ポート セキュリティ

ポート セキュリティの概要

ポートセキュリティ機能を使用して、このポートへのアクセスを許可されたワークステーションの MAC アドレスを制限し、明らかにすることにより、インターフェイスへの入力を制限することができます。これは、各インターフェイスの MAC アドレスの格納を学習し、制御するのに役立ちます。ハブやスイッチなどのプラグインされている CAM オーバーフロー攻撃や不正な機器から保護するために使用されます。ポートセキュリティ対応ポートはセキュア ポートと呼ばれ、そのポートで許可される MAC アドレスはセキュア MAC アドレスと呼ばれます。セキュア ポートにセキュア MAC アドレスを割り当てると、ポートは定義済みのアドレスのグループ外の送信元アドレスを持つパケットを転送しません。セキュア MAC アドレス数を 1 つに制限し、単一のセキュア MAC アドレスをセキュアな MAC アドレスに割り当てると、そのポートに接続されたワークステーションに、ポートの帯域幅全体が保証されます。

ポートに最大セキュアな MAC アドレス数を設定すると、セキュアなア MAC アドレスを次のいずれかの方法でアドレス テーブルに含めることができます。

- すべてのセキュア MAC アドレスを、switchport port-security mac-address *mac_address* インターフェイス コンフィギュレーション コマンドを使用して設定します。
- 接続されているデバイスの MAC アドレスで、ポートがセキュア MAC アドレスをダイナミックに設定できるようにします。
- 多数のアドレスを設定し、残りのアドレスはダイナミックに設定されるように指定します。

（注） ポートがシャットダウンされると、ダイナミックに学習されたアドレスはすべて削除されます。

- MACアドレスをステッキ—に設定します。MACアドレスは動的に学習されるか、または手動で設定され、アドレステーブル内に格納され、実行コンフィギュレーションに追加されます。これらのアドレスをコンフィギュレーションファイルに保存した場合は、スイッチを再起動しても、インターフェイスはダイナミックにこれらのアドレスを再学習する必要がありません。スティッキ セキュア アドレスを手動で設定することもできますが、推奨しません。

MAC ラーニング

インターフェイスでポート セキュリティが有効になり、新しいMACアドレスがインターフェイスに表示された後で、新しい MAC アドレスのセキュリティの検証が行われます。この検証に基づいて、MACアドレスはアドレステーブルに追加されます-通常のエントリまたはドロップ エントリとしてのいずれか。

ポート セキュリティ違反

次のいずれかの場合に、ポート セキュリティ違反が発生します。

- ポート セキュリティは、セキュア MAC アドレスがセキュア ポートで最大数に達した場合に、識別されたどのセキュア MAC アドレスとも入力トラフィックの送信元 MAC アドレスが異なると、設定された違反モードを適用します。
- あるセキュア ポートで設定または学習されたセキュアMACアドレスを持つトラフィックが、同一VLAN内の別のセキュア ポートにアクセスしようとすると、ポート セキュリティが設定された違反モードを適用します。これは、MAC 移動違反とも呼ばれる。

ポートセキュリティの3つの違反アクションがあります。これらのいずれかの違反アクションに対してポートを設定できます。

- **Shutdown**—ポート セキュリティ違反が発生すると、ポートがただちにシャットダウンします。
- **Restrict**—ポートのセキュリティ違反が発生すると、データが制限され、SecurityViolation カウンタの値が増加し、SNMP トラップが生成されます。制限アクションでは、10回の違反の後に、学習がポートで無効になります。制限は、ポート セキュリティ違反のデフォルトの動作です。
- **Protect**—ポート セキュリティ違反では、未知のMACアドレスからのデータをドロップさせます。SecurityViolation カウンタは増分されず、SNMP トラップを生成できません。

UCS 6454 でファブリック インターコネクトのポート セキュリティに関するガイドライン

次のガイドラインは、UCS 6454 ファブリック インターコネクトのポートにポートセキュリティを設定するときに適用されます。

- ポート セキュリティは、NIV ポートでのみ設定できます。BIF ポートではサポートされません。
- VLAN ごとに 1 つの MAC アドレスのみが、NIV ポートに対してセキュリティで保護することができます。
- 仮想インターフェイスでポートセキュリティ違反の制限は、デフォルトの違反アクションです。
- 10 回の違反の後に、MAC ラーニングはセキュア ポートで無効になっています。
- セキュアな MAC アドレスは、エージ アウトすることはありません。
- 設定できる最大数のセキュア MAC アドレスは次の通りです。
  - デバイス上 — ポートごとの 1 つの MAC アドレスに加えて、最大 8000 のセキュアな MAC アドレス
  - インターフェイス — インターフェイスごとの最大 1000 の MAC アドレス
  - VLAN — VLAN のポートあたり 1 つのセキュア MAC アドレスのみ

ポート セキュリティの設定

ポートにアクセスできるステーションの MAC アドレスを制限および識別することにより、このポートを通過するトラフィックを制限するには、次の作業を行います。

手順の概要

1. switch(config)# **interface** *interface_id*
2. switch(config-if)# **switchport mode access**
3. switch(config-if)# [**no**] **switchport port-security**
4. switch(config-if)# **switchport port-security maximum** *value*
5. switch(config-if)# **switchport port-security violation** {**restrict** | **shutdown** | **protect**}
6. switch(config-if)# **switchport port-security mac-address** *mac_address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch(config)# **interface** *interface_id*	インターフェイス設定モードを開始します。
ステップ 2	switch(config-if)# **switchport mode access**	インターフェイス モードを access に設定します。デフォルト モード（dynamic desirable）のインターフェイスをセキュア ポートに設定できません。
ステップ 3	switch(config-if)# [**no**] **switchport port-security**	インターフェイス上でポート セキュリティをイネーブルにします。 セキュア ポートではないデフォルトの状態にインターフェイスを戻すには、no switchport port-security インターフェイス設定コマンドを使用します。
ステップ 4	switch(config-if)# **switchport port-security maximum** *value*	インターフェイスのセキュア MAC アドレスの最大数を設定します。指定できる範囲は 1 ～ 1000 です。 インターフェイスのセキュア MAC アドレス数をデフォルトに戻すには、no switchport port-security maximum *value*インターフェイス設定コマンドを使用します。
ステップ 5	switch(config-if)# **switchport port-security violation** {**restrict** | **shutdown** | **protect**}	セキュリティ違反が検出された場合に実行するアクションを設定します。次のいずれかの処理を選択できます。 • **Shutdown**—ポート セキュリティ違反が発生すると、ポートがただちにシャットダウンします。 • **Restrict**—ポートのセキュリティ違反が発生すると、データが制限され、SecurityViolation カウンタの値が増加し、SNMP トラップが生成されます。制限アクションでは、10 回の違反の後に、学習がポートで無効になります。制限は、ポートセキュリティ違反のデフォルトの動作です。 • **Protect**—ポート セキュリティ違反では、未知の MAC アドレスからのデータをドロップさせます。SecurityViolation カウンタは増分されず、SNMP トラップを生成できません。 違反モードをデフォルト状態（shutdown モード）に戻すには、no switchport port-security violation {restrict| shutdown | protect} インターフェイス 設定コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 6	switch(config-if)# **switchport port-security mac-address** *mac_address*	インターフェイスのセキュア MAC アドレスを入力しますこのコマンドを使用すると、最大数のセキュア MAC アドレスを入力できます。設定したセキュア MAC アドレスが最大数より少ない場合、残りの MAC アドレスは動的に学習されます。 アドレス テーブルから特定の MAC アドレスを削除するには、no switchport port-security mac-address *mac_address* インターフェイス設定コマンドを使用します。