



snmp-server engineID local ~ snmp trap link-status

- [snmp-server file-transfer access-group, 2 ページ](#)
- [snmp-server ip dscp, 4 ページ](#)
- [snmp-server ip precedence, 5 ページ](#)
- [snmp-server manager, 6 ページ](#)
- [snmp-server manager session-timeout, 8 ページ](#)
- [snmp-server queue-length, 10 ページ](#)
- [snmp-server queue-limit, 12 ページ](#)
- [snmp-server source-interface, 14 ページ](#)
- [snmp-server trap authentication unknown-context, 16 ページ](#)
- [snmp-server trap authentication vrf, 17 ページ](#)
- [snmp-server trap link, 19 ページ](#)
- [snmp-server trap link switchover, 21 ページ](#)
- [snmp-server trap retry, 23 ページ](#)
- [snmp-server trap timeout, 25 ページ](#)
- [snmp-server trap-authentication, 27 ページ](#)
- [snmp-server trap-timeout, 28 ページ](#)
- [snmp-server usm cisco, 30 ページ](#)
- [snmp trap if-monitor, 32 ページ](#)
- [snmp trap link-status, 33 ページ](#)

snmp-server file-transfer access-group

転送プロトコル TFTP、FTP、リモート コピー プロトコル (RCP)、セキュア コピー プロトコル (SCP)、およびセキュア ファイル転送プロトコル (SFTP) にアクセス リストを関連付けるには、グローバル コンフィギュレーション モードで **snmp-server file-transfer access-group** コマンドを使用します。アクセス リストの関連付けを解除するには、このコマンドの **no** 形式を使用します。

snmp-server file-transfer access-group {*acl-number*|*acl-name*} [**protocol** *p-name*]

no snmp-server file-transfer access-group {*acl-number*|*acl-name*}

構文の説明

<i>acl-number</i>	標準 ACL を指定する 1 ~ 99 の範囲の整数。
<i>acl-name</i>	標準 ACL を指定する文字列。
protocol	(任意) ユーザが指定されたプロトコルにアクセスグループを関連付けることができるようにします。
<i>p-name</i>	(任意) 転送プロトコルの名前。有効な値は、 ftp 、 rcp 、 scp 、 sftp 、および tftp です。

コマンド デフォルト

プロトコルが指定されていない場合、すべてのプロトコルがアクセス リストに関連付けられません。

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
12.4(12)	このコマンドが導入されました。 snmp-server tftp-server-list コマンドが、このコマンドに置き換えられました。

使用上のガイドライン

snmp-server tftp-server-list コマンドは、Cisco IOS ソフトウェアでまだサポートされていますが、**snmp-server tftp-server-list 10** として設定されている場合、**snmp-server file-transfer access-group 10 protocol tftp** コマンドに置き換えられます。

簡易ネットワーク管理プロトコル (SNMP) 経由で開始された設定の転送を制限するには、**snmp-server file-transfer access-group** コマンドを使用します。アクセスリストをプロトコルに関連付けることによって、特定の転送プロトコルの転送を制限できます。

例

次の例では、転送プロトコル FTP および RCP にアクセス グループ 10 を関連付けます。

```
Router(config)# snmp-server file-transfer access-group 10 protocol ftp
Router(config)# snmp-server file-transfer access-group 10 protocol rcp
```

関連コマンド

コマンド	説明
snmp-server tftp-server-list	SNMP によって制御される TFTP 操作で使用される TFTP サーバをアクセスリストで指定されたサーバに関連付けます。

snmp-server ip dscp

簡易ネットワーク管理プロトコル (SNMP) トラフィックの IP DiffServ コードポイント (DSCP) 値を設定するには、グローバルコンフィギュレーションモードで **snmp-server ip dscp** コマンドを使用します。設定値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。

snmp-server ip dscp value

no snmp-server ip dscp value

構文の説明

<i>value</i>	SNMP トラフィックに適用する IP DSCP 値。IP DSCP の有効な値は 0 ~ 63 です。デフォルトは 0 です。
--------------	--

コマンド デフォルト

SNMP トラフィックの IP DSCP のデフォルト値は 0 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

リリース	変更内容
12.0(26)S	このコマンドが導入されました。
12.4(20)T	このコマンドが、Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

このコマンドは、IP DSCP 値を指定して、ネットワークでの SNMP トラフィックのプライオリティを高くしたり低くしたりするために使用します。

次に、IP DSCP 値を 45 に設定する例を示します。

```
Router(config)# snmp-server ip dscp 45
```

関連コマンド

コマンド	説明
snmp-server ip precedence	IP precedence 値を設定します。

snmp-server ip precedence

snmp-server ip precedence *value*

no snmp-server ip precedence *value*

構文の説明

<i>value</i>	SNMP トラフィックに適用する IP precedence 値。 IP precedence の有効な値は 0 ~ 7 です。デフォルトは 0 です。
--------------	--

コマンド デフォルト

SNMP トラフィックの IP precedence のデフォルト値は 0 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
12.0(26)S	このコマンドが導入されました。
12.4(20)T	このコマンドが、Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

このコマンドは、IP precedence 値を指定して、ネットワークでの SNMP トラフィックのプライオリティを高くしたり低くしたりするために使用します。

例

次の例に、IP precedence 値を 7 に設定する方法を示します。

```
Router(config)# snmp-server ip precedence
7
```

関連コマンド

コマンド	説明
snmp-server ip dscp	IP DSCP 値を設定します。

snmp-server manager

簡易ネットワーク管理プロトコル (SNMP) マネージャプロセスを開始するには、グローバル コンフィギュレーション モードで **snmp-server manager** コマンドを使用します。SNMP マネージャ プロセスを停止するには、このコマンドの **no** 形式を使用します。

snmp-server manager

no snmp-server manager

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

ディセーブル

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
11.3T	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。
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。

使用上のガイドライン

SNMP マネージャプロセスは SNMP 要求をエージェントに送信し、エージェントから SNMP 応答と通知を受け取ります。SNMP マネージャプロセスがイネーブルになっているときには、ルータはその他の SNMP エージェントに問い合わせ、送信されてきた SNMP トラップを処理できません。

ほとんどのネットワークセキュリティポリシーでは、ルータが SNMP 要求を受け付け、SNMP 応答を送信し、SNMP 通知を送信するものと想定されています。SNMP マネージャ機能がイネーブルになっている状態では、ルータは、SNMP 要求の送信、SNMP 応答の受信、および SNMP 通知の受信も行います。場合によっては、この機能をイネーブルにする前にセキュリティポリシーの実装を更新する必要がある場合もあります。

通常、SNMP 要求は UDP ポート 161 に送信されます。通常、SNMP 応答は UDP ポート 161 から送信されます。通常、SNMP 通知は UDP ポート 162 に送信されます。

例

次に、SNMP マネージャ プロセスをイネーブルにする例を示します。

```
Router(config)# snmp-server manager
```

関連コマンド

コマンド	説明
show snmp	SNMP 通信のステータスをチェックします。
show snmp pending	保留状態の SNMP 要求の現在のセットを表示します。
show snmp sessions	現在の SNMP セッションを表示します。
snmp-server manager session-timeout	非アクティブなセッションが破棄されるまでの時間を設定します。

snmp-server manager session-timeout

非アクティブなセッションが破棄されるまでの時間を設定するには、グローバル コンフィギュレーション モードで **snmp-server manager session-timeout** コマンドを使用します。値を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。

snmp-server manager session-timeout *seconds*

no snmp-server manager session-timeout

構文の説明

<i>seconds</i>	アイドルセッションがタイムアウトするまでの秒数。デフォルト値は 600 です。
----------------	---

コマンド デフォルト

アイドルセッションは 600 秒 (10 分) 後にタイムアウトします。

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
11.3T	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せん。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォームハードウェアによって異なります。
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。

使用上のガイドライン

セッションは、ルータ内の SNMP マネージャが SNMP 要求 (インフォーム要求など) をホストに送信したとき、またはホストから SNMP 通知を受信したときに作成されます。各宛先ホストに 1 つずつセッションが生成されます。それ以降、セッションのタイムアウト期間内にルータとホスト間で通信が行われない場合、セッションは削除されます。

ルータは、各セッションについて、ホストに到達するために必要な平均ラウンドトリップ時間などの統計情報を追跡します。ルータ内の SNMP マネージャは、セッションの統計情報を使用し

て、そのホストへの今後の要求（インフォームなど）のための適切なタイムアウト期間を設定できます。セッションが削除されると、すべての統計情報が失われます。その後、同じホストとの別のセッションが作成された場合は、応答の要求タイムアウト値はデフォルト値に戻ります。

ただし、セッションはメモリを消費します。適切なセッションのタイムアウト値は、定期的に使用されるセッションが必要以上に早く削除されない程度に大きいが、不定期に使用されるセッションまたはワンショットセッションが早く消去されるよう小さくする必要があります。

例

次に、デフォルトよりも大きい値にセッション タイムアウトを設定する例を示します。

```
Router(config)# snmp-server manager
Router(config)# snmp-server manager session-timeout 1000
```

関連コマンド

コマンド	説明
show snmp pending	保留状態のSNMP要求の現在のセットを表示します。
show snmp sessions	現在のSNMPセッションを表示します。
snmp-server manager	SNMP マネージャ プロセスを開始します。

snmp-server queue-length

各トラップホストのメッセージキューの長さを設定するには、グローバルコンフィギュレーションモードで **snmp-server queue-length** コマンドを使用します。

snmp-server queue-length *length*

構文の説明

<i>length</i>	保持できるトラップイベントの数を指定する整数。この数を超えると、キューを空にする必要があります。デフォルトは 10 です。
---------------	---

コマンド デフォルト

キュー長は 10. に設定されます。

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
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。

使用上のガイドライン

このコマンドは、各トラップホストのメッセージキューの長さを定義します。トラップメッセージが正常に送信された場合、Cisco IOS ソフトウェアは引き続きキューを空にしますが、1 秒あたり 4 トラップメッセージよりも早いレートではありません。

デバイスの起動時に、一部のトラップがデバイス上のトラップキューオーバーフローのためにドロップされる可能性があります。トラップはドロップされていると思われる場合は、トラップキューのサイズ（たとえば 100）を大きくして、起動時にトラップを送信できるかどうかを確認できます。

例

次に、簡易ネットワーク管理プロトコル（SNMP）通知キューを 50 イベントに設定する例を示します。

```
Router(config)# snmp-server queue-length 50
```

関連コマンド

コマンド	説明
snmp-server packetsize	SNMP サーバが要求を受信または応答を生成するときに許可される SNMP パケットの最大サイズに対する制御を設定します。

snmp-server queue-limit

さまざまなキューのメッセージキューサイズを設定するには、グローバルコンフィギュレーションモードで **snmp-server queue-limit** コマンドを使用します。設定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。

snmp-server queue-limit {dispatcher| engine| notification-host} queue-length

no snmp-server queue-limit {dispatcher| engine| notification-host}

構文の説明

dispatcher	SNMP PDU ディスパッチャ キューの長さを指定します。
engine	SNMP エンジン キューの長さを指定します。
notification-host	各通知ホストのメッセージキューの長さを指定します。
<i>queue-length</i>	キューの長さ。 dispatcher と engine の範囲は 1 ~ 1000 です。 notification-host の範囲は 1 ~ 5000 です。 notification-host のデフォルトの <i>queue-length</i> 値は 10 です。

コマンド デフォルト

デフォルトでは、メッセージ キュー サイズは設定されません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンド履歴

リリース	変更内容
12.0(33)S	このコマンドが導入されました。
12.4(20)T	このコマンドが、Cisco IOS Release 12.4(20)T に統合されました。
12.4(22)T	このコマンドが変更されました。通知ホストのキューの長さの範囲が 1 ~ 5000 に変更されました。

使用上のガイドライン 異なるキューのメッセージキュー サイズを設定するには、**snmp-server queue-limit** コマンドを使用します。このコマンドを使用して、ディスパッチャ、エンジン、およびホストトラップのキューのサイズを変更できます。

例 次に、各通知ホストのメッセージキューの長さを 50 に設定する例を示します。

```
Router(config)# snmp-server queue-limit notification-host 50
```

関連コマンド

コマンド	説明
snmp-server queue-length	各トラップホストのメッセージキューの長さを設定します。

snmp-server source-interface

簡易ネットワーク管理プロトコル（SNMP）トラップがインフォームやトラップの送信元とするインターフェイスを指定するには、グローバル コンフィギュレーション モードで **snmp-server source-interface** コマンドを使用します。送信元の指定を削除するには、このコマンドの **no** 形式を使用します。

snmp-server source-interface {traps| informs} *interface*

no snmp-server source-interface {traps| informs} [*interface*]

構文の説明

traps	SNMP トラップを指定します。
informs	SNMP インフォームを指定します。
<i>interface</i>	送信元インターフェイスのインターフェイス タイプ、およびモジュールとポート番号を指定します。

コマンド デフォルト

インターフェイスは指定されません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンド履歴

リリース	変更内容
12.2(18)SXB2	このコマンドが導入されました。
12.2(18)SXF6	informs キーワードが追加されました。 snmp-server trap-source コマンドが、このコマンドに置き換えられました。
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、フィアチャセット、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 **snmp-server trap-source** コマンドが、このコマンドに置き換えられました。



(注) **snmp-server trap-source** コマンドは、下位互換性のために Cisco IOS ソフトウェアの他のバージョンで使用できます。

送信元インターフェイスには IP アドレスが必要です。 *interface-type module/port* のフォーマットで、*interface* 引数を入力します。

Cisco SNMP サーバから送信された SNMP トラップまたはインフォームには、その時点で送出されたインターフェイスの通知 IP アドレスが設定されています。特定のインターフェイスからの通知をモニタするには、このコマンドを使用します。

例

次に、ギガビットイーサネットインターフェイス 5/2 をすべてのインフォームの送信元として指定する例を示します。

```
snmp-server source-interface informs gigabitethernet5/2
```

次に、ギガビットイーサネットインターフェイス 5/3 をすべてのトラップの送信元として指定する例を示します。

```
snmp-server source-interface traps gigabitethernet5/3
```

次に、特定のインターフェイスの全トラップの送信元指定を削除する例を示します。

```
no snmp-server source-interface traps gigabitethernet5/3
```

関連コマンド

コマンド	説明
snmp-server enable traps	ルータからの SNMP トラップおよびインフォームの送信をイネーブルにします。
snmp-server host	SNMP 通知動作の指定
snmp-server trap-source	SNMP トラップの送信元とするインターフェイスを指定します。

snmp-server trap authentication unknown-context

不明なコンテキストエラー発生時の簡易ネットワーク管理プロトコル (SNMP) 許可失敗 (authFail) トラップ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 **snmp-server trap authentication unknown-context** コマンドを使用します。authFail トラップ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。

snmp-server trap authentication unknown-context

no snmp-server trap authentication unknown-context

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

authFail トラップは生成されません。

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
12.2(18)SXF5	このコマンドが、Supervisor Engine 720 および Supervisor Engine 32 に導入されました。
12.4(22)T	このコマンドは、Cisco IOS Release 12.4(22)T よりも前のリリースに統合されました。
12.2(33)SXI	このコマンドは、Cisco IOS Release 12.2(33)SXI よりも前のリリースに統合されました。

例

次に、不明なコンテキストエラー発生時の許可失敗トラップをイネーブルにする例を示します。

```
Router(config)# snmp-server trap authentication unknown-context
```

次に、不明なコンテキストエラー発生時の許可失敗トラップをディセーブルにする例を示します。

```
Router(config)# no snmp-server trap authentication unknown-context
```

snmp-server trap authentication vrf

バーチャルプライベートネットワーク（VPN）ルーティングおよび転送（VRF）インスタンスコンテキスト認証通知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 **snmp-server trap authentication vrf** コマンドを使用します。他のすべての SNMP 認証通知をイネーブルにしたまま、特に VRF コンテキストの不一致が原因でドロップされた簡易ネットワーク管理プロトコル（SNMP）パケットの認証通知を抑制するには、このコマンドの **no** 形式を使用します。

snmp-server trap authentication vrf

no snmp-server trap authentication vrf

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

SNMP 認証通知がイネーブルになっていない場合、VRF 固有の認証通知はイネーブルになりません。

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(23)S	このコマンドが導入されました。
12.3(2)T	このコマンドが、Release 12.3(2)T に統合されました。
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。
12.2(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。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされません。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォームハードウェアによって異なります。
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

snmp-server enable traps snmp authentication コマンドは SNMP 認証トラップを制御し、このコマンドの **no** 形式はすべての SNMP 認証失敗通知をディセーブルにします。**snmp-server trap authentication vrf** コマンドでは、これらの通知をより細かく制御できます。

コンテキストベースの MIB アクセスによって、各 VRF の SNMP 要求は、特定のコンテキストに関連付けられます。このコンテキストは、アクセスコントロールに使用されます。SNMP コンテキストが VPN 用に設定されている場合、設定済みコンテキストに一致しない SNMP 要求により、SNMP 認証失敗通知が生成されます。**no snmp-server trap authentication vrf** コマンドを使用すると、他のすべての SNMP 認証失敗通知をイネーブルにしたまま、これらの VRF コンテキストに固有の認証失敗通知を抑制できます。

no snmp-server trap authentication vrf コマンドは、**snmp-server enable traps snmp authentication** コマンドが設定されていない場合は効果がありません。

例

次に、すべての VRF 認証トラップをディセーブルにしたまま、ルータがコミュニティストリング **public** を使用してホスト **myhost.cisco.com** にすべての SNMP 認証トラップを送信できるようにする例を示します。

```
Router(config)# snmp-server enable traps snmp authentication

Router(config)# no snmp-server trap authentication vrf
Router(config)# snmp-server host myhost.cisco.com public
```

関連コマンド

コマンド	説明
snmp-server enable traps snmp	RFC 1157 SNMP 通知の送信をイネーブルにします。
snmp-server host	SNMP 通知動作の指定

snmp-server trap link

RFC2233に準拠するリンクアップ/リンクダウン簡易ネットワーク管理プロトコル (SNMP) トラップ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 **snmp-server trap link** コマンドを使用します。IETF に準拠した機能をディセーブルにし、リンクアップ/リンクダウントラップのデフォルトのシスコ実装に戻すには、このコマンドの **no** 形式を使用します。

snmp-server trap link ietf

no snmp-server trap link ietf

構文の説明

ietf	コマンドパーサーに（以前のシスコ実装ではなく）Internet Engineering Task Force (IETF) 標準に SNMP リンクアップ/リンクダウントラップの機能をリンクするように通知します。
-------------	--

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

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
12.1(2)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 12.2(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

snmp-server trap link ietf コマンドは、リンクアップ/リンクダウントラップの RFC 2233 IETF 標準ベースの実装を使用するようにルータを設定するために使用します。以前のシスコ実装のリンクアップ/リンクダウントラップを使用することを選択した場合は、これを使用し続けられるよう、このコマンドはデフォルトではディセーブルにされています。

ただし、デフォルトのシスコ オブジェクト定義を使用する場合は、リンクアップ/リンクダウン
トラップがサブインターフェイスに対して正しく生成されないことに注意してください。デフォ
ルトの実装では、任意の値がサブインターフェイスのリンクアップ/リンクダウントラップにある
locIfReason オブジェクトに使用されるため、意図しない結果がもたらされる可能性があります。
これは、*locIfReason* オブジェクトが OLD-CISCO-INTERFACES-MIB.my を使用する現在のシスコ
実装でサブインターフェイスに対して定義されていないためです。

この機能をイネーブルにしない場合、リンクトラップの varbind リストは、{ifIndex, ifDescr, ifType,
locIfReason} で構成されます。 **snmp-server trap link ietf** コマンドを使用してこの機能をイネーブ
ルにした後では、変数バインドリストは、{inIndex, ifAdminStatus, ifOperStatus, ifDescr, ifType} で
構成されます。 *locIfReason* オブジェクトも、そのオブジェクトにとって意味のある情報が取得で
きるかどうかによって、条件付きで、このリストに含まれます。設定されたサブインターフェイ
スは、取得可能な情報を生成します。非 HWIDB インターフェイスでは、*locIfReason* に対して定
義されている値はないため、トラップメッセージからは省略されます。

例

次に、特権 EXEC モードを開始して、RFC 2233 のリンクアップ/リンクダウントラップをイネー
ブルにする例を示します。

```
Router#
configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
snmp-server trap link ietf

Router(config)#
end
Router#
more system:running configuration
.
.
.
!
snmp-server engineID local 000000090000000A1616C2056
snmp-server community public RO
snmp-server community private RW
snmp-server trap link ietf
!
.
.
.
```

関連コマンド

コマンド	説明
debug snmp packets	トラブルシューティングのために、ルータが送受信したすべての SNMP パケットに関する情報を表示します。

snmp-server trap link switchover

スイッチ フェールオーバー時に、リンクアップトラップによって引き継がれるリンクダウントラップの送信をスイッチのすべてのインターフェイスで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 **snmp-server trap link switchover** コマンドを使用します。スイッチ フェールオーバー時のリンクダウン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。

snmp-server trap link switchover

no snmp-server trap link switchover

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

このコマンドは、デフォルトでイネーブルになっています。

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
12.2(18)SXF2	このコマンドが、Supervisor Engine 720 および Supervisor Engine 32 に導入されました。
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

デフォルトでは、スイッチオーバー時にリンクトラップが生成されません。

例

次に、スイッチフェールオーバー時に、リンクアップトラップによって引き継がれるリンクダウントラップの送信をスイッチのすべてのインターフェイスでイネーブルにする例を示します。

```
snmp-server trap link switchover
```

次に、スイッチフェールオーバー時に、リンクアップトラップによって引き継がれるリンクダウンをスイッチのすべてのインターフェイスでディセーブルにする例を示します。

```
no snmp-server trap link switchover
```

snmp-server trap retry

トラップを送信するまでにデバイスの簡易ネットワーク管理プロトコル (SNMP) エージェントがルートの検索を試行する回数を定義するには、グローバル コンフィギュレーション モードで **snmp-server trap retry** コマンドを使用します。

snmp-server trap retry *number*

構文の説明

<i>number</i>	メッセージが再送信される回数を設定する 0～10 の整数。デフォルトは 3 です。
---------------	---

コマンド デフォルト

メッセージは再送信されません。

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
12.2(33)SRA	このコマンドが導入されました。

使用上のガイドライン

SNMP エージェントは、宛先にトラップを送信する前にシステムの設定済みルートを検索します。ルートがない場合、トラップがトラップ キューに格納され、キューがいっぱいになると廃棄されます。 **snmp-server trap retry** コマンドが設定されている場合、ルート検索の試行回数に応じて、エージェントはトラップを送信するまでにルートを検索する回数を把握します。

また、**snmp-server trap retry** コマンドを設定すると、ポリシーベースルーティングトラップが送信され、廃棄されません。ポリシーベーストラップはすぐに送信する必要があり、ルートは必要ではありません。ポリシーベーストラップをすぐに送信するように、再試行回数を 0 に設定する必要があります。

例

次に、デバイスの SNMP エージェントがルートを検索する回数を 10 に設定する例を示します。

```
Router(config)# snmp-server trap retry 10
```

関連コマンド

コマンド	説明
snmp-server trap timeout	再送信キューのトラップの再送信間隔を定義します。

snmp-server trap timeout

再送信キューにあるトラップメッセージの再送信間隔を定義するには、グローバルコンフィギュレーションモードで **snmp-server trap timeout** コマンドを使用します。

snmp-server trap timeout seconds

構文の説明

<i>seconds</i>	メッセージの再送信間隔（秒単位）を設定する 1 ~ 1000 の整数。デフォルトは 30 です。
----------------	--

コマンド デフォルト

このコマンドはディセーブルです。

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
12.2(33)SRA	このコマンドが導入されました。Cisco IOS Release 12.2SR でのみ、 snmp-server trap-timeout コマンドがこのコマンドに置き換えられました。

使用上のガイドライン

トラップが送信される前に、SNMP エージェントは、宛先アドレスへのルートを検索します。既知のルートがない場合、トラップは再送信キューに保存されます。再送信を試みる間隔の秒数を指定するには、**snmp-server trap timeout** コマンドを使用します。

例

次に、トラップの再送信の間隔として 20 秒を設定する例を示します。

```
Router(config)# snmp-server trap timeout 20
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の指定

コマンド	説明
snmp-server queue-length	各トラップホストのメッセージキューの長さを設定します。

snmp-server trap-authentication

snmp-server trap-authentication コマンドは、**snmp-server enable traps snmp authentication** コマンドに置き換えられました。詳細については、この章の **snmp-server enable traps snmp** コマンドの説明を参照してください。

snmp-server trap-timeout



(注) このコマンドは、Cisco IOS Release 12.2SR ではサポートされません。Cisco IOS Release 12.2SR では、**snmp-server trap timeout** コマンドを使用します。

再送信キューにあるトラップメッセージの再送信を試みる間隔を定義するには、グローバルコンフィギュレーションモードで **snmp-server trap-timeout** コマンドを使用します。

snmp-server trap-timeout seconds

構文の説明

<i>seconds</i>	メッセージの再送信間隔（秒単位）を設定する 1 ~ 1000 の整数。デフォルトは 30 です。
----------------	--

コマンド デフォルト

30 秒

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	Cisco IOS Release 12.2SR では、このコマンドが snmp-server trap timeout コマンドに置き換えられました。

使用上のガイドライン

snmp-server trap-timeout コマンドは互換性を維持するために Cisco IOS ソフトウェアに残されていますが、設定には **snmp-server trap timeout** として書き込まれます。

Cisco IOS ソフトウェアは、トラップの送信を試みる前に、宛先アドレスまでのルートを検索します。既知のルートがない場合、トラップは再送信キューに保存されます。**snmp-server trap-timeout** コマンドは、再送信を試みる間隔を秒数で指定します。

例

次に、再送信キューのトラップメッセージの再送信を 20 秒間隔で試みるように設定する例を示します。

```
Router(config)# snmp-server trap-timeout 20
```

関連コマンド

コマンド	説明
snmp-server host	SNMP 通知動作の指定
snmp-server queue-length	各トラップホストのメッセージキューの長さを設定します。

snmp-server usm cisco

ユーザベース セキュリティ モデル (USM) である簡易ネットワーク管理プロトコルバージョン 3 (SNMPv3) のシスコ固有のエラー メッセージ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 **snmp-server usm cisco** コマンドを使用します。SNMPv3 USM のシスコ固有のエラー メッセージ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。

snmp-server usm cisco

no snmp-server usm cisco

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

SNMPv3 USM のシスコ固有のエラー メッセージはディセーブルになっています。

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
15.2(1)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

RFC 3414 準拠のエラーメッセージは具体的であり、悪意のあるユーザによる情報の不正使用が発生する可能性があります。正確なエラー状態を非表示にするのに役立つシスコ固有のメッセージをイネーブルにするには、**snmp-server usm cisco** コマンドを使用します。SNMPv3 のシスコ固有のメッセージをイネーブルにすると、RFC 3414 から逸脱することになります。

例

次に、SNMPv3 USM のシスコ固有のエラー メッセージをイネーブルにする例を示します。

```
Router> enable
Router# configure terminal
Router(config)# snmp-server usm cisco
Router(config)# exit
```

関連コマンド

コマンド	説明
show running-config	現在実行されている設定ファイル、または特定のモジュール、レイヤ2 VLAN、クラスマップ、インターフェイス、マップクラス、ポリシーマップ、仮想回線（VC）クラスの設定内容を表示します。

snmp trap if-monitor

特定のインターフェイスの if-monitor トラップ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 **snmp trap if-monitor** コマンドを使用します。インターフェイスのトラップ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。

snmp trap if-monitor

no snmp trap if-monitor

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

トラップは生成されません。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンド履歴

リリース	変更内容
12.3(1)	このコマンドが導入されました。

使用上のガイドライン

特定のインターフェイスのトラップが送信されるのは、**snmp-server enable traps if-monitor** コマンドを発行してグローバルにイネーブルにしてから、**snmp trap if-monitor** コマンドを発行して明示的にそのインターフェイスでイネーブルにした場合のみです。

例

次に、特定のインターフェイスの if-monitor トラップをイネーブルにする例を示します。

```
Router(config)# snmp-server enable traps if-monitor
Router(config)# interface ethernet 1/1
Router(config-if)# snmp trap if-monitor
```

関連コマンド

コマンド	説明
snmp-server enable traps if-monitor	if-monitor トラップをグローバルにイネーブルにします。

snmp trap link-status

簡易ネットワーク管理プロトコル（SNMP）リンク トラップの生成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 モードまたはサービス インスタンス コンフィギュレーション モードで **snmp trap link-status** コマンドを使用します。SNMP リンク トラップの生成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。

snmp trap link-status [permit duplicates]

no snmp trap link-status [permit duplicates]

構文の説明

permit duplicates	(任意) SNMP リンクアップトラップおよびリンクダウン トラップの重複を許可します。
--------------------------	--

コマンド デフォルト

SNMP リンク トラップは、インターフェイスがアップまたはダウンした場合に生成されます。

コマンド モード

インターフェイス コンフィギュレーション (config-if)、サービス インスタンス コンフィギュレーション (config-if-srv)

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(30)S	このコマンドが変更されました。 permit duplicates キーワードペアが追加されました。
12.3(8)T	このコマンドが Cisco IOS Release 12.3(8)T に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(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	このコマンドの動作は、使用上のガイドラインに従って、PRE3 用と PRE4 用の Cisco 10000 シリーズ ルータで変更されました。

リリース	変更内容
12.2(33)SRD1	このコマンドのサポートが、サービス インスタンス コンフィギュレーション モードに拡張されました。
12.2(33)SRE6	このコマンドが変更されました。このリリース以降、このコマンドは、各サブ インターフェイスでイネーブルにする必要があります。
15.1(3)S3	このコマンドが、Cisco IOS Release 15.1(3)S3 に統合されました。

使用上のガイドライン

デフォルトでは、SNMP リンク トラップは、インターフェイスがアップまたはダウンしたときに送信されます。通常使用中もアップまたはダウンすると予想される ISDN インターフェイスなどのインターフェイスでは、これらのトラップによって生成される出力は有用でない場合があります。このコマンドの **no** 形式を使用すると、これらのトラップがディセーブルになります。

permit および **duplicates** キーワードは、一緒に使用され、個別には使用できません。インターフェイスが SNMP リンクアップトラップ、リンクダウントラップ、または両方を生成しない場合に **permit duplicates** キーワードペアを使用します。 **snmp trap link-status permit duplicates** コマンドを設定すると、複数のトラップが同じリンクアップまたはリンクダウン遷移に対して送信される場合があります。

permit duplicates キーワードペアは SNMP リンク トラップが生成されることを保証するものではなく、トラップを受信するためにこれらのキーワードの設定は必須ではありません。

デフォルトでは、サービス インスタンス コンフィギュレーション モードで SNMP リンク トラップは送信されません。また、サービス インスタンス コンフィギュレーション モードでは **permit duplicates** キーワードペアを使用できません。

ATM サブインターフェイスで SNMP トラップ通知をイネーブルにするには、**snmp trap link-status** コマンドを **snmp-server enable traps atm subif** コマンドとともに使用する必要があります。

snmp-server enable traps atm subif コマンドをグローバル コンフィギュレーション モードで設定する必要があり、その後、SNMP トラップ通知をイネーブルにする各 ATM サブインターフェイスで **snmp trap link-status** コマンドを設定する必要があります。

Cisco 10000 シリーズ ルータ

Cisco IOS Release 12.2(33)SB では、**virtual-template snmp** コマンドに新しいデフォルト設定があります。デフォルトでイネーブルになるのではなく、**no virtual-template snmp** がデフォルト設定です。この設定は、スケーリングを拡張し、MIB ifTable における多数のエントリを防ぐことにより、SNMP がインターフェイス MIB およびその他の関連 MIB を使用するとき CPU Hog メッセージを回避します。

no virtual-template snmp コマンドを設定すると、デバイスは仮想テンプレート インターフェイスで **snmp trap link-status** コマンドを受け入れなくなります。代わりに、次のような設定エラーメッセージが表示されます。

```
Device (config)# interface virtual-template 1
```

```
Device(config-if)# snmp trap link-status
%Unable set link-status enable/disable for interface
```

すでに設定で仮想テンプレートインターフェイスに **snmp trap link-status** コマンドが設定されている場合、Cisco IOS Release 12.2(33)SB にアップグレードすると、仮想テンプレートインターフェイスがインターフェイス MIB ですでに登録されていても、デバイスのリロード時に設定エラーが表示されます。

例

次に、ISDN BRI インターフェイス 0 に関連する SNMP リンク トラップをディセーブルにする例を示します。

```
Device(config)# interface bri 0
Device(config-if)# no snmp trap link-status
```

次に、イーサネットインターフェイス 0/1 のサービス インスタンス 50 の SNMP リンク トラップをイネーブルにする例を示します。

```
Device(config)# interface ethernet 0/1
Device(config-if)# service instance 50 ethernet
Device(config-if-srv)# snmp trap link-status
Device(config-if-srv)# end
```

関連コマンド

コマンド	説明
snmp-server enable traps atm subif	ATM サブインターフェイスの SNMP 通知の送信をイネーブルにします。
virtual-template snmp	仮想アクセスインターフェイスを作成または再利用するときに SNMP に登録できます。

