APPLICATION NOTES

NETWORK SWITCH CONFIGURATIONS FOR DANTE & AES67

NETWORK SWITCH CONFIGURATIONS FOR DANTE & AES67

This document aims to provide general recommendations and configurations for network switches to be used with Powersoft amplifiers for Dante and AES67 connectivity, including examples.

For remote control and monitoring of amplifiers, any type of network switch running on at least 100 Mbps will be sufficient. However, for transport of audio over IP via Dante or AES67, dedicated network switches and configurations may be necessary. This is specially the case in large and heavily loaded, or mixed, networks (e.g. audio + other data types).

General Recommendations for Dante & AES67

For maximum Dante and/or AES67 network reliability, it is recommended that switches be/have:

- Rated for gigabit Ethernet – although 100Mbps may be enough for a small and audio-dedicated network, larger and heavier installations may require a switch running on at least 1Gbps.

- Non-blocking – in this type of device (almost every switch nowadays), all ports can run at full speed without any loss of data packets. The switch can handle the total bandwidth on all ports, establishing routing to any free output port without interfering with other traffic.

- Managed – differently from unmanaged switches (plug-and-play), managed switches offer a series of different options and adjustments, such as the ability to prioritise the transport of certain types of data over others, and creating Virtual Local Area Networks (VLANs), which are particularly important in mixed networks where audio is combined with other types of data. For small and audio-dedicated networks, unmanaged switches may be sufficient for Dante and AES67 operation. However, in heavily loaded networks, or where audio streams share the network with other data (e.g. video, security, etc.), a managed switch will likely be necessary.

- Quality of Service (QoS) management – only available in managed switches. QoS network management allows the switch to prioritise certain types of data packets over others. Such packets get preferential treatment and are “moved to the front of the line" ahead of other traffic (Figure 1). In the case of audio streams, the priority must first be given to clocks for device and audio signal synchronization, followed by the audio packets themselves. This is to guarantee low-latency and high-quality audio streams across the network. Dante networks require at least four priority queues, whilst AES67 only requires three.

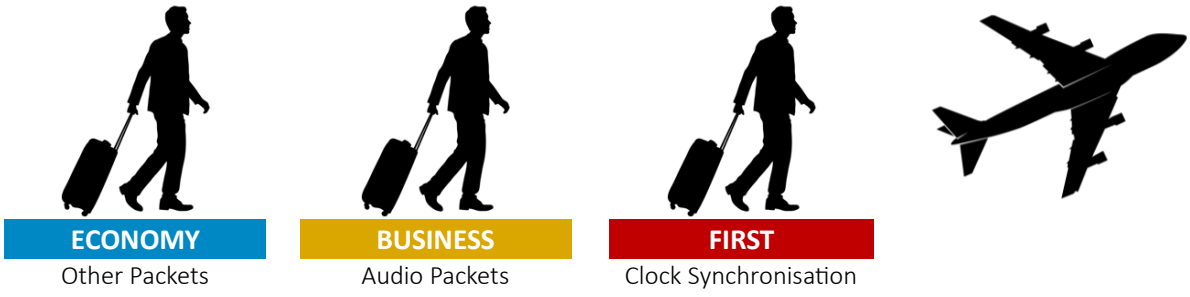

Figure 1 – Sketch of different priority queues for audio data management in an AES67 network.

- **Differentiated Services Code Points (DSCP) QoS** – DSCP is a type of QoS management. In order to prioritise the different packets of information, Dante/AES67 networks use DSCP labels and numbers to organise these packets in different priority queues. Such management is done by the switch and, therefore, where managed network switches are necessary, these must work with DSCP QoS.

  Many switches have Layer 2 "CoS QoS" management enabled by default, and this configuration needs to be changed to Layer 3 "DiffServ/DSCP QoS". Once enabled, check the priority assignments. The switch will require special configuration to recognise and prioritise the specific DSCP values used by Dante (Table 1) and by AES67 (Table 2). A configuration example is covered later on in this document.

PRIORITY QUEUES	USAGE	DSCP LABEL	DSCP NUMBER
1. High	Clock synchronisation	CS7	56
2. Medium	Audio packets	EF	46
3. Low	(Reserved)	CS1	8
4. None	Other packets	Best-Effort	0

Table 1 – Dante's different priority queues and their respective DSCP values.

PRIORITY QUEUES	USAGE	DSCP LABEL	DSCP NUMBER
1. High	Clock synchronisation	EF	46
2. Medium	Audio packets	AF41	34
3. None	Other packets	Best-Effort	0

Table 2 – AES67's different priority queues and their respective DSCP values.

In mixed networks with Dante and AES67 streams generated from a Dante card, it is always recommended that the DSCP values from Table 1 are used, and that clock synch packets always receive the highest priority treatment. The values in Table 2 should only be used in AES67 networks that do not contain Dante streams.

IMPORTANT NOTE:
In larger Wide Area Network (WAN) connections, such as those used in large corporate environments, DSCP tags may not be respected by edge routers. Consult your network administrator to discuss options to bypass this constraint if it exists.

- **EEE (Energy Efficient Ethernet) DISABLED** – switches that do not have energy efficient or energy save modes do not require any additional configuration. However, this function needs to be disabled in switches that offer it, as it will impede proper operation of low-latency audio over IP. The energy-save function tends to delay packets sent over the network.

  EEE is also sometimes referred to as 'Green Ethernet' or 'IEEE 802'. An example of turning EEE off in a Cisco switch is given later on in this document.

  Beware that some unmanaged switches have EEE enabled by default and will not allow the user to disable this function.

Additional Recommendations for Multicast Traffic

The following switch configurations apply to networks containing multicast data traffic. Dante devices may be configured to transmit either unicast or multicast audio streams, while AES67 only works with multicast transmission.

For Dante, unicast data traffic will require less switch and routing configurations, making it a simpler and faster solution for small and dedicated networks, under normal circumstances. However, in larger scenarios, and specially where multiple devices receive the same audio stream, the use of multicast over unicast for audio transmission may be beneficial. If correctly configured, multicast can be more efficient than unicast in terms of bandwidth consumption.

For maximum multicast efficiency and reliability, it is recommended that network switches have:

- IGMP Snooping Activated – When using multicast traffic, it is important to configure the network accordingly to increase efficiency and reduce bandwidth consumption. Without a proper configuration to manage this traffic, multicast packets will be broadcast to all receivers in the domain, including devices that have not requested those packets (Figure 2). This could be a problem to some amplifiers that may not be able to manage a high count of incoming data packets. To overcome this issue, IGMP Snooping must be activated in the network switch.

  Internet Group Management Protocol (IGMP) is a communication protocol used to establish multicast groups and manage memberships of receiving and transmitting devices. When a multicast transmission starts, a multicast group is created and an announcement is sent to all devices over the network, after which devices wishing to receive the multicast packets will send IGMP join messages, specifying the IP multicast group they want to join.

  IGMP Snooping is the process where the network switch examines the IGMP communications between devices to create a table with what multicast packets are needed and in which of its ports. In this process, the switch will only forward multicast data packets to the designated ports and receivers (Figure 2).

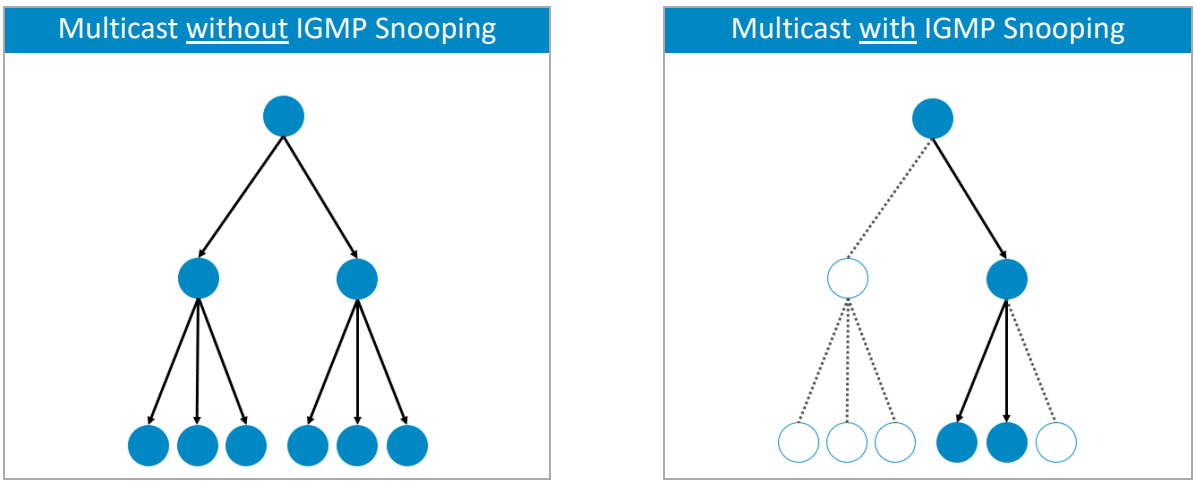

Figure 2 – Difference between multicast packet transmission with and without IGMP Snooping in operation.

For the purpose of a stable IGMP Snooping operation, an **IGMP Snooping Querier** must also be enabled. The aim of a querier is to keep the table with all the multicast group memberships up to date. It sends out IGMP queries on a timed interval to all members belonging to the IP multicast group. All devices wishing to remain in the group must reply to the query with a confirmation. Those devices that do not respond within a defined amount of time will be removed from the group's table and will no longer be forwarded those multicast streams.

Although a network can accommodate multiple IGMP Snooping Queriers (and will automatically select one), it is safer to have only one IGMP querier enabled, preferably on a switch sitting close to the root of the network topology.

Some switches also allow the configuration of a 'Query Interval', which is related to the group membership timeout, and is the number of seconds that must pass before the switch determines that no more members of a multicast group exist on the network. When the 'Query Interval' is large, the time required for the multicast stream to start or stop working becomes longer and the user may experience than an amplifier will take longer to start playing audio.

An example of IGMP Snooping configuration for a Cisco switch is given later on in this document.

Finally, IGMP has three different versions: v1, v2, and v3. However, IGMPv2 supports IGMPv1, and IGMPv3 supports IGMPv2. Although not all features of an earlier version of IGMP are supported, the features related to membership query and membership report messages are supported for all IGMP versions. For Dante and AES67, IGMPv2 or IGMPv3 are recommended.

Final Recommendations

The following are general recommendations for consideration, especially in the case of larger networks:

- Topology – Although “daisy chaining” may be suitable for connecting devices in a network, the failure of any device in the chain will break connections to devices further down in the “stream”. In general, switched networks are best thought of when using a “star”, or “hub and spoke” topology. In such a setup, all devices on a star are connected to a single switch and, if any device fails, the others continue to communicate. As the network gets larger, additional switches may be brought in to extend the network. The star topology can be easily extended in a multiple-star arrangement to suit larger systems (Figure 3).

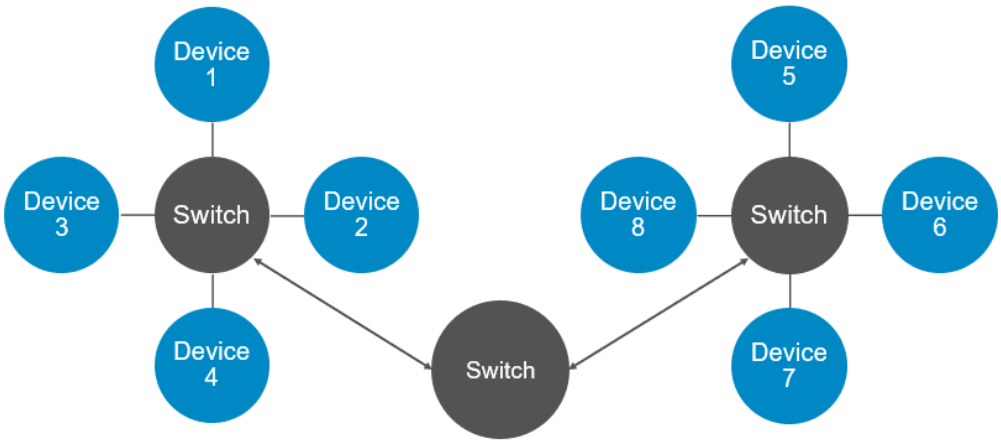

Figure 3 – Example of a multiple-star topology, where no device is more than 4 “hops” away from any other.

- Cabling – Any type of ethernet cable is suitable for a Dante or AES67 network, although in gigabit speed network CAT5e or CAT6 cables are recommended. CAT6 cables are rated for greater noise resistance in electrically noisy environments, however, CAT5e is enough for most applications. The maximum allowed length for a normal ethernet cable is approximately 100m. For longer distances, fibre optics will be necessary, as it can run for several kilometres when required. The drawback is that fibre connections will require network interfaces that can support it, such as Small Form-Factor Pluggable (SFP).

NETWORK SWITCH CONFIGURATION EXAMPLE: CISCO SG300-10

The following is an example of how to configure a Cisco switch with some of the key parameters for a correct Dante/AES67 operation.

The configurations page for most switches can be accessed by typing its IP address in any web browser address bar. For this to work correctly, the computer must be in the same IP range/subnet of the switch it is connected to. By default, Cisco switches are in the IP range 192.168.1.X.

To change the computer's IP address and subnet mask, in WINDOWS:

1. Connect the computer to any of the switch ethernet ports.

2. On a Windows PC, access the **Ethernet Status** window (Figure 4). Usually this is done from the 'Network and Sharing Centre', by clicking on 'Ethernet' from the active networks.

3. In the Ethernet Status window, click on 'Properties' to open the **Ethernet Properties** window, select 'Internet Protocol Version 4 (TCP/IPv4)', and click 'Properties' (Figure 5).

4. In the **TCP/IPv4 Properties** window, select 'Use the following IP address' to configure a static IP address for the PC (Figure 6).

5. Type in an IP address following 192.168.1.X; where X can be any number from 1 to 253, assuming there are no other devices in the same subnet connected to the switch for which one of those numbers has already been allocated.

6. Under Subnet Mask, type in 255.255.255.0, and click 'OK'.

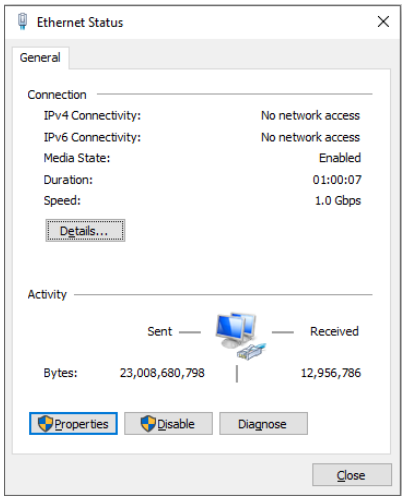

Figure 4 – Ethernet Status window.

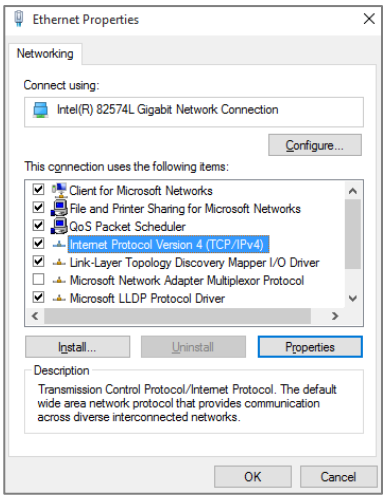

Figure 5 – Ethernet Properties.

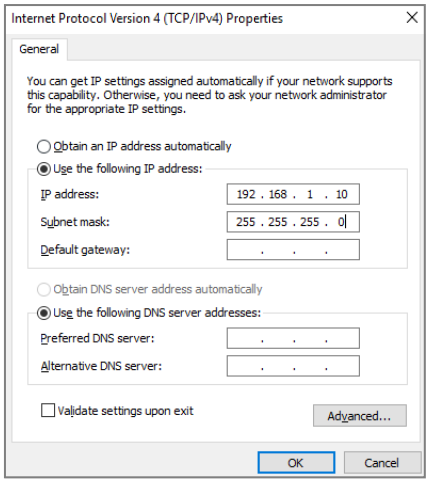

Figure 6 – TCP/IPv4 Properties.

After the configuration of the switch is done, remember to revert the operation by selecting 'Obtain an IP address automatically' from the **TCP/IPv4 Properties** window and clicking OK.

Once both the computer and the network switch are on the same subnet IP range:

1. Open any web browser on the computer and type the IP address of the switch in the address bar. By default, Cisco switches use the IP address 192.168.1.254.

2. This should open the switch configurations page (Figure 7). Type in the request username and password. The default for the SG350-10 is “cisco” for both fields.

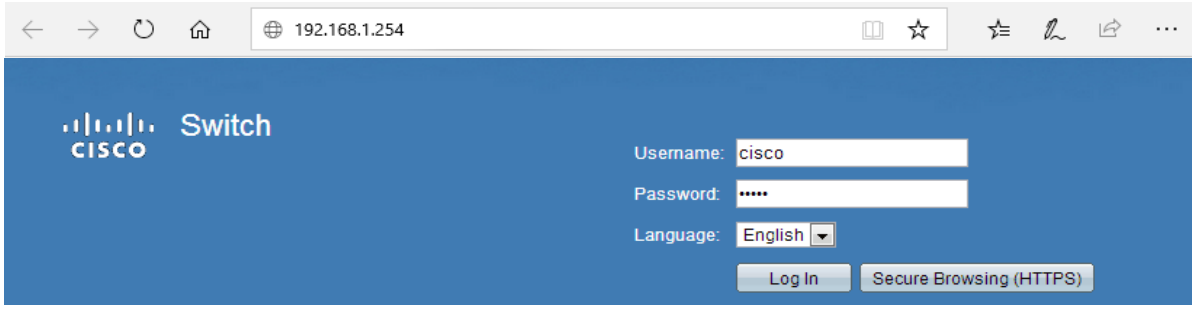

Figure 7 – Ethernet Status window.

Once connected to the switch and logged into the configurations page, it will be possible to access and adjust each one of the configuration parameters.

DSCP Configuration for QoS Management

To configure DSCP parameters:

1. From the main switch configurations page, using the left-hand side menu, follow the path ‘Quality of Service > General > QoS Properties’ and enable **QoS Advanced Mode** (Figure 8).

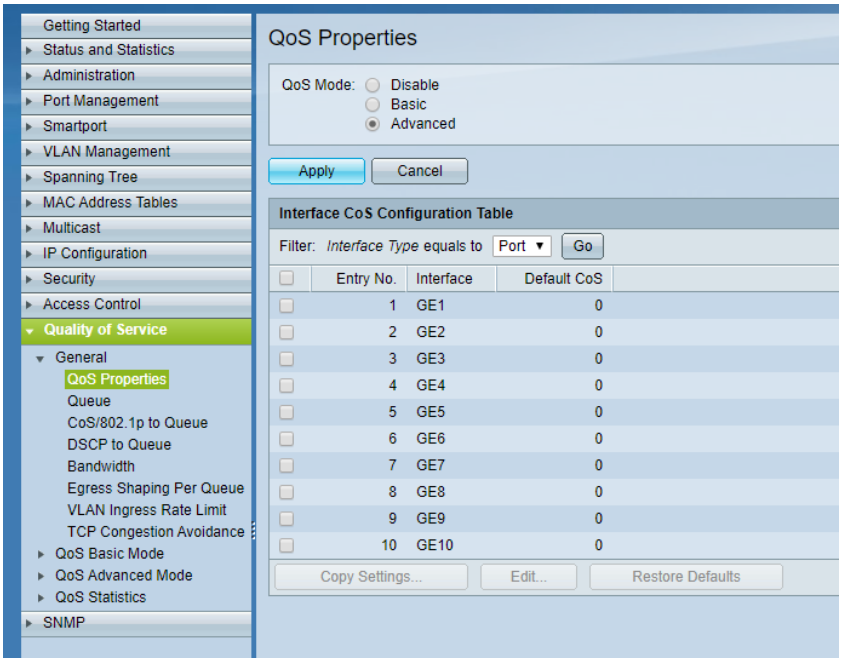

Figure 8 – Enabling QoS Advanced Mode.

2. It is then necessary to change the settings from Layer 2 CoS management to Layer 3 DSCP. Under 'Quality of Service > QoS Advanced Mode > Global Settings', select **DSCP** as the 'Trust Mode', **Trusted** as the 'Default Mode Status', and click 'Apply' (Figure 9).

Figure 9 – Global settings configuration.

3. Next, go to 'Quality of Service > General > DSCP to Queue', specify the priority output queue of each DSCP label, and click 'Apply' (Figure 10). In Cisco switches, queue number 1 has the lowest priority, while queue 4 has the highest.

   The labels to which a priority must be given depend on the type of audio network in use.

For Dante		**AES67 (non-Audinate)**	
56 (CS7)	4	46 (EF)	4
46 (EF)	3	34 (AF41)	3
8 (CS1)	2	-	2
Everything else	1	Everything else	1

IMPORTANT NOTE:
Consult your network administrator in case the network presents other pre-existing systems, such as a LAN VoIP, as the settings above may need to be reviewed.

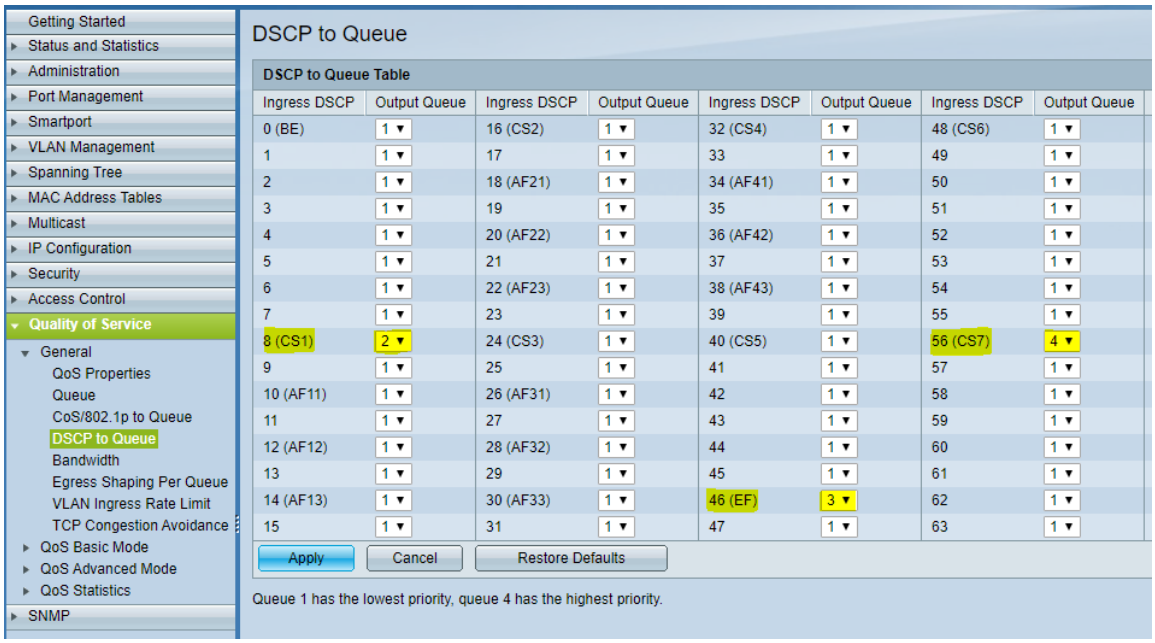

Figure 10 – Configuration of DSCP queues.

Disabling Energy Efficient Ethernet (EEE)

To disable EEE in the Cisco switch:

1. From the main switch configurations page, using the left-hand side menu, follow the path 'Port Management > Green Ethernet > Properties' (Figure 11).

2. Untick the '802.3 Energy Efficient Ethernet (EEE)' enable box and click 'Apply'.

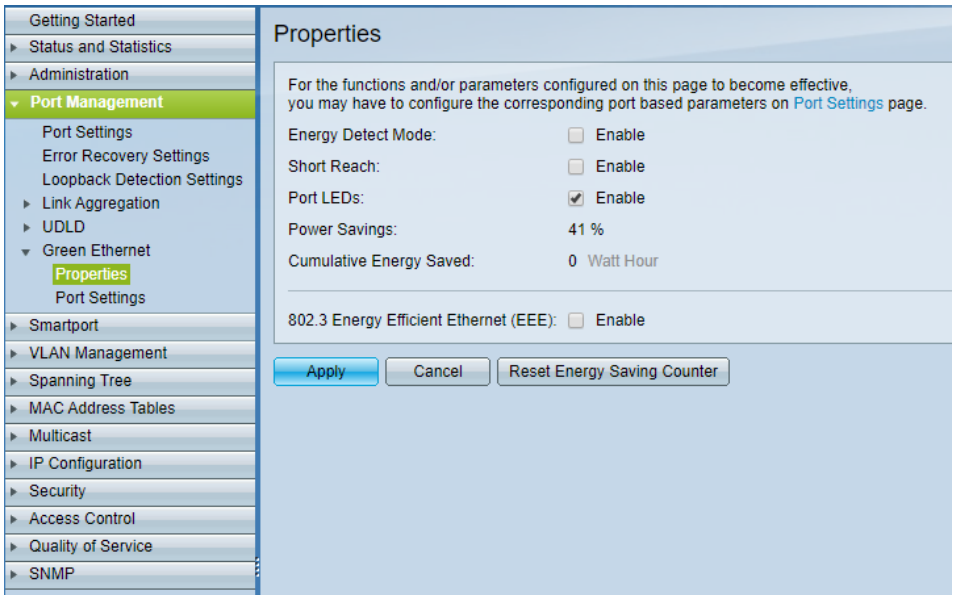

Figure 11 – Disabling EEE.

Enabling and Configuring IGMP Snooping

To enable IGMP Snooping in the Cisco switch, for when multicast traffic is necessary:

1. From the main switch configurations page, using the left-hand side menu, follow the path 'Multicast > Properties' (Figure 12).

2. Tick the enable check box for 'Bridge Multicast Filtering Status'.

3. Under 'VLAN ID', select the VLAN for which multicast traffic will be used. If no VLANs have been configured, select 1.

4. Select **IP Group Address** for both 'Forwarding Method IPv6' and 'Forwarding Method IPv4'.

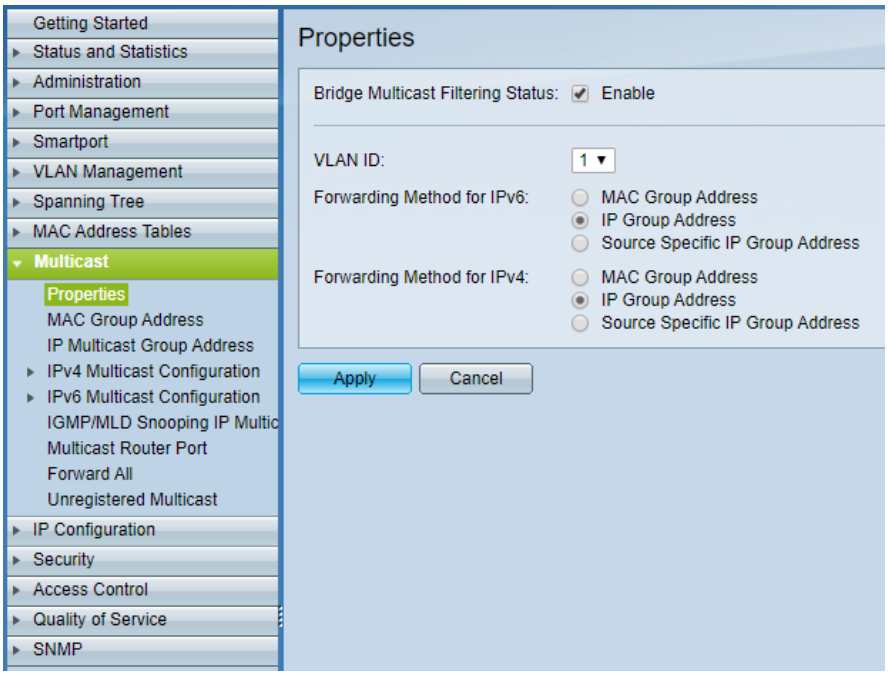

Figure 12 – Setting up multicast properties.

5. Next, go to 'Multicast > IPv4 Multicast Configuration > IGMP Snooping' (Figure 13).

6. Select the enable check box for both 'IGMP Snooping Status' and 'IGMP Querier Status' and click 'Apply'.

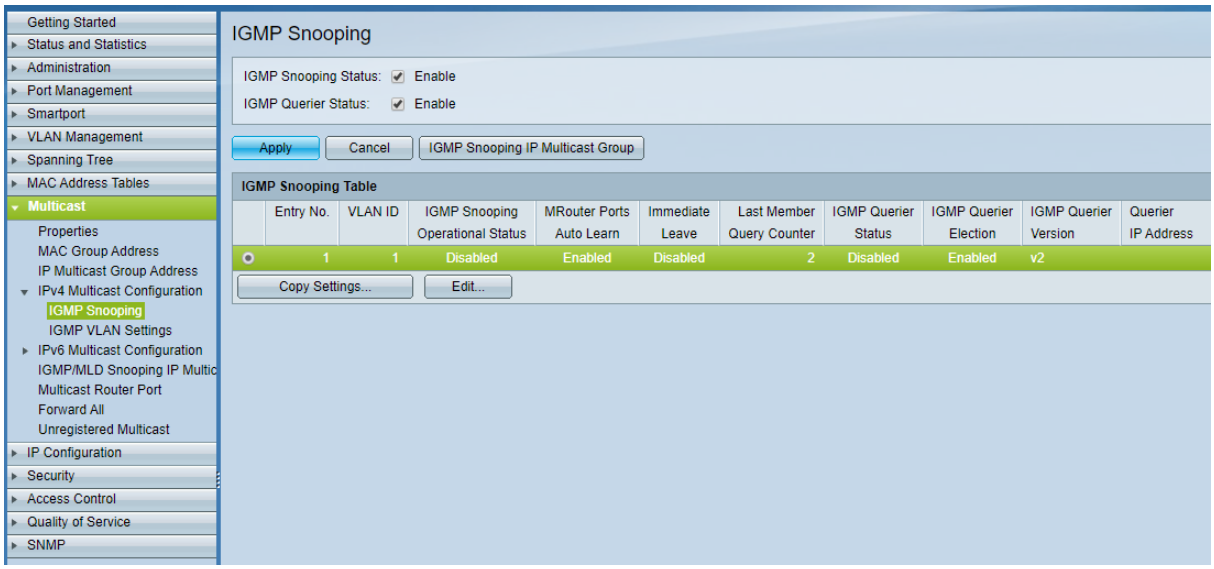

Figure 13 – Enabling IGMP Snooping.

7. To edit the IGMP Snooping settings, still on the same page, under 'IGMP Snooping Table', select the multicast VLAN ID and click 'Edit'. This will open the 'Edit IGMP Snooping' window (Figure 14).

8. Make sure the 'IGMP Snooping Status' is enabled, as well as 'MRouter Ports Auto Learn'.

9. Next, enable the 'IGMP Querier Status', 'IGMP Querier Election', and set the 'IGMP Querier Version' to IGMPv3 and click 'Apply'. This is a recommended setting. As mentioned previously, Dante and AES67 both support IGMPv2 and IGMPv3. The important thing is that all switches in the network are configured to run on the same version.

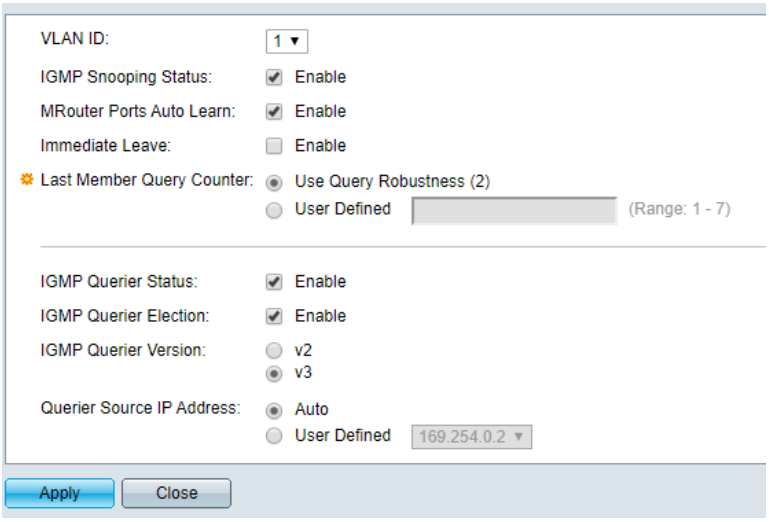

Figure 14 – IGMP Snooping Settings.

IMPORTANT NOTE:
Remember from the previous sections of this document that in networks using multiple switches, it is safer to have only one IGMP Querier enabled, preferably on a switch sitting close to the root of the network topology. In this case, the functions in step 9 above should be disabled for all switches down in the connection chain and that will not operate as IGMP Queriers.

Document Title: NETWORK SWITCH CONFIGURATIONS FOR DANTE & AES67
Reference: DO000277.00 REV.00

Powersoft S.p.A
Via E. Conti, 5- Scandicci (Fi) 50018- Italy
TELEPHONE: +39 055 7350230

General Enquires: info@powersoft.it
Sales: sales@powersoft.it
Application & Technical Support: support.audio@powersoft.it
Service & Maintenance: service@powersoft.it

www.powersoft.com