

Cisco Business 220スイッチのポートセキュリティ

目的

この記事では、Cisco Business 220シリーズスイッチのポートセキュリティのオプションについて説明します。

該当するデバイス | ファームウェアのバージョン

- CBS220シリーズ ([データシート](#)) | 2.0.0.17

概要

特定のMACアドレスを持つユーザへのポートへのアクセスを制限することで、ネットワークセキュリティを強化できます。MACアドレスは、動的に学習することも、静的に設定することもできます。ポートセキュリティは、受信パケットと学習パケットをモニタします。ロックされたポートへのアクセスは、特定のMACアドレスを持つユーザに制限されます。

ポートセキュリティは、802.1Xが有効になっているポート、またはSPAN宛先として定義されているポートでは有効にできません。

ポートセキュリティには2つのモードがあります。

- **クラシックロック** : ポートで学習されたすべてのMACアドレスがロックされ、ポートは新しいMACアドレスを学習しません。学習したアドレスは、エイジングや再学習の対象になりません。
- **制限付きダイナミックロック** : デバイスは、設定された許可アドレスの上限までMACアドレスを学習します。制限に達すると、デバイスは追加のアドレスを学習しません。このモードでは、アドレスはエイジングおよび再学習の対象になります。

新しいMACアドレスからのフレームが承認されていないポートで検出された場合 (ポートが古典的にロックされ、新しいMACアドレスが存在するか、ポートが動的にロックされ、許可されるアドレスの最大数を越えた場合)、保護メカニズムが呼び出されます。

- フレームは廃棄されます。
- フレームが転送されます。
- フレームが廃棄され、SYSLOGメッセージが生成されます。
- ポートがシャットダウンされます。

セキュアMACアドレスが別のポートで見つかった場合、フレームは転送されますが、そのポートではMACアドレスが学習されません。

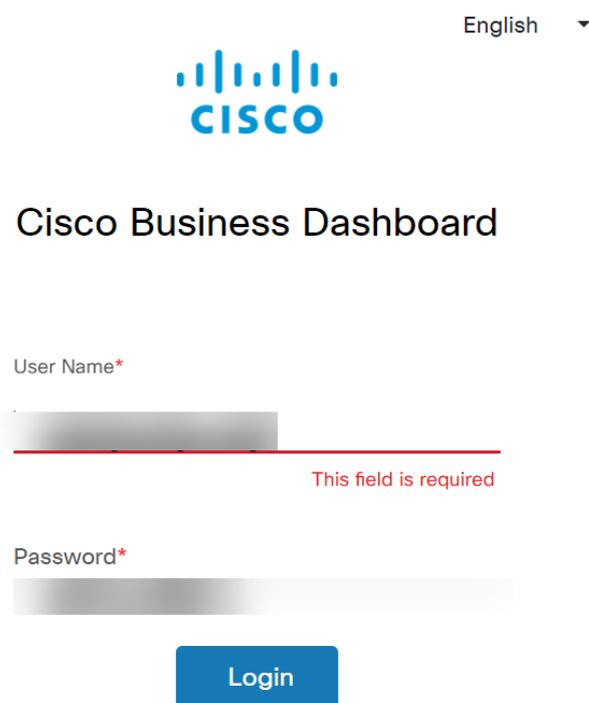
これらのアクションに加えて、トラップを生成し、デバイスの過負荷を回避するためにその頻度と数を制限することもできます。

ポートセキュリティの設定

手順 1

Webユーザインターフェイス(UI)にログインします。

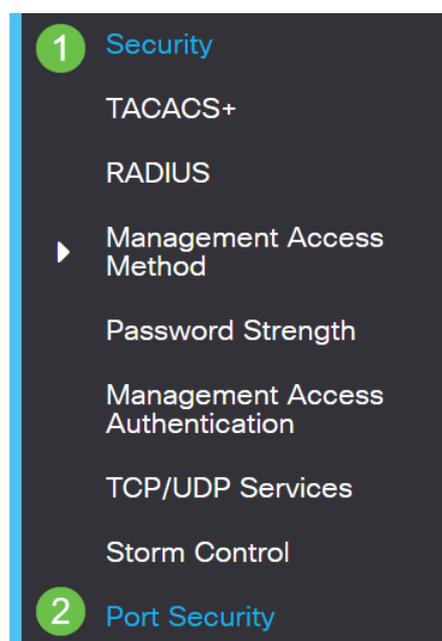
English ▾



The image shows the Cisco Business Dashboard login page. At the top right, there is a language dropdown menu set to "English". Below it is the Cisco logo. The main heading is "Cisco Business Dashboard". There are two input fields: "User Name*" and "Password*", both with red asterisks indicating they are required. The "User Name*" field has a red error message below it that says "This field is required". Below the password field is a blue "Login" button.

手順 2

左側のメニューから、[Security] > [Port Security]を選択します。



手順 3

変更するインターフェースを選択し、編集アイコンをクリックします。

Port Security Table



Entry No. Port Interface Status Learning Mode Max No. of Address

Entry No.	Port	Interface Status	Learning Mode	Max No. of Address
1	GE1	Disabled	Classic Lock	1

手順 4

パラメータを入力します。

- **Interface** : インターフェイス名を選択します。
- **管理ステータス** : ポートをロックする場合に選択します。
- **ラーニングモード** : ポートロックのタイプを選択します。このフィールドを設定するには、[Interface Status]をロック解除する必要があります。[Learning Mode]フィールドは、[Interface Status]フィールドがロックされている場合にのみ有効になります。ラーニングモードを変更するには、ロックインターフェイスをクリアする必要があります。モードが変更されると、ロックインターフェイスを復元できます。次のオプションがあります。
 - **クラシックロック** : すでに学習されたアドレスの数に関係なく、ポートを即時にロックします。
 - **制限付きダイナミックロック** : ポートに関連付けられている現在のダイナミックMACアドレスを削除して、ポートをロックします。ポートは、ポートで許可されている最大アドレスまで学習します。MACアドレスの再学習とエージングの両方が有効になります。
- **Max Number of Addresses Allowed**: Limited Dynamic Lock learning modeが選択されている場合に、ポートで学習できるMACアドレスの最大数を入力します。番号0は、インターフェイスでスタティックアドレスだけがサポートされていることを示します。
- **違反に対するアクション** : ロックポートに到着するパケットに適用するアクションを選択します。次のオプションがあります。
 - **Discard** : 学習されていない送信元からのパケットを廃棄します。
 - **転送**: MACアドレスを学習せずに、未知の送信元からパケットを転送します
 - **Discard and Log** : 学習されていない送信元からのパケットを廃棄し、インターフェイスをシャットダウンし、イベントをログに記録し、指定されたトラップレシーバにトラップを送信します。ポートは、再アクティブ化されるか、デバイスがリブートされるまでシャットダウンされたままです。
 - **Trap Frequency** : トラップ間の最小経過時間 (秒) を入力します

[Apply] をクリックします。

Edit Port Settings



Interface: **1** Port GE1 ▾

Administrative Status: **2** Enable

Learning Mode: **3** Classic Lock
 Limited Dynamic Lock

✦ Max No. of Address Allowed: **4** (Range: 1 - 256, Default: 1)

Action on Violation: **5** Discard
 Forward
 Discard and Log
 Shutdown

✦ Trap Frequency (sec): **6** (Range: 1 - 1000000, Default: 10)

7

CBS220のポートセキュリティのデフォルトの動作の例を見るには、「ポートセキュリティの動作」を確認 [してください](#)。

結論

これはあれほど簡単だ。セキュアなネットワークを楽しんでください。

その他の設定については、『[Cisco Business 220シリーズスイッチアドミニストレーションガイド](#)』を参照してください。

その他の記事を見るには、『[Cisco Business 220 Series Switch Support Page](#)』を参照してください。