

MERGING TECHNOLOGIES

Cisco SG350-10 Auto-configuration - Legacy



i General Info.

This is in no case an exhaustive configuration procedure, It's a simple guide on how to configure these switches to use with Ravenna/AES67 networks.

This guide applies to both SG350-10 and SG350-10P

Before Starting

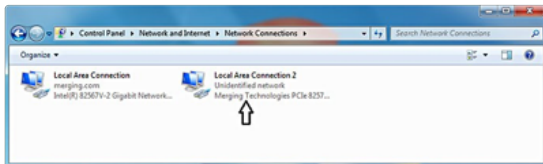
Important! If you have problems accessing the switch for configuration when connected to the Merging MassCore PCIe Ethernet card (NET-MSC-GBEX1) please connect it to the PC's on-board Ethernet port. When configuration is completed reconnect the switch to the MassCore Ethernet card.

⚠ Dante devices requires an additional configuration, not included in the configuration files.
See the [Dante devices Multicast Group configuration page](#) for details

Cisco SG350 Switch Auto-configuration Procedure

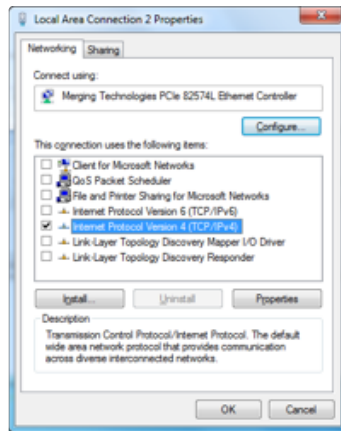
Note: For Cisco SG350 Switches other than the **SG350-10** please use the manual configuration procedure.

1. Right click on the Network icon in the Windows Taskbar.
2. Select: **Open Network and Sharing Center**
3. Click on: **Change Adapter Settings** on the left of the pane.



4. Right-click the **Merging Technologies PCIe 8257** RAVENNA Network Card and select **Properties:**
(same procedure applies with any other network adapter)

MERGING TECHNOLOGIES



5. Select **Internet Protocol Version 4 (TCP/IP)** and Click on **Properties**:



6. Click on the **Use the following IP address**: radio button and enter **192.168.1.2** (the Cisco SG350 switch has a factory default IP address of **192.168.1.254**).

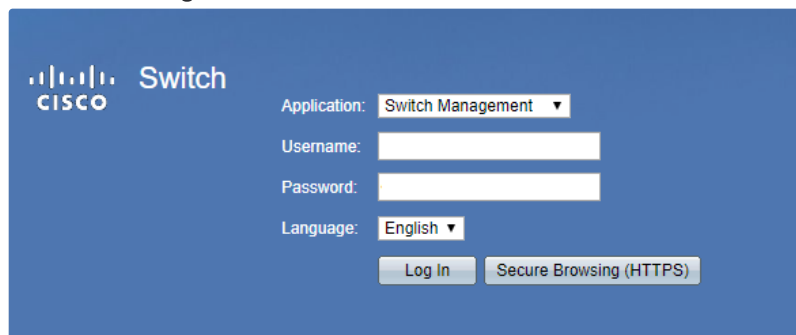
Click on the **OK** button to accept the settings and close the dialog.

- a. **Note**: if the switch cannot be accessed at the address 192.168.1.254, it could be that a DHCP is present, in which case, open MTDISCOVERY and check if the switch appears with the name "SwitchABCDEF" with the last digits being its MAC address.

7. Open a browser and type **192.168.1.254** in the address bar.

Default user name: "**cisco**" – password: "**cisco**".

Click on the **Log in** button .



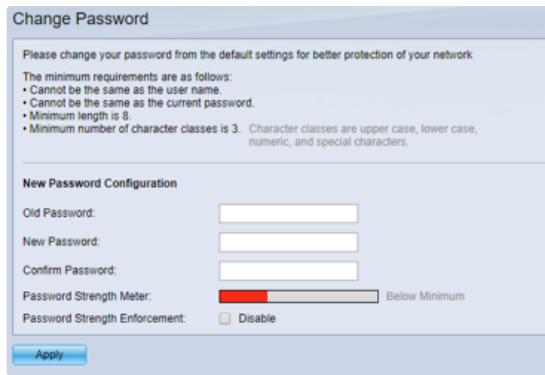
8. After the login prompt, you will be asked to change that default password to whatever you want.

It is a required step and the first one into securing you're router/switch, it is also a one time step only.

After the default is changed, if you wish to change it again you will have to do that in the Administration page.

Resetting the switch to "factory defaults" will also ask you to do this step again.

MERGING TECHNOLOGIES



Change Password

Please change your password from the default settings for better protection of your network.

The minimum requirements are as follows:

- Cannot be the same as the user name.
- Cannot be the same as the current password.
- Minimum length is 8.
- Minimum number of character classes is 3. Character classes are upper case, lower case, numeric, and special characters.

New Password Configuration

Old Password:

New Password:

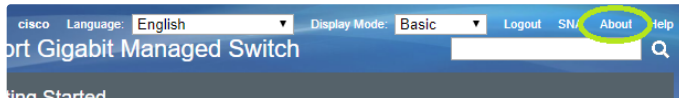
Confirm Password:

Password Strength Meter: Below Minimum

Password Strength Enforcement: ☐ Disable

9. Make sure the switch is running firmware **2.3.5.63** or above.

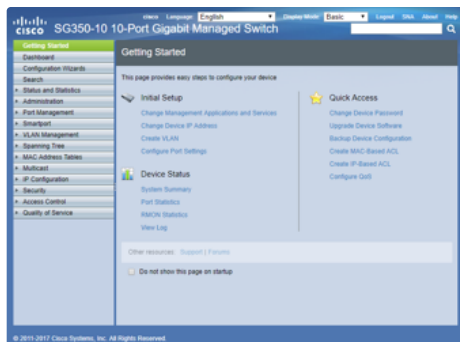
Click on the **About** button on top right of the screen.



If you have to update the firmware, refer to [*Cisco 350, 350X, and 550X Series Managed Switches Administration Guide - Firmware Operations*](#) section.

[Click here to access Cisco documentation website](#)

10. The Administration page will now load and you can start configuring your switch.



11. Download the latest configuration file for your Cisco SG350 switch model :

[Cisco SG350-10](#)

[Cisco SG350-10 - Dual VLAN](#) (Port 1 to 5 : Regular network. Port 6 to 10 : RAVENNA/AES67)

[Cisco SG350-10 - ACL Port 8](#) (Port 8 configured to filter all Multicast Streams, allowing to connect a non-RAVENNA/AES67 Network. Eg. Connect directly an AP WIFI for some remote control purpose (tablet, smartphone), connect your Internet router.)

The Merging RAVENNA configuration file will auto-configure various settings /protocols to optimize the RAVENNA / AES67 network, and also sets the definitive fixed IP address of the switch: **169.254.1.254**)

12. Go into **"Administration"** then click **"File Management"** to expand, then click **"File Operations"** to open its pane.

MERGING TECHNOLOGIES

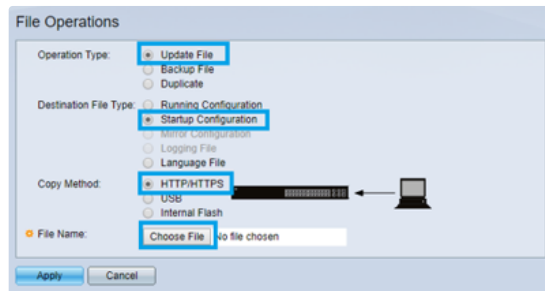


13. Now select

Operation Type : **Update File**

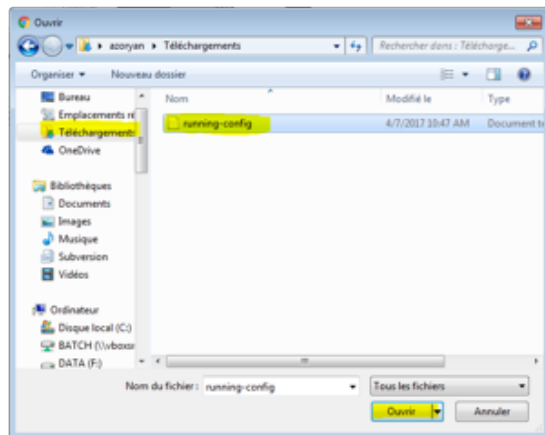
Destination File Type : **Startup Configuration**

Copy Method : **HTTP/HTTPS**

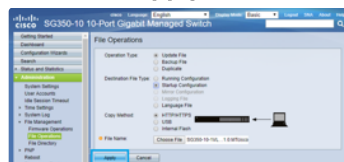


14. Then click **Choose File** and a new window will pop up.

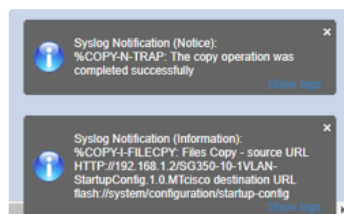
In the **Choose File** window point to the downloaded configuration file location, select it and click **Open**.



15. Then click **Apply** for it to load your configuration file into the STARTUP CONFIG.



16. The switch will send a notification that the operation has been completed.



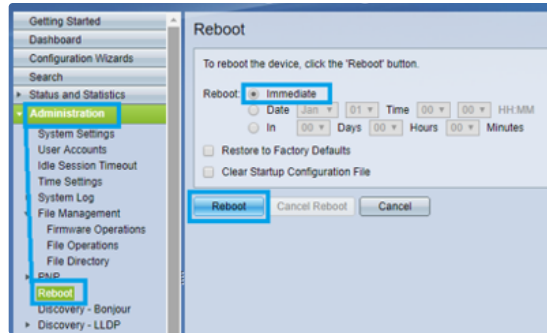
MERGING TECHNOLOGIES

17. You must now restart the switch for the changes to apply.

Click **Administration > Reboot**

Select **Immediate** and click on **Reboot** button.

Note that the device might take some time to reboot.



18. In the Network Connections window (see steps 3. 4. and 5. above), right-click the Merging Technologies PCIe 8257 RAVENNA Network Card and select Properties.

Select the Obtain an IP address automatically radio button and also select Obtain DNS server address automatically, click on OK.



19. The switch is now configured and ready to use, and the Merging RAVENNA Network Card should have auto-configured itself with an IP in the 169.254.x.x range.

You can verify this by opening a browser and typing 169.254.1.254 in the address bar, and log in.

Cisco SG350 Routers Manual Switch Configuration - Legacy

General Info.

This is in no case an exhaustive configuration procedure, It's a simple guide on how to configure these switches to use them with Ravenna/AES67 networks.

Access SG350 switch Administration

Config Files

Please note that this only applies if you are accessing the router for the 1st time.

MERGING TECHNOLOGIES

If you load one of Merging configuration files, the ip address for the admin page is **169.254.1.254** and the default user name and password is **cisco**

If you are doing this without one of our config files then follow this guide.

1. Plug a network cable to the router/switch and to your computer.
2. Set your computer to **use an IP** in the **192.168.1.x** address pool.

i The Cisco routers/switch's come with a default network configuration in that IP pool.

Default IP: 192.168.1.254

In order for your computer to communicate with the router/switch you must set your computer to use an IP that is in that IP RANGE.

The router/switch default IP can be changed configuration page once you are logged into it.

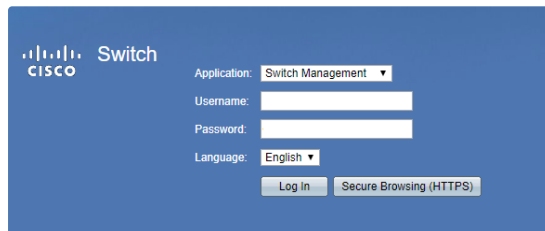
You can find more information about it in the CISCO user manual

3. Open a navigator page to navigate to: <http://192.168.1.254>
4. Once the page loads you will be prompted to enter the user name and password to login.

[HTTP://192.168.1.254](http://192.168.1.254)

Default user name: **cisco**

Default password: **cisco**

The image shows the login page for a Cisco switch. It has a blue header with the Cisco logo and the word "Switch". Below the header, there are fields for "Application" (set to "Switch Management"), "Username", "Password", and "Language" (set to "English"). There are "Log In" and "Secure Browsing (HTTPS)" buttons at the bottom.

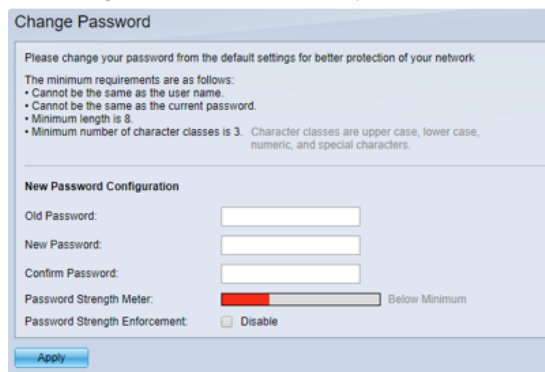
5. Change default user password.

After the login prompt, you will be asked to change that default password to whatever you want.

It is a required step and the first one into securing you're router/switch, it is also a one time step only.

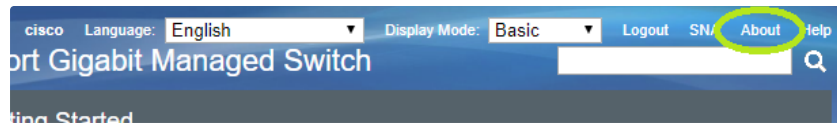
After the default is changed, if you wish to change it again it you will have to do that in the Administration page.

Resetting the switch to "factory defaults" that will also ask you to do this step again.

The image shows the "Change Password" page. It has a title "Change Password" and a message: "Please change your password from the default settings for better protection of your network". Below this, it lists minimum requirements: "Cannot be the same as the user name", "Cannot be the same as the current password", "Minimum length is 8", and "Minimum number of character classes is 3. Character classes are upper case, lower case, numeric, and special characters." There is a section for "New Password Configuration" with fields for "Old Password", "New Password", and "Confirm Password". Below these is a "Password Strength Meter" showing a red bar and the text "Below Minimum". There is also a checkbox for "Password Strength Enforcement" which is currently unchecked. An "Apply" button is at the bottom.

6. The Administration page will now load and you cant start configuring your switch.
7. Make sure the switch is running firmware **2.3.5.63** or above.
Click on the **About** button on top right of the screen.

MERGING TECHNOLOGIES



If you have to update the firmware, refer to [*Cisco 350, 350X, and 550X Series Managed Switches Administration Guide - Firmware Operations*](#) section.

[Click here to access Cisco documentation website](#)

SG-350 - Single VLAN configuration

First step is to change the IP configuration to use a APIPA (Automatic Private Internet Protocol Addressing) type of IP.

The administration page will then be only accessed through this new IP.

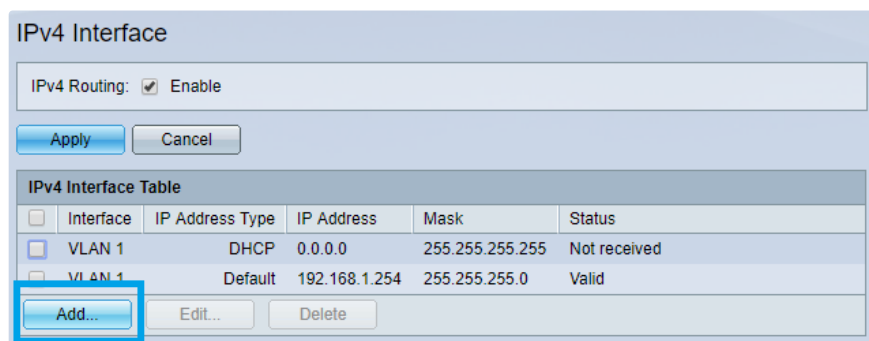
Putting this in an APIPA IP range (169.254.0.0/16) will ensure that you can always access its administration page.

Ravenna devices generally use APIPA IP range to communicate over the network.

1. In the **Getting Started** page, click on **Change Device IP Address**



2. Click on the **Add** button at the bottom of the IPv4 Interface Table.

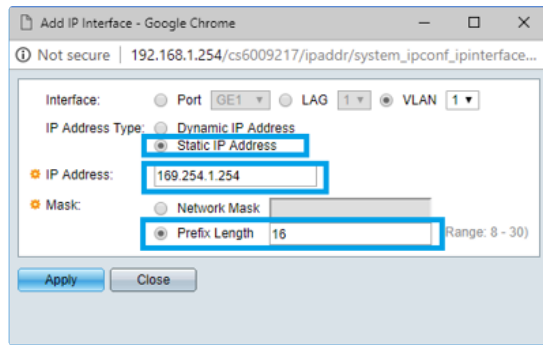


3. Set the *IP Address type* to **Static IP Address**.

Enter **169.254.1.254** in the *IP Address* field.

For the *Mask* setting, select **Prefix Length** and enter **16**.

MERGING TECHNOLOGIES



That will make your switch administration page respond to that IP address.

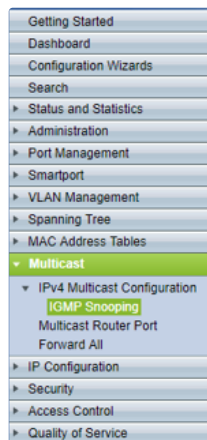
Note that we used Prefix Length instead of Network mask (16 is the same as 255.255.0.0).

4. Click on **Apply** to save the changes.
5. The switch will now change its IP address, therefore the 192.168.1.254 page you are actually using will stop responding.
6. The switch is now only accessible on [HTTP://169.254.1.254](http://169.254.1.254)
You will probably need to change to change your computer IP to "Obtain an IP address automatically"
7. Enter **169.254.1.254** in your browser, and enter your credentials.

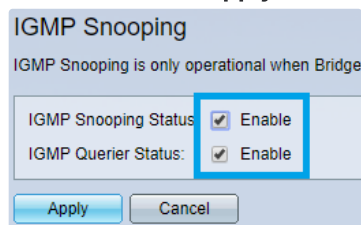
8. On the left pane menu, click on **MULTICAST**.

Then click on **IPv4 Multicast Configuration** to expand it.

Click now on **IGMP SNOOPING**.

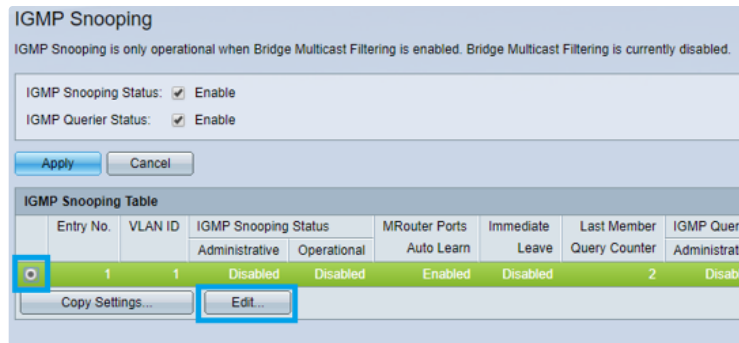


9. In the IGMP Snooping page, enable both the **IGMP Snooping Status** and **IGMP Querier Status** checkboxes.
Then click on **Apply**.

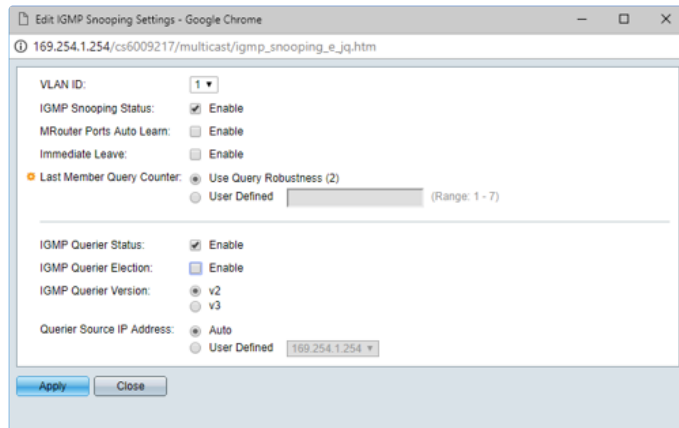


10. On the **IGMP Snooping Table**, click on the radio button to select and then click on **Edit**.

MERGING TECHNOLOGIES



11. Configure the IGMP Snooping Settings as on the picture below, and click **Apply** once done.

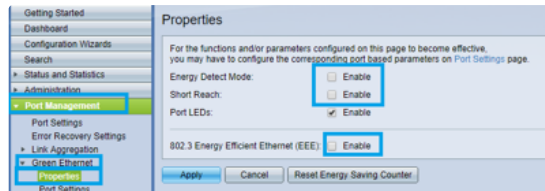


12. By default, Green Ethernet settings are applied, this needs to be disabled.

Please browse to **Port Management > Green Ethernet > Properties**

Untick both **Energy Detect Mode** and **Short Reach**, and untick **802.3 Energy Efficient Ethernet (IEEE)** as well.

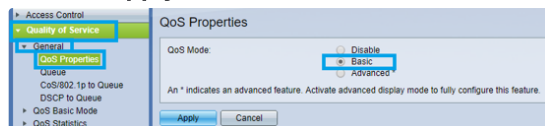
Click on **Apply** once done.



13. Browse now to **Quality of Service > General > QoS Properties**.

The **QoS Mode** should be set to **Basic**.

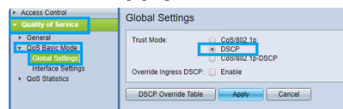
Click on **Apply**



14. Go now in **Quality of Service > QoS Basic Mode > Global settings**.

The **Trust Mode** should be set to **DSCP**

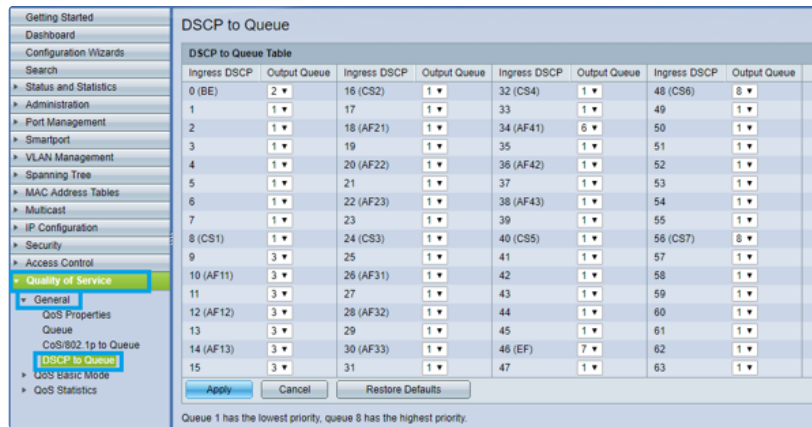
Click on **Apply**.



15. Go back to **Quality of Service > General**, then **DSCP to Queue**.

Change the **DSCP to Queue** Settings as shown in the following picture and click **Apply** once done.

MERGING TECHNOLOGIES



Note : Queue 34 : RTP AES67 / Queue 46 : PTP AES67 / RTP Ravenna / Queue 48 : PTP Ravenna / Queue 56 : PTP Dante

16. Now is a good time to save the configuration.

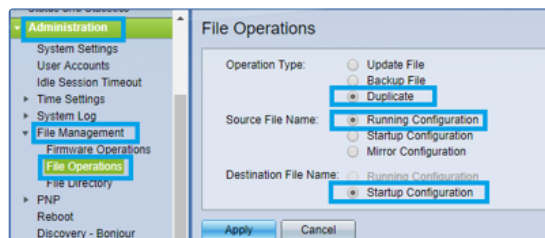
Go in **Administration > File Management > File Operations**.

Select **Duplicate** as *Operation Type*.

Source File Name : **Running Configuration**

Destination File Name : **Startup Configuration**

Click on **Apply**



This will apply the current settings to the start up configuration.

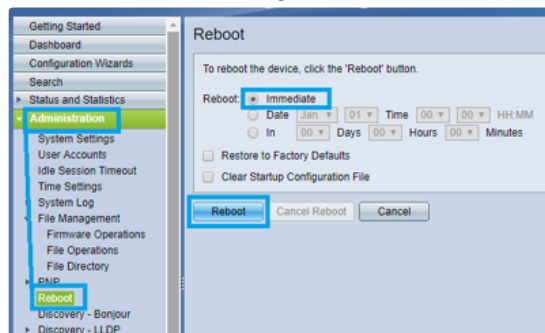
In other terms that makes that configuration to be permanent (unless a reset of the device is done).

17. You must now restart the switch for the changes to apply.

Click **Administration > Reboot**

Select **Immediate** and click on **Reboot** button.

Note that the device might take some time to reboot.



SG-350 - Dual VLAN configuration

Adding VLANs.

MERGING TECHNOLOGIES

1x VLAN for the Ravenna AES67 and 1x VLAN for regular networking.

VLAN1 : will be used for regular networking.

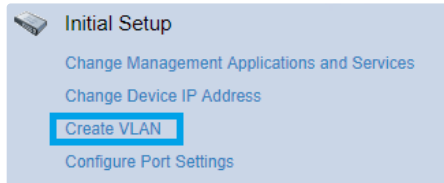
VLAN2 : will be used for Ravenna AES67.

By default the switch already has VLAN1 created with defaults for regular networking.

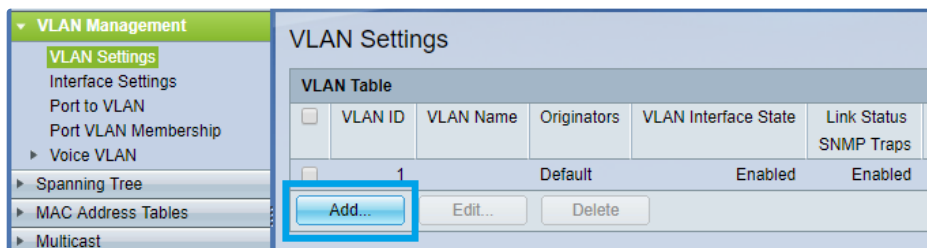
So we will be adding VLAN2 for the for the Ravenna AES67 networking.

Once connected to the switch :

1. In the **Getting Started** page, click on **Create VLAN**.



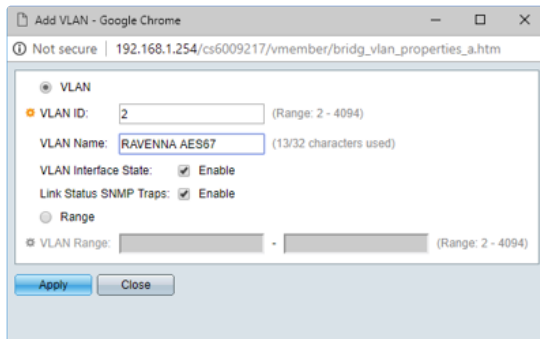
2. Click on the **Add** button at the bottom of the VLAN Table.



3. Set the **VLAN ID**: 2 and enter a **VLAN NAME** (can be anything you want, please do not use special characters).

Make sure **VLAN Interface Status** and **Link Status SNMP Traps** are both active.

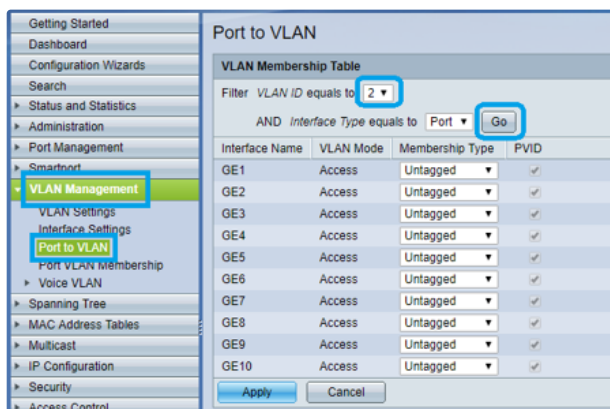
Click on **Apply** once done.



4. Go to **VLAN Management > PORT TO VLAN**,

In the *Filter* section, set the **VLAN ID** to 2, and **Interface Type** to **Port**.

Click on **Go**.



MERGING TECHNOLOGIES

5. Now you can see that all ports for VLAN 2 are excluded, you need to assign the required ports to this RAVENNA/AES67 VLAN.

Set the required ports from *Excluded* to **Untagged** (in the picture below, ports 5 to 8 and port 10 are assigned to VLAN 2).

Click on **Apply** once done.

Port to VLAN

VLAN Membership Table

Filter VLAN ID equals to 2

AND Interface Type equals to Port Go

Interface Name	VLAN Mode	Membership Type	PVID
GE1	Access	Excluded	☐
GE2	Access	Excluded	☐
GE3	Access	Excluded	☐
GE4	Access	Excluded	☐
GE5	Access	Untagged	☒
GE6	Access	Untagged	☒
GE7	Access	Untagged	☒
GE8	Access	Untagged	☒
GE9	Access	Excluded	☐
GE10	Access	Untagged	☒

Apply Cancel

6. You may now check your VLAN1 config.

In the *Filter* section, set the *VLAN ID* to 1, and *Interface Type* to **Port**.

Click on **Go**.

You can see that the ports you have added to VLAN 2 are excluded from VLAN 1.

Port to VLAN

VLAN Membership Table

Filter VLAN ID equals to 1

AND Interface Type equals to Port Go

Interface Name	VLAN Mode	Membership Type	PVID
GE1	Access	Untagged	☒
GE2	Access	Untagged	☒
GE3	Access	Untagged	☒
GE4	Access	Untagged	☒
GE5	Access	Excluded	☐
GE6	Access	Excluded	☐
GE7	Access	Excluded	☐
GE8	Access	Excluded	☐
GE9	Access	Untagged	☒
GE10	Access	Excluded	☐

Apply Cancel

7. In the **Getting Started** page, click on **Change Device IP Address**

Initial Setup

- Change Management Applications and Services
- Change Device IP Address**
- Create VLAN
- Configure Port Settings

8. Click on the **Add** button at the bottom of the IPv4 Interface Table.

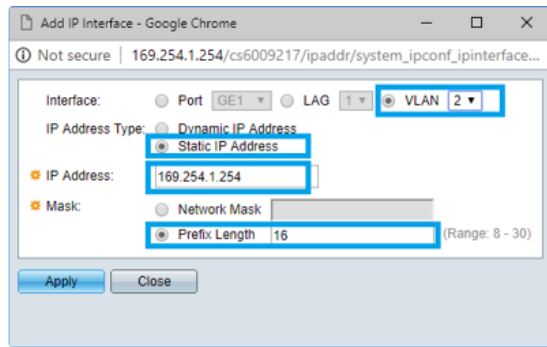
Make sure **VLAN is set to 2**

Set the *IP Address type* to **Static IP Address**.

Enter **169.254.1.254** in the *IP Address* field.

For the *Mask* setting, select **Prefix Length** and enter **16**.

MERGING TECHNOLOGIES

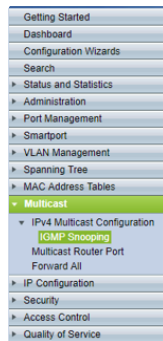


That will make your switch administration page respond to that IP address.

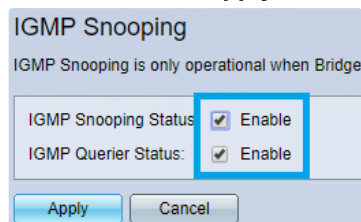
Note that we used Prefix Length instead of Network mask (16 is the same as 255.255.0.0).

9. Click on **Apply** to save the changes.
10. The switch will now change its IP address, therefore the 192.168.1.254 page you are actually using will stop responding.
11. The switch is now only accessible on [HTTP://169.254.1.254](http://169.254.1.254)
You will probably need to change to change your computer IP to "Obtain an IP address automatically"
Please make sure you are physically connected to a port assign to **VLAN2** (in our example, port 6)
Note : you can do the same operation for VLAN1, to be able to access the Management interface for both VLANs.
But you have to use another IP address (192.168.1.254 for example)
12. Enter **169.254.1.254** in your browser, and enter your credentials.
13. On the left pane menu, click on **MULTICAST**.
14. Then click on **IPv4 Multicast Configuration** to expand it.

Click now on **IGMP SNOOPING**.

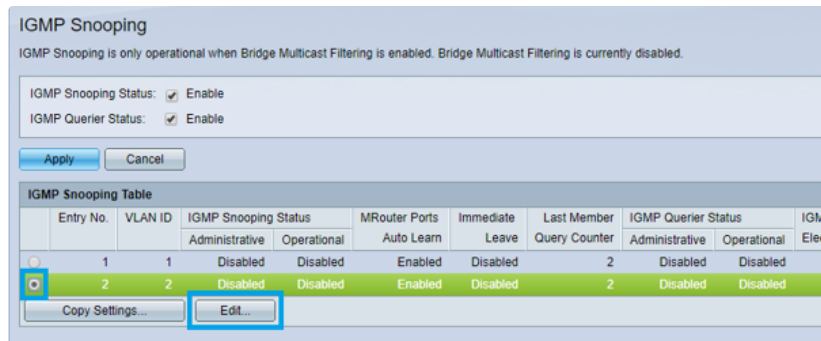


15. In the IGMP Snooping page, enable both the **IGMP Snooping Status** and **IGMP Querier Status** checkboxes.
Then click on on **Apply**.

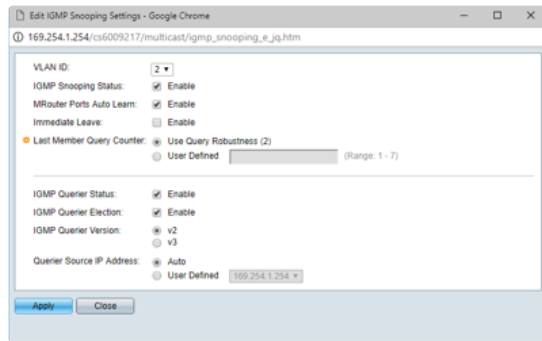


16. On the **IGMP Snooping Table**, click on the radio button next to **VLAN 2** to select and then click on **Edit**.

MERGING TECHNOLOGIES



17. Configure the IGMP Snooping Settings as on the picture below, and click **Apply** once done.

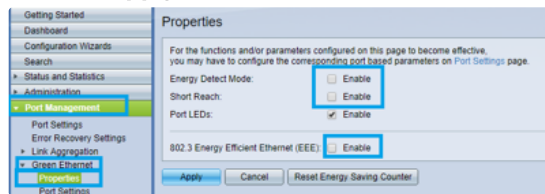


18. By default, Green Ethernet settings are applied, this needs to be disabled.

Please browse to **Port Management > Green Ethernet > Properties**

Untick both **Energy Detect Mode** and **Short Reach**, and untick **802.3 Energy Efficient Ethernet (IEEE)** as well.

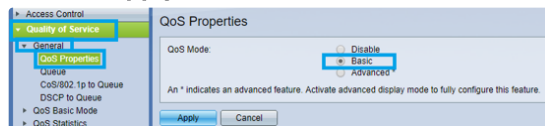
Click on **Apply** once done.



19. Browse now to **Quality of Service > General > QoS Properties**.

The **QoS Mode** should be set to **Basic**.

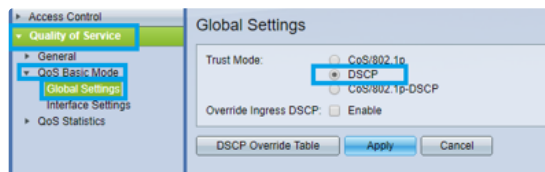
Click on **Apply**



20. Go now in **Quality of Service > QoS Basic Mode > Global settings**.

The **Trust Mode** should be set to **DSCP**

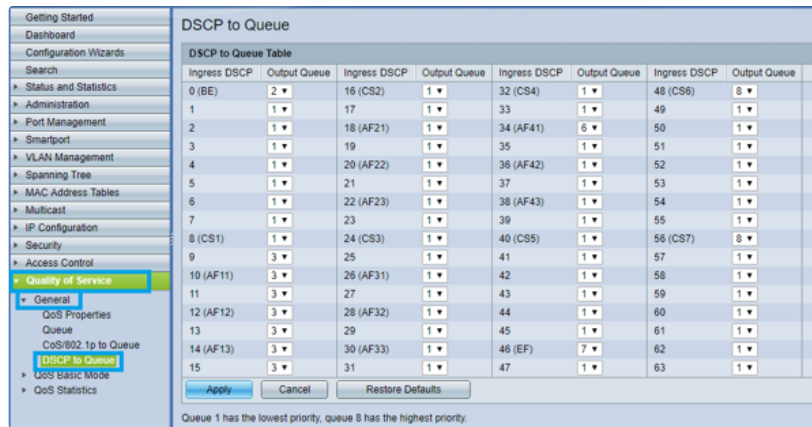
Click on **Apply**.



21. Go back to **Quality of Service > General**, then **DSCP to Queue**.

Change the **DSCP to Queue** Settings as shown in the following picture and click **Apply** once done.

MERGING TECHNOLOGIES



Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue
0 (BE)	2	16 (CS2)	1	32 (CS4)	1	48 (CS6)	8
1	1	17	1	33	1	49	1
2	1	18 (AF21)	1	34 (AF41)	6	50	1
3	1	19	1	35	1	51	1
4	1	20 (AF22)	1	36 (AF42)	1	52	1
5	1	21	1	37	1	53	1
6	1	22 (AF23)	1	38 (AF43)	1	54	1
7	1	23	1	39	1	55	1
8 (CS1)	1	24 (CS3)	1	40 (CS5)	1	56 (CS7)	8
9	3	25	1	41	1	57	1
10 (AF11)	3	26 (AF31)	1	42	1	58	1
11	3	27	1	43	1	59	1
12 (AF12)	3	28 (AF32)	1	44	1	60	1
13	3	29	1	45	1	61	1
14 (AF13)	3	30 (AF33)	1	46 (EF)	7	62	1
15	3	31	1	47	1	63	1

Note : Queue 34 : RTP AES67 / Queue 46 : PTP AES67 / RTP Ravenna / Queue 48 : PTP Ravenna / Queue 56 : PTP Dante

22. Now is a good time to save the configuration.

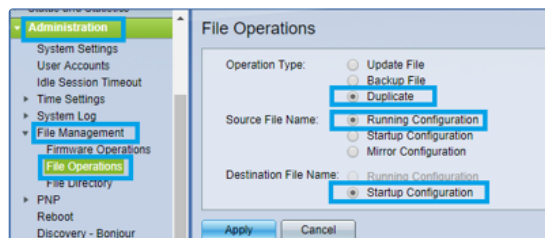
Go in **Administration > File Management > File Operations**.

Select **Duplicate** as *Operation Type*.

Source File Name : **Running Configuration**

Destination File Name : **Startup Configuration**

Click on **Apply**



This will apply the current settings to the start up configuration.

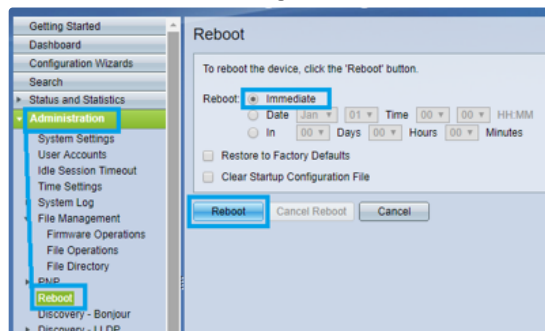
In other terms that makes that configuration to be permanent (unless a reset of the device is done).

23. You must now restart the switch for the changes to apply.

Click **Administration > Reboot**

Select **Immediate** and click on **Reboot** button.

Note that the device might take some time to reboot.



SG350 - Backup Switch Configuration

1. Go to **Administration** and click **File Management** to expand it.

Click on **File Operations**.

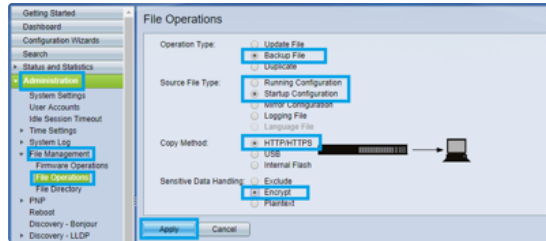
MERGING TECHNOLOGIES

2. *Operation Type* has to be set to **Backup File**.

Source File Type : select **Running** or **Startup Configuration**, depending on your needs.

Copy Method : **HTTP/HTTPS**

Sensitive Data Handling : **Encrypt**



3. Click on **Apply**.

The configuration file can be downloaded in your browser (as a .txt file)

SG350 - Import Switch Configuration file

IMPORTANT NOTE :

If you try to import a configuration file into the Running Configuration (the current one), **it will fail.**

What you need to do is import from a configuration file **to the startup configuration file as a destination** and then reboot.

1. Go into **Administration** then click **File Management** to expand, then click **File Operations** to open its pane.

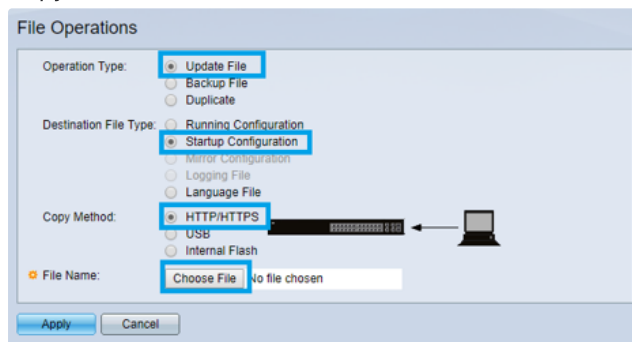


2. Now select

Operation Type : **Update File**

Destination File Type : **Startup Configuration**

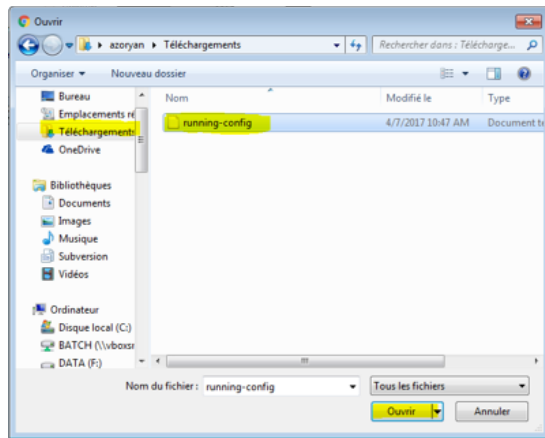
Copy Method : **HTTP/HTTPS**



3. Then click **Choose File** and a new window will pop up.

In the **Choose File** window point to the downloaded configuration file location, select it and click **Open**.

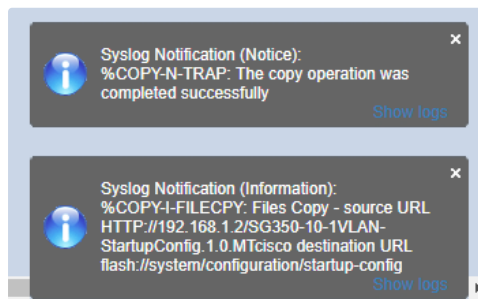
MERGING TECHNOLOGIES



4. Then click **Apply** for it to load your configuration file into the STARTUP CONFIG.



5. The switch will send a notification that the operation has been completed.



6. You must now restart the switch for the changes to apply.

Click **Administration > Reboot**

Select **Immediate** and click on **Reboot** button.

Note that the device might take some time to reboot.