ネットワーク管理コンフィギュレーション ガイド、Cisco IOS XE Release 3.6E（Catalyst 3850 スイッチ）

初版：2014 年 06 月 27 日

最終更新：2013 年 10 月 07 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/

Text Part Number: OL-32604-01-J

【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。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。 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)

© 2014 Cisco Systems, Inc. All rights reserved.

目 次

はじめに xi

表記法 xi

関連資料 xiii

マニュアルの入手方法およびテクニカル サポート xiii

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

コマンドの省略形 5

コマンドの no 形式および default 形式 5

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 6

ヘルプ システムの使用 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 10

キー入力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

スイッチ スタックでの CLI へのアクセス 14

コンソール接続または Telnet 経由で CLI にアクセスする 14

Cisco IOS Configuration Engine の設定 17

機能情報の確認 17

Configuration Engine を設定するための前提条件 17

Configuration Engine の設定に関する制約事項 18
Configuration Engine の設定について 18
Cisco Configuration Engine ソフトウェア 18
コンフィギュレーション サービス 19
イベント サービス 20
NSM 20
Cisco Networking Service ID およびデバイスのホスト名 20
ConfigID 21
DeviceID 21
ホスト名および DeviceID 21
ホスト名、DeviceID、および ConfigID 22
Cisco IOS CNS エージェント 22
初期設定 22
差分（部分的）設定 23
コンフィギュレーションの同期 24
自動 CNS 設定 24
Configuration Engine の設定方法 25
CNS イベント エージェントのイネーブル化 25
Cisco IOS CNS エージェントのイネーブル化 27
Cisco IOS CNS エージェントの初期設定のイネーブル化 30
DeviceID の更新 35
Cisco IOS CNS エージェントの部分的設定のイネーブル化 37
CNS 設定のモニタリング 39
その他の関連資料 40
Configuration Engine の機能の履歴と情報 41
Cisco Discovery Protocol の設定 43
機能情報の確認 43
CDP に関する情報 43
CDP の概要 43
CDP およびスタック 44
CDP のデフォルト設定 44
CDP の設定方法 45
CDP 特性の設定 45

CDP のディセーブル化 47
Enabling CDP 48
インターフェイス上での CDP のディセーブル化 50
インターフェイス上での CDP のイネーブル化 52
CDP のモニタおよびメンテナンス 54
その他の関連資料 55
Cisco Discovery Protocol の機能の履歴と情報 56
簡易ネットワーク管理プロトコルの設定 57
機能情報の確認 57
SNMP の前提条件 58
SNMP の制約事項 60
SNMP に関する情報 61
SNMP の概要 61
SNMP マネージャ機能 61
SNMP エージェント機能 62
SNMP コミュニティ ストリング 62
SNMP MIB 変数アクセス 63
SNMP 通知 63
SNMP ifIndex MIB オブジェクト値 64
SNMP のデフォルト設定 64
SNMP 設定時の注意事項 65
SNMP の設定方法 66
SNMP エージェントのディセーブル化 66
コミュニティ ストリングの設定 68
SNMP グループおよびユーザの設定 70
SNMP 通知の設定 73
エージェント コンタクトおよびロケーションの設定 79
SNMP を通して使用する TFTP サーバの制限 81
SNMP のトラップフラグの設定 83
SNMP ワイヤレス トラップ通知のイネーブル化 85
SNMP ステータスのモニタリング 86
SNMP での例 87

その他の関連資料 88
簡易ネットワーク管理プロトコルの機能の履歴と情報 89
Web Cache Communication Protocol を使用したキャッシュ サービスの設定 91
機能情報の確認 91
WCCP の前提条件 91
WCCP に関する制約事項 92
WCCP に関する情報 93
WCCP の概要 93
WCCP メッセージ交換 94
WCCP ネゴシエーション 94
MD5 セキュリティ 95
パケットのリダイレクトおよびサービス グループ 95
WCCP およびスイッチ スタック 97
WCCP の設定方法 97
WCCP のデフォルト設定 97
キャッシュ サービスのイネーブル化 97
その他の関連資料 103
Web Cache Communication Protocol の機能の履歴と情報 104
サービス レベル契約の設定 105
機能情報の確認 105
SLA の制約事項 106
SLA について 106
Cisco IOS IP サービス レベル契約（SLA） 106
Cisco IOS IP SLA でのネットワーク パフォーマンスの測定 108
IP SLA レスポンダおよび IP SLA 制御プロトコル 108
IP SLA の応答時間の計算 109
IP SLA 動作のスケジューリング 110
IP SLA 動作のしきい値のモニタリング 111
UDP ジッター 111
IP SLA 動作の設定方法 112
デフォルト設定 112
設定時の注意事項 113

IP SLA レスポンダの設定 113
IP SLA ネットワーク パフォーマンス測定の実装 115
UDP ジッター動作を使用した IP サービス レベルの分析 119
ICMP エコー動作を使用した IP サービス レベルの分析 123
IP SLA 動作のモニタリング 126
IP SLA 動作のモニタリングの例 127
その他の関連資料 128
サービス レベル契約の機能の履歴と情報 130
ローカル ポリシーの設定 131
機能情報の確認 131
ローカル ポリシー設定の制約事項 131
ローカル ポリシーの設定に関する情報 132
ローカル ポリシーの設定方法 133
ローカル ポリシーの設定（CLI） 133
サービス テンプレートの作成（CLI） 134
インターフェイス テンプレートの作成（CLI） 135
パラメータ マップの作成（CLI） 135
クラス マップの作成（CLI） 137
ポリシー マップの作成（CLI） 137
WLAN 上のデバイスへのローカル ポリシーの適用（CLI） 139
ローカル ポリシーの設定（GUI） 140
サービス テンプレートの作成（GUI） 140
ポリシー マップの作成（GUI） 141
WLAN へのローカル ポリシーの適用（GUI） 142
ローカル ポリシーのモニタリング 142
例：ローカル ポリシーの設定 143
ローカル ポリシーの設定に関する追加情報 144
ローカル ポリシーの設定の実行に関する機能履歴 145
SPAN および RSPAN の設定 147
機能情報の確認 147
SPAN および RSPAN の前提条件 148
SPAN および RSPAN の制約事項 148

SPAN および RSPAN について 151
SPAN および RSPAN 151
ローカル SPAN 151
リモート SPAN 153
SPAN と RSPAN の概念および用語 154
SPAN セッション 154
監視対象トラフィック 155
送信元ポート 157
送信元 VLAN 157
VLAN フィルタリング 158
宛先ポート 158
RSPAN VLAN 160
SPAN および RSPAN と他の機能の相互作用 160
SPAN と RSPAN とデバイス スタック 162
フローベースの SPAN 162
SPAN および RSPAN のデフォルト設定 163
設定時の注意事項 164
SPAN 設定時の注意事項 164
RSPAN 設定時の注意事項 164
FSPAN および FRSPAN 設定時の注意事項 165
SPAN および RSPAN の設定方法 165
ローカル SPAN セッションの作成 165
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 168
フィルタリングする VLAN の指定 171
RSPAN VLAN としての VLAN の設定 173
RSPAN 送信元セッションの作成 175
フィルタリングする VLAN の指定 177
RSPAN 宛先セッションの作成 179
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 182
FSPAN セッションの設定 184
FRSPAN セッションの設定 187
SPAN および RSPAN 動作のモニタリング 190

SPAN および RSPAN の設定例 191
例：ローカル SPAN の設定 191
例：RSPAN VLAN の作成 192
その他の関連資料 193
SPAN および RSPAN の機能の履歴と情報 195
Wireshark の設定 197
機能情報の確認 197
Wireshark の前提条件 198
Wireshark の制約事項 198
Wireshark に関する情報 200
Wireshark の概要 200
キャプチャ ポイント 200
接続ポイント 201
フィルタ 202
処理 203
キャプチャ パケットのメモリ内のバッファへのストレージ 203
.pcap ファイルにキャプチャされたパケットのストレージ 203
パケットのデコードおよび表示 204
パケットのストレージおよび表示 205
Wireshark キャプチャ ポイントのアクティブ化および非アクティブ化 205
Wireshark 機能 206
Wireshark のガイドライン 208
デフォルトの Wireshark の設定 211
Wireshark の設定方法 211
キャプチャ ポイントの定義 212
キャプチャ ポイント パラメータの追加または変更 217
キャプチャ ポイント パラメータの削除 220
キャプチャ ポイントの削除 222
キャプチャ ポイントをアクティブまたは非アクティブにする 224
キャプチャ ポイント バッファのクリア 225
Wireshark のモニタリング 227
Wireshark の設定例 228

例：.pcap ファイルからの概要出力の表示 **228**

例：.pcap ファイルからの詳細出力の表示 **229**

例：単純なキャプチャおよび表示 **232**

例：単純なキャプチャおよび保存 **233**

例：バッファのキャプチャの使用 **234**

例：キャプチャ セッション **239**

例：ロック ステップ モードのキャプチャおよび保存 **240**

例：出方向のパケットの簡単なキャプチャおよび保存 **241**

その他の関連資料 **243**

WireShark の機能履歴と情報 **244**

はじめに

- 表記法，xi ページ
- 関連資料，xiii 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，xiii 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、およびユーザが入力したテキストは、**太字**フォントで示しています。
Italic 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、*italic* 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。
...	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。

表記法	説明
|	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　安全上の重要な注意事項

「危険」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。 装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。 警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。 Statement 1071

これらの注意事項を保管しておいてください。

関連資料

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

- 次の URL にある Cisco Catalyst 3850 スイッチ のマニュアル：
  http://www.cisco.com/go/cat3850_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
- 次の URL にあるエラー メッセージ デコーダ：
  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

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/c/en/us/td/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。

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

セッションを開始するときは、ユーザ モード（別名ユーザ EXEC モード）が有効です。 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、switch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、switchをリブートする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。 • 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。 このモードを使用して、アクセスポイントの特権 EXEC コマンドを実行します。これらのコマンドはコントローラの実行コンフィギュレーションの一部ではなく、アクセスポイントの IOS コンフィギュレーションに送信されます。
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)#`		

モード	アクセス方法	プロンプト	終了方法	モードの用途
			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、switch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。 このモードを使用して、コントローラの実行コンフィギュレーションの一部であるアクセス ポイント コマンドを設定します。
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。	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switch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。

モード	アクセス方法	プロンプト	終了方法	モードの用途
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。

コマンドの省略形

switch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switch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"`	switch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入れません。 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 モードで利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

switch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。

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	*abbreviated-command-entry* **?**
	
	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	*abbreviated-command-entry* <Tab>
	
	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一覧表示します。
ステップ 5	*command* **?** 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	*command keyword* **?**
	
	例：
	`Switch(config)# cdp holdtime ?`
	`  <10-255> Length of time (in sec) that receiver must keep this packet`
		キーワードに関連する引数を一覧表示します。

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、switch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switch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 セッション中の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イネーブルに設定されますが、ディセーブルにしたり、再びイネーブルにしたりできます。

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。

キー入力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	switch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：
	`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)# $15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45`
		1 行分を超えるグローバル コンフィギュレーション コマンド入力を表示します。
		最初にカーソルが行末に達すると、その行は 10 文字分だけ左へシフトされ、再表示されます。 ドル記号（$）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： `Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2$`	完全な構文をチェックします。 行末に表示されるドル記号（$）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。 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。 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。

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	{**show** | **more**} *command* | {**begin** | **include** | **exclude**} *regular-expression*
	
	例：
	`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`
		出力を検索およびフィルタリングします。
		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。

スイッチ スタックでの CLI へのアクセス

CLI にはコンソール接続、Telnet、SSH、またはブラウザを使用することによってアクセスできます。

スイッチ スタックおよびスタック メンバ インターフェイスは、active switchを経由して管理します。 スイッチごとにスタック メンバを管理することはできません。 1 つまたは複数のスタック メンバーのコンソール ポートまたはイーサネット管理ポートを経由してactive switchへ接続できます。 active switchで複数の CLI セッションを使用する場合は注意してください。 1 つのセッションで入力したコマンドは、別のセッションには表示されません。 したがって、コマンドを入力したセッションを追跡できない場合があります。

（注） スイッチ スタックを管理する場合は、1 つの CLI セッションを使用することを推奨します。

特定のスタック メンバ ポートを設定する場合は、CLI コマンド インターフェイス表記にスタック メンバ番号を含めてください。

スタンバイ スイッチをデバッグするには、アクティブなスイッチから **session standby ios** 特権 EXEC コマンドを使用してスタンバイ スイッチの IOS コンソールにアクセスします。 特定のスタック メンバをデバッグするには、アクティブなスイッチから **session switch** *stack-member-number* 特権 EXEC コマンドを使用して、スタック メンバの診断シェルにアクセスします。 これらのコマンドの詳細情報については、スイッチ コマンド リファレンスを参照してください。

コンソール接続または Telnet 経由で CLI にアクセスする

CLI にアクセスするには、switchのハードウェア インストレーション ガイドに記載されている手順で、switch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、switchの電源をオンにする必要があります。

switch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switchを設定しておく必要があります。

次のいずれかの方法で、switchとの接続を確立できます。

- switch 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、switchのハードウェア インストレーション 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。 switch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、switch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。
  - switch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。
  - switch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。

- ネットワーク管理コンフィギュレーション ガイド、Cisco IOS XE Release 3.6E（Catalyst 3850 スイッチ）

第 2 章

Cisco IOS Configuration Engine の設定

- 機能情報の確認，17 ページ
- Configuration Engine を設定するための前提条件，17 ページ
- Configuration Engine の設定に関する制約事項，18 ページ
- Configuration Engine の設定について，18 ページ
- Configuration Engine の設定方法，25 ページ
- CNS 設定のモニタリング，39 ページ
- その他の関連資料，40 ページ
- Configuration Engine の機能の履歴と情報，41 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。 最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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switch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switchesは、イベント バスにアクセスする必要があります。 switchを起源とする DeviceID は、Cisco Configuration Engine 内の対応するswitch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，（20 ページ）
DeviceID，（21 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switches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switches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，（20 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（switches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。

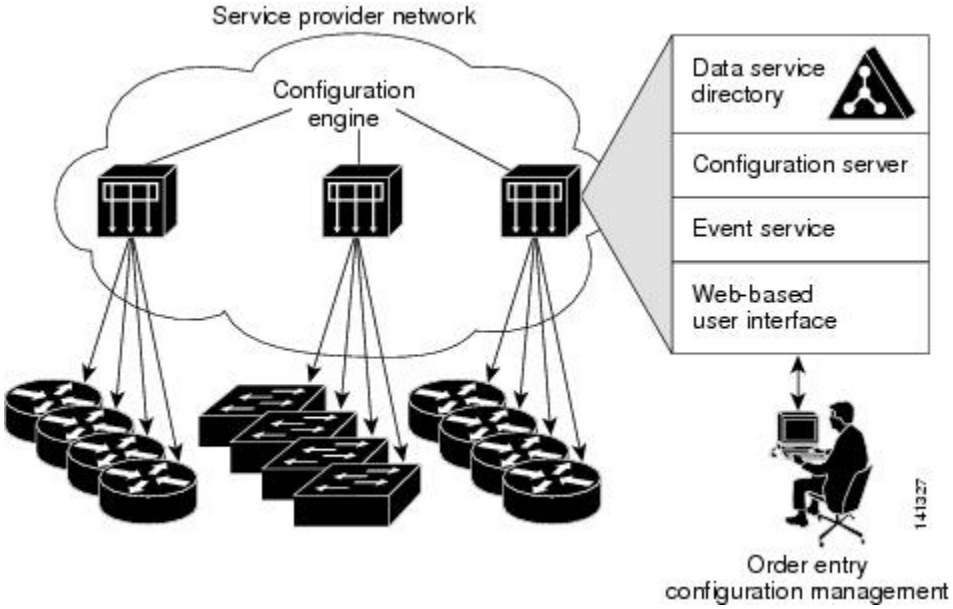
- コンフィギュレーション サービス
  - Web サーバ
  - ファイル マネージャ

- 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。switch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switchに配信します。 Switches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switch上にあり、switch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で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, （25 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switch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, （17 ページ）
Configuration Engine の設定に関する制約事項, （18 ページ）

ConfigID

設定対象のswitch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switch 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。 switchで定義された ConfigID は、Cisco Configuration Engine 上の対応するswitch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、switch 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switchごとに一意の DeviceID があります。これはswitchの送信元アドレスに似ているので、switch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、switch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、switch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switch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、switchおよび対応する DeviceID を表示します。

switch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、switch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, （17 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、switch ホスト名を再設定した場合でも変更されません。

switchでswitch ホスト名を変更するとき、DeviceID を更新する唯一の方法は、switch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、switch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、switch 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, （35 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switch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、switch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、switch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。 switch 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、switchを接続して、自動的に設定できます。

関連トピック

Cisco IOS CNS エージェントのイネーブル化, （27 ページ）

初期設定

switch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 switch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switchに IP ア

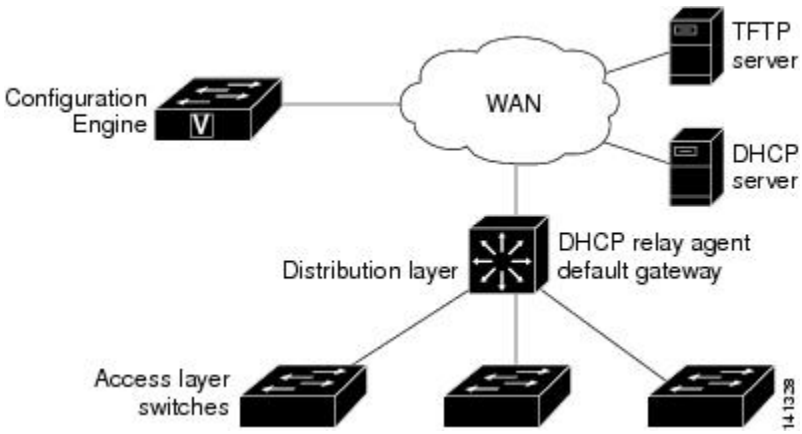
ドレスを割り当て、Trivial File Transfer Protocol（TFTP）サーバのインターネット プロトコル（IP）アドレス、ブートストラップ コンフィギュレーション ファイルへのパス、デフォルト ゲートウェイの IP アドレスを、DHCP リレー エージェントに対するユニキャスト応答に組み入れます。 DHCP リレー エージェントは、この応答をswitchに転送します。

switch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す。 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、switch 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、switch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

Cisco IOS CNS エージェントの初期設定のイネーブル化，（30 ページ）
CNS 設定のモニタリング，（39 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、switch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、switch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。

switch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、switch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。 switch 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。 switch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。

関連トピック

Cisco IOS CNS エージェントの部分的設定のイネーブル化，（37 ページ）
CNS 設定のモニタリング，（39 ページ）

コンフィギュレーションの同期

switch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switchに指示します。 switch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switch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

switch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switchの電源を入れます。 **setup** プロンプトでは何も入力しません。switch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switch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 switch	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 switch	• 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）

デバイス	必要な設定
DHCP サーバ	• 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
TFTP サーバ	• switch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）switch 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switch • switch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。

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） switch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。

switch上で CNS イベント エージェントをイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **cns event** {*hostname* | *ip-address*} [*port-number*] [[**keepalive** *seconds retry-count*] [**failover-time** *seconds*] [**reconnect-time** *time*] | **backup**]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**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。 • {*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、switch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switch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switch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、switch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。

	コマンドまたはアクション	目的
		• （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。
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	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

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, （20 ページ）

Cisco IOS CNS エージェントのイネーブル化

switch上で Cisco IOS CNS エージェントをイネーブルにするには、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、switch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. **enable**
2. **configure terminal**
3. **cns config initial** {*hostname* | *ip-address*} [*port-number*]
4. **cns config partial** {*hostname* | *ip-address*} [*port-number*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**
8. Cisco IOS CNS エージェントを、switch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	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**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。 • {*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。 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、switchで初期設定を開始します。

	コマンドまたはアクション	目的
ステップ 4	**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。 • {*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。 Cisco IOS CNS エージェントをイネーブルにして、switchで部分的設定を開始します。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 8	Cisco IOS CNS エージェントを、switchで開始します。	

次の作業

リモートで差分設定をswitch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

Cisco IOS CNS エージェント，（22 ページ）

Cisco IOS CNS エージェントの初期設定のイネーブル化

switch上で、CNS 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て初期設定を開始するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **cns template connect** *name*
4. **cli** *config-text*
5. 別の CNS 接続テンプレートを設定する場合は、ステップ 3 ～ 4 を繰り返します。
6. **exit**
7. **cns connect** *name* [**retries** *number*] [**retry-interval** *seconds*] [**sleep** *seconds*] [**timeout** *seconds*]
8. **discover** {**controller** *controller-type* | **dlci** [**subinterface** *subinterface-number*] | **interface** [*interface-type*] | **line** *line-type*}
9. **template** *name* [*... name*]
10. ステップ 8 ～ 9 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。
11. **exit**
12. **hostname** *name*
13. **ip route** *network-number*
14. **cns id** *interface num* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**]
15. **cns id** {**hardware-serial** | **hostname** | **string** *string* | **udi**} [**event**] [**image**]
16. **cns config initial** {*hostname* | *ip-address*} [*port-number*] [**event**] [**no-persist**] [**page** *page*] [**source** *ip-address*] [**syntax-check**]
17. **end**
18. **show running-config**
19. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**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 3	**cns template connect** *name* 例： `Switch(config)# cns template connect template-dhcp`	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 4	**cli** *config-text* 例： `Switch(config-tmpl-conn)# cli ip address dhcp`	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 5	別の CNS 接続テンプレートを設定する場合は、ステップ 3 ～ 4 を繰り返します。	
ステップ 6	**exit** 例： `Switch(config)# 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 7	**cns connect** *name* [**retries** *number*] [**retry-interval** *seconds*] [**sleep** *seconds*] [**timeout** *seconds*] 例： `Switch(config)# cns connect dhcp`	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。switch は CNS 接続プロファイルを使用して Configuration Engine に接続します。 • CNS 接続プロファイルの *name* 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。

	コマンドまたはアクション	目的
ステップ 8	**discover** {**controller** *controller-type* | **dlci** [**subinterface** *subinterface-number*] | **interface** [*interface-type*] | **line** *line-type*} 例： `Switch(config-cns-conn)# discover interface gigabitethernet`	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。 • **controller** *controller-type* に、コントローラ タイプを入力します。 • **dlci** 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 9	**template** *name* [*... name*] 例： `Switch(config-cns-conn)# template template-dhcp`	switch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 10	ステップ 8 ～ 9 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 11	**exit** 例： `Switch(config-cns-conn)# 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 12	**hostname** *name* 例： `Switch(config)# hostname device1`	switchのホスト名を入力します。
ステップ 13	**ip route** *network-number* 例： `RemoteSwitch(config)# ip route 172.28.129.22 255.255.255.255 11.11.11.1`	（任意）IP アドレスが *network-number* の Configuration Engine へのスタティック ルートを確立します。

	コマンドまたはアクション	目的
ステップ 14	**cns id** *interface num* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**] 例： `RemoteSwitch(config)# cns id GigabitEthernet1/0/1 ipaddress`	（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。 • *interface num* に、インターフェイスのタイプを入力します。 たとえば、ethernet、group-async、loopback、virtual-template 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。 • {**dns-reverse** | **ipaddress** | **mac-address**} 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 **dns-reverse** を入力し、IP アドレスを使用するには **ipaddress** を入力し、MAC アドレスを一意の ID として使用するには **mac-address** を入力します。 • （任意）ID をswitchの識別に使用する event-id 値になるように設定するには、**event** を入力します。 • （任意）ID をswitchの識別に使用する image-id 値になるように設定するには、**image** を入力します。 （注） **event** と **image** キーワードの両方を省略した場合は、switch の識別には image-id 値が使用されます。
ステップ 15	**cns id** {**hardware-serial** | **hostname** | **string** *string* | **udi**} [**event**] [**image**] 例： `RemoteSwitch(config)# cns id hostname`	（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** *interface num* {**dns-reverse** | **ipaddress** | **mac-address**} [**event**] [**image**] コマンドを入力しないでください。 • { **hardware-serial** | **hostname** | **string** *string* | **udi** } で、**hardware-serial** を入力してswitchのシリアル番号を一意の ID として設定するか、**hostname**（デフォルト）を入力してswitch のホスト名を一意の ID として選択するか、**string** *string* 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 **udi** 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 16	**cns config initial** {*hostname* | *ip-address*} [*port-number*] [**event**] [**no-persist**] [**page** *page*] [**source** *ip-address*] [**syntax-check**]	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。 • {*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。

	コマンドまたはアクション	目的
	例： `RemoteSwitch(config)# cns config initial 10.1.1.1 no-persist`	• （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。 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 **event** をイネーブルにします。 • （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。 （注） コマンドラインのヘルプ ストリングに表示されますが、**encrypt**、**status** *url*、**inventory** キーワードはサポートされていません。
ステップ 17	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 18	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 19	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

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 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。

関連トピック

初期設定，（22 ページ）
CNS 設定のモニタリング，（39 ページ）

DeviceID の更新

switch上でホスト名を変更するときに DeviceID を更新するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show cns config connections**
3. 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。
4. **show cns event connections**
5. ステップ 4 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。
6. **configure terminal**
7. **no cns event** *ip-address port-number*
8. **cns event** *ip-address port-number*
9. **end**
10. **show cns event connections** からの出力を調べて、switch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。
11. **show running-config**
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**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。
ステップ 3	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。 • 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switch 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 4	**show cns event connections** 例： `Switch# show cns event connections`	switchのイベント接続情報を表示します。
ステップ 5	ステップ 4 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 6	**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 7	**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 5 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、switch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 8	**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 5 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、switchとイベント ゲートウェイ間の接続が再確立されます。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show cns event connections** からの出力を調べて、switch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。	
ステップ 11	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 12	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ホスト名および DeviceID, （21 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

switch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、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **cns config partial** {*ip-address* | *hostname*} [*port-number*] [**source** *ip-address*]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**cns config partial** {*ip-address* | *hostname*} [*port-number*] [**source** *ip-address*] 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。 • {*ip-address* | *hostname*} 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）*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。 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。 （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 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`startup-config`	

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。

関連トピック

差分（部分的）設定, （23 ページ）
CNS 設定のモニタリング, （39 ページ）

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`	switch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# show cns event subject`	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。

関連トピック

Cisco IOS CNS エージェントの部分的設定のイネーブル化，（37 ページ）
差分（部分的）設定，（23 ページ）
Cisco IOS CNS エージェントの初期設定のイネーブル化，（30 ページ）
初期設定，（22 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
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

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
なし	-

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	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
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。 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。 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。	http://www.cisco.com/support

Configuration Engine の機能の履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SECisco IOS XE 3.2SE	この機能が導入されました。

- ネットワーク管理コンフィギュレーション ガイド、**Cisco IOS XE Release 3.6E**（**Catalyst 3850** スイッチ）

第 3 章

Cisco Discovery Protocol の設定

- 機能情報の確認，43 ページ
- CDP に関する情報，43 ページ
- CDP の設定方法，45 ページ
- CDP のモニタおよびメンテナンス，54 ページ
- その他の関連資料，55 ページ
- Cisco Discovery Protocol の機能の履歴と情報，56 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。 最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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 に関する情報

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switch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。 switch 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 switch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。

関連トピック

CDP 特性の設定，（45 ページ）
CDP のモニタおよびメンテナンス，（54 ページ）

CDP およびスタック

switch スタックは、ネットワーク内の 1 つのswitch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、switch 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、switch スタック メンバーシップに変更があった場合、switch 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

関連トピック

Enabling CDP, （48 ページ）
CDP のディセーブル化, （47 ページ）
インターフェイス上での CDP のイネーブル化, （52 ページ）
インターフェイス上での CDP のディセーブル化, （50 ページ）

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 3 ～ 5 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。

CDP 特性を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **cdp timer** *seconds*
4. **cdp holdtime** *seconds*
5. **cdp advertise-v2**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**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 4	**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。
ステップ 5	**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 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

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 の概要, （43 ページ）
CDP のモニタおよびメンテナンス, （54 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） Switch 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、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no cdp run**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**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 3	**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 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

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

Enabling CDP, （48 ページ）
CDP のデフォルト設定, （44 ページ）

Enabling CDP

CDP はデフォルトで有効になっています。

（注） Switch 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 を無効にすると、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。

無効になっている CDP を有効にするには、次の手順を実行します。

はじめる前に

CDP を無効にする必要があります。そのようにしないと有効にできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **cdp run**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**cdp run** 例： `Switch(config)# cdp run`	無効にされている場合は、CDP を有効にします。
ステップ 4	**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 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

次の作業

CDP が有効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 の有効化が表示されないことがあります。

関連トピック

CDP のデフォルト設定, （44 ページ）
CDP のディセーブル化, （47 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） Switch 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、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **no cdp enable**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**interface** *interface-id* 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 4	**no cdp enable** 例： `Switch(config-if)# no cdp enable`	ステップ 3 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 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

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, （52 ページ）
CDP のデフォルト設定, （44 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） Switch 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。

ポート上でディセーブルになっている CDP をイネーブルにするには、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. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **cdp enable**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**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 4	**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。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

CDP のデフォルト設定, （44 ページ）

インターフェイス上での CDP のディセーブル化, （50 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**]	特定のネイバーに関する情報を表示します。 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。 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。
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, （45 ページ）

CDP の概要, （43 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	*Network Management Command Reference, Cisco IOS XE Release 3E*

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
なし	-

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	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
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。 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。 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。	http://www.cisco.com/support

Cisco Discovery Protocol の機能の履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SECisco IOS XE 3.2SE	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，57 ページ
- SNMP の前提条件，58 ページ
- SNMP の制約事項，60 ページ
- SNMP に関する情報，61 ページ
- SNMP の設定方法，66 ページ
- SNMP ステータスのモニタリング，86 ページ
- SNMP での例，87 ページ
- その他の関連資料，88 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，89 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。 最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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す。 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）	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。 次の暗号化アルゴリズムで、User-based Security Model（USM）を指定できます。 • 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、switchに常駐します。 switch 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。

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。
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。

関連トピック

SNMP エージェントのディセーブル化, （66 ページ）
SNMP ステータスのモニタリング, （86 ページ）

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 switch 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 switch 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 switchがメンバ switches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 switch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 switch番号（@esN、N はswitch番号）を追加し、これらのストリングをメンバ switchesに伝播します。

関連トピック

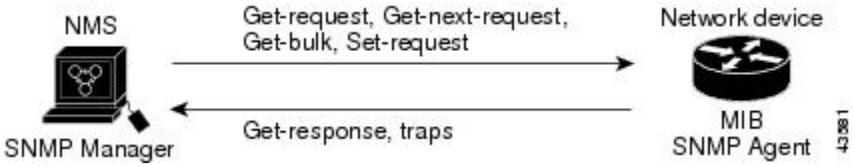
コミュニティ ストリングの設定, （68 ページ）

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、switch 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、switch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が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、switch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switch 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。

関連トピック

SNMP 通知の設定, （73 ページ）
SNMP ステータスのモニタリング, （86 ページ）

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。switchの再起動またはswitch ソフトウェアのアップグレード時に、switch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、switchのポート 2 に 10003 という ifIndex 値が割り当てられていると、switchの再起動後も同じ値が使用されます。

switch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	5000 ～ 5012
ループバック	5013 ～ 5077
Tunnel	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

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

機能	デフォルト設定
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。
SNMP バージョン	バージョン 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、switch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

switchが起動し、switch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、そのユーザを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、switch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 ストリングも再設定する必要があります。

関連トピック

SNMP グループおよびユーザの設定, （70 ページ）
SNMP ステータスのモニタリング, （86 ページ）

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、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. **enable**
2. **configure terminal**
3. **no snmp-server**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**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。
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	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

SNMP エージェント機能，（62 ページ）
SNMP ステータスのモニタリング，（86 ページ）

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、switch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

switch上でコミュニティ ストリングを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [*access-list-number*]
4. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**snmp-server community** *string* [**view** *view-name*] [**ro**	**rw**] [*access-list-number*]	コミュニティ ストリングを設定します。 （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。

	コマンドまたはアクション	目的
	例： `Switch(config)# snmp-server community comaccess ro 4`	• *string* 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）**view** 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）*access-list-number* 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 4	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Switch(config)# access-list 4 deny any`	（任意）ステップ 3 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。 • *access-list-number* には、ステップ 3 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。 • *source* 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）*source-wildcard* には、source 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することに注意してください。
ステップ 5	**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 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

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。

switch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。

関連トピック

SNMP コミュニティ ストリング, （62 ページ）

SNMP グループおよびユーザの設定

switch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。

switch上の SNMP グループとユーザを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server engineID** {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*] *engineid-string*}
4. **snmp-server group** *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]
5. **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*]
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**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。 • *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 4	**snmp-server group** *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*]	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。

	コマンドまたはアクション	目的
	[**notify** *notifyview*] [**access** *access-list*] 例： `Switch(config)# snmp-server group public v2c access lmnop`	次のいずれかのセキュリティ モデルを指定します。 • **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伝送できます。 • 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。 **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）。 （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。 （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。 （任意）**notify** *notifyview* 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。 （任意）**access** *access-list* 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。
ステップ 5	**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*] 例： `Switch(config)# snmp-server user Pat public v2c`	SNMP グループに対して新規ユーザを追加します。 *username* は、エージェントに接続するホスト上のユーザ名です。 *group-name* は、ユーザが関連付けられているグループの名前です。 **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。 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。 • **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 *auth-password*（64 文字以下）が必要です。

	コマンドまたはアクション	目的
		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 *priv-password* を設定できます。 • **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。 （任意）**access** *access-list* 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。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

SNMP 設定時の注意事項，（65 ページ）
SNMP ステータスのモニタリング，（86 ページ）

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switch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 Switches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。

snmp-server host グローバル コンフィギュレーション コマンドを組み合わせて使用することによって、次の表に示す通知タイプを特定のホストで受信できます。 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
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。
flash	SNMP FLASH 通知を生成します。 switch 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switch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。 switch スタックでは、このトラップはスタックにおけるswitch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。

通知タイプのキーワード	説明
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。
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*
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。

通知タイプのキーワード	説明
vlandelete	SNMP VLAN 削除トラップを生成します。
vtp	VLAN トランキング 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switchを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server engineID remote** *ip-address engineid-string*
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*] }
5. **snmp-server group** *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]
6. **snmp-server host** *host-addr* [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}] *community-string* [*notification-type*]
7. **snmp-server enable traps** *notification-types*
8. **snmp-server trap-source** *interface-id*
9. **snmp-server queue-length** *length*
10. **snmp-server trap-timeout** *seconds*
11. **end**
12. **show running-config**
13. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**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 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*] } 例： `Switch(config)# snmp-server user Pat public v2c`	SNMP ユーザを設定し、ステップ 3 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 5	**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 6	**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。 *host-addr* 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。 （任意）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。 （注） **priv** キーワードは、暗号化ソフトウェア イメージがインストールされている場合のみ使用可能です。 *community-string* 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ティ ストリングを入力します。 **version 3** が指定されている場合、SNMPv3 ユーザ名を入力します。

	コマンドまたはアクション	目的
		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。 （任意）*notification-type* 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。
ステップ 7	**snmp-server enable traps** *notification-types* 例： `Switch(config)# snmp-server enable traps snmp`	switchでのトラップまたはインフォームの送信をイネーブルにし、送信する通知の種類を指定します。 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。 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。 （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*
ステップ 8	**snmp-server trap-source** *interface-id* 例： `Switch(config)# snmp-server trap-source GigabitEthernet1/0/1`	（任意）送信元インターフェイスを指定します。このインターフェイスによってトラップ メッセージの IP アドレスが提供されます。 情報の送信元 IP アドレスも、このコマンドで設定します。
ステップ 9	**snmp-server queue-length** *length* 例： `Switch(config)# snmp-server queue-length 20`	（任意）各トラップ ホストのメッセージ キューの長さを指定します。 指定できる範囲は 1 ～ 1000 です。デフォルトは 10 です。
ステップ 10	**snmp-server trap-timeout** *seconds* 例： `Switch(config)# snmp-server trap-timeout 60`	（任意）トラップ メッセージを再送信する頻度を指定します。指定できる範囲は 1 ～ 1000 です。デフォルトは 30 秒です。
ステップ 11	**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 12	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 13	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

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。

関連トピック

SNMP 通知, （63 ページ）
SNMP ステータスのモニタリング, （86 ページ）

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、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server contact** *text*
4. **snmp-server location** *text*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**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 4	**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 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

SNMP を通して使用する TFTP サーバの制限

SNMP を介したコンフィギュレーション ファイルの保存とロードに使用する TFTP サーバを、アクセス リストで指定されたサーバに限定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server tftp-server-list** *access-list-number*
4. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**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。 *access-list-number* 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 4	**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。 *access-list-number* には、ステップ 3 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。 *source* には、switch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）*source-wildcard* には、source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 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

SNMP のトラップフラグの設定

手順の概要

1. **configure terminal**
2. **trapflags ap** { **interfaceup | register**}
3. **trapflags client** {**dot11 | excluded**}
4. **trapflags dot11-security** {**ids-sig-attack | wep-decrypt-error**}
5. **trapflags mesh**
6. **trapflags rogueap**
7. **trapflags rrm-params** {**channels | tx-power**}
8. **trapflags rrm-profile** {**coverage | interference | load | noise**}
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	**trapflags ap** { **interfaceup	register**} 例： `Switch(config)# trapflags ap interfaceup`	AP 関連トラップの送信をイネーブルにします。 トラップ フラグをディセーブルにするには、このコマンドの **no** 形式を使用します。 • interfaceup：Cisco AP インターフェイス（A または B）が起動したときにトラップをイネーブルにします。 • register：Cisco AP が Cisco switch に登録するときにトラップをイネーブルにします。
ステップ 3	**trapflags client** {**dot11	excluded**} 例： `Switch(config)# trapflags client excluded`	クライアント関連DOT11 トラップの送信をイネーブルにします。 トラップ フラグをディセーブルにするには、このコマンドの**no**形式を使用します。 • dot11：クライアントのDOT11 トラップをイネーブルにします。 • excluded：クライアント用の除外されたトラップ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	**trapflags dot11-security** {**ids-sig-attack** | **wep-decrypt-error**} 例： `Switch(config)# trapflags dot11-security wep-decrypt-error`	802.11 セキュリティ関連トラップの送信をイネーブルにします。 トラップフラグをディセーブルにするには、このコマンドの **no** 形式を使用します。 • ids-sig-attack：IDS シグニチャ攻撃トラップをイネーブルにします。 • wep-decrypt-error：クライアントの WEP 復号化エラーのトラップをイネーブルにします。
ステップ 5	**trapflags mesh** 例： `Switch(config)# trapflags mesh`	メッシュのトラップをイネーブルにします。 トラップ フラグをディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 6	**trapflags rogueap** 例： `Switch(config)# trapflags rogueap`	不正 AP 検出のトラップをイネーブルにします。 トラップ フラグをディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 7	**trapflags rrm-params** {**channels** | **tx-power**} 例： `Switch(config)# trapflags rrm-params tx-power`	RRM-parameter 更新関連トラップの送信をイネーブルにします。 トラップフラグをディセーブルにするには、このコマンドの **no** 形式を使用します。 • channels：RF マネージャが自動的に Cisco AP インターフェイスのチャネル番号を変更するときにトラップをイネーブルにします。 • tx-power：RF マネージャが自動的に Cisco AP インターフェイスの Tx-Power レベルを変更するときにトラップをイネーブルにします。
ステップ 8	**trapflags rrm-profile** {**coverage** | **interference** | **load** | **noise**} 例： `Switch(config)# trapflags rrm-profile interference`	RRM-Profile 関連トラップの送信をイネーブルにします。 トラップフラグをディセーブルにするには、このコマンドの **no** 形式を使用します。 • coverage：RF マネージャによって保持されるカバレッジ プロファイルでエラーが発生したときにトラップをイネーブルにします。 • interference：RF マネージャによって保持される干渉プロファイルでエラーが発生したときにトラップをイネーブルにします。 • load：RF マネージャによって保持される負荷プロファイルでエラーが発生したときにトラップをイネーブルにします。

	コマンドまたはアクション	目的
		• noise：RF マネージャによって保持されるノイズ プロファイルでエラーが発生したときにトラップをイネーブルにします。
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

SNMP ワイヤレス トラップ通知のイネーブル化

手順の概要

1. **configure terminal**
2. **snmp-server enable traps wireless** [**AP** | **RRM** | **bsn80211SecurityTrap** | **bsnAPParamUpdate** | **bsnAPProfile** | **bsnAccessPoint** | **bsnMobileStation** | **bsnRogue** | **client** | **mfp** | **rogue**]
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	**snmp-server enable traps wireless** [**AP**	**RRM**	**bsn80211SecurityTrap**	**bsnAPParamUpdate**	**bsnAPProfile**	**bsnAccessPoint**	**bsnMobileStation**	**bsnRogue**	**client**	**mfp**	**rogue**] 例： `Switch(config)# snmp-server enable traps wireless AP`	SNMP ワイヤレス トラップ通知をイネーブルにします。 • AP：アクセス ポイント トラップをイネーブルにします。 • RRM：RRM トラップをイネーブルにします。 • bsn80211SecurityTrap：セキュリティ関連のトラップをイネーブルにします。 • bsnAPParamUpdate：更新される AP パラメータのトラップをイネーブルにします。 • bsnAPProfile：BSN AP プロファイル トラップをイネーブルにします。

	コマンドまたはアクション	目的
		• bsnAccessPoint：BSN アクセス ポイント トラップをイネーブルにします。 • bsnMobileStation：ワイヤレス クライアント トラップを制御します。 • bsnRogue：BSN 不正関連トラップをイネーブルにします。 • client：クライアント トラップをイネーブルにします。 • mfp：MFP トラップをイネーブルにします。 • rogue：不正関連トラップ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。

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。

コマンド	目的
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。

関連トピック

SNMP エージェントのディセーブル化, （66 ページ）
SNMP エージェント機能, （62 ページ）
SNMP グループおよびユーザの設定, （70 ページ）
SNMP 設定時の注意事項, （65 ページ）
SNMP 通知の設定, （73 ページ）
SNMP 通知, （63 ページ）

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、switch 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。 switch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、switch 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switch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
```

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
SNMP コマンド	*Network Management Command Reference, Cisco IOS XE Release 3E*

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
なし	-

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	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
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。 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。 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。	http://www.cisco.com/support

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 XE 3.2SECisco IOS XE 3.2SE	この機能が導入されました。

ネットワーク管理コンフィギュレーション ガイド、**Cisco IOS XE Release 3.6E**（**Catalyst 3850** スイッチ）

第 5 章

Web Cache Communication Protocol を使用したキャッシュ サービスの設定

- 機能情報の確認，91 ページ
- WCCP の前提条件，91 ページ
- WCCP に関する制約事項，92 ページ
- WCCP に関する情報，93 ページ
- WCCP の設定方法，97 ページ
- その他の関連資料，103 ページ
- Web Cache Communication Protocol の機能の履歴と情報，104 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。 最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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。

WCCP の前提条件

スイッチで WCCP を設定する前に、次の設定要件に従ってください。

- 同じサービス グループ内のアプリケーション エンジンおよびスイッチは、WCCP 対応のスイッチに直接接続された同一サブネットワーク内に存在する必要があります。
- クライアント、アプリケーション エンジン、およびレイヤ 3 インターフェイスとしてのサーバ（ルーテッド ポートおよびスイッチ仮想インターフェイス（SVI））に接続されたスイッチ インターフェイスを設定します。 WCCP パケットのリダイレクトが機能するためには、サーバ、アプリケーション エンジン、およびクライアントが、異なるサブネット上に存在する必要があります。
- 各アプリケーション エンジンに 1 つのマルチキャスト アドレスを設定するときは、予約されていないマルチキャスト アドレスだけを使用します。
- WCCP エントリおよび PBR エントリは、同じ TCAM リージョンを使用します。 WCCP は、PBR（アクセス、ルーティング、デュアル IPv4/v6 ルーティング）をサポートするテンプレート上でだけサポートされます。
- TCAM エントリを WCCP エントリの追加に使用できない場合、パケットはリダイレクトされず、標準ルーティング テーブルを使用して転送されます。
- 使用可能な PBR ラベルの数は、WCCP 入力方法でイネーブルになるインターフェイスが増えるにつれて減っていきます。 サービス グループをサポートする各インターフェイスでは、ラベルが 1 つ消費されます。 WCCP ラベルは PBR ラベルから取得されます。 PBR と WCCP 間で使用可能なラベルを監視および管理する必要があります。 ラベルが使用できないと、スイッチはサービス グループを追加できなくなります。 ただし、別のインターフェイスに同じ一連のサービス グループがある場合、新しいラベルは必要にならず、グループをインターフェイスに追加できます。
- スタック メンバー スイッチで設定されたルーティング最大伝送単位（MTU）サイズは、クライアント MTU サイズより長い必要があります。 アプリケーション エンジンに接続されたポートで設定された MAC レイヤ MTU サイズは、GRE トンネル ヘッダー バイトを考慮する必要があります。

WCCP に関する制約事項

サポートしない WCCP 機能

次の WCCP 機能は、このソフトウェア リリースでサポートされていません。

- **ip wccp redirect out** インターフェイス コンフィギュレーション コマンドを使用して設定された発信インターフェイスでのパケットのリダイレクト
- パケット リダイレクトの GRE 転送方式
- GRE リダイレクトおよび GRE リターン
- ロードバランシング用のハッシュ割り当て方式
- WCCP の SNMP サポート
- ハードウェアでのハッシュ割り当て マスク割り当てのみを使用したロード バランスの実行

- フラグメント化されたパケットのリダイレクト これは、セキュリティ機能です。

全般的な制約事項

- サービス グループの最大数：8 入力および 8 出力。
- 同じスイッチ インターフェイス上では、WCCP と VPN ルーティングおよび転送（VRF）を設定できません。
- 同じスイッチ インターフェイス上では、WCCP および PBR を設定できません。
- 同じスイッチ インターフェイス上では、WCCP およびプライベート VLAN（PVLAN）を設定できません。
- **ip wccp redirect exclude in** コマンドは、出力 WCCP 方式から入力パケットを除外できるようにします。 これは、CE へのインターフェイスでは必要ではありません。
- キャッシュ エンジンが使用できない場合は、一致するパケットはドロップされます。 これは、クローズ グループのサポートです。 VRF 認識 WCCP のサポート、IPv6 WCCP のサポートはありません。
- デバイスを **ip wccp check services all** コマンドで設定すると、リダイレクト ACL がパケットと一致しなかった場合、次のプライオリティのサービス グループと照合されます。

WCCP に関する情報

WCCP の概要

（注） この機能を使用するには、デバイス上で IP Services フィーチャー セットが稼働している必要があります。

WCCP はシスコが開発したコンテンツ ルーティング技術です。WCCP を使用すると広域アプリケーション エンジン（以降、アプリケーション エンジンと呼ぶ）をネットワーク インフラストラクチャに統合できます。アプリケーションエンジンは、頻繁にアクセスのあるコンテンツを透過的に格納し、その同じコンテンツへの要求を満たし、サーバから繰り返し伝送されることを防ぎます。アプリケーションエンジンは、コンテンツ配信を加速させ、最大限のスケーラビリティとコンテンツの可用性を実現します。 サービスプロバイダー ネットワークのアクセス ポイント（POP）で、WCCPおよびアプリケーションエンジン ソリューションを展開できます。 エンタープライズ ネットワークでは、地域サイトまたは小規模ブランチ オフィスで WCCP およびアプリケーション エンジン ソリューションを展開できます。

WCCPおよびシスコのキャッシュ エンジン（またはWCCPが稼働している他のアプリケーション エンジン）は、ネットワークでのトラフィック パターンをローカライズし、コンテンツ要求がローカルで実現されるようにします。

WCCP により、サポート対象のシスコ ルータおよびswitchesは、コンテンツ要求を透過的にリダイレクトできます。透過リダイレクトを使用すると、ユーザは使用しているブラウザがWebプロキシを使用するように設定する必要がありません。 代わりに、ターゲット URL を使用してコンテンツを要求でき、その要求は自動的にアプリケーションエンジンにリダイレクトされます。透過という用語は、エンドユーザが、自分の要求したファイル（Webページなど）が、もとの指定したサーバからではなくアプリケーション エンジンから送信されるのを知らないという意味です。

アプリケーションエンジンが要求を受け取ると、自身のローカルキャッシュからサービスしようとします。要求された情報が存在しない場合、アプリケーションエンジンは別個の要求をエンドサーバに送信し、要求された情報を取得します。取得した情報は、アプリケーションエンジンが要求元のクライアントに転送するとともに、その後の要求に応えるため、情報をキャッシュします。

WCCPでは、アプリケーションエンジンクラスタ（一連のアプリケーションエンジン）は、、複数のルータまたはswitchesにサービスできます。

WCCP メッセージ交換

次の一連のイベントは、WCCP メッセージ交換について説明します。

1. アプリケーション エンジンは、WCCP を使用して IP アドレスを WCCP 対応switchに送信し、Here I am メッセージを通して自己の存在を伝えます。 switchおよびアプリケーション エンジンは、UDP ポート 2048 に基づき、制御チャネルを介して互いに通信します。
2. WCCP 対応switchは、アプリケーション エンジンの IP 情報を使用してクラスタ ビュー（クラスタ内のアプリケーション エンジンのリスト）を作成します。 このビューが、I see you メッセージでクラスタ内の各アプリケーション エンジンに送信すると、本質的にすべてのアプリケーション エンジンが互いの存在を認識するようになります。 クラスタのメンバーシップが一定時間同じままになった後で、安定したビューが確立されます。
3. 安定したビューが確立されると、クラスタ内の低い IP アドレスを持つアプリケーション エンジンが指定アプリケーション エンジンとして選択されます。

WCCP ネゴシエーション

WCCP プロトコル メッセージを交換する際、指定アプリケーション エンジンおよび WCCP 対応switchは次の項目をネゴシエートします。

- 転送方式（switchがパケットをアプリケーション エンジンに転送するときに使用される方式）。 switchは、パケット宛先MACアドレスをターゲットアプリケーションエンジンMACアドレスに置き換えて、レイヤ2ヘッダーを書き換えます。 次にスイッチは、パケットをアプリケーション エンジンに転送します。 この転送方式では、ターゲット アプリケーション エンジンがレイヤ 2 でswitchに直接接続されている必要があります。
- 割り当て方式（パケットをクラスタ内のアプリケーションエンジン間に配信するときに使用される方式）。 switchは宛先 IP アドレス、送信元 IP アドレス、宛先レイヤ 4 ポート、およ

び送信元レイヤ 4 ポートの一部のビットを使用して、リダイレクトされたパケットを受け取るアプリケーション エンジンを判別します。

- パケット戻し方式（パケットをアプリケーション エンジンから通常の転送用switchに戻すときに使用される方式）。 アプリケーション エンジンがパケットを拒否し、パケット戻し機能を起動するのには以下の理由があります。
  - アプリケーション エンジンが過負荷となり、パケットにサービスする余裕がない。
  - アプリケーション エンジンがサーバからエラー メッセージ（プロトコル エラーや認証エラーなど）を受け取り、ダイナミック クライアント バイパス機能を使用している。 バイパスは、クライアントがアプリケーションエンジンをバイパスし、サーバに直接接続できるようにします。

アプリケーション エンジンはパケットを WCCP 対応switchに戻し、アプリケーション エンジンが存在しないかのようにサーバに転送します。 アプリケーションエンジンは、再接続試行を代行受信しません。 このようにして、アプリケーション エンジンは効率的にアプリケーション エンジンへのパケットのリダイレクトをキャンセルし、バイパス フローを作成します。 戻し方式がレイヤ 2 書き換えである場合、パケットはハードウェア内でターゲット サーバに転送されます。 サーバが情報に応答しているとき、switchは通常のレイヤ 3 転送を使用して、情報を要求しているクライアントに戻します。

MD5 セキュリティ

WCCP は各プロトコル メッセージでオプションのセキュリティ コンポーネントを提供し、switch とアプリケーション エンジン間のメッセージで MD5 認証をswitchが使用できるようにします。（switchの認証がイネーブルになっているとき）MD5 で認証されないメッセージは、switchによって廃棄されます。 パスワード文字列は、MD5 値と組み合され、switchとアプリケーション エンジン間の接続のセキュリティを確立します。 各アプリケーションエンジンで同じパスワードを設定する必要があります。

パケットのリダイレクトおよびサービス グループ

WCCP を設定して、FTP、プロキシ Web キャッシュ処理、音声およびビデオアプリケーションなど、リダイレクト用トラフィックを分類できます。 この分類はサービス グループと呼ばれ、プロトコル タイプ（TCP または UDP）およびレイヤ 4 送信元ポート番号と宛先ポート番号に基づきます。 サービス グループは、TCP ポート 80 を意味する、Web キャッシュなどの Well-known 名または 0 ～ 99 のサービス番号のいずれかで識別されます。 サービス グループは、プロトコルおよびレイヤ 4 ポート番号にマッピングするように設定され、独立して確立および維持されます。 WCCPは、アプリケーションエンジンに加入して分類基準を動的に提供するダイナミック サービス グループを許可します。

スイッチswitchたはスイッチswitchスタックでは最大 8 つまでのサービス グループを、サービス グループにつき 32 までのキャッシュ エンジンを設定できます。 WCCP のグループ定義には、サービス グループのプライオリティがあります。 WCCP は、プライオリティを使用して、switch ハー

ドウェアのサービス グループを設定します。 たとえば、サービス グループ 1 はプライオリティ 100 で、宛先ポート 80 を探していて、サービス グループ 2 はプライオリティ 50 で、送信元ポート 80 を探している場合、送信元および宛先ポート 80 の着信パケットは、サービス グループ 1 を使用して転送されます。これは、サービス グループ 1 の方がプライオリティが高いためです。

WCCP は各サービス グループのアプリケーション エンジンのクラスタをサポートします。 リダイレクトされたトラフィックは、アプリケーション エンジンの 1 つに送信可能です。 switchは、サービスグループのクラスタ内のアプリケーションエンジン間で、トラフィックのロードバランシングのマスク割り当て方式をサポートします。

WCCPがswitch上で設定された後、switchはクライアントから受信したすべてのサービス グループパケットをアプリケーションエンジンに転送します。ただし、次のパケットはリダイレクトされません。

- アプリケーションエンジンから発信され、サーバに宛てられたパケット
- アプリケーション エンジンから発信され、クライアントに宛てられたパケット
- アプリケーションエンジンにより返送または拒否されたパケット。 これらのパケットはサーバに送信されます。

プロトコル メッセージの送受信用に、サービス グループにつき 1 つのマルチキャスト アドレスを設定できます。 マルチキャスト アドレスが 1 つの場合、アプリケーション エンジンは通知を 1 つのアドレスに送信することになり、たとえば 225.0.0.0 など、サービス グループのすべてのルータにカバレッジを提供します。 ルータを動的に追加および削除する場合、1 つのマルチキャストアドレスを使用することで、コンフィギュレーションが簡単になります。これは、特にWCCPネットワークのすべてのデバイスのアドレスを入力する必要がないためです。

ルータ グループ リストを使用すれば、アプリケーション エンジンから受け取ったプロトコル パケットを検証できます。 グループ リストのアドレスに一致するパケットは処理され、グループ リスト アドレスに一致しないパケットはドロップされます。

特定クライアント、サーバ、またはクライアントとサーバのペアのキャッシングをディセーブルにするには、WCCP リダイレクト アクセス コントロール リスト（ACL）を使用します。 リダイレクト ACL に一致しないパケットはキャッシュをバイパスし、通常通りに転送されます。

WCCPパケットがリダイレクトされる前、switchはインターフェイス上に設定されているすべての着信機能に関連した ACL をテストし、パケットが ACL 内のエントリと一致するかどうかによって、パケットの転送を許可または拒否します。

（注） WCCP リダイレクト リストでは、許可と拒否の両方の ACL エントリがサポートされます。

パケットがリダイレクトされると、リダイレクトされたインターフェイスに関連付けられた出力 ACL がパケットに適用されます。 元のポートに関連付けられた ACL は、リダイレクトされたインターフェイス上で必須出力 ACL を特に設定しない限り適用されません。

WCCP およびスイッチ スタック

switch スタックの WCCP サポート機能は、スタンドアロン switchの場合と同じです。 WCCP の設定情報は、スタック内のすべてのswitchesに伝播されます。 スタック マスターを含むスタック内のすべてのswitchesでは、情報が処理され、ハードウェアがプログラムされます

スタック マスターは、次の WCCP 機能を実行します。

- WCCP 対応インターフェイスからのプロトコル パケットを受信し、そのパケットをスタックの WCCP 対応インターフェイスに送信します。
- WCCP 設定を処理し、情報をすべてのスタック メンバに伝播します。
- WCCP 情報を、スタックに加入しているすべてのswitchに配信します。
- 処理する WCCP 情報を使用して、ハードウェアをプログラミングします。

スタック メンバーはマスター switchから WCCP 情報を受け取り、ハードウェアをプログラミングします。

WCCP の設定方法

WCCP のデフォルト設定

機能	デフォルト設定
WCCP イネーブル ステート	WCCP サービスはディセーブルです。
プロトコル バージョン	WCCPv2
インターフェイス上で受信したトラフィックのリダイレクト	ディセーブル

関連トピック

キャッシュ サービスのイネーブル化, （97 ページ）

キャッシュ サービスのイネーブル化

WCCP パケット リダイレクトが機能するために、クライアントに接続されたswitch インターフェイスが着信パケットをリダイレクトするように設定する必要があります。

この手順では、ルーテッド ポートでこれらの機能を設定する方法を示します。 これらの機能を SVI で設定するには、手順に従った設定例を参照してください。

キャッシュ サービスをイネーブルにしたり、マルチキャスト グループ アドレスまたはグループ リストを設定したり、ルーテッド インターフェイスを設定したり、クライアントから受信した着信パケットをアプリケーション エンジンにリダイレクトしたり、マルチキャスト アドレスを受信するようにインターフェイスをイネーブルにしたり、パスワードを設定したりするには、次の手順を実行します。 この手順は必須です。

はじめる前に

SDM テンプレートを設定し、デバイスをリブートします。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip wccp** {**web-cache** | *service-number*} [**group-address** *groupaddress*] [**group-list** *access-list*] [**redirect-list** *access-list*] [**password** *encryption-number password*]
4. **interface** *interface-id*
5. **no switchport**
6. **ip address** *ip-address subnet-mask*
7. **no shutdown**
8. **exit**
9. **interface** *interface-id*
10. **no switchport**
11. **ip address** *ip-address subnet-mask*
12. **no shutdown**
13. **ip wccp** {**web-cache** | *service-number*} **redirect in**
14. **ip wccp** {**web-cache** | *service-number*} **group-listen**
15. **exit**
16. **end**
17. **show running-config**
18. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**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 3	**ip wccp** {**web-cache** | *service-number*} [**group-address** *groupaddress*] [**group-list** *access-list*] [**redirect-list** *access-list*] [**password** *encryption-number password*] 例： `Switch(config)# ip wccp web-cache`	キャッシュ サービスをイネーブルにし、アプリケーション エンジンで定義されたダイナミック サービスに対応するサービス番号を指定します。 デフォルトでは、この機能はディセーブルになっています。 （任意）**group-address** *groupaddress* には、switchesおよびアプリケーション エンジンがサービス グループに加入するときに使用するマルチキャスト グループ アドレスを指定します。 （任意）**group-list** *access-list* には、マルチキャスト グループ アドレスが使用されない場合、サービス グループに加入しているアプリケーション エンジンに対応する有効な IP アドレスのリストを指定します。 （任意）**redirect-list** *access-list* には、特定ホストのリダイレクト サービスまたはホストから特定パケットを指定します。 （任意）**password** *encryption-number password* には、暗号化番号を指定します。 指定できる範囲は 0 ～ 7 です。 暗号化しない場合は 0、独自の場合は 7 を使用します。 7 文字以内でパスワード名を指定します。 switchは、パスワードと MD5 認証値を組み合わせて、switchとアプリケーションエンジンとの接続にセキュリティを確保します。 デフォルトでは、パスワードは設定されておらず、認証も実行されていません。 各アプリケーション エンジンで同じパスワードを設定する必要があります。 認証がイネーブルになっている場合、switchは認証されないメッセージを廃棄します。
ステップ 4	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	アプリケーションエンジンまたはサーバに接続された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 5	**no switchport** 例： `Switch(config-if)# no switchport`	レイヤ 3 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 6	**ip address** *ip-address subnet-mask* 例： `Switch(config-if)# ip address 172.20.10.30 255.255.255.0`	IP アドレスとサブネット マスクを設定します。
ステップ 7	**no shutdown** 例： `Switch(config-if)# no shutdown`	インターフェイスをイネーブルにします。
ステップ 8	**exit** 例： `Switch(config-if)# 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。 アプリケーション エンジンとサーバごとにステップ 4 ～ 8 を繰り返します。
ステップ 9	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	クライアントに接続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 10	**no switchport** 例： `Switch(config-if)# no switchport`	レイヤ 3 モードを開始します。
ステップ 11	**ip address** *ip-address subnet-mask* 例： `Switch(config-if)# ip address 175.20.20.10 255.255.255.0`	IP アドレスとサブネット マスクを設定します。
ステップ 12	**no shutdown** 例： `Switch(config-if)# no shutdown`	インターフェイスをイネーブルにします。
ステップ 13	**ip wccp** {**web-cache** | *service-number*} **redirect in** 例： `Switch(config-if)# ip wccp web-cache redirect in`	クライアントから受信したパケットをアプリケーション エンジンにリダイレクトします。 クライアントに接続されているインターフェイス上で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 14	**ip wccp** {**web-cache** | *service-number*} **group-listen** 例： `Switch(config-if)# ip wccp web-cache group-listen`	（任意）マルチキャスト グループ アドレスを使用するとき、**group-listen** キーワードはインターフェイスをイネーブルにしてマルチキャスト アドレスをリッスンします。 アプリケーションエンジンに接続されているインターフェイス上でイネーブルにします。
ステップ 15	**exit** 例： `Switch(config-if)# 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。 クライアントごとにステップ 9 ～ 15 を繰り返します。
ステップ 16	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 17	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 18	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

設定例

次に、ルーテッド インターフェイスを設定し、マルチキャスト グループ アドレスとリダイレクト アクセス リストでキャッシュ サービスをイネーブルにする例を示します。 ギガビット イーサネット ポート 1 はアプリケーション エンジンに接続され、IP アドレス 172.20.10.30 のルーテッド ポートとして設定され、再イネーブル化されています。 ギガビット イーサネット ポート 2 はインターネット経由でサーバに接続され、IP アドレス 175.20.20.10 のルーテッド ポートとして設定され、再イネーブル化されています。 ギガビット イーサネット ポート 3 ～ 6 はクライアントに接続され、IP アドレス 175.20.30.20、175.20.40.30、175.20.50.40、および 175.20.60.50 のルーテッド ポートとして設定されています。 switchはマルチキャスト トラフィックを受信し、クライアント インターフェイスから受信したパケットをアプリケーションエンジンにリダイレクトします。

```
Switch# configure terminal
Switch(config)# ip wccp web-cache group-address 224.1.1.100 redirect list 12
Switch(config)# access-list 12 permit host 10.1.1.1
```

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.20.10.30 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache group-listen
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.20.10 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.30.20 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.40.30 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/5
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.50.40 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/6
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.60.50 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
```

次に、SVIを設定し、マルチキャスト グループ リストでキャッシュ サービスをイネーブルにする例を示します。 VLAN 299は、IPアドレス175.20.20.10で作成および設定されています。 ギガビット イーサネットのポート1をインターネット経由でサーバに接続し、VLAN 299のアクセス ポートとして設定します。 VLAN 300は、IPアドレス172.20.10.30で作成および設定されています。 ギガビット イーサネット ポート2はアプリケーション エンジンに接続され、VLAN 300のアクセス ポートとして設定されています。 VLAN 301は、IPアドレス175.20.30.50で作成および設定されています。 クライアントに接続されているファスト イーサネット ポート3 ～ 6は、VLAN 301のアクセス ポートとして設定されています。 switchは、クライアント インターフェイスから受信したパケットをアプリケーション エンジンにリダイレクトします。

（注） WCCP リダイレクト リストでは、許可と拒否の両方の ACL エントリがサポートされます。

```
Switch# configure terminal
Switch(config)# ip wccp web-cache group-list 15
Switch(config)# access-list 15 permit host 171.69.198.102
Switch(config)# access-list 15 permit host 171.69.198.104
Switch(config)# access-list 15 permit host 171.69.198.106
Switch(config)# vlan 299
Switch(config-vlan)# exit
Switch(config)# interface vlan 299
Switch(config-if)# ip address 175.20.20.10 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 299
Switch(config)# vlan 300
```

```
Switch(config-vlan)# exit
Switch(config)# interface vlan 300
Switch(config-if)# ip address 171.69.198.100 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 300
Switch(config-if)# exit
Switch(config)# vlan 301
Switch(config-vlan)# exit
Switch(config)# interface vlan 301
Switch(config-if)# ip address 175.20.30.20 255.255.255.0
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# exit
Switch(config)# interface range gigabitethernet1/0/3 - 6
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 301
Switch(config-if-range)# exit
```

次の作業

キャッシュ サービスをディセーブルにするには、**no ip wccp web-cache** 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。 着信パケット リダイレクトをディセーブルにするには、**no ip wccp web-cache redirect in** インターフェイス コンフィギュレーション コマンドを使用します。この手順を完了した後、ネットワークでアプリケーション エンジンを設定します。

関連トピック

WCCP のデフォルト設定, （97 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
SNMP コマンド	*Network Management Command Reference, Cisco IOS XE Release 3E*

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
なし	-

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	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
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。 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。 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。	http://www.cisco.com/support

Web Cache Communication Protocol の機能の履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SECisco IOS XE 3.2SE	この機能が導入されました。

第 6 章

サービス レベル契約の設定

この章では、スイッチで Cisco IOS IP サービス レベル契約（SLA）を使用する方法について説明します。

特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチまたはスイッチ スタックを意味します。

- 機能情報の確認，105 ページ
- SLA の制約事項，106 ページ
- SLA について，106 ページ
- IP SLA 動作の設定方法，112 ページ
- IP SLA 動作のモニタリング，126 ページ
- IP SLA 動作のモニタリングの例，127 ページ
- その他の関連資料，128 ページ
- サービス レベル契約の機能の履歴と情報，130 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。 最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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。

SLA の制約事項

ここでは、SLA の制約事項を示します。

次に示すのは、IP SLA ネットワーク パフォーマンス測定の制約事項です。

- switchは、ゲートキーパー登録遅延動作測定を使用した Voice over IP（VoIP）サービス レベルはサポートしていません。
- Cisco IOS デバイスだけが宛先 IP SLA Responder の送信元になります。
- 他社製のデバイスに IP SLA Responder を設定することはできません。また、Cisco IOS IP SLA はこれらのデバイス固有のサービスに対してだけ動作パケットを送信できます。

関連トピック

IP SLA ネットワーク パフォーマンス測定の実装, （115 ページ）
Cisco IOS IP SLA でのネットワーク パフォーマンスの測定, （108 ページ）
IP SLA レスポンダおよび IP SLA 制御プロトコル, （108 ページ）

SLA について

Cisco IOS IP サービス レベル契約（SLA）

Cisco IOS IP SLA はネットワークにデータを送信し、複数のネットワーク ロケーション間あるいは複数のネットワーク パス内のパフォーマンスを測定します。 Cisco IOS IP SLA は、ネットワーク データおよび IP サービスをシミュレーションし、ネットワーク パフォーマンス情報をリアルタイムで収集します。 Cisco IOS IP SLA は、Cisco IOS デバイス間のトラフィックまたは Cisco IOS デバイスからネットワーク アプリケーション サーバのようなリモート IP デバイスへのトラフィックを生成し、分析します。 さまざまな Cisco IOS IP SLA 動作で評価を実行し、トラブルシューティング、問題分析、ネットワーク トポロジの設計に使用します。

Cisco IOS IP SLA 動作に応じてシスコ デバイスのネットワーク パフォーマンス統計情報がモニタリングされ、コマンドライン インターフェイス（CLI）MIB および簡易ネットワーク管理プロトコル（SNMP）MIB に格納されます。 IP SLA パケットには設定可能な IP レイヤおよびアプリケーション層のオプションがあります。たとえば、発信元および宛先 IP アドレス、ユーザデータグラム プロトコル（UDP）/TCP ポート番号、タイプ オブ サービス（ToS）バイト（DiffServ コード ポイント（DSCP）および IP プレフィックス ビットを含む）、VPN ルーティング/転送インスタンス（VRF）、URL Web アドレスなどが設定できます。

Cisco IP SLA はレイヤ 2 転送に依存していないので、異なるネットワーク間にエンドツーエンド動作を設定してエンドユーザが経験しそうなメトリックを最大限に反映させることができます。IP SLA は、次のパフォーマンス メトリックを収集して分析するために、Cisco Mediatrace と Cisco Performance Monitor の使用をサポートしています。

- 遅延（往復および一方向）
- ジッター（方向性あり）
- パケット損失（方向性あり）
- パケット シーケンス（パケット順序）
- パス（ホップ単位）
- 接続（方向性あり）
- サーバまたは Web サイトのダウンロード時間

加えて、switchは、ネットワーク インフラストラクチャで幅広いビデオ アプリケーションのためのインテリジェント サービスを可能にするためにCisco Medianet もサポートします。 Cisco Medianet は、ビデオ会議サービスを提供するエンドポイントと Auto Smartport 経由の IP サーベイランス カメラの自動プロビジョニングをサポートします。

Cisco Mediatrace と Cisco Performance Monitor は、IP Base イメージまたは IP Services イメージを実行しているswitches上で使用できます。

Cisco IP SLA は SNMP によるアクセスが可能なので、Cisco Prime Internetwork Performance Monitor（IPM）やサードパーティ製パフォーマンス管理製品などのパフォーマンス モニタリング アプリケーションでも使用できます。

IP SLA を使用すると、次の利点が得られます。

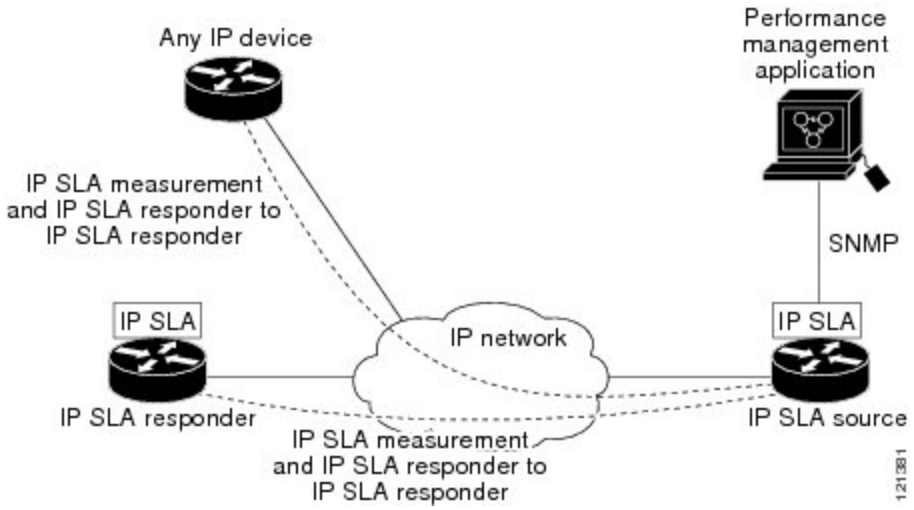
- SLA モニタリング、評価、検証。
- ネットワーク パフォーマンス モニタリング。
  - ネットワークのジッター、遅延、パケット損失の測定。
  - 連続的で信頼性のある予測可能な測定。
- IP サービス ネットワーク ヘルス アセスメントにより、既存の QoS が新しい IP サービスに適していることを確認できる。
- 端末間のネットワーク アベイラビリティをモニタリングして、ネットワーク リソースをあらかじめ検証し接続をテストできる（たとえば、ビジネス上の重要なデータを保存する NFS サーバのネットワーク アベイラビリティをリモート サイトから確認できる）。
- 問題をすぐに認識し、トラブルシューティングにかかる時間を短縮できる一貫性のある信頼性の高い測定によるネットワーク動作のトラブルシューティング。
- マルチプロトコル ラベル スイッチング（MPLS）パフォーマンス モニタリングとネットワークの検証を行う（switchが MPLS をサポートする場合）。

Cisco IOS IP SLA でのネットワーク パフォーマンスの測定

IP SLA を使用して、プローブを物理的に配置せずに、コア、分散、エッジといったネットワーク内の任意のエリア間のパフォーマンスをモニタリングすることができます。 2 つのネットワーク デバイス間のネットワーク パフォーマンスは、生成トラフィックで測定します。

次の図に、送信元デバイスが宛先デバイスに生成パケットを送信するときに IP SLA が開始される手順を示します。 宛先デバイスがパケットを受信すると、IP SLA 動作の種類によって、送信元のタイム スタンプ情報に応じてパフォーマンス メトリックを算出します。 IP SLA 動作は、特定のプロトコル（UDP など）を使用してネットワークの送信元から宛先へのネットワーク測定を行います。

図 *4*：*Cisco IOS IP SLA* 動作



関連トピック

IP SLA ネットワーク パフォーマンス測定の実装, （115 ページ）
SLA の制約事項, （106 ページ）

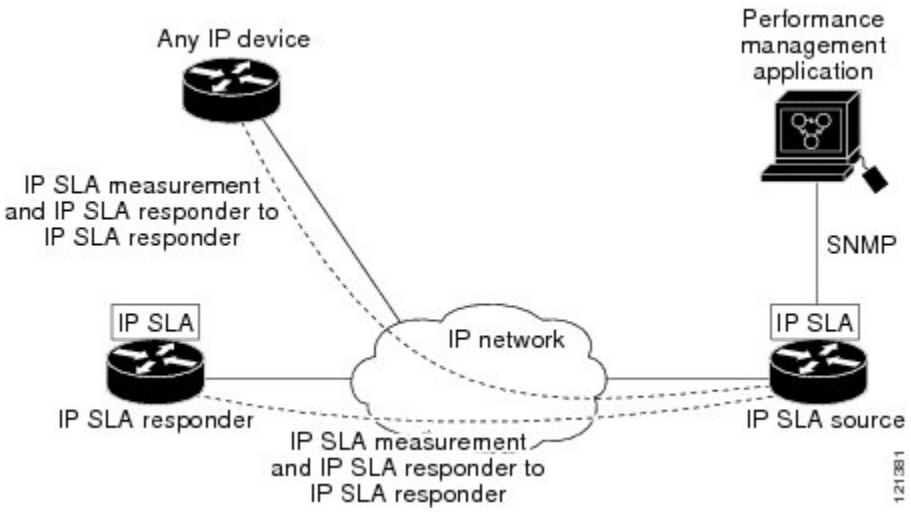
IP SLA レスポンダおよび IP SLA 制御プロトコル

IP SLA レスポンダは宛先 Cisco デバイスに組み込まれたコンポーネントで、システムが IP SLA 要求パケットを予想して応答します。 レスポンダは専用プローブなしで正確な測定を行います。 レスポンダは、受信および応答するポートが通知されるメカニズムを Cisco IOS IP SLA コントロール プロトコルを通じて実現します。

（注） IP SLA レスポンダはレスポンダ設定可能なswitchである Cisco IOS レイヤ 2 にすることもできます。 レスポンダは、IP SLA 機能を全面的にサポートする必要はありません。

次の図は、IP ネットワーク内での Cisco IOS IP SLA レスポンダの配置場所を示します。 レスポンダは、IP SLA 動作から送信されたコントロール プロトコル メッセージを指定されたポートで受信します。 コントロール メッセージを受信したら、指定された UDP または TCP ポートを指定された時間だけイネーブルにします。 この間に、レスポンダは要求を受け付け、応答します。 レスポンダは、IP SLA パケットに応答した後または指定の時間が経過したら ポートをディセーブルにします。セキュリティの向上のために、コントロール メッセージでは MD5 認証が利用できます。

図 *5*：*Cisco IOS IP SLA* 動作



すべての IP SLA 動作に対して宛先デバイスのレスポンダをイネーブルにする必要はありません。たとえば、宛先ルータが提供しているサービス（Telnet や HTTP など）はレスポンダでは必要ありません。

関連トピック

SLA の制約事項, （106 ページ）

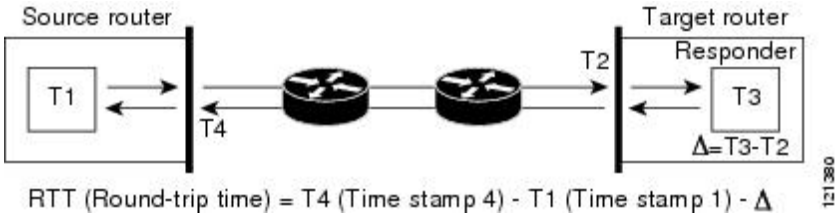
IP SLA の応答時間の計算

スイッチ、コントローラ、ルータは、他のハイ プライオリティ プロセスがあるために、着信パケットの処理に数十ミリ秒かかることがあります。 この遅延により応答時間が影響を受けます。テストパケットの応答が処理待ちのキューに入っていることもあるからです。 この場合、応答時間は正しいネットワーク遅延を反映しません。 IP SLA はソース デバイスとターゲット デバイス（レスポンダが使用されている場合）の処理遅延を最小化し、正しいラウンドトリップ時間（RTT）を識別します。 IP SLA テスト パケットは、タイム スタンプによって処理遅延を最小化します。

IP SLA レスポンダがイネーブルの場合、パケットが割り込みレベルでインターフェイスに着信したときおよびパケットが出て行くときにターゲットデバイスでタイムスタンプを付け、処理時間は含めません。 タイム スタンプはサブミリ秒単位で構成されます。

次の図は、レスポンダの動作を示します。 RTT を算出するためのタイム スタンプが 4 つ付けられます。 ターゲット ルータでレスポンダ機能がイネーブルの場合、タイム スタンプ 3（TS3）からタイム スタンプ 2（TS2）を引いてテスト パケットの処理にかかった時間を求め、デルタ（Δ）で表します。 次に全体の RTT からこのデルタの値を引きます。 IP SLA により、この方法はソース ルータにも適用されます。その場合、着信タイム スタンプ 4（TS4）が割り込みレベルで付けられ、より正確な結果を得ることができます。

図 *6*：*Cisco IOS IP SLA* レスポンダ タイム スタンプ



この他にも、ターゲット デバイスに 2 つのタイム スタンプがあれば一方向遅延、ジッター、方向性を持つパケット損失がトラッキングできるという利点があります。 大半のネットワーク動作は非同期なので、このような統計情報があるのは問題です。 ただし一方向遅延測定を取り込むには、ソース ルータとターゲット ルータの両方にネットワーク タイム プロトコル（NTP）を設定し、両方のルータを同じくロック ソースに同期させる必要があります。 一方向ジッター測定にはクロック同期は不要です。

IP SLA 動作のスケジューリング

IP SLA 動作を設定する場合、統計情報の取り込みとエラー情報の収集から開始するように動作をスケジューリングする必要があります。 スケジューリングは、すぐに動作を開始する、または特定の月、日、時刻に開始するように設定できます。 また、*pending* オプションを使用して、あとで動作を開始するように設定することもできます。 pending オプションは動作の内部状態に関するもので、SNMP で表示できます。 トリガーを待機する反応（しきい値）動作の場合も pending オプションを使用します。 スケジューリングでは、1 度に 1 つの IP SLA 動作をさせることも、グループの動作をさせることもできます。

Cisco IOS CLI または CISCO RTTMON-MIB で 1 つのコマンドを使用して、複数の IP SLA 動作をスケジューリングできます。 等間隔で動作を実行するようにスケジューリングすると、IP SLA モニタリング トラフィックの数を制御できます。 IP SLA 動作をこのように分散させると CPU 使用率を最小限に抑え、ネットワーク スケーラビリティを向上させることができます。

IP SLA 複数動作のスケジューリング機能の詳細については、『*Cisco IOS IP SLA Configuration Guide*』の「IP SLAs—Multiple Operation Scheduling」の章を参照してください。

IP SLA 動作のしきい値のモニタリング

サービス レベル契約モニタリングを正しくサポートするには、違反が発生した場合にすぐに通知されるメカニズムにする必要があります。 IP SLA は次のような場合にイベントによってトリガーされる SNMP トラップを送信できます。

- 接続の損失
- タイムアウト
- RTT しきい値
- 平均ジッターしきい値
- 一方向パケット損失
- 一方向ジッター
- 一方向平均オピニオン評点（MOS）
- 一方向遅延

IP SLA しきい値違反が発生した場合も、あとで分析するために別の IP SLA 動作がトリガーされます。 たとえば、回数を増やしたり、Internet Control Message Protocol（ICMP）パス エコーや ICMP パス ジッター動作を開始してトラブルシューティングを行うことができます。

ICMP エコー

ICMP エコー動作は、シスコ デバイスと IP を使用するその他のデバイス間のエンドツーエンド応答時間を測定します。 応答時間は、ICMP エコー要求メッセージを宛先に送信し、ICMP エコー応答を受信するのにかかる時間を測定して算出されます。 多くのお客様は、IP SLA ICMP ベース動作、社内 ping テスト、またはこの応答所要時間を測定するために ping ベース専用プローブを使用します。 IP SLA ICMP エコー動作は、ICMP ping テストと同じ仕様に準拠しており、どちらの方法でも同じ応答所要時間になります。

関連トピック

ICMP エコー動作を使用した IP サービス レベルの分析, （123 ページ）

UDP ジッター

ジッターとは、パケット間遅延の差異を説明する簡単な用語です。 複数のパケットが送信元から宛先まで 10 ミリ秒の間隔で継続的に送信される場合、宛先は 10 ミリ秒間隔で受信します（ネットワークが正常に動作している場合）。 しかし、ネットワークに遅延がある場合（キューイングや代替ルートを通じた到着など）、パケットの着信の間隔が 10 ミリ秒を超える場合や 10 ミリ秒未満になる場合があります。 正のジッター値は、パケットが 10 ミリ秒を超える間隔で到着することを示します。 負のジッター値は、パケットが 10 ミリ秒未満の間隔で到着することを示します。 パケットの到着が 12 ミリ秒間隔の場合、正のジッター値は 2 ミリ秒です。8 ミリ秒間隔で到

着する場合、負のジッター値は 2 ミリ秒です。 遅延による影響を受けやすいネットワークの場合、正のジッター値は望ましくありません。ジッター値 0 が理想的です。

ジッターのモニタリング以外にも、IP SLA UDP ジッター動作を多目的データ収集動作に使用できます。 IP SLA によって生成されるパケットは、データを送受信するパケットを含めて、送信元および動作ターゲットからシーケンス情報とタイム スタンプを伝送します。 このデータに基づいて、UDP ジッター動作は次を測定します。

- 方向別ジッター（送信元から宛先へ、宛先から送信元へ）
- 方向別パケット損失
- 方向別遅延（一方向遅延）
- ラウンドトリップ遅延（平均 RTT）

データを送受信するパスが異なる場合もあるので（非同期）、方向別データを使用すればネットワークで発生している輻輳や他の問題の場所を簡単に突き止めることができます。

UDP ジッター動作では合成（シミュレーション）UDP トラフィックを生成し、送信元ルータからターゲット ルータに多数の UDP パケットを送信します。その際の各パケットのサイズ、パケット同士の間隔、送信間隔は決められています。 デフォルトでは、10 バイトのペイロード サイズのパケット フレームを 10 ミリ秒で 10 個生成し、60 秒間隔で送信します。 これらのパラメータは、提供する IP サービスを最適にシミュレートするように設定できます。

一方向遅延を正確に測定する場合、（NTP によって提供される）送信元デバイスとターゲット デバイス間のクロック同期が必要です。 一方向ジッターおよびパケット損失を測定する場合は、クロック同期は不要です。 送信元デバイスとターゲットデバイスの間でクロックが同期していない場合、一方向ジッターとパケット損失のデータは戻されますが、UDP ジッター動作による一方向遅延測定は 0 の値が戻ります。

関連トピック

UDP ジッター動作を使用した IP サービス レベルの分析, （119 ページ）

IP SLA 動作の設定方法

ここでは、利用可能なすべての動作の設定情報について説明されているわけではありません。設定情報の詳細については『*Cisco IOS IP SLAs Configuration Guide*』を参照してください。 ここでは、応答側の設定、UDP ジッター動作の設定（応答側が必要）、ICMP エコー動作の設定（応答側が不要）などの動作例を説明します。 他の動作の設定の詳細については、次の URL の『*Cisco IOS IP SLAs Configuration Guide*』を参照してください。

デフォルト設定

IP SLA 動作は設定されていません。

設定時の注意事項

IP SLA のコマンドについては、『*Cisco IOS IP SLA Command Reference, Release 12.4T*』のコマンドリファレンスを参照してください。

説明と設定手順の詳細については、『*Cisco IOS IP SLAs Configuration Guide, Release 12.4TL*』を参照してください。

ガイドに記載されている IP SLA コマンドまたは動作の中にはswitchでサポートされないものもあります。 switchでは、UDP ジッター、UDP エコー、HTTP、TCP 接続、ICMP エコー、ICMP パス エコー、ICMP パス ジッター、FTP、DNS、DHCP を使用する IP サービス レベル分析がサポートされます。また、複数動作スケジューリングおよび事前に設定されたしきい値のモニタリングもサポートされます。 ゲートキーパー登録遅延動作測定を使用した Voice over IP（VoIP）サービス レベルはサポートしていません。

IP SLA アプリケーションを設定する前に、**show ip sla application** 特権 EXEC コマンドを使用してソフトウェアイメージで動作タイプがサポートされていることを確認してください。 コマンド出力例は次のとおりです。

```
Switch# show ip sla application

        IP Service Level Agreements
Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III

Supported Operation Types:
        icmpEcho, path-echo, path-jitter, udpEcho, tcpConnect, http
        dns, udpJitter, dhcp, ftp, udpApp, wspApp

Supported Features:
        IPSLAs Event Publisher

IP SLAs low memory water mark: 33299323
Estimated system max number of entries: 24389

Estimated number of configurable operations: 24389
Number of Entries configured  : 0
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0
Time of last change in whole IP SLAs: *13:04:37.668 UTC Wed Dec 19 2012
```

IP SLA レスポンダの設定

IP SLA レスポンダは、Cisco IOS ソフトウェアベース デバイスだけで利用可能です。これには、IP SLA 機能をフルにサポートしていない一部のレイヤ 2 switchesも含まれます。

ターゲット デバイス（動作ターゲット）上の IP SLA 応答側を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla responder** {**tcp-connect** | **udp-echo**} **ipaddress** *ip-address* **port** *port-number*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**ip sla responder** {**tcp-connect** | **udp-echo**} **ipaddress** *ip-address* **port** *port-number* 例： `Switch(config)# ip sla responder udp-echo 172.29.139.134 5000`	switchを IP SLA レスポンダとして設定します。 キーワードの意味は次のとおりです。 • **tcp-connect**：レスポンダの TCP 接続動作をイネーブルにします。 • **udp-echo**：レスポンダのユーザ データグラム プロトコル（UDP）エコー動作またはジッター動作をイネーブルにします。 • **ipaddress** *ip-address*：宛先 IP アドレスを入力します。 • **port** *port-number*：宛先ポート番号を入力します。 （注） IP アドレスとポート番号は、IP SLA 動作のソース デバイスに設定した IP アドレスおよびポート番号と一致している必要があります。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IP SLA ネットワーク パフォーマンス測定の実装

switch上で IP SLA ネットワーク パフォーマンス測定を実施するには、次の手順を実行します。

はじめる前に

show ip sla application 特権 EXEC コマンドを使用して、ソフトウェア イメージで目的の動作タイプがサポートされていることを確認してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*]
5. **frequency** *seconds*
6. **threshold** *milliseconds*
7. **exit**
8. **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**]
9. **end**
10. **show running-config**
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**ip sla** *operation-number* 例： `Switch(config)# ip sla 10`	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。
ステップ 4	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*]	IP SLA 動作を目的の動作タイプとして設定して（例ではUDP ジッター動作が使用されています）、そのコンフィギュレーションモードを開始します（例ではUDPジッターコンフィギュレーションモードが使用されています）。 • *destination-ip-address* | *destination-hostname*：宛先 IP アドレスまたはホスト名を指定します。

	コマンドまたはアクション	目的
	例： `Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000`	• *destination-port*：宛先ポート番号を 1 ～ 65535 の範囲で指定します。 • （任意）**source-ip** {*ip-address*|*hostname*}：送信元 IP アドレスまたはホスト名を指定します。 送信元 IP アドレスまたはホスト名が指定されていない場合、IP SLA では、宛先に最も近い IP アドレスが選択されます。 • （任意）**source-port** *port-number*：送信元ポート番号を 1 ～ 65535 の範囲で指定します。 ポート番号を指定しない場合、IP SLA は利用可能なポートを選択します。 • （任意）**control**：IP SLA 制御メッセージの IP SLA レスポンダへの送信をイネーブルまたはディセーブルにします。デフォルトでは、IP SLA 制御メッセージは宛先デバイスに送信され、IP SLA レスポンダとの接続が確立されます。 • （任意）**num-packets** *number-of-packets*：生成するパケット数を入力します。 指定できる範囲は 1 ～ 6000 です。デフォルトは 10 です。 • （任意）**interval** *inter-packet-interval*：パケットの送信間隔をミリ秒で指定します。 指定できる範囲は 1 ～ 6000 です。デフォルトは 20 ミリ秒です。
ステップ 5	**frequency** *seconds* 例： `Switch(config-ip-sla-jitter)# frequency 45`	（任意）SLA 動作のオプションを設定します。 次の例では、指定された IP SLA 動作が繰り返されるレートを設定します。 指定できる範囲は 1 ～ 604800 秒で、デフォルトは 60 秒です。
ステップ 6	**threshold** *milliseconds* 例： `Switch(config-ip-sla-jitter)# threshold 200`	（任意）しきい値条件を設定します。 次の例では、指定された IP SLA 動作のしきい値が 200 に設定されます。 有効な範囲は 0 ～ 60000 ミリ秒です。
ステップ 7	**exit** 例： `Switch(config-ip-sla-jitter)# exit`	SLA 動作コンフィギュレーション モード（この例では UDP ジッター コンフィギュレーション モード）を終了し、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	**ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*]	個々の IP SLA 動作のスケジューリング パラメータを設定します。 • *operation-number*：RTR エントリ番号を入力します。

	コマンドまたはアクション	目的
	| **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**] 例： `Switch(config)# ip sla schedule 10 start-time now life forever`	• （任意）**life**：動作の実行を無制限（**forever**）に指定するか、秒数（*seconds*）を指定します。 有効な範囲は 0 ～ 2147483647 です。 デフォルトは 3600 秒（1 時間）です。 • （任意）**start-time**：情報の収集を開始する時刻を入力します。 特定の時刻に開始する場合は、時、分、秒（24時間表記）、月日を入力します。月を入力しない場合、当月がデフォルト設定です。 **pending** と入力すれば、開始時刻を指定するまでは情報を収集しません。 **now** と入力すれば、ただちに動作を開始します。 **after** *hh:mm:ss* と入力すれば、指定した時刻の経過後に動作を開始します。 • （任意）**ageout***seconds*：情報を収集していないとき、メモリの動作を保存する秒数を指定します。 指定できる範囲は 0 ～ 2073600 秒です。デフォルトは 0 秒（いつまでも保存する）です。 • （任意）**recurring**：毎日、動作を自動的に実行します。
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

UDP ジッター コンフィギュレーション

次に、UDP ジッター IP SLA 動作の設定例を示します。

```
Switch(config)# ip sla 10
Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000
Switch(config-ip-sla-jitter)# frequency 30
Switch(config-ip-sla-jitter)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 10
IP SLAs, Infrastructure Engine-II.

Entry number: 10
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 30
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
Enhanced History:
```

関連トピック

Cisco IOS IP SLA でのネットワーク パフォーマンスの測定, （108 ページ）

SLA の制約事項, （106 ページ）

UDP ジッター動作を使用した IP サービス レベルの分析

送信元デバイス上の UDP ジッタ動作を設定するには、次の手順を実行します。

はじめる前に

送信元デバイス上でUDP ジッター動作を設定するには、ターゲットデバイス（動作ターゲット）で、IP SLA レスポンダをイネーブルにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*]
5. **frequency** *seconds*
6. **exit**
7. **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**]
8. **end**
9. **show running-config**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**ip sla** *operation-number* 例： `Switch(config)# ip sla 10`	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。
ステップ 4	**udp-jitter** {*destination-ip-address* | *destination-hostname*} *destination-port* [**source-ip** {*ip-address* | *hostname*}] [**source-port** *port-number*] [**control** {**enable** | **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*]	IP SLA 動作を UDP ジッター動作として設定し、UDP ジッター コンフィギュレーション モードを開始します。 • *destination-ip-address* | *destination-hostname*：宛先 IP アドレスまたはホスト名を指定します。 • *destination-port*：宛先ポート番号を 1 ～ 65535 の範囲で指定します。

	コマンドまたはアクション	目的
	例： `Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000`	• （任意）**source-ip** {*ip-address* | *hostname*}：送信元 IP アドレスまたはホスト名を指定します。 送信元 IP アドレスまたはホスト名が指定されていない場合、IP SLA では、宛先に最も近い IP アドレスが選択されます。 • （任意）**source-port** *port-number*：送信元ポート番号を 1 ～ 65535 の範囲で指定します。 ポート番号を指定しない場合、IP SLA は利用可能なポートを選択します。 • （任意）**control**：IP SLA 制御メッセージの IP SLA レスポンダへの送信をイネーブルまたはディセーブルにします。 デフォルトでは、IP SLA 制御メッセージは宛先デバイスに送信され、IP SLA レスポンダとの接続が確立されます。 • （任意）**num-packets** *number-of-packets*：生成するパケット数を入力します。 指定できる範囲は 1 ～ 6000 です。デフォルトは 10 です。 • （任意）**interval** *inter-packet-interval*：パケットの送信間隔をミリ秒で入力します。 指定できる範囲は 1 ～ 6000 です。デフォルトは 20 ミリ秒です。
ステップ 5	**frequency** *seconds* 例： `Switch(config-ip-sla-jitter)# frequency 45`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。 指定できる範囲は 1 ～ 604800 秒で、デフォルトは 60 秒です。
ステップ 6	**exit** 例： `Switch(config-ip-sla-jitter)# exit`	UDP ジッター コンフィギュレーション モードを終了し、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 7	**ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**] 例： `Switch(config)# ip sla schedule 10 start-time now life forever`	個々の IP SLA 動作のスケジューリング パラメータを設定します。 • *operation-number*：RTR エントリ番号を入力します。 • （任意）**life**：動作の実行を無制限（**forever**）に指定するか、秒数（*seconds*）を指定します。 有効な範囲は 0 ～ 2147483647 です。 デフォルトは 3600 秒（1 時間）です。 • （任意）**start-time**：情報の収集を開始する時刻を入力します。 特定の時刻に開始する場合は、時、分、秒（24 時間表記）、月日を入力します。 月を入力しない場合、当月がデフォルト設定です。

	コマンドまたはアクション	目的
		pending と入力すれば、開始時刻を指定するまでは情報を収集しません。 **now** と入力すれば、ただちに動作を開始します。 **after** *hh:mm:ss* と入力すれば、指定した時刻の経過後に動作を開始します。 • （任意）**ageout** *seconds*：情報を収集していないとき、メモリの動作を保存する秒数を指定します。 指定できる範囲は 0 ～ 2073600 秒です。デフォルトは 0 秒（いつまでも保存する）です。 • （任意）**recurring**：毎日、動作を自動的に実行します。
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

UDP ジッター IP SLA 動作の設定

次に、UDP ジッター IP SLA 動作の設定例を示します。

```
Switch(config)# ip sla 10
Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000
Switch(config-ip-sla-jitter)# frequency 30
Switch(config-ip-sla-jitter)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 10
IP SLAs, Infrastructure Engine-II.

Entry number: 10
Owner:
Tag:
```

```
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 30
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
Enhanced History:
```

関連トピック

UDP ジッター, （111 ページ）

ICMP エコー動作を使用した IP サービス レベルの分析

送信元デバイス上の ICMP エコー動作を設定するには、次の手順を実行します。

はじめる前に

この動作では、IP SLA レスポンダ側を有効にしておく必要はありません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla** *operation-number*
4. **icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface** *interface-id*]
5. **frequency** *seconds*
6. **exit**
7. **ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**]
8. **end**
9. **show running-config**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**ip sla** *operation-number* 例： `Switch(config)# ip sla 10`	IP SLA 動作を作成し、IP SLA コンフィギュレーション モードを開始します。
ステップ 4	**icmp-echo** {*destination-ip-address* | *destination-hostname*} [**source-ip** {*ip-address* | *hostname*} | **source-interface** *interface-id*] 例： `Switch(config-ip-sla)# icmp-echo 172.29.139.134`	IP SLA 動作を ICMP エコー動作として設定し、ICMP エコー コンフィギュレーション モードを開始します。 • *destination-ip-address* | *destination-hostname*：宛先 IP アドレスまたはホスト名を指定します。 •（任意）**source-ip** {*ip-address* | *hostname*}：送信元 IP アドレスまたはホスト名を指定します。 送信元 IP アドレスまたはホスト名が指定されていない場合、IP SLA では、宛先に最も近い IP アドレスが選択されます。 •（任意）**source-interface** *interface-id*：動作に対する送信元インターフェイスを指定します。
ステップ 5	**frequency** *seconds* 例： `Switch(config-ip-sla-echo)# frequency 30`	（任意）指定した IP SLA 動作を繰り返す間隔を設定します。 指定できる範囲は 1 ～ 604800 秒で、デフォルトは 60 秒です。
ステップ 6	**exit** 例： `Switch(config-ip-sla-echo)# exit`	UDP エコー コンフィギュレーション モードを終了します。続いて、グローバル コンフィギュレーション 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 7	**ip sla schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**] 例： `Switch(config)# ip sla schedule 5 start-time now life forever`	個々の IP SLA 動作のスケジューリング パラメータを設定します。 • *operation-number*：RTR エントリ番号を入力します。 •（任意）**life**：動作の実行を無制限（**forever**）に指定するか、秒数（*seconds*）を指定します。 有効な範囲は 0 ～ 2147483647 です。 デフォルトは 3600 秒（1 時間）です。 •（任意）**start-time**：情報の収集を開始する時刻を入力します。 特定の時刻に開始する場合は、時、分、秒（24時間表記）、月日を入力します。 月を入力しない場合、当月がデフォルト設定です。 **pending** と入力すれば、開始時刻を指定するまでは情報を収集しません。 **now** と入力すれば、ただちに動作を開始します。 **after** *hh:mm:ss* と入力すれば、指定した時刻の経過後に動作を開始します。 •（任意）**ageout** *seconds*：情報を収集していないとき、メモリの動作を保存する秒数を指定します。 指定できる範囲は 0 ～ 2073600 秒です。デフォルトは 0 秒（いつまでも保存する）です。 •（任意）**recurring**：毎日、動作を自動的に実行します。
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ICMP エコー IP SLA 動作の設定

次に、ICMP エコー IP SLA 動作の設定例を示します。

```
Switch(config)# ip sla 12
Switch(config-ip-sla)# icmp-echo 172.29.139.134
Switch(config-ip-sla-echo)# frequency 30
Switch(config-ip-sla-echo)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 22
IP SLAs, Infrastructure Engine-II.

Entry number: 12
Owner:
Tag:
Type of operation to perform: echo
Target address: 2.2.2.2
Source address: 0.0.0.0
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Schedule:
    Operation frequency (seconds): 60
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
History Statistics:
    Number of history Lives kept: 0
    Number of history Buckets kept: 15
    History Filter Type: None
Enhanced History:
```

関連トピック

IP SLA 動作のしきい値のモニタリング, （111 ページ）

IP SLA 動作のモニタリング

次の表で、IP SLA 動作の設定と結果を表示するために使用するコマンドについて説明します。

表 *12* : *IP SLA* 動作のモニタリング

show ip sla application	Cisco IOS IP SLA のグローバル情報を表示します。

show ip sla authentication	IP SLA 認証情報を表示します。
show ip sla configuration [*entry-number*]	すべての IP SLA 動作または特定の IP SLA動作に関する、デフォルト値をすべて含めた設定値を表示します。
show ip sla enhanced-history {**collection-statistics** | **distribution statistics**} [*entry-number*]	収集した履歴バケットの拡張履歴統計情報、あるいはすべての IP SLA 動作または特定の IP SLA 動作に関する分散統計情報を表示します。
show ip sla ethernet-monitor configuration [*entry-number*]	IP SLA 自動イーサネット設定を表示します。
show ip sla group schedule [*schedule-entry-number*]	IP SLA グループ スケジューリング設定と個別情報を表示します。
show ip sla history [*entry-number* | **full** | **tabular**]	すべての IP SLA 動作について収集した履歴を表示します。
show ip sla mpls-lsp-monitor {**collection-statistics** | **configuration** | **ldp operational-state** | **scan-queue** | **summary** [*entry-number*] | **neighbors**}	MPLS ラベルスイッチドパス（LSP）ヘルス モニタ動作を表示します。
show ip sla reaction-configuration [*entry-number*]	すべての IP SLA 動作または特定の IP SLA動作に関する、予防的しきい値のモニタリングの設定を表示します。
show ip sla reaction-trigger [*entry-number*]	すべての IP SLA 動作または特定の IP SLA動作に関する反応トリガー情報を表示します。
show ip sla responder	IP SLA レスポンダ側の情報を表示します。
show ip sla statistics [*entry-number* | **aggregated** | **details**]	動作ステータスおよび統計情報の現在値または合計値を表示します。

IP SLA 動作のモニタリングの例

次の例は、アプリケーションごとのすべての IP SLA を示しています。

```
Switch# show ip sla application

        IP Service Level Agreements
```

```
Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III

Supported Operation Types:
        icmpEcho, path-echo, path-jitter, udpEcho, tcpConnect, http
        dns, udpJitter, dhcp, ftp, udpApp, wspApp

Supported Features:
        IPSLAs Event Publisher

IP SLAs low memory water mark: 33299323
Estimated system max number of entries: 24389

Estimated number of configurable operations: 24389
Number of Entries configured  : 0
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0
Time of last change in whole IP SLAs: *13:04:37.668 UTC Wed Dec 19 2012
```

次の例は、すべての IP SLA ディストリビューション統計情報を示しています。

```
Switch# show ip sla enhanced-history distribution-statistics

Point by point Enhanced History
Entry    = Entry Number
Int      = Aggregation Interval
BucI     = Bucket Index
StartT   = Aggregation Start Time
Pth      = Path index
Hop      = Hop in path index
Comps    = Operations completed
OvrTh    = Operations completed over thresholds
SumCmp   = Sum of RTT (milliseconds)
SumCmp2L = Sum of RTT squared low 32 bits (milliseconds)
SumCmp2H = Sum of RTT squared high 32 bits (milliseconds)
TMax     = RTT maximum (milliseconds)
TMin     = RTT minimum (milliseconds)

Entry Int BucI StartT     Pth Hop Comps OvrTh SumCmp     SumCmp2L    SumCmp2H    T
Max    TMin
```

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
Cisco Medianet Metadata Guide	http://www.cisco.com/en/US/docs/ios-xml/ios/mdata/configuration/15-sy/mdata-15-sy-book/mdata-framework.pdf
Cisco Media Services Proxy Configuration Guide	http://www.cisco.com/en/US/docs/ios-xml/ios/msp/configuration/15-mt/msp-15-mt-book.pdf
Cisco Mediatrace and Cisco Performance Monitor Configuration Guide	http://www.cisco.com/en/US/docs/ios-xml/ios/mcl_mmon/configuration/15-mt/mm-15-mt-book/mm-mediatrace.pdf

ネットワーク管理コンフィギュレーション ガイド、**Cisco IOS XE Release 3.6E**（**Catalyst 3850** スイッチ）

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
なし	-

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	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
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。 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。 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。	http://www.cisco.com/support

サービス レベル契約の機能の履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SECisco IOS XE 3.2SE	この機能が導入されました。

第 7 章

ローカル ポリシーの設定

- 機能情報の確認，131 ページ
- ローカル ポリシー設定の制約事項，131 ページ
- ローカル ポリシーの設定に関する情報，132 ページ
- ローカル ポリシーの設定方法，133 ページ
- ローカル ポリシーのモニタリング，142 ページ
- 例：ローカル ポリシーの設定，143 ページ
- ローカル ポリシーの設定に関する追加情報，144 ページ
- ローカル ポリシーの設定の実行に関する機能履歴，145 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。 最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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。

ローカル ポリシー設定の制約事項

switchでサポートされているポリシーマップの属性は、QoS、VLAN、セッションタイムアウト、および ACL です。

ローカル ポリシーの設定に関する情報

ローカル ポリシーは、HTTP と DHCP に基づいてデバイスをプロファイリングして、ネットワーク上のエンド デバイスを識別することができます。 ユーザは、デバイス ベースのポリシーを設定し、ネットワーク上でユーザまたはデバイス ポリシーごとにポリシーを適用できます。

ローカルポリシーにより、モバイルデバイスのプロファイリングと、特定のVLANへのプロファイリングされたデバイスの基本的なオンボーディングが可能になります。 また、ACLおよびQoSを割り当てたり、セッション タイムアウトを設定します。

2 つの個別のコンポーネントとしてローカル ポリシーを設定できます。

- ネットワークに参加するクライアントに固有のサービス テンプレートとしてのポリシー属性の定義およびポリシー一致基準の適用。
- ポリシーへの一致基準の適用。

次のポリシー一致属性は、ローカル ポリシーを設定するために使用されます。

- デバイス：デバイスのタイプを定義します。 Windowsベースのコンピュータ、スマートフォン、iPad や iPhone などの Apple デバイス。
- ユーザ名：ユーザのユーザ名を定義します。
- ユーザ ロール：学生や従業員など、ユーザ タイプまたはユーザが属するユーザ グループを定義します。
- MAC：エンド ポイントの mac-address を定義します。
- MAC OUI：mac-address OUI を定義します。

エンドポイントごとにこれらのパラメータに対応する一致がswitchにあると、ポリシーを追加できます。 ポリシーの適用により、次のセッション属性に基づいてモバイルデバイスの基本的なデバイス オンボーディングが可能になります。

- VLAN
- QoS
- ACL
- Session timeout

これらのポリシーを設定して、指定されたポリシーでエンドポイントを適用できます。 ワイヤレス クライアントは、MAC OUI、DHCP および HTTP ユーザ エージェント（正常な HTTP プロファイリングには有効なインターネットが必要です）MAC OUI および DHCP に基づいてプロファイリングされます。 switchは、これらの属性と事前定義された分類プロファイルを使用してデバイスを識別します。

デフォルトのプロファイル テキスト ファイルの置き換え

新しいデバイスが分類されていない場合は、デバイスの MAC アドレスを使用してシスコ サポート チームにお問い合わせください。 シスコ サポート チームにより、新しい **dc_default_profile.txt**

ファイルが提供されます。そのファイルにはMACアドレスが含まれています。**dc_default_profile.txt** ファイルを以前のファイルと置き換える必要があります。 **dc_default_profile.txt** ファイルを変更するには、次の手順に従ってください。

1 次のコマンドを入力して、デバイスの分類子を停止します。
switch**(config)# no device classifier**

2 次のコマンドを入力して、ファイルをコピーします。
switch**# device classifier profile location** *filepath*

3 次のコマンドを入力して、デバイスの分類子を開始します。
switch**(config)# device classifier**

トランク ポートのセッション モニタのディセーブル化

アップリンク トランク ポートでは、セッション モニタリングを作成しないでください。 デフォルトでは、セッション モニタリングがイネーブルになっています。 セッション モニタリングをディセーブルにする必要があります。

1 次のコマンドを入力して、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。
switch**# configure terminal**

2 次のコマンドを入力して、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。
switch**(config)# interface** *interface-id*

3 次のコマンドを入力して、セッション モニタリングをディセーブルにします。
switch**(config-if)# no access-session monitor**

ローカル ポリシーの設定方法

ローカル ポリシーの設定（CLI）

ローカル ポリシーを設定するには、次の手順を完了します。

1 サービス テンプレートを作成します。
2 インターフェイス テンプレートを作成します。
3 パラメータ マップを作成します。
4 ポリシー マップを作成します。
5 WLAN でローカル ポリシーを適用します。

サービス テンプレートの作成（CLI）

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	**service-template** *service-template-name*
	
	例：
	`Switch(config)# service-template cisco-phone-template`
	`Switch(config-service-template)#`
		サービス テンプレート 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	**access-group** *acl_list* 例： `Switch(config-service-template)# access-group foo-acl`	適用するアクセス リストを指定します。
ステップ 4	**vlan** *vlan_id* 例： `Switch(config-service-template)# vlan 100`	VLAN ID を指定します。 1 ～ 4094 の値を指定できます。
ステップ 5	**absolute-timer** *seconds* 例： `Switch(config-service-template)# absolute-timer 20`	サービステンプレートのセッションタイムアウト値を指定します。 1～65535 の値を指定できます。
ステップ 6	**service-policy qos** {**input** | **output**} 例： `Switch(config-service-template)# service-policy qos input foo-qos`	クライアントの QoS ポリシーを設定します。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

インターフェイス テンプレートの作成（CLI）

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	**template** *interface-template-name*
	
	例：
	
	`Switch(config)# template cisco-phone-template`
	`Switch(config-template)#`
		インターフェイス テンプレート 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	**switchport mode access** 例： `Switch(config-template)# switchport mode access`	トランキングなし、タグなしの単一 VLAN イーサネット インターフェイスとして、インターフェイスを設定します。 アクセス ポートは、1 つの VLAN のトラフィックだけを伝送できます。 アクセス ポートは、デフォルトで、VLAN 1 のトラフィックを送受信します。
ステップ 4	**switchport voice vlan** *vlan_id* 例： `Switch(config-template)# switchport voice vlan 20`	指定された VLAN 経由ですべての音声トラフィックを転送するように指定します。 1 ～ 4094 の値を指定できます。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

パラメータ マップの作成（CLI）

クラス マップよりもパラメータ マップを使用することが推奨されます。

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	**parameter-map type subscriber attribute-to-service** *parameter-map-name* 例： `Switch(config)# parameter-map type subscriber attribute-to-service Aironet-Policy-para`	パラメータ マップのタイプと名前を指定します。
ステップ 3	*map-index* **map** { **device-type** | **mac-address** | **oui** | **user-role** | **username**} {**eq** | **not-eq** | **regex** *filter-name* } 例： `Switch(config-parameter-map-filter)# 10 map device-type eq "WindowsXP-Workstation"`	パラメータ マップの属性フィルタ基準を指定します。

ステップ 4	**service-template** *service-template-name*
	
	例：
	`Switch(config-parameter-map-filter-submode)# service-template cisco-phone-template`
	`Switch(config-parameter-map-filter-submode)#`
		サービステンプレート コンフィギュレーション モードを開始します。

ステップ 5	**interface-template** *interface-template-name*
	
	例：
	`Switch(config-parameter-map-filter-submode)# interface-template cisco-phone-template`
	`Switch(config-parameter-map-filter-submode)#`
		サービステンプレート 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	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

クラス マップの作成（CLI）

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	**class-map type control subscriber** *class-map-name* { **match-all** | **match-any** | **match-first** } 例： `Switch(config)# class-map type control subscriber CLASS_AC_1 match-all`	クラス マップのタイプと名前を指定します。
ステップ 3	**match** {**device-type** | **mac-address** | **oui** | **username** | **userrole**} *filter-type-name* 例： `Switch(config-class-map)# match device-type Cisco-IP-Phone-7961`	クラス マップの属性フィルタ基準を指定します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ポリシー マップの作成（CLI）

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	**policy-map type control subscriber** *policy-map-name*	ポリシー マップのタイプを指定します。

	コマンドまたはアクション	目的
	例： `Switch(config)# policy-map type control subscriber Aironet-Policy`	
ステップ 3	**event identity-update** {**match-all** | **match-first**} 例： `Switch(config-policy-map)# event identity-update match-all`	ポリシーマップに一致基準を指定します。
ステップ 4	*class_number* **class** {*class_map_name* | **always** } {**do-all** | **do-until-failure** | **do-until-success**} 例： `Switch(config-class-control-policymap)# 1 class local_policy1_class do-until-success`	ローカル プロファイリングのポリシー クラス マップ番号を設定し、操作の実行方法を指定します。クラスマップ コンフィギュレーション モードには、次のコマンド オプションが含まれます。 • **always**：一致を行うことなく実行しますが、success を返します。 • **do-all**：すべてのアクションを実行します。 • **do-until-failure**：一致の失敗が発生するまですべてのアクションを実行します。 これはデフォルト値です。 • **do-until-success**：一致の成功が発生するまですべてのアクションを実行します。
ステップ 5	*action-index* **map attribute-to-service table** *parameter-map-name* 例： `Switch(config-policy-map)# 10 map attribute-to-service table Aironet-Policy-para`	使用するパラメータ マップ テーブルを指定します。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

WLAN 上のデバイスへのローカル ポリシーの適用（CLI）

はじめる前に

サービス ポリシーがパラメータ マップにデバイス タイプに基づくルールを含んでいる場合は、デバイスの分類子がすでにイネーブルになっ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	**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	**wlan** *wlan-name* 例： `Switch(config)# wlan wlan1`	WLAN 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	**service-policy type control subscriber** *policymapname* 例： `Switch(config-wlan)# service-policy type control subscriber Aironet-Policy`	WLAN にローカル ポリシーを適用します。
ステップ 4	**profiling local http**（任意） 例： `Switch(config-wlan)# profiling local http`	HTTP プロトコルに基づいて、デバイスのプロファイリングのみをイネーブルにします（任意）。
ステップ 5	**profiling radius http**（任意） 例： `Switch(config-wlan)# profiling radius http`	ISE 上のデバイスのプロファイリングをイネーブルにします（任意）。
ステップ 6	**no shutdown** 例： `Switch(config-wlan)# no shutdown`	WLANをシャットダウンしないように指定します。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ローカル ポリシーの設定（GUI）

ローカル ポリシーを設定するには、次の手順を完了します。

1 サービス テンプレートを作成します。
2 ポリシー マップを作成します。
3 ユーザが作成したローカル ポリシーを WLAN に適用します。

サービス テンプレートの作成（GUI）

ステップ 1 [Configuration] > [Security] > [Local Policies] > [Service Template] を選択し、[Service Template] ページを開きます。

ステップ 2 次のようにして、新しいテンプレートを作成します。

a) [New] をクリックして、[Service Template] > [New] ページを開きます。
b) [Service Template name] テキスト ボックスに、新しいサービス テンプレート名を入力します。
c) [VLAN ID] テキスト ボックスに、ポリシーに関連付ける必要のある VLAN ID を入力します。 値の範囲は 1 ～ 4094 です。
d) [Session timeout] テキスト ボックスに、最大時間を秒単位で入力します。この後、クライアントは強制的に再認証されます。 値の範囲は、1 ～ 65535 秒です。
e) [Access control list] ドロップダウン リストから、ポリシーにマッピングされるアクセス コントロール リストを選択します。
f) [Ingress QoS] ドロップダウン リストから、適用させる入力 QoS ポリシーを選択します。
g) [Egress QoS] ドロップダウン リストから、適用させる出力 QoS ポリシーを選択します。
h) [Apply] をクリックして、設定を保存します。

ステップ 3 次のようにサービス テンプレートを編集します。

a) [Service Template] ページから、サービス テンプレートをクリックして [Service Template] > [Edit] ページを開きます。
b) [VLAN ID] テキスト ボックスに、ポリシーに関連付ける必要のある VLAN ID を入力します。 値の範囲は 1 ～ 4094 です。
c) [Session timeout] テキスト ボックスに、最大時間を秒単位で入力します。この後、クライアントは強制的に再認証されます。 値の範囲は、1 ～ 65535 秒です。
d) [Access control list] ドロップダウン リストから、ポリシーにマッピングされるアクセス コントロール リストを選択します。
e) [Ingress QoS] ドロップダウン リストから、適用させる入力 QoS ポリシーを選択します。
f) [Egress QoS] ドロップダウン リストから、適用させる出力 QoS ポリシーを選択します。
g) [Apply] をクリックして、設定を保存します。

ステップ 4 次のようにサービス テンプレートを削除します。

a) [Service Template] ページから、サービス テンプレートを選択します。

b) [Remove] をクリックします。
c) [Apply] をクリックして、設定を保存します。

ポリシー マップの作成（GUI）

ステップ 1 [Configuration] > [Security] > [Local Policies] > [Policy Map] を選択し、[Policy Map] ページを開きます。

ステップ 2 新しいポリシー マップを次のように作成します。

a) [New] をクリックして、[Policy Map] > [New] ページを開きます。
b) [Policy Map name] テキスト ボックスに、新しいポリシー マップの名前を入力します。
c) [Add] をクリックして、[Match Criteria] 領域を開きます。
d) [Device Type]ドロップダウン リストから、デバイス タイプを選択します。 デバイス タイプの一致基準は、選択しているデバイス タイプごとに、eq、not-eq、または regex を指定できます。
e) [User Role] ドロップダウン リストから、一致基準を eq、not-eq、または regex から選択し、ユーザ タイプまたはユーザのユーザ グループ（たとえば、学生、教員など）を入力します。
f) [Service Template] ドロップダウン リストから、ポリシーにマッピングされるサービス テンプレートを選択します。
g) [Add] をクリックします。 一致基準が一致基準リストに追加されます。
h) [Match Criteria Lists] 領域で、[Add] をクリックしてポリシーに一致基準を追加します。
i) [Apply] をクリックして、設定を保存します。

ステップ 3 ポリシー マップを次のように編集します。

a) [Policy Map] ページで、編集するポリシー マップを選択し、[Edit] をクリックして [Policy Map] > [Edit] ページを開きます。
b) [Match Criteria] 領域で、[Device Type] ドロップダウン リストからデバイス タイプを選択します。 デバイス タイプの一致基準は、選択しているデバイス タイプごとに、eq、not-eq、または regex を指定できます。
c) [Match Criteria] 領域で、[User Role] ドロップダウン リストからユーザ ロールを選択します。 一致基準を eq、not-eq、または regex から選択し、ユーザ タイプまたはユーザのユーザ グループを入力します。
d) [Service Template] ドロップダウン リストから、ポリシーにマッピングされるサービス テンプレートを選択します。
e) 設定を保存するには [Ok] を、または設定を破棄するには [Cancel] をクリックします。
f) デバイス タイプ、ユーザ ロール、サービス テンプレートに基づいて追加の一致基準をポリシーに追加するには、[Add] をクリックします。
g) [Match Criteria Lists] 領域で、一致基準を選択し、[Move to] をクリックして行テキスト ボックスに入力した値に対して一致基準を移動させます。
h) 一致基準をリストの上に移動させるには、一致基準を選択し、[Move up] をクリックします。
i) 一致基準をリストの下に移動させるには、一致基準を選択し、[Move down] をクリックします。

j) ポリシー マップ リストから一致基準を削除するには、一致基準を選択し、[Remove] をクリックします。
k) [Apply] をクリックして、設定を保存します。

ステップ 4 ポリシー マップを次のように削除します。

a) [Policy Map] ページから、ポリシー マップを選択します。
b) [Remove] をクリックします。
c) [Apply] をクリックして、設定を保存します。

WLAN へのローカル ポリシーの適用（GUI）

ステップ 1 [Configuration] > [Wireless] > [WLAN] を選択して、[WLANs] ページを開きます。
ステップ 2 対応する WLAN プロファイルをクリックします。 [WLANs > Edit] ページが表示されます。
ステップ 3 [Policy-Mapping] タブをクリックします。
ステップ 4 [Device Classification] チェックボックスをオンにして、デバイス タイプに基づいた分類をイネーブルにします。
ステップ 5 [Local Subscriber Policy] ドロップダウン リストから、WLAN に適用させるポリシーを選択します。
ステップ 6 [Local HTTP Profiling] を選択して、HTTP に基づいてデバイスのプロファイリングをイネーブルにします（任意）。
ステップ 7 [Radius HTTP Profiling] を選択して、RADIUS に基づいてデバイスのプロファイリングをイネーブルにします（任意）。
ステップ 8 [Apply] をクリックして、設定を保存します。

ローカル ポリシーのモニタリング

次のコマンドを使用して、switchで設定されたローカル ポリシーを監視できます。

表 *13*：ローカル ポリシーのモニタリング コマンド

コマンド	目的
show access-session	表示される各クライアントまたは MAC アドレスの承認ステータス、方式、およびドメインを含むアクセスセッションのサマリーを表示します。

show access-session cache	クライアントの最新の分類を表示します。
show device classifier attached detail	Mac、DHCP、HTTP などのパラメータに基づいてクライアントの最新の分類を表示します。
show access-session mac *mac-address* **details**	マッピングされたポリシー、使用されたサービステンプレート、およびクライアントの属性を表示します。
show access-session mac *mac-address* **policy**	マッピングされたポリシー、使用されたサービステンプレート、およびクライアントの属性を表示します。 また、次の情報を表示する [Resultant Policy] も確認できます。 • セッションが属性をローカルで設定している場合にセッションに適用された最終属性。 • サーバから適用された属性。

例：ローカル ポリシーの設定

次に、サービス テンプレートを作成する例を示します。

```
Switch(config)# service-template test3
Switch(config-service-template)# access-group josephacl
Switch(config-service-template)# vlan 137
Switch(config-service-template)# absolute-timer 500
Switch(config-service-template)#  service-policy qos input qosingress
Switch(config-service-template)# end
```

次に、パラメータ マップを作成する例を示します。

```
Switch(config)# parameter-map type subscriber attribute-to-service apple-tsim-param
Switch(config-parameter-map)# 1 map device-type eq "Apple-Device"
Switch(config-parameter-map)# 1 service-template test1
Switch(config-parameter-map)# 2 map device-type eq "Apple-Ipad"
Switch(config-parameter-map)# 1 service-template test2
Switch(config-parameter-map)# 3 map device-type eq "Android"
Switch(config-parameter-map)# 1 service-template test3
Switch(config-parameter-map)# end
```

（注） 各コンフィギュレーション コマンド ラインの最後に CTRL Z を入力して、コマンドを実行し次の行に移動します。

次に、インターフェイス テンプレートを作成する例を示します。

```
Switch# configure terminal
Switch(config)#template cisco-phone-template
Switch(config-template)#switchport mode access
Switch(config-template)#switchport voice vlan 20
Switch(config-template)# end
```

次に、パラメータ マップを作成する例を示します。

```
Switch# configure terminal
Switch(config)#parameter-map type subscriber attribute-to-service param-wired
Switch(config-parameter-map-filter)#10 map device-type regex Cisco-IP-Phone
Switch(config-parameter-map-filter-submode)#10 interface-template cisco-phone-template
Switch(config-parameter-map)# end
```

次に、ポリシー マップを作成する例を示します。

```
Switch(config)# policy-map type control subscriber apple-tsim
Switch(config-policy-map)# event identity-update match-all
Switch(config-policy-map)# 1 class always do-until-failure
Switch(config-policy-map)# 1 map attribute-to-service table apple-tsim-param
Switch(config-policy-map)# end
```

次に、WLAN 上のデバイスにポリシーを適用する例を示します。

```
Switch(config)# wlan wlan1
Switch(config-wlan)# client vlan VLAN0054
Switch(config-wlan)# profiling local http
Switch(config-wlan)# service-policy type control subscriber apple-tsim
Switch(config-wlan)# no shutdown
Switch# end
```

ローカル ポリシーの設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*（セキュリティ コマンド リファレンス ガイド、*Cisco IOS XE Release 3SE*（*Cisco WLC 5700* シリーズ））

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	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	Link
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。 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。 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。	http://www.cisco.com/support

ローカル ポリシーの設定の実行に関する機能履歴

リリース	機能情報
Cisco IOS XE 3E	この機能が導入されました。

ネットワーク管理コンフィギュレーション ガイド、**Cisco IOS XE Release 3.6E**（**Catalyst 3850** スイッチ）

第 8 章

SPAN および RSPAN の設定

- 機能情報の確認，147 ページ
- SPAN および RSPAN の前提条件，148 ページ
- SPAN および RSPAN の制約事項，148 ページ
- SPAN および RSPAN について，151 ページ
- SPAN および RSPAN の設定方法，165 ページ
- SPAN および RSPAN 動作のモニタリング，190 ページ
- SPAN および RSPAN の設定例，191 ページ
- その他の関連資料，193 ページ
- SPAN および RSPAN の機能の履歴と情報，195 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。 最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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

- 各switchでは、最大で 8 つの送信元セッションおよび 58 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。
- switch ポートを SPAN 宛先ポートとして設定すると、通常のswitch 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。
- スタックは、LAN Base イメージを実行しているスイッチのみでサポートされています。

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。
- switchは、最大 2 つのローカル SPAN または RSPAN 送信元セッションをサポートします。
  - 同じswitchまたはswitch 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。 switchまたはswitch スタックは合計 66 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 switch スタックあたりに設定できる宛先ポートは最大で 66 個です。
- SPANセッションがswitch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。
- switch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switchまたはswitch 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 は、BPDU パケット モニタリングまたは他のレイヤ 2 switch 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switches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、switchはスパンされたトラフィックをモニタしないため、switch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ッディングが防止されます。
- RSPAN を使用するには、スイッチが LAN Base イメージを実行している必要があります。

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

- 複数の SPAN または RSPAN セッションに ACL をアタッチできます。 ただし、ACL のサイズは FSPAN に割り当てられたメモリ TCAM のサイズを超過することはできません。
- 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。
- switch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、switchのリブート後、switch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switch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switch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switch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に出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。

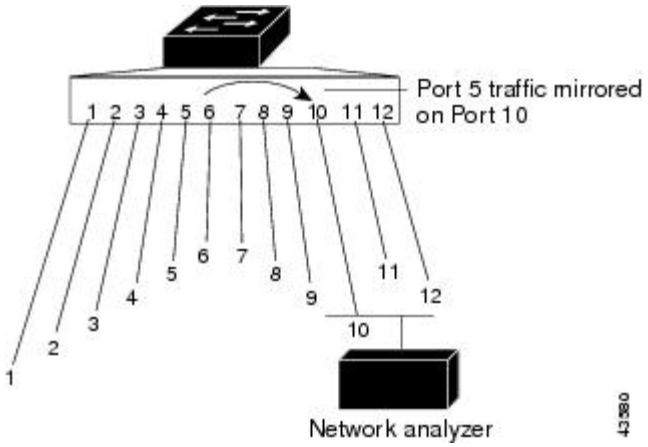
ネットワーク セキュリティ デバイスからトラフィックを注入する場合、SPAN または RSPAN 宛先ポートを使用できます。 たとえば、Cisco侵入検知システム（IDS）センサー装置を宛先ポートに接続した場合、IDSデバイスはTCPリセットパケットを送信して、疑わしい攻撃者のTCPセッションを停止させることができます。

ローカル SPAN

ローカル SPAN は 1 つのswitch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switchまたはswitch 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。

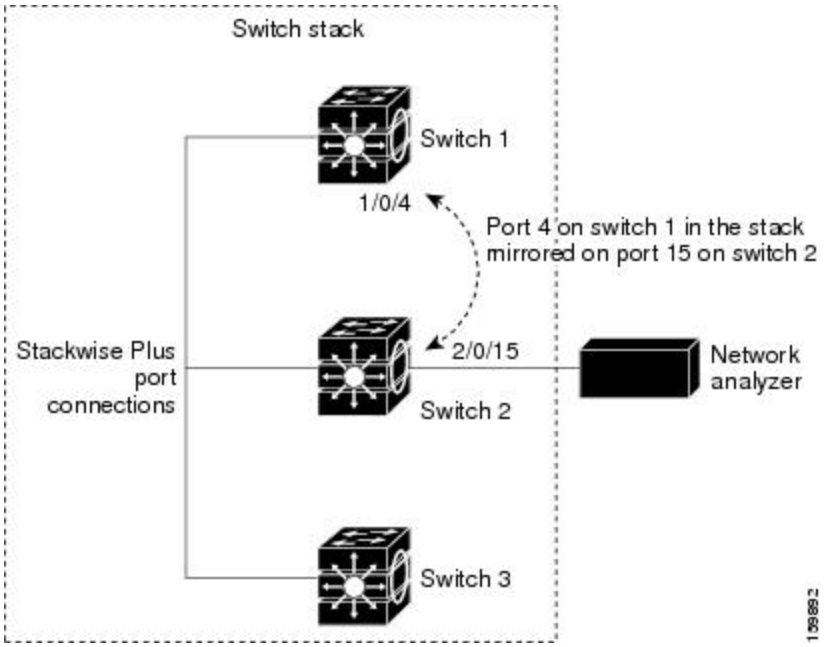
ポート 5（送信元ポート）上のすべてのトラフィックがポート 10（宛先ポート）にミラーリングされます。 ポート 10 のネットワーク アナライザは、ポート 5 に物理的には接続されていませんが、ポート 5 からのすべてのネットワーク トラフィックを受信します。

図 *7*：単一デバイスでのローカル *SPAN* の設定例



これは、switch 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 *8*：デバイス スタックでのローカル *SPAN* の設定例



関連トピック

ローカル SPAN セッションの作成，（165 ページ）
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，（168 ページ）

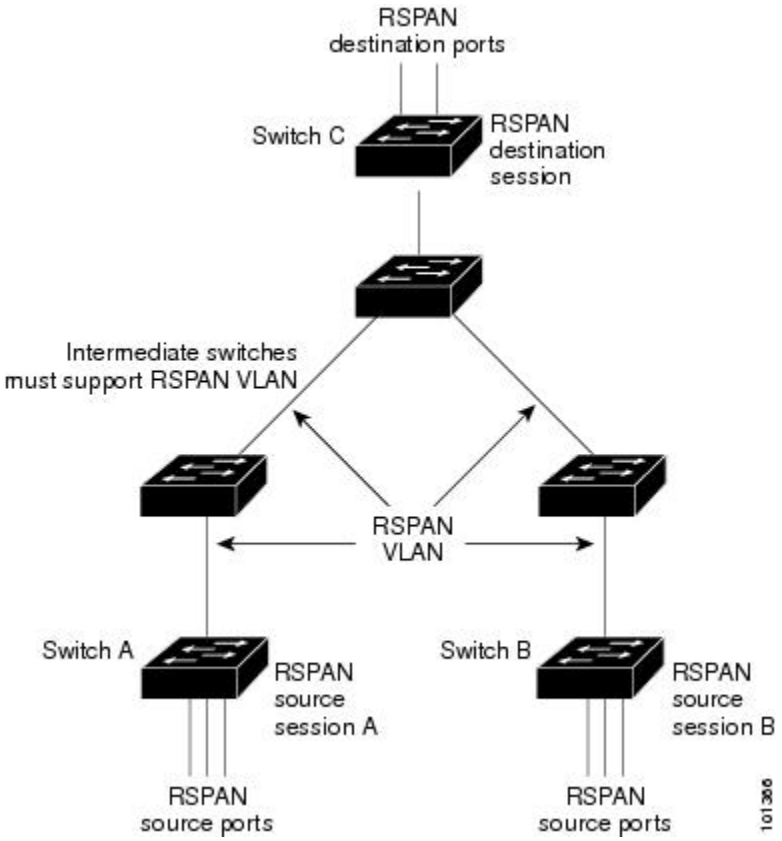
例：ローカル SPAN の設定, （191 ページ）

リモート SPAN

RSPAN は、異なるswitches（または異なるswitch 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ので、ネットワーク上で複数のswitchesをリモートモニタリングできます。

次の図に、Switch A およびSwitch 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switches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switch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Switch C のように、宛先は常に物理ポートになります。

図 *9*：*RSPAN* の設定例



関連トピック

RSPAN 送信元セッションの作成, （175 ページ）
RSPAN 宛先セッションの作成, （179 ページ）

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, （182 ページ）
例：RSPAN VLAN の作成, （192 ページ）

SPAN と RSPAN の概念および用語

• SPAN セッション
• 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パケット 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switch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 のタギングを除去し、宛先ポートに送ります。 セッションは、（レイヤ 2 制御パケットを除く）すべての RSPAN VLAN パケットのコピーを分析のためにユーザに提供します。

複数のソースおよび宛先ポートを持つ単一 RSPAN セッションを同じセッションに使用できますが、ソースが同じリモート VLAN であるソース セッションの複数使用は許可されていません。

SPAN セッションでのトラフィックのモニタには、次のような制約があります。

- 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。
- switchは、最大 2 つのローカル SPAN または RSPAN 送信元セッションをサポートします。
  - 同じswitchまたはswitch 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。 switchまたはswitch 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switch 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switch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）。 したがって、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。
- switch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switchまたはswitch 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。

関連トピック

ローカル SPAN セッションの作成, （165 ページ）
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, （168 ページ）
例：ローカル SPAN の設定, （191 ページ）

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、switch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、switch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、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。

Switch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。

- switchの輻輳が原因でドロップされた出力パケットは、出力SPANからもドロップされます。

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switch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。 switchは、任意の数の送信元ポート（switch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、switch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（2 つ）（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switchまたはswitch スタックに存在している必要があります。 RSPAN セッションの場合は、RSPAN 宛先セッションを含むswitch上にあります。 RSPAN 送信元セッションのみを実行するswitchまたはswitch 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、変更は有効になりません。

（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 グループにすることができます。
- 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。
- switchまたはswitch 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switches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。

関連トピック

RSPAN 送信元セッションの作成，（175 ページ）
RSPAN 宛先セッションの作成，（179 ページ）
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，（182 ページ）
例：RSPAN VLAN の作成，（192 ページ）

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 switch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、switch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、switches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、未編集のパケットが 1 つだけ SPAN宛先ポートに送信されます。 マルチキャスト パケット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

switchesのスタックは1つの論理switch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switchesである場合があります。 したがって、スタック内でのswitches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。 switchがスタックから削除されると、アクティブ セッションが非アクティブになります。また、switch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、switch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、switch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switches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switches上でアンロードされたものとして処理され、switch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switches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。

関連トピック

FSPAN セッションの設定, （184 ページ）
FRSPAN セッションの設定, （187 ページ）

SPAN および RSPAN のデフォルト設定

表 *14* : *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。

関連トピック

ローカル SPAN セッションの作成, （165 ページ）
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, （168 ページ）
例：ローカル SPAN の設定, （191 ページ）

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、特定のパケット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switches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switches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 ステートになります。
- 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switches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switchesで RSPAN がサポートされている。

関連トピック

RSPAN 送信元セッションの作成, （175 ページ）
RSPAN 宛先セッションの作成, （179 ページ）

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, （182 ページ）
例：RSPAN VLAN の作成, （192 ページ）

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。

関連トピック

FSPAN セッションの設定, （184 ページ）
FRSPAN セッションの設定, （187 ページ）

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、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]
5. **monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**]}
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**no monitor session** {*session_number* | **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。 • *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 4	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**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。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* には、モニタ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** *port-channel-number*）があります。 有効なポートチャネル番号は 1 ～ 48 です。 • *vlan-id* 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。 • （任意）**both** | **rx** | **tx**：モニタ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

	コマンドまたはアクション	目的
		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。 ◦ **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。 （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。
ステップ 5	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**]} 例： `Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2 encapsulation replicate`	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。 （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。 • *session_number* には、ステップ 4 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。 （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。 （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。
ステップ 6	**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 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ローカル SPAN, （151 ページ）
SPAN セッション, （154 ページ）
SPAN 設定時の注意事項, （164 ページ）

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、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**no monitor session** {*session_number* | **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。 • *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 4	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**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 5	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**] [**ingress** {**dot1q vlan** *vlan-id* | **isl** | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]} 例： `Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate ingress dot1q vlan 6`	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。 • *session_number* には、ステップ 4 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）[**,** | **-**]：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

	コマンドまたはアクション	目的
		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。 ◦ **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。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

ローカル SPAN, （151 ページ）
SPAN セッション, （154 ページ）
SPAN 設定時の注意事項, （164 ページ）
例：ローカル SPAN の設定, （191 ページ）

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、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session** *session_number* **source interface** *interface-id*
5. **monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**]
6. **monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**]}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**no monitor session** {*session_number* | **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。 • *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 4	**monitor session** *session_number* **source interface** *interface-id* 例： `Switch(config)# monitor session 2`	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。 • *session_number* の範囲は、1 ～ 66 です。

	コマンドまたはアクション	目的
	source interface gigabitethernet1/0/2 rx	• *interface-id* 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 5	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**] 例： `Switch(config)# monitor session 2 filter vlan 1 - 5 , 9`	SPAN 送信元トラフィックを特定の VLAN に制限します。 • *session_number* には、ステップ 4 で指定したセッション番号を入力します。 • *vlan-id* 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 6	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**]} 例： `Switch(config)# monitor session 2 destination interface gigabitethernet1/0/1`	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。 • *session_number* には、ステップ 4 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 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

RSPAN VLAN としての VLAN の設定

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、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **vlan** *vlan-id*
4. **remote-span**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**vlan** *vlan-id* 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 4	**remote-span** 例： `Switch(config-vlan)# remote-span`	VLAN を RSPAN VLAN として設定します。
ステップ 5	**end** 例： `Switch(config-vlan)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

RSPAN に参加するすべてのswitches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 switchに RSPAN VLAN を作成し、VTP がこの RSPAN VLAN を VTP ドメイン内の他のswitches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switches、および中間switches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、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]
5. **monitor session** *session_number* **destination remote vlan** *vlan-id*
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**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。 • *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。

	コマンドまたはアクション	目的
ステップ 4	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**] 例： `Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 tx`	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。 • *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。 ◦ *interface-id* 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** *port-channel-number*）があります。 有効なポートチャネル番号は 1 ～ 48 です。 ◦ *vlan-id* 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）。 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。 • （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。 ◦ **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 5	**monitor session** *session_number* **destination remote vlan** *vlan-id* 例： `Switch(config)# monitor session 1 destination remote vlan 100`	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。 • *session_number* には、ステップ 4 で指定した番号を入力します。 • *vlan-id* には、モニタする送信元 RSPAN VLAN を指定します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

リモート SPAN, （153 ページ）
RSPAN VLAN, （160 ページ）
RSPAN 設定時の注意事項, （164 ページ）

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、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session** *session_number* **source interface** *interface-id*
5. **monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**]
6. **monitor session** *session_number* **destination remote vlan** *vlan-id*
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Switch(config)# no monitor session 2`	セッションに対する既存の SPAN 設定を削除します。 • *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 4	**monitor session** *session_number* **source interface** *interface-id* 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。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* 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 5	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**] 例： `Switch(config)# monitor session 2 filter vlan 1 - 5 , 9`	SPAN 送信元トラフィックを特定の VLAN に制限します。 • *session_number* には、ステップ 4 で指定したセッション番号を入力します。 • *vlan-id* 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。

	コマンドまたはアクション	目的
ステップ 6	**monitor session** *session_number* **destination remote vlan** *vlan-id* 例： `Switch(config)# monitor session 2 destination remote vlan 902`	RSPAN セッションおよび宛先リモート VLAN（RSPAN VLAN）を指定します。 • *session_number* には、ステップ 4 で指定したセッション番号を入力します。 • *vlan-id* 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 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

RSPAN 宛先セッションの作成

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

このswitch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、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **vlan** *vlan-id*
4. **remote-span**
5. **exit**
6. **no monitor session** {*session_number* | **all** | **local** | **remote**}
7. **monitor session** *session_number* **source remote vlan** *vlan-id*
8. **monitor session** *session_number* **destination interface** *interface-id*
9. **end**
10. **show running-config**
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**vlan** *vlan-id* 例： `Switch(config)# vlan 901`	送信元switch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switches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 3 ～ 5 は不要です。
ステップ 4	**remote-span** 例： `Switch(config-vlan)# remote-span`	VLAN を RSPAN VLAN として識別します。
ステップ 5	**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。

	コマンドまたはアクション	目的
ステップ 6	**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。 • *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 7	**monitor session** *session_number* **source remote vlan** *vlan-id* 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。 • *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 8	**monitor session** *session_number* **destination interface** *interface-id* 例： `Switch(config)# monitor session 1 destination interface gigabitethernet2/0/1`	RSPAN セッションと宛先インターフェイスを指定します。 • *session_number* には、ステップ 7 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。
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show running-config** 例： `Switch# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

リモート SPAN, （153 ページ）
RSPAN VLAN, （160 ページ）
RSPAN 設定時の注意事項, （164 ページ）

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ネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session** *session_number* **source remote vlan** *vlan-id*
5. **monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**ingress** {**dot1q vlan** *vlan-id* | **isl** | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]}
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**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 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Switch(config)# no monitor session 2`	セッションに対する既存の SPAN 設定を削除します。 • *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 4	**monitor session** *session_number* **source remote vlan** *vlan-id* 例： `Switch(config)# monitor session 2 source remote vlan 901`	RSPAN セッションと送信元 RSPAN VLAN を指定します。 • *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 5	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**ingress** {**dot1q vlan** *vlan-id* | **isl** | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]} 例： `Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress vlan 6`	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。 • *session_number* には、ステップ 5 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
		◦ **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** *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転送します。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

リモート SPAN, （153 ページ）
RSPAN VLAN, （160 ページ）
RSPAN 設定時の注意事項, （164 ページ）
例：RSPAN VLAN の作成, （192 ページ）

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、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Switch(config)# no monitor session 2`	セッションに対する既存の SPAN 設定を削除します。 • *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 4	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**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。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* 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** *port-channel-number*）があります。 有効なポートチャネル番号は 1 ～ 48 です。

	コマンドまたはアクション	目的
		• *vlan-id* 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）**[,**	**-]**：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。 （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。
ステップ 5	**monitor session** *session_number* **destination** {**interface** *interface-id* **[,** | **-] [encapsulation replicate]**} 例： `Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate`	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。 • *session_number* には、ステップ 4 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。 ◦ *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。 ◦ （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。

	コマンドまたはアクション	目的
		（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。 **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。
ステップ 6	**monitor session** *session_number* **filter** {**ip** | **ipv6** | **mac**} **access-group** {*access-list-number* | *name*} 例： `Switch(config)# monitor session 2 filter ipv6 access-group 4`	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。 • *session_number* には、 手順 4： • *access-list-number* 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。 • *name* 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 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

フローベースの SPAN, （162 ページ）
FSPAN および FRSPAN 設定時の注意事項, （165 ページ）

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、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**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 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Switch(config)# no monitor session 2`	セッションに対する既存の SPAN 設定を削除します。 • *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 4	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**] 例： `Switch(config)# monitor session`	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。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* 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

	コマンドまたはアクション	目的
	2 source interface gigabitethernet1/0/1	よびポート チャネル論理インターフェイス（**port-channel** *port-channel-number*）があります。 有効なポートチャネル番号は 1 ～ 48 です。 • *vlan-id* 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）[**,**	**-**]：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。 （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。
ステップ 5	**monitor session** *session_number* **destination remote vlan** *vlan-id* 例： `Switch(config)# monitor session 2 destination remote vlan 5`	RSPAN セッションと宛先 RSPAN VLAN を指定します。 • *session_number* には、ステップ 4 で指定した番号を入力します。 • *vlan-id* には、モニタする宛先 RSPAN VLAN を指定します。
ステップ 6	**vlan** *vlan-id* 例： `Switch(config)# vlan 10`	VLAN コンフィギュレーション モードを開始します。 *vlan-id* には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 7	**remote-span** 例： `Switch(config-vlan)# remote-span`	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。

	コマンドまたはアクション	目的
ステップ 8	**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 9	**monitor session** *session_number* **filter** {**ip** | **ipv6** | **mac**} **access-group** {*access-list-number* | *name*} 例： `Switch(config)# monitor session 2 filter ip access-group 7`	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。 • *session_number* には、 手順 4： • *access-list-number* 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。 • *name* 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 10	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 12	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

フローベースの SPAN, （162 ページ）
FSPAN および FRSPAN 設定時の注意事項, （165 ページ）

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 *15* : *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> enable
Switch# configure terminal
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> enable
Switch# configure terminal
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> enable
Switch# configure terminal
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> enable
Switch# configure terminal
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> enable
Switch# configure terminal
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> enable
Switch# configure terminal
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
```

関連トピック

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, （168 ページ）
ローカル SPAN, （151 ページ）
SPAN セッション, （154 ページ）
SPAN 設定時の注意事項, （164 ページ）

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> enable
Switch# configure terminal
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> enable
Switch# configure terminal
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> enable
Switch# configure terminal
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> enable
Switch# configure terminal
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> enable
Switch# configure terminal
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
```

関連トピック

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, （182 ページ）
リモート SPAN, （153 ページ）
RSPAN VLAN, （160 ページ）
RSPAN 設定時の注意事項, （164 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
system コマンド	*Network Management Command Reference, Cisco IOS XE Release 3E*

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
なし	-

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	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
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。 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。 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。	http://www.cisco.com/support

SPAN および RSPAN の機能の履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SECisco IOS XE 3.2SE	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 プローブを使用してポートまたは VLAN のswitch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。
Cisco IOS XE 3.2SECisco IOS XE 3.2SE	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。 この機能が導入されました。
Cisco IOS XE 3.2SECisco IOS XE 3.2SE	EtherChannel での SPAN 宛先ポートのサポート：EtherChannel で SPAN 宛先ポートを設定できるようにします。 この機能が導入されました。
Cisco IOS XE 3.2SECisco IOS XE 3.2SE	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。 この機能が導入されました。

ネットワーク管理コンフィギュレーション ガイド、Cisco IOS XE Release 3.6E（Catalyst 3850 スイッチ）

第 9 章

Wireshark の設定

- 機能情報の確認，197 ページ
- Wireshark の前提条件，198 ページ
- Wireshark の制約事項，198 ページ
- Wireshark に関する情報，200 ページ
- Wireshark の設定方法，211 ページ
- Wireshark のモニタリング，227 ページ
- Wireshark の設定例，228 ページ
- その他の関連資料，243 ページ
- WireShark の機能履歴と情報，244 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。 最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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。

Wireshark の前提条件

- Wireshark は、Supervisor Engine 7-E、Supervisor Engine 7L-E、Catalyst 3850、Catalyst 3650、ワイヤレス LAN コントローラ 5700 シリーズ、Catalyst 4500X-16、および Catalyst 4500X-32 でサポートされます。
- IP Base イメージまたは IP Services イメージが組み込み Wireshark には必要です。

Wireshark の制約事項

- Cisco IOS Release XE 3.3.0(SE) 以降では、Wireshark のグローバル キャプチャはサポートされません。
- キャプチャ フィルタはサポートされません。
- Wireshark を設定するための CLI では、機能を EXEC モードからのみ実行する必要があります。 通常は設定サブモードで発生するアクション（キャプチャ ポイントの定義など）は、代わりに EXEC モードから処理されます。 すべての主要コマンドは NVGEN の対象ではなく、NSF と SSO のシナリオではスタンバイ スーパーバイザに同期されません。
- インターフェイスの出力方向にキャプチャされたパケットは、スイッチ rewrite（TTL、VLAN タグ、CoS、チェックサム、MAC アドレス、DSCP、precedent、UP などを含む）によって加えられる変更を反映しない場合があります。
- ファイル サイズによる循環ファイル保存の制限はサポートされません。
- 組み込み Wireshark は LAN Base イメージを実行しているスイッチ上ではサポートされません。

ワイヤレス パケット キャプチャ

- ワイヤレス キャプチャの唯一の形式は CAPWAP トンネル キャプチャです。
- CAPWAP トンネルをキャプチャする場合、同じキャプチャ ポイントで他のインターフェイス タイプを接続ポイントとして使用することはできません。
- 複数の CAPWAP トンネルのキャプチャがサポートされています。
- コア フィルタは適用されず、CAPWAP トンネルをキャプチャする場合は省略する必要があります。
- CAPWAP データ トンネルをキャプチャするために、各 CAPWAP トンネルは物理的ポートにマッピングされ、トラフィックをフィルタするための適切な ACL が適用されます。
- CAPWAP 非データ トンネルをキャプチャするため、スイッチはすべてのポート上のトラフィックをキャプチャし、トラフィックをフィルタするための適切な ACL を適用するように設定されます。

- 種類に関係なく、CAPWAP トンネルをキャプチャするため、コントローラはすべての物理的ポートでトラフィックをキャプチャし、トラフィックをフィルタするための適切な ACL を適用するよう指定されます。

設定の制限

- 複数のキャプチャ ポイントを定義できますが、一度にアクティブにできるのは 1 つだけです。 1 つ開始するには 1 つ停止する必要があります。
- VRF、管理ポート、プライベート VLAN はいずれも接続ポイントとして使用することはできません。
- Wireshark クラス マップでは、ACL は各タイプ（IPv4、IPv6、MAC）で 1 つのみ許可されます。 クラス マップでは、IPv4 に 1 つ、IPv6 に 1 つ、MAC に 1 つの最大 3 つの ACL が可能です。
- Wireshark は宛先 SPAN ポートでパケットをキャプチャできません。
- Wireshark は、キャプチャ ポイントにアタッチされる接続ポイント（インターフェイス）のいずれかが動作を停止するとキャプチャを停止します。 たとえば、接続ポイントに関連付けられているデバイスがスイッチから切断された場合です。 キャプチャを再開するには、手動で再起動する必要があります。
- CPU 注入されたパケットは、コントロールプレーン パケットと見なされます。 したがって、これらのタイプのパケットはインターフェイスの出力キャプチャではキャプチャされません。
- MAC ACL は、ARP などの非 IP パケットだけに使用されます。 レイヤ 3 ポートまたは SVI ではサポートされません。
- IPv6 ベースの ACL は VACL ではサポートされません。
- レイヤ 2 およびレイヤ 3 EtherChannel はサポートされません。
- ACL ロギングおよび Wireshark には互換性がありません。 Wireshark はアクティブになると優先されます。 任意のポートにロギング中の ACL にキャプチャされているものも含めたすべてのトラフィックが Wireshark にリダイレクトされます。 Wireshark を開始する前に、ACL ロギングを非アクティブにすることをお勧めします。 これを実行しないと、Wireshark のトラフィックは ACL ロギング トラフィックに汚染されます。
- Wireshark は floodblock によってドロップされるパケットをキャプチャしません。
- 同じポートの PACL および RACL の両方をキャプチャすると、1 つのコピーだけが CPU に送信されます。 DTLS 暗号化 CAPWAP インターフェイスをキャプチャすると、暗号化されたものと復号化されたものの 2 つのコピーが Wireshark に送信されます。 DTLS 暗号化 CAPWAP トラフィックを運ぶレイヤ 2 インターフェイスをキャプチャすると同じ動作が発生します。 コア フィルタは外部 CAPWAP ヘッダーに基づいています。

Wireshark に関する情報

Wireshark の概要

Wireshark は、複数のプロトコルをサポートし、テキストベース ユーザ インターフェイスで情報を提供する、以前は Ethereal と呼ばれていたパケット アナライザ プログラムです。

トラフィックをキャプチャおよび分析する機能により、ネットワーク アクティビティにデータを提供します。 Cisco IOS Release XE 3.3.0(SE) 以前のリリースでは、このニーズに対応したのは SPAN およびデバッグ プラットフォーム パケットの 2 つの機能だけでした。 これらにはいずれも制限があります。 SPAN は、パケットのキャプチャにおいては理想的ですが、指定したローカルまたはリモートの宛先にパケットを転送することによりこれを実現しているだけで、ローカル表示や分析をサポートしていません。 **debug platform packet** コマンドは、Catalyst 4500 シリーズに固有で、ソフトウェア プロセス フォワーディング パスから生成されたパケットだけで動作します。また、**debug platform packet** コマンドは、ローカル表示機能に制限があり、分析がサポートされていません。

そのため、ハードウェアおよびソフトウェア送信トラフィックの両方に適用可能で、可能なら既知のインターフェイスを使用した高度なパケット キャプチャ、表示、および分析サポートを提供する、トラフィック キャプチャおよび分析機構のニーズが存在します。

Wireshark は、.pcap と呼ばれる既知の形式を使用してファイルへパケットをダンプし、個々のインターフェイスに対して適用されイネーブルになります。 EXEC モードでインターフェイスを指定し、フィルタおよび他のパラメータも指定します。 Wireshark アプリケーションは、**start** コマンドを入力した場合にだけ適用され、Wireshark が自動または手動でキャプチャを停止した場合にだけ削除されます。

キャプチャ ポイント

キャプチャ ポイントとは、Wireshark 機能の一元的なポリシー定義です。 キャプチャ ポイントは、どのパケットをキャプチャするか、どこからキャプチャするか、キャプチャ パケットに何を実行するか、およびいつ停止するかなど、Wireshark の特定のインスタンスに関連付けられたすべての特徴を説明します。 キャプチャ ポイントは作成後に変更する場合があり、**start** コマンドを使用して明示的にアクティブ化しない限り、アクティブになりません。 このプロセスは、キャプチャ ポイントのアクティブ化またはキャプチャ ポイントの開始といいます。 キャプチャ ポイントは名前で識別され、手動または自動で非アクティブ化または停止する場合もあります。

複数のキャプチャ ポイントを定義してできますが、一度にアクティブにできるのは 1 つだけです。 1 つ開始するには 1 つ停止する必要があります。

関連トピック

キャプチャ ポイントの定義, （212 ページ）
キャプチャ ポイント パラメータの追加または変更, （217 ページ）
キャプチャ ポイント パラメータの削除, （220 ページ）

キャプチャ ポイントの削除, （222 ページ）
キャプチャ ポイントをアクティブまたは非アクティブにする, （224 ページ）
キャプチャ ポイント バッファのクリア, （225 ページ）
例：単純なキャプチャおよび表示, （232 ページ）
例：単純なキャプチャおよび保存, （233 ページ）
例：バッファのキャプチャの使用, （234 ページ）
例：キャプチャ セッション, （239 ページ）
例：ロック ステップ モードのキャプチャおよび保存, （240 ページ）
例：出方向のパケットの簡単なキャプチャおよび保存, （241 ページ）

接続ポイント

接続ポイントは、キャプチャポイントに関連付けられた論理パケットのプロセスパスのポイントです。接続ポイントはキャプチャ ポイントの属性です。 接続ポイントに影響するパケットはキャプチャ ポイント フィルタに対してテストされます。一致するパケットはキャプチャ ポイントの関連する Wireshark インスタンスにコピーされ、送信されます。 特定のキャプチャ ポイントを複数の接続ポイントに関連付けることができます。異なるタイプ接続ポイントの混合に制限はありません。一部の制限は、異なるタイプの添付ポイントを指定すると適用されます。接続ポイントは、常に双方向であるレイヤ 2 VLAN の接続ポイントを除き、方向性あり（入力/出力/両方）です。

関連トピック

キャプチャ ポイントの定義, （212 ページ）
キャプチャ ポイント パラメータの追加または変更, （217 ページ）
キャプチャ ポイント パラメータの削除, （220 ページ）
キャプチャ ポイントの削除, （222 ページ）
キャプチャ ポイントをアクティブまたは非アクティブにする, （224 ページ）
キャプチャ ポイント バッファのクリア, （225 ページ）
例：単純なキャプチャおよび表示, （232 ページ）
例：単純なキャプチャおよび保存, （233 ページ）
例：バッファのキャプチャの使用, （234 ページ）
例：キャプチャ セッション, （239 ページ）
例：ロック ステップ モードのキャプチャおよび保存, （240 ページ）
例：出方向のパケットの簡単なキャプチャおよび保存, （241 ページ）

フィルタ

フィルタは、Wiresharkにコピーされ、渡されるキャプチャ ポイントの接続ポイントを通過するトラフィックのサブセットを識別し制限するキャプチャ ポイントの属性です。 Wireshark で表示されるためには、パケットは接続ポイントと、キャプチャ ポイントに関連付けられたすべてのフィルタも通過する必要があります。

キャプチャ ポイントには以下のタイプのフィルタがあります。

- コア システム フィルタ：コア システム フィルタはハードウェアによって適用され、一致基準はハードウェアによって制限されます。 このフィルタは、ハードウェア転送トラフィックが Wireshark の目的でソフトウェアにコピーするかどうかを決定します。
- 表示フィルタ：表示フィルタは、Wireshark によって適用されます。 表示フィルタに失敗したパケットは表示されません。

コア システム フィルタ

クラス マップまたは ACL を使用して、または CLI を使用して明示的にコア システム フィルタの一致基準を指定できます。

（注） CAPWAP を接続ポイントとして指定すると、コア システム フィルタは使用されません。

一部のインストール済み環境では、承認プロセスが長い場合さらに遅延を引き起こす可能性がある スイッチ の設定を変更する権限を取得する必要があります。 これにより、ネットワーク管理者の機能がトラフィックの監視および分析に制限される場合があります。 この状況に対処するため、Wireshark は、EXEC モード CLI から、コア システム フィルタ一致基準の明示的な仕様をサポートします。 この対処方法の欠点は、指定できる一致基準が、クラスマップがサポートする対象の限定的なサブセットである（MAC、IP送信元アドレスおよび宛先アドレス、イーサネット タイプ、IP プロトコル、および TCP/UDP の発信元および宛先ポートなど）ことです。

コンフィギュレーションモードを使用する場合はACLを定義するか、クラスマップでそこへキャプチャ ポイントを参照させることができます。 明示的かつ ACL ベースの一致基準がクラス マップとポリシー マップの作成に内部的に使用されます。

注：ACL およびクラス マップの設定はシステムの一部であり、Wireshark 機能の側面ではありません。

表示フィルタ

表示フィルタを使用すると、.pcap ファイルからデコードして表示するときに表示するパケットの集合をさらに絞り込むように Wireshark に指示できます。

関連トピック

その他の関連資料, （243 ページ）

処理

Wireshark はライブ トラフィックまたは前の既存 .pcap ファイルで呼び出すことができます。 ライブ トラフィックに対して起動されたとき、その表示フィルタを通過するパケットに対して次の 4 種類の処理を実行できます。

- デコード、分析、保存のためにメモリ内バッファへキャプチャ
- .pcap ファイルへ保存
- デコードおよび表示
- 保存および表示

.pcap ファイルのみに対して起動された場合は、デコードと表示の処理だけが適用できます。

キャプチャ パケットのメモリ内のバッファへのストレージ

パケットは、メモリ内のキャプチャ バッファに格納して、後でデコード、分析、または .pcap ファイルへ保存できます。

キャプチャ バッファは線形モードまたは循環モードを選択できます。 線形モードでは、バッファが上限に達すると、新しいパケットが廃棄されます。 循環モードでは、バッファが上限に達すると、新しいパケットを格納するために最も古いパケットが廃棄されます。 必要に応じてバッファをクリアすることもできますが、このモードは、ネットワーク トラフィックのデバッグに主に使用されます。

（注） パケットをバッファ内に保存する複数のキャプチャがある場合、メモリ ロスを避けるため、新しいキャプチャを開始する前にバッファをクリアしてください。

.pcap ファイルにキャプチャされたパケットのストレージ

（注） WireShark がスタック内のスイッチで使用される場合は、パケット キャプチャをアクティブ スイッチに接続されたフラッシュまたは USB フラッシュ デバイスにのみ保存できます。

たとえば、flash1 がアクティブなスイッチに接続されており、flash2 がセカンダリ スイッチに接続されている場合、flash1 にのみパケット キャプチャを保存できます。

アクティブ スイッチに接続されたフラッシュまたは USB フラッシュ デバイス以外のデバイスにパケット キャプチャを保存しようとすると、エラーが発生する場合があります。

Wireshark は .pcap ファイルにキャプチャされたパケットを保存できます。 キャプチャ ファイルは次のストレージ デバイスに配置可能です。

- Switchオンボード フラッシュ ストレージ（flash:）
- USB ドライブ(usbflash0:)

（注） サポートされていないデバイスまたはアクティブなスイッチに接続されていないデバイスにパケット キャプチャを保存しようとするとエラーが発生する可能性があります。

Wireshark のキャプチャ ポイントを設定する場合は、ファイル名を関連付けることができます。キャプチャ ポイントをアクティブにすると、Wireshark は指定された名前でファイルを作成し、パケットを書き込みます。ファイルの関連付け、またはキャプチャ ポイントのアクティブ化を行う際にファイルがすでに存在する場合、Wireshark はファイルを上書きできるかどうかについて問い合わせます。特定のファイル名には 1 つのキャプチャ ポイントのみ関連付けることができます。

Wireshark が書き込んでいるファイル システムが一杯になると、Wireshark はファイルの一部のデータで失敗します。そのため、キャプチャ セッションを開始する前に、ファイル システムに十分な領域があることを確認する必要があります。Cisco IOS Release IOS XE 3.3.0(SE) では、ファイル システムの完全なステータスは一部のストレージ デバイスに対しては検出されません。

パケット全体ではなくセグメントのみを保持して、必要な記憶域を減らすことができます。通常、最初の 64 または 128 バイトを超える詳細は不要です。デフォルトの動作は、パケット全体の保存です。

ファイルシステムを処理し、ファイルシステムへの書き込みを行う際、パケットのドロップの発生を避けるため、Wireshark ではオプションでメモリ バッファを使用してパケットの到着時に一時的に保持できます。メモリ バッファのサイズは、キャプチャ ポイントが .pcap ファイルに関連付けられる際に指定できます。

パケットのデコードおよび表示

Wireshark はコンソールにパケットをデコードして表示できます。この機能は、ライブ トラフィックに適用されるキャプチャ ポイントと前の既存 .pcap ファイルに適用されるキャプチャ ポイントで使用可能です。

（注） パケットをデコードして表示すると、CPU への負荷が高くなる場合があります。

Wireshark は、幅広い種類のパケット形式に対してパケット詳細をデコードおよび表示できます。詳細は、**monitor capture name start** コマンドを以下のキーワード オプションと入力することで表示されます。これにより表示およびデコード モードが開始します。

- brief : パケットごとに 1 行表示します（デフォルト）。
- detailed : プロトコルがサポートされているすべてのパケットのすべてのフィールドをデコードして表示します。詳細モードでは、他の 2 種類のモードよりも多くの CPU が必要です。
- (hexadecimal) dump : パケット データの 16 進ダンプおよび各パケットの印刷可能文字としてパケットごとに 1 行表示します。

capture コマンドをデコードおよび表示オプションで入力すると、Wireshark 出力が Cisco IOS に返され、コンソール上に変更なしに表示されます。

ライブ トラフィックの表示

Wireshark はコア システムからパケットのコピーを受信します。 Wireshark は、表示フィルタを適用して、不要なパケットを破棄し、残りのパケットをデコードおよび表示します。

.pcap ファイルの表示

Wireshark は、以前に保存された .pcap ファイルからのパケットをデコードして表示し、選択的にパケットを表示するように表示フィルタに指示できます。

パケットのストレージおよび表示

機能的には、このモードは以前の 2 種類のモードの組み合わせです。 Wireshark は指定された .pcap ファイルにパケットを保存し、これらをコンソールにデコードおよび表示します。 ここではコア フィルタ フィルタだけが該当します。

Wireshark キャプチャ ポイントのアクティブ化および非アクティブ化

Wireshark のキャプチャ ポイントが、接続ポイント、フィルタ、アクション、およびその他のオプションで定義された場合、Wireshark をアクティブにする必要があります。 キャプチャ ポイントがアクティブになるまで、実際にパケットをキャプチャしません。

キャプチャ ポイントがアクティブになる前に、一部の機能性チェックが実行されます。 キャプチャ ポイントは、コア システム フィルタと接続ポイントのどちらも定義されていない場合はアクティブにできません。 これらの要件を満たしていないキャプチャ ポイントをアクティブ化しようとすると、エラーが生成されます。*

（注） *ワイヤレス キャプチャを CAPWAP トンネリング インターフェイスで実行する場合、コア システムのフィルタは必要なく、使用することができません。

表示フィルタを必要に応じて指定します。

Wireshark のキャプチャ ポイントはアクティブになると、複数の方法で非アクティブにできます。 .pcap ファイルにパケットを格納するだけのキャプチャ ポイントは手動で停止することも、また時間制限またはパケット制限付きで設定することもでき、その後でキャプチャ ポイントは自動的に停止します。

Wireshark のキャプチャ ポイントがアクティブになると、固定レート ポリサーがハードウェアに自動的に適用され、CPU が Wireshark によって指示されたパケットでフラッディングしないようになります。 レート ポリサーの短所は、リソースが使用可能な場合でも、確立されたレートを超えて連続するパケットをキャプチャできないことです。

Wireshark 機能

ここでは、Wireshark 機能が スイッチ 環境でどのように動作するかについて説明します。

- ポート セキュリティおよび Wireshark が入力キャプチャに適用された場合でも、ポート セキュリティによってドロップされたパケットは Wireshark でキャプチャされます。 ポート セキュリティが入力キャプチャに適用され、Wireshark が出力キャプチャに適用された場合、ポート セキュリティによってドロップされたパケットは Wireshark ではキャプチャされません。
- ダイナミック ARP インスペクション（DAI）によってドロップされたパケットは Wireshark ではキャプチャされません。
- STP ブロック ステートのポートが接続ポイントとして使用され、コア フィルタが一致する場合、Wireshark は、パケットがスイッチにドロップされる場合でもポートに入ってくるパケットをキャプチャします。
- 分類ベースのセキュリティ機能：入力分類ベースのセキュリティ機能によってドロップされたパケット（ACL および IPSG など）は同じ層の接続ポイントに接続する Wireshark キャプチャ ポイントでは検出されません。 一方、出力分類ベースのセキュリティ機能によってドロップされたパケットは、同じ層の接続ポイントに接続されている Wireshark のキャプチャ ポイントでキャッチされます。 論理モデルは、Wireshark の接続ポイントが、入力側のセキュリティ機能のルックアップ後、および出力側のセキュリティ機能のルックアップ前に発生することです。

  入力では、パケットはレイヤ 2 ポート、VLAN、およびレイヤ 3 ポート/SVI を介して送信されます。 出力では、パケットはレイヤ 3 ポート/SVI、VLAN、およびレイヤ 2 ポートを介して送信されます。 接続ポイントがパケットがドロップされるポイントの前にある場合、Wireshark はパケットをキャプチャします。 これ以外の場合は、Wireshark はパケットをキャプチャしません。 たとえば、入力方向のレイヤ 2 接続ポイントに接続される Wireshark のキャプチャ ポリシーはレイヤ 3 分類ベースのセキュリティ機能によってドロップされたパケットをキャプチャします。 対照的に、出力方向のレイヤ 3 接続ポイントに接続する Wireshark のキャプチャ ポリシーは、レイヤ 2 分類ベースのセキュリティ機能によりドロップされたパケットをキャプチャします。
- ルーテッド ポートおよびスイッチ仮想インターフェイス（SVIs）：SVI の出力から送信されるパケットは CPU で生成されるため、Wireshark は SVI の出力をキャプチャできません。 これらのパケットをキャプチャするには、コントロールプレーンを接続ポイントとして含めます。
- VLAN：VLAN が Wireshark の接続ポイントとして使用されている場合、パケットは、入力方向でのみキャプチャされます。
- リダイレクション機能：入力方向では、レイヤ 3（PBR および WCCP など）でリダイレクトされる機能トラフィックは、レイヤ 3 の Wireshark の接続ポイントよりも論理的に後です。 Wireshark は、後で別のレイヤ 3 インターフェイスにリダイレクトされる可能性がある場合でも、これらのパケットをキャプチャします。 対照的に、レイヤ 3 によってリダイレクトされ

る出力機能（出力 WCCP など）は論理的にレイヤ 3 接続ポイントの前にあり、Wireshark ではキャプチャされません。

- SPAN：Wireshark は SPAN 送信元または宛先として設定されたインターフェイス上でパケットを収集できません。
- ACL が適用されていない場合、最大 1000 の VLAN からパケットを一度にキャプチャできます。 ACL が適用されている場合、Wireshark の使用できるハードウェア領域はより少なくなります。 結果として、パケット キャプチャに一度に使用できる VLAN の最大数は低くなります。 1000 以上の VLAN トンネルを一度に使用したり、ACL を多数使用すると予測されない結果が生じる可能性があります。 たとえば、モビリティがダウンする可能性があります。

（注） 過剰な CPU 使用につながり、予測されないハードウェア動作の原因となる可能性があるため、過剰な数の接続ポイントを一度にキャプチャしないことを強くお勧めします。

Wireshark でのワイヤレス パケット キャプチャ

- ワイヤレス トラフィックは CAPWAP パケット内にカプセル化されます。 ただし、CAPWAP トンネル内の特定のワイヤレス クライアントのトラフィックだけの検出は、CAPWAP トンネルを接続ポイントとして使用する場合はサポートされません。 特定のワイヤレス クライアントのトラフィックだけをキャプチャするには、クライアント VLAN を接続ポイントとして使用し、それに応じてコア フィルタを設定します。
- 内部ワイヤレス トラフィックのデコードは制限付きでサポートされます。 暗号化された CAPWAP トンネル内の内部ワイヤレス パケットのデコードはサポートされません。
- 同じキャプチャ ポイント上で他のインターフェイス タイプを CAPWAP トンネリング インターフェイスと併用することはできません。 CAPWAP トンネリング インターフェイスおよびレベル 2 ポートは、同じキャプチャ ポイントの接続ポイントにはできません。
- CAPWAP トンネルを介して Wireshark にパケットをキャプチャする場合、コア フィルタの指定はできません。 ただし、Wireshark 表示フィルタを使用して、特定のワイヤレス クライアントに対してワイヤレス クライアントをフィルタすることができます。
- ACL が適用されていない場合、最大 135 の CAPWAP トンネルからパケットを一度にキャプチャできます。 ACL が適用されている場合、Wireshark の使用できるハードウェア メモリ領域はより少なくなります。 結果として、パケット キャプチャに一度に使用できる CAPWAP トンネルの最大数は低くなります。 一度に 135 以上の CAPWAP トンネル、または多くの ACL を使用すると予測できない結果が生じる場合があります。 たとえば、モビリティがダウンする可能性があります。

（注） 過剰な CPU 使用につながり、予測されないハードウェア動作の原因となる可能性があるため、過剰な数の接続ポイントを一度にキャプチャしないことを強くお勧めします。

Wireshark のガイドライン

- Wireshark でのパケット キャプチャ中に、ハードウェア転送が同時に発生します。
- Wireshark のキャプチャ プロセスを開始する前に、CPU 使用率が妥当であり、十分なメモリ（少なくとも 200 MB）が使用可能であることを確認します。
- ストレージ ファイルにパケットを保存する予定の場合、Wireshark キャプチャ プロセスを開始する前に十分なスペースが利用可能であることを確認してください。
- Wireshark のキャプチャ中の CPU 使用率は、設定された基準に一致するパケットの数と、一致したパケット用のアクション（ストア、デコードして表示、あるいはこの両方）によって異なります。
- 高CPU使用率および他の不要な条件を避けるため、可能な限りキャプチャを最小限に抑えてください（パケット、期間による制限）。
- パケット転送はハードウェアで通常実行されるため、パケットは、ソフトウェア処理のために CPU にコピーされません。 Wireshark のパケット キャプチャの場合、パケットは CPU にコピーされ、配信されて、これが CPU 使用率の増加につながります。

  CPU 使用率を高くしないようにするには、次の手順を実行します。

  - 関連ポートだけに接続します。
  - 一致条件を表すにはクラス マップを使用し、二次的にアクセス リストを使用してください。 いずれも実行可能でない場合は、明示的な、インライン フィルタを使用します。
  - フィルタ規則に正しく準拠させます。 緩和されたのではなく制限的な ACL で、トラフィック タイプを（IPv4のみなどに）制限して、不要なトラフィックを引き出します。

- パケット キャプチャを短い期間または小さなパケット番号に常に制限します。 capture コマンドのパラメータにより、次を指定することができます。

  - キャプチャ期間
  - キャプチャされたパケットの数
  - ファイル サイズ
  - パケットのセグメント サイズ

- コア フィルタと一致するトラフィックが非常に少ないことが判明している場合は、制限なしでキャプチャ セッションを実行します。
- 次の場合に高い CPU（またはメモリ）使用率になる可能性があります。

  - キャプチャ セッションをイネーブルにし長期間不在のままにして、予期しないトラフィックのバーストが起きた場合。

- リング ファイルまたはキャプチャ バッファを使用してキャプチャ セッションを起動して、長期間不在のままにするとし、パフォーマンスまたはシステム ヘルスの問題が引き起こされます。

- キャプチャ セッション中に、スイッチ のパフォーマンスやヘルスに影響する可能性のある Wireshark による高い CPU 使用率およびメモリ消費がないか監視します。 こうした状況が発生した場合、Wireshark セッションをすぐに停止します。
- 大きなファイルの .pcap ファイルからのパケットをデコードして表示することは避けてください。 代わりに、PC に .pcap ファイルを転送し PC 上で Wireshark を実行します。
- Wireshark インスタンスは最大 8 個まで定義できます。 .pcap ファイルまたはキャプチャ バッファからパケットをデコードして表示するアクティブな **show** コマンドは、1 個のインスタンスとしてカウントされます。 ただし、アクティブにできるインスタンスは 1 つだけです。
- 実行中のキャプチャに関連付けられた ACL が変更された場合は常に、ACL 変更を有効にするにはキャプチャを再起動する必要があります。 キャプチャを再起動しないと、変更前の元の ACL が継続して使用されます。
- パケット損失を防ぐには、次の点を考慮します。
  - ライブ パケットをキャプチャしている間は、CPU に負荷のかかる操作であるデコードと表示ではなく（特に detailed モードの場合）、保存のみを使用します（display オプションを指定しない場合）。
  - パケットをバッファ内に保存する複数のキャプチャがある場合、メモリ ロスを避けるため、新しいキャプチャを開始する前にバッファをクリアしてください。
  - デフォルト バッファ サイズを使用し、パケットが失われている場合、バッファ サイズを増加してパケットの喪失を防ぐことができます。
  - フラッシュ ディスクへの書き込みは、CPUに負荷のかかる操作であるため、キャプチャ レートが不十分な場合、バッファ キャプチャの使用をお勧めします。
  - Wireshark キャプチャ セッションは、パケットのキャプチャおよび処理の両方が行われるストリーミング モードで正常に動作しています。 ただし、32 MB 以上のバッファ サイズを指定すると、セッションは Wireshark のキャプチャ セッションがキャプチャおよびプロセスの 2 フェーズに分割されるロックステップ モードを自動的にオンにします。 キャプチャ フェーズでは、パケットは一時バッファに保存されます。 ロックステップ モードの duration パラメータは、セッション期間ではなくキャプチャ期間として機能します。 バッファがいっぱいになるかまたはキャプチャ期間またはパケット制限に到達すると、パケットの受け入れを停止してバッファのパケットの処理を開始するプロセス フェーズへセッションは移行します。 キャプチャを手動で停止することもできます。 キャプチャが停止した場合出力にメッセージが表示されます。 この 2 番目の方法（ロック ステップ モード）を使用して、より高いキャプチャ スループットを達成できます。

（注） バッファからパケットをキャプチャする場合、ファイル ストレージは定義されません。 したがって、バッファから静的ストレージ ファイルにキャプチャをエクスポートする必要があります。 **monitor capture** *capture-name* **export** *file-location* : *file-name* コマンドを使用します。

- ストリーミング キャプチャ モードは約 1000 pps をサポートし、ロックステップ モードは約 2 Mbps（256 バイト パケットで測定）をサポートします。 一致するトラフィック レートがこの値を超えると、パケット損失が発生する可能性があります。

- コンソール ウィンドウのライブ パケットをデコードして表示する場合は、Wireshark セッションが短いキャプチャ期間によって抑制されていることを確認します。

（注） 警告：期間制限がより長いまたはキャプチャ期間がない（**term len 0** コマンドを使用して auto-more サポートのない端末を使用した）Wireshark セッションでは、コンソールまたは端末が使用できなくなる場合があります。

- 高 CPU 使用率につながるライブ トラフィックのキャプチャに Wireshark を使用している場合、QoS ポリシーを一時的に適用して、キャプチャ プロセスが終了するまで実際のトラフィックを制限することを考慮してください。
- すべての Wireshark 関連のコマンドは EXEC モードで、コンフィギュレーション コマンドは、Wireshark にありません。

  Wireshark CLI でアクセス リストまたはクラスマップを使用する必要がある場合は、コンフィギュレーション コマンドでアクセス リストおよびクラスマップを定義する必要があります。
- 特定の順序はキャプチャ ポイントを定義する場合には適用されません。CLI で許可されている任意の順序でキャプチャ ポイント パラメータを定義できます。 Wireshark CLI では、単一行のパラメータ数に制限はありません。 これはキャプチャ ポイントを定義するために必要なコマンドの数を制限します。
- 接続ポイントを除くすべてのパラメータは、単一の値を取ります。 通常、コマンドを再入力することにより、値を新しいものに置き換えることができます。 ユーザの確認後にシステムが新しい値を受け入れ、古い値を上書きします。 コマンドの **no** 形式には新規値を入力する必要はありませんが、パラメータを削除する必要があります。
- Wireshark では 1 つ以上の接続ポイントを指定することができます。 複数の接続ポイントを追加するには、新しい接続ポイントでコマンドを再入力します。 接続ポイントを削除するには、コマンドの **no** 形式を使用します。 接続ポイントとしてインターフェイス範囲を指定できます。 たとえば、**monitor capture mycap interface GigabitEthernet1/0/1 in** を入力します。 ここではインターフェイス GigabitEthernet1/0/1 が接続ポイントです。

  またインターフェイス GigabitEthernet1/0/2 にも接続する必要がある場合、次のように、別の行で指定します。

monitor capture mycap interface GigabitEthernet1/0/2 in

- セッションがアクティブである間にキャプチャ ポイントの任意のパラメータを変更できますが、変更を有効にするにはセッションを再起動する必要があります。
- 実行する処理は、いずれのパラメータが必須であるかを決定します。 Wireshark CLI では **start** コマンドを入力する前に任意のパラメータを指定または変更することができます。 **start** コマンドを入力すると、Wireshark はすべての必須パラメータが入力されたと判断した後でのみ開始します。
- キャプチャ ファイルがすでに存在する場合、警告が表示され、継続するために確認が要求されます。 これにより、誤ってファイルが上書きされるのを防ぐことができます。
- コア フィルタは明示的なフィルタ、アクセス リスト、またはクラス マップにできます。 これらのタイプの新しいフィルタを指定すると、既存のものを置き換えます。

（注） コア フィルタは、CAPWAP トンネル インターフェイスをキャプチャ ポイントの接続ポイントとして使用している場合を除き、必須です。

- 明示的な **stop** コマンドを使用するか、automore モードに「**q**」を入力して、Wireshark のセッションを終了します。 セッションは、期間やパケット キャプチャの制限などの停止の条件が満たされたときに、自身を自動的に終了することができます。

デフォルトの Wireshark の設定

次の表は、デフォルトの Wireshark の設定を示しています。

機能	デフォルト設定
持続時間	制限なし
パケット	制限なし
パケット長	制限なし（フル パケット）
ファイル サイズ	制限なし
リング ファイル ストレージ	なし
バッファのストレージ モード	線形

Wireshark の設定方法

Wireshark を設定するには、次の基本的な手順を実行します。

1 キャプチャ ポイントを定義します。

2 （任意）キャプチャ ポイントのパラメータを追加または変更します。

3 キャプチャ ポイントをアクティブ化または非アクティブ化します。

4 キャプチャ ポイントを今後使用しない場合は削除します。

関連トピック

キャプチャ ポイントの定義, （212 ページ）
キャプチャ ポイント パラメータの追加または変更, （217 ページ）
キャプチャ ポイント パラメータの削除, （220 ページ）
キャプチャ ポイントの削除, （222 ページ）
キャプチャ ポイントをアクティブまたは非アクティブにする, （224 ページ）
キャプチャ ポイント バッファのクリア, （225 ページ）
例：単純なキャプチャおよび表示, （232 ページ）
例：単純なキャプチャおよび保存, （233 ページ）
例：バッファのキャプチャの使用, （234 ページ）
例：キャプチャ セッション, （239 ページ）
例：ロック ステップ モードのキャプチャおよび保存, （240 ページ）
例：出方向のパケットの簡単なキャプチャおよび保存, （241 ページ）

キャプチャ ポイントの定義

この手順の例では、非常にシンプルなキャプチャ ポイントを定義します。必要に応じて、**monitor capture** コマンドの 1 つのインスタンスを使用してキャプチャ ポイントとそのすべてのパラメータを定義できます。

（注） 接続ポイント、キャプチャの方向、およびコア フィルタが機能するキャプチャ ポイントを持つよう定義する必要があります。

コア フィルタを定義する必要がないのは、CAPWAP トンネリング インターフェイスを使用してワイヤレス キャプチャ ポイントを定義する場合です。この場合、コア フィルタは定義しません。これは使用できません。

キャプチャ ポイントを定義するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show capwap summary**
3. **monitor capture** {*capture-name*}{**interface** *interface-type interface-id* | **control-plane**}{**in** | **out** | **both**}
4. **monitor capture** {*capture-name*}[**match** {**any** | **ipv4 any any** | **ipv6**} **any any**}]
5. **show monitor capture** {*capture-name*}[**parameter**]
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**show capwap summary** 例： `Switch# show capwap summary`	ワイヤレス キャプチャの接続ポイントとして使用できるCAPWAPトンネルを表示します。 （注） このコマンドは、ワイヤレス キャプチャを実行するためにCAPWAPトンネルを接続ポイントとして使用している場合にのみ使用します。 例の項のCAPWAPの例を参照してください。
ステップ 3	**monitor capture** {*capture-name*}{**interface** *interface-type interface-id*	**control-plane**}{**in**	**out**	**both**} 例： `Switch# monitor capture mycap interface GigabitEthernet1/0/1 in`	キャプチャ ポイントを定義し、キャプチャ ポイントが関連付けられている接続ポイントを指定し、キャプチャの方向を指定します。 キーワードの意味は次のとおりです。 • *capture-name*：定義するキャプチャ ポイントの名前を指定します（例では mycap が使用されています）。 • （任意）**interface** *interface-type interface-id*：キャプチャ ポイントが関連付けられる接続ポイントを指定します（例では GigabitEthernet1/0/1 が使用されています）。 （注） オプションで、このコマンド インスタンス 1 つでこのキャプチャ ポイントの複数の接続ポイントおよびパラメータすべてを定義できます。 これらのパラメータについては、キャプチャ ポイント パラメータの変更に関する手順で説明されています。範囲のサポートは、接続ポイントを追加および削除するためにも使用できます。 *interface-type* には次のいずれかを使用します。

	コマンドまたはアクション	目的
		◦ **GigabitEthernet**：接続ポイントを GigabitEthernet として指定します。 ◦ **vlan**：接続ポイントを VLAN として指定します。 （注） このインターフェイスを接続ポイントとして使用する場合は、入力キャプチャのみが可能です。 ◦ **capwap**：接続ポイントを CAPWAP トンネルとして指定します。 （注） このインターフェイスを接続ポイントとして使用すると、コア フィルタは使用できません。 • （任意）**control-plane**：接続ポイントとしてコントロール プレーンを指定します。 • **in**	**out**	**both**：キャプチャの方向を指定します。
ステップ 4	**monitor capture** {*capture-name*}[**match** {**any**	**ipv4 any any**	**ipv6**} **any any**}] 例： `Switch# monitor capture mycap interface GigabitEthernet1/0/1 in match any`	コア システムのフィルタを定義します。 （注） コア フィルタが使用できなくなるため、CAPWAP のトンネリングインターフェイスを接続ポイントとして使用する場合はこの手順を実行しないでください。 キーワードの意味は次のとおりです。 • *capture-name*：定義するキャプチャ ポイントの名前を指定します（例では mycap が使用されています）。 • **match**：フィルタを指定します。 定義されている最初のフィルタはコア フィルタです。 （注） キャプチャ ポイントは、コア システム フィルタと接続ポイントのどちらも定義されていない場合はアクティブにできません。 これらの要件を満たしていないキャプチャ ポイントをアクティブ化しようとすると、エラーが生成されます。 • **ipv4**：IPバージョン 4 のフィルタを指定します。 • **ipv6**：IPバージョン 6 のフィルタを指定します。

ステップ 5	**show monitor capture** {*capture-name*}[**parameter**]
	
	例：
	`Switch# show monitor capture mycap parameter`
	`monitor capture mycap`
		ステップ 2 で定義したキャプチャ ポイント パラメータを表示し、キャプチャ ポイントを定義したことを確認します。

	コマンドまたはアクション	目的

	`interface GigabitEthernet1/0/1`
	` in`
	`  monitor capture mycap match`
	` any`	

ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

CAPWAP 接続ポイントでキャプチャ ポイントを定義するには次を実行します。

```
Switch# show capwap summary

CAPWAP Tunnels General Statistics:
  Number of Capwap Data Tunnels       = 1
  Number of Capwap Mobility Tunnels   = 0
  Number of Capwap Multicast Tunnels  = 0


Name   APName                           Type PhyPortIf Mode      McastIf
------ -------------------------------- ---- --------- --------- -------
Ca0    AP442b.03a9.6715                 data Gi3/0/6   unicast   -


Name   SrcIP           SrcPort DestIP          DstPort DtlsEn MTU   Xact
------ --------------- ------- --------------- ------- ------ ----- ----
Ca0    10.10.14.32     5247    10.10.14.2      38514   No     1449  0

Switch# monitor capture mycap interface capwap 0 both
Switch# monitor capture mycap file location flash:mycap.pcap
Switch# monitor capture mycap file buffer-size 1
Switch# monitor capture mycap start

*Aug 20 11:02:21.983: %BUFCAP-6-ENABLE: Capture Point mycap enabled.on

Switch# show monitor capture mycap parameter
   monitor capture mycap interface capwap  0 in
   monitor capture mycap interface capwap  0 out
   monitor capture mycap file location flash:mycap.pcap buffer-size 1
Switch#
Switch# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
  Interface: CAPWAP,
    Ingress:
 0
    Egress:
 0
   Status : Active
  Filter Details:
```

```
    Capture all packets
  Buffer Details:
   Buffer Type: LINEAR (default)
  File Details:
   Associated file name: flash:mycap.pcap
   Size of buffer(in MB): 1
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Packets per second: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
Switch#
Switch# show monitor capture file flash:mycap.pcap
  1   0.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  2   0.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  3   2.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  4   2.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  5   3.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  6   4.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  7   4.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  8   5.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  9   5.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 10   6.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 11   8.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 12   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 13   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 14   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 15   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 16   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 17   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 18   9.236987   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 19  10.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 20  10.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 21  12.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 22  12.239993   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 23  12.244997   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 24  12.244997   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 25  12.250994   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 26  12.256990   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 27  12.262987   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 28  12.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 29  12.802012   10.10.14.3 -> 10.10.14.255 NBNS Name query NB WPAD.<00>
 30  13.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
```

次の作業

さらなる接続ポイントを追加して、キャプチャ ポイントのパラメータを変更し、アクティブ化できます。または、キャプチャ ポイントをそのまま使用したい場合はすぐにアクティブ化することもできます。

（注） このトピックで説明されているメソッドを使用してキャプチャ ポイントのパラメータを変更することはできません。

関連トピック

Wireshark の設定方法, （211 ページ）
キャプチャ ポイント, （200 ページ）
接続ポイント, （201 ページ）
例：単純なキャプチャおよび表示, （232 ページ）
例：単純なキャプチャおよび保存, （233 ページ）
例：バッファのキャプチャの使用, （234 ページ）
例：キャプチャ セッション, （239 ページ）
例：ロック ステップ モードのキャプチャおよび保存, （240 ページ）
例：出方向のパケットの簡単なキャプチャおよび保存, （241 ページ）

キャプチャ ポイント パラメータの追加または変更

パラメータの値を指定する手順は、順番にリストされますが、任意の順序で実行できます。1行、2 行、または複数行で指定できます。 複数指定が可能な接続ポイントを除き、同じオプションを再定義することで、任意の値をより最近の値に置き換えることができます。

キャプチャ ポイントのパラメータを変更するには、次の手順を実行します。

はじめる前に

以下の手順を実行する前にキャプチャ ポイントを定義する必要があります。

手順の概要

1. **enable**
2. **monitor capture** {*capture-name*} **match** {**any** | **mac** *mac-match-string* | **ipv4** {**any** | **host** | **protocol**} {**any** | **host**} | **ipv6** {**any** | **host** | **protocol**} {**any** | **host**}}
3. **monitor capture** {*capture-name*} **limit** {[**duration** *seconds*][**packet-length** *size*][**packets** *num*]}
4. **monitor capture** {*capture-name*} **file** {**location** *filename*}
5. **monitor capture** {*capture-name*} **file** {**buffer-size** *size*}
6. **show monitor capture** {*capture-name*}[**parameter**]
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**monitor capture** {*capture-name*} **match** {**any** | **mac** *mac-match-string* | **ipv4** {**any** | **host** | **protocol**}{**any** | **host**} | **ipv6** {**any** | **host** | **protocol**}{**any** | **host**}} 例： `Switch# monitor capture mycap match ipv4 any any`	明示的に、または ACL を介して、またはクラスマップを介して定義されたコア システム フィルタ（**ipv4 any any**）を定義します。 （注） CAPWAP トンネリング インターフェイスを使用してワイヤレス キャプチャを定義している場合、このコマンドには効果がないので使用しないでください。
ステップ 3	**monitor capture** {*capture-name*} **limit** {[**duration** *seconds*][**packet-length** *size*][**packets** *num*]} 例： `Switch# monitor capture mycap limit duration 60 packet-len 400`	秒単位のセッション制限（60）、キャプチャされたパケット、または Wireshark によって保持されるパケット セグメント長（400）を指定します。
ステップ 4	**monitor capture** {*capture-name*} **file** {**location** *filename*} 例： `Switch# monitor capture mycap file location flash:mycap.pcap`	キャプチャ ポイントがパケットを表示するだけでなくキャプチャできるようにする場合は、ファイルのアソシエーションを指定します。
ステップ 5	**monitor capture** {*capture-name*} **file** {**buffer-size** *size*} 例： `Switch# monitor capture mycap file buffer-size 100`	トラフィック バーストの処理に Wireshark で使用されるメモリ バッファのサイズを指定します。

ステップ 6	**show monitor capture** {*capture-name*}[**parameter**]
	
	例：
	`Switch# show monitor capture mycap parameter`
	`monitor capture mycap interface GigabitEthernet1/0/1 in`
	`monitor capture mycap match ipv4 any any`
	`monitor capture mycap limit duration 60 packet-len 400`
	`monitor capture point mycap file location bootdisk:mycap.pcap`
	`monitor capture mycap file buffer-size 100`
		以前に定義したキャプチャ ポイント パラメータを表示します。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

例

パラメータの変更

キャプチャ ファイルの関連付けまたは関連付け解除

```
Switch# monitor capture point mycap file location flash:mycap.pcap
Switch# no monitor capture mycap file
```

パケット バーストの処理にメモリ バッファ サイズを指定する

```
Switch# monitor capture mycap buffer size 100
```

IPv4 と IPv6 の両方に一致するように、明示的なコア システム フィルタを定義する

```
Switch# monitor capture mycap match any
```

次の作業

キャプチャ ポイントに必要なパラメータがすべて含まれている場合はアクティブ化します。

関連トピック

Wireshark の設定方法，（211 ページ）
キャプチャ ポイント，（200 ページ）
接続ポイント，（201 ページ）
例：単純なキャプチャおよび表示，（232 ページ）
例：単純なキャプチャおよび保存，（233 ページ）
例：バッファのキャプチャの使用，（234 ページ）
例：キャプチャ セッション，（239 ページ）

例：ロック ステップ モードのキャプチャおよび保存, （240 ページ）
例：出方向のパケットの簡単なキャプチャおよび保存, （241 ページ）

キャプチャ ポイント パラメータの削除

順番に表示されていますが、パラメータを削除する手順は任意の順序で実行できます。 1 行、2 行、または複数行で削除できます。 複数が可能な接続ポイントを除いて、任意のパラメータを削除できます。

キャプチャ ポイントのパラメータを削除するには、次の手順を実行します。

はじめる前に

キャプチャ ポイント パラメータは、以下の手順を使用して削除する前に定義する必要があります。

手順の概要

1. **enable**
2. **no monitor capture** {*capture-name*} **match**
3. **no monitor capture** {*capture-name*} **limit** [**duration**][**packet-length**][**packets**]
4. **no monitor capture** {*capture-name*} **file** [**location**] [**buffer-size**]
5. **show monitor capture** {*capture-name*}[**parameter**]
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**no monitor capture** {*capture-name*} **match** 例： `Switch# no monitor capture mycap match`	キャプチャ ポイント（mycap）で定義されているすべてのフィルタを削除します。

	コマンドまたはアクション	目的

ステップ 3	**no monitor capture** {*capture-name*} **limit** [**duration**][**packet-length**][**packets**]
	
	例：
	`Switch# no monitor capture mycap limit duration packet-len`
	`Switch# no monitor capture mycap limit`
		Wireshark によって保持されるセッション タイム制限およびパケット セグメント長を削除します。 その他の指定された制限はそのままになります。
		
		Wireshark のすべての制限をクリアします。

ステップ 4	**no monitor capture** {*capture-name*} **file** [**location**] [**buffer-size**]
	
	例：
	`Switch# no monitor capture mycap file`
	`Switch# no monitor capture mycap file location`
		ファイルの関連付けを削除します。 キャプチャ ポイントはパケットをキャプチャしなくなります。 表示だけが実行されます。
		
		ファイル位置の関連付けを削除します。 ファイル位置はキャプチャ ポイントとは関連付けられなくなります。 ただし、他の定義されたファイル関連付けはこのアクションによっては影響を受けません。

ステップ 5	**show monitor capture** {*capture-name*}[**parameter**]
	
	例：
	`Switch# show monitor capture mycap parameter`
	`monitor capture mycap interface GigabitEthernet1/0/1 in`
		パラメータの削除操作後にまだ定義されているキャプチャ ポイント パラメータを表示します。 このコマンドは、キャプチャ ポイントと関連付けられるパラメータを確認するために手順の任意の地点で実行できます。

ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

キャプチャ ポイントに必要なパラメータがすべて含まれている場合はアクティブ化します。

関連トピック

Wireshark の設定方法, （211 ページ）
キャプチャ ポイント, （200 ページ）
接続ポイント, （201 ページ）
例：単純なキャプチャおよび表示, （232 ページ）
例：単純なキャプチャおよび保存, （233 ページ）
例：バッファのキャプチャの使用, （234 ページ）
例：キャプチャ セッション, （239 ページ）
例：ロック ステップ モードのキャプチャおよび保存, （240 ページ）
例：出方向のパケットの簡単なキャプチャおよび保存, （241 ページ）

キャプチャ ポイントの削除

キャプチャ ポイントを削除するには、次の手順を実行します。

はじめる前に

キャプチャ ポイントは、以下の手順を使用して削除する前に定義する必要があります。

手順の概要

1. **enable**
2. **no monitor capture** {*capture-name*}
3. **show monitor capture** {*capture-name*}[**parameter**]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**no monitor capture** {*capture-name*} 例： `Switch# no monitor capture mycap`	指定されたキャプチャ ポイント（mycap）を削除します。

	コマンドまたはアクション	目的

ステップ 3	**show monitor capture** {*capture-name*}[**parameter**]
	
	例：
	`Switch# show monitor capture mycap parameter`
	
	`Capture mycap does not exist`
		指定されたキャプチャ ポイントは削除されたため存在しないことを示すメッセージを表示します。

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	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次の作業

削除したものと同じ名前の新規キャプチャ ポイントを定義できます。これらの手順は通常、キャプチャ ポイントの定義をやり直したい場合に実行します。

関連トピック

Wireshark の設定方法，（211 ページ）
キャプチャ ポイント，（200 ページ）
接続ポイント，（201 ページ）
例：単純なキャプチャおよび表示，（232 ページ）
例：単純なキャプチャおよび保存，（233 ページ）
例：バッファのキャプチャの使用，（234 ページ）
例：キャプチャ セッション，（239 ページ）
例：ロック ステップ モードのキャプチャおよび保存，（240 ページ）
例：出方向のパケットの簡単なキャプチャおよび保存，（241 ページ）

キャプチャ ポイントをアクティブまたは非アクティブにする

キャプチャ ポイントをアクティブまたは非アクティブにするには、次の手順を実行します。

はじめる前に

接続ポイントとコア システム フィルタが定義され、関連するファイル名（存在する場合）が存在していなければ、キャプチャ ポイントをアクティブにできません。 関連するファイル名のないキャプチャ ポイントは、表示するためだけにアクティブにできます。 キャプチャ フィルタまたは表示フィルタが指定されていない場合、コア システム フィルタによってキャプチャされたすべてのパケットが表示されます。 デフォルトの表示モードは brief です。

（注） CAPWAP のトンネリング インターフェイスを接続ポイントとして使用すると、コア フィルタは使用されないため、この場合は定義する必要はありません。

手順の概要

1. **enable**
2. **monitor capture** {*capture-name*} **start**[**display** [**display-filter** *filter-string*]][**brief** | **detailed** | **dump**]
3. **monitor capture** {*capture-name*} **stop**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**monitor capture** {*capture-name*} **start**[**display** [**display-filter** *filter-string*]][**brief**	**detailed**	**dump**] 例： `Switch# monitor capture mycap start display display-filter "stp"`	キャプチャ ポイントをアクティブ化し、「stp」を含むパケットだけが表示されるように表示をフィルタします。
ステップ 3	**monitor capture** {*capture-name*} **stop** 例： `Switch# monitor capture name stop`	キャプチャ ポイントを非アクティブにします。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

Wireshark の設定方法，（211 ページ）
キャプチャ ポイント，（200 ページ）
接続ポイント，（201 ページ）
例：単純なキャプチャおよび表示，（232 ページ）
例：単純なキャプチャおよび保存，（233 ページ）
例：バッファのキャプチャの使用，（234 ページ）
例：キャプチャ セッション，（239 ページ）
例：ロック ステップ モードのキャプチャおよび保存，（240 ページ）
例：出方向のパケットの簡単なキャプチャおよび保存，（241 ページ）

キャプチャ ポイント バッファのクリア

次の手順に従ってバッファ コンテンツをクリアするか、外部ファイルにストレージとして保存します。

（注） パケットをバッファ内に保存する複数のキャプチャがある場合、メモリ ロスを避けるため、新しいキャプチャを開始する前にバッファをクリアしてください。

手順の概要

1. **enable**
2. **monitor capture** {*capture-name*} [**clear** | **export** *filename*]
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**monitor capture** {*capture-name*} [**clear** | **export** *filename*] 例： `Switch# monitor capture mycap clear`	キャプチャ バッファ コンテンツをクリアするか、パケットをファイルに保存します。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 5	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

例：キャプチャ ポイント バッファの処理

キャプチャのファイルへのエクスポート

```
Switch# monitor capture mycap export flash:mycap.pcap
Storage configured as File for this capture
```

キャプチャ ポイント バッファのクリア

```
Switch# monitor capture mycap clear
 Capture configured with file options
```

関連トピック

Wireshark の設定方法，（211 ページ）
キャプチャ ポイント，（200 ページ）
接続ポイント，（201 ページ）
例：単純なキャプチャおよび表示，（232 ページ）
例：単純なキャプチャおよび保存，（233 ページ）
例：バッファのキャプチャの使用，（234 ページ）
例：キャプチャ セッション，（239 ページ）
例：ロック ステップ モードのキャプチャおよび保存，（240 ページ）
例：出方向のパケットの簡単なキャプチャおよび保存，（241 ページ）

Wireshark のモニタリング

このテーブルのコマンドは Wireshark のモニタリングに使用されます。

コマンド	目的
show monitor capture [*capture-name*]	キャプチャ ポイント ステートが表示され、キャプチャ ポイントの定義状況、属性、アクティブ状況を確認することができます。 キャプチャ ポイントの名前を指定すると、特定のキャプチャ ポイントの細部が表示されます。
show monitor capture [*capture-name* **parameter**]	キャプチャ ポイント パラメータを表示します。
show capwap summary	スイッチ のすべての CAPWAP トンネルを表示します。このコマンドを使用して、ワイヤレス キャプチャにどの CAPWAP トンネルを使用できるかを判断します。

Wireshark の設定例

例：.pcap ファイルからの概要出力の表示

次のように入力して、.pcap ファイルからの出力を表示できます。

```
Switch# show monitor capture file flash:mycap.pcap
  1   0.000000   10.1.1.140 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  2   1.000000   10.1.1.141 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  3   2.000000   10.1.1.142 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  4   3.000000   10.1.1.143 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  5   4.000000   10.1.1.144 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  6   5.000000   10.1.1.145 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  7   6.000000   10.1.1.146 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  8   7.000000   10.1.1.147 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  9   8.000000   10.1.1.148 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 10   9.000000   10.1.1.149 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 11  10.000000   10.1.1.150 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 12  11.000000   10.1.1.151 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 13  12.000000   10.1.1.152 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 14  13.000000   10.1.1.153 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 15  14.000000   10.1.1.154 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 16  15.000000   10.1.1.155 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 17  16.000000   10.1.1.156 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 18  17.000000   10.1.1.157 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 19  18.000000   10.1.1.158 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 20  19.000000   10.1.1.159 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 21  20.000000   10.1.1.160 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 22  21.000000   10.1.1.161 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 23  22.000000   10.1.1.162 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 24  23.000000   10.1.1.163 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 25  24.000000   10.1.1.164 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 26  25.000000   10.1.1.165 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 27  26.000000   10.1.1.166 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 28  27.000000   10.1.1.167 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 29  28.000000   10.1.1.168 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

```
30  29.000000   10.1.1.169 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
31  30.000000   10.1.1.170 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
32  31.000000   10.1.1.171 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
33  32.000000   10.1.1.172 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
34  33.000000   10.1.1.173 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
35  34.000000   10.1.1.174 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
36  35.000000   10.1.1.175 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
37  36.000000   10.1.1.176 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
38  37.000000   10.1.1.177 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
39  38.000000   10.1.1.178 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
40  39.000000   10.1.1.179 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
41  40.000000   10.1.1.180 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
42  41.000000   10.1.1.181 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
43  42.000000   10.1.1.182 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
44  43.000000   10.1.1.183 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
45  44.000000   10.1.1.184 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
46  45.000000   10.1.1.185 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
47  46.000000   10.1.1.186 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
48  47.000000   10.1.1.187 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
49  48.000000   10.1.1.188 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
50  49.000000   10.1.1.189 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
51  50.000000   10.1.1.190 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
52  51.000000   10.1.1.191 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
53  52.000000   10.1.1.192 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
54  53.000000   10.1.1.193 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
55  54.000000   10.1.1.194 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
56  55.000000   10.1.1.195 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
57  56.000000   10.1.1.196 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
58  57.000000   10.1.1.197 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
59  58.000000   10.1.1.198 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

例：.pcap ファイルからの詳細出力の表示

次のように入力して、.pcap ファイルの出力詳細を表示できます。

```
Switch# show monitor capture file flash:mycap.pcap detailed

Frame 1: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits)
    Arrival Time: Mar 21, 2012 14:35:09.111993000 PDT
    Epoch Time: 1332365709.111993000 seconds
```

```
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 256 bytes (2048 bits)
    Capture Length: 256 bytes (2048 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:udp:data]
Ethernet II, Src: 00:00:00:00:03:01 (00:00:00:00:03:01), Dst: 54:75:d0:3a:85:3f
(54:75:d0:3a:85:3f)
    Destination: 54:75:d0:3a:85:3f (54:75:d0:3a:85:3f)
        Address: 54:75:d0:3a:85:3f (54:75:d0:3a:85:3f)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Source: 00:00:00:00:03:01 (00:00:00:00:03:01)
        Address: 00:00:00:00:03:01 (00:00:00:00:03:01)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
    Frame check sequence: 0x03b07f42 [incorrect, should be 0x08fcee78]
Internet Protocol, Src: 10.1.1.140 (10.1.1.140), Dst: 20.1.1.2 (20.1.1.2)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 238
    Identification: 0x0000 (0)
    Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x5970 [correct]
        [Good: True]
        [Bad: False]
    Source: 10.1.1.140 (10.1.1.140)
    Destination: 20.1.1.2 (20.1.1.2)
User Datagram Protocol, Src Port: 20001 (20001), Dst Port: 20002 (20002)
    Source port: 20001 (20001)
    Destination port: 20002 (20002)
    Length: 218
    Checksum: 0x6e2b [validation disabled]
        [Good Checksum: False]
        [Bad Checksum: False]
Data (210 bytes)

0000  00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f   ................
0010  10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f   ................
0020  20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f    !"#$%&'()*+,-./
0030  30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f   0123456789:;<=>?
0040  40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f   @ABCDEFGHIJKLMNO
0050  50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f   PQRSTUVWXYZ[\]^_
0060  60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f   `abcdefghijklmno
0070  70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f   pqrstuvwxyz{|}~.
0080  80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f   ................
0090  90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f   ................
00a0  a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af   ................
00b0  b0 b1 b2 b3 b4 b5 b6 b7 b8 b9 ba bb bc bd be bf   ................
00c0  c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf   ................
00d0  d0 d1                                            ..
    Data: 000102030405060708090a0b0c0d0e0f1011121314151617...
    [Length: 210]

Frame 2: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits)
    Arrival Time: Mar 21, 2012 14:35:10.111993000 PDT
Example: Displaying a Hexadecimal Dump Output from a .pcap File
You can display the hexadecimal dump output by entering:
Switch# show monitor capture file bootflash:mycap.pcap dump
```

```
  1   0.000000   10.1.1.140 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002

0000  54 75 d0 3a 85 3f 00 00 00 00 03 01 08 00 45 00   Tu.:.?........E.
0010  00 ee 00 00 00 00 40 11 59 70 0a 01 01 8c 14 01   ......@.Yp......
0020  01 02 4e 21 4e 22 00 da 6e 2b 00 01 02 03 04 05   ..N!N"..n+......
0030  06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15   ................
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25   .......... !"#$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35   &'()*+,-./012345
0060  36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45   6789:;<=>?@ABCDE
0070  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55   FGHIJKLMNOPQRSTU
0080  56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65   VWXYZ[\]^_`abcde
0090  66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75   fghijklmnopqrstu
00a0  76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85   vwxyz{|}~.......
00b0  86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95   ................
00c0  96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5   ................
00d0  a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5   ................
00e0  b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5   ................
00f0  c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 03 b0 7f 42   ...............B

  2   1.000000   10.1.1.141 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002

0000  54 75 d0 3a 85 3f 00 00 00 00 03 01 08 00 45 00   Tu.:.?........E.
0010  00 ee 00 00 00 00 40 11 59 6f 0a 01 01 8d 14 01   ......@.Yo......
0020  01 02 4e 21 4e 22 00 da 6e 2a 00 01 02 03 04 05   ..N!N"..n*......
0030  06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15   ................
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25   .......... !"#$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35   &'()*+,-./012345
0060  36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45   6789:;<=>?@ABCDE
0070  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55   FGHIJKLMNOPQRSTU
0080  56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65   VWXYZ[\]^_`abcde
0090  66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75   fghijklmnopqrstu
00a0  76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85   vwxyz{|}~.......
00b0  86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95   ................
00c0  96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5   ................
00d0  a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5   ................
00e0  b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5   ................
00f0  c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 95 2c c3 3f   .............,.?

  3   2.000000   10.1.1.142 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002

0000  54 75 d0 3a 85 3f 00 00 00 00 03 01 08 00 45 00   Tu.:.?........E.
0010  00 ee 00 00 00 00 40 11 59 6e 0a 01 01 8e 14 01   ......@.Yn......
0020  01 02 4e 21 4e 22 00 da 6e 29 00 01 02 03 04 05   ..N!N"..n).....
0030  06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15   ................
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25   .......... !"#$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35   &'()*+,-./012345
0060  36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45   6789:;<=>?@ABCDE
0070  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55   FGHIJKLMNOPQRSTU
0080  56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65   VWXYZ[\]^_`abcde
0090  66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75   fghijklmnopqrstu
00a0  76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85   vwxyz{|}~.......
00b0  86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95   ................
00c0  96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5   ................
00d0  a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5   ................
00e0  b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5   ................
00f0  c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 6c f8 dc 14   ............l...

  4   3.000000   10.1.1.143 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002

0000  54 75 d0 3a 85 3f 00 00 00 00 03 01 08 00 45 00   Tu.:.?........E.
0010  00 ee 00 00 00 00 40 11 59 6d 0a 01 01 8f 14 01   ......@.Ym......
0020  01 02 4e 21 4e 22 00 da 6e 28 00 01 02 03 04 05   ..N!N"..n(......
0030  06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15   ................
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25   .......... !"#$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35   &'()*+,-./012345
Example: Displaying Packets from a .pcap File with a Display Filter
You can display the .pcap file packets output by entering:
Switch# show monitor capture file bootflash:mycap.pcap display-filter "ip.src == 10.1.1.140"
 dump
  1   0.000000   10.1.1.140 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002

0000  54 75 d0 3a 85 3f 00 00 00 00 03 01 08 00 45 00   Tu.:.?........E.
0010  00 ee 00 00 00 00 40 11 59 70 0a 01 01 8c 14 01   ......@.Yp......
```

```
0020  01 02 4e 21 4e 22 00 da 6e 2b 00 01 02 03 04 05   ..N!N"..n+......
0030  06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15   ................
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25   .......... !"#$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35   &'()*+,-./012345
0060  36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45   6789:;<=>?@ABCDE
0070  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55   FGHIJKLMNOPQRSTU
0080  56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65   VWXYZ[\]^_`abcde
0090  66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75   fghijklmnopqrstu
00a0  76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85   vwxyz{|}~.......
00b0  86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95   ................
00c0  96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5   ................
00d0  a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5   ................
00e0  b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5   ................
00f0  c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 03 b0 7f 42   ...............B
```

例：単純なキャプチャおよび表示

次の例は、レイヤ 3 インターフェイス ギガビット イーサネット 1/0/1 でトラフィックをモニタする方法を示しています。

ステップ 1：次のように入力して関連トラフィックで一致するキャプチャ ポイントを定義します。

```
Switch# monitor capture mycap interface GigabitEthernet1/0/1 in
Switch# monitor capture mycap match ipv4 any any
Switch# monitor capture mycap limit duration 60 packets 100
Switch# monitor capture mycap buffer size 100
```

CPU使用率の上昇を避けるため、制限として最も低いパケット数および時間が設定されています。

ステップ 2：次のように入力してキャプチャ ポイントが正確に定義されていることを確認します。

```
Switch# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
   monitor capture mycap match ipv4  any any
   monitor capture mycap buffer size 100
   monitor capture mycap limit packets 100 duration 60

Switch# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/1, Direction: in
   Status : Inactive
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: LINEAR (default)
   Buffer Size (in MB): 100
  File Details:
   File not associated
  Limit Details:
   Number of Packets to capture: 100
   Packet Capture duration: 60
   Packet Size to capture: 0 (no limit)
   Packets per second: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
```

ステップ 3：キャプチャ プロセスを開始し、結果を表示します。

```
Switch# monitor capture mycap start display
  0.000000    10.1.1.30 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  1.000000    10.1.1.31 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  2.000000    10.1.1.32 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  3.000000    10.1.1.33 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  4.000000    10.1.1.34 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  5.000000    10.1.1.35 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

```
  6.000000    10.1.1.36 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  7.000000    10.1.1.37 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  8.000000    10.1.1.38 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  9.000000    10.1.1.39 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

ステップ 4：次のように入力してキャプチャ ポイントを削除します。

```
Switch# no monitor capture mycap
```

関連トピック

キャプチャ ポイントの定義，（212 ページ）
キャプチャ ポイント パラメータの追加または変更，（217 ページ）
キャプチャ ポイント パラメータの削除，（220 ページ）
キャプチャ ポイントの削除，（222 ページ）
キャプチャ ポイントをアクティブまたは非アクティブにする，（224 ページ）
キャプチャ ポイント バッファのクリア，（225 ページ）
Wireshark の設定方法，（211 ページ）
キャプチャ ポイント，（200 ページ）
接続ポイント，（201 ページ）

例：単純なキャプチャおよび保存

次の例は、フィルタにパケットをキャプチャする方法を示しています。

ステップ 1：次のように入力して、関連トラフィックで一致するキャプチャ ポイントを定義し、それをファイルに関連付けます。

```
Switch# monitor capture mycap interface GigabitEthernet1/0/1 in
Switch# monitor capture mycap match ipv4 any any
Switch# monitor capture mycap limit duration 60 packets 100
Switch# monitor capture mycap file location flash:mycap.pcap
```

ステップ 2：次のように入力してキャプチャ ポイントが正確に定義されていることを確認します。

```
Switch# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
   monitor capture mycap match ipv4  any any
   monitor capture mycap file location flash:mycap.pcap
   monitor capture mycap limit packets 100 duration 60

Switch# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/1, Direction: in
   Status : Inactive
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: LINEAR (default)
  File Details:
   Associated file name: flash:mycap.pcap
  Limit Details:
```

```
Number of Packets to capture: 100
Packet Capture duration: 60
Packet Size to capture: 0 (no limit)
Packets per second: 0 (no limit)
Packet sampling rate: 0 (no sampling)
```

ステップ 3：次のように入力してパケットを開始します。

```
Switch# monitor capture mycap start
```

ステップ 4：十分な時間の経過後に、次のように入力してキャプチャを停止します。

```
Switch# monitor capture mycap stop
```

（注） あるいは、時間の経過またはパケット カウントが一致した後に、キャプチャ操作を自動的に停止させることもできます。

mycap.pcap ファイルには、キャプチャしたパケットが含まれます。

ステップ 5：次のように入力してパケットを表示します。

```
Switch# show monitor capture file flash:mycap.pcap

  0.000000    10.1.1.30 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  1.000000    10.1.1.31 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  2.000000    10.1.1.32 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  3.000000    10.1.1.33 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  4.000000    10.1.1.34 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  5.000000    10.1.1.35 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  6.000000    10.1.1.36 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  7.000000    10.1.1.37 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  8.000000    10.1.1.38 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  9.000000    10.1.1.39 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

ステップ 6：次のように入力してキャプチャ ポイントを削除します。

```
Switch# no monitor capture mycap
```

関連トピック

キャプチャ ポイントの定義，（212 ページ）
キャプチャ ポイント パラメータの追加または変更，（217 ページ）
キャプチャ ポイント パラメータの削除，（220 ページ）
キャプチャ ポイントの削除，（222 ページ）
キャプチャ ポイントをアクティブまたは非アクティブにする，（224 ページ）
キャプチャ ポイント バッファのクリア，（225 ページ）
Wireshark の設定方法，（211 ページ）
キャプチャ ポイント，（200 ページ）
接続ポイント，（201 ページ）

例：バッファのキャプチャの使用

次に、バッファのキャプチャを使用する例を示します。

ステップ 1：次のように入力してバッファ キャプチャ オプションでキャプチャ セッションを起動します。

```
Switch# monitor capture mycap interface GigabitEthernet1/0/1 in
Switch# monitor capture mycap match ipv4 any any
Switch# monitor capture mycap buffer circular size 1
Switch# monitor capture mycap start
```

ステップ 2：次のように入力してキャプチャがアクティブであるかどうかを決定します。

```
Switch# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/1, Direction: in
   Status : Active
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: CIRCULAR
   Buffer Size (in MB): 1
  File Details:
   File not associated
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Packets per second: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
```

ステップ 3：次のように入力してバッファのパケットを表示します。

```
Switch# show monitor capture mycap buffer brief

  0.000000   10.1.1.215 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  1.000000   10.1.1.216 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  2.000000   10.1.1.217 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  3.000000   10.1.1.218 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  4.000000   10.1.1.219 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  5.000000   10.1.1.220 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  6.000000   10.1.1.221 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  7.000000   10.1.1.222 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  8.000000   10.1.1.223 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  9.000000   10.1.1.224 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 10.000000   10.1.1.225 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 11.000000   10.1.1.226 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 12.000000   10.1.1.227 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 13.000000   10.1.1.228 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 14.000000   10.1.1.229 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 15.000000   10.1.1.230 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 16.000000   10.1.1.231 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 17.000000   10.1.1.232 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 18.000000   10.1.1.233 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 19.000000   10.1.1.234 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 20.000000   10.1.1.235 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 21.000000   10.1.1.236 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

パケットがバッファに入ったことに注意してください。

ステップ 4：他の表示モードでパケットを表示します。

```
Switch# show monitor capture mycap buffer detailed

Frame 1: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits)
    Arrival Time: Apr 15, 2012 15:50:02.398966000 PDT
    Epoch Time: 1334530202.398966000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
```

```
    Frame Number: 1
    Frame Length: 256 bytes (2048 bits)
    Capture Length: 256 bytes (2048 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:udp:data]
Ethernet II, Src: 00:00:00:00:03:01 (00:00:00:00:03:01), Dst: 54:75:d0:3a:85:3f
(54:75:d0:3a:85:3f)
    Destination: 54:75:d0:3a:85:3f (54:75:d0:3a:85:3f)
        Address: 54:75:d0:3a:85:3f (54:75:d0:3a:85:3f)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Source: 00:00:00:00:03:01 (00:00:00:00:03:01)
        Address: 00:00:00:00:03:01 (00:00:00:00:03:01)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
…
Switch# show monitor capture mycap buffer dump

  0.000000   10.1.1.215 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002

0000  54 75 d0 3a 85 3f 00 00 00 00 03 01 08 00 45 00   Tu.:.?........E.
0010  00 ee 00 00 00 00 40 11 59 25 0a 01 01 d7 14 01   ......@.Y%......
0020  01 02 4e 21 4e 22 00 da 6d e0 00 01 02 03 04 05   ..N!N"..m.......
0030  06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15   ................
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25   .......... !"#$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35   &'()*+,-./012345
0060  36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45   6789:;<=>?@ABCDE
0070  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55   FGHIJKLMNOPQRSTU
0080  56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65   VWXYZ[\]^_`abcde
0090  66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75   fghijklmnopqrstu
00a0  76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85   vwxyz{|}~.......
00b0  86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95   ................
00c0  96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5   ................
00d0  a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5   ................
00e0  b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5   ................
00f0  c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 03 3e d0 33   ............>.3
```

ステップ 5a：次のように入力してバッファをクリアします。

```
Switch# monitor capture mycap clear
```

ステップ 5b：10 秒待ちます。

ステップ 5c：次のように入力してトラフィックを停止します。

```
Switch# monitor capture mycap stop
```

ステップ 6：次のように入力して、同じパケット セットがこの時間空白の後に表示されることを確認します。

```
Switch# show monitor capture mycap buffer brief

  0.000000     10.1.1.2 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  1.000000     10.1.1.3 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  2.000000     10.1.1.4 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  3.000000     10.1.1.5 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  4.000000     10.1.1.6 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  5.000000     10.1.1.7 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  6.000000     10.1.1.8 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  7.000000     10.1.1.9 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  8.000000    10.1.1.10 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  9.000000    10.1.1.11 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

ステップ 7：10 秒待ってから、次のように入力して待機後も同じパケットのセットが表示されることを確認します。

```
Switch# show monitor capture mycap buffer brief

  0.000000     10.1.1.2 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

```
  1.000000     10.1.1.3 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  2.000000     10.1.1.4 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  3.000000     10.1.1.5 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  4.000000     10.1.1.6 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  5.000000     10.1.1.7 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  6.000000     10.1.1.8 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  7.000000     10.1.1.9 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  8.000000    10.1.1.10 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  9.000000    10.1.1.11 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

ステップ 8：ステップ 7 を繰り返します。

ステップ 9：次のように入力してバッファをクリアします。

```
Switch# monitor capture mycap clear
```

ステップ 10：次のように入力してバッファが現在空であることを確認します。

```
Switch# show monitor capture mycap buffer brief
```

ステップ 11：約 10 秒待ってから、次のように入力してコンテンツをさらに表示します。

```
Switch# show monitor capture mycap buffer brief
```

ステップ 12：トラフィックを再開し、10 秒待ってから次のように入力してバッファ コンテンツを表示します。

```
Switch# monitor capture mycap start
wait for 10 seconds...
Switch# show monitor capture mycap buffer brief

  0.000000     10.1.1.2 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  1.000000     10.1.1.3 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  2.000000     10.1.1.4 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  3.000000     10.1.1.5 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  4.000000     10.1.1.6 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  5.000000     10.1.1.7 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  6.000000     10.1.1.8 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  7.000000     10.1.1.9 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  8.000000    10.1.1.10 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  9.000000    10.1.1.11 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

ステップ 13：次のように入力して、内部 flash: storage デバイス内の mycap1.pcap ファイルにバッファ コンテンツを保存します。

```
Switch# monitor capture mycap export flash:mycap1.pcap
Exported Successfully
```

ステップ 14：次のように入力して、ファイルが作成されたこと、また、そこにパケットが含まれていることを確認します。

```
Switch# dir flash:mycap1.pcap
Directory of flash:/mycap1.pcap

14758  -rw-       20152  Apr 15 2012 16:00:28 -07:00  mycap1.pcap

831541248 bytes total (831340544 bytes free)
Switch# show monitor capture file flash:mycap1.pcap brief
  1   0.000000     10.1.1.2 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002

  2   1.000000     10.1.1.3 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002

  3   2.000000     10.1.1.4 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002

  4   3.000000     10.1.1.5 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002

  5   4.000000     10.1.1.6 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

```
  6   5.000000     10.1.1.7 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  7   6.000000     10.1.1.8 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  8   7.000000     10.1.1.9 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  9   8.000000    10.1.1.10 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 10   9.000000    10.1.1.11 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 11  10.000000    10.1.1.12 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 12  11.000000    10.1.1.13 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 13  12.000000    10.1.1.14 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 14  13.000000    10.1.1.15 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 15  14.000000    10.1.1.16 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 16  15.000000    10.1.1.17 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

ステップ 15：次のように入力して、パケット キャプチャを停止し、バッファの内容を表示します。

```
Switch# monitor capture mycap stop
Switch# show monitor capture mycap buffer brief

  0.000000     10.1.1.2 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  1.000000     10.1.1.3 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  2.000000     10.1.1.4 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  3.000000     10.1.1.5 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  4.000000     10.1.1.6 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  5.000000     10.1.1.7 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  6.000000     10.1.1.8 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  7.000000     10.1.1.9 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  8.000000    10.1.1.10 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  9.000000    10.1.1.11 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 10.000000    10.1.1.12 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 11.000000    10.1.1.13 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

ステップ 16：次のように入力して、バッファをクリアしてから、バッファからのパケットを表示します。

```
Switch# monitor capture mycap clear
Switch# show monitor capture mycap buffer brief
```

ステップ 17：次のように入力して、キャプチャ ポイントを削除します。

```
Switch# no monitor capture mycap
```

関連トピック

キャプチャ ポイントの定義，（212 ページ）
キャプチャ ポイント パラメータの追加または変更，（217 ページ）
キャプチャ ポイント パラメータの削除，（220 ページ）
キャプチャ ポイントの削除，（222 ページ）
キャプチャ ポイントをアクティブまたは非アクティブにする，（224 ページ）
キャプチャ ポイント バッファのクリア，（225 ページ）
Wireshark の設定方法，（211 ページ）

キャプチャ ポイント，（200 ページ）
接続ポイント，（201 ページ）

例：キャプチャ セッション

```
Switch# monitor capture mycap start display display-filter "stp"
  0.000000 20:37:06:cf:08:b6 -> 01:80:c2:00:00:00 STP Conf. Root = 32768/100/20:37:06:ce:f0:80
   Cost = 0  Port = 0x8136
  2.000992 20:37:06:cf:08:b6 -> 01:80:c2:00:00:00 STP Conf. Root = 32768/100/20:37:06:ce:f0:80
   Cost = 0  Port = 0x8136
  2.981996 20:37:06:cf:08:b6 -> 20:37:06:cf:08:b6 LOOP Reply
  4.000992 20:37:06:cf:08:b6 -> 01:80:c2:00:00:00 STP Conf. Root = 32768/100/20:37:06:ce:f0:80
   Cost = 0  Port = 0x8136
  6.000000 20:37:06:cf:08:b6 -> 01:80:c2:00:00:00 STP Conf. Root = 32768/100/20:37:06:ce:f0:80
   Cost = 0  Port = 0x8136
  7.998001 20:37:06:cf:08:b6 -> 01:80:c2:00:00:00 STP Conf. Root = 32768/100/20:37:06:ce:f0:80
   Cost = 0  Port = 0x8136
  9.998001 20:37:06:cf:08:b6 -> 01:80:c2:00:00:00 STP Conf. Root = 32768/100/20:37:06:ce:f0:80
   Cost = 0  Port = 0x8136
Capture test is not active Failed to Initiate Wireshark
Switch# show monitor capture mycap parameter
   monitor capture mycap control-plane both
   monitor capture mycap match any
   monitor capture mycap file location flash:mycap1.1 buffer-size 90
   monitor capture mycap limit duration 10

Switch# monitor capture mycap start display display-filter "udp.port == 20002"
A file by the same capture file name already exists, overwrite?[confirm] [ENTER]
after a minute or so...
Capture mycap is not active Failed to Initiate Wireshark
*Oct 13 15:00:44.649: %BUFCAP-6-ENABLE: Capture Point mycap enabled.
*Oct 13 15:00:46.657: %BUFCAP-6-DISABLE_ASYNC: Capture Point mycap disabled. Rea
son : Wireshark Session Ended

Switch# monitor capture mycap start display display-filter "udp.port == 20002" dump
A file by the same capture file name already exists, overwrite?[confirm]
after a minute or so...
Capture mycap is not active Failed to Initiate Wireshark
*Oct 13 15:00:44.649: %BUFCAP-6-ENABLE: Capture Point mycap enabled.
*Oct 13 15:00:46.657: %BUFCAP-6-DISABLE_ASYNC: Capture Point mycap disabled. Rea
son : Wireshark Session Ended

Switch# no monitor capture mycap file
Switch# monitor capture mycap start display display-filter "udp.port == 20002" dump
 Please associate capture file/buffer
Unable to activate Capture.

Switch# monitor capture mycap start display display-filter "udp.port == 20002"
 Please associate capture file/buffer
Unable to activate Capture.

Switch# monitor capture mycap start display detailed
 Please associate capture file/buffer
Unable to activate Capture.
```

関連トピック

キャプチャ ポイントの定義，（212 ページ）
キャプチャ ポイント パラメータの追加または変更，（217 ページ）
キャプチャ ポイント パラメータの削除，（220 ページ）
キャプチャ ポイントの削除，（222 ページ）
キャプチャ ポイントをアクティブまたは非アクティブにする，（224 ページ）
キャプチャ ポイント バッファのクリア，（225 ページ）

Wireshark の設定方法，（211 ページ）
キャプチャ ポイント，（200 ページ）
接続ポイント，（201 ページ）

例：ロック ステップ モードのキャプチャおよび保存

ここでは、リアルタイムのトラフィックをキャプチャし、パケットをロック ステップモードにすることで例を示しています。

（注） キャプチャ レートは最初の 15 秒間遅延する場合があります。 可能な場合、必要に応じてトラフィックをキャプチャ セッション開始後 15 秒後に開始してください。

ステップ 1：次のように入力して、関連トラフィックで一致するキャプチャ ポイントを定義し、それをファイルに関連付けます。

```
Switch# monitor capture mycap interface GigabitEthernet1/0/1 in
Switch# monitor capture mycap match ipv4 any any
Switch# monitor capture mycap limit duration 60 packets 100
Switch# monitor capture mycap file location flash:mycap.pcap buffer-size 64
```

ステップ 2：次のように入力してキャプチャ ポイントが正確に定義されていることを確認します。

```
Switch# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
   monitor capture mycap file location flash:mycap.pcap buffer-size 64
   monitor capture mycap limit packets 100 duration 60

Switch# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/1, Direction: in
   Status : Inactive
  Filter Details:
   Filter not attached
  Buffer Details:
   Buffer Type: LINEAR (default)
  File Details:
   Associated file name: flash:mycap.pcap
   Size of buffer(in MB): 64
  Limit Details:
   Number of Packets to capture: 100
   Packet Capture duration: 60
   Packet Size to capture: 0 (no limit)
   Packets per second: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
```

ステップ 3：次のように入力してパケットを開始します。

```
Switch# monitor capture mycap start
A file by the same capture file name already exists, overwrite?[confirm]
Turning on lock-step mode

Switch#
*Oct 14 09:35:32.661: %BUFCAP-6-ENABLE: Capture Point mycap enabled.
```

ステップ 4：次のように入力してパケットを表示します。

```
Switch# show monitor capture file flash:mycap.pcap
  0.000000    10.1.1.30 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  1.000000    10.1.1.31 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

```
  2.000000    10.1.1.32 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  3.000000    10.1.1.33 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  4.000000    10.1.1.34 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  5.000000    10.1.1.35 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  6.000000    10.1.1.36 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  7.000000    10.1.1.37 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  8.000000    10.1.1.38 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  9.000000    10.1.1.39 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

ステップ 5：次のように入力してキャプチャ ポイントを削除します。

```
Switch# no monitor capture mycap
```

関連トピック

キャプチャ ポイントの定義，（212 ページ）
キャプチャ ポイント パラメータの追加または変更，（217 ページ）
キャプチャ ポイント パラメータの削除，（220 ページ）
キャプチャ ポイントの削除，（222 ページ）
キャプチャ ポイントをアクティブまたは非アクティブにする，（224 ページ）
キャプチャ ポイント バッファのクリア，（225 ページ）
Wireshark の設定方法，（211 ページ）
キャプチャ ポイント，（200 ページ）
接続ポイント，（201 ページ）

例：出方向のパケットの簡単なキャプチャおよび保存

次の例は、フィルタにパケットをキャプチャする方法を示しています。

ステップ 1：次のように入力して、関連トラフィックで一致するキャプチャ ポイントを定義し、それをファイルに関連付けます。

```
Switch# monitor capture mycap interface Gigabit 1/0/1 out match ipv4 any any
Switch# monitor capture mycap limit duration 60 packets 100
Switch# monitor capture mycap file location flash:mycap.pcap buffer-size 90
```

ステップ 2：次のように入力してキャプチャ ポイントが正確に定義されていることを確認します。

```
Switch# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 out
   monitor capture mycap match ipv4  any any
   monitor capture mycap file location flash:mycap.pcap buffer-size 90
   monitor capture mycap limit packets 100 duration 60

Switch# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
   Interface: GigabitEthernet1/0/1, Direction: out
   Status : Inactive
  Filter Details:
   IPv4
    Source IP:  any
    Destination IP:  any
   Protocol: any
  Buffer Details:
   Buffer Type: LINEAR (default)
```

```
  File Details:
   Associated file name: flash:mycap.pcap
   Size of buffer(in MB): 90
  Limit Details:
   Number of Packets to capture: 100
   Packet Capture duration: 60
   Packet Size to capture: 0 (no limit)
   Packets per second: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
```

ステップ 3：次のように入力してパケットを開始します。

```
Switch# monitor capture mycap start
A file by the same capture file name already exists, overwrite?[confirm]
Turning on lock-step mode

Switch#
*Oct 14 09:35:32.661: %BUFCAP-6-ENABLE: Capture Point mycap enabled.
```

（注） 時間の経過またはパケット カウントが一致した後に、キャプチャ操作を自動的に停止させてください。 出力に次のメッセージが表示された場合は、キャプチャ処理が停止していることを意味します。

```
*Oct 14 09:36:34.632: %BUFCAP-6-DISABLE_ASYNC: Capture Point mycap disabled. Rea
son : Wireshark Session Ended
```

mycap.pcap ファイルには、キャプチャしたパケットが含まれます。

ステップ 4：次のように入力してパケットを表示します。

```
Switch# show monitor capture file flash:mycap.pcap
  0.000000    10.1.1.30 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  1.000000    10.1.1.31 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  2.000000    10.1.1.32 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  3.000000    10.1.1.33 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  4.000000    10.1.1.34 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  5.000000    10.1.1.35 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  6.000000    10.1.1.36 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  7.000000    10.1.1.37 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  8.000000    10.1.1.38 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  9.000000    10.1.1.39 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

ステップ 5：次のように入力してキャプチャ ポイントを削除します。

```
Switch# no monitor capture mycap
```

関連トピック

キャプチャ ポイントの定義，（212 ページ）
キャプチャ ポイント パラメータの追加または変更，（217 ページ）
キャプチャ ポイント パラメータの削除，（220 ページ）
キャプチャ ポイントの削除，（222 ページ）
キャプチャ ポイントをアクティブまたは非アクティブにする，（224 ページ）
キャプチャ ポイント バッファのクリア，（225 ページ）
Wireshark の設定方法，（211 ページ）
キャプチャ ポイント，（200 ページ）
接続ポイント，（201 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
一般的なパケット フィルタリング	一般的なパケット フィルタリングについては、次を参照してください。 フィルタ リファレンスの表示

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
なし	-

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	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 のダウンロードには、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
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役立て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。 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。 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。	http://www.cisco.com/support

関連トピック

フィルタ，（202 ページ）

WireShark の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.3SE	この機能が導入されました。

索 引

C

Cisco Discovery Protocol（CDP） 43
Cisco IOS IP SLA 106
Cisco Networking Service 20
CNS 20
Configuration Engine 18
　制約事項 18

I

ICMP エコー動作 123
　IP SLAs 123
　設定 123
Inter-Switch Link; スイッチ間リンク 148
　「ISL」を参照 148
IP SLAs 106, 107, 108, 109, 110, 111, 112, 119, 123
　ICMP エコー動作 123
　SNMP のサポート 107
　UDP ジッター動作 111, 119
　応答時間 109
　サポートされるメトリック 106
　設定 112
　ネットワーク パフォーマンスの測定 108
　複数動作のスケジューリング 110
　利点 107
IP SLA 108, 111, 113, 126
　しきい値監視 111
　設定時の注意事項 113
　モニタリング 126
　レスポンダ 108, 113
　　イネーブル化 113
　　説明 108

N

NSM 20

R

RSPAN 148, 151, 152, 153, 154, 155, 156, 157, 158, 160, 162, 163, 164, 173, 174, 177, 182
　VLAN ベース 157
　宛先ポート 158
　およびスタックの変更 162
　概要 151
　監視対象ポート 157
　受信トラフィック 155
　セッション 154, 173, 174, 177, 182
　　イネーブルにされた入力トラフィック 182
　　監視対象ポートの指定 173, 174
　　作成 173, 174
　　定義 154
　　特定の VLAN への送信元トラフィックの制限 177
　セッションの制限 148
　設定時の注意事項 164
　送信トラフィック 156
　送信元ポート 157
　デバイス スタック内 152
　デフォルト設定 163
　特性 160
　ポートのモニタリング 158
　他の機能との相互作用 160

S

SNMP 107
　および IP SLA 107
SPAN 148, 151, 154, 155, 156, 157, 158, 160, 162, 163, 164, 165, 168, 171, 184
　VLAN ベース 157
　宛先ポート 158
　およびスタックの変更 162
　概要 151
　監視対象ポート 157

SPAN *(続き)*
受信トラフィック 155
セッション 154, 164, 165, 168, 171, 184
宛先（モニタリング）ポートの削除 164
イネーブルにされた入力トラフィック 168
監視対象ポートの指定 165, 184
作成 165, 184
定義 154
特定の VLAN への送信元トラフィックの制限 171
セッションの制限 148
設定時の注意事項 164
送信トラフィック 156
送信元ポート 157
デフォルト設定 163
ポートのモニタリング 158
他の機能との相互作用 160
SPAN トラフィック 155

U

UDP ジッター、設定する 119
UDP ジッター動作、IP SLA 111, 119

V

VLAN 171, 177
RSPAN での送信元トラフィックの制限 177
SPAN での送信元トラフィックの制限 171
VLAN フィルタリングと SPAN 158

い

イベント サービス 20

お

応答時間、IP SLA で測定する 109

か

簡易ネットワーク管理プロトコル（SNMP） 43

さ

サービス 20
ネットワーキング 20
サブネットワーク アクセス プロトコル（SNAP） 43

し

しきい値監視、IP SLA 111
侵入検知システム 151
IDS アプライアンスを参照 151

す

スタックの変更、影響 162
SPAN および RSPAN 162

せ

制約事項 18
Configuration Engine 18

て

定義 20, 43
NSM 20
イベント サービス 20
デバイス スタック 44
デフォルト設定 163
RSPAN 163
SPAN 163

ね

ネットワーク パフォーマンス、IP SLA で測定する 108

ふ

複数動作のスケジューリング、IP SLA 110

ほ

ポリシー マップ 141

み

ミラーリング トラフィック、分析用の 151

も

モニタリング 126, 151
IP SLA の動作 126
プローブでの分析用のネットワーク トラフィック 151

り

リモート SPAN 153

れ

レスポンダ、IP SLA 108, 113
イネーブル化 113
説明 108

ろ

ローカル SPAN 151