

# Setting up a switch for use with Dante

Using the Cisco SG300-20 or Teqsas CyberTEQ-m



# Contents

Chapter	Title	Page
1.0	The advantages of this Switch	2
2.0	Getting Started: Firmware, IP Address & Password	2
2.1	Login	2
2.2	Firmware Update	3
2.3	IP Address	5
2.4	System Information	5
2.5	EEE	6
3.0	Simple System Network Design	7
3.1	System Topology Tips	9
4.0	Programming VLANs	11
4.1	Using one switch for several different types of data	11
4.2	Create A VLAN	11
4.3	Switch Port Mode	11
4.4	Planning the use of VLANs	12
4.5	Assigning Ports to VLANs	13
5.0	Programming a LAG (or Trunk)	15
5.1	Cable Redundancy between two switches	15
5.2	Create a LAG	15
5.3	Assign a LAG to VLANs	16
6.0	Using Wi-Fi on the same VLAN as Dante	17
6.1	Multicast Filtering	17
7.0	Programming QoS for Dante	18
8.0	Save & Load switch configurations	20
8.1	Backup	20
8.2	Download	21
Appendix		22
A1	Settings needed for using this switch with EtherSound	22
A2	Spanning-Tree Protocol	22
A3	IGMP Snooping	25
A4	Trouble-Shooting	28
	Switch Log, Cable Check, Reboot & Initialize	29

# 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.

(ou can get IP settings assigned a his capability. Otherwise, you ne for the appropriate IP settings.	automatically if your network support eed to ask your network administrator
Obtain an IP address autom	atically
Output In the following IP address	5:
IP address:	192.168.1.100
Subnet mask:	255.255.255.0
Default gateway:	
Obtain DNS server address	automatically
Use the following DNS serve	r addresses:
Preferred DNS server:	· · · ·
Alternate DNS server:	•
-	(

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.

Small Business		cisco Language English	<ul> <li>Logout About Help</li> </ul>
cisco SG 300-20	20-Port Gigabit Managed Switch		
0000020	20 Fort organit managoa o mitor		
Getting Started	Cotting Started		
<ul> <li>Status and Statistics</li> </ul>	Getting Started		
<ul> <li>Administration</li> </ul>			and the second
<ul> <li>Port Management</li> </ul>	This page provides easy steps to configure your device		
▶ Smartport			
▶ VLAN Management	Notial Setup	🔀 Quick Access	
Spanning Tree	Change Device IP Address	Change Device Password	
MAC Address Tables	Create VI AN	Upgrade Device Software	
▶ Multicast	Configure Dark Collings	Reduc Davies Configuration	
▶ IP Configuration	Conligure Fort Settings	Backup Device Configuration	
▶ Security		Create MAC-Based ACL	
Access Control	Device Status	Create IP-Based ACL	
<ul> <li>Quality of Service</li> </ul>	System Summary	Configure QoS	
► SNMP	Port Statistics	Configure Port Mirroring	
	RMON Statistics		
	View Log		
		5	
	Other many research Frances		
	Other resources, Support Forums		
	Do not show this page on startup		

#### 2.2 Firmware Update

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

2000	cisco SG300-20 2	20-Port Gigabit M	anaged Switch			
	Getting Started	System Summary				
	<ul> <li>Status and Statistics</li> <li>System Summary</li> </ul>	System Information			Software Information	
	Interface Etherlike	System Operational Mode:	L2 Mode		Firmware Version (Active Image):	1.3.0.62
	GVRP	System Description:	20-port Gigabit Managed Switch		Firmware MD5 Checksum (Active Image):	22347bc1ad4f7f75526896a565dc71c5
	802.1x EAP	System Location:	Stage-Primary	Edit	Firmware Version (Non-active):	1.2.7.76
	► RMON	System Contact:	Andy	Edit	Firmware MD5 Checksum (Non-active):	01e9f0b789ff44bf7e8956fbdb339f2c
	▶ View Log	Host Name:	switch632a90	Edit	Boot Version:	1.1.0.6
	<ul> <li>Administration</li> </ul>	System Object ID:	1.3.6.1.4.1.9.6.1.83.20.1		Boot MD5 Checksum:	8c6b1f42c0754ab9c70324a815a45f08
	<ul> <li>Port Management</li> </ul>	System Uptime:	0 day(s), 0 hr(s), 12 min(s) and 58 sec(s)	i.	Locale:	en-US
	<ul> <li>Smartport</li> <li>VLAN Management</li> </ul>	Current Time:	15:07:59;2013-May-02		Language Version:	1.3.0.62
	<ul> <li>Spanning Tree</li> </ul>	Base MAC Address:	64:d8:14:63:2a:90		Language MD5 Checksum:	N/A
	MAC Address Tables	Jumbo Frames:	Disabled			
	a barration and					

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

						(invite in the second
🕣 🧭 http://se	oftware. <b>cisco.com</b> /download/release	.html?mdfid=283019616&flowid=18904&softwa 🔎 - 🖹 C 🗙 🧔 Cisco	Systems ×	Const. or	Course of Garden, 1	â 🖈
	10.10		M	issingResourceException	[] MissingResourceException	
	cisco				Q	
	Download Sc	oftware		B Download Cart	(0 items) + Feedback Help	
	Downloads Home > Produ	icts > Switches > LAN Switches - Small Business > Cisco Small Business	300 Series Managed Swit	ches >		
	Cisco SG300-20 20-Port G	igabit Managed Switch > Switch Firmware-1.3.0.62	ooo oonoo managoo om			
	Cisco \$G300-20 20	Port Gigabit Managed Switch				
	01300 30300-20 20	- or olgabit managed owner				
	Search.	Release 1.3.0.62	Release	Notes and Open So	urce Documentation	
	Search Collapse All	Release 1.3.0.62	Release Date	Notes and Open So	urce Documentation 🛛 🗮 🚕	
	Search (Collapse All Expand All   Collapse All • Latest Releases 13.0.62 1.1.2.0	Release 1.3.0.62 File Information A \$x300 Firmware Version 1.3.6.2 \$x300 FirM_1.3.0 62.res	Release Date 21-MAY-2013	Notes and Open So Size 6.58 MB	Download	
	Search Expand All   Collapse All - Latest Releases 1.3.0.02 1.1.2.0 - All Releases + 1.1	Release 1.3.0.62 File Information A 5:300 [FW] 13.0.62 5:300 [FW] 13.0.62 res 5:300 German (Germany) Language File Version 1.3.0.62 5:300 LAVG, eb E, 13.0.62 lang	Release Release Date 21-MAY-2013 21-MAY-2013	Notes and Open So Size 6.58 MB 0.76 MB	Download	
	Expand All   Collapse All Expand All   Collapse All Latest Releases 1.2.0 All Releases 1.1 All Releases 1.1 1	Release 1.3.0.62 File Information Study Envoyee Version 1.3.0.62 Study Envoyee Version 1.3.0.62 Study Envoyee Dec 1.3.0.62 Study Envoyee Dec 1.3.0.62 Study Envoyee Dec 1.3.0.62 Study Envoyee Study Envoyee File Version 1.3.0.62 Study Envoyee	Release Date           21-MAY-2013           21-MAY-2013           21-MAY-2013	Notes and Open So Size 6.58 MB 0.76 MB 0.73 MB	Luce Documentation R A	
	Search. Expand All Collapse All • Latest Releases 1.12.0 • All Releases • 1.1 • 1	Release 1.3.0.62           File Information *           S309 Firmware Version 1.3.6.2           S309 Low (Gramary) Language File Version 1.3.0.62           S309 Carbon (Gramary) Language File Version 1.3.0.62           S309 Carbon (Final Coll Language File Version 1.3.0.62           S309 Low (Final Coll Language File Version 1.3.0.62           S309 Low (Final Coll Language File Version 1.3.0.62           S309 Low (Final Coll Language File Version 1.3.0.62	Release         Date           21-MAY-2013         21-MAY-2013           21-MAY-2013         21-MAY-2013           21-MAY-2013         21-MAY-2013	Noles and Open So Size 6.58 MB 0.76 MB 0.73 MB 0.75 MB	Looving Contention Contentico Contentico Contentico Contentico Contentico Contentico Con	
	Search. Erpand All Colapse All • Latest Releases 1.1.2.0 • All Releases • 1.1 • 1	Release 1.3.0.62           File Information A           SX00 Firmware Version 1.3.6.2           SX00 prw.1.3.0.62 res           SX00 cross (Gremany) Language File Version 1.3.0.62           SX00 press (LATAM) Language File Version 1.3.0.62           SX00 press (LATCA) (LATAM) Language File Version 1.3.0.62           SX00 press (LATCA) (LATAM) Language File Version 1.3.0.62           SX00 press (LATCA) (LATAM) (LANGUAGE)           SX00 press (LATCA) (LATCA) (LANGUAGE)	Release         Release           Release Date         21-MAY-2013           21-MAY-2013         21-MAY-2013           21-MAY-2013         21-MAY-2013           21-MAY-2013         21-MAY-2013	Notes and Open So           Size           6.58 MB           0.76 MB           0.75 MB           0.75 MB           0.72 MB	La construction R A	

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].

CISCO SG 300-20 2	0-Port Gigabit Managed Switch	Logout About Help
Getting Started Status and Statistics	Upgrade/Backup Firmware/Language	
Administration     System Settings     Management Interface	Transfer Method: C via TFTP Via HTTP/HTTPS	
User Accounts Idle Session Timeout Time Settings System Log	Save Action: V Upgrade C Backup File Type: V Firmware Image	
<ul> <li>File Management         Upgrade Rookup Filmwarel Active Image Download/Backup Configur.     </li> </ul>	Boot Code     Clanguage File     Browse	
Configuration Files Properti Copy/Save Configuration DHCP Auto Configuration Reboot Diagnostics	The firmware is upgraded to the inactive image file. You must activate the firmware using the "Active Image" page. Apply Cancel	

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.

Getting Started	IPv4 Interface		
Status and Statistics     Administration	Management VLAN:	1 -	
Management Interface     IPv4 Interface	IP Address Type:	⊂ Dynamic ● Static	
IPv6 Global Configuration IPv6 Interface	🙁 IP Address:	192.168.0.21	
IPv6 Addresses IPv6 Default Router List IPv6 Tunnel	🐱 Mask:	Network Mask 255.255.255.0     Prefix Length	(Range: 8 - 30)
IPv6 Neighbors IPv6 Routes User Accounts Idle Session Timeout	Administrative Default Gateway:	<ul> <li>User Defined</li> <li>None</li> </ul>	
<ul> <li>▶ Time Settings</li> <li>▶ System Log</li> </ul>	Operational Default Gateway:	- Enable	
<ul> <li>File Management Reboot</li> </ul>	Auto Configuration via DHCP:	Enabled	
<ul> <li>Diagnostics</li> <li>Discovery - Bonjour</li> <li>Discovery - LLDP</li> </ul>	Apply Cancel		

#### 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".

cisco SG300-20 2	20-Port Gigabit M	anaged Switch			
Getting Started  Status and Statistics	System Summary				
System Summary	System Information			Software Information	
Interface Ethoriike	System Operational Mode:	L2 Mode		Firmware Version (Active Image):	1.3.0.62
GVRP	System Description:	20-port Gigabit Managed Switch		Firmware MD5 Checksum (Active Image):	22347bc1ad4f7f75526896a565dc71c5
802.1x EAP	System Location:	Stage-Primary	Edit	Firmware Version (Non-active):	1.2.7.76
TCAM Utilization	System Contact:	Andy	Edit	Firmware MD5 Checksum (Non-active):	01e9f0b789ff44bf7e8956fbdb339f2c
<ul> <li>View Log</li> </ul>	Host Name:	switch632a90	Edit	Boot Version:	1.1.0.6
<ul> <li>Administration</li> </ul>	System Object ID:	1.3.6.1.4.1.9.6.1.83.20.1	_	Boot MD5 Checksum:	8c6b1f42c0754ab9c70324a815a45f08
System Settings	System Uptime:	0 day(s), 1 hr(s), 31 min(s) and 32 sec(	5)	Locale:	en-US
Console Settings     Management Interface	Current Time:	18:00:36;2013-Oct-01		Language Version:	1.3.0.62
User Accounts	Base MAC Address:	64:d8:14:63:2a:90		Language MD5 Checksum:	N/A
Idle Session Timeout	Jumbo Frames	Disabled			
System Log					

### 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].

Small Business		
CISCO SG300-20 2	20-Port Gigabit Managed Switch	
Getting Started	Bronottion	
<ul> <li>Status and Statistics</li> </ul>	Fiopenies	
<ul> <li>Administration</li> </ul>	For the functions and/or parameters configured on this page	e to herome effertive
✓ Port Management	you may have to configure the corresponding port based pa	rameters on Port Settings page.
Port Settings	Energy Detect Mode:	Enable
<ul> <li>Link Aggregation</li> </ul>	Chart Deach:	- Enable
<ul> <li>Green Ethernet</li> </ul>	Short Neach.	Litable
Properties	Port LEDs:	🔽 Enable
Port Settings	Power Savings:	77 %
<ul> <li>Smartport</li> </ul>	Cumulative Energy Saved:	0 Watt Hour
<ul> <li>VLAN Management</li> </ul>	Cumulative Energy Saveu.	o waarioor
<ul> <li>Spanning Tree</li> </ul>		
<ul> <li>MAC Address Tables</li> </ul>	802.3 Energy Efficient Ethernet (EEE):	📃 Enable
<ul> <li>Multicast</li> </ul>		
<ul> <li>IP Configuration</li> </ul>	Apply Cancel	
► Security		

# 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.



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 troubleshoot, 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.

Getting Started Create VLAN Status and Statistics Administration VLAN Table Port Management VLAN ID VLAN Name Type Smartport 厂 1 Default 2 Dante Primary Static Default VLAN Settings 3 Dante Support Band Static Add... Edit. Interface Settings Port to VLAN Port VLAN Membership **GVRP** Settings VLAN Groups Voice VLAN

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!

VLAN ID:	2	(Range: 2 - 4094)	
VLAN Name:	Dante Primary	(13/32 Characters Used)	
C Range VLAN Range:		-	(Range: 2 - 4094

### 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.

Getting Started	Inter	face Se	ttinge	-			
<ul> <li>Status and Statistics</li> </ul>	inte	nace Se	ungs				
<ul> <li>Administration</li> </ul>		Succose	To perm	anontiv cavo t	the configuration	on an to t	DO Convilonuo
<ul> <li>Port Management</li> </ul>		Success.	ro penna	anenity save i	ine configuration	on, go to t	ic copyraave
<ul> <li>Smartport</li> </ul>	Inte	daan Cattin	- Table				
<ul> <li>VLAN Management</li> </ul>	inte	nace setur	ig rable		$\sim$		
Default VLAN Settings	Filte	r: Interface	Type equ	als to Port 🔻	Go		
Create VLAN		Entry No.	Interface	Interface	Administrative	Frame	Ingress
Port to VI AN				VLAN Mode	PVID	Туре	Filtering
Port VLAN Membership	0	1	GE1	Access	1	Admit All	Enabled
GVRP Settings	0	2	GE2	Access	1	Admit All	Enabled
<ul> <li>VLAN Groups</li> </ul>	0	3	GE3	Access	1	Admit All	Enabled
► Voice VLAN	C	4	GE4	Access	1	Admit All	Enabled
Access Port Multicast TV VLAP Customer Port Multicast TV VI	0	5	GE5	Access	1	Admit All	Enabled
Snanning Tree	0	6	GE6	Access	1	Admit All	Enabled
MAC Address Tables	0	7	GE7	Access	1	Admit All	Enabled
Multicast	C	8	GE8	Access	1	Admit All	Enabled
IP Configuration	0	9	GE9	Access	1	Admit All	Enabled
<ul> <li>Security</li> </ul>	0	10	GE10	Access	1	Admit All	Enabled
Access Control	0	11	GE11	Access	1	Admit All	Enabled
Quality of Service	C	12	GE12	Access	1	Admit All	Enabled
▶ SNMP	0	13	GE13	Access	1	Admit All	Enabled
	C	14	GE14	Access	1	Admit All	Enabled
	0	15	GE15	Access	1	Admit All	Enabled
	C	16	GE16	Access	1	Admit All	Enabled
	0	17	GE17	Access	1	Admit All	Enabled
	0	18	GE18	Access	1	Admit All	Enabled
	0	19	GE19	Trunk	1	Admit All	Enabled
	C	20	GE20	Trunk	1	Admit All	Enabled
		Copy Set	tings	Edit			
•             •	1						

Interface: Interface VLAN Mode:	<ul> <li>Port G</li> <li>General</li> </ul>	
	Access	
	C Custom	er (The switch will be in Q-in-Q mode when it has one or more customer ports
Administrative PVID:	1	(Range: 1 - 4094, Default: 1)
Frame Type:	Admit Al	l agged Only ntagged Only
Ingress Filtering:	Enable	
Apply Close		

Copy configuration	from entry 1 (GE1)
to: 2-18	(Example: 1,3,5-10 or: GE1,GE3-GE5)
Apply	Close

#### 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.

Getting Started	Port to VI AN																				
<ul> <li>Status and Statistics</li> </ul>	FUILIO VLAIN																				
<ul> <li>Administration</li> </ul>		norm	anonti	v covo	tho c	opfique	ration	an to	the Cr	nulCou	o Confi	ourotio		or clic	k tho	Cavo i	con				
Port Management	Success. To	penn	anenu	y save	e une cu	Jinigu	auon	go io	uie ou	pyioav	e com	guradu	page	OF CH	A the	Savei	COII.				
<ul> <li>Smartport</li> </ul>			_																		
<ul> <li>VLAN Management</li> </ul>	Filter: VLAN ID	equals	to 2	▼ A1	ND Inte	rface Tj	iype e	quals to	Port	•	Go										
Default VLAN Settings				-					_												
Create VLAN	Interface	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10	GE11	GE12	GE13	GE14	GE15	GE16	GE17	GE18	GE19	GE20
Interface Settings	Access	6	()	6	6	6	6	6	6	(	()	6	C	6	6	C	6	6	()	C	C
Port to VLAN	Trunk	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	6	6
Port VLAN Membership	General	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C
GVRP Settings	Customer	C	C	C	C	C	C	C	C	0	C	C	C	C	0	C	C	0	c	C	C
<ul> <li>VLAN Groups</li> </ul>	Cashiddee	-		0	-	-	-	-	~	-		-	0		0	0	0	0		0	0
Voice VLAN	Forbidden	2				-	-	-													
<ul> <li>Access Port Multicast TV VLAN</li> </ul>	Excluded	C	C)	C	C	0	C	0	C	C	C	C	C	C	0	C	C	C	C	C	C
<ul> <li>Customer Port Multicast TV VL</li> </ul>	Tagged	C	C	0	C	C	0	C	C	0	0	0	C	0	C	C	C	C	C	(•	•
<ul> <li>Spanning Tree</li> </ul>	Untagged	C	C	C	C	•	(•	•	(•	C	C	C	C	C	C	С	C	C	C	С	C
<ul> <li>MAC Address Tables</li> </ul>	Multicast TV VLAN	C	С	С	C	C	C	С	C	С	C	С	C	C	C	С	C	C	С	C	C
<ul> <li>Multicast</li> </ul>	PVID	Г		Π.	Г	$\overline{\mathbf{v}}$	$\overline{\mathbf{V}}$	1V	$\overline{\mathbf{V}}$	Г			Г		Г	П	Г	Г			Г
<ul> <li>IP Configuration</li> </ul>																					
▶ Security	Apply	ancel	P	ort VLA	V Memb	ership	Table														
Access Control								~													

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.

Getting Started	Port to VI AN																				
<ul> <li>Status and Statistics</li> </ul>	FOILIO VLAN																				
Administration			anonti		the e	opfiqu	ration	an to	the or					oralia	uk the	Cours i					
Port Management	Success. To	penn	anenu	y save	e une c	onngu	nation,	yo to	ine ci	py/sav	e Conii	guratio	page		.k ule	Saver	COII.				
Smartport																					
<ul> <li>VLAN Management</li> </ul>	Filter: VLAN ID	equals	s to 3	▼ Al	VD Inte	erface T	vpe e	quals to	Port	•	Go										
Default VLAN Settings																					
Create VLAN	Interface	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10	GE11	GE12	GE13	GE14	GE15	GE16	GE17	GE18	GE19	GE20
Interface Settings	Access	0	6	6	()	6	6	6	G	(	6	6	6	6	6	6	6	6	6	C	C
Port to VLAN	Trunk	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	6	(=
Port VLAN Membership		C	C	C	C	C	C	C	C	C	C	0	C	C	C	C	C	C	C	C	C
GVRP Settings	Customer	~	~	~	~	0	~	~	0	~	~	~	~	0	~	~	~	~	~	~	~
VLAN Groups	Customer	1	1	2		19/		1			1	2		-	-	1	1	1	1	12	
Voice VLAN	Forbidden	(	(•	(•	(•	•	(•			0	C	0	C	•	(•	0	(	(•	0	C	0
Access Port Multicast TV VLAN	Excluded	C	C	C	С	С	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C
Customer Port Multicast TV VL	Tagged	0	C	C	C	C	0	0	C	C	0	C	C	C	C	C	C	0	C		
Spanning Tree	Untagged	C	C	C	C	С	С	C	C		(•			С	C	C	C	C	C	С	C
MAC Address Tables	Multicast TV VLAN	C	C	C	C	C	C	C	C	C	C	C	C	C	C	с	C	C	C	C	C
Multicast	PVID	Г	_	Г		F		Г	Г	V	2			F		Г	Г	Г	_	Г	F
IP Configuration	2.937.2	5.9H	100	(See	A. Carlos	11	0-0	Ser	100	Sin (	See.	Shirt	a starter	15	0-0	Seat	Sec.	0.00	100	0.00	All search
Security	Apply	ancel	P	ort VLA	N Memi	bership	Table	1													
Access Control								)													

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

Getting Started	Port to VI AN																				
<ul> <li>Status and Statistics</li> </ul>	FUILIO VLAN																				
<ul> <li>Administration</li> </ul>				-					-												
Port Management	Filter: VLAN ID	equals	s to 1	• Al	ND Inte	rface T	ype e	quals to	Port	-	Go										
<ul> <li>Smartport</li> </ul>	Interface	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10	GE11	GE12	GE13	GE14	GE15	GE16	GE17	GE18	GE19	GE20
✓ VLAN Management	Access	0	0	0	6	6	6	0	6	0	6	0	6	0	0	G	6	0	0	C	C
Default VLAN Settings	Trunk	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	6	6
Create VLAN	General	C	C	C	C	C	C	0	0	C	C	C	C	0	0	0	C	0	C	C	C
Interface Settings	Customor	0	~	~	~	~	~	~	~	~	~	~	~	~	~	~	~	~	~	~	
Port to VLAN	Customer	-	2	0	-	~	0	0	-	-	-	-	-	-	-	-	-	2	2	-	0
Port VLAN Membership	Forbidden			-	-	-	-		-			-	-	-	-	-	-			-	
GVRP Settings	Excluded	1	- 63	9	0	(0)	(0)	(*	(0)	(0)	(0)	0	(0)	0	C	0	9	0	- 63	0	0
VLAN Groups	Tagged	C.	0	0	0	0	C	C	0	C	0	0	0	0	0	C	C	C.	0	C	C
VOICE VLAN	Untagged	(	•	•	(•	C	C	C	C	C	C	C	C	۲		(	•	•	(•	•	(•
Access Port Multicast TV VLAP Customer Port Multicast TV VLAP	Multicast TV VLAN	C	C	C	C	0	C	0	C	C	0	C	C	0	0	C	C	C	C	C	C
<ul> <li>Spanning Tree</li> </ul>	PVID	M	ম		V	Г		Г	-	Г	Г	Γ		V	M	M	1	1	ন		
MAC Address Tables								2													
Multicast	Apply	ancel	P	ort VLAI	N Memi	pership	Table	J													

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**).

Cetting Started								
Status and Statistics	Por	t VLAN	Membe	rship				
Administration	F-F	orbidden me	mber	T - Tagged member	U - Untagged m	ember	I - Internally used VLAN	P - PVID
<ul> <li>Port Management</li> </ul>								
<ul> <li>Smadport</li> </ul>	Po	rt VLAN Mer	nbership	Table				
VLAN Management	Filt	er: Interfa	ce Type e	equals to Port 👻 Go	•			
Default VLAN Settings		Interface	Mode	Administrative VLANs	Operational VLANs	LAG		
Create VLAN	0	GE1	Access	1UP, 2F, 3F, 4F	1UP			
Interface Settings	C	GE2	Access	1UP, 2F, 3F, 4F	1UP			
Port to VLAN	C	GE3	Access	1UP. 2F. 3F. 4F	1UP			
Port VLAN Membership	C	GE4	Access	1UP 2F 3F 4F	1UP			
VI AN Groups	C	GE5	Access	1E 2UP 3E 4E	2UP			
<ul> <li>Voice VLAN</li> </ul>	C	GE6	Access	1E 2UP 3E 4E	211P			
► Access Port Multicast TV VLAN	0	GE7	Access	1E 2UP 3E 4E	201			
<ul> <li>Customer Port Multicast TV VL</li> </ul>	6	CER	Accord	15 2017 35,45	201			
<ul> <li>Spanning Tree</li> </ul>		050	Access	45.05.000.45	201			
MAC Address Tables		GE9	Access	1F, 2F, 3UP, 4F	30P			
Multicast		GE10	Access	1F, 2F, 3UP, 4F	30P			
<ul> <li>IP Configuration</li> </ul>	0	GE11	Access	1F, 2F, 3UP, 4F	3UP			
<ul> <li>Security</li> </ul>	0	GE12	Access	1F, 2F, 3UP, 4F	3UP			
Access Control	0	GE13	Access	1F, 2F, 3F, 4UP	4UP			
<ul> <li>Quality of Service</li> </ul>	0	GE14	Access	1F, 2F, 3F, 4UP	4UP			
▶ SNMP	0	GE15	Access	1F, 2F, 3F, 4UP	4UP			
	C	GE16	Access	1F, 2F, 3F, 4UP	4UP			
	0	GE17	Access	1UP, 2F, 3F, 4F	1UP			
	C	GE18	Access	1UP, 2F, 3F, 4F	1UP			
	C	GE19	Trunk	1UP, 2T, 3T, 4T	1UP, 2T, 3T, 4T			
	C	GE20	Trunk	1UP, 2T, 3T, 4T	1UP, 2T, 3T, 4T			
	Jo	in VLAN	Detail	s				
	F-F	orbidden me	mber	T - Tagged member	U - Untagged m	ember	I - Internally used VLAN	P - PVID

# 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].

Getting Started	LAC Management													
<ul> <li>Status and Statistics</li> </ul>	LAC	a wan	ageme	m										
<ul> <li>Administration</li> </ul>	1.02	d Balan	e Algoriti	nm: 🔎	MAC Address									
<ul> <li>Port Management</li> </ul>		u Duluin	gona	0	IP/MAC Address									
Port Settings <ul> <li>Link Aggregation</li> <li>LAG Management</li> </ul>		<b>\pply</b>	Can	icel										
LAG Settings	LAC	LAG Management Table												
LACP ▶ Green Ethernet		LAG	Name	LACP	Link State	Active Member	Standby Member							
Smartport	۰	LAG 1		(	Link Not Present									
VLAN Management	0	LAG 2			Link Not Present									
Spanning Tree	C	LAG 3			Link Not Present									
MAC Address Tables	С	LAG 4			Link Not Present									
Multicast	C	LAG 5			Link Not Present									
IP Configuration	C	LAG 6			Link Not Present									
<ul> <li>Security</li> </ul>	С	LAG 7			Link Not Present									
<ul> <li>Access Control</li> </ul>	С	LAG 8			Link Not Present									
Quality of Service     SNMP		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].

🔮 Edit LAG Me	embership - 168.0.21/cse	Windows Inte 7bdeb6e/Brid	emet Explorer	×
LAG: LAG Name: LACP:	1 ▼ Fibre Trun	k	(11/64 Characters Used)	
Port List GE11 GE12 GE13 GE14 GE15 GE16 GE17 GE18	* > E <	GE19 GE20	IS:	
Apply	Close		€,100%	•

### 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.

Getting Started	Dort to MI AN	_		-					
<ul> <li>Status and Statistics</li> </ul>	POIL O VLAN								
<ul> <li>Administration</li> </ul>							1		
Port Management	Filter: VLAN ID	equals	s to 1	▼ A	ND Inte	erface 1	Type	equals to	LAG - Go
Smartport	Interface	1	2	3	4	5	6	7	8
<ul> <li>VLAN Management</li> </ul>	Access	Ċ	C.	C	C	C	C	C	C
Default VLAN Settings	Trunk	0	0	()	G	0	0	(	6
Create VLAN Interface Settings	General	C	C	C	С	C	C	C	C
Port to VLAN	Customer	C	C	C	C	0	C	C	C
Port VLAN Membership	Forbidden	C	C	C	C	С	C	С	C
GVRP Settings	Excluded	C	C	C	C	C	C	C	C
<ul> <li>VLAN Groups</li> </ul>	Tagged	С	С	C	С	C	C	C	С
Voice VLAN	Untagged	(•	(•	(•	æ	•	æ	•	(•
Access Port Multicast TV VLAP Customer Port Multicast TV VL	Multicast TV VLAN	C	C	C	C	0	C	C	C
<ul> <li>Spanning Tree</li> </ul>	PVID			V			V	V	
MAC Address Tables								_	
Multicast	Apply	Cancel		ort VLA	N Mem	bership	o Tabl	е	

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].

Getting Started	Por		Memb	ershin		
<ul> <li>Status and Statistics</li> </ul>			vienio	cromp		
Administration	F-Fo	orbidden me	ember	T - Ta	gged member	U - Untagged member
Port Management	Por	t VLAN Mer	nbership	Table		
<ul> <li>Smartport</li> </ul>						
<ul> <li>VLAN Management</li> </ul>	Filte	er: Interfa	ce Type	equals to		0
Default VLAN Settings		Interface	Mode	Administ	trative VLANs	Operational VLANs
Create VLAN	۲					
Interface Settings	C	LAG2	Trunk	1UP		1UP
Port to VLAN	0	LAG3	Trunk	1UP		1UP
OVER Settings	C	LAG4	Trunk	1UP		1UP
<ul> <li>VLAN Groups</li> </ul>	C	LAG5	Trunk	1UP		1UP
Voice VLAN	C	LAG6	Trunk	1UP		1UP
Access Port Multicast TV VLAN	C	LAG7	Trunk	1UP		1UP
<ul> <li>Customer Port Multicast TV VL</li> </ul>	C	LAG8	Trunk	1UP		1UP
<ul> <li>Spanning Tree</li> </ul>			(			
MAC Address Tables	Jo	IN VLAN	Deta	IIS		
Multicast	E.E	vrhidden me	mbor	Т. Та	aged member	LL-Lintanged member
<ul> <li>ID Configuration</li> </ul>	1 - 1 4	n biologien me	mber	1-14	ggeumennber	0 - Onlagged member

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].

Getting Started	Unregistered Multicast
<ul> <li>Status and Statistics</li> </ul>	
<ul> <li>Administration</li> </ul>	
<ul> <li>Port Management</li> </ul>	Filter: Interface Type equals to Port - Go
<ul> <li>Smartport</li> </ul>	Port GE1 GE2 GE3 GE4 GE5 GE6 GE1 GE8 DE9 GE10 GE11 GE12 GE13 GE14 GE14 GE16 GE17 GE18 GE10 GE20
VLAN Management	
Spanning Tree	
MAC Address Tables	
🝷 Multicast	Anniv
Properties	
MAC Group Address	
IP Multicast Group Address	
IGMP Snooping	
MLD Snooping	
IGMP/MLD IP Multicast Group	
Multicast Router Port	
Forward All	
Unregistered Multicast	
IP Configuration	

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].

Getting Started	0.00	Dronartia	-		
<ul> <li>Status and Statistics</li> </ul>	Qos	Propenie	S		
<ul> <li>Administration</li> </ul>	0.081	Mode: 🔿 Dis	sahla	1	
Port Management	0001	(0008. O Dia Ba	sic		
<ul> <li>Smartport</li> </ul>		🔘 Ad	vanced		
VLAN Management				-	
<ul> <li>Spanning Tree</li> </ul>	Ар	ply C	ancel		
MAC Address Tables	Interf				
Multicast	intern	ace cos com	iguration rap		
<ul> <li>IP Configuration</li> </ul>	Filter:	Interface Typ	be equals to	Port 💌 Go	
▶ Security		Entry No.	Interface	Default CoS	
<ul> <li>Access Control</li> </ul>		1	GE1	0	
<ul> <li>Quality of Service</li> </ul>		2	GE2	0	
		3	GE3	0	
QoS Properties		4	GE4	0	
Queue CoS(802 1n to Queue		5	GE5	0	
DSCP to Queue		6	GE6	0	
Bandwidth		7	GE7	0	
Egress Shaping Per Queue		8	GE8	0	
VLAN Ingress Rate Limit		9	GE9	0	
<ul> <li>Congestion Avoidance</li> <li>Cons Basic Mode</li> </ul>		10	GE10	0	
QoS Advanced Mode		11	GE11	0	
<ul> <li>QoS Statistics</li> </ul>		12	GE12	0	
▶ SNMP		13	GE13	0	

Now select the <b>DSCP</b>
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.

Getting Started	DECD to O							
<ul> <li>Status and Statistics</li> </ul>	DSCP 10 QL	ieue						
<ul> <li>Administration</li> </ul>	DSCP to Queue	Table						
Port Management	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue
<ul> <li>Smartport</li> </ul>	0 (BE)	1 +	16 (CS2)	1 +	32 (CS4)	1 -	48 (CS6)	1 -
<ul> <li>VLAN Management</li> </ul>	1	1 -	17	1 -	33	1 -	49	1 -
<ul> <li>Spanning Tree</li> </ul>	2	1 -	18 (AF21)	1 -	34 (AF41)	1 -	50	1 -
MAC Address Tables	3	1 -	19	1 -	35	1 -	51	1 -
Multicast	4	1 -	20 (AF22)	1 •	36 (AF42)	1 -	52	1 -
<ul> <li>IP Configuration</li> </ul>	5	1 -	21	1 -	37	1 -	53	1 -
<ul> <li>Security</li> </ul>	6	4 -	20 (4500)	1 -	20 (4542)	4 -	55	4 -
<ul> <li>Access Control</li> </ul>	0	1.	22 (AF23)	1	30 (AF43)	1 1	54	
<ul> <li>Quality of Service</li> </ul>			23	1 •	39	1 •		
<ul> <li>General</li> </ul>	8 (CS1)	2 -	24 (CS3)	1 -	40 (CS5)	1 -	56 (CS7)	4 -
QoS Properties	9		25	1 -	41	1 -	57	
Queue	10 (AF11)	1 🔻	26 (AF31)	1 -	42	1 -	58	1 -
CoS/802.1p to Queue	11	1 🔻	27	1 🔻	43	1 🛨	59	1 🔻
DSIGE to Olleve Rondwidth	12 (AF12)	1 👻	28 (AF32)	1 🔻	44	1 👻	60	1 🕶
Egress Shaping Per Queue	13	1 -	29	1 -	45	1 -	61	1 -
VLAN Ingress Rate Limit	14 (AF13)	1 🔻	30 (AF33)	1 -	46 (EF)	3 🔻	62	1 🔻
TCP Congestion Avoidance	15	1 -	31	1 -	4/	1.	63	1 -
<ul> <li>QoS Basic Mode</li> <li>QoS Advanced Mode</li> </ul>	Apply	Cancel	Restore De	faults				
<ul> <li>QoS Statistics</li> </ul>	Queue 1 has the	lowest priority, a	unue d has the him	best priority				
▶ SNMP	aucus i lida life	iowest phone, qu	reac + nas ure my	preor priority.				

Now to enable the DSCP scheme, openGetting Startedthe QoS Basic Mode sub-menu, and> Status and Statusselect the Global Settings page.> Port ManagemeSet "DSCP" as the Trust Mode.> VLAN ManagemeThen click [Apply].> MAC Address TOnce again, remember to save the<br/>configuration (see page 20).> Security



#### 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.

Getting Started	Download/Backup Configuration/Log
Status and Statistics	Download/Dackup Configuration/Log
Administration	Transfer Method: C via TETP
System Settings	via HTTP/HTTPS
Console Settings	C via SCP (Over SSH)
Management Interface	
User Accounts	
Idle Session Timeout	Save Action: C Download
▶ Time Settings	Backup
System Log	Source File Type: <ul> <li>Running configuration</li> </ul>
<ul> <li>File Management</li> </ul>	<ul> <li>Startup configuration</li> </ul>
Upgrade/Backup Firmwa	<ul> <li>Backup configuration</li> </ul>
Active Image	<ul> <li>Mirror configuration</li> </ul>
Download/Backup Config	C Flash Log
Configuration Files Prop	Papalitius Data: C. Evolutio
Copy/Save Configuration	G Encounted
DHCP Auto Configuration	C Blaintant
Reboot =	Available sensitive data options are determined by the current user's SSD rules
<ul> <li>Diagnostics</li> </ul>	
Discovery - Bonjour	
Discovery - LLDP	Apply Cancel

### 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.

Getting Started	Download/Bookup	Configuration/Log
<ul> <li>Status and Statistics</li> </ul>	Бомпоац/Баскир	Configuration/Log
<ul> <li>Administration</li> </ul>	Transfer Method:	C via TETP
System Settings Console Settings Management Interface	Hansiel metrice.	<ul> <li>via HTTP/HTTPS</li> <li>via SCP (Over SSH)</li> </ul>
User Accounts Idle Session Timeout Time Settings	Save Action:	<ul> <li>Download</li> <li>Backup</li> </ul>
► System Log	Source File Name:	Browse
File Management     Upgrade/Backup Firmwa     Active Image     Download/Backup Config     Configuration Files Press	Destination File Type:	<ul> <li>Running configuration</li> <li>Startup configuration</li> <li>Backup configuration</li> </ul>
Conjugation Files Prop Copy/Save Configuration DHCP Auto Configuration Reboot	Apply Cancel	

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].

Getting Started	Dreparties			
Status and Statistics	Properties			
Administration	LLDP Properties			
System Settings Console Settings Management Interface User Accounts	LLDP Status: LLDP Frames Handling:	L .	Enable Filtering	
Idle Session Timeout  Time Settings  System Log	C TLV Advertise Interval:	00	Use Default User Defined 30	
<ul> <li>File Management Reboot</li> <li>Diagnostics</li> </ul>	C Topology Change SNMP Notification Interval:	00	Use Default User Defined	
Discovery - Bonjour Discovery - LLDP	🌣 Hold Multiplier.	00	Use Default User Defined	
Port Settings	🌣 Reinitializing Delay:	Ce	Use Default User Defined	
LLDP MED Port Settings LLDP Port Status LLDP Local Information	Ø Transmit Delay:	Ce	Use Default User Defined	
LLDP Neighbor Informati LLDP Statistics LLDP Overloading	LLDP-MED Properties	_		_
<ul> <li>Discovery - CDP Ping Traceroute</li> </ul>	Apply Cancel	3		Times (Range, 1

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

Getting Started	Proportion	
Status and Statistics	Fiopenties	
<ul> <li>Administration</li> </ul>	CDP Status:	Enable
System Settings Console Settings Management Interface User Accounts Idle Session Timeout	CDP Frames Handling:	Bridging     Filtering     Flooding
<ul> <li>Time Settings</li> </ul>	CDP Voice VLAN Advertisement	Enable
<ul> <li>System Log</li> <li>File Management</li> </ul>	CDP Mandatory TLVs Validation:	Enable
Reboot > Diagnostics	CDP Version:	C Version 1 C Version 2
Discovery - Bonjour  Discovery - LLDP  Discovery - CDP	CDP Hold Time:	<ul> <li>Use Default</li> <li>User Defined</li> </ul>
Properties Interface Settings	CDP Transmission Rate:	Use Default     User Defined
CDP Local Information CDP Neighbor Information CDP Statistics Ping	Device ID Format:	MAC Address     Serial Number
Traceroute Port Management	Source Interface:	Use Default
Smartport		C User Defined
VLAN Management	Interface:	Port GET -
Spanning Tree		
MAC Address Tables		
Multicast	Syslog Voice VLAN Mismatch:	Enable
IP Configuration	Syslog Native VLAN Mismatch:	Enable
Security	Syslog Duplex Mismatch:	Enable
Access Control		

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".

Getting Started	CTI			Hingo					
<ul> <li>Status and Statistics</li> </ul>	511	miena	e Se	ungs					
<ul> <li>Administration</li> </ul>	STR	Interface S	etting T	able					
Port Management	Filte	r Interface	Type e	quals to	Port	- Go			
<ul> <li>Smartport</li> </ul>		E-t- No	interfe	qualete		Educ Ded	Destaura	DDDU O	0001111-0
<ul> <li>VLAN Management</li> </ul>	-	Entry No.	іптепа	ce S	P	Edge Port	Root Guard	BPDU Guard	BPDU Handlin
<ul> <li>Spanning Tree</li> </ul>	0	1	GE1	Ena	bled	Enabled	Disabled	Enabled	Guarding
STP Status & Global Settings	C	2	GE2	Ena	bled	Enabled	Disabled	Enabled	Guarding
STP Interface Settings	0	3	GE3	Ena	bled	Enabled	Disabled	Enabled	Guarding
RSTP Interface Settings	C	4	GE4	Ena	bled	Enabled	Disabled	Enabled	Guarding
MSTP Properties	0	5	GE5	Ena	bled	Enabled	Disabled	Enabled	Guarding
VLAN to MSTP Instance	C	6	GE6	Ena	bled	Enabled	Disabled	Enabled	Guarding
MSTP Interface Settings	C	7	GE7	Ena	bled	Enabled	Disabled	Enabled	Guarding
MAC Address Tables	С	8	GE8	Ena	bled	Disabled	Disabled	Enabled	Guarding
▶ Multicast	۲	9	GE9	Disa	bled	Disabled	Disabled	Enabled	Guarding
IP Configuration	С	10	GE10	Disa	bled	Disabled	Disabled	Enabled	Guarding
▹ Security	0	11	GE11	Disa	bled	Disabled	Disabled	Enabled	Guarding
<ul> <li>Access Control</li> </ul>	C	12	GE12	Disa	bled	Disabled	Disabled	Enabled	Guarding
Quality of Service	0	13	GE13	Ena	bled	Enabled	Disabled	Enabled	Guarding
▶ SNMP	C	14	GE14	Ena	bled	Enabled	Disabled	Enabled	Guarding
	C	15	GE15	Ena	bled	Enabled	Disabled	Enabled	Guarding
	С	16	GE16	Ena	bled	Enabled	Disabled	Enabled	Guarding
	C	17	GE17	Ena	bled	Disabled	Disabled	Disabled	STP
	C	18	GE18	Ena	bled	Disabled	Disabled	Disabled	STP
	C	19	GE19	Ena	bled	Disabled	Disabled	Disabled	STP
	C	20	GE20	Ena	bled	Disabled	Disabled	Disabled	STP
		Copy Set	ings		Edit.				

# 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.

Interface:	● Port GE1 ▼ C LAG
STP:	🔽 Enable
Edge Port:	Enable
	C Auto C Disable
Root Guard:	Enable
BPDU Guard:	Enable
BPDU Handling:	Use Global Settings
	C Filtering
Path Cost	<ul> <li>Lee Default</li> </ul>
T dill 003L	C User Defined 20000 (Range: 1 - 20000000)
Priority:	128 -
Port State:	Forwarding
Designated Bridge ID:	32768-a0:cf:5b:e5:47:60
Designated Port ID:	128-49
Designated Cost:	0
Forward Transitions:	1
Speed:	1000M
LAG:	N/A

Getting Started	OT		an Cottin										
<ul> <li>Status and Statistics</li> </ul>	511	miena	ce Settin	igs									
<ul> <li>Administration</li> </ul>	STP	Interface S	Setting Tabl	e									
<ul> <li>Port Management</li> </ul>	Filte	r Intorface		ale to Port	<b>*</b> [00]								
<ul> <li>Smartport</li> </ul>	Fille	a. mienace	rype equa										
<ul> <li>VLAN Management</li> </ul>		Entry No.	Interface	STP	Edge Port	Root Guard	BPDU Guard	BPDU Handling	Port Role	Path Cost	Priority	Port State	Designated Bri
<ul> <li>Spanning Tree</li> </ul>	0	1	GE1	Enabled	Enabled	Disabled	Enabled	Guarding	Designated	20000	128	Forwarding	32768-a0:cf:5b
STP Status & Global Settings	0	2	GE2	Enabled	Enabled	Disabled	Enabled	Guarding	Designated	200000	128	Forwarding	32768-a0:cf:5b
STP Interface Settings	C	3	GE3	Enabled	Enabled	Disabled	Enabled	Guarding	Disabled	2000000	128	Disabled	N/A
RSTP Interface Settings	С	4	GE4	Enabled	Enabled	Disabled	Enabled	Guarding	Disabled	2000000	128	Disabled	N/A
MSTP Properties	0	5	GE5	Enabled	Enabled	Disabled	Enabled	Guarding	Designated	20000	128	Forwarding	32768-a0:cf:5b
MSTP Instance Settings	C	6	GE6	Enabled	Enabled	Disabled	Enabled	Guarding	Designated	20000	128	Forwarding	32768-a0:cf:5b
MSTP Interface Settings	0	7	GE7	Enabled	Enabled	Disabled	Enabled	Guarding	Disabled	2000000	128	Disabled	N/A
MAC Address Tables	C	8	GE8	Enabled	Enabled	Disabled	Enabled	Guarding	Designated	20000	128	Forwarding	32768-a0:cf:5b
Multicast	C	9	GE9	Enabled	Enabled	Disabled	Enabled	Guarding	Disabled	2000000	128	Disabled	N/A
<ul> <li>IP Configuration</li> </ul>	C	10	GE10	Enabled	Enabled	Disabled	Enabled	Guarding	Disabled	2000000	128	Disabled	N/A
<ul> <li>Security</li> </ul>	0	11	GE11	Enabled	Enabled	Disabled	Enabled	Guarding	Disabled	2000000	128	Disabled	N/A
<ul> <li>Access Control</li> </ul>	C	12	GE12	Enabled	Enabled	Disabled	Enabled	Guarding	Disabled	2000000	128	Disabled	N/A
Quality of Service	0	13	GE13	Enabled	Enabled	Disabled	Enabled	Guarding	Disabled	2000000	128	Disabled	N/A
▶ SNMP	0	14	GE14	Enabled	Enabled	Disabled	Enabled	Guarding	Disabled	2000000	128	Disabled	N/A
	C	15	GE15	Enabled	Enabled	Disabled	Enabled	Guarding	Disabled	2000000	128	Disabled	N/A
	С	16	GE16	Enabled	Enabled	Disabled	Enabled	Guarding	Disabled	2000000	128	Disabled	N/A
	0	17	GE17	Enabled	Disabled	Disabled	Disabled	STP	Disabled	2000000	128	Disabled	N/A
	C	18	GE18	Enabled	Disabled	Disabled	Disabled	STP	Disabled	2000000	128	Disabled	N/A
	C	19	GE19	Enabled	Disabled	Disabled	Disabled	STP	Disabled	2000000	128	N/A	N/A
	C	20	GE20	Enabled	Disabled	Disabled	Disabled	STP	Disabled	2000000	128	N/A	N/A
		Copy Set	tings	Edi									

# 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.

Getting Started	Dreportion	
<ul> <li>Status and Statistics</li> </ul>	Properties	
<ul> <li>Administration</li> </ul>	Bridge Multicast Filtering Status:	
Port Management	bridge manoaber mening claub.	i cindolo
<ul> <li>Smartport</li> </ul>	- Alexandra	
<ul> <li>VLAN Management</li> </ul>	VLAN ID:	1 -
Spanning Tree	Forwarding Method for IPv6:	MAC Group Address
MAC Address Tables		IP Group Address
<ul> <li>Multicast</li> </ul>		C Source Specific IP Group Address
Properties	Forwarding Method for IPv4:	MAC Group Address
MAC Group Address		IP Group Address
IP Multicast Group Address		C Source Specific IP Group Address
IGMP Snooping		
MLD Snooping	Apply Cancel	
IGMP/MLD IP Multicast Group		
Multicast Router Port		
Forward All		
Unregistered Multicast		
IP Configuration		

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

Getting Started			nina								
<ul> <li>Status and Statistics</li> </ul>	IGI	/iF 31100	ping								
<ul> <li>Administration</li> </ul>	IG	IP Snooping	status: 🔽	Enable							
Port Management		in oneoping	y otatao. ji	Lindolo							
<ul> <li>Smartport</li> </ul>		Apply	Cancel								
VLAN Management	_										
Spanning Tree	IGN	IP Snooping	Table								
MAC Address Tables		Entry No.	VLAN ID	IGMP Snooping	Router	MRouter Ports	Query	Query	Query Max Response	Last Member	Last Memb
<ul> <li>Multicast</li> </ul>	-			Operational Status	IGMP Version	Auto Learn	Robustness	Interval (sec.)	Interval (sec.)	Query Counter	Interval
Properties	0	1	1	Enabled	v3	Enabled	2	30	10	2	
MAC Group Address	C	2	2	Enabled	v3	Enabled	2	30	10	2	
IP Multicast Group Address	0	3	3	Enabled	v3	Enabled	2	30	10	2	
MLD Snooping	C	4	4	Enabled	v3	Enabled	2	30	10	2	
IGMP/MLD IP Multicast Group		Copy Set	tings	Edit							
Multicast Router Port Forward All											
Unregistered Multicast											

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.

VLAN ID:	1	*			
IGMP Snooping Status:	~	Enable			
MRouter Ports Auto Learn:	<b>V</b>	Enable			
Query Robustness:	2		(Ra	nge: 1 - 7, De	efault: 2)
🗱 Query Interval:	30		sec	(Range: 30	- 18000, Default 125)
© Query Max Response Interval:	10		sec	(Range: 5 -	20, Default: 10)
Last Member Query Counter:	(•	Use Default			
	С	User Defined			(Range: 1 - 7, Default: 2 (Query Robustness
🖇 Last Member Query Interval:	10	00	mS	(Range: 100	- 25500, Default: 1000)
Immediate leave:		Enable			
IGMP Querier Status:	~	Enable			
Administrative Querier Source IP Address:	(	Auto			
	С	User Defined	192.168.0	.21 🔻	
IGMP Querier Version:	C	IGMPV2			



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].

Getting Started	Eo	nuare												
<ul> <li>Status and Statistics</li> </ul>	10	ware												
<ul> <li>Administration</li> </ul>						_							_	
Port Management	Fi	ter: l	'LAN ID	equals	to 1	- AN	ID Inter	face T	ype eq	uals to	Port	- 0	90	
<ul> <li>Smartport</li> </ul>	- Pr		GE1	GE2	GE2	GEA	GE6	GER	GE7	GE0	0E0	GE10	GE11	GE12
<ul> <li>VLAN Management</li> </ul>		otic	OLI	012	OL3	024	OE3	OLU	OE7	OLU O	OL5	OEIO	OLIT	OE12
<ul> <li>Spanning Tree</li> </ul>		auc			0	0			0	0			0	
MAC Address Tables		noluuei		0					0	0	0	0		0
✓ Multicast		Jue	•	•	•	•	0	•	•	•	•	•	•	•
Properties		0 mmhu		Concol										
MAC Group Address		whhile		Cancer										
IP Multicast Group Addre	ess													
IGMP Snooping														
MLD Snooping														
IGMP/MLD IP Multicast C	Group													
Multicast Router Port														
Forward All														
Unregistered Multicast														
<ul> <li>ID Configuration</li> </ul>														

#### 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].

192.168.0.220/csc6b64841/mul	ticast/IPMulticastGroup_	add.htm		
e VLAN ID:	2	(Range: 1 - 4094)		
ta IP Version:	Version 6 @ Vers	alon 4		
IP Multicast Group Address:	224.0.0.251		ulticast Filtering must b	e enabled.
Source Specific:	Include			
Source IP Address:			(Range: 1 - 4094)	
P P				Go Clear Filter
GVRP Settings	VLAN ID	IP Multicast Group Addr	ess	Source IP Address
Voice VLAN	1	239.255.255.250		•
Access Port Multicast TV VLAP 📃	1	ff02::1:ff63:2a90		•
Customer Port Multicast TV VL	Add Delete	Details		
panning Tree				
AC ADDress Tables				
Prenetice				
MAC Group Address				
IP Multicast Group Address				
IGMP Snooping				
MLD Snooping				

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.

Getting Started		Hisast Crown Address		
<ul> <li>Status and Statistics</li> </ul>	IF IVIU	licasi Group Address		
Administration	The Brid	ge Multicast Filtering is currently enabled.		
Port Management	For IP M	ulticast Configuration to be effective, the Bridge Mul	icast Filtering must be enabled.	
Smartport	IP Mult	icast Group Address Table		
<ul> <li>VLAN Management</li> </ul>	Filter:			
Default VLAN Settings Create VLAN		IP Version equals to Version 4		
Port to VLAN Port VLAN Membership		IP Multicast Group Address equals to     Source IP Address equals to	Go Clear Filter	
GVRP Settings		VLAN ID IP Multicast Group Address	Source I	P Address
<ul> <li>VLAN Groups</li> <li>Voice VLAN</li> </ul>		1 239.255.255.250	•	
► Access Port Multicast TV VLAN		1 ff02::1:ff63:2a90		
► Customer Port Multicast TV VL	7	2 224.0.0.251		
<ul> <li>Spanning Tree</li> </ul>	Ad	d Delete Details		
MAC Address Tables				
+ Multicast			-	
Properties				
MAC Group Address				
IGMP Spooning				
MI D Snooping				

VLAN IU:				2																
P Version:				Ve	rsion	4														
P Multicas	t Gro	up Ad	dress	s: 22	4.0.0.:	251														
Source IP /	Addre			*																
		_			-		_													
Filter: <i>Inte</i>	rface	Туре	equa	als to	Por	t 💌	Go													
Filter: <i>Inte</i> nterface	rface GE1	Type GE2	equa	als to GE4	Port GE5	t 💌 GE6	Go GE7	GE8	GE9	GE10	GE11	GE12	GE13	GE14	GE15	GE16	GE17	GE18	GE19	9 GE20
Filter: <i>Inte</i> Interface Static	rface GE1	Type GE2	equa GE3	als to GE4	Port GE5	t 💌 GE6	Go GE7 ම	GE8	GE9	GE10	GE11 ()	GE12 ()	GE13	GE14	GE15	GE16	GE17	GE18	GE19	9 GE20 ©
Filter: <i>Inte</i> Interface Static Dynamic	rface GE1 ©	GE2	GE3	GE4	Port GE5 O	GE6	Gc GE7 O	GE8 O	GE9 O	GE10	GE11 ()	GE12	GE13	GE14	GE15	GE16	GE17	GE18	GE19	9 GE20
Filter: <i>Inte</i> Interface Static Dynamic Forbidden	rface GE1 O	GE2	GE3	als to GE4 O O	Port GE5 O	GE6	GE7 ©	GE8 O	GE9	GE10	GE11 () () () () ()	GE12	GE13	GE14 GE14	GE15	GE16	GE17 © ©	GE18	GE19 © ©	) GE20 () () () () () () () () () ()

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.

Getting Started	Statistics					
<ul> <li>Status and Statistics</li> </ul>	Statistics					
System Summary Interface	Interface:	● Port GE6 ▼ C LAG 🚺 マ				
Etherlike	Refresh Rate:	No Refresh				
GVRP		C 15 sec.				
802.1x EAP		O 30 sec.				
TCAM Utilization		C 60 sec.				
* RMON						
Statistics History	Bytes Received:	2163518168				
Events	Drop Events:	0				
Alarms View Log	Packets Received:	130633523				
RAM Memory	Broadcast Packets Received:	1816				
Flash Memory	Multicast Packets Received	80563322				
Administration	ODO 8 Alian Emany					
<ul> <li>Port Management</li> </ul>	CRC & Aligh Errors.	0				
Port Settings	Undersize Packets:	0				
Link Aggregation	Oversize Packets:	0				
Green Ethernet	Fragments:	0				
<ul> <li>Smartport</li> </ul>	labhars:	0				
<ul> <li>VLAN Management</li> </ul>	Sabbers.					
Spanning Tree	Collisions:	0				
MAC Address Tables	Frames of 64 Bytes:	28435				
Multicast	Frames of 65 to 127 Bytes:	94526				
IP Configuration	Frames of 128 to 255 Bytes:	9854754				
<ul> <li>Security</li> </ul>	Frames of 256 to 511 Bytes:	120655282				
<ul> <li>Access Control</li> </ul>	Frames of 512 to 1022 Bites:	205				
Quality of Service	Frames of 512 to 1023 Bytes:	390				
SNMP	Frames Greater than 1024 Bytes:	: 139				
	Clear Interface Counters Cle	ar All Interfaces Counters				

#### 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.

Getting Started	RAM Mem			
<ul> <li>Status and Statistics</li> </ul>	TO UN MEMO			
System Summary	Alert Icon Blinkin	ng: Enabled Disable	Alert Icon Blinkin	g
Interface	PAM Momony			Phowing 1 50 of 04 50
CVRP	RAM Memory			Showing 1-50 of 94 - 50 - 1
802.1x EAP	Log Index	Log Time	Severity	Description
TCAM Utilization	214/483553	2012-Jul-19 20:39:20	Notice	%COPY-N-TRAP: The copy operation was completed successfully
▼ RMON	2147483554	2012-Jul-19 20:39:17	Informational	%COPY-I-FILECPY: Files Copy - source URL running-config destination URL flash://startup-config
Statistics	2147483555	2012-Jul-19 20:05:57	Warning	%COPY-W-TRAP: The copy operation has failed
History	2147483556	2012-Jul-19 20:05:50	Informational	%COPY-I-FILECPY: Files Copy - source URL HTTP://192.168.0.202/ destination URL running-config
Events	2147483557	2012-Jul-19 20:00:31	Notice	%COPY-N-TRAP: The copy operation was completed successfully
v View Log	2147483558	2012-Jul-19 20:00:18	Informational	%COPY-I-FILECPY: Files Copy - source URL running-config destination URL HTTP://192.168.0.202/
RAM Memory	2147483559	2012-Jul-19 19:48:06	Notice	%COPY-N-TRAP: The copy operation was completed successfully
Flash Memory	2147483560	2012-Jul-19 19:47:54	Informational	%COPY-I-FILECPY: Files Copy - source URL running-config destination URL HTTP://192.168.0.202/
<ul> <li>Administration</li> </ul>	2147483561	2012-Jul-19 19:39:35	Notice	%COPY-N-TRAP: The copy operation was completed successfully
<ul> <li>Port Management</li> </ul>	2147483562	2012-Jul-19 19:39:33	Informational	%COPY-I-FILECPY: Files Copy - source URL running-config destination URL flash://startup-config
Port Settings	2147483563	2012-Jul-19 19:25:16	Warning	%STP-W-PORTSTATUS: gi8: STP status Forwarding
<ul> <li>Link Aggregation</li> </ul>	2147483564	2012-Jul-19 19:25:13	Warning	%STP-W-PORTSTATUS: gi5: STP status Forwarding
Green Ethernet	2147483565	2012-Jul-19 19:25:11	Informational	%LINK-I-Up: gi8
Sinalipoli	2147483566	2012-Jul-19 19:25:10	Warning	%STP-W-PORTSTATUS: gi6: STP status Forwarding
Spapping Trap	2147483567	2012-Jul-19 19:25:09	Informational	%LINK-I-Up; gi5
MAC Address Tables	2147483568	2012-Jul-19 19:25:09	Warning	%LINK-W-Down: gi17
<ul> <li>Multicact</li> </ul>	2147483569	2012-Jul-19 19:25:06	Warning	%LINK-W-Down: gi3, aggregated (1)
> IP Configuration	2147483570	2012-Jul-19 19:25:06	Informational	%LINK-I-Up: Vlan 2
<ul> <li>Security</li> </ul>	2147483571	2012-Jul-19 19:25:06	Informational	%LINK-I-Up: gi6
Access Control	2147483572	2012-Jul-19 19:25:03	Warning	%LINK-W-Down; gi4
Quality of Service	2147483573	2012-Jul-19 19:20:45	Warning	%STP-W-PORTSTATUS: gi2: STP status Forwarding
SNMP	2147483574	2012- Jul-19 19:20:40	Informational	%LINK-LUn: ni2
	2147483575	2012-Jul-19 19:20:25	Warning	%STP-W-PORTSTATUS; gi3: STP status Forwarding, aggregated (1)

#### **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.