



Catalyst 2960-XR スイッチ ネットワーク管理コンフィギュレーションガイド、Cisco IOS リリース 15.0(2)EX1

初版：2013年08月08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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2013 Cisco Systems, Inc. All rights reserved.



目次

はじめに ix

表記法 ix

関連資料 xi

マニュアルの入手方法およびテクニカル サポート xi

コマンドライン インターフェイスの使用 1

コマンドライン インターフェイスの使用に関する情報 1

コマンド モード 1

ヘルプ システムの使用 5

コマンドの省略形 6

コマンドの no 形式および default 形式 6

CLI のエラー メッセージ 6

コンフィギュレーション ロギング 7

CLI を使用して機能を設定する方法 8

コマンド履歴の設定 8

コマンド履歴バッファ サイズの変更 8

コマンドの呼び出し 8

コマンド履歴機能のディセーブル化 9

編集機能のイネーブル化およびディセーブル化 9

キーストロークによるコマンドの編集 10

画面幅よりも長いコマンドラインの編集 12

show および more コマンド出力の検索およびフィルタリング 13

コンソール接続または Telnet による CLI アクセス 13

Cisco IOS Configuration Engine の設定 15

機能情報の確認 15

Configuration Engine を設定するための前提条件 15

Configuration Engine の設定に関する制約事項 16

Configuration Engine の設定について	16
Cisco Configuration Engine ソフトウェア	16
コンフィギュレーションサービス	17
イベント サービス	18
NSM	18
Cisco Networking Service ID およびデバイスのホスト名	18
ConfigID	19
DeviceID	19
ホスト名および DeviceID	19
ホスト名、DeviceID、および ConfigID	20
Cisco IOS CNS エージェント	20
初期設定	20
差分（部分的）設定	21
コンフィギュレーションの同期	21
自動 CNS 設定	22
Configuration Engine の設定方法	23
CNS イベント エージェントのイネーブル化	23
Cisco IOS CNS エージェントのイネーブル化	25
Cisco IOS CNS エージェントの初期設定のイネーブル化	27
DeviceID の更新	32
Cisco IOS CNS エージェントの部分的設定のイネーブル化	34
CNS 設定のモニタリング	35
その他の関連資料	36
Configuration Engine の機能の履歴と情報	37
Cisco Discovery Protocol の設定	39
機能情報の確認	39
CDP の概要	39
CDP の概要	39
CDP およびスタック	40
CDP のデフォルト設定	40
CDP の設定方法	41
CDP 特性の設定	41
CDP のディセーブル化	42

CDP のイネーブル化	43
インターフェイス上での CDP のディセーブル化	44
インターフェイス上での CDP のイネーブル化	46
CDP のモニタおよびメンテナンス	47
その他の関連資料	48
Cisco Discovery Protocol の機能の履歴と情報	49
簡易ネットワーク管理プロトコルの設定	51
機能情報の確認	51
SNMP の前提条件	51
SNMP の制約事項	54
SNMP に関する情報	55
SNMP の概要	55
SNMP マネージャ機能	55
SNMP エージェント機能	56
SNMP コミュニティストリング	56
SNMP MIB 変数アクセス	57
SNMP 通知	57
SNMP ifIndex MIB オブジェクト値	58
SNMP のデフォルト設定	58
SNMP 設定時の注意事項	59
SNMP の設定方法	60
SNMP エージェントのディセーブル化	60
コミュニティストリングの設定	61
SNMP グループおよびユーザの設定	63
SNMP 通知の設定	66
エージェント コンタクトおよびロケーションの設定	71
SNMP を通して使用する TFTP サーバの制限	72
SNMP ステータスのモニタリング	73
SNMP での例	74
簡易ネットワーク管理プロトコルの機能の履歴と情報	75
SPAN および RSPAN の設定	77
機能情報の確認	77

SPAN および RSPAN の前提条件	77
SPAN および RSPAN の制約事項	78
SPAN および RSPAN について	81
SPAN および RSPAN	81
ローカル SPAN	81
リモート SPAN	83
SPAN と RSPAN の概念および用語	83
SPAN セッション	84
監視対象トラフィック	84
送信元ポート	86
送信元 VLAN	86
VLAN フィルタリング	87
宛先ポート	87
RSPAN VLAN	88
SPAN および RSPAN と他の機能の相互作用	89
SPAN と RSPAN とデバイス スタック	90
フローベースの SPAN	91
SPAN および RSPAN のデフォルト設定	92
設定時の注意事項	92
SPAN 設定時の注意事項	92
RSPAN 設定時の注意事項	93
FSPAN および FRSPAN 設定時の注意事項	93
SPAN および RSPAN の設定方法	93
ローカル SPAN セッションの作成	93
ローカル SPAN セッションの作成および着信トラフィックの設定	96
フィルタリングする VLAN の指定	98
RSPAN VLAN としての VLAN の設定	99
RSPAN 送信元セッションの作成	101
フィルタリングする VLAN の指定	103
RSPAN 宛先セッションの作成	104
RSPAN 宛先セッションの作成および着信トラフィックの設定	106
FSPAN セッションの設定	108

FRSPAN セッションの設定	110
SPAN および RSPAN 動作のモニタリング	113
SPAN および RSPAN の設定例	113
例：ローカル SPAN の設定	113
例：RSPAN VLAN の作成	114
SPAN および RSPAN の機能の履歴と情報	115



はじめに

- [表記法, ix ページ](#)
- [関連資料, xi ページ](#)
- [マニュアルの入手方法およびテクニカル サポート, xi ページ](#)

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
^ または Ctrl	^ 記号と Ctrl は両方ともキーボードの Control (Ctrl) キーを表します。たとえば、 ^D または Ctrl+D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します（ここではキーを大文字で表記していますが、小文字で入力してもかまいません）。
bold フォント	コマンド、キーワード、およびユーザーが入力したテキストは、 太字 フォントで示しています。
<i>Italic</i> フォント	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、 <i>italic</i> フォントで示しています。
courier フォント	システムが表示するターミナルセッションおよび情報は、courier フォントで示しています。
太字の courier フォント	太字の courier フォントは、ユーザーが入力しなければならないテキストを示します。
[x]	角カッコの中の要素は、省略可能です。

表記法	説明
...	構文要素の後の省略記号（3つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。
	パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示します。
[x y]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
{x y}	必ずいずれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x {y z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
string	引用符を付けない一組の文字。stringの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてstringとみなされます。
<>	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[]	システムプロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。

読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。



(注)

「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。



ヒント

「問題解決に役立つ情報」です。



注意

「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。



ワンポイントアドバイス

時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。



警告

「警告」の意味です。人身事故を予防するための注意事項が記述されています。

関連資料



(注)

スイッチをインストールまたはアップグレードする前に、スイッチのリリース ノートを参照してください。

- 次の URL にある Catalyst 2960-XR スイッチのマニュアル :

http://www.cisco.com/go/cat2960xr_docs

- 次の URL にある Cisco SFP および SFP+ モジュールのマニュアル (互換性マトリクスを含む) :

http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html

- 次の URL にある Cisco Validated Design (CVD) のマニュアル :

<http://www.cisco.com/go/designzone>

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。



第 1 章

コマンドラインインターフェイスの使用

- [コマンドラインインターフェイスの使用に関する情報, 1 ページ](#)
- [CLIを使用して機能を設定する方法, 8 ページ](#)

コマンドラインインターフェイスの使用に関する情報

コマンドモード

Cisco IOS ユーザインターフェイスは、いくつかのモードに分かれています。使用できるコマンドの種類は、現在のモードによって異なります。システムプロンプトに疑問符 (?) を入力すると、各コマンドモードで使用できるコマンドの一覧が表示されます。

コンソール接続、Telnet、SSH、またはブラウザを使用することによってCLIセッションを開始できます。

セッションを開始すると、ユーザモード（別名ユーザ EXEC モード）から始まります。ユーザ EXEC モードでは、限られた一部のコマンドしか使用できません。たとえばユーザ EXEC コマンドの大部分は、**show** コマンド（現在のコンフィギュレーションステータスを表示する）、**clear** コマンド（カウンタまたはインターフェイスをクリアする）などのように、1 回限りのコマンドです。ユーザ EXEC コマンドは、スイッチをリブートするときには保存されません。

すべてのコマンドにアクセスするには、特権 EXEC モードを開始する必要があります。特権 EXEC モードを開始するには、通常、パスワードが必要です。このモードでは、任意の特権 EXEC コマンドを入力でき、また、グローバルコンフィギュレーションモードを開始することもできます。

コンフィギュレーションモード（グローバル、インターフェイス、およびライン）を使用して、実行コンフィギュレーションを変更できます。設定を保存した場合はこれらのコマンドが保存され、スイッチをリブートときに使用されます。各種のコンフィギュレーションモードにアクセスするには、まずグローバルコンフィギュレーションモードを開始する必要があります。グローバルコンフィギュレーションモードから、インターフェイスコンフィギュレーションモードおよびラインコンフィギュレーションモードに移行できます。

次の表に、主要なコマンドモード、各モードへのアクセス方法、各モードで表示されるプロンプト、およびモードの終了方法を示します。

表 1: コマンドモードの概要

モード	アクセス方法	プロンプト	終了方法	モードの用途
ユーザ EXEC	Telnet、SSH、またはコンソールを使用してセッションを開始します。	Switch>	logout または quit を入力します。	このモードを使用して次の作業を行います。 <ul style="list-style-type: none"> • 端末の設定変更 • 基本テストの実行 • システム情報の表示
特権 EXEC	ユーザ EXEC モードで、 enable コマンドを入力します。	Switch#	disable を入力して終了します。	このモードを使用して、入力したコマンドを確認します。パスワードを使用して、このモードへのアクセスを保護します。
グローバル コンフィギュレーション	特権 EXEC モードで、 configure コマンドを入力します。	Switch(config)#	終了して特権 EXEC モードに戻るには、 exit または end コマンドを入力するか、 Ctrl+Z を押します。	このモードは、スイッチ全体に適用するパラメータを設定する場合に使用します。
VLAN コンフィギュレーション	グローバル コンフィギュレーションモードで、 vlan vlan-id コマンドを入力します。	Switch(config-vlan)#	グローバル コンフィギュレーションモードに戻る場合は、 exit コマンドを入力します。 特権 EXEC モードに戻るには、 Ctrl+Z を押すか、 end を入力します。	

モード	アクセス方法	プロンプト	終了方法	モードの用途
				このモードを使用して、VLAN（仮想LAN）パラメータを設定します。VTPモードがトランスペアレントであるときは、拡張範囲 VLAN（VLAN ID が 1006 以上）を作成してスイッチのスタートアップコンフィギュレーションファイルに設定を保存できます。
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードで、 interface コマンド を入力し、インター フェイスを指定 します。	Switch(config-if)#	終了してグローバル コンフィギュレーション モードに戻るには、 exit を入力します。 特権 EXEC モード に戻るには、 Ctrl+Z を押すか、 end を入力しま す。	このモードを使用 して、イーサネット ポートのパラ メータを設定しま す。
ライン コンフィ ギュレーション	グローバル コン フィギュレーション モードで、 line vty または line console コマンド を使用して回線を 指定します。	Switch(config-line)#	終了してグローバル コンフィギュレーション モードに戻るには、 exit を入力します。 特権 EXEC モード に戻るには、 Ctrl+Z を押すか、 end を入力しま す。	このモードを使用 して、端末回線の パラメータを設定 します。

ヘルプ システムの使用

システム プロンプトで疑問符 (?) を入力すると、各コマンドモードに使用できるコマンドのリストが表示されます。また、任意のコマンドについて、関連するキーワードおよび引数の一覧を表示することもできます。

手順の概要

1. **help**
2. *abbreviated-command-entry ?*
3. *abbreviated-command-entry <Tab>*
4. **?**
5. *command ?*
6. *command keyword ?*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	help 例： Switch# help	コマンドモードのヘルプ システムの簡単な説明を表示します。
ステップ 2	<i>abbreviated-command-entry ?</i> 例： Switch# di? dir disable disconnect	特定のストリングで始まるコマンドのリストを表示します。
ステップ 3	<i>abbreviated-command-entry <Tab></i> 例： Switch# sh conf<tab> Switch# show configuration	特定のコマンド名を補完します。
ステップ 4	? 例： Switch> ?	特定のコマンドモードで使用可能なすべてのコマンドをリストします。
ステップ 5	<i>command ?</i> 例： Switch> show ?	コマンドに関連するキーワードを一覧表示します。

	コマンドまたはアクション	目的
ステップ 6	<p><i>command keyword ?</i></p> <p>例 :</p> <pre>Switch(config)# cdp holdtime ? <10-255> Length of time (in sec) that receiver must keep this packet</pre>	キーワードに関連する引数を一覧表示します。

コマンドの省略形

スイッチでコマンドが一意に認識される長さまでコマンドを入力します。

show configuration 特権 EXEC コマンドを省略形で入力する方法を次に示します。

```
Switch# show conf
```

コマンドの **no** 形式および **default** 形式

大部分のコンフィギュレーション コマンドに、**no** 形式があります。**no** 形式は一般に、特定の機能または動作をディセーブルにする場合、あるいはコマンドの動作を取り消す場合に使用します。たとえば、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイスのシャットダウンが取り消されます。**no** キーワードなしでコマンドを使用すると、ディセーブルにされた機能を再度イネーブルにしたり、デフォルトでディセーブルになっている機能をイネーブルにすることができます。

コンフィギュレーション コマンドには、**default** 形式もあります。コマンドの **default** 形式は、コマンドの設定値をデフォルトに戻します。大部分のコマンドはデフォルトでディセーブルに設定されているので、**default** 形式は **no** 形式と同じになります。ただし、デフォルトでイネーブルに設定されていて、なおかつ変数が特定のデフォルト値に設定されているコマンドもあります。これらのコマンドについては、**default** コマンドを使用すると、コマンドがイネーブルになり、変数がデフォルト値に設定されます。

CLI のエラー メッセージ

次の表に、CLI を使用してスイッチを設定するときに表示される可能性のあるエラー メッセージの一部を紹介します。

表 2: CLIの代表的なエラー メッセージ

エラー メッセージ	意味	ヘルプの表示方法
% Ambiguous command: "show con"	スイッチがコマンドとして認識できるだけの文字数が入力されていません。	コマンドを再入力し、最後に疑問符 (?) を入力します。コマンドと疑問符の間にはスペースを1つ入れます。 コマンドとともに使用できるキーワードが表示されます。
% Incomplete command.	コマンドに必須のキーワードまたは値が、一部入力されていません。	コマンドを再入力し、最後に疑問符 (?) を入力します。コマンドと疑問符の間にはスペースを1つ入れます。 コマンドとともに使用できるキーワードが表示されます。
% Invalid input detected at '^' marker.	コマンドの入力ミスです。間違っている箇所をキャレット (^) 記号で示しています。	疑問符 (?) を入力すると、そのコマンドモードで使用できるすべてのコマンドが表示されます。 コマンドとともに使用できるキーワードが表示されます。

コンフィギュレーション ロギング

スイッチの設定変更を記録して表示させることができます。 Configuration Change Logging and Notification 機能を使用することで、セッションまたはユーザ ベースごとに変更内容をトラッキングできます。ログに記録されるのは、適用された各コンフィギュレーションコマンド、コマンドを入力したユーザ、コマンドの入力時間、コマンドに対するパーサからのリターンコードです。この機能には、登録しているアプリケーションの設定が変更されるときに通知される非同期通知方式もあります。 Syslog へこの通知を送信することも選択できます。



(注) CLI または HTTP の変更のみがログとして記録されます。

CLI を使用して機能を設定する方法

コマンド履歴の設定

入力したコマンドは、ソフトウェア側にコマンド履歴として残されます。コマンド履歴機能は、アクセスコントロールリストの設定時など、長い複雑なコマンドまたはエントリを何度も入力しなければならない場合、特に便利です。必要に応じて、この機能をカスタマイズできます。

コマンド履歴バッファ サイズの変更

デフォルトでは、スイッチは履歴バッファにコマンドライン 10 行を記録します。現在の端末セッションまたは特定回線のすべてのセッションで、この数を変更できます。この手順は任意です。

手順の概要

1. **terminal history [size number-of-lines]**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	terminal history [size number-of-lines] 例： Switch# terminal history size 200	特権 EXEC モードで現在のターミナルセッション中にスイッチが記録するコマンドラインの数を変更します。サイズは 0 から 256 までの間で設定できます。

コマンドの呼び出し

履歴バッファにあるコマンドを呼び出すには、次の表に示すいずれかの操作を行います。これらの操作は任意です。



(注) 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

手順の概要

1. **Ctrl+P** または上矢印キー
2. **Ctrl+N** または下矢印キー
3. **show history**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Ctrl+P または上矢印キー	履歴バッファ内のコマンドを呼び出します。最後に実行したコマンドが最初に呼び出されます。キーを押すたびに、より古いコマンドが順次表示されます。
ステップ 2	Ctrl+N または下矢印キー	Ctrl+P または上矢印キーでコマンドを呼び出した後で、履歴バッファ内のより新しいコマンドに戻ります。キーを押すたびに、より新しいコマンドが順次表示されます。
ステップ 3	show history 例： Switch# show history	特権 EXEC モードで、直前に入力したコマンドをいくつか表示します。表示されるコマンドの数は、 terminal history グローバルコンフィギュレーション コマンドおよび history ライン コンフィギュレーション コマンドの設定値によって指定されます。

コマンド履歴機能のディセーブル化

コマンド履歴機能は、自動的にイネーブルになっています。現在の端末セッションまたはコマンドラインでディセーブルにできます。この手順は任意です。

手順の概要

1. terminal no history

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	terminal no history 例： Switch# terminal no history	特権 EXEC モードで現在のターミナルセッションにおけるこの機能をディセーブルにします。

編集機能のイネーブル化およびディセーブル化

拡張編集モードは自動的に有効に設定されますが、ディセーブルにしてから、再びイネーブルにすることもできます。

手順の概要

1. terminal editing
2. terminal no editing

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	terminal editing 例： Switch# terminal editing	特権 EXEC モードで現在のターミナルセッションにおける拡張編集モードを再びイネーブルにします。
ステップ 2	terminal no editing 例： Switch# terminal no editing	特権 EXEC モードで現在のターミナルセッションにおける拡張編集モードをディセーブルにします。

キーストロークによるコマンドの編集

キーストロークは、コマンドラインの編集に役立ちます。これらのキーストロークは任意です。



(注) 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

表 3: 編集コマンド

編集コマンド	説明
Ctrl-B または 左矢印キー	カーソルを 1 文字後退させます。
Ctrl-F または 右矢印キー	カーソルを 1 文字前進させます。
Ctrl+A	コマンドラインの先頭にカーソルを移動します。
Ctrl+E	カーソルをコマンドラインの末尾に移動します。
Esc B	カーソルを 1 単語後退させます。
Esc F	カーソルを 1 単語前進させます。

Ctrl+T	カーソルの左にある文字を、カーソル位置の文字と置き換えます。
Delete キーまたは Backspace キー	カーソルの左にある文字を消去します。
Ctrl+D	カーソル位置にある文字を削除します。
Ctrl+K	カーソル位置からコマンドラインの末尾までのすべての文字を削除します。
Ctrl+U または Ctrl+X	カーソル位置からコマンドラインの先頭までのすべての文字を削除します。
Ctrl+W	カーソルの左にある単語を削除します。
Esc D	カーソルの位置から単語の末尾までを削除します。
Esc C	カーソル位置のワードを大文字にします。
Esc L	カーソルの場所にある単語を小文字にします。
Esc U	カーソルの位置から単語の末尾までを大文字にします。
Ctrl+V または Esc Q	特定のキーストロークを実行可能なコマンド（通常はショートカット）として指定します。
Return キー	1 行または 1 画面下へスクロールして、端末画面に収まりきらない表示内容を表示させます。 (注) show コマンドの出力など、端末画面に一度に表示できない長い出力では、 More プロンプトが使用されます。 More プロンプトが表示された場合は、 Return キーおよび Space キーを使用してスクロールできます。
Space バー	1 画面分下にスクロールします。
Ctrl+L または Ctrl+R	スイッチから画面に突然メッセージが出力された場合に、現在のコマンドラインを再表示します。

画面幅よりも長いコマンドラインの編集

画面上で 1 行分を超える長いコマンドラインについては、コマンドのラップアラウンド機能を使用できます。カーソルが右マージンに達すると、そのコマンドラインは 10 文字分だけ左へシフトされます。コマンドラインの先頭から 10 文字までは見えなくなりますが、左へスクロールして、コマンドの先頭部分の構文をチェックできます。これらのキー操作は任意です。

コマンドの先頭にスクロールして入力内容をチェックするには、**Ctrl+B** キーまたは←キーを繰り返し押しします。コマンドラインの先頭に直接移動するには、**Ctrl+A** を押しします。



(注) 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

次に、画面上で 1 行分を超える長いコマンドラインを折り返す例を示します。

手順の概要

1. **access-list**
2. **Ctrl+A**
3. **Return** キー

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	access-list 例： <pre>Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 Switch(config)# \$ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25 Switch(config)# \$t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq Switch(config)# \$15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45</pre>	1 行分を超えるグローバル コンフィギュレーション コマンド 入力を表示します。 最初にカーソルが行末に達すると、その行は 10 文字分だけ左へシフトされ、再表示されます。ドル記号 (\$) は、その行が左へスクロールされたことを表します。カーソルが行末に達するたびに、その行は再び 10 文字分だけ左へシフトされます。
ステップ 2	Ctrl+A 例： <pre>Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2\$</pre>	完全な構文をチェックします。 行末に表示されるドル記号 (\$) は、その行が右へスクロールされたことを表します。
ステップ 3	Return キー	コマンドを実行します。

	コマンドまたはアクション	目的
		<p>ソフトウェアでは、端末画面は 80 カラム幅であると想定されています。画面の幅が異なる場合は、terminal width 特権 EXEC コマンドを使用して端末の幅を設定します。</p> <p>ラップアラウンド機能とコマンド履歴機能を併用すると、前に入力した複雑なコマンドエントリを呼び出して変更できます。</p>

show および more コマンド出力の検索およびフィルタリング

show および **more** コマンドの出力を検索およびフィルタリングできます。この機能は、大量の出力をソートする場合や、出力から不要な情報を除外する場合に役立ちます。これらのコマンドの使用は任意です。

手順の概要

1. `{show | more} command | {begin | include | exclude} regular-expression`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<p><code>{show more} command {begin include exclude} regular-expression</code></p> <p>例 :</p> <pre>Switch# show interfaces include protocol Vlan1 is up, line protocol is up Vlan10 is up, line protocol is down GigabitEthernet1/0/1 is up, line protocol is down GigabitEthernet1/0/2 is up, line protocol is up</pre>	<p>出力を検索およびフィルタリングします。</p> <p>文字列では、大文字と小文字が区別されます。たとえば、 exclude output と入力した場合、output を含む行は表示されませんが、Output を含む行は表示されます。</p>

コンソール接続または Telnet による CLI アクセス

CLIにアクセスするには、スイッチのハードウェア インストールガイドに記載されている手順で、スイッチのコンソールポートに端末またはPCを接続するか、またはPCをイーサネット管理ポートに接続して、スイッチの電源をオンにする必要があります。

スイッチがすでに設定されている場合は、ローカル コンソール接続またはリモート Telnet セッションによって CLI にアクセスできますが、このタイプのアクセスに対応できるように、先にスイッチを設定しておく必要があります。

次のいずれかの方法で、スイッチとの接続を確立できます。

- スイッチ コンソールポートに管理ステーションまたはダイヤルアップモデムを接続するか、またはイーサネット管理ポートに PC を接続します。コンソールポートまたはイーサネット管理ポートへの接続については、スイッチのハードウェア インストールガイドを参照してください。
- リモート管理ステーションから任意の Telnet TCP/IP または暗号化 Secure Shell (SSH; セキュアシェル) パッケージを使用します。スイッチは Telnet または SSH クライアントとのネットワーク接続が可能でなければなりません。また、スイッチにイネーブル シークレット パスワードを設定しておくことも必要です。
 - スイッチは同時に最大 16 の Telnet セッションをサポートします。1 人の Telnet ユーザによって行われた変更は、他のすべての Telnet セッションに反映されます。
 - スイッチは最大 5 つの安全な SSH セッションを同時にサポートします。

コンソールポート、イーサネット管理ポート、Telnet セッション、または SSH セッションを通じて接続すると、管理ステーション上にユーザ EXEC プロンプトが表示されます。



第 2 章

Cisco IOS Configuration Engine の設定

- 機能情報の確認, 15 ページ
- Configuration Engine を設定するための前提条件, 15 ページ
- Configuration Engine の設定に関する制約事項, 16 ページ
- Configuration Engine の設定について, 16 ページ
- Configuration Engine の設定方法, 23 ページ
- CNS 設定のモニタリング, 35 ページ
- その他の関連資料, 36 ページ
- Configuration Engine の機能の履歴と情報, 37 ページ

機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

Configuration Engine を設定するための前提条件

- ユーザが接続している設定エンジン インスタンスの名前を取得します。
- CNS は、イベント バスとコンフィギュレーション サーバの両方を使用してデバイスに設定を提供するので、設定済みのスイッチごとに ConfigID と DeviceID の両方を定義する必要があります。

- **cns config partial** 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されたすべてのスイッチは、イベントバスにアクセスする必要があります。スイッチを起源とする DeviceID は、Cisco Configuration Engine 内の対応するスイッチ定義の DeviceID と一致する必要があります。ユーザが接続しているイベントバスのホスト名を把握する必要があります。

関連トピック

- [Cisco Networking Service ID およびデバイスのホスト名, \(18 ページ\)](#)
- [DeviceID, \(19 ページ\)](#)

Configuration Engine の設定に関する制約事項

- コンフィギュレーションサーバの1つのインスタンスでは、設定済みの2つのスイッチが同じ ConfigID 値を共有できません。
- イベントバスの1つのインスタンスでは、設定済みの2つのスイッチが同じ DeviceID 値を共有できません。

関連トピック

- [Cisco Networking Service ID およびデバイスのホスト名, \(18 ページ\)](#)

Configuration Engine の設定について

Cisco Configuration Engine ソフトウェア

Cisco Configuration Engine は、ネットワーク管理ユーティリティソフトウェアで、ネットワークデバイスおよびサービスの配置と管理を自動化するためのコンフィギュレーションサービスとして機能します。各 Cisco Configuration Engine は、シスコデバイス（スイッチとルータ）のグループとデバイスが提供するサービスを管理し設定を保存して、必要に応じて配信します。Cisco Configuration Engine は、デバイス固有のコンフィギュレーション変更を生成してデバイスに送信し、コンフィギュレーション変更を実行して結果をログに記録することにより、初期設定とコンフィギュレーションの更新を自動化します。

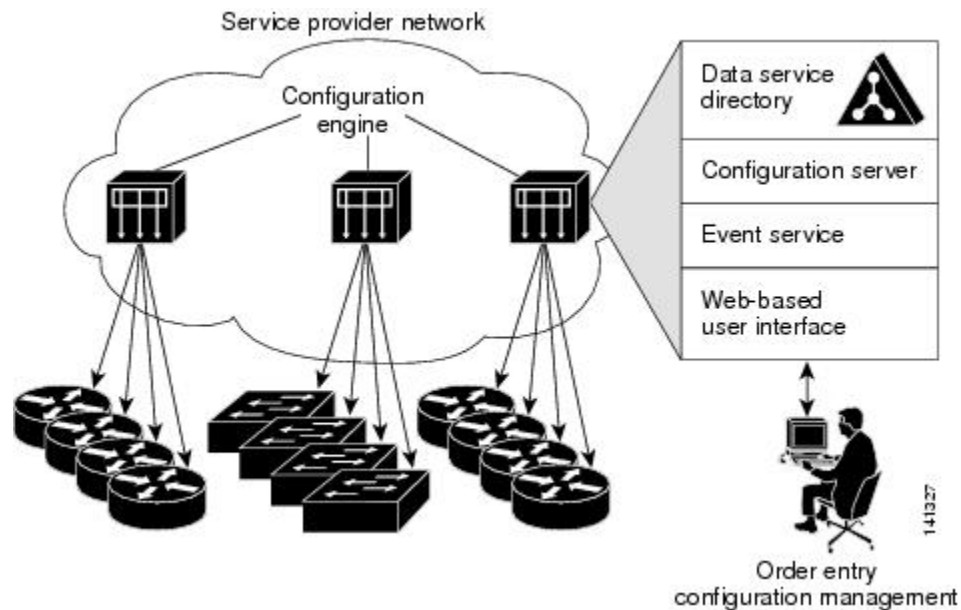
Cisco Configuration Engine は、スタンドアロンモードとサーバモードをサポートし、次の Cisco Networking Service (CNS) コンポーネントがあります。

- コンフィギュレーション サービス
 - Web サーバ
 - ファイル マネージャ
 - ネームスペース マッピング サーバ
- イベント サービス (イベント ゲートウェイ)

- データ サービス ディレクトリ (データ モデルおよびスキーマ)

スタンドアロンモードでは、Cisco Configuration Engine は組み込み型ディレクトリ サービスをサポートします。このモードでは、外部ディレクトリまたはその他のデータストアは必要ありません。サーバモードでは、ユーザが定義した外部ディレクトリの使用がサポートされます。

図 1 : Cisco Configuration Engine のアーキテクチャの概要



コンフィギュレーションサービス

コンフィギュレーション サービスは、Cisco Configuration Engine の中核コンポーネントです。スイッチ上にある Cisco IOS CNS エージェントと連携して動作するコンフィギュレーションサーバで構成されています。コンフィギュレーションサービスは、初期設定と論理グループによる大規模な再設定のために、デバイスとサービスの設定をスイッチに配信します。スイッチはネットワーク上で初めて起動するときに、コンフィギュレーション サービスから初期設定を受信します。

コンフィギュレーション サービスは CNS イベント サービスを使用して設定変更イベントを送受信し、成功および失敗の通知を送信します。

コンフィギュレーション サーバは Web サーバであり、コンフィギュレーション テンプレートと組み込み型ディレクトリ (スタンドアロン モード) またはリモート ディレクトリ (サーバモード) に保存されているデバイス固有の設定情報を使用します。

コンフィギュレーション テンプレートは、CLI (コマンドライン インターフェイス) コマンド形式で静的な設定情報を含んだテキスト ファイルです。テンプレートでは、変数は、Lightweight Directory Access Protocol (LDAP) URL を使用して指定します。この URL はディレクトリに保存されているデバイス固有の設定情報を参照します。

Cisco IOS エージェントは受信したコンフィギュレーションファイルの構文をチェックし、イベントを発行して構文チェックが成功または失敗したかを表示します。コンフィギュレーションエージェントは設定をただちに適用することも、あるいは同期化イベントをコンフィギュレーションサーバから受信するまで適用を遅らせることもできます。

イベント サービス

Cisco Configuration Engine は、設定イベントの受信および生成にイベントサービスを使用します。イベントサービスはイベント エージェント、イベント ゲートウェイから構成されます。イベント エージェントはスイッチ上にあり、スイッチと Cisco Configuration Engine のイベント ゲートウェイ間の通信を容易にします。

イベント サービスは、非常に有効なパブリッシュ サブスクライブ通信方式です。イベント サービスは、サブジェクトベースのアドレス指定を使用して、メッセージを宛先に送信します。サブジェクトベースのアドレス表記法では、メッセージおよび宛先には簡単に均一なネームスペースを定義します。

関連トピック

[CNS イベント エージェントのイネーブル化](#), (23 ページ)

NSM

Cisco Configuration Engine はネームスペース マッパー (NSM) を備えています。これは、アプリケーション、デバイスまたはグループ ID、およびイベントに基づいてデバイスの論理グループを管理するための検索サービスを提供します。

Cisco IOS デバイスは、たとえば `cisco.cns.config.load` といった、Cisco IOS ソフトウェアで設定されたサブジェクト名と一致するイベント サブジェクト名のみを認識します。ネームスペース マッピングサービスを使用すると、希望する命名規則を使用することでイベントを指定できます。サブジェクト名でデータストアにデータを入力した場合、NSM はイベント サブジェクト名ストリングを、Cisco IOS が認識するものに変更します。

サブスクライバの場合、一意のデバイス ID とイベントが指定されると、ネームスペース マッピングサービスは、サブスクライブ対象のイベントセットを返します。同様にパブリッシャの場合、一意のグループ ID、デバイス ID、およびイベントが指定されると、マッピングサービスは、パブリッシュ対象のイベントセットを返します。

Cisco Networking Service ID およびデバイスのホスト名

Cisco Configuration Engine は、設定対象の各スイッチに一意の識別子が関連付けられていることを前提としています。一意の識別子は複数の同義語を持つことができますが、各同義語は特定のネームスペース内で一意です。イベントサービスは、ネームスペースの内容を使用してメッセージのサブジェクトベース アドレス指定を行います。

Cisco Configuration Engine は、イベントバス用とコンフィギュレーションサーバ用の2つの名前空間を交差します。コンフィギュレーションサーバのネームスペースでは、*ConfigID* という用語がデバイスの一意な識別子です。イベントバスのネームスペースでは、*DeviceID* という用語がデバイスの CNS 一意識別子です。

関連トピック

[Configuration Engine を設定するための前提条件](#), (15 ページ)

[Configuration Engine の設定に関する制約事項](#), (16 ページ)

ConfigID

設定対象のスイッチはそれぞれ固有の ConfigID を持ちます。これは Cisco Configuration Engine ディレクトリからスイッチ CLI 属性の対応するセットを取得するためのキーとなります。スイッチで定義された ConfigID は、Cisco Configuration Engine 上の対応するスイッチ定義の ConfigID と一致する必要があります。

ConfigID は起動時に固定され、スイッチホスト名を再設定した場合でもデバイスを再起動するまで変更できません。

DeviceID

イベントバスに参加している設定済みのスイッチごとに一意の DeviceID があります。これはスイッチの送信元アドレスに似ているので、スイッチをバス上の特定の宛先として指定できます。

DeviceID の発信元は、スイッチの Cisco IOS ホスト名によって定義されます。ただし、DeviceID 変数およびその使用は、スイッチに隣接するイベントゲートウェイ内にあります。

イベントバス上の Cisco IOS の論理上の終点は、イベントゲートウェイに組み込まれ、それがスイッチの代わりにプロキシとして動作します。イベントゲートウェイはイベントバスに対して、スイッチおよび対応する DeviceID を表示します。

スイッチは、イベントゲートウェイとの接続が成功するとすぐに、そのホスト名をイベントゲートウェイに宣言します。接続が確立されるたびに、イベントゲートウェイは DeviceID 値を Cisco IOS ホスト名に組み合わせます。イベントゲートウェイは、スイッチと接続している間、この DeviceID 値を保持します。

関連トピック

[Configuration Engine を設定するための前提条件](#), (15 ページ)

ホスト名および DeviceID

DeviceID は、イベントゲートウェイと接続したときに固定され、スイッチホスト名を再設定した場合でも変更されません。

スイッチでスイッチホスト名を変更するとき、DeviceID を更新する唯一の方法は、スイッチとイベントゲートウェイ間の接続を切断することです。DeviceID 更新の手順については、以下の「関連項目」を参照してください。

接続が再確立されると、スイッチは変更したホスト名をイベントゲートウェイに送信します。イベントゲートウェイは DeviceID を新しい値に再定義します。



注意

Cisco Configuration Engine ユーザインターフェイスを使用するときは、最初に DeviceID フィールドを、スイッチが前ではなく後に取得するホスト名値に設定する必要があります。Cisco IOS CNS エージェント用に設定を再初期化する必要があります。そのようにしないと、後続の部分的なコンフィギュレーション コマンド操作で誤動作が発生する可能性があります。

関連トピック

[DeviceID の更新](#), (32 ページ)

ホスト名、DeviceID、および ConfigID

スタンドアロンモードでは、ホスト名の値をスイッチに設定すると、コンフィギュレーションサーバはイベントをホスト名に送信する場合、そのホスト名を DeviceID として使用します。ホスト名が設定されていない場合、イベントはデバイスの `cn=<value>` で送信されます。

サーバモードでは、ホスト名は使用されません。このモードでは、バス上のイベント送信には常に一意の DeviceID 属性が使用されます。この属性が設定されていない場合、スイッチを更新できません。

Cisco Configuration Engine で **Setup** を実行する場合、これらの属性および関連する属性（タグ値のペア）を設定します。

Cisco IOS CNS エージェント

CNS イベントエージェント機能によって、スイッチはイベントバス上でイベントにパブリッシュおよびサブスクライブを行い、Cisco IOS CNS エージェントと連携できます。スイッチ Cisco IOS ソフトウェアに組み込まれているこれらのエージェントでは、スイッチを接続して、自動的に設定できます。

初期設定

スイッチが最初に起動すると、ネットワークで Dynamic Host Configuration Protocol (DHCP) 要求をブロードキャストすることで IP アドレスを取得しようとします。サブネット上には DHCP サーバがないものと想定し、ディストリビューションスイッチは DHCP リレーエージェントとして動作し、要求を DHCP サーバに転送します。DHCP サーバは要求を受信すると、新しいスイッチに IP アドレスを割り当て、Trivial File Transfer Protocol (TFTP) サーバのインターネットプロトコル (IP) アドレス、ブートストラップコンフィギュレーションファイルへのパス、デフォルトゲートウェイの IP アドレスを、DHCP リレーエージェントに対するユニキャスト応答に組み入れます。DHCP リレーエージェントは、この応答をスイッチに転送します。

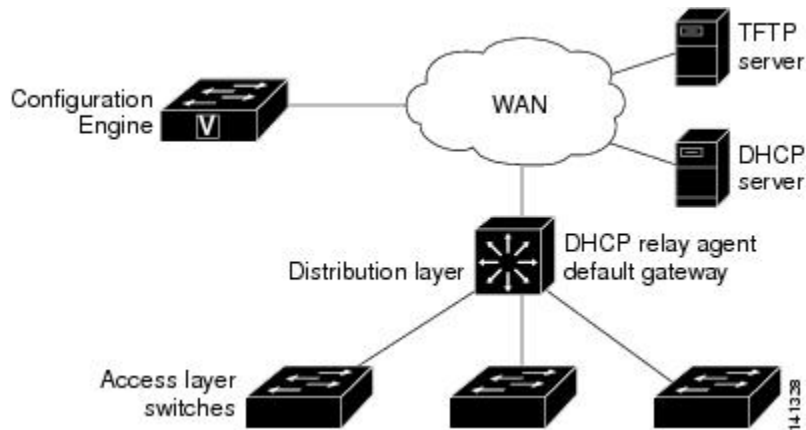
スイッチは、割り当てられた IP アドレスを自動的にインターフェイス VLAN 1 (デフォルト) に設定し、TFTP サーバからブートストラップコンフィギュレーションファイルをダウンロードし

まず、ブートストラップ コンフィギュレーション ファイルが正常にダウンロードされると、スイッチはそのファイルを実行コンフィギュレーションにロードします。

Cisco IOS CNS エージェントは、該当する ConfigID および EventID を使用して Configuration Engine との通信を開始します。Configuration Engine はこの ConfigID をテンプレートにマッピングして、スイッチに完全なコンフィギュレーション ファイルをダウンロードします。

次の図に、DHCP ベースの自動設定を使用して初期ブートストラップ コンフィギュレーション ファイルを取得するためのネットワーク構成例を示します。

図 2: 初期設定



関連トピック

[自動 CNS 設定, \(22 ページ\)](#)

差分（部分的）設定

ネットワークが稼働すると、Cisco IOS CNS エージェントを使用して新しいサービスを追加できます。差分（部分）設定は、スイッチに送信できます。実際の設定を、イベントペイロードとしてイベントゲートウェイを介して（プッシュ処理）送信するか、スイッチにプルオペレーションを開始させる信号イベントとして送信できます。

スイッチは、適用する前に設定の構文をチェックできます。構文が正しい場合は、スイッチは差分設定を適用し、コンフィギュレーションサーバに成功を信号で伝えるイベントを発行します。スイッチが差分設定を適用しない場合、エラーステータスを示すイベントを発行します。スイッチが差分設定を適用した場合、不揮発性 RAM (NVRAM) に書き込むか、または書き込むように指示されるまで待つことができます。

コンフィギュレーションの同期

スイッチは、設定を受信した場合、書き込み信号イベントの受信時に設定の適用を遅らせることができます。書き込み信号イベントは、更新された設定を NVRAM に保存しないようにスイッチに指示します。スイッチは更新された設定を実行コンフィギュレーションとして使用します。こ

れによりスイッチの設定は、次のリブート時の使用のために NVRAM に設定を保存する前に、他のネットワーク アクティビティと同期化されます。

自動 CNS 設定

スイッチの自動 CNS 設定をイネーブルにするには、まずこのトピックに示す前提条件を完了する必要があります。条件設定を完了したらスイッチの電源を入れます。 **setup** プロンプトでは何も入力しません。スイッチが初期設定を開始します。コンフィギュレーションファイル全体がスイッチにロードされると作業は完了です。

初期設定中の動作については、「関連項目」を参照してください。

表 4: 自動設定イネーブル化の条件

デバイス	必要な設定
アクセス スイッチ	出荷時の設定 (コンフィギュレーションファイルなし)
ディストリビューション スイッチ	<ul style="list-style-type: none"> • IP ヘルパー アドレス • DHCP リレー エージェントのイネーブル化¹ • IP ルーティング (デフォルト ゲートウェイとして使用する場合)
DHCP サーバ	<ul style="list-style-type: none"> • IP アドレスの割り当て • TFTP サーバの IP アドレス • TFTP サーバのブートストラップ コンフィギュレーション ファイルへのパス • デフォルト ゲートウェイの IP アドレス

デバイス	必要な設定
TFTP サーバ	<ul style="list-style-type: none"> • スイッチと Configuration Engine との通信を可能にする CNS コンフィギュレーション コマンドを含むブートストラップ コンフィギュレーション ファイル • (デフォルトのホスト名の代わりに) スイッチ MAC アドレスまたはシリアル番号のいずれかを使用して ConfigID および EventID を生成するように設定されたスイッチ • スイッチにコンフィギュレーション ファイルをプッシュするように設定された CNS イベント エージェント
CNS Configuration Engine	デバイス タイプ別の 1 つまたは複数のテンプレートで、テンプレートにデバイスの ConfigID がマッピングされています。

¹ DHCP リレーは、DHCP サーバがクライアントとは異なるサブネット上にある場合にのみ必要です。

関連トピック

[初期設定, \(20 ページ\)](#)

Configuration Engine の設定方法

CNS イベント エージェントのイネーブル化



(注) スイッチ上で CNS イベント エージェントをイネーブルにしてから、CNS 設定エージェントをイネーブルにする必要があります。

スイッチ上で CNS イベント エージェントをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **cns event {hostname | ip-address} [port-number] [[keepalive seconds retry-count] [failover-time seconds] [reconnect-time time] | backup]**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	cns event {hostname ip-address} [port-number] [[keepalive seconds retry-count] [failover-time seconds] [reconnect-time time] backup] 例 : Switch(config)# cns event 10.180.1.27 keepalive 120 10	イベントエージェントをイネーブルにして、ゲートウェイパラメータを入力します。 <ul style="list-style-type: none"> • {hostname ip-address} に、イベントゲートウェイのホスト名または IP アドレスを入力します。 • (任意) port number に、イベントゲートウェイのポート番号を入力します。デフォルトのポート番号は 11011 です。 • (任意) keepalive seconds に、スイッチがキープアライブメッセージを送信する間隔を入力します。retry-count に、キープアライブメッセージへの応答がない場合に接続を終了するまでのスイッチのメッセージ送信回数を入力します。デフォルト値はいずれも 0 です。 • (任意) failover-time seconds に、バックアップゲートウェイが確立された後にスイッチがプライマリゲートウェイルートを待つ時間を入力します。 • (任意) reconnect-time time に、スイッチがイベントゲートウェイに再接続しようとする前の最大時間間隔を入力します。 • (任意) バックアップゲートウェイであることを示す場合は、backup を入力します (省略した場合は、プライマリゲートウェイになります)。 (注) encrypt キーワードおよび clock-timeout time キーワードは、コマンドラインのヘルプストリングに表示されますが、サポートされていません。

	コマンドまたはアクション	目的
ステップ 3	end 例 : Switch(config)# end	特権 EXEC モードに戻ります。

次に、CNS イベントエージェントをイネーブルにして、IP アドレスゲートウェイを 10.180.1.27、キープアライブ間隔を 120 秒、再試行回数を 10 回に設定する例を示します。

```
Switch(config)# cns event 10.180.1.27 keepalive 120 10
```

次の作業

イベント エージェントに関する情報を確認するには、**show cns event connections** コマンドを特権 EXEC モードで使用します。

CNS イベント エージェントをディセーブルにするには、**no cns event { ip-address | hostname }** グローバル コンフィギュレーション コマンドを使用します。

関連トピック

[イベント サービス, \(18 ページ\)](#)

Cisco IOS CNS エージェントのイネーブル化

スイッチで Cisco IOS CNS エージェントをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

はじめる前に

このエージェントをイネーブルにする前に、スイッチで CNS イベントエージェントをイネーブルにする必要があります。

手順の概要

1. **configure terminal**
2. **cns config initial {hostname | ip-address} [port-number]**
3. **cns config partial {hostname | ip-address} [port-number]**
4. **end**
5. Cisco IOS CNS エージェントを、スイッチで開始します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	cns config initial {hostname ip-address} [port-number] 例： Switch(config)# cns config initial 10.180.1.27 10	Cisco IOS CNS エージェントをイネーブルにし、コンフィギュレーション サーバ パラメータを入力します。 <ul style="list-style-type: none"> • {hostname ip-address} に、コンフィギュレーション サーバのホスト名または IP アドレスを入力します。 • (任意) port number に、コンフィギュレーション サーバのポート番号を入力します。 <p>このコマンドが Cisco IOS CNS エージェントをイネーブルにして、スイッチで初期設定を開始します。</p>
ステップ 3	cns config partial {hostname ip-address} [port-number] 例： Switch(config)# cns config partial 10.180.1.27 10	Cisco IOS CNS エージェントをイネーブルにし、コンフィギュレーション サーバ パラメータを入力します。 <ul style="list-style-type: none"> • {hostname ip-address} に、コンフィギュレーション サーバのホスト名または IP アドレスを入力します。 • (任意) port number に、コンフィギュレーション サーバのポート番号を入力します。 <p>Cisco IOS CNS エージェントをイネーブルにして、スイッチで部分的設定を開始します。</p>
ステップ 4	end 例： Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 5	Cisco IOS CNS エージェントを、スイッチで開始します。	

次の作業

リモートで差分設定をスイッチに送信するために、Cisco Configuration Engine を使用できるようになりました。

関連トピック

[DeviceID の更新, \(32 ページ\)](#)

Cisco IOS CNS エージェントの初期設定のイネーブル化

スイッチ上で CNS 設定エージェントをイネーブルにして初期設定を開始するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **cns template connect name**
3. **cli config-text**
4. 別の CNS 接続テンプレートを設定する場合は、ステップ 2 ~ 3 を繰り返します。
5. **exit**
6. **cns connect name [retries number] [retry-interval seconds] [sleep seconds] [timeout seconds]**
7. **discover {controller controller-type | dcli [subinterface subinterface-number] | interface [interface-type] | line line-type}**
8. **template name [... name]**
9. ステップ 7 ~ 8 を繰り返し、CNS 接続プロファイルにさらに多くのインターフェイスパラメータと CNS 接続テンプレートを指定します。
10. **exit**
11. **hostname name**
12. **ip route network-number**
13. **cns id interface num {dns-reverse | ipaddress | mac-address} [event] [image]**
14. **cns id {hardware-serial | hostname | string string | udi} [event] [image]**
15. **cns config initial {hostname | ip-address} [port-number] [event] [no-persist] [page page] [source ip-address] [syntax-check]**
16. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	<p>cns template connect name</p> <p>例 :</p> <pre>Switch(config)# cns template connect template-dhcp</pre>	CNS テンプレート接続コンフィギュレーションモードを開始して、CNS 接続テンプレートの名前を指定します。
ステップ 3	<p>cli config-text</p> <p>例 :</p> <pre>Switch(config-tmpl-conn)# cli ip address dhcp</pre>	CNS 接続テンプレートにコマンドラインを入力します。テンプレート内の各コマンドラインにこの手順を繰り返します。
ステップ 4	別の CNS 接続テンプレートを設定する場合は、ステップ 2～3 を繰り返します。	
ステップ 5	<p>exit</p> <p>例 :</p> <pre>Switch(config)# exit</pre>	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	<p>cns connect name [retries number] [retry-interval seconds] [sleep seconds] [timeout seconds]</p> <p>例 :</p> <pre>Switch(config)# cns connect dhcp</pre>	<p>CNS 接続コンフィギュレーションモードを開始し、CNS 接続プロファイルの名前を指定し、プロファイルパラメータを定義します。スイッチは CNS 接続プロファイルを使用して Configuration Engine に接続します。</p> <ul style="list-style-type: none"> • CNS 接続プロファイルの <i>name</i> を入力します。 • (任意) retries number に、接続のリトライ回数を入力します。指定できる範囲は 1～30 です。デフォルト値は 3 です。 • (任意) retry-interval seconds に、Configuration Engine への連続する接続の試行間隔を入力します。指定できる範囲は 1～40 秒です。デフォルトは 10 秒です。 • (任意) sleep seconds に、最初の接続試行を実行するまで待機する時間を入力します。指定できる範囲は 0～250 秒です。デフォルト値は 0 です。 • (任意) timeout seconds に、接続が終了しようとした後に待機する時間を入力します。指定できる範囲は 10～2000 秒です。デフォルト値は 120 です。
ステップ 7	<p>discover {controller controller-type dlci [subinterface subinterface-number] interface [interface-type] line line-type}</p>	<p>CNS 接続プロファイル内のインターフェイスパラメータを入力します。</p> <ul style="list-style-type: none"> • controller controller-type に、コントローラタイプを入力します。

	コマンドまたはアクション	目的
	例 : <pre>Switch(config-cns-conn)# discover interface gigabitethernet</pre>	<ul style="list-style-type: none"> • dcli に、アクティブなデータリンク接続識別子 (DLCI) を入力します。 (任意) subinterface subinterface-number に、アクティブな DLCI の検索に使用するポイントツーポイントサブインターフェイス番号を指定します。 • interface [interface-type] に、インターフェイスのタイプを入力します。 • line line-type に、回線タイプを入力します。
ステップ 8	template name [... name] 例 : <pre>Switch(config-cns-conn)# template template-dhcp</pre>	スイッチの設定に適用する CNS 接続プロファイル内の CNS 接続テンプレートのリストを指定します。複数のテンプレートを指定できます。
ステップ 9	ステップ 7～8 を繰り返し、CNS 接続プロファイルにさらに多くのインターフェイスパラメータと CNS 接続テンプレートを指定します。	
ステップ 10	exit 例 : <pre>Switch(config-cns-conn)# exit</pre>	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	hostname name 例 : <pre>Switch(config)# hostname device1</pre>	スイッチのホスト名を入力します。
ステップ 12	ip route network-number 例 : <pre>RemoteSwitch(config)# ip route 172.28.129.22 255.255.255.255 11.11.11.1</pre>	(任意) IP アドレスが <i>network-number</i> の Configuration Engine へのスタティック ルートを確立します。
ステップ 13	cns id interface num {dns-reverse ipaddress mac-address} [event] [image]	(任意) Configuration Engine が使用する一意の EventID または ConfigID を設定します。このコマンドを入力する場合は、 cns id {hardware-serial hostname string string udi} [event] [image] コマンドを入力しないでください。

	コマンドまたはアクション	目的
	<p>例 :</p> <pre>RemoteSwitch(config)# cns id GigabitEthernet1/0/1 ipaddress</pre>	<ul style="list-style-type: none"> • <i>interface num</i> に、インターフェイスのタイプを入力します。たとえば、<code>ethernet</code>、<code>group-async</code>、<code>loopback</code>、<code>virtual-template</code> を入力します。この設定では、一意の ID を定義するためにどのインターフェイスから IP アドレスまたは MAC アドレスを取得するかを指定します。 • <code>{dns-reverse ipaddress mac-address}</code> では、ホスト名を取得してそのホスト名を一意の ID として割り当てるには <code>dns-reverse</code> を入力し、IP アドレスを使用するには <code>ipaddress</code> を入力し、MAC アドレスを一意の ID として使用するには <code>mac-address</code> を入力します。 • (任意) ID をスイッチの識別に使用する <code>event-id</code> 値になるように設定するには、<code>event</code> を入力します。 • (任意) ID をスイッチの識別に使用する <code>image-id</code> 値になるように設定するには、<code>image</code> を入力します。 <p>(注) <code>event</code> と <code>image</code> キーワードの両方を省略した場合は、スイッチの識別には <code>image-id</code> 値が使用されます。</p>
ステップ 14	<p><code>cns id {hardware-serial hostname string string udi} [event] [image]</code></p> <p>例 :</p> <pre>RemoteSwitch(config)# cns id hostname</pre>	<p>(任意) Configuration Engine が使用する一意の EventID または ConfigID を設定します。このコマンドを入力する場合は、<code>cns id interface num {dns-reverse ipaddress mac-address} [event] [image]</code> コマンドを入力しないでください。</p> <ul style="list-style-type: none"> • <code>{ hardware-serial hostname string string udi }</code> で、<code>hardware-serial</code> を入力してスイッチのシリアル番号を一意の ID として設定するか、<code>hostname</code> (デフォルト) を入力してスイッチのホスト名を一意の ID として選択するか、<code>string string</code> に任意のテキストストリングを一意の ID として入力するか、または <code>udi</code> を入力して Unique Device Identifier (UDI) を一意の ID として設定します。
ステップ 15	<p><code>cns config initial {hostname ip-address} [port-number] [event] [no-persist] [page page] [source ip-address] [syntax-check]</code></p> <p>例 :</p> <pre>RemoteSwitch(config)# cns config initial 10.1.1.1 no-persist</pre>	<p>Cisco IOS エージェントをイネーブルにして、初期設定を開始します。</p> <ul style="list-style-type: none"> • <code>{hostname ip-address}</code> に、コンフィギュレーション サーバのホスト名または IP アドレスを入力します。 • (任意) <code>portnumber</code> に、コンフィギュレーションサーバのポート番号を入力します。デフォルトのポート番号は 80 です。 • (任意) 設定が完了したときの設定の成功、失敗、または警告のメッセージ用に <code>event</code> をイネーブルにします。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • (任意) cns config initial グローバル コンフィギュレーション コマンドの入力結果によってプルされた設定の NVRAM への自動書き込みを抑制するには、no-persist を入力します。 no-persist キーワードを入力しない場合、cns config initial コマンドを使用すると、その結果の設定が自動的に NVRAM に書き込まれます。 • (任意) page page に、初期設定の Web ページを入力します。デフォルトは /Config/config/asp です。 • (任意) 送信元 IP アドレスに使用するには、source ip-address を入力します。 • (任意) このパラメータを使用したときの構文をチェックするには、syntax-check をイネーブルにします。 <p>(注) コマンドラインのヘルプ スtring に表示されますが、encrypt、status url、inventory キーワードはサポートされていません。</p>
ステップ 16	end 例： RemoteSwitch(config)# end	特権 EXEC モードに戻ります。

次に、スイッチの設定が不明な場合に、リモート スイッチに初期設定を設定する例 (CNS ゼロ タッチ機能) を示します。

```
Switch(config)# cns template connect template-dhcp
Switch(config-tmpl-conn)# cli ip address dhcp
Switch(config-tmpl-conn)# exit
Switch(config)# cns template connect ip-route
Switch(config-tmpl-conn)# cli ip route 0.0.0.0 0.0.0.0 ${next-hop}
Switch(config-tmpl-conn)# exit
Switch(config)# cns connect dhcp
Switch(config-cns-conn)# discover interface gigabitethernet
Switch(config-cns-conn)# template template-dhcp
Switch(config-cns-conn)# template ip-route
Switch(config-cns-conn)# exit
Switch(config)# hostname RemoteSwitch
RemoteSwitch(config)# cns config initial 10.1.1.1 no-persist
```

次に、スイッチ IP アドレスが不明の場合に、リモート スイッチに初期設定を設定する例を示します。 Configuration Engine の IP アドレスは 172.28.129.22 です。

```
Switch(config)# cns template connect template-dhcp
Switch(config-tmpl-conn)# cli ip address dhcp
Switch(config-tmpl-conn)# exit
Switch(config)# cns template connect ip-route
Switch(config-tmpl-conn)# cli ip route 0.0.0.0 0.0.0.0 ${next-hop}
```

```
Switch(config-tmpl-conn)# exit
Switch(config)# cns connect dhcp
Switch(config-cns-conn)# discover interface gigabitethernet
Switch(config-cns-conn)# template template-dhcp
Switch(config-cns-conn)# template ip-route
Switch(config-cns-conn)# exit
Switch(config)# hostname RemoteSwitch
RemoteSwitch(config)# ip route 172.28.129.22 255.255.255.255 11.11.11.1
RemoteSwitch(config)# cns id ethernet 0 ipaddress
RemoteSwitch(config)# cns config initial 172.28.129.22 no-persist
```

次の作業

コンフィギュレーション エージェントに関する情報を確認するには、**show cns config connections** コマンドを特権 EXEC モードで使用します。

CNS Cisco IOS エージェントをディセーブルにするには、**no cns config initial { ip-address | hostname }** グローバル コンフィギュレーション コマンドを使用します。

DeviceID の更新

スイッチでホスト名を変更するときに、DeviceID を更新するには、特権 EXEC モードで、次の手順を実行します。

手順の概要

1. **show cns config connections**
2. CNS イベント エージェントがイベント ゲートウェイに正しく接続されていることを確認します。
3. **show cns event connections**
4. 手順3の出力に基づいて、次に示す現在接続されている接続に関する情報を記録します。この手順の以降のステップで IP アドレスとポート番号を使用します。
5. **configure terminal**
6. **no cns event ip-address port-number**
7. **cns event ip-address port-number**
8. **end**
9. **show cns event connections** からの出力を調べて、スイッチとイベント接続間の接続が再確立されていることを確認します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	show cns config connections 例 : Switch# show cns config connections	CNS イベント エージェントがゲートウェイに接続しているか、接続されているか、またはアクティブか、およびイベント エージェントに使用されているゲートウェイ、その IP アドレス、およびポート番号を表示します。

	コマンドまたはアクション	目的
ステップ 2	CNS イベントエージェントがイベントゲートウェイに正しく接続されていることを確認します。	次のように show cns config connections の出力を確認します。 <ul style="list-style-type: none"> • 接続がアクティブになっている。 • 接続で現在設定されているスイッチホスト名を使用している。 DeviceID はこれらの手順を使用して、新しいホスト名の設定に対応するように更新されます。
ステップ 3	show cns event connections 例： Switch# show cns event connections	スイッチのイベント接続情報を表示します。
ステップ 4	手順3の出力に基づいて、次に示す現在接続されている接続に関する情報を記録します。この手順の以降のステップで IP アドレスとポート番号を使用します。	
ステップ 5	configure terminal 例： Switch# configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 6	no cns event ip-address port-number 例： Switch(config)# no cns event 172.28.129.22 2012	このコマンドで、ステップ4で記録した IP アドレスとポート番号を指定します。 このコマンドで、スイッチとイベントゲートウェイ間の接続が解除されます。最初に接続を解除し、次にこの接続を再確立して、DeviceID を更新する必要があります。
ステップ 7	cns event ip-address port-number 例： Switch(config)# cns event 172.28.129.22 2012	このコマンドで、ステップ4で記録した IP アドレスとポート番号を指定します。 このコマンドで、スイッチとイベントゲートウェイ間の接続が再確立されます。
ステップ 8	end 例： Switch(config)# end	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	show cns event connections からの出力を調べて、スイッチとイベント接続間の接続が再確立されていることを確認します。	

関連トピック

[Cisco IOS CNS エージェントのイネーブル化, \(25 ページ\)](#)

[ホスト名および DeviceID, \(19 ページ\)](#)

Cisco IOS CNS エージェントの部分的設定のイネーブル化

スイッチ上で Cisco IOS CNS エージェントをイネーブルにして部分設定を開始するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **cns config partial** {*ip-address* | *hostname*} [*port-number*] [**source** *ip-address*]
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	cns config partial { <i>ip-address</i> <i>hostname</i> } [<i>port-number</i>] [source <i>ip-address</i>] 例： Switch(config)# cns config partial 172.28.129.22 2013	コンフィギュレーション エージェントをイネーブルにし、部分設定を開始します。 <ul style="list-style-type: none"> • {<i>ip-address</i> <i>hostname</i>} に、コンフィギュレーション サーバの IP アドレスまたはホスト名を入力します。 • (任意) <i>port number</i> に、コンフィギュレーション サーバのポート番号を入力します。デフォルトのポート番号は 80 です。 • (任意) 送信元 IP アドレスに使用するには、source ip-address を入力します。

	コマンドまたはアクション	目的
		(注) encrypt キーワードは、コマンドラインのヘルプストリングに表示されますが、サポートされていません。
ステップ 3	end 例 : Switch(config)# end	特権 EXEC モードに戻ります。

次の作業

コンフィギュレーションエージェントに関する情報を確認するには、**show cns config stats** または **show cns config outstanding** コマンドのいずれかを特権 EXEC モードで使用します。

Cisco IOS エージェントをディセーブルにするには、**no cns config partial** { ip-address | hostname } グローバルコンフィギュレーションコマンドを使用します。部分設定を取り消すには、**cns config cancel** グローバルコンフィギュレーションコマンドを使用します。

CNS 設定のモニタリング

表 5: **CNS show** コマンド

コマンド	目的
show cns config connections Switch# show cns config connections	CNS Cisco IOS CNS エージェントの接続のステータスを表示します。
show cns config outstanding Switch# show cns config outstanding	開始されたがまだ終了していない差分（部分）CNS 設定に関する情報を表示します。
show cns config stats Switch# show cns config stats	Cisco IOS CNS エージェントに関する統計情報を表示します。
show cns event connections Switch# show cns event connections	CNS イベントエージェントの接続のステータスを表示します。
show cns event gateway Switch# show cns event gateway	スイッチのイベントゲートウェイ情報を表示します。
show cns event stats Switch# show cns event stats	CNS イベントエージェントに関する統計情報を表示します。

コマンド	目的
show cns event subject Switch# <code>show cns event subject</code>	アプリケーションによってサブスクライブされたイベントエージェントのサブジェクト一覧を表示します。

その他の関連資料

関連資料

関連項目	マニュアルタイトル
Configuration Engine のセットアップ	『Cisco Configuration Engine Installation and Setup Guide, 1.5 for Linux』 http://www.cisco.com/en/US/docs/net_mgmt/configuration_engine/1.5/installation_linux/guide/setup_1.html

MIB

MIB	MIB のリンク
	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 を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<p>http://www.cisco.com/support</p>

Configuration Engine の機能の履歴と情報

リリース	変更内容
Cisco IOS 15.0(2)EX1	この機能が導入されました。



第 3 章

Cisco Discovery Protocol の設定

- 機能情報の確認, 39 ページ
- CDP の概要, 39 ページ
- CDP の設定方法, 41 ページ
- CDP のモニタおよびメンテナンス, 47 ページ
- その他の関連資料, 48 ページ
- Cisco Discovery Protocol の機能の履歴と情報, 49 ページ

機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

CDP の概要

CDP の概要

CDP はすべてのシスコデバイス（ルータ、ブリッジ、アクセスサーバ、コントローラ、およびスイッチ）のレイヤ 2（データリンク層）で動作するデバイス検出プロトコルです。ネットワーク管理アプリケーションは CDP を使用することにより、既知のデバイスにネイバー シスコデバイスを検出できます。また、下位レイヤのトランスペアレントプロトコルが稼働しているネイバーデバイスのデバイス タイプや、簡易ネットワーク管理プロトコル（SNMP）エージェント アドレ

スを学習することもできます。この機能によって、アプリケーションからネイバー デバイスに SNMP クエリーを送信できます。

CDP は、サブネットワーク アクセス プロトコル (SNAP) をサポートしているすべてのメディアで動作します。CDP はデータリンク層でのみ動作するため、異なるネットワーク層プロトコルをサポートする 2 つのシステムで互いの情報を学習できます。

CDP が設定された各デバイスはマルチキャストアドレスに定期的にメッセージを送信して、SNMP メッセージを受信可能なアドレスを 1 つまたは複数アドバタイズします。このアドバタイズには、受信側デバイスで CDP 情報を廃棄せずに保持する時間を表す存続可能時間、つまりホールドタイム情報も含まれます。各デバイスは他のデバイスから送信されたメッセージも待ち受けて、ネイバー デバイスについて学習します。

CDP はスイッチ上で Network Assistant をイネーブルにすることで、ネットワークをグラフィカルに表示できます。スイッチは CDP を使用してクラスタ候補を検出し、クラスタ メンバ、およびコマンドスイッチから最大 3 台 (デフォルト) 離れたクラスタ対応の他のデバイスについての情報を維持します。

CDP およびスタック

スイッチスタックは、ネットワーク内の 1 つのスイッチとして表示されます。したがって、CDP は、個々のスタック メンバではなく、スイッチスタックを検出します。スタック メンバの追加または削除など、スイッチスタックメンバーシップに変更があった場合、スイッチスタックにより、ネイバー ネットワーク デバイスに CDP メッセージが送信されます。

CDP のデフォルト設定

この表は、CDP のデフォルト設定を示します。

機能	デフォルト設定
CDP グローバル ステート	イネーブル
CDP インターフェイス ステート	イネーブル
CDP タイマー (パケット更新頻度)	60 秒
CDP ホールドタイム (廃棄までの時間)	180 秒
CDP バージョン 2 アドバタイズ	イネーブル

CDP の設定方法

CDP 特性の設定

次の CDP 特性を設定できます。

- CDP 更新の頻度
- 破棄するまで情報を保持する時間の長さ
- バージョン 2 アドバタイズを送信するかどうか



(注) ステップ 2～4 はすべて任意であり、どの順番で実行してもかまいません。

これらの特性を設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **cdp timer seconds**
3. **cdp holdtime seconds**
4. **cdp advertise-v2**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 2	cdp timer seconds 例： Switch(config)# cdp timer 20	(任意) CDP 更新の送信頻度を秒単位で設定します。 指定できる範囲は 5～254 です。デフォルトは 60 秒です。
ステップ 3	cdp holdtime seconds 例： Switch(config)# cdp holdtime 60	(任意) 受信デバイスがこのデバイスから送信された情報を破棄せずに保持する時間を指定します。 指定できる範囲は 10～255 秒です。デフォルトは 180 秒です。

	コマンドまたはアクション	目的
ステップ 4	cdp advertise-v2 例： Switch(config)# cdp advertise-v2	(任意) バージョン2アドバタイズを送信するように CDP を設定します。 これは、デフォルトの状態です。
ステップ 5	end 例： Switch(config)# end	特権 EXEC モードに戻ります。

例

次に、CDP の特性を設定する例を示します。

```
Switch# configure terminal
Switch(config)# cdp timer 50
Switch(config)# cdp holdtime 120
Switch(config)# cdp advertise-v2
Switch(config)# end
```

次の作業

デフォルト設定に戻すには、CDP コマンドの **no** 形式を使用します。

関連トピック

[CDP のモニタおよびメンテナンス, \(47 ページ\)](#)

CDP のディセーブル化

CDP はデフォルトで有効になっています。



(注) スイッチクラスタと他のシスコデバイス (Cisco IP Phone など) は、CDP メッセージを定期的に交換します。CDP をディセーブルにすると、クラスタ検出が中断され、デバイスの接続が切断されます。

CDP デバイス検出機能をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **no cdp run**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no cdp run 例： Switch(config)# no cdp run	CDP をディセーブルにします。
ステップ 3	end 例： Switch(config)# end	特権 EXEC モードに戻ります。

次の作業

CDP を使用するには、再びイネーブルにする必要があります。

関連トピック

[CDP のイネーブル化, \(43 ページ\)](#)

CDP のイネーブル化

CDP はデフォルトで有効になっています。



- (注) スイッチ クラスタと他のシスコ デバイス (Cisco IP Phone など) は、CDP メッセージを定期的に交換します。CDP をディセーブルにすると、クラスタ検出が中断され、デバイスの接続が切断されます。

ディセーブル化されている CDP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

はじめる前に

CDP をディセーブルにする必要があります。そのようにしないとイネーブルにできません。

手順の概要

1. **configure terminal**
2. **cdp run**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	cdp run 例： Switch(config)# cdp run	ディセーブルにされている場合は、CDP をイネーブルにします。
ステップ 3	end 例： Switch(config)# end	特権 EXEC モードに戻ります。

例

次の例は、ディセーブルにされている場合の CDP をイネーブルにする方法を示しています。

```
Switch# configure terminal
Switch(config)# cdp run
Switch(config)# end
```

次の作業

CDP がイネーブルになっていることを示すには、**show run all** コマンドを使用します。 **show run** だけを入力した場合、CDP のイネーブル化が表示されないことがあります。

関連トピック

[CDP のディセーブル化, \(42 ページ\)](#)

インターフェイス上での CDP のディセーブル化

CDP 情報を送受信するために、サポートされているすべてのインターフェイス上では CDP がデフォルトでイネーブルになっています。



(注) スイッチクラスタと他のシスコデバイス（Cisco IP Phone など）は、CDP メッセージを定期的に交換します。CDP をディセーブルにすると、クラスタ検出が中断され、デバイスの接続が切断されます。

ポート上で CDP をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface *interface-id***
3. **no cdp enable**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface <i>interface-id</i> 例： Switch(config)# interface gigabitethernet1/0/1	CDP をディセーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	no cdp enable 例： Switch(config-if)# no cdp enable	ステップ 2 で指定したインターフェイスで CDP をディセーブルにします。
ステップ 4	end 例： Switch(config-if)# end	特権 EXEC モードに戻ります。

関連トピック

[インターフェイス上での CDP のイネーブル化](#)、（46 ページ）

インターフェイス上での CDP のイネーブル化

CDP 情報を送受信するために、サポートされているすべてのインターフェイス上では CDP がデフォルトでイネーブルになっています。



(注) スイッチクラスタと他のシスコデバイス（Cisco IP Phone など）は、CDP メッセージを定期的に交換します。CDP をディセーブルにすると、クラスタ検出が中断され、デバイスの接続が切断されます。

CDP がディセーブルにされているポート上で CDP をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

はじめる前に

CDP をイネーブルにしようとしているポートで、CDP をディセーブルになっている必要があります。そうでない場合は、イネーブルにできません。

手順の概要

1. **configure terminal**
2. **interface interface-id**
3. **cdp enable**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id 例： Switch(config)# interface gigabitethernet1/0/1	CDP をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	cdp enable 例： Switch(config-if)# cdp enable	ディセーブルにされているインターフェイスで CDP をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	end 例： Switch(config-if)# end	特権 EXEC モードに戻ります。

例

次の例は、ディセーブルにされているポートで CDP をイネーブルにする方法を示しています。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# cdp enable
Switch(config-if)# end
```

関連トピック

[インターフェイス上での CDP のディセーブル化, \(44 ページ\)](#)

CDP のモニタおよびメンテナンス

表 6: CDP 情報を表示するためのコマンド

コマンド	説明
clear cdp counters	トラフィック カウンタを 0 にリセットします。
clear cdp table	ネイバー デバイスに関する情報を収めた CDP テーブルを削除します。
show cdp	送信間隔、送信したパケットの保持時間などのグローバル情報を表示します。
show cdp entry entry-name [version] [protocol]	<p>特定のネイバーに関する情報を表示します。</p> <p>アスタリスク (*) を入力してすべての CDP ネイバーを表示することも、情報が必要なネイバーの名前を入力することもできます。</p> <p>また、指定されたネイバー上でイネーブルになっているプロトコルの情報や、デバイス上で稼働しているソフトウェアのバージョン情報が表示されるように、表示内容を制限することもできます。</p>

コマンド	説明
show cdp interface [interface-id]	CDP がイネーブルに設定されているインターフェイスの情報を表示します。 必要なインターフェイスの情報だけを表示できます。
show cdp neighbors [interface-id] [detail]	装置タイプ、インターフェイス タイプ、インターフェイス番号、保持時間の設定値、機能、プラットフォーム、ポート ID を含めたネイバー情報を表示します。 特定のインターフェイスに関するネイバー情報だけを表示したり、詳細表示にするため表示内容を拡張したりできます。
show cdp traffic	CDP カウンタ（送受信されたパケット数およびチェックサム エラーを含む）を表示します。

関連トピック

[CDP 特性の設定, \(41 ページ\)](#)

その他の関連資料

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	<i>Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3850 Switches)</i>

MIB

MIB	MIB のリンク
	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 を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<p>http://www.cisco.com/support</p>

Cisco Discovery Protocol の機能の履歴と情報

リリース	変更内容
Cisco IOS 15.0(2)EX1	この機能が導入されました。



第 4 章

簡易ネットワーク管理プロトコルの設定

- 機能情報の確認, 51 ページ
- SNMP の前提条件, 51 ページ
- SNMP の制約事項, 54 ページ
- SNMP に関する情報, 55 ページ
- SNMP の設定方法, 60 ページ
- SNMP ステータスのモニタリング, 73 ページ
- SNMP での例, 74 ページ
- 簡易ネットワーク管理プロトコルの機能の履歴と情報, 75 ページ

機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

SNMP の前提条件

サポートされている SNMP バージョン

このソフトウェア リリースは、次の SNMP バージョンをサポートしています。

- SNMPv1 : RFC1157 に規定された SNMP (完全インターネット標準)。

- SNMPv2C は、SNMPv2Classic のバルク検索機能を残し、エラー処理を改善したうえで、SNMPv2Classic のパーティベースの管理およびセキュリティフレームワークをコミュニティストリングベースの管理フレームワークに置き換えたものです。次の機能があります。
 - SNMPv2 : RFC 1902 ~ 1907 に規定された SNMP バージョン 2 (ドラフト版インターネット標準)
 - SNMPv2C : RFC 1901 に規定された SNMPv2 のコミュニティストリングベースの管理フレームワーク (試験版インターネットプロトコル)
- SNMPv3 : SNMP のバージョン 3 は、RFC 2273 ~ 2275 に規定されている相互運用可能な標準ベースプロトコルです。SNMPv3 は、ネットワーク上のパケットを認証、暗号化することでデバイスへのアクセスに対するセキュリティを提供します。SNMPv3 は、次のセキュリティ機能を備えています。
 - メッセージの完全性 : パケットが伝送中に改ざんされないようにします。
 - 認証 : 有効な送信元からのメッセージであるかどうかを判別します。
 - 暗号化 : パッケージの内容をミキシングし、許可されていない送信元に内容が読まれることを防止します。



(注) 暗号化を選択するには、**priv** キーワードを入力します。

SNMPv1 と SNMPv2C は、ともにコミュニティベース形式のセキュリティを使用します。エージェントの MIB にアクセスできるマネージャのコミュニティが、IP アドレス アクセス コントロール リストおよびパスワードによって定義されます。

SNMPv2C にはバルク検索機能が組み込まれ、より詳細なエラー メッセージを管理ステーションに報告します。バルク検索機能は、テーブルや大量の情報を検索し、必要な往復回数を削減します。SNMPv2C ではエラー処理機能が改善され、さまざまなエラーを区別するための拡張エラーコードが使用されています。これらのエラーは、SNMPv1 では単一のエラー コードで報告されません。SNMPv2 では、エラー リターン コードでエラー タイプが報告されるようになりました。

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。セキュリティモデルは、ユーザとユーザが属しているグループ用に設定された認証方式です。セキュリティレベルとは、セキュリティモデル内で許可されるセキュリティのレベルです。セキュリティレベルとセキュリティモデルの組み合わせにより、SNMP パケットを扱うときに使用するセキュリティ方式が決まります。使用可能なセキュリティモデルは、SNMPv1、SNMPv2C、および SNMPv3 です。

次の表では、この特性を識別し、セキュリティモデルとセキュリティレベルの異なる組み合わせを比較します。

表 7: **SNMP** セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
SNMPv1	noAuthNoPriv	コミュニティスト リング	No	コミュニティスト リングの照合を使 用して認証しま す。
SNMPv2C	noAuthNoPriv	コミュニティスト リング	No	コミュニティスト リングの照合を使 用して認証しま す。
SNMPv3	noAuthNoPriv	ユーザ名	No	ユーザ名の照合を 使用して認証しま す。
SNMPv3	authNoPriv	Message Digest 5 (MD5) または Secure Hash Algorithm (SHA)	No	HMAC-MD5 アル ゴリズムまたは HMAC-SHA アル ゴリズムに基づい て認証します。

モデル	レベル	認証	暗号化	結果
SNMPv3	authPriv	MD5 または SHA	データ暗号規格 (DES) または Advanced Encryption Standard (AES)	<p>HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。</p> <p>次の暗号化アルゴリズムで、User-based Security Model (USM) を指定できます。</p> <ul style="list-style-type: none"> • CBC-DES (DES-56) 規格に基づく認証に加えた DES 56 ビット暗号化 • 3DES 168 ビット暗号化 • AES 128 ビット暗号化、192 ビット暗号化、または 256 ビット暗号化

管理ステーションでサポートされている SNMP バージョンを使用するには、SNMP エージェントを設定する必要があります。エージェントは複数のマネージャと通信できるため、SNMPv1、SNMPv2C、および SNMPv3 を使用する通信をサポートするようにソフトウェアを設定できます。

SNMP の制約事項

バージョンの制約事項

- SNMPv1 は informs をサポートしていません。

SNMP に関する情報

SNMP の概要

SNMP は、マネージャとエージェント間の通信のメッセージフォーマットを提供するアプリケーションレイヤプロトコルです。SNMP システムは、SNMP マネージャ、SNMP エージェント、および管理情報ベース (MIB) で構成されます。SNMP マネージャは、Cisco Prime Infrastructure などのネットワーク管理システム (NMS) に統合できます。エージェントおよび MIB は、スイッチに常駐します。スイッチ上で SNMP を設定するには、マネージャとエージェント間の関係を定義します。

SNMP エージェントは MIB 変数を格納し、SNMP マネージャはこの変数の値を要求または変更できます。マネージャはエージェントから値を取得したり、エージェントに値を格納したりできます。エージェントは、デバイスパラメータやネットワークデータの保存場所である MIB から値を収集します。また、エージェントはマネージャのデータ取得またはデータ設定の要求に応答できます。

エージェントは非送信請求トラップをマネージャに送信できます。トラップは、ネットワーク上のある状態を SNMP マネージャに通知するメッセージです。トラップは不正なユーザ認証、再起動、リンクステータス (アップまたはダウン)、MAC アドレス追跡、TCP 接続の終了、ネイバーとの接続の切断などの重要なイベントの発生を意味する場合があります。

アクティブスイッチでは、スイッチスタック全体に対する SNMP 要求およびトラップが処理されます。アクティブスイッチでは、すべてのスタックメンバに関連するすべての要求またはトラップが透過的に管理されます。新しいアクティブスイッチが選択されると、新しいアクティブスイッチで制御が開始された後でも SNMP 管理ステーションに対する IP 接続が維持されたままの場合、新しいアクティブスイッチでは、前のアクティブスイッチで設定済みの SNMP 要求およびトラップの処理が続行されます。

SNMP マネージャ機能

SNMP マネージャは、MIB 情報を使用して、次の表に示す動作を実行します。

表 8: **SNMP** の動作

動作	説明
get-request	特定の変数から値を取得します。
get-next-request	テーブル内の変数から値を取得します。 ²
get-bulk-request ³	テーブルの複数の行など、通常はサイズの小さい多数のデータブロックに分割して送信する必要がある巨大なデータブロックを取得します。
get-response	NMS から送信される get-request、get-next-request、および set-request に対して応答します。

動作	説明
set-request	特定の変数に値を格納します。
trap	SNMP エージェントから SNMP マネージャに送られる、イベントの発生を伝える非送信請求メッセージです。

- ² この動作では、SNMP マネージャに正確な変数名を認識させる必要はありません。テーブル内を順に検索して、必要な変数を検出します。
- ³ get-bulk コマンドを使用できるのは、SNMPv2 以上に限られます。

SNMP エージェント機能

SNMP エージェントは、次のようにして SNMP マネージャ要求に応答します。

- MIB 変数の取得：SNMP エージェントは NMS からの要求に応答して、この機能を開始します。エージェントは要求された MIB 変数の値を取得し、この値を使用して NMS に応答します。
- MIB 変数の設定：SNMP エージェントは NMS からのメッセージに応答して、この機能を開始します。SNMP エージェントは、MIB 変数の値を NMS から要求された値に変更します。

エージェントで重要なイベントが発生したことを NMS に通知するために、SNMP エージェントは非送信請求トラップメッセージも送信します。トラップ条件の例には、ポートまたはモジュールがアップまたはダウン状態になった場合、スパニングツリートポロジが変更された場合、認証に失敗した場合などがあります。

SNMP コミュニティストリング

SNMP コミュニティストリングは、MIB オブジェクトに対するアクセスを認証し、組み込みパスワードとして機能します。NMS がスイッチにアクセスするには、NMS 上のコミュニティストリング定義がスイッチ上の3つのコミュニティストリング定義の少なくとも1つと一致しなければなりません。

コミュニティストリングの属性は、次のいずれかです。

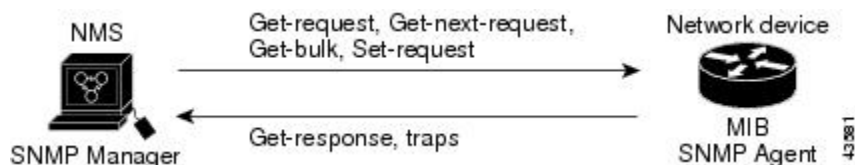
- 読み取り専用 (RO)：コミュニティストリングを除き MIB 内のすべてのオブジェクトに、許可された管理ステーションに対する読み取りアクセス権を与えますが、書き込みアクセスは許可しません。
- 読み取り-書き込み (RW)：MIB 内のすべてのオブジェクトに、許可された管理ステーションに対する読み取りおよび書き込みアクセス権を与えますが、コミュニティストリングへのアクセスは許可しません。
- クラスタを作成すると、コマンドスイッチがメンバスイッチと SNMP アプリケーション間のメッセージ交換を管理します。Network Assistant ソフトウェアは、コマンドスイッチ上で最初に設定された RW および RO コミュニティストリングにメンバスイッチ番号 (@esN、N はスイッチ番号) を追加し、これらのストリングをメンバスイッチに伝播します。

SNMP MIB 変数アクセス

NMS の例として、Cisco Prime Infrastructure ネットワーク管理ソフトウェアがあります。Cisco Prime Infrastructure 2.0 ソフトウェアは、スイッチ MIB 変数を使用して装置変数を設定し、ネットワーク上の装置をポーリングして特定の情報を取得します。ポーリング結果は、グラフ形式で表示されます。この結果を解析して、インターネットワーキング関連の問題のトラブルシューティング、ネットワーク パフォーマンスの改善、デバイス設定の確認、トラフィック負荷のモニタなどを行うことができます。

次の図に示すように、SNMP エージェントは MIB からデータを収集します。エージェントは SNMP マネージャに対し、トラップ（特定イベントの通知）を送信でき、SNMP マネージャはトラップを受信して処理します。トラップは、ネットワーク上で発生した不正なユーザ認証、再起動、リンクステータス（アップまたはダウン）、MAC アドレストラッキングなどの状況を SNMP マネージャに通知します。SNMP エージェントはさらに、SNMP マネージャから `get-request`、`get-next-request`、および `set-request` 形式で送信される MIB 関連のクエリに応答します。

図 3: SNMP ネットワーク



SNMP 通知

SNMP を使用すると、特定のイベントが発生した場合に、スイッチから SNMP マネージャに通知を送信できます。SNMP 通知は、トラップまたは情報要求として送信できます。コマンド構文では、トラップまたは情報を選択するオプションがコマンドにない限り、キーワード `traps` はトラップ、情報、またはその両方を表します。 `snmp-server host` コマンドを使用して、トラップまたは情報として SNMP 通知を送信するかどうかを指定します。



(注) SNMPv1 は `informs` をサポートしていません。

トラップは信頼性に欠けます。受信側はトラップを受信しても確認応答を送信しないので、トラップが受信されたかどうか送信側にわからないからです。情報要求の場合、受信した SNMP マネージャは SNMP 応答プロトコルデータユニット (PDU) でメッセージを確認します。送信側が応答を受信しなかった場合は、再び情報要求を送信できます。再送信できるので、情報の方がトラップより意図した宛先に届く可能性が高くなります。

情報の方がトラップより信頼性が高いのは、スイッチおよびネットワークのリソースを多く消費するという特性にも理由があります。送信と同時に廃棄されるトラップと異なり、情報要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持されます。トラップの送信は 1 回限りですが、情報は数回にわたって再送信つまり再試行が可能です。再送信の回数

が増えるとトラフィックが増加し、ネットワークのオーバーヘッドが高くなる原因にもなります。したがって、トラップにするか情報にするかは、信頼性を取るかリソースを取るかという選択になります。SNMP マネージャですべての通知を受信することが重要な場合は、情報要求を使用してください。ネットワークまたはスイッチのメモリ上のトラフィックが問題になる場合で、なおかつ通知が不要な場合は、トラップを使用してください。

SNMP ifIndex MIB オブジェクト値

NMS の IF-MIB は、物理インターフェイスまたは論理インターフェイスを識別する、ゼロより大きい一意の値である interface index (ifIndex) オブジェクト値の生成および割り当てを行います。スイッチの再起動またはスイッチ ソフトウェアのアップグレード時に、スイッチは、インターフェイスにこれと同じ値を使用します。たとえば、スイッチのポート 2 に 10003 という ifIndex 値が割り当てられていると、スイッチの再起動後も同じ値が使用されます。

スイッチは、次の表内のいずれかの値を使用して、インターフェイスに ifIndex 値を割り当てます。

表 9 : ifIndex 値

インターフェイス タイプ	ifIndex 範囲
SVI ⁴	1 ~ 4999
EtherChannel	5001 ~ 5048
トンネル	5078 ~ 5142
種類とポート番号に基づく物理 (ギガビット イーサネットまたは SFP ⁵ モジュール インターフェイス)	10000 ~ 14500
ヌル	14501
ループバックおよびトンネル	24567+

⁴ SVI = Switch Virtual Interface

⁵ SFP = Small Form-Factor Pluggable

SNMP のデフォルト設定

機能	デフォルト設定
SNMP エージェント	ディセーブル ⁶ .
SNMP トラップ レシーバ	未設定
SNMP トラップ	TCP 接続のトラップ (tty) 以外は、イネーブルではありません。

機能	デフォルト設定
SNMP バージョン	version キーワードがない場合、デフォルトはバージョン 1 になります。
SNMPv3 認証	キーワードを入力しなかった場合、セキュリティ レベルはデフォルトで noauth (noAuthNoPriv) になります。
SNMP 通知タイプ	タイプが指定されていない場合、すべての通知が送信されます。

- ⁶ これは、スイッチが起動し、スタートアップ コンフィギュレーションに **snmp-server** グローバル コンフィギュレーション コマンドが設定されていない場合のデフォルトです。

SNMP 設定時の注意事項

スイッチが起動し、スイッチのスタートアップ コンフィギュレーションに少なくとも 1 つの **snmp-server** グローバル コンフィギュレーション コマンドが設定されている場合、SNMP エージェントはイネーブルになります。

SNMP グループは、SNMP ユーザを SNMP ビューに対応付けるテーブルです。SNMP ユーザは、SNMP グループのメンバです。SNMP ホストは、SNMP トラップ動作の受信側です。SNMP エンジン ID は、ローカルまたはリモート SNMP エンジンの名前です。

SNMP を設定する場合は、以下の注意事項に従ってください。

- SNMP グループを設定するときは、通知ビューを指定しません。 **snmp-server host** グローバル コンフィギュレーション コマンドがユーザの通知ビューを自動生成し、そのユーザに対応するグループに追加します。グループの通知ビューを変更すると、そのグループに対応付けられたすべてのユーザが影響を受けます。
- リモートユーザを設定する場合は、ユーザが存在するデバイスのリモート SNMP エージェントに対応する IP アドレスまたはポート番号を指定します。
- 特定のエージェントのリモートユーザを設定する前に、**snmp-server engineID** グローバル コンフィギュレーション コマンドを **remote** オプションとともに使用して、SNMP エンジン ID を設定してください。リモートエージェントの SNMP エンジン ID およびユーザパスワードを使用して認証およびプライバシー ダイジェストが算出されます。先にリモートエンジン ID を設定しておかないと、コンフィギュレーション コマンドがエラーになります。
- SNMP 情報を設定するときには、プロキシ要求または情報の送信先となるリモートエージェントの SNMP エンジン ID を SNMP データベースに設定しておく必要があります。
- ローカルユーザがリモートホストと関連付けられていない場合、スイッチは **auth** (authNoPriv) および **priv** (authPriv) の認証レベルの情報を送信しません。
- SNMP エンジン ID の値を変更すると、重大な影響が生じます。(コマンドラインで入力された) ユーザのパスワードは、パスワードおよびローカルエンジン ID に基づいて、MD5 または SHA セキュリティ ダイジェストに変換されます。コマンドラインのパスワードは、RFC 2274 の規定に従って廃棄されます。このようにパスワードが廃棄されるため、エンジ

ン ID 値を変更した場合は SNMPv3 ユーザのセキュリティ ダイジェストが無効となり、**snmp-server user username** 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、SNMP ユーザを再設定する必要があります。 エンジン ID を変更した場合は、同様の制限によって コミュニティ スtring も再設定する必要があります。

SNMP の設定方法

SNMP エージェントのディセーブル化

no snmp-server グローバル コンフィギュレーション コマンドは、デバイス上で実行している SNMP エージェントのすべてのバージョン（バージョン 1、バージョン 2C、バージョン 3）をディセーブルにします。 入力した最初の **snmp-server** グローバル コンフィギュレーション コマンドによって、SNMP エージェントのすべてのバージョンを再度イネーブルにします。 特に SNMP をイネーブルにするために指定された Cisco IOS コマンドはありません。

SNMP エージェントをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

はじめる前に

SNMP エージェントをディセーブルにする前にイネーブルにする必要があります。 デバイス上で入力した最初の **snmp-server** グローバル コンフィギュレーション コマンドによって SNMP エージェントがイネーブルになります。

手順の概要

1. **configure terminal**
2. **no snmp-server**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no snmp-server 例： Switch(config)# no snmp-server	SNMP エージェント動作をディセーブルにします。

	コマンドまたはアクション	目的
ステップ 3	end 例： Switch(config)# end	特権 EXEC モードに戻ります。

コミュニティストリングの設定

SNMP マネージャとエージェントの関係を定義するには、SNMP コミュニティストリングを使用します。コミュニティストリングは、スイッチ上のエージェントへのアクセスを許可する、パスワードと同様の役割を果たします。ストリングに対応する次の特性を1つまたは複数指定することもできます。

- コミュニティストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスのアクセスリスト
- 指定のコミュニティにアクセスできるすべての MIB オブジェクトのサブセットを定義する MIB ビュー
- コミュニティにアクセスできる MIB オブジェクトの読み書き権限または読み取り専用権限

スイッチ上でコミュニティストリングを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **snmp-server community string [view view-name] [ro | rw] [access-list-number]**
3. **access-list access-list-number {deny | permit} source [source-wildcard]**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	<p>snmp-server community string [view view-name] [ro rw] [access-list-number]</p> <p>例 :</p> <pre>Switch(config)# snmp-server community comaccess ro 4</pre>	<p>コミュニティストリングを設定します。</p> <p>(注) コンテキスト情報を区切るには @ 記号を使用します。このコマンドの設定時に SNMP コミュニティストリングの一部として @ 記号を使用しないでください。</p> <ul style="list-style-type: none"> • <i>string</i> には、パスワードと同様に機能し、SNMP プロトコルへのアクセスを許可するストリングを指定します。任意の長さのコミュニティストリングを 1 つまたは複数設定できます。 • (任意) <i>view-name</i> には、コミュニティがアクセスできるビューレコードを指定します。 • (任意) 許可された管理ステーションで MIB オブジェクトを取得する場合は読み取り専用 (ro)、許可された管理ステーションで MIB オブジェクトを取得および変更する場合は読み書き (rw) を指定します。デフォルトでは、コミュニティストリングはすべてのオブジェクトに対する読み取り専用アクセスを許可します。 • (任意) <i>access-list-number</i> には、1 ~ 99 および 1300 ~ 1999 の標準 IP アクセスリスト番号を入力します。
ステップ 3	<p>access-list access-list-number {deny permit} source [source-wildcard]</p> <p>例 :</p> <pre>Switch(config)# access-list 4 deny any</pre>	<p>(任意) ステップ 2 で標準 IP アクセスリスト番号を指定してリストを作成した場合は、必要に応じてコマンドを繰り返します。</p> <ul style="list-style-type: none"> • <i>access-list-number</i> には、ステップ 2 で指定したアクセスリスト番号を入力します。 • deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 • <i>source</i> には、コミュニティストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスを入力します。 • (任意) <i>source-wildcard</i> には、<i>source</i> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>アクセスリストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>
ステップ 4	<p>end</p> <p>例 :</p> <pre>Switch(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>

次に、comaccess ストリングを SNMP に割り当てて読み取り専用アクセスを許可し、IP アクセスリスト 4 がこのコミュニティストリングを使用してスイッチの SNMP エージェントにアクセスできるように指定する例を示します。

```
Switch(config)# snmp-server community comaccess ro 4
```

次の作業

SNMP コミュニティのアクセスをディセーブルにするには、そのコミュニティのコミュニティストリングをヌルストリングに設定します（コミュニティストリングに値を入力しないでください）。

特定のコミュニティストリングを削除するには、**no snmp-server** コミュニティストリンググローバル コンフィギュレーション コマンドを使用します。

スイッチのローカルまたはリモート SNMP サーバエンジンを表す識別名（エンジン ID）を指定できます。SNMP ユーザを SNMP ビューにマッピングする、SNMP サーバグループを設定し、新規ユーザを SNMP グループに追加できます。

SNMP グループおよびユーザの設定

スイッチのローカルまたはリモート SNMP サーバエンジンを表す識別名（エンジン ID）を指定できます。SNMP ユーザを SNMP ビューにマッピングする、SNMP サーバグループを設定し、新規ユーザを SNMP グループに追加できます。

スイッチ上で SNMP グループとユーザを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **snmp-server engineID** {local *engineid-string* | remote *ip-address* [*udp-port port-number*] *engineid-string*}
3. **snmp-server group** *group-name* {v1 | v2c | v3 {auth | noauth | priv}} [read *readview*] [write *writeview*] [notify *notifyview*] [access *access-list*]
4. **snmp-server user** *username group-name* {remote *host* [*udp-port port*]} {v1 [access *access-list*] | v2c [access *access-list*] | v3 [encrypted] [access *access-list*] [auth {md5 | sha} *auth-password*] } [priv {des | 3des | aes {128 | 192 | 256}}] *priv-password*]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	snmp-server engineID {local engineid-string remote ip-address [udp-port port-number] engineid-string} 例： Switch(config)# snmp-server engineID local 1234	SNMP のローカル コピーまたはリモート コピーに名前を設定します。 <ul style="list-style-type: none"> • engineid-string は、SNMP のコピー名を指定する 24 文字の ID ストリングです。後続ゼロが含まれる場合は、24 文字のエンジン ID すべてを指定する必要はありません。指定するのは、エンジン ID のうちゼロのみが続く箇所を除いた部分だけです。手順例では、123400000000000000000000 のエンジン ID を設定します。 • remote を指定した場合、SNMP のリモート コピーが置かれているデバイスの ip-address を指定し、任意でリモート デバイスのユーザデータグラム プロトコル (UDP) ポートを指定します。デフォルトは 162 です。
ステップ 3	snmp-server group group-name {v1 v2c v3 {auth noauth priv}} [read readview] [write writeview] [notify notifyview] [access access-list] 例： Switch(config)# snmp-server group public v2c access lmnop	リモート デバイス上で新しい SNMP グループを設定します。 group-name には、グループの名前を指定します。 次のいずれかのセキュリティ モデルを指定します。 <ul style="list-style-type: none"> • v1 は、最も安全性の低いセキュリティ モデルです。 • v2c は、2 番めに安全性の低いセキュリティ モデルです。標準の 2 倍の幅で情報および整数を送送できます。 • 最も安全な v3 の場合には、次の認証レベルの 1 つを選択する必要があります。 <ul style="list-style-type: none"> auth : MD5 および SHA によるパケット認証が可能です。 noauth : noAuthNoPriv というセキュリティ レベルをイネーブルにします。キーワードを指定しなかった場合、これがデフォルトです。 priv : データ暗号規格 (DES) によるパケット暗号化をイネーブルにします (privacy とも呼ばれます)。 <p>(任意) read readview とともに、エージェントの内容を表示できるビューの名前を表すストリング (64 文字以下) を入力します。</p> <p>(任意) write writeview とともに、データを入力し、エージェントの内容を設定できるビューの名前を表すストリング (64 文字以下) を入力します。</p>

	コマンドまたはアクション	目的
		<p>(任意) notify <i>notifyview</i> とともに、通知、情報、またはトラップを指定するビューの名前を表すストリング (64 文字以下) を入力します。</p> <p>(任意) access <i>access-list</i> とともに、アクセスリスト名のストリング (64 文字以下) を入力します。</p>
<p>ステップ 4</p>	<p>snmp-server user <i>username</i> <i>group-name</i> {remote <i>host</i> [udp-port <i>port</i>]} {v1 [access <i>access-list</i>] v2c [access <i>access-list</i>] v3 [encrypted] [access <i>access-list</i>] [auth {md5 sha} <i>auth-password</i>] } [priv {des 3des aes {128 192 256}} <i>priv-password</i>]</p> <p>例 :</p> <pre>Switch(config)# snmp-server user Pat public v2c</pre>	<p>SNMP グループに対して新規ユーザを追加します。</p> <p><i>username</i> は、エージェントに接続するホスト上のユーザ名です。</p> <p><i>group-name</i> は、ユーザが関連付けられているグループの名前です。</p> <p>remote を入力して、ユーザが所属するリモート SNMP エンティティおよびそのエンティティのホスト名または IP アドレスとともに、任意で UDP ポート番号を指定します。デフォルトは 162 です。</p> <p>SNMP バージョン番号 (v1、v2c、または v3) を入力します。 v3 を入力する場合は、次のオプションを追加します。</p> <ul style="list-style-type: none"> • encrypted は、パスワードを暗号化形式で表示するように指定します。このキーワードは、v3 キーワードが指定されている場合のみ使用可能です。 • auth は認証レベル設定セッションで、HMAC-MD5-96 (md5) または HMAC-SHA-96 (sha) 認証レベルを使用できます。パスワードストリング <i>auth-password</i> (64 文字以下) が必要です。 <p>v3 を入力すると、次のキーワードを使用して (64 文字以下)、プライベート (priv) 暗号化アルゴリズムおよびパスワードストリング <i>priv-password</i> を設定できます。</p> <ul style="list-style-type: none"> • priv は、ユーザベースセキュリティ モデル (USM) を指定します。 • des は、56 ビット DES アルゴリズムの使用を指定します。 • 3des は、168 ビット DES アルゴリズムの使用を指定します。 • aes は、DES アルゴリズムの使用を指定します。128 ビット暗号化、192 ビット暗号化、または 256 ビット暗号化のいずれかを選択する必要があります。 <p>(任意) access <i>access-list</i> とともに、アクセスリスト名のストリング (64 文字以下) を入力します。</p>
<p>ステップ 5</p>	<p>end</p> <p>例 :</p> <pre>Switch(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>

SNMP 通知の設定

トラップマネージャは、トラップを受信して処理する管理ステーションです。トラップは、特定のイベントが発生したときにスイッチが生成するシステムアラートです。デフォルトでは、トラップマネージャは定義されず、トラップは送信されません。この Cisco IOS Release が稼働しているスイッチでは、トラップマネージャを無制限に設定できます。



(注) コマンド構文で **traps** というワードを使用するコマンドは多数あります。トラップまたは情報を選択するオプションがコマンドにない限り、キーワード **traps** はトラップ、情報のいずれか、またはその両方を表します。 **snmp-server host** 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、トラップまたは情報として SNMP 通知を送信するかどうかを指定します。

次の表に示す通知タイプを受信するには、特定のホストに対して **snmp-server host** グローバル コンフィギュレーションコマンドを使用します。これらのトラップの一部または全部をイネーブルにして、これを受信するようにトラップマネージャを設定できます。

表 10: デバイスの通知タイプ

通知タイプのキーワード	説明
bgp	ボーダー ゲートウェイ プロトコル (BGP) 状態変化トラップを生成します。このオプションは、IP サービス フィーチャ セットがイネーブルになっている場合にだけ使用できます。
bridge	STP ブリッジ MIB トラップを生成します。
cluster	クラスタ設定が変更された場合に、トラップを生成します。
config	SNMP 設定が変更された場合に、トラップを生成します。
copy-config	SNMP コピー設定が変更された場合に、トラップを生成します。
cpu threshold	CPU に関連したトラップをイネーブルにします。
entity	SNMP エンティティが変更された場合に、トラップを生成します。
envmon	環境モニタトラップを生成します。ファン (fan)、シャットダウン (shutdown)、ステータス (status)、電源 (supply)、温度 (temperature) の環境トラップのいずれかまたはすべてをイネーブルにできます。

通知タイプのキーワード	説明
flash	SNMP FLASH 通知を生成します。スイッチスタックでは、オプションとして、フラッシュの追加または削除に関する通知をイネーブルにできます。このようにすると、スタックからスイッチを削除するか、またはスタックにスイッチを追加した場合に（物理的な取り外し、電源の再投入、またはリロードの場合に）、トラップが発行されます。
fru-ctrl	エンティティ現場交換可能ユニット（FRU）制御トラップを生成します。スイッチスタックでは、このトラップはスタックにおけるスイッチの挿入/取り外しを意味します。
hsrp	ホットスタンバイルータプロトコル（HSRP）が変更された場合に、トラップを生成します。
ipmulticast	IP マルチキャストルーティングが変更された場合に、トラップを生成します。
mac-notification	MAC アドレス通知のトラップを生成します。
msdp	Multicast Source Discovery Protocol（MSDP）が変更された場合に、トラップを生成します。
ospf	Open Shortest Path First（OSPF）が変更された場合に、トラップを生成します。シスコ固有、エラー、リンクステートアドバタイズ、レート制限、再送信、ステート変更に関するトラップを任意にイネーブルにできます。
pim	Protocol-Independent Multicast（PIM）が変更された場合に、トラップを生成します。無効な PIM メッセージ、ネイバー変更、およびランデブーポイント（RP）マッピングの変更に関するトラップを任意にイネーブルにできます。
port-security	SNMP ポートセキュリティトラップを生成します。1 秒あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ～ 1000 秒です。デフォルトは 0 秒で、レート制限がないという意味です。 (注) 通知タイプ port-security を使用してトラップを設定する際に、まずポートセキュリティトラップを設定して、次に以下のポートセキュリティトラップレートを設定します。 1 snmp-server enable traps port-security 2 snmp-server enable traps port-security trap-rate rate
rtr	SNMP Response Time Reporter（RTR）のトラップを生成します。

通知タイプのキーワード	説明
snmp	認証、コールドスタート、ウォームスタート、リンクアップ、またはリンクダウンについて、SNMP タイプ通知のトラップを生成します。
storm-control	SNMP ストーム制御のトラップを生成します。1分あたりの最大トラップ速度も設定できます。指定できる範囲は0～1000です。デフォルトは0に設定されています（制限なしの状態では、発生ごとにトラップが送信されます）。
stpx	SNMP STP 拡張 MIB トラップを生成します。
syslog	SNMP の Syslog トラップを生成します。
tty	TCP接続のトラップを生成します。このトラップは、デフォルトでイネーブルに設定されています。
vlan-membership	SNMP VLAN メンバーシップが変更された場合に、トラップを生成します。
vlancreate	SNMP VLAN 作成トラップを生成します。
vlandelete	SNMP VLAN 削除トラップを生成します。
vtp	VLAN トランッキング プロトコル (VTP) が変更された場合に、トラップを生成します。

ホストにトラップまたは情報を送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **snmp-server engineID remote ip-address engineid-string**
3. **snmp-server user username group-name {remote host [udp-port port]} {v1 [access access-list] | v2c [access access-list] | v3 [encrypted] [access access-list] [auth {md5 | sha} auth-password]}**
4. **snmp-server group group-name {v1 | v2c | v3 {auth | noauth | priv}} [read readview] [write writeview] [notify notifyview] [access access-list]**
5. **snmp-server host host-addr [informs | traps] [version {1 | 2c | 3 {auth | noauth | priv}}] community-string [notification-type]**
6. **snmp-server enable traps notification-types**
7. **snmp-server trap-source interface-id**
8. **snmp-server queue-length length**
9. **snmp-server trap-timeout seconds**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	snmp-server engineID remote ip-address engineid-string 例： Switch(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b	リモート ホストのエンジン ID を指定します。
ステップ 3	snmp-server user username group-name {remote host [udp-port port]} {v1 [access access-list] v2c [access access-list] v3 [encrypted] [access access-list] [auth {md5 sha} auth-password]} 例： Switch(config)# snmp-server user Pat public v2c	SNMP ユーザを設定し、ステップ 2 で作成したリモート ホストに関連付けます。 (注) アドレスに対応するリモートユーザを設定するには、先にリモート ホストのエンジン ID を設定しておく必要があります。このようにしないと、エラーメッセージが表示され、コマンドが実行されません。
ステップ 4	snmp-server group group-name {v1 v2c v3 {auth noauth priv}} [read readview] [write writeview] [notify notifyview] [access access-list] 例： Switch(config)# snmp-server group public v2c access lmnop	SNMP グループを設定します。
ステップ 5	snmp-server host host-addr [informs traps] [version {1 2c 3 {auth noauth priv}}] community-string [notification-type] 例： Switch(config)# snmp-server host 203.0.113.1 comaccess snmp	SNMP トラップ動作の受信先を指定します。 <i>host-addr</i> には、ホスト (対象となる受信側) の名前またはインターネット アドレスを指定します。 (任意) SNMP トラップをホストに送信するには、 traps (デフォルト) を指定します。SNMP 情報をホストに送信するには、 informs を指定します。 (任意) SNMP version (1、2c、または 3) を指定します。SNMPv1 は informs をサポートしていません。 (任意) バージョン 3 の場合、認証レベルとして auth、noauth、または priv を選択します。 <i>community-string</i> には、 version 1 または version 2c が指定されている場合、通知動作で送信される、パスワードに類似したコミュニ

	コマンドまたはアクション	目的
		<p>ニティ スtringを入力します。 version 3 が指定されている場合、SNMPv3 ユーザ名を入力します。</p> <p>コンテキスト情報を区切るには @ 記号を使用します。このコマンドの設定時にSNMPコミュニティStringの一部として @ 記号を使用しないでください。</p> <p>(任意) <i>notification-type</i> には、上の表に記載されているキーワードを使用します。タイプが指定されていない場合、すべての通知が送信されます。</p>
ステップ 6	<p>snmp-server enable traps notification-types</p> <p>例： Switch(config)# snmp-server enable traps snmp</p>	<p>スイッチがトラップまたは情報を送信できるようにし、送信する通知のタイプを指定します。通知タイプの一覧については、上の表を参照するか、snmp-server enable traps ? と入力してください。</p> <p>複数のトラップタイプをイネーブルにするには、トラップタイプごとに snmp-server enable traps コマンドを個別に入力する必要があります。</p> <p>(注) 通知タイプ port-security を使用してトラップを設定する際に、まずポートセキュリティトラップを設定して、次に以下のポートセキュリティトラップレートを設定します。</p> <ol style="list-style-type: none"> snmp-server enable traps port-security snmp-server enable traps port-security trap-rate rate
ステップ 7	<p>snmp-server trap-source interface-id</p> <p>例： Switch(config)# snmp-server trap-source GigabitEthernet1/0/1</p>	<p>(任意) 送信元インターフェイスを指定します。そこからトラップメッセージに対応する IP アドレスが取得されます。情報の送信元 IP アドレスも、このコマンドで設定します。</p>
ステップ 8	<p>snmp-server queue-length length</p> <p>例： Switch(config)# snmp-server queue-length 20</p>	<p>(任意) 各トラップホストのメッセージキュー長を設定します。指定できる範囲は 1 ~ 1000 です。デフォルトは 10 です。</p>
ステップ 9	<p>snmp-server trap-timeout seconds</p> <p>例： Switch(config)# snmp-server trap-timeout 60</p>	<p>(任意) トラップメッセージを再送信する間隔を設定します。指定できる範囲は 1 ~ 1000 です。デフォルトは 30 秒です。</p>

	コマンドまたはアクション	目的
ステップ 10	end 例： Switch(config)# end	特権 EXEC モードに戻ります。

次の作業

snmp-server host コマンドでは、通知を受信するホストを指定します。 **snmp-server enable trap** コマンドによって、指定された通知方式（トラップおよび情報）がグローバルでイネーブルになります。ホストが情報を受信できるようにするには、そのホストに対応する **snmp-server host informs** コマンドを設定し、**snmp-server enable traps** コマンドを使用して情報をグローバルにイネーブルにする必要があります。

指定したホストがトラップを受信しないようにするには、**no snmp-server host host** グローバル コンフィギュレーションコマンドを使用します。キーワードを指定しないで **no snmp-server host** コマンドを使用すると、ホストへのトラップはディセーブルになりますが、情報はディセーブルになりません。情報をディセーブルにするには、**no snmp-server host informs** 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ください。特定のトラップタイプをディセーブルにするには、**no snmp-server enable traps notification-types** グローバル コンフィギュレーション コマンドを使用します。

エージェントコンタクトおよびロケーションの設定

SNMP エージェントのシステム接点およびロケーションを設定して、コンフィギュレーション ファイルからこれらの記述にアクセスできるようにするには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **snmp-server contact text**
3. **snmp-server location text**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	snmp-server contact text 例： Switch(config)# snmp-server contact Dial System Operator at beeper 21555	システムの連絡先文字列を設定します。
ステップ 3	snmp-server location text 例： Switch(config)# snmp-server location Building 3/Room 222	システムの場所を表す文字列を設定します。
ステップ 4	end 例： Switch(config)# end	特権 EXEC モードに戻ります。

SNMP を通して使用する TFTP サーバの制限

SNMP を通してコンフィギュレーション ファイルを保存およびロードするために使用する TFTP（簡易ファイル転送プロトコル）サーバを、アクセスリストに指定されているサーバに限定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **snmp-server tftp-server-list access-list-number**
3. **access-list access-list-number {deny | permit} source [source-wildcard]**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	snmp-server tftp-server-list access-list-number 例： Switch(config)# snmp-server tftp-server-list 44	SNMP を介したコンフィギュレーション ファイルのコピーに使用する TFTP サーバを、アクセス リストのサーバに限定します。 <i>access-list-number</i> には、1 ~ 99 および 1300 ~ 1999 の標準 IP アクセス リスト番号を入力します。
ステップ 3	access-list access-list-number {deny permit} source [source-wildcard] 例： Switch(config)# access-list 44 permit 10.1.1.2	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。 <i>access-list-number</i> には、ステップ 2 で指定したアクセス リスト番号を入力します。 deny キーワードは、条件が一致した場合にアクセスを拒否します。 permit キーワードは、条件が一致した場合にアクセスを許可します。 <i>source</i> には、スイッチにアクセスできる TFTP サーバの IP アドレスを入力します。 (任意) <i>source-wildcard</i> には、 <i>source</i> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
ステップ 4	end 例： Switch(config)# end	特権 EXEC モードに戻ります。

SNMP ステータスのモニタリング

不正なコミュニティストリングエントリ、エラー、要求変数の数など、SNMP の入出力統計情報を表示するには、**show snmp** 特権 EXEC コマンドを使用します。また、次の表にリストされたその他の特権 EXEC コマンドを使用して、SNMP 情報を表示することもできます。

表 11: SNMP 情報を表示するためのコマンド

コマンド	目的
show snmp	SNMP 統計情報を表示します。
show snmp engineID	デバイスに設定されているローカル SNMP エンジンおよびすべてのリモートエンジンに関する情報を表示します。
show snmp group	ネットワーク上の各 SNMP グループに関する情報を表示します。
show snmp pending	保留中の SNMP 要求の情報を表示します。
show snmp sessions	現在の SNMP セッションの情報を表示します。
show snmp user	SNMP ユーザ テーブルの各 SNMP ユーザ名に関する情報を表示します。 (注) このコマンドは、 auth noauth priv モードの SNMPv3 設定情報を表示するときに使用する必要があります。この情報は、 show running-config の出力には表示されません。

SNMP での例

次に、SNMP の全バージョンをイネーブルにする例を示します。この設定では、任意の SNMP マネージャがコミュニティ ストリング *public* を使用して、読み取り専用権限ですべてのオブジェクトにアクセスできます。この設定では、スイッチはトラップを送信しません。

```
Switch(config)# snmp-server community public
```

次に、任意の SNMP マネージャがコミュニティ ストリング *public* を使用して、読み取り専用権限ですべてのオブジェクトにアクセスする例を示します。スイッチはさらに、SNMPv1 を使用してホスト 192.180.1.111 および 192.180.1.33 に、SNMPv2C を使用してホスト 192.180.1.27 に VTP トラップを送信します。コミュニティ ストリング *public* は、トラップとともに送信されます。

```
Switch(config)# snmp-server community public
Switch(config)# snmp-server enable traps vtp
Switch(config)# snmp-server host 192.180.1.27 version 2c public
Switch(config)# snmp-server host 192.180.1.111 version 1 public
Switch(config)# snmp-server host 192.180.1.33 public
```

次に、*comaccess* コミュニティ ストリングを使用するアクセス リスト 4 のメンバに、すべてのオブジェクトへの読み取り専用アクセスを許可する例を示します。その他の SNMP マネージャは、どのオブジェクトにもアクセスできません。SNMP 認証障害トラップは、SNMPv2C がコミュニティ ストリング *public* を使用してホスト *cisco.com* に送信します。

```
Switch(config)# snmp-server community comaccess ro 4
Switch(config)# snmp-server enable traps snmp authentication
Switch(config)# snmp-server host cisco.com version 2c public
```

次に、エンティティ MIB トラップをホスト *cisco.com* に送信する例を示します。コミュニティストリングは制限されます。1行めで、スイッチはすでにイネーブルになっているトラップ以外に、エンティティ MIB トラップを送信できるようになります。2行目はこれらのトラップの宛先を指定し、ホスト *cisco.com* に対する以前の **snmp-server host** コマンドを無効にします。

```
Switch(config)# snmp-server enable traps entity
Switch(config)# snmp-server host cisco.com restricted entity
```

次に、コミュニティストリング *public* を使用して、すべてのトラップをホスト *myhost.cisco.com* に送信するようにスイッチをイネーブルにする例を示します。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

次に、ユーザとリモートホストを関連付けて、ユーザがグローバルコンフィギュレーションモードのときに **auth** (authNoPriv) 認証レベルで情報を送信する例を示します。

```
Switch(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b
Switch(config)# snmp-server group authgroup v3 auth
Switch(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5 mypassword
Switch(config)# snmp-server user authuser authgroup v3 auth md5 mypassword
Switch(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server inform retries 0
```

簡易ネットワーク管理プロトコルの機能の履歴と情報

リリース	変更内容
Cisco IOS 15.0(2)EX1	この機能が導入されました。



第 5 章

SPAN および RSPAN の設定

- 機能情報の確認, 77 ページ
- SPAN および RSPAN の前提条件, 77 ページ
- SPAN および RSPAN の制約事項, 78 ページ
- SPAN および RSPAN について, 81 ページ
- SPAN および RSPAN の設定方法, 93 ページ
- SPAN および RSPAN 動作のモニタリング, 113 ページ
- SPAN および RSPAN の設定例, 113 ページ
- SPAN および RSPAN の機能の履歴と情報, 115 ページ

機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

SPAN および RSPAN の前提条件

SPAN

- SPAN トラフィックを特定の VLAN に制限するには、**filter vlan** キーワードを使用します。トランクポートをモニタしている場合、このキーワードで指定された VLAN 上のトラフィック

クのみがモニタされます。デフォルトでは、トランク ポート上のすべての VLAN がモニタされます。

RSPAN

- RSPAN VLAN を設定してから、RSPAN 送信元または宛先セッションを設定することを推奨します。

SPAN および RSPAN の制約事項

SPAN

SPAN の制約事項は次のとおりです。

- 各スイッチにつき、最大 4 つの送信元セッション（スイッチが Catalyst 2960-S スイッチでスタック構成されている場合は最大 2 つ）および 64 の RSPAN 宛先セッションを設定できます。送信元セッションは、ローカル SPAN セッションまたは RSPAN 送信元セッションのどちらかになります。
- SPAN 送信元の場合は、セッションごとに、単一のポートまたは VLAN、一連のポートまたは VLAN、一定範囲のポートまたは VLAN のトラフィックをモニタできます。1 つの SPAN セッションに、送信元ポートおよび送信元 VLAN を混在させることはできません。
- 宛先ポートを送信元ポートにすることはできません。同様に、送信元ポートを宛先ポートにすることもできません。
- 同じ宛先ポートで 2 つの SPAN セッションを設定することはできません。
- スイッチ ポートを SPAN 宛先ポートとして設定すると、通常のスイッチ ポートではなくなります。SPAN 宛先ポートを通過するのは、監視対象トラフィックのみになります。
- SPAN コンフィギュレーション コマンドを入力しても、前に設定した SPAN パラメータは削除されません。設定されている SPAN パラメータを削除するには、**no monitor session {session_number | all | local | remote}** グローバル コンフィギュレーション コマンドを入力する必要があります。
- ローカル SPAN では、**encapsulation replicate** キーワードが指定されている場合、SPAN 宛先ポートを経由する発信パケットは元のカプセル化ヘッダー（タグなし、ISL、または IEEE 802.1Q）を伝送します。このキーワードが指定されていない場合、パケットはネイティブ形式で送信されます。
- ディセーブルのポートを送信元ポートまたは宛先ポートとして設定することはできますが、SPAN 機能が開始されるのは、宛先ポートと少なくとも 1 つの送信元ポートまたは送信元 VLAN がイネーブルになってからです。
- 単一の SPAN セッションに、送信元 VLAN とフィルタ VLAN を混在させることはできません。

SPAN セッションのトラフィック モニタリングには次の制約事項があります。

- ポートまたは VLAN を送信元にできますが、同じセッション内に送信元ポートと送信元 VLAN を混在させることはできません。
- ◦ 同じスイッチまたはスイッチ スタック内で、ローカル SPAN と RSPAN の送信元セッションの両方を実行できます。スイッチまたはスイッチ スタックは合計 64 の送信元および RSPAN 宛先セッションをサポートします。
 - 別個のまたは重複する SPAN 送信元ポートと VLAN のセットによって、SPAN または RSPAN 送信元セッションを 2 つ個別に設定できます。スイッチドポートおよびルーテッドポートはいずれも SPAN 送信元および宛先として設定できます。
- 1 つの SPAN セッションに複数の宛先ポートを設定できますが、1 つのスイッチ スタックあたりに設定できる宛先ポートは最大で 64 個です。
- SPAN セッションがスイッチの通常の動作を妨げることはありません。ただし、10 Mbps のポートで 100 Mbps のポートをモニタするなど、オーバーサブスクライブの SPAN 宛先は、パケットのドロップまたは消失を招くことがあります。
- SPAN または RSPAN がイネーブルの場合、監視中の各パケットは 2 回送信されます（1 回は標準トラフィックとして、もう 1 回は監視されたパケットとして）。多数のポートまたは VLAN をモニタすると、大量のネットワーク トラフィックが生成されることがあります。
- ディセーブルのポート上に SPAN セッションを設定することはできますが、そのセッション用に宛先ポートと少なくとも 1 つの送信元ポートまたは VLAN をイネーブルにしない限り、SPAN セッションはアクティブになりません。
- スイッチは、単一セッション内でのローカル SPAN と RSPAN の併用をサポートしません。
 - RSPAN 送信元セッションにローカル宛先ポートを設定できません。
 - RSPAN 宛先セッションにローカル送信元ポートを設定できません。
 - 同じスイッチまたはスイッチ スタック上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行できません。

RSPAN

RSPAN の制約事項は次のとおりです。

- RSPAN は、BPDU パケット モニタリングまたは他のレイヤ 2 スイッチ プロトコルをサポートしません。
- RSPAN VLAN はトランク ポートにのみ設定されており、アクセス ポートには設定されていません。不要なトラフィックが RSPAN VLAN に発生しないようにするために、参加しているすべてのスイッチで VLAN RSPAN 機能がサポートされていることを確認してください。
- 送信元トランク ポートにアクティブな RSPAN VLAN が設定されている場合、RSPAN VLAN はポートベース RSPAN セッションの送信元として含まれます。また、RSPAN VLAN を SPAN セッションの送信元に設定することもできます。ただし、スイッチはスパンされたトラフィックをモニタしないため、スイッチの RSPAN 送信元セッションの宛先として識別された RSPAN VLAN では、パケットの出力スパニングがサポートされません。

- VTP および VTP プルーニングをイネーブルにすると、トランク内で RSPAN トラフィックが プルーニングされ、1005 以下の VLAN ID に関して、ネットワークで不必要な RSPAN トラフィックのフラディングが防止されます。

フローベースの SPAN (FSPAN) およびフローベースの RSPAN (FRSPAN)

フローベースの SPAN (FSPAN) およびフローベースの RSPAN (FRSPAN) の制約事項は次のとおりです。

- ACL は、一度に 1 つの SPAN または RSPAN にしか接続できません。
- FSPAN ACL が接続されていない場合、FSPAN はディセーブルで、すべてのトラフィックが SPAN 宛先ポートにコピーされます。
- SPAN セッションに空の FSPAN ACL を接続すると、パケットはフィルタリングされず、すべてのトラフィックが監視されます。
- FSPAN ACL は、ポート単位 VLAN 単位のセッションに適用できません。ポート単位 VLAN 単位のセッションは、最初にポートベースのセッションを設定し、次にセッションに特定の VLAN を設定することにより設定できます。次に例を示します。

```
Switch(config)# monitor session session_number source interface interface-id
Switch(config)# monitor session session_number filter vlan vlan-id
Switch(config)# monitor session session_number filter ip access-group {access-list-number | name}
```



(注) **filter vlan** および **filter ip access-group** の両方のコマンドを同時に設定できません。一方を設定すると、他方が拒否されます。

- EtherChannel は FSPAN セッションでサポートされていません。
- TCP フラグまたは **log** キーワードが付いている FSPAN ACL はサポートされていません。
- スイッチで拡張 IP サービス フィーチャセットを稼働中に IPv6 FSPAN ACL を設定し、のちに異なるフィーチャセットを稼働した場合、スイッチのリブート後、スイッチでの IPv6 FSPAN ACL 設定が失われる可能性があります。
- IPv6 FSPAN ACL は、IPv6 対応の SDM テンプレートでだけサポートされています。IPv6 対応の SDM テンプレートを稼働中に IPv6 FSPAN ACL を設定し、のちに非 IPv6 SDM テンプレートを設定してスイッチをリブートすると、IPv6 FSPAN ACL 設定が失われます。

SPAN および RSPAN について

SPAN および RSPAN

ポートまたは VLAN を通過するネットワークトラフィックを解析するには、SPAN または RSPAN を使用して、そのスイッチ上、またはネットワークアナライザやその他のモニタデバイス、あるいはセキュリティデバイスに接続されている別のスイッチ上のポートにトラフィックのコピーを送信します。SPAN は送信元ポート上または送信元 VLAN 上で受信、送信、または送受信されたトラフィックを宛先ポートにコピー（ミラーリング）して、解析します。SPAN は送信元ポートまたは VLAN 上のネットワークトラフィックのスイッチングには影響しません。宛先ポートは SPAN 専用にする必要があります。SPAN または RSPAN セッションに必要なトラフィック以外、宛先ポートがトラフィックを受信したり転送したりすることはありません。

SPAN を使用してモニタできるのは、送信元ポートを出入りするトラフィックまたは送信元 VLAN に入入りするトラフィックだけです。送信元 VLAN にルーティングされたトラフィックはモニタできません。たとえば、着信トラフィックをモニタしている場合、別の VLAN から送信元 VLAN にルーティングされているトラフィックはモニタできません。ただし、送信元 VLAN で受信し、別の VLAN にルーティングされるトラフィックは、モニタできます。

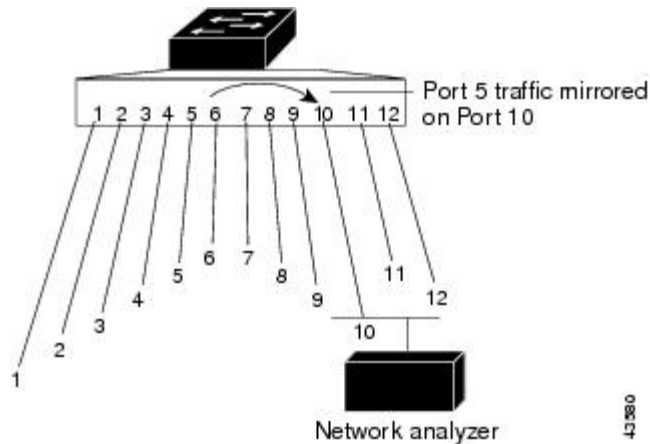
ネットワークセキュリティデバイスからトラフィックを注入する場合、SPAN または RSPAN 宛先ポートを使用できます。たとえば、Cisco 侵入検知システム（IDS）センサー装置を宛先ポートに接続した場合、IDS デバイスは TCP リセットパケットを送信して、疑わしい攻撃者の TCP セッションを停止させることができます。

ローカル SPAN

ローカル SPAN は 1 つのスイッチ内の SPAN セッション全体をサポートします。すべての送信元ポートまたは送信元 VLAN、および宛先ポートは、同じスイッチまたはスイッチスタック内にあります。ローカル SPAN は、任意の VLAN 上の 1 つまたは複数の送信元ポートからのトラフィック、あるいは 1 つまたは複数の VLAN からのトラフィックを解析するために宛先ポートへコピーします。

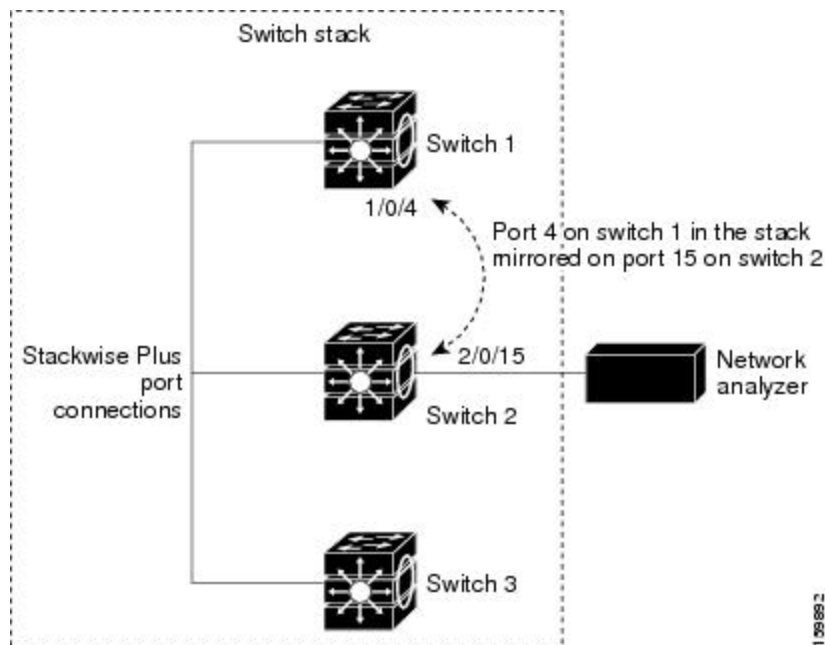
ポート 5 (送信元ポート) 上のすべてのトラフィックがポート 10 (宛先ポート) にミラーリングされます。ポート 10 のネットワークアナライザは、ポート 5 に物理的には接続されていませんが、ポート 5 からのすべてのネットワークトラフィックを受信します。

図 4: 単一デバイスでのローカル SPAN の設定例



これは、スイッチスタック内のローカル SPAN の例です。送信元ポートと宛先ポートは異なるスタックメンバにあります。

図 5: デバイスタックでのローカル SPAN の設定例

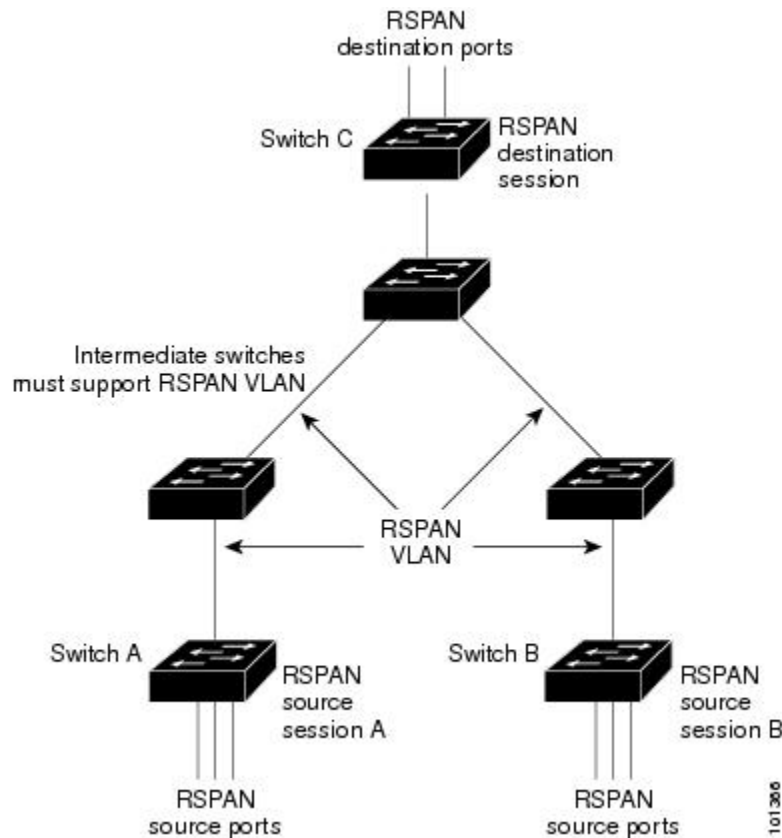


リモート SPAN

RSPANは、異なるスイッチ（または異なるスイッチスタック）上の送信元ポート、送信元VLAN、および宛先ポートをサポートしているため、ネットワーク上で複数のスイッチをリモートモニタリングできます。

次の図に、スイッチ A およびスイッチ B の送信ポートを示します。各 RSPAN セッションのトラフィックは、ユーザが指定した RSPAN VLAN 上で伝送されます。この RSPAN VLAN は、参加しているすべてのスイッチで RSPAN セッション専用です。送信元ポートまたは VLAN からの RSPAN トラフィックは RSPAN VLAN にコピーされ、RSPAN VLAN を伝送するトランクポートを介して、RSPAN VLAN をモニタする宛先セッションに転送されます。各 RSPAN 送信元スイッチには、ポートまたは VLAN のいずれかが RSPAN 送信元として必要です。図中のスイッチ C のように、宛先は常に物理ポートになります。

図 6 : RSPAN の設定例



SPAN と RSPAN の概念および用語

- [SPAN セッション](#)、31-4 ページ
- [監視対象トラフィック](#)

- 送信元ポート
- 送信元 VLAN
- VLAN フィルタリング
- 宛先ポート
- RSPAN VLAN

SPAN セッション

SPANセッション（ローカルまたはリモート）を使用すると、1つまたは複数のポート上、あるいは1つまたは複数のVLAN上でトラフィックをモニタし、そのモニタしたトラフィックを1つまたは複数の宛先ポートに送信できます。

ローカルSPANセッションは、宛先ポートと送信元ポートまたは送信元VLAN（すべて単一のネットワークデバイス上にある）を結び付けたものです。ローカルSPANには、個別の送信元および宛先のセッションはありません。ローカルSPANセッションはユーザが指定した入力および出力の packets セットを収集し、SPAN データ ストリームを形成して、宛先ポートに転送します。

RSPAN は少なくとも1つのRSPAN送信元セッション、1つのRSPAN VLAN、および少なくとも1つのRSPAN宛先セッションで構成されています。RSPAN送信元セッションとRSPAN宛先セッションは、異なるネットワークデバイス上に別々に設定します。デバイスにRSPAN送信元セッションを設定するには、一連の送信元ポートまたは送信元VLANをRSPAN VLANに関連付けます。このセッションの出力は、RSPAN VLANに送信されるSPANパケットのストリームです。別のデバイスにRSPAN宛先セッションを設定するには、宛先ポートをRSPAN VLANに関連付けます。宛先セッションはRSPAN VLANトラフィックをすべて収集し、RSPAN宛先ポートに送信します。

RSPAN送信元セッションは、パケットストリームが転送される点を除き、ローカルSPANセッションに非常に似ています。RSPAN送信元セッションでは、SPANパケットにRSPAN VLAN IDラベルが再設定され、通常のトランクポートを介して宛先スイッチに転送されます。

RSPAN宛先セッションはRSPAN VLAN上で受信されたすべてのパケットを取得し、VLANのタグングを除去し、宛先ポートに送ります。RSPAN宛先セッションの目的は、（レイヤ2制御パケットを除く）すべてのRSPAN VLANパケットを解析のためにユーザにコピーすることです。

同じRSPAN VLAN内で、複数の送信元セッションと複数の宛先セッションをアクティブにできます。RSPAN送信元セッションと宛先セッションを分離する中間スイッチを配置することもできます。これらのスイッチにはRSPANの実行機能は不要ですが、RSPAN VLANの要求に応答する必要があります。

監視対象トラフィック

SPANセッションは、次のトラフィックタイプをモニタできます。

- 受信 (Rx) SPAN : 受信（または入力）SPANは、スイッチが変更または処理を行う前に、送信元インターフェイスまたはVLANが受信したすべてのパケットをできるだけ多くモニタリングします。送信元が受信した各パケットのコピーがそのSPANセッションに対応する宛先ポートに送られます。

Diffserv コードポイント (DSCP) の変更など、ルーティングや Quality of Service (QoS) が原因で変更されたパケットは、変更される前にコピーされます。

受信処理中にパケットをドロップする可能性のある機能は、入力 SPAN には影響を与えません。宛先ポートは、実際の着信パケットがドロップされた場合でも、パケットのコピーを受信します。パケットをドロップする可能性のある機能は、標準および拡張 IP 入力アクセスコントロールリスト (ACL)、入力 QoS ポリシング、VLAN ACL、および出力 QoS ポリシングです。

- 送信 (Tx) SPAN : 送信 (または出力) SPAN は、スイッチによる変更または処理がすべて実行されたあとに、送信元インターフェイスから送信されたすべてのパケットをできる限り多くモニタリングします。送信元が送信した各パケットのコピーがその SPAN セッションに対応する宛先ポートに送られます。コピーはパケットの変更後に用意されます。

ルーティングが原因で変更されたパケット (存続可能時間 (TTL)、MAC アドレス、QoS 値の変更など) は、宛先ポートで (変更されて) コピーされます。

送信処理中にパケットをドロップする可能性のある機能は、SPAN 用の複製コピーにも影響します。これらの機能には、標準および拡張 IP 出力 ACL、出力 QoS ポリシングがあります。

- 両方 : SPAN セッションで、受信パケットと送信パケットの両方について、ポートまたは VLAN をモニタすることもできます。これはデフォルトです。

ローカル SPAN セッション ポートのデフォルト設定では、すべてのタグなしパケットが送信されます。通常、SPAN は Cisco Discovery Protocol (CDP)、VLAN トランキングプロトコル (VTP)、Dynamic Trunking Protocol (DTP)、スパンニングツリープロトコル (STP)、ポート集約プロトコル (PAgP) などのブリッジプロトコルデータユニット (BPDU) パケットおよびレイヤ 2 プロトコルをモニタしません。ただし、宛先ポートを設定するときに **encapsulation replicate** キーワードを入力すると、次の変更が発生します。

- 送信元ポートと同じカプセル化設定 (タグなし、Inter-Switch Link (ISL)、または IEEE 802.1Q) を使用して、パケットが宛先ポートに送信されます。
- BPDU やレイヤ 2 プロトコルパケットを含むすべてのタイプのパケットがモニタされます。

したがって、カプセル化レプリケーションがイネーブルにされたローカル SPAN セッションでは、タグなし、ISL、および IEEE 802.1Q タグ付きパケットが宛先ポートに混在することがあります。

スイッチの輻輳により、入力送信元ポート、出力送信元ポート、または SPAN 宛先ポートでパケットがドロップされることがあります。一般に、これらの特性は互いに無関係です。次に例を示します。

- パケットは通常どおり転送されますが、SPAN 宛先ポートのオーバーサブスクライブが原因でモニタされないことがあります。
- 入力パケットが標準転送されないにもかかわらず、SPAN 宛先ポートに着信することがあります。
- スイッチの輻輳が原因でドロップされた出力パケットは、出力 SPAN からドロップされません。

SPANの設定によっては、同一送信元のパケットのコピーが複数、SPAN宛先ポートに送信されます。たとえば、ポート A での RX モニタ、ポート B での TX モニタ用に、双方向 (RX と TX) SPAN セッションが設定されているとします。パケットがポート A からスイッチに入ってポート B にスイッチされると、着信パケットも発信パケットも宛先ポートに送信されます。このため、両方のパケットは同じものになります。レイヤ 3 書き換えが行われた場合には、パケット変更のため異なるパケットになります。

送信元ポート

送信元ポート (別名監視対象ポート) は、ネットワークトラフィック分析のために監視するスイッチドポートまたはルーテッドポートです。1つのローカル SPAN セッションまたは RSPAN 送信元セッションでは、送信元ポートまたは VLAN のトラフィックを単一方向または双方向でモニタできます。スイッチは、任意の数の送信元ポート (スイッチで利用可能なポートの最大数まで) と任意の数の送信元 VLAN (サポートされている VLAN の最大数まで) をサポートしています。ただし、スイッチが送信元ポートまたは VLAN でサポートするセッション数には上限 (ローカルまたは RSPAN) があります。単一のセッションにポートおよび VLAN を混在させることはできません。

送信元ポートの特性は、次のとおりです。

- 複数の SPAN セッションでモニタできます。
- モニタする方向 (入力、出力、または両方) を指定して、各送信元ポートを設定できます。
- すべてのポートタイプ (EtherChannel、ギガビットイーサネットなど) が可能です。
- EtherChannel 送信元の場合は、EtherChannel 全体で、または物理ポートがポートチャンネルに含まれている場合は物理ポート上で個別に、トラフィックをモニタできます。
- アクセスポート、トランクポート、ルーテッドポート、または音声 VLAN ポートに指定できます。
- 宛先ポートにすることはできません。
- 送信元ポートは同じ VLAN にあっても異なる VLAN にあってもかまいません。
- 単一セッション内で複数の送信元ポートをモニタすることが可能です。

送信元 VLAN

VLAN ベースの SPAN (VSPAN) では、1つまたは複数の VLAN のネットワークトラフィックをモニタできます。VSPAN 内の SPAN または RSPAN 送信元インターフェイスが VLAN ID となり、トラフィックはその VLAN のすべてのポートでモニタされます。

VSPAN には次の特性があります。

- 送信元 VLAN 内のすべてのアクティブポートは送信元ポートとして含まれ、単一方向または双方向でモニタできます。
- 指定されたポートでは、モニタ対象の VLAN 上のトラフィックのみが宛先ポートに送信されます。

- 宛先ポートが送信元VLANに所属する場合は、送信元リストから除外され、モニタされません。
- ポートが送信元VLANに追加または削除されると、これらのポートで受信された送信元VLANのトラフィックは、モニタ中の送信元に追加または削除されます。
- VLAN 送信元と同じセッション内のフィルタ VLAN を使用することはできません。
- モニタできるのは、イーサネット VLAN だけです。

VLAN フィルタリング

トランク ポートを送信元ポートとしてモニタする場合、デフォルトでは、トランク上でアクティブなすべてのVLANがモニタされます。VLAN フィルタリングを使用して、トランク送信元ポートでのSPAN トラフィックのモニタ対象を特定のVLANに制限できます。

- VLAN フィルタリングが適用されるのは、トランク ポートまたは音声 VLAN ポートのみです。
- VLAN フィルタリングはポートベースセッションにのみ適用され、VLAN 送信元によるセッションでは使用できません。
- VLAN フィルタ リストが指定されている場合、トランク ポートまたは音声 VLAN アクセスポートではリスト内の該当VLANのみがモニタされます。
- 他のポートタイプから着信するSPAN トラフィックは、VLAN フィルタリングの影響を受けません。つまり、すべてのVLANを他のポートで使用できます。
- VLAN フィルタリング機能は、宛先SPAN ポートに転送されたトラフィックにのみ作用し、通常のトラフィックのスイッチングには影響を与えません。

宛先ポート

各ローカルSPAN セッションまたはRSPAN 宛先セッションには、送信元ポートおよびVLANからのトラフィックのコピーを受信し、SPAN パケットをユーザ（通常はネットワークアナライザ）に送信する宛先ポート（別名モニタ側ポート）が必要です。

宛先ポートの特性は、次のとおりです。

- ローカルSPAN セッションの場合、宛先ポートは送信元ポートと同じスイッチまたはスイッチスタックに存在する必要があります。RSPAN セッションの場合は、RSPAN 宛先セッションを含むスイッチ上にあります。RSPAN 送信元セッションのみを実行するスイッチまたはスイッチスタックには、宛先ポートはありません。
- ポートをSPAN 宛先ポートとして設定すると、元のポート設定が上書きされます。SPAN 宛先設定を削除すると、ポートは以前の設定に戻ります。ポートがSPAN 宛先ポートとして機能している間にポートの設定が変更されると、SPAN 宛先設定が削除されるまで、変更は無効になりません。



(注) SPAN の宛先ポートに QoS が設定されている場合、QoS はただちに有効になります。

- ポートが EtherChannel グループに含まれていた場合、そのポートが宛先ポートとして設定されている間、グループから削除されます。削除されたポートがルーテッドポートであった場合、このポートはルーテッドポートでなくなります。
- 任意のイーサネット物理ポートにできます。
- セキュアポートにすることはできません。
- 送信元ポートにすることはできません。
- EtherChannel グループまたは VLAN にすることはできません。
- 一度に 1 つの SPAN セッションにしか参加できません (ある SPAN セッションの宛先ポートは、別の SPAN セッションの宛先ポートになることはできません)。
- アクティブな場合、着信トラフィックはディセーブルになります。ポートは SPAN セッションに必要なトラフィック以外は送信しません。宛先ポートでは着信トラフィックを学習したり、転送したりしません。
- 入力トラフィック転送がネットワークセキュリティデバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。
- レイヤ 2 プロトコル (STP、VTP、CDP、DTP、PAgP) のいずれにも参加しません。
- 任意の SPAN セッションの送信元 VLAN に所属する宛先ポートは、送信元リストから除外され、モニタされません。
- スイッチまたはスイッチ スタックの宛先ポートの最大数は 64 です。

ローカル SPAN および RSPAN 宛先ポートは、VLAN タギングおよびカプセル化で次のように動作が異なります。

- ローカル SPAN では、宛先ポートに **encapsulation replicate** キーワードが指定されている場合、各パケットに元のカプセル化が使用されます (タグなし、ISL、または IEEE 802.1Q)。これらのキーワードが指定されていない場合、パケットはタグなしフォーマットになります。したがって、**encapsulation replicate** がイネーブルになっているローカル SPAN セッションの出力に、タグなし、ISL、または IEEE 802.1Q タグ付きパケットが混在することがあります。
- RSPAN の場合は、元の VLAN ID は RSPAN VLAN ID で上書きされるため失われます。したがって、宛先ポート上のすべてのパケットはタグなしになります。

RSPAN VLAN

RSPAN VLAN は、RSPAN の送信元セッションと宛先セッション間で SPAN トラフィックを伝送します。RSPAN VLAN には、次の特性があります。

- RSPAN VLAN 内のすべてのトラフィックは、常にフラッディングされます。
- RSPAN VLAN では MAC アドレスは学習されません。
- RSPAN VLAN トラフィックが流れるのは、トランク ポート上のみです。
- RSPAN VLAN は、**remote-span VLAN** コンフィギュレーションモードコマンドを使用して、VLAN コンフィギュレーション モードで設定する必要があります。
- STP は RSPAN VLAN トランク上で実行できますが、SPAN 宛先ポート上では実行できません。
- RSPAN VLAN を、プライベート VLAN のプライマリまたはセカンダリ VLAN にはできません。

VLAN トランキング プロトコル (VTP) に対して可視である VLAN 1 ~ 1005 の場合、VLAN ID および対応する RSPAN 特性は VTP によって伝播されます。拡張 VLAN 範囲 (1006 ~ 4094) 内の RSPAN VLAN ID を割り当てる場合は、すべての中間スイッチを手動で設定する必要があります。

通常は、ネットワークに複数の RSPAN VLAN を配置し、それぞれの RSPAN VLAN でネットワーク全体の RSPAN セッションを定義します。つまり、ネットワーク内の任意の場所にある複数の RSPAN 送信元セッションで、パケットを RSPAN セッションに送信できます。また、ネットワーク全体に対して複数の RSPAN 宛先セッションを設定し、同じ RSPAN VLAN をモニタしたり、ユーザにトラフィックを送信したりできます。セッションは RSPAN VLAN ID によって区別されます。

SPAN および RSPAN と他の機能の相互作用

SPAN は次の機能と相互に作用します。

- ルーティング：SPAN はルーテッドトラフィックを監視しません。VSPAN が監視するのはスイッチに出入りするトラフィックに限られ、VLAN 間でルーティングされるトラフィックは監視しません。たとえば、VLAN が受信モニタされ、スイッチが別の VLAN から監視対象 VLAN にトラフィックをルーティングする場合、そのトラフィックは監視されず、SPAN 宛先ポートで受信されません。
- STP：SPAN または RSPAN セッションがアクティブな間、宛先ポートは STP に参加しません。SPAN または RSPAN セッションがディセーブルになると、宛先ポートは STP に参加できます。送信元ポートでは、SPAN は STP ステータスに影響を与えません。STP は RSPAN VLAN を伝送するトランク ポート上でアクティブにできます。
- CDP：SPAN セッションがアクティブな間、SPAN 宛先ポートは CDP に参加しません。SPAN セッションがディセーブルになると、ポートは再び CDP に参加します。
- VTP：VTP を使用すると、スイッチ間で RSPAN VLAN のプルーニングが可能です。
- VLAN および トランキング：送信元ポート、または宛先ポートの VLAN メンバーシップまたはトランクの設定値を、いつでも変更できます。ただし、宛先ポートの VLAN メンバーシップまたはトランクの設定値に対する変更が有効になるのは、SPAN 宛先設定を削除してから

です。送信元ポートの VLAN メンバーシップまたはトランクの設定値に対する変更は、ただちに有効になり、対応する SPAN セッションが変更に応じて自動的に調整されます。

- **EtherChannel** : EtherChannel グループを送信元ポートとして設定することはできますが、SPAN 宛先ポートとして設定することはできません。グループが SPAN 送信元として設定されている場合、グループ全体がモニタされます。

モニタ対象の EtherChannel グループに物理ポートを追加すると、SPAN 送信元ポートリストに新しいポートが追加されます。モニタ対象の EtherChannel グループからポートを削除すると、送信元ポートリストからそのポートが自動的に削除されます。

EtherChannel グループに所属する物理ポートを SPAN 送信元ポートとして設定し、引き続き EtherChannel の一部とすることができます。この場合、この物理ポートは EtherChannel に参加しているため、そのポートからのデータはモニタされます。ただし、EtherChannel グループに含まれる物理ポートを SPAN 宛先として設定した場合、その物理ポートはグループから削除されます。SPAN セッションからそのポートが削除されると、EtherChannel グループに再加入します。EtherChannel グループから削除されたポートは、グループメンバのままですが、inactive または suspended ステートになります。

EtherChannel グループに含まれる物理ポートが宛先ポートであり、その EtherChannel グループが送信元の場合、ポートは EtherChannel グループおよびモニタ対象ポートリストから削除されます。

- マルチキャストトラフィックをモニタできます。出力ポートおよび入力ポートのモニタでは、未編集の packets が 1 つだけ SPAN 宛先ポートに送信されます。マルチキャスト packets の送信回数は反映されません。
- プライベート VLAN ポートは、SPAN 宛先ポートには設定できません。
- セキュアポートを SPAN 宛先ポートにすることはできません。

SPAN セッションでは、入力転送が宛先ポートでイネーブルの場合、出力をモニタしているポートでポートセキュリティをイネーブルにしないでください。RSPAN 送信元セッションでは、出力をモニタしているポートでポートセキュリティをイネーブルにしないでください。

- IEEE 802.1x ポートは SPAN 送信元ポートにできます。SPAN 宛先ポート上で IEEE 802.1x をイネーブルにできますが、SPAN 宛先としてこのポートを削除するまで、IEEE 802.1x はディセーブルに設定されます。

SPAN セッションでは、入力転送が宛先ポートでイネーブルの場合、出力をモニタしているポートで IEEE 802.1x をイネーブルにしないでください。RSPAN 送信元セッションでは、出力をモニタしているポートで IEEE 802.1x をイネーブルにしないでください。

SPAN と RSPAN とデバイススタック

スイッチのスタックは 1 つの論理スイッチを表すため、ローカル SPAN の送信元ポートおよび宛先ポートは、スタック内の異なるスイッチである場合があります。したがって、スタック内でのスイッチの追加または削除は、RSPAN の送信元セッションまたは宛先セッションだけではなく、ローカル SPAN セッションにも影響を及ぼします。スイッチがスタックから削除されると、アク

タイプセッションが非アクティブになります。また、スイッチがスタックに追加されると、非アクティブセッションがアクティブになります。

フローベースの SPAN

送信元ポートで監視されるトラフィックにアクセスコントロールリスト (ACL) を適用するフローベース SPAN (FSPAN) またはフローベース RSPAN (FRSPAN) を使用して、SPAN または RSPAN で監視するネットワークトラフィックのタイプを制御できます。FSPAN ACL は、IPv4、IPv6、および監視される非 IP トラフィックをフィルタリングするように設定できます。

インターフェイスを通して ACL を SPAN セッションに適用します。ACL は SPAN セッション内のすべてのインターフェイスで監視されるすべてのトラフィックに適用されます。この ACL によって許可されるパケットは、SPAN 宛先ポートにコピーされます。ほかのパケットは SPAN 宛先ポートにコピーされません。

元のトラフィックは継続して転送され、接続している任意のポート、VLAN、およびルータ ACL が適用されます。FSPAN ACL は転送の決定に影響を与えることはありません。同様に、ポート、VLAN、およびルータ ACL は、トラフィックのモニタリングに影響を与えません。セキュリティ入力 ACL がパケットを拒否したために転送されない場合でも、FSPAN ACL が許可すると、パケットは SPAN 宛先ポートにコピーされます。しかし、セキュリティ出力 ACL がパケットを拒否したために転送されない場合、パケットは SPAN 宛先ポートにコピーされません。ただし、セキュリティ出力 ACL がパケットの送信を許可した場合だけ、パケットは、FSPAN ACL が許可した場合 SPAN 宛先ポートにコピーされます。これは RSPAN セッションについてもあてはまります。

SPAN セッションには、次の 3 つのタイプの FSPAN ACL を接続できます。

- IPv4 FSPAN ACL : IPv4 パケットだけをフィルタリングします。
- IPv6 FSPAN ACL : IPv6 パケットだけをフィルタリングします。
- MAC FSPAN ACL : IP パケットだけをフィルタリングします。

セキュリティ ACL は、スイッチ上の FSPAN ACL よりも高いプライオリティをもっています。FSPAN ACL が適用され、その後ハードウェアメモリに収まらないセキュリティ ACL を追加する場合、適用された FSPAN ACL は、セキュリティ ACL のスペースを確保するためにメモリから削除されます。この処理 (アンローディングと呼ばれる) は、システムメッセージにより通知されます。メモリ内に常駐するスペースが確保できたら、スイッチ上のハードウェアメモリに FSPAN ACL が追加されます。この処理 (リローディングと呼ばれる) は、システムメッセージにより通知されます。IPv4、IPv6、および MAC FSPAN ACL は、別個にアンロードまたはリロードできます。

スタックに設定された VLAN ベースの FSPAN セッションが 1 つまたは複数のスイッチ上のハードウェアメモリに収まらない場合、セッションはこれらのスイッチ上でアンロードされたものとして処理され、スイッチでの FSPAN ACL およびソーシングのためのトラフィックは、SPAN 宛先ポートにコピーされません。FSPAN ACL は継続して正しく適用され、トラフィックは FSPAN ACL がハードウェアメモリに収まるスイッチの SPAN 宛先ポートにコピーされます。

空の FSPAN ACL が接続されると、一部のハードウェア機能により、その ACL の SPAN 宛先ポートにすべてのトラフィックがコピーされます。十分なハードウェア リソースが使用できない場合、空の FSPAN ACL もアンロードされる可能性があります。

IPv4 および MAC FSPAN ACL は、すべてのフィーチャセットでサポートされています。IPv6 FSPAN ACL は、拡張 IP Services フィーチャセットでだけサポートされています。

SPAN および RSPAN のデフォルト設定

表 12: SPAN および RSPAN のデフォルト設定

機能	デフォルト設定
SPAN のステート (SPAN および RSPAN)	ディセーブル
モニタする送信元ポート トラフィック	受信トラフィックと送信トラフィックの両方 (both)
カプセル化タイプ (宛先ポート)	ネイティブ形式 (タグなしパケット)
入力転送 (宛先ポート)	ディセーブル
VLAN フィルタリング	送信元ポートとして使用されるトランク インターフェイス上では、すべての VLAN がモニタリングされます。
RSPAN VLAN	未設定

設定時の注意事項

SPAN 設定時の注意事項

- SPAN セッションから送信元ポート、宛先ポート、または VLAN を削除する場合は、**no monitor session session_number source {interface interface-id | vlan vlan-id}** グローバル コンフィギュレーション コマンドまたは **no monitor session session_number destination interface interface-id** グローバル コンフィギュレーション コマンドを使用します。宛先インターフェイスの場合、このコマンドの **no** 形式では、**encapsulation** オプションは無視されます。
- トランク ポート上のすべての VLAN をモニタするには、**no monitor session session_number filter** グローバル コンフィギュレーション コマンドを使用します。

RSPAN 設定時の注意事項

- すべての SPAN 設定時の注意事項が RSPAN に適用されます。
- RSPAN VLAN には特性があるので、RSPAN VLAN として使用するためにネットワーク上の VLAN をいくつか確保し、それらの VLAN にはアクセス ポートを割り当てないでおく必要があります。
- RSPAN トラフィックに出力 ACL を適用して、特定の packets を選択的にフィルタリングまたはモニタできます。RSPAN 送信元スイッチ内の RSPAN VLAN 上で、これらの ACL を指定します。
- RSPAN を設定する場合は、送信元ポートおよび宛先ポートをネットワーク内の複数のスイッチに分散させることができます。
- RSPAN VLAN 上のアクセス ポート（音声 VLAN ポートを含む）は、非アクティブ状態になります。
- 次の条件を満たす限り、任意の VLAN を RSPAN VLAN として設定できます。
 - すべてのスイッチで、RSPAN セッションに同じ RSPAN VLAN が使用されている。
 - 参加しているすべてのスイッチで RSPAN がサポートされている。

FSPAN および FRSPAN 設定時の注意事項

- 少なくとも 1 つの FSPAN ACL が接続されている場合、FSPAN はイネーブルになります。
- SPAN セッションに空ではない FSPAN ACL を少なくとも 1 つ接続し、ほかの 1 つまたは複数の FSPAN ACL を接続しなかった場合（たとえば、空ではない IPv4 ACL を接続し、IPv6 と MAC ACL を接続しなかった場合）、FSPAN は、接続されていない ACL によってフィルタリングされたと思われるトラフィックをブロックします。したがって、このトラフィックは監視されません。

SPAN および RSPAN の設定方法

ローカル SPAN セッションの作成

SPAN セッションを作成し、送信元（モニタ対象）ポートまたは VLAN、および宛先（モニタ側）ポートを指定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **no monitor session** {*session_number* | **all** | **local** | **remote**}
3. **monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [,|-] [**both** | **rx** | **tx**]
4. **monitor session** *session_number* **destination** {**interface** *interface-id* [,|-] [**encapsulation replicate**]}
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no monitor session { <i>session_number</i> all local remote } 例： Switch(config)# no monitor session all	セッションに対する既存の SPAN 設定を削除します。 <ul style="list-style-type: none"> • <i>session_number</i> の範囲は、1 ~ 66 です。 • all : すべての SPAN セッションを削除します。 • local : すべてのローカルセッションを削除します。 • remote : すべてのリモート SPAN セッションを削除します。
ステップ 3	monitor session <i>session_number</i> source { interface <i>interface-id</i> vlan <i>vlan-id</i> } [, -] [both rx tx] 例： Switch(config)# monitor session 1 source interface gigabitethernet1/0/1	SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 <ul style="list-style-type: none"> • <i>session_number</i> の範囲は、1 ~ 66 です。 • <i>interface-id</i> には、監視する送信元ポートまたは送信元 VLAN を指定します。 • 送信元 <i>interface-id</i> には、モニタする送信元ポートを指定します。物理インターフェイスだけが有効です。 • <i>vlan-id</i> には、モニタする送信元 VLAN を指定します。指定できる範囲は 1 ~ 4094 です（RSPAN VLAN は除く）。 (注) 1つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1つのセッション内では送信元ポートと送信元 VLAN を併用できません。 • (任意) [, -] は、一連または一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを1つずつ入力します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • (任意) モニタリングするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、SPAN は送信トラフィックと受信トラフィックの両方をモニタします。 • both : 送信トラフィックと受信トラフィックの両方をモニタします。これはデフォルトです。 • rx : 受信トラフィックをモニタします。 • tx : 送信トラフィックをモニタします。 <p>(注) monitor session session_number source コマンドを複数回使用すると、複数の送信元ポートを設定できます。</p>
ステップ 4	<p>monitor session session_number destination {interface interface-id [, -] [encapsulation replicate]}</p> <p>例 :</p> <pre>Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2 encapsulation replicate</pre>	<p>SPAN セッションおよび宛先ポート (モニタ側ポート) を指定します。</p> <p>(注) ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。</p> <ul style="list-style-type: none"> • session_number には、ステップ 3 で入力したセッション番号を指定します。 • interface-id には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 • (任意) [, -] は、一連または一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 <p>(任意) encapsulation replicate は、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式 (タグなし) でのパケットの送信です。</p> <p>(注) monitor session session_number destination コマンドを複数回使用すると、複数の宛先ポートを設定できます。</p>
ステップ 5	<p>end</p> <p>例 :</p> <pre>Switch(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>

ローカル SPAN セッションの作成および着信トラフィックの設定

SPAN セッションを作成し、さらに送信元ポートまたは VLAN および宛先ポートを指定した後、宛先ポートでネットワーク セキュリティ デバイス (Cisco IDS センサー装置等) 用に着信トラフィックをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **no monitor session** {*session_number* | **all** | **local** | **remote**}
3. **monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [, | -] [**both** | **rx** | **tx**]
4. **monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation replicate**] [**ingress** {**dot1q vlan** *vlan-id* | **isl** | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]}
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no monitor session { <i>session_number</i> all local remote }	セッションに対する既存の SPAN 設定を削除します。 • <i>session_number</i> の範囲は、1 ~ 66 です。 • all : すべての SPAN セッションを削除します。 • local : すべてのローカル セッションを削除します。 • remote : すべてのリモート SPAN セッションを削除します。
ステップ 3	monitor session <i>session_number</i> source { interface <i>interface-id</i> vlan <i>vlan-id</i> } [, -] [both rx tx] 例： Switch(config)# monitor session 2 source gigabitethernet1/0/1 rx	SPAN セッションおよび送信元ポート (モニタ対象ポート) を指定します。
ステップ 4	monitor session <i>session_number</i> destination { interface <i>interface-id</i> [, -] [encapsulation replicate] [ingress { dot1q vlan <i>vlan-id</i> isl untagged vlan <i>vlan-id</i> vlan <i>vlan-id</i> }]}	SPAN セッション、宛先ポート、パケットカプセル化、および入力 VLAN とカプセル化を指定します。 • <i>session_number</i> には、ステップ 3 で入力したセッション番号を指定します。

	コマンドまたはアクション	目的
	<p>例 :</p> <pre>Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate ingress dot1q vlan 6</pre>	<ul style="list-style-type: none"> • interface-id には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 • (任意) [, -] は、一連または一定範囲のインターフェイスを指定します。カンマまたはハイフンの前後にスペースを1つずつ入力します。 • (任意) encapsulation replicate は、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式 (タグなし) でのパケットの送信です。 • ingress は、宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定します。 <ul style="list-style-type: none"> ◦ dot1q vlan vlan-id : デフォルトの VLAN として指定した VLAN で、IEEE 802.1Q でカプセル化された着信パケットを受信します。 ◦ isl : ISLカプセル化を使用して入力パケットを転送します。 ◦ untagged vlan vlan-id または vlan vlan-id : デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを受信します。 • dot1q vlan vlan-id : デフォルトの VLAN として指定した VLAN で、IEEE 802.1Q でカプセル化された着信パケットを受信します。 • isl : ISLカプセル化を使用して着信パケットを転送します。 • untagged vlan vlan-id または vlan vlan-id : デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを受信します。
ステップ 5	<p>end</p> <p>例 :</p> <pre>Switch(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>

フィルタリングする VLAN の指定

SPAN 送信元トラフィックを特定の VLAN に制限するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **no monitor session** {*session_number* | **all** | **local** | **remote**}
3. **monitor session** *session_number* **source interface** *interface-id*
4. **monitor session** *session_number* **filter vlan** *vlan-id* [, | -]
5. **monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation replicate**]}
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no monitor session { <i>session_number</i> all local remote }	セッションに対する既存の SPAN 設定を削除します。 • <i>session_number</i> の範囲は、1 ~ 66 です。 • all : すべての SPAN セッションを削除します。 • local : すべてのローカルセッションを削除します。 • remote : すべてのリモート SPAN セッションを削除します。
ステップ 3	monitor session <i>session_number</i> source interface <i>interface-id</i> 例： Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx	送信元ポート（モニタ対象ポート）と SPAN セッションの特性を指定します。 • <i>session_number</i> の範囲は、1 ~ 66 です。 • <i>interface-id</i> には、モニタする送信元ポートを指定します。指定したインターフェイスは、あらかじめトランクポートとして設定しておく必要があります。
ステップ 4	monitor session <i>session_number</i> filter vlan <i>vlan-id</i> [, -]	SPAN 送信元トラフィックを特定の VLAN に制限します。 • <i>session_number</i> には、ステップ 3 で指定したセッション番号を入力します。

	コマンドまたはアクション	目的
	例 : <pre>Switch(config)# monitor session 2 filter vlan 1 - 5 , 9</pre>	<ul style="list-style-type: none"> • <i>vlan-id</i> に指定できる範囲は 1 ~ 4094 です。 • (任意) カンマ (,) を使用して一連の VLAN を指定するか、ハイフン (-) を使用して VLAN 範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 5	<pre>monitor session <i>session_number</i> destination {interface <i>interface-id</i> [, -] [encapsulation replicate]}</pre> 例 : <pre>Switch(config)# monitor session 2 destination interface gigabitethernet1/0/1</pre>	SPAN セッションおよび宛先ポート (モニタ側ポート) を指定します。 <ul style="list-style-type: none"> • <i>session_number</i> には、ステップ 3 で入力したセッション番号を指定します。 • <i>interface-id</i> には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 • (任意) [, -] は、一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • (任意) encapsulation replicate は、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式 (タグなし) でのパケットの送信です。
ステップ 6	<pre>end</pre> 例 : <pre>Switch(config)# end</pre>	特権 EXEC モードに戻ります。

RSPAN VLAN としての VLAN の設定

最初に、RSPAN セッションの RSPAN VLAN となる VLAN を新規に作成します。

新しい VLAN を作成し、RSPAN セッション用の RSPAN VLAN になるように設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **vlan *vlan-id***
3. **remote-span**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vlan <i>vlan-id</i> 例： Switch(config)# vlan 100	VLAN ID を入力して VLAN を作成するか、または既存の VLAN の VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。指定できる範囲は 2 ~ 1001 または 1006 ~ 4094 です。 RSPAN VLAN を VLAN 1 (デフォルト VLAN) または VLAN ID 1002 ~ 1005 (トークンリングおよび FDDI VLAN 専用) にすることはできません。
ステップ 3	remote-span 例： Switch(config-vlan)# remote-span	VLAN を RSPAN VLAN として設定します。
ステップ 4	end 例： Switch(config-vlan)# end	特権 EXEC モードに戻ります。

次の作業

RSPAN に参加するすべてのスイッチに RSPAN VLAN を作成する必要があります。RSPAN VLAN ID が標準範囲 (1005 未満) であり、VTP がネットワーク内でイネーブルである場合は、1 つのスイッチに RSPAN VLAN を作成し、VTP がこの RSPAN VLAN を VTP ドメイン内の他のスイッチに伝播するように設定できます。拡張範囲 VLAN (1005 を超える ID) の場合、送信元と宛先の両方のスイッチ、および中間スイッチに RSPAN VLAN を設定する必要があります。

VTP プルーニングを使用して、RSPAN トラフィックが効率的に流れるようにするか、または RSPAN トラフィックの伝送が不要なすべてのトランクから、RSPAN VLAN を手動で削除します。

VLAN からリモート SPAN 特性を削除して、標準 VLAN に戻すように変換するには、**no remote-span** VLAN コンフィギュレーション コマンドを使用します。

SPAN セッションから送信元ポートまたは VLAN を削除するには、**no monitor session session_number source {interface interface-id | vlan vlan-id}** グローバル コンフィギュレーション コマンドを使用します。セッションから RSPAN VLAN を削除するには、**no monitor session session_number destination remote vlan vlan-id** コマンドを使用します。

RSPAN 送信元セッションの作成

RSPAN 送信元セッションを作成および開始し、モニタ対象の送信元および宛先 RSPAN VLAN を指定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **no monitor session {session_number | all | local | remote}**
3. **monitor session session_number source {interface interface-id | vlan vlan-id} [,|-] [both | rx | tx]**
4. **monitor session session_number destination remote vlan vlan-id**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no monitor session {session_number all local remote} 例： Switch(config)# no monitor session 1	セッションに対する既存の SPAN 設定を削除します。 <ul style="list-style-type: none"> • session_number の範囲は、1 ～ 66 です。 • all : すべての SPAN セッションを削除します。 • local : すべてのローカルセッションを削除します。 • remote : すべてのリモート SPAN セッションを削除します。
ステップ 3	monitor session session_number source {interface interface-id vlan vlan-id} [, -] [both rx tx] 例： Switch(config)# monitor session	RSPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 <ul style="list-style-type: none"> • session_number の範囲は、1 ～ 66 です。 • RSPAN セッションの送信元ポートまたは送信元 VLAN を入力します。

	コマンドまたはアクション	目的
	<pre>1 source interface gigabitethernet1/0/1 tx</pre>	<ul style="list-style-type: none"> ◦ <i>interface-id</i> には、モニタリングする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポートチャネル論理インターフェイス (port-channel <i>port-channel-number</i>) があります。有効なポートチャネル番号は 1 ~ 48 です。 ◦ <i>vlan-id</i> には、モニタする送信元 VLAN を指定します。指定できる範囲は 1 ~ 4094 です (RSPAN VLAN は除く)。 <p>1 つのセッションに、一連のコマンドで定義された複数の送信元 (ポートまたは VLAN) を含めることができます。ただし、1 つのセッション内で送信元ポートと送信元 VLAN を併用することはできません。</p> <ul style="list-style-type: none"> • (任意) [<i>, -</i>] は、一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • (任意) both rx tx は、モニタリングするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、送信元インターフェイスは送信トラフィックと受信トラフィックの両方を送信します。 <ul style="list-style-type: none"> ◦ both : 送信トラフィックと受信トラフィックの両方をモニタします。 ◦ rx : 受信トラフィックをモニタします。 ◦ tx : 送信トラフィックをモニタします。
ステップ 4	<pre>monitor session session_number destination remote vlan vlan-id</pre> <p>例 :</p> <pre>Switch(config)# monitor session 1 destination remote vlan 100</pre>	<p>RSPAN セッション、宛先 RSPAN VLAN、および宛先ポートグループを指定します。</p> <ul style="list-style-type: none"> • <i>session_number</i> には、ステップ 3 で指定した番号を入力します。 • <i>vlan-id</i> には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 5	<pre>end</pre> <p>例 :</p> <pre>Switch(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>

フィルタリングする VLAN の指定

RSPAN 送信元トラフィックを特定の VLAN に制限するように RSPAN 送信元セッションを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **no monitor session** {*session_number* | **all** | **local** | **remote**}
3. **monitor session** *session_number* **source interface** *interface-id*
4. **monitor session** *session_number* **filter vlan** *vlan-id* [, |-]
5. **monitor session** *session_number* **destination remote vlan** *vlan-id*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no monitor session { <i>session_number</i> all local remote }	セッションに対する既存の SPAN 設定を削除します。 • <i>session_number</i> の範囲は、1 ~ 66 です。 • all : すべての SPAN セッションを削除します。 • local : すべてのローカル セッションを削除します。 • remote : すべてのリモート SPAN セッションを削除します。
ステップ 3	monitor session <i>session_number</i> source interface <i>interface-id</i> 例： Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx	送信元ポート（モニタ対象ポート）と SPAN セッションの特性を指定します。 • <i>session_number</i> の範囲は、1 ~ 66 です。 • <i>interface-id</i> には、モニタする送信元ポートを指定します。指定したインターフェイスは、あらかじめトランクポートとして設定しておく必要があります。
ステップ 4	monitor session <i>session_number</i> filter vlan <i>vlan-id</i> [, -]	SPAN 送信元トラフィックを特定の VLAN に制限します。 • <i>session_number</i> には、ステップ 3 で指定したセッション番号を入力します。

	コマンドまたはアクション	目的
	例 : <pre>Switch(config)# monitor session 2 filter vlan 1 - 5 , 9</pre>	<ul style="list-style-type: none"> • <i>vlan-id</i> に指定できる範囲は 1 ~ 4094 です。 • (任意) , - : カンマ (,) を使用して一連の VLAN を指定するか、ハイフン (-) を使用して VLAN 範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 5	<pre>monitor session session_number destination remote vlan vlan-id</pre> 例 : <pre>Switch(config)# monitor session 2 destination remote vlan 902</pre>	RSPAN セッションおよび宛先リモート VLAN (RSPAN VLAN) を指定します。 <ul style="list-style-type: none"> • <i>session_number</i> には、ステップ 3 で指定したセッション番号を入力します。 • <i>vlan-id</i> には、宛先ポートにモニタ対象トラフィックを伝送する RSPAN VLAN を指定します。
ステップ 6	<pre>end</pre> 例 : <pre>Switch(config)# end</pre>	特権 EXEC モードに戻ります。

RSPAN 宛先セッションの作成

RSPAN 宛先セッションは、別のスイッチまたはスイッチ スタック（送信元セッションが設定されていないスイッチまたはスイッチ スタック）に設定します。

このスイッチ上で RSPAN VLAN を定義し、RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **vlan *vlan-id***
3. **remote-span**
4. **exit**
5. **no monitor session {*session_number* | all | local | remote}**
6. **monitor session *session_number* source remote vlan *vlan-id***
7. **monitor session *session_number* destination interface *interface-id***
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vlan <i>vlan-id</i> 例： Switch(config)# vlan 901	送信元スイッチで作成された RSPAN VLAN の VLAN ID を指定し、VLAN コンフィギュレーション モードを開始します。 両方のスイッチが VTP に参加し、RSPAN VLAN ID が 2 ~ 1005 である場合は、VTP ネットワークを介して RSPAN VLAN ID が伝播されるため、ステップ 2 ~ 4 は不要です。
ステップ 3	remote-span 例： Switch(config-vlan)# remote-span	VLAN を RSPAN VLAN として識別します。
ステップ 4	exit 例： Switch(config-vlan)# exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	no monitor session {<i>session_number</i> all local remote} 例： Switch(config)# no monitor session 1	セッションに対する既存の SPAN 設定を削除します。 <ul style="list-style-type: none"> • <i>session_number</i> の範囲は、1 ~ 66 です。 • all : すべての SPAN セッションを削除します。 • local : すべてのローカルセッションを削除します。 • remote : すべてのリモート SPAN セッションを削除します。
ステップ 6	monitor session <i>session_number</i> source remote vlan <i>vlan-id</i> 例： Switch(config)# monitor session 1 source remote vlan 901	RSPAN セッションと送信元 RSPAN VLAN を指定します。 <ul style="list-style-type: none"> • <i>session_number</i> の範囲は、1 ~ 66 です。 • <i>vlan-id</i> には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 7	monitor session <i>session_number</i> destination interface <i>interface-id</i> 例： Switch(config)# monitor session 1	RSPAN セッションと宛先インターフェイスを指定します。 <ul style="list-style-type: none"> • <i>session_number</i> には、ステップ 6 で指定した番号を入力します。

	コマンドまたはアクション	目的
	<pre>destination interface gigabitethernet2/0/1</pre>	<ul style="list-style-type: none"> • RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 • <i>interface-id</i> には、宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。 • encapsulation replicate はコマンドラインのヘルプストリングに表示されますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。
ステップ 8	<pre>end</pre> <p>例 :</p> <pre>Switch(config)# end</pre>	特権 EXEC モードに戻ります。

RSPAN 宛先セッションの作成および着信トラフィックの設定

RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定し、宛先ポートでネットワークセキュリティ デバイス (Cisco IDS センサー装置等) 用に着信トラフィックをイーネブルにするには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **no monitor session** {*session_number* | **all** | **local** | **remote**}
3. **monitor session** *session_number* **source remote vlan** *vlan-id*
4. **monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**ingress** {**dot1q vlan** *vlan-id* | **isl** | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]}
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>Switch# configure terminal</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no monitor session {session_number all local remote} 例： <pre>Switch(config)# no monitor session 2</pre>	セッションに対する既存の SPAN 設定を削除します。 <ul style="list-style-type: none"> • session_number の範囲は、1 ~ 66 です。 • all : すべての SPAN セッションを削除します。 • local : すべてのローカルセッションを削除します。 • remote : すべてのリモート SPAN セッションを削除します。
ステップ 3	monitor session session_number source remote vlan vlan-id 例： <pre>Switch(config)# monitor session 2 source remote vlan 901</pre>	RSPAN セッションと送信元 RSPAN VLAN を指定します。 <ul style="list-style-type: none"> • session_number の範囲は、1 ~ 66 です。 • vlan-id には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 4	monitor session session_number destination {interface interface-id [, -] [ingress {dot1q vlan vlan-id isl untagged vlan vlan-id vlan vlan-id}}} 例： <pre>Switch(config)# monitor session 2 destination interface gigabitEthernet1/0/2 ingress vlan 6</pre>	SPAN セッション、宛先ポート、パケット カプセル化、および着信 VLAN とカプセル化を指定します。 <ul style="list-style-type: none"> • session_number には、ステップ 4 で指定した番号を入力します。RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 • interface-id には、宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。 • encapsulation replicate はコマンドラインのヘルプ ストリングに表示されますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。 • (任意) [, -] は、一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • 宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定するには、ingress を追加のキーワードと一緒に入力します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> ◦ dot1q vlan <i>vlan-id</i> : デフォルトの VLAN として指定した VLAN で、IEEE 802.1Q でカプセル化された着信パケットを転送します。 ◦ isl : ISL カプセル化を使用して入力パケットを転送します。 ◦ untagged vlan <i>vlan-id</i> または vlan <i>vlan-id</i> : デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを転送します。
ステップ 5	end 例 : Switch(config)# end	特権 EXEC モードに戻ります。

FSPAN セッションの設定

SPAN セッションを作成し、送信元（監視対象）ポートまたは VLAN、および宛先（モニタ側）ポートを指定し、セッションに FSPAN を設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **no monitor session** {*session_number* | **all** | **local** | **remote**}
3. **monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [, | -] [**both** | **rx** | **tx**]
4. **monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation replicate**]}
5. **monitor session** *session_number* **filter** {**ip** | **ipv6** | **mac**} **access-group** {*access-list-number* | *name*}
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	<p>no monitor session {<i>session_number</i> all local remote}</p> <p>例 :</p> <pre>Switch(config)# no monitor session 2</pre>	<p>セッションに対する既存の SPAN 設定を削除します。</p> <ul style="list-style-type: none"> • <i>session_number</i> の範囲は、1 ~ 66 です。 • all : すべての SPAN セッションを削除します。 • local : すべてのローカルセッションを削除します。 • remote : すべてのリモート SPAN セッションを削除します。
ステップ 3	<p>monitor session <i>session_number</i> source {interface <i>interface-id</i> vlan <i>vlan-id</i>} [, -] [both rx tx]</p> <p>例 :</p> <pre>Switch(config)# monitor session 2 source interface gigabitethernet1/0/1</pre>	<p>SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。</p> <ul style="list-style-type: none"> • <i>session_number</i> の範囲は、1 ~ 66 です。 • <i>interface-id</i> には、監視する送信元ポートまたは送信元 VLAN を指定します。 • 送信元 <i>interface-id</i> には、モニタする送信元ポートを指定します。物理インターフェイスだけが有効です。 • <i>vlan-id</i> には、モニタする送信元 VLAN を指定します。指定できる範囲は 1 ~ 4094 です（RSPAN VLAN は除く）。 <p>(注) 1つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたはVLAN）を含めることができます。ただし、1つのセッション内では送信元ポートと送信元VLANを併用できません。</p> <ul style="list-style-type: none"> • (任意) [, -] は、一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを1つずつ入力します。 • (任意) [both rx tx] は、モニタリングするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、SPANは送信トラフィックと受信トラフィックの両方をモニタします。 <ul style="list-style-type: none"> ◦ both : 送信トラフィックと受信トラフィックの両方をモニタします。これはデフォルトです。 ◦ rx : 受信トラフィックをモニタします。 ◦ tx : 送信トラフィックをモニタします。 <p>(注) monitor session <i>session_number</i> source コマンドを複数回使用すると、複数の送信元ポートを設定できます。</p>
ステップ 4	<p>monitor session <i>session_number</i> destination {interface <i>interface-id</i> [, -] [encapsulation replicate]}</p>	<p>SPAN セッションおよび宛先ポート（モニタ側ポート）を指定します。</p>

	コマンドまたはアクション	目的
	<p>例 :</p> <pre>Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate</pre>	<ul style="list-style-type: none"> • <i>session_number</i> には、ステップ 3 で入力したセッション番号を指定します。 • destination に対して、次のパラメータを指定します。 <ul style="list-style-type: none"> ◦ <i>interface-id</i> には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 ◦ (任意) [<i> </i>-] は、一連または一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを1つずつ入力します。 ◦ (任意) encapsulation replicate は、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式 (タグなし) でのパケットの送信です。 <p>(注) ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。</p> <p>monitor session session_number destination コマンドを複数回使用すると、複数の宛先ポートを設定できます。</p>
ステップ 5	<pre>monitor session session_number filter {ip ipv6 mac} access-group {access-list-number name}</pre> <p>例 :</p> <pre>Switch(config)# monitor session 2 filter ipv6 access-group 4</pre>	<p>SPANセッション、フィルタリングするパケットのタイプ、およびFSPANセッションで使用する ACL を指定します。</p> <ul style="list-style-type: none"> • <i>session_number</i> には、手順 3 : • <i>access-list-number</i> には、トラフィックのフィルタリングに使用したい ACL 番号を指定します。 • <i>name</i> には、トラフィックのフィルタリングに使用したい ACL の名前を指定します。
ステップ 6	<p>end</p> <p>例 :</p> <pre>Switch(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>

FRSPAN セッションの設定

RSPAN 送信元セッションを開始し、監視対象の送信元および宛先 RSPAN VLAN を指定し、セッションに FRSPAN を設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **no monitor session** {*session_number* | **all** | **local** | **remote**}
3. **monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [, | -] [**both** | **rx** | **tx**]
4. **monitor session** *session_number* **destination remote vlan** *vlan-id*
5. **vlan** *vlan-id*
6. **remote-span**
7. **exit**
8. **monitor session** *session_number* **filter** {**ip** | **ipv6** | **mac**} **access-group** {*access-list-number* | *name*}
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no monitor session { <i>session_number</i> all local remote }	セッションに対する既存の SPAN 設定を削除します。 <ul style="list-style-type: none"> • <i>session_number</i> の範囲は、1 ~ 66 です。 • all : すべての SPAN セッションを削除します。 • local : すべてのローカル セッションを削除します。 • remote : すべてのリモート SPAN セッションを削除します。
ステップ 3	monitor session <i>session_number</i> source { interface <i>interface-id</i> vlan <i>vlan-id</i> } [, -] [both rx tx] 例： Switch(config)# monitor session 2 source interface gigabitethernet1/0/1	SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 <ul style="list-style-type: none"> • <i>session_number</i> の範囲は、1 ~ 66 です。 • <i>interface-id</i> には、監視する送信元ポートまたは送信元 VLAN を指定します。 • 送信元 <i>interface-id</i> には、モニタする送信元ポートを指定します。物理インターフェイスだけが有効です。 • <i>vlan-id</i> には、モニタする送信元 VLAN を指定します。指定できる範囲は 1 ~ 4094 です（RSPAN VLAN は除く）。 <p>(注) 1つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1つのセッション内では送信元ポートと送信元 VLAN を併用できません。</p>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • (任意) [, -] : 一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後およびハイフンの前後にスペースを1つずつ入力します。 • (任意) [both rx tx] : モニタリングするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、SPAN は送信トラフィックと受信トラフィックの両方をモニタします。 • both : 送信トラフィックと受信トラフィックの両方をモニタします。これはデフォルトです。 • rx : 受信トラフィックをモニタします。 • tx : 送信トラフィックをモニタします。 <p>(注) monitor session session_number source コマンドを複数回使用すると、複数の送信元ポートを設定できます。</p>
ステップ 4	monitor session session_number destination remote vlan vlan-id 例 : <pre>Switch(config)# monitor session 2 destination remote vlan 5</pre>	RSPAN セッションと宛先 RSPAN VLAN を指定します。 <ul style="list-style-type: none"> • <i>session_number</i> には、ステップ 3 で指定した番号を入力します。 • <i>vlan-id</i> には、モニタする宛先 RSPAN VLAN を指定します。
ステップ 5	vlan vlan-id 例 : <pre>Switch(config)# vlan 10</pre>	VLAN コンフィギュレーションモードを開始します。 <i>vlan-id</i> には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 6	remote-span 例 : <pre>Switch(config-vlan)# remote-span</pre>	ステップ 5 で指定した VLAN が RSPAN VLAN の一部であることを指定します。
ステップ 7	exit 例 : <pre>Switch(config-vlan)# exit</pre>	グローバル コンフィギュレーションモードに戻ります。
ステップ 8	monitor session session_number filter {ip ipv6 mac} access-group {access-list-number name}	RSPAN セッション、フィルタリングするパケットのタイプ、および FRSPAN セッションで使用する ACL を指定します。 <ul style="list-style-type: none"> • <i>session_number</i> には、手順 3 :

	コマンドまたはアクション	目的
	例 : <pre>Switch(config)# monitor session 2 filter ip access-group 7</pre>	<ul style="list-style-type: none"> • <i>access-list-number</i> には、トラフィックのフィルタリングに使用したい ACL 番号を指定します。 • <i>name</i> には、トラフィックのフィルタリングに使用したい ACL の名前を指定します。
ステップ 9	end 例 : <pre>Switch(config)# end</pre>	特権 EXEC モードに戻ります。

SPAN および RSPAN 動作のモニタリング

次の表で、SPAN および RSPAN 動作の設定と結果を表示して動作を監視するために使用するコマンドについて説明します。

表 13: SPAN および RSPAN 動作のモニタリング

コマンド	目的
show monitor	現在の SPAN、RSPAN、FSPAN、または FRSPAN 設定を表示します。

SPAN および RSPAN の設定例

例 : ローカル SPAN の設定

次に、SPAN セッション 1 を設定し、宛先ポートへ向けた送信元ポートのトラフィックをモニタする例を示します。最初に、セッション 1 の既存の SPAN 設定を削除し、カプセル化方式を維持しながら、双方向トラフィックを送信元ポート GigabitEthernet 1 から宛先ポート GigabitEthernet 2 にミラーリングします。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
encapsulation replicate
Switch(config)# end
```

次に、SPAN セッション 1 の SPAN 送信元としてのポート 1 を削除する例を示します。

```
Switch(config)# no monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# end
```

次に、双方向モニタが設定されていたポート 1 で、受信トラフィックのモニタをディセーブルにする例を示します。

```
Switch(config)# no monitor session 1 source interface gigabitethernet1/0/1 rx
```

ポート 1 で受信するトラフィックのモニタはディセーブルになりますが、このポートから送信されるトラフィックは引き続きモニタされます。

次に、SPAN セッション 2 内の既存の設定を削除し、VLAN 1～3 に属するすべてのポートで受信トラフィックをモニタするように SPAN セッション 2 を設定し、モニタされたトラフィックを宛先ポート GigabitEthernet 2 に送信する例を示します。さらに、この設定は VLAN 10 に属するすべてのポートですべてのトラフィックをモニタするよう変更されます。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2
Switch(config)# monitor session 2 source vlan 10
Switch(config)# end
```

次に、SPAN セッション 2 の既存の設定を削除し、送信元ポート GigabitEthernet 1 上で受信されるトラフィックをモニタするように SPAN セッション 2 を設定し、送信元ポートと同じ出力カプセル化方式を使用してそれを宛先ポート GigabitEthernet 2 に送信し、VLAN 6 をデフォルトの入力 VLAN として IEEE 802.1Q カプセル化を使用する入力転送をイネーブルにする例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source gigabitethernet1/0/1 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation
  replicate ingress dot1q vlan 6
Switch(config)# end
```

次に、SPAN セッション 2 の既存の設定を削除し、トランク ポート GigabitEthernet 2 で受信されたトラフィックをモニタするように SPAN セッション 2 を設定し、VLAN 1～5 および 9 に対してのみトラフィックを宛先ポート GigabitEthernet 1 に送信する例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/1
Switch(config)# end
```

例 : RSPAN VLAN の作成

この例は、RSPAN VLAN 901 の作成方法を示しています。

```
Switch(config)# vlan 901
Switch(config-vlan)# remote span
Switch(config-vlan)# end
```

次に、セッション 1 に対応する既存の RSPAN 設定を削除し、複数の送信元インターフェイスをモニタするように RSPAN セッション 1 を設定し、さらに宛先を RSPAN VLAN 901 に設定する例を示します。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 tx
Switch(config)# monitor session 1 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 1 source interface port-channel 2
Switch(config)# monitor session 1 destination remote vlan 901
Switch(config)# end
```

次に、RSPAN セッション 2 の既存の設定を削除し、トランク ポート 2 で受信されるトラフィックをモニタするように RSPAN セッション 2 を設定し、VLAN 1 ~ 5 および 9 に対してのみトラフィックを宛先 RSPAN VLAN 902 に送信する例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination remote vlan 902
Switch(config)# end
```

次に、送信元リモート VLAN として VLAN 901、宛先インターフェイスとしてポート 1 を設定する例を示します。

```
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface gigabitethernet2/0/1
Switch(config)# end
```

次に、RSPAN セッション 2 で送信元リモート VLAN として VLAN 901 を設定し、送信元ポート GigabitEthernet 2 を宛先インターフェイスとして設定し、VLAN 6 をデフォルトの受信 VLAN として着信トラフィックの転送をイネーブルにする例を示します。

```
Switch(config)# monitor session 2 source remote vlan 901
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress vlan 6
Switch(config)# end
```

SPAN および RSPAN の機能の履歴と情報

リリース	変更内容
Cisco IOS 15.0(2)EX1	スイッチ ポート アナライザ (SPAN) : スニファやアナライザまたは RMON プロブを使用してポートまたは VLAN のスイッチのトラフィックを監視できます。 この機能が導入されました。

リリース	変更内容
Cisco IOS 15.0(2)EX1	<p>フローベースのスイッチ ポートアナライザ (SPAN) : 指定されたフィルタを使用してエンドホスト間の必要な (関心のある) データのみをキャプチャする手段を提供します。フィルタは、IPv4、IPv6 または IPv4 と IPv6、あるいは指定された送信元と宛先アドレス間の IP トラフィック (MAC) 以外を制限するアクセス リストの観点から定義されます。</p> <p>この機能が導入されました。</p>
Cisco IOS 15.0(2)EX1	<p>EtherChannel での SPAN 宛先ポートのサポート :</p> <p>EtherChannel で SPAN 宛先ポートを設定できるようにします。</p> <p>この機能が導入されました。</p>
Cisco IOS 15.0(2)EX1	<p>スイッチ ポートアナライザ (SPAN) - 分散型出力 SPAN : ラインカードにすでに分散された入力 SPAN とともにラインカードに出力 SPAN 機能を分散させます。出力 SPAN 機能をラインカードに分散させることで、システムのパフォーマンスが向上します。</p> <p>この機能が導入されました。</p>



索引

C

- Cisco Discovery Protocol (CDP) [39](#)
- Cisco Networking Service [18](#)
- CNS [18](#)
- 設定エンジン [16](#)
 - 制約事項 [16](#)

I

- Inter-Switch Link; スイッチ間リンク [78](#)
 - 「ISL」を参照 [78](#)

N

- NSM [18](#)

R

- RSPAN [78, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 92, 93, 99, 100, 103, 106](#)
 - VLAN ベース [86](#)
 - 宛先ポート [87](#)
 - およびスタックの変更 [90](#)
 - 概要 [81](#)
 - 監視対象ポート [86](#)
 - 受信トラフィック [84](#)
 - セッション [84, 99, 100, 103, 106](#)
 - イネーブルにされた入力トラフィック [106](#)
 - 監視対象ポートの指定 [99, 100](#)
 - 作成 [99, 100](#)
 - 定義 [84](#)
 - 特定の VLAN への送信元トラフィックの制限 [103](#)
 - セッションの制限 [78](#)
 - 設定時の注意事項 [93](#)
 - 送信トラフィック [85](#)
 - 送信元ポート [86](#)

RSPAN (続き)

- デバイス スタック内 [82](#)
- デフォルト設定 [92](#)
- 特性 [88](#)
- ポートのモニタリング [87](#)
- 他の機能との相互作用 [89](#)

S

- SPAN [78, 81, 84, 85, 86, 87, 89, 90, 92, 93, 96, 98, 108](#)
 - VLAN ベース [86](#)
 - 宛先ポート [87](#)
 - およびスタックの変更 [90](#)
 - 概要 [81](#)
 - 監視対象ポート [86](#)
 - 受信トラフィック [84](#)
 - セッション [84, 92, 93, 96, 98, 108](#)
 - 宛先 (モニタリング) ポートの削除 [92](#)
 - イネーブルにされた入力トラフィック [96](#)
 - 監視対象ポートの指定 [93, 108](#)
 - 作成 [93, 108](#)
 - 定義 [84](#)
 - 特定の VLAN への送信元トラフィックの制限 [98](#)
 - セッションの制限 [78](#)
 - 設定時の注意事項 [92](#)
 - 送信トラフィック [85](#)
 - 送信元ポート [86](#)
 - デフォルト設定 [92](#)
 - ポートのモニタリング [87](#)
 - 他の機能との相互作用 [89](#)
- SPAN トラフィック [84](#)

V

- VLAN [98, 103](#)
 - RSPAN での送信元トラフィックの制限 [103](#)

VLAN (続き)

SPAN での送信元トラフィックの制限 [98](#)

VLAN フィルタリングと SPAN [87](#)

い

イベント サービス [18](#)

か

簡易ネットワーク管理プロトコル (SNMP) [39](#)

さ

services [18](#)

 ネットワークキング [18](#)

サブネットワーク アクセス プロトコル (SNAP) [39](#)

し

侵入検知システム [81](#)

 IDS アプライアンスを参照 [81](#)

す

スイッチド ポート アナライザ [77](#)

 「SPAN」を参照 [77](#)

スタックの変更、影響 [90](#)

 SPAN および RSPAN [90](#)

せ

制約事項 [16](#)

 設定エンジン [16](#)

て

定義 [18, 39](#)

 NSM [18](#)

 イベント サービス [18](#)

デバイス スタック [40](#)

デフォルト設定 [92](#)

 RSPAN [92](#)

 SPAN [92](#)

み

ミラーリング トラフィック、分析用の [81](#)

も

モニタリング [81](#)

 プローブでの分析用のネットワーク トラフィック [81](#)

り

リモート SPAN [83](#)

ろ

ローカル SPAN [81](#)