Cisco IOS セキュリティ コマンド リファレンス：コマンド S から Z、Cisco IOS XE Release 3SE（Catalyst 3850 スイッチ）

初版：2013 年 01 月 11 日

最終更新：2013 年 01 月 11 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

sa ipsec から sessions maximum まで

server_（Diameter）

Diameter サーバを Diameter 認証、許可、アカウンティング（AAA）サーバ グループに関連付けるには、Diameter サーバ グループ コンフィギュレーション サブモードで **server** コマンドを使用します。 サーバ グループからサーバを削除するには、このコマンドの **no** 形式を入力します。

server *name*

no server *name*

構文の説明

name	Diameter サーバ名の指定に使用する文字列。 （注） このコマンドに指定した名前は、**diameter peer** コマンドを使用して定義した Diameter ピアの名前と一致する必要があります。

コマンド デフォルト

Diameter AAA サーバ グループに関連付けられているサーバはありません。

コマンド モード

Diameter サーバ グループ 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
12.4(9)T	このコマンドが導入されました。

使用上のガイドライン

server コマンドを使用して、Diameter サーバを Diameter サーバ グループに関連付けることができます。

例

次に、Diameter サーバを Diameter サーバ グループに関連付ける例を示します。

```
Router (config-sg-diameter)# server
 dia_peer_1
```

関連コマンド

コマンド	説明
aaa accounting	課金またはセキュリティ目的のために、要求されたサービスのAAAアカウンティングをイネーブルにします。
aaa authentication login	ログイン時の AAA 認証を設定します。
aaa authorization	ネットワークへのユーザアクセスを制限するパラメータを設定します。
aaa group server diameter	Diameter 用のサーバ グループを設定します。

server（RADIUS）

グループ サーバに対して、RADIUS サーバの IP アドレスを設定するには、サーバグループ コンフィギュレーション モードで **server** コマンドを使用します。 関連付けられたサーバを認証、許可、アカウンティング（AAA）グループ サーバから削除するには、このコマンドの **no** 形式を使用します。

server *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

no server *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

構文の説明

ip-address	RADIUS サーバ ホストの IP アドレスです。
auth-port *port-number*	（任意）認証要求に対するユーザデータグラム プロトコル（UDP）宛先ポートを指定します。 port-number 引数は、認証要求に対するポート番号を指定します。 この値が 0 に設定されている場合、そのホストは認証に使用されません。
acct-port *port-number*	（任意）アカウンティング要求に対する UDP 宛先ポートを指定します。 port number 引数は、アカウンティング要求に対するポート番号を指定します。 この値が 0 に設定されている場合、そのホストはアカウンティング サービスに使用されません。

コマンド デフォルト

ポート属性が定義されていない場合、デフォルトは次のようになります。

- 認証ポート：1645
- アカウンティング ポート：1646

コマンド モード

サーバグループ 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
12.0(5)T	このコマンドが導入されました。

リリース	変更内容
12.0(7)T	次の新しいキーワードと引数が追加されました。 • **auth-port** *port-number* • **acct-port** *port-number*
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。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。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。

使用上のガイドライン

server コマンドを使用して、特定のサーバを定義済みのグループ サーバに関連付けることができます。 サーバを識別する方法は、AAA サービスを提供する方法に応じて 2 種類あります。 IP アドレスを使用して単純にサーバを識別する方法と、オプションの **auth-port** キーワードおよび **acct-port** キーワードを使用して複数のホスト インスタンスまたはエントリを識別する方法があります。

オプションのキーワードを使用すると、ネットワーク アクセス サーバにより、IPアドレスと特定の UDP ポート番号に基づいてグループ サーバに関連付けられている RADIUS セキュリティ サーバおよびホスト インスタンスが識別されます。 IPアドレスとUDPポート番号の組み合わせによって一意の ID を作成し、特定の AAA サービスを提供する RADIUS ホスト エントリとして各ポートを個々に定義できます。 1 台の RADIUS サーバ上にある異なる 2 つのホスト エントリが 1 つのサービス（アカウンティングなど）に設定されている場合、設定されている 2 番目のホスト エントリは最初のホスト エントリのフェールオーバー バックアップとして動作します。 この例の場合、最初のホストエントリがアカウンティング サービスの提供に失敗すると、同じデバイスに設定されている 2 番めのホスト エントリを使用してアカウンティング サービスを提供するように、ネットワーク アクセス サーバが試行します （試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

例

例

次に、同じ IP アドレスを持つ複数の RADIUS ホスト エントリを認識する、ネットワーク アクセス サーバの例を示します。 同じ RADIUS サーバ上にある 2 つのホスト エントリは、同じサービス（認証とアカウンティング）のために設定されています。 設定されている 2 番めのホスト エントリは、1 番めのエントリのフェールオーバー バックアップとして動作します （試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

```
! This command enables AAA.
aaa new-model
```

```
! The next command configures default RADIUS parameters.
aaa authentication ppp default radius
! The next set of commands configures multiple host entries for the same IP address.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 2000 acct-port 2000
```

例

次の例では、ネットワーク アクセス サーバは異なる 2 つの RADIUS グループ サーバを認識するように設定されます。 一方のグループである group1 には、同じ RADIUS サーバ上に同じサービス用に設定された 2 つのホスト エントリがあります。 設定されている 2 番めのホスト エントリは、1 番めのエントリのフェールオーバー バックアップとして動作します

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group group1
! The following commands define the group1 RADIUS group server and associates servers
! with it.
aaa group server radius group1
   server 172.20.0.1 auth-port 1000 acct-port 1001
! The following commands define the group2 RADIUS group server and associates servers
! with it.
aaa group server radius group2
   server 172.20.0.1 auth-port 2000 acct-port 2001
! The following set of commands configures the RADIUS attributes for each host entry
! associated with one of the defined group servers.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.31.0.1 auth-port 1645 acct-port 1646
```

関連コマンド

コマンド	説明
aaa group server	各種のサーバホストを別個のリストと別個の方式にグループ化します。
aaa new-mode l	AAA アクセス コントロール モデルをイネーブルにします。
radius-server host	RADIUS サーバ ホストを指定します。

server name（IPv6 TACACS+）

IPv6 TACACS+ サーバを指定するには、TACACS+ グループ サーバ コンフィギュレーション モードで **server name** コマンドを使用します。 コンフィギュレーションから IPv6 TACACS+ サーバを削除するには、このコマンドの **no** 形式を使用します。

server name *server-name*

no server name *server-name*

構文の説明

server-name	使用する IPv6 TACACS+ サーバ。

コマンド デフォルト

サーバ名は指定されていません。

コマンド モード

TACACS+ グループ サーバ コンフィギュレーション（config-sg-tacacs+）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2S	このコマンドが導入されました。

使用上のガイドライン

このコマンドを設定する前に、**aaa group server tacacs** コマンドを設定する必要があります。

IPv6 TACACS+ サーバを指定するには、**server name** コマンドを入力します。

例

次に、server1 という名前の IPv6 TACACS+ サーバを指定する例を示します。

```
Router(config)# aaa group server tacacs+
Router(config-sg-tacacs+)# server name server1
```

関連コマンド

コマンド	説明
aaa group server tacacs	IPv6 または IPv4 に対して TACACS+ サーバを設定して、TACACS+ サーバ コンフィギュレーション モードを開始します。

server-private（RADIUS）

グループ サーバに対して、プライベート RADIUS サーバの IP アドレスを設定するには、サーバ グループ コンフィギュレーション モードで **server-private** コマンドを使用します。 関連付けられたプライベート サーバを認証、許可、アカウンティング（AAA）グループ サーバから削除するには、このコマンドの **no** 形式を使用します。

server-private *ip-address* [**auth-port** *port-number*| **acct-port** *port-number*] **[non-standard]** [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

no server-private *ip-address* [**auth-port** *port-number*| **acct-port** *port-number*] **[non-standard]** [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

構文の説明

ip-address	プライベート RADIUS サーバ ホストの IP アドレス。
auth-port *port-number*	（任意）認証要求に対するユーザ データグラム プロトコル（UDP）宛先ポート。 デフォルト値は 1645 です。
acct-port *port-number*	（任意）アカウンティング要求用の UDP 宛先ポート。 デフォルト値は 1646 です。
non-standard	（任意）RADIUS サーバは、ベンダー固有の RADIUS 属性を使用しています。
timeout *seconds*	（任意）ルータが RADIUS サーバの応答を待機し、再送信するまでの時間間隔（秒単位）です。 この設定は、radius-server timeout コマンドのグローバル値を上書きします。 タイムアウト値が指定されていない場合は、グローバル値が使用されます。
retransmit *retries*	（任意）サーバが応答しない、または応答が遅い場合に、そのサーバに RADIUS 要求を再送信する回数。 この設定は、radius-server retransmit コマンドのグローバル値を上書きします。
key *string*	（任意）ルータと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用される認証および暗号キー。 このキーは、radius-server key コマンドのグローバル値を上書きします。 キー文字列を指定しない場合、グローバル値が使用されます。

コマンド デフォルト

server-private パラメータが指定されていない場合、グローバル コンフィギュレーションが使用されます。グローバル コンフィギュレーションが指定されていない場合、デフォルト値が使用されます。

コマンド モード

サーバグループ 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
12.2(1)DX	このコマンドが Cisco 7200 シリーズおよび Cisco 7401ASR に導入されました。
12.2(2)DD	このコマンドが、Cisco IOS Release 12.2(2)DD に統合されました。
12.2(4)B	このコマンドが Cisco IOS Release 12.2(4)B に組み込まれました。
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(33)SRC	このコマンドが、Cisco IOS Release 12.2(33)SRC に統合されました。
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。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI に統合されました。

使用上のガイドライン

server-private コマンドを使用して、特定のプライベート サーバを定義済みのサーバ グループに関連付けることができます。 Virtual Route Forwarding（VRF）間でのプライベート アドレスの重複を防止するために、プライベート サーバ（プライベート アドレスを持つサーバ）をサーバ グループ内に定義し、他のグループからは見えない状態にしておくことができます。この場合も、グローバル プール（デフォルトの「radius」サーバ グループ）にあるサーバは、IP アドレスとポート番号で参照できます。 このように、サーバ グループ内のサーバのリストには、グローバル コンフィギュレーションにおけるホストの参照情報とプライベート サーバの定義が含まれます。

（注） **radius-server directed-request** コマンドが設定されている場合、**server-private**（RADIUS）コマンドを設定して、プライベート RADIUS サーバをグループ サーバとして使用することはできません。

例

次に、sg_water RADIUS グループ サーバを定義し、これにプライベート サーバを関連付ける例を示します。

```
aaa group server radius sg_water
 server-private 10.1.1.1 timeout 5 retransmit 3 key xyz
 server-private 10.2.2.2 timeout 5 retransmit 3 key xyz
```

関連コマンド

コマンド	説明
aaa group server	各種のサーバ ホストを別個のリストと別個の方式にグループ化します。
aaa new-mode l	AAA アクセス コントロール モデルをイネーブルにします。
radius-server host	RADIUS サーバ ホストを指定します。
radius-server directed-request	ユーザが Cisco Network Access Server（NAS）にログインし、認証に RADIUS サーバを選択することを許可します。

server-private（TACACS+）

グループ サーバに対して、プライベート TACACS+ サーバの IPv4 または IPv6 アドレスを設定するには、サーバグループ コンフィギュレーション モードで **server-private** コマンドを使用します。関連付けられたプライベート サーバを認証、許可、アカウンティング（AAA）グループ サーバから削除するには、このコマンドの **no** 形式を使用します。

server-private {*ip-address*| *name*| *ipv6-address*} **[nat] [single-connection]** [**port** *port-number*] [**timeout** *seconds*] [**key** [**0**| **7**] *string*]

no server-private

構文の説明

ip-address	プライベート RADIUS または TACACS+ サーバ ホストの IP アドレス。
name	プライベート RADIUS または TACACS+ サーバ ホストの名前。
ipv6-address	プライベート RADIUS または TACACS+ サーバ ホストの IPv6 アドレス。
nat	（任意）リモート デバイスのポート ネットワーク アドレス変換（NAT）アドレスを指定します。このアドレスは TACACS+ サーバに送信されます。
single-connection	（任意）ルータと TACACS+ サーバ間で単一のオープンな接続を保守します。
port *port-number*	（任意）サーバのポート番号を指定します。この設定によって、デフォルトのポート 49 は上書きされます。
timeout *seconds*	（任意）タイムアウト値を指定します。この値によって、**tacacs-server timeout** コマンドで設定したグローバル タイムアウト値がこのサーバに限り上書きされます。

key [**0** | **7**]	（任意）認証および暗号キーを指定します。このキーは TACACS+ デーモンで使用されるキーと一致する必要があります。このキーを指定すると、このサーバに限り、グローバル **tacacs-server key** コマンドで設定されているキーが上書きされます。 • 番号が入力されていないか、0 が入力されている場合、入力されたストリングはプレーン テキストであると見なされます。7 が入力されている場合、入力されたストリングは暗号化テキストであると見なされます。
string	（任意）認証および暗号キーを指定する文字列。

コマンド デフォルト

server-private パラメータが指定されていない場合、グローバル コンフィギュレーションが使用されます。グローバル コンフィギュレーションが指定されていない場合、デフォルト値が使用されます。

コマンド モード

サーバグループ コンフィギュレーション（server-group）

コマンド履歴

リリース	変更内容
12.3(7)T	このコマンドが導入されました。
12.2(33)SRA1	このコマンドが、Cisco IOS Release 12.2(33)SRA1 に統合されました。
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。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI に統合されました。
12.2(54)SG	このコマンドが、Cisco IOS Release 12.2(54)SG に統合されました。
Cisco IOS XE Release 3.2S	このコマンドが変更されました。 引数 *ipv6-address* が追加されました。

使用上のガイドライン

server-private コマンドを使用して、特定のプライベート サーバを定義済みのサーバ グループに関連付けることができます。 Virtual Route Forwarding（VRF）間でのプライベート アドレスの重複を防止するために、プライベート サーバ（プライベート アドレスを持つサーバ）をサーバ グループ内に定義し、他のグループからは見えない状態にしておくことができます。この場合も、グローバル プール（デフォルトの「TACACS+」サーバ グループ）にあるサーバは、IP アドレスとポート番号で参照できます。このように、サーバ グループ内のサーバのリストには、グローバル コンフィギュレーションにおけるホストの参照情報とプライベート サーバの定義が含まれます。

例

次に、tacacs1 TACACS+ グループ サーバを定義し、これにプライベート サーバを関連付ける例を示します。

```
aaa group server tacacs+ tacacs1
    server-private 10.1.1.1 port 19 key cisco
  ip vrf cisco
   rd 100:1
  interface Loopback0
   ip address 10.0.0.2 255.0.0.0
   ip vrf forwarding cisco
```

関連コマンド

コマンド	説明
aaa group server	各種のサーバ ホストを別個のリストと別個の方式にグループ化します。
aaa new-mode l	AAA アクセス コントロール モデルをイネーブルにします。
ip tacacs source-interface	すべての発信 TACACS+ パケットに対して、指定されたインターフェイスの IP アドレスを使用します。
ip vrf forwarding（**server-group**）	AAA RADIUS または TACACS+ サーバ グループの VRF 参照を設定します。
tacacs-server host	TACACS+ サーバ ホストを指定します。

service password-encryption

パスワードを暗号化するには、グローバル コンフィギュレーション モードで **service password-encryption** コマンドを使用します。 デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

service password-encryption

no service password-encryption

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

パスワードは暗号化されません。

コマンド モード

グローバル 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
10.0	このコマンドが導入されました。
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。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。 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。
12.2(33)SB	このコマンドが、Cisco IOS Release 12.2(33)SB に統合されました。

使用上のガイドライン

実際の暗号化プロセスは、現在の設定が保存されるとき、またはパスワードが設定されるときに行われます。 パスワードの暗号化は、ユーザ名パスワード、認証キーパスワード、特権コマンドパスワード、コンソールおよび仮想端末回線アクセスパスワード、およびボーダーゲートウェイプロトコル ネイバー パスワードを含む、すべてのパスワードに適用されます。 このコマンドは、主に未許可ユーザがコンフィギュレーション ファイル内のパスワードを閲覧するのを防ぐために役立ちます。

パスワードの暗号化をイネーブルにした場合、**more system:running-config** コマンドを入力すると、パスワードの暗号化された形式が表示されます。

注意 このコマンドでは、高レベルのネットワーク セキュリティは確保されません。 このコマンドを使用する場合は、その他のネットワーク セキュリティ手段も講じる必要があります。

（注） 暗号化パスワードを忘れた場合、回復はできません。 NVRAM を消去し、新しいパスワードを設定する必要があります。

例

次に、パスワードの暗号化を実行する例を示します。

```
service password-encryption
```

関連コマンド

コマンド	説明
enable password	さまざまな権限レベルへのアクセスを制御するローカル パスワードを設定します。
key-string（認証）	キーの認証文字列を指定します。
neighbor password	2 つの BGP ピアの間の TCP 接続で MD5 認証をイネーブルにします。

service password-recovery

パスワード回復機能をイネーブルにするには、グローバル コンフィギュレーション モードで **service password-recovery** コマンドを使用します。 パスワード回復機能をディセーブルにするには、**no service password-recovery** コマンドを使用します。

service password-recovery

no service password-recovery

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

パスワード回復機能はイネーブルです。

コマンド モード

グローバル 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(8)YA	このコマンドが導入されました。
12.3(14)T	このコマンドが、Cisco IOS Release 12.3(14)T に統合されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

使用上のガイドライン

（注） このコマンドは、一部のプラットフォームでは使用できません。 Feature Navigator を使用して、お使いのプラットフォームで使用できるかどうかを確認してください。

no service password-recovery コマンドを使用してパスワード回復機能をディセーブルにする場合は、デバイスとは別の場所にシステム コンフィギュレーション ファイルのコピーを保存しておくことを推奨します。 VTP トランスペアレント モードで動作するデバイスを使用している場合、デバイスとは別の場所に、vlan.dat ファイルのコピーを保存することも推奨しています。

⚠

注意 no **service password-recovery** コマンドをコマンドラインに入力すると、パスワード回復がディセーブルになります。 パスワード回復機能をサポートしないイメージにダウングレードする場合は、ダウングレード後はパスワードを回復できなくなるため、ダウングレード前にこのコマンドをディセーブルにしてください。

このコマンドが設定されているときに、ROMMON を開始する方法をなくすため、コンフィギュレーション レジスタ ブート ビットをイネーブルにする必要があります。 Cisco IOS ソフトウェアは、ユーザによるコンフィギュレーション レジスタのブート フィールドの設定を防止する必要があります。

スタートアップ コンフィギュレーションを無視するビット 6、およびブレークをイネーブルにするビット 8 を設定する必要があります。

ルータの起動中は、Break キーをディセーブルにし、この機能をイネーブルにしている場合は、Cisco IOS ソフトウェアでディセーブルにする必要があります。

no service password-recovery コマンドを入力する前に、**config-register** グローバル コンフィギュレーション コマンドを使用して、コンフィギュレーション レジスタが自動的に起動するようにしておくことが必要な場合もあります。 **show version** EXEC コマンドの最後の行は、コンフィギュレーション レジスタの設定を表示します。 **show version** EXEC コマンドを使用して現在のコンフィギュレーション レジスタ値を取得し、必要に応じて **config-register** コマンドを使用してルータが自動起動するように設定してから、**no service password-recovery** コマンドを入力します。

ディセーブルにすると、**no service password-recovery** コマンドでは次のコンフィギュレーション レジスタ値が無効になります。

- 0x0
- 0x2002（ビット 8 制限）
- 0x0040（ビット 6）
- 0x8000（ビット 15）

Catalyst スイッチ動作

パスワード回復メカニズムを再度イネーブル（デフォルト）にするには、**service password-recovery** コマンドを使用します。 このメカニズムでは、スイッチに物理的にアクセスするユーザは、スイッチの電源投入時に Mode ボタンを押してブート プロセスを中断し、新しいパスワードを割り当てることができます。 パスワード回復機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

パスワード回復メカニズムがディセーブルになると、ユーザがシステムをデフォルト設定に戻すことに同意した場合だけ、ブート プロセスを中断できます。 スイッチでパスワード回復がイネーブルか、ディセーブルかを確認するには、**show version** EXEC コマンドを使用します。

service password-recovery コマンドは、Catalyst 3550 ファスト イーサネット スイッチでだけ有効です。ギガビット イーサネット スイッチでは使用できません。

例

例

次に、（この例では自動起動に設定されている）コンフィギュレーション レジスタ設定を取得し、パスワード回復機能を無効にしてから、設定がシステムのリロード後も維持されることを確認する方法の例を示します。 **noconfirm** キーワードは、確認プロンプトにより起動プロセスが中断することを防止します。

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 5300 Software (C7200-P-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Wed 05-Mar-03 10:16 by xxx
Image text-base: 0x60008954, data-base: 0x61964000
ROM: System Bootstrap, Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
BOOTLDR: 7200 Software (C7200-KBOOT-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
Router uptime is 10 minutes
System returned to ROM by reload at 16:28:11 UTC Thu Mar 6 2003
.
.
.
125440K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
8192K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x2012
Router# configure terminal
Router(config)# no service password-recovery noconfirm
WARNING:
Executing this command will disable the password recovery mechanism.
Do not execute this command without another plan for password recovery.
Are you sure you want to continue? [yes/no]: yes
.
.
.
Router(config)# exit
Router#
Router# reload
Proceed with reload? [confirm] yes
00:01:54: %SYS-5-RELOAD: Reload requested
System Bootstrap, 12.3(8)YA...
Copyright (c) 1994-2004 by cisco Systems, Inc.
C7400 platform with 262144 Kbytes of main memory
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
.
.
.
```

次に、中断を確定する場合と、中断を確定しない場合に生じる状態を示します。

例

```
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
program load complete, entry point: 0x80013000, size: 0x8396a8
Self decompressing the image :
################################################################################################################################
 [OK] !The 5-second window starts.
telnet> send break
              Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
Cisco Systems, Inc.
```

```
170 West Tasman Drive
San Jose, California 95134-1706
Cisco IOS Software, C831 Software (C831-K9O3SY6-M), Version 12.3(8)YA
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Fri 13-Aug-04 03:21
Image text-base: 0x80013200, data-base: 0x81020514
PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to factory default configuration and proceed [y/n]?
!The user enters "y" here.
Reset router configuration to factory default.
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use encryption.
 Importers, exporters, distributors and users are responsible for compliance with U.S. and
 local country laws. By using this product you agree to comply with applicable laws and
regulations. If you are unable to comply with U.S. and local laws, return this product
immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
Cisco C831 (MPC857DSL) processor (revision 0x00) with 46695K/2457K bytes of memory.
Processor board ID 0000 (1314672220), with hardware revision 0000 CPU rev number 7
3 Ethernet interfaces
4 FastEthernet interfaces
128K bytes of NVRAM
24576K bytes of processor board System flash (Read/Write)
2048K bytes of processor board Web flash (Read/Write)
         --- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
!Start up config is erased.
SETUP: new interface FastEthernet1 placed in "up" state
SETUP: new interface FastEthernet2 placed in "up" state
SETUP: new interface FastEthernet3 placed in "up" state
SETUP: new interface FastEthernet4 placed in "up" state
Press RETURN to get started!
Router> enable
Router# show startup configuration
startup-config is not present
Router# show running-config | incl service
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption !The "no service password-recovery" is disabled.
==========================================================================================
```

例

```
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
telnet> send break
program load complete, entry point: 0x80013000, size: 0x8396a8
Self decompressing the image :
##################################################################################################################################################
 [OK]
telnet> send break
              Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Cisco IOS Software, C831 Software (C831-K9O3SY6-M), Version 12.3(8)YA
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Fri 13-Aug-04 03:21
Image text-base: 0x80013200, data-base: 0x81020514
PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to factory default configuration and proceed [y/n]?
!The user enters "n" here.
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
```

```
products does not imply third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for compliance with U.S. and
local country laws. By using this product you agree to comply with applicable laws and
regulations. If you are unable to comply with U.S. and local laws, return this product
immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
Cisco C831 (MPC857DSL) processor (revision 0x00) with 46695K/2457K bytes of memory.
Processor board ID 0000 (1314672220), with hardware revision 0000 CPU rev number 7
3 Ethernet interfaces
4 FastEthernet interfaces
128K bytes of NVRAM
24576K bytes of processor board System flash (Read/Write)
2048K bytes of processor board Web flash (Read/Write)
Press RETURN to get started! !The Cisco IOS software boots as if it is not interrupted.
Router> enable
Router# show startup configuration
Using 984 out of 131072 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service password-recovery
!
hostname Router
!
boot-start-marker
boot-end-marker
!
memory-size iomem 5
!
no aaa new-model
ip subnet-zero
!
ip ips po max-events 100
no ftp-server write-enable
!
interface Ethernet0
 no ip address
 shutdown
!
interface Ethernet1
 no ip address
 shutdown
 duplex auto
!
interface Ethernet2
 no ip address
 shutdown
!
interface FastEthernet1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet3
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet4
 no ip address
 duplex auto
 speed auto
!
```

```
ip classless
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
 no modem enable
 transport preferred all
 transport output all
line aux 0
line vty 0 4
!
scheduler max-task-time 5000
end
Router# show running-configuration | incl service
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service password-recovery
```

例

no service password-recovery コマンドは、ルータのコンフィギュレーション レジスタが自動起動するように設定されていることを想定しています。 **no service password-recovery** コマンドを入力する前に、コンフィギュレーション レジスタが自動起動以外に設定されている場合は、次の例のようなプロンプトが表示され、**config-register** グローバル コンフィギュレーション コマンドを使用して設定を変更するように促されます。

```
Router(config)# no service password-recovery
Please setup auto boot using config-register first.
```

（注） このコマンドの動作により、意図しない結果が生じることを回避するには、**show version** コマンドを使用して、現在のコンフィギュレーション レジスタ値を取得します。 自動起動に設定されていない場合、**no service password-recovery** コマンドを入力する前に、**config-register** コマンドを使用して、ルータを自動起動に設定する必要があります。

パスワード回復をディセーブルにすると、ビット パターン値を 0x40、0x8000、または 0x0（自動起動をディセーブル化）に設定できません。 次に、パスワード回復をディセーブルにしたルータで、無効なコンフィギュレーション レジスタ設定が試行された場合に表示されるメッセージの例を示します。

```
Router(config)# config-register 0x2143
Password recovery is disabled, cannot enable diag or ignore configuration.
```

コマンドは無効なビット パターンをリセットし、無関係なビット パターンの変更を許可し続けます。 コンフィギュレーション レジスタの値は次回のシステム リロード時に 0x3 にリセットされます。これは、**show version** コマンドの出力の最後の行をチェックすることで確認できます。

```
Configuration register is 0x2012 (will be 0x3 at next reload)
```

例

次の例では、スイッチ上でパスワード回復をディセーブルにする方法を示します。ユーザはデフォルト設定に戻すことに同意する場合のみパスワードをリセットできます。

```
Switch(config)# no service-password recovery
Switch(config)# exit
```

パスワード回復手順を実行する場合、スイッチに物理的にアクセスするユーザは、スイッチの電源投入時とポート 1X の上にある LED が消灯してから 1 ～ 2 秒後に Mode ボタンを押します。 ボタンを放すと、システムは初期化を続けます。 パスワード回復メカニズムがディセーブルの場合は、次のメッセージが表示されます。

```
The password-recovery mechanism has been triggered, but is currently disabled. Access to
the boot loader prompt through the password-recovery mechanism is disallowed at this point.
 However, if you agree to let the system be reset back to the default system configuration,
 access to the boot loader prompt can still be allowed.
Would you like to reset the system back to the default configuration (y/n)?
```

システムをデフォルト設定にリセットしないことを選択した場合は、**Mode** ボタンを押さないときと同じように、通常の起動プロセスが続行されます。 システムをデフォルト設定にリセットする場合、フラッシュ メモリ内のコンフィギュレーション ファイルが削除され、VLAN データベース ファイル flash:vlan.dat（存在する場合）が削除されます。

次に、パスワード回復がディセーブルのデバイスでの、**show version** コマンドの出力例を示します。

```
Switch# show version
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Wed 24-Oct-01 06:20 by xxx
Image text-base: 0x00003000, data-base: 0x004C1864
ROM: Bootstrap program is C3550 boot loader
flam-1-6 uptime is 1 week, 6 days, 3 hours, 59 minutes
System returned to ROM by power-on
Cisco WS-C3550-48 (PowerPC) processor with 65526K/8192K bytes of memory.
Last reset from warm-reset
Running Layer2 Switching Only Image
Ethernet-controller 1 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 2 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 3 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 4 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 5 has 1 Gigabit Ethernet/IEEE 802.3 interface
Ethernet-controller 6 has 1 Gigabit Ethernet/IEEE 802.3 interface
48 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
The password-recovery mechanism is disabled.
32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: AA:00:0B:2B:02:00
Configuration register is 0x10F
```

関連コマンド

コマンド	説明
config-register	コンフィギュレーション レジスタの設定を変更します。

コマンド	説明
show version	ハードウェアおよびファームウェアのバージョン情報を表示します。

set aggressive-mode client-endpoint から show content-scan まで

show aaa servers

AAA サーバ MIB によって解釈される、すべてのパブリックおよびプライベート認証、許可、アカウンティング（AAA）RADIUS サーバとの間で送受信されるパケットのステータスと数を表示するには、ユーザ EXEC または特権 EXEC モードで **show aaa servers** コマンドを使用します。

show aaa servers [**private**| **public**]

構文の説明

private	（任意）プライベート AAA サーバのみを表示します。AAA サーバ MIB によっても表示されます。
public	（任意）パブリック AAA サーバのみを表示します。AAA サーバ MIB によっても表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.2(6)T	このコマンドが導入されました。
12.3(7)T	このコマンドが、Cisco IOS Release 12.3(7)T に統合されました。
12.2(33)SRE	このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。
15.1(1)S	このコマンドが変更されました。 CISCO-AAA-SERVER-MIB のプライベート RADIUS サーバのサポートが追加されました。
15.1(4)M	このコマンドが変更されました。 CISCO-AAA-SERVER-MIB のプライベート RADIUS サーバのサポートが追加されました。
15.2(4)S1	このコマンドが変更されました。 コマンド出力に、未処理の、およびスロットルされたトランザクション（アクセスとアカウンティング）を概算で表示するサポートが追加されました。

使用上のガイドライン

show aaa servers コマンドでは、RADIUS サーバのみがサポートされます。

コマンドは、すべての AAA トランザクション タイプ（認証、許可、アカウンティング）で送受信されたパケットに関する情報を表示します。

例

次に、**show aaa servers private** コマンドの出力例を示します。 表示の最初の 4 行のみがプライベート RADIUS サーバの状態に関係するため、表示のこの部分の出力フィールドを次の表で説明します。

```
Router# show aaa servers private

RADIUS: id 24, priority 1, host 172.31.164.120, auth-port 1645, acct-port 1646
     State: current UP, duration 375742s, previous duration 0s
     Dead: total time 0s, count 0
     Quarantined: No
     Authen: request 5, timeouts 1, failover 0, retransmission 1
             Response: accept 4, reject 0, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 14ms
             Transaction: success 4, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Author: request 0, timeouts 0, failover 0, retransmission 0
             Response: accept 0, reject 0, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Account: request 5, timeouts 0, failover 0, retransmission 0
             Request: start 3, interim 0, stop 2
             Response: start 3, interim 0, stop 2
             Response: unexpected 0, server error 0, incorrect 0, time 12ms
             Transaction: success 5, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Elapsed time since counters last cleared: 4d8h22m
     Estimated Outstanding Access Transactions: 0
     Estimated Outstanding Accounting Transactions: 0
     Estimated Throttled Access Transactions: 0
     Estimated Throttled Accounting Transactions: 0
     Maximum Throttled Transactions: access 0, accounting 0
     Requests per minute past 24 hours:
             high - 8 hours, 22 minutes ago: 0
             low  - 8 hours, 22 minutes ago: 0
             average: 0
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *1*：*show aaa servers* のフィールドの説明

フィールド	説明
id	ルータに定義されているすべての AAA サーバの固有識別子。
priority	グループ内サーバの使用順序。
host	プライベート RADIUS サーバ ホストの IP アドレス。
auth-port	認証と許可要求に使用する AAA サーバの UDP 宛先ポート。 デフォルト値は 1645 です。

フィールド	説明
acct-port	アカウンティング要求に使用する AAA サーバの UDP 宛先ポート。 デフォルト値は 1646 です。
State	AAA サーバの現在の状態、同サーバがその状態を続けている時間（秒単位）、および同サーバが以前の状態を続けていた時間（秒単位）を示します。 次の状態が示されます。 • DEAD：サーバが現在ダウンしていること、およびフェールオーバーの際に同サーバがグループ内で最後に残ったサーバでなければ省略されることを示します。 • duration：サーバが現在の状態（UP または DEAD のいずれか）であると見なされる時間。 • previous duration：サーバが以前の状態にあったと見なされる時間。 • UP：サーバが現在稼働していると見なされ、そのサーバとの通信が試みられることを示します。
Dead	サーバが稼働していないとマークされた回数と、その状態にある時間を累積して秒単位で表します。

フィールド	説明
Authen	

フィールド	説明
	サーバと送受信した認証パケット、および成功または失敗した認証トランザクションに関する情報を提供します。 このフィールドでは、次の情報が報告されます。 • request：AAA サーバに送信された認証要求の数。 • timeouts：このサーバへの送信があった際に確認されたタイムアウト（応答なし）の数。 • Response：このサーバで確認された応答に関する統計情報。次のレポートが含まれます。 • unexpected：予期しない応答の数。 パケットのタイムアウト期間の期限を過ぎた後で受信された応答は、予期しないものと見なされます。 たとえば、サーバへのリンクが混雑している場合などに発生します。また、サーバが明確な理由なく応答を生成した場合も、予期しない応答が作成される場合があります。 • server error：サーバ エラーの数。 このカテゴリは、前のカテゴリのいずれにも当てはまらないエラー パケットの「キャッチオール」です。 • incorrect：不正な応答の数。 応答の形式が、プロトコルが予測するもの以外の不正な形式であれば、不正な応答と見なされます。 不正なサーバ キーがルータに設定されている場合に発生の可能性が高くなります。 • time：認証パケットに応答するために要した時間（ミリ秒単位）。 • Transaction：これらのフィールドは、サーバに関連する認証、許可、アカウンティング トランザクションに関する情報を提供します。 トランザクションは、AAA モジュール、または AAA クライアント (PPP

フィールド	説明
	など) によって AAA プロトコル (RADIUS またはTACACS+) に送信される認証情報、許可情報、またはアカウンティング情報の要求として定義されます。この場合、複数のパケット送信および再送信が行われる場合があります。 トランザクションでは、成功または失敗を確認するために 1 つのサーバグループ内の 1 つまたは複数のサーバへのパケット再送信が必要な場合があります。 成功または失敗は、RADIUS およびTACACS+プロトコルによって、次のように AAA に報告されます • success：トランザクションが成功すると増加します。 • failure：サーバグループの別のサーバへのパケット再送信が失敗または成功しなかった場合など、トランザクションが失敗すると増加します。 アクセス拒否など、アクセス要求に対する否定的な応答は、トランザクションの成功として見なされます。
Author	このカテゴリのフィールドは、Authen: フィールドと似ています。 ただし、作成者情報が RADIUS プロトコルの認証パケットで送信されるため、RADIUS を使用する場合これらのフィールドは増加しない点が大きく異なります。
Account	このカテゴリのフィールドは Authen: フィールドと似ていますが、アカウンティング トランザクションとパケットの統計情報を提供する点で異なります。
Elapsed time since counters last cleared	カウンタが最後にクリアされてから経過した日数、時間数、および分数を表示します。

（注） Intelligent Services Gateway（ISG）の場合、推定未完了アカウンティング トランザクションはゼロになるまでに時間がかかります。 これは、中間アカウンティング要求に常にチャーンがあるためです。

show aaa servers コマンド出力のフィールドは、Cisco AAA-SERVER-MIB の簡易ネットワーク管理プロトコル（SNMP）オブジェクトにマッピングされ、SNMP レポートで使用されます。 **show aaa servers** コマンドの出力例の最初の行（RADIUS: id 24, priority 1, host 172.31.164.120, auth-port 1645, acct-port 1646）は、次のように Cisco AAA-SERVER-MIB にマッピングされます。

- id は casIndex へマップ
- priority は casPriority へマップ
- host は casAddress へマップ
- auth-port は casAuthenPort へマップ
- acct-port maps は casAcctPort へマップ

Cisco AAA-SERVER-MIB マップにリストされている次のオブジェクトのセットを、**show aaa servers** コマンドで表示されるフィールドにマップすることは、より簡単です。たとえば、casAuthenRequests フィールドは、レポートの Authen: request 部分に対応し、casAuthenRequestTimeouts はレポートの Authen: timeouts 部分に対応します。以下も同様です。

- casAuthenRequests
- casAuthenRequestTimeouts
- casAuthenUnexpectedResponses
- casAuthenServerErrorResponses
- casAuthenIncorrectResponses
- casAuthenResponseTime
- casAuthenTransactionSuccesses
- casAuthenTransactionFailures
- casAuthorRequests
- casAuthorRequestTimeouts
- casAuthorUnexpectedResponses
- casAuthorServerErrorResponses
- casAuthorIncorrectResponses
- casAuthorResponseTime
- casAuthorTransactionSuccesses
- casAuthorTransactionFailures
- casAcctRequests

- casAcctRequestTimeouts
- casAcctUnexpectedResponses
- casAcctServerErrorResponses
- casAcctIncorrectResponses
- casAcctResponseTime
- casAcctTransactionSuccesses
- casAcctTransactionFailures
- casState
- casCurrentStateDuration
- casPreviousStateDuration
- casTotalDeadTime
- casDeadCount

選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を検索およびダウンロードするには、http://www.cisco.com/go/mibs にある MIB Locator を使用してください。

関連コマンド

コマンド	説明
radius-server dead-criteria	一方または両方の基準値（RADIUS サーバを停止状態としてマーキングするために使用）を、指定の定数値に強制的に設定します。
server-private	特定のプライベート RADIUS サーバを定義済みのサーバ グループに関連付けます。

show access-lists

現在のアクセス リストの内容を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show access-lists** コマンドを使用します。

show access-lists [*access-list-number*| *access-list-name*]

構文の説明

access-list-number	（任意）表示するアクセス リストの数です。デフォルトでは、システムによりすべてのアクセス リストが表示されます。
access-list-name	（任意）表示する IP アクセス リストの名前です。

コマンド デフォルト

システムは、すべてのアクセス リストを表示します。

コマンド モード

ユーザ EXEC 特権 EXEC

コマンド履歴

リリース	変更内容
10.0	このコマンドが導入されました。
12.0(6)S	出力でコンパイルされた ACL を識別できるように変更されました。
12.1(1)E	このコマンドが Cisco 7200 シリーズに実装されました。
12.1(5)T	コマンド出力でコンパイルされた ACL を識別できるように変更されました。
12.1(4)E	このコマンドが Cisco 7100 シリーズに実装されました。
12.2(2)T	コマンド出力に IPv6 アクセス リストの情報が表示されるように変更されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
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。

リリース	変更内容
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す。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。

使用上のガイドライン

show access-lists コマンドは、ルータで動作している現在の ACL を表示するために使用します。高速化された ACL として動作している各アクセス リストには、Compiled 表示を使用してフラグが付けられます。

この表示には、ACL 内の各エントリと一致したパケットの数も示されるため、ユーザは、許可または拒否された特定のパケットをモニタすることができます。 また、このコマンドは、アクセス リストがコンパイルされたアクセス リストとして実行されているかどうかも示します。

例

次は、アクセス リスト 101 が指定されている場合の、**show access-lists** コマンドの出力例を示します。

```
Router# show access-lists 101
Extended IP access list 101
    permit tcp host 198.92.32.130 any established (4304 matches) check=5
    permit udp host 198.92.32.130 any eq domain (129 matches)
    permit icmp host 198.92.32.130 any
    permit tcp host 198.92.32.130 host 171.69.2.141 gt 1023
    permit tcp host 198.92.32.130 host 171.69.2.135 eq smtp (2 matches)
    permit tcp host 198.92.32.130 host 198.92.30.32 eq smtp
    permit tcp host 198.92.32.130 host 171.69.108.33 eq smtp
    permit udp host 198.92.32.130 host 171.68.225.190 eq syslog
    permit udp host 198.92.32.130 host 171.68.225.126 eq syslog
    deny   ip 150.136.0.0 0.0.255.255 224.0.0.0 15.255.255.255
    deny   ip 171.68.0.0 0.1.255.255 224.0.0.0 15.255.255.255 (2 matches) check=1
    deny   ip 172.24.24.0 0.0.1.255 224.0.0.0 15.255.255.255
    deny   ip 192.82.152.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.173.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.174.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.239.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.240.0 0.0.7.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.248.0 0.0.3.255 224.0.0.0 15.255.255.255
```

アクセス リスト カウンタは、アクセス リストの各行により、何個のパケットが許可されたかをカウントします。 この数字は一致した数として表示されます。 Check は、1 つのパケットがアクセス リストと比較され、一致しなかった回数を意味します。

次に、Turbo Access Control List（ACL）機能が次のアクセス リストすべてで設定されているときの show access-lists コマンドの出力例を示します。

（注） show access-lists コマンドによって表示される許可および拒否の情報は、access-list コマンドを使用して入力した順序と同じではない可能性があります。

```
Router# show access-lists
```

```
Standard IP access list 1 (Compiled)
    deny   any
Standard IP access list 2 (Compiled)
    deny   192.168.0.0, wildcard bits 0.0.0.255
    permit any
Standard IP access list 3 (Compiled)
    deny   0.0.0.0
    deny   192.168.0.1, wildcard bits 0.0.0.255
    permit any
Standard IP access list 4 (Compiled)
    permit 0.0.0.0
    permit 192.168.0.2, wildcard bits 0.0.0.255
```

次に、ネットワークで IPv6 が設定されている場合に、IPv6 アクセス リストの情報を表示する、**show access-lists** コマンドの出力例を示します。

```
Router# show access-lists
IPv6 access list list2
     deny ipv6 FEC0:0:0:2::/64 any sequence 10
     permit ipv6 any any sequence 20
```

関連コマンド

コマンド	説明
access-list（IP 拡張）	拡張 IP アクセス リストを定義します。
access-list（IP 標準）	標準 IP アクセス リストを定義します。
clear access-list counters	アクセス リストのカウンタをクリアします。
clear access-template	ダイナミック アクセス リストから一時アクセス リストのエントリを手動でクリアします。
ip access-list	IP アクセス リストを名前で定義します。
show ip access-lists	現在のすべての IP アクセス リストの内容を表示します。
show ipv6 access-list	現在のすべての IPv6 アクセス リストの内容を表示します。

show authentication interface

特定のインターフェイスの認証マネージャに関する情報を表示するには、特権 EXEC モードで **show authentication interface** コマンドを使用します。

show authentication interface *type number*

構文の説明

type	インターフェイス タイプ。 詳細については、疑問符（?）オンライン ヘルプ機能を使用します。
number	インターフェイス番号を指定します。 ネットワーキングデバイスに対する番号付け構文の詳細については、疑問符（?）のオンライン ヘルプ機能を使用してください。

コマンド モード

特権 EXEC（#）

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。

使用上のガイドライン

show authentication interface コマンドを使用して、特定のインターフェイスの認証マネージャに関する情報を表示します。

例

次に、**show authentication interface** コマンドの出力例を示します。

```
Switch# show authentication interface g1/0/23
Client list:
  MAC Address     Domain   Status         Handle      Interface
  000e.84af.59bd  DATA     Authz Success  0xE0000000  GigabitEthernet1/0/23
Available methods list:
  Handle  Priority  Name
  3        0        dot1x
Runnable methods list:
```

```
  Handle  Priority  Name
  3        0        dot1x
```

下の表で、この出力で表示される重要なフィールドについて説明しています。 その他のフィールドは説明がなくても理解できます。

表 *2*：*show authentication interface* のフィールドの説明

フィールド	説明
MAC Address	クライアントの MAC アドレス。
Domain	クライアントのドメイン（DATA または VOICE）。
Status	認証セッションのステータス。 次の値が可能です。 • Authc Failed：このセッションで認証方式が実行され、認証は失敗しました。 • Authc Success：このセッションで認証方式が実行され、認証は成功しました。 • Authz Failed：機能が失敗し、セッションが終了しました。 • Authz Success：すべての機能がセッションに適用され、セッションがアクティブです。 • Idle：このセッションは初期化されていますが、認証方式が実行されませんでした。これは中間の状態です。 • No methods：このセッションの結果を出した認証方式はありません。 • Running：このセッションの認証方式が実行中です。
Interface	認証インターフェイスのタイプと番号。
Available methods list	インターフェイスで使用できる認証方式のサマリー情報。
Runnable methods list	インターフェイスで実行できる認証方式のサマリー情報。

関連コマンド

コマンド	説明
show authentication registrations	認証マネージャに登録されている認証方式に関する情報を表示します。
show authentication sessions	現在の認証マネージャ セッションに関する情報を表示します。

show authentication registrations

認証マネージャに登録されている認証方式に関する情報を表示するには、特権 EXEC モードで **show authentication registrations** コマンドを使用します。

show authentication registrations

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

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。

使用上のガイドライン

show authentication re gistrations コマンドを使用して、認証マネージャに登録されているすべての方式に関する情報を表示します。

例

次に、show authentication registrations コマンドの出力例を示します。

```
Switch# show authentication registrations
Auth Methods registered with the Auth Manager:
   Handle   Priority   Name
     3         0       dot1x
     2         1       mab
     1         2       webauth
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *3* : *show authentication registrations* のフィールドの説明

フィールド	説明
Priority	方式のプライオリティ。 **authentication priority** コマンドを使用して認証方式のプライオリティが設定されていない場合、デフォルトのプライオリティが表示されます。最高から最低までのデフォルトは dot1x、mab、および webauth です。
Name	認証方式の名前。 値は、dot1x、mab、および webauth です。

関連コマンド

コマンド	説明
show authentication interface	特定のインターフェイスの認証マネージャに関する情報を表示します。
show authentication sessions	現在の認証マネージャ セッションに関する情報を表示します。

show authentication sessions

現在の認証マネージャ セッションに関する情報を表示するには、特権 EXEC モードで **show authentication sessions** コマンドを使用します。

（注） Cisco IOS Release 12.2(33)SXI から、**show dot1x** コマンドは **show authentication sessions** コマンドで補完されます。 **show dot1x** コマンドは 802.1X 認証方式の使用に固有の出力を表示するために予約されています。 **show authentication sessions** コマンドは、すべての認証方式と許可機能の情報を表示します。

Cisco IOS XE Release 3SE and Later Releases

show authentication sessions [**[database]**| [**handle** *handle-number*| **interface** *type number*| **mac** *mac-address*| **method** *method-name* [**interface** *type number*]| **session-id** *session-id*]] **[details]**

All Other Releases

show authentication sessions [**handle** *handle-number*| **interface** *type number*| **mac** *mac-address*| **method** *method-name* **interface** *type number*| **session-id** *session-id*]

構文の説明

database	（任意）セッション データベースに保存されたセッション データを表示します。 このキーワードを使用することで、内部にキャッシュされた VLAN ID などの情報を表示できます。 セッションデータベースに格納されているデータが内部にキャッシュされたデータと一致しない場合は、警告メッセージが表示されます。
handle *handle-id*	（任意）認証マネージャ情報を表示する特定のハンドルを指定します。
interface *type number*	（任意）認証マネージャ情報を表示する特定のインターフェイスのタイプおよび番号を指定します。 インターフェイスに対する有効なキーワードおよび引数を表示するには、疑問符（?）によるオンライン ヘルプ機能を使用します。
mac *mac-address*	（任意）情報を表示する特定の MAC アドレスを指定します。

method *method-name*	（任意）認証マネージャ情報を表示する特定の認証方式を指定します。 有効な方式は次のいずれかです。 • **dot1x**：IEEE 802.1X 認証方式。 • **mab**：MAC 認証バイパス（MAB）方式。 • **webauth**：Web 認証方式。 方式を指定する場合は、インターフェイスも指定できます。
session-id *session-id*	（任意）認証マネージャ情報を表示する特定のセッションを指定します。
details	（任意）セッションに関する 1 行のサマリーを表示する代わりに、各セッションの詳細情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.2(33)SXH	このコマンドがサポートされるようになりました。
12.2(33)SXI	このコマンドは、**handle** *handle* キーワードおよび引数を追加して出力に情報を追加するために変更されました。
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。
Cisco IOS XE Release 3.2SE	このコマンドが変更されました。 **database** キーワードと **details** キーワードが追加されました。

使用上のガイドライン

show authentication sessions コマンドを使用して、現在の認証マネージャ セッションすべてに関する情報を表示します。 特定の認証マネージャ セッションに関する情報を表示するには、1 つ以上のキーワードを使用します。

例

次に、スイッチ上のすべての認証セッションを表示する例を示します。

```
Device# show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Gi1/48     0015.63b0.f676  dot1x    DATA     Authz Success  0A3462B1000000102983C05C
Gi1/5      000f.23c4.a401  mab      DATA     Authz Success  0A3462B10000000D24F80B58
Gi1/5      0014.bf5d.d26d  dot1x    DATA     Authz Success  0A3462B10000000E29811B94
```

次に、インターフェイス上のすべての認証セッションを表示する例を示します。

```
Device# show authentication sessions interface gigabitethernet2/47

Interface:  GigabitEthernet2/47
          MAC Address:  Unknown
           IP Address:  Unknown
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Guest Vlan
          Vlan Policy:  20
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C8000000000002763C
      Acct Session ID:  0x00000002
               Handle:  0x25000000
Runnable methods list:
       Method   State
       mab      Failed over
       dot1x    Failed over
----------------------------------------
            Interface:  GigabitEthernet2/47
          MAC Address:  0005.5e7c.da05
           IP Address:  Unknown
            User-Name:  00055e7cda05
               Status:  Authz Success
               Domain:  VOICE
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C8000000010002A238
      Acct Session ID:  0x00000003
               Handle:  0x91000001
Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

次に、指定したセッション ID の認証セッションを表示する例を示します。

```
Device# show authentication sessions session-id 0B0101C70000004F2ED55218

            Interface:  GigabitEthernet9/2
          MAC Address:  0000.0000.0011
           IP Address:  20.0.0.7
             Username:  johndoe
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Critical Auth
          Vlan policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0B0101C70000004F2ED55218
```

```
      Acct Session ID:  0x00000003
               Handle:  0x91000001
Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

次に、指定した認証方式によって許可されたすべてのクライアントを表示する例を示します。

```
Device# show authentication sessions method mab

No Auth Manager contexts match supplied criteria

Device# show authentication sessions method dot1x

Interface  MAC Address     Domain   Status         Session ID
Gi9/2      0000.0000.0011  DATA     Authz Success  0B0101C70000004F2ED55218
```

下の表で、この出力で表示される重要なフィールドについて説明します。

表 *4*：*show authentication sessions* のフィールドの説明

フィールド	説明
Interface	認証インターフェイスのタイプと番号。
MAC Address	クライアントの MAC アドレス。
Domain	ドメインの名前（DATA または VOICE）。
Status	認証セッションのステータス。 次の値が可能です。 • Authc Failed：このセッションで認証方式が実行され、認証は失敗しました。 • Authc Success：このセッションで認証方式が実行され、認証は成功しました。 • Authz Failed：機能が失敗し、セッションが終了しました。 • Authz Success：すべての機能がセッションに適用され、セッションがアクティブです。 • Idle：このセッションは初期化されていますが、認証方式が実行されませんでした。これは中間の状態です。 • No methods：このセッションの結果を出した認証方式はありません。 • Running：このセッションの認証方式が実行中です。

フィールド	説明
Handle	コンテキストのハンドル。
State	レポートされた認証セッションの動作状態。 次の値が可能です。 • Not run：このセッションの方式が実行されませんでした。 • Running：このセッションの方式が実行中です。 • Failed over：この方式が失敗し、次の方式で結果を提供すると想定されています。 • Success：この方式は、セッションの成功した認証結果を提供しました。 • Authc Failed：この方式は、セッションの失敗した認証結果を提供しました。

関連コマンド

コマンド	説明
show access-sessions	セッション対応ネットワーキングセッションに関する情報を表示します。
show authentication registrations	認証マネージャに登録されている認証方式に関する情報を表示します。
show authentication statistics	認証マネージャセッションの統計情報を表示します。
show dot1x	802.1X 認証方式の使用に固有のアイデンティティ プロファイルの詳細を表示します。

show diameter peer から show object-group まで

show dot1x

アイデンティティ プロファイルの詳細を表示するには、特権 EXEC モードで **show dot1x** コマンドを使用します。

（注） Cisco IOS Release 12.2(33)SXI から、**show dot1x** コマンドは **show authentication** コマンドで補完されます。 **show dot1x** コマンドは 802.1X 認証方式の使用に固有の出力を表示するために予約されています。 **show authentication sessions** コマンドは、すべての認証方式と許可機能の情報の表示する、より幅広い権限があります。 詳細は、**show authentication sessions** コマンドを参照してください。

show dot1x [**all [summary]**| **interface** *interface-name*| **details**| **statistics**]

構文の説明

all	（任意）すべてのインターフェイスの 802.1X ステータスを表示します。
summary	（任意）すべてのインターフェイスの 802.1X ステータスのサマリーを表示します。
interface *interface-name*	（任意）インターフェイス名と番号を指定します。
details	（任意）インターフェイスの設定と、インターフェイスのオーセンティケータインスタンスを表示します。
statistics	（任意）すべてのインターフェイスの 802.1X 統計情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.1(11)AX	このコマンドが導入されました。
12.1(14)EA1	**all** キーワードが追加されました。

リリース	変更内容
12.3(2)XA	このコマンドが、Cisco IOS Release 12.3(2)XA に統合されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。
12.2(25)SED	認証ステートのマシン ステートおよびポート ステータス フィールドに auth-fail-vlan 情報が含まれるように出力の表示が拡張されました。
12.2(25)SEE	**details** キーワードと **statistics** キーワードが追加されました。
12.3(11)T	**show dot1x** コマンドの出力に PAE、HeldPeriod、StartPeriod および MaxStart フィールドが追加されました。
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す。 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。

使用上のガイドライン

ポートを指定しない場合は、グローバルパラメータおよびサマリーが表示されます。 ポートを指定する場合、ポートの詳細が出力に表示されます。

（注） 802.1X 認証方式以外の認証方式が使用されている場合、一部の IOS バージョンでは、**show dot1x** コマンドで、Port Status コマンド出力フィールドに AUTHORIZED または UNAUTHORIZED 値が表示されない場合があります。 Port Status フィールドに値が含まれていない場合は、**show authentication sessions** コマンドを使用して、Authz Success または Authz Failed ポート ステータス認証値を表示します。

例

次に、**interface** キーワードと **details** キーワードの両方を使用した **show dot1x** コマンドの出力例を示します。 次の例では、クライアントは正常に認証されています。

```
Router# show dot1x interface ethernet1/0 details
Dot1x Info for Ethernet1/0
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 1
TxPeriod                  = 30
Dot1x Authenticator Client List
-------------------------------
```

```
Supplicant                = aabb.cc00.c901
Session ID                = 0A3462800000000000009F8
    Auth SM State         = AUTHENTICATED
    Auth BEND SM State    = IDLE
```

次に、**interface** キーワードと **details** キーワードの両方を使用した **show dot1x** コマンドの出力例を示します。 次の例では、クライアントは認証に失敗しています。

```
Router# show dot1x interface ethernet1/0 details
Dot1x Info for Ethernet1/0
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 1
TxPeriod                  = 30
Dot1x Authenticator Client List Empty
```

下の表で、この出力で表示される重要なフィールドについて説明します。

表 *5*：*show dot1x* のフィールドの説明

フィールド	説明
PAE	ポート アクセス エンティティ。 インターフェイスのロールを定義します（サプリカント、オーセンティケータ、またはオーセンティケータとサプリカントとして）。
PortControl	ポート制御値。 • AUTO：クライアント PC の認証ステータスは認証プロセスによって決定されます。 • Force-authorize：インターフェイスのすべてのクライアント PC が許可されます。 • Force-unauthorized：インターフェイスのすべてのクライアント PC が許可されません。
ControlDirection	IEEE 802.1X 制御ポートの制御が両方向（入力と出力）に適用されるか、またはインバウンド方向（入力）だけに適用されるかを示します。詳細については、「dot1x control-direction」、または Cisco IOS Release 12.2(33)SXI より導入された authentication control-direction を参照してください。

フィールド	説明
HostMode	ホストモードがシングルホストまたはマルチホストかを示します。Cisco IOS Release 12.2(33)SXI 以降では、マルチ認証かマルチドメインかについても示します。 詳細については、「dot1x host-mode」、または Cisco IOS Release 12.2(33)SXI より導入された「authentication host-mode」を参照してください。
QuietPeriod	クライアントの認証に失敗すると、秒単位で示された待機時間の経過後に、認証が再起動されます。
ServerTimeout	RADIUS に設定されたタイムアウトが再試行されます。 802.1X パケットがサーバに送信され、そのサーバが応答しなかった場合、そのパケットは表示された秒数の経過後に再度送信されます。
SuppTimeout	サプリカント（クライアント PC）再試行に設定された時間。 802.1X パケットがサプリカントに送信され、そのサプリカントが応答しなかった場合、そのパケットは表示された秒数の経過後に再度送信されます。
ReAuthMax	クライアント PC の自動再認証が開始されるまでの最大時間（秒単位）。
MaxReq	クライアント PC が 802.1X をサポートしていないと判断されるまでに、ルータからクライアント PC に送信する拡張認証プロトコル（EAP）要求/アイデンティティ フレーム（応答が受信されないと想定）の最大送信回数。
TxPeriod	サプリカントの再試行のタイムアウト、つまり EAP アイデンティティ要求のタイムアウト。 詳細については、「dot1x timeout tx-period」を参照してください。
Supplicant	クライアント PC または 802.1X クライアントの MAC アドレス。
Session ID	ネットワーク セッションの ID。

フィールド	説明
Auth SM State	クライアント PC の状態を AUTHENTICATED または UNAUTHENTICATED で示します。
Auth BEND SM State	IEEE 802.1X オーセンティケータのバックエンド ステート マシンの状態。

関連コマンド

コマンド	説明
clear dot1x	802.1X インターフェイス情報を消去します。
debug dot1x	802.1X デバッグ情報を表示します。
dot1x default	グローバル 802.1X パラメータをデフォルト値にリセットします。
identity profile	アイデンティティ プロファイルを作成します。
show authentication sessions	現在の認証マネージャ セッションに関する情報を表示します。

show ip access-lists

現在のすべての IP アクセス リストの内容を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip access-lists** コマンドを使用します。

show ip access-lists [*access-list-number*| *access-list-number-expanded-range*| *access-list-name*| **dynamic** [*dynamic-access-list-name*]| **interface** *name number* [**in**| **out**]]

構文の説明

access-list-number	（任意）表示する IP アクセス リストの数です。
access-list-number-expanded-range	（任意）表示する IP アクセス リストの拡張範囲。
access-list-name	（任意）表示する IP アクセス リストの名前です。
dynamic *dynamic-access-list-name*	（任意）指定したダイナミック IP アクセス リストを表示します。
interface *name number*	（任意）指定したインターフェイスのアクセス リストを表示します。
in	（任意）入力インターフェイスの統計情報を表示します。
out	（任意）出力インターフェイスの統計情報を表示します。

コマンド デフォルト

すべての標準および拡張 IP アクセス リストが表示されます。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更内容
10.3	このコマンドが導入されました。
12.3(7)T	**dynamic** キーワードが追加されました。

リリース	変更内容
12.4(6)T	**interface** *name* と *number* のキーワードと引数のペアが追加されました。**in** キーワードと **out** キーワードが追加されました。
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。
12.4(11)T	このコマンドが変更されました。 **dynamic** キーワードの出力例が追加されました。
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す。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。
12.4(20)T	このコマンドが変更されました。 このコマンドの出力が拡張され、オブジェクト グループを含むアクセス リストが表示されるようになりました。
Cisco IOS XE Release 2.5	このコマンドが、Cisco IOS XE Release 2.5 に統合されました。

使用上のガイドライン

show ip access-lists コマンドの出力は、IP 固有であり、特定のアクセス リストを指定できるという点以外は **show access-lists** コマンドの出力と同じです。

例

次に、すべてのアクセス リストが要求されている場合の、**show ip access-lists** コマンドの出力例を示します。

```
Router# show ip access-lists
Extended IP access list 101
   deny udp any any eq nntp
   permit tcp any any
   permit udp any any eq tftp
   permit icmp any any
   permit udp any any eq domain
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *6*：*show ip access-lists* のフィールドの説明

フィールド	説明
Extended IP access list	拡張 IP アクセスリストの番号。
deny	拒否するパケット。
udp	ユーザ データグラム プロトコル。

フィールド	説明
any	送信元ホストと宛先ホスト。
eq	特定のポート番号のパケット。
nntp	ネットワーク ニュース トランスポート プロトコル。
permit	転送するパケット。
tcp	伝送制御プロトコル。
tftp	Trivial File Transfer Protocol。
icmp	Internet Control Message Protocol（インターネット制御メッセージ プロトコル）。
domain	ドメイン ネーム サービス。

次に、特定のアクセス リストの名前要求されている場合の、**show ip access-lists** コマンドの出力例を示します。

```
Router# show ip access-lists Internetfilter
Extended IP access list Internetfilter
   permit tcp any 192.0.2.0 255.255.255.255 eq telnet
   deny tcp any any
   deny udp any 192.0.2.0 255.255.255.255 lt 1024
   deny ip any any log
```

次に、オブジェクト グループが含まれている特定のアクセス リストの名前要求されている場合の、**show ip access-lists** コマンドの出力例を示します。

```
Router# show ip access-lists my-ogacl-policy
Extended IP access list my-ogacl-policy
   10 permit object-group eng-service any any
```

次の **show ip access-lists** コマンドの出力例は、ファスト イーサネット インターフェイス 0/0 の入力統計情報を示します。

```
Router#
 show ip access-lists interface FastEthernet0/0 in

Extended IP access list 150 in
   10 permit ip host 10.1.1.1 any
   30 permit ip host 10.2.2.2 any (15 matches)
```

次に、**dynamic** キーワードを使用した **show ip access-lists** コマンドの出力例を示します。

```
Router#
show ip access-lists dynamic CM_SF#1
Extended IP access list CM_SF#1
    10 permit udp any any eq 5060 (650 matches)
    20 permit tcp any any eq 5060
    30 permit udp any any dscp ef (806184 matches)
```

設定を確認するには、**show run interfaces cable** コマンドを使用します。

```
Router#
show run interfaces cable 0/1/0
Building configuration...
Current configuration : 144 bytes
!
interface cable-modem0/1/0
 ip address dhcp
 load-interval 30
 no keepalive
  service-flow primary upstream
   service-policy output llq
end
```

関連コマンド

コマンド	説明
deny	パケットを拒否するネームド IP アクセス リストまたは OGACL の条件を設定します。
ip access-group	インターフェイスまたはサービス ポリシーマップに ACL または OGACL を適用します。
ip access-list	IP アクセス リストまたは OGACL を名前または番号で定義します。
object-group network	OGACL で使用するネットワーク オブジェクト グループを定義します。
object-group service	OGACL で使用するサービス オブジェクト グループを定義します。
permit	パケットを許可するネームド IP アクセス リストまたは OGACL の条件を設定します。
show object-group	設定されたオブジェクト グループに関する情報を表示します。
show run interfaces cable	ケーブル モデムの統計情報を表示します。

show ip admission

ネットワーク アドミッション キャッシュ エントリと Web 認証セッションに関する情報を表示するには、ユーザ EXEC または特権 EXEC モードで **show ip admission** コマンドを使用します。

Cisco IOS XE Release 3SE and Later Releases

show ip admission {**cache**| **statistics** [**brief**| **details**| **httpd**| **input-feature**]| **status** [**banners**| **custom-pages**| **httpd**| **parameter-map** [*parameter-map-name*]]| **watch-list**}

All Other Releases

show ip admission {**cache** [**consent**| **eapoudp**| **ip-addr** *ip-address*| **username** *username*]| **configuration**| **httpd**| **statistics**| [**brief**| **details**| **httpd**]| **status [httpd]| watch-list**}

構文の説明

cache	ネットワーク アドミッション エントリの現在のリストを表示します。
statistics	Web 認証の統計情報を表示します。
brief	（任意）Web認証の統計情報の要約を表示します。
details	（任意）Web認証の統計情報の詳細を表示します。
httpd	（任意）Web 認証 HTTP プロセスに関する情報を表示します。
input-feature	Web認証パケットに関する統計情報を表示します。
status	バナー、カスタム ページ、HTTP プロセス、およびパラメータ マップなど、設定済みの Web 認証機能に関するステータス情報を表示します。
banners	Web認証用に設定されているバナーに関する情報を表示します。

custom-pages	Web 認証用に設定されているカスタム ページに関する情報を表示します。 カスタム ファイルはローカル キャッシュに読み込まれ、キャッシュから実行されます。バックグラウンドプロセスは定期的にファイルを再キャッシュする必要があるかどうかを確認します。
parameter-map *parameter-map-name*	すべてのパラメータ マップについて、あるいは指定したパラメータ マップのみについて、設定されたバナーおよびカスタムページに関する情報を表示します。
watch-list	ウォッチ リストに IP アドレスのリストを表示します。
consent	（任意）承諾 Web ページのキャッシュ エントリを表示します。
eapoudp	（任意）UDP（EAPoUDP）ネットワーク アドミッション キャッシュ エントリを介した拡張認証プロトコルを表示します。 ホストの IP アドレス、セッション タイムアウト、ポスチャの状態が含まれます。
ip-addr *ip-address*	（任意）クライアント IP アドレスに関する情報を表示します。
username *username*	（任意）クライアントのユーザ名に関する情報を表示します。
configuration	（任意）NAC 設定を表示します。 （注） このキーワードは、Cisco IOS XE Release 3.2SE 以降のリリースではサポートされません。 **show running-config all** コマンドを使用して、実行中の Web 認証設定と、デフォルト パラメータで設定されたコマンドを表示します。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.3(8)T	このコマンドが導入されました。
12.4(11)T	このコマンドが変更されました。 このコマンドの出力が拡張され、AAA タイムアウト ポリシーが設定されているかどうかが表示されるようになりました。
12.4(15)T	このコマンドが変更されました。 **consent** キーワードが追加されました。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI に統合されました。
15.3(1)T	このコマンドが変更されました。 **statistics**、**brief**、**details**、**httpd**、および **status** キーワードが追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが変更されました。 **input-feature**、**banners**、**custom-pages**、および **parameter-map** キーワードが追加されました。 **configuration** キーワードが削除されました。

使用上のガイドライン

ネットワーク アドミッション エントリと、Web 認証セッションに関する情報を表示するには、**show ip admission** コマンドを使用します。

例

次に、**show ip admission cache** コマンドの出力例を示します。

```
Device# show ip admission cache

Authentication Proxy Cache
Total Sessions: 1 Init Sessions: 1
 Client MAC 5cf3.fc25.7e3d Client IP 1.150.128.2 IPv6 :: Port 0, State INIT, Method Webauth
```

次に、**show ip admission statistics** コマンドの出力例を示します。

```
Device# show ip admission statistics

Webauth input-feature statistics:
                                                        IPv4          IPv6
  Total packets received                                46            0
    Delivered to TCP                                    46            0
    Forwarded                                           0             0
    Dropped                                             0             0
    TCP new connection limit reached                    0             0

Webauth HTTPd statistics:

  HTTPd process 1
    Intercepted HTTP requests:                          8
    IO Read events:                                     9
    Received HTTP messages:                             7
    IO write events:                                    11
    Sent HTTP replies:                                  7
```

```
    IO AAA messages:                                4
    SSL OK:                                         0
    SSL Read would block:                           0
    SSL Write would block:                          0
    HTTPd process scheduled count:                  23
```

次に、**show ip admission status** コマンドの出力例を示します。

```
Device# show ip admission status

IP admission status:
  Enabled interfaces            1
  Total sessions                1
  Init sessions                 1     Max init sessions allowed     100
    Limit reached               0     Hi watermark                  1
  TCP half-open connections     0     Hi watermark                  0
  TCP new connections           0     Hi watermark                  0
  TCP half-open + new           0     Hi watermark                  0
  HTTPD1 Contexts               0     Hi watermark                  1

  Parameter Map: Global
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBAUTH
    Custom Pages
      Custom pages not configured
    Banner
      Type: text
        Banner                  " <H2>Login Page Banner</H2> "
        Html                    " <H2>Login Page Banner</H2> "
        Length                  48

  Parameter Map: PMAP_CONSENT
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBCONSENT
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBAUTH_CUSTOM_FLASH
    Custom Pages
      Type: "login"
        File                    flash:webauth_login.html
        File status             Ok - File cached
        File mod time           2012-07-20T02:29:36.000Z
        File needs re-cached    No
        Cache                   0x3AEE1E1C
        Cache len               246582
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
      Type: "success"
        File                    flash:webauth_success.html
        File status             Ok - File cached
        File mod time           2012-02-21T06:57:28.000Z
        File needs re-cached    No
        Cache                   0x3A529B3C
        Cache len               70
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
      Type: "failure"
        File                    flash:webauth_fail.html
        File status             Ok - File cached
        File mod time           2012-02-21T06:55:49.000Z
        File needs re-cached    No
        Cache                   0x3A5BEBC4
        Cache len               67
```

```
      Cache time              2012-09-18T13:56:57.000Z
      Cache access            0 reads, 1 write
    Type: "login expired"
      File                    flash:webauth_expire.html
      File status             Ok - File cached
      File mod time           2012-02-21T06:55:25.000Z
      File needs re-cached    No
      Cache                   0x3AA20090
      Cache len               69
      Cache time              2012-09-18T13:56:57.000Z
      Cache access            0 reads, 1 write
  Banner
    Banner not configured

Parameter Map: PMAP_WEBAUTH_CUSTOM_EXTERNAL
  Custom Pages
    Custom pages not configured
  Banner
    Banner not configured
```

次に、**banner text** コマンドを使用して設定されたバナーに対する **show ip admission status banners** コマンドの出力例を示します。

```
Device# show ip admission status banners

IP admission status:
  Parameter Map: Global
    Banner not configured

  Parameter Map: PMAP_WEBAUTH
    Type: text
      Banner                  " <H2>Login Page Banner</H2> "
      Html                    " <H2>Login Page Banner</H2> "
      Length                  48
```

次に、**banner file** コマンドを使用して設定されたバナーに対する **show ip admission status banners** コマンドの出力例を示します。

```
Device# show ip admission status banners

IP admission status:
  Parameter Map: Global
    Banner not configured

  Parameter Map: PMAP_WEBAUTH
    Type: file
      Banner                  <h2>Cisco Systems</h2>
<h3>Webauth Banner from file</h3>

      Length                  60
      File                    flash:webauth_banner1.html
      File status             Ok - File cached
      File mod time           2012-07-24T07:07:09.000Z
      File needs re-cached    No
      Cache                   0x3AF6CEE4
      Cache len               60
      Cache time              2012-09-19T10:13:59.000Z
      Cache access            0 reads, 1 write
```

次に、**show ip admission status custom pages** コマンドの出力例を示します。

```
Device# show ip admission status custom pages

IP admission status:
  Parameter Map:  Global
    Custom pages not configured
  Parameter Map:  PMAP_WEBAUTH
    Type: "login"
      File                    flash:webauth_login.html
      File status             Ok - File cached
      File mod time           2012-07-20T02:29:36.000Z
      File needs re-cached    No
      Cache                   0x3B0DCEB4
      Cache len               246582
```

```
    Cache time                2012-09-18T16:26:13.000Z
    Cache access              0 reads, 1 write
  Type: "success"
    File                      flash:webauth_success.html
    File status               Ok - File cached
    File mod time             2012-02-21T06:57:28.000Z
    File needs re-cached      No
    Cache                     0x3A2E9090
    Cache len                 70
    Cache time                2012-09-18T16:26:13.000Z
    Cache access              0 reads, 1 write
  Type: "failure"
    File                      flash:webauth_fail.html
    File status               Ok - File cached
    File mod time             2012-02-21T06:55:49.000Z
    File needs re-cached      No
    Cache                     0x3AF6D1A4
    Cache len                 67
    Cache time                2012-09-18T16:26:13.000Z
    Cache access              0 reads, 1 write
  Type: "login expired"
    File                      flash:webauth_expire.html
    File status               Ok - File cached
    File mod time             2012-02-21T06:55:25.000Z
    File needs re-cached      No
    Cache                     0x3A2E8284
    Cache len                 69
    Cache time                2012-09-18T16:26:13.000Z
    Cache access              0 reads, 1 write
Parameter Map:  PMAP_CONSENT
  Custom pages not configured
```

次の表に、上記の出力で表示される重要なフィールドについて説明します。

表 *7*： *show ip admission* フィールドの説明

File mod time	ファイルがファイルシステムに変更されたときのタイムスタンプ。
Cache time	ファイルが最後にキャッシュに読み込まれたときのタイムスタンプ。

次の出力では、ルータに設定されているすべての IP アドミッション制御ルールを示します。

```
Device# show ip admission configuration

Authentication Proxy Banner not configured
Consent Banner is not configured
Authentication Proxy webpage
        Login page              : flash:test1.htm
        Success page            : flash:test1.htm
        Fail page               : flash:test1.htm
        Login Expire page       : flash:test1.htm
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 5 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

次の出力では、ホスト IP アドレス、セッション タイムアウト、およびポスチャの状態を示します。 ポスチャの状態が POSTURE ESTAB である場合、ホスト検証は成功しました。

```
Device# show ip admission cache eapoudp

Posture Validation Proxy Cache
Total Sessions: 3 Init Sessions: 1
 Client IP 10.0.0.112, timeout 60, posture state POSTURE ESTAB
 Client IP 10.0.0.142, timeout 60, posture state POSTURE INIT
 Client IP 10.0.0.205, timeout 60, posture state POSTURE ESTAB
```

出力にはフィールドの説明も表示されます。

関連コマンド

コマンド	説明
banner（パラメータ マップ Web 認証）	Web 認証ログイン Web ページにバナーを表示します。
clear ip admission cache	ルータからの IP アドミッション キャッシュ エントリをクリアします。
custom-page	Web 認証ログイン時にカスタム Web ページが表示されます。
ip admission name	レイヤ 3 ネットワーク アドミッション制御ルールを作成します。

show ip interface

IP に設定されたインターフェイスのユーザビリティ ステータスを表示するには、特権 EXEC モードで **show ip interface** コマンドを使用します。

show ip interface [*type number*] **[brief]**

構文の説明

type	（任意）インターフェイス タイプ。
number	（任意）インターフェイス番号。
brief	（任意）各インターフェイスのユーザビリティ ステータスの概要を表示します。

コマンド デフォルト

IP に対して設定されているすべてのインターフェイスについて、完全なユーザビリティ ステータスが表示されます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
10.0	このコマンドが導入されました。
12.0(3)T	**ip wccp redirect out** コマンドと **ip wccp redirect exclude add in** コマンドのステータスを表示するよう、コマンドの出力が変更されました。
12.2(14)S	サブインターフェイスの NetFlow のステータスを表示するよう、コマンドの出力が変更されました。
12.2(15)T	サブインターフェイスの NetFlow のステータスを表示するよう、コマンドの出力が変更されました。
12.3(6)	出力においてダウンストリーム VPN ルーティング/転送（VRF）インスタンスを識別できるよう、コマンドの出力が変更されました。
12.3(14)YM2	Multiprocessor Forwarding（MPF）用に設定され、Cisco 7301 ルータおよび Cisco 7206VXR ルータに実装されているインターフェイスのユーザビリティ ステータスを表示するよう、コマンドの出力が変更されました。

リリース	変更内容
12.2(14)SX	このコマンドがスーパーバイザ エンジン 720 に実装されました。
12.2(17d)SXB	このコマンドが Supervisor Engine 2 の Cisco IOS 12.2(17d)SXB に統合され、ハードウェア フローのステータスの NDE が含まれるようにコマンドの出力が変更されました。
12.4(4)T	このコマンドが Cisco IOS Release 12.4(4)T に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
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)SB2	ユニキャスト リバース パス転送（RPF）通知機能に関する情報を表示するよう、コマンドの出力が変更されました。
12.4(20)T	ユニキャスト RPF 通知機能に関する情報を表示するよう、コマンドの出力が変更されました。
12.2(33)SXI2	このコマンドが変更されました。 ユニキャスト RPF 通知機能に関する情報を表示するよう、コマンドの出力が変更されました。
Cisco IOS XE Release 2.5	このコマンドが変更されました。 このコマンドが、Cisco ASR 1000 シリーズの集約サービス ルータに実装されました。

使用上のガイドライン

インターフェイスが使用可能な場合（パケットを送受信できる場合）、Cisco IOS ソフトウェアによって、直接接続されているルートがルーティング テーブルに自動的に入力されます。インターフェイスが使用不可である場合、直接接続されているルーティング エントリはルーティング テーブルから削除されます。 エントリが削除されると、ソフトウェアはダイナミック ルーティング プロトコルを使用してネットワークへのバックアップ ルートを決定するようになります（存在する場合）。

インターフェイスで双方向通信が提供される場合、回線プロトコルは「up」とマークされます。インターフェイス ハードウェアが使用可能な場合、インターフェイスは「up」とマークされます。

オプションのインターフェイス タイプを指定すると、その特定のインターフェイスに関する情報が表示されます。 オプションの引数を指定しないと、すべてのインターフェイスの情報が表示されます。

PPP またはシリアル ライン インターネット プロトコル（SLIP）によって非同期インターフェイスがカプセル化されると、IP 高速スイッチングがイネーブルになります。 PPP または SLIP によってカプセル化された非同期インターフェイスに対して **show ip interface** コマンドを実行すると、IP 高速スイッチングがイネーブルであることを示すメッセージが表示されます。

ルータ インターフェイスの概要を表示するには、**show ip interface brief** コマンドを使用できます。このコマンドでは、IP アドレス、インターフェイスのステータス、およびその他の情報が表示されます。

show ip interface brief コマンドでは、ユニキャスト RPF に関連する情報は表示されません。

例

次に、ギガビット イーサネット 0/3 インターフェイスの設定情報を表示する例を示します。 次の例では、出力側（パケットがインターフェイスから送信される場所）に IP フローの出力機能を設定し、入力側（パケットがインターフェイスに着信する場所）に PBRNAME という名前のポリシー ルート マップを設定しています。

```
Router# show running-config interface gigabitethernet 0/3
interface GigabitEthernet0/3
 ip address 10.1.1.1 255.255.0.0
 ip flow egress
 ip policy route-map PBRNAME
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
end
```

次に、ギガビット イーサネット インターフェイス 0/3 のインターフェイス情報を表示する例を示します。 この例では、MPF がイネーブルであり、ポリシーベース ルーティング（PBR）と NetFlow 機能の両方が MPF でサポートされておらず、無視されています。

```
Router# show ip interface gigabitethernet 0/3
GigabitEthernet0/3 is up, line protocol is up
  Internet address is 10.1.1.1/16
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Feature Fast switching turbo vector
  IP VPN Flow CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is enabled, using route map PBR
  Network address translation is disabled
  BGP Policy Mapping is disabled
  IP Multi-Processor Forwarding is enabled
     IP Input features, "PBR",
         are not supported by MPF and are IGNORED
```

```
    IP Output features, "NetFlow",
        are not supported by MPF and are IGNORED
```

次に、ダウンストリームVRFインスタンスを識別する例を示します。この例では、「Downstream VPN Routing/Forwarding "D"」の表示でダウンストリーム VRF インスタンスを識別できます。

```
Router# show ip interface virtual-access 3
Virtual-Access3 is up, line protocol is up
  Interface is unnumbered. Using address of Loopback2 (10.0.0.8)
  Broadcast address is 255.255.255.255
  Peer address is 10.8.1.1
  MTU is 1492 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Feature Fast switching turbo vector
  IP VPN CEF switching turbo vector
  VPN Routing/Forwarding "U"
  Downstream VPN Routing/Forwarding "D"
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

次に、ユニキャストRPFのドロップ レートの通知が設定されている場合に表示される情報の例を示します。

```
Router# show ip interface ethernet 2/3
Ethernet2/3 is up, line protocol is up
  Internet address is 10.0.0.4/16
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Null turbo vector
  IP Null turbo vector
```

```
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are No CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

例

```
  Input features: uRPF
  IP verify source reachable-via RX, allow default
   0 verification drops
   0 suppressed verification drops
   0 verification drop-rate
Router#
```

次に、特定の VLAN のユーザビリティ ステータスを表示する例を示します。

```
Router# show ip interface vlan 1
Vlan1 is up, line protocol is up
  Internet address is 10.0.0.4/24
  Broadcast address is 255.255.255.255
Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Fast switching turbo vector
  IP Normal CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
  Sampled Netflow is disabled
  IP multicast multilayer switching is disabled
  Netflow Data Export (hardware) is enabled
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *8*：*show ip interface* のフィールドの説明

フィールド	説明
Virtual-Access3 is up	インターフェイス ハードウェアが使用可能（アップ状態）かどうかを示します。インターフェイスが使用可能となるには、インターフェイス ハードウェアと回線プロトコルの両方がアップ状態である必要があります。
Broadcast address is	ブロードキャスト アドレス。
Peer address is	ピア アドレス。
MTU is	インターフェイスに設定されている MTU の値（バイト単位）。
Helper address	ヘルパー アドレス（設定されている場合）。
Directed broadcast forwarding	指定ブロードキャスト転送がイネーブルかどうかを示します。
Outgoing access list	インターフェイスに発信アクセス リストが設定されているかどうかを示します。
Inbound access list	インターフェイスに着信アクセス リストが設定されているかどうかを示します。
Proxy ARP	プロキシアドレス解決プロトコル（ARP）がインターフェイスでイネーブルであるかどうかを示します。
Security level	このインターフェイスに対して設定されている IP Security Option（IPSO）セキュリティ レベル。
Split horizon	スプリット ホライズンがイネーブルかどうかを示します。
ICMP redirects	このインターフェイスでリダイレクト メッセージが送信されるかどうかを示します。
ICMP unreachables	このインターフェイスで到達不能メッセージが送信されるかどうかを示します。
ICMP mask replies	マスク応答がこのインターフェイスで送信されるかどうかを示します。

フィールド	説明
IP fast switching	高速スイッチングがこのインターフェイスでイネーブルかどうかを示します。通常、このようなシリアルインターフェイス上ではイネーブルです。
IP Flow switching	フロースイッチングがこのインターフェイスでイネーブルかどうかを示します。
IP CEF switching	シスコ エクスプレス フォワーディング スイッチングがインターフェイスでイネーブルになっているかどうかを示します。
Downstream VPN Routing/Forwarding "D"	PPP ピア ルートおよび AAA ユーザ単位ルートがインストールされている VRF インスタンスを示します。
IP multicast fast switching	マルチキャスト高速スイッチングがこのインターフェイスでイネーブルかどうかを示します。
IP route-cache flags are Fast	NetFlow がインターフェイスでイネーブルかどうかを示します。インターフェイスで NetFlow がイネーブルであることを表すには「Flow init」と表示されます。 **ip flow ingress** コマンドを使用してサブインターフェイスで NetFlow がイネーブルになっていることを表すには、「Ingress Flow」と表示されます。 **ip route-cache flow** コマンドを使用してメイン インターフェイスで NetFlow がイネーブルになっていることを表すには、「Flow」と表示されます。
Router Discovery	検出プロセスがこのインターフェイスでイネーブルかどうかを示します。 シリアル インターフェイス上では通常はディセーブルです。
IP output packet accounting	このインターフェイスで IP アカウンティングがイネーブルかどうかと、そのしきい値（エントリの最大数）を示します。
TCP/IP header compression	圧縮がイネーブルかどうかを示します。

フィールド	説明
WCCP Redirect outbound is disabled	インターフェイスで受信されたパケットがキャッシュエンジンにリダイレクトされるかどうかのステータスを示します。「enabled」または「disabled」と表示されます。
WCCP Redirect exclude is disabled	インターフェイス宛てのパケットがキャッシュエンジンへのリダイレクトから除外されるかどうかのステータスを示します。「enabled」または「disabled」と表示されます。
Netflow Data Export (hardware) is enabled	インターフェイスのNetFlowデータエクスポート（NDE）のハードウェアフローステータス。

次に、各インターフェイスのユーザビリティ ステータスのサマリーを表示する例を示します。

```
Router# show ip interface brief
Interface     IP-Address     OK?  Method  Status                   Protocol
Ethernet0     10.108.00.5    YES  NVRAM   up                       up
Ethernet1     unassigned     YES  unset   administratively down   down
Loopback0     10.108.200.5   YES  NVRAM   up                       up
Serial0       10.108.100.5   YES  NVRAM   up                       up
Serial1       10.108.40.5    YES  NVRAM   up                       up
Serial2       10.108.100.5   YES  manual  up                       up
Serial3       unassigned     YES  unset   administratively down   down
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *9*：*show ip interface brief* のフィールドの説明

フィールド	説明
Interface	インターフェイスのタイプ。
IP-Address	インターフェイスに割り当てられている IP アドレス。
OK?	「Yes」は IP アドレスが有効であることを意味します。「No」は IP アドレスが無効であることを意味します。

フィールド	説明
Method	このフィールドは次の値を持ちます。 • RARP または SLARP：逆アドレス解決プロトコル（RARP）または Serial Line Address Resolution Protocol（SLARP）の要求。 • BOOTP：Bootstrap プロトコル。 • TFTP：TFTP サーバから取得したコンフィギュレーション ファイル。 • manual：コマンドライン インターフェイスで手動で変更。 • NVRAM：NVRAM のコンフィギュレーション ファイル。 • IPCP：**ip address negotiated** コマンド。 • DHCP：**ip address dhcp** コマンド。 • unset：設定解除。 • other：不明。
Status	インターフェイスのステータスを示します。有効な値とその意味は次のとおりです。 • up：インターフェイスはアップ状態です。 • down：インターフェイスはダウン状態です。 • administratively down：インターフェイスは管理のためにダウン状態です。
Protocol	このインターフェイスのルーティング プロトコルの動作ステータスを示します。

関連コマンド

コマンド	説明
ip address	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。

コマンド	説明
ip vrf autoclassify	送信元インターフェイスで VRF autoclassify をイネーブルにします。
match ip source	VRF 接続されたルートに基づいて設定された必須ルート マップに一致するように送信元 IP アドレスを指定します。
route-map	1 つのルーティング プロトコルから他のルーティング プロトコルへのルートを再配布するか、またはポリシー ルーティングをイネーブルにするための条件を定義します。
set vrf	ポリシー ベース ルーティングの VRF 選択のために、ルート マップ内での VPN VRF 選択をイネーブルにします。
show ip arp	SLIP アドレスがパーマネント ARP テーブル エントリとして表示される ARP キャッシュを表示します。
show route-map	スタティック ルート マップおよびダイナミック ルート マップを表示します。

show ip ssh

セキュア シェル（SSH）のバージョンおよび設定データを表示するには、特権 EXEC モードで **show ip ssh** コマンドを使用します。

show ip ssh

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.0(5)S	このコマンドが導入されました。
12.1(1)T	このコマンドが Cisco IOS Release 12.1 T に統合されました。
12.1(5)T	このコマンドが SSH のステータス（イネーブルまたはディセーブル）を表示するように変更されました。
12.2(17a)SX	このコマンドが Cisco IOS Release 12.2(17a)SX に統合されました。
12.2(33)SRA	このコマンドが Cisco IOS Release 12.(33)SRA に統合されました。

使用上のガイドライン

再試行およびタイムアウトなどの、設定済みオプションのステータスを表示するには、**show ip ssh** コマンドを使用します。 このコマンドで、SSH がイネーブルか、またはディセーブルかを調べることができます。

例

次に、SSH がイネーブルの場合の **show ip ssh** コマンドの出力例を示します。

```
Router# show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
The following is sample output from the show ip ssh
 command when SSH has been disabled:
Router# show ip ssh
%SSH has not been enabled
```

関連コマンド

コマンド	説明
show ssh	SSH サーバ接続のステータスを表示します。

show ipv6 access-list

現在のすべての IPv6 アクセス リストの内容を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 access-list** コマンドを使用します。

show ipv6 access-list [*access-list-name*]

構文の説明

access-list-name	（任意）アクセス リストの名前

コマンド デフォルト

すべての IPv6 アクセス リストが表示されます。

コマンド モード

ユーザ EXEC 特権 EXEC

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.0(23)S	priority フィールドが sequence に変更され、レイヤ 4 プロトコル情報（拡張IPv6アクセスリスト機能）が出力表示に追加されました。
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
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(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.2(50)SY	このコマンドが変更されました。 IPv4 および IPv6 ハードウェア統計情報に関する情報が表示されます。

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

IPv6 専用である点を除いて、**show ipv6 access-list** コマンドの出力は **show ip access-list** コマンドと類似しています。

例

次の例では、**show ipv6 access-list** コマンドで出力された inbound、tcptraffic、および outbound という名の IPv6 アクセス リストを示します。

```
Router# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
       left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
    (time left 296) sequence 2
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

次の出力例は、IPSec で使用するための IPv6 アクセス リスト情報を示します。

```
Router#  show ipv6 access-list
IPv6 access list Tunnel0-head-0-ACL (crypto)
     permit ipv6 any any (34 matches) sequence 1
IPv6 access list Ethernet2/0-ipsecv6-ACL (crypto)
     permit 89 FE80::/10 any (85 matches) sequence 1
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *10*：*show ipv6 access-list* のフィールドの説明

フィールド	説明
ipv6 access list inbound	IPv6 アクセス リスト名（例：inbound）。
permit	指定されたプロトコル タイプと一致するパケットを許可します。
tcp	伝送制御プロトコル。パケットが一致しなければならない高いレベル（レイヤ 4）のプロトコル タイプ。
any	::/0 と同じです。
eq	TCP または UDP パケットの送信元または宛先ポートを比較する equal オペランド。

フィールド	説明
bgp	ボーダー ゲートウェイ プロトコル。 パケットが同じでなければならない低いレベル（レイヤ3）のプロトコル タイプ。
reflect	再帰 IPv6 アクセス リストを示します。
tcptraffic (8 matches)	再帰 IPv6 アクセス リストの名前およびアクセス リストとの一致の数。 **clear ipv6 access-list** 特権EXECコマンドは、IPv6アクセスリストの一致カウンタをリセットします。
sequence 10	着信パケットが比較されるアクセスリストの行のシーケンス。 アクセス リストの行は、最初のプライオリティ（最低の数、たとえば10）から最後のプライオリティ（最高の数、たとえば80）の順に並んでいます。
host 2001:0DB8:1::1	パケットの送信元アドレスが一致する必要がある、送信元 IPv6 ホスト アドレス。
host 2001:0DB8:1::2	パケットの宛先アドレスが一致する必要がある、宛先 IPv6 ホスト アドレス。
11000	発信接続用のエフェメラル送信元ポート番号。
timeout 300	アイドル時間の合計間隔（秒単位）。これを過ぎると、tcptraffic という名前の一時的な IPv6 再帰アクセスリストが、示されたセッションに対してタイムアウトします。
(time left 243)	残りの合計アイドル時間（秒単位）。これを過ぎると、tcptraffic という名前の一時的な IPv6 再帰アクセスリストが、示されたセッションに対して削除されます。 示されたセッションに一致する追加受信トラフィックにより、この値は 300 秒にリセットされます。
evaluate udptraffic	udptraffic という名前の IPv6 再帰アクセス リストが、outbound という名前の IPv6 アクセス リスト内にネストされていることを示します。

関連コマンド

コマンド	説明
clear ipv6 access-list	IPv6 アクセス リストの一致カウンタをリセットします。
hardware statistics	ハードウェア統計情報の収集をイネーブルにします。
show ip access-list	現在のすべての IP アクセス リストの内容を表示します。
show ip prefix-list	プレフィックス リストまたはプレフィックス リスト エントリに関する情報を表示します。
show ipv6 prefix-list	IPv6 プレフィックス リストまたは IPv6 プレフィックスリストのエントリに関する情報を表示します。

show mab

MAC 認証バイパス（MAB）情報を表示するには、特権 EXEC モードで **show mab** コマンドを使用します。

show mab {**all**| **interface** *type number*} **[detail]**

構文の説明

all	すべてのインターフェイスを指定します。
interface *type number*	MAB 情報を表示する、特定のインターフェイスを指定します。
detail	（任意）詳細情報を表示します。

コマンド モード

特権 EXEC（#）

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(3)T	このコマンドが変更されました。 認証結果のステータスは、コマンド出力で AUTHORIZED または UNAUTHORIZED ではなく、SUCCESS または FAIL で表示されます。

使用上のガイドライン

show mab コマンドを使用して、MAB ポートおよび MAB セッションに関する情報を表示します。

例

次に、MAB セッションが許可された場合の **show mab interface detail** コマンドの出力例を示します。

```
Switch# show mab interface
FastEthernet1/0/1
 detail
MAB details for FastEthernet1/0/1
--------------------------------------
Mac-Auth-Bypass           = Enabled
Inactivity Timeout        = None
```

```
MAB Client List
---------------
Client MAC                = 000f.23c4.a401
MAB SM state              = TERMINATE
Auth Status               = SUCCESS
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *11*：*show mab* のフィールドの説明

フィールド	説明
Mac-Auth-Bypass	MAB をイネーブルにするか、ディセーブルにするかを指定します。
Inactivity Timeout	これを過ぎるとセッションが終了する、アクティビティなしの期間。
Client MAC	クライアントの MAC アドレス。
MAB SM state	MAB ステート マシンの状態。 開始から終了までに使用される値は次のとおりです。 • INITIALIZE：初期化されているときのセッションの状態。 • ACQUIRING：MACアドレスをクライアントから取得しているときのセッションの状態。 • AUTHORIZING：MAC アドレスを許可しているときのセッションの状態。 • TERMINATE：許可結果が取得されたときのセッションの状態。
Auth Status	MAB セッションの許可ステータス。 次の値が可能です。 • SUCCESS：セッションが正常に許可されました。 • FAIL：セッションは許可されませんでした。

関連コマンド

コマンド	説明
show authentication interface	特定のインターフェイスの認証マネージャに関する情報を表示します。
show authentication registrations	認証マネージャに登録されている認証方式に関する情報を表示します。
show authentication sessions	認証マネージャ セッションに関する情報を表示します。

show mac-address-table

MAC アドレス テーブルを表示するには、特権 EXEC モードで **show mac-address-table** コマンドを使用します。

Cisco 2600, 3600, and 3700 Series Routers

show mac-address-table [**secure**| **self**| **count**][**address***macaddress*][**interface***type/number*]{**fa** | **gi***slot/port*}[**atm***slot/port*][**atm***slot/port*][**vlan***vlan-id*]

Catalyst 4500 Series Switches

show mac-address-table {**assigned**| **ip**| **ipx**| **other**}

Catalyst 6000/6500 Series Switches and 7600 Series Routers

show mac-address-table [**address** *mac-addr* [**all** | **interface** *type/number* | **module** *number* | **vlan** *vlan-id*] | **aging-time** [**vlan** *vlan-id*] | **count**[**module** *number* | **vlan** *vlan-id*] | **interface** *type/number* | **limit** [**vlan** *vlan-id* | **module** *number* | **interface** *type*] | **module** *number* | **multicast** [**count**] [**igmp-snooping** | **mld-snooping** | **user**][**vlan** *vlan-id*] | **notification** {**mac-move**[**counter**[**vlan**]]| **threshold**| **change**}[**interface** [*number*]] | **synchronize statistics** | **unicast-flood** | **vlan** *vlan-id* [**all**| **module** *number*]]

構文の説明

secure	（任意）セキュアアドレスだけを表示します。
self	（任意）スイッチ自体が追加したアドレスだけを表示します。
count	（任意）MAC アドレス テーブル内の現在のエントリ数を表示します。
address *mac-addr*	（任意）特定の MAC アドレスの MAC アドレステーブルに関する情報を表示します。フォーマットの詳細については、「Usage Guidelines」のセクションを参照してください。
interface *type* / *number*	（任意）特定のインターフェイスのアドレスを表示します。 Catalyst 6500 および 6000 シリーズ スイッチの場合、有効値は **atm**、**fastethernet**、**gigabitethernet**、および **port-channel** です。 Cisco 7600 シリーズの場合、有効値は **atm**、**ethernet**、**fastethernet**、**ge-wan**、**gigabitethernet**、**tengigabitethernet**、および **pos** です。
fa	（任意）ファスト イーサネット インターフェイスを指定します。

gi	（任意）ギガビットイーサネットインターフェイスを指定します。
slot / *port*	（任意）スロット 1 または 2 のモジュールにダイナミックアドレスを追加します。スラッシュ記号が必要です。
atm *slot /port*	（任意）ATM モジュール *slot/port* にダイナミック アドレスを追加します。 スロット番号には 1 または 2 を使用します。 ポート番号として 0 を使用します。 スラッシュ記号が必要です。
vlan *vlan -id*	（任意）特定の VLAN のアドレスを表示します。 Cisco 2600、3600、および 3700 シリーズの場合、有効値は 1 ～ 1005 です。先行ゼロを入力しないでください。 Cisco IOS Release 12.4(15)T 以降、有効な VLAN ID の範囲は 1 ～ 4094 です。 Catalyst 6500 および 6000 シリーズ スイッチおよび 7600 シリーズの場合、有効値は 1 ～ 4094 です。
assigned	割り当てられたプロトコルエントリを指定します。
ip	IP プロトコル エントリを指定します。
ipx	IPX プロトコル エントリを指定します。
other	その他のプロトコル エントリを指定します。
all	（任意）転送テーブル内にある、指定された MAC アドレスのすべてのインスタンスを表示します。
type / *number*	（任意）モジュールおよびインターフェイス番号
module *number*	（任意）特定の Distributed Forwarding Card（DFC）モジュールの MAC アドレス テーブルに関する情報を表示します。
aging-time	（任意）VLAN のエージング タイムを表示します。

limit	MAC 使用情報を表示します。
multicast	マルチキャスト MAC アドレス テーブル エントリに関する情報だけを表示します。
igmp-snooping	インターネット グループ管理プロトコル（IGMP）スヌーピングによって学習されたアドレスを表示します。
mld-snooping	Multicast Listener Discover version 2（MLDv2）スヌーピングによって学習されたアドレスを表示します。
user	手動で入力された（スタティック）アドレスを表示します。
notification mac-move	MAC 移動通知ステータスを表示します。
notification mac-move counter	（任意）MAC が移動した回数およびシステムで発生したこれらのインスタンスの数を表示します。
vlan	（任意）表示する VLAN を指定します。Catalyst 6500 および 6000 シリーズ スイッチおよび 7600 シリーズの場合、有効値は 1 ～ 4094 です。
notification threshold	連想メモリ（CAM）テーブル利用通知ステータスを表示します。
notification change	MAC 通知パラメータおよび履歴テーブルを表示します。
synchronize statistics	スイッチ プロセッサまたは DFC で収集された統計情報を表示します。
unicast-flood	ユニキャスト フラッディング情報を表示します。

コマンド モード　特権 EXEC（#）

コマンド履歴

リリース	変更内容
11.2(8)SA	このコマンドが導入されました。
11.2(8)SA3	このコマンドが変更されました。 **aging-time** 、**count**、**self**、および **vlan** *vlan -id* キーワードと引数が追加されました。
11.2(8)SA5	このコマンドが変更されました。 **atm***slot*/*port* キーワードと引数のペアが追加されました。
12.2(2)XT	このコマンドが変更されました。 このコマンドが Cisco 2600、3600、および 3700 シリーズ ルータに実装されました。
12.1(8a)EW	このコマンドが変更されました。 このコマンドが Catalyst 4500 シリーズ スイッチに実装されました。
12.2(8)T	このコマンドが、Cisco 2600、3600、および 3700 シリーズ ルータの Cisco IOS Release 12.2(8)T に統合されました。
12.2(11)T	このコマンドが Cisco IOS Release 12.2(11)T に統合されました。
12.2(14)SX	このコマンドが変更されました。 このコマンドがスーパーバイザ エンジン 720 に実装されました。
12.2(17a)SX	このコマンドが変更されました。 Catalyst 6500 および 6000 シリーズ スイッチ、7600 シリーズの場合、次のオプションのキーワードおよび引数をサポートするようにこのコマンドが変更されました。 • **count module** *number* • **limit** [**vlan** *vlan-id* | **port** *number* | **interface** *interface-type* • **notification threshold** • **unicast-flood**
12.2(17d)SXB	このコマンドが変更されました。 このコマンドのサポートが Supervisor Engine 2 に追加されました。
12.2(18)SXE	このコマンドが変更されました。 Catalyst 6500 および 6000 シリーズ スイッチ、Cisco 7600 シリーズの場合、Supervisor Engine 720 上でのみ **mld-snooping** キーワードのサポートが追加されました。
12.2(18)SXF	このコマンドが変更されました。 Catalyst 6500 および 6000 シリーズ スイッチ、Cisco 7600 シリーズの場合、Supervisor Engine 720 上でのみ **synchronizestatistics** キーワードのサポートが追加されました。

リリース	変更内容
12.2(33)SRA	このコマンドが変更されました。 このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.4(15)T	このコマンドは、指定されたプラットフォームに対する VLAN ID の有効範囲を 1 ～ 4094 に拡張するために修正されました。
12.2(33)SXH	このコマンドが変更されました。 **change** キーワードが追加されました。
12.2(33)SXI	このコマンドが変更され、**counter** キーワードが追加されました。

使用上のガイドライン

Cisco 2600、3600、および 3700 シリーズ ルータ

show mac-address-table コマンドは、スイッチの MAC アドレス テーブルを表示します。 オプションのキーワードおよび引数を使用することによって、特定のビューを定義できます。 複数のオプションのキーワードが使用される場合は、表示されるそのエントリに対して、すべての条件が当てはまる必要があります。

Catalyst 4500 シリーズ スイッチ

ルーテッド ポートで使用される MAC アドレス テーブル エントリの場合、「vlan」カラムには内部 VLAN 番号ではなくルーテッド ポートの名前が表示されます。

Catalyst 6000 および 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ

モジュール番号を指定しないと、 **show mac-address-table** コマンドの出力にスーパーバイザ エンジンに関する情報が表示されます。 DFC の MAC アドレス テーブルに関する情報を表示するには、モジュール番号または **all** キーワードを入力する必要があります。

mac-addr の値は 48 ビット MAC アドレスです。 有効なフォーマットは H.H.H です。

interface *number* 引数では、モジュールおよびポート番号を指定します。 有効値は、指定されたインターフェイス タイプ、および使用されるシャーシとモジュールによって異なります。 たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ～ 13、ポート番号の有効値は 1 ～ 48 になります。

オプションの **module** *number* キーワードと引数のペアは、DFC モジュールだけでサポートされています。 **module** *number* キーワードと引数のペアは、モジュール番号を指定します。

mac-group-address 引数の有効値は 1 ～ 9 です。

オプションの **count** キーワードは、マルチキャスト エントリ数を表示します。

オプションの **multicast** キーワードは、VLAN 内のマルチキャスト MAC アドレス（グループ）を表示したり、スタティックに導入された、または IGMP スヌーピングによって学習されたレイヤ 2 テーブル内のすべてのエントリを表示したりします。

show mac-address-table unicast-flood コマンドの出力で表示される情報は次のとおりです。

- フィルタ モードの使用を設定されていないすべての VLAN 間で共有された、最大 50 のフラッディング エントリを記録できます。
- 出力フィールドの表示は、次のように定義されます。
  - ALERT：情報は約 3 秒ごとに更新されます。
  - SHUTDOWN：情報は約 3 秒ごとに更新されます。

（注） 宛先 MAC アドレスで表示される情報は、ポートがシャットダウンしてフラッディングが停止するとただちに削除されます。

- 情報はフィルタを導入するたびに更新されます。 この情報はフィルタを削除するまで維持されます。

Learn フィールドに表示されるダイナミック エントリは、常に Yes に設定されます。

show mac-address-table limit コマンドの出力は、次の情報を表示します。

- MAC アドレスの現在数
- 許可された MAC エントリの最大数
- 使用率（%）

show mac-address-table synchronize statistics コマンドの出力は、次の情報を表示します。

- 各時間間隔で処理されるメッセージ数
- 同期化用に送信されるアクティブ エントリの数
- 更新されたエントリ、作成されたエントリ、無視されたエントリ、または失敗したエントリの数

例

次に、**show mac-address-table** コマンドの出力例を示します。

```
Switch# show mac-address-table

Dynamic Addresses Count:                 9
Secure Addresses (User-defined) Count: 0
Static Addresses (User-defined) Count: 0
System Self Addresses Count:             41
Total MAC addresses:                     50
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0010.0de0.e289       Dynamic          1  FastEthernet0/1
0010.7b00.1540       Dynamic          2  FastEthernet0/5
0010.7b00.1545       Dynamic          2  FastEthernet0/5
0060.5cf4.0076       Dynamic          1  FastEthernet0/1
0060.5cf4.0077       Dynamic          1  FastEthernet0/1
0060.5cf4.1315       Dynamic          1  FastEthernet0/1
0060.70cb.f301       Dynamic          1  FastEthernet0/1
```

```
00e0.1e42.9978       Dynamic          1  FastEthernet0/1
00e0.1e9f.3900       Dynamic          1  FastEthernet0/1
```

例

次の例では、特定のプロトコル タイプ（この場合は「assigned」）の MAC アドレス テーブル エントリを表示する方法を示します。

```
Switch# show mac-address-table protocol assigned

vlan   mac address     type    protocol  qos             ports
-----+---------------+--------+---------+---+--------------------------------
 200  0050.3e8d.6400  static   assigned  --  Switch
 100  0050.3e8d.6400  static   assigned  --  Switch
   5  0050.3e8d.6400  static   assigned  --  Switch
4092  0000.0000.0000  dynamic  assigned  --  Switch
   1  0050.3e8d.6400  static   assigned  --  Switch
   4  0050.3e8d.6400  static   assigned  --  Switch
4092  0050.f0ac.3058  static   assigned  --  Switch
4092  0050.f0ac.3059  dynamic  assigned  --  Switch
   1  0010.7b3b.0978  dynamic  assigned  --  Fa5/9
```

次に、上記の例の「other」の出力を表示する例を示します。

```
Switch# show mac-address-table protocol other

Unicast Entries
 vlan   mac address     type        protocols               port
-------+---------------+--------+---------------------+--------------------
   1    0000.0000.0201   dynamic other                  FastEthernet6/15
   1    0000.0000.0202   dynamic other                  FastEthernet6/15
   1    0000.0000.0203   dynamic other                  FastEthernet6/15
   1    0000.0000.0204   dynamic other                  FastEthernet6/15
   1    0030.94fc.0dff    static ip,ipx,assigned,other  Switch
   2    0000.0000.0101   dynamic other                  FastEthernet6/16
   2    0000.0000.0102   dynamic other                  FastEthernet6/16
   2    0000.0000.0103   dynamic other                  FastEthernet6/16
   2    0000.0000.0104   dynamic other                  FastEthernet6/16
Fa6/1   0030.94fc.0dff    static ip,ipx,assigned,other  Switch
Fa6/2   0030.94fc.0dff    static ip,ipx,assigned,other  Switch
Multicast Entries
 vlan    mac address     type    ports
-------+---------------+-------+-----------------------------------------------
   1    ffff.ffff.ffff   system Switch,Fa6/15
   2    ffff.ffff.ffff   system Fa6/16
1002    ffff.ffff.ffff   system
1003    ffff.ffff.ffff   system
1004    ffff.ffff.ffff   system
1005    ffff.ffff.ffff   system
Fa6/1   ffff.ffff.ffff   system Switch,Fa6/1
Fa6/2   ffff.ffff.ffff   system Switch,Fa6/2
```

例

次に、**show mac-address-table** コマンドの出力例を示します。

```
Switch# show mac-address-table

Dynamic Addresses Count:                9
Secure Addresses (User-defined) Count: 0
Static Addresses (User-defined) Count: 0
System Self Addresses Count:           41
Total MAC addresses:                   50
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
```

```
0010.0de0.e289       Dynamic          1  FastEthernet0/1
0010.7b00.1540       Dynamic          2  FastEthernet0/5
0010.7b00.1545       Dynamic          2  FastEthernet0/5
0060.5cf4.0076       Dynamic          1  FastEthernet0/1
0060.5cf4.0077       Dynamic          1  FastEthernet0/1
0060.5cf4.1315       Dynamic          1  FastEthernet0/1
0060.70cb.f301       Dynamic          1  FastEthernet0/1
00e0.1e42.9978       Dynamic          1  FastEthernet0/1
00e0.1e9f.3900       Dynamic          1  FastEthernet0/1
```

（注） 分散 Distributed Encoded Address Recognition Logic（EARL）スイッチでは、アスタリスク（*）はこの EARL に対応付けられたポート上で学習された MAC アドレスを示します。

次に、Supervisor Engine 720 で特定の MAC アドレスの MAC アドレス テーブルに関する情報を表示する例を示します。

```
Switch# show mac-address-table address 001.6441.60ca

Codes: * - primary entry
  vlan   mac address     type    learn qos            ports
------+----------------+--------+-----+---+--------------------------
Supervisor:
*  ---  0001.6441.60ca    static  No    --  Router
```

次に、Supervisor Engine 720 で特定の MAC アドレスの MAC アドレス テーブルに関する情報を表示する例を示します。

```
Router# show mac-address-table address 0100.5e00.0128

Legend: * - primary entry
        age - seconds since last seen
        n/a - not available
  vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
Supervisor:
*   44  0100.5e00.0128    static  Yes          -   Fa6/44,Router
*    1  0100.5e00.0128    static  Yes          -   Router
Module 9:
*   44  0100.5e00.0128    static  Yes          -   Fa6/44,Router
*    1  0100.5e00.0128    static  Yes          -   Router
```

次に、すべての VLAN に現在設定されているエージング タイムを表示する例を示します。

```
Switch# show mac-address-table aging-time

Vlan    Aging Time
----    ----------
*100     300
200     1000
```

次に、特定のスロットのエントリ数を表示する例を示します。

```
Switch# show mac-address-table count module 1

MAC Entries on slot 1 :
Dynamic Address Count:                4
Static Address (User-defined) Count:  25
Total MAC Addresses In Use:           29
Total MAC Addresses Available:        131072
```

次に、Supervisor Engine 720 で特定のインターフェイスの MAC アドレス テーブルに関する情報を表示する例を示します。

```
Switch# show mac-address-table interface fastethernet 6/45

Legend: * - primary entry
        age - seconds since last seen
        n/a - not available
  vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
*   45  00e0.f74c.842d   dynamic  Yes          5   Fa6/45
```

（注） 先行アスタリスク（*）は、外部装置から特定のモジュールへの着信パケットに基づいて学習された MAC アドレスからのエントリを示します。

次に、特定のスロットの制限に関する情報を表示する例を示します。

```
Switch# show mac-address-table limit vlan 1 module 1

vlan    switch   module    action      maximum  Total entries  flooding
-------+--------+---------+-----------+--------+--------------+------------
1          1        7       warning      500      0             enabled
1          1        11      warning      500      0             enabled
1          1        12      warning      500      0             enabled

Router#show mac-address-table limit vlan 1 module 2

vlan    switch   module    action      maximum  Total entries  flooding
-------+--------+---------+-----------+--------+--------------+------------
1          2         7      warning      500      0             enabled
1          2         9      warning      500      0             enabled
```

次に、MAC-move 通知ステータスを表示する例を示します。

```
Switch# show mac-address-table notification mac-move

MAC Move Notification: Enabled
```

次に、MAC-move 統計情報を表示する例を示します。

```
Router# show mac-address-table notification mac-move counter

-------------------------------------------------------------------------------------
Vlan Mac Address From Mod/Port To Mod/Port Count
---- ----------------- ---------------------- ---------------------- ------------
1 00-01-02-03-04-01 2/3 3/1 10
20 00-01-05-03-02-01 5/3 5/1 20
```

次に、CAM-table 使用率通知ステータスを表示する例を示します。

```
Router# show mac-address-table notification threshold

Status limit Interval
-------------+-----------+-------------
enabled 1 120
```

次に、MAC 通知パラメータおよびヒストリ テーブルを表示する例を示します。

```
Switch# show mac-address-table notification change
```

```
MAC Notification Feature is Disabled on the switch
MAC Notification Flags For All Ethernet Interfaces :
--------------------------------------------------
Interface                   MAC Added Trap MAC Removed Trap
--------------------        -------------- ----------------
```

次に、特定のインターフェイスの MAC 通知パラメータおよびヒストリ テーブルを表示する例を示します。

```
Switch# show mac-address-table notification change interface gigabitethernet5/2

MAC Notification Feature is Disabled on the switch
Interface                   MAC Added Trap MAC Removed Trap
--------------------        -------------- ----------------
GigabitEthernet5/2          Disabled       Disabled
```

次に、unicast-flood 情報を表示する例を示します。

```
Switch# show mac-address-table unicast-flood

> > Unicast Flood Protection status: enabled
> >
> > Configuration:
> > vlan Kfps action timeout
> > ------+----------+-----------------+----------
> > 2 2 alert none
> >
> > Mac filters:
> > No. vlan source mac addr. installed
> > on time left (mm:ss)
> >
> >-----+------+-----------------+------------------------------+------------------
> >
> > Flood details:
> > Vlan source mac addr. destination mac addr.
> >
> >------+---------------+-----------------------------------------------------
> > 2 0000.0000.cafe 0000.0000.bad0, 0000.0000.babe,
> > 0000.0000.bac0
> > 0000.0000.bac2, 0000.0000.bac4,
> > 0000.0000.bac6
> > 0000.0000.bac8
> > 2 0000.0000.caff 0000.0000.bad1, 0000.0000.babf,
> > 0000.0000.bac1
> > 0000.0000.bac3, 0000.0000.bac5,
> > 0000.0000.bac7
> > 0000.0000.bac9
```

次に、特定の VLAN の MAC アドレス テーブルに関する情報を表示する例を示します。

```
Switch#show mac-address-table vlan 100

vlan   mac address     type    protocol  qos             ports
-----+---------------+--------+---------+---+--------------------------------
 100  0050.3e8d.6400  static   assigned  --  Router
 100  0050.7312.0cff  dynamic        ip  --  Fa5/9
 100  0080.1c93.8040  dynamic        ip  --  Fa5/9
 100  0050.3e8d.6400  static        ipx  --  Router
 100  0050.3e8d.6400  static      other  --  Router
 100  0100.0cdd.dddd  static      other  --  Fa5/9,Router,Switch
 100  00d0.5870.a4ff  dynamic        ip  --  Fa5/9
 100  00e0.4fac.b400  dynamic        ip  --  Fa5/9
 100  0100.5e00.0001  static         ip  --  Fa5/9,Switch
 100  0050.3e8d.6400  static         ip  --  Router
```

次に、MLDv2 スヌーピングの MAC アドレス テーブルに関する情報を表示する例を示します。

```
Switch# show mac-address-table multicast mld-snooping

vlan mac address type learn qos ports
-----+---------------+--------+-----+---+--------------------------------
--- 3333.0000.0001 static Yes - Switch,Stby-Switch
--- 3333.0000.000d static Yes - Fa2/1,Fa4/1,Router,Switch
--- 3333.0000.0016 static Yes - Switch,Stby-Switch
```

下の表で、この出力で表示される重要なフィールドについて説明します。

表 *12*：*show mac-address-table* のフィールドの説明

フィールド	説明
Dynamic Addresses Count	MAC アドレス テーブルのダイナミック アドレスの総数。
Secure Addresses (User-defined) Count	MAC アドレス テーブルのセキュア アドレスの総数。
Static Addresses (User-defined) Count	MAC アドレス テーブルのスタティック アドレスの総数。
System Self Addresses Count	MAC アドレス テーブルのアドレスの総数。
Total MAC addresses	MAC アドレス テーブルの MAC アドレスの総数。
Destination Address	MAC アドレス テーブルに存在する宛先アドレス。
Address Type	アドレス タイプ（static または dynamic）。
VLAN	VLAN 番号。
Destination Port	MAC アドレス テーブルに存在する宛先ポートに関する情報。
mac address	エントリの MAC アドレス。
protocol	MACアドレステーブルに存在するプロトコル。
qos	MAC アドレス テーブルに関連付けられる Quality of Service。
ports	ポート タイプ。

フィールド	説明
age	インターフェイスの最後のオカレンス後の経過時間（秒単位）。
Aging Time	エントリのエージング タイム。
module	モジュール番号。
action	アクションのタイプ。
flooding	フラッディングの状態。

関連コマンド

コマンド	説明
clear mac-address-table	MAC アドレス テーブルからエントリを削除します。
mac-address-table aging-time	レイヤ2テーブル内のエントリにエージング タイムを設定します。
mac-address-table limit	MAC 制限をイネーブルにします。
mac-address-table notification mac-move	MAC 移動通知をイネーブルにします。
mac-address-table static	MAC アドレス テーブルにスタティック エントリを追加するか、アドレスの IGMP スヌーピングがディセーブルになっているスタティック MAC アドレスを設定します。
mac-address-table synchronize	レイヤ 2 MAC アドレス テーブルのエントリを PFC およびすべての DFC 間で同期化します。
show mac-address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。

show parameter-map type consent から show users まで

show port-security

EXEC コマンドモードのポートセキュリティ設定に関する情報を表示するには、**show port-security** コマンドを使用します。

show port-security [**interface** *interface interface-number*]

show port-security [**interface** *interface interface-number*] {**address**| **vlan**}

構文の説明

interface *interface*	（任意）インターフェイス タイプを指定します。有効値は **ethernet**、**fastethernet**、**gigabitethernet**、および **longreachethernet** です。
interface-number	インターフェイス番号を指定します。 有効値の範囲は 1 ～ 6 です。
address	すべてのスイッチインターフェイスまたは指定されたインターフェイスに設定されたすべてのセキュア MAC アドレス、および各アドレスのエージング情報を表示します。
vlan	Virtual LAN（仮想 LAN）。

コマンド デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	Supervisor Engine 2 上のこのコマンドのサポートがリリース 12.2(17d)SXB に拡張されました。
12.2(18)SXE	**address** キーワードが追加され、Supervisor Engine 720 のトランク ポートで VLAN 単位で設定されている MAC アドレスの最大数のみを表示できるようになりました。
12.2(33)SRA	このコマンドが Cisco IOS Release 12.(33)SRA に統合されました。

使用上のガイドライン

vlan キーワードは、トランク ポートだけでサポートされ、トランク ポートに対して設定された VLAN あたりの最大数を表示します。

interface-number 引数では、モジュールおよびポート番号を指定します。 *interface-number* の有効な値は、指定するインターフェイス タイプと、使用するシャーシおよびモジュールによって異なります。 たとえば、13 スロット シャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビットイーサネットインターフェイスを指定すると、モジュール番号の有効値は 1 ～ 13、ポート番号の有効値は 1 ～ 48 になります。

例

次に、オプションを指定しなかった場合の **show port-security** コマンドの出力例を示します。

```
Router# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security
Action
                    (Count)        (Count)      (Count)
------------------------------------------------------------------------------

     Fa5/1           11            11            0            Shutdown
     Fa5/5           15            5             0            Restrict
     Fa5/11          5             4             0            Protect
------------------------------------------------------------------------------

Total Addresses in System: 21
Max Addresses limit in System: 128
Router#
```

次に、指定されたインターフェイスのポートセキュリティ情報を表示する例を示します。

```
Router# show port-security interface fastethernet 5/1
Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 11
Total MAC Addresses: 11
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
Router#
```

次に、すべてのスイッチ インターフェイスまたは指定されたインターフェイスに設定されたすべてのセキュア MAC アドレス、および各アドレスのエージング情報を表示する例を示します。

```
Router# show port-security address
Default maximum: 10
VLAN Maximum Current
1    5       3
2    4       4
3    6       4
Router#
```

関連コマンド

コマンド	説明
clear port-security	MAC アドレス テーブルからセキュア MAC アドレスおよびスティッキ MAC アドレスを削除します。

show privilege

現在の特権レベルを表示するには、EXEC モードで **show privilege** コマンドを使用します。

show privilege

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
10.3	このコマンドが導入されました。
12.2(33)SRA	このコマンドが Cisco IOS Release 12.(33)SRA に統合されました。
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す。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。

例

次に、**show privilege** コマンドの出力例を示します。 現在の特権レベルは 15 です。

```
Router# show privilege
Current privilege level is 15
```

関連コマンド

コマンド	説明
enable password	さまざまな権限レベルへのアクセスを制御するローカル パスワードを設定します。
enable secret	**enable password** コマンドよりも強化したセキュリティ レイヤを指定します。

show radius statistics

アカウンティング パケットと認証パケットに関する RADIUS 統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show radius statistics** コマンドを使用します。

show radius statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.1(3)T	このコマンドが導入されました。
12.2(33)SRA	このコマンドが Cisco IOS Release 12.(33)SRA に統合されました。
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す。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。
15.1(1)S	このコマンドが Cisco IOS Release 15.1(1)S に統合されました。CISCO-RADIUS-EXT-MIB のサポートが追加されました。
15.1(4)M	このコマンドが変更されました。CISCO-RADIUS-EXT-MIB のサポートが追加されました。

例

次に、**show radius statistics** コマンドの出力例を示します。

```
Router# show radius statistics
                                  Auth.      Acct.       Both
Maximum inQ length:                NA         NA         1
Maximum waitQ length:              NA         NA         2
Maximum doneQ length:              NA         NA         1
Total responses seen:              33         67         100
Packets with responses:            33         67         100
Packets without responses:         0          0          0
Access Rejects           :         0
Average response delay(ms) :       1331       124        523
Maximum response delay(ms):        5720       4800       5720
Number of Radius timeouts:         8          2          10
Duplicate ID detects:              0          0           0
Buffer Allocation Failures:        0          0           0
```

```
Maximum Buffer Size (bytes):     156        327        327
Malformed Responses         :    0          0          0
Bad Authenticators          :    0          0          0
Source Port Range: (2 ports only)
1645 - 1646
Last used Source Port/Identifier:
1645/33
1646/69
```

下の表で、この出力で表示される重要なフィールドについて説明します。

表 *13*：*show radius statistics* のフィールドの説明

フィールド	説明
Auth.	認証パケットの統計情報。
Acct.	アカウンティング パケットの統計情報。
Both	認証パケットとアカウンティングパケットの合計統計情報。
Maximum inQ length	未送信のRADIUSメッセージを保持するキューで許可される、最大エントリ数。
Maximum waitQ length	送信済みで応答を待っているRADIUSメッセージを保持するキューで許可される、最大エントリ数。
Maximum doneQ length	応答を受信済みで、メッセージを待っているコードに転送される予定のRADIUSメッセージを保持するキューで許可される、最大エントリ数。
Total responses seen	サーバから見た、RADIUS応答数。予想されるパケット数に加えて、この数には繰り返しのパケットと、waitQ に一致するメッセージがないパケットも含まれます。
Packets with responses	RADIUS サーバから応答を受信したパケット数。
Packets without responses	いずれのRADIUSサーバからも応答を受信しなかったパケット数。
Access Rejects	RADIUSサーバによってアクセス要求が拒否された回数。

フィールド	説明
Average response delay	パケットが最初に送信されてから、応答を受信するまでの平均時間（ミリ秒（ms）単位）。応答がタイムアウトし、パケットが再送信された場合は、この値にはタイムアウトが含まれます。パケットが応答を受信していない場合、この値は平均に含まれません。
Maximum response delay	平均応答遅延情報を収集している間に観測された、最大遅延（ms 単位）。
Number of RADIUS timeouts	サーバが応答せず、RADIUS サーバがパケットを再送信した回数。
Duplicate ID detects	RADIUS には、最大 255 個の一意の ID があります。 場合によっては、255 個を超える未処理のパケットがあります。パケットが受信されると、doneQ は最も古いエントリから新しいエントリの順で検索されます。 ID が同じ場合、より高度な手法を使用して応答がこのエントリに一致するかどうかが確認されます。応答が一致しない場合、重複 ID 検出カウンタが増加します。
Buffer Allocation Failures	バッファを割り当てられなかった回数。
Maximum Buffer Size (bytes)	バッファの最大サイズを表示します。
Malformed Responses	破損していた応答の数。ほとんどの場合、Bad Authenticators が原因です。
Bad Authenticators	共有秘密の不一致による認証失敗の回数。
Source Port Range: (2 ports only)	ポート番号を表示します。
Last used Source Port/Identifier	認証のために最後に RADIUS サーバに使用されたポート。

出力のフィールドは、CISCO-RADIUS-EXT-MIB の簡易ネットワーク管理プロトコル（SNMP）オブジェクトにマッピングされ、SNMP レポートで使用されます。 レポートの最初の行は CISCO-RADIUS-EXT-MIB に次のようにマッピングされます。

- Maximum inQ length は creClientTotalMaxInQLength へマップ
- Maximum waitQ length は creClientTotalMaxWaitQLength へマップ

- Maximum doneQ length は creClientTotalMaxDoneQLength へマップ

出力のフィールド「Both」は、認証とアカウンティングの MIB オブジェクトから取得できます。出力に表示されている、各フィールドの計算式を次の表に示します。

表 *14*：*show radius statistics* コマンド出力の *Both* フィールドの計算式

show radius statistics コマンドの出力データ	Both フィールドの計算式
Maximum inQ length	creClientTotalMaxInQLength
Maximum waitQ length	creClientTotalWaitQLength
Maximum doneQ length	creClientDoneQLength
Total responses seen	creAuthClientTotalResponses + creAcctClientTotalResponses
Packets with responses	creAuthClientTotalPacketsWithResponses + creAcctClientTotalPacketsWithResponses
Packets without responses	creAuthClientTotalPacketsWithoutResponses + creAcctClientTotalPacketsWithoutResponses
Access Rejects	creClientTotalAccessRejects
Average response delay	creClientAverageResponseDelay
Maximum response delay	MAX(creAuthClientMaxResponseDelay, creAcctClientMaxResponseDelay)
Number of RADIUS timeouts	creAuthClientTimeouts + creAcctClientTimeouts
Duplicate ID detects	creAuthClientDupIDs + creAcctClientDupIDs
Buffer Allocation Failures	creAuthClientBufferAllocFailures + creAcctClientBufferAllocFailures
Maximum Buffer Size (bytes)	MAX(creAuthClientMaxBufferSize, creAcctClientMaxBufferSize)
Malformed Responses	creAuthClientMalformedResponses + creAcctClientMalformedResponses
Bad Authenticators	creAuthClientBadAuthenticators + creAcctClientBadAuthenticators

CISCO-RADIUS-EXT-MIB マップにリストされている次のオブジェクトのセットを、**show radius statistics** コマンドで表示されるフィールドにマップすることは簡単です。 たとえば、

creClientLastUsedSourcePort フィールドは、レポートの Last used Source Port/Identifier 部分に対応し、creAuthClientBufferAllocFailures は認証パケットの Buffer Allocation Failures に対応し、creAcctClientBufferAllocFailure はアカウンティング パケットの Buffer Allocation Failures に対応します。以下も同様です。

- creClientTotalMaxInQLength
- creClientTotalMaxWaitQLength
- creClientTotalMaxDoneQLength
- creClientTotalAccessRejects
- creClientTotalAverageResponseDelay
- creClientSourcePortRangeStart
- creClientSourcePortRangeEnd
- creClientLastUsedSourcePort
- creClientLastUsedSourceId
- creAuthClientBadAuthenticators
- creAuthClientUnknownResponses
- creAuthClientTotalPacketsWithResponses
- creAuthClientBufferAllocFailures
- creAuthClientTotalResponses
- creAuthClientTotalPacketsWithoutResponses
- creAuthClientAverageResponseDelay
- creAuthClientMaxResponseDelay
- creAuthClientMaxBufferSize
- creAuthClientTimeouts
- creAuthClientDupIDs
- creAuthClientMalformedResponses
- creAuthClientLastUsedSourceId
- creAcctClientBadAuthenticators
- creAcctClientUnknownResponses
- creAcctClientTotalPacketsWithResponses
- creAcctClientBufferAllocFailures
- creAcctClientTotalResponses
- creAcctClientTotalPacketsWithoutResponses
- creAcctClientAverageResponseDelay
- creAcctClientMaxResponseDelay

- creAcctClientMaxBufferSize
- creAcctClientTimeouts
- creAcctClientDupIDs
- creAcctClientMalformedResponses
- creAcctClientLastUsedSourceId

選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を検索およびダウンロードするには、http://www.cisco.com/go/mibs にある MIB Locator を使用してください。

関連コマンド

コマンド	説明
radius-server host	RADIUS サーバ ホストを指定します。
radius-server retransmit	Cisco IOS ソフトウェアが RADIUS サーバ ホストのリストを検索する回数の最大値を指定します。
radius-server timeout	サーバホストが応答するまでルータが待機する間隔を設定します。

show ssh

ルータ上のセキュア シェル（SSH）サーバの接続状態を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ssh** コマンドを使用します。

show ssh vty [*ssh-number*]

構文の説明

vty	仮想端末回線（VTY）接続の詳細を表示します。
ssh-number	（任意）ルータ上の SSH サーバ接続の数。 指定できる範囲は 0 ～ 1510 です。 デフォルト値は 0 です

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.1(15)T	このコマンドが導入されました。
12.2(33)SRA	このコマンドが変更されました。 Cisco IOS Release 12.2(33) SRA に統合されました。
12.2(33)SXI	このコマンドが変更されました。 Cisco IOS Release 12.2(33) SXI に統合されました。
Cisco IOS XE Release 2.1	このコマンドが変更されました。 Cisco IOS XE Release 2.1 に統合されました。

使用上のガイドライン

show ssh コマンドを使用して、ルータ上の SSH 接続のステータスを表示します。 このコマンドでは、SSH の設定データは表示されません。 タイムアウトや再試行回数などの SSH 設定情報を表示するには **show ip ssh** コマンドを使用します。

例

次に、SSH がイネーブルの場合の **show ssh** コマンドの出力例を示します。

```
Router# show ssh
```

```
Connection     Version      Encryption     State                Username
0               1.5         3DES           Session Started       guest
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 *15*：*show ssh* フィールドの説明

フィールド	説明
Connection	ルータ上の SSH 接続の数。
Version	SSH 端末のバージョン番号。
Encryption	転送暗号化のタイプ。
State	セッションが開始したか停止したかを示す、SSH 接続の状態。
Username	SSH にログインするためのユーザ名。

関連コマンド

コマンド	説明
show ip ssh	SSH のバージョンおよび設定データを表示します。

show vlan group から switchport port-security violation まで

single-connection

単一の TCP 接続を使用したすべての TACACS パケットの同じサーバへの送信をイネーブルにするには、TACACS+ サーバ コンフィギュレーション モードで **single-connection** コマンドを使用します。 この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

single-connection

no single-connection

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

TACACS パケットは単一の TCP 接続では送信されません。

コマンド モード

TACACS+ サーバ コンフィギュレーション（config-server-tacacs）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2S	このコマンドが導入されました。

使用上のガイドライン

single-connection コマンドを使用して、単一の TCP 接続を介してすべての TACACS パケットを同じサーバに向けて多重化します。

例

次に、単一の TCP 接続を介して、すべての TACACS パケットを TACACS サーバに向けて多重化する例を示します。

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# single-connection
```

関連コマンド

コマンド	説明
tacacs server	IPv6 または IPv4 に対して TACACS+ サーバを設定して、config server tacacs モードを開始します。

source

送信元アドレスに順次番号を付けるには、IKEv2 FlexVPN クライアント プロファイル コンフィギュレーション モードで **source** コマンドを使用します。 シーケンスを削除するには、このコマンドの **no** 形式を使用します。

source *sequence interface* **track** *track-number*

no source *sequence*

構文の説明

sequence	シーケンス番号を割り当てます。
interface	インターフェイスのタイプと番号
track *track-number*	トラック番号を使用して送信元アドレスをトラッキングします。

コマンド デフォルト

トラック ステータスは常にアップ状態です。

コマンド モード

IKEv2 FlexVPN クライアント プロファイル コンフィギュレーション（config-ikev2-flexvpn）

コマンド履歴

リリース	変更内容
15.2(1)T	このコマンドが導入されました。
Cisco IOS XE Release 3.7S	このコマンドが、Cisco IOS XE Release 3.7S に統合されました。

使用上のガイドライン

このコマンドをイネーブルにする前に、**crypto ikev2 client flexvpn** コマンドを設定する必要があります。

シーケンス番号が一番小さいものが送信元アドレスで、これに対しては送信元 IP アドレスがトンネル インターフェイスのトンネル VRF で使用可能な場合だけ、トラック オブジェクトがアップ状態になります。 送信元に対してセッションがアップ状態である場合、その送信元は「現在アクティブな送信元」と呼ばれます。

（注） このコマンドが変更された結果、アクティブなセッションが終了されます。

例

次に、スタティック ピアを定義する例を示します。

```
Router(config)# crypto ikev2 client flexvpn client1
Router(config-ikev2-flexvpn)# source 1 Ethernet 0/1 track 11
```

関連コマンド

コマンド	説明
crypto ikev2 client flexvpn	IKEv2 FlexVPN クライアント プロファイルを定義します。

ssh

リモート ネットワーキング デバイスとの暗号化されたセッションを開始するには、特権 EXEC モードまたはユーザ EXEC モードで **ssh** コマンドを使用します。

ssh [**-v** {**1**| **2**}| **c** {**3des**| **aes128-cbc**| **aes192-cbc**| **aes256-cbc**}| **-l** *userid*| **-l** *userid:vrfname number ip-address ip-address*| **-l** *userid:rotary number ip-address*| **-m** {**hmac-md5**| **hmac-md5-96**| **hmac-sha1**| **hmac-sha1-96**}| **-o numberofpasswordprompts** *n*| **-p** *port-num*] {**ip-addr**| **hostname**} [**command**| **-vrf**]

構文の説明

-v	（任意）サーバに接続するために使用する、セキュア シェル（SSH）のバージョンを指定します。 • **1**：SSH バージョン 1 を使用して接続します。 • **2**：SSH バージョン 2 を使用して接続します。

-c { 3des | aes128-cbc | aes192-cbc | aes256-cbc }	（任意）データの暗号化に使用する暗号化アルゴリズムとして、データ暗号規格（DES）、トリプルDES（3DES）、高度暗号化規格（AES）のいずれかを指定します。サポートされているAESアルゴリズムは、aes128-cbc、aes192-cbc、およびaes256-cbcです。 • SSHバージョン1を使用するには、ルータで暗号化イメージを実行していなければいけません。暗号化を含むCiscoソフトウェアイメージは、指定子「k8」（DES）または「k9」（3DES）を持ちます。 • SSHバージョン2は、aes128-cbc、aes192-cbc、aes256-cbcおよび3des-cbc暗号化アルゴリズムだけをサポートしています。SSHバージョン2は、3DESイメージでのみサポートされています。 • **-c**キーワードを指定しない場合、ネゴシエーション中にリモート ネットワーキング デバイスは、サポートされているすべてのクリプトアルゴリズムを送信します。 • **-c**キーワードを設定しても、指定した引数（des、3des、aes128-cbc、aes192-cbc、aes256-cbcのいずれか）をサーバがサポートしていない場合、リモート ネットワーキング デバイスは接続を閉じます。
-l *userid*	（任意）SSHサーバを実行しているリモートネットワーキングデバイスにログインするときに使用するユーザIDを指定します。ユーザIDを省略すると、デフォルトとして現在のユーザIDが使用されます。

-l *userid* **:** *vrfname number ip-address*	（任意）*userid* フィールドにポート情報を含めることで、リバース SSH を設定するときにユーザ ID を指定します。 • **:**：**ポート番号と端末 IP アドレスがユーザ ID に続くことを示します。** • vrfname：ユーザ固有の VRF。 • *number*：端末または補助回線番号。 • *ip-address*：ターミナル サーバの IP アドレス。 （注） *userid* フィールドにポート情報を含めることでリバース SSH を設定する場合（各端末または補助回線を別々のコマンド コンフィギュレーション行にリストする長いメソッドよりも簡単なメソッド）、*userid* 引数と **:** *number ip-address* デリミタおよび引数を使用する必要があります。vrfname を使用することで、SSH は VRF インスタンスにアドレスが存在するホストとのセッションを確立できます。
-l *userid* **:rotary** *number ip-address*	（任意）端末回線がリバース SSH のロータリー グループの下でグループ化されることを指定します。 • **:**：ロータリー グループ番号と端末 IP アドレスが続くことを示します。 • *number* ：端末または補助回線番号。 • *ip-address*：ターミナル サーバの IP アドレス。 （注） *userid* フィールドにロータリー情報を含めることでリバース SSH を設定する場合（各端末または補助回線を別々のコマンド コンフィギュレーション行にリストする長いプロセスよりも簡単なプロセス）、*userid* 引数および **:rotary{** *number} {ip-address}* デリミタおよび引数を使用する必要があります。

-m {**hmac-md5** | **hmac-md5-96** | **hmac-sha1** | **hmac-sha1-96**	（任意）ハッシュされたメッセージ認証コード（HMAC）アルゴリズムを指定します。 • SSH バージョン 1 では、HMAC がサポートされていません。 • **-m** キーワードを指定しない場合、ネゴシエーション中にリモート ネットワーキング デバイスは、サポートされているすべての HMAC アルゴリズムを送信します。**-m** キーワードを設定しても、指定した引数（hmac-md5、hmac-md5-96、hmac-sha1、および hmac-sha1-96）をサーバがサポートしていない場合、リモート デバイスは接続を閉じます。
-o numberofpasswordprompts *n*	（任意）セッションを終了するまでにソフトウェアが生成するパスワードプロンプトの回数を指定します。SSH サーバが、試行回数に制限を適用する場合もあります。サーバによって設定された制限が **-o numberofpasswordprompts** キーワードで市営された値を下回る場合、サーバによって設定された制限が優先されます。デフォルトの試行回数は 3 回です。これは、Cisco IOS SSH サーバのデフォルトでもあります。指定できる値の範囲は、1 ～ 5 です。
-p *port-num*	（任意）リモート ホストの目的のポート番号を示します。デフォルトのポート番号は 22 です。
ip-addr | *hostname*	リモート ネットワーキング デバイスの IPv4 または IPv6 アドレスまたはホスト名を指定します。
command	（任意）リモート ネットワーキング デバイスで実行する Cisco IOS コマンドを指定します。リモート ホストが Cisco IOS ソフトウェアを実行していない場合、これはリモート ホストによって認識される任意のコマンドで構いません。コマンドにスペースが含まれる場合、コマンドを引用符で囲む必要があります。

-vrf	（任意）SSH クライアント側機能に VRF 認識を追加します。 クライアントの VRF インスタンス名は、正しいルーティングテーブルを検索し接続を確立するために、IP アドレスで指定されます。

コマンド デフォルト

コマンドが使用されない場合、暗号化セッションは存在しません。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.1(3)T	このコマンドが導入されました。
12.2(8)T	IPv6 アドレスのサポートが追加されました。
12.0(21)ST	IPv6 アドレスのサポートが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	IPv6 アドレスのサポートが Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	IPv6 アドレスのサポートが Cisco IOS Release 12.2(14)S に統合されました。
12.2(17a)SX	このコマンドが Cisco IOS Release 12.2(17a)SX に統合されました。
12.3(7)T	このコマンドは、セキュア シェル バージョン 2 をサポートするように拡張されました。 **-c** キーワードは、aes128-cbc、aes192-cbc、および aes256-cbc 暗号アルゴリズムのサポートを含めるために拡張されました。 **-m** キーワードが、アルゴリズム hmac-md5、hmac-md5-96、hmac-sha1、および hmac-sha1-96 とあわせて追加されました。 **-v** キーワードと引数**1** および **2** が追加されました。
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。
12.3(11)T	**-l** *userid* **:** *number ip-address* および **-l** *userid* **: rotary** *number ip-address* キーワードと引数オプションが追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。

リリース	変更内容
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.3(7)JA	このコマンドが、Cisco IOS Release 12.3(7)JA に統合されました。
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。
12.0(32)SY	このコマンドが、Cisco IOS Release 12.0(32)SY に統合されました。
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。
12.4(20)T	**-l** *userid* **:** *vrfname number ip-address* キーワードと引数および *-vrf* キーワードが追加されました。
Cisco IOS XE Release 2.4	このコマンドは、Cisco ASR 1000 シリーズルータで導入されました。

使用上のガイドライン

ssh コマンドを使用することで、Cisco ルータは別の Cisco ルータまたは SSH バージョン 1 またはバージョン2サーバを実行しているデバイスとの間に、安全で暗号化された接続を確立できます。この接続は、接続が暗号化されている点を除き、アウトバウンド Telnet 接続の機能と同様です。認証と暗号化により、SSH クライアントは、セキュリティ保護されていないネットワーク上でもセキュアな通信を実現できます。

（注） SSH バージョン 1 は、DES（56 ビット）および 3DES（168 ビット）データ暗号化ソフトウェア イメージでだけサポートされます。 DES ソフトウェア イメージの場合、使用できる暗号化アルゴリズムは DES だけです。 3DES ソフトウェア イメージの場合、DES と 3DES の両方の暗号化アルゴリズムを使用できます。

- SSH バージョン 2 は、aes128-cbc、aes192-cbc、および aes256-cbc 暗号化アルゴリズムだけをサポートしています。 SSH バージョン 2 は、3DES イメージでのみサポートされています。
- SSH バージョン 1 では、HMAC アルゴリズムがサポートされていません。

次に、ローカル ルータとリモート ホスト HQhost の間で安全なセッションを開始し、**show users** コマンドを実行する例を示します。 **show users** コマンドの結果は、HQhost にログインしている有効なユーザのリストです。 リモート ホストは、ユーザ adminHQ を認証するために、adminHQ パスワードを要求します。 認証ステップが成功すると、リモート ホストは、**show users** コマンドの結果をローカル ルータに返してから、セッションを閉じます。

```
ssh -l adminHQ HQhost "show users"
```

次に、ローカル ルータとエッジ ルータ HQedge の間で安全なセッションを開始し、**show ip route** コマンドを実行する例を示します。 この例では、エッジ ルータはユーザを認証するために、

adminHQ パスワードを要求します。 認証ステップが成功すると、エッジ ルータは、**show ip route** コマンドの結果をローカル ルータに返します。

```
ssh -l adminHQ HQedge "show ip route"
```

次に、3DES を使用して HQedge ルータと安全なリモート コマンド接続を開始する SSH クライアントの例を示します。 HQedge で稼働している SSH サーバは、標準の認証方式を使用して HQedge ルータの admin7 ユーザのセッションを認証します。 認証が機能するためには、HQedge ルータで SSH がイネーブルになっている必要があります。

```
ssh -l admin7 -c 3des -o numberofpasswordprompts 5 HQedge
```

次に、**show running-config** コマンドを実行するための、ローカル ルータとアドレス 3ffe:1111:2222:1044::72 のリモート IPv6 ルータとの間の安全なセッションの例を示します。 この例では、リモート IPv6 ルータはユーザを認証するために、adminHQ パスワードを要求します。 認証ステップが成功すると、リモート IPv6 ルータは、**show unning-config** コマンドの結果をローカル ルータに返してから、セッションを閉じます。

```
ssh -l adminHQ 3ffe:1111:2222:1044::72 "show running-config"
```

（注） 最後の例では、IPv6 アドレス 3ffe:1111:2222:1044::72 にマップするホスト名が使用される可能性があります。

次に、クリプト アルゴリズム aes256-cbc と hmac-sha1-96 の HMAC を使用する SSH バージョン 2 セッションの例を示します。 ユーザ ID は user2、IP アドレスは 10.76.82.24 です。

```
ssh -v 2 -c aes256-cbc -m hmac-sha1-96 -1 user2 10.76.82.24
```

次に、SSH クライアントでリバース SSH が設定されている例を示します。

```
ssh -l lab:1 router.example.com
```

次のコマンドは、リバース SSH がロータリー グループの最初の空き回線に接続されることを表示します。

```
ssh -l lab:rotary1 router.example.com
```

関連コマンド

コマンド	説明
ip ssh	ルータに SSH サーバの制御パラメータを設定します。
show ip ssh	SSH のバージョンおよび設定データを表示します。
show ssh	SSH サーバ接続のステータスを表示します。

switchport port-security

インターフェイスでポート セキュリティをイネーブルにするには、インターフェイス コンフィギュレーション モードで **switchport port-security** コマンドを使用します。 ポート セキュリティをディセーブルにするには、このコマンドの **no** 形式を使用します。

switchport port-security

no switchport port-security

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

ディセーブル

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

コマンド履歴

リリース	変更内容
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	Supervisor Engine 2 上のこのコマンドのサポートがリリース 12.2(17d)SXB に拡張されました。
12.2(18)SXE	Supervisor Engine 720 でこのコマンドが次のように変更されました。 • リリース 12.2(18)SXE 以降のリリースでは、トランクでポート セキュリティがサポートされます。 • リリース 12.2(18)SXE 以降のリリースでは、802.1Q トンネル ポートでポート セキュリティがサポートされます。
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。

使用上のガイドライン

ポート セキュリティを設定するときには、次の注意事項に従ってください。

- リリース 12.2(18)SXE 以降のリリースでは、トランクでポート セキュリティがサポートされます。
- リリース 12.2(18)SXE よりも前のリリースでは、トランクでポート セキュリティはサポートされません。

- リリース 12.2(18)SXE 以降のリリースでは、802.1Q トンネル ポートでポート セキュリティがサポートされます。
- リリース 12.2(18)SXE よりも前のリリースでは、802.1Q トンネル ポートでポート セキュリティはサポートされません。
- セキュア ポートは、スイッチド ポート アナライザ（SPAN）の宛先ポートにできません。
- セキュア ポートは、EtherChannel に所属できません。
- セキュア ポートはトランク ポートにはできません。
- セキュア ポートは 802.1X ポートにはできません。 セキュア ポートで 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、802.1x はイネーブルになりません。 802.1x 対応ポートをセキュア ポートに変更しようとしても、エラー メッセージが表示され、セキュリティ設定は変更されません。

例

次に、ポート セキュリティをイネーブルにする例を示します。

```
Router(config-if)#
switchport port-security
```

次に、ポート セキュリティをディセーブルにする例を示します。

関連コマンド

コマンド	説明
show port-security	ポート セキュリティ設定情報を表示します。

tacacs-server administration から title-color まで

tacacs server

IPv6 または IPv4 の TACACS+ サーバを設定し、TACACS+ サーバ コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **tacacs server** コマンドを使用します。 設定を削除するには、このコマンドの **no** 形式を使用します。

tacacs server *name*

no tacacs server

構文の説明

name	プライベート TACACS+ サーバ ホストの名前。

コマンド デフォルト

TACACS+ サーバは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2S	このコマンドが導入されました。

使用上のガイドライン

tacacs server コマンドは、*name* 引数を使用して TACACS サーバを設定し、TACACS+ サーバ コンフィギュレーション モードを開始します。 この設定は、設定を終了し、TACACS+ サーバ コンフィギュレーション モードを終了すると適用されます。

例

次に、名前 server1 を使用して TACACS+ サーバ コンフィギュレーション モードを開始し、TACACS サーバを設定する例を示します。

```
Router(config)# tacacs server server1
Router(config-server-tacacs)#
```

関連コマンド

コマンド	説明
address ipv6（**TACACS+**）	TACACS+ サーバの IPv6 アドレスを設定します。

コマンド	説明
key（**TACACS+**）	TACACS+ サーバでサーバ単位の暗号キーを設定します。
port（**TACACS+**）	TACACS+ 接続に使用する TCP ポートを指定します。
send-nat-address（**TACACS+**）	クライアントの NAT 後のアドレスを TACACS+ サーバに送信します。
single-connection（**TACACS+**）	単一の TCP 接続を使用してすべての TACACS パケットを同じサーバに送信できるようにします。
timeout（**TACACS+**）	指定された TACACS サーバからの応答を待機する時間を設定します。

tacacs-server host

TACACS+ ホストを指定するには、グローバル コンフィギュレーション モードで **tacacs-server host** コマンドを使用します。 指定された名前またはアドレスを削除するには、このコマンドの **no** 形式を使用します。

tacacs-server host{*host-name*| *host-ip-address*}[**key***string*][**[nat]**[**port**[*integer*]]**[single-connection]**[**timeout**[*integer*]]]

no tacacs-server host{*host-name*| *host-ip-address*}

構文の説明

host-name	ホストの名前。
host-ip-address	ホストの IP アドレス。
key	（任意）認証および暗号キーを指定します。 これは TACACS+ デーモンで使用されるキーと一致する必要があります。 このキーを指定すると、このサーバに限り、グローバル コマンド **tacacs-server key** で設定されているキーが上書きされます。
string	（任意）認証および暗号キーを指定する文字列。
nat	（任意）クライアントのポート ネットワーク アドレス変換（NAT）アドレスが TACACS+ サーバに送信されます。
port	（任意）TACACS+ サーバのポート番号を指定します。 この設定によって、デフォルトのポート 49 は上書きされます。
integer	（任意）サーバのポート番号です。 有効なポート番号の範囲は 1 ～ 65535 です。
single-connection	（任意）ルータと TACACS+ サーバ間で単一のオープンな接続を保守します。
timeout	（任意）タイムアウト値を指定します。 これによって、**tacacs-server timeout** コマンドで設定したグローバル タイムアウト値がこのサーバに限り上書きされます。

integer	（任意）タイムアウト間隔の整数値（秒単位）。 値は 1 ～ 1000 です。

コマンド デフォルト

TACACS+ ホストは指定されません。

コマンド モード

グローバル 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
10.0	このコマンドが導入されました。
12.1(11)、12.2(6)	**nat** キーワードが追加されました。
12.2(8)T	**nat** キーワードが、Cisco IOS Release 12.2(8)T に統合されました。
12.2(33)SRA	このコマンドが Cisco IOS Release 12.(33)SRA に統合されました。
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す。 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。

使用上のガイドライン

複数の **tacacs-server host** コマンドを使用して、追加のホストを指定できます。 Cisco IOS ソフトウェアは、指定された順序でホストを検索します。 AAA/TACACS+ サーバを実行している場合のみ、**port**、**timeout**、**key**、**single-connection**、および **nat** キーワードを使用します。

tacacs-server host コマンドのパラメータの一部は、**tacacs-server timeout** コマンドおよび **tacacs-server key** コマンドによるグローバル設定よりも優先されるため、このコマンドを使用して個別のルータを一意に設定することで、ネットワークのセキュリティを強化できます。

single-connection キーワードは、単一の接続を指定します（CiscoSecure Release 1.0.1 以降でのみ有効）。 通信が必要になるたびに、ルータが TCP 接続を開閉するのではなく、single-connection オプションによって、ルータとサーバ間の単一のオープンな接続を保守します。 単一の接続のほうが、サーバがより多くの TACACS 操作を処理できるようになるため、より効率的です。

例

次に、Sea_Change という名前の TACACS+ ホストを指定する例を示します。

```
tacacs-server host Sea_Change
```

次に、認証、許可、アカウンティング（AAA）、AAA(AAA)の確認のために、ルータがポート番号51でSea_Cureという名前のTACACS+サーバホストに打診することを指定する例を示します。この接続における要求のタイムアウト値は3秒で、暗号キーはa_secretです。

```
tacacs-server host Sea_Cure port 51 timeout 3 key a_secret
```

関連コマンド

コマンド	説明
aaa authentication	AAA 認証を指定するか、またはイネーブルにします。
aaa authorization	ネットワークへのユーザアクセスを制限するパラメータを設定します。
aaa accounting	課金またはセキュリティのために、要求されたサービスの AAA アカウンティングをイネーブルにします。
ppp	PPP を使用して非同期接続を開始します。
slip	SLIP を使用してリモート ホストへのシリアル接続を開始します。
tacacs-server key	アクセス サーバと TACACS+デーモンとのすべての TACACS+ 通信に使用される認証暗号キーを設定します。

telnet

Telnetをサポートしているホストにログインするには、ユーザEXECモードまたは特権EXECモードで **telnet** コマンドを使用します。

telnet *host* [*port*] [*keyword*]

構文の説明

host	ホスト名または IP アドレス。
port	（任意）10 進数の TCP ポート番号またはポート名。デフォルトはホストの Telnet のルータポート（10 進数値 23）。
keyword	（任意）次の表にリストされているキーワードいずれか 1 つ。

コマンド モード

ユーザ EXEC 特権 EXEC

コマンド履歴

リリース	変更内容
10.0	このコマンドが導入されました。
12.0(21)ST	**/ipv4** キーワードおよび **/ipv6** キーワードが追加されました。
12.1	**/quiet** キーワードが追加されました。
12.2(2)T	**/ipv4** キーワードおよび **/ipv6** キーワードが追加されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
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。

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ ルータで追加されました。

使用上のガイドライン

次の表は、オプションの **telnet** コマンド キーワードのリストです。

表 *16* : *telnet* キーワード オプション

オプション	説明
/debug	Telnet デバッグ モードをイネーブルにします。
/encrypt kerberos	暗号化された Telnet セッションをイネーブルにします。 このキーワードは、Kerberos 対応 Telnet サブシステムがある場合にだけ使用できます。 Kerberos 証明書を使用して認証を実行する場合、このキーワードの使用により、リモート サーバとの暗号化ネゴシエーションが開始されます。暗号化ネゴシエーションが失敗すると、Telnet 接続がリセットされます。 暗号化ネゴシエーションが成功すると、Telnet 接続が確立され、暗号化モードで引き続き Telnet セッションが続行されます（セッションではすべての Telnet トラフィックが暗号化されます）。
/ipv4	IP プロトコルのバージョン 4 を指定します。IPv4 と IPv6 プロトコル スタックの両方をサポートするネットワークで IP プロトコルのバージョンが指定されていない場合、IPv6 が最初に試行され、次に IPv4 が試行されます。
/ipv6	IP プロトコルのバージョン 6 を指定します。IPv4 と IPv6 プロトコル スタックの両方をサポートするネットワークで IP プロトコルのバージョンが指定されていない場合、IPv6 が最初に試行され、次に IPv4 が試行されます。

オプション	説明
/line	Telnet 回線モードをイネーブルにします。 このモードでは、ユーザが **Enter** キーを押すまで Cisco IOS ソフトウェアはホストにデータを送信しません。 標準の Cisco IOS ソフトウェアのコマンド編集文字を使用して回線を編集できます。 **/line** キーワードはローカル スイッチです。リモート ルータには、モードの変更は通知されません。
/noecho	ローカル エコーをディセーブルにします。
/quiet	Cisco IOS ソフトウェアからのすべてのメッセージを画面上に表示しないようにします。
/route: *path*	ルース送信元ルーティングを指定します。 *path* 引数は、最終的な宛先で終了するネットワーク ノードを指定するホスト名または IP アドレスのリストです。
/source-interface	送信元インターフェイスを指定します。
/stream	*stream* 処理をオンにします。これにより、Telnet の制御シーケンスなしの raw TCP ストリームがイネーブルになります。 ストリーム接続は Telnet オプションを処理せず、UNIX 間コピー プログラム（UUCP）や他の非 Telnet プロトコルを実行するポート接続に適している場合があります。
port-number	ポート番号。
bgp	ボーダー ゲートウェイ プロトコル。
chargen	文字ジェネレータ。
cmd *rcmd*	リモート コマンド。
daytime	デイタイム。
discard	廃棄。
domain	ドメイン ネーム サービス。
echo	エコー。

オプション	説明
exec	EXEC
finger	フィンガ。
ftp	File Transfer Protocol（ファイル転送プロトコル）。
ftp-data	FTP データ接続（めったに使用しない）。
gopher	Gopher。
hostname	ホストネーム サーバ。
ident	Ident プロトコル。
irc	インターネット リレー チャット。
klogin	Kerberos ログイン。
kshell	Kerberos シェル。
login	ログイン（rlogin）。
lpd	印刷サービス。
nntp	ネットワーク ニュース トランスポート プロトコル。
pim-auto-rp	Protocol Independent Multicast（PIM）の自動ランデブー ポイント（RP）。
node	特定のローカルエリア トランスポート（LAT）ノードに接続します。
pop2	Post Office Protocol v2。
pop3	Post Office Protocol v3。
port	宛先ローカルエリア トランスポート（LAT）ポート名。
smtp	シンプル メール転送プロトコル。
sunrpc	Sun Remote Procedure Call。

オプション	説明
syslog	Syslog。
tacacs	TACACS セキュリティを指定します。
talk	Talk（517）。
Telnet	Telnet（23）。
time	Time（37）。
uucp	UNIX 間コピー プログラム（540）。
whois	ニックネーム（43）。
www	World Wide Web（HTTP、80）。

Cisco IOS の TCP/IP 実装では、端末接続を確立するために、**connect** または **telnet** コマンドを入力する必要はありません。 次の条件をすべて満たす場合に限り、学習されたホスト名だけを入力できます。

- ホスト名がルータのコマンド ワードとは異なる。
- 優先トランスポート プロトコルが **telnet** に設定されている。

利用可能なホストを一覧表示するには、**show hosts** コマンドを使用します。 すべての TCP 接続のステータスを表示するには、**show tcp** コマンドを使用します。

Cisco IOS ソフトウェアから各接続に論理名が割り当てられ、これらの名前を使用する複数のコマンドによって接続が識別されます。 論理名は、その名前が使用中の場合と、**name-connection** EXEC コマンドで接続名が変更された場合を除き、ホスト名と同じになります。 この名前が使用中の場合、Cisco IOS ソフトウェアによりヌル名が接続に割り当てられます。

Telnet ソフトウェアは Telnet シーケンス形式の特殊な Telnet コマンドをサポートします。このシーケンスは、一般的な端末制御機能をオペレーティング システム固有の機能にマッピングします。特殊な Telnet コマンドを発行するには、エスケープ シーケンスを入力してからコマンド文字を入力します。 デフォルトのエスケープ シーケンスは、Ctrl-^（Ctrl キーと Shift キーを押しながら数字の 6 キーを押す）です。 大文字のコマンド文字は Ctrl キーを押しながら、小文字のコマンド文字は Ctrl キーを離して入力するとそれぞれ入力できます。 次の表は、特殊な Telnet のエスケープ シーケンスを示します。

表 *17*：特殊な *Telnet* のエスケープ シーケンス

エスケープ シーケンス[1]	目的
Ctrl-^ b	ブレーク

エスケープ シーケンス[1]	目的
Ctrl-^ c	プロセスの割り込み（IP および IPv6）
Ctrl-^ h	文字の消去（EC）
Ctrl-^ o	出力の中断（AO）
Ctrl-^ t	そこにいますか。（AYT）
Ctrl-^ u	行の消去（EL）

1 キャレット（^）記号は、キーボードの Shift + 6 で入力します。

アクティブな Telnet セッション中の任意の時点で、システム プロンプトでエスケープ シーケンス キーを押してから疑問符を入力（Ctrl-^ **?**）すると、Telnet コマンドを一覧表示できます

次に、この一覧の例を示します。 この出力例では、最初のキャレット（^）記号は Ctrl キーを表し、2 番目のキャレット記号はキーボードの Shift + 6 を表しています。

```
router> ^^?
[Special telnet escape help]
^^B  sends telnet BREAK
^^C  sends telnet IP
^^H  sends telnet EC
^^O  sends telnet AO
^^T  sends telnet AYT
^^U  sends telnet EL
```

複数の並列 Telnet セッションを開き、セッション間を切り替えることができます。 以降のセッションを開くには、最初に、エスケープ シーケンスで（デフォルトでは Ctrl-Shift-6、x [Ctrl^x] の順に押す）現在の接続を一時停止してシステム コマンド プロンプトに戻ります。 その後、**telnet** コマンドで新しい接続を開きます。

アクティブな Telnet セッションを終了するには、接続しているデバイスのプロンプトから次のいずれかのコマンドを入力します。

- **close**
- **disconnect**
- **exit**
- **logout**
- **quit**

例

次に、ルータから host1 というリモート ホストに対して暗号化された Telnet セッションを確立する例を示します。

```
router>

telnet host1 /encrypt kerberos
```

次に、送信元システム host1 から example.com、10.1.0.11 の順にパケットをルーティングし、最後に *host1* に返す例を示します。

```
router>
telnet host1 /route:example.com 10.1.0.11 host1
```

次に、論理名 host1 のホストに接続する例を示します。

```
router>
host1
```

次に、ログインおよびログアウト時にCisco IOS ソフトウェアからの画面メッセージをすべて抑制する例を示します。

```
router>

telnet host2 /quiet
```

次に、接続がオプションの **/quiet** キーワードを使用して接続を確立したときに表示される、制限されたメッセージの例を示します。

```
login:User2
Password:
         Welcome to OpenVMS VAX version V6.1 on node CRAW
     Last interactive login on Tuesday, 15-DEC-1998 11:01
     Last non-interactive login on Sunday,  3-JAN-1999 22:32
Server3)logout
    User2        logged out at  16-FEB-2000 09:38:27.85
```

関連コマンド

コマンド	説明
connect	Telnet、rlogin、または LAT をサポートするホストにログインします。
kerberos clients mandatory	**rsh**、**rcp**、**rlogin**、および **telnet** コマンドでリモート サーバと Kerberos プロトコルのネゴシエーションができない場合、これらのコマンドは失敗します。
name connection	接続に論理名を割り当てます。
rlogin	rlogin を使用して UNIX ホストにログインします。
show hosts	デフォルトのドメイン名、名前ルックアップ サービス、ネーム サーバ ホストのリスト、およびホスト名とアドレスのキャッシュされたリストを表示します。
show tcp	TCP 接続のステータスを表示します。

test aaa group

着信番号識別サービス（DNIS）または発信回線 ID（CLID）ユーザ プロファイルを RADIUS サーバに送信されたレコードに関連付けるか、または手動でロードバランシング サーバのステータスをテストするには、特権 EXEC モードで **test aaa group** コマンドを使用します。

DNIS and CLID User Profile

test aaa group {*group-name*| **radius**} *username password* **new-code** [**profile** *profile-name*]

RADIUS Server Load Balancing Manual Testing

test aaa group *group-name* [**server** *ip-address*] [**auth-port** *port-number*] [**acct-port** *port-number*] *username password* **new-code** [**count** *requests*] [**rate** *requests-per-second*] [**blocked** {**yes**| **no**}]

構文の説明

group-name	サーバ グループのグループ名で定義されている、RADIUS サーバのサブセット。
radius	認証に RADIUS サーバを使用します。
username	テスト ユーザの名前。 **注意** このコマンドを使用して手動で RADIUS ロードバランシング サーバの状態をテストする場合、テスト ユーザが正しく設定されていない場合に発生するセキュリティ上の問題を防止するために、テスト ユーザ（RADIUS サーバ上で定義されていないもの）を使用することを推奨します。
password	パスワード。
new-code	RADIUS サーバとの CLID または DNIS ユーザ プロファイル アソシエーションをサポートする、新しいコードまでのコード パス。
profile *profile-name*	（任意）aaa user profile コマンドで指定されたユーザ プロファイルを識別します。 ユーザ プロファイルを RADIUS サーバに関連付けるには、ユーザプロファイル名を識別する必要があります。

server *ip-address*	（任意）RADIUS サーバのロードバランシングのために、サーバ グループ内のどのサーバにテスト パケットを送信するかを指定します。
auth-port	（任意）認証要求に対するユーザ データグラム プロトコル（UDP）宛先ポート。
port-number	（任意）認証要求用のポート番号です。0 に設定されている場合、認証にホストは使用されません。指定しない場合、ポート番号はデフォルトの 1646 になります。
acct-port	（任意）アカウンティング要求用の UDP 宛先ポート。
port-number	（任意）アカウンティング要求用のポート番号です。0 に設定されている場合、アカウンティングにホストは使用されません。指定しない場合、ポート番号はデフォルトの 1646 になります。
count *requests*	（任意）サーバの各ポートに送信される認証およびアカウンティング要求の数。 有効な範囲は、1 ～ 50000 です。 デフォルト：1。
rate *requests-per-second*	（任意）サーバに送信される 1 秒あたりの要求の数。 範囲は 1 ～ 1000 です。 デフォルトは 10 です。
blocked {**yes** | **no**}	（任意）要求をブロッキング モードで送信するか、ノンブロッキング モードで送信するかを指定します。 **blocked** キーワードを使用せず 1 つの要求を送信する場合、デフォルトは **yes** です。複数の要求を送信する場合は、デフォルトは **no** です。

コマンド デフォルト

DNIS または CLID 属性値は、RADIUS サーバに送信されません。

RADIUS サーバ ロードバランシングの手動テスト

コマンド モード

RADIUS サーバ ロードバランシングのサーバ ステータス手動テストは実行されません。
特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.2(4)T	このコマンドが導入されました。
12.2(28)SB	RADIUS ロード バランシング手動テスト機能を設定するために、次のキーワードと引数が追加されました。**server** *ip-address*、**auth-port** *port-number*、**acct-port** *port-number*、**count** *request*、**rate** *requests-per-second*、**blocked**。
12.4(11)T	このコマンドが Cisco IOS Release 12.4(11)T に統合されました。
12.2(31)ZV1	このコマンドは、認証が成功した場合に RADIUS 認証から返されるユーザ属性を表示するように拡張されました。
Cisco IOS XE Release 2.4	このコマンドが、Cisco IOS XE Release 2.4 に統合されました。

使用上のガイドライン

test aaa group コマンドは、次の目的に使用できます

- DNIS または CLID ネームド ユーザ プロファイルを RADIUS サーバに送信されるレコードに関連付けます。これにより、サーバが RADIUS レコードを受信した際に、DNIS または CLID 情報にアクセスできるようになります。
- RADIUS ロードバランシング サーバのステータスを確認します。

（注） **test aaa group** コマンドは、TACACS+ では機能しません。

例

次に、「prfl1」という名前の dnis = dnisvalue ユーザ プロファイルを設定し、**test aaa group** コマンドを使用して関連付ける例を示します。

```
aaa user profile prfl1
  aaa attribute dnis
  aaa attribute dnis dnisvalue
  no aaa attribute clid
! Attribute not found.
  aaa attribute clid clidvalue
  no aaa attribute clid
  exit
!
! Associate the dnis user profile with the test aaa group command.
test aaa group radius user1 pass new-code profile prfl1
```

次の例は、ユーザ名の「test」がユーザ プロファイルと一致しない場合の動作中の RADIUS ロード バランシング サーバからの応答を示しています。 サーバは、**test aaa group** コマンドで生成さ

れた AAA パケットに対する Access-Reject 応答を発行した時点で動作中であることが確認されます。

```
Router# test aaa group SG1 test lab new-code

00:06:07: RADIUS/ENCODE(00000000):Orig. component type = INVALID
00:06:07: RADIUS/ENCODE(00000000): dropping service type, "radius-server attribute 6
on-for-login-auth" is off
00:06:07: RADIUS(00000000): Config NAS IP: 192.0.2.4
00:06:07: RADIUS(00000000): sending
00:06:07: RADIUS/ENCODE: Best Local IP-Address 192.0.2.141 for Radius-Server 192.0.2.176
00:06:07: RADIUS(00000000): Send Access-Request to 192.0.2.176:1645 id 1645/1, len 50
00:06:07: RADIUS:  authenticator CA DB F4 9B 7B 66 C8 A9 - D1 99 4E 8E A4 46 99 B4
00:06:07: RADIUS:  User-Password       [2]   18  *
00:06:07: RADIUS:  User-Name           [1]   6   "test"
00:06:07: RADIUS:  NAS-IP-Address      [4]   6   192.0.2.141
00:06:07: RADIUS: Received from id 1645/1 192.0.2.176:1645, Access-Reject, len 44
00:06:07: RADIUS:  authenticator 2F 69 84 3E F0 4E F1 62 - AB B8 75 5B 38 82 49 C3
00:06:07: RADIUS:  Reply-Message       [18]  24
00:06:07: RADIUS:   41 75 74 68 65 6E 74 69 63 61 74 69 6F 6E 20 66  [Authentication ]
00:06:07: RADIUS:   61 69 6C 75 72 65                               [failure]
00:06:07: RADIUS(00000000): Received from id 1645/1
00:06:07: RADIUS/DECODE: Reply-Message fragments, 22, total 22 bytes
```

例

次に、test aaa コマンドを発行し認証が成功したときに、RADIUS サーバから返されるユーザ属性リストの例を示します。

```
Router# test aaa group radius viral viral new-code blocked no
AAA/SG/TEST: Sending 1 Access-Requests @ 10/sec, 0 Accounting-Requests @ 10/sec
CLI-1#
AAA/SG/TEST: Testing Status
AAA/SG/TEST:      Authen Requests to Send    : 1
AAA/SG/TEST:      Authen Requests Processed  : 1
AAA/SG/TEST:      Authen Requests Sent       : 1
AAA/SG/TEST:      Authen Requests Replied    : 1
AAA/SG/TEST:      Authen Requests Successful : 1
AAA/SG/TEST:      Authen Requests Failed     : 0
AAA/SG/TEST:      Authen Requests Error      : 0
AAA/SG/TEST:      Authen Response Received   : 1
AAA/SG/TEST:      Authen No Response Received: 0
AAA/SG/TEST: Testing Status
AAA/SG/TEST:      Account Requests to Send    : 0
AAA/SG/TEST:      Account Requests Processed  : 0
AAA/SG/TEST:      Account Requests Sent       : 0
AAA/SG/TEST:      Account Requests Replied    : 0
AAA/SG/TEST:      Account Requests Successful : 0
AAA/SG/TEST:      Account Requests Failed     : 0
AAA/SG/TEST:      Account Requests Error      : 0
AAA/SG/TEST:      Account Response Received   : 0
AAA/SG/TEST:      Account No Response Received: 0
USER ATTRIBUTES
username             "Username:viral"
nas-ip-address       3.1.1.1
interface            "210"
service-type         1 [Login]
Framed-Protocol      3 [ARAP]
ssg-account-info     "S20.5.0.2"
ssg-command-code     0B 4C 32 54 50 53 55 52 46
Router
```

関連コマンド

コマンド	説明
aaa attribute	ユーザ プロファイルに DNIS または CLID 属性値を追加します。
aaa user profile	AAA ユーザ プロファイルを作成します。
load-balance	RADIUS-named サーバ グループに対して RADIUS サーバ ロード バランシングをイネーブルにします。
radius-server host	ロードバランシング用の RADIUS 自動テストをイネーブルにします。
radius-server load-balance	グローバル RADIUS サーバ グループに対して RADIUS サーバ ロードバランシングをイネーブルにします。

timeout（TACACS+）

指定された TACACS サーバからの応答を待機する時間を設定するには、TACACS+ サーバ コンフィギュレーション モードで **timeout** コマンドを使用します。 コマンド デフォルトに戻すには、このコマンドの **no** 形式を使用します。

timeout *seconds*

no timeout *seconds*

構文の説明

seconds	（任意）合計時間（秒単位）。

コマンド デフォルト

待機時間は 5 秒です。

コマンド モード

TACACS+ サーバ コンフィギュレーション（config-server-tacacs）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2S	このコマンドが導入されました。

使用上のガイドライン

timeout コマンドを使用して、TACACS サーバからの応答を待機する時間を秒単位で設定します。**timeout** コマンドが設定されている場合、指定された秒数は、5 秒のデフォルト時間を上書きします。

例

次に、待機時間を 10 秒に設定する例を示します。

```
Router(config)# tacacs server server1
Router(config-server-tacacs)# timeout 10
```

関連コマンド

コマンド	説明
tacacs server	IPv6 または IPv4 に対して TACACS+ サーバを設定して、TACACS サーバ コンフィギュレーション モードを開始します。

traffic-export から zone security まで

username

ユーザ名に基づいた認証システムを確立するには、グローバル コンフィギュレーション モードで **username** コマンドを使用します。 確立されたユーザ名ベースの認証を削除するには、このコマンドの **no** 形式を使用します。

username *name* [**aaa attribute list** *aaa-list-name*]

username *name* [**access-class** *access-list-number*]

username *name* [**autocommand** *command*]

username *name* [**callback-dialstring** *telephone-number*]

username *name* [**callback-line [tty]** *line-number* [*ending-line-number*]]

username *name* [**callback-rotary** *rotary-group-number*]

username *name* **[dnis]**

username *name* **[mac]**

username *name* **[nocallback-verify]**

username *name* **[noescape]**

username *name* **[nohangup]**

username *name* [**nopassword**| **password** *password*| **password** *encryption-type encrypted-password*]

username *name* [**one-time** {**password** {**0**| **7**| *password*}| **secret** {**0**| **5**| *password*}}]

username *name* [**password** *secret*]

username *name* [**privilege** *level*]

username *name* [**secret** {**0**| **5**| *password*}]

username *name* [**user-maxlinks** *number*]

username [lawful-intercept] *name* [**privilege** *privilege-level*| **view** *view-name*] **password** *password*

no username *name*

構文の説明

name	ホスト名、サーバ名、ユーザ ID、またはコマンド名。 *name* 引数には 1 つの単語だけ使用できます。 空白や二重引用符は使用できません。
aaa attribute list *aaa-list-name*	指定された認証、許可、アカウンティング（AAA）メソッド リストを使用します。
access-class *access-list-number*	（任意）ライン コンフィギュレーション モードで使用可能な **access-class** コマンドで指定されたアクセス リストを上書きする発信アクセス リストを指定します。 これはユーザ セッション中に使用されます。

autocommand *command*	（任意）ユーザがログインした後に、自動的に指定されたコマンドが発行されるようにします。 コマンドが完了すると、セッションが終了します。 コマンドの長さは任意で、埋め込みスペースが含まれる可能性があるため、**autocommand** キーワードを使用したコマンドは、行の最後のオプションである必要があります。
callback-dialstring *telephone-number*	（任意）非同期コールバックの場合のみ：DCE デバイスに渡すための電話番号を指定できます。
callback-line *line-number*	（任意）非同期コールバックの場合のみ：コールバック用の特定のユーザ名をイネーブルにする、端末回線（または連続したグループの最初の行）の相対番号。 番号付けはゼロから始まります。
ending-line-number	（任意）コールバック用の特定のユーザ名をイネーブルにする、連続したグループの最後の行の相対番号。 キーワード（**tty** など）を省略すると、line-number および ending-line-number は相対ではなく絶対回線番号になります。
tty	（任意）非同期コールバックの場合のみ：標準非同期回線。
callback-rotary *rotary-group-number*	（任意）非同期コールバックの場合のみ：コールバック用に特定のユーザ名をイネーブルにする、ロータリーグループ番号を指定できます。 ロータリーグループの次の使用可能な回線が選択されます。 範囲は 1 ～ 100 です。
dnis	着信番号識別サービス（DNIS）経由で取得されると、パスワードは必要ではありません。
mac	MAC アドレスが、ローカルで実行される MAC フィルタリング用のユーザ名として使用できるようになります。
nocallback-verify	（任意）指定された回線上の EXEC コールバックで、認証が必要ないことを指定します。

noescape	（任意）ユーザが接続しているホストで、そのユーザがエスケープ文字を使用することを防ぎます。
nohangup	（任意）自動コマンド（**autocommand** キーワードで設定）が完了した後に、Cisco IOS ソフトウェアがユーザを切断することを防ぎます。代わりに、ユーザは別の EXEC プロンプトを受け取ります。
nopassword	このユーザがログインするためにパスワードは必要はありません。これは通常、**autocommand** キーワードと組み合わせて使用するには最も有用なキーワードです。
password	パスワードが *name* 引数にアクセスするように指定します。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。
password	ユーザが入力するパスワード。
encryption-type	（任意）直後に続くテキストを暗号化するかどうかと、暗号化する場合は使用する暗号化の種類を定義する 1 桁の数字。定義されている暗号化タイプは、後続するテキストは暗号化されない 0 と、テキストがシスコにより定義された暗号化アルゴリズムを使用して暗号化される 7 です。
encrypted-password	ユーザが入力する暗号化パスワード。
one-time	ユーザ名とパスワードは 1 回だけ有効であることを指定します。この設定は、デフォルトのクレデンシャルがユーザ設定に残ることを防ぐために使用されます。
0	非暗号化パスワードまたは秘密キー（設定に依存）が続くことを指定します。
7	非表示のパスワードが続くことを指定します。
5	非表示の秘密が続くことを指定します。
secret	ユーザの秘密を指定します。

secret	チャレンジ ハンドシェイク認証プロトコル（CHAP）認証の場合、ローカル ルータまたはリモート デバイスの秘密を指定します。 秘密はローカル ルータに保存するときに暗号化されます。 秘密は、11 文字までの任意の ASCII 文字の文字列で構成されます。 指定可能なユーザ名とパスワードの組み合わせに制限はないため、認証できるリモート デバイスの数は任意です。
privilege *privilege-level*	（任意）ユーザの特権レベルを設定します。 有効な範囲は、1 ～ 15 です。
user-maxlinks *number*	ユーザに許可されるインバウンド リンクの最大数。
lawful-intercept	（任意）シスコ デバイス上で合法的傍受ユーザを設定します。
name	ホスト名、サーバ名、ユーザ ID、またはコマンド名。 *name* 引数には 1 つの単語だけ使用できます。 空白や二重引用符は使用できません。
view *view-name*	（任意）CLI ビューの場合のみ：**parser view** コマンドで指定されたローカル AAA データベースと CLI ビュー名を関連付けます。
password *password*	CLI ビューにアクセスするためのパスワード。

コマンド デフォルト

ユーザ名に基づく認証システムは確立されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
10.0	このコマンドが導入されました。

リリース	変更内容
11.1	このコマンドが変更されました。 次のキーワードと引数が追加されました。 • **callback-dialstring** *telephone-number* • **callback-rotary** *rotary-group-number* • **callback-line** [**tty**] *line-number* [*ending-line-number* • **nocallback-verify**
12.3(7)T	このコマンドが変更されました。 次のキーワードと引数が追加されました。 • **lawful-intercept** • **view** • *view-name*
12.2(33)SRB	このコマンドが変更されました。 次のキーワードと引数が、Cisco IOS Release 12.2(33)SRB に統合されました。 • **lawful-intercept** • **view** • *view-name*
12.2(33)SB	このコマンドが変更されました。 次のキーワードと引数が、Cisco IOS Release 12.2(33)SB に統合されました。 • **lawful-intercept** • **view** • *view-name*
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI に統合されました。
12.4	このコマンドが変更されました。 次のキーワードが、Cisco IOS Release 12.4 に統合されました。 • **one-time** • **secret** • **0**、**5**、**7**

リリース	変更内容
15.1(1)S	このコマンドが変更されました。 **nohangup** キーワードのサポートがセキュア シェル（SSH）から除外されました。
Cisco IOS XE Release 3.2SE	このコマンドが変更されました。 **mac** キーワードが追加されました。

使用上のガイドライン

username コマンドは、ユーザ名認証またはパスワード認証（またはその両方）をログインの目的のみで指定します。

複数の **username** コマンドを、単一のユーザに対するオプションを指定するために使用できます。

ローカル ルータが通信し、認証を要求する各リモート システムにユーザ名エントリを追加します。 リモート デバイスは、ローカル ルータに対してユーザ名エントリを持っている必要があります。 このエントリは、そのリモート デバイスに対するローカル ルータのエントリと同じパスワードを持っている必要があります。

このコマンドは、特殊な取り扱いが必要なユーザ名を定義する場合に便利です。 たとえば、このコマンドを使用すると、パスワードが不要で、ユーザを汎用の情報サービスに接続する「info」ユーザ名を定義できます。

username コマンドは、CHAP の設定の一部として必要です。 ローカル ルータが認証を要求する各リモート システムにユーザ名エントリを追加します。

（注） リモート CHAP チャレンジに対するローカル ルータの応答をイネーブルにするには、1 つの **username** *name* エントリは、別のルータに割り当て済みの **hostname** エントリと同じである必要があります。

- 特権レベル 1 のユーザがより上位の権限レベルを開始する状況を避けるために、1 以外でユーザ単位の特権レベルを設定します（たとえば、0 または 2 ～ 15）。
- ユーザ単位の特権レベルは、仮想端末の特権レベルよりも優先されます。

Cisco IOS Release 15.1(1)S 以降のリリースでは、 **nohangup** キーワードは、SSH ではサポートされません。 **username** *user* **autocommand** *command-name* コマンドが設定されており、SSH が使用されている場合は、設定されているコマンドが実行された後にセッションが切断されます。 SSH のこの動作は Telnet の動作とは逆で、Telnet の動作では、ユーザが Telnet を終了するまで Telnet は継続的に認証を要求し、コマンドを実行し続けます。

CLI および合法的傍受ビュー

CLI ビューおよび合法的傍受ビューの両方とも、特定のコマンドと設定情報へのアクセスを制限します。 合法的傍受ビューを使用すれば、ユーザは、コールとユーザに関する情報を保存する簡易ネットワーク管理プロトコル（SNMP）コマンドの特別なセットである TAP-MIB 内に保持された合法的傍受コマンドへのアクセスを保護できます。

lawful-intercept キーワードを使用して指定されたユーザは、別の特権レベルまたはビュー名が明示的に指定されていない場合、デフォルトで合法的傍受ビューに配置されます。

secret 引数に値が指定されておらず **debug serial-interface** コマンドがイネーブルの場合、リンクが確立されたときにエラーが表示され、CHAP チャレンジは実行されません。 CHAP デバッグ情報は、**debug ppp negotiation**、**debug serial-interface**、および**debug serial-packet** コマンドを使用することで利用できます。 **debug** コマンドの詳細については、『*Cisco IOS Debug Command Reference*』を参照してください。

例

次に、ログイン プロンプトで入力し、ルータの現在のユーザをリストする UNIX の **who** コマンドに似たサービスを実装する例を示します。

```
username who nopassword nohangup autocommand show users
```

次に、パスワードを使用する必要のない情報サービスを実装する例を示します。 コマンドは次の形式になります。

```
username info nopassword noescape autocommand telnet nic.ddn.mil
```

次に、すべての TACACS+ サーバで障害が発生しても機能する ID を実装する例を示します。 コマンドは次の形式になります。

```
username superuser password superpassword
```

次に、「server_1」のインターフェイス シリアル 0 で CHAP をイネーブルにする例を示します。また、「server_r」という名前のリモート サーバのパスワードも定義します。

```
hostname server_1
username server_r password theirsystem
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

次に、暗号化されたパスワードを表示した **show running-config** コマンドの出力を示します。

```
hostname server_1
username server_r password 7 121F0A18
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

次の例では、特権レベル 1 ユーザが、1 よりも高い特権レベルへのアクセスを拒否されています。

```
username user privilege 0 password 0 cisco
username user2 privilege 2 password 0 cisco
```

次に、user2 に対するユーザ名ベースの認証を削除する例を示します。

```
no username user2
```

関連コマンド

コマンド	説明
arap callback	ARA クライアントが ARA クライアントからのコールバックを要求できるようにします。

コマンド	説明
callback forced-wait	Cisco IOS ソフトウェアが、要求元クライアントに対するコールバックを開始する前に待機するように強制します。
debug ppp negotiation	PPP の始動時に、PPP オプションをネゴシエートするために送信された PPP パケットを表示します。
debug serial-interface	シリアル接続障害に関する情報を表示します。
debug serial-packet	**debug serial interface** コマンドを使用して取得したものよりも詳細なシリアルインターフェイスのデバッグ情報を表示します。
ppp callback（**DDR**）	DTR インターフェイスではないダイヤラ インターフェイスが、コールバックを要求するクライアントとして、またはコールバック要求を受け入れるコールバック サーバとして機能できるようにします。
ppp callback（**PPP クライアント**）	PPP クライアントが非同期インターフェイスにダイヤルインして、コールバックを要求できるようにします。
show users	ルータのアクティブ回線に関する情報を表示します。

username secret

不可逆的な暗号化を使用してユーザパスワードを暗号化するには、グローバル コンフィギュレーション モードで **username secret** コマンドを使用します。

username *name* **secret** {**0** *password*| **5** *secret-string*| **4** *secret-string*}

構文の説明

name	ユーザ名。
0	非暗号化シークレットを指定します。
password	クリアテキスト パスワード。
5 *secret-string*	暗号化されたユーザ パスワードとして保存される、メッセージ ダイジェスト アルゴリズム 5（MD5）で暗号化された秘密テキスト ストリング。
4 *secret-string*	暗号化されたユーザ パスワードとして保存される、SHA256 で暗号化された秘密テキスト ストリング。

コマンド デフォルト

ユーザ名に基づく認証システムは確立されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.0(18)S	このコマンドが導入されました。
12.1(8a)E	このコマンドが Cisco IOS Release 12.1(8a)E に統合されました。
12.2(8)T	このコマンドが Cisco IOS Release 12.2(8)T に統合されました。
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	Supervisor Engine 2 上のこのコマンドのサポートが Cisco IOS Release 12.2(17d)SXB に拡張されました。

リリース	変更内容
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。
15.0(1)S	このコマンドが Cisco IOS Release 15.0(1)S に統合されました。 暗号化タイプ **0**、**4**、および **5** が追加されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

使用上のガイドライン

username secret コマンドを使用して、ユーザ名および MD5 で暗号化されたユーザ パスワードを設定します。 MD5 暗号化は、取得不可能な強力な暗号化方式です。したがって、チャレンジ ハンドシェイク認証プロトコル（CHAP）などのクリアテキスト パスワードを必要とするプロトコルでは MD5 暗号化を使用できません。

username secret コマンドは、ユーザ名パスワードに追加のセキュリティ レイヤを提供します。 また、不可逆的な MD5 暗号化を使用してパスワードを暗号化し、暗号化されたテキストを保存することにより、さらにセキュリティが向上します。 追加された MD5 暗号化のレイヤは、パスワードがネットワークを越える、または TFTP サーバに格納される環境で便利です。

ルータ コンフィギュレーション ファイルからコピーした暗号化パスワードをこのコマンドに貼り付ける場合は、暗号化タイプとして MD5 を使用します。

このコマンドを使用すると、指定された取得不可能なユーザ名に対して拡張パスワード セキュリティがイネーブルになります。 このコマンドは、パスワードの MD5 カプセル化をイネーブルにします。 MD5 暗号化は強力な暗号化方式です。 CHAP などのクリアテキスト パスワードを必要とするプロトコルと MD5 との併用はできません。

このコマンドは、特殊な取り扱いが必要なユーザ名を定義する場合に便利です。 たとえば、このコマンドを使用すると、パスワードが不要で、ユーザを汎用の情報サービスに接続する「info」ユーザ名を定義できます。

username コマンドは、ログインだけを目的としてユーザ名または秘密の認証を行います。 *name* 引数に指定できるのは、1 ワードだけです。 スペースと引用符は使用できません。 複数の **username** コマンドを使用して、単一ユーザのオプションを指定できます。

例

次に、ユーザ名「abc」を設定し、クリアテキスト パスワード「xyz」で MD5 暗号化をイネーブルにする例を示します。

```
username abc secret 0 xyz
```

次に、ユーザ名「cde」を設定し、ユーザ名のパスワードとして保存される MD5 暗号化テキスト ストリングを入力する例を示します。

```
username cde secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
```

次に、ユーザ名「xyz」を設定し、ユーザ名のパスワードとして保存される MD5 暗号化テキストストリングを入力する例を示します。

```
username xyz secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
```

関連コマンド

コマンド	説明
enable password	さまざまな権限レベルへのアクセスを制御するローカル パスワードを設定します。
enable secret	enable password コマンドよりも強化したセキュリティ レイヤを指定します。
username	ユーザ名をベースとした認証システムを構築します。