



Cisco SG350-10 の設定

[Cisco SG350-10 の自動設定](#)

[Danteデバイスを接続する場合の追加設定](#)

[複数のCiscoスイッチを使用する場合の追加設定](#)

[基本的な考え方](#)

[スイッチの設定](#)

[Cisco SG350 スwitchのマニュアル設定](#)

[Single VLAN の設定](#)

[Dual VLAN の設定](#)

[スイッチ設定のバックアップ](#)

[スイッチ設定のインポート](#)

[付録](#)



この情報は、Cisco SG350-10とSG350-10PをRavenna/ AES67ネットワークで使用するためにスイッチを設定する方法に関する簡単なガイドで、製品の設定方法全体を説明するものではありません。

重要！

設定を行うには、スイッチを PC の LANポート または MassCore NIC の LANポート に接続します。どちらも IP アドレスを変更する必要があります。作業の前に一般的な LANポート の IP アドレスの変更方法を習得してください。



Dante デバイスを接続する必要がある場合は、追加の設定が必要です。
追加情報の通りに設定を行ってください。



複数の Cisco スイッチを使用する場合は、追加の設定が必要です。
追加情報の通りに設定を行ってください。

スイッチ自動設定用のファイルは2種類用意されています。用途にあったものを予め下記リンクよりダウンロードしておいてください。

- [Cisco SG350-10](#) - 全てのポートがRAVENNA/AES67に最適化されている
- [Cisco SG350-10 - Dual VLAN](#) (Port 1 - 5 : 通常のネットワークとして使用: Port 6 - 10 : RAVENNA/AES67に最適化)
- [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.)

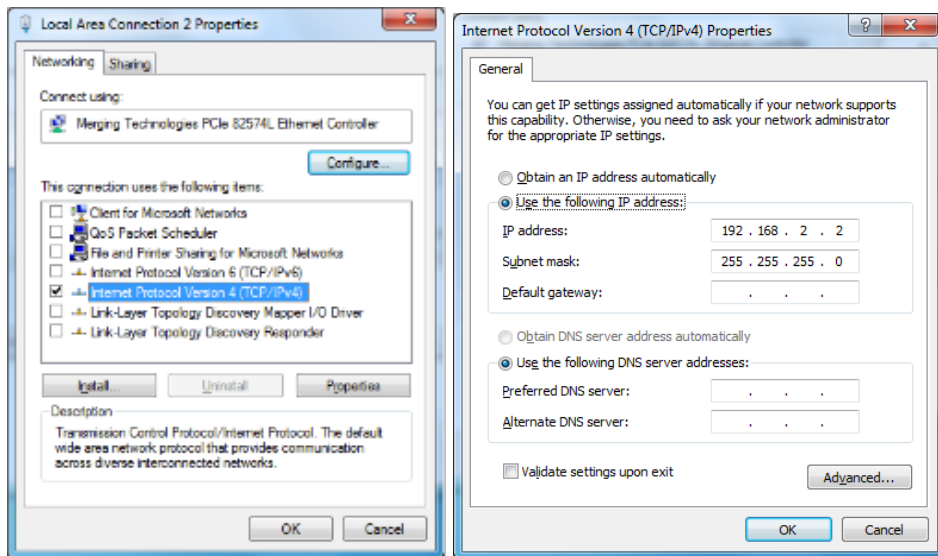
Merging社のネットワークについて

Merging社が推奨するRAVENNA/AES67ネットワークはDHCPで構成されます。従ってこの情報もそれに沿った説明をしています。静的ネットワークを使用されている場合は、PCの設定等を考慮して作業してください。



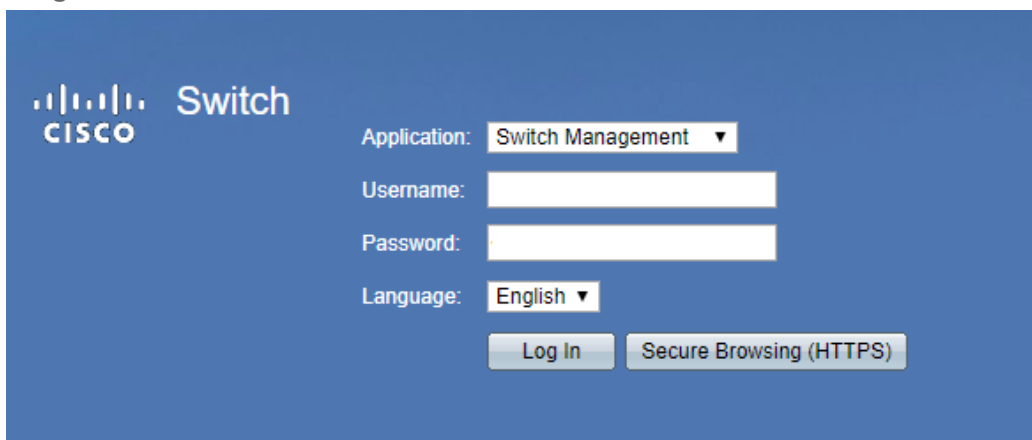
Cisco SG350-10 の自動設定

1. Ciscoスイッチに接続しているPCのコントロールパネル > ネットワーク共有センター を開き、「アダプターの設定の変更」をクリックします。
2. Ciscoスイッチに接続しているPCのLANポートを右クリックして プロパティ を開きます。
3. 「インターネット プロトコル バージョン 4 (TCP/IPv4)」をクリックで選択し、「プロパティ」をクリックします。
4. IPアドレスを **192.168.1.2** に設定します。※以前の設定を記録しておいてください。
5. サブネットを **255.255.255.0** に設定します。※以前の設定を記録しておいてください。
6. OKをクリックしてダイアログを閉じます。



※ Cisco SG350のIPアドレスは、工場出荷時のデフォルトで **192.168.1.254** に設定されています。

7. ブラウザ(Google Chrome)を起動し、アドレスバーに **192.168.1.254** と入力すると、下図のダイアログが表示されます。デフォルトの Username と Password は両方 "cisco" です。これらを入力して **Log In** をクリックします。



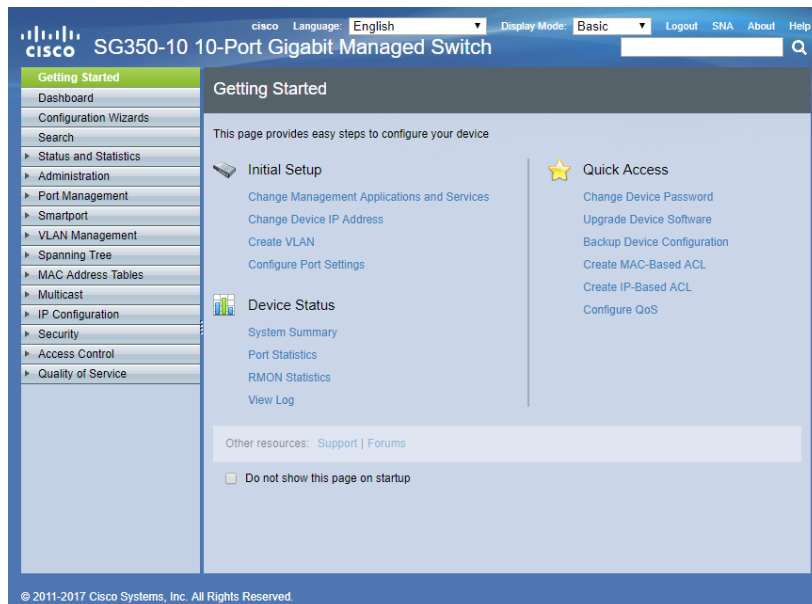


8. Loginするとデフォルトパスワードを変更するように求められます。これは初回ログイン時のみ表示されます。デフォルトを変更した後、再度変更する場合は、Administration ページで変更する必要があります。”factory defaults”にリセットすると、この手順を再度実行するように求められます。

The image shows a web page titled "Change Password". It contains instructions to change the password for better network protection. The minimum requirements are listed: 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 (upper case, lower case, numeric, and special characters). Below this is a "New Password Configuration" section with three input fields for "Old Password:", "New Password:", and "Confirm Password:". There is also a "Password Strength Meter" showing a red bar and the text "Below Minimum", and a "Password Strength Enforcement" checkbox labeled "Disable". An "Apply" button is at the bottom.

※注意:このプログラム後、これらは再度 cosco に戻されます。

9. 右上にある "About" をクリックして、スイッチのファームウェアが 2.3.5.63 以上であることを確認してください。アップデートの必要がある場合は、[Cisco 350, 350X, and 550X Series Managed Switches Administration Guide - Firmware Operations](#)のセクションを参照してアップデートを行ってください。
10. Administration ページにはスイッチの設定ファイルをロードすることができる機能があります。



11. スwitchの用途により、下記リンクより設定ファイルをダウンロードしてください。

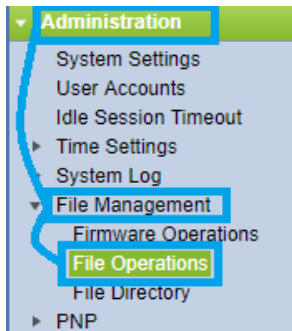
[Cisco SG350-10](#)

[Cisco SG350-10 - Dual VLAN](#) (Port 1 to 5 : 通常のネットワーク: Port 6 to 10 : RAVENNA/AES67)

※注意:これらの設定ファイルで設定を行うと、スイッチはRAVENNA/AES67ネットワークに最適化され、スイッチのアドレスは **169.254.1.254** に設定されます。

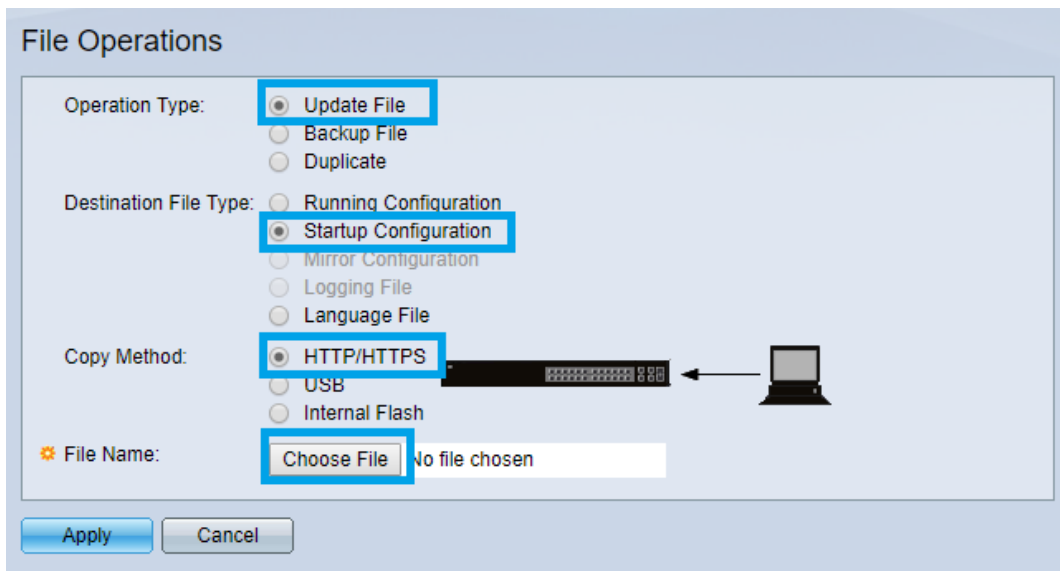


12. “Administration” ページの “File Management” をクリックしてドロップダウンさせると、“File Operations” が表示されますので、クリックします。



13. 次に下記の通りに選択します。

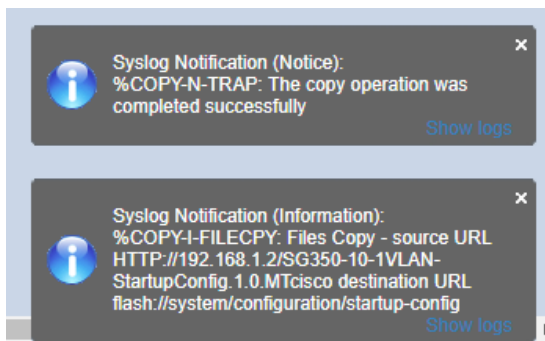
Operation Type : **Update File**
Destination File Type : **Startup Configuration**
Copy Method : **HTTP/HTTPS**



14. “Choose File” をクリックし、エクスプローラで上記9でダウンロードしておいたファイルのディレクトリまで進み、ファイルを選択します。

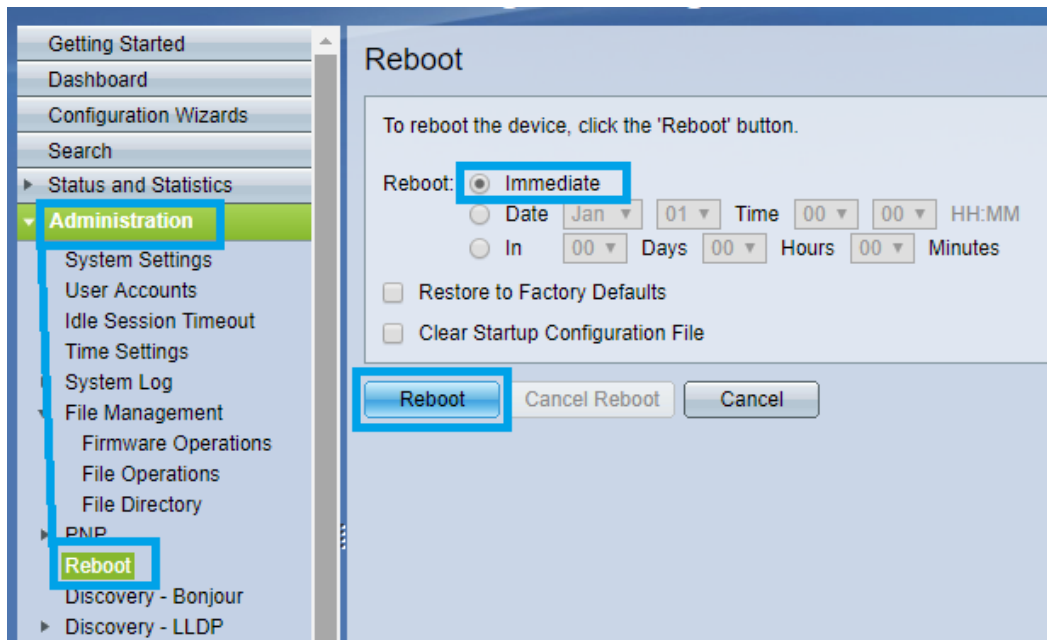
15. “Apply” をクリックすると自動設定が開始されます。

16. 設定が完了すると、次のダイアログが表示されます。





17. 設定を有効するためにはスイッチを再起動させます。“Administration” > “Reboot” をクリックして開き、“Immediate” を選択して “Reboot” ボタンをクリックします。再起動が完了するのに暫く時間がかかります。



18. スイッチが接続されているLANポートのIPアドレスを以前の設定に戻し、MassCore ユーザーはスイッチの接続をMassCore NICのLANポートに接続します。
19. 以上でスイッチの設定は完了しているはずです。ブラウザ(Chrome)でアドレスバーに **169.254.1.254** と入力すると Login 画面が表示されるはずです。



Danteデバイスを接続する場合の追加設定

Mergingファイルで自動設定したCiscoスイッチにDante機器を接続する場合、以下の追加設定が必要となります。

Dante AES67を使用するためには、IPマルチキャストグループを加えます。

前提条件として、CiscoスイッチはMergingファイルにより自動設定され、再起動が終了しているとします。

1. ブラウザ(Google Chrome)のアドレスバーに、**169.254.1.254** と入力して“**Administration**” ページを開きます。
2. “**Advanced**” モードにして“**Administration**” ページを表示させます。
3. “**Multicast**” > “**IP Multicast Group Address**” を開き、“**Add**” をクリックします。
4. “**VLAN ID**” に “1” と入力し、“**IP Multicast Group Address**” に “**224.0.0.230**” と入力して “**Apply**” をクリックします。
5. 同様に、**224.0.0.231**, **224.0.0.232**, **224.0.0.233** を加えてください。
6. ブラウザ上部に赤文字で “save” が点滅しているのでクリックして保存します。
7. 次に、**224.0.0.230 Group** を選択して、“**Details**” をクリックします。Dante機器が接続される(されている)ポートのチェックを “**Static**” に変更して、“**Apply**” をクリックします。
8. 同様の設定を アドレス **224.0.0.231**, **224.0.0.232**, **224.0.0.233** を加えて行ってください。

※ Danteデバイスをポート9と10に接続する場合の例:

VLAN ID: 1
IP Version: Version 4
IP Multicast Group Address: 224.0.0.230
Source IP Address: *

Filter: *Interface Type equals to* Port

Interface	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10
Static	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Dynamic	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Forbidden	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
None	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>



複数のCiscoスイッチを使用する場合の追加設定

複数のCisco SG350/SG300 スイッチを使用して接続を行う場合、マルチキャスト ルーターを設定する必要があります。そうしないと PTP パケットがスイッチを介して送信されず、スイッチごとに1つのマスター PTP が存在するか、デバイスに不要なストリームが殺到し、PTP スレーブがロックできなくなります。

ここで解説している設定方法は、CISCO スイッチのみに適用されます。

※ 注意: この設定にはネットワークに関するスキルが必要です。

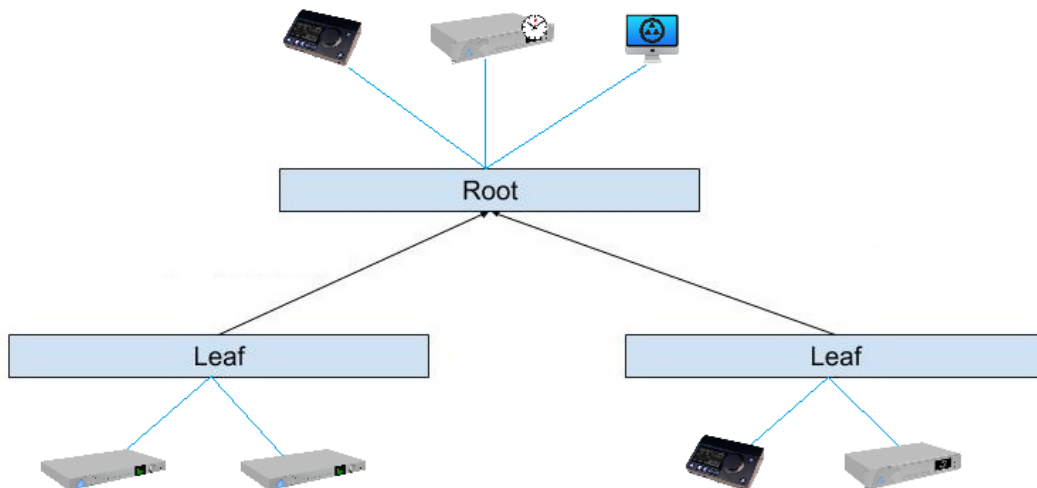
基本的な考え方

ネットワーク内に複数のスイッチが存在する場合、1つの Root スイッチ (Master) と1つ以上の Leaf スイッチ (Slave) として構成されます。

Root スイッチは IGMP クエリアであり、他の Leaf スイッチは入力として取得した全てのストリームを Root に送信します。

そのため Root に至るまでのアップリンクごとに帯域幅が増加するため、コンジェスション (飽和) に注意が必要です。混雑したネットワークでは、10Gb uplink を備えた 10Gb Root スイッチが必要になる場合があります。

PTP Master となるデバイスは Root スイッチに接続して PTP ジッタの増加を防ぐ必要があります。



スイッチの設定

1. スイッチは既に Merging ファイルにより設定が行われているものと仮定します。
2. Leaf スイッチには、Root スイッチに使用した Config ファイルを書き直して使用します。書き直す部分は、IP アドレス部分です。Root スイッチは “169.254.1.254” に設定されますので、この部分を Leaf では “169.254.1.253” に変更してプログラムしてください。

※ 注意: Cisco 350 では、IP をブラウザの設定から変更することはできません。



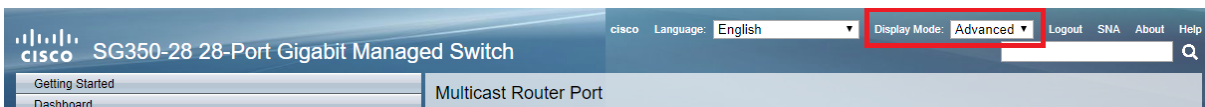
適当なテキスト エディターで SG350-10-1VLAN-StartupConfig.1.0.MTcisco を開くと、#79 行目にIP設定があります。

```
70 qos map dscp queue 00 00 1
71 hostname switchfb453d
72 no passwords complexity enable
73 username cisco password encrypted 7af78c911c
74 ip ssh server
75 snmp-server server
76 ip telnet server
77 !
78 interface vlan 1
79 ip address 169.254.1.253 255.255.0.0
80 no ip address dhcp
81 bridge multicast mode ipv4-group
82 bridge multicast ipv6 mode ip-group
83 !
84 interface GigabitEthernet1
```

SG350-10-2VLAN-StartupConfig.1.0.MTcisco では、#83 行目にIP設定があります。

```
75 no passwords complexity enable
76 username cisco password encrypted 7af78c
77 ip ssh server
78 snmp-server server
79 ip telnet server
80 !
81 interface vlan 2
82 name "RAVENNA AES67"
83 ip address 169.254.1.254 255.255.0.0
84 !
85 interface GigabitEthernet6
86 switchport access vlan 2
87 !
88 interface GigabitEthernet7
89 switchport access vlan 2
```

3. ブラウザでログインします。
4. **Display Mode** を "Advanced" にします (SG350のみ)。





5. “Multicast” > “Properties” を開きます。
”Bridge Multicast Filtering Status”にある“Forwarding Method for IPv6”と“Forwarding Method for IPv4”を両方“IP Group Address”に設定します。

Getting Started
Dashboard
Configuration Wizards
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
 IGMP Snooping
 IGMP Interface Settings
 IGMP VLAN Settings
 IGMP Proxy

Properties

Bridge Multicast Filtering Status: Enable

VLAN ID: 1 ▼

Forwarding Method for IPv6:
 MAC Group Address
 IP Group Address
 Source Specific IP Group Address

Forwarding Method for IPv4:
 MAC Group Address
 IP Group Address
 Source Specific IP Group Address

Apply Cancel

6. “Multicast” > “IPv4 Multicast Configuration” > “IGMP Snooping” を開きます。
※ この設定は Root と Leaf で異なります。

a. Root スイッチ: このスイッチを Master Querier と設定します。

Getting Started
Dashboard
Configuration Wizards
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
 IGMP Snooping
 IGMP Interface Settings
 IGMP VLAN Settings
 IGMP Proxy

IGMP Snooping

IGMP Snooping is only operational when [Bridge Multicast Filtering](#) is enabled.

IGMP Snooping Status: Enable
IGMP Querier Status: Enable

Apply Cancel IGMP Snooping IP Multicast Group

IGMP Snooping Table

Entry No.	VLAN ID	IGMP Snooping Status		MRouter Port Auto Learning
		Administrative	Operational	
1	1	Enabled	Enabled	Enabled

Copy Settings... Edit...



さらに "Edit" をクリックし、以下の設定を行います。

Getting Started
Dashboard
Configuration Wizards
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
 IGMP Snooping
 IGMP Interface Settings
 IGMP VLAN Settings
 IGMP Proxy
▶ IPv6 Multicast Configuration
IGMP/MLD Snooping IP Multic
Multicast Router Port
Forward All
Unregistered Multicast
▶ IP Configuration
▶ Security
▶ Access Control
▶ Quality of Service
▶ SNMP

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

Entry No.	VLAN ID	IGMP Snooping Status		MRouter Ports Auto Learn	Immediate Leave	Last Member Query Counter	IGMP Qu Administ
		Administrative	Operational				
1	1	Enabled	Enabled	Enabled	Enabled	2	En

Edit IGMP Snooping Settings - Google Chrome

Not secure | 172.16.1.250/csaea71193/multicast/igmp_snooping_e_jq.htm

VLAN ID: 1

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



b. **Leaf スイッチ**: このスイッチは Slave ですので、同じステップで異なる設定となります。

The screenshot displays the configuration page for IGMP Snooping. The left sidebar shows a navigation menu with 'Multicast' expanded to 'IGMP Snooping'. The main content area is titled 'IGMP Snooping' and includes a status message: 'IGMP Snooping is only operational when Bridge Multicast Filtering is enabled. Bridge Multicast Filtering is currently enabled.' Below this, the 'IGMP Snooping Status' is set to 'Enable' (checked), and the 'IGMP Querier Status' is set to 'Disable' (unchecked), with the latter highlighted by a red box. There are 'Apply' and 'Cancel' buttons, and a link for 'IGMP Snooping IP Multicast Group'. A table titled 'IGMP Snooping Table' shows one entry for VLAN 1 with various status indicators. Below the table are 'Copy Settings...' and 'Edit...' buttons. A modal window titled 'Edit IGMP Snooping Settings - Google Chrome' is open, showing detailed settings for VLAN 1, also highlighted with a red box. The settings include: VLAN ID: 1; IGMP Snooping Status: Enable (checked); MRouter Ports Auto Learn: Disable (unchecked); Immediate Leave: Disable (unchecked); Last Member Query Counter: Use Query Robustness (2) (selected); IGMP Querier Status: Disable (unchecked); IGMP Querier Election: Disable (unchecked); IGMP Querier Version: v2 (selected); Querier Source IP Address: Auto (selected).

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



7. "Multicast" > "IPv4 Multicast Configuration" > "IGMP VLAN Settings" を開き、VLAN を選択して "Edit" をクリックします。

Entry No.	Interface Name	Router	Query IGMP Version	Query Robustness	Query Interval (sec)
	VLAN1	v2		2	30

8. "Query Interval" の値を "30" (秒) に設定し、"Apply" をクリックします。

Interface Name: VLAN 1

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)

Apply Close

9. "Multicast" > "IPv4 Multicast Configuration" > "IGMP Proxy" を開き、Enable のチェックを全て外し、"Apply" をクリックします。

Getting Started

Dashboard

Configuration Wizards

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

IGMP Snooping

IGMP Interface Settings

IGMP VLAN Settings

IGMP Proxy

IPv6 Multicast Configuration

IGMP/MLD Snooping IP Multic

IGMP Proxy

IGMP Proxy is only operational if IPv4 routing is enabled. IPv4 routing is

Global IGMP Proxy Settings

IGMP Multicast Routing: Enable

Downstream Protection: Enable

Source Specific Multicast: Enable

SSM IPv4 Access List: Default list
 User defined access list

Apply Cancel

IGMP Proxy Table

<input type="checkbox"/>	Upstream Interface	Downstream Interface	Downstream Pro
0 results found.			

Add... Delete

IPv4 MRoute Table

Source Address	Group Address	Incoming Interface	Outgoing I
0 results found.			



10. “Multicast” > “Multicast Router Port” を開きます。

a. Root スイッチ 側:

各インターフェースを “**Forbidden**” に設定し、“Apply” をクリックします。

Getting Started
Dashboard
Configuration Wizards
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
IGMP Snooping
IGMP Interface Settings
IGMP VLAN Settings
IGMP Proxy
IPv6 Multicast Configuration
IGMP/MLD Snooping IP Multic
Multicast Router Port
Forward All
Unregistered Multicast

Multicast Router Port

Filter: VLAN ID equals to 1 AND IP Version equals to Version 4 AND Interface Type equals to Port Go

Port	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10	GE11	GE12	GE13	GE14	GE15	GE16	GE17	GE18	GE19	GE20	GE21	GE22	GE23	GE24
Static	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Dynamic	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Forbidden	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
None	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Port GE25 GE26 GE27 GE28

Static	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Dynamic	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Forbidden	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
None	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Apply Cancel

b. Leaf スイッチ 側:

各インターフェースを “**Forbidden**” に設定し、次に Root スイッチ へのリンクに使用するポートのみを “**STATIC**” に設定して、“Apply” をクリックします。

Getting Started
Dashboard
Configuration Wizards
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
IGMP Snooping
IGMP Interface Settings
IGMP VLAN Settings
IGMP Proxy
IPv6 Multicast Configuration
IGMP/MLD Snooping IP Multic
Multicast Router Port
Forward All
Unregistered Multicast

Multicast Router Port

Filter: VLAN ID equals to 1 AND IP Version equals to Version 4 AND Interface Type equals to Port Go

Port	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10	GE11	GE12	GE13	GE14	GE15	GE16	GE17	GE18	GE19	GE20	GE21	GE22	GE23	GE24
Static	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Dynamic	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Forbidden	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
None	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

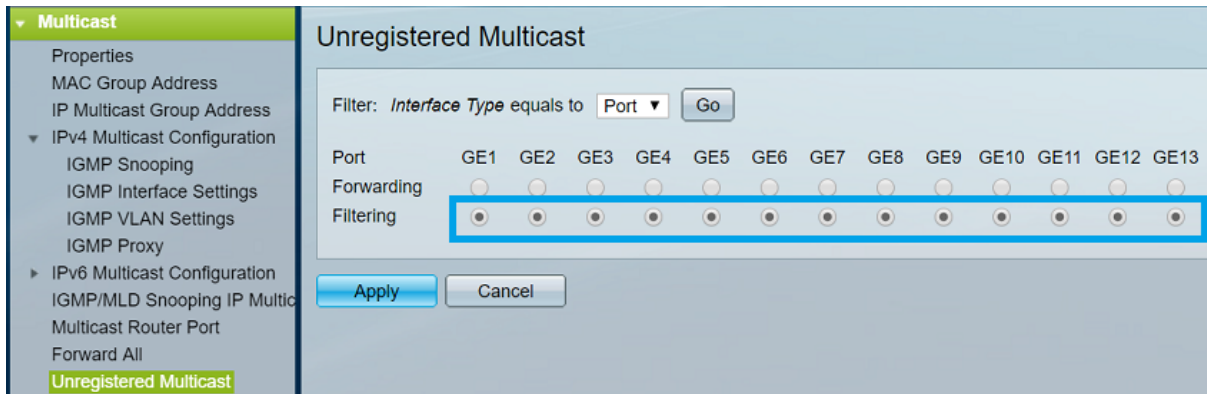
Port GE25 GE26 GE27 GE28

Static	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Dynamic	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Forbidden	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
None	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Apply Cancel



11. “Multicast” > “Unregistered Multicast” を開きます。
全てのポートを “Filtering” に設定し、“Apply” をクリックします。



Dante AES67 デバイスを使用する場合は、IP Multicast Groups を加える必要があります。

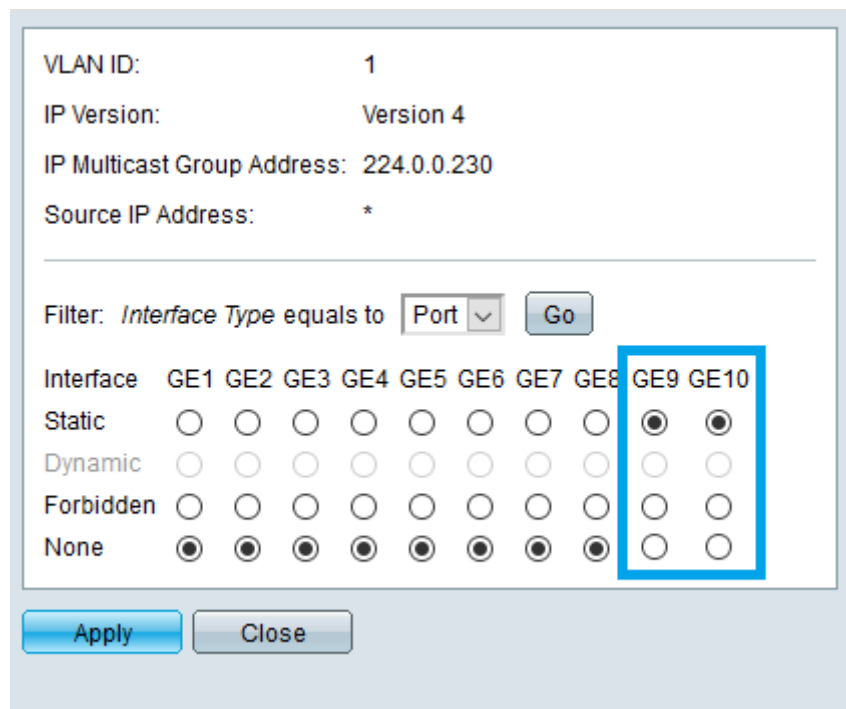
“Multicast” > “Unregistered Multicast” を開き、“Add” をクリックします。

“VLAN ID 1”に入り、“IP Multicast Group Address” に “224.0.0.230” と入力して “Apply” をクリックします。

次に、**224.0.0.230 Group** を選択して、“Details” をクリックします。Dante機器が接続される(されている)ポートのチェックを “Static” に変更して、“Apply” をクリックします。

同様の設定を アドレス **224.0.0.231**, **224.0.0.232**, **224.0.0.233** に行います。

※ Danteデバイスをポート9と10に接続した例：



注意: Dante 機器の設定をハブ経由で行う場合、設定するPCは必ずDanteポートに接続してください。



12. 各スイッチは、独自のアドレスを保つ必要があります。

“Administration” > “Management Interface” > “IPv4 Interface” を開き、IP Address フィールドを変更して、“Apply” をクリックします。

Getting Started
▶ Status and Statistics
▼ Administration
System Settings
Console Settings
▼ Management Interface
IPv4 Interface
IPv6 Global Configuration
IPv6 Interfaces
IPv6 Addresses
IPv6 Default Router List
IPv6 Tunnel

IPv4 Interface

Management VLAN: 1

IP Address Type: Dynamic Static

IP Address: 169.254.1.254

Mask: Network Mask 255.255.0.0 Prefix Length (Range: 8 - 30)

13. “Service” > “General” > “DSCP to Queue” を開きます。

スイッチのモデルにより次の様に設定し、“Apply” をクリックします。

Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue
0 (BE)	1	16 (CS2)	1	32 (CS4)	1	48 (CS6)	4
1	1	17	1	33	1	49	1
2	1	18 (AF21)	1	34 (AF41)	2	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)	4
9	1	25	1	41	1	57	1
10 (AF11)	1	26 (AF31)	1	42	1	58	1
11	1	27	1	43	1	59	1
12 (AF12)	1	28 (AF32)	1	44	1	60	1
13	1	29	1	45	1	61	1
14 (AF13)	1	30 (AF33)	1	46 (EF)	3	62	1
15	1	31	1	47	1	63	1

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

14. 設定を保存します:

“Administration” > “File Management” > “File Operations” を開きます。

Operation Type を “Duplicate”

Source File Name を “Running Configuration”

Destination File Name を “Startup Configuration”

に設定して “Apply” をクリックします。

Administration
System Settings
User Accounts
Idle Session Timeout
▶ Time Settings
▶ System Log
▼ File Management
Firmware Operations
File Operations
File Directory
▶ PNP
Reboot
Discovery - Bonjour

File Operations

Operation Type: Update File Backup File Duplicate

Source File Name: Running Configuration Startup Configuration Mirror Configuration

Destination File Name: Running Configuration Startup Configuration

Apply Cancel



設定を反映させるためにはスイッチを再起動させる必要があります。

”Administration” > ”Reboot” を開き、”Immediate” を選択して ”Reboot” ボタンをクリックしてください。
再起動には時間がかかります。

The screenshot shows a web interface for configuring a device's reboot settings. On the left is a navigation menu with the following items: Getting Started, Dashboard, Configuration Wizards, Search, Status and Statistics, Administration (highlighted in green), System Settings, User Accounts, Idle Session Timeout, Time Settings, System Log, File Management, Firmware Operations, File Operations, File Directory, PNP, Reboot (highlighted in green), Discovery - Bonjour, and Discovery - LLDP. The main content area is titled "Reboot" and contains the following elements: a heading "Reboot", a sub-heading "To reboot the device, click the 'Reboot' button.", a "Reboot:" label followed by three radio button options: "Immediate" (selected and highlighted with a blue box), "Date" (with dropdowns for "Jan" and "01"), and "In" (with dropdowns for "00" Days, "00" Hours, and "00" Minutes). Below these are two unchecked checkboxes: "Restore to Factory Defaults" and "Clear Startup Configuration File". At the bottom are three buttons: "Reboot" (highlighted with a blue box), "Cancel Reboot", and "Cancel".



Cisco SG350 スイッチのマニュアル設定

この情報は、Cisco SG350 をマニュアルで設定する場合の解説です。つまり、Mergingファイルで設定された項目の解説と同義です。

Single VLAN の設定

最初のステップは、APIPA(自動プライベートインターネットプロトコルアドレッシング)タイプのIPを使用するようにIP設定を変更します。

Administration ページは、この新しいIPからのみアクセスできます。

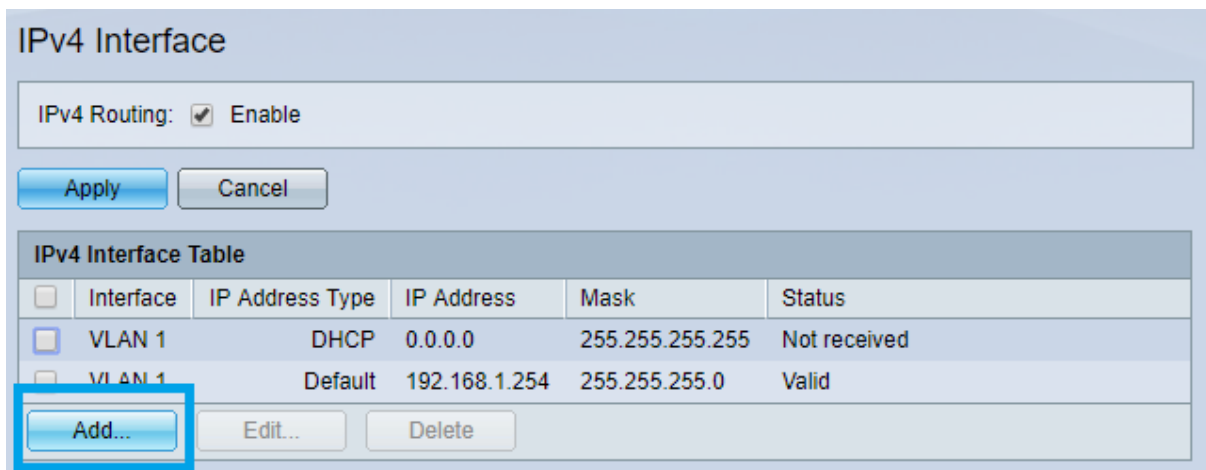
これをAPIPA IPレンジ(169.254.0.0/16)に入れると、常に Administration ページにアクセスできるようになります。

Ravennaデバイスは通常、APIPA IPレンジを使用してネットワーク経由で通信します。

1. “Getting Started” ページで、“Change Device IP Adress” をクリックします。



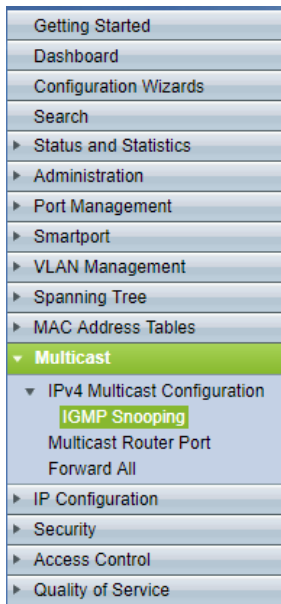
2. IPv4 Interface テーブルの下部にある “Add” ボタンをクリックします。



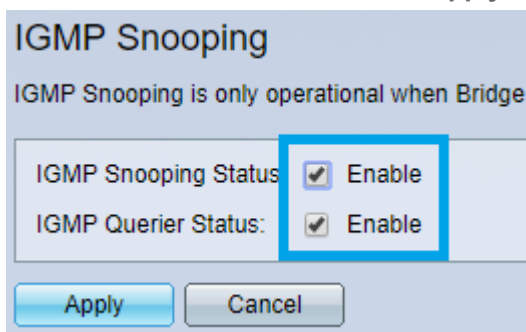
3. “IP Address type” を “Static IP Address” に設定します。
IP Address フィールドに **169.254.1.254** を入力します。
Mask には Prefix Length に **16** を入力します。これは “255.255.255.0” と同義になります。
4. “Apply” をクリックして変更を保存します。
5. スイッチは 192.168.1.254 でアクセスできなくなりますのでご注意ください。
6. スイッチは [HTTP://169.254.1.254](http://169.254.1.254) でアクセスできます。



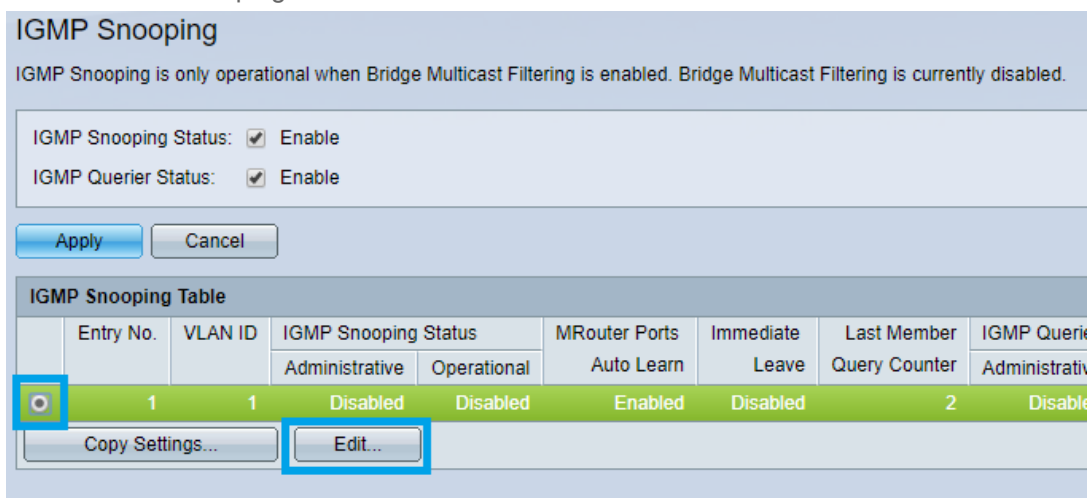
7. ブラウザ(Google Chrome)でアドレスバーに 169.254.1.254 と入力します。
8. 左の欄の **MULTICAST** をクリックします。
IPv4 Multicast Configuration をクリックして広げます。
IGMP SNOOPING をクリックします。



9. IGMP Snooping のページでは、**IGMP Snooping Status** と **IGMP Querier Status** のチェックボックスにチェックを入れ、**Enable** にして **Apply** をクリックします。



10. IGMP Snooping Table では、まずラジオボタンで選択して **Edit** をクリックします。





11. IGMP Snooping Settings 内を下図の通り設定し、“Apply” をクリックします。

VLAN ID: 1

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

12. スイッチはデフォルトで グリーンイーサネット仕様となっているため、これを無効に設定します。
”Port Management” > ”Green Ethernet” > ”Properties” を開き、”Energy Detect Mode”と”Short Reach”, ”802.3 Energy Efficient Ethernet (IEEE)” のチェックを外して ”Apply” をクリックします。

Getting Started

Dashboard

Configuration Wizards

Search

Status and Statistics

Administration

Port Management

Port Settings

Error Recovery Settings

Link Aggregation

Green Ethernet

Properties

Port Settings

Properties

For the functions and/or parameters configured on this page to become effective, you may have to configure the corresponding port based parameters on [Port Settings](#) page.

Energy Detect Mode: Enable

Short Reach: Enable

Port LEDs: Enable

802.3 Energy Efficient Ethernet (EEE): Enable

Apply Cancel Reset Energy Saving Counter

13. “Quality of Service” > “General” > “QoS Properties” を開きます。
QoS Mode を “Basic” に設定し、“Apply” をクリックします。

Access Control

Quality of Service

General

QoS Properties

Queue

CoS/802.1p to Queue

DSCP to Queue

QoS Basic Mode

QoS Statistics

QoS Properties

QoS Mode: Disable
 Basic
 Advanced *

An * indicates an advanced feature. Activate advanced display mode to fully configure this feature.

Apply Cancel



14. “Quality of Service” > “QoS Basic Mode” > “Global settings” を開きます。
Trust Mode を “DSCP” に設定し、“Apply” をクリックします。

The screenshot shows the 'Global Settings' configuration page. In the left-hand navigation menu, 'Quality of Service' is expanded to show 'QoS Basic Mode', which is further expanded to 'Global Settings'. The main content area shows 'Trust Mode' with three radio button options: 'CoS/802.1p', 'DSCP' (which is selected and highlighted with a blue box), and 'CoS/802.1p-DSCP'. Below this, 'Override Ingress DSCP' is set to 'Enable' with an unchecked checkbox. At the bottom, there are three buttons: 'DSCP Override Table', 'Apply' (highlighted with a blue box), and 'Cancel'.

15. “Quality of Service” > “General” に戻り、“DSCP to Queue” を開きます。
”DSCP to Queue” の設定を下図のように設定し、“Apply” をクリックします。

The screenshot shows the 'DSCP to Queue' configuration page. The left-hand navigation menu shows 'Quality of Service' expanded to 'General', which is further expanded to 'DSCP to Queue'. The main content area features a table titled 'DSCP to Queue Table' with 8 columns: 'Ingress DSCP', 'Output Queue', 'Ingress DSCP', 'Output Queue', 'Ingress DSCP', 'Output Queue', 'Ingress DSCP', and 'Output Queue'. The table contains 16 rows of mappings. Below the table are three buttons: 'Apply' (highlighted with a blue box), 'Cancel', and 'Restore Defaults'. A note at the bottom states: 'Queue 1 has the lowest priority, queue 8 has the highest priority.'

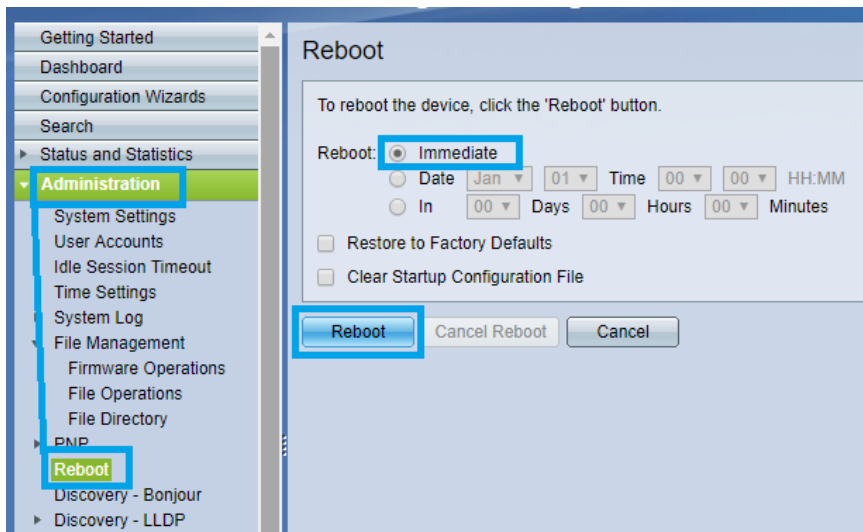
Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue
0 (BE)	2	16 (CS2)	1	32 (CS4)	1	48 (CS6)	8
1	1	17	1	33	1	49	1
2	1	18 (AF21)	1	34 (AF41)	6	50	1
3	1	19	1	35	1	51	1
4	1	20 (AF22)	1	36 (AF42)	1	52	1
5	1	21	1	37	1	53	1
6	1	22 (AF23)	1	38 (AF43)	1	54	1
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

16. ここで設定を保存します。
”Administration” > “File Management” > “File Operations” を開きます。
Operation Type を “Duplicate”
Source File Name を “Running Configuration”
Destination File Name を “Startup Configuration”
に設定して”Apply” をクリックします。

The screenshot shows the 'File Operations' configuration page. The left-hand navigation menu shows 'Administration' expanded to 'File Management', which is further expanded to 'File Operations'. The main content area shows 'Operation Type' with three radio button options: 'Update File', 'Backup File', and 'Duplicate' (which is selected and highlighted with a blue box). Below this, 'Source File Name' has three radio button options: 'Running Configuration' (selected and highlighted with a blue box), 'Startup Configuration', and 'Mirror Configuration'. 'Destination File Name' has two radio button options: 'Running Configuration' and 'Startup Configuration' (selected and highlighted with a blue box). At the bottom, there are two buttons: 'Apply' (highlighted with a blue box) and 'Cancel'.



17. 設定を反映させるためにはスイッチを再起動させる必要があります。
”Administration” > “Reboot” を開き、”Immediate” を選択して “Reboot” ボタンをクリックしてください。
再起動には時間がかかります。





Dual VLAN の設定

この章では1つのSG350で2系統のVLANを使用する場合の設定例を紹介します。

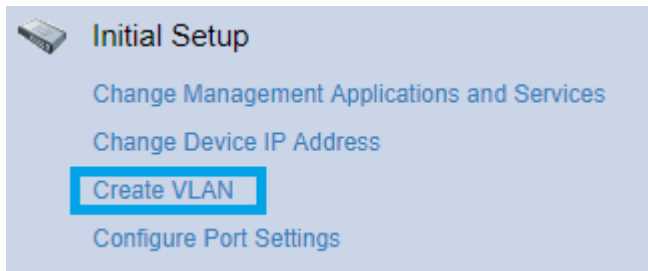
「2系統のVLAN」とは、

- VLAN1:一般的なPCのネットワーク
- VLAN2:Ravenna AES67

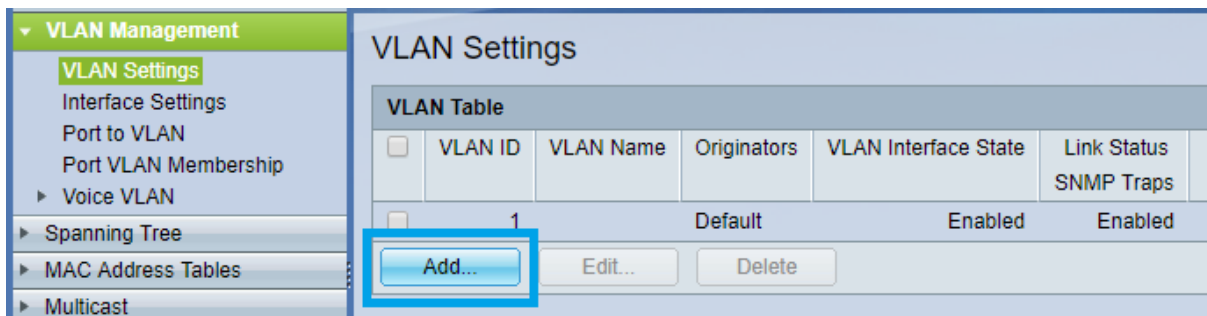
を指します。

スイッチは、デフォルトで一般的なPCで利用するVLAN1が作成されています。そのためRavenna AES67に使用するVLAN2を加える方法について解説します。

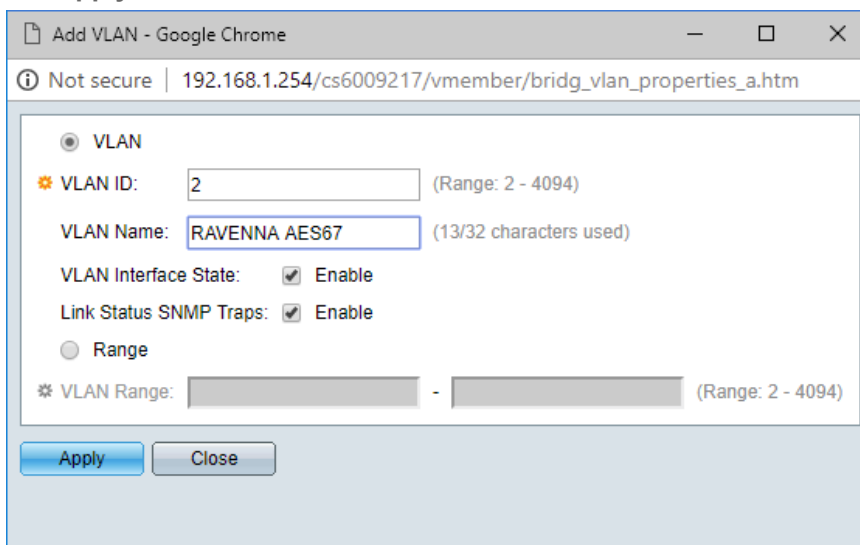
1. “Getting Started” ページで “Create VLAN” をクリックします。



2. VLANテーブルの下部にある “Add” ボタンをクリックします。



3. “VLAN ID” に “2” を入力し、“VLAN NAME” に適当な名前を入力します。“VLAN Interface Status” と “Link Status SNMP Traps” の Enable にチェックが入っていることを確認して、“Apply” をクリックしてください。





4. “VLAN Management” > “PORT TO VLAN” を開きます。
”Filter” セクションで “2” を選択し、”Interface Type” を “Port” に選択して、”Go” をクリックします。

Interface Name	VLAN Mode	Membership Type	PVID
GE1	Access	Untagged	<input checked="" type="checkbox"/>
GE2	Access	Untagged	<input checked="" type="checkbox"/>
GE3	Access	Untagged	<input checked="" type="checkbox"/>
GE4	Access	Untagged	<input checked="" type="checkbox"/>
GE5	Access	Untagged	<input checked="" type="checkbox"/>
GE6	Access	Untagged	<input checked="" type="checkbox"/>
GE7	Access	Untagged	<input checked="" type="checkbox"/>
GE8	Access	Untagged	<input checked="" type="checkbox"/>
GE9	Access	Untagged	<input checked="" type="checkbox"/>
GE10	Access	Untagged	<input checked="" type="checkbox"/>

5. VLAN 2 はスイッチのすべてのLANポートで除外(Exclude)されていることがわかります。VLAN2に割り当てたいLANポートをこの RAVENNA / AES67 VLAN に割り当てます。
VLAN2に割り当てたいLANポートを ”Exclude” から “Untagged” に変更します(下の例では、ポート 5~8 および ポート10をVLAN 2に割り当てています)。
完了したら ”Apply” をクリックします。

Interface Name	VLAN Mode	Membership Type	PVID
GE1	Access	Excluded	<input type="checkbox"/>
GE2	Access	Excluded	<input type="checkbox"/>
GE3	Access	Excluded	<input type="checkbox"/>
GE4	Access	Excluded	<input type="checkbox"/>
GE5	Access	Untagged	<input checked="" type="checkbox"/>
GE6	Access	Untagged	<input checked="" type="checkbox"/>
GE7	Access	Untagged	<input checked="" type="checkbox"/>
GE8	Access	Untagged	<input checked="" type="checkbox"/>
GE9	Access	Excluded	<input type="checkbox"/>
GE10	Access	Untagged	<input checked="" type="checkbox"/>

6. VLAN1側をチェックしてみましょう。



”Filter” セクションで “1” を選択し、”Interface Type” を “Port” に選択して、”Go” をクリックします。
VLAN2に加えた LANポート がVLAN1では ”Excluded” になっていることが確認できます。

Interface Name	VLAN Mode	Membership Type	PVID
GE1	Access	Untagged	<input checked="" type="checkbox"/>
GE2	Access	Untagged	<input checked="" type="checkbox"/>
GE3	Access	Untagged	<input checked="" type="checkbox"/>
GE4	Access	Untagged	<input checked="" type="checkbox"/>
GE5	Access	Excluded	<input type="checkbox"/>
GE6	Access	Excluded	<input type="checkbox"/>
GE7	Access	Excluded	<input type="checkbox"/>
GE8	Access	Excluded	<input type="checkbox"/>
GE9	Access	Untagged	<input checked="" type="checkbox"/>
GE10	Access	Excluded	<input type="checkbox"/>

7. “Getting Started” ページで “Change Device IP Address” をクリックします。

8. IPv4テーブルの下部にある “Add” ボタンをクリックします。
”VLAN” を “2” にすることを忘れないでください。
”IP Address Type” を “Static IP Address” に設定し、
”IP Address” フィールドに “169.254.1.254” を入力します。
”Mask” の “Prefix Length” に “16” と入力します。

Interface: Port GE1 LAG 1 VLAN 2

IP Address Type: Dynamic IP Address Static IP Address

IP Address: 169.254.1.254

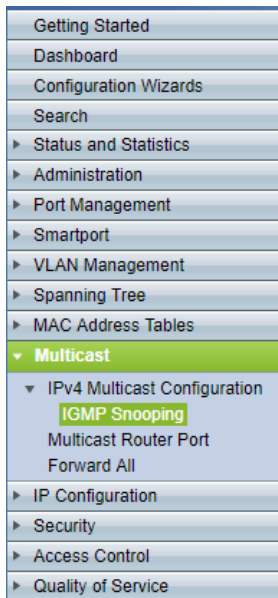
Mask: Network Mask Prefix Length 16 (Range: 8 - 30)

これにより、スイッチの Administration ページがそのIPアドレスで応答するようになります。

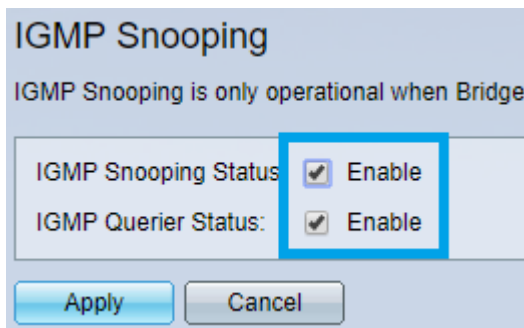


ネットワークマスクの代わりにプレフィックス長を使用したことに注意してください(“16”は“255.255.0.0”と同じです)。“255.255.0.0”で設定することもできます。

9. 完了したら **”Apply”** をクリックします。
10. スイッチはIPアドレスが変更されるため、現在使用している 192.168.1.254 では応答しくなくなります。
11. スイッチはHTTP://169.254.1.254でのみアクセス可能になりました。
おそらく、PC側のIPアドレスを「IPアドレスを自動的に取得する(DHCP)」に変更する必要があります。
この例では、VLAN2に割り当てられているポート(この例ではポート6)に物理的に接続されていることを確認してください。
注: VLAN1からも両方のVLANの管理インターフェイスにアクセスできます。ただし、別のIPアドレス(たとえば、192.168.1.254)を使用する必要があります。
12. ブラウザ(Google Chrome)のアドレスバーに **“169.254.1.254”** と入力します。
13. 左の欄のメニューから **“MULTICAST”** をクリックします。
14. **“IPv4 Multicast Configuration”** をクリックして広げ、**”IGMP SNOOPING”** をクリックします。



15. **”IGMP Snooping Status”** と **”IGMP Querier Status”** のチェックボックスにチェックを入れ、**”Apply”** をクリックします。



16. **”IGMP Snooping Table”** にある **“VLAN2”** のラジオボタンをクリックし、**”Edit”** をクリックします。



IGMP Snooping

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

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		IGM Elec
		Administrative	Operational				Administrative	Operational	
<input type="radio"/>	1	1	Disabled	Disabled	Enabled	Disabled	2	Disabled	Disabled
<input checked="" type="radio"/>	2	2	Disabled	Disabled	Enabled	Disabled	2	Disabled	Disabled

17. IGMP Snooping Settings を下図のように設定し、“Apply” をクリックします。

Edit IGMP Snooping Settings - Google Chrome

169.254.1.254/cs6009217/multicast/igmp_snooping_e_jq.htm

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



18. スイッチはデフォルトでグリーンイーサネット仕様となっているため、これを無効に設定します。
”Port Management” > ”Green Ethernet” > ”Properties” を開き、”Energy Detect Mode”と”Short Reach”, ”802.3 Energy Efficient Ethernet (IEEE)” のチェックを外して ”Apply” をクリックします。

Getting Started
Dashboard
Configuration Wizards
Search
▶ Status and Statistics
▶ Administration
▼ Port Management
 Port Settings
 Error Recovery Settings
 ▶ Link Aggregation
 ▼ Green Ethernet
 Properties
 Port Settings

Properties

For the functions and/or parameters configured on this page to become effective, you may have to configure the corresponding port based parameters on [Port Settings](#) page.

Energy Detect Mode: Enable

Short Reach: Enable

Port LEDs: Enable

802.3 Energy Efficient Ethernet (EEE): Enable

Apply Cancel Reset Energy Saving Counter

19. ”Quality of Service” > ”General” > ”QoS Properties” を開きます。
QoS Mode を ”Basic” に設定し、”Apply” をクリックします。

▶ Access Control
▼ Quality of Service
 General
 QoS Properties
 Queue
 CoS/802.1p to Queue
 DSCP to Queue
 ▶ QoS Basic Mode
 ▶ QoS Statistics

QoS Properties

QoS Mode: Disable Basic Advanced *

An * indicates an advanced feature. Activate advanced display mode to fully configure this feature.

Apply Cancel

20. ”Quality of Service” > ”QoS Basic Mode” > ”Global settings” を開きます。
Trust Mode を ”DSCP” に設定し、”Apply” をクリックします。

▶ Access Control
▼ Quality of Service
 General
 ▼ QoS Basic Mode
 Global Settings
 Interface Settings
 ▶ QoS Statistics

Global Settings

Trust Mode: CoS/802.1p DSCP CoS/802.1p-DSCP

Override Ingress DSCP: Enable

DSCP Override Table Apply Cancel



21. “Quality of Service” > “General” に戻り、“DSCP to Queue” を開きます。
“DSCP to Queue” の設定を下図のように設定し、“Apply” をクリックします。

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

Apply Cancel Restore Defaults

Queue 1 has the lowest priority, queue 8 has the highest priority.

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

22. 設定を保存します。
“Administration” > “File Management” > “File Operations” を開きます。
- Operation Type を “Duplicate”
 - Source File Name を “Running Configuration”
 - Destination File Name を “Startup Configuration”
- に設定して“Apply” をクリックします。

File Operations

Operation Type: Update File
 Backup File
 Duplicate

Source File Name: Running Configuration
 Startup Configuration
 Mirror Configuration

Destination File Name: Running Configuration
 Startup Configuration

Apply Cancel

23. 設定を反映させるためにはスイッチを再起動させる必要があります。
“Administration” > “Reboot” を開き、“Immediate” を選択して “Reboot” ボタンをクリックしてください。
再起動には時間がかかります。



Getting Started
Dashboard
Configuration Wizards
Search
▶ Status and Statistics
▼ Administration
System Settings
User Accounts
Idle Session Timeout
Time Settings
System Log
File Management
Firmware Operations
File Operations
File Directory
▶ PNP
Reboot
Discovery - Bonjour
▶ Discovery - LLDP

Reboot

To reboot the device, click the 'Reboot' button.

Reboot: Immediate
 Date Jan 01 Time 00:00 HH:MM
 In 00 Days 00 Hours 00 Minutes

Restore to Factory Defaults
 Clear Startup Configuration File

Reboot Cancel Reboot Cancel

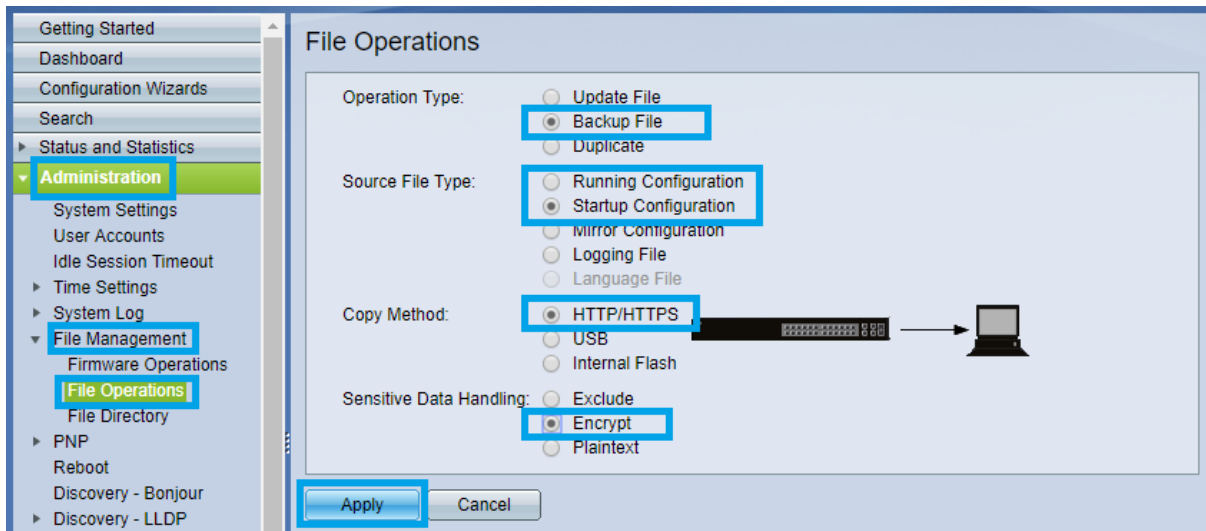
Mergingの設定ファイルをプログラムすると、以降、設定ページにアクセスするアドレス, User Name, Password が変更されます。

アドレス: 169.254.1.254
User Name: MergingCisco
Password: Merging2020



スイッチ設定のバックアップ

1. “Administration” の “File Management” をクリックして広げ、“File Operations” をクリックします。
2. Operation Type を “Backup File”
Source File Type を “Running” または “Startup Configuration”
Copy Method を “HTTP/HTTPS”
Sensitive Data Handling を “Encrypt”
に設定します。



3. “Apply” をクリックすると、設定ファイルがブラウザにテキストファイル(.txt)としてダウンロードされます。

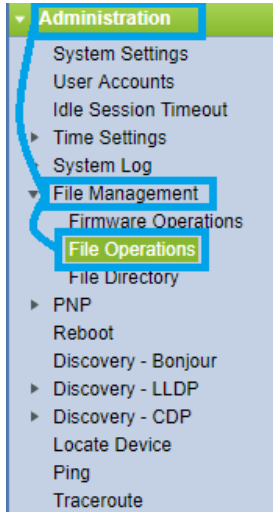


スイッチ設定のインポート

重要:

スイッチの設定ファイルを *Destination File Type* を “Running Configuration” としてインポートしようすると失敗します。必ず “Startup Configuration” としてインポートし、スイッチを再起動させてください。

1. “Administration” の “File Management” をクリックして広げ、“File Operations” をクリックします。



2. 次に以下に設定します。

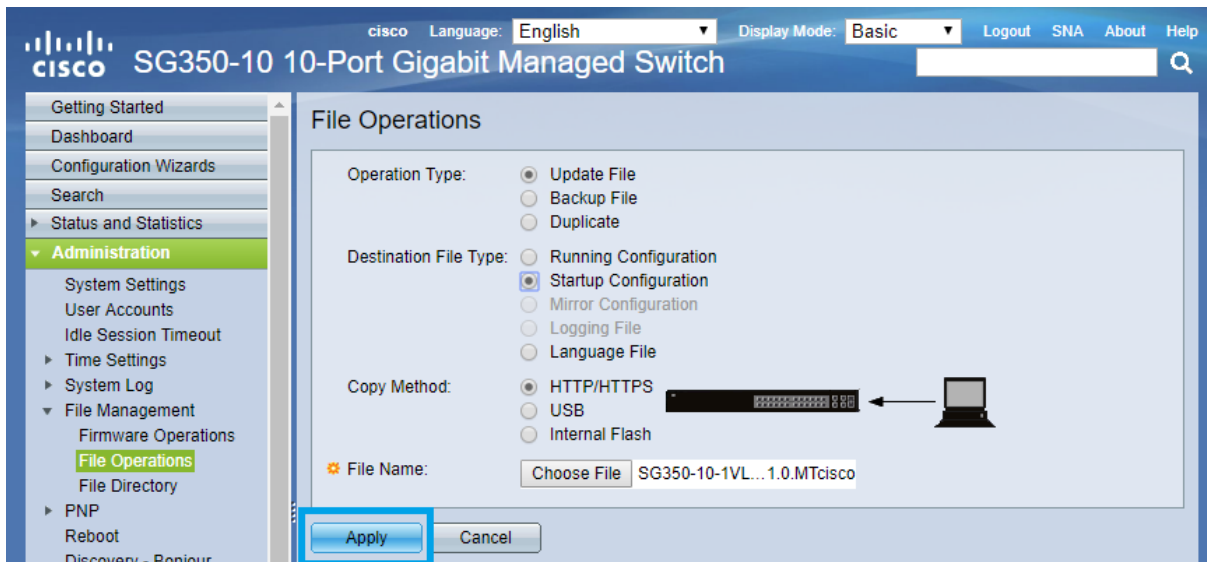
Operation Type : **Update File**

Destination File Type : **Startup Configuration**

Copy Method : **HTTP/HTTPS**

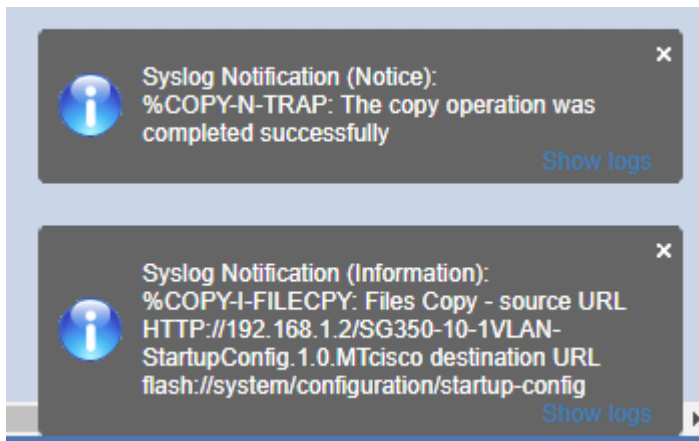
“Choose File” をクリックし、ファイルを選択したら “Open” をクリックします。

”Apply” をクリックして起動設定ファイルとしてロードします。

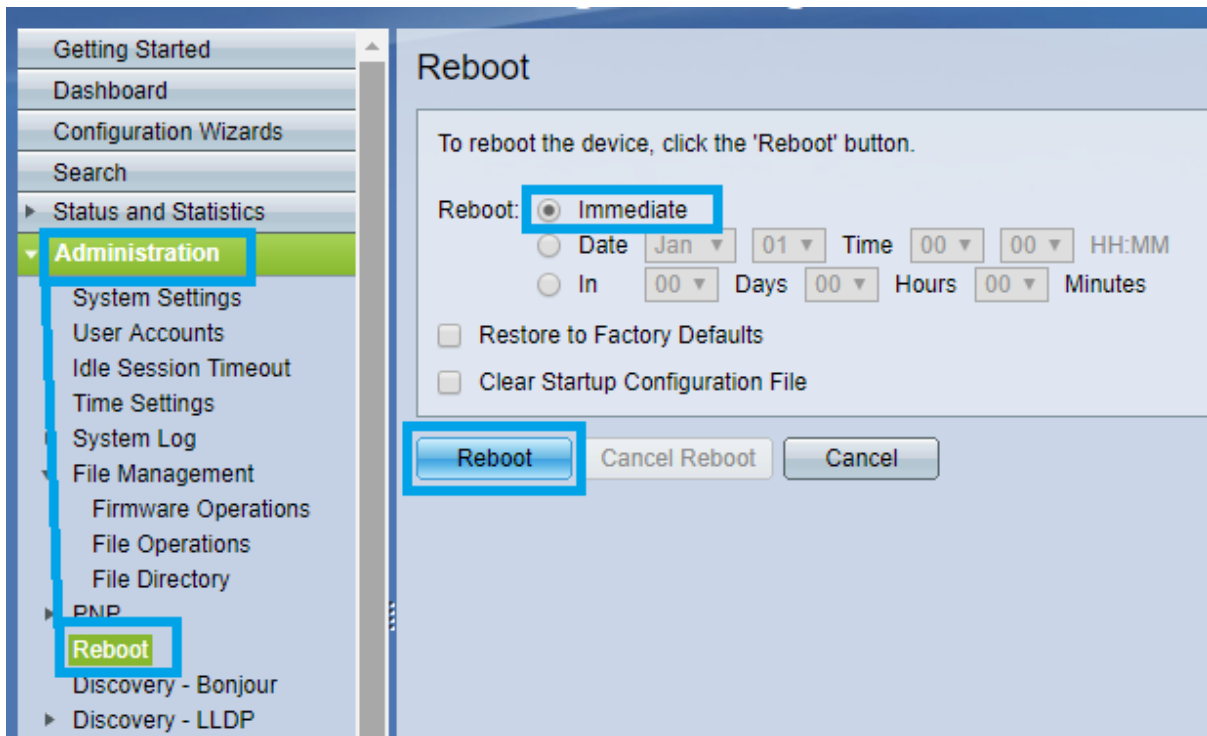




- ロードが完了すると下図のダイアログが表示されます。



- 設定の変更を有効にするには再起動が必要です。
Administration > Reboot で ”Immediate” を選択して “Reboot” をクリックします。
再起動が完了するには時間がかかります。





付録

DSCP (DiffServ Code Point)

Queue 34 : RTP AES67

Queue 46 : PTP AES67 / RTP Ravenna

Queue 48 : PTP Ravenna

Queue 56 : PTP Dante

DSCP to Queue

DSCP to Queue Table							
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 ▼

Apply Cancel Restore Defaults

Queue 1 has the lowest priority, queue 8 has the highest priority.