Setting up a switch for use with Dante

Using the **Cisco SG300-20** or **Teqsas CyberTEQ-m**

Contents

1.0 The advantages of this Switch

This switch is frequently selected for small audio networks using Dante for a number of reasons:

- Reasonable price and world-wide availability from a reputable company
- Ease of use with a Web-Browser interface
- Initial settings that work well enough in many cases
- Features such as VLANs, QoS with DSCP, Multicast Filtering, and Spanning-Tree Protocol
- Optional fibre-optic interfaces
- Every port is 1Gbps capable, and the whole switch can process 40Gbps of data
- Rack-mount kit is included, and it has no cooling fan!

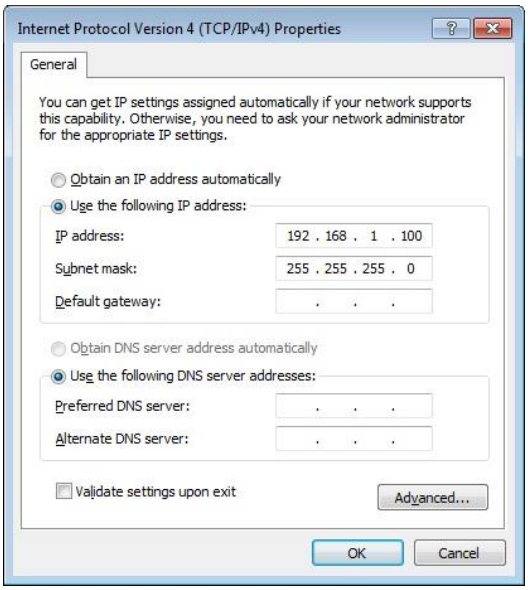
If the requirement is to use just one switch for Dante audio networking mixed with a variety of control data using a Wi-Fi connection, then this switch is possibly the only option within its price range.

2.0 Getting Started: Firmware, IP Address & Password

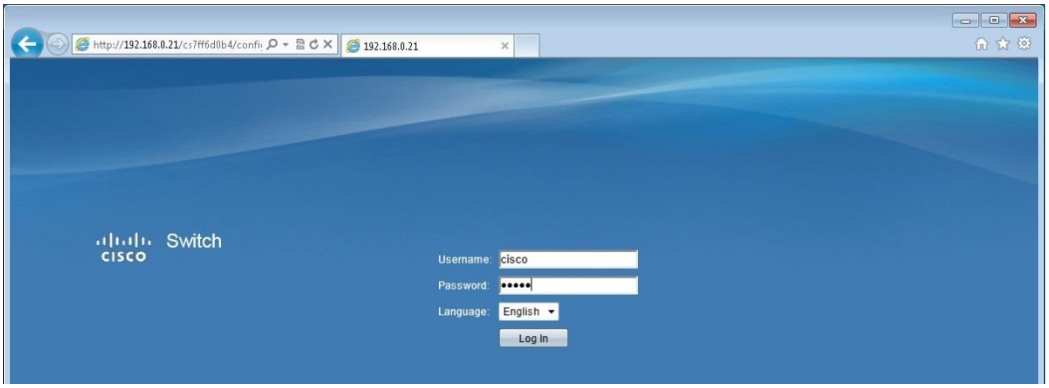
2.1 Login

This switch is easiest to manage via a web interface. Any standard web browser application can be used. Give the computer an IP address in the same range as the switch.

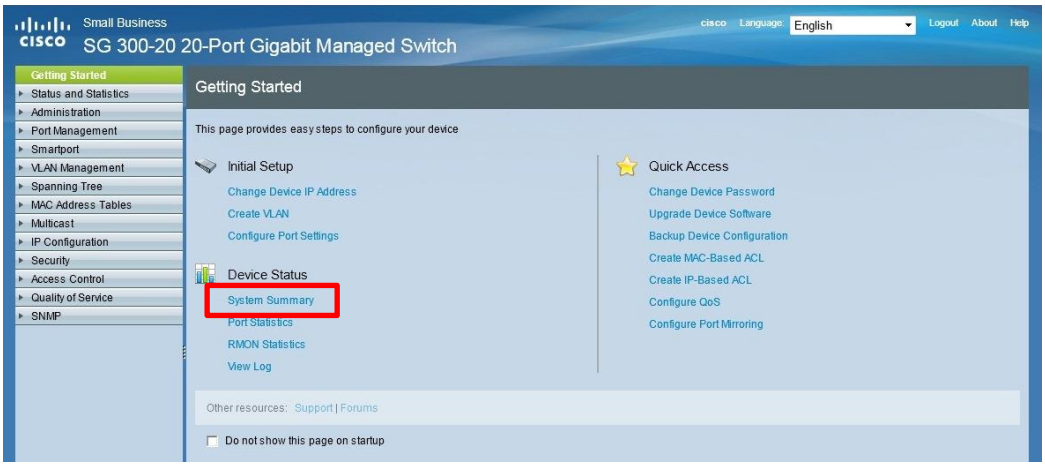
The Cisco default is 192.168.1.254, in which case the computer could be given an IP address of 192.168.1.100 for example.
The Teqsas default is 192.168.0.**, so the computer can be given an IP address of 192.168.0.100 for example.



Type the switch IP address into the address bar of the web browser. When the user first logs in, the default Username is “cisco”. The password is the same. It is a good idea to change this, to increase security. But don’t forget it!

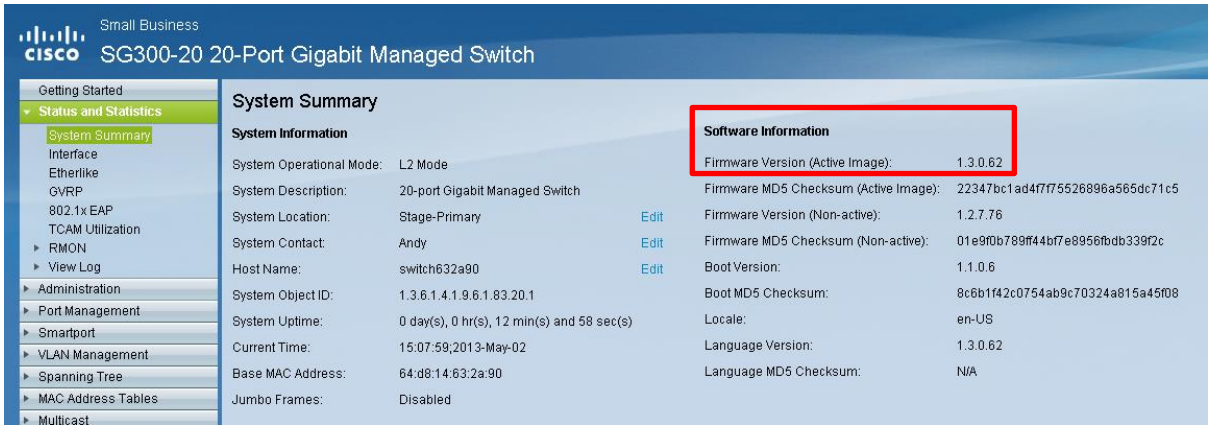


After logging in, the first page shown is the **Getting Started** menu.

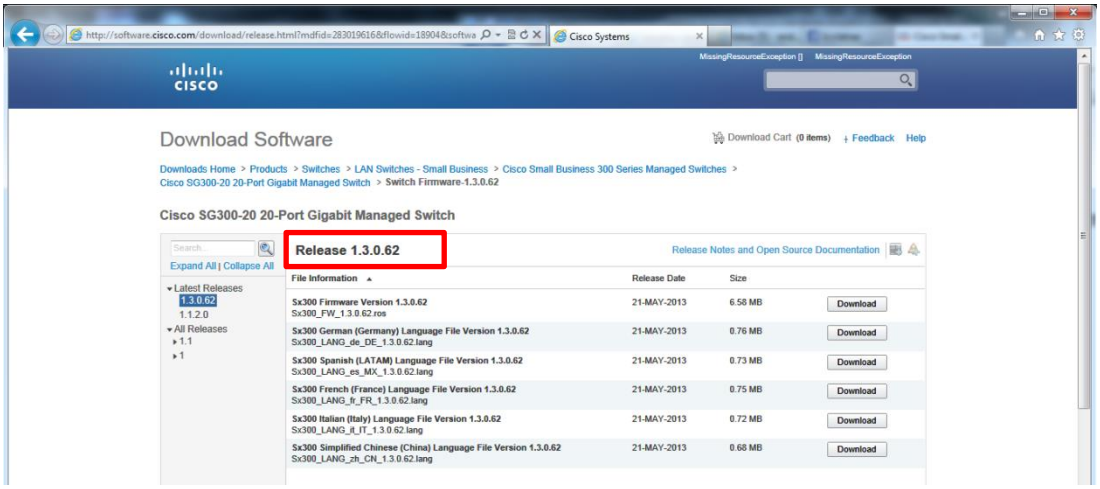


2.2 Firmware Update

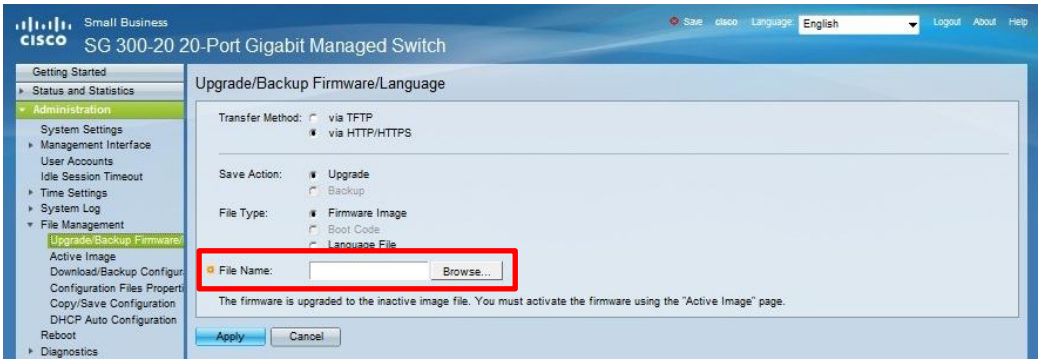
First check the firmware version. Click on the “System Summary” short-cut to view the information.



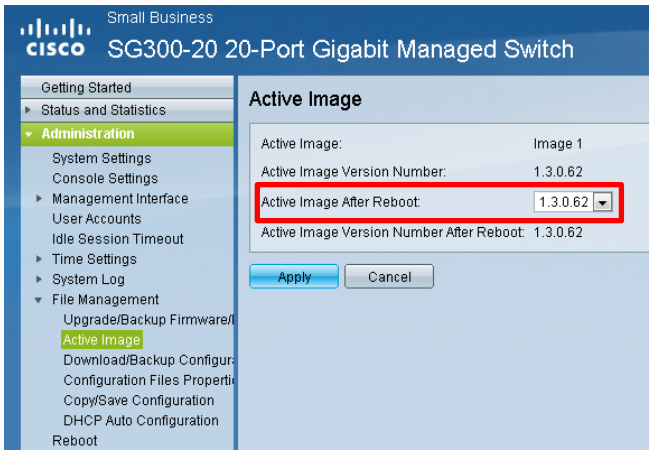
Compare this to the firmware versions available from www.cisco.com. At the time of writing, the latest version is 1.3.0.62.



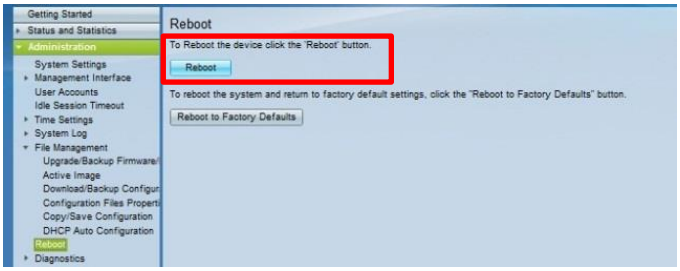
If you want to upgrade the switch firmware, to make the most of the new features and bug fixes, first download the file from Cisco's website. Next, in the left menu of the SG300 web interface, open the **Administration** menu, then the **File Management** sub-menu, and select the **Upgrade/Backup Firmware** page. The HTTP/HTTPS transfer method is the simplest way to upgrade. Select "Firmware Image" as the file type. Browse for the firmware file, and click [Apply].



The upgrade will take around 3 minutes.
After that, the switch will need to be rebooted with the image that contains the new firmware: in the **Active Image** page, select the image with the new firmware.
Click [Apply].



Then in the **Reboot** page, click [Reboot].

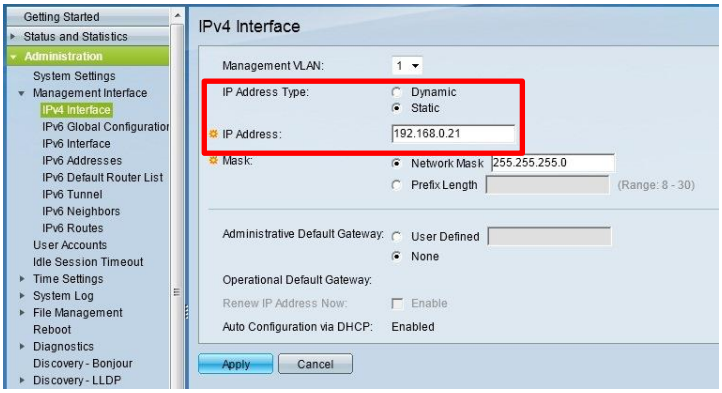


2.3 IP Address

The IP address of the switch can be changed. In a typical small audio network, it is a good idea to give the switch a static IP address in the same range as other control equipment on the network, so the switch performance can be monitored along with the other gear. For example, give everything an address in the 192.168.0.xxx range. Make sure every device has a different last number, between 1 and 254. Use a subnet mask of 255.255.255.0.

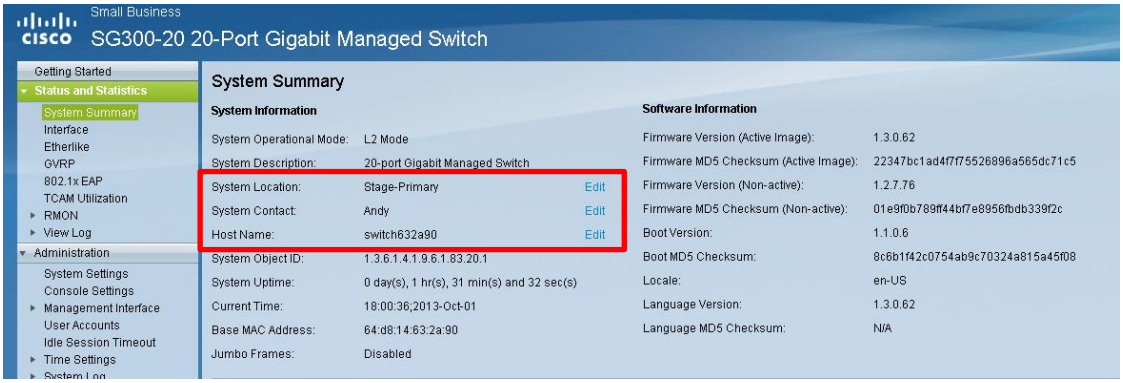
In the **Administration** menu, select **IPv4 Interface**. Select the "Static" IP Address type, and enter the new IP Address.

After changing the IP Address, the user may need to log in again, via the Web Browser. Make sure again that the PC has an IP address in the same range as the switch.



2.4 System Information

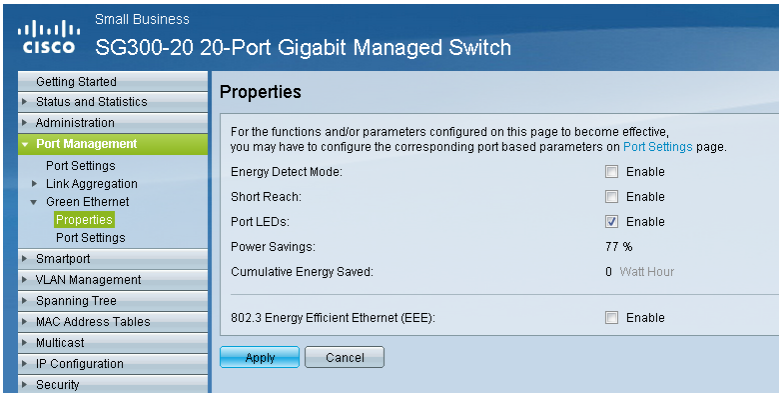
Back in the **System Summary** window, it is a good idea to edit the System Location, System Contact and Host Name. This is useful for identifying the switch in a system that contains a large number of similar devices. For example: "FOH Primary" or "Amp Rack-Delay-L1".



2.5 EEE

In the interests of saving energy, many switches implement a set of “green Ethernet” or “Energy Efficient Ethernet” (EEE) functions. With the SG300 this does not normally cause a problem, but some other types of switch cause the Dante device synchronisation to become unstable. Therefore it is good practise to always disable the EEE functions.

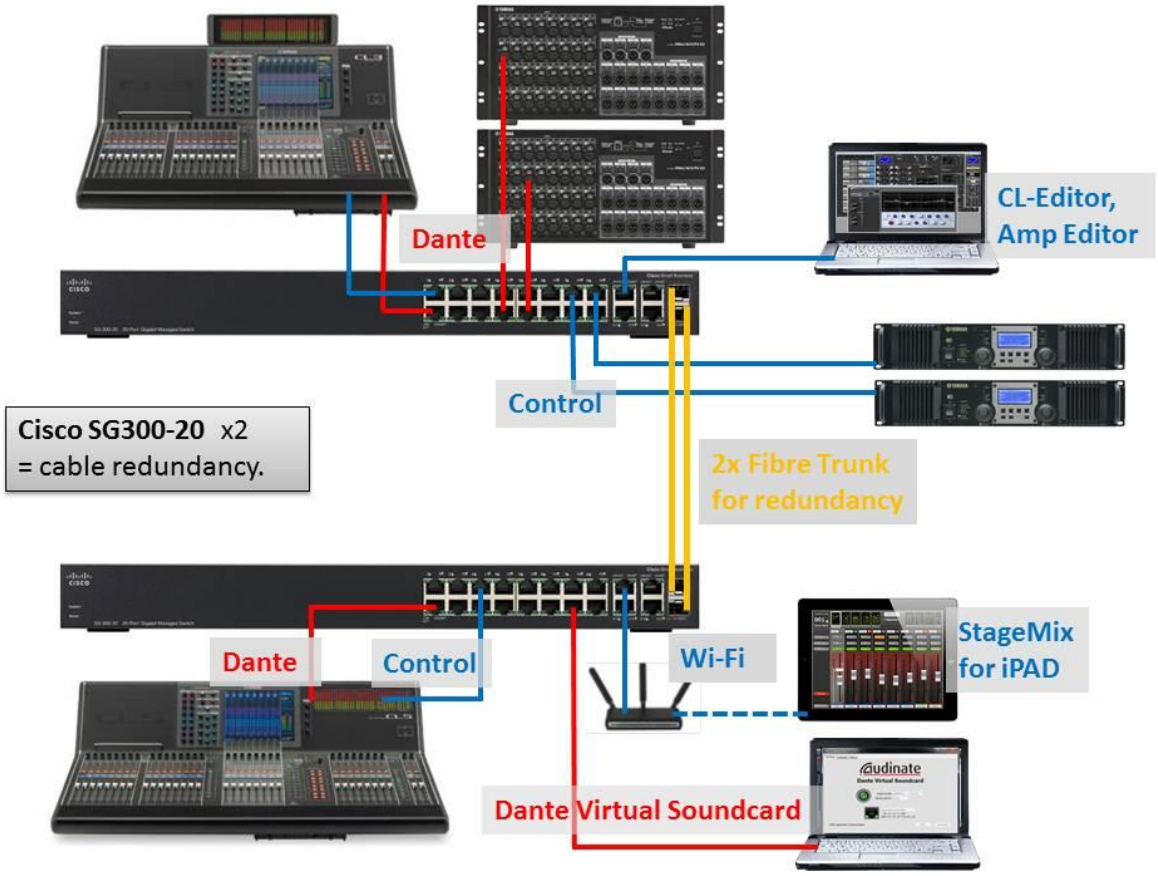
To disable EEE, open the **Port Management** menu, and select **Green Ethernet Properties**. Disable “Energy Detect Mode”, “Short Reach” and “802.3 Energy Efficient Ethernet”. Click [Apply].



3.0 Simple System Network Design

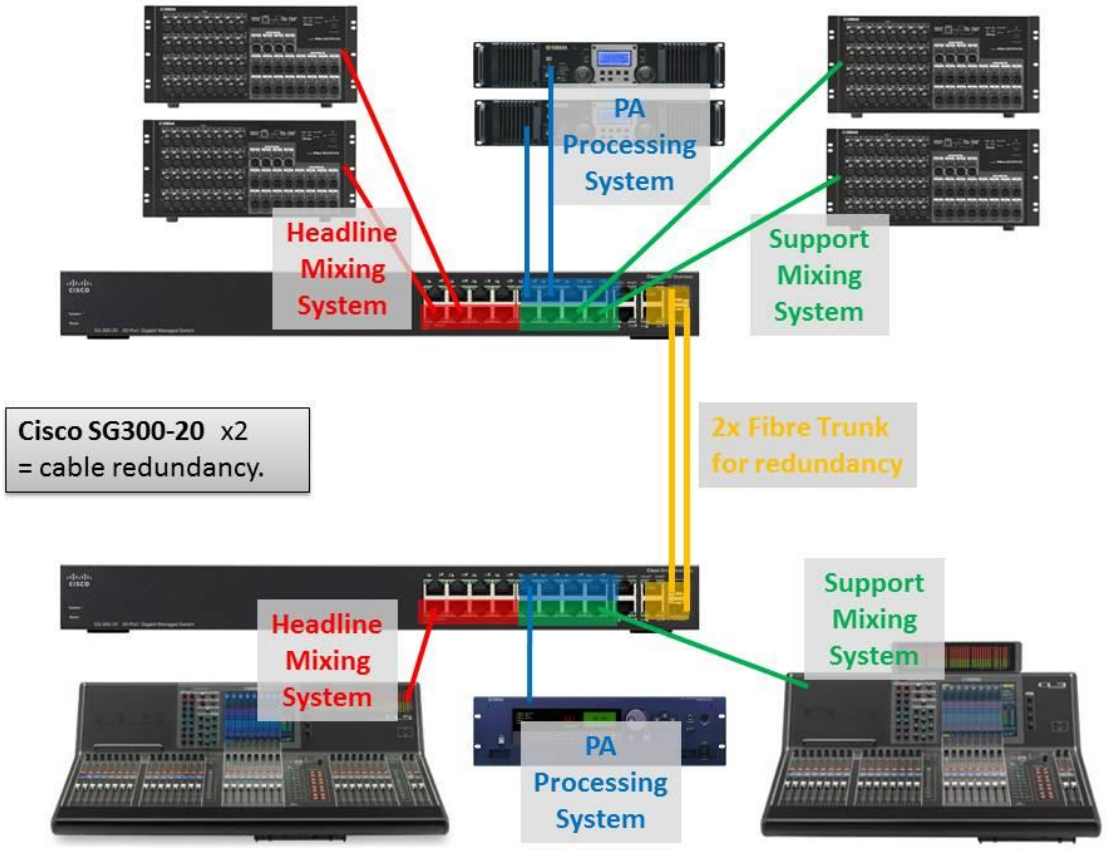
Below is an example system, shown with two Cisco SG300-20 switches. This setup is best achieved with 2 VLANs (virtual local area networks): one for Dante and another for the Control data (CL-StageMix on iPad, CL-Editor on a PC, Amp Controller, etc.). Because two fibre cables are used between the switches to provide redundancy, a Link Aggregation Group (LAG) needs to be programmed.

Optionally, a third VLAN could be used for Dante Secondary ports. The Dante Secondary network always needs to be completely separate from the Primary network. The most effective way is by using separate switches, but if that is not possible due to budget or space constraints, then VLANs can be used. It will provide redundancy for the cables, but not for the switches.



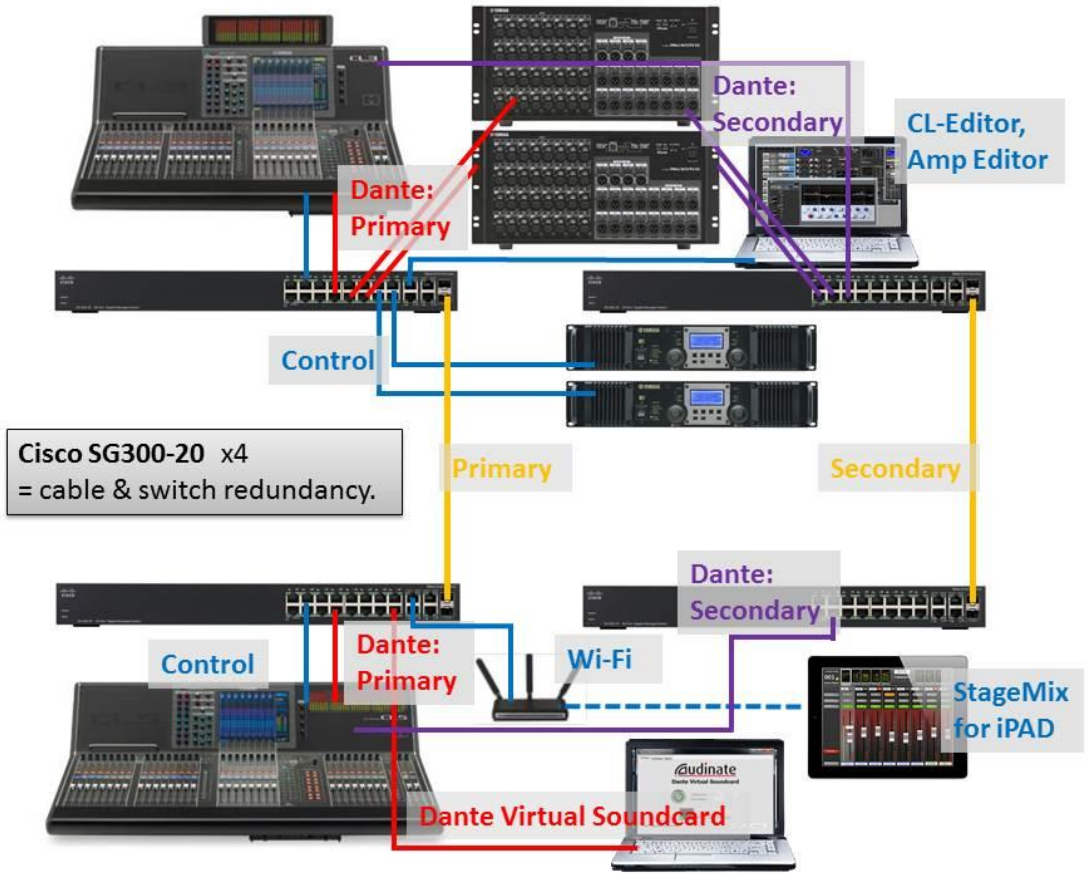
System Example 1: VLANS to separate Dante and Control data.

A second example using the same concept is shown below, with different VLANs used for different sections of the audio system. In a typical touring system, different engineers will have different responsibilities. For example, the headline band's engineer will not be interested in sharing his system with the support band engineer. And the PA system engineer will want complete independence for his system. It makes trouble-shooting easier. In such an example, the mixing systems will have an audio link to the PA processing system via AES/EBU with sample-rate converters (by using a Yamaha MY8-AE96S card in DME64N for example).



System Example 2: multiple VLANS for segmenting the audio system.

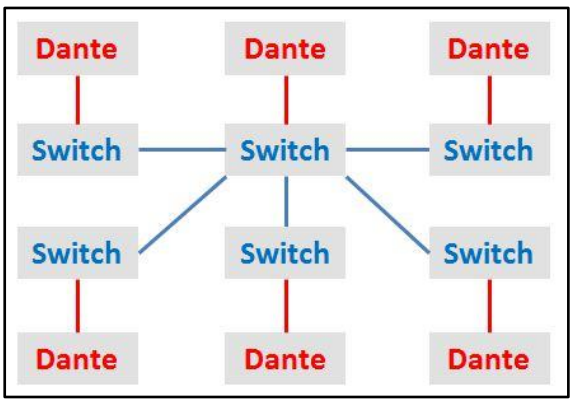
A third system example shown below is a fully redundant system, where a separate secondary Dante network is created. For correct operation, the Primary and Secondary networks must not be linked. If any switch or cable fails, audio will not stop. In this case, Link Aggregation Groups are not required. More switches could easily be added in a daisy-chain or star configuration, to connect all the amplifier racks.



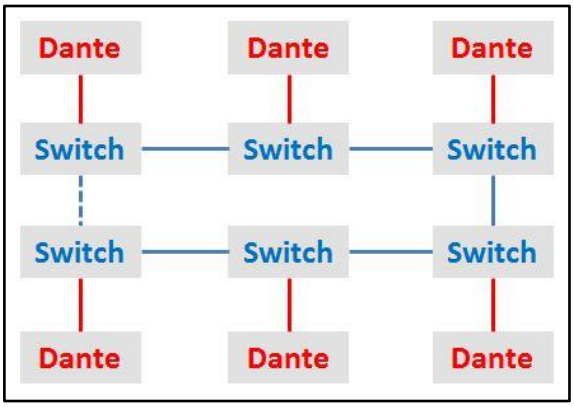
System Example 3: Redundancy for Dante.

3.1 System Topology Tips

It is good practise to design a system with as few switches in the audio signal flow as possible. This will enable the Dante network to utilise lower latency settings. This means a star topology would be preferred over a daisy-chain or ring. In the diagram below, the star has a maximum number of 3 switches in any audio path between Dante devices. Whereas with a ring, there will be up to 6 switches in the audio path.



Star Topology

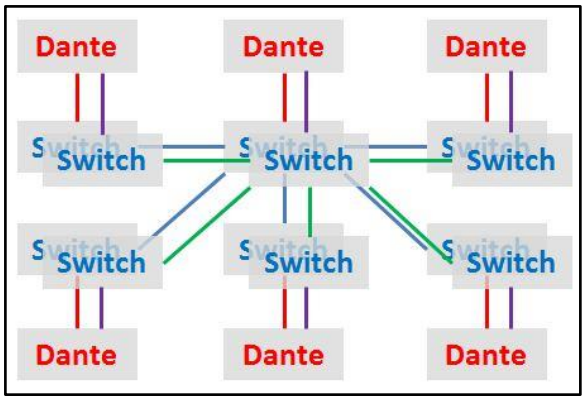


Ring Topology

A ring topology should only be used when Spanning-Tree Protocol is enabled on the switches. Spanning-Tree Protocol automatically detects rings or loops in a system, and will

block them temporarily. If a topology change is detected, the block link may become active again if it is necessary for getting the data to its required destination. If a network ring is created without using Spanning-Tree Protocol, it will be much like creating an audio feedback loop by placing a mic too close to a loud speaker: the network will become overloaded with data and may crash! With Dante, because of how its redundancy mechanism works, there is no need to use a ring topology.

Spanning-Tree Protocol can cause periods of unwanted silence in a system when there is a fault, so it is best avoided with Dante networks. Dual redundant stars are therefore the preferred method of redundancy. They are easier to setup, maintain, and trouble-shoot, as well as allowing for lower latency audio.



Redundant Star Topology

4.0 Programming VLANs

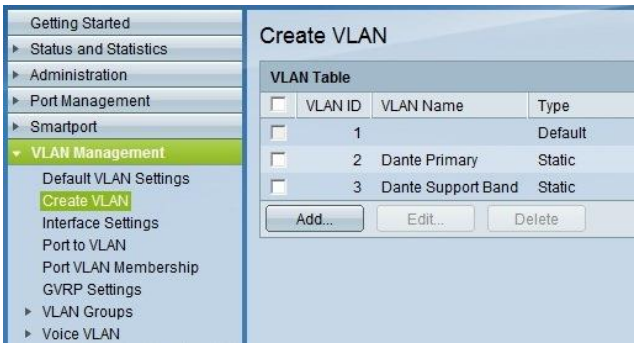
4.1 Using one switch for several different types of data

Though Dante network data can co-exist with most other types of network data, it is sometimes best avoided to make system management and trouble-shooting easier. That is where VLANs are useful: Virtual Local Area Networks sharing the same cables and switches, but otherwise completely separated. In this way the management of Dante devices can be separate from other audio control devices. And non-audio devices used by other people, such as DMX-Ethernet converters for lighting control can also be kept apart. Of course, separate switches could be used for each type of data, but by sharing the network hardware, cost and space are saved.

Using different VLANs for Dante Primary and Dante Secondary networks is a low cost form of redundancy: if any cable breaks, there is no loss of audio.

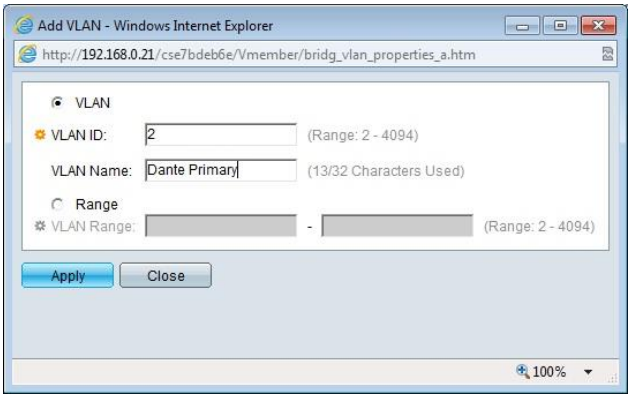
4.2 Create A VLAN

To create some new VLANs in the switch, open the **VLAN Management** menu, and select the **Create VLAN** page.



Click [Add…], and give the VLAN a name and number. Use the same numbers on all the switches in the system, or else they will not be able to communicate. The name is not important for the VLAN to function: it is just for the network administrators' reference.

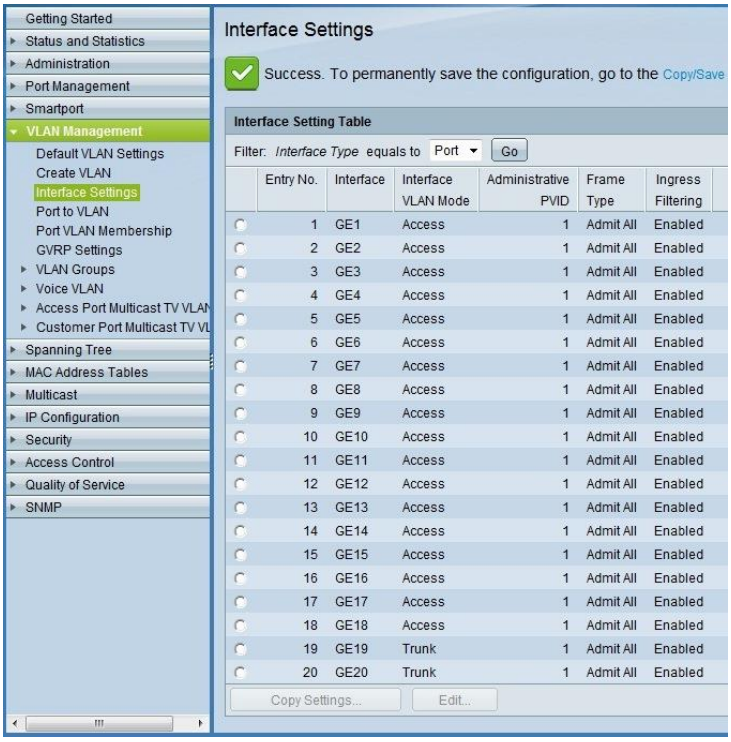
Add as many VLANs as are needed: there could be a different VLAN for each port in the switch!



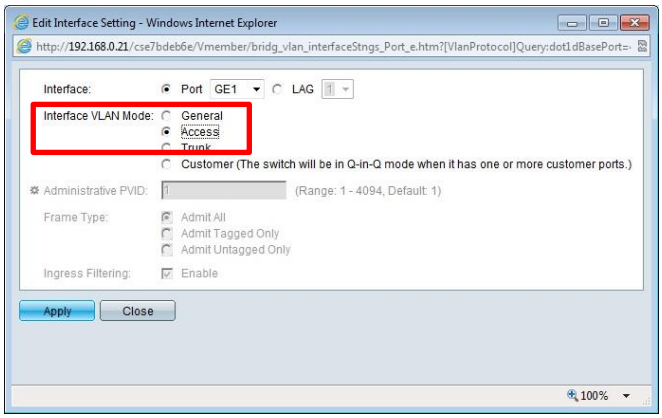
4.3 Switch Port Mode

Next, the VLAN mode should be set for each port of the switch. This is not essential to do, but it will avoid confusion when programming VLANs.

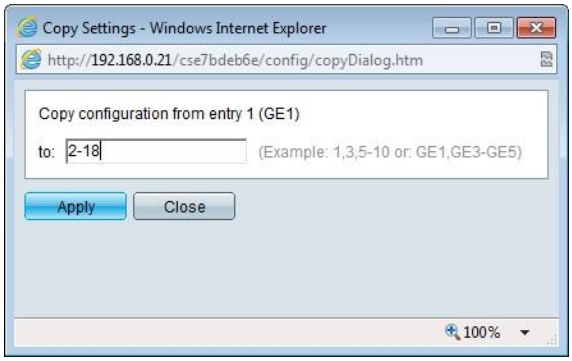
Open the **Interface Settings** page in the **VLAN Management** menu. By default, all ports are set to "Trunk" mode, which means they are all capable of carrying multiple VLANs. However, this is only necessary for the ports that link to other switches in the network. By setting all other ports to "Access" mode, the VLAN programming will be simplified: this will limit each port to one VLAN only, which is perfect for connecting to the audio and control equipment.



Select port 1 (GE1) and then click [Edit]. The Edit Interface Settings window will open. Select "Access" Mode and click [Apply].



Now the setting of port 1 can be quickly copied to the other ports: select GE1 again, and click [Copy Settings]. Enter "2-18" into the Copy Settings window, and click [Apply]. Now only ports 19-20 will still be Trunks: these are the ports normally used to link with other switches in the network.



4.4 Planning the use of VLANs

As standard, all ports are assigned to VLAN 1, the default VLAN. It is convenient to use the default VLAN for all control data, as the default VLAN is also used to manage the switch. Any port that needs to be used for the Primary Dante network, assign to VLAN 2 for

example. Any switch port used by the support band equipment needs to be assigned to VLAN 3 as another example.

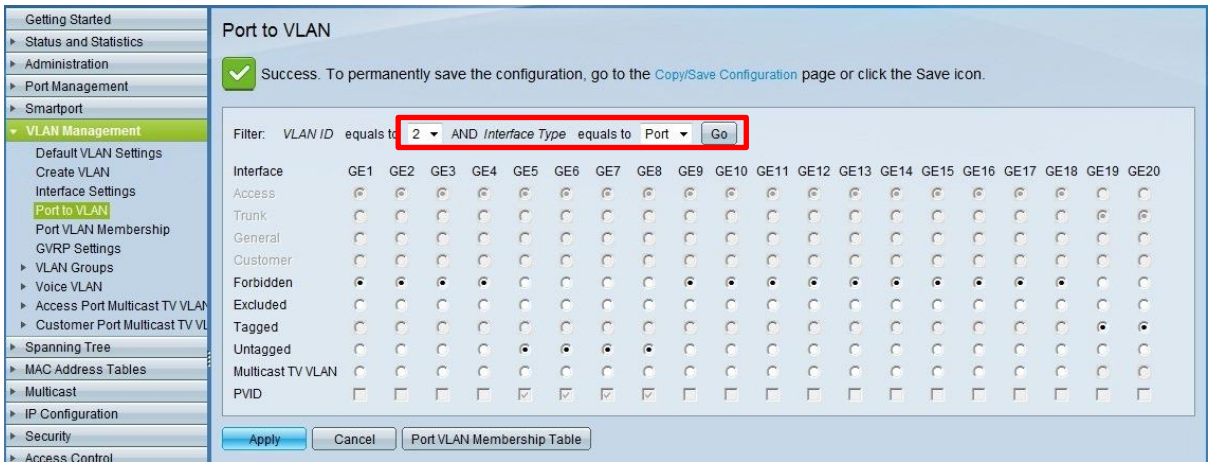
Plan how many ports are needed for each VLAN, and make a note of the required assignments. It is a good idea to have the same assignment for each switch in the system: it will make trouble-shooting and servicing easier: switches can easily be swapped without being reprogrammed. "Trunk" ports that are used for connecting to other switches in the network might need to carry multiple VLANs.

NOTE:

Always keep at least one port assigned to VLAN1. This is needed for the web-browser interface! If you change the VLAN assignment for the port being used by the PC to communicate with the switch, communication will be lost!

4.5 Assigning Ports to VLANs

In the **Port to VLAN** window, select the required VLAN at the top, and then click [Go]. This will display the port assignments to that VLAN. Now assign ports to that VLAN by choosing "Untagged". "Untagged" basically means that any data will be allowed into the switch via that port, and it will be assigned to the chosen VLAN.

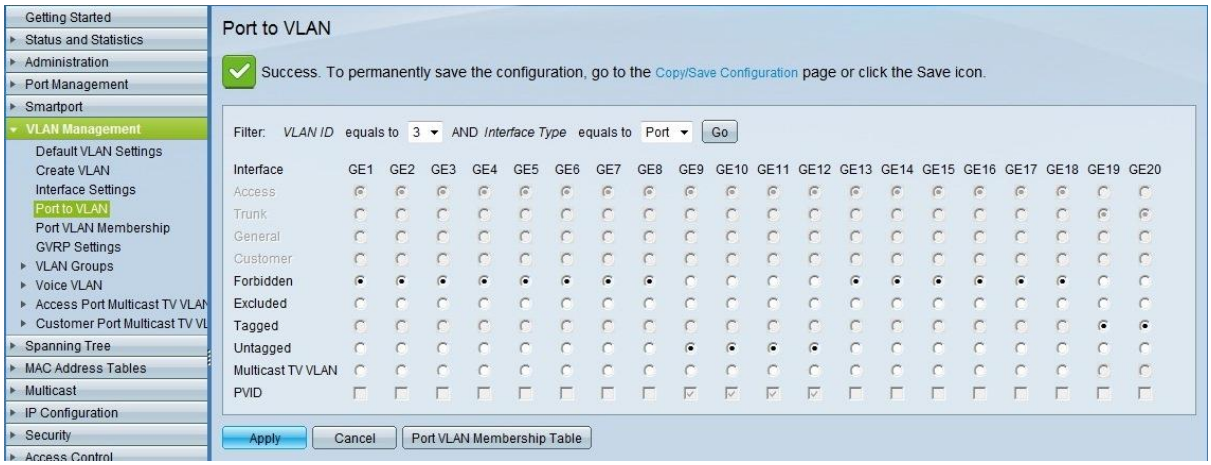


For the Trunk ports, choose "Tagged" for all new VLANs (Trunks should remain "Untagged" only for VLAN 1). In the example above, ports 5-8 are assigned to VLAN2, and ports 19-20 are Tagged with VLAN2. Because ports 19-20 will link with other switches in the network, they need to carry all VLANs. By having the VLANs tagged, the data will be kept separate. For all the other ports, choose "Forbidden" to make sure the data from VLAN2 will not pass through them.

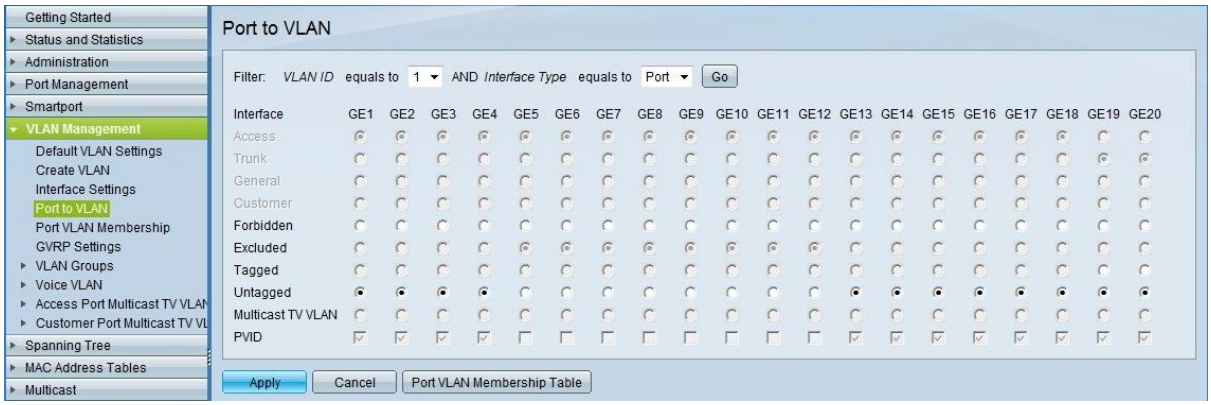
NOTE:

If ports 19 and 20 are to be used as a redundant link to the same switch (as a Link Aggregation Group), then keep those ports with their default settings for now (Untagged with VLAN1, Excluded from all other VLANs).

VLAN3 can be assigned in a similar way: ports 9-12 are “Untagged” and ports 19-20 are “Tagged” again.



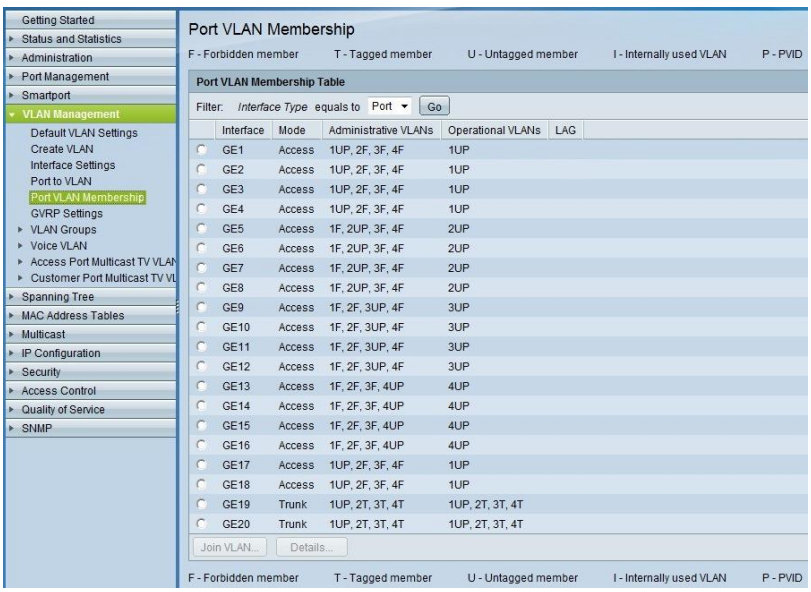
As a result, the settings for VLAN1 will now look like this:



It is necessary to actually “Forbid” the excluded ports from VLAN1, to complete the VLAN programming.

Confirm the VLAN assignments by viewing the **Port VLAN Membership** table.

At this point it is a good idea to save the settings, so they are kept after the power is turned off. (See page **20**).



5.0 Programming a LAG (or Trunk)

5.1 Cable Redundancy between two switches

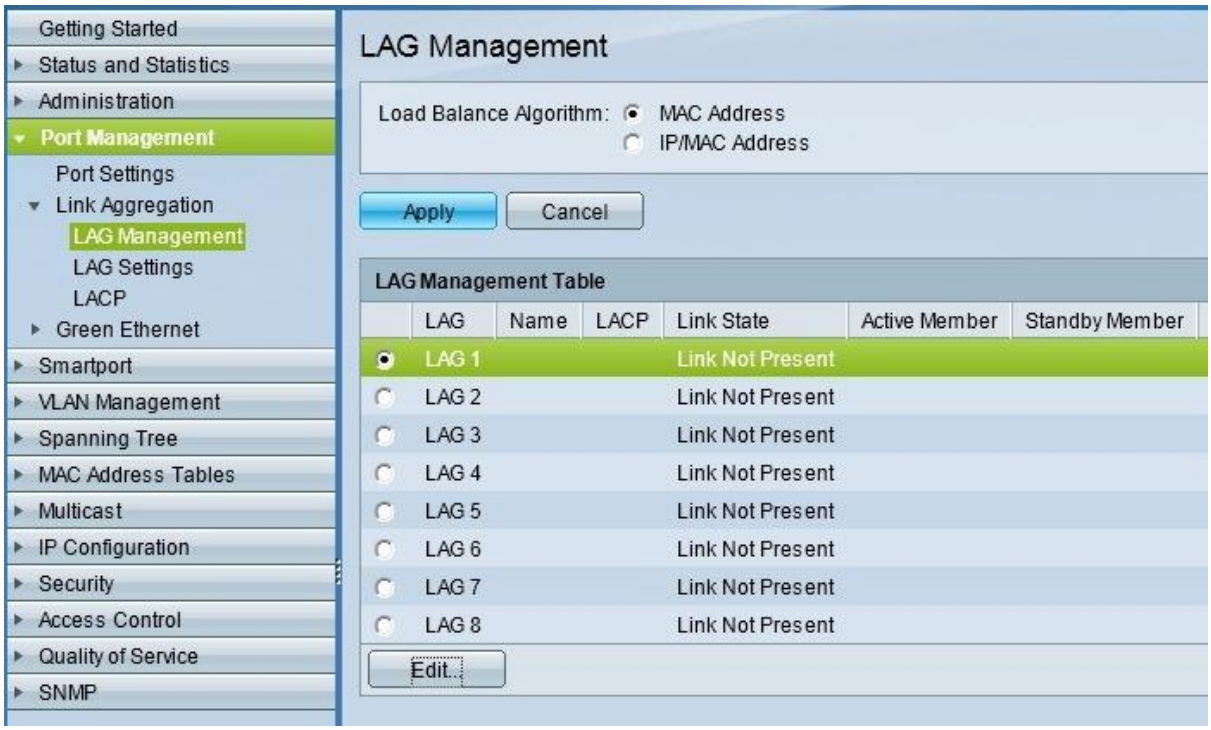
A LAG is a Link Aggregation Group. Some other switch manufacturers call this a Trunk. It allows multiple cables to make the same connection between switches. It is a form of cable redundancy: if one cable fails, the other one continues to carry all the data, so long as the bandwidth is not exceeded. With a 1GB bandwidth, the link is good for over 500 Dante audio channels at 48kHz, 24-bit. Note that this form of redundancy is not perfect: it can result in 0.5 to 1 second of silence after a break or a repair.

If the switch has just 2 fibre ports and they each need to connect to a different switch, then there is no reason to create a LAG. (Though of course a LAG could be created using two copper ports).

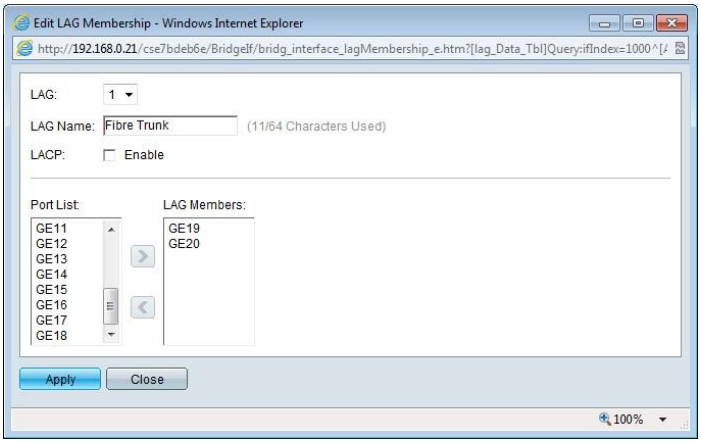
Before creating a LAG, make sure that the required ports are excluded from all VLANs other than the default VLAN1. Normally the LAG will be created to use ports 19 and 20: the two ports with optional fibre modules.

5.2 Create a LAG

To create a LAG, first open the **Port Management** menu, and select the **LAG Management** page. Then select LAG1 and click [Edit].



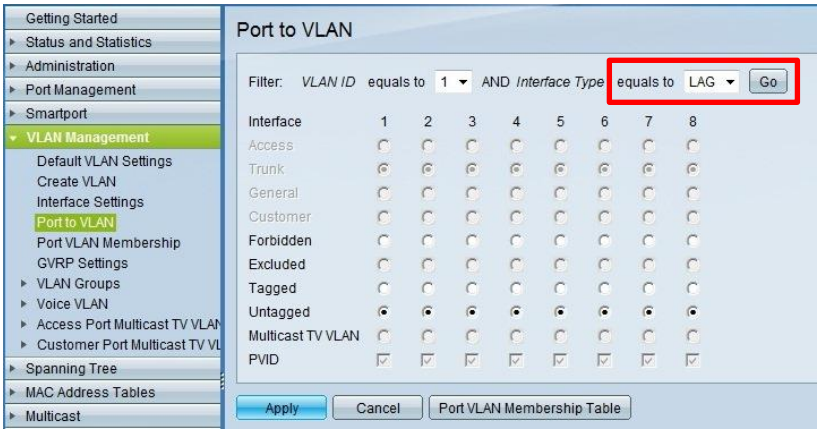
In the **Edit LAG Membership** window, give the LAG a suitable name, just for reference. You don't need to enable LACP. Select the LAG members from the port list: GE19 and GE20 in this case. Click [Apply].



5.3 Assign a LAG to VLANs

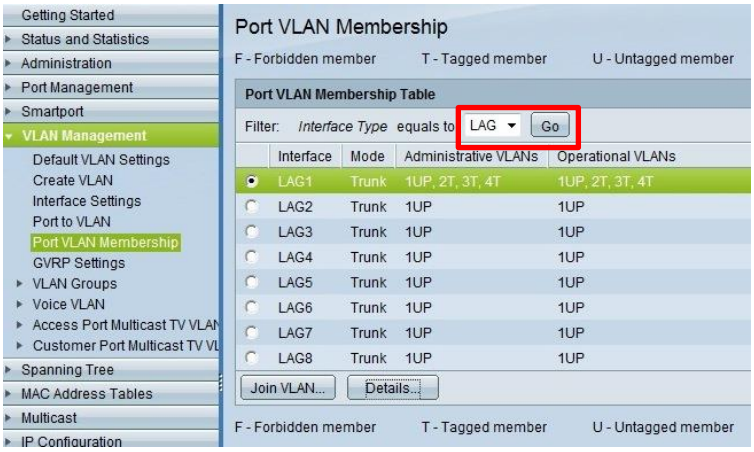
Once a LAG has been created, it needs to be assigned to VLANs, in the same way as a single port is assigned. The LAG should be left "untagged" for VLAN1, and "Tagged" for all the other VLANs.

This can be edited back in the **VLAN Management** menu, in the **Port To VLAN** page. Select "LAG" in the filter at the top of the window, then click [Go]. Then edit each VLAN setting in turn for LAG 1.



The most likely assignment for LAG 1 is to be "Untagged" with VLAN1 and "Tagged" with all other VLANs. LAGs 2-8 are unlikely to be used, unless the switch is placed at the centre of a star topology and cable redundancy is required.

The overall VLAN assignment can be checked in the **Port VLAN Membership** page, by selecting "LAG" as the filter and clicking [Go].



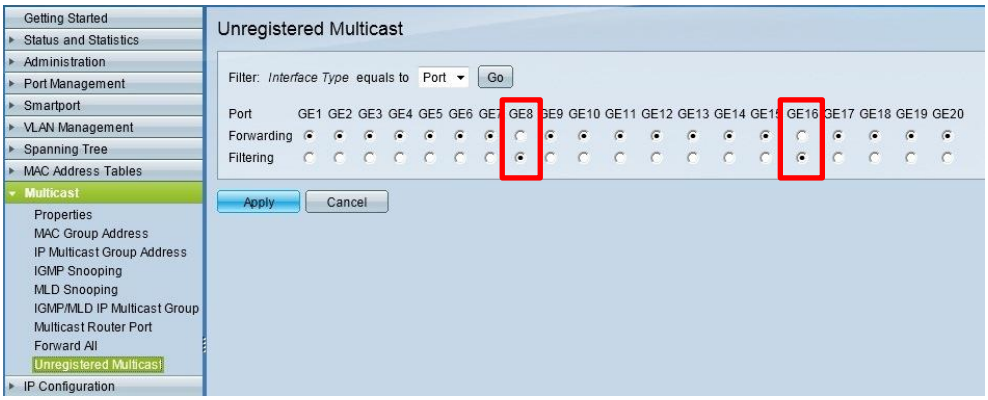
Remember to save the settings in the switch (see page **20**), and now it is ready to perform a wide range of tasks. Read on for further details about settings for more specialist duties.

6.0 Using Wi-Fi on the same VLAN as Dante

In many cases, communication data needing Wi-Fi will be kept on a separate VLAN to Dante data, so no special settings are required. However in some instances, Wi-Fi communication will be required to share the same VLAN as Dante. Using Lake Controller on a tablet PC to communicate with Lake LM44 or LM26 and Lab.Gruppen PLM amps is one example. In this case some extra settings are required. This is because Dante networks contain a certain amount of multicast data which can overload a Wi-Fi device. The solution is to filter out this multicast data from the Wi-Fi network.

6.1 Multicast Filtering

Open the **Multicast** menu, and view the **Unregistered Multicast** page. For the ports that are connected to Wi-Fi devices, select "Filtering" and click [Apply].



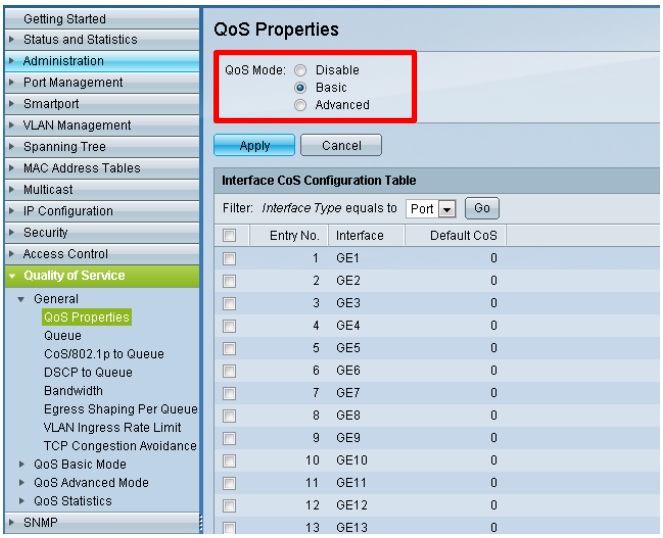
Now Wi-Fi control can be used on the same VLAN as Dante (though Dante audio cannot be transmitted over Wi-Fi, and Dante Controller software will also not function over Wi-Fi).

> *Note:*
> *If the "Wireless DCP" iPhone app is being used with Yamaha MTX3 or MTX5D, all ports should be kept in a "Forwarding" state, because this app uses Multicast data to detect the devices in the network. In that case, follow the advice in Appendix A3, regarding "IGMP Snooping".*

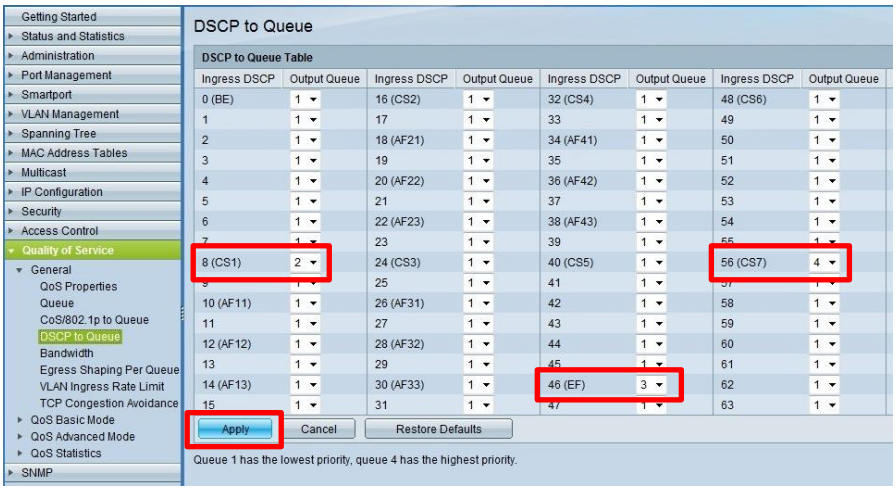
7.0 Programming QoS for Dante

In the majority of small audio networks, where all Dante devices have 1GB ports and there is little or no other data sharing the switch, QoS settings will not be important. However, as the channel count increases, or as other data types increase in bandwidth, editing the QoS settings will have benefits. Also, if some Dante devices in the system have 100MB ports, the correct QoS settings will be essential. Dante uses the DSCP type of QoS (Quality of Service). Different types of data are given different levels of priority. Timing data is most important, followed by audio and then control. All other data is of minimum importance.

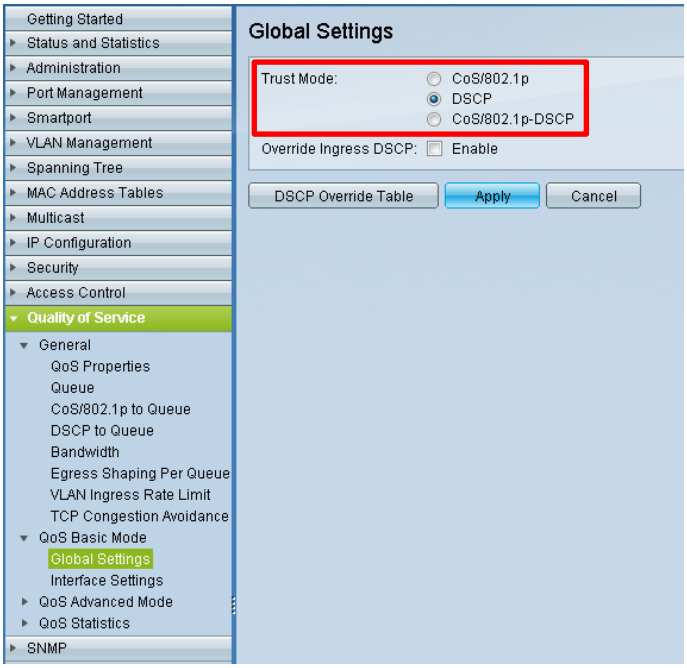
Open the **Quality of Service** menu, then open the **General** sub-menu, and select the **QoS Properties** page. Select the "Basic" mode for QoS, and click [Apply].



Now select the **DSCP to Queue** page. Make the following settings, then click [Apply]:
Set 56 (CS7) to 4,
Set 46 (EF) to 3,
Set 8 (CS1) to 2,
Set all others to 1.



Now to enable the DSCP scheme, open the **QoS Basic Mode** sub-menu, and select the **Global Settings** page.
Set “DSCP” as the Trust Mode.
Then click [Apply].
Once again, remember to save the configuration (see page **20**).



Correction:

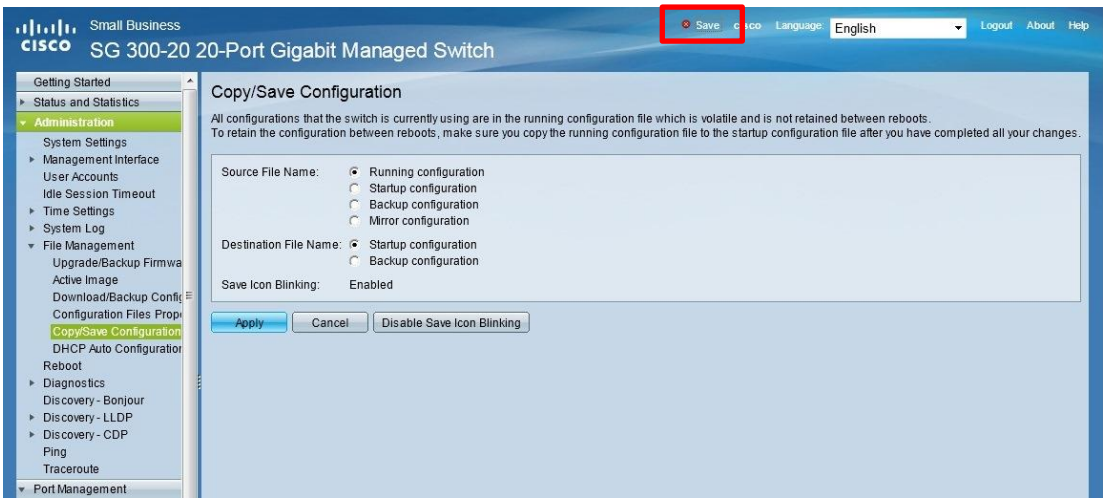
*In a previous version of this document, it wrongly stated to use the “Not Trusted” Default Mode in **QoS Advanced Mode, Global Settings**. Advanced Mode can still be used as an alternative, but it must have “Trusted” status for DSCP.*

Note:

In a mixed traffic environment, such as an office installation, and especially where a VoIP telephone system is used, these DSCP settings might need to be modified. Such modification is best left to a qualified network consultant who understands the various needs of all the services making use of the network.

8.0 Save & Load Switch Configurations

If you don't save the switch configuration, all the new settings will be lost after power is turned off. To save the settings, first click on the flashing "Save" icon at the top of the web browser window. Or open the **Administration** menu, then the **File Management** sub-menu, and view the **Copy/Save Configuration** page.



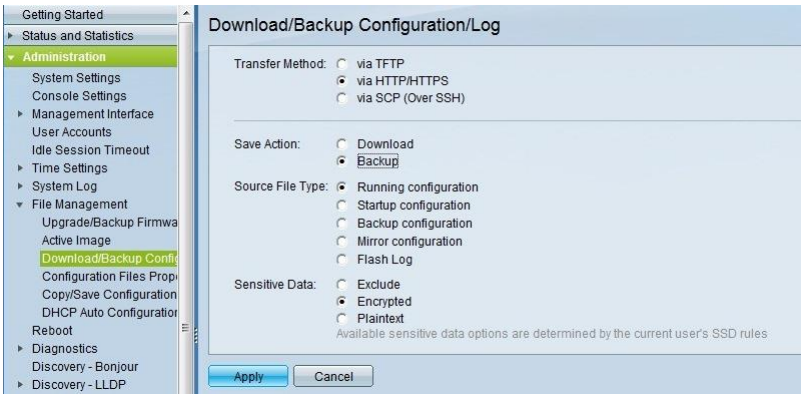
Select the "Running configuration" as the Source File, and the "Startup configuration" as the Destination File. Then click [Apply]. The process should take around 10 seconds to complete.

8.1 Backup

To backup the settings from the switch to the computer, so the same settings can be loaded into another switch, view the **Download/Backup Configuration** page in the same menu.

Select the "via HTTP/HTTPS" Transfer Method, and select the "Backup" Save Action. Then select the "Running Configuration" as the Source File. Click [Apply].

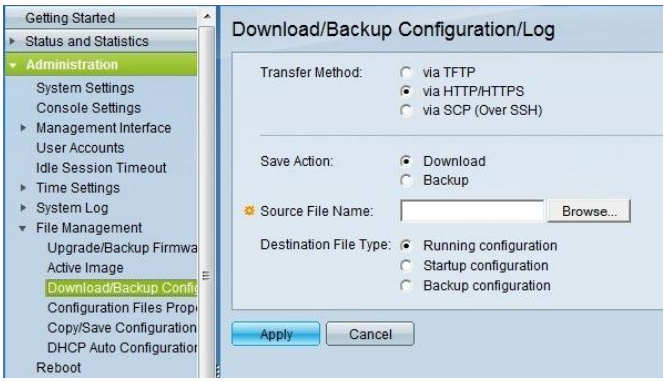
The resulting .txt file can be saved in the normal way via the web browser.



8.2 Download

To download a configuration from the computer to the switch, a lot of programming time can be saved. Use the same page in the web interface: **Download/Backup Configuration**.

Select the "via HTTP/HTTPS" Transfer Method, and select the "Download" Save Action. Browse for the Source File, and select "Running Configuration" as the Destination File. Click [Apply]. The process will normally take around 10 seconds to complete.

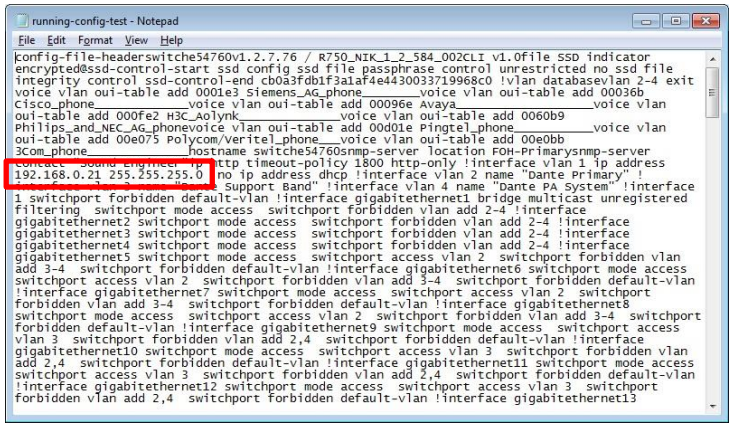


With older firmware versions, the "Running Configuration" option was not available as the Destination File. An option is to select "Startup Configuration". In that case, the switch will need to be rebooted after the download for the settings to take effect (see page **27**).

Note:

If the IP address contained in the new file is different to that of the switch's current IP address, communication with the PC may cease, and will need to be re-activated using the new IP address.

There is a way to check and edit the IP address before downloading the file to the switch: simply open the file with a text editor. Find where the IP address is listed, edit it, and save it. Now download it. Quick and easy!



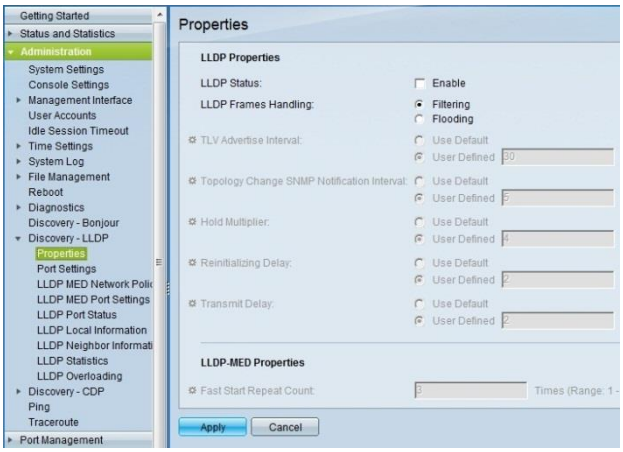
Appendix

A1 Settings needed for using this switch with EtherSound

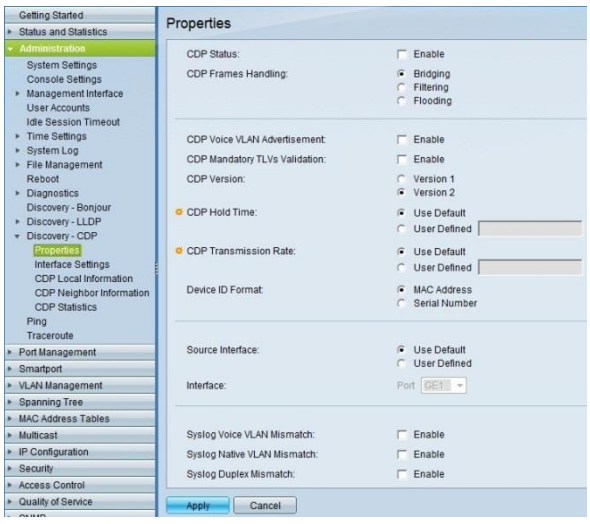
EtherSound audio networks require careful management. The EtherSound data must not be mixed with any other type of network data, so must be isolated by VLANs. It is strongly advised not to put EtherSound on VLAN1, which is the default VLAN used for switch management. The following settings need to be disabled, as they interfere with the EtherSound audio data.

Open the Administration menu, and view the **Discovery-Bonjour** page. Un-check “Enable” and click [Apply].

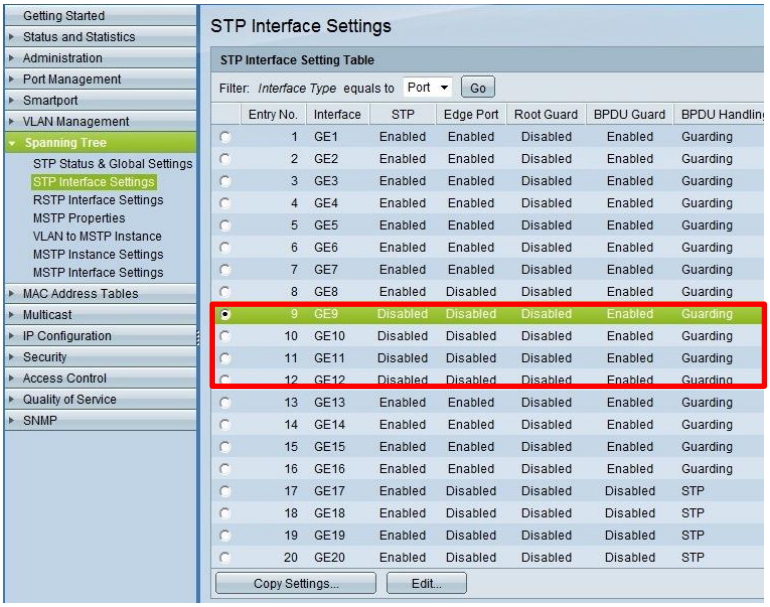
Open the **Discovery-LLDP** sub-menu and view the **Properties** page. Un-check “Enable” for the LLDP Status, and click [Apply].



Open the **Discovery-CDP** sub-menu and view the **Properties** page. Un-check “Enable” in all boxes. Click [Apply].



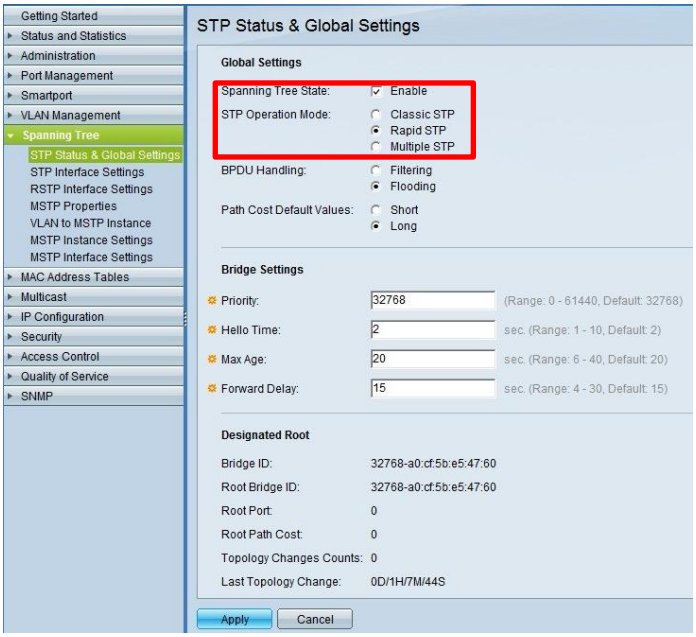
In the **Spanning Tree** menu, either disable Spanning Tree globally in the **STP Status & Global Settings** page (see below), or if Spanning Tree is required on the network, open the **STP Interface Settings** page, select the port used by EtherSound, and click [Edit]. Uncheck the “Enable” box for STP and click [Apply]. Do this for all the ports used by EtherSound devices. They should now be listed as “STP Disabled”.



A2 Spanning-Tree Protocol

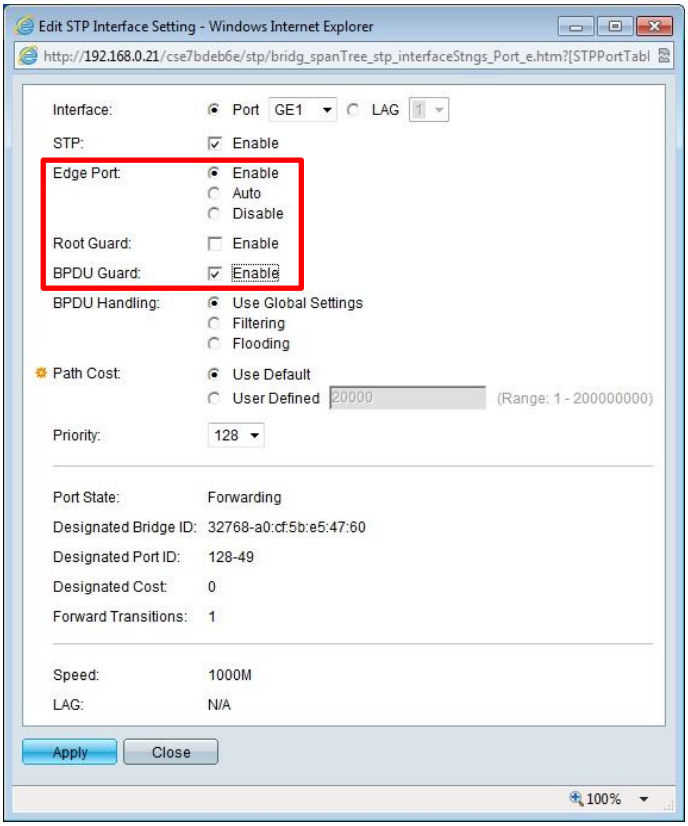
As explained in section **3.1**, Spanning-Tree Protocol is a form of network redundancy that will work alongside Dante, but will not cause glitch-free switch-overs. It is possible that silences of between 5 and 10 seconds will be experienced after a failure or a repair. However, using Spanning-Tree Protocol may be a requirement for a building or office network. In that case, it is best to leave the settings to a qualified network consultant. This document deals with the basic settings that can be prepared for the audio network.

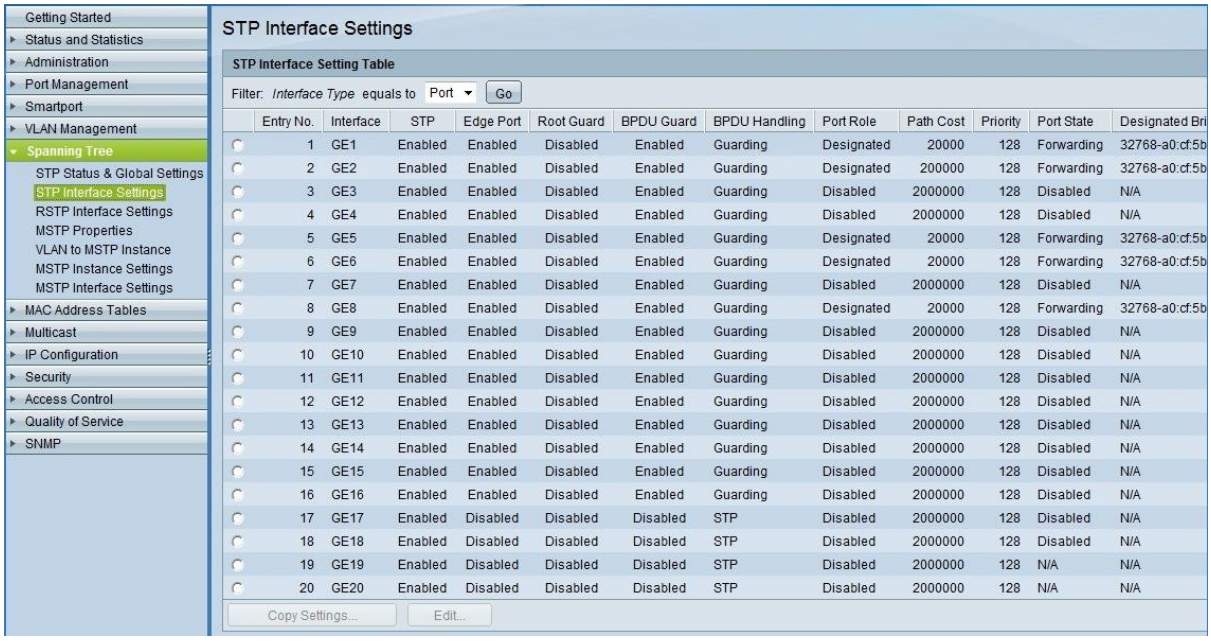
Open the **Spanning-Tree** menu, and select the **STP Status & Global Settings** page.
Check “Enable” for the Spanning Tree Stage, and select “Rapid STP” as the Operation Mode. Leave the other settings at their default value, and click [Apply].



In the **STP Interface Settings**, some configuration is recommended to limit the amount of STP traffic on all the ports that are not connected to another switch. Select the first port and click [Edit].

Select “Enable” for the Edge Port, and Enable the BPDU Guard.
Click [Apply].
Back in the **STP Interface Settings** page, select the first port again, and click [Copy Settings].
Type the numbers of the other ports in the “to” field, and click [Apply].
Remember, do not change the settings of the ports used to link with other switches, such as ports 19-20.

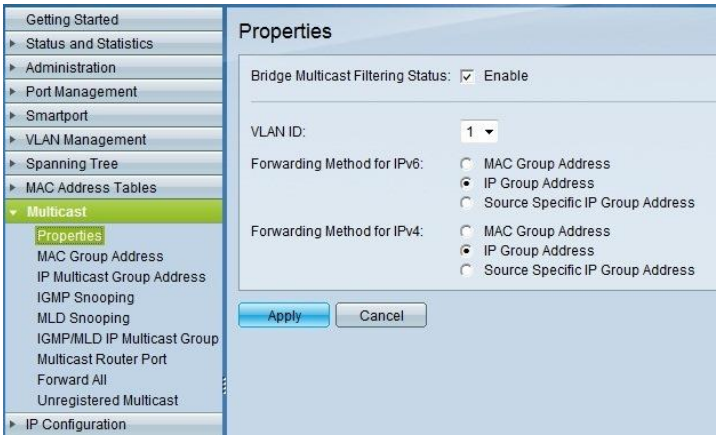




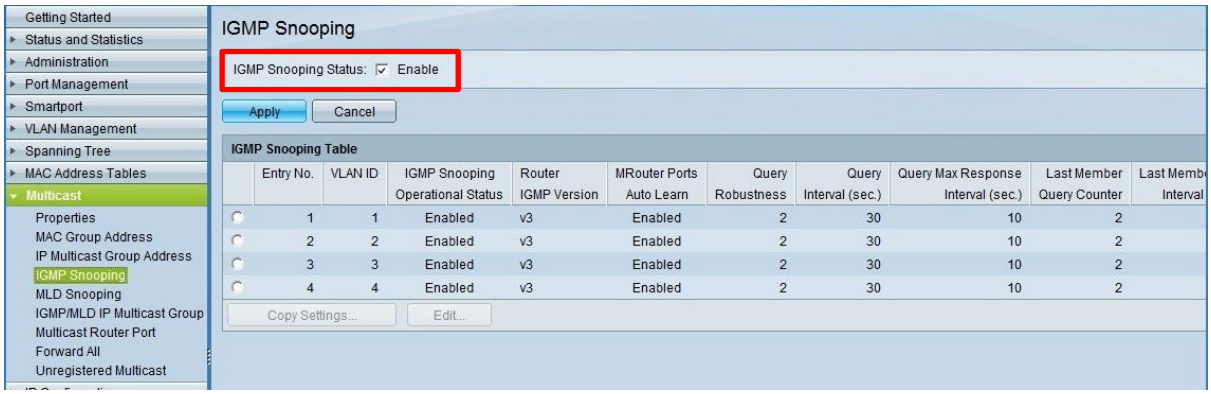
A3 IGMP Snooping

IGMP stands for Internet Group Management Protocol. It is a way of managing multicast data, so that a network does not get flooded with too much unnecessary data: it will stop multicast traffic from arriving at devices that do not need to receive it. For many audio networks used for live sound, it will not be necessary to enable. However, IGMP Snooping will be essential where multicast transmission is used with Dante devices that work at 100Mbps (rather than 1Gbps), and where audio control functions share the Dante network (as with Yamaha Nuage systems, Yamaha MTX5D, and many Lake & Lab.Gruppen devices). There are currently three different versions of IGMP Snooping. Version 3, with a "querier" function, is the most appropriate to use with a Dante network. It is a rare feature to find in lower cost switches: Cisco SG300 is one of the few in its price range to include IGMP Snooping V3.

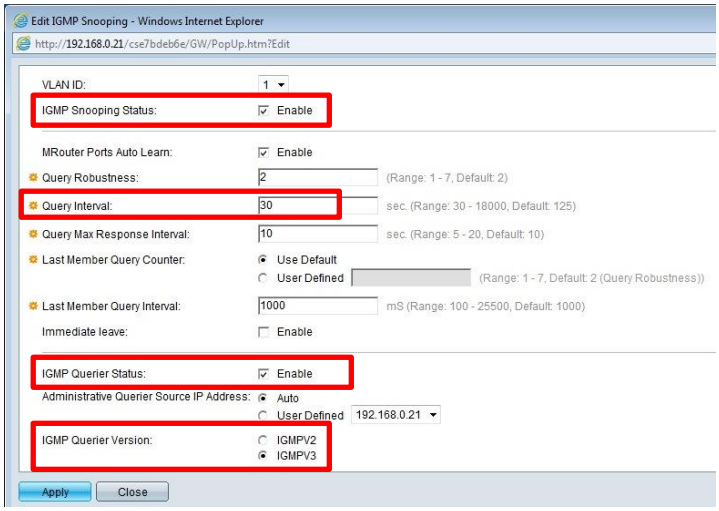
Firstly, open the **Multicast** menu. View the **Properties** page. Check the "Enable" box, select the required VLAN ID number, and select "IP Group Address" as the Forwarding Method for IPv6 and IPv4. Do the same for all required VLANs.



Next, view the **IGMP Snooping** page, and check the "Enable" box for IGMP Snooping Status. Now select the first required VLAN and click [Edit].

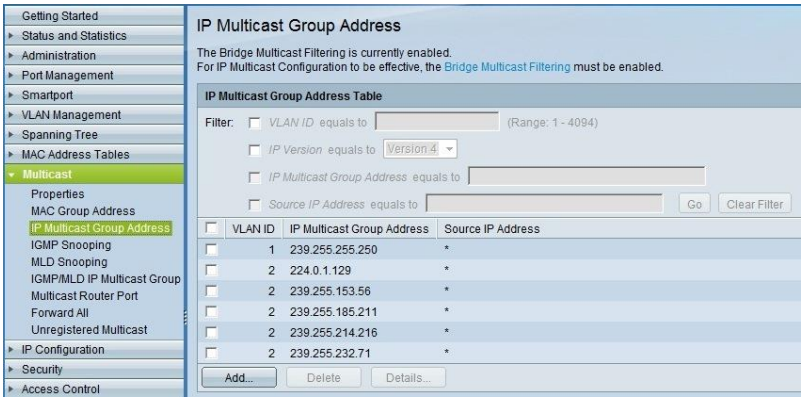


Enable the IGMP Snooping Status, set the Query Interval to 30, enable the IGMP Querier Status, and select IGMPv3 as the Querier Version. Click [Apply].
This querier status need not be enabled if there is a router or another switch in the network that is already performing that function.



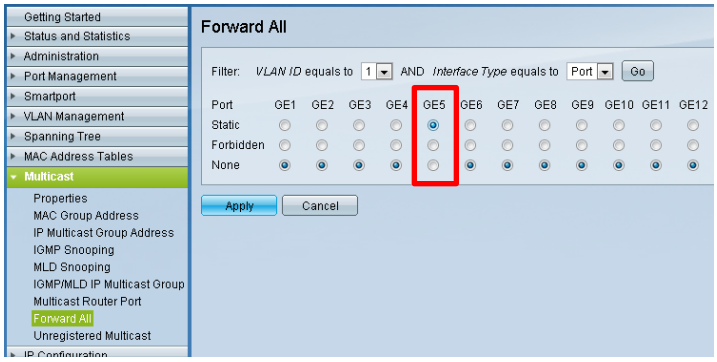
Apply the same settings to all the VLANs that are used for Dante.

Now the Multicast Group addresses can be seen in the **IP Multicast Group Address** page. This page can take up to 30 seconds to detect a new Multicast Group.



If IGMP snooping is enabled, the **Unregistered Multicast** filtering function mentioned in section 6 of this document should not be needed, and all ports can be set to “Forwarding” in that page.

IGMP Snooping & Dante Virtual Soundcard:
In some cases, a computer running DVS will fall silent during playback in a network where IGMP Snooping is enabled. This will be due to the limitations of the computer’s network interface.
To overcome this problem, the “Forward All” setting will need to be enabled for the switch port used by the computer. This needs to be used with caution, because it will allow all multicast traffic through the port. In the **Forward All** page, select “Static” for the required port, and click [Apply].



Special setting for "Wireless DCP" iPhone app:

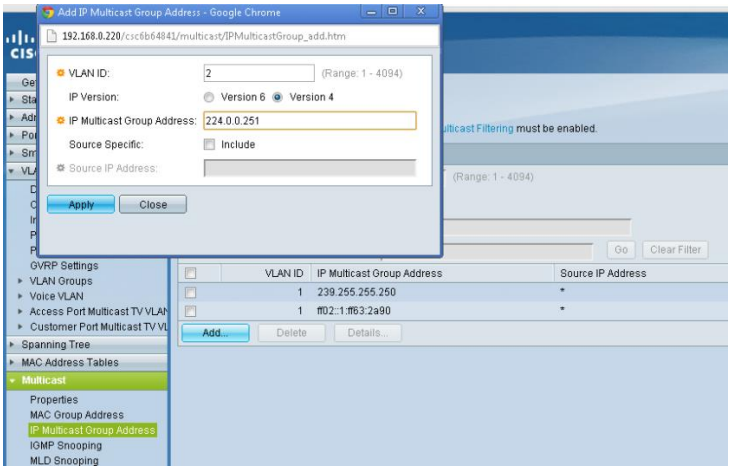
The "Wireless DCP" iPhone app, working with Yamaha MTX3 and MTX5D units, uses multicast traffic to discover the devices. In some cases, this might be blocked by the IGMP snooping function. To ensure that this data is not blocked, it is a good idea to manually register the IP address used by the multicast data:

In the **IP Multicast Group Address** page, click [Add].

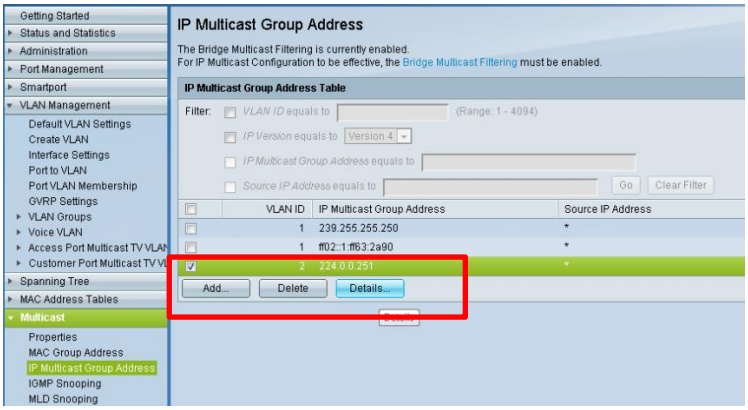
Select the appropriate VLAN ID, and type the IP address **224.0.0.251**.

This is the specific address used by "Wireless DCP".

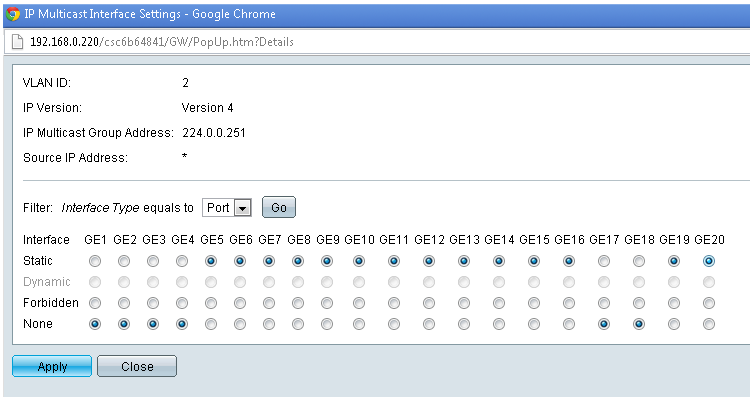
Click [Apply].



Now click in the checkbox for this Multicast Group Address, and click [Details].



Select "Static" for all the ports and LAGs used by Wireless DCP and the devices it needs to control.

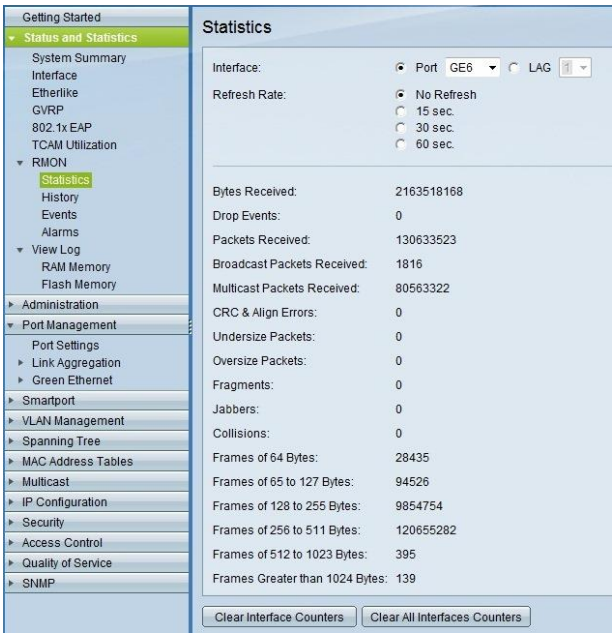


Once again, it is recommended to not deviate from these IGMP Snooping settings in a network unless it is administered by a qualified network engineer.

A4 Trouble-Shooting

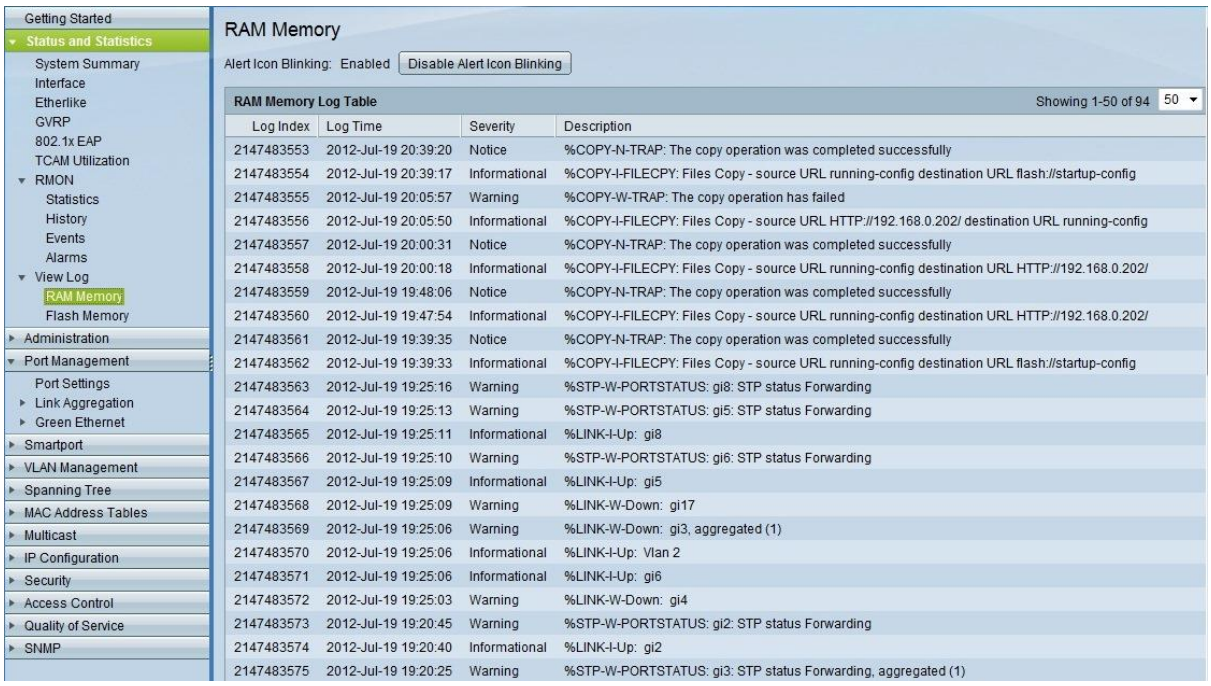
When trouble-shooting a network, it must be remembered that the vast majority of problems are caused by cable faults: whether they are crushed, bent, cut, stretched, or badly terminated. Or especially in the case of fibre-optics: dirty. Problem cables will cause lost data, or errors. These can be monitored in the web browser interface of the switch.

Open the **Status and Statistics** menu, then the **RMON** menu. And select the **Statistics** page. RMON is "Remote Network Monitoring". It will show the number of errors that have occurred, and the number of packets that have passed through each port.



Switch Log

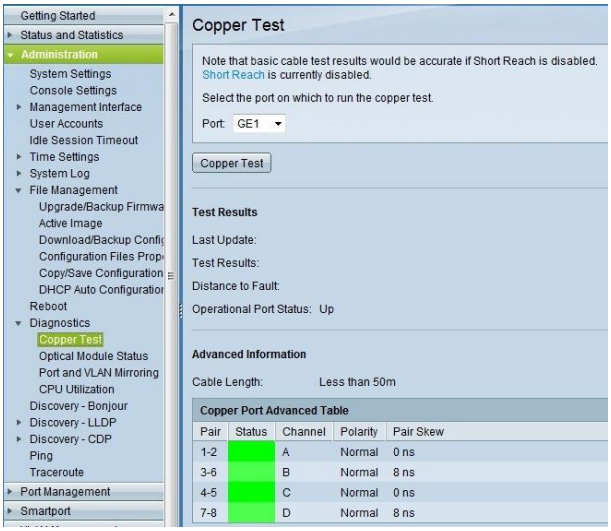
If there is an intermittent connection between a cable and the switch, it could show up in the Log. Also the activity of connecting and disconnecting cables can be checked. Open the **View Log** sub-menu, and select the **RAM Memory** page.



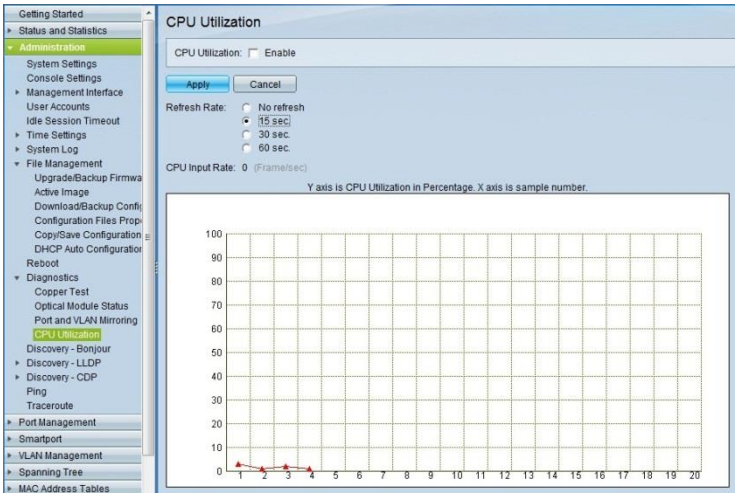
Cable Check

This switch can perform a simple cable test, to check for problems. Open the **Diagnostics** sub-menu and select the **Copper Test** page. The cable must be connected to a device at the other end. Select the required Port, and click [Copper Test].

If there is an audio device at the far end, remember to mute the outputs first, just in case.



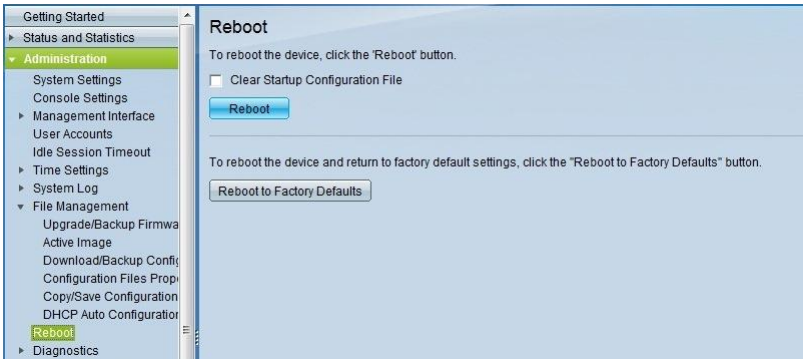
To check how hard the switch itself is working, open the **Diagnostics** sub-menu, and select the **CPU Utilization** page. It should be highly unusual to ever reach 70%. If it does, it would be time to think about a network upgrade!



Reboot & Initialize

To Reboot the switch without needing to access the power connector, open the **Administration** menu, and select the **Reboot** page. Click [Reboot].

Don't check the "Clear Startup Configuration File" box, unless all the settings need to be returned to their initial status (including the IP Address).



To completely initialize all the switch settings, a paper clip (or similar item) can be inserted into the small hole marked "Reset" on the left side of the front panel. Press and hold for more than 10 seconds, then release and wait 2 minutes for the switch to fully reboot. Alternatively, click [Reboot to Factory Defaults] in the **Reboot** page.