Standalone MAB Support

Standalone MAC Authentication Bypass（MAB; MAC 認証バイパス）は、802.1x 機能またはクレデンシャルにかかわらず、特定の MAC アドレスへのネットワーク アクセスを許可する認証方式です。このため、レジ、ファクス機、プリンタなどのデバイスをすぐに認証し、認証ポリシーに基づくネットワーク機能を使用可能にできます。

Standalone MAB Support が使用可能になるまで、MAB は、802.1x 認証のためのフェールオーバー方式として設定することしかできませんでした。Standalone MAB は、802.1x 認証とは独立しています。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「Standalone MAB Support の機能情報」（P.10）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

Standalone MAB Support の前提条件

IEEE 802.1x：ポートベースのネットワーク アクセス コントロール

ポートベースのネットワーク アクセス コントロールの概念とシスコのプラットフォーム上のポートベースのネットワーク アクセス コントロールの設定方法を理解しておく必要があります。詳細については、『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 15.0』を参照してください。

RADIUS および ACL

RADIUS プロトコルの概念と Access Control List（ACL; アクセス コントロール リスト）の作成および適用方法を理解しておく必要があります。詳細については、シスコのプラットフォームのマニュアル、および『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 15.0』を参照してください。

スイッチが RADIUS 設定されていて、Cisco Secure Access Control Server（ACS; アクセス コントロール サーバ）に接続されている必要があります。詳細については、『*User Guide for Secure ACS Appliance 3.2*』を参照してください。

Standalone MAB Support について

Standalone MAB をセットアップするには、次の概念を理解しておく必要があります。

- 「Cisco IOS Auth Manager の概要」（P.2）
- 「Standalone MAB」（P.3）

Cisco IOS Auth Manager の概要

指定されたネットワークに接続するデバイスの機能は異なっている可能性があるため、ネットワークはさまざまな認証方式および認証ポリシーをサポートする必要があります。Cisco IOS Auth Manager は、認証方法に関係なく、ネットワーク認証要求を処理し、認証ポリシーを強制します。Auth Manager は、すべてのポートベースのネットワーク接続試行、認証、認可、および接続解除に対する運用データを維持することで、セッション マネージャとして機能します。

Auth Manager セッションには、次のような状態が考えられます。

- Idle：idle 状態では、認証セッションは初期化されていますが、実行されている方式はありません。これは中間の状態です。
- Running：現在、方式が実行されています。これは中間の状態です。
- Authc Success：認証方式の実行に成功しました。これは中間の状態です。
- Authc Failed：認証方式が失敗しました。これは中間の状態です。
- Authz Success：このセッションに対するすべての機能の適用に成功しました。これは最終的な状態です。
- Authz Failed：このセッションに対して、少なくとも 1 つの機能の適用に失敗しました。これは最終的な状態です。
- No methods：このセッションに結果を提供する方式がありません。これは最終的な状態です。

Standalone MAB

MAB はネットワーク アクセスの許可または拒否に、接続デバイスの MAC アドレスを使用します。MAB をサポートするため、RADIUS 認証サーバは、ネットワークへのアクセスを必要とするデバイスの MAC アドレスのデータベースを維持します。MAB は、Calling-Station-Id（アトリビュート 31）で MAC アドレスを使用し、Service-Type（アトリビュート 6）で値 10 を使用して、RADIUS 要求を生成します。認証に成功すると、Auth Manager は、ACL 割り当ておよび VLAN 割り当てなど認証ポリシーによって指定されたさまざまな認証機能をイネーブルにします。

Standalone MAB の設定方法

ここでは、次の作業について説明します。

Standalone MAB のイネーブル化

Standalone MAB 機能でイネーブルにされたポートは、ネットワーク アクセスの許可または拒否に接続デバイスの MAC アドレスを使用できます。個別ポートで、Standalone MAB をイネーブルにするには、この項で説明する手順を実行します。

前提条件

Standalone MAB を設定する前に、スイッチを Cisco Secure ACS サーバに接続し、RADIUS Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）を設定する必要があります。

制約事項

Standalone MAB は、スイッチド ポート上でのみ設定できます。ルーテッド ポートでは設定できません。

（注） MAB または MAB EAP がスイッチド ポート上でイネーブルにされているかディセーブルにされているかわからない場合は、インターフェイス コンフィギュレーション モードで、**default mab** または **default mab eap** コマンドを使用して、MAB または MAB EAP をデフォルトに設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **switchport**
5. **switchport mode access**

6. **authentication port-control auto**
7. **mab** [**eap**]
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Switch> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type slot*/*port* **例：** `Switch(config)# interface FastEthernet2/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport** **例：** `Switch(config-if)# switchport`	レイヤ 2 スイッチド モードでインターフェイスを配置します。
ステップ 5	**switchport mode access** **例：** `Switch(config-if)# switchport mode access`	非トランキング、非タグ付き、シングル VLAN レイヤ 2 インターフェイスを設定します。
ステップ 6	**authentication port-control auto** **例：** `Switch(config-if)# authentication port-control auto`	ポートの認証ステートを設定します。
ステップ 7	**mab** [**eap**] **例：** `Switch(config-if)# mab`	MAB をイネーブルにします。
ステップ 8	**end** **例：** `Switch(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。

トラブルシューティングのヒント

次のコマンドは、Standalone MAB のトラブルシューティングに役立ちます。

- **debug authentication**
- **debug mab all**
- **show authentication registrations**

- **show authentication sessions**
- **show mab**

ポート上の再認証のイネーブル化

デフォルトでは、ポートは自動的に再認証されません。自動再認証をイネーブルにし、再認証の頻度を指定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot*/*port*
4. **switchport**
5. **switchport mode access**
6. **authentication port-control auto**
7. **mab** [**eap**]
8. **authentication periodic**
9. **authentication timer reauthenticate** {*seconds* | **server**}
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Switch> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type slot*/*port* **例：** `Switch(config)# interface FastEthernet2/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport** **例：** `Switch(config-if)# switchport`	レイヤ 2 スイッチド モードでインターフェイスを配置します。
ステップ 5	**switchport mode access** **例：** `Switch(config-if)# switchport mode access`	非トランキング、非タグ付き、シングル VLAN レイヤ 2 インターフェイスを設定します。

	コマンドまたはアクション	目的
ステップ 6	**authentication port-control auto** **例：** `Switch(config-if)# authentication port-control auto`	ポートの認証ステートを設定します。
ステップ 7	**mab** [**eap**] **例：** `Switch(config-if)# mab`	MAB をイネーブルにします。
ステップ 8	**authentication periodic** **例：** `Switch(config-if)# authentication periodic`	再認証をイネーブルにします。
ステップ 9	**authentication timer reauthenticate** {*seconds* | **server**} **例：** `Switch(config-if)# authentication timer reauthenticate 900`	再認証の間隔（秒単位）を設定します。
ステップ 10	**end** **例：** `Switch(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。

セキュリティ違反モードの指定

ポート上でセキュリティ違反がある場合、ポートをシャットダウンするか、トラフィックを制限できます。デフォルトでは、ポートはシャットダウンされます。ポートをシャットダウンする一定の時間を設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **switchport**
5. **switchport mode access**
6. **authentication port-control auto**
7. **mab** [**eap**]
8. **authentication violation** {**restrict** | **shutdown**}
9. **authentication timer restart** *seconds*
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Switch> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type slot*/*port* **例：** `Switch(config)# interface FastEthernet2/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport** **例：** `Switch(config-if)# switchport`	レイヤ 2 スイッチド モードでインターフェイスを配置します。
ステップ 5	**switchport mode access** **例：** `Switch(config-if)# switchport mode access`	非トランキング、非タグ付き、シングル VLAN レイヤ 2 インターフェイスを設定します。
ステップ 6	**authentication port-control auto** **例：** `Switch(config-if)# authentication port-control auto`	ポートの認証ステートを設定します。
ステップ 7	**mab** [**eap**] **例：** `Switch(config-if)# mab`	MAB をイネーブルにします。
ステップ 8	**authentication violation** {**restrict** | **shutdown**} **例：** `Switch(config-if)# authentication violation shutdown`	ポート上でセキュリティ違反が生じた場合に取るアクションを設定します。
ステップ 9	**authentication timer restart** *seconds* **例：** `Switch(config-if)# authentication timer restart 30`	未認証のポートの認証の間隔（秒単位）を設定します。
ステップ 10	**end** **例：** `Switch(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。

Standalone MAB の設定例

ここでは、次の例について説明します。

Standalone MAB の設定：例

次に、ポート上で Standalone MAB を設定する方法の例を示します。この例で、クライアントは 1200 秒ごとに再認証され、接続は 600 秒の非アクティビティでドロップされます。

```
enable
 configure terminal
  interface GigabitEthernet2/1
   switchport
   switchport mode access
   switchport access vlan 2
   authentication port-control auto
   mab
   authentication violation shutdown
   authentication timer restart 30
   authentication periodic
   authentication timer reauthenticate 1200
   authentication timer inactivity 600
```

その他の参考資料

ここでは、Standalone MAB 機能に関する関連資料について説明します。

関連資料

内容	参照先
認証コマンド	『*Cisco IOS Security Command Reference*』
IEEE 802.1x：フレキシブルな認証	『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 15.0』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
• CISCO-AUTH-FRAMEWORK-MIB • CISCO-MAC-AUTH-BYPASS-MIB • CISCO-PAE-MIB • IEEE8021-PAE-MIB	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 3580	「*IEEE 802.1x Remote Authentication Dial In User Service (RADIUS)*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

Standalone MAB Support の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　Standalone MAB Support の機能情報

機能名	リリース	機能情報
Standalone MAB Support	12.2(33)SXI	この機能は、802.1x 機能またはクレデンシャルにかかわらず、MAC アドレスに基づいてデバイスへのネットワーク アクセスを許可します。 この機能により、次のコマンドが導入または変更されました。**authentication periodic**、**authentication port-control**、**authentication timer inactivity**、**authentication timer reauthenticate**、**authentication timer restart**、**authentication violation**、**debug authentication**、**mab**、**show authentication interface**、**show mab**、**show authentication registrations**、**show authentication sessions**