



---

## **Cisco CBS350 Managed switch manual configuration**

<b>Cisco CBS350 Managed switch manual configuration</b>	<b>1</b>
<b>CBS350スイッチの Administration ページにアクセスする</b>	<b>2</b>
<b>Single VLAN Configuration</b>	<b>5</b>
<b>Dual VLAN Configuration</b>	<b>12</b>
<b>Dante AES67 Additional configuration</b>	<b>21</b>
<b>設定のバックアップとインポート</b>	<b>22</b>
設定をファイルにしてバックアップする	22
設定ファイルのインポート	23



この情報は、Ravenna/AES67ネットワークで Cisco CBS350 を使用するための設定方法を簡単に説明しています。

複数のCiscoスイッチを接続する場合は、追加の設定が必要です。  
複数のネットワークスイッチの考慮事項のページと [Cisco SG300/350 複数のスイッチの構成ガイド](#)を参照してください。

#### **DANTE-AES67** 機器に関する重要な注意事項

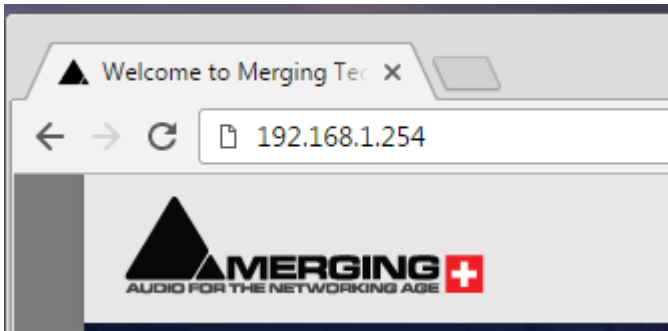
DanteデバイスをMerging 方式の設定でCiscoスイッチに接続する場合、追加の設定が必要です。  
スイッチの設定後、以降の手順に従ってください。

### CBS350スイッチの Administration ページにアクセスする

#### Merging Technologies Config Files

Mergingの設定ファイルを読み込んだ場合、AdminページのIPアドレスは169.254.1.254です。  
デフォルトのユーザー名は **MergingCisco**、パスワードは **Merging2020** (大文字と小文字を区別します)です。  
初めて接続する場合、または Mering社の設定ファイルを使用せずに接続する場合は、このガイドに従ってください。

1. ネットワークケーブルをスイッチとPCに接続してください。  
スイッチは初期化が必要です。初期化するとアクセスできるようになるまで数分かかります。
2. PCのIPアドレスを **192.168.1.x** に設定して下さい。
3. ブラウザのナビゲーションバーに **http://192.168.1.254** と入力してアクセスしてください(CiscoスイッチのデフォルトIPアドレスです)。



4. ユーザー名とパスワードを入力してログインします。

User name: **cisco**

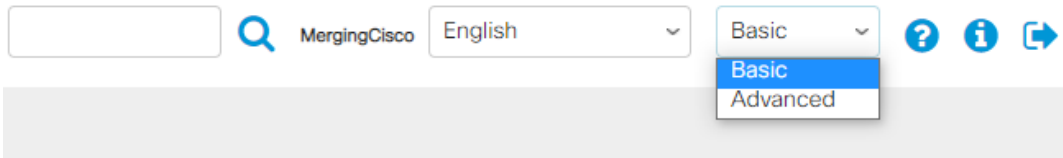
Passwaord: **cisco**

© 2020 Cisco Systems, Inc. All Rights Reserved.  
Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

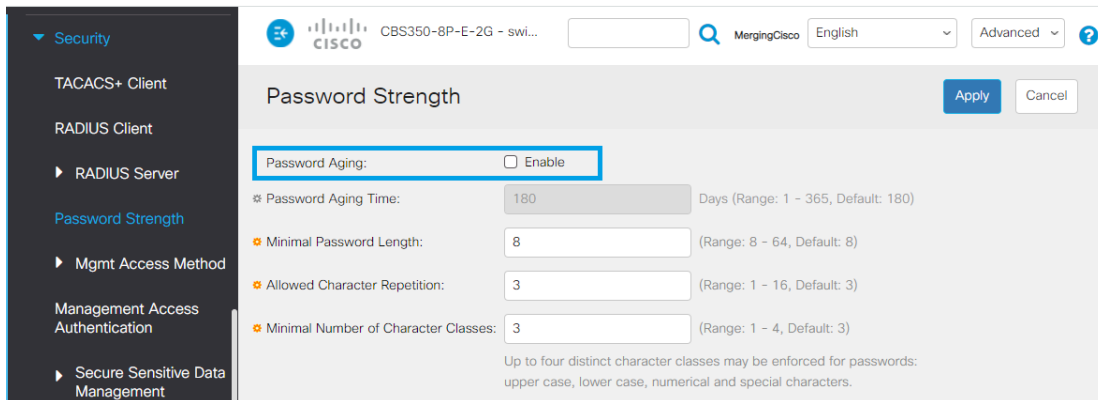
5. ログイン後、パスワードを設定するように求められます。最低文字数とパスワード強度に注意して設定して下さい。

パスワードを後で変更する場合、**Administration > User Account** ページで行います。スイッチを“Factory Default”に初期化する場合も同様です。

6. 画面右上で **Advanced mode** に設定して下さい。



7. デフォルトでは、スイッチは 6ヶ月毎にパスワードの更新を求めてきます。この動作はセキュリティを強化しますが、**Security > Password Strength** で **Password Aging** オプションのチェックを外して無効にすることができます。





## Single VLAN Configuration

まず、APIPAアドレス(Automatic Private Internet Protocol Addressing)を使用するようにIP設定を変更します。Administration ページには、この新しいIPを経由してのみアクセスできます。

スイッチをAPIPA IP範囲(169.254.0.0/16)に設定すると、システムから Administration ページにアクセスすることができます。Merging 社の Ravenna デバイスは通常APIPA IPレンジを使用してネットワーク上で通信します(Horus/Hapi/Anubis/...)。

1. **IPv4 Configuration > IPv4 Interface** を開き、+ボタンをクリックして Static Address を加えて下さい。

Interface	IP Address Type	IP Address	Mask	Status
<input type="checkbox"/> VLAN 1	DHCP	0.0.0.0	255.255.255.255	Not received
<input checked="" type="checkbox"/> VLAN 1	Default	192.168.1.254	255.255.255.0	Valid

2. IP Address type を **Static IP Address** にセットします。  
IP Address フィールドに **169.254.1.254** と入力してください。  
Mask setting には、**Prefix Length** を選択して **16** を入力してください。  
これにより、このアドレスで Administration ページにアクセスできるようになります。

### 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. **Apply** をクリックして変更を保存します。スイッチは変更の確認をしてきます。
4. スwitchの IP アドレスが **169.254.1.254** に変わります。そのため 192.168.1.254 のページは反応しなくなります。
5. スwitchにアクセスするには、PCを **169.254.x.x** アドレスプールの IP を使用するように設定してください。
6. ブラウザで **169.254.1.254** にアクセスしてください。Administration ページで **Advanced mode** (右上) になっていることを確認してください。
7. **Multicast > Properties** を開きます。  
**Bridge Multicast Filtering Status** を **Enable** にセットします。  
**Forwarding method for IPv6** と **IPv4** を両方 **IP Group address** にセットします。  
**Apply** をクリックします。

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

8. 次に **Multicast > IPv4 Multicast Configuration > IGMP Snooping** を開きます。

**IGMP Snooping Status** と **IGMP Querier Status** のチェックボックスを **Enable** にして **Apply** 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 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	
		Administrative	Operational				Administrative	Operation
1	1	Disabled	Disabled	Enabled	Disabled	0	Disabled	Disabled

9. **IGMP Snooping Table** で **ラジオボタン** をクリックし、**Edit** アイコンをクリックして下さい。



### IGMP Snooping

Apply Cancel IGMP Snooping IP Multicast Group

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		
		Administrative	Operational				Administrative	Operation	
1	1	Disabled	Disabled	Enabled	Disabled	0	Disabled	Disabled	

10. IGMP Snooping Settings を下図の様に設定し、**Apply** をクリックして下さい。

## Edit IGMP Snooping Settings

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

SSM - IGMP v3



SSM (Source-Specific Multicast)を使用する場合は、Mergingデバイスの Advanced page にある IGMP v3 も有効にしてください。

11. **Multicast > IPV4 Multicast Configuration > IGMP VLAN Settings** を開き、ラジオボタンをクリックして **Edit** アイコンをクリックして下さい。

IGMP VLAN Settings

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. **Router IGMP Version** を **V2** にセットし、**Query Interval** を **30** にして **Apply** をクリックして下さい

### Edit IGMP Settings

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)

#### SSM - IGMP v3

SSM (Source-Specific Multicast)を使用する場合は、Mergingデバイスの Advanced page にある IGMP v3 も有効にしてください。

13. **Multicast > Unregistered Multicast** を開き、全ての **port** を **Filtering** にセットして **Apply** をクリックします。





Unregistered Multicast

Filter: Interface Type equals to Port Go

Port	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10
Forwarding	<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"/>
Filtering	<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"/>

14. デフォルトで Green Ethernet が Enable になっていますが、これは無効にする必要があります。Port Management > Green Ethernet > Properties を開き、Energy Detect Mode と Short Reach のチェックを外し、802.3 Energy Efficient Ethernet (IEEE) のチェックも外して下さい。設定したら Apply をクリックして下さい。

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

15. Quality of Service > General > QoS Properties を開き、QoS Mode を Basic にセットして Apply をクリックして下さい。

QoS Properties

QoS Mode:  Disable  Basic  Advanced

16. Quality of Service > QoS Basic Mode > Global settings を開き、Trust Mode を DSCP にセットして Apply をクリックして下さい。

Global Settings

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

Override Ingress DSCP:  Enable



17. **Quality of Service > General > DSCP to Queue** を開き、**DSCP to Queue** の設定を下図の様に設定して **Apply** をクリックして下さい。

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

18. 設定を保存します。  
**Administration > File Management > File Operations** を開き、  
*Operation Type* で **Duplicate** を選択し、  
*Source File Name* で **Running Configuration** を選び、  
*Destination File Name* は **Startup Configuration** を選びます。  
**Apply** をクリックして下さい。

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

以上で現在の設定を起動時の設定にすることができました。  
言い換えれば、その設定は(デバイスのリセットが行われない限り)永久的なものになります。

19. これまでの変更を有効にするにはスイッチの再起動が必要です。  
**Administration > Reboot** をクリックします。  
**immediate** を選択して **Reboot** ボタンをクリックしてください。  
再起動が完了するにはしばらく時間がかかります。



Administration  
User Accounts  
Idle Session Timeout  
▶ Time Settings  
▶ System Log  
▶ File Management  
Cisco Business Dashboard Settings  
▶ PNP

CISCO CBS350-8P-E-2G - switch20... MergingCisco English Advanced ? i ↗

### 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



## Dual VLAN Configuration

スイッチはデフォルトの状態では VLAN1 が作成されており、通常のネットワークができるようになっています。これに Ravenna AES67 用に VLAN2 を加える設定を解説します。

VLAN1: 通常のネットワーク

VLAN2: Ravenna AES67 専用ネットワーク

前項で説明した要領で Administration ページにアクセスしてください。

注意: Administration ページは、VLAN2 からのみアクセスできます。

1. VLAN Management > VLAN Settings を開き、VLANテーブルの下にある + ボタンをクリックします。

VLAN ID	VLAN Name	Originators	VLAN Interface State	Link Status	SNMP Traps
1		Default	Disabled	Enabled	

2. VLAN ID を 2 にセットし、VLAN NAME に(特殊文字以外で)名前をつけてください。VLAN Interface Status と Link Status SNMP Traps をアクティブにして、Apply をクリックして下さい。

## Add IP Interface

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)

Apply Close

3. VLAN Management > Port to VLAN を開いて下さい。Filter セクションで VLAN ID を 2 にセットして下さい。Interface Type を Port にして Go をクリックして下さい。



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"/>

- VLAN 2のポートが全て除外されていることがわかりますので、必要なポートをこの RAVENNA/AES67 VLANに割り当てる必要があります。  
割り当てたいポートを Excluded から **Untagged** に設定します(下図ではポート5~8とポート10を VLAN 2に割り当てています)。  
完了後、**Apply** をクリックしてください。

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"/>

- VLAN1 もチェックしてください。Filter セクションで VLAN ID を 1 にセットし、Interface Type を Port にして Go をクリックしてください。VLAN1 では VLAN2 に設定したポート以外のポートが割り当てられているはずですが。
- IPv4 Configuration > IPv4 Interface** を開き、+をクリックして static address を追加します。
- まず **VLAN が 2** にセットされていることを確認してください。  
*IP Address type* を **Static IP Address** にセットし、*IP Address* フィールドに **169.254.1.254** と入力してください。*Mask Setting* には **Prefix Length** を選択して **16** と入力してください。



## Add IP Interface

X

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)

Apply

Close

- Apply をクリックして変更を保存してください。スイッチは変更の確認を行います。
- これでスイッチのアドレスは **169.254.1.254** になりました。そのため、192.168.1.254 はアクセスできなくなりました。
- スイッチにアクセスするためには、PCのIPアドレスを 169.254.x.x にセットする必要がありますが、今回は DHCP にセットしてください。
- PCが **VLAN2** に設定したポートに接続していることを確かめて下さい(この例では port6)。注意:同様の操作を VLAN1に対しても行うことで、両方の VLAN の Management インターフェイスにアクセスすることができます。ただし別のIPアドレス(例: 192.168.1.254)を使用する必要があります。**169.254.1.254** とブラウザに入力して下さい。Administration ページの右上が **Advanced mode** になっていることを確認してください。
- Multicast > Properties** を開き、**VLAN ID** を **2** にセットし、**Bridge Multicast Filtering Status** を **Enable** にセットし、**Forwarding method for IPv6 とIPv4** を両方 **IP Group address** にセットして、**Apply** をクリックしてください。



Properties

Bridge Multicast Filtering Status:  Enable

VLAN ID: 2

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

13. Multicast > IPV4 Multicast Configuration > IGMP Snooping を開き、  
IGMP Snooping Status と IGMP Querier Status のチェックボックスをチェックし、  
Apply をクリックして下さい。

IGMP Snooping

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 Querier Status	
		Administrative	Operational				Administrative	Operation
1	1	Disabled	Disabled	Enabled	Disabled	0	Disabled	Disabled

14. IGMP Snooping Table で、VLAN ID2 行 のラジオボタンをクリックして Edit アイコンをクリックしま  
す。

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	Querier IP Address
		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. 次の図の通りに IGMP Snooping Settings を設定して Apply をクリックして下さい。



## 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

### SSM - IGMP v3

SSM (Source-Specific Multicast)を使う場合は、Mergingデバイスの Advanced page にある IGMP v3 も有効にしてください。

16. Multicast > IPv4 Multicast > Configuration > IGMP VLAN Settings を開き、VLAN 2 行 の ラジオ ボタンをクリックして **Edit** アイコンをクリックします。

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
<input type="radio"/> 1	VLAN 1	v3	2	125	10	1000	0
<input checked="" type="radio"/> 2	VLAN 2	v2	2	30	10	1000	0

Router IGMP Version を **V2** にセットし、Query Interval を **30** にセットして **Apply** をクリックして下さい。





## 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)

17.

### SSM - IGMP v3

SSM (Source-Specific Multicast)を使う場合は、Mergingデバイスの Advanced page にある IGMP v3 も有効にしてください。

18. **Multicast > Unregistered Multicast** を開き、VLAN2 にアサインしたポート(この例では5から8と10)を **Filtering** にセットして **Apply** をクリックして下さい。

**Multicast**

- IPv4 Multicast Configuration
- IPv6 Multicast Configuration
- IGMP/MLD Snooping IP Multicast Group
- Multicast Router Port
- Forward All
- Unregistered Multicast

CBS350-8P-E-2G - switch20

Unregistered Multicast

Filter: Interface Type equals to

Port	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10
Forwarding	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Filtering	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

19. デフォルトの状態では **Green Ethernet** の設定がされていますので、これを無効にする必要があります。**Port Management > Green Ethernet > Properties** を開き、**Energy Detect Mode** と **Short Reach** のチェックを両方外して下さい。また、**802.3 Energy Efficient Ethernet (IEEE)** のチェックも外し、**Apply** をクリックして下さい。



Port Management

Port Settings

Error Recovery Settings

Loopback Detection Settings

▶ Link Aggregation

▶ UDLD

▶ PoE

Green Ethernet

Properties

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

20. Quality of Service > General > QoS Properties を開き、QoS Mode を Basic にセットして Apply をクリックして下さい。

Access Control

Quality of Service

General

QoS Properties

Queue

CoS/802.1p to

QoS Properties

QoS Mode:  Disable  Basic  Advanced

Apply Cancel

21. Quality of Service > Qos Basic Mode > Global settings を開き、Trust Mode を DSCP にセットして Apply をクリックして下さい。

Access Control

Quality of Service

General

QoS Basic Mode

Global Settings

Interface Settings

Global Settings

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

Override Ingress DSCP:  Enable

DSCP Override Table Apply Cancel

22. Quality of Service > General > DSCP to Queue に戻り、DSCP to Queue の設定を次の図の通りに設定して Apply をクリックして下さい。



The screenshot shows the 'DSCP to Queue' configuration page in Cisco IOS. The left sidebar contains a navigation menu with 'Quality of Service' expanded to 'DSCP to Queue'. The main content area displays a table with 16 rows, each representing a DSCP value and its mapping to an output queue. The table has columns for 'Ingress DSCP' and 'Output Queue' repeated four times. Buttons for 'Apply', 'Cancel', and 'Restore Defaults' are visible at the top right.

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

23. これまで行ってきた設定を保存します。

**Administration > File Management > File Operations** を開き、  
*Operation Type* を **Duplicate** にセットし、  
*Source File Name* を **Running Configuration** に、  
*Destination File Name* を **Startup Configuration** にセットして  
**Apply** をクリックして下さい。

The screenshot shows the 'File Operations' configuration page in Cisco IOS. The left sidebar contains a navigation menu with 'Administration' expanded to 'File Management' and 'File Operations' selected. The main content area shows three sections: 'Operation Type' with radio buttons for 'Update File', 'Backup File', and 'Duplicate' (selected); 'Source File Name' with radio buttons for 'Running Configuration' (selected), 'Startup Configuration', and 'Mirror Configuration'; and 'Destination File Name' with radio buttons for 'Running Configuration' and 'Startup Configuration' (selected). Buttons for 'Apply' and 'Cancel' are visible at the top right.

以上で現在の設定を起動時の設定にすることができました。

言い換えれば、その設定は(デバイスのリセットが行われない限り)永久的なものになります。

24. 変更を有効にするためには再起動が必要です。

**Administration > Reboot** をクリックし、  
**Immediate** を選択して **Reboot** ボタンをクリックして下さい。  
スイッチは再起動に時間がかかります。



Administration  
User Accounts  
Idle Session Timeout  
▶ Time Settings  
▶ System Log  
▶ File Management  
Cisco Business Dashboard Settings  
▶ PNP

CBS350-8P-E-2G - switch20... MergingCisco English Advanced ? i ↗

### 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



## Dante AES67 Additional configuration

まず、Dante機器がAES67に対応しているかどうかをご確認ください。

メーカーまたは Audinate のホームページでご確認ください。

DanteデバイスをMerging設定ファイルで設定したCiscoスイッチに接続する場合、追加の設定手順が必要です。

### Dante AES67 ユーザーは IP Multicast Group を追加してください：

設定ファイルを読み込ませ、スイッチの再起動が終わったら次の操作を行って下さい。

- Cisco Administration ページを開きます (Merginファイルで設定した場合、アドレスは169.254.1.254です)。
- Cisco Administration ページの **Display Mode** が **Advanced** にセットしてあることを確認してください。
- **Multicast > IP Multicast Group Address** を開き、**Add** をクリックします。
- VLAN ID 1 (VLANが1つあると仮定) と入力し、IP Multicast Group Address に 224.0.0.230 を入力して **Apply** をクリックします。
- 224.0.0.230 Group を選択し、**Detail** をクリックします。  
Danteデバイスを接続しているポートを **Static** に設定し、**Apply** をクリックします。
- 224.0.0.231, 224.0.0.232, 224.0.0.233 のアドレスに対しても同じ操作を繰り返してください。

例：Dante機器をポート9-10に接続する場合

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"/>

**SG300 / 350**

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 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"/>
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"/>

**CBS350**



## 設定のバックアップとインポート

設定をファイルにしてバックアップする

設定をファイルとしてバックアップします。

1. **Administration > File Management** を開き、**File Operations** を選択します。
2. *Operation Type* を **Backup File** にセットし、  
*Source File Type* を **Running** または **Startup Configuration** にセットします。  
*Copy Method* を **HTTP/HTTPS** にセット、  
*Sensitive Data Handling* を **Encrypt** にセットします。

The screenshot shows the Cisco File Operations configuration page. The left sidebar contains a navigation menu with 'File Management' expanded to show 'File Operations'. The main content area is titled 'File Operations' and contains the following settings:

- Operation Type:  Backup File
- Source File Type:  Running Configuration
- Copy Method:  HTTP/HTTPS
- Sensitive Data Handling:  Encrypt

The 'Apply' button is visible in the top right corner of the configuration area.

3. **Apply** をクリックします。  
これで設定ファイルがブラウザからダウンロードされます。



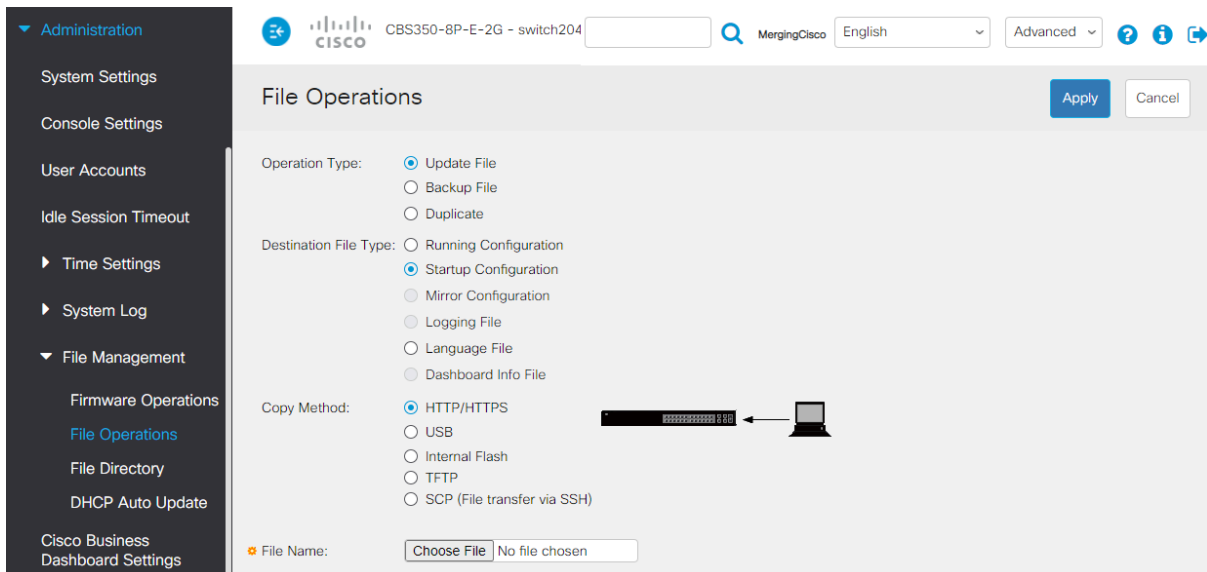
## 設定ファイルのインポート

### 重要な注意:

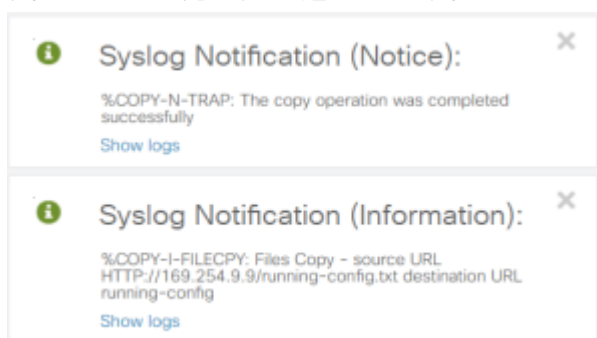
実行中のコンフィグレーション(現在のコンフィグレーション)に設定ファイルをインポートしようとする、失敗します。

コンフィグレーションファイルを startup configuration にインポートして、再起動してください。

1. **Administration > File Management** を開き、**File Operations** を選択します。
2. *Operation Type* を **Update File**  
*Destination File Type* を **Startup Configuration**  
*Copy Method* を **HTTP/HTTPS** にセットします。



3. **Choose File** をクリックしてインポートしたい設定ファイルをブラウザして選択し、**Open** をクリックして下さい。
4. メイン ウィンドウに戻って **Apply** をクリックすると、設定ファイルが Startup Configuration に入ります。インポートが完了すると通知されます。



5. 変更を有効にするためには、スイッチの再起動が必要です。**Administration > Reboot** をクリックし、**Immediate** を選択して **Reboot** ボタンをクリックして下さい。スイッチは再起動に時間がかかります。



Administration  
User Accounts  
Idle Session Timeout  
Time Settings  
System Log  
File Management  
Cisco Business Dashboard Settings  
PNP

CBS350-8P-E-2G - switch20... MergingCisco English Advanced ? i

### 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**