know this group of ports is to be treated as one logical path.

When to use a LAG	When not to use a LAG
	
In this topology, a LAG can be engaged to use the bandwidth of both links between the two switches. Without a LAG, STP would make one link dormant to prevent a broadcast storm.	In this topology, a LAG should not be engaged. In fact, once you create a LAG, those ports must go to the same switch or bad things will happen. (Yes, that is a sufficiently technical explanation.)

To be clear, if the two trunk ports need to go to different switches, you do not configure them in a link aggregation group. This is only useful if multiple trunk links will connect the same two switches together.

LAGs and Redundancy

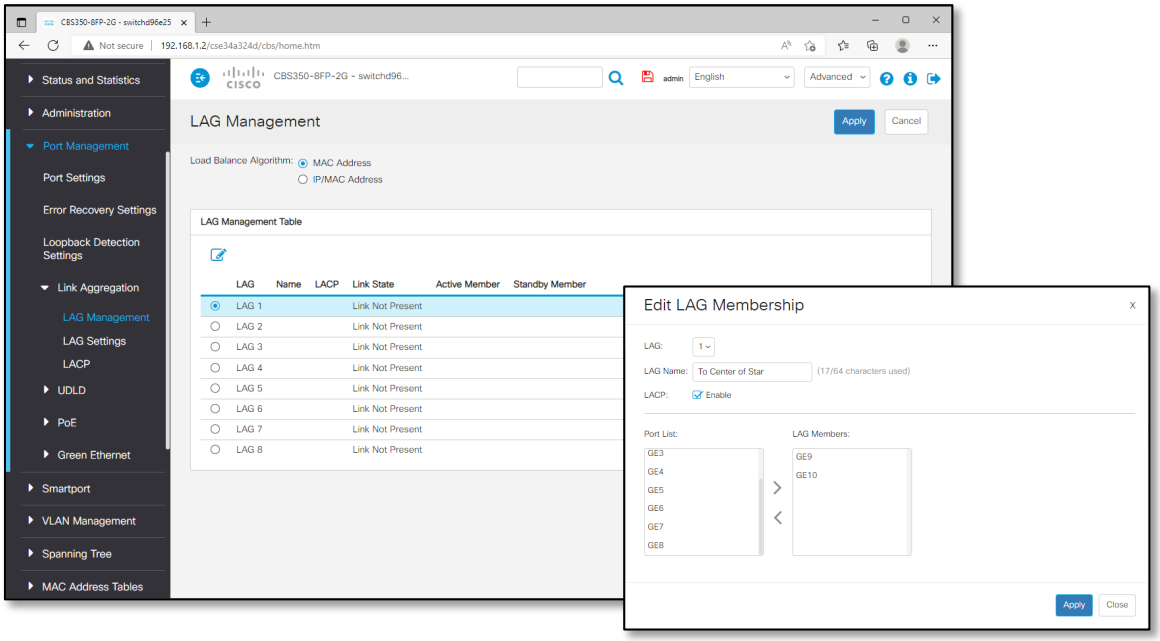
In the IT space, LAGs are also considered a form of redundancy. If a LAG is programmed and only one cable is present, it will use that one link. You can set this up, add and remove the cables and watch the switch adapt to the new cable paths.

In a sense, this is similar to Spanning Tree Protocol (STP). The difference is LAGs will use the bandwidth of all links, STP puts cables in a dormant state, so the same bandwidth is available when a back-up link is used.

It is worth noting that LAGs and STP will not respond seamlessly when a link fails. Older STP protocols could take a minute or more; modern Rapid Spanning Tree Protocol (RSTP) may react more quickly – perhaps 5 seconds. These will not provide seamless failover like Dante's Redundant Networks capability (running a completely separate, duplicate network). In mission critical systems, these differences should be considered in network design.

And of course, it is possible to use STP or LAGs on Dante networks set up redundantly for incredibly high uptime. However, this returns to the discussion of, "How much redundancy do you want or need?" This is a good conversation to have in the design phase of a project.

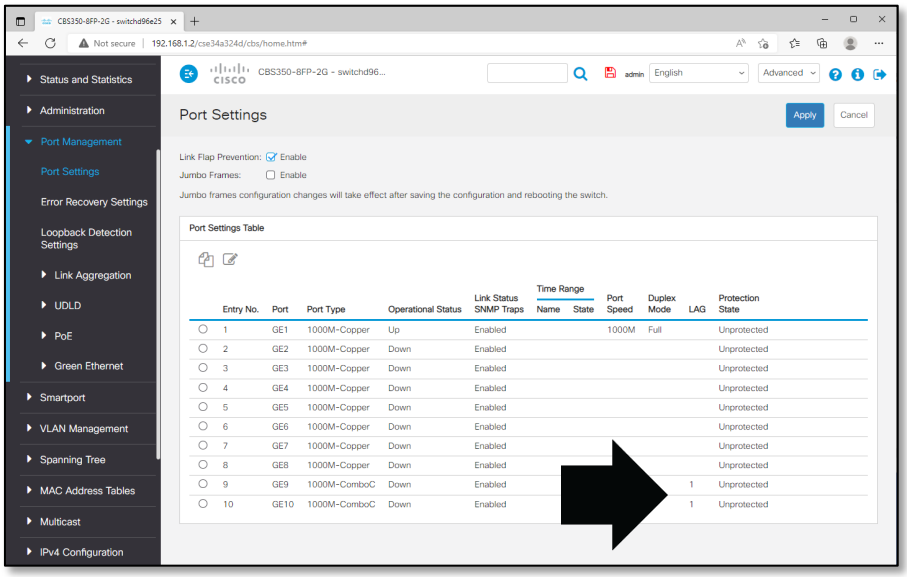
To make a LAG on ports 9-10:



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 the icon to edit.
    b. In the port list, select GE9 and click the right arrow to make it a LAG member.
    c. Repeat for GE10.
2) Click **Apply**.

Verifying LAG Configuration

To confirm assignment to the LAG, go to **Port Management** and select **Port Settings.**



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, Second Edition. To sign up for this free, on-demand training program, go to https://audinate.com/certify.

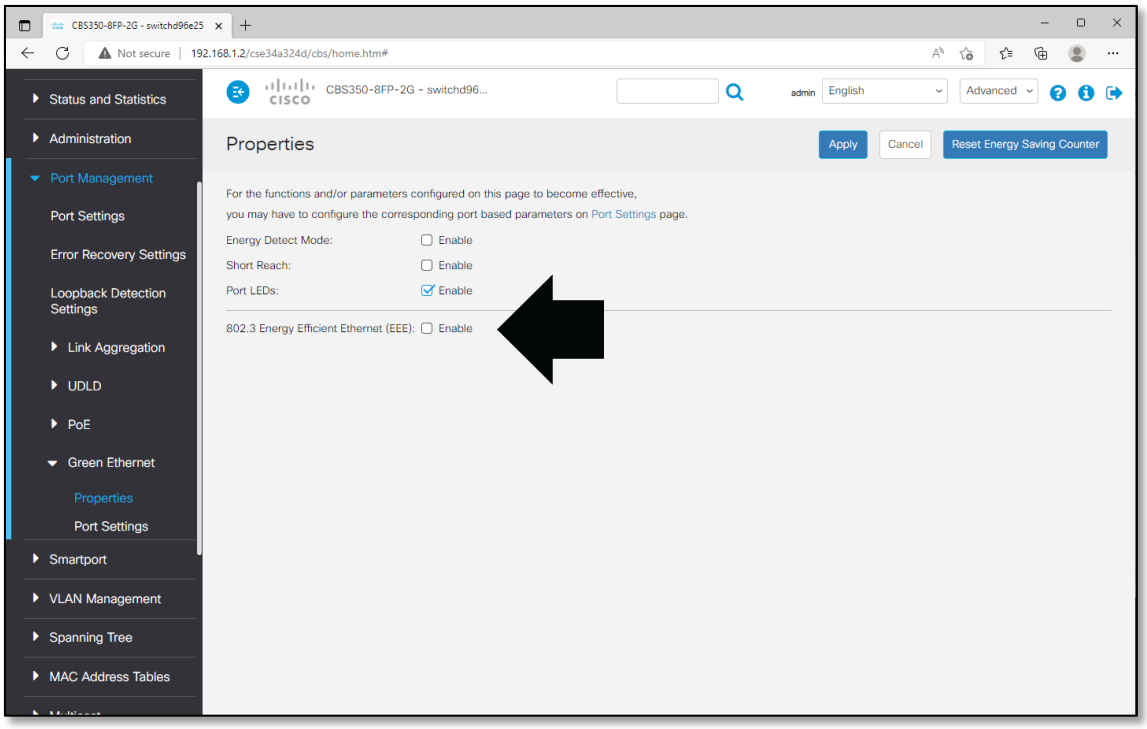
Switch Example Design

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 – such as a MacOS computer running Dante Virtual Soundcard – 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 CBS350-series 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 for real-time systems. Disabling this feature is always recommended for critical live performance systems.



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 Paths reach or exceed 70% of bandwidth capacity)
3) You have Dante devices with 100Mbit interfaces. (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 consider a Link Aggregation Group (LAG) or upgrading to a switch with faster trunk links. More bandwidth is a better cure than QoS.

Note – on the CBS350-series, 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 CBS350-series, 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

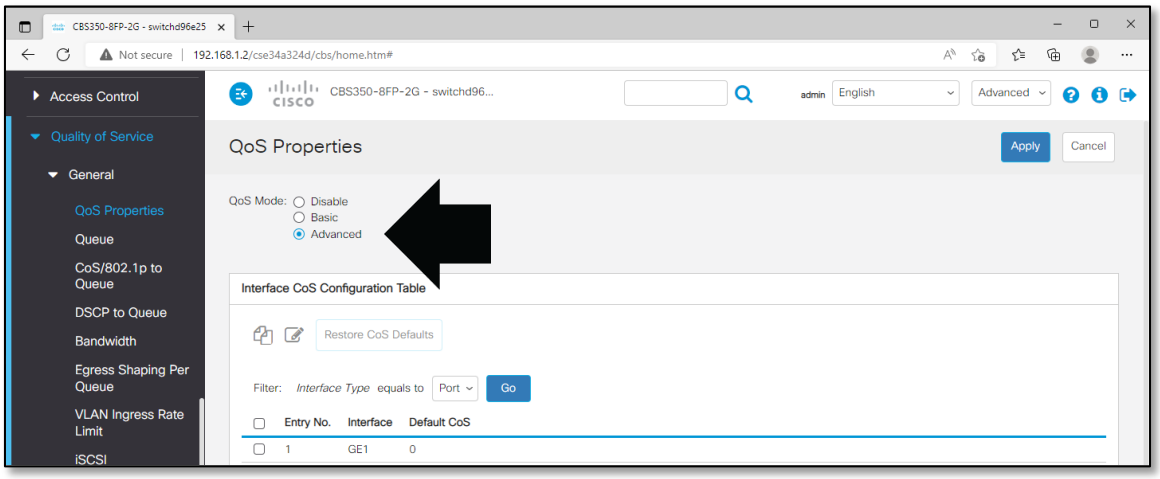
Type	Priority	DSCP Label	Decimal	Hex	Binary
Clocking (PTP)	High	CS7	56	0x38	111000
Dante Audio	Medium	EF	46	0x2E	101110
Control	Low	CS1	8	0x08	001000

DSCP values on the packets will range from 0-63. These numbers do not signify the importance of the data, the CBS350 switch will read these values and place the packets in one of eight QoS priority queues as we decide. *(Other switches may have different numbers of ques - the older Cisco SG300-series had four queues.)*

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. Since the CBS3500-series has 8 QoS Queues, then queue 8 is the highest priority. It is common for beginners to set up QoS completely backwards – so watch out for this!

Setting QoS for Dante

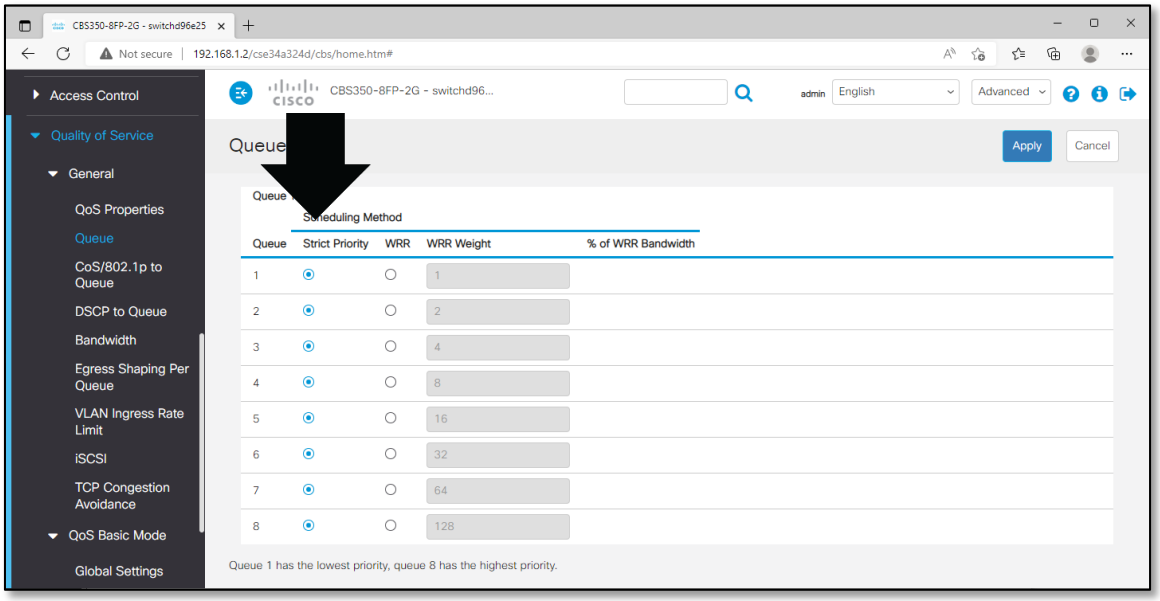
To set QoS for Dante:



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

    a. Select the **Advanced** radio button for QoS Mode.

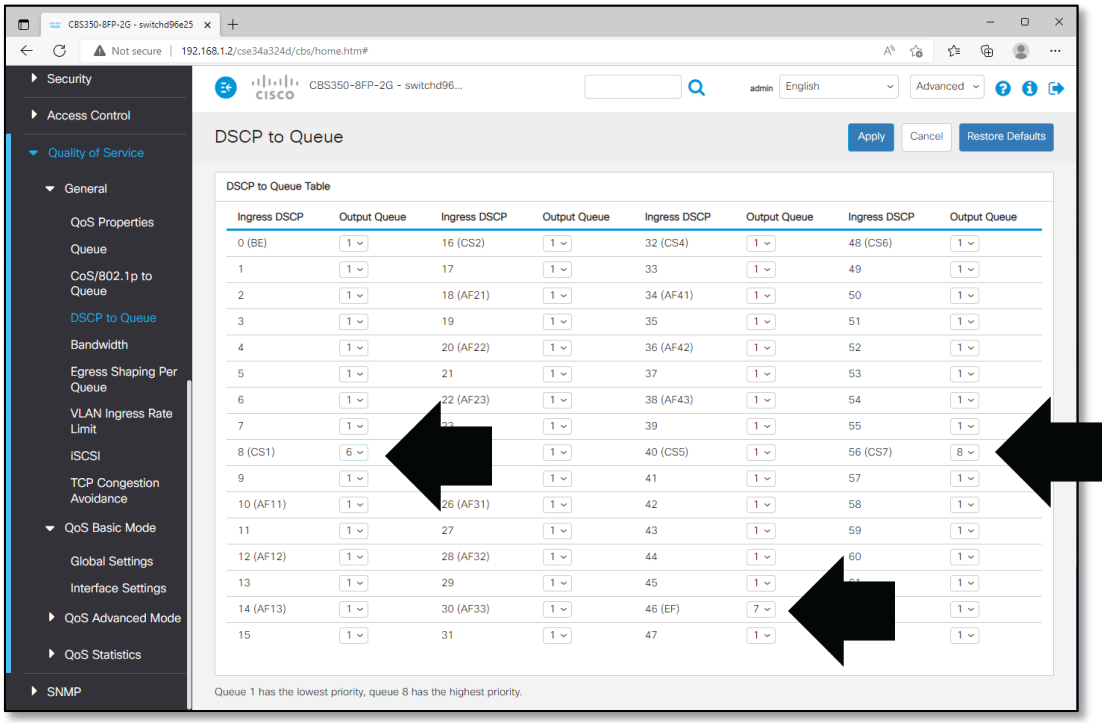
    b. Click **Apply**.



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.**



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

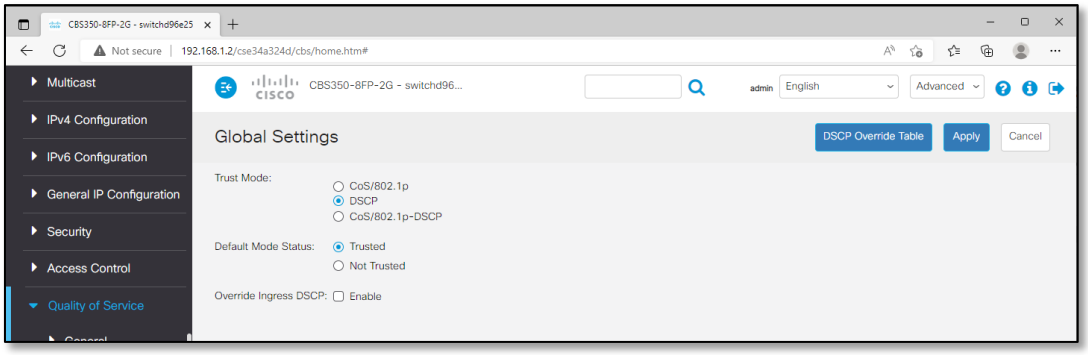
   a. Set all DSCP values to queue 1 (or some value below 6), for now.

   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



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

   a. Set Trust Mode to DSCP.

   b. Set Default Mode Status to Trusted.

   Leave Ingress DSCP unchecked.

   c. Click **Apply** to confirm.

Reminder:
Now is a good time to save.

4.3. IGMP Snooping

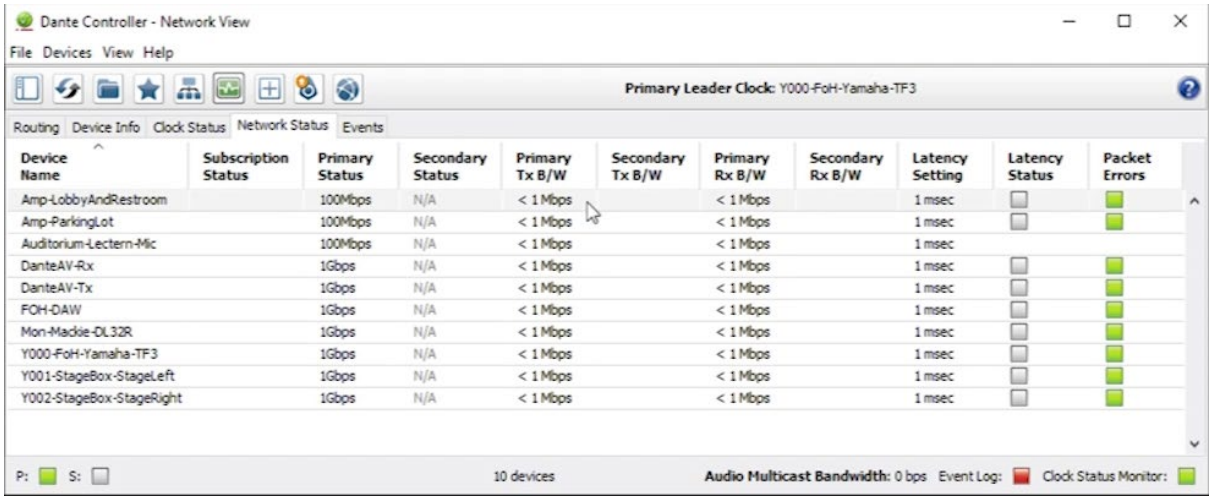
Dante networks certainly use multicast for discovery and clocking, but that is a small data load. This may account for 20Kbps on a small network, which would be about 0.002% of a 1Gbit port's capacity.

Dante audio and video are unicast by default. When flows are flipped to multicast, an unmanaged switch would forward all of that to all ports. The audio-video traffic can be more substantial, at which point IGMP snooping becomes more valuable.

When considering what is "a lot" of multicast, think in terms of the slowest port in the VLAN. The presence of 100Mbit or even 10Mbit ports will accelerate the benefits of IGMP snooping as media networks grow.

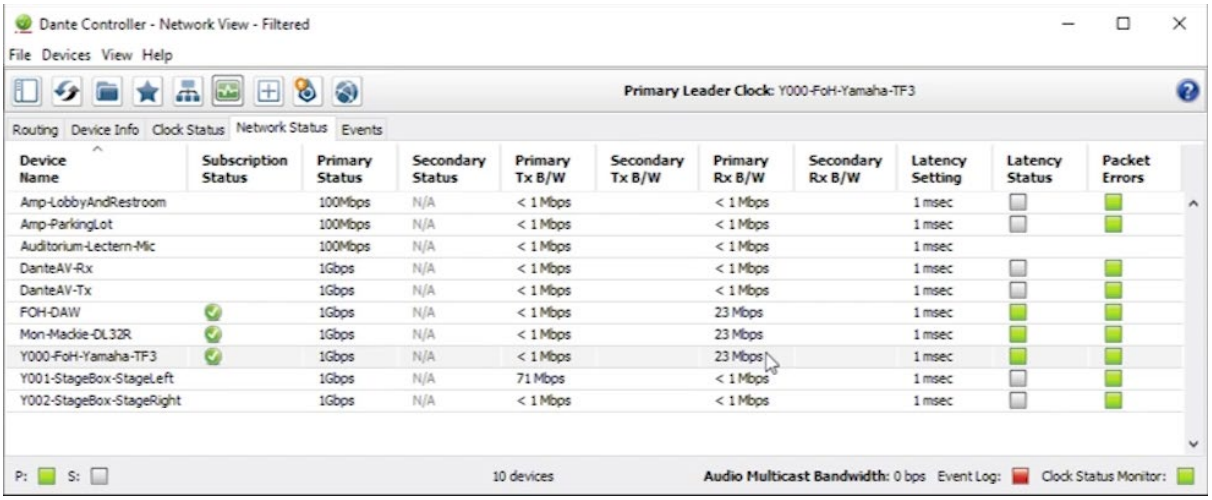
A Simple Demonstration in Unicast, Multicast and IGMP Snooping

It is easy to understand the impact of IGMP Snooping using a few Dante devices and Dante Controller. In Dante Controller's Network Status tab, we can see how much data any device is sending or receiving.



❶ Start with a clean slate.

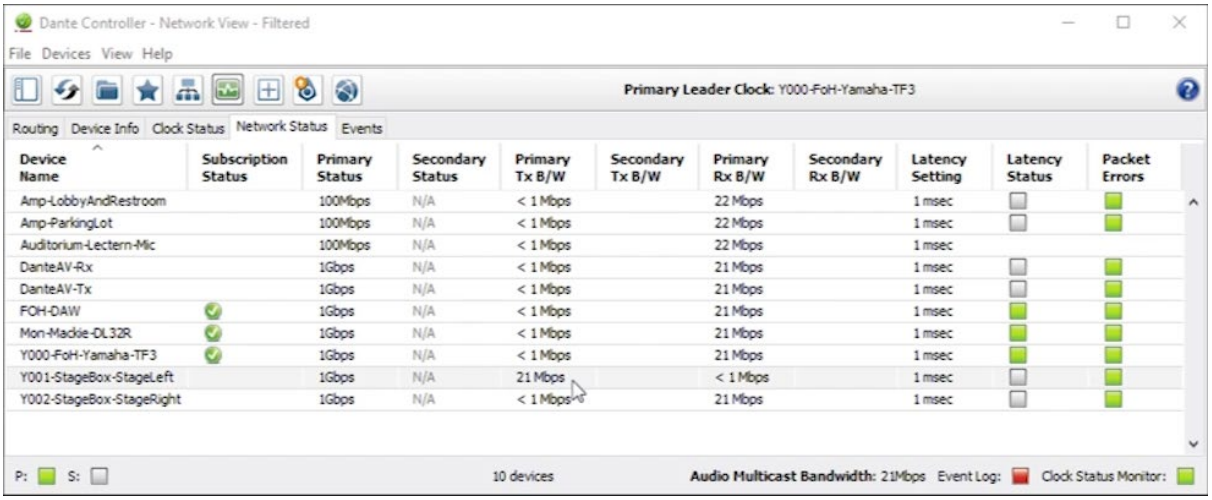
We begin by removing all subscriptions. In the Network Status Tab, we can see every device is sending and receiving < 1Mbps. In this case, this is the clocking and discovery traffic – quite negligible.



❷ See the impact of sending unicast to multiple destinations

This example sends all 16 audio channels from the stagebox to three different audio consoles. We can see the three consoles are receiving 23Mbps each, but the transmitter is sending 71Mbps – it is having to send that data out three times.

For the math sticklers, we know 3x 23Mbps = 69Mbps. The discrepancy is a rounding variance.

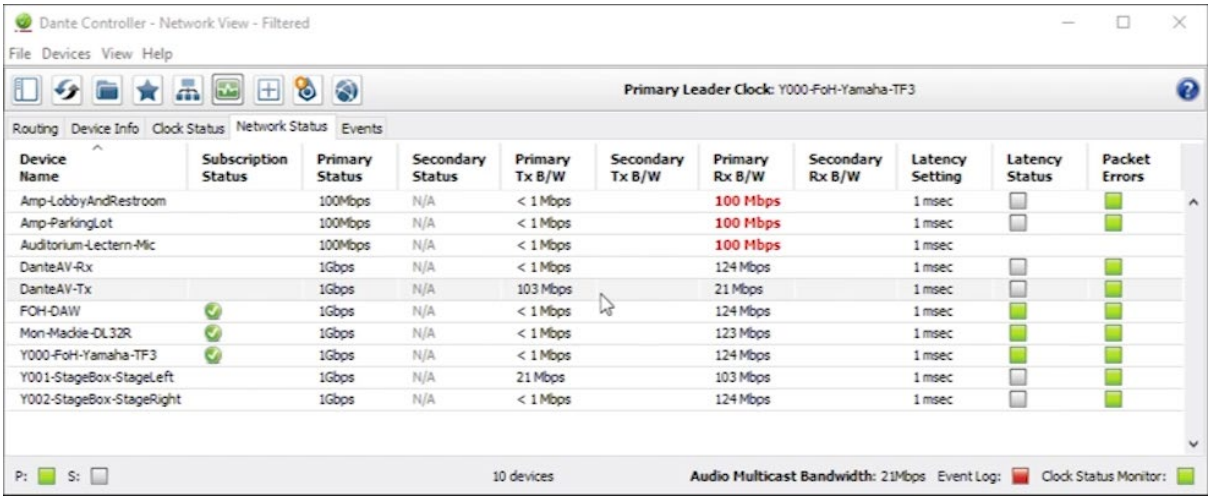


❸ Convert those flows to Multicast – a little multicast without IGMP snooping is OK.

Now that we convert the audio channels to multicast, the transmitter only has to send it once, and it is taking 21Mbps.

Again, for the mathematically inclined, notice the stream reduced in size 23Mbps to 21Mbps. Multicast streams are packed a bit more efficiently. The payload is the same; the network overhead changed.

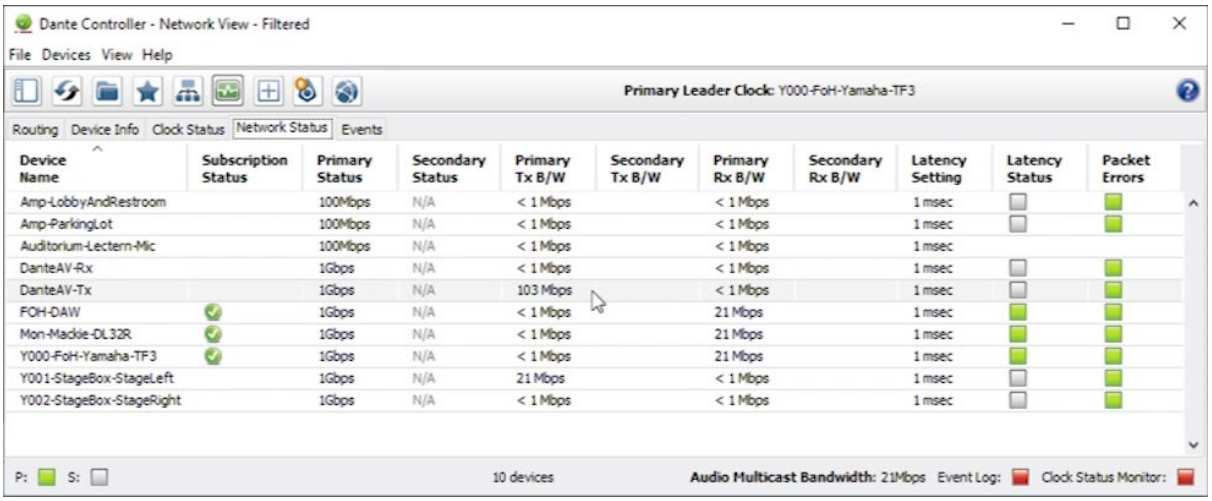
If we look in the Tx and Rx bandwidth readouts, we can see the transmission bandwidth from that device, as well as the receipt of that traffic at every port on the network. From this, we know IGMP snooping is not running, yet. If you have a modest amount of multicast, this might be OK.



❹ Too much multicast will start to overwhelm ports.

In the example above, we added a multicast video stream in multicast that is a bit over 100Mbps. Remember that multicast transmitters don't know who should receive the stream, they just transmit the data and let the switch figure out where to send it. In this case – without IGMP snooping – that stream is hitting all destinations, even though no device requested it.

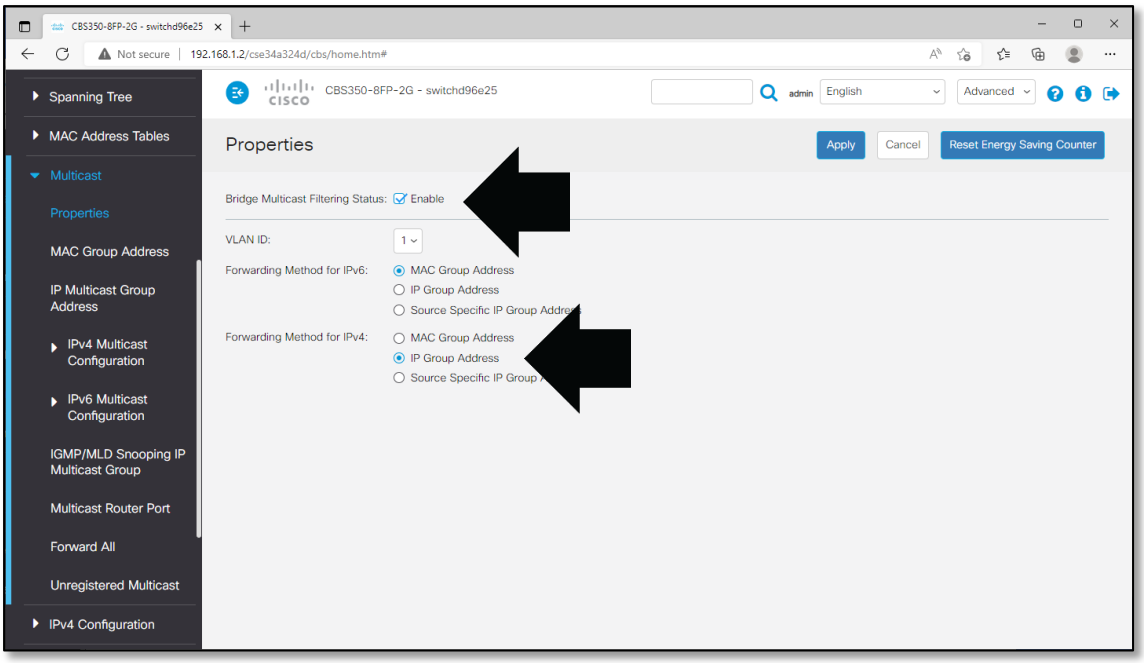
The combined traffic of the audio and video multicast flows is now approximately 124Mbps of multicast. We can see the three 100Mbps network interfaces at the top of the list are completely overwhelmed – Dante Controller indicates that by showing them in red.



❺ If we turn on IGMP Snooping, we can see the traffic only goes to the destinations that requested it. We can see the audio from the stagebox is going to three different mixers. Meanwhile, since the video signal wasn't requested by any device, it was not delivered anywhere, yet. Once a video receiver subscribes, it will receive the stream.

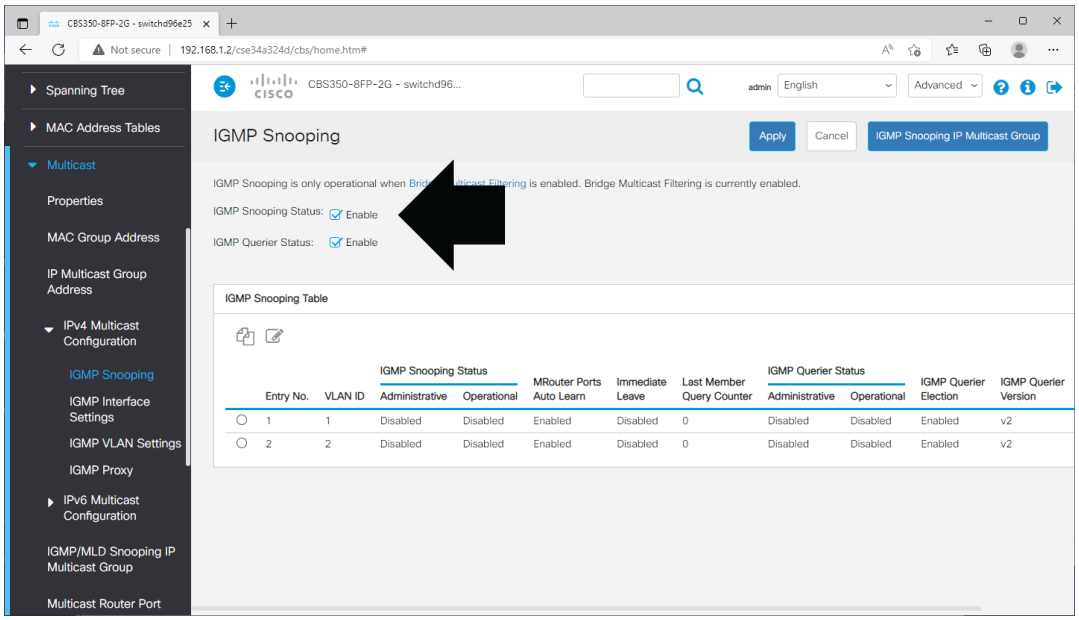
Set IGMP Snooping based on IP Group Address

On the CBS350-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.



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 IGMP 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)



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

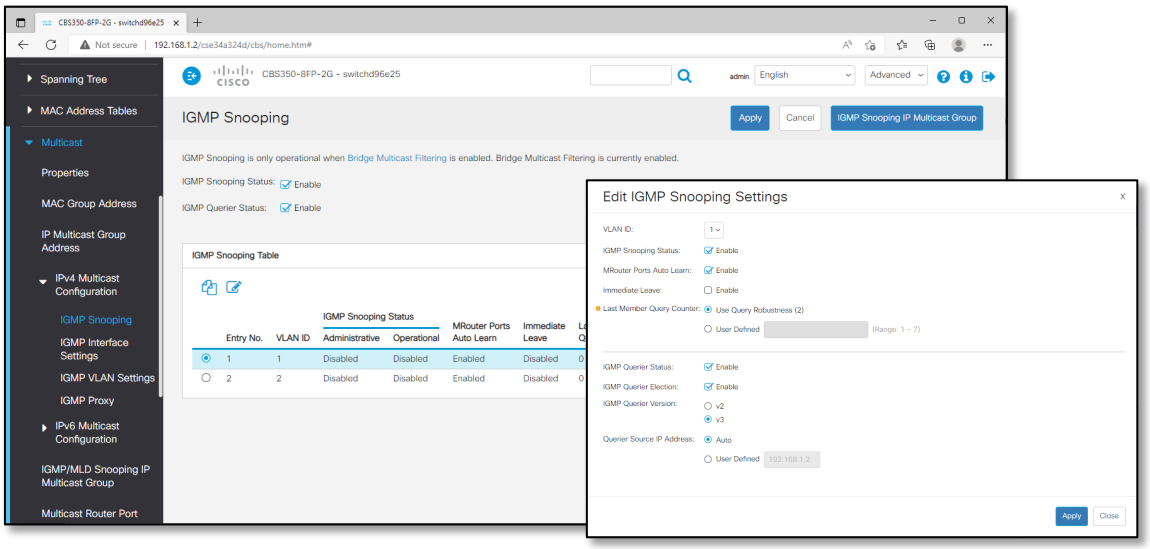
   a. Check the box for **IGMP Snooping Status** for all switches in the network.

   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



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

2) Check the box to select a the VLAN with Dante traffic and click the icon to 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).

   a. IGMP Querier Status: ☑ Enabled

   b. IGMP Querier Election: ☑ Enabled

   c. IGMP Querier Version: ○ v2
   ⦿ v3

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

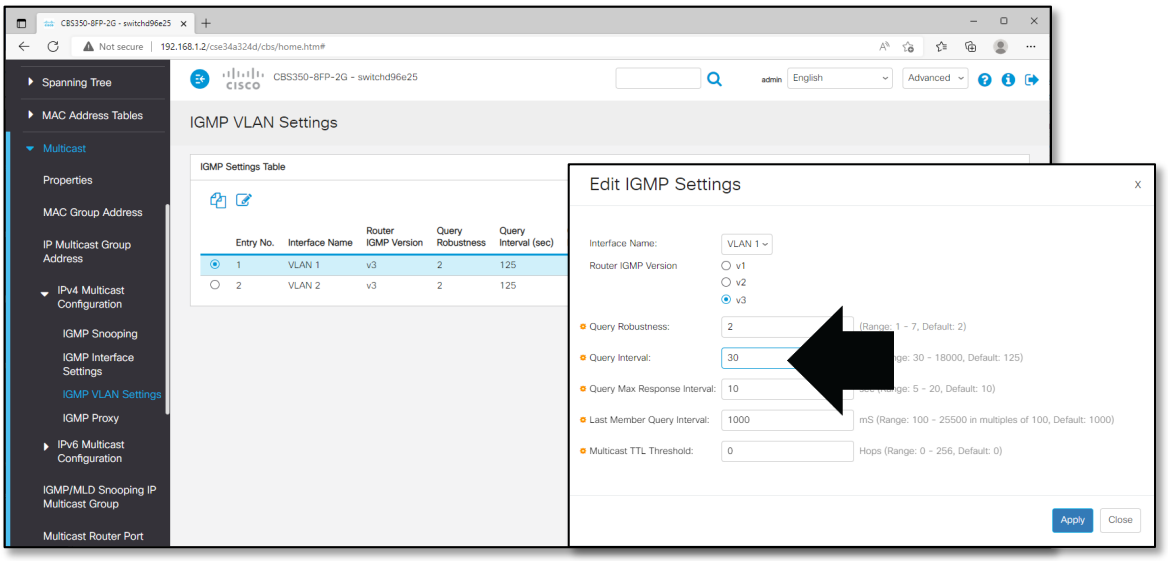
Note:

In Chapter 5, we will configure a DHCP server which will issue an address for our IGMP Querier, so we set this to Auto. If you will not continue to that chapter and will not have a DHCP server, you may want to select "User Defined" so you can assign a static IP address in your subnet for the querier, likely matching the managed interface IP. In this case, it would be 192.168.1.2.

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



1) Open **Multicast** > **IPv4 Multicast Configuration** > **IGMP VLAN Settings**.
2) Check the box to select a the VLAN with Dante traffic and click the icon to 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).

A note for Mac OS users running Dante Virtual Soundcard

Unless your network switch was designed specifically for the professional AV space, using IGMP snooping will likely cause Mac OS-X machines running Dante Virtual Soundcard to lose clock. You'll know this is the case because In the Clock Status tab, it will show a status of "listening" – this means the device is looking for a clock source but cannot find it.

When IGMP snooping is used, it subscribes to a multicast stream with a Time to Live (TTL). At the end of that time, it needs to refresh its subscription. We believe MacOS is not doing this.

In these situations, you can manually forward the traffic to that computer to keep this operational. Continue to the next section for instructions.

4.4. Manually Forwarding Multicast Streams

Some devices do not operate properly with IGMP snooping – the most common example is the Mac OS platform with Dante Virtual Soundcard (DVS) is an example where conflicts arise. When the network 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 – this can be a crude but simple way to solve the issue.

For example, if a Mac OS-X machine has a 1Gbit port and there is 200Mbit of multicast traffic in the broadcast domain, and the network is dedicated to AV production, this may be a simple, acceptable solution. Especially if that Mac OS-X machine is a DAW recording all sources, anyway.

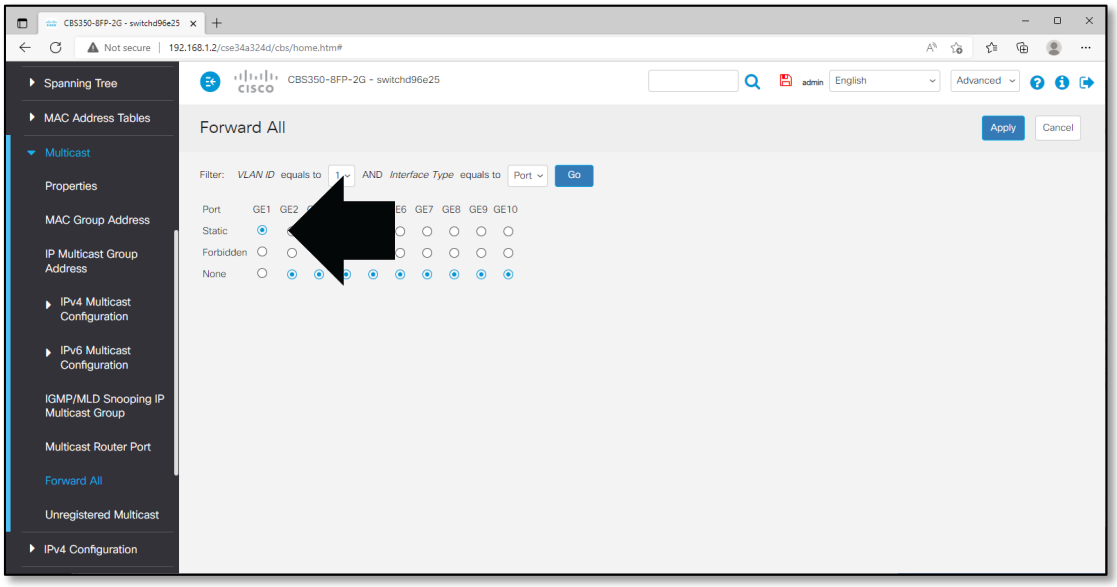
Manually Forwarding Multicast also does what it sounds like. If the required streams are known and fixed, the switch can be manually instructed to send specific multicast streams to a port. This is more precise than Forward All Multicast, not only alleviating unnecessary bandwidth on a particular port, 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. Simply forwarding clocking and discovery would manage all the multicast it needs.

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



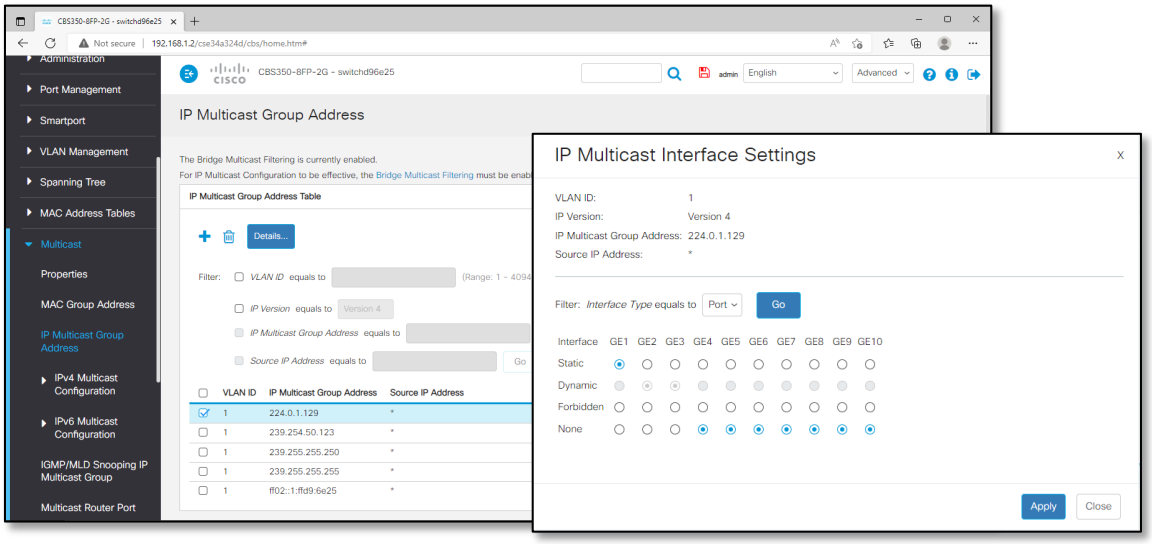
1) Go to **Multicast** > **Forward All**.
    a. Choose the appropriate VLAN. If changed, click **Go**. *If there are no VLANs, use ID 1.*
    b. Select the **Static** radio button for the desired ports. *In the above example, we target port 1.*
2) Click **Apply**.

Option 2: Manually Forwarding Individual Multicast Streams for a Port

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

Our CBS350-8FP-2G did not appear to offer access down to the multicast stream port level, it only offered the ability to forward by multicast IP.



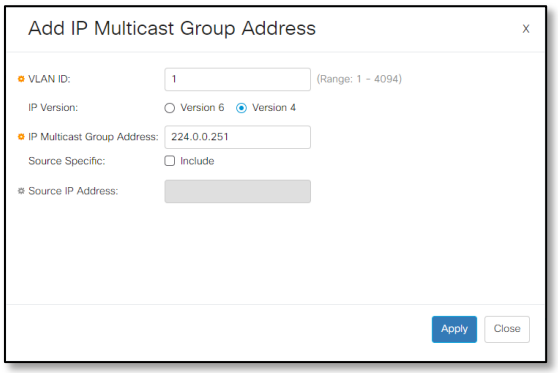
1) Go to **Multicast** > **IP Multicast Group Addresses**.

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

2) 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**.

3) Click **Apply**.



4) 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.

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, Second Edition. (The original Dante Certification Level 3 will not be enough.)

DHCP service, while a very simple concept, is included in this chapter because the CBS350 intertwines DHCP service with Inter-VLAN routing. (It does make sense, when you see it.) This is why DHCP is listed in this more advanced chapter.

To sign up for this free, on-demand 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	

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 Inter-VLAN Router on this switch

5.1. Reapply Lesson from Prior Chapter Switch Modifications

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

VLAN 1 will move the management interface to 192.168.1.1. This will become the router's address for this subnet. To do this, you will need to go back to IPv4 Configuration > IPv4 Interface. The system will not let you simply change the IP address of the management interface, but it will let you create another IP address in another subnet. It is clunky.

1) Go to **IPv4 Configuration** > **IPv4 Interface**
2) Add a management interface at another IP address in another subnet like 192.168.0.1.
3) Delete the current address of 192.168.1.2.
4) Move your computer to the other subnet (i.e. - 192.168.0.100) and log back in.
5) Add the management interface we want at 192.168.1.1.
6) Delete the current address of 192.168.0.1.
7) Move your computer back to the other subnet (i.e. – 192.168.1.100) and log back in.

In this example, we will have a Dante Domain Manager server on port 5 in VLAN 1 at 192.168.1.2. This will enable AV to be routed between VLANs/subnets.

VLAN 2 will be converted to another Dante VLAN. (We will be engaging Inter-VLAN routing, so we can route between subnets.) You can refer to earlier chapters for step-by-step instructions, but here are the guides to the screens:

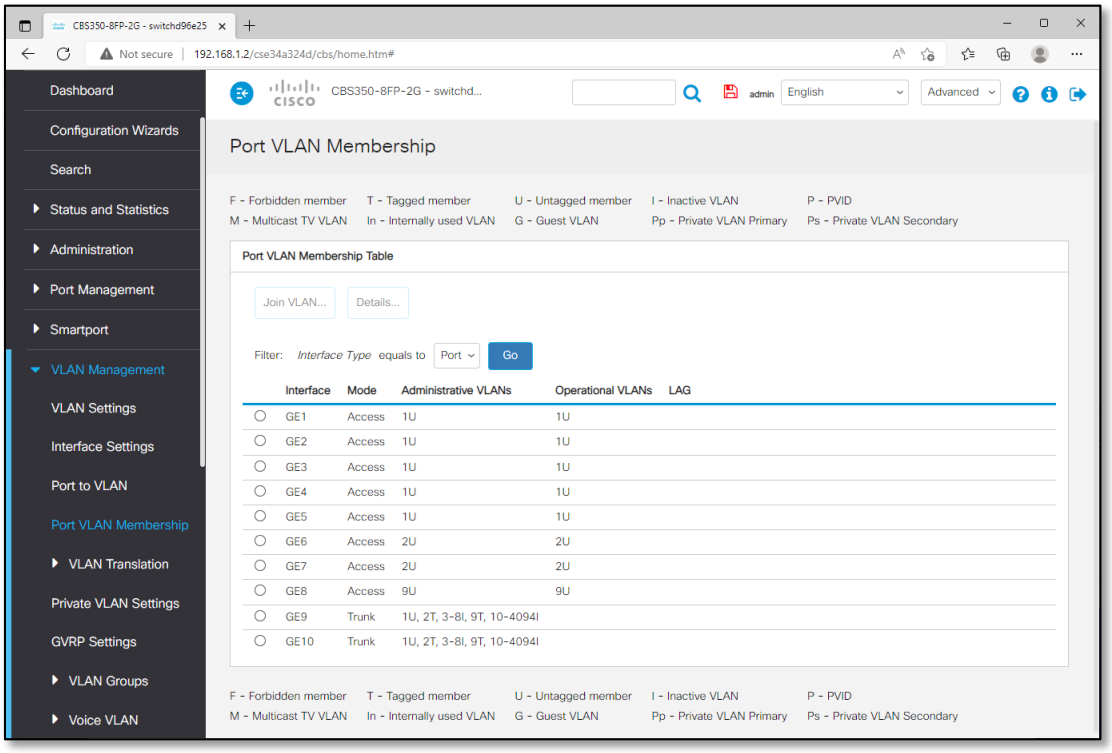
1) Go to **VLAN Management** > **VLAN Settings** to change the name for VLAN 2.
2) Go to **Multicast** > **IP v4 Multicast Configuration** > **IGMP Snooping** to enable IGMP Snooping/Querier.
3) Go to **Multicast** > **IP v4 Multicast Configuration** > **IGMP VLAN Settings** to match Snooping Settings (probably set Query Interval to 30).

VLAN 9 will be added to bring in internet service from an edge router.

1) Go to **VLAN Management** > **VLAN Settings** to add VLAN 9 for the Router/Internet.
2) Go to **VLAN Management** > **Port to VLAN** to set port 8 on VLAN 9 as untagged.

Now, this is where you may need to add a router to then network. Your typical router bundled from your home Internet Service Provider won't have the next-hop routing feature we need. In this example, we will be using a Cisco RV340 router. This will be connected later.

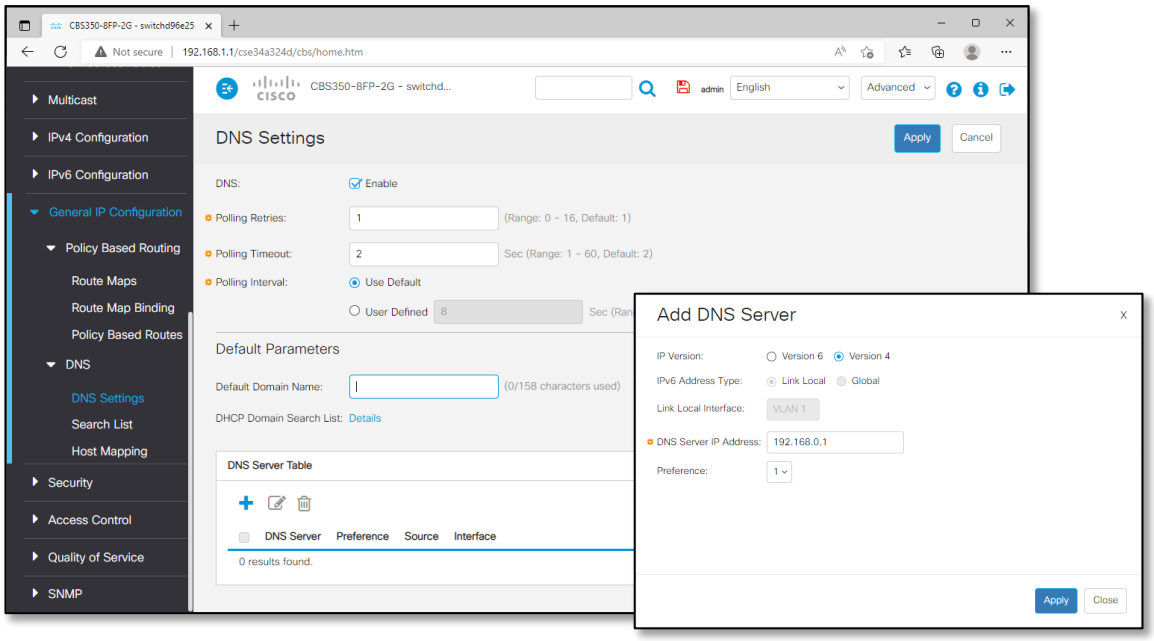
If you assigned any IGMP Querier(s) to static IP addresses on page 35, set it to Auto so it picks an address from the DHCP server, or adjust our future lessons so your DHCP pool does not overlap.



The most important part at this point is the VLAN assignment. If you go to **VLAN Management** > **Port VLAN Membership**, it should look like the above.

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.



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

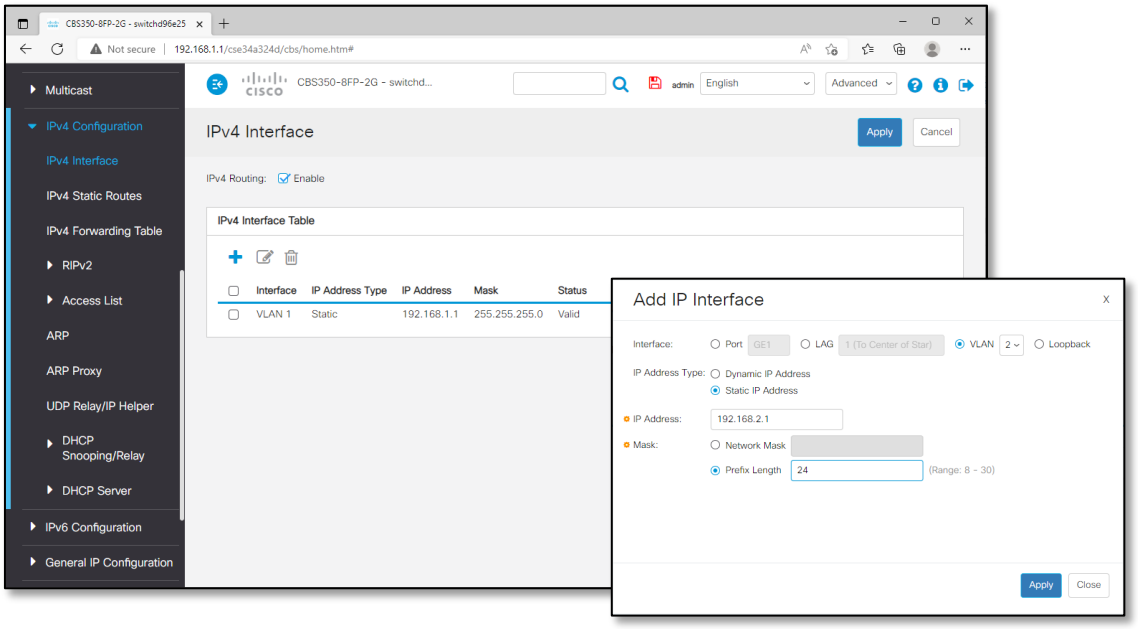
   a. Under **DNS Server Table**, click the ✚ icon to add.

   b. Add the **DNS Server's IP Address**. In this example, this will be coming from the Cisco router through VLAN 9 – that is located at **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



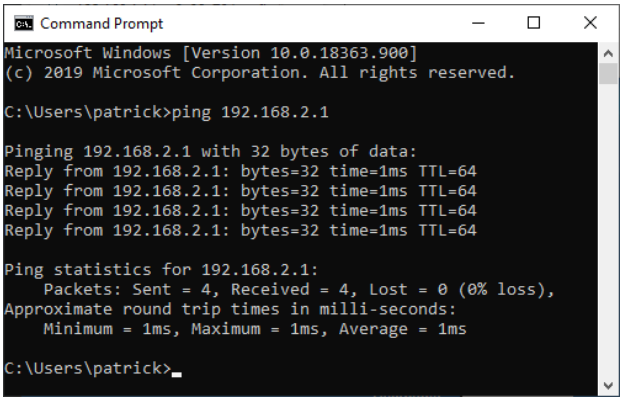
1) Open the **IPv4 Configuration** menu and select **IPv4 Interface.**
2) Click the ✚ icon to add.
    a. Ensure **VLAN 1** is selected at the top.
    b. Select the radio button for **IP Address type** as **Static IP Address.**
    c. Type in an address of **192.168.1.1.**
    d. Select a **Network 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.

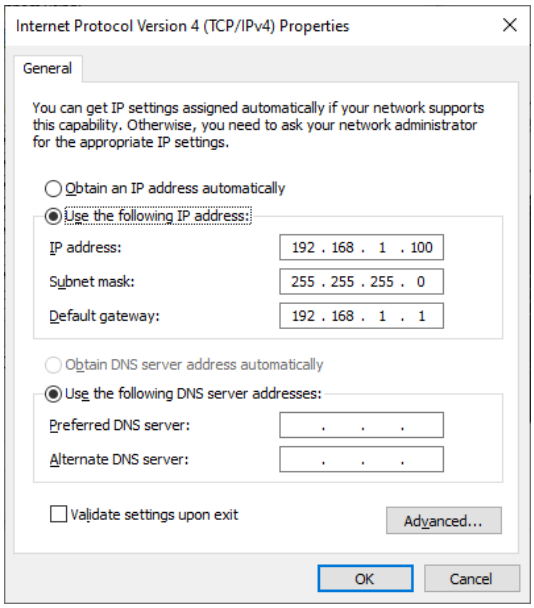
When you are done with this, your table should look as follows:

IPv4 Interface Table

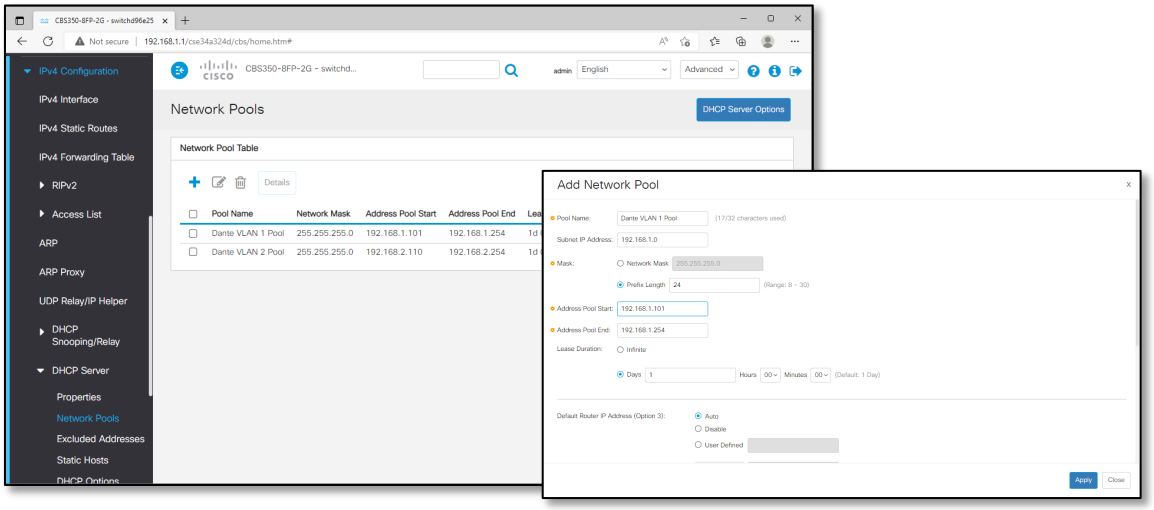
Interface	IP Address Type	IP Address	Mask	Status
VLAN 9	Static	192.168.0.2	255.255.255.0	Valid
VLAN 1	Static	192.168.1.1	255.255.255.0	Valid
VLAN 2	Static	192.168.2.1	255.255.255.0	Valid

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.





5.4. Assign DHCP Service in VLANs 1 and 2



1) Open **IPv4 Configuration > DHCP Server** > **Network Pools**

2) Click the ✚ icon to 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

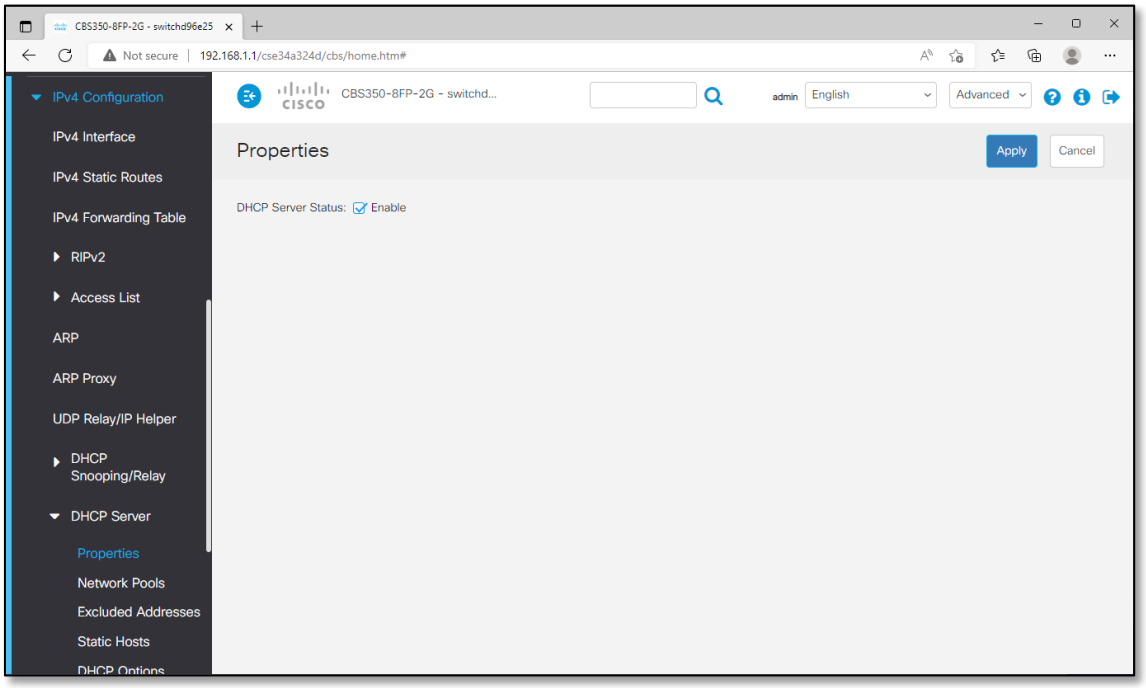
Leave the rest of the settings alone

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

5) Click **Apply**.



Open **IPv4 Configuration > DHCP Server** > **Properties**

a. Check DHCP Server Status: ☑ Enable

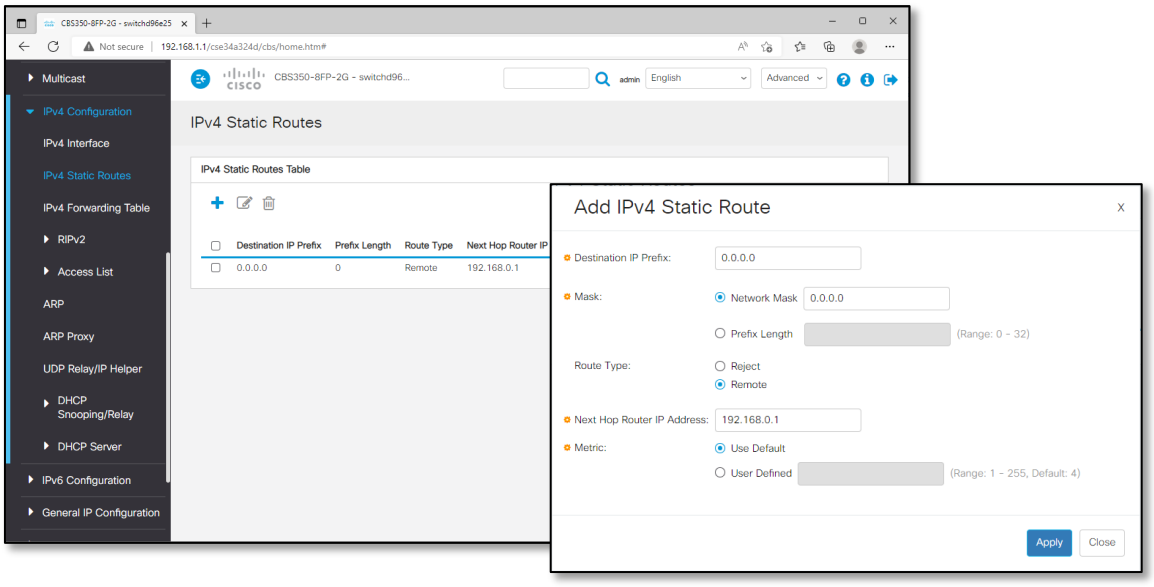
b. Click **Apply.**

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 CBS350 switch for Inter-VLAN routing. In order to link the switch to another router, we need to give the switch instructions on how to find it. In this example, we will set up a static route for the switch's internal router.



1) Open the **IPv4 Configuration** menu and select **IPv4 Static Routes.**

   a. Click the ✚ icon to 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**.

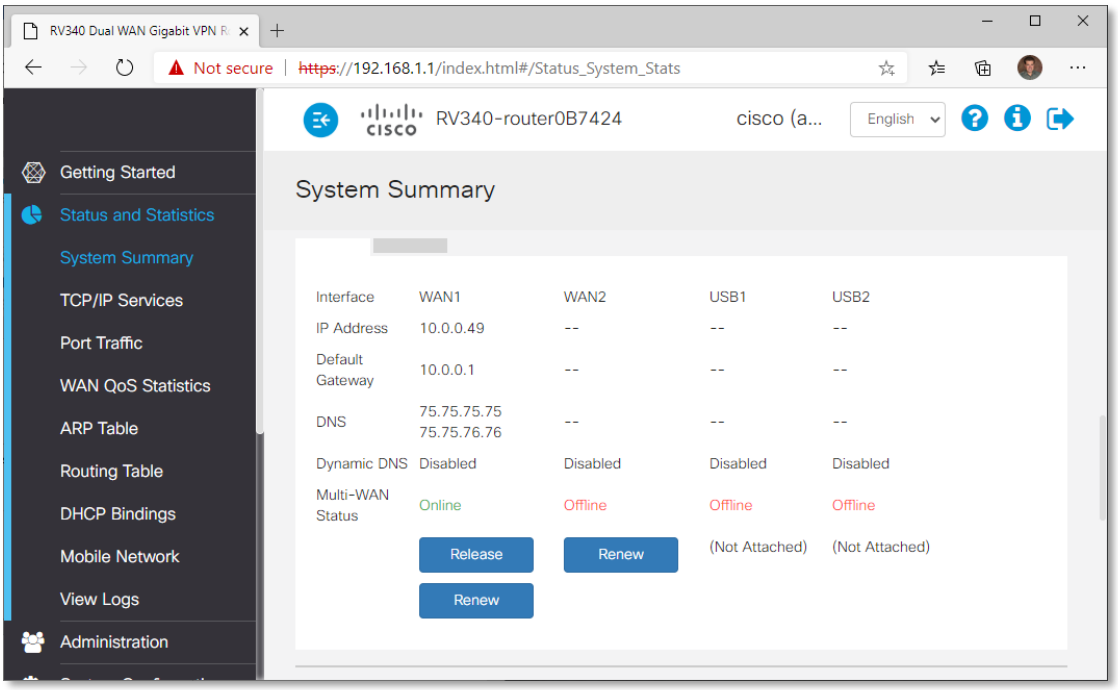
5.6. Prepping the Edge Router (RV340) for this Exercise

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 CBS350-8P-E-2G 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.

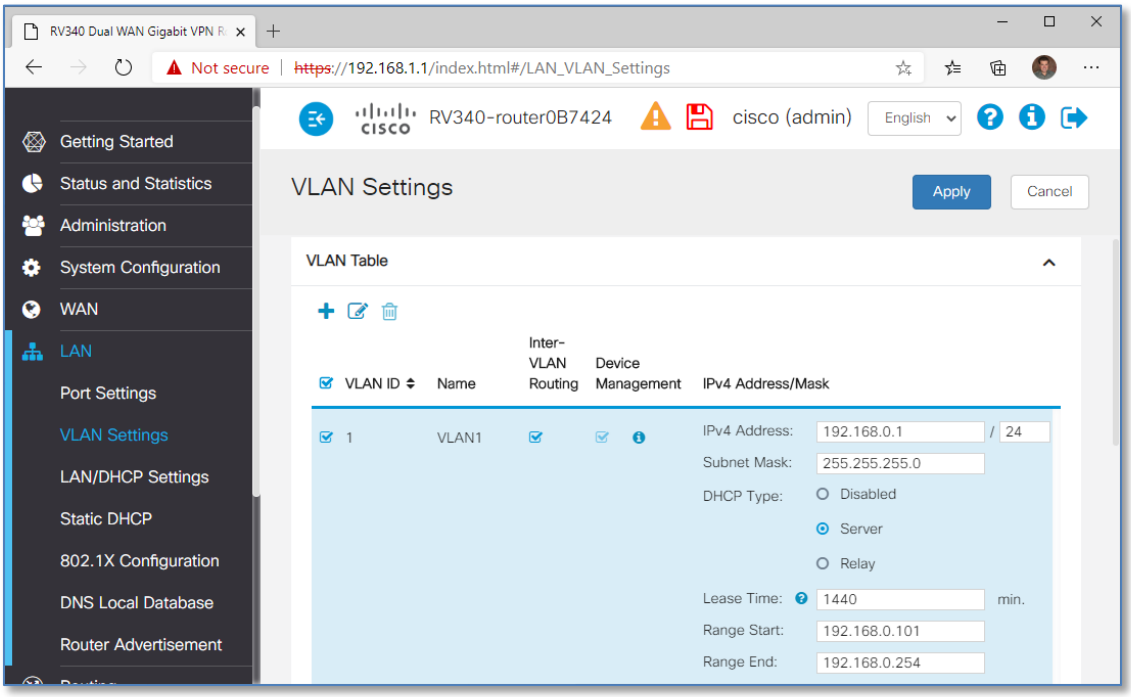
    Once the password is entered, you'll have to log back in again.



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.*



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.

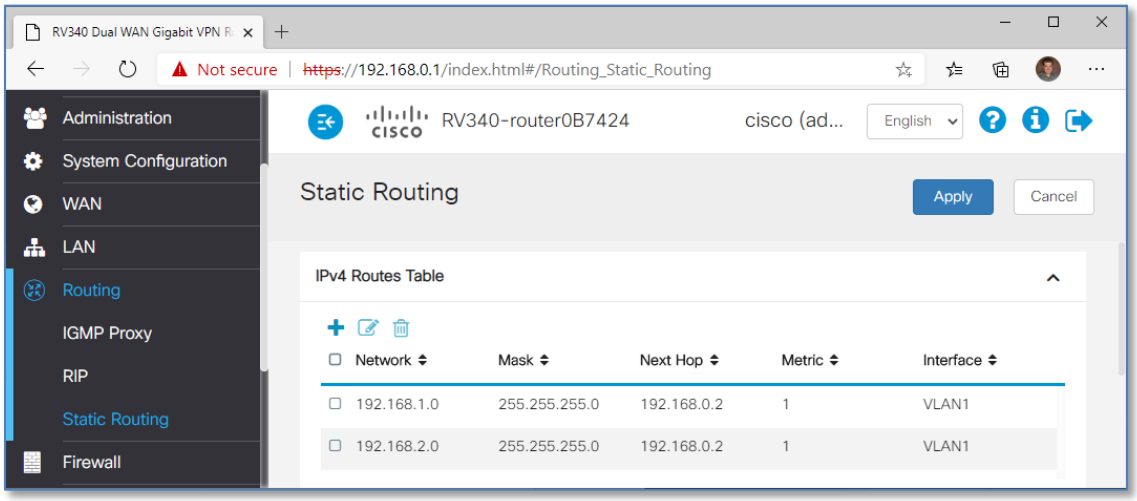
   Remember that your computer may need to reset IP address to be in the same subnet, as well.

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



8) Make static routes for the subnets that are managed in the CBS350-8P-E-2G.
    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* CBS350-8P-E-2G.
        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* CBS350-8P-E-2G.
        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

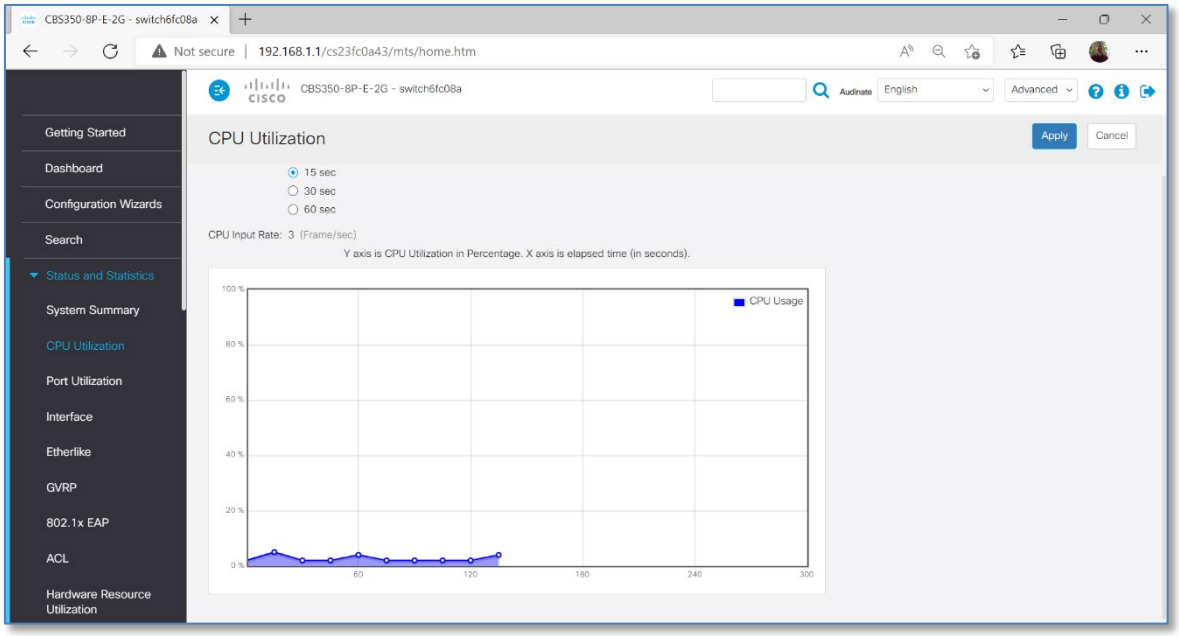
If your configuration followed ours, connect port 8 of the CBS350 switch to any LAN port on the RV340 router. Of course, also make sure a WAN port on the router is connected to the incoming internet service. Now, you can plug in to any port on the router or switch, and have routed connectivity on the LAN, and to the internet! Congratulations!

6. Switch Utilities

The CBS350-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.



To view this utility:

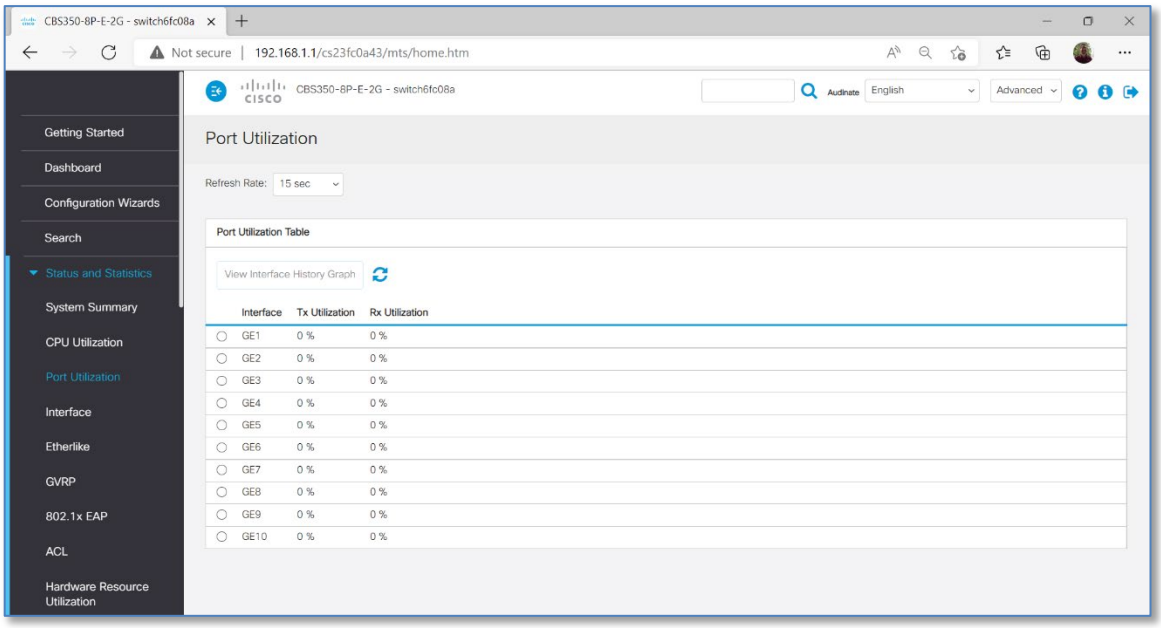
1) Go to **Status and Statistics** > **CPU Utilization**

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.



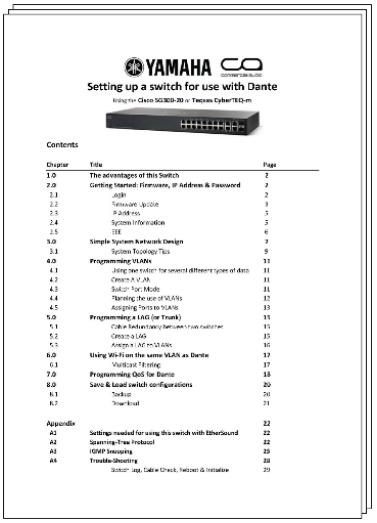
To view this utility

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

In 2013, Yamaha and Audinate developed a guide to the Cisco SG300. This coincided with the time Dante was surging in market adoption, and many in the audio industry had their first experience managing network switches with this document in hand.


YAMAHA

Setting up a switch for use with Dante

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	GUI	4
3.0	Simple System Network Design	7
3.1	System Topology Tips	9
4.0	Programming VLANs	11
4.1	Using two switch: the 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	23
A4	Trouble-Shooting	28
	Status Log, Cable Check, Reboot & Initialize	29

The original Dante guide for the SG300, released in 2013.

As a result, the SG300 became a popular model, indeed. Other switches could have worked as well, but for the early adopters of Dante, networks just need to *work*. The SG300 became a known quantity. Since other people seemed to be using it, they were able to share tips with each other – another bonus for such a small industry.

Other manufacturers like Shure, QSC and Crestron began offering instructions for additional tweaks their products could benefit from, again using the SG300 as an example. Even as Dante Certification Training came online around 2015, many students appreciated these guides as a chance to get hands on experience and gain an immersive perspective on networking, and often showed up to their installations with the guides in hand. The wiser ones even read it before they showed up.

When the SG300 was discontinued, Audinate's training department created a consolidated guide around the replacement – SG350. While that guide was written from scratch in 2020, we certainly wanted to recognize how much we learned and were inspired by the contributions from the preceding guides.

And of course, as the SG350 was discontinued, we updated the guide again to this version based on the CBS350. And again, new topics were added and enhanced.

We would like to recognize the contributions of these many guides that came before this one. The Professional AV community has grown its networking skill as an industry through these contributions, to the point that fundamentals of networking is now a routine skill.

Yamaha's Original SG300 Guide:	Topic Selection: Writing, Editing, Testing:	Chris Ware Kieran Walsh Andy Cooper Steve Seable
Audinate's SG350 Adaptation	Topic Selection, Writing, Editing: Testing	Patrick Killianey Kathryn Taub Augusto Marcondes Miguel Garcia
Audinate's CBS350 Adaptation	Additional Topics, Writing, Testing	Patrick Killianey Justin Alquist