



## mab ~ mime-type

---

- [mab](#), 2 ページ
- [mac access-group](#), 4 ページ
- [mac-address \(RITE\)](#), 6 ページ
- [match class-map](#), 8 ページ

# mab

ポートで MAC ベースの認証を有効にするには、インターフェイス コンフィギュレーション モードまたはテンプレート コンフィギュレーション モードで **mab** コマンドを使用します。MAC ベースの認証を無効にするには、このコマンドの **no** 形式を使用します。

**mab [cap]**

**no mab**

## 構文の説明

|            |   |
|------------|---|
| <b>cap</b> | (オプション) Extensible Authentication Protocol (EAP) を使用するようにポートを設定します。 |
|------------|---|

## コマンド デフォルト

MAC ベースの認証は有効になっていません。

## コマンド モード

インターフェイス コンフィギュレーション (config-if)

テンプレート コンフィギュレーション (config-template)

## コマンド履歴

| リリース                      | 変更内容  |
|---------------------------|---|
| 12.2(33)SXI               | このコマンドが導入されました。   |
| 15.2(2)T                  | このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。  |
| 15.2(2)E                  | このコマンドが、Cisco IOS リリース 15.2(2)E に統合されました。このコマンドは、テンプレート コンフィギュレーション モードでサポートされます。   |
| Cisco IOS XE Release 3.6E | このコマンドが Cisco IOS XE Release 3.6E に統合されました。このコマンドは、テンプレート コンフィギュレーション モードでサポートされます。 |

## 使用上のガイドライン

ポートで MAC ベースの認証を有効にするには、**mab** コマンドを使用します。ポートで EAP を有効にするには、**mabeap** コマンドを使用します。



(注) MAB または MAB EAP がスイッチド ポート上で有効または無効のいずれであるかがわからない場合は、インターフェイス コンフィギュレーション モードで、**defaultmab** コマンドまたは **defaultmabeap** 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。

## 例

次に、ギガビット イーサネット ポートで MAC ベースの認証を設定する例を示します。

```
Switch(config)# interface GigabitEthernet6/2
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-if)# mab
Switch(config-if)# end
```

次に、インターフェイス テンプレートで MAC ベースの認証を設定する例を示します。

```
Device# configure terminal
Device(config)# template user-templ1
Device(config-template)# mab
Device(config-template)# end
```

## 関連コマンド

| コマンド           | 説明                |
|----------------|-------------------|
| <b>showmab</b> | MAB に関する情報を表示します。 |

## mac access-group

MAC アクセス コントロール リスト (ACL) を使用して、ギガビットイーサネット インターフェイス、802.1Q VLAN サブインターフェイス、802.1Q-in-Q スタック VLAN サブインターフェイスでの着信トラフィックの受信を制御するには、インターフェイスまたはサブインターフェイス コンフィギュレーション モードで **macaccess-group** コマンドを使用します。MAC ACL を削除するには、このコマンドの **no** 形式を使用します。

**mac access-group** *access-list-number* **in**

**no mac access-group** *access-list-number* **in**

### 構文の説明

|                           |   |
|---------------------------|---|
| <i>access-list-number</i> | インターフェイスまたはサブインターフェイスに適用する MAC ACL の番号 ( <b>access-list(MAC)</b> コマンドで指定された番号)。これは 10 進数の 700 ~ 799 です。 |
| <b>in</b>                 | インバウンドパケットに対してフィルタリングします。   |

### コマンド デフォルト

インターフェイスまたはサブインターフェイスにアクセス リストは適用されていません。

### コマンド モード

インターフェイス コンフィギュレーション (**config-if**) サブインターフェイス コンフィギュレーション (**config-subif**)

### コマンド履歴

| リリース        | 変更内容  |
|-------------|---|
| 12.0(32)S   | このコマンドが Cisco 12000 シリーズ インターネット ルータに追加されました。   |
| 12.2(33)SXH | このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。 |

### 使用上のガイドライン

MAC ACL は、ギガビットイーサネット インターフェイスおよび VLAN サブインターフェイス上の着信トラフィックに対して適用されます。ネットワークング デバイスでパケットを受信すると、Cisco IOS ソフトウェアはアクセス リストと、ギガビットイーサネット、802.1Q VLAN、ま

たは 802.1Q-in-Q のパケットの送信元 MAC アドレスを照合します。MAC アクセスリストでアドレスが許可されている場合、ソフトウェアはパケットの処理を続行します。アクセスリストでアドレスが拒否されている場合、ソフトウェアはパケットを廃棄し、インターネット制御メッセージプロトコル (ICMP) ホスト到達不能メッセージを返します。

指定した MAC ACL がインターフェイスまたはサブインターフェイス上に存在しない場合、パケットはすべて通過します。

Catalyst 6500 シリーズスイッチの場合、このコマンドをサポートするのはレイヤ 2 ポートだけです。



(注) VLAN サブインターフェイス上で **macaccess-group** コマンドをサポートするのは、すでに VLAN がサブインターフェイス上で設定済みの場合だけです。

## 例

次は、ギガビットイーサネットインターフェイス 0 で受信した着信トラフィックに対して MAC ACL 101 を適用する例です。

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0
Router(config-if)# mac access-group 101 in
```

## 関連コマンド

| Command                              | Description                                 |
|--------------------------------------|---|
| <b>access-list(MAC)</b>              | MAC ACL を定義します。                             |
| <b>clearmacaccess-listcounters</b>   | MAC ACL のカウンタをクリアします。                       |
| <b>ipaccess-group</b>                | 非同期ホストから送信されたパケットに対して使用する IP アクセスリストを設定します。 |
| <b>showaccess-groupmodeinterface</b> | レイヤ 2 インターフェイスの ACL コンフィギュレーションを表示します。      |
| <b>showmacaccess-list</b>            | 1 つまたはすべての MAC ACL の内容を表示します。               |

## mac-address (RITE)

宛先ホストのイーサネットアドレスを指定するには、ルータ IP トラフィック エクスポート (RITE) コンフィギュレーション モードで **mac-address** コマンドを使用します。宛先ホストの MAC アドレスを変更するには、このコマンドの **no** 形式を使用します。

**mac-address** *H.H.H*

**nomac-address** *H.H.H*

### 構文の説明

|              |                  |
|--------------|------------------|
| <i>H.H.H</i> | 48 ビット MAC アドレス。 |
|--------------|------------------|

### コマンド デフォルト

宛先ホストは不明です。

### コマンド モード

RITE コンフィギュレーション

### コマンド履歴

| リリース      | 変更内容  |
|-----------|---|
| 12.3(4)T  | このコマンドが導入されました。                               |
| 12.2(25)S | このコマンドが、Cisco IOS Release 12.2(25)S に統合されました。 |

### 使用上のガイドライン

**mac-address** コマンドは、エクスポートされたトラフィックを受信する宛先ホストを指定するコマンドであり、着信および発信の両方の IP トラフィック エクスポートの各種属性を制御する RITE コンフィギュレーション モード コマンドスイートの一部です。

**iptraffic-exportprofile** コマンドでは、選択したルータ入力インターフェイスで着信または発信される IP パケットをエクスポートするために設定できるプロファイルを開始できます。指定された出力インターフェイスは、キャプチャされた IP パケットをルータからエクスポートします。したがってルータは未変更の IP パケットを直接接続デバイスにエクスポートできます。

### 例

次に、プロファイル「corp1」を設定する例を示します。このプロファイルは、キャプチャされた IP トラフィックを、インターフェイス「FastEthernet 0/1」でホスト「00a.8aab.90a0」へ送信します。また、このプロファイルは 50 パケットごとに 1 つのパケットをエクスポートし、アクセス

コントロールリスト (ACL) 「ham\_ACL」からの着信トラフィックだけを許可するように設定されています。

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

#### 関連コマンド

| コマンド                           | 説明  |
|--------------------------------|---|
| <b>iptraffic-exportprofile</b> | IP トラフィック エクスポート プロファイルを作成または編集し、入力インターフェイス上でこのプロファイルを有効にします。 |

## match class-map

トラフィック クラスを分類ポリシーとして使用するには、クラス マップまたはポリシー インライン コンフィギュレーション モードで **match class-map** コマンドを使用します。一致基準としての特定のトラフィック クラスを削除するには、このコマンドの **no** 形式を使用します。

**match class-map** *class-map-name*

**no match class-map** *class-map-name*

### 構文の説明

|                       |                           |
|-----------------------|---------------------------|
| <i>class-map-name</i> | 一致基準として使用するトラフィック クラスの名前。 |
|-----------------------|---------------------------|

### コマンド デフォルト

一致基準が指定されていません。

### コマンド モード

クラス マップ コンフィギュレーション (config-cmap)

### コマンド履歴

| リリース                      | 変更内容  |
|---------------------------|---|
| 12.0(5)XE                 | このコマンドが導入されました。   |
| 12.1(1)E                  | このコマンドが Cisco IOS Release 12.1(1)E に統合されました。  |
| 12.1(5)T                  | このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。  |
| 12.4(6)T                  | このコマンドが拡張され、ゾーンベース ポリシー ファイアウォールをサポートするようになりました。  |
| 12.2(33)SRA               | このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。   |
| 12.2(31)SB                | このコマンドは、Cisco 10000 シリーズに実装されました。   |
| 12.2SX                    | このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされません。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォームハードウェアによって異なります。 |
| Cisco IOS XE Release 3.2S | このコマンドが、Cisco IOS XE Release 3.2S に統合されました。   |

**使用上のガイドライン** 1つのトラフィック クラスに **match-any** 特性と **match-all** 特性の両方を使用する唯一の方法は、**match class-map** コマンドを使用する方法です。**match-any** 特性と **match-all** 特性を結合して1つのクラスにするには、次のいずれかを実行します。

- **match-any** 指示を使用してトラフィック クラスを作成し、一致基準として **match-all** 指示を使用して設定したクラスを使用します (**match class-map** コマンドを使用)。
- **match-all** 指示を使用してトラフィック クラスを作成し、一致基準として **match-any** 指示を使用して設定したクラスを使用します (**match class-map** コマンドを使用)。

また、**match class-map** コマンドを使用してトラフィック クラスを別のクラス内にネストすることもできます。これにより、以前に設定したトラフィック クラスにほとんどの情報が存在している場合に、ユーザが新しいトラフィック クラスを再作成するオーバーヘッドが削減されます。

パケットがクラス マップに一致すると、それらのパケットのトラフィック レートが生成されます。ゾーンベースファイアウォールポリシーでは、ポリシーと一致するのは、セッションを作成した最初のパケットのみです。このフローの後続パケットは、設定されたポリシー内のフィルタと一致しませんが、セッションとは直接一致します。後続パケットに関連する統計情報は、検査アクションの一部として表示されます。

---

## 例

---

## 例

次の例で、トラフィック クラス **class1** の特性は、トラフィック クラス **class2** の特性とほぼ同じですが、トラフィック クラス **class1** では、一致基準として宛先アドレスが追加されています。トラフィック クラス **class1** をゼロから設定する代わりに、**match class-map class2** コマンドを使用できます。このコマンドを使用すると、トラフィック クラス **class2** のすべての特性をトラフィック クラス **class1** に取り込み、トラフィック クラスを再設定することなく、新しい宛先アドレスの一致条件を追加できます。

```
Router(config)# class-map match-any class2
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 3
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# class-map match-all class1
Router(config-cmap)# match class-map class2
Router(config-cmap)# match destination-address mac 1.1.1
Router(config-cmap)# exit
```

次に、2つのトラフィック クラスの特性を組み合わせる例を示します。1つは **match-any** 特性を使用し、1つは **match-all** 特性を使用しています。これを、**match class-map** コマンドで1つのトラフィック クラスとして設定します。**class4** というトラフィック クラスの場合、パケットが **class4** トラフィック クラスのメンバーとして見なされるためには、3つの一致基準 (IP プロトコルかつ QoS グループ 4、宛先 MAC アドレス 1.1.1、またはアクセス グループ 2) のいずれかを満たしている必要があります。一致基準である IP プロトコルかつ QoS グループ 4 は、トラフィック クラス **class3** の定義が必要であり、**match class-map class3** コマンドによって、トラフィック クラス **class4** の定義に可能な一致として含まれています。

この例では、トラフィック クラス class4 だけがサービス ポリシー policy1 に使用されています。

```
Router(config)# class-map match-all class3
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 4
Router(config-cmap)# exit
Router(config)# class-map match-any class4
Router(config-cmap)# match class-map class3
Router(config-cmap)# match destination-address mac 1.1.1
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class4
Router(config-pmap-c)# police 8100 1500 2504 conform-action transmit exceed-action
set-qos-transmit 4
Router(config-pmap-c)# exit
```

#### 関連コマンド

| コマンド             | 説明                                     |
|------------------|--|
| <b>class-map</b> | 指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。 |