



## show parameter-map type consent から show users まで

---

- [show port-security, 2 ページ](#)
- [show privilege, 5 ページ](#)
- [show radius statistics, 6 ページ](#)
- [show ssh, 12 ページ](#)

# 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

<b>interface</b> <i>interface</i>	(任意) インターフェイス タイプを指定します。有効値は <b>ethernet</b> 、 <b>fastethernet</b> 、 <b>gigabitethernet</b> 、および <b>longreachethernet</b> です。
<i>interface-number</i>	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。
<b>address</b>	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イジング情報を表示します。
<b>vlan</b>	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	<b>address</b> 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
<b>clear port-security</b>	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
<b>enable password</b>	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。
<b>enable secret</b>	<b>enable password</b> 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

アカウントリング 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 1 : *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.	アカウントングパケットの統計情報。
Both	認証パケットとアカウント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。パケットを受信されると、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を確認されます。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、認証とアカウントングの 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 2 : *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 はアカウントングパケットの 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
<b>radius-server host</b>	RADIUS サーバホストを指定します。
<b>radius-server retransmit</b>	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。
<b>radius-server timeout</b>	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

<b>vtty</b>	仮想端末回線 (VTY) 接続の詳細を表示します。
<i>ssh-number</i>	(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 3: *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
<b>show ip ssh</b>	SSH のバージョンおよび設定データを表示します。

