

MERGING TECHNOLOGIES

Cisco C1300-8 Auto-configuration

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.

This guide applies to the whole Cisco Catalyst series (C1300)

Before Starting

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

 Connecting several Cisco switches together requires additional configuration.

Please also see the [Multiple network switches considerations page](#) and [Cisco Multiple switches configuration guide](#).

 Dante-AES67 devices requires an additional configuration, not included in the configuration files.

See the [Dante devices Multicast Group configuration page](#) for details

Cisco C1300 Switch Auto-configuration Procedure

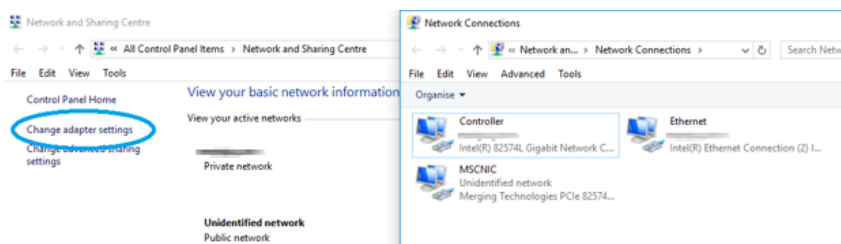
1. Plug a network cable from the switch and to your computer.

The switch will need to initialize, this will take a few minutes before being accessible.

2. Set your computer to use an IP in the **192.168.1.x** address pool.

✓ How to manually setup an IP address on Windows

Go in *Windows Control Panel > Network and Sharing Center*, then click on *Change Adapter settings* (left)



Right click on the adapter that you have to configure and select *Properties*.

Select the *Internet Protocol Version 4 (TCP/IP)*, then click on the *Properties* button.

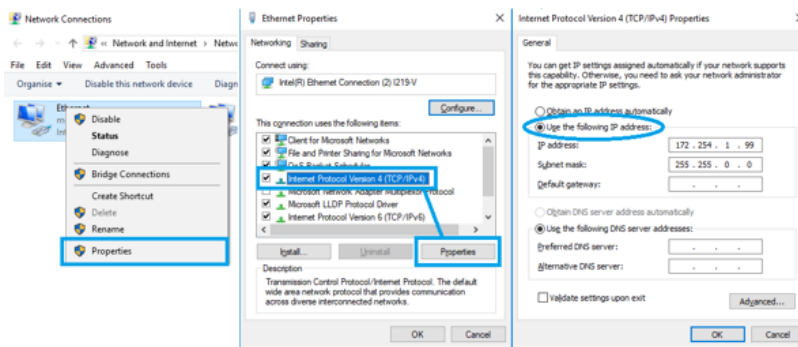
Set it to "**Use the following IP addresses**", then enter the IP address. It must be in the same range as the Cisco switch connected on it, for example : adapter IP is **192.168.1.1**

The Subnet mask is mandatory; Windows can set it automatically, simply click in the Subnet mask field.

You may need to also change the attached network device(s) IP address, consult their documentation for

MERGING TECHNOLOGIES

details.



- ✓ How to manually setup an IP address on MacOS

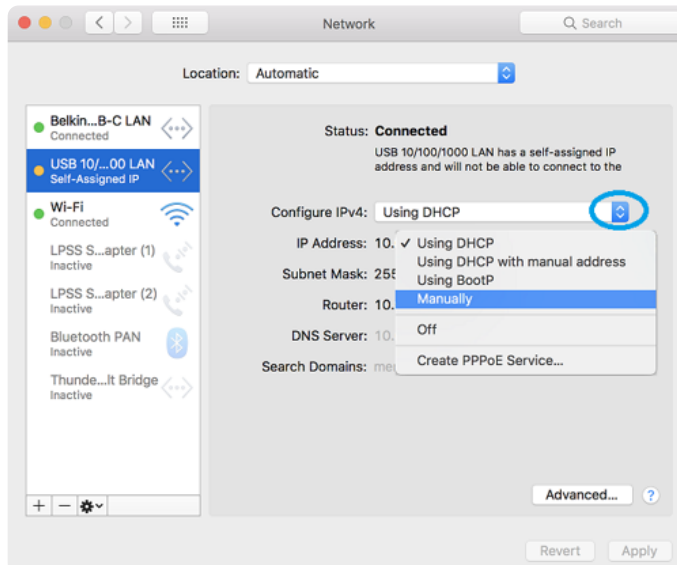
Go in the *System Preferences* and select *Network*.



Select the adapter that needs to be configured, and click on the arrow next to *Configure IPv4*.

Select **Manually** in the drop down list, and enter the required IP address.

It must be in the same range as the Cisco switch connected on it, for example : adapter IP is **192.168.1.1**



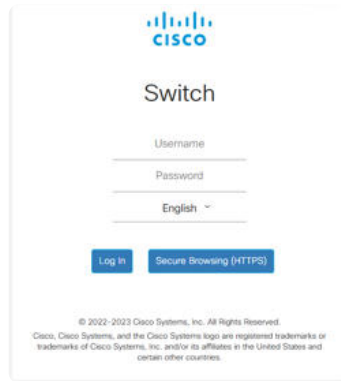
The Subnet mask is mandatory; MacOS can set it automatically, simply click in the Subnet mask field.

3. Open a navigator page to navigate to **http://192.168.1.254** (Cisco switches default IP address)

You will be prompted to enter the user name and password to login.

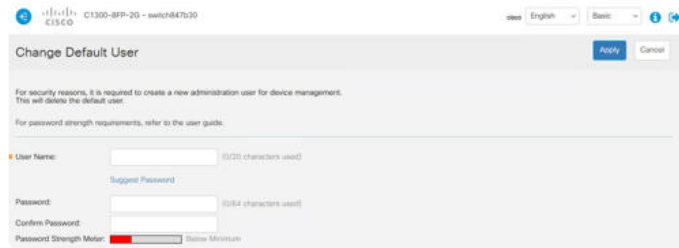
Default user name: **cisco** Default password: **cisco**

MERGING TECHNOLOGIES



4. After the login prompt, you will be asked to set your own password.

Please note the minimum character numbers and password complexity required.

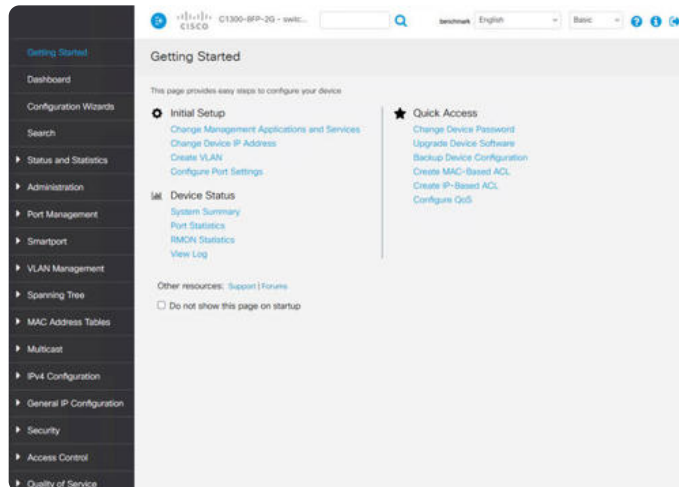


If you wish to change the password later, you will have to go in the Administration > User Accounts page. Resetting the switch to "factory defaults" will also require to do this step again.

5. For ease of use, please activate the side bar by clicking on the blue icon on the top left corner.



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



7. Download the latest configuration file for your Cisco C1300 switch model :

[Cisco C1300-8 - Single VLAN](#)

[Cisco C1300-8 - Dual VLAN](#) Port 1 to 4 and 9 : Regular network, Port 5 to 8 and 10 : Ravenna Network

Note : After applying the Dual VLAN config file, the switch Administration pages will only be accessible on port 6 to 8 and 10.

MERGING TECHNOLOGIES

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**)

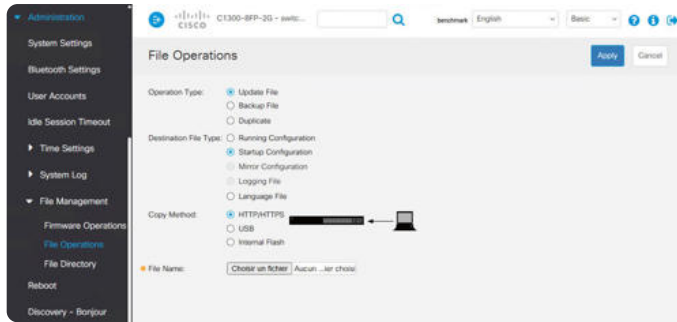
8. Go to **Administration > File Management**.

Select **File Operations**.

9. *Operation Type* : **Update File**

Destination File Type : **Startup Configuration**

Copy Method : **HTTP/HTTPS**

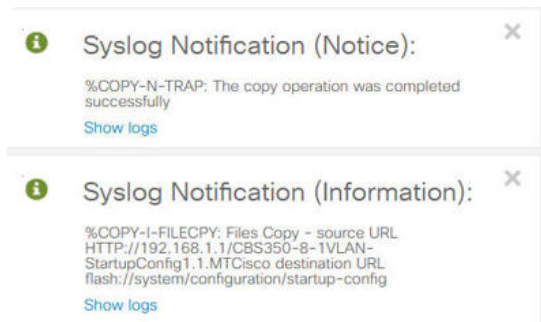


10. Now click on **Choose File** and in the choose file window, browse to the configuration file you want to import.

Select the configuration file and click on **Open**.

11. Back in the main window, click on **Apply** to load your configuration file into the Startup Configuration.

Once imported, the switch will send a notification that the operation has been completed.

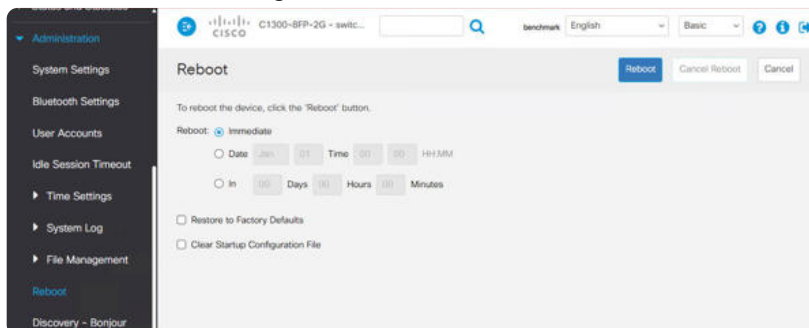


12. You must now restart the switch for the changes to apply.

Click **Administration > Reboot**

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

Note that the device might take some time to reboot.



13. The switch will now change its IP address to **169.254.1.254**, therefore the 192.168.1.254 page you are actually using will stop responding.

To be able to access the switch now, please set your computer to use an IP in the **169.254.x.x** address pool.

MERGING TECHNOLOGIES

Refer to the ["How to manually setup an IP address"](#) above, but this time, set your network adapter to *automatically obtain an IP address* (Windows) - *Using DHCP* (MacOS)

14. 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.
15. You will have to log in using the same default credentials as point 3, to then chose a new user login and password.

Please note that any changes requires you to click on **Apply** and that you then have to go in **Administration > File Management > File Operations** to properly save the changes (Duplicate from the Running Configuration to the Startup Configuration)

SSM - IGMP V3

The configuration files are set to use IGMP v2. If you plan to use SSM (Source-Specific Multicast - see Merging devices Advanced pages), you will have to activate IGMP v3 manually.

Please see the C1300 Manual configuration

MERGING TECHNOLOGIES

C1300 Managed switch manual configuration



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.

Connecting several Cisco switches together requires additional configuration.

Please also see the [Multiple network switches considerations page](#)

Important note for DANTE-AES67 devices

When Dante devices are connected to a Cisco switch configured with the Merging settings, an additional configuration step is required.

Please follow the instructions below after the switch configuration.

Access C1300 switch Administration page

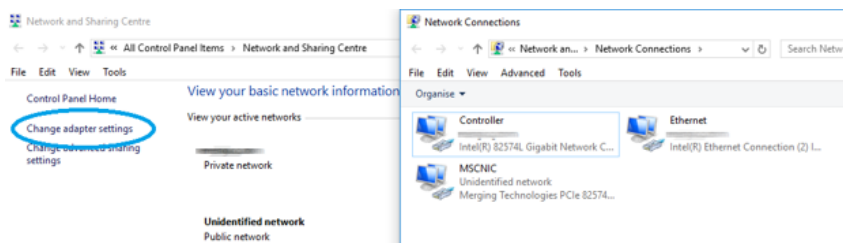
1. Plug a network cable from the switch and to your computer.

The switch will need to initialize, this will take a few minutes before being accessible.

2. Set your computer to use an IP in the **192.168.1.x** address pool.

✓ How to manually setup an IP address on Windows

Go in *Windows Control Panel > Network and Sharing Center*, then click on *Change Adapter settings* (left)



MERGING TECHNOLOGIES

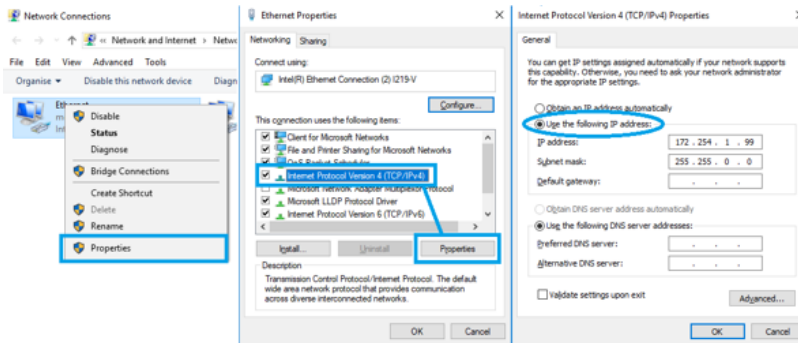
Right click on the adapter that you have to configure and select *Properties*.

Select the *Internet Protocol Version 4 (TCP/IP)*, then click on the *Properties* button.

Set it to "**Use the following IP addresses**", then enter the IP address. It must be in the same range as the Cisco switch connected on it, for example : adapter IP is **192.168.1.1**

The Subnet mask is mandatory; Windows can set it automatically, simply click in the Subnet mask field.

You may need to also change the attached network device(s) IP address, consult their documentation for details.



-
- ✓ How to manually setup an IP address on MacOS

Go in the *System Preferences* and select *Network*.

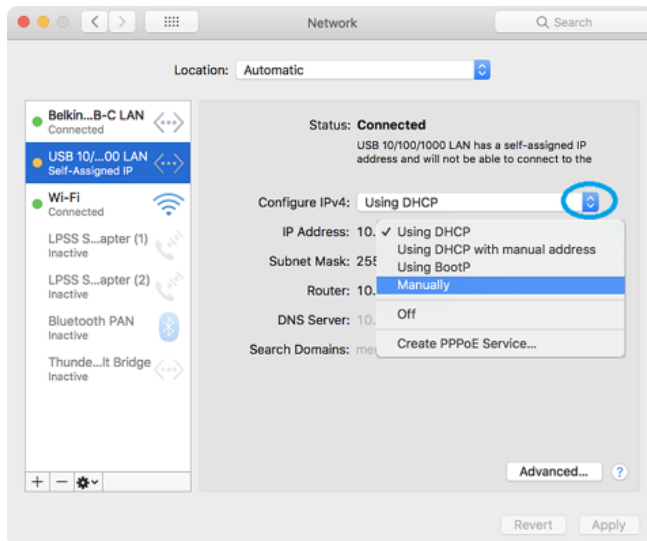


Select the adapter that needs to be configured, and click on the arrow next to *Configure IPv4*.

Select **Manually** in the drop down list, and enter the required IP address.

It must be in the same range as the Cisco switch connected on it, for example : adapter IP is **192.168.1.1**

MERGING TECHNOLOGIES

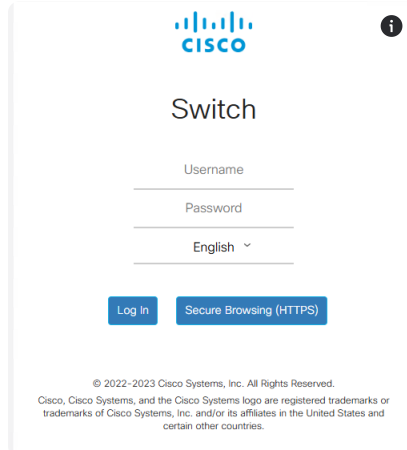


The Subnet mask is mandatory; MacOS can set it automatically, simply click in the Subnet mask field.

3. Open a navigator page to navigate to **http://192.168.1.254** (Cisco switches default IP address)
4. **You will be prompted to enter the user name and password to login.**

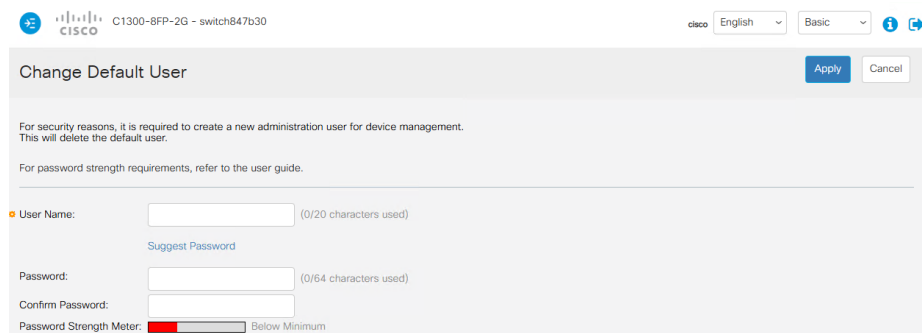
Default user name: **cisco**

Default password: **cisco**



5. After the login prompt, you will be asked to set your own password.

Please note the minimum character numbers and password complexity required.



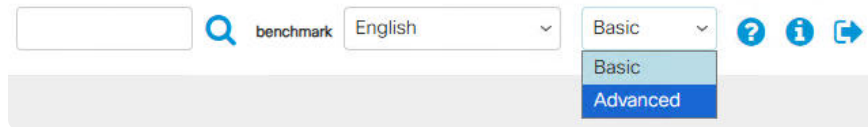
MERGING TECHNOLOGIES

If you wish to change the password later, you will have to go in the Administration > User Accounts page.

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

6. Log back into the switch using the credentials you just chose

7. Set the switch in **Advanced mode** on the top right corner.

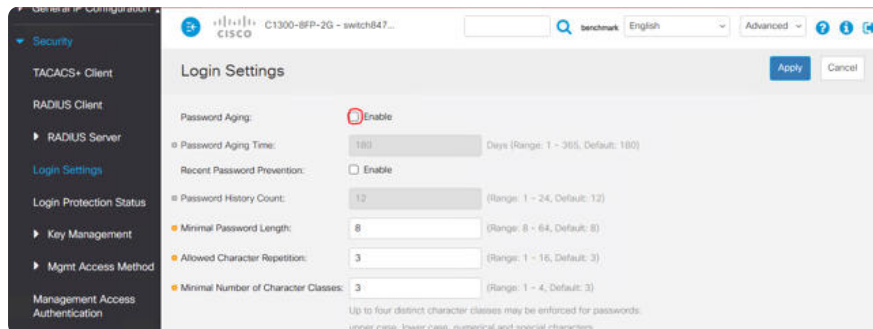


For ease of use, please also activate the side bar by clicking on the blue icon on the top left corner.



8. By default, the switch may ask you to renew the password every 6 months.

While this behavior enhances the security, you may disable it in **Security > Login Settings**, by removing the **Password Aging** option.



Single VLAN Configuration

The first step is to change the IP configuration to use an APIPA address (Automatic Private Internet Protocol Addressing).

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

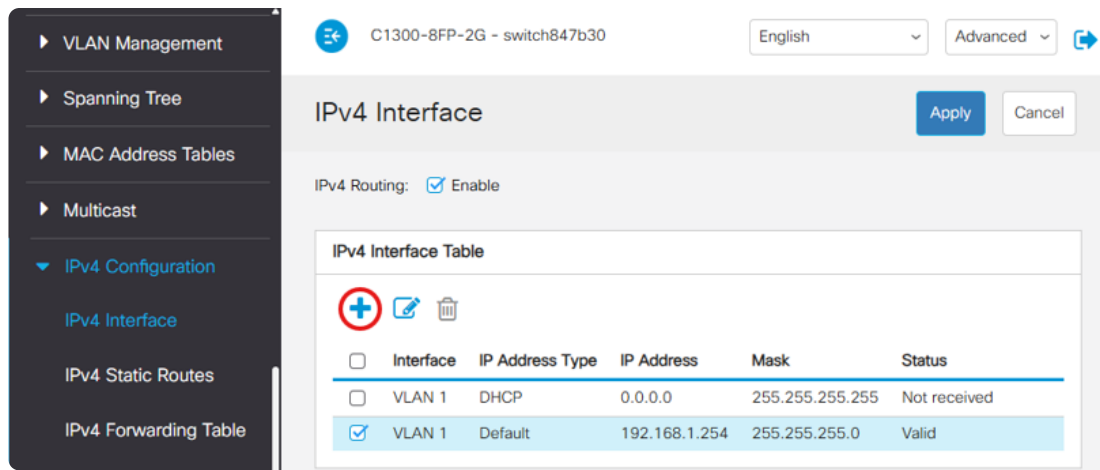
Setting the switch in the APIPA IP range (169.254.0.0/16) will ensure that you can always access its administration page.

Merging Ravenna devices generally use APIPA IP range to communicate over the network (Network - Auto setting on Horus/Hapi/Anubis/...)

1. Browse to **IPv4 Configuration > IPv4 Interface**

Click on the **±** button to add a static address

MERGING TECHNOLOGIES



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**.

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

Add IP Interface

X

Interface:

☐ Port GE1

☐ LAG 1

☒ VLAN 1

☐ Loopback

IP Address Type:

☐ Dynamic IP Address

☒ Static IP Address

IP Address:

169.254.1.254

Mask:

☐ Network Mask

☒ Prefix Length 16 (Range: 8 - 30)

Apply

Close

3. Click on **Apply** to save the changes.

The switch will ask you to confirm the change.

4. The switch will now change its IP address to **169.254.1.254**, therefore the 192.168.1.254 page you are actually using will stop responding.

5. To be able to access the switch now, please set your computer to use an IP in the **169.254.x.x** address pool.

Refer to the "How to manually setup an IP address" above, but this time, set your network adapter to *automatically obtain an IP address* (Windows) - *Using DHCP* (MacOS)

6. Enter **169.254.1.254** in your browser, and enter your credentials.

Make sure the switch administration page is in **Advanced mode** (top right corner)

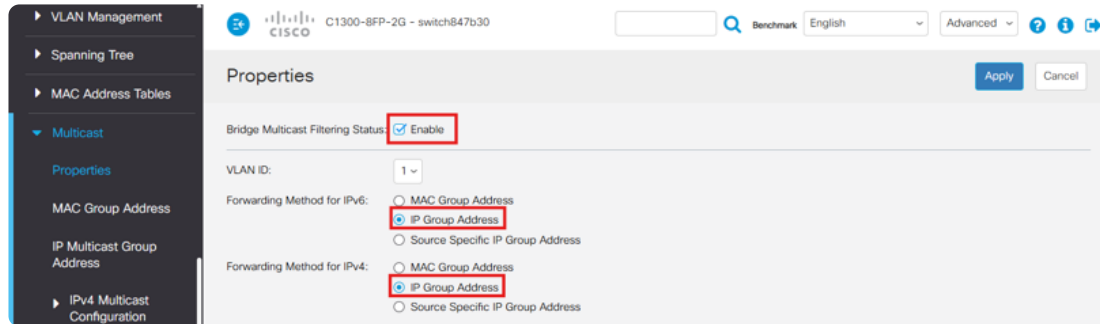
MERGING TECHNOLOGIES

7. Please browse to **Multicast > Properties**.

Set the *Bridge Multicast Filtering Status* to **Enable**

Set both *Forwarding method for IPv6* and *IPv4* to **IP Group address**.

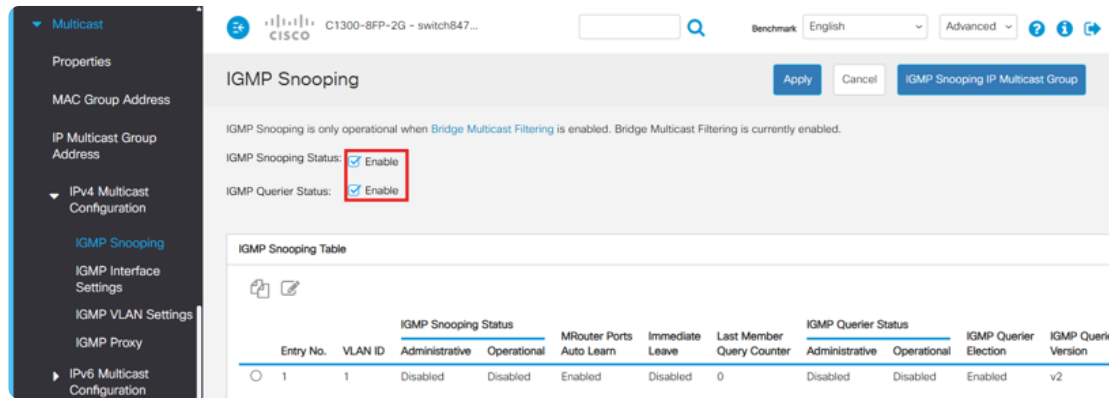
Click on **Apply** once done.



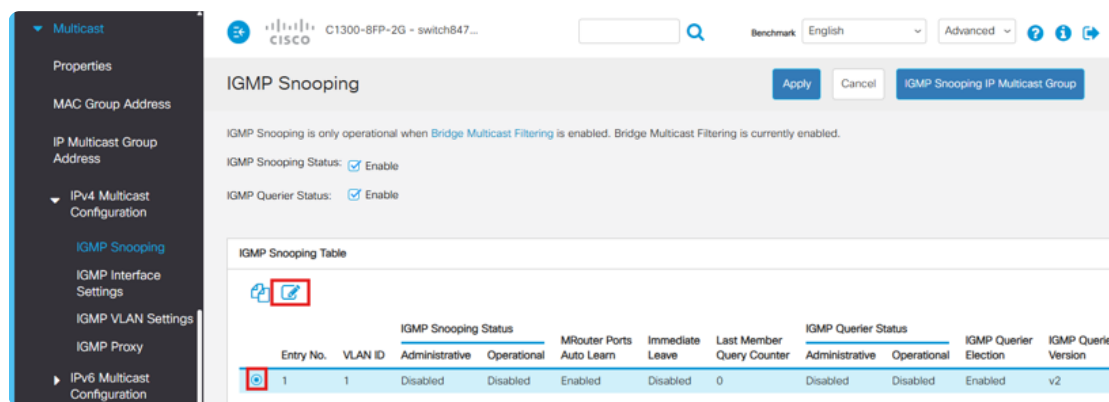
8. Now go in **Multicast > IPv4 Multicast Configuration > IGMP Snooping**.

Enable both the **IGMP Snooping Status** and **IGMP Querier Status** checkboxes.

Then click on **Apply**.



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



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

MERGING TECHNOLOGIES

Edit IGMP Snooping Settings

X

VLAN ID:

IGMP Snooping Status: ☒ Enable

MRouter Ports Auto Learn: ☐ Enable

Immediate Leave: ☐ Enable

Last Member Query Counter: ☒ Use Query Robustness (2)
☐ User Defined (Range: 1 - 7)

IGMP Querier Status: ☒ Enable

IGMP Querier Election: ☒ Enable

IGMP Querier Version: ☒ v2
☐ v3

Querier Source IP Address: ☒ Auto
☐ User Defined

Apply

Close

Note: SSM - IGMP v3

If you plan to use SSM (Source-Specific Multicast - see Merging devices Advanced pages), please activate IGMP v3.

11. Go in **Multicast > IPv4 Multicast Configuration > IGMP VLAN Settings**

Click on the radio button to select and then click on the **Edit** icon.

IGMP VLAN Settings

IGMP Settings Table

Entry No.	Interface Name	Router IGMP Version	Query Robustness	Query Interval (sec)	Query Max Response Interval (sec)	Last Member Query Interval (msec)	Multicast TTL Threshold
1	VLAN 1	v3	2	125	10	1000	0

12. Please set the *Router IGMP Version* to **v2**

And the *Query Interval* to **30**

Click on **Apply**

MERGING TECHNOLOGIES

Edit IGMP Settings

X

Interface Name:

Router IGMP Version
☐ v1
☒ v2
☐ v3

Query Robustness: (Range: 1 - 7, Default: 2)

Query Interval: sec (Range: 30 - 18000, Default: 125)

Query Max Response Interval: sec (Range: 5 - 20, Default: 10)

Last Member Query Interval: mS (Range: 100 - 25500 in multiples of 100, Default: 1000)

Multicast TTL Threshold: Hops (Range: 0 - 256, Default: 0)

Apply

Close

Note: SSM - IGMP v3

If you plan to use SSM (Source-Specific Multicast - see Merging devices Advanced pages), please activate IGMP v3.

13. Browse now to **Multicast > Unregistered Multicast**

Set all ports to **Filtering**

Click on **Apply**

VLAN Management
Spanning Tree
MAC Address Tables
Multicast
Properties
MAC Group Address
IP Multicast Group Address
IPv4 Multicast Configuration
IPv6 Multicast Configuration
IGMP/MLD Snooping IP Multicast Group
Multicast Router Port
Forward All
Unregistered Multicast

CISCO C1300-8FP-2G - switch847...

Unregistered Multicast

Filter: Interface Type equals to Port Go

Port	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10
Forwarding	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Filtering	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

14. Go to the **Multicast > IP Multicast Group Address**

Click on the “+” icon :

MERGING TECHNOLOGIES

Search

- ▶ Status and Statistics
- ▶ Administration
- ▶ Port Management
- ▶ Smartport
- ▶ VLAN Management
- ▶ Spanning Tree
- ▶ MAC Address Tables
- ▼ Multicast
 - Properties
 - MAC Group Address
 - IP Multicast Group Address

IP Multicast Group Address

The Bridge Multicast Filtering is currently enabled.
For IP Multicast Configuration to be effective, the [Bridge Multicast Filtering](#) must be enabled.

IP Multicast Group Address Table

+ Details...

Filter: ☐ VLAN ID equals to (Range: 1 - 4094)

☐ IP Version equals to

☐ IP Multicast Group Address equals to

☐ Source IP Address equals to Go Clear Filter

☐	VLAN ID	IP Multicast Group Address	Source IP Address
☐	1	224.0.0.251	*

15. Add the “224.0.0.251” IPV4 address, on VLAN 1, to allow discovery of the devices and streams :

Add IP Multicast Group Address X

✱ VLAN ID: (Range: 1 - 4094)

IP Version: ☐ Version 6 ☒ Version 4

✱ IP Multicast Group Address:

Source Specific: ☐ Include

✱ Source IP Address:

Apply Close

Click on **Apply** once done.

16. Now, select this new address, and open its “details :

MERGING TECHNOLOGIES

Search

- ▶ Status and Statistics
- ▶ Administration
- ▶ Port Management
- ▶ Smartport
- ▶ VLAN Management
- ▶ Spanning Tree
- ▶ MAC Address Tables
- ▼ Multicast
 - Properties
 - MAC Group Address
 - IP Multicast Group Address

IP Multicast Group Address

The Bridge Multicast Filtering is currently enabled.
For IP Multicast Configuration to be effective, the [Bridge Multicast Filtering](#) must be enabled.

IP Multicast Group Address Table

+ Details...

Filter: ☐ VLAN ID equals to (Range: 1 - 4094)

☐ IP Version equals to

☐ IP Multicast Group Address equals to

☐ Source IP Address equals to

☐	VLAN ID	IP Multicast Group Address	Source IP Address
☒	1	224.0.0.251	*

17. Set the routing of this IP to “static” on every port :

IP Multicast Interface Settings

X

VLAN ID: 1
IP Version: Version 4
IP Multicast Group Address: 224.0.0.251
Source IP Address: *

Filter: Interface Type equals to

Interface	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10
Static	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Dynamic	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Forbidden	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
None	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Click on **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**

MERGING TECHNOLOGIES

Ethernet (IEEE) as well.

Click on **Apply** once done.

The screenshot shows the 'Properties' page for Port Management on a Cisco switch. The left sidebar lists various settings under 'Port Management', with 'Properties' selected. The main area contains several configuration options, all of which are set to 'Enable' and are highlighted with red boxes: 'Energy Detect Mode', 'Short Reach', 'Port LEDs', and '802.3 Energy Efficient Ethernet (EEE)'. The top of the page shows the device name 'C1300-8FP-2G - switch847...' and a search bar.

19. By default, the Bluetooth functionality is also enabled.

You may disable it under **Administration > Bluetooth Settings**

Untick **Bluetooth Service**

Click on **Apply** once done.

The screenshot shows the 'Bluetooth Settings' page on a Cisco switch. The left sidebar lists various settings under 'Administration', with 'Bluetooth Settings' selected. The main area contains several configuration options. The 'Bluetooth Service' checkbox is checked and highlighted with a red box. Other options include 'PIN' (set to Encrypted), 'Bluetooth Device Name' (set to Switch Host Name), 'BT Interface Description', 'BT IP Interface' (set to None), 'BT IP Address', 'BT IP Mask' (set to Network Mask), and 'Dongle Present' (set to No). The top of the page shows the device name 'C1300-8FP-2G - switch847b30' and a search bar.

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

Set **QoS Mode** to **Basic**.

Click on **Apply**

The screenshot shows the 'QoS Properties' page on a Cisco switch. The left sidebar lists various settings under 'Quality of Service', with 'General' selected and 'QoS Properties' highlighted. The main area contains several configuration options. The 'QoS Mode' radio button is selected and highlighted with a red box. Below it, there is a table for 'Interface CoS Configuration Table' and a 'Filter' section. The top of the page shows the device name 'C1300-8FP-2G - switch847b30' and a search bar.

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

Set **Trust Mode** to **DSCP**

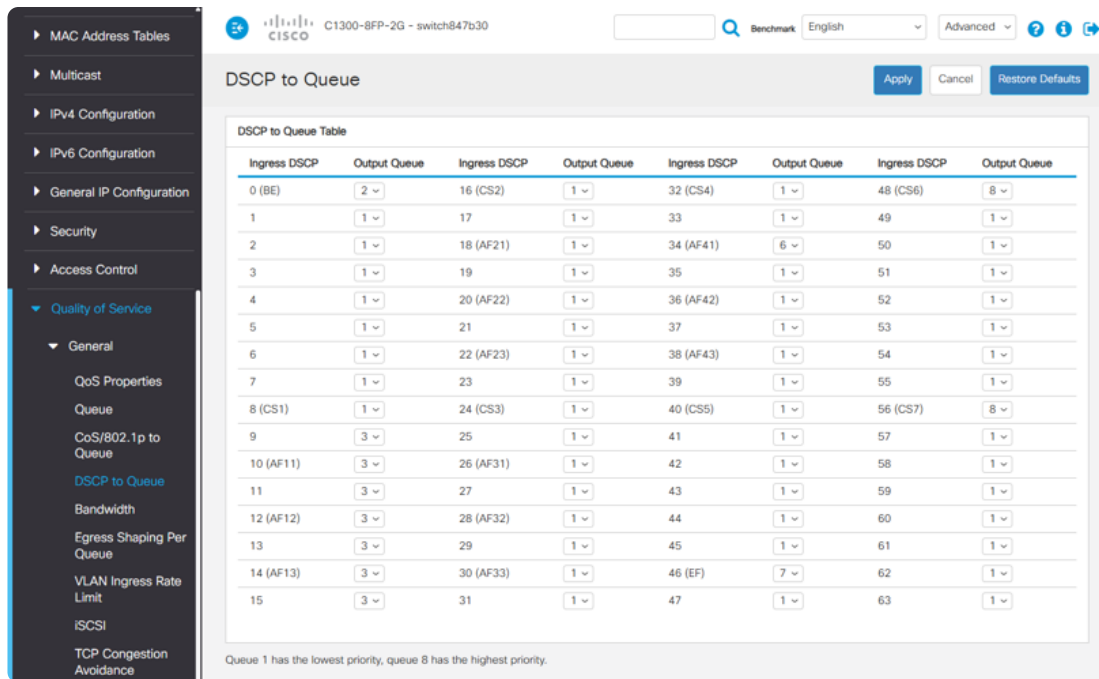
Click on **Apply**.

MERGING TECHNOLOGIES



22. Go back to **Quality of Service > General > DSCP to Queue**.

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



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

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

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

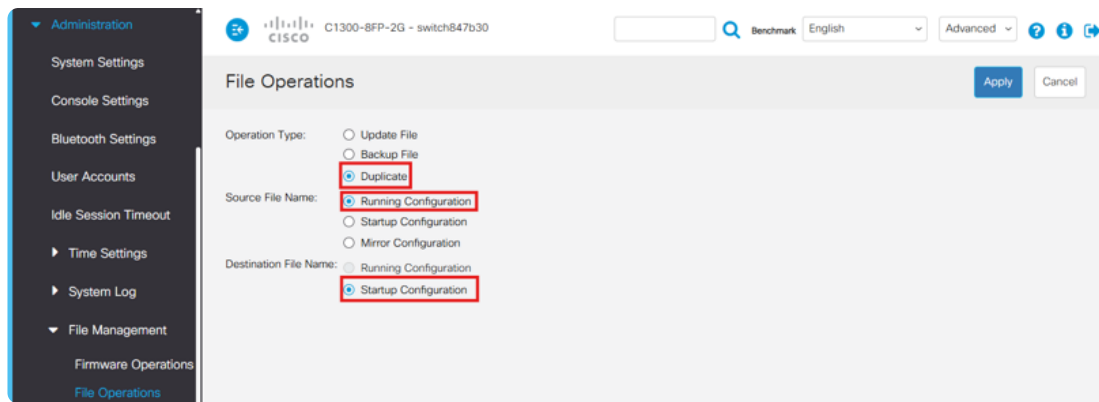
Select **Duplicate** as *Operation Type*.

Source File Name : **Running Configuration**

Destination File Name : **Startup Configuration**

Click on **Apply**

MERGING TECHNOLOGIES



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

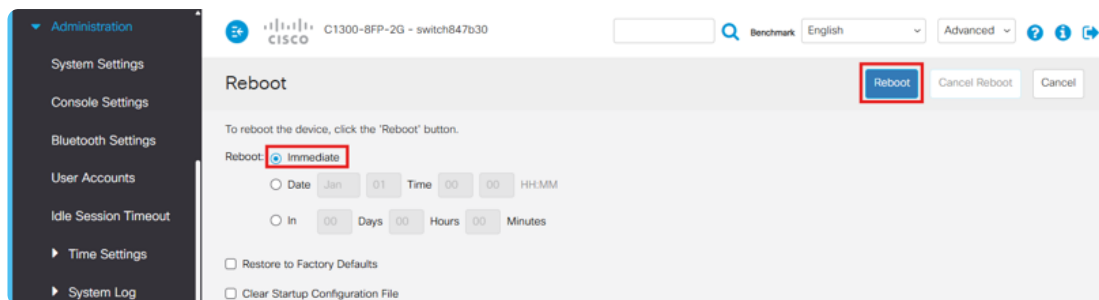
In other terms that makes the configuration to be permanent (unless a reset of the device is done).

24. 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.



Dual VLAN Configuration

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.

VLAN1 : will be used for regular networking.

VLAN2 : will be used for Ravenna AES67.

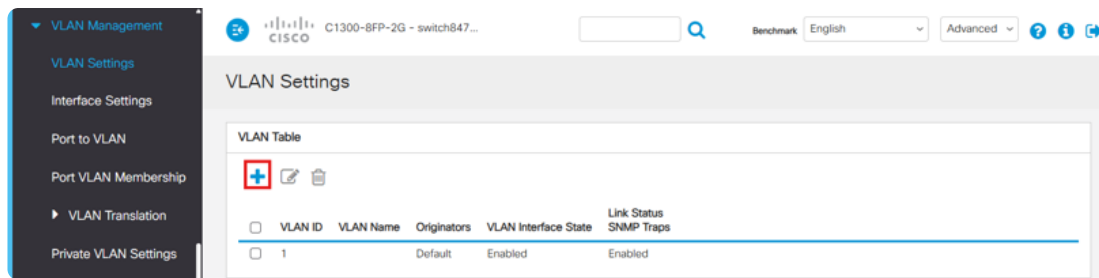
Once connected to the switch as described above.

Note : The switch Administration pages will only be accessible from VLAN 2.

1. Go in **VLAN Management > VLAN Settings**

Click on the **±** button at the bottom of the VLAN Table.

MERGING TECHNOLOGIES



2. 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

Add VLAN

VLAN

VLAN ID: 2 (Range: 2 - 4094)

VLAN Name: RAV/AES67 (9/32 characters used)

VLAN Interface State: ☒ Enable

Link Status SNMP Traps: ☒ Enable

☐ Range

* VLAN Range: - (Range: 2 - 4094)

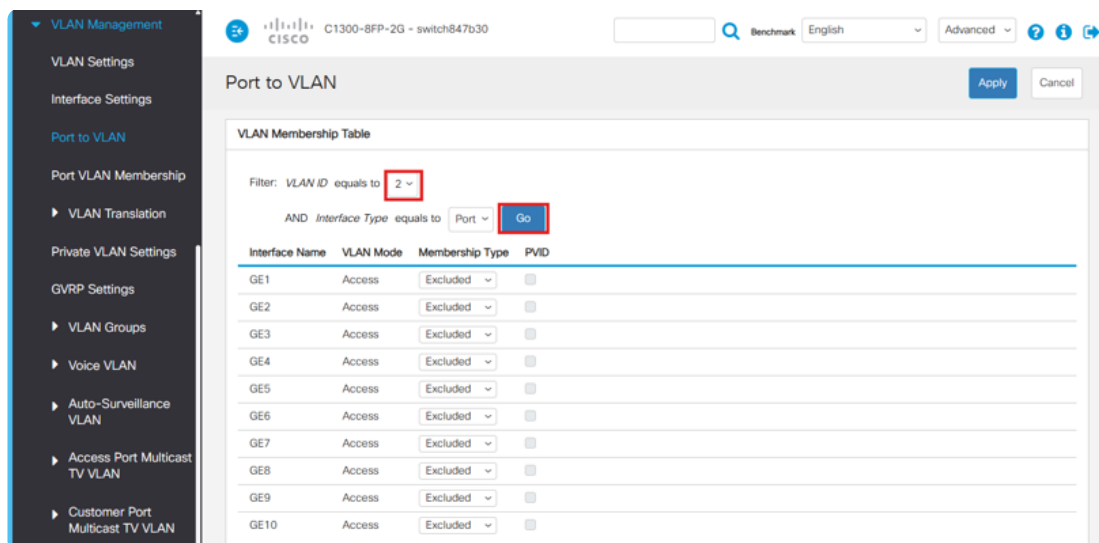
Apply

Close

3. 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

4. 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	

5. 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**.

Port to VLAN

VLAN Membership Table

Filter: VLAN ID equals to 1

AND Interface Type equals to Port Go

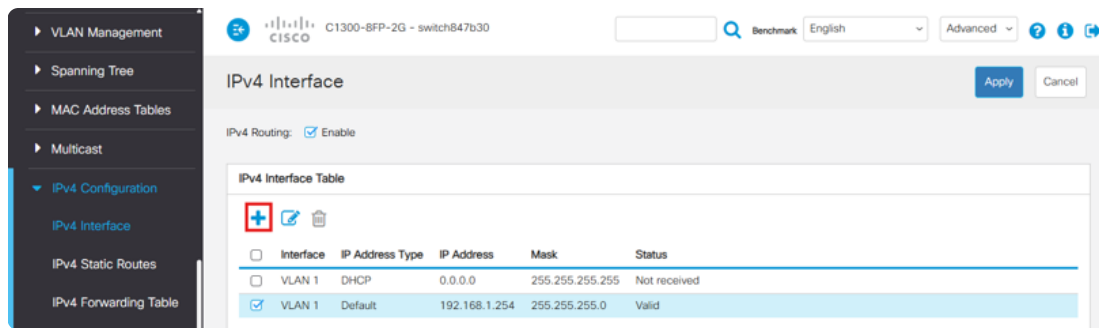
Interface Name	VLAN Mode	Membership Type	PVID
GE1	Access	Untagged	
GE2	Access	Untagged	
GE3	Access	Untagged	
GE4	Access	Untagged	
GE5	Access	Excluded	
GE6	Access	Excluded	
GE7	Access	Excluded	
GE8	Access	Excluded	
GE9	Access	Untagged	
GE10	Access	Excluded	

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

6. Browse to **IPv4 Configuration > IPv4 Interface**

Click on the **±** button to add a static address

MERGING TECHNOLOGIES



7. 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**.

Add IP Interface X

Interface: ☐ Port GE1 ☐ LAG 1 ☒ VLAN 2 ☐ Loopback

IP Address Type: ☐ Dynamic IP Address ☒ Static IP Address

IP Address: 169.254.1.254

Mask: ☐ Network Mask ☒ Prefix Length 16 (Range: 8 - 30)

8. Click on **Apply** to save the changes.

The switch will ask you to confirm the change.

9. The switch will now change its IP address to **169.254.1.254**, therefore the 192.168.1.254 page you are actually using will stop responding.

To be able to access the switch now, please set your computer to use an IP in the **169.254.x.x** address pool.

Refer to the [Cisco CBS350 Managed switch manual configuration.#IPWin](#) "How to manually setup an IP address" above, but this time, set your network adapter to *automatically obtain an IP address* (Windows) - *Using DHCP* (MacOS)

10. Please make sure you are physically connected to a port assign to **VLAN2** (in our example, port 6)

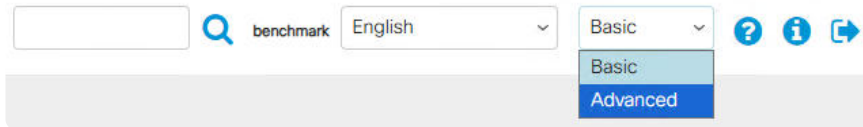
Note : you can do the same operation for VLAN1, to be able to access the Management interface for both VLANs.

But you have to use another IP address (192.168.1.254 for example)

MERGING TECHNOLOGIES

11. Enter **169.254.1.254** in your browser, and enter your credentials.

Make sure the switch administration page is in **Advanced mode** (top right corner)



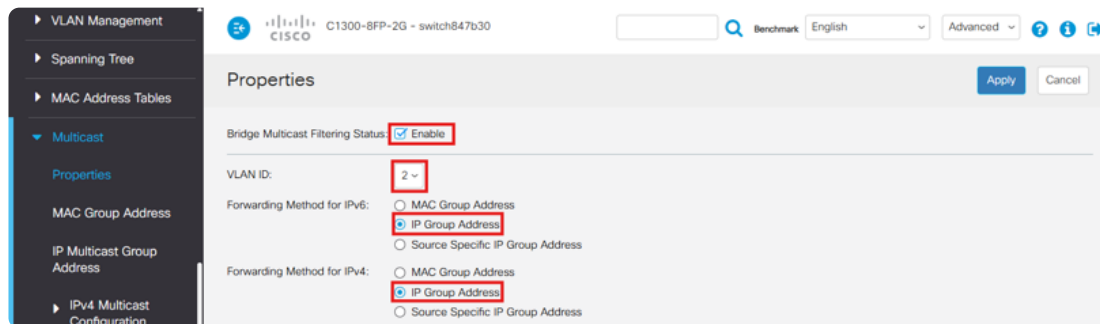
12. Please browse to **Multicast > Properties**.

First set the *VLAN ID* to **2**

Set the *Bridge Multicast Filtering Status* to **Enable**

Set both *Forwarding method for IPv6* and *IPv4* to **IP Group address**.

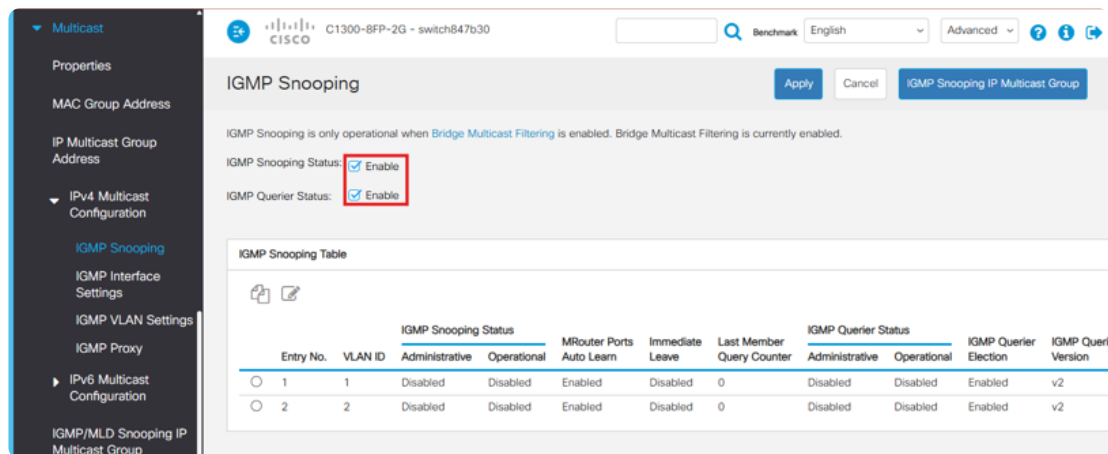
Click on **Apply** once done.



13. Now go in **Multicast > IPV4 Multicast Configuration > IGMP Snooping**.

Enable both the **IGMP Snooping Status** and **IGMP Querier Status** checkboxes.

Then click on on **Apply**.



14. On the **IGMP Snooping Table**, click on the radio button on the VLAN ID2 line to select and then click on the **Edit** icon.

MERGING TECHNOLOGIES

IGMP Snooping

IGMP Snooping is only operational when Bridge Multicast Filtering is enabled. Bridge Multicast Filtering is currently enabled.

IGMP Snooping Status: ☒ Enable

IGMP Querier Status: ☒ Enable

IGMP Snooping Table

Entry No.	VLAN ID	IGMP Snooping Status		MRouter Ports Auto Learn	Immediate Leave	Last Member Query Counter	IGMP Querier Status		IGMP Querier Election	IGMP Querier Version
		Administrative	Operational				Administrative	Operational		
1	1	Disabled	Disabled	Enabled	Disabled	0	Disabled	Disabled	Enabled	v2
2	2	Disabled	Disabled	Enabled	Disabled	0	Disabled	Disabled	Enabled	v2

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

Edit IGMP Snooping Settings

VLAN ID: 2

IGMP Snooping Status: ☒ Enable

MRouter Ports Auto Learn: ☐ Enable

Immediate Leave: ☐ Enable

Last Member Query Counter: ☒ Use Query Robustness (2)
☐ User Defined (Range: 1 - 7)

IGMP Querier Status: ☒ Enable

IGMP Querier Election: ☒ Enable

IGMP Querier Version: ☒ v2
☐ v3

Querier Source IP Address: ☒ Auto
☐ User Defined 169.254.1.254

Apply **Close**

Note: SSM - IGMP v3

If you plan to use SSM (Source-Specific Multicast - see Merging devices Advanced pages), please activate IGMP v3.

16. Go in **Multicast > IPv4 Multicast Configuration > IGMP VLAN Settings**

Click on the radio button on the VLAN 2 line to select and then click on the **Edit** icon.

IGMP VLAN Settings

IGMP Settings Table

Entry No.	Interface Name	Router IGMP Version	Query Robustness	Query Interval (sec)	Query Max Response Interval (sec)	Last Member Query Interval (msec)	Multicast TTL Threshold
1	VLAN 1	v3	2	125	10	1000	0
2	VLAN 2	v3	2	125	10	1000	0

MERGING TECHNOLOGIES

17. Please set the *Router IGMP Version* to **v2**

And the *Query Interval* to **30**

Click on **Apply**

Edit IGMP Settings

X

Interface Name:

VLAN 2

Router IGMP Version

☐ v1

☒ v2

☐ v3

Query Robustness:

2

(Range: 1 - 7, Default: 2)

Query Interval:

30

sec (Range: 30 - 18000, Default: 125)

Query Max Response Interval:

10

sec (Range: 5 - 20, Default: 10)

Last Member Query Interval:

1000

mS (Range: 100 - 25500 in multiples of 100, Default: 1000)

Multicast TTL Threshold:

0

Hops (Range: 0 - 256, Default: 0)

Apply

Close

Note: SSM - IGMP v3

If you plan to use SSM (Source-Specific Multicast - see Merging devices Advanced pages), please activate IGMP v3.

18. Browse now to **Multicast > Unregistered Multicast**

Set the ports you have assigned to VLAN 2 to **Filtering** (in our example, ports 5 to 8 and 10)

Click on **Apply**

VLAN Management

Spanning Tree

MAC Address Tables

Multicast

Properties

MAC Group Address

CISCO

C1300-8FP-2G - switchB47...

Benchmark

English

Advanced

?

i

+

Unregistered Multicast

Apply

Cancel

Filter: Interface Type equals to Port Go

Port

GE1

GE2

GE3

GE4

GE5

GE6

GE7

GE8

GE9

GE10

Forwarding

☒

☒

☒

☒

☐

☐

☐

☐

☒

☐

Filtering

☐

☐

☐

☐

☒

☒

☒

☒

☐

☒

19. Go to the **Multicast > IP Multicast Group Address**

Click on the “+” icon :

MERGING TECHNOLOGIES

The screenshot shows the Cisco Meraki configuration interface for a switch (C1300-8FP-2G - switch847b30). The left sidebar contains a navigation menu with options: Search, Status and Statistics, Administration, Port Management, Smartport, VLAN Management, Spanning Tree, MAC Address Tables, Multicast (selected), Properties, MAC Group Address, and IP Multicast Group Address. The main content area is titled "IP Multicast Group Address" and includes a note: "The Bridge Multicast Filtering is currently enabled. For IP Multicast Configuration to be effective, the Bridge Multicast Filtering must be enabled." Below this is the "IP Multicast Group Address Table" with a filter section and a table of entries.

Search

► Status and Statistics

► Administration

► Port Management

► Smartport

► VLAN Management

► Spanning Tree

► MAC Address Tables

▼ Multicast

Properties

MAC Group Address

IP Multicast Group Address

CISCO C1300-8FP-2G - switch847b30

IP Multicast Group Address

The Bridge Multicast Filtering is currently enabled.
For IP Multicast Configuration to be effective, the [Bridge Multicast Filtering](#) must be enabled.

IP Multicast Group Address Table

[Details...](#)

Filter: ☐ VLAN ID equals to (Range: 1 - 4094)

☐ IP Version equals to

☐ IP Multicast Group Address equals to

☐ Source IP Address equals to [Go](#) [Clear Filter](#)

☐	VLAN ID	IP Multicast Group Address	Source IP Address
☐	1	ff02::1:ff84:7b30	*

20. Add the “224.0.0.251” IPV4 address, on VLAN 2, to allow discovery of the devices and streams :

The dialog box titled "Add IP Multicast Group Address" contains the following fields: VLAN ID (set to 2), IP Version (Version 4 selected), IP Multicast Group Address (set to 224.0.0.251), Source Specific (Include unchecked), and Source IP Address (empty). The dialog has "Apply" and "Close" buttons at the bottom right.

Add IP Multicast Group Address

VLAN ID: (Range: 1 - 4094)

IP Version: ☐ Version 6 ☒ Version 4

IP Multicast Group Address:

Source Specific: ☐ Include

* Source IP Address:

[Apply](#) [Close](#)

Click on **Apply** once done

21. Now, select this new address, and open its “etails :

MERGING TECHNOLOGIES

Search

► Status and Statistics

► Administration

► Port Management

► Smartport

► VLAN Management

► Spanning Tree

► MAC Address Tables

▼ Multicast

Properties

MAC Group Address

IP Multicast Group Address

► IPv4 Multicast Configuration

► IPv6 Multicast Configuration

IGMP/MLD Snooping IP Multicast Group

 C1300-8FP-2G - switch847b30

IP Multicast Group Address

The Bridge Multicast Filtering is currently enabled.
For IP Multicast Configuration to be effective, the [Bridge Multicast Filtering](#) must be enabled.

IP Multicast Group Address Table



Details...

Filter: ☐ VLAN ID equals to (Range: 1 - 4094)
☐ IP Version equals to
☐ IP Multicast Group Address equals to
☐ Source IP Address equals to

☐	VLAN ID	IP Multicast Group Address	Source IP Address
☐	1	ff02::1:ff84:7b30	*
☒	2	224.0.0.251	*
☐	2	224.0.1.129	*
☐	2	239.1.1.250	*
☐	2	239.1.86.101	*
☐	2	239.1.219.2	*
☐	2	239.255.255.250	*
☐	2	239.255.255.255	*

22. Set the routing of this IP to “static” on every port previously assigned to VLAN 2 :

IP Multicast Interface Settings X

VLAN ID: 2

IP Version: Version 4

IP Multicast Group Address: 224.0.0.251

Source IP Address: *

Filter: *Interface Type* equals to

Interface	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10
Static	☐	☐	☐	☐	☒	☒	☒	☒	☐	☒
Dynamic	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Forbidden	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
None	☒	☒	☒	☒	☐	☐	☐	☐	☒	☐

MERGING TECHNOLOGIES

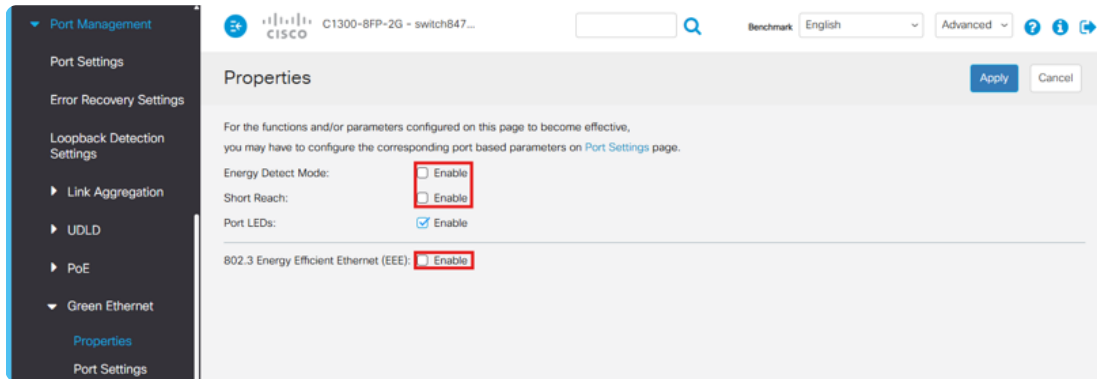
Click on **Apply** once done.

23. 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.

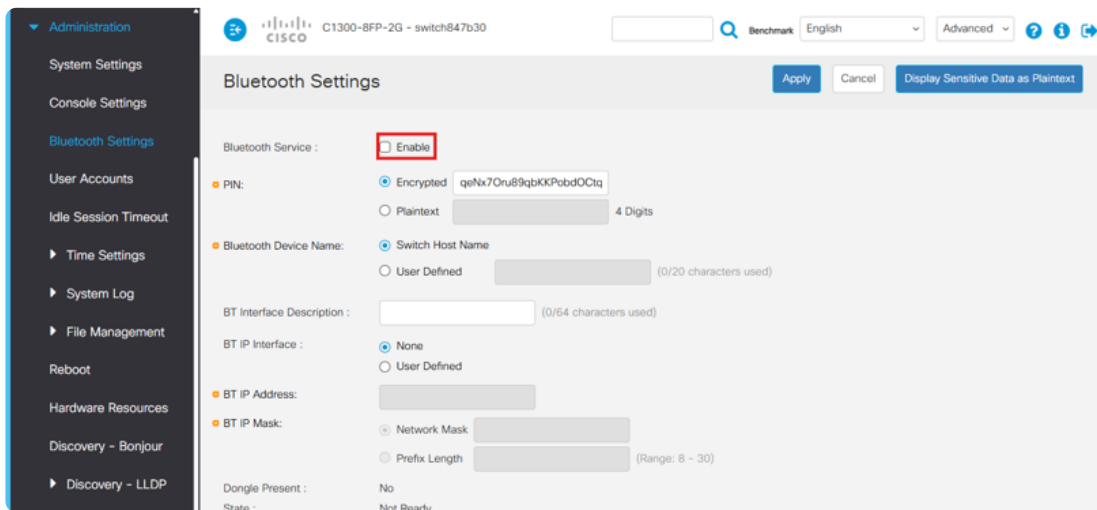


24. By default, the Bluetooth functionality is also enabled.

You may disable it under **Administration > Bluetooth Settings**

Untick **Bluetooth Service**

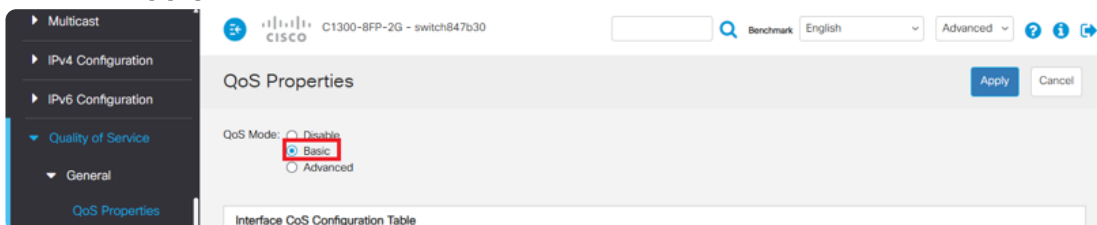
Click on **Apply** once done.



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

Set **QoS Mode** to **Basic**.

Click on **Apply**



MERGING TECHNOLOGIES

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

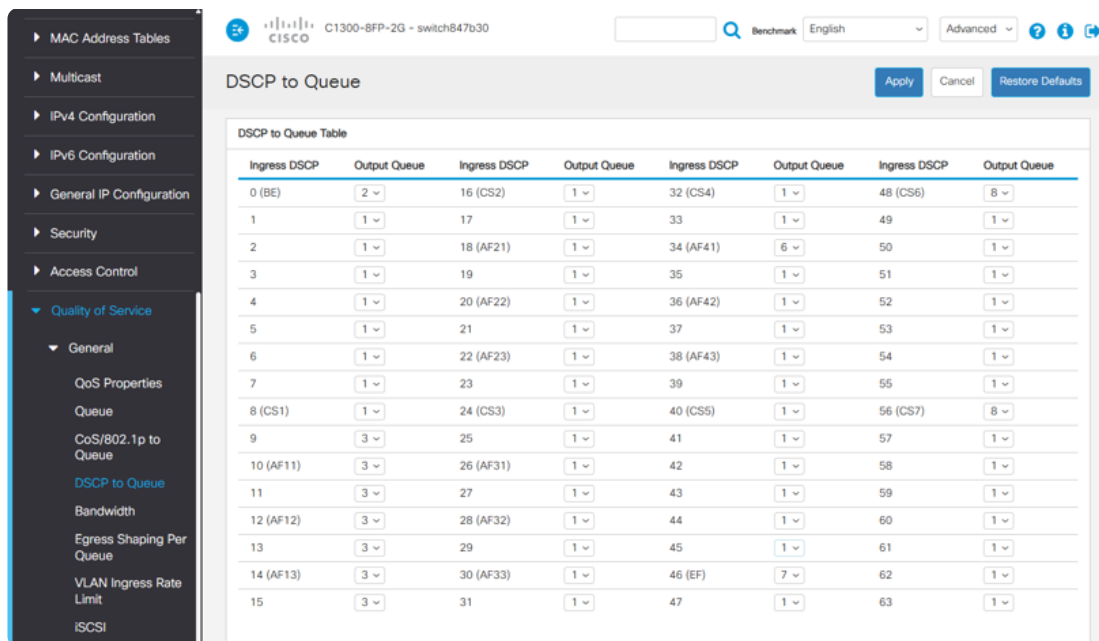
Set **Trust Mode** to **DSCP**

Click on **Apply**.



27. Go back to **Quality of Service > General > DSCP to Queue**.

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



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

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

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

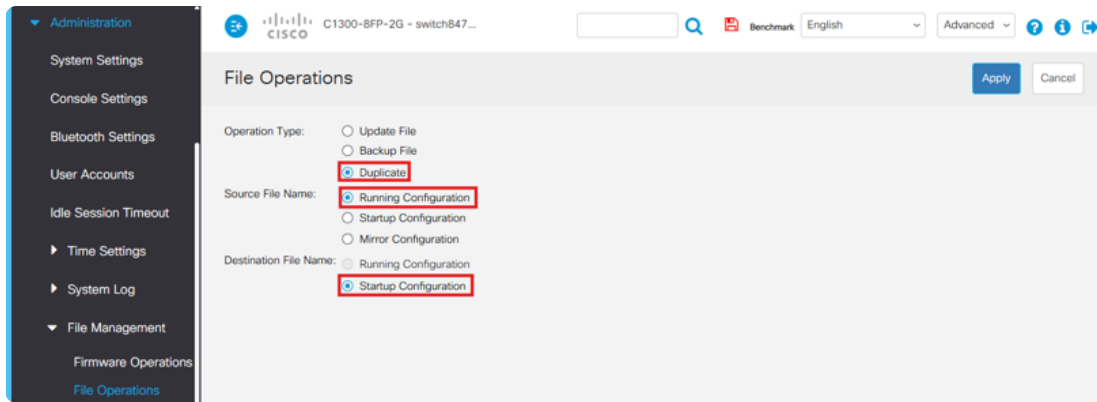
Select **Duplicate** as *Operation Type*.

Source File Name : **Running Configuration**

Destination File Name : **Startup Configuration**

Click on **Apply**

MERGING TECHNOLOGIES



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

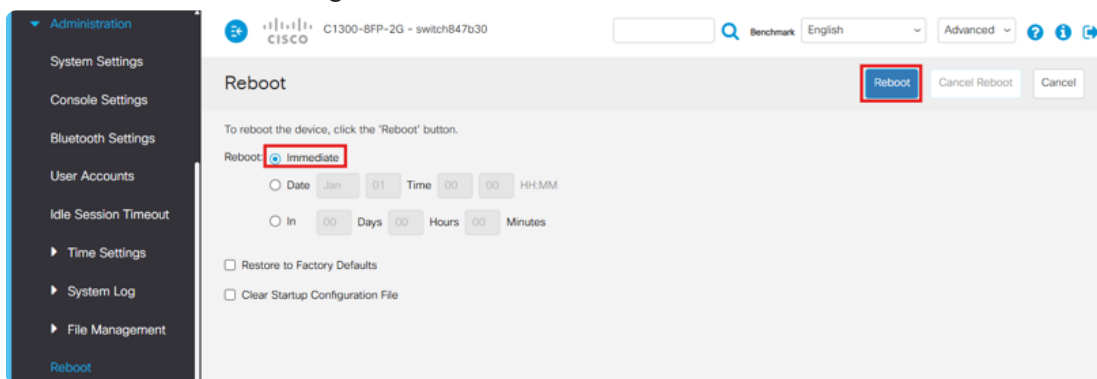
In other terms that makes the configuration to be permanent (unless a reset of the device is done).

29. 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.



How to Backup and import configuration files

Backup your configuration to a file

1. Go to **Administration > File Management**.

Select **File Operations**.

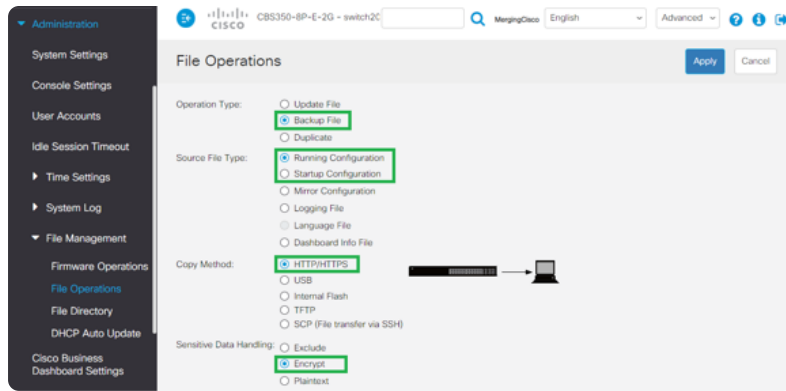
2. *Operation Type* has to be set to **Backup File**.

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

Copy Method : **HTTP/HTTPS**

Sensitive Data Handling : **Encrypt**

MERGING TECHNOLOGIES



3. Click on **Apply**.

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

Import a 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** and then reboot.

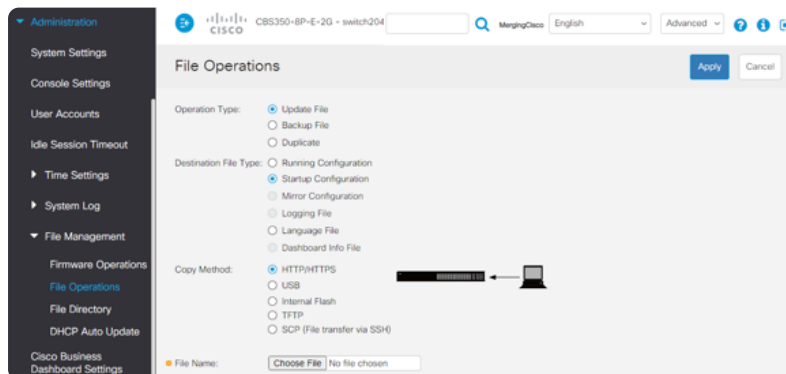
1. Go to **Administration > File Management**.

Select **File Operations**.

2. *Operation Type* : **Update File**

Destination File Type : **Startup Configuration**

Copy Method : **HTTP/HTTPS**



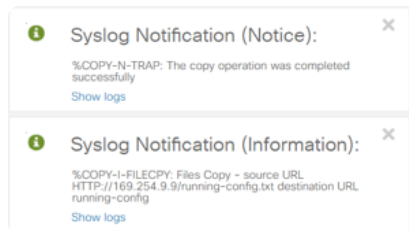
3. Now click on **Choose File** and in the choose file window, browse to the configuration file you want to import.

Select the configuration file and click on **Open**.

4. Back in the main window, click on **Apply** to load your configuration file into the Startup Configuration.

Once imported, the switch will send a notification that the operation has been completed.

MERGING TECHNOLOGIES



5. 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.

