

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.

eneral		
	automatically if your network sup eed to ask your network administr	
Obtain an IP address autom	atically	
() Use the following IP address	8	
IP address:	192 . 168 . 1 . 100	
Subnet mask:	255 . 255 . 255 . 0	
Default gateway:		
Obtain DNS server address a	automatically	
Use the following DNS serve	10000000000000000000000000000000000000	
Preferred DNS server:		
Alternate DNS server:		
Validate settings upon exit	Advanc	

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 👻 Logou	it About Help
CISCO SG 300-20	20-Port Gigabit Managed Switch		
	Lo r ort organit managoa o mitan		
Getting Started	Getting Started		
 Status and Statistics 	Getting Started		
 Administration 			
 Port Management 	This page provides easy steps to configure your device		
▶ Smartport			
▶ VLAN Management	Nitial Setup	Cuick Access	
 Spanning Tree 	Change Device IP Address	Change Device Password	
MAC Address Tables	Create VLAN	Upgrade Device Software	
▶ Multicast	Configure Port Settings	Backup Device Configuration	
 IP Configuration 	Conligure Port Settings		
▶ Security		Create MAC-Based ACL	
 Access Control 	Device Status	Create IP-Based ACL	
 Quality of Service 	System Summary	Configure QoS	
► SNMP	Port Statistics	Configure Port Mirroring	
	RMON Statistics		
	View Log		
	Other resources: Support Forums		
	ourer resources, outport porditis		
	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.

Getting Started Status and Statistics	System Summary				
System Summary	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):	22347bc1ad4f7f75526896a565dc71
802.1x EAP	System Location:	Stage-Primary	Edit	Firmware Version (Non-active):	1.2.7.76
TCAM Utilization RMON	System Contact:	Andy	Edit	Firmware MD5 Checksum (Non-active):	01e9f0b789ff44bf7e8956fbdb339f2c
View Log	Host Name:	switch632a90	Edit	Boot Version:	1.1.0.6
Administration	System Object ID:	1.3.6.1.4.1.9.6.1.83.20.1		Boot MD5 Checksum:	8c6b1f42c0754ab9c70324a815a45fl
Port Management	System Uptime:	0 day(s), 0 hr(s), 12 min(s) and 5	i8 sec(s)	Locale:	en-US
Smartport	Current Time:	15:07:59;2013-May-02		Language Version:	1.3.0.62
VLAN Management Spanning Tree	Base MAC Address:	15:07:59;2013-May-02 64:d8:14:63:2a:90		Language Version. Language MD5 Checksum:	N/A
MAC Address Tables	Jumbo Frames:	Disabled			
Multicast					

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

			ssingResourceException	n [] MissingResourceException
cisco				Q
Download S	oftware) Download Cart	(0 items) + Feedback Help
Downloads Home > Pro	ducts > Switches > LAN Switches - Small Business > Cisco Small Business	300 Series Managed Swit	ches >	
Cisco SG300-20 20-Port	Gigabit Managed Switch > Switch Firmware-1.3.0.62			
Cisco SG300-20.2	0-Port Gigabit Managed Switch			
	of or organic managed owner			
Search		Release	Notes and Open So	ource Documentation
Expand All Collapse /		Release Release Date	Notes and Open So Size	purce Documentation 🛛 🗮 🐣
	All			Download
Expand All Collapse J • Latest Releases 1.3.0.62 1.1.2.0 • All Releases + 1.1	File Information Sx300 Firmware Version 1.3.0.62	Release Date	Size	
Expand All Collapse / • Latest Releases 133.062 1.1.2.0 • All Releases	File Information Studie File Information Studie File Version 1.3.0.62 Studie File Version 1.3.0.62 Studie File Version 1.3.0.62	Release Date 21-MAY-2013	Size 6.58 MB	Download
Expand All Collapse J • Latest Releases 1.3.0.62 1.1.2.0 • All Releases + 1.1	Viii File Information ▲ Sx200 Firmware Version 1.3.0.62 Sx200 Firmware Version 1.3.0.62 Sx200 Grown (Grownary) Language File Version 1.3.0.62 Sx200 Grown (Grownary) Language File Version 1.3.0.62 Sx200 Grown (Grownary) Language File Version 1.3.0.62 Sx200 Grown (Grownary) Language File Version 1.3.0.62	Release Date 21-MAY-2013 21-MAY-2013	Size 6.58 MB 0.76 MB	Download
Expand All Collapse J • Latest Releases 1.3.0.62 1.1.2.0 • All Releases + 1.1	VI File Information . Sx200 Firmware Version 1.3.0.62 Sx300 Gramma (Grammay) Language File Version 1.3.0.62 Sx200 Quarter (Grammay) Language File Version 1.3.0.62 Sx200 Quarter (Grammay) Language File Version 1.3.0.62 Sx200 Quarter (Grammay) Language File Version 1.3.0.62 Sx200 Quarter (Gramma) Language File Version 1.3.0.62 Sx200 Quarter (Gramma) Language File Version 1.3.0.62 Sx200 File Version 1.3.0.62	Release Date 21-MAY-2013 21-MAY-2013 21-MAY-2013	Size 6.58 MB 0.76 MB 0.73 MB	Download Download Download

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	20-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: # Upgrade Backup File Type: # Firmware Image	
 File Management Upgrade Backup Filmware Active Image Download/Backup Configur. 	Boot Code C Language 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 Status and Statistics	IPv4 Interface		
 Administration System Settings 	Management VLAN:	1 -	
 Management Interface IPv4 Interface 	IP Address Type:	C Dynamic Static	
IPv6 Global Configuration IPv6 Interface	💐 IP Address:	192.168.0.21	
IPv6 Addresses IPv6 Default Router List IPv6 Tunnel IPv6 Neighbors	Mask:	Network Mask 255.255.255.0 Prefix Length (Ran	ige: 8 - 30)
IPv6 Routes User Accounts Idle Session Timeout	Administrative Default Gateway:	 User Defined None 	
Time Settings System Log File Management	Operational Default Gateway: Renew IP Address Now:	🗖 Enable	
Reboot > Diagnostics	Auto Configuration via DHCP:	Enabled	
Discovery - Bonjour Discovery - LLDP	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".

Getting Started					
Status and Statistics	System Summary				
System Summary	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
TCAM Utilization RMON	System Contact	Andy	Edit	Firmware MD5 Checksum (Non-active):	01e9f0b789ff44bf7e8956fbdb339f2c
View Log	Host Name:	switch632a90	Edit	Boot Version:	1.1.0.6
Administration	System Object ID:	1.3.6.1.4.1.9.6.1.83.20.1		Boot MD5 Checksum:	8c6b1f42c0754ab9c70324a815a45f08
System Settings Console Settings	System Uptime:	0 day(s), 1 hr(s), 31 min(s) and 32 se	ec(s)	Locale:	en-US
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 Time Settings	Jumbo Frames:	Disabled			

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	Properties	
 Status and Statistics 		
 Administration 	For the functions and/or parameters configured on this page	to become effective
✓ Port Management	you may have to configure the corresponding port based par	
Port Settings	Energy Detect Mode:	Enable
 Link Aggregation 	Short Reach:	Enable
 Green Ethernet 		
Properties	Port LEDs:	Enable
Port Settings	Power Savings:	77 %
 Smartport 	Cumulative Energy Saved:	0 Watt Hour
 VLAN Management 	Complainte Energy Durea.	e waarioar
 Spanning Tree 		
 MAC Address Tables 	802.3 Energy Efficient Ethernet (EEE):	📃 Enable
Multicast		
IP Configuration	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.



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	Inte	rfaaa Ca	ttinge				
 Status and Statistics 	inte	rface Se	attings				
 Administration 	2	Sussee	Topormo	nonthe cave	the configuration		
 Port Management 		Success.	ro perme	incluy save	une configuratio	Jii, yo to ti	ne copysavi
 Smartport 	Inde		Table				
✓ VLAN Management	Inte	rface Settir	ig lable				
Default VLAN Settings	Filte	er: Interface	Type equa	als to Port -	Go		
Create VLAN		Entry No.	Interface	Interface	Administrative	Frame	Ingress
Interface Settings Port to VLAN				VLAN Mode	PVID	Туре	Filtering
Port VLAN Membership	C	1	GE1	Access	1	Admit All	Enabled
GVRP Settings	C	2	GE2	Access	1	Admit All	Enabled
VLAN Groups	0	3	GE3	Access	1	Admit All	Enabled
▶ Voice VLAN	С	4	GE4	Access	1	Admit All	Enabled
 Access Port Multicast TV VLAN Customer Port Multicast TV VL 	0	5	GE5	Access	1	Admit All	Enabled
 Spanning Tree 	C	6	GE6	Access	1	Admit All	Enabled
 MAC Address Tables 	0	7	GE7	Access	1	Admit All	Enabled
 Multicast 	С	8	GE8	Access	1	Admit All	Enabled
 IP Configuration 	0	9	GE9	Access	1	Admit All	Enabled
► Security	C	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
	C	18	GE18	Access	1	Admit All	Enabled
	C	19	GE19	Trunk	1	Admit All	Enabled
	C	20	GE20	Trunk	1	Admit All	Enabled
	-	Copy Set	tinge	Edit			
< >		Coby Set	ungs	Edit			



Copy configuration f	rom entry 1 (GE1)
to: 2-18	(Example: 1,3,5-10 or: GE1,GE3-GE5)
Apply C	lose

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 VLAN																				
Status and Statistics	IU VLAN																				
Administration	Success. To	norm	anoni	the cove	tho c	opfiqu	ration	ao to	the Cr	nul Cou	o Confi	ourotio		or clic	k tho	Savo i	con				
 Port Management 	Success. To	penn	anen	uy save	ane c	onngu	auon	yo to	uie ou	pyroav	e com	gurado	page	UI CII	A UIC	Saver	COII.				
Smartport			_																		
VLAN Management Filter	r: VLAN ID	equals	to 2	2 - AN	ID Inte	rface T	vpe e	quals to	Port	•	Go										
Default VLAN Settings								-													
Create VLAN Inter	face	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10	GE11	GE12	GE13	GE14	GE15	GE16	GE17	GE18	GE19	GE20
Interface Settings Acce	ISS	6	0	6	6	6	0	6	6	6	0	6	C	6	6	C	6	6	(C	C
Port to VLAN Trun	ĸ	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	6	6
Port VLAN Membership Gen		C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C
GVRP Settings		C	6	0	C	C	0	C	0	~	0	C	C	C	0	C	0	0	~	0	C
VLAN Groups	idden					~	~	~	~						6					~	-
P VOICE VEAN				-		-	1			<u> </u>				-							2
Access Port Multicast TV VLAN Exclusion		0	0	0	0	0	0	-	C	10	0	0	C	0	0		6	0	0	6	C.
 Customer Port Multicast TV VL Tagg 	ged	0	0	0	C	0	0	C	C	0	0	0	0	0	0	C	C	0	0	e	•
Spanning Tree Unta	igged	C	C	С	C	•	(e	(•	C	C	C	C	0	C	C	C	C	C	C	C
MAC Address Tables Multi	cast TV VLAN	C	C	C	C	C	C	C	С	С	C	С	С	C	C	С	C	C	С	C	C
Multicast PVID)	Г	Г	Г	Г		V	V		Г	Г	Г	Г	Г	Г	F	Г	Г	Г	Г	Г
IP Configuration				A Sector		in sector to							(and a designed to						a benefit	a fan f	
Security	oply C	ancel	F	ort VLAN	Memt	pership	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	ort to VLAN																				
Status and Statistics	OIT TO VEAN																				
Administration	Success. To	norm	anont	h cour	tho c	onfiqu	ration	an to	the Ce	nul Cou	o Confi	ourotio		or clic	k tho	Savo i	con				
Port Management	Juccess. To	penn	anenu	y save	uie c	unigu	ration,	yo to		pyloav	e conii	guranoi	paye	UI CIIC	K UIC	Savei	con.				
Smartport																					
VLAN Management	Filter: VLAN ID	equals	to 3	▼ AI	ND Inte	erface T	vpe e	quals to	Port	•	Go										
Default VLAN Settings																					
Create VLAN	nterface	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	6	6	6	6	6	6	6	6	6	6	C	0
Port to VLAN	Frunk	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		C	C	C	C	C	C	C	C	C	C	0	C	C	C	C	C	C	C	C	C
VLAN Groups	Forbidden									-	~	2	~	•					•	~	C
VOICE VLAIN	Excluded	~	~	~	~	~	~	-	~	~	~	~	~	~	~	-	0	~	2	~	
		-			-		0		-	-						0	-				
	Fagged	10	0	9	0	6	0	9	10	1	0	9	6	C	9	0	10	6	0		•
8	Jntagged	0	0	C	0	C	C	0	C	•	•	۲	•	C	0	0	C	0	0	C	C
MAC Address Tables	Multicast TV VLAN	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	С	C	C	C	C
Multicast	PVID			Г	Γ	Г	Г		Г	$\overline{\mathbf{v}}$	$\overline{\mathbf{M}}$	$\overline{\mathbf{N}}$	2	Г	Γ		Г	Γ		Г	
IP Configuration		(Tarre																0.010			110
Security	Apply	ancel	P	ort VLAI	V Mem	bership	Table]													
Access Control								,													

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

Getting Started	Port to VLAN																				
 Status and Statistics 	-OIL IO VLAN																				
Administration										— c											
Port Management	Filter: VLAN ID	equals	s to 1	• Al	VD Inte	rface T	ype e	quals to	Port	•	Go										
Smartport	Interface	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10	GE11	GE12	GE13	GE14	GE15	GE16	GE17	GE18	GE19	GE20
VLAN Management	Access	G	6	6	G	6	C	6	6	GEO	G	6	G	G	6	G	G	6	6	C	C
Default VLAN Settings	Trunk	0	0	C	0	0	0	0	C	0	0	0	0	C	0	C	0	0	0	6	6
Create VLAN		0	0	0	C	0	0	0	~	0	0	0	C	0	~	0	0	0	0	0	C
Interface Settings	Customer	~	~	~	~	~	~	~	~	~	2	2	~	~	~	~	-	~	~	~	-
Port to VLAN		-	0	-	-	-	0	0	-	0			-	-	0	0	-	-	2	-	-
Port VLAN Membership	Forbidden	-	1	t.	6		C	C	9	10		19	6	C	C	-	0			t.	C
GVRP Settings	Excluded	0	9	0	0	6	6	6	0	6	6	0	6	0	0	0	0	0	0	0	0
 VLAN Groups 	Tagged	C	C.	C	0	0	C	C	C	C	C	0	C	C	0	C	C	C	0	C	C
Voice VLAN	Untagged	•			(•	C	C	C	C	С	C	C	С	((•
Access Port Multicast TV VLAN	Multicast TV VLAN	C	C	C	C	0	C	C	C	C	C	C	C	0	C	C	C	C	C	C	C
Customer Port Multicast TV VL Spanning Tree	PVID	M	ম	2	V		Г	Г	Г	Г	Г	Г	Г	V	V	M	N	N	2		V
MAC Address Tables								2													
Multicast	Apply C	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**).

Getting Started Status and Statistics	Port	VLAN I	Membe	rship				
 Administration 	F-Fo	rbidden me	mber	T - Tagged member	U - Untagged mer	mber	I - Internally used VLAN	P - PVID
 Port Management 	Por	VLAN Men	nbership	Fable				
Smartport			77	quals to Port 👻 Go	7			
▼ VLAN Management	Filte			-	2			
Default VLAN Settings		Interface	Mode	Administrative VLANs		LAG		
Create VLAN	0	GE1	Access	1UP, 2F, 3F, 4F	1UP			
Interface Settings Port to VLAN	C	GE2	Access	1UP, 2F, 3F, 4F	1UP			
Port VLAN Membership	C	GE3	Access	1UP, 2F, 3F, 4F	1UP			
GVRP Settings	C	GE4	Access	1UP, 2F, 3F, 4F	1UP			
VLAN Groups	0	GE5	Access	1F, 2UP, 3F, 4F	2UP			
Voice VLAN	C	GE6	Access	1F, 2UP, 3F, 4F	2UP			
Access Port Multicast TV VLAN	C	GE7	Access	1F, 2UP, 3F, 4F	2UP			
 Customer Port Multicast TV VL 	C	GE8	Access	1F, 2UP, 3F, 4F	2UP			
 Spanning Tree 	0	GE9	Access	1F, 2F, 3UP, 4F	3UP			
MAC Address Tables	C	GE10	Access	1F, 2F, 3UP, 4F	3UP			
 Multicast 	C	GE11	Access	1F. 2F. 3UP. 4F	3UP			
 IP Configuration 	C	GE12	Access	1F, 2F, 3UP, 4F	3UP			
Security Access Control	C	GE13	Access	1F, 2F, 3F, 4UP	4UP			
Quality of Service	C	GE14	Access	1F. 2F. 3F. 4UP	4UP			
SNMP	C	GE15	Access	1F, 2F, 3F, 4UP	4UP			
▶ SIMMP	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	GE10 GE19	Trunk	10P, 2F, 3F, 4P	1UP, 2T, 3T, 4T			
	0	GE19 GE20						
			Trunk	1UP, 2T, 3T, 4T	1UP, 2T, 3T, 4T			
	Joi	n VLAN	Detail	S				
	F-Fo	rbidden me	mber	T - Tagged member	U - Untagged mer	mber	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	1.00	Man		mt			
Status and Statistics	LAC	5 Man	ageme	int			
 Administration 	1.02	ad Balan	ce Algoriti	ım: 🔎	MAC Address		
 Port Management 		ad Dalam			P/MAC Address		
Port Settings Link Aggregation LAG Management 		Apply	Can	cel			
LAG Settings LACP	LAG	GManage	ement Ta	ble			
 Green Ethernet 		LAG	Name	LACP	Link State	Active Member	Standby Member
Smartport	•	LAG 1	er u	×	Link Not Present		
VLAN Management	0	LAG 2			Link Not Present		
Spanning Tree	0	LAG 3			Link Not Present		
MAC Address Tables	0	LAG 4			Link Not Present		
▶ Multicast	0	LAG 5			Link Not Present		
 IP Configuration 	0	LAG 6			Link Not Present		
Security	0	LAG 7			Link Not Present		
Access Control	C	LAG 8			Link Not Present		
Quality of Service		Edit.	1				
▶ SNMP							

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			terret Explorer dgelf/bridg_interface_lagMembership_e.htm?[lag_Data_Tbl]Query:ifIndex=1000/	
LAG: LAG Name: LACP:	1 ▼ Fibre Trun □ Enable		(11/64 Characters Used)	
Port List GE11 GE12 GE13 GE14 GE15 GE16 GE17 GE18	* > E <	GE19 GE20	275	
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	Port to VLAN								
 Status and Statistics 	OIL TO VEAN								
 Administration 				_			٦		
Port Management	Filter: VLAN ID	equals	to 1	▼ A	ND Inte	erface 1	ype	equals to	LAG - Go
 Smartport 	Interface	1	2	3	4	5	6	7	8
 VLAN Management 	Access	C	C	C	C	C	C	C	c
Default VLAN Settings	Trunk	6	0	6	6	0	6	C	0
Create VLAN Interface Settings	General	C	C	C	C	C	0	C	C
	Customer	C	C	C	C	0	C	C	C
	Forbidden	C	C	C	C	С	C	С	C
GVRP Settings	Excluded	C	C	C	C	C	C	C	C
 VLAN Groups 	Tagged	С	С	C	С	C	C	C	С
Voice VLAN	Untagged		œ	•	(e	(•	•	•
Access Port Multicast TV VLAN Customer Port Multicast TV VL	Multicast TV VLAN	C	C	C	C	0	C	C	C
	PVID	V	V		M		V	2	V
MAC Address Tables							_		
▶ Multicast	Apply	ancel		ort VLA	N Mem	bership	Table	•	

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	t VLAN I	Momb	orchin		
 Status and Statistics 	FUI		Memb	ersnip		
Administration	F-Fo	orbidden me	ember	T - Ta	gged member	U - Untagged membe
Port Management	Pol	rt VLAN Mer	nbershir	Table		
 Smartport 				101-101-101-101-101-101-101-101-101-101		
 VLAN Management 	Filt	er: Interfa	ce Type	equals to	LAG 🗕 🖸	io
Default VLAN Settings		Interface	Mode	Administ	rative VLANs	Operational VLANs
Create VLAN	۲					
Interface Settings	C	LAG2	Trunk	1UP		1UP
Port to VLAN Port VLAN Membership	0	LAG3	Trunk	1UP		1UP
GVRP Settings	C	LAG4	Trunk	1UP		1UP
▹ VLAN Groups	0	LAG5	Trunk	1UP		1UP
▹ Voice VLAN	C	LAG6	Trunk	1UP		1UP
 Access Port Multicast TV VLAN 		LAG7	Trunk	1UP		1UP
 Customer Port Multicast TV VL 	C	LAG8	Trunk	1UP		1UP
Spanning Tree	C .		(
MAC Address Tables	Jo	in VLAN	Deta	uls		
Multicast	E.E	orbidden me	mher	T - Ta	gged member	U - Untagged membe
IP Configuration	1-11	and den me	most	1-14	ggou member	o ontagged membe

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	
 Status and Statistics 	Unregistered Multicast
Administration Port Management Smartport VLAN Management Spanning Tree	Filter: Interface Type equals to Port Go Port GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8 3E9 GE10 GE11 GE12 GE13 GE14 GE12 Forwarding G G G G Forwarding G G G G G G Filtering G G G G G G G G
Multicast Properties MAC Group Address IP Multicast Group Address IP Multicast Group Address IGMP Snooping MLD Snooping IGMP/MLD IP Multicast Group Multicast Router Port Forward All Unregistered Multicast) IP Configuration	Apply Cancel

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	QoS Properties
 Status and Statistics 	
 Administration 	QoS Mode: 💿 Disable
Port Management	Basic
 Smartport 	Advanced
 VLAN Management 	
 Spanning Tree 	Apply Cancel
MAC Address Tables	Interface CoS Configuration Table
 Multicast 	
IP Configuration	Filter: Interface Type equals to Port 💽 Go
 Security 	Entry No. Interface Default CoS
 Access Control 	1 GE1 0
 Quality of Service 	2 GE2 0
▼ General	🖻 3 GE3 0
QoS Properties Queue	🖻 4 GE4 0
CoS/802.1p to Queue	5 GE5 0
DSCP to Queue	🖻 6 GE6 0
Bandwidth	T GE7 0
Egress Shaping Per Queue	🖻 8 GE8 0
VLAN Ingress Rate Limit TCP Congestion Avoidance	9 GE9 0
 QoS Basic Mode 	10 GE10 0
 QoS Advanced Mode 	11 GE11 0
QoS Statistics	12 GE12 0
SNMP	13 GE13 0
	13 0213

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.

Getting Started	DSCP to Qu							
 Status and Statistics 	DOOP to Qu	leue						
 Administration 	DSCP to Queue	Table						
Port Management	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue
Smartport	0 (BE)	1 -	16 (CS2)	1 -	32 (CS4)	1 👻	48 (CS6)	1 -
VLAN Management	1	1 -	17	1 -	33	1 -	49	1 -
Spanning Tree	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 -
IP Configuration	5	1 -	21	1 -	37	1 -	53	1 -
Security	6	1 -	22 (AF23)	1 -	38 (AF43)	1 -	54	1 -
Access Control	-	1 -	22 (AF23) 23			1 -	55	1 *
Quality of Service		-		1 -	39	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		
 General 	8 (CS1)	2 🕶	24 (CS3)	1 -	40 (CS5)	1 -	56 (CS7)	4 🕶
QoS Properties	3	<u> </u>	25	1 -	41	1 -	57	1.1
Queue	10 (AF11)	1 -	26 (AF31)	1 🛨	42	1 -	58	1 🔻
CoS/802.1p to Queue	11	1 -	27	1 🔻	43	1 🔻	59	1 🔻
DSCP to Queue Bandwidth	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 -
QoS Basic Mode QoS Advanced Mode	Apply	Cancel	Restore De	faults				
QoS Statistics SNMP	Queue 1 has the	lowest priority, qu	ueue 4 has the hig	ghest 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> IP Configurationconfiguration (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.

Status and Statistics		up 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:	Download
Time Settings		Backup
System Log	Source File Type:	Running configuration
File Management		C Startup configuration
Upgrade/Backup Firmwa		C Backup configuration
Active Image		C Mirror configuration
Download/Backup Config		C Flash Log
Configuration Files Prop	Sensitive Data:	C Exclude
Copy/Save Configuration	Censilive Data.	Encrypted
DHCP Auto Configuration		C Plaintext
Reboot E		Available sensitive data options are determined by the current user's SSD rules
Diagnostics		

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/Reakup	Configuration/Log
 Status and Statistics 	Download/Backup	Configuration/Log
 Administration 	Transfer Method:	C via TFTP
System Settings Console Settings Management Interface	nanoici metrica.	 via HTTP/HTTPS via SCP (Over SSH)
User Accounts Idle Session Timeout Time Settings	Save Action:	 Download Backup
▶ System Log	Source File Name:	Browse
File Management Upgrade/Backup Firmwa Active Image Download/Backup Confic Configuration Files Prop	Destination File Type:	 Running configuration Startup configuration Backup configuration
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].

Status and Statustics Administration System Settings Console Settings Management Interface User Accounts Time Settings System Log File Management Reboot Diagnostics Discovery - Bonjour Obscovery - Status LDDP Ford Settings LDDP Ford Settings LDDP Pord Settings LDDP Pord Settings LDDP Pord Settings LDDP Pord Settings LDDP Verifoading © Transmit Delay: © User Defined © Transmit Delay: © User Defined © User Defined © Transmit Delay: © User Defined © User Defined © Transmit Delay: © User Defined © Statistics LLDP Wethour Anding © Fast Statist Repeat Count:	Getting Started	Properties			
System Settings LLDP Properties Use Accounts LLDP Status: Imagement Interface Visit Management Rebot Consoler Consoler > Diagnostics Consoler Consoler Diagnostics Consoler Consoler Diagnostics Consoler Consoler Discovery - Bonjour Consoler Cose Default Port Settings Cose Default Cose Default LLDP MED Network Point Cose Default Cose Default Port Settings Cose Default Cose Default LLDP MED Network Point Cose Default Cose Default Cosevery - LIDP Cose Default Cose Default Cosevery - Core Default Cose Default Cose Default LIDP Verof Settings Cose Default Cose Default LLDP Net Defort Settings Cose Default Cose Default LLDP Net Dork Settings Cose Default Cose Default LLDP Verof Status Cose Default Cose Default LLDP Verof Status Cose Default Cose Default LLDP Verof Status Cose Default Cose Default LLDP Verof St	Status and Statistics	Flopenies			
Console Settings LLDP Status: Enable Management Interface User Accounts Idle Session Timeout Idle Session Timeout Reboot LLDP Frames Handling: FileInting 9 Time Settings ILLP Advertise Interval: Ouser Defined Dio 9 Time Settings Idle Session Timeout Ouser Defined Dio 9 Time Settings Idle Hold Multiplier: Ouser Defined Dio 9 Topology Change SNMP Notification Interval: User Defined Dio 9 Topology Change SNMP Notification Interval: Ouser Defined Dio 9 Topology Change SNMP Notification Interval: Ouser Defined Dio 9 Topology Change SNMP Notification Interval: Ouser Defined Dio 9 Topology Change SNMP Notification Interval: Ouser Defined Dio 9 Topology Change SNMP Notification Interval: Ouser Defined Dio 9 Topology Change SNMP Notification Interval: Ouser Defined Dio 9 Topology Change SNMP Notification Interval: Ouser Defined Dio 9 Topology Change Status Ouser Defined Dio Dio 1LDP MeD Notynchronation Cuser Defined Dio Dio 1LDP Nelphober Information User Defi	Administration	LLDP Properties			
Idle Session Timeout Idle Session Timeout Time Settings Topology Change SNMP Notification Interval: Use Default Use Default Topology Change SNMP Notification Interval: Use Default Topology Change SNMP Notification Interval: Use Default Use Default Topology Change SNMP Notification Interval: Use Default Use Default Discovery-EuDP Use Default Costinitiant Port Settings Reinitializing Defay: User Default User Default User Default Transmit Defay: User Default User Default User Default User Default User Default Transmit Defay: User Default User Default	Console Settings Management Interface			Filtering	
Rebot C 10pting) Change Great Production Interior. C Use Default > Discovery - Bonjour C Hold Multiplier: C Use Default > Discovery - LDP C Hold Multiplier: C Use Default Prostings C Reinitializing Defay: C Use Default LDP MeD Port Settings C Reinitializing Defay: C Use Default ULDP MED Port Settings C Transmit Defay: C Use Default ULDP Neighbor Informatin LLDP Neighbor Informatin LLDP MED Properties LLDP Vertoading Prast Start Repeat Count: Times (Range:	► Time Settings	4 TLV Advertise Interval:		Use Default	
 Discovery - LLDP Port Settings LLDP MED Prof Settings C Reinitializing Delay: C User Defined C Transmit Delay: C User Defined C Transmit Delay: C User Defined C User Defined C User Defined C Transmit Delay: C Transmit Delay: C User Defined C Transmit Delay: C Transmit Delay: C User Defined <	Reboot	Change SNMP Notification Interval			
Port Settings P Reinitializing Delay: C Use Default LLDP MED Port Settings C User Defined P LLDP Neiphoor Information C User Defined P Ping P Fast Start Repeat Count. P Times (Range:	 Discovery - LLDP 	C Hold Multiplier.			
LLDP Port Status LLDP Local Information LLDP Statistics LLDP Verbrading > Discovery- CDP Pring Ping	Port Settings	Reinitializing Delay.			
LLDP Statistics LLDP Overloading ▷ Discovery - CDP Pring US Statistics Start Repeat Count. 3 Times (Range: Pring)	LLDP Port Status LLDP Local Information	Ø Transmit Delay.			
Discovery- CDP Ø Fast Start Repeat Count: J Times (Range: Ping	LLDP Statistics	LLDP-MED Properties			
Port Management Cancel	 Discovery - CDP Ping Traceroute 		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	Properties	
 Status and Statistics 	Flopenies	
 Administration 	CDP Status:	Enable
System Settings Console Settings Management Interface User Accounts Idle Session Timeout	CDP Frames Handling:	Bridging Filtering Filtering Flooding
Time Settings	CDP Voice VLAN Advertisement.	Enable
System Log File Management	CDP Mandatory TLVs Validation:	Enable
Reboot > Diagnostics	CDP Version:	C Version 1 Version 2
Discovery - Bonjour	CDP Hold Time:	Use Default User Defined
	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 Organization 	Source Interface:	 Use Default User Defined
Smartport VLAN Management	Interface	Port GE1
 Spanning Tree 	internation.	
MAC Address Tables		
Multicast	Syslog Voice VLAN Mismatch:	Enable
IP Configuration	Syslog Native VLAN Mismatch:	Enable
Security	Syslog Duplex Mismatch:	Enable
 Access Control 	oyardy pupies midiliater.	1 LINUN
Quality of Service	Apply Cancel	

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	e T	nterfa		100				
Status and Statistics	511	miena	e Settii	igs				
Administration	STP	Interface S	etting Tabl	e				
Port Management	Filto	r Interface		als to Port	- Go			
 Smartport 	Tinte						D	F
 VLAN Management 	-	Entry No.	Interface	STP	Edge Port	Root Guard	BPDU Guard	BPDU Handlin
 Spanning Tree 	0	1	GE1	Enabled	Enabled	Disabled	Enabled	Guarding
STP Status & Global Settings	C	2	GE2	Enabled	Enabled	Disabled	Enabled	Guarding
STP Interface Settings	0	3	GE3	Enabled	Enabled	Disabled	Enabled	Guarding
RSTP Interface Settings	C	4	GE4	Enabled	Enabled	Disabled	Enabled	Guarding
MSTP Properties VLAN to MSTP Instance	0	5	GE5	Enabled	Enabled	Disabled	Enabled	Guarding
MSTP Instance Settings	C	6	GE6	Enabled	Enabled	Disabled	Enabled	Guarding
MSTP Interface Settings	C	7	GE7	Enabled	Enabled	Disabled	Enabled	Guarding
MAC Address Tables	С	8	GE8	Enabled	Disabled	Disabled	Enabled	Guarding
▶ Multicast	۲	9	GE9	Disabled	Disabled	Disabled	Enabled	Guarding
 IP Configuration 	C	10	GE10	Disabled	Disabled	Disabled	Enabled	Guarding
▶ Security	C	11	GE11	Disabled	Disabled	Disabled	Enabled	Guarding
Access Control	C	12	GE12	Disabled	Disabled	Disabled	Enabled	Guarding
Quality of Service	0	13	GE13	Enabled	Enabled	Disabled	Enabled	Guarding
▶ SNMP	C	14	GE14	Enabled	Enabled	Disabled	Enabled	Guarding
	C	15	GE15	Enabled	Enabled	Disabled	Enabled	Guarding
	С	16	GE16	Enabled	Enabled	Disabled	Enabled	Guarding
	C	17	GE17	Enabled	Disabled	Disabled	Disabled	STP
	C	18	GE18	Enabled	Disabled	Disabled	Disabled	STP
	C	19	GE19	Enabled	Disabled	Disabled	Disabled	STP
	C	20	GE20	Enabled	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 1 ▼
STP:	🔽 Enable
Edge Port:	Enable
	C Auto C Disable
Root Guard:	Enable
BPDU Guard:	Enable
BPDU Handling:	Use Global Settings
	C Filtering C Flooding
Path Cost	Use Default
Tall Cost.	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:	T
Speed:	1000M
LAG:	N/A

Getting Started	STF	Interfa	ce Settir	nas									
Status and Statistics	-			<u> </u>									
Administration	STP	Interface S	Setting Tabl	е									
Port Management	Filte	r: Interface	Type equa	als to Port	- Go								
Smartport		Entry No.	Interface	STP	Edge Port	Root Guard	BPDU Guard	BPDU Handling	Port Role	Path Cost	Priority	Port State	Designated 8
VLAN Management	C	Enuy NO. 1	GE1	Enabled	Enabled	Disabled	Enabled	Guarding	Designated	20000	128	Forwarding	32768-a0:cf:
Spanning Tree								and the second	A CONTRACTOR OF STREET, STREET			Second Contractor	
STP Status & Global Settings	0	2	GE2	Enabled	Enabled	Disabled	Enabled	Guarding	Designated	200000	128	Forwarding	32768-a0:cf:
STP Interface Settings	C	3	GE3	Enabled	Enabled	Disabled	Enabled	Guarding	Disabled	2000000	128	Disabled	N/A
RSTP Interface Settings MSTP Properties	C	4	GE4	Enabled	Enabled	Disabled	Enabled	Guarding	Disabled	2000000	128	Disabled	N/A
VI AN to MSTP Instance	0	5	GE5	Enabled	Enabled	Disabled	Enabled	Guarding	Designated	20000	128	Forwarding	32768-a0:cf:
MSTP Instance Settings	C	6	GE6	Enabled	Enabled	Disabled	Enabled	Guarding	Designated	20000	128	Forwarding	32768-a0:cf:
MSTP Interface Settings	C	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:
Multicast	C	9	GE9	Enabled	Enabled	Disabled	Enabled	Guarding	Disabled	2000000	128	Disabled	N/A
IP Configuration	C	10	GE10	Enabled	Enabled	Disabled	Enabled	Guarding	Disabled	2000000	128	Disabled	N/A
Security	C	11	GE11	Enabled	Enabled	Disabled	Enabled	Guarding	Disabled	2000000	128	Disabled	N/A
Access Control	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	C	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
	C	16	GE16	Enabled	Enabled	Disabled	Enabled	Guarding	Disabled	2000000	128	Disabled	N/A
	C	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	120	N/A	N/A
	-	Copy Set	100000000	Enabled		Disabled	Disabled	oir	Disabled	2000000	120	11/7	1WA

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					
 Status and Statistics 	Properties					
 Administration 	Bridge Multicast Filtering Status:	Enable				
Port Management	bridge multicastri itering status.	, iv Lindois				
Smartport	and the second sec					
VLAN Management	VLAN ID:	1 -				
 Spanning Tree 	Forwarding Method for IPv6:	MAC Group Address				
MAC Address Tables		 IP Group Address 				
 Multicast 		C Source Specific IP Group Address				
Properties MAC Group Address	Forwarding Method for IPv4:	MAC Group Address IP Group Address Source Specific IP Group Address				
IP Multicast Group Address IGMP Snooping MLD Snooping IGMP/MLD IP Multicast Group Multicast Router Port	Apply Cancel					
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		/IP Snoo	ning								
 Status and Statistics 	IGIN	//F 31100	ping								
 Administration 	IG	MP Snooping	Status: 🔽	Enable							
Port Management		in oneophig	rotatao. p	Lindolo							
 Smartport 		Apply	Cancel								
 VLAN Management 	_			_							
 Spanning Tree 	IGN	AP Snooping	Table								
 MAC Address Tables 		Entry No.	VLAN ID	IGMP Snooping	Router	MRouter Ports	Query	Query	Query Max Response	Last Member	Last Memb
✓ Multicast	-			Operational Status	IGMP Version	Auto Learn	Robustness	Interval (sec.)	Interval (sec.)	Query Counter	Interval
Properties	0	1	1	Enabled	v 3	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	v 3	Enabled	2	30	10	2	
IGMP Snooping MLD Snooping	C	4	4	Enabled	v3	Enabled	2	30	10	2	
IGMP/MLD IP Multicast Group		Copy Set	tings	Edit							
Multicast Router Port	<u></u>										
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:	1	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:	Γ	Enable			
IGMP Querier Status:	~	Enable			
Administrative Querier Source IP Address:					
	С	User Defined	192.168.0	.21 🔻	
IGMP Querier Version:		IGMPV2 IGMPV3			



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	Forwar	d All											
	 Status and Statistics 	TOTWAL												
	 Administration 					_								
	 Port Management 	Filter:	VLAN IC) equals	to 1	▼ AN	ID Inte	rface T	<i>ype</i> eq	uals to	Port	- 0) 0	
	 Smartport 	Port	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10	GE11	GE12
	 VLAN Management 	Static	000	012	023	004	0E3	020	00	020	023	0010	000	0012
	 Spanning Tree 	Forbidde	~	0	0	0	0	0	0	0	0	0	0	0
	MAC Address Tables	None	en () ()	۲	۲	•		0	0	۲	0	0	۲	۲
	✓ Multicast	None	•	•	•	•	0		•	•	•	•	•	•
1	Properties	Apply		Cance										
	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													

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].

1 192.168.0.220/csc6b64841/mul	ticast/IPMulticastGroup_	add.htm					
e VLAN ID:	2	(Range: 1 - 4094)					
IP Version:	Version 6 Version	sion 4					
dr 🗢 IP Multicast Group Address:	224.0.0.251		ulticast Filtering must be enabled.				
Source Specific:	Include						
Source IP Address:			(Range: 1 - 4094)				
C Apply Close				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							
ulticast							
Properties 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	ID MAL	Iticast Group Address		
 Status and Statistics 	IP IVIU	licasi Group Address		
 Administration 		ge Multicast Filtering is currently enabled.		
Port Management	For IP M	ulticast Configuration to be effective, the Bridge M	ulticast Filtering must be enabled.	
Smartport	IP Mult	icast Group Address Table		
 VLAN Management 	Filter:	VLAN ID equals to	(Range: 1 - 4094)	
Default VLAN Settings Create VLAN		IP Version equals to Version 4		
Interface Settings Port to VLAN Port VLAN Membership		Go Clear Filter		
GVRP Settings		VLAN ID IP Multicast Group Address	Source	IP Address
VLAN Groups Voice VLAN		1 239.255.255.250	*	
Access Port Multicast TV VLAN		1 ff02::1:ff63:2a90		
Customer Port Multicast TV VL	2	2 224.0.0.251		
 Spanning Tree MAC Address Tables 	Ad	d Delete Details	_	
 Multicast 		(Details)	_	
Properties				
MAC Group Address IP Multicast Group Address				
IGMP Snooping				
MLD Snooping				

VLAN ID:				2																
IP Version:				Ve	rsion	4														
P Multicast Group Address: 224.0.0.251																				
Source IP /	٩ddre	ess:		*																
Filter: <i>Int</i> e	rface	Туре	equa	als to	Por	t 👻	G)												
								_	GE9	GE10	GE11	GE12	GE13	GE14	GE15	GE16	GE17	GE18	GE19	GE20
nterface								_	GE9 ()	GE10	GE11	GE12	GE13	GE14	GE15 ()	GE16 ()	GE17	GE18	GE19 ම	GE20
nterface Static		GE2			GE5	GE6	GE7	GE8									GE17			
Filter: <i>Inte</i> Interface Static Dynamic Forbidden	GE1	GE2			GE5	GE6	GE7	GE8		۲	۲	۲	۲	۲	۲	۲	0	0	۲	۲

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.

	Statistics					
 Status and Statistics 						
System Summary Interface	Interface:	● Port GE6 - C LAG -				
Etherlike	Refresh Rate:	No Refresh				
GVRP		C 15 sec.				
802.1x EAP		C 30 sec.				
TCAM Utilization		C 60 sec.				
RMON Statistics						
History	Bytes Received:	2163518168				
Events	Drop Events:	0				
Alarms	Packets Received:	130633523				
 View Log RAM Memory 	Broadcast Packets Received:	1816				
Flash Memory		80563322				
 Administration 	Multicast Packets Received:					
 Port Management 	CRC & Align Errors:	0				
Port Settings	Undersize Packets:	0				
 Link Aggregation 	Oversize Packets:	0				
Green Ethernet	Fragments:	0				
 Smartport 	Jabbers:	0				
 VLAN Management 		0				
Spanning Tree	Collisions:	U				
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				
▶ Security	Frames of 256 to 511 Bytes:	120655282				
 Access Control 	Frames of 512 to 1023 Bytes:	395				
Quality of Service						
▶ SNMP	Frames Greater than 1024 Bytes	: 139				

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 Status and Statistics	RAM Memory								
System Summary	Alert Icon Blinkir	ig: Enabled Disable/	Alert Icon Blinkin	g					
Interface Etherlike	RAM Memory	Log Table		Showing 1-50 of 94 50 -					
GVRP	Log Index	-	Severity	Description					
802.1x EAP	2147483553	2012-Jul-19 20:39:20	Notice	%COPY-N-TRAP: The copy operation was completed successfully					
TCAM Utilization	2147483554	2012-Jul-19 20:39:17	Informational	%COPY-I-FILECPY: Files Copy - source URL running-config destination URL flash://startup-config					
 RMON 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					
Alarms	2147483558	2012-Jul-19 20:00:18	Informational	%COPY-I-FILECPY: Files Copy - source URL running-config destination URL HTTP://192.168.0.202/					
 View Log 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/					
Administration	2147483561	2012-Jul-19 19:39:35	Notice	%COPY-N-TRAP: The copy operation was completed successfully					
 Port Management 	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					
 Link Aggregation 	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					
 Smartport 	2147483566	2012-Jul-19 19:25:10	Warning	%STP-W-PORTSTATUS: gi6: STP status Forwarding					
 VLAN Management 	2147483567	2012-Jul-19 19:25:09	Informational	%LINK-I-Up: qi5					
Spanning Tree	2147483568	2012-Jul-19 19:25:09	Warning	%LINK-W-Down: gi17					
 MAC Address Tables Multicast 	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					
Security	2147483571	2012-Jul-19 19:25:06	Informational	%LINK-I-Up; qi6					
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-I-Up: gi2					
	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.