MAC 認証バイパスの設定

この章では、Catalyst 6500 シリーズ スイッチ上で MAC（メディア アクセス制御）認証バイパスを設定する手順について説明します。

（注） この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

（注） IEEE 802.1X 認証の設定については、第 39 章「802.1X 認証の設定」を参照してください。

（注） イーサネット、ファスト イーサネット、またはギガビット イーサネット ポートへのアクセスを試みたステーションの MAC アドレスが、そのポートに指定されている MAC アドレスと異なる場合に、ポート セキュリティ機能を使用してポートへのアクセスをブロックする手順については、第 37 章「ポート セキュリティの設定」を参照してください。また、ホスト MAC アドレスに基づく指定ホストに送信、または指定ホストから受信したトラフィックをフィルタリングする場合に、ポート セキュリティ機能を使用する手順についても説明します。

（注） Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）を設定して、Catalyst 6500 シリーズ スイッチの CLI（コマンドライン インターフェイス）へのアクセスをモニタおよび制御する方法については、第 38 章「AAA によるスイッチ アクセスの設定」を参照してください。

この章で説明する内容は、次のとおりです。

MAC 認証バイパス機能の概要

ここでは、Catalyst 6500 シリーズ スイッチの MAC 認証バイパス機能について説明します。

概要

MAC 認証バイパスは、802.1X の要求元機能を持たない装置（プリンタおよび IP Phone など）へのネットワーク アクセスを可能にする 802.1 X に代わるものです。MAC 認証バイパスは、接続装置の MAC アドレスを使用してネットワーク アクセスを許可または拒否します。

MAC 認証バイパスをサポートするために、RADIUS 認証サーバでは、ネットワークへのアクセスが必要な装置の MAC アドレスのデータベースを維持します。MAC 認証バイパスは、Calling-Station-ID（属性 31）として MAC アドレスおよび値が 10 の Service-Type（属性 6）を含む RADIUS 要求を生成します。

装置の MAC アドレスを入手するには、スイッチ ポートを VLAN（仮想 LAN）内でフォワーディング ステートにする必要があります。ポートが VLAN でフォワーディング ステートでなければ、スイッチ上でユニキャスト トラフィックを受信または送信できません。スイッチ ポートは、ポート上でラーニングがディセーブルなネイティブ VLAN で起動するため、パケットはスーパバイザ エンジンにリダイレクトされます。スーパバイザ エンジンが新しい MAC アドレスを確認すると、CAM（連想メモリ）エントリおよびトラップ ビットを挿入します。トラップ ビットは、MAC アドレスからの不必要なフラッディングからスーパバイザ エンジンを保護するよう設定されています。スーパバイザ エンジンは、MAC 認証が終了するまで、それ以上のパケットをリダイレクトしません。認証が成功すると、RADIUS サーバが VLAN を送信し、ポートはこの VLAN に移行します。認証成功後、トラップ エントリは削除されます。RADIUS サーバ指定の VLAN に移行したポートは、他のスイッチ ポートと同様に動作します。MAC 認証が失敗した場合、ポートは認証失敗 VLAN（設定されている場合）に移行します（認証失敗 VLAN については、「認証失敗 VLAN の設定」[p.39-37]を参照）。

MAC アドレス再認証の概要

再認証モードでは、ポートは RADIUS サーバ指定の VLAN のままで自身を再認証しようとします。再認証が成功した場合、ポートは RADIUS サーバ指定の VLAN のままです。再認証が失敗した場合、ポートは認証失敗 VLAN（設定されている場合）に移行されるか、または既存の VLAN から管理上設定された VLAN に移行されます。失敗したポートには、定期的に再認証が試されます。以前認証された VLAN 上の失敗ポートの MAC アドレス CAM エントリは削除され、ポートは初期化プロセスにより、自動的に管理上設定された VLAN に移行し、ポート自身への再認証を試行します。再認証が成功した場合、ポートは RADIUS サーバ指定の VLAN に移行されます。

また、RADIUS サーバ指定のタイマーも再認証をトリガーします。RADIUS サーバの属性 27 および 29 は、再認証動作を制御します。属性 27（セッション タイムアウト）では、認証が再試行されるまでの時間を指定し、属性 29（ターミネーション アクション）では、再認証動作が次のいずれになるかを指定します。

- 初期化 — 既存のセッションは、再認証結果が確認できるまで、中断されます。
- 再認証 — 再認証試行中は、既存のセッションは中断されません。

MAC 認証バイパス ステートの概要

ここでは、次の MAC 認証バイパス ステートについて説明します。

- 待機 — 待機ステートの場合、スイッチは認証される必要がある MAC アドレスの受信を待機します。ラーニングはディセーブルで、アイドル タイマーが開始します。ポートは、フォワーディング ステートでユニキャスト トラフィックを受信し、ポート上のすべてのレイヤ 2 エントリは消去されます。他に機能が設定されている場合は、ポートは認証結果を待ってから（結果が成功でも失敗でも）他のステートに移行します。トラフィックが確認されなければ、ポートは待機ステートのままです。
- 認証 — スイッチがリダイレクトされたパケットからポートの MAC アドレスを学習すると、MAC 認証バイパス ステート マシンは認証に移行します。このステートでは、RADIUS 要求が作成され、RADIUS サーバに送信されます。スイッチは、RADIUS サーバ応答を待機します。認証が成功すると、ポートは認証済みステートに移行します。このステートでは、ポート上で RADIUS サーバ指定の VLAN が設定され、スタティック CAM エントリが RADIUS サーバ指定の VLAN に挿入され、古い VLAN 上のトラップ エントリは削除されます。認証に失敗すると、ポートは認証失敗ステートに移行します。RADIUS タイムアウトまたは初期化が発生した場合、ポートは再度待機ステートに移行します。
- 認証済み — 認証済みステートでは、RADIUS が受信したポリシー（VLAN）がポート上で設定されます。初期化がある場合、ポートは待機ステートに移行し、再認証イベントを受信すると、認証ステートに移行します。認証済みステートでは、ポート上のトラップ エントリが古い VLAN から削除され、スタティック CAM エントリが新しい VLAN に挿入されます。
- 認証失敗 — 認証失敗ステートでは、他の機能が設定されていなければ、ポートは待機ステートに移行するまで [auth-fail-timeout]（秒）待機します。フォールバック機能（Web ベースのプロキシ認証、802.1X、または認証失敗 VLAN など）が設定されている場合、ポートはこれらのステートに移行します。トラップは認証失敗ステートのまま存在するため、MAC アドレスは [auth-fail-timeout]（秒）間自身を再認証できません。ポートが認証失敗ステートから待機ステートに移行すると、トラップ エントリは消去され、ポートは認証プロセスを再開します。
- 終了 — MAC 認証バイパスがホストの認証に失敗すると、アクセスを許可する可能性がある他の機能（Web ベースのプロキシ認証、802.1X、または認証失敗 VLAN）がポートに設定されていない場合は、終了ステートになります。終了ステートでは、ポートの許可 / アップ、およびほかの機能で必要とされる任意のポリシーの付加が行われます。たとえば、ゲスト VLAN が設定されている場合、ポートはゲスト VLAN に追加されます。Web ベースのプロキシ認証が設定されている場合は、HTTP リダイレクションなどで Dynamic Host Configuration Protocol（DHCP）、Domain Name System（DNS; ドメイン ネーム システム）、Access Control Entry（ACE; アクセス制御エントリ）を許可するためにポリシーが付加されます。他の機能が設定されていない場合は、認証が失敗すると、ポートは待機、認証、認証失敗、および待機ステートを移動するか、またはトラフィックを確認するまで待機ステートのままです。

MAC 認証バイパス ステート イベントの概要

ここでは、次の MAC 認証バイパス イベントについて説明します。

- AuthenticateMac — このイベントは、コンポーネントを処理するリダイレクトされたパケットがポート上で MAC アドレスを確認すると、通知されます。このイベントは、MAC 認証バイパス ステート マシンが待機ステートの場合に通知されます。
- Initialize — このイベントは CLI によりトリガーされ、どのステートでも受信されます。このイベントを受信すると、ポートは待機ステートに移行し、クリーンアップ（ポートの拒否、任意のスタティック エントリまたはトラップ CAM エントリのクリーンアップなど）が必要な場合は、実行します。
- Reauthenticate — このイベントは、セッションタイムアウトの時間切れか、または CLI トリガー（CLI から入力された実行コマンド）が原因で受信されます。このイベントは、ポートが認証済みステートである場合にのみ受け入れられます。それ以外の場合、無視されます。CLI により発生したイベントでは、CLI はポートが認証済みステートの場合にのみ受け入れられることを通知します。

- Authentication success — このイベントは、RADIUS サーバからの認証が成功した場合に、通知されます。このイベントは、ポートが認証ステートの場合にのみ受け入れられ、ポートを認証済みステートに移行させます。
- Authentication failure — このイベントは、RADIUS サーバからの認証失敗を受信した場合に、通知されます。このイベントは、ポートが認証ステートの場合にのみ受け入れられ、このポートを認証失敗ステートに移行させます。
- RADIUS timeout — このイベントは、RADIUS サーバが応答しない場合に受信されます。このイベントはポートが認証ステートの場合にのみ受け入れられ、最大再試行回数の満了後、RADIUS サーバが応答しなければ、ポートを待機ステートに移行させます。
- AuthFail timeout — このイベントは、ポートが RADIUS サーバの認証失敗による認証失敗ステートにあり、ポートをアップにするその他の潜在的機能が設定されていない場合に、受信されます。このイベントにより、ポートは待機ステートに移行し、認証プロセスを再開します。
- Security violation — このイベントは、待機ステート以外のすべてのステートで受信されます。このイベントは、ポート上で 2 つめの MAC アドレスが確認された場合に通知されます。セキュリティ違反の場合に行う措置は、MAC アドレスの制限またはポートのシャット ダウンのいずれかで、設定されたグローバル違反モードによって異なります。

MAC 認証バイパスの設定時の注意事項および制限事項

ここでは、MAC 認証バイパスの設定時の注意事項および制限事項について説明します。

- セキュリティ違反 — MAC 認証バイパスでは、ポートごとに 1 つのホストのみがサポートされます。ポート上に複数のホストが表示された場合、セキュリティ違反となりポートはシャットダウンします。補助 VLAN ポートの場合、ポートごとに 1 つのホストの制限はデータ VLAN 上のホストにのみ適用されます。つまり、補助（音声）VLAN ではホスト数の制限はありません。
- ポリシーの適用 — MAC 認証バイパスでは、802.1X でサポートされるすべてのポリシー適用メカニズムがサポートされます。
- DHCP スヌーピング — MAC 認証バイパスは、DHCP スヌーピングとは無関係です。MAC アドレスが認証に成功するまでは、MAC アドレスからのトラフィックは許可されず（トラップ エントリのため）、MAC 認証のトリガーとなるトラフィックは DHCP など任意のタイプのトラフィックとなります。
- 802.1X — MAC 認証バイパスは独立した機能ですが、802.1X と組み合わせて使用する場合は、MAC アドレス認証の代替として機能します。ポート上で MAC 認証バイパスと 802.1X の両方が設定されている場合、ポートは 802.1X を使用して認証しようとします。ホストが EAPOL 要求に応答しない場合、認証試行を継続せずに、802.1X ポートが MAC 認証バイパス ステートに移行され、MAC 認証バイパスを使用して認証が試行されます。
- 認証失敗 VLAN — 802.1X 認証が失敗すると、MAC 認証バイパスが設定されているかどうかに関わらず、認証失敗 VLAN が設定されている場合は、ポートは認証失敗 VLAN に移行されます。この認証失敗 VLAN は、802.1X 認証失敗ユーザ専用で、MAC 認証バイパス用の汎用認証失敗 VLAN ではありません。認証失敗 VLAN については、「認証失敗 VLAN の設定」（p.39-37）を参照してください。
- ゲスト VLAN — 802.1X ゲスト VLAN および MAC 認証バイパスは、既存のゲスト VLAN 動作に対する一部の変更点を除いて、連動します。MAC 認証バイパスおよび ゲスト VLAN が設定されていて、ポートで Extensible Authentication Protocol over LAN （EAPOL）パケットが受信されない場合、802.1X ステート マシンは MAC 認証バイパス ステートに移行され、ポートをネイティブ VLAN でフォワーディングに設定し、ラーニングをディセーブルにします。ゲスト VLAN が設定されていない場合、ポートは MAC 認証バイパス ステートのままでポート上の MAC アドレスを待機します。ゲスト VLAN の詳細については、「ゲスト VLAN に対する 802.1X 認証の概要」（p.39-8）を参照してください。
- ポート セキュリティ — 新しくリダイレクトされた MAC アドレスは、ポート セキュリティより先に MAC 認証バイパス機能により確認されます。MAC アドレスが認証に成功すると、新しく学習された MAC アドレスがポート セキュリティ機能に通知されます。着信パスでは、MAC 認証バイパス機能はどのポート セキュリティ機能よりも先に開始します。
- 補助 VLAN — MAC 認証バイパスは、補助（音声）VLAN でサポートされます。MAC 認証バイパスは、ポート VLAN 上でのみ表示される MAC アドレスに制限されます。Cisco Discovery Protocol（CDP）を介して学習されるすべての IP Phone MAC アドレスは、補助 VLAN 上で許可されます。
- Dynamic ARP Inspection（DAI）— MAC 認証バイパスと連動します。
- VLAN Management Policy Server（VMPS; VLAN マネジメント ポリシー サーバ）— MAC 認証バイパスおよび VMPS を同時に使用することはできません。CLI により、同時に両方の機能を設定できないようにされます。
- LAN ポート IP — MAC 認証バイパスと LAN ポート IP の両方を設定する場合、先に MAC 認証バイパスが実行されます。認証後、MAC 認証バイパス機能が LAN ポート IP 機能のトリガーとなります。LAN ポート IP 例外リスト内のホストは、MAC 認証バイパス（設定されている場合）による認証後、アクセスできるようになります。
- Web ベース プロキシ認証 — インターフェイスで MAC 認証バイパスと Web ベース プロキシ認証の両方が設定されている場合、MAC 認証バイパスはレイヤ 2 の機能であるため、Web ベース プロキシ認証より先に MAC 認証バイパスが開始します。レイヤ 2 の機能は常に、レイヤ 3 の機能よりも先に試行されます。
- RADIUS アカウンティング — RADIUS アカウンティングがサポートされます。

- SNMP（簡易ネットワーク管理プロトコル）— 必要な Set および Get 要求はすべて、SNMP にエクスポートされます。MAC 認証バイパスに対する SNMP サポートは、今後のソフトウェア リリースで対応する予定です。
- ハイ アベイラビリティ — ハイ アベイラビリティがサポートされます。ポートの MAC 認証バイパス の開始ステートと終了ステート（許可および無許可）は、スタンバイ スーパバイザ エンジンに同期化されます。中間ステートは、同期化されません。

MAC 認証バイパスの設定

ここでは、MAC 認証バイパスを設定する手順について説明します。

MAC 認証バイパスのグローバルなイネーブル化およびディセーブル化

デフォルトの設定はディセーブルです。MAC 認証バイパスをグローバルにイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
MAC 認証バイパスをグローバルにイネーブルまたはディセーブルにします。	**set mac-auth-bypass {disable | enable}**

次に、MAC 認証バイパスをグローバルにイネーブルにする例を示します。

```
Console> (enable) set mac-auth-bypass enable
Mac-Auth-Bypass enabled globally.
Console> (enable)
```

ポート上での MAC 認証バイパスのイネーブル化およびディセーブル化

ポート上で MAC 認証バイパスをイネーブルまたはディセーブルにする場合、同じポート上の PortFast も自動的にイネーブルまたはディセーブルになります。デフォルトでは、イネーブルです。

ポートで MAC 認証バイパスをイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
ポート上で MAC 認証バイパスをイネーブルまたはディセーブルにします。	**set port mac-auth-bypass** *mod/port* {**disable** | **enable**}

次に、ポートで MAC 認証バイパスをイネーブルにする例を示します。

```
Console> (enable) set port mac-auth-bypass 3/1 enable
MAC-Auth-Bypass successfully enabled on 3/1.
Console> (enable)
```

ポートの MAC 認証バイパス ステートの初期化

ポートの MAC 認証バイパス ステートを初期化して、ポートが再度認証を行えるようにするには、イネーブル モードで次の作業を実行します。

作業	コマンド
ポートの MAC 認証バイパス ステートを初期化して、ポートが再度認証を行えるようにします。	**set port mac-auth-bypass** *mod/port* **initialize**

次に、ポートの MAC 認証バイパス ステートを初期化して、ポートが再度認証を行えるようにする例を示します。

```
Console> (enable) set port mac-auth-bypass 3/1 initialize
Mac-Auth-Bypass successfully Initialized 3/1.
Console> (enable)
```

ポートの MAC アドレスの再認証

ポートの MAC アドレスを再認証するには、イネーブル モードで次の作業を行います。

作業	コマンド
ポートの MAC アドレスを再認証します。	**set port mac-auth-bypass** *mod/port* **reauthenticate**

次に、ポートの MAC アドレスを再認証する例を示します。

```
Console> (enable) set port mac-auth-bypass 3/1 reauthenticate
Reauthenticating MAC address 00-00-00-00-00-01 on port 3/1 using Mac-Auth-Bypass.
Console> (enable)
```

シャットダウン タイムアウト時間の指定

ポート上でセキュリティ違反があった場合、ポートはシャット ダウンされます。ポートが自動的に再イネーブル化されるまでのシャット ダウン時間（秒）を指定するには、グローバルな **set mac-auth-bypass shutdown-timeout** *seconds* コマンドを使用します。範囲は、30 ～ 65535 秒です。デフォルトは 60 秒です。シャットダウン タイムアウト時間を 0 秒に指定すると、自動ポート イネーブル機能がディセーブルとなり、手動でポートを再イネーブル化する必要があります。

シャットダウン タイムアウト時間を指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
シャットダウン タイムアウト時間を指定します。	**set mac-auth-bypass shutdown-timeout** *seconds*

次に、シャットダウン タイムアウト時間を指定する例を示します。

```
Console> (enable) set mac-auth-bypass shutdown-timeout 40
Shutdown Timeout set to 40 seconds.
Console> (enable)
```

認証失敗タイムアウト時間の指定

グローバルな **set mac-auth-bypass auth-fail-timeout** *seconds* コマンドにより、ポートが再認証を試行するまで認証失敗（AuthFail）ステートで待機する時間（秒）を指定できます。範囲は、5 ～ 65535 秒です。デフォルトの設定は 60 秒です。

認証失敗タイムアウト時間を指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
認証失敗タイムアウト時間を指定します。	**set mac-auth-bypass auth-fail-timeout** *seconds*

次に、認証失敗タイムアウト時間を指定する例を示します。

```
Console> (enable) set mac-auth-bypass auth-fail-timeout 60
Authfail Timeout set to 60 seconds.
Console> (enable)
```

再認証タイムアウト時間の指定

グローバルな **set mac-auth-bypass reauth-timeout** *seconds* コマンドにより、グローバルな再認証がイネーブルとなってから、再認証がトリガーされるまでの時間（秒）を指定できます。範囲は、300 ～ 65535 秒です。デフォルトの設定は 3600 秒です。

再認証タイムアウト時間を指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
再認証タイムアウト時間を指定します。	**set mac-auth-bypass reauth-timeout** *seconds*

次に、再認証タイムアウト時間を指定する例を示します。

```
Console> (enable) set mac-auth-bypass reauth-timeout 400
Reauth Timeout set to 400 seconds.
Console> (enable)
```

再認証のイネーブル化またはディセーブル化

グローバルな **set mac-auth-bypass re-authentication** コマンドをイネーブルにすると、すべての MAC 認証バイパス値がデフォルトに戻ります。デフォルトの設定はディセーブルです。

MAC 認証バイパス再認証をグローバルにイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
MAC 認証バイパス再認証をグローバルにイネーブルまたはディセーブルにします。	**set mac-auth-bypass reauthentication {disable | enable}**

次に、MAC 認証バイパス再認証をグローバルにイネーブルにする例を示します。

```
Console> (enable) set mac-auth-bypass reauthentication enable
Global reauthentication mode enabled.
Console> (enable)
```

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発生すると、ポートは制限モードになるか、またはシャット ダウンされます。制限モードでは、セキュリティ違反の原因となる MAC アドレスが、トラップ エントリとしてフォワーディング テーブルに追加されます。デフォルトの設定はシャットダウンです。

セキュリティ違反モードをグローバルに指定するには、イネーブル モードで次の作業を行います。

作業	コマンド
セキュリティ違反モードをグローバルに指定します。	**set mac-auth-bypass violation {restrict | shutdown}**

次に、セキュリティ違反モードで [restricted] を指定する例を示します。

```
Console> (enable) set mac-auth-bypass violation restrict
Mac-Auth-Bypass security violation mode set to restrict.
Console> (enable)
```

MAC 認証バイパス RADIUS アカウンティングのイネーブル化またはディセーブル化

デフォルトの設定はディセーブルです。MAC 認証バイパス RADIUS アカウンティングをイネーブルまたはディセーブルにするには、イネーブル モードで次の作業を行います。

作業	コマンド
MAC 認証バイパス RADIUS アカウンティングをイネーブルまたはディセーブルにします。	**set mac-auth-bypass radius-accounting {disable | enable}**
MAC 認証バイパス RADIUS アカウンティングステートを確認します。	**show mac-auth-bypass config**

次に、MAC 認証バイパス RADIUS アカウンティングをイネーブルにする例を示します。

```
Console> (enable) set mac-auth-bypass radius-accounting enable
Radius Accounting for MacAuth enabled.
Console> (enable)
```

次に、MAC 認証バイパス RADIUS アカウンティング ステートを確認する例を示します。

```
Console> (enable) show mac-auth-bypass config
Mac-Auth-Bypass Global Config
-----------------------------
Mac-Auth-Bypass Status      = Enabled
AuthFail Timeout            = 60
RadiusAccounting            = Enabled
Reauthentication            = Disabled
Reauth Timeout              = 3600
Shutdown Timeout            = 60
Violation mode              = Shutdown
Console> (enable)
```

MAC 認証バイパス情報の表示

show port mac-auth-bypass {*mod/port*} コマンドにより、ポート ステート（認証、認証済み、送信元 MAC アドレス学習の待機など）、およびポートの RADIUS サーバ指定の VLAN が表示されます。

MAC 認証バイパス情報を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
MAC 認証バイパスがイネーブルなスイッチ上のすべてのポートまたは単一のポートの MAC 認証バイパス情報を表示します。	**show port mac-auth-bypass** [*mod/port*]
MAC 認証バイパスがイネーブルなスイッチ上のすべてのポートまたは指定の MAC アドレスを持つポートの MAC 認証バイパス情報を表示します。	**show mac-auth-bypass** {**all** | **config** | *mac_address*}

次に、ポート 5/1 の MAC 認証バイパス情報を表示する例を示します。

```
Console> (enable) show port mac-auth-bypass 5/1
Port  Mac-Auth-Bypass State MAC Address       Auth-State     Vlan
----- --------------------- ----------------- -------------- -----
 5/1  Disabled              -                 -              1

Port  Termination action Session Timeout Shutdown/Time-Left
----- ------------------ --------------- ------------------
 5/1  -                  3600            -        -
Console> (enable)
```

次に、MAC 認証バイパスがイネーブルなスイッチ上のすべてのポートの MAC 認証バイパス情報を表示する例を示します。

```
Console> (enable) show mac-auth-bypass all

Port  Mac-Auth-Bypass State MAC Address       Auth-State     Vlan
----- --------------------- ----------------- -------------- -----
 5/1  Disabled              -                 -              1
 5/2  Enabled               00-00-00-00-00-00 waiting        1
 5/3  Enabled               00-00-00-00-00-00 waiting        1
 5/4  Enabled               00-00-00-00-00-00 waiting        1
 5/5  Enabled               00-00-00-00-00-00 waiting        1
 5/6  Enabled               00-00-00-00-00-00 waiting        1
 5/7  Enabled               00-00-00-00-00-00 waiting        1
 5/8  Enabled               00-00-00-00-00-00 waiting        1
.
.
.
Port  Termination action Session Timeout Shutdown/Time-Left
----- ------------------ --------------- ------------------
 5/1  -                  3600            -        -
 5/2  reauthenticate     3600            NO       -
 5/3  reauthenticate     3600            NO       -
 5/4  reauthenticate     3600            NO       -
 5/5  reauthenticate     3600            NO       -
 5/6  reauthenticate     3600            NO       -
 5/7  reauthenticate     3600            NO       -
 5/8  reauthenticate     3600            NO       -
.
.
.
Console> (enable)
```

MAC 認証バイパスのグローバル設定の表示

show mac-auth-bypass config コマンドにより、MAC 認証バイパスのグローバルな設定値（タイマー値、違反モード、グローバル再認証モードなど）が表示されます。

MAC 認証バイパスのグローバルな設定値を表示するには、ユーザ モードで次の作業を行います。

作業	コマンド
MAC 認証バイパスのグローバルな設定値を表示します。	**show mac-auth-bypass** {**all** | **config** | *mac_address*}

次に、MAC 認証バイパスのグローバルな設定値を表示する例を示します。

```
Console> (enable) show mac-auth-bypass config
Mac-Auth-Bypass Global Config
-----------------------------
Mac-Auth-Bypass Status      = Enabled
AuthFail Timeout            = 60
RadiusAccounting            = Enabled
Reauthentication            = Disabled
Reauth Timeout              = 3600
Shutdown Timeout            = 60
Violation mode              = Shutdown
Console> (enable)
```