

# **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 2022Firmware Version:3.2.0.84 (used on CBS350-8FP-2G)



#### Copyright

© 2022 Audinate Pty Ltd All Rights Reserved.

Audinate®, the Audinate logo and Dante® are registered trademarks of Audinate Pty Ltd.

All other trademarks are the property of their respective owners.

Audinate products are protected by one or more of US Patents 7747725, 8005939, 7978696, 8171152 and other patents pending or issued. See www.audinate.com/patents.

#### 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: <u>www.audinate.com/software-licensing-notice</u>

#### Contacts

Australia:	North/South America:	Europe, Middle East, Africa:	Asia/Pacific:
Audinate Pty Ltd	Audinate, Inc	Audinate Ltd	Audinate Limited
Level 7, 64 Kippax St	1200 NW Naito Parkway	Future Business Centre	Suite 1106-08
Surry Hills NSW 2010	Suite 630	Kings Hedges Rd	11/F Tai Yau Building
AUSTRALIA	Portland, OR 97209	Cambridge CB4 2HY	No 181 Johnston Road
Tel. +61 2 8090 1000	USA	United Kingdom	Wanchai, Hong Kong
Postal Address:	Tel. +1 503 224 2998	+44 (0) 1273 921695	Tel. +(852)-3588 0030 +(852)-3588 0031
Audinate Pty Ltd PO Box 855 Broadway NSW 2007 AUSTRALIA			Fax +(852)-2975 8042
info@audinate.com www.audinate.com			

Version 1.00, September 2022



## Contents

1.	Pr	reface	4
	1.1.	This a Tutorial. not a "Certified Switch Configuration"	4
	1.2.	What to Look for in a Managed Network Switch	4
	1.3.	CBS350-Series Naming Conventions	4
2.	Ва	asic Switch Set-Up	5
	2.1.	Initialize the Switch	5
	2.2.	Log in to the Management Interface, Set an Admin Password	6
	2.3.	Advanced Mode	7
	2.4.	Symbols	7
	2.5.	Update Firmware If Desired	8
	2.6.	Change the Management IP address	
	2.7.	Switch Information Fields: Location, Contact, Log-in Banner	
	2.8.	Stored Configurations: Running, Boot-Up and Factory Reset	13
	2.9.	Exporting/Saving Switch Configurations	14
	2.10.	. Loading a Saved Configuration to the Switch	15
3.	VL	LANs, Trunks, Link Aggregation Groups (LAGs)	16
	3.1.	Creating VLANs	17
	3.2.	Assigning Ports to VLANs	19
	3.3.	Assigning Ports to a Link Aggregation Group (LAG)	23
4.	Op	ptimizing for Dante Audio-Video Traffic	25
4.	<b>O</b> p 4.1.	ptimizing for Dante Audio-Video Traffic Disable Energy Efficient Ethernet (EEE, Green Ethernet, 802.3az)	<b>25</b> 26
4.	<b>Or</b> 4.1. 4.2.	<b>ptimizing for Dante Audio-Video Traffic</b> Disable Energy Efficient Ethernet (EEE, Green Ethernet, 802.3az) Quality of Service (QoS)	<b>25</b> 26 27
4.	<b>O</b> ¢ 4.1. 4.2. 4.3.	ptimizing for Dante Audio-Video Traffic Disable Energy Efficient Ethernet (EEE, Green Ethernet, 802.3az) Quality of Service (QoS) IGMP Snooping	<b>25</b> 26 27 30
4.	<b>Or</b> 4.1. 4.2. 4.3.	ptimizing for Dante Audio-Video Traffic Disable Energy Efficient Ethernet (EEE, Green Ethernet, 802.3az) Quality of Service (QoS) IGMP Snooping A Simple Demonstration in Unicast, Multicast and IGMP Snooping	<b>25</b> 26 27 30 30
4.	<b>O</b> ţ 4.1. 4.2. 4.3.	ptimizing for Dante Audio-Video Traffic Disable Energy Efficient Ethernet (EEE, Green Ethernet, 802.3az) Quality of Service (QoS) IGMP Snooping A Simple Demonstration in Unicast, Multicast and IGMP Snooping Set IGMP Snooping based on IP Group Address	25 26 30 30 33
4.	<b>O</b> ţ 4.1. 4.2. 4.3.	ptimizing for Dante Audio-Video Traffic Disable Energy Efficient Ethernet (EEE, Green Ethernet, 802.3az) Quality of Service (QoS) IGMP Snooping A Simple Demonstration in Unicast, Multicast and IGMP Snooping Set IGMP Snooping based on IP Group Address Engage IGMP Snooping (and Choose One Switch as Querier)	25 26 27 30 30 33 33 34
4.	Or 4.1. 4.2. 4.3.	ptimizing for Dante Audio-Video Traffic Disable Energy Efficient Ethernet (EEE, Green Ethernet, 802.3az) Quality of Service (QoS) IGMP Snooping A Simple Demonstration in Unicast, Multicast and IGMP Snooping Set IGMP Snooping based on IP Group Address Engage IGMP Snooping (and Choose One Switch as Querier) Edit IGMP Snooping Parameters for Dante VLANs, Part 2.	25 26 27 30 30 33 33 34 34 36
4.	Or 4.1. 4.2. 4.3.	ptimizing for Dante Audio-Video Traffic Disable Energy Efficient Ethernet (EEE, Green Ethernet, 802.3az) Quality of Service (QoS) IGMP Snooping A Simple Demonstration in Unicast, Multicast and IGMP Snooping Set IGMP Snooping based on IP Group Address Engage IGMP Snooping (and Choose One Switch as Querier) Edit IGMP Snooping Parameters for Dante VLANs, Part 2 A note for Mac OS users running Dante Virtual Soundcard	25 26 27 30 30 33 33 34 34 36 37
4.	Or 4.1. 4.2. 4.3.	ptimizing for Dante Audio-Video Traffic Disable Energy Efficient Ethernet (EEE, Green Ethernet, 802.3az) Quality of Service (QoS) IGMP Snooping A Simple Demonstration in Unicast, Multicast and IGMP Snooping Set IGMP Snooping based on IP Group Address Engage IGMP Snooping (and Choose One Switch as Querier) Edit IGMP Snooping Parameters for Dante VLANs, Part 2. A note for Mac OS users running Dante Virtual Soundcard Manually Forwarding Multicast Streams	25 26 27 30 30 33 33 34 34 36 37 37
4.	Or 4.1. 4.2. 4.3.	ptimizing for Dante Audio-Video Traffic Disable Energy Efficient Ethernet (EEE, Green Ethernet, 802.3az) Quality of Service (QoS) IGMP Snooping A Simple Demonstration in Unicast, Multicast and IGMP Snooping Set IGMP Snooping based on IP Group Address Engage IGMP Snooping (and Choose One Switch as Querier) Edit IGMP Snooping Parameters for Dante VLANs, Part 2. A note for Mac OS users running Dante Virtual Soundcard Manually Forwarding Multicast Streams Option 1: Forward All Multicast for a Port	25 26 27 30 30 33 33 34 34 36 37 37 37 38
4.	Or 4.1. 4.2. 4.3.	ptimizing for Dante Audio-Video Traffic Disable Energy Efficient Ethernet (EEE, Green Ethernet, 802.3az) Quality of Service (QoS) IGMP Snooping A Simple Demonstration in Unicast, Multicast and IGMP Snooping Set IGMP Snooping based on IP Group Address Engage IGMP Snooping (and Choose One Switch as Querier) Edit IGMP Snooping Parameters for Dante VLANs, Part 2. A note for Mac OS users running Dante Virtual Soundcard Manually Forwarding Multicast Streams Option 1: Forward All Multicast for a Port Option 2: Manually Forwarding Individual Multicast Streams for a Port	25 26 27 30 30 33 33 34 34 36 37 37 37 38 38
4.	Or 4.1. 4.2. 4.3. 4.4.	ptimizing for Dante Audio-Video Traffic Disable Energy Efficient Ethernet (EEE, Green Ethernet, 802.3az) Quality of Service (QoS) IGMP Snooping A Simple Demonstration in Unicast, Multicast and IGMP Snooping Set IGMP Snooping based on IP Group Address Engage IGMP Snooping (and Choose One Switch as Querier) Edit IGMP Snooping Parameters for Dante VLANs, Part 2. A note for Mac OS users running Dante Virtual Soundcard Manually Forwarding Multicast Streams Option 1: Forward All Multicast for a Port Option 2: Manually Forwarding Individual Multicast Streams for a Port ter-VLAN Routing, DHCP	25 26 27 30 30 33 33 34 36 37 37 38 38 38 40
4.	Or 4.1. 4.2. 4.3. 4.4. 5.1.	ptimizing for Dante Audio-Video Traffic Disable Energy Efficient Ethernet (EEE, Green Ethernet, 802.3az) Quality of Service (QoS) IGMP Snooping A Simple Demonstration in Unicast, Multicast and IGMP Snooping Set IGMP Snooping based on IP Group Address. Engage IGMP Snooping (and Choose One Switch as Querier) Edit IGMP Snooping Parameters for Dante VLANs, Part 2. A note for Mac OS users running Dante Virtual Soundcard Manually Forwarding Multicast Streams Option 1: Forward All Multicast for a Port Option 2: Manually Forwarding Individual Multicast Streams for a Port Reapply Lesson from Prior Chapter Switch Modifications.	25 26 27 30 30 33 33 34 36 37 37 37 38 38 38 40 41
4.	Or 4.1. 4.2. 4.3. 4.4. 5.1. 5.1. 5.2.	ptimizing for Dante Audio-Video Traffic Disable Energy Efficient Ethernet (EEE, Green Ethernet, 802.3az) Quality of Service (QoS) IGMP Snooping A Simple Demonstration in Unicast, Multicast and IGMP Snooping Set IGMP Snooping based on IP Group Address Engage IGMP Snooping (and Choose One Switch as Querier) Edit IGMP Snooping Parameters for Dante VLANs, Part 2 A note for Mac OS users running Dante Virtual Soundcard Manually Forwarding Multicast Streams Option 1: Forward All Multicast for a Port Option 2: Manually Forwarding Individual Multicast Streams for a Port Reapply Lesson from Prior Chapter Switch Modifications Add a DNS Server:	25 26 27 30 30 33 34 34 36 37 37 37 38 38 38 40 41
4.	Or 4.1. 4.2. 4.3. 4.4. 5.1. 5.2. 5.3.	ptimizing for Dante Audio-Video Traffic Disable Energy Efficient Ethernet (EEE, Green Ethernet, 802.3az) Quality of Service (QoS) IGMP Snooping A Simple Demonstration in Unicast, Multicast and IGMP Snooping Set IGMP Snooping based on IP Group Address Engage IGMP Snooping (and Choose One Switch as Querier) Edit IGMP Snooping Parameters for Dante VLANs, Part 2 A note for Mac OS users running Dante Virtual Soundcard Manually Forwarding Multicast Streams Option 1: Forward All Multicast for a Port Option 2: Manually Forwarding Individual Multicast Streams for a Port Pter-VLAN Routing, DHCP Assign Router IP Address in Each VLAN for Inter-VLAN routing	25 26 27 30 30 33 33 34 36 37 37 38 38 38 40 41 43 44
4.	Or 4.1. 4.2. 4.3. 4.4. 5.1. 5.2. 5.3. 5.4.	ptimizing for Dante Audio-Video Traffic Disable Energy Efficient Ethernet (EEE, Green Ethernet, 802.3az) Quality of Service (QoS) IGMP Snooping A Simple Demonstration in Unicast, Multicast and IGMP Snooping Set IGMP Snooping based on IP Group Address Engage IGMP Snooping (and Choose One Switch as Querier) Edit IGMP Snooping Parameters for Dante VLANs, Part 2 A note for Mac OS users running Dante Virtual Soundcard Manually Forwarding Multicast Streams Option 1: Forward All Multicast for a Port Option 2: Manually Forwarding Individual Multicast Streams for a Port Option 2: Manually Forwarding Individual Multicast Streams for a Port Add a DNS Server: Assign Router IP Address in Each VLAN for Inter-VLAN routing Assign DHCP Service in VLANs 1 and 2	25 26 27 30 30 33 33 34 36 37 37 37 37 38 38 40 41 41 43 44 44
4.	Or 4.1. 4.2. 4.3. 4.4. 5.1. 5.1. 5.2. 5.3. 5.4. 5.5.	ptimizing for Dante Audio-Video Traffic         Disable Energy Efficient Ethernet (EEE, Green Ethernet, 802.3az)         Quality of Service (QoS)         IGMP Snooping         A Simple Demonstration in Unicast, Multicast and IGMP Snooping         Set IGMP Snooping based on IP Group Address         Engage IGMP Snooping (and Choose One Switch as Querier)         Edit IGMP Snooping Parameters for Dante VLANs, Part 2.         A note for Mac OS users running Dante Virtual Soundcard         Manually Forwarding Multicast Streams         Option 1: Forward All Multicast for a Port         Option 2: Manually Forwarding Individual Multicast Streams for a Port         Reapply Lesson from Prior Chapter Switch Modifications         Add a DNS Server:         Assign Router IP Address in Each VLAN for Inter-VLAN routing         Assign DHCP Service in VLANs 1 and 2.         Create a Static Route from the Switch to the Edge Router	25 26 27 30 30 33 34 34 36 37 37 37 38 38 38 40 41 41 43 44 44 46 48

	5.7.	Create the Static Route from the Router to the Switch	
	5.8.	Connect the Router and Switch	
6.	Sw	vitch Utilities	52
	6.1.	CPU Utilization	52
	6.2.	Port Utilization	53
7.	Cr	edits and Acknowledgements	54

## 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 <u>https://audinate.com/certify</u>.

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	ΡοΕ	15W
2009	802.3at	Type 2	PoE+	30W
2018	802.3bt	Type 3	PoE++	60W
2010 002.55t		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



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.

Internet Protocol Version 4 (TCP/IPv4)	Properties	×
General		
You can get IP settings assigned auton this capability. Otherwise, you need to for the appropriate IP settings.	natically if your network supports ask your network administrator	
Ogbtain an IP address automatical	ly	
Use the following IP address:		- 1
IP address:	192 . 168 . 1 . 100	
Subnet mask:	255 . 255 . 255 . 0	
Default gateway:		
Obtain DNS server address auton	natically	
• Use the following DNS server add	resses:	- 1
Preferred DNS server:		
Alternate DNS server:		
Validate settings upon exit	Ad <u>v</u> anced	
	OK Cance	ł



For security reasons, it is This will delete the defar	s required to create a ne ult user.	w administration user for device management.
The minimum requireme	ints for password are as	follows:
· Cannot be the same as	s the user name.	
Minimum length is 8.		
- Minimum number of ch	aracter classes is 3. CP	
Minimum number of ch	aracter classes is 3. CP	
Minimum number of ch User Name:	aracter classes is 3. Or admin	anacter classes are upper case, lower case, numeric, and special characters. (5/20 characters used)
- Minimum number of ch User Name: Password:	admin	anacter classes are upper case, lower case, numeric, and special characters. (5/20 characters used) (9/64 characters used)
- Minimum number of ch User Name: Password: Confirm Password:	admin	executer classes are upper case, lower case, numeric, and special characters. (5/20 characters used) (8/64 characters used)

### 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.

	ttat CBS	350-8FP-2G - switchd96e25	× +				- • ×
$\leftarrow$	С	A Not secure 192	2.168.1.254/csd24b6ca/mts/hom	e.htm			2 A to to to 🗈 🖷
			CISCO	0-8FP-2G - switchd96		🔍 🖺 admin English	✓ Advanced ✓ ? 3 ➡
	Getting	Started	System Summa	Ŷ			
	Dashbo	bard	System Information		•	Softwara Information	
	Configu	uration Wizards	System Description:	CBS350-8FP-2G 8-Port Gigabit	th	Firmware Version (Active Image):	3.0.0.69
	Search		System Location: System Contact:			Firmware MD5 Checksum (Active Image): Firmware Version (Non-active):	7520543df10e96a355ec0d1bd5785e39 3.0.0.69
-		and Statistics	Host Name: System Object ID:	switchd96e25 1.3.6.1.4.1.9.6.1.1004.10.15 0.dec(c) 0.bc(c) 25 min(c) and 17 an		Firmware MD5 Checksum (Non-active):	7520543dt10e96a355ec0d1bd5785e39
		n Summary	Current Time: Base MAC Address:	00:30:21;2022-Sep-17 34:b8:83:d9:6e:25	(C(S)		
	CPU U	tilization	Jumbo Frames:	Disabled			
	Port Ut	ilization					
	Interfac	ce	TCP/UDP Services S	Status Edit		PoE Power Information	Detail
	Etherlik	æ	HTTP Service: HTTPS Service: SNMP Service:	Enabled Enabled Disabled		Maximum Available PoE Power(W): Total PoE Power Consumption(W): PoE Power Mode:	120 0 Class Limit
	GVRP		Telnet Service: SSH Service:	Disabled Disabled			
	802.1x	EAP					
	ACL		Serial Number: PSZ26251	F8E PID VID: CBS350-8FP-2G V02			
	Hardwa Utilizati	are Resource ion	elado cisco o en IIII	<u> </u>			
	Health	and Power	Ø 17 m	7 74 57 7 7 Y	9* ¥10 9*	<u>10</u>	

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....

CBS350-8FP-2G - switchd96e25	× +					- 0	×
← C ▲ Not secure   19	2.168.1.254/csd24b6ca/mts/ho	me.htm		P A	° to t≞	<b>H</b>	
<ul> <li>Administration</li> </ul>	CISCO	350-8FP-2G - switchd96	🔍 🖺 admin	English	- Advanced -	00	•
System Settings	Firmware Oper	rations			Apply	Canc	el
Console Settings							
User Accounts	Active Firmware File: Active Firmware Version:	image1.bin 3.0.0.69					
Idle Session Timeout	Operation Type:	Update Firmware     Backup Firmware					
Time Settings	Coov Method:	Swap Image     HTTP/HTTPS					
System Log		O USB O TETP					
▼ File Management		O SCP (File transfer via SSH)					
Firmware Operations	File Name:	Choose File image_cbsigned.bin					
File Operations							
File Directory							
DHCP Auto Update							
Cisco Business Dashboard Settings							
▶ PNP							
Reboot							
Hardware Resources							
Discovery - Bonjour							

- 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.

Сс	onfirm Interface Creation	х
	This interface already has a dynamic IP address. Adding the static IP address will delete the dynamic IP address from this interface.	
	Do you want to continue?	
	Don't show me this again	
	OK Cance	H



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:

CBS350-8FP-2G - switchd96e2	5 × +					-	o x		
← C ▲ Not secure   19	92.168.1.2/cse34a324d/cbs/	home.htm			A	6 6 6			
Status and Statistics	🚭 uludu o cisco	BS350-8FP-2G - switchd96e25		Q admin	English ~	Advanced ~	0 🕩		
<ul> <li>Administration</li> </ul>	System Sett	ings				Apply Car	icel		
System Settings	System Setting	-							
Console Settings	System Description:	CBS350-8FP-2G 8-Port Gigabit PoE Managed Switch		🗖 😆 192.	.168.1.2/cse34a324d/cbs/con 🗙	+	_	-	o x
User Accounts	System Location:	Training Room (13/160 characters used)		<ul><li>&lt; 0</li></ul>	A Not secure   192.16	58.1.2/cse34a324d/c 🖉	AN to t	≡ @	۰۰ ۱
Idle Session Timeout	System Contact:	Training Mgr x4307 (18/160 characters used)			(	Student 14 Training Room			
Time Settings	Host Name:	Use Default							
System Log		O User Defined switchd96e25 (12/58 char	acters used; Defau			CISCO			
File Management	Custom Banner	Settings				Switch			
Cisco Business Dashboard Settings	Login Banner:	Student 14 Training Room Cisco CBS350-8FP-2G				Switch			
						Usemanie			
F FINF		(46/1000 characters used)				Password			
Reboot	Preview					English ~			
Hardware Resources	Malaama Baaaan						_		
Discovery - Bonjour	welcome banner.				Log Ir	Secure Browsing (HT	TPS)		
Discovery - LLDP		(0/1000 characters used)			© 2021-202	22 Cisco Systems, Inc. All Rights	Reserved.		
Discovery - CDP	Preview				Cisco, Cisco Systems, ar trademarks of Cisco Sys	nd the Cisco Systems logo are re- stems, Inc. and/or its affiliates in t certain other countries.	sistered trademar he United States	us or and	

- 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.





## 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:

CBS350-8FP-2G - switchd96e25	× +		- 0 ×
← C ▲ Not secure   192	.168.1.2/cse34a324d/cbs/hc	me.htm	A to to 🕲
Status and Statistics	G cisco	S350-8FP-2G - switchd96e25	h v Advanced v 💡 🚯 🕞
<ul> <li>Administration</li> </ul>	File Operation	s	Apply Cancel
System Settings			
Console Settings	Operation Type:	Update File     Backup File     Developed	
User Accounts	Source File Type:	Running Configuration	
Idle Session Timeout		Startup Configuration Mirror Configuration	
Time Settings		O Logging File	
System Log		Language File     Dashboard Info File	
✓ File Management	Copy Method:	● HTTP/HTTPS ○ USB	
Firmware Operations		O Internal Flash	
File Operations		O SCP (File transfer via SSH)	
File Directory	Sensitive Data Handling	C Exclude	
DHCP Auto Update		Encrypt	
Cisco Business Dashboard Settings		U maintext	
▶ PNP			
Reboot			
Hardware Resources			

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.





 $\Box \times$ 

...

#### Loading a Saved Configuration to the Switch 2.10.

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.

☆ CBS350-8FP-2G - switchd96e25 × + 4 C Not secure | 192.168.1.2/cse34a324d/cbs/home.htm A۵ sã s≦= ۰<u>ه</u> CBS350-8FP-2G - switchd96e25 Q admin English Advanced ~ 00 Status and Statistics **File Operations** Cancel System Settings Operation Type: Update File O Backup File Console Settings Duplicate User Accounts Destination File Type: O Running Configuration Startup Configuration Idle Session Timeout Mirror Configuration Logging File Time Settings C Language File O Dashboard Info File System Log Copy Method: HTTP/HTTPS File Management O USB O Internal Flash Firmware Operations ) TETP O SCP (File transfer via SSH) File Directory Choose File running-config.txt File Name: DHCP Auto Update Cisco Business Dashboard Settings

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.

PNP Reboot

Hardware Resources

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 <u>https://audinate.com/certify</u>.



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 (Dant	e)				2 - U (Contr	ol)		1 - U (Da 2 - T (Co	nte) ntrol)
Туре	Acces	S							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.

CBS350-8FP-2G - switchd96e25	< +	- D X
← C ▲ Not secure   192.1	68.1.2/cse34a324d/cbs/home.htm	A ta ta 🕲
Status and Statistics	CBS350-8FP-2G - switchd96e25	Q admin English v Advanced v 2 1 (*
Administration	VLAN Settings	
Port Management	V8 AN Table	
Smartport		
✓ VLAN Management		
VLAN Settings	Link Status ULAN ID VLAN Name Originators VLAN Interface State SNIMP Traps	
Interface Settings	D 1 Default Enabled Enabled	
Port to VLAN		
Port VLAN Membership		Add VLAN ×
VLAN Translation		VLAN
Private VLAN Settings		• VLAN ID: 2 (Range: 2 - 4094)
GVRP Settings		VLAN Name: Control Network (15/32 characters used)
VLAN Groups		VLAN Interface State: 🖌 Enable
Voice VLAN		Link Status SNMP Iraps: 12 Enable
<ul> <li>Access Port Multicast TV VLAN</li> </ul>		© VLAN Range: (Range: 2 - 4094)
Customer Port Multicast TV VLAN		Apply Close

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.



CBS350-8FP-2G - switchd96e25 ×	+										- 0	×		
← C ▲ Not secure   192.168.	.1.2/	cse34	4a324d/cbs/	/home.htm#						A <sup>n</sup> tõ ti≡	۲ ک			
<ul> <li>Status and Statistics</li> </ul>	æ	, I C	liulii ( cisco	CBS350-8FP-2G -	switchd96			Q	B admin English	~ Advanced	00	۲		
Administration	VL.	AN	Settin	gs										
Port Management														
Smartport	VL	AN '	Table									- 1		
<ul> <li>VLAN Management</li> </ul>		+	<b>B</b>											
VLAN Settings		0	VLAN ID	VLAN Name	Originators	VLAN Interface State	Link Status SNMP Traps							
Interface Settings		g	1		Default	Enabled	Enabled							
			2	Control Network	Static	Enabled	Enabled							
Port to VLAN								Г						
Port VLAN Membership									Edit VLAN					×
VLAN Translation									VLAN ID:	1 ~				
Private VLAN Settings									VLAN Name:	Dante Network	(13/32 chara	acters use	d)	
GV/PP Settings									VLAN Interface State:	G Enable				
Contr Settings									Link Status SNMP Traps	: 장 Enable				
VLAN Groups														
Voice VLAN														
Access Port Multicast     TV VLAN														
Customer Port Multicast TV VI AN													Apply	Close

To go back and add a name the first VLAN:

- 2) Check the box for the first VLAN and click the  $\square$  icon to edit.
  - a. Update the VLAN Name. In this example, use Dante Network.
  - b. Click Apply.

CBS350-8FP-2G - switchd96e25	× +								- 0
C A Not secure   192.1	168.1.2/cse	34a324d/cbs	/home.htm#						A 😘 🗲 🕀 😩
Status and Statistics	•	cisco	CBS350-8FP-2G -	switchd96			Q	admin English	<ul><li>Advanced &lt; (2) (1)</li></ul>
Administration	VLAN	∖ Settin	igs						
Port Management									
Smartport	VLAN	Table							
<ul> <li>VLAN Management</li> </ul>	+	Ø 🖻							
VLAN Settings		VLAN ID	VLAN Name	Originators	VLAN Interface State	Link Status SNMP Traps			
Interface Settings	0	1	Dante Network	Default	Enabled	Enabled			
Port to VI AN		2	Control Network	Static	Enabled	Enabled			
Port VLAN Membership									
VLAN Translation									
Private VLAN Settings									
GVRP Settings									
VLAN Groups									
Voice VLAN									
Access Port Multicast     TV VLAN									
Customer Port Multicast TV VI AN									



#### 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.

CBS350-8FP-2G - switchd96e25	× +						- 0	> ×
← C ▲ Not secure   192.	168.1.2/cse34a324d/cb	;/home.htm					A 16 19 🖲	
Status and Statistics	es cisco	CBS350-8FP-20	3 - switchd96		Q	admin English	<ul> <li>Advanced &lt; 🕜</li> </ul>	0 🕩
Administration	Port to VLA	N					Apply Car	ncel
Port Management	VI AN Members	hin Table						
Smartport								
✓ VLAN Management	Filter: VLAN I	equals to 1	r Dart w	Go				
VLAN Settings	AND //	tenace type eq	uais to Port *	60				
Interface Settings	GE1	Access	Untagged ~	PVID				- 1
Port to VLAN	GE2	Access	Untagged v					
Port VLAN Membership	GE3	Access	Untagged v					
	GE4	Access	Untagged v	5				
VLAN Translation	GE5	Access	Untagged ~	<b>`</b>				
Private VLAN Settings	GE6	Access	Untagged 👻	<b></b>				
C)/DD Cattings	GE7	Access	Untagged v	<b></b>				
GVRP Settings	GE8	Access	Untagged 👻	<b></b>				
VLAN Groups	GE9	Access	Untagged v	5				
Voice VLAN	GE10	Access	Untagged ~					
<ul> <li>Access Port Multicast TV VLAN</li> </ul>								
Customer Port								

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:

CBS350-8FP-2G - switchd96e25 :	× +												-	0	×
← C ▲ Not secure   192.1	68.1.2/cse34a324d/cbs/h	ome.htm								A∌ .	ô	£^≡	ŵ		
Status and Statistics	S cisco	3S350-8FP-2G	- switchd96			Q	🖹 a	dmin 🗌	English	~	Adva	inced	- 3	0	•
Administration	Port to VLAN											Apply		Cancel	
Port Management															
Smartport	Success. To per	manently save	the configuration, go	o to the File Operatio	ns page or click the S	Save icon									
✓ VLAN Management	VLAN Membership	Table													
VLAN Settings															
Interface Settings	Filter: VLAN ID	equals to 2 ~													
Port to VLAN	AND Inte	<i>rface Type</i> equ	als to Port ~	Go											
Port VLAN Membership	GE1	VLAN Mode	Membership Type	PVID											
VLAN Translation	GE2	Access	Excluded ~												
Private VLAN Settings	GE3	Access	Excluded ~												
	GE4	Access	Excluded ~												
GVRP Settings	GE5	Access	Excluded ~												
VLAN Groups	GE6	Access	Untagged ~												
Voice VLAN	GE7	Access	Untagged 👻												
	GE8	Access	Untagged v	1. Alian and a second s											
<ul> <li>Access Port Multicast TV VLAN</li> </ul>	GE9	Access	Excluded ~												
	GE10	Access	Excluded ~												
<ul> <li>Customer Port Multicast TV VLAN</li> </ul>															-



## 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:

CBS350-8FP-2G - switchd96e25	x +
← C ▲ Not secure   192	1681.2/cas343244/cbg/home.htm# A 🙃 🎓 😨 …
Administration	G t∐tu∐t C8S350-8FP-2G - switchd96 Q admin English ✓ Advanced ✓ Ø () ()
Port Management	Interface Settings Edit Interface Settings ×
Smartport     VLAN Management     VLAN Settings     Interface Settings     Port to VLAN     Port VLAN Membership     VLAN Translation	Global Ethertype Targing: © Dot1 q - 8100       Imerace:       @ Port @E - OLd 1         O Dot1 al - 88a8       3100       Switchport Mode:       @ Layr 3         0 3100       3200       Imerace:       @ Layr 3         Interface Settings Table       @ Lue Global Seting (Dot1a)       @ Dot1al - 88a8         @ Interface Settings Table       @ Lue Global Seting (Dot1a)       @ Dot1al - 88a8         @ Interface Settings Table       @ Dot1al - 88a8       @ Dot1al - 88a8         @ Interface Settings Table       @ Dot1al - 88a8       @ Dot1al - 88a8         @ Interface Settings Table       @ Dot1al - 88a8       @ Dot1al - 88a8         @ Interface Settings Table       @ Dot1al - 88a8       @ Dot1al - 88a8         @ Interface Settings Table       @ Anno Unsugado Doty       @ Anno Unsugado Doty
Private VLAN Settings	Interface Entry No. Interface Switchport Mode VLAN Mode Primary VLAN: None
GVRP Settings	O 1 GE1 Layer 2 Access Secondary VLAN - Host:
VLAN Groups	O         2         GE2         Layer 2         Access         Available Secondary VLANe:         Selected Secondary VLANe:           O         3         GE3         Layer 2         Access         Access
Voice VLAN	O 4 GE4 Layer 2 Access
Access Port Multicast     TV VLAN	O         5         GE5         Layer 2         Access           O         6         GE6         Layer 2         Access           O         7         GE7         Layer 2         Access
<ul> <li>Customer Port Multicast TV VLAN</li> </ul>	O 8 GEB Layer 2 Access Dot1q - 8100 (Global) N/A N/A
Spanning Tree	Image: Product of the state of the

- 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:*

	the CBS350-8FP-2G - switchd96e25	× +												-	0	×
←	C A Not secure   192.	.168.1.2/cse3	34a324d/cbs/	home.htm#							A <sup>s,</sup>	ŵ	£j≡	œ	۲	
		<b>B</b>	cisco	BS350-8FP	-2G - switchd96			Q	🖹 adm	English	~	Adva	inced	~ 3	) ()	۲
	Getting Started	Interf	face Se	ttings									Apply		Cancel	
	Dashboard	Global E	thertype Tag	ging: 💿 Da	t1a - 8100											
	Configuration Wizards			O Do	t1ad - 88a8											
	Search			0 92	00											
•	Status and Statistics															
•	Administration	Intert	ace Settings	Table												-
•	Port Management	6	] 🖉													
►	Smartport	Filte	er: Interfac	e <i>Type</i> equa	als to Port ~	Зо										
•	VLAN Management		Entry No.	Interface	Switchport Mode	Interface VLAN Mode	Ethertype Tagging	Frame Type	Ingress Filtering	Primary VLAN	Secondar	y VLAN	s			
	VLAN Settings	0	1	GE1	Layer 2	Access	Dot1q - 8100 (Global)	N/A	N/A							
		0	2	GE2	Layer 2	Access	Dot1q - 8100 (Global)	N/A	N/A							
	Interface Settings	0	3	GE3	Layer 2	Access	Dot1q - 8100 (Global)	N/A	N/A							
	Port to VLAN	0	4	GE4	Layer 2	Access	Dot1q - 8100 (Global)	N/A	N/A							
		0	5	GE5	Layer 2	Access	Dot1q - 8100 (Global)	N/A	N/A							
	Port VLAN Membership	0	6	GE6	Layer 2	Access	Dot1q - 8100 (Global)	N/A	N/A							
	VLAN Translation		/	GE/	Layer 2	Access	Dot1q - 8100 (Global)	N/A	N/A							
			0	GEO	Layer 2	Trunk	Dottig = 8100 (Global)	N/A	N/A							
	Private VLAN Settings	0	10	GE10	Laver 2	Trunk	Dot1g - 8100 (Global)	N/A	N/A							
	GVRP Settings						2									



## **Confirming Trunk Assignments**

	CBS350-8FP-2G - switchd96e25 ×	4								-		×
$\leftarrow$	C A Not secure   192.16	58.1.2/cse3	4a324d/cbs/h	nome.htm#					4" to .	ć= ⊕	۲	
		₿ '	cisco	BS350-8F	P-2G - switchd96		Q	admin English	~ Advanc	ced ~	0	•
	Getting Started	Port \	VLAN M	lembe	rship							
	Dashboard	E Eastai	ddaa mambaab		acced member	U. Unioned member	L Incohine MI AN	D DM/D				
	Configuration Wizards	M - Multi	icast TV VLA	N In-I	nternally used VLAN	G - Guest VLAN	Pp - Private VLAN Primary	Ps - Private VLAN Seconda	ry			
	Search	Port VI	LAN Member	ship Table								
•	Status and Statistics	Jo	in VLAN	Details.								
Þ	Administration	Filte	r; Interface	<i>Type</i> eq	uals to Port ~ G	0						
Þ	Port Management		Interface	Mode	Administrative VLANs	Operational VLANs	LAG					
•	Smartport	0	GE1	Access	1U	1U						-
-		0	GE2	Access	10	1U						
Ī	VLAN Management	0	GE3	Access	10	1U						
	VLAN Settings	0	GE4	Access	1U	1U						
		0	GE5	Access	10	10						
	Interface Settings	0	GE6	Access	2U	2U						
	Port to VLAN	0	GE7	Access	2U	2U						_
		0	GE8	Access	2U	2U						
	Port VLAN Membership	0	GE9	Trunk	1U, 2T, 3-4094I	1U, 2T						
	VLAN Translation	0	GE10	Trunk	1U, 2T, 3-4094I	1U, 2T						
	Private VLAN Settings	F - Forbi	dden membe	er T-T	agged member	U - Untagged member	I - Inactive VLAN	P - PVID				
javascri	stvoid(0); Settings	M - Multi	icast TV VLAI	N In - I	nternally used VLAN	G - Guest VLAN	Pp - Private VLAN Primary	Ps - Private VLAN Seconda	у			

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.



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:

CBS350-8FP-2G - switchd96e25	5 x +	- • ×
← C ▲ Not secure   19	22.168.1.2/cse34a324d/cbs/home.htm	A* ta t= Ta 😩 …
Status and Statistics	(111111) CBS350-8FP-2G - switchd96     (15C0	) 🖺 admin English 🗸 Advanced 🗸 🕢 🚯
Administration	LAG Management	Apply Cancel
<ul> <li>Port Management</li> </ul>	Load Balance Algorithm:   MAC Address	
Port Settings	O IP/MAC Address	
Error Recovery Settings	LAG Management Table	
Loopback Detection Settings	C	
<ul> <li>Link Aggregation</li> </ul>	LAG Name LACP Link State Active Member Standby Member	
LAG Management	LAG 1 Link Not Present	Edit LAG Membership ×
LAG Settings	O LAG 2 Link Not Present	-
	O LAG 3 Link Not Present	LAG: 1 -
LAUP	O LAG 4 Link Not Present	LAG Name: To Center of Star (17/64 characters used)
► UDLD	LAG 5     Link Not Present	LACP: Grable
▶ PoE	LAG 7     Link Not Present	
	O LAG 8 Link Not Present	Port List: LAG Members:
Green Ethernet		GE3 GE9
Smartport		GE5 GE10
		GE6
VLAN Management		GE7
Spanning Tree		GE8
MAC Address Tables		Appy Close

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.

CBS350-8FP-2G - switchd96e25	× +											-		×
← C ▲ Not secure   192.	.168.1.2/cse34a324d/cb	s/home.htr	n#								A% 50	ć= G	۲	
Status and Statistics	🕃 uludu cisco	CBS350-	3FP-2G - switchd96				۹	🖺 admir	English		~ Advar	nced 🗸	9 0	۲
Administration	Port Setting	IS										Apply	Cance	я
✓ Port Management		~ .												
Port Settings	Jumbo Frames:	Enat	ile Ile											
Error Recovery Settings	Jumbo frames conf	iguration c	hanges will take effe	ct after saving the cor	figuration and re	booting th	e switch							
Loopback Detection Settings	Port Settings Tab	le												
Link Aggregation	tè <i>C</i>					Time Ran	ige							
► UDLD	Entry No	. Port	Port Type	Operational Status	Link Status SNMP Traps	Name	State	Port Speed	Duplex Mode	LAG	Protection State			
▶ PoE	0 1	GE1	1000M-Copper	Up	Enabled			1000M	Full		Unprotected			
	0 2	GE2	1000M-Copper	Down	Enabled						Unprotected			
<ul> <li>Green Ethernet</li> </ul>	0 3	GE3	1000M-Copper	Down	Enabled						Unprotected			
Smartport	0 4	GE4	1000M-Copper	Down	Enabled						Unprotected			
	0 5	GE5	1000M-Copper	Down	Enabled						Unprotected			
VLAN Management	0 6	GE6	1000M-Copper	Down	Enabled						Unprotected			
Spanning Tree	0 7	GE7	1000M-Copper	Down	Enabled						Unprotected			
	0 8	GE8	1000M-Copper	Down	Enabled						Unprotected			
MAC Address Tables	0 9	GE9	1000M-ComboC	Down	Enabled					1	Unprotected			
Multicast	0 10	GE10	1000M-ComboC	Down	Enabled				/	1	Unprotected			
IPv4 Configuration														



## 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 <u>https://audinate.com/certify</u>.



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 (Cont	rol)		1 - U (Da 2 - T (Co	inte) ntrol)
Туре	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.

CBS350-8FP-2G - switchd96e25	× +					- o ×
← C ▲ Not secure   192	2.168.1.2/cse34a324d/cbs/home.ht	n#				A to to 🕲 …
Status and Statistics	CISCO CBS350-	8FP-2G - switchd96		Q	admin English	✓ Advanced ✓ ? ?
Administration	Properties				Apply	Cancel Reset Energy Saving Counter
<ul> <li>Port Management</li> <li>Port Settings</li> </ul>	For the functions and/or para you may have to configure the	meters configured on this page to b a corresponding port based parame	become effective, eters on Port Settings page.			
Error Recovery Settings	Energy Detect Mode: Short Reach:	Enable     Enable				
Loopback Detection Settings	Port LEDs:	C Enable				
Link Aggregation	802.3 Energy Efficient Ethern	at (EEE): Lable				
► UDLD			l			
▶ PoE						
<ul> <li>Green Ethernet</li> </ul>						
Properties						
Port Settings						
Smartport						
VLAN Management						
Spanning Tree						
MAC Address Tables						

- 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.

Туре	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

Dante DSCP Classes

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:

CBS350-8FP-2G - switchd96e25	+		- 0	×
← C ▲ Not secure   192.10	8.1.2/cse34a324d/cbs/home.htm#	A <sup>N</sup> t <b>∂</b> t <sup>⊆</sup>	۵	
Access Control	S 111111 CBS350-8FP-2G - switchd96 Q admin English	~ Advanced ~	00	۲
<ul> <li>Quality of Service</li> <li>General</li> </ul>	QoS Properties	Apply	Cancel	
QoS Properties Queue	QoS Mode: O Disable O Basic I Advanced			
CoS/802.1p to Queue	Interface CoS Configuration Table			
DSCP to Queue	Pan Restore CoS Defaulte			-
Bandwidth				
Egress Shaping Per Queue	Filter: Interface Type equals to Port - Go			
VLAN Ingress Rate Limit	Entry No. Interface Default CoS			
iSCSI	D 1 GE1 0			

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

- a. Select the **Advanced** radio button for QoS Mode.
- b. Click Apply.

CBS350-8FP-2G - switchd96e25	× +								-	0	×
← C ▲ Not secure   192.	168.1.2/cse34a3	24d/cbs/home.ht	tm#					A∥ 20 <b>0 20</b> ≣	<u>ب</u>		
Access Control	ili cıs	cBS350-	-8FP-2G	- switchd96		Q	admin English	<ul> <li>Advanced </li> </ul>	•	0	•
<ul> <li>Quality of Service</li> </ul>	Queue							Apply	Ca	ncel	
		-									
QoS Properties	Queue	Scheduling Me	ethod								
Queue	Queue	Strict Priority	WRR	WRR Weight	% of WRR Bandwidth						
CoS/802.1p to Queue	1	۲	0	1							
DSCP to Queue	2	۲	0	2							
Bandwidth	3	۲	0	4							
Egress Shaping Per Queue	4	۲	0	8							
VLAN Ingress Rate Limit	5	۲	0	16							
iSCSI	6	۲	0	32							
TCP Congestion Avoidance	7	۲	0	64							
	8	۲	0	128							
Global Settings	Queue 1 has	the lowest prior	ity, queu	e 8 has the highest priority.							

#### 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.

CBS350-8FP-2G - switchd96e25	( +							- 0 ×					
← C ▲ Not secure   192.16	58.1.2/cse34a324d/cbs/h	ome.htm#					A* 20	순 🕀 😩 …					
Security	CISCO	3S350-8FP-2G - swi	tchd96		Q	admin English	~ Ad	vanced - 😯 🕄 🕩					
Access Control							Analys Com	Desters Defaults					
<ul> <li>Quality of Service</li> </ul>	DSCP to Que	eue					Can	Restore Derauits					
✓ General DSCP to Queue Table													
QoS Properties	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue					
Queue	0 (BE)	1 -	16 (CS2)	1 -	32 (CS4)	1 ~	48 (CS6)	1 ~					
CoS/802.1p to	1	1 -	17	1 -	33	1 ~	49	1 ~					
Queue	2	1 -	18 (AF21)	1 🛩	34 (AF41)	1 ~	50	1 ~					
DSCP to Queue	3	1 ~	19	1 ~	35	1 ~	51	1 ~					
Bandwidth	4	1 ~	20 (AF22)	1 ~	36 (AF42)	1 ~	52	1 ~					
Egress Shaping Per Oueue	5	1 ~	21	1 -	37	1 -	53	1 ~					
VI AN Incress Rate	6	1 ~	22 (AF23)	1 ~	38 (AF43)	1 ~	54	1~					
Limit	7	1~	23	1 -	39	1 ~	55	1 ~					
iSCSI	8 (CS1)	6~		1 ~	40 (CS5)	1 ~	56 (CS7)	8~					
TCP Congestion	9	1~		1 ~	41	1 ~	57	1~					
Avoidance	10 (AF11)	1 -	26 (AF31)	1 -	42	1 ~	58	1~					
<ul> <li>QoS Basic Mode</li> </ul>	11	1 ~	27	1 ~	43	1 ~	59	1 ~					
Global Settings	12 (AF12)	1 ~	28 (AF32)	1 🛩	44	1 ~	60	1 ~					
Interface Settings	13	1 ~	29	1 ~	45	1~	61	1 ~					
OoS Advanced Mode	14 (AF13)	1 ~	30 (AF33)	1 ~	46 (EF)	7 ~		1 ~					
<ul> <li>QoS Statistics</li> </ul>	15	1 -	31	1 -	47	1~		1~					
► SNMP	Queue 1 has the lowe	st priority, queue 8 ha	is 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.
- 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

	the CBS350+8FP+2G - switchd96e25	× +					-		×
$\leftarrow$	C A Not secure   192	.168.1.2/cse34a324d/cbs/h	ome.htm#			A™ 56 51≣	œ		
•	Multicast	G cisco	IS350-8FP-2G - switchd96	Q	admin English	~ Advanced	~ (	0	•
	IPv4 Configuration	Global Setting	as		DSCP C	Iverride Table Ap	ply	Cancel	
Þ	IPv6 Configuration		-						
Þ	General IP Configuration	Trust Mode:	<ul> <li>CoS/802.1p</li> <li>DSCP</li> </ul>						
	Security	Default Mode Status:	Cos/802.1p-DSCP     Trusted						
Þ	Access Control		O Not Trusted						
	Quality of Service	Override Ingress DSCF	: 🗍 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.

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.

🗉 🗲 🖬 🗲 🛛	fi 🖾 🖽 🤇	۵ ۵			Primary Le	ader Clock: Y	000-FoH-Yamaha-	TF3			0
Routing Device Info Clock	Status Network St	atus Events									
Device Name	Subscription Status	Primary Status	Secondary Status	Primary Tx B/W	Secondary Tx B/W	Primary Rx B/W	Secondary Rx B/W	Latency Setting	Latency Status	Packet	
Amp-LobbyAndRestroom		100Mbps	N/A	< 1 Mbps		< 1 Mbps		1 msec			-
Amp-ParkingLot		100Mbps	N/A	< 1 Mbps	}	< 1 Mbps		1 msec			
Auditorium-Lectern-Mic		100Mbps	N/A	< 1 Mbps		< 1 Mbps		1 msec			
DanteAV-Rx		1Gbps	N/A	< 1 Mbps		< 1 Mbps		1 msec			
DanteAV-Tx		1Gbps	N/A	< 1 Mbps		< 1 Mbps		1 msec			
FOH-DAW		1Gbps	N/A	< 1 Mbps		< 1 Mbps		1 msec			
Mon-Mackie-DL32R		1Gbps	N/A	< 1 Mbps		< 1 Mbps		1 msec			
Y000-FoH-Yamaha-TF3		1Gbps	N/A	< 1 Mbps		< 1 Mbps		1 msec			
Y001-StageBox-StageLeft		1Gbps	N/A	< 1 Mbps		< 1 Mbps		1 msec			
Y002-StageBox-StageRight		1Gbps	N/A	< 1 Mbps		< 1 Mbps		1 msec			

• 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.



🗋 😏 🖬 🚖 🌡	fi 🖾 🕀 🖇	۵ 🚷			Primary Le	ader Clock: Y	000-FoH-Yamaha-	TF3			0
Routing Device Info Clock	Status Network St	tatus Events									
Device Name	Subscription Status	Primary Status	Secondary Status	Primary Tx B/W	Secondary Tx B/W	Primary Rx B/W	Secondary Rx B/W	Latency Setting	Latency Status	Packet Errors	
Amp-LobbyAndRestroom		100Mbps	N/A	< 1 Mbps		< 1 Mbps		1 msec			^
Amp-ParkingLot		100Mbps	N/A	< 1 Mbps		< 1 Mbps		1 msec			
Auditorium-Lectern-Mic		100Mbps	N/A	< 1 Mbps		< 1 Mbps		1 msec			
DanteAV-Rx		1Gbps	N/A	< 1 Mbps		< 1 Mbps		1 msec			
DanteAV-Tx		1Gbps	N/A	< 1 Mbps		< 1 Mbps		1 msec			
FOH-DAW	0	1Gbps	N/A	< 1 Mbps		23 Mbps		1 msec			
Mon-Mackie-DL32R	0	1Gbps	N/A	< 1 Mbps		23 Mbps		1 msec			
Y000-FoH-Yamaha-TF3	0	1Gbps	N/A	< 1 Mbps		23 Mbps		1 msec			
Y001-StageBox-StageLeft		1Gbps	N/A	71 Mbps		< 1 Mbps		1 msec			
Y002-StageBox-StageRight		1Gbps	N/A	< 1 Mbps		< 1 Mbps		1 msec			

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.

] 😏 💼 🚖	🚠 🔛 🗄 🕯	۵ ۵			Primary Le	ader Clock: Y	000-FoH-Yamaha-	TF3		
outing Device Info Cloc	k Status Network St	atus Events								
Device A	Subscription Status	Primary Status	Secondary Status	Primary Tx B/W	Secondary Tx B/W	Primary Rx B/W	Secondary Rx B/W	Latency Setting	Latency Status	Packet
Amp-LobbyAndRestroom		100Mbps	N/A	< 1 Mbps		22 Mbps		1 msec		
Amp-ParkingLot		100Mbps	N/A	< 1 Mbps		22 Mbps		1 msec		
Auditorium-Lectern-Mic		100Mbps	N/A	< 1 Mbps		22 Mbps		1 msec		
DanteAV-Rx		1Gbps	N/A	< 1 Mbps		21 Mbps		1 msec		
DanteAV-Tx		1Gbps	N/A	< 1 Mbps		21 Mbps		1 msec		
OH-DAW	<b>S</b>	1Gbps	N/A	< 1 Mbps		21 Mbps		1 msec		
Ion-Madvie-DL32R	<b>O</b>	1Gbps	N/A	< 1 Mbps		21 Mbps		1 msec		
(000-FoH-Yamaha-TF3	0	1Gbps	N/A	< 1 Mbps		21 Mbps		1 msec		
(001-StageBox-StageLeft		1Gbps	N/A	21 Mbps		< 1 Mbps		1 msec		
Y002-StageBox-StageRigh	t	1Gbps	N/A	< 1 Mbps-0		21 Mbps		1 msec		

€ 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.



**④** 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.

🗋 🕗 🖬 🔺 🖁	5 🖾 🕀 🤇	۵ ۵			Primary Le	eader Clock: Y	000-FoH-Yamaha-	TF3			0
Routing Device Info Clock	Status Network St	tatus Events									
Device Name	Subscription Status	Primary Status	Secondary Status	Primary Tx B/W	Secondary Tx B/W	Primary Rx B/W	Secondary Rx B/W	Latency Setting	Latency Status	Packet Errors	
Amp-LobbyAndRestroom		100Mbps	N/A	< 1 Mbps		< 1 Mbps		1 msec			-
Amp-ParkingLot		100Mbps	N/A	< 1 Mbps		< 1 Mbps		1 msec			
Auditorium-Lectern-Mic		100Mbps	N/A	< 1 Mbps		< 1 Mbps		1 msec			
DanteAV-Rx		1Gbps	N/A	< 1 Mbps		< 1 Mbps		1 msec			
DanteAV-Tx		1Gbps	N/A	103 Mbps	N	< 1 Mbps		1 msec			
FOH-DAW	0	1Gbps	N/A	< 1 Mbps	13	21 Mbps		1 msec			
Mon-Madvie-DL32R	0	1Gbps	N/A	< 1 Mbps		21 Mbps		1 msec			
Y000-FoH-Yamaha-TF3	0	1Gbps	N/A	< 1 Mbps		21 Mbps		1 msec			
Y001-StageBox-StageLeft		1Gbps	N/A	21 Mbps		< 1 Mbps		1 msec			
Y002-StageBox-StageRight		1Gbps	N/A	< 1 Mbps		< 1 Mbps		1 msec			

• 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.

**Audinate** 



## 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.

CBS350-8FP-2G - switchd96e25	× +			- o ×
← C ▲ Not secure   192	.168.1.2/cse34a324d/cbs/home.htm	#		A to to 🕲
Spanning Tree	CISCO CBS350-8	FP-2G - switchd96e25	Q admin English	Advanced ~ ? 1
MAC Address Tables	Properties		Apply	Cancel Reset Energy Saving Counter
<ul> <li>Multicast</li> <li>Properties</li> </ul>	Bridge Multicast Filtering Status	s: 🕑 Enable		
MAC Group Address	VLAN ID: Forwarding Method for IPv6:	1 → ● MAC Group Address		
IP Multicast Group Address		IP Group Address     Source Specific IP Group Address		
<ul> <li>IPv4 Multicast Configuration</li> </ul>	Forwarding Method for IPv4:	<ul> <li>MAC Group Address</li> <li>IP Group Address</li> <li>Source Specific IP Group Address</li> </ul>		
<ul> <li>IPv6 Multicast Configuration</li> </ul>				
IGMP/MLD Snooping IP Multicast Group				
Multicast Router Port				
Forward All				
Unregistered Multicast				
IPv4 Configuration				

- 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)

	the CBS350+8FP-2G - switchd96e25	× +										-		×
$\leftarrow$	C A Not secure   192.	168.1.2/cse3	34a324d/cbs/l	nome.htm#							A٩ ۲	° t≓ @		
•	Spanning Tree	<b>B</b>	iliiilii c cisco	BS350-8FP	-2G - switchd96				Q ad	min English	~	Advanced 🖌	00	•
•	MAC Address Tables	IGMF	Snoop	ing						Apply Canc	el IGMP S	nooping IP Multic	ast Group	
·	Multicast Properties MAC Group Address	IGMP Sn IGMP Sn IGMP Qu	looping is onl looping Statu Jerier Status:	y operationa <sup>3:</sup> 🕑 Enabl 🕑 Enabl	al when Brid	uticast Eiltering	is enabled. Bridg	ge Multicast Fi	Itering is currently	enabled.				
	IP Multicast Group Address	IGMP	Snooping Tal	ble										
	<ul> <li>IPv4 Multicast Configuration</li> </ul>	2												
	IGMP Snooping				IGMP Snooping	Status	MRouter Ports	Immediate	l ast Member	IGMP Querier S	itatus	IGMP Querier	IGMP OI	erier
	IGMP Interface		Entry No.	VLAN ID	Administrative	Operational	Auto Learn	Leave	Query Counter	Administrative	Operational	Election	Version	
	Settings	0	1	1	Disabled	Disabled	Enabled	Disabled	0	Disabled	Disabled	Enabled	v2	
	IGMP VLAN Settings	0	2	2	Disabled	Disabled	Enabled	Disabled	0	Disabled	Disabled	Enabled	v2	
	IGMP Proxy													
	<ul> <li>IPv6 Multicast Configuration</li> </ul>													
	IGMP/MLD Snooping IP Multicast Group													
	Multicast Router Port													

- 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

CBS350-8FP-2G - switchd96e25	× +	0 hter#						- 0 X	
Spanning Tree	(1100.1.2/cses4asz4d/cos/ cisco	CBS350-8FP-2G - switchds	6e25			Q	admin English	A <sup>+</sup> 1₀ 1= ₩ 3 m Advanced ~ ? ? () ()	
MAC Address Tables	IGMP Snoop	ping					Apply Cancel	IGMP Snooping IP Multicast Group	
Multicast     Properties     MAC Group Address	IGMP Snooping is on IGMP Snooping Statu	lly operational when Bridge JS: G Enable	Multicast Filterin	g is enabled. Bridg	ge Multicast Filter	Edit IGMP Snot	oping Settings		×
IP Multicast Group Address	IGMP Querier Status:	: 🖌 Enable				VLAN ID: IGMP Snooping Status:	1 v i Enable		
<ul> <li>IPv4 Multicast Configuration</li> </ul>	<b>C</b>					MRouter Ports Auto Learn: Immediate Leave:	Enable     Enable     Enable		
IGMP Snooping	Entry No.	IGMP Snoopi VLAN ID Administrative	ng Status Operational	MRouter Ports Auto Learn	Immediate L Leave C	a case member query counter	User Defined	(Range: 1 - 7)	
Settings IGMP VLAN Settings	<ul> <li>1</li> <li>2</li> </ul>	1 Disabled 2 Disabled	Disabled Disabled	Enabled Enabled	Disabled 0 Disabled 0	IGMP Querier Status: IGMP Querier Election:	✓ Enable ✓ Enable		
IGMP Proxy IPv6 Multicast Configuration						IGMP Querier Version: Querier Source IP Address:	<ul> <li>v2</li> <li>v3</li> <li>Auto</li> </ul>		
IGMP/MLD Snooping IP Multicast Group							O User Defined 192.168.1.2		
Multicast Router Port									Apply Close

- 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  $\square$  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: O Use Query Robustness (2) O 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	Note:
b.	IGMP Querier Election:	🗹 Enabled	In Chapter 5, we will configure a DHCP server which will issue an address for our
c.	IGMP Querier Version:	O v2 ⊙ v3	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
d.	Querier Source IP Address:	<ul><li>Auto</li><li>O User Defined</li></ul>	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

CBS350-8FP-2G - switchd96e25	× +								- • ×
← C ▲ Not secure   19	2.168.1.2/cse	e34a324d/o	bs/home.htm#						A to to 🕲
Spanning Tree	€	cisco	CBS350-8FP-2G -	switchd96e25			O	admin English	✓ Advanced ✓ <i> <i> <i> <i> <i> <i> <i> <i> <i> <i></i></i></i></i></i></i></i></i></i></i>
MAC Address Tables	IGM	IP VLA	V Settings						
<ul> <li>Multicast</li> </ul>									
Properties	IGM	P Settings	able				Edit IGMP Settin	ngs	х
MAC Group Address									
IP Multicast Group		Entry N	o. Interface Name	Router IGMP Version	Query Robustness	Query Interval (sec)	Interface Name:	VLAN 1 ~	
Address	۲	) 1	VLAN 1	v3	2	125	Router IGMP Version	O v1	
<ul> <li>IPv4 Multicast Configuration</li> </ul>	0	2	VLAN 2	v3	2	125		<ul> <li>∨2</li> <li>• v3</li> </ul>	
IGMP Snooping							Query Robustness:	2	(Range: 1 - 7, Default: 2)
IGMP Interface Settings							Query Interval:	30	nge: 30 - 18000, Default: 125)
IGMP VLAN Settings							Query Max Response Interval:	10	see (nahge: 5 - 20, Default: 10)
IGMP Proxy							• Last Member Query Interval:	1000	mS (Range: 100 - 25500 in multiples of 100, Default: 1000)
<ul> <li>IPv6 Multicast Configuration</li> </ul>							• Multicast TTL Threshold:	0	Hops (Range: 0 - 256, Default: 0)
IGMP/MLD Snooping IP Multicast Group									
Multicast Router Port									Apply Close

- 1) Open Multicast > IPv4 Multicast Configuration > IGMP VLAN Settings.
- 2) Check the box to select a the VLAN with Dante traffic and click the  $\square$  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:	O v1 O 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**

CBS350-8FP-2G - switchd96e25	× +		- o ×
← C ▲ Not secure   19	2.168.1.2/cse34a324d/cbs/home.htm#		A to to to 🗈
Spanning Tree	CISCO CBS350-8FP-2G - switchd96e25	Q 💾 admin English	✓ Advanced ✓ ? () ►
MAC Address Tables	Forward All		Apply Cancel
<ul> <li>Multicast</li> </ul>			
Properties	Filter: VLAN ID equals to 1 ~ AND Interface Type equals to Port ~ Go		
MAC Group Address	Port         GE1         GE2         E6         GE7         GE8         GE9         GE10           Static         Image: Comparison of the state		
IP Multicast Group Address	Forbidden O O O O O O O O O O O O O O O O O O O		
<ul> <li>IPv4 Multicast Configuration</li> </ul>			
<ul> <li>IPv6 Multicast Configuration</li> </ul>			
IGMP/MLD Snooping IP Multicast Group			
Multicast Router Port			
Forward All			
Unregistered Multicast			
IPv4 Configuration			

- 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

Туре	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.



CBS350-8FP-2G - switchd96e25	x +	- 0 X
← C ▲ Not secure   192	168.1.2/cse34a324d/cbs/home.htm#	A* 16 12 ····
Administration     Port Management	CBS350-8FP-2G - switchd96e25	Q 🖺 asam English v Advanced v 🔗 🚯 🚱
Smartport	IP Multicast Group Address	
VLAN Management	The Bridge Multicast Filtering is currently enabled.	Multicast Interface Settings ×
Spanning Tree	For IP Multicast Configuration to be effective, the Bridge Multicast Filtering must be enab	
• • • • • • • • •	IP Multicast Group Address Table VL/	IN ID: 1
MAC Address Tables	(P)	Version: Version 4
✓ Multicast	P Details IP ! Soi	Julticast Group Address: 224.0.1.129 arce IP Address:  *
Properties	Filter: D VLAN ID equals to (Range: 1 - 4094	
MAC Group Address	IP Version equals to Version 4	<i>x: Interface Type</i> equals to Port → Go
IP Multicast Group	IP Multicast Group Address equals to	adama 051 052 053 054 055 057 059 050 0510
Address	Source IP Address equals to Go Stu	
IPv4 Multicast	Dy	namic 💿 💿 💿 💿 💿 💿
Conliguration	VLAN ID IP Multicast Group Address Source IP Address	
IPv6 Multicast	✓         1         224.0.1.129         ×	
Configuration		
IGMP/MLD Snooping IP		
Multicast Group	1 f02-1-ff49-6e25 *	
Multicast Router Port	0 1 m02.11.005/02/0	Apply Close

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.

Add IP Multicas	Add IP Multicast Group Address						
• VLAN ID:	1	(Range: 1 - 4094)					
IP Version:	O Version 6   Version 4						
• IP Multicast Group Address:	224.0.0.251						
Source Specific:	Include						
☆ Source IP Address:							
			Apply Close				

- 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 <u>https://audinate.com/certify</u>.

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

Switch Example Design

#### Exercise VLANs, Subnet Assignments and Static IPs

VLAN	Subnet	Static IPs	
1 - Dante Subnet 1	192.168.1.0 /24	192.168.1.1	Router, Switch Management Address
		192.168.1.2	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	Internet Router
		192.168.0.2	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.
- 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.

-	. CBS350-8EP-2G - switchd96e25	× +											_	0	×
4		102 1 2/0002	4-334d/obc/k	ma htm#							~ ~	~	G		
~	A Not secure 1 132.1	168.1.2/CSep	483240/005/1	iome.num							4" λ <b>ο</b>	λ=	۳		
	Dashboard	B '	cisco	BS350-8FI	P-2G - switchd		Q	💾 admin	English		~ Ad	vanced	~ ?	0	•
	Configuration Wizards	Port	VLAN M	lembe	rship										
	Search														
•	Status and Statistics	F - Forbi M - Multi	dden membe icast TV VLAf	er T – Ta N In – Ir	agged member U - Un Internally used VLAN G - G	ntagged member uest VLAN	I - Inactive \ Pp - Private	VLAN VLAN Prima	P - PV ary Ps - Pr	'ID rivate VLAI	N Second	ary			
•	Administration	Port VI	LAN Member	ship Table											
Þ	Port Management	Jo	oin VLAN	Details.											
	Constant														
►	Smartport														
•	VLAN Management	Filte	r: Interface	<i>Type</i> equ	als to Port - Go	Operational VLAN	Ns LAG								
•	VLAN Management VLAN Settings	Filte	er: Interface Interface GE1	<i>Type</i> equ Mode Access	Administrative VLANs	Operational VLAN	Ns LAG								
•	VLAN Management VLAN Settings Interface Settings	Filte	er: Interface Interface GE1 GE2	Mode Access Access	Administrative VLANs 1U 1U	Operational VLAN	Ns LAG								
•	VLAN Management VLAN Settings Interface Settings	Filte	r: Interface Interface GE1 GE2 GE3	Mode Access Access Access	Administrative VLANs U U U U U U	Operational VLAN 1U 1U 1U	Ns LAG								
•	VLAN Management VLAN Settings Interface Settings Port to VLAN	Filte	er: Interface Interface GE1 GE2 GE3 GE4	Mode Access Access Access Access	Administrative VLANs Co U U U U U U U U U U U U U U U U U U	Operational VLAM           1U           1U           1U           1U           1U           1U	√s LAG								
•	VLAN Management VLAN Settings Interface Settings Port to VLAN Port VLAN Membership	Filte	er: Interface Interface GE1 GE2 GE3 GE4 GE5	Mode Access Access Access Access Access Access	Administrative VLANs 1U 1U 1U 1U 1U 1U 1U 1	Operational VLAM           1U           1U           1U           1U           1U           1U           1U           1U           1U	NS LAG								
•	VLAN Management VLAN Settings Interface Settings Port to VLAN Port VLAN Membership	Filte 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Interface GE1 GE2 GE3 GE4 GE5 GE6	Mode Access Access Access Access Access Access	Administrative VLANs Co Administrative VLANs U U U U U U U U 2U	Operational VLAN           1U           1U           1U           1U           1U           2U	Ns LAG								
•	VLAN Management VLAN Settings Interface Settings Port to VLAN Port VLAN Membership VLAN Translation	Filte 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Interface GE1 GE2 GE3 GE4 GE5 GE6 GE7	Mode Access Access Access Access Access Access Access Access	Administrative VLANs Co Administrative VLANs U U U U U U U U 2U 2U 2U	Operational VLAM           1U           1U           1U           1U           2U           2U	√s LAG								
•	VLAN Management VLAN Settings Interface Settings Port to VLAN Port VLAN Membership VLAN Translation Private VLAN Settings	Filte	r: Interface [Interface GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8	Access Access Access Access Access Access Access Access Access	Administrative VLANs Co Administrative VLANs U U U U U U U U U U U U U U U U U U U	Operational VLAM           1U           1U           1U           2U           2U           9U	Vs LAG								
•	VLAN Management VLAN Settings Interface Settings Port to VLAN Port VLAN Membership ► VLAN Translation Private VLAN Settings	Filte	r: Interface GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8 GE9	Access Access Access Access Access Access Access Access Access Access Access	Administrative VLANs  Control	Operational VLAM           1U           1U           1U           2U           2U           9U	NS LAG								
•	VLAN Management VLAN Settings Interface Settings Port to VLAN Port VLAN Membership VLAN Translation Private VLAN Settings GVRP Settings	Filte	r: Interface [102] [1	Access Access Access Access Access Access Access Access Access Access Access Trunk	Administrative VLANs  Comparison  Comparison Comparison  Comparison  Comparison  Comparison  Comparison  Comparison  Comparison  Comparison  Comparison  Compariso	Operational VLAM           1U           1U           1U           1U           2U           2U           9U	NS LAG								
•	VLAN Management VLAN Settings Interface Settings Port to VLAN Port VLAN Membership VLAN Translation Private VLAN Settings GVRP Settings VLAN Groups	Filte	r: Interface GE1 GE2 GE3 GE4 GE5 GE6 GE6 GE7 GE8 GE9 GE10 dden membe	Access Access Access Access Access Access Access Access Access Trunk Trunk	Balls to         Port         Go           Administrative VLANs         1U           1U         1U           2U         1U           2U         1U           1U, 2T, 3-8I, 9T, 10-4094I         1U, 2T, 3-8I, 9T, 10-4094I           1U, 2T, 3-8I, 9T, 10-4094I         1U, 2T, 3-8I, 9T, 10-4094I	Operational VLAM           1U           1U           1U           1U           2U           2U           9U	NS LAG	VLAN	P - PV	ID					

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 <u>www.audinate.com</u>) 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.

CBS350-8FP-2G - switchd96e2	5 x + - 0	×
← C ▲ Not secure   19	22.168.1.1/cse34a324d/cbs/home.htm A 😘 🎓 😨	
Multicast	CISCO CBS350-BFP-2G - switchd Q 🖺 admin English v Advanced v 🕑 3	) 🕞
IPv4 Configuration	DNS Settings Cance	al
IPv6 Configuration	DNS: Gr Enable	
<ul> <li>General IP Configuration</li> </ul>	Polling Retries:     (Range: 0 - 16, Default: 1)	
<ul> <li>Policy Based Routing</li> </ul>	Polling Timeout:     Sec (Range: 1 - 60, Default: 2)	
Route Maps	Polling Interval:     O Use Default	
Route Map Binding	O User Defined 8 Sec (Ran Add DNS Server	x
Policy Based Routes	Default Parameters	
▼ DNS	IP Version 6 • Version 4	
DNS Settings	Default Domain Name: (0/158 characters used)	
Search List	DHCP Domain Search List: Details	
Host Mapping	ONS Server IP Address: 192.168.0.1	
Security	Preference: 1 -	
	DNS Server Preference Source Interface	
Quality of Service	0 results found.	
► SNMP		Apply Close

- 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

CBS350-8FP-2G - switchd96e25	x + - • ×
← C ▲ Not secure   192	2.168.1.1/cse34a324d/cbs/home.htm# A 🖓 🎓 🔂 🖤
Multicast	
✓ IPv4 Configuration	IPv4 Interface Cancel
IPv4 Interface	IPv4 Routing: 😡 Enable
IPv4 Static Routes IPv4 Forwarding Table	IPv4 Interface Table
► RIPv2	+ 🕫 🗎
Access List	Interface         IP Address Type         IP Address         Mask         Status           VLAN 1         Static         192.168.1.1         255.255.255.0         Valid
ARP	Interface: O Port GE1 O LAG 1 (To Center of Star) O VLAN 2 - O Loopback
ARP Proxy	IP Address Type: O Dynamic IP Address <ul> <li>Static IP Address</li> </ul>
UDP Relay/IP Helper	• IP Address: 192.168.2.1
<ul> <li>DHCP Snooping/Relay</li> </ul>	Mask:     Network Mask
DHCP Server	(institute congress and institute or only)
IPv6 Configuration	
General IP Configuration	Andre Plane
	Appy Udse

- 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 **255.255.0** *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						
+	<b>e</b>					
	Interface	IP Address Type	IP Address	Mask	Status	
	VLAN 9	Static	192.168.0.2	255.255.255.0	Valid	
$\Box$	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.

Command Prompt	-		$\times$
Microsoft Windows [Version 10.0.18363.900] (c) 2019 Microsoft Corporation. All rights r	eserved		ĺ
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 TT	L=64		
Reply from 192.168.2.1: Dytes=32 time=1ms	L=64		
Reply from 192.168.2.1: bytes=32 time=1ms II	L=04		
Reply from 192.168.2.1: bytes=32 time=1ms	L=64		
Ping statistics for 192.168.2.1: Packets: Sent = 4, Received = 4, Lost = Approximate round trip times in milli-second Minimum = 1ms, Maximum = 1ms, Average =	0 (0% 1 s: 1ms	oss),	
C:\Users\patrick>_			

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.									
ODbtain an IP address automatical	O <u>O</u> btain 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 autom	natically								
• Us <u>e</u> the following DNS server add	resses:								
Preferred DNS server:									
Alternate DNS server:									
Vaļidate settings upon exit	Ad <u>v</u> anced								
	OK Cancel								

## 5.4. Assign DHCP Service in VLANs 1 and 2

CBS350-8FP-2G - switchd96e25	+ - 0 X
← C ▲ Not secure   192.16	\$8.1.1/ccs24a324d/cbs/home.htm# A <sup>1</sup> 🏠 😰 💮 🕲 …
<ul> <li>IPv4 Configuration</li> </ul>	8 1 11 1 C88350-8FP-2G - switchd       Q     admin     English     ✓     Advanced     Ø     ●
IPv4 Interface	Network Pools DHCP Server Options
IPv4 Static Routes	
IPv4 Forwarding Table	Network Pool Table
► RIPv2	+ C 🛍 Details Add Network Pool x
Access List	Pool Name Network Mask Address Pool Start Address Pool End Lea entry for the Pool Name Oreite VLW1 Pool (17/02 cherektern sine)
ARP	Dante VLAN I Pool 255.255.255.0 192.168.1.101 192.168.1.254 1d Scene IP Address 102.168.1.0
100.0	Dante VLAN 2 Pool 255 255.255.0 192.168.2.110 192.168.2.254 101 • Mark: O Network Mark 262.052.05.0
ARP Proxy	(6) Pedet Lorge (5 - 50)
UDP Relay/IP Helper	Addess Post Sant 1921681.101
▶ DHCP	Address Pool End: 192 168 1.264
Snooping/Relay	Lasse Durative 🔘 Intera
<ul> <li>DHCP Server</li> </ul>	(8) Days 1 Hours (80~) Minutes (80~) (Instant: 1 Day)
Properties	
Network Pools	Default Router P Address (Option 3)   Anton Default Router P Address (Option 3)  Anton Default Router P Address
Excluded Addresses	U tobe
Static Hosts	
DHCP Ontions	Avr Com

- 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:	O 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:	O Network Mask
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.

Ren

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.

CBS350-8FP-2G - switchd96e25	× +		- • ×	1
← C ▲ Not secure   192.	2.168.1.1/cse34a324d/cbs/home.htm#	A G 🕼 🚇 🔍 …		
Multicast	CISCO CBS350-8FP-2G - switchd96	Q admin English	~ Advanced ~ ? ()	
<ul> <li>IPv4 Configuration</li> </ul>	IPv4 Static Routes			
IPv4 Interface				
IPv4 Static Routes	IPv4 Static Routes Table			
IPv4 Forwarding Table	+ 2 @	Add IPv4 Statio	c Route	×
► RIPv2	Destination IP Prefix Prefix Length Route Type Next Hop Router IF	Destination IP Prefix:	0.0.0.0	
Access List	0.0.0.0 0 Remote 192.168.0.1			
ARP		Mask:	Network Mask     0.0.0.0	
ARP Proxy			O Prefix Length	(Range: 0 - 32)
UDP Relay/IP Helper		Route Type:	O Reject	
▶ DHCP			Remote	
Snooping/Relay		Next Hop Router IP Address	: 192.168.0.1	
DHCP Server		o Metric:	<ul> <li>Use Default</li> </ul>	
IPv6 Configuration			O User Defined	(Range: 1 - 255, Default: 4)
General IP Configuration				
				Apply Close

#### 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.



	RV340 Dual WAN Gigabit VF							-		×
$\leftarrow$	→ Ŭ 🔺 N	☆ 🎽	Ē	۲						
				RV340-route	cisco (a	English 🗸	8	6	•	
() () ()	Getting Started Status and Statistic	s	System Su	mmary						
	System Summary									
	TCP/IP Services		Interface	WAN1	WAN2	USB1	USB2			
	Port Traffic		IP Address	10.0.0.49						
	WAN QoS Statistic	s	Default Gateway	10.0.0.1						
	ARP Table		DNS	75.75.75.75 75.75.76.76						
	Routing Table		Dynamic DNS	Disabled	Disabled	Disabled	Disabled			
	DHCP Bindings		Multi-WAN Status	Online	Offline	Offline	Offline			
	Mobile Network			Release	Renew	(Not Attached)	(Not Attached)			
	View Logs			Renew						
**	Administration									_

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.

	RV340 Dual WAN Gigabit VPN R × +										-		×
$\leftarrow$	$\rightarrow$ $\circlearrowright$ $\bigstar$ Not secure	htt	<del>ps</del> :/	/192.168.1.1	/index.html#	/LAN_VL/	AN_S	ettings		☆ 🏂	Ē	۲	
<b>\</b>	Getting Started	E	ŧ	ıılııılıı cısco	RV340-rou	uter0B74	24	A	💾 cisco (ac	lmin) English 🗸	8	•	•
•	Status and Statistics	VL		N Settin	gs					Apply		Cance	əl
2	Administration												
٠	System Configuration	V	LAN	N Table								^	
۲	WAN		+	<b>ø</b>									
#	LAN					Inter- VLAN	Dev	ice					
	Port Settings		Ø	VLAN ID 🗘	Name	Routing	Mar	agemen	it IPv4 Address/Ma	ask			
	VLAN Settings			1	VLAN1			0	IPv4 Address:	192.168.0.1	/ 2	4	
	LAN/DHCP Settings								Subnet Mask:	255.255.255.0			
	Static DHCP								DHCP Type:	O Disabled			
										• Server			
	802.1X Configuration									O Relay			
	DNS Local Database								Lease Time: 😧	1440	mii	n.	
	Router Advertisement								Range End:	192.168.0.101			
<u>_</u>	Deuties								Hange End.	132.100.0.204			

- 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

	RV340 Dual WAN Gigabit VPN R 🗙 🕂						- 0	×
$\leftarrow$	$\rightarrow$ $\circlearrowright$ $\blacktriangle$ Not secure	https://192.168.0.1	/index.html#/Routing_S	tatic_Routing		☆ 🖆 🖻	È 🔇	
쌸	Administration	🔄	RV340-router0B742	24	cisco (ad	English 🗸 💡	0	•
٠	System Configuration							
۲	WAN	Static Routin	g			Apply	Cancel	
<b>.</b>	LAN							
8	Routing	IPv4 Routes Table	•				^	
	IGMP Proxy	+ 🕜 🏛						
	RIP	Network \$	Mask 🗢	Next Hop 🗢	Metric \$	Interface 🗢		
	Static Routing	□ 192.168.1.0	255.255.255.0	192.168.0.2	1	VLAN1		
	Firewall	□ 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 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.

CBS350-8P-E-2G - switch6fc0	08a × +		-	0	×
	lot secure   192.168.1.1/cs23fc0a43/mts/home.htm	A" Q 10	€ @	<b>(</b>	
	3 111111 C85350-8P-E-2G - switch6fc08a CISCO	Q Audinate English ~	Advanced ~	00	•
Getting Started	CPU Utilization		Apply	Cancel	
Dashboard	<ul> <li>15 sec</li> </ul>				
Configuration Wizards	○ 30 sec ○ 60 sec				
Search	CPU Input Rate: 3 (Frame/sec) Y axis is CPU Utilization in Percentage. X axis is elapsed time (in seconds).				
<ul> <li>Status and Statistics</li> </ul>	100 %				
System Summary	CPU Usage				
CPU Utilization	80 %				
Port Utilization	60 %				
Interface					_
Etherlike	40%				
GVRP					_
802.1x EAP	20.5				
ACL		0			
Hardware Resource Utilization					

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.

dide CBS350-8P-E-2G - switch6fc0	)8a ×	+								-	٥	×
← → C A Not secure   192.168.1.1/cs23fc0a43/mts/home.htm							$\forall_{\mathscr{P}} \in$	1 20	ť≡	Ē		
CISCO CBS350-8P-E			CBS350-8P-E	-2G - switch6fc08a		Q Audinate	English	~	Advar	iced ~	0	) (+
Getting Started Port Utilization												
Dashboard Refresh Bater 15 sec												
Configuration Wizards												
Search Port Utilization Table												
<ul> <li>Status and Statistics</li> </ul>	View Interface History Graph			0								
System Summary		Interface	Tx Utilization	Rx Utilization								
CPU Utilization	0	GE1	0 %	0 %								
	0	GE2	0 %	0 %								
Port Utilization	0	GE3	0 %	0 %								
Interface	0	GE4	0 %	0 %								
	0	GE5	0 %	0 %								
Etherlike	0	GE6	0%	0%								
GVRP	0	GE7	0 %	0 %								
	0	GE8	0 %	0 %								
802.1x EAP	0	GE9	0 %	0%								
ACI	0	GE10	0 %	0 %								
Hardware Resource Utilization												

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.

The fact that SMB switches like the SG300 used a web browser for configuration (rather than command line) allowed many AV professionals to adapt to network management quickly – it was a logical step up from configuring their home router. Because Cisco was certainly an acceptable brand for IT professionals, there was little resistance to it on installations. Pricewise, this fit the budget.

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.

<image><image><image><image><section-header><text><text><image>

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

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