



Cisco IOS XE Gibraltar 16.12.x (Catalyst 9200 スイッチ) ネットワーク管理コンフィギュレーションガイド

初版：2019年7月31日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター
0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

Autoconf の設定 1

Autoconf の前提条件 1

Autoconf の制約事項 1

Autoconf に関する情報 2

Autoconf の利点 2

アイデンティティセッション管理とテンプレート 2

Autoconf の動作 3

テンプレートを使用する利点 6

Autoconf の機能 7

Autoconf の設定方法 8

エンドデバイスへの組み込みテンプレートの適用 8

エンドデバイスへの変更された組み込みテンプレートの適用 12

ASP から Autoconf への移行 14

プラットフォーム タイプ フィルタの設定 15

クラスマップのプラットフォーム タイプ フィルタの設定 15

パラメータマップのプラットフォーム タイプ フィルタの設定 16

Autoconf の設定例 17

例：エンドデバイスへの組み込みテンプレートの適用 17

例：エンドデバイスへの変更された組み込みテンプレートの適用 17

例：ASP マクロから Autoconf への移行 18

例：プラットフォーム タイプ フィルタの設定 18

Autoconf のその他の参考資料 18

Autoconf の機能情報 19

第 2 章	Cisco プラグ アンド プレイの設定 21
	Cisco プラグ アンド プレイの設定 21

第 3 章	Cisco Discovery Protocol の設定 23
	Cisco Discovery Protocol について 23
	Cisco Discovery Protocol のデフォルト設定 23
	Cisco Discovery Protocol の概要 24
	Cisco Discovery Protocol の設定方法 24
	Cisco Discovery Protocol の特性の設定 24
	Cisco Discovery Protocol のディセーブル化 26
	Cisco Discovery Protocol の有効化 27
	インターフェイス上で Cisco Discovery Protocol をディセーブルにします。 28
	インターフェイス上での Cisco Discovery Protocol のイネーブル化 30
	Cisco Discovery Protocol のモニタリングとメンテナンス 31
	Cisco Discovery Protocol の機能情報 33

第 4 章	Cisco Discovery Protocol バイパスの設定 35
	Cisco Discovery Protocol バイパスの制約事項 35
	Cisco Discovery Protocol バイパスについて 35
	Cisco Discovery Protocol バイパスの設定方法 36
	Cisco Discovery Protocol バイパスの設定例 38
	例：Cisco Discovery Protocol バイパスの有効化 38
	Cisco Discovery Protocol ネイバーの無効化 38
	例：Cisco Discovery Protocol バイパスの無効化 38
	Cisco Discovery Protocol バイパスの機能情報 39

第 5 章	簡易ネットワーク管理プロトコルの設定 41
	SNMP の前提条件 41
	SNMP の制約事項 43
	SNMP に関する情報 44

SNMP の概要	44
SNMP マネージャ機能	44
SNMP エージェント機能	45
SNMP コミュニティストリング	45
SNMP MIB 変数アクセス	46
SNMP 通知	46
SNMP ifIndex MIB オブジェクト値	47
SNMP と Syslog、IPv6 による	47
SNMP のデフォルト設定	48
SNMP 設定時の注意事項	48
SNMP の設定方法	49
SNMP コミュニティストリング	49
SNMP グループおよびユーザの設定	50
SNMP 通知	54
エージェント コンタクトおよびロケーションの設定	54
SNMP を通して使用する TFTP サーバの制限	55
SNMP エージェントのディセーブル化	57
SNMP の例	58
SNMP ステータスのモニタリング	59
簡易ネットワーク管理プロトコルの機能の履歴と情報	60
<hr/>	
第 6 章	サービス レベル契約の設定 61
	SLA の制約事項 61
	サービスレベル契約に関する情報 61
	Cisco IOS IP サービス レベル契約 (SLA) 62
	Cisco IOS IP SLA でのネットワーク パフォーマンスの測定 63
	IP SLA レスポンダおよび IP SLA 制御プロトコル 63
	IP SLA の応答時間の計算 64
	IP SLA 動作のスケジューリング 65
	IP SLA 動作のしきい値のモニタリング 65
	UDP ジッター 66

IP SLA 動作の設定方法	67
デフォルト設定	67
設定時の注意事項	67
IP SLA レスポンダの設定	68
IP SLA ネットワーク パフォーマンス測定の実装	70
UDP ジッター動作を使用した IP サービス レベルの分析	74
ICMP エコー動作を使用した IP サービス レベルの分析	78
IP SLA 動作のモニタリング	81
IP SLA 動作のモニタリングの例	82
その他の参考資料	83
サービスレベル契約の機能情報	84

第 7 章

SPAN および RSPAN の設定	85
SPAN および RSPAN の前提条件	85
SPAN および RSPAN の制約事項	85
SPAN および RSPAN について	87
SPAN および RSPAN	88
ローカル SPAN	88
リモート SPAN	89
SPAN と RSPAN の概念および用語	90
SPAN および RSPAN と他の機能の相互作用	96
SPAN と RSPAN とデバイス スタック	97
フローベースの SPAN	98
SPAN および RSPAN のデフォルト設定	98
SPAN および RSPAN の設定	99
SPAN 設定時の注意事項	99
RSPAN 設定時の注意事項	99
FSPAN および FRSPAN 設定時の注意事項	100
SPAN および RSPAN の設定方法	100
ローカル SPAN セッションの作成	100
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	104

フィルタリングする VLAN の指定	106
RSPAN VLAN としての VLAN の設定	108
RSPAN 送信元セッションの作成	110
フィルタリングする VLAN の指定	113
RSPAN 宛先セッションの作成	115
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	117
FSPAN セッションの設定	119
FRSPAN セッションの設定	123
SPAN および RSPAN 動作のモニタリング	127
SPAN および RSPAN の設定例	127
例：ローカル SPAN の設定	127
例：RSPAN VLAN の作成	128
SPAN および RSPAN の機能の履歴と情報	130

第 8 章
パケットキャプチャの設定 131

パケットキャプチャ設定の前提条件	131
組み込みパケットキャプチャ設定の前提条件	131
組み込みパケットキャプチャの制約事項	132
パケットキャプチャについて	133
組み込みパケットキャプチャについて	133
組み込みパケットキャプチャの利点	133
パケットデータキャプチャ	133
組み込みパケットキャプチャの実装方法	134
パケットデータキャプチャの管理	134
キャプチャされたデータのモニタリングとメンテナンス	135
組み込みパケットキャプチャの設定例	136
例：パケットデータキャプチャの管理	136
例：キャプチャされたデータのモニタリングとメンテナンス	137
パケットキャプチャ設定の機能履歴と情報	139

第 9 章
Flexible NetFlow の設定 141

Flexible NetFlow の前提条件	141
Flexible Netflow に関する制約事項	142
Flexible NetFlow に関する情報	144
Flexible NetFlow の概要	144
以前の NetFlow と Flexible NetFlow の利点	145
Flexible NetFlow のコンポーネント	146
フロー レコード	146
フロー エクスポート	151
フロー モニタ	153
フロー サンプラー	155
サポートされている Flexible NetFlow フィールド	155
デフォルト設定	162
Autonomous System Number	162
Flexible NetFlow の設定方法	163
フロー レコードの作成	163
フロー エクスポートの作成	164
カスタマイズしたフロー モニタの作成	167
フローサンプラーの作成	169
インターフェイスへのフローの適用	170
VLAN 上でのブリッジ型 NetFlow の設定	172
レイヤ 2 NetFlow の設定	173
Flexible NetFlow の監視	174
Flexible NetFlow の設定例	174
例：フローの設定	174
例：IPv4 入力トラフィックのモニタリング	175
例：IPv4 出力トラフィックのモニタリング	176
Flexible NetFlow の機能情報	177



第 1 章

Autoconf の設定

ここでは、Autoconf に関する情報と Autoconf の設定方法について説明します。

- [Autoconf の前提条件](#) (1 ページ)
- [Autoconf の制約事項](#) (1 ページ)
- [Autoconf に関する情報](#) (2 ページ)
- [Autoconf の設定方法](#) (8 ページ)
- [Autoconf の設定例](#) (17 ページ)
- [Autoconf のその他の参考資料](#) (18 ページ)
- [Autoconf の機能情報](#) (19 ページ)

Autoconf の前提条件

- Autoconf を有効にする前に、Auto SmartPort (ASP) マクロ、デバイス分類子を無効にしてから、セッションモニタにアクセスします。

Autoconf の制約事項

- ASP マクロと Autoconf は、同じインターフェイスでは同時にサポートされません。Autoconf または ASP のいずれかをインターフェイスごとのレベルで無効にする必要があります。
- インターフェイス テンプレートは、ワイヤレスセッションには適用されません。
- **autoconf enable** コマンドを使用して Autoconf 機能を有効にすると、デフォルトの Autoconf サービスポリシーがすべてのインターフェイスに適用されます。**service-policy** コマンドを使用して他のサービスポリシーをグローバルに適用することはできません。別のサービスポリシーを適用するには、そのインターフェイスで Autoconf を無効にする必要があります。サービスポリシーをグローバルに適用する場合は、Autoconf 機能を無効にしてから有効にする必要があります。

- ローカル（インターフェイスレベル）ポリシーとグローバルサービスポリシーの両方が存在する場合、ローカルポリシーが優先されます。グローバルサービスポリシーは、ローカルポリシーが削除された場合にのみ有効になります。
- サービステンプレートはインターフェイスに適用できません。また、インターフェイステンプレートはサービスインスタンスに適用できません。
- インターフェイステンプレート内にネストできるサービステンプレートは1つだけです。

Autoconf に関する情報

ここでは、Autoconf について説明します。

Autoconf の利点

Autoconf 機能では、エンドデバイスとインターフェイス間のハードバインディングが可能です。Autoconf は、Cisco Smart Operations ソリューションに含まれます。Smart Operations は、LAN スイッチの導入を簡素化および改善し、組織がネットワーク上で優れた運用と拡張サービスを提供できるようにする包括的な機能セットです。

Autoconf 機能は、デバイスポートに必要な設定を自動的に適用し、インターフェイステンプレート内で設定された一連のインターフェイス設定を使用して、直接接続された各エンドデバイスの効率的なパフォーマンスを実現します。

- Autoconf は、パーサーが毎回各コマンドを解析する必要がないため、コマンドをインターフェイスに効率的に適用します。
- Autoconf 機能を使用して適用された設定は、ポートの以前の設定または後続の設定に影響を与えることなく、確実にポートから削除できます。
- Autoconf 機能は、インターフェイスおよびサービステンプレートを使用して、組み込みの設定およびユーザ定義の設定を提供します。テンプレートを使用して適用された設定は、1回の操作で一元的に更新できます。
- Autoconf 機能を使用すると、ポートおよびアクセスセッションに設定を適用できます。
- Autoconf 機能は、デバイスと接続されたエンドデバイスを直感的で自動設定可能にすることで、継続的なメンテナンスを削減します。これにより、運用コスト（OPEX）が削減され、総所有コスト（TCO）が削減されます。

アイデンティティセッション管理とテンプレート

Autoconf 機能の主な利点は、コアセッション管理機能がアプリケーション固有のロジックから分離されていることです。これにより、ポリシー決定の基準や適用されるポリシーの性質に関係なく、同じフレームワークを使用できます。

アイデンティティセッション管理インフラストラクチャでは、設定またはポリシー、またはその両方をテンプレートとして適用できます。

サービスとインターフェイスの両方のテンプレートは、設定とポリシーのコンテナとして名前が付けられます。サービステンプレートはアクセスセッションにのみ適用でき、インターフェイステンプレートはポートにのみ適用できます。サービステンプレートがアクセスセッションに適用されると、含まれている設定とポリシーはターゲットセッションにのみ適用され、同じアクセスポートでホストされている他のセッションには影響しません。同様に、インターフェイステンプレートがアクセスポートに適用されると、そのポートで交換されるすべてのトラフィックに影響します。

Autoconf機能は、一連の組み込みマップと組み込みテンプレートを使用します。組み込みテンプレートは、インターフェイス設定のベストプラクティスに基づいて設計されています。組み込みテンプレートは、カスタマイズされた設定を含めるようにユーザが変更できるため、新しいテンプレートを作成する必要がありません。

ユーザが作成したテンプレートは、ユーザ定義テンプレートと呼ばれます。これらのテンプレートはデバイスで定義でき、組み込みまたはユーザ定義のトリガーにマッピングできます。

Autoconfテンプレートと手動設定によって適用される全体的な適用設定を表示するには、**show derived-config** コマンドを使用します。**show running-config interface type number** コマンドの出力に表示されるインターフェイスコマンドは、必ずしも動作設定ではありません。Autoconf機能は、インターフェイスにテンプレートを動的に適用し、すでに適用されている競合する静的設定を上書きします。

Autoconf の動作

Autoconfは、デバイス分類子を使用して、ポートに接続されているエンドデバイスを識別します。

Autoconf機能は、Cisco Discovery Protocol、LLDP、DHCP、MACアドレスから収集したデバイス分類情報、およびデバイス分類子によって識別される組織固有識別子（OUI）を使用します。

デバイス分類子は、改善されたデバイス分類機能および精度、拡張デバイス可視性、および拡張設定管理を提供します。

グローバル コンフィギュレーション モードで **autoconf enable** コマンドを使用して Autoconf 機能を有効にすると、デバイス分類が有効になります。

デバイス検出はイベントトリガーとして機能し、適切な自動テンプレートをインターフェイスに適用します。

Autoconf機能は、3層階層に基づいています。

- ポリシーマップは、Autoconf機能を適用するためのトリガータイプを識別します。
- パラメータマップは、エンドデバイスに基づいて、適用する必要がある適切なテンプレートを識別します。
- テンプレートには、適用する設定が含まれています。

Autoconf 組み込みテンプレートおよびトリガーは、上記のタスクを自動的に実行します。

Autoconf 機能は、次の組み込みテンプレートを提供します。

- AP_INTERFACE_TEMPLATE
- DMP_INTERFACE_TEMPLATE
- IP_CAMERA_INTERFACE_TEMPLATE
- IP_PHONE_INTERFACE_TEMPLATE
- LAP_INTERFACE_TEMPLATE
- MSP_CAMERA_INTERFACE_TEMPLATE
- MSP_VC_INTERFACE_TEMPLATE
- PRINTER_INTERFACE_TEMPLATE
- ROUTER_INTERFACE_TEMPLATE
- SWITCH_INTERFACE_TEMPLATE
- TP_INTERFACE_TEMPLATE



(注) デフォルトでは、組み込みテンプレートは実行中の設定では表示されません。組み込みテンプレートは、編集した場合にのみ実行中の設定に表示されます。

選択されるテンプレートは、インターフェイスに適用されるパラメータマップ情報に基づいています。この情報は、次の基準に基づく場合があります。

- エンドデバイスタイプ
- MAC アドレス
- OUI
- プラットフォームタイプ
- ユーザ ロール
- ユーザ名

Autoconf 機能は、次の設定の 1 つの組み込みパラメータマップ (BUILTIN_DEVICE_TO_TEMPLATE) を提供します。

```
Parameter-map name: BUILTIN_DEVICE_TO_TEMPLATE
Map: 10 map device-type regex "Cisco-IP-Phone"
Action(s):
  20 interface-template IP_PHONE_INTERFACE_TEMPLATE
Map: 20 map device-type regex "Cisco-IP-Camera"
Action(s):
  20 interface-template IP_CAMERA_INTERFACE_TEMPLATE
Map: 30 map device-type regex "Cisco-DMP"
Action(s):
  20 interface-template DMP_INTERFACE_TEMPLATE
```

```

Map: 40 map oui eq "00.0f.44"
Action(s):
  20 interface-template DMP_INTERFACE_TEMPLATE
Map: 50 map oui eq "00.23.ac"
Action(s):
  20 interface-template DMP_INTERFACE_TEMPLATE
Map: 60 map device-type regex "Cisco-AIR-AP"
Action(s):
  20 interface-template AP_INTERFACE_TEMPLATE
Map: 70 map device-type regex "Cisco-AIR-LAP"
Action(s):
  20 interface-template LAP_INTERFACE_TEMPLATE
Map: 80 map device-type regex "Cisco-TelePresence"
Action(s):
  20 interface-template TP_INTERFACE_TEMPLATE
Map: 90 map device-type regex "Surveillance-Camera"
Action(s):
  10 interface-template MSP_CAMERA_INTERFACE_TEMPLATE
Map: 100 map device-type regex "Video-Conference"
Action(s):
  10 interface-template MSP_VC_INTERFACE_TEMPLATE

```



- (注) 組み込みパラメータマップの設定を表示するには、**show parameter-map type subscriber attribute-to-service All** コマンドを使用します。

Autoconf機能は、次の設定の1つの組み込みポリシーマップ (BUILTIN_AUTOCONF_POLICY) を提供します。

```

BUILTIN_AUTOCONF_POLICY
event identity-update match-all
  10 class always do-until-failure
    10 map attribute-to-service table BUILTIN_DEVICE_TO_TEMPLATE

```



- (注) 組み込みポリシーマップの設定を表示するには、**show policy-map type control subscriber BUILTIN_AUTOCONF_POLICY** コマンドを使用します。

ポリシーマップ、パラメータマップ、およびテンプレートを手動で作成することもできます。特定のユーザ情報に基づいてトリガーが作成されると、ローカル 802.1X Cisco Identity Services Engine (ISE) サーバがトリガーを認証し、操作のセキュリティを確保します。

インターフェイステンプレートは、次のいずれかの方法を使用して (インターフェイス上で) 動的にアクティブ化できます。

- **RADIUS CoA** : 認可変更 (CoA) コマンドは、1つ以上のアクセスセッションを対象としていますが、参照先テンプレートは、参照先セッションをホストしているインターフェイスに適用する必要があります。
- **RADIUS Access-Accept** (クライアントの認証または認可用) : **Access-Accept** で返される参照先インターフェイステンプレートは、認可されたアクセスセッションをホストしているポートに適用する必要があります。
- **サービステンプレート** : インターフェイステンプレートが、ローカルに定義されているサービステンプレートか AAA サーバから送信されたサービステンプレートで参照されて

いる場合、サービステンプレートが適用されるアクセスセッションをホストしているインターフェイスにインターフェイステンプレートを適用する必要があります。（ローカルに定義されたサービステンプレート内からインターフェイステンプレート参照用の新しいコマンドを追加します。）

- 加入者制御ポリシーアクション：加入者制御ポリシーの下のマッピングアクションは、フィルタのタイプに基づいてサービスまたはインターフェイステンプレート（パラメータマップで参照）または両方をアクティブ化し、以前のポリシーに関連付けられているテンプレートがある場合は削除します。
- デバイスからテンプレートパラメータへのマップ：フィルタタイプからサービスまたはインターフェイステンプレートへのマッピング、またはその両方を効率的で読み取り可能な方法で指定できる加入者パラメータマップ。

テンプレートを使用する利点

自動設定にテンプレートを使用すると、次の利点があります。

- テンプレートは、定義時に一度解析されます。これにより、テンプレートの動的な適用が非常に効率的になります。
- テンプレートは、エンドデバイスのタイプに基づいて、エンドデバイスに接続されているイーサネットインターフェイスに適用できます。
- サービステンプレートを使用すると、セッション指向機能をアクティブ化できます。一方、インターフェイステンプレートは、セッションをホストしているインターフェイスに設定を適用します。
- サービステンプレートはアクセスセッションに適用されるため、ポート上の単一のエンドポイントと交換されるトラフィックにのみ影響します。
- デバイスのスタートアップ設定と実行中の設定は、テンプレートの動的な適用によって変更されません。
- ポリシーの適用は、アクセスセッションのライフサイクルと同期されます。これは、リンクアップまたはリンクダウンを含む使用可能なすべての手法を使用して、フレームワークによって追跡されます。
- テンプレートは、1回の操作で更新できます。この操作中に、適用されたテンプレートのすべてのインスタンスも更新されます。
- テンプレートの構成コマンドは、実行中の設定には表示されません。
- 以前の設定や後続の設定に影響を与えることなく、テンプレートを削除できます。
- テンプレートの適用が確認され、障害発生時に修復アクションの同期と実行が可能になります。
- データ VLAN、Quality of Service (QoS) パラメータ、ストーム制御、および MAC ベースのポートセキュリティは、スイッチに接続されているエンドデバイスに基づいて自動的に設定されます。

- スイッチポートは、デバイスがポートから切断されたときに設定を削除することで完全にクリーンアップされます。
- インストールと設定のプロセスにおける人的エラーが減少します。

Autoconf の機能

Autoconf 機能は、デフォルトではグローバル コンフィギュレーション モードで無効になっています。Autoconf 機能をグローバル コンフィギュレーション モードで有効にすると、デフォルトでインターフェイスレベルで有効になります。組み込みテンプレート設定は、すべてのインターフェイスで検出されたエンドデバイスに基づいて適用されます。

Autoconf がグローバルレベルで有効になっている場合でも、インターフェイスレベルで手動で Autoconf を無効にするには、**access-session inherit disable autoconf** コマンドを使用します。

Autoconf をグローバルレベルで無効にすると、すべてのインターフェイスレベルの設定が無効になります。

表 1: Autoconf の機能

グローバル	インターフェイスレベル	AutoConf ステータス
無効	無効	エンドデバイスが接続されている場合、自動設定は適用されません。
有効	有効	Autoconf がグローバルレベルで有効になっている場合は、デフォルトでインターフェイスレベルでも有効です。組み込みテンプレート設定は、すべてのインターフェイスで検出されたエンドデバイスに基づいて適用されます。
有効	無効	グローバルレベルで有効です。インターフェイスレベルで無効です。Autoconf が無効になっているインターフェイスにエンドデバイスが接続されている場合、自動設定は適用されません。

Autoconf では、グローバル コンフィギュレーション モードで Autoconf スティッキ機能の **access-session interface-template sticky** コマンドを設定することで、エンドデバイスへのリンクがダウンした場合やエンドデバイスが切断された場合でも、テンプレートを保持できます。Autoconf スティッキ機能により、エンドデバイスを検出し、リンクフラップまたはデバイスが取り外されて接続し直されるたびにテンプレートを適用する必要がなくなります。

access-session interface-template sticky コマンドは、**access-session** コマンドを含む組み込みテンプレートをインターフェイスに適用するために必須です。サービスポリシーを使用してポートにインターフェイス テンプレートを適用するには **access-session interface-template sticky** コマンドを設定します。

特定のインターフェイスで Autoconf 機能を無効にするには、インターフェイス コンフィギュレーションモードで **access-session inherit disable interface-template-sticky** コマンドを使用します。

Autoconf の設定方法

ここでは、Autoconf の設定方法について説明します。

エンドデバイスへの組み込みテンプレートの適用

次のタスクでは、Cisco IP 電話などのエンドデバイスに接続されているインターフェイスに組み込みテンプレートを適用する方法を示します。

始める前に

Cisco IP 電話などのエンドデバイスがスイッチポートに接続されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。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： Device(config)# 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	autoconf enable 例： Device(config)# autoconf enable	Autoconf 機能を有効にします。
ステップ 4	end 例： Device(config)# end	グローバル コンフィギュレーションモードを終了し、特権 EXEC モードを開始します。
ステップ 5	show device classifier attached interface interface-type interface-number 例： Device# show device classifier attached interface Gi3/0/26	（任意）エンドデバイスが正しい属性を持つデバイス分類子によって分類されているかどうかを表示します。

	コマンドまたはアクション	目的
ステップ 6	show template binding target <i>interface-type interface-number</i> 例 : Device# show template binding target gi3/0/26	インターフェイス上のテンプレートを介して適用された設定を表示します。

例

次の例は、IP 電話が正しい属性を持つデバイス分類子によって分類されることを示しています。

```
Device# show device classifier attached interface GigabitEthernet 3/0/26
```

Summary:

MAC_Address	Port_Id	Profile Name	Device Name
0026.0bd9.7bbb	Gi3/0/26	Cisco-IP-Phone-7962	Cisco IP Phone 7962

次の例は、組み込みインターフェイステンプレートがインターフェイスに適用されることを示しています。

```
Device# show template binding target GigabitEthernet 3/0/26
```

```
Interface Templates
=====
Interface: Gi4/0/11
Method      Source      Template-Name
-----
dynamic     Built-in    IP_PHONE_INTERFACE_TEMPLATE
```

次の例は、インターフェイステンプレートが GigabitEthernet インターフェイス 3/0/26 に接続された IP 電話に適用された後にインターフェイス設定を確認する方法を示しています。

```
Device# show running-config interface GigabitEthernet 3/0/26
```

Building configuration...

```
Current configuration : 624 bytes
!
interface GigabitEthernet3/0/26
!
End
```

```
Device# show derived-config interface GigabitEthernet 3/0/26
```

Building configuration...

```
Derived configuration : 649 bytes
!
interface GigabitEthernet3/0/26
 switchport mode access
 switchport block unicast
 switchport port-security maximum 3
```

```

switchport port-security maximum 2 vlan access
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
switchport port-security
load-interval 30
storm-control broadcast level pps 1k
storm-control multicast level pps 2k
storm-control action trap
spanning-tree portfast
spanning-tree bpduguard enable
service-policy input AutoConf-4.0-CiscoPhone-Input-Policy
service-policy output AutoConf-4.0-Output-Policy
ip dhcp snooping limit rate 15
end

```

次の例は、Autoconfを設定した後にグローバルコンフィギュレーションを確認する方法を示しています。

```

Device# show running config
class-map match-any AutoConf-4.0-Scavenger-Queue
  match dscp cs1
  match cos 1
  match access-group name AutoConf-4.0-ACL-Scavenger
class-map match-any AutoConf-4.0-VoIP
  match dscp ef
  match cos 5
class-map match-any AutoConf-4.0-Control-Mgmt-Queue
  match cos 3
  match dscp cs7
  match dscp cs6
  match dscp cs3
  match dscp cs2
  match access-group name AutoConf-4.0-ACL-Signaling
class-map match-any AutoConf-4.0-Multimedia-Conf
  match dscp af41
  match dscp af42
  match dscp af43
class-map match-all AutoConf-4.0-Broadcast-Vid
  match dscp cs5
class-map match-any AutoConf-4.0-Bulk-Data
  match dscp af11
  match dscp af12
  match dscp af13
class-map match-all AutoConf-4.0-Realtime-Interact
  match dscp cs4
class-map match-any AutoConf-4.0-VoIP-Signal
  match dscp cs3
  match cos 3
class-map match-any AutoConf-4.0-Trans-Data-Queue
  match cos 2
  match dscp af21
  match dscp af22
  match dscp af23
  match access-group name AutoConf-4.0-ACL-Transactional-Data
class-map match-any AutoConf-4.0-VoIP-Data
  match dscp ef
  match cos 5
class-map match-any AutoConf-4.0-Multimedia-Stream
  match dscp af31
  match dscp af32
  match dscp af33
class-map match-all AutoConf-4.0-Internetwork-Ctrl

```

```
match dscp cs6
class-map match-all AutoConf-4.0-VoIP-Signal-Cos
match cos 3
class-map match-any AutoConf-4.0-Multimedia-Stream-Queue
match dscp af31
match dscp af32
match dscp af33
class-map match-all AutoConf-4.0-Network-Mgmt
match dscp cs2
class-map match-all AutoConf-4.0-VoIP-Data-Cos
match cos 5
class-map match-any AutoConf-4.0-Priority-Queue
match cos 5
match dscp ef
match dscp cs5
match dscp cs4
class-map match-any AutoConf-4.0-Bulk-Data-Queue
match cos 1
match dscp af11
match dscp af12
match dscp af13
match access-group name AutoConf-4.0-ACL-Bulk-Data
class-map match-any AutoConf-4.0-Transaction-Data
match dscp af21
match dscp af22
match dscp af23
class-map match-any AutoConf-4.0-Multimedia-Conf-Queue
match cos 4
match dscp af41
match dscp af42
match dscp af43
match access-group name AutoConf-4.0-ACL-Multimedia-Conf
class-map match-all AutoConf-4.0-Network-Ctrl
match dscp cs7
class-map match-all AutoConf-4.0-Scavenger
match dscp cs1
class-map match-any AutoConf-4.0-Signaling
match dscp cs3
match cos 3
!
!
policy-map AutoConf-4.0-Cisco-Phone-Input-Policy
class AutoConf-4.0-VoIP-Data-Cos
set dscp ef
police cir 128000 bc 8000
exceed-action set-dscp-transmit cs1
exceed-action set-cos-transmit 1
class AutoConf-4.0-VoIP-Signal-Cos
set dscp cs3
police cir 32000 bc 8000
exceed-action set-dscp-transmit cs1
exceed-action set-cos-transmit 1
class class-default
set dscp default
set cos 0
policy-map AutoConf-4.0-Output-Policy
class AutoConf-4.0-Scavenger-Queue
bandwidth remaining percent 1
class AutoConf-4.0-Priority-Queue
priority
police cir percent 30 bc 33 ms
class AutoConf-4.0-Control-Mgmt-Queue
bandwidth remaining percent 10
class AutoConf-4.0-Multimedia-Conf-Queue
```

```

bandwidth remaining percent 10
class AutoConf-4.0-Multimedia-Stream-Queue
bandwidth remaining percent 10
class AutoConf-4.0-Trans-Data-Queue
bandwidth remaining percent 10
    dbl
class AutoConf-4.0-Bulk-Data-Queue
bandwidth remaining percent 4
    dbl
class class-default
bandwidth remaining percent 25
    dbl
policy-map AutoConf-DMP
class class-default
    set dscp cs2
policy-map AutoConf-IPVSC
class class-default
    set cos dscp table AutoConf-DscpToCos
policy-map AutoConf-4.0-Input-Policy
class AutoConf-4.0-VoIP
class AutoConf-4.0-Broadcast-Vid
class AutoConf-4.0-Realtime-Interact
class AutoConf-4.0-Network-Ctrl
class AutoConf-4.0-Internetwork-Ctrl
class AutoConf-4.0-Signaling
class AutoConf-4.0-Network-Mgmt
class AutoConf-4.0-Multimedia-Conf
class AutoConf-4.0-Multimedia-Stream
class AutoConf-4.0-Transaction-Data
class AutoConf-4.0-Bulk-Data
class AutoConf-4.0-Scavenger

```

エンドデバイスへの変更された組み込みテンプレートの適用

次のタスクは、複数のワイヤレスアクセスポイントと IP カメラがスイッチに接続されている場合に、組み込みテンプレートを変更する方法を示しています。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。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： Device(config)# 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	template <i>template-name</i> 例： Device(config)# template AP_INTERFACE_TEMPLATE	組み込みテンプレートのテンプレート コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	switchport access vlan <i>vlan-id</i> 例： Device(config-template)# switchport access vlan 20	インターフェイスがアクセス モードのときに VLAN を設定します。
ステップ 5	description 説明 例： Device(config-template)# description modifiedAP	組み込みテンプレートの説明を変更します。
ステップ 6	exit 例： Device(config-template)# exit	テンプレート 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 モードを開始します。
ステップ 7	autoconf enable 例： Device(config)# autoconf enable	Autoconf 機能を有効にします。
ステップ 8	end 例： Device(config)# end	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 9	show template interface binding all 例： Device# show template interface binding all	テンプレートがインターフェイスに適用されているかどうかを表示します。

例

次の例は、IP カメラとアクセスポイントが正しい属性を持つデバイス分類子によって分類されることを示しています。

```
Device# show device classifier attached detail
```

```
DC default profile file version supported = 1
```

```
Detail:
```

MAC_Address	Port_Id	Cert	Parent	Proto	ProfileType	Profile Name
001d.a1ef.23a8	Gi1/0/7	30	3	C	M	Cisco-AIR-AP-1130
cisco AIR-AP1131AG-A-K9						
001e.7a26.eb05	Gi1/0/30	70	2	C	M	Cisco-IP-Camera
Cisco IP Camera						

次の例は、組み込みインターフェイステンプレートがインターフェイスに適用されることを示しています。

```
Device# show template interface binding all
```

Template-Name	Source	Method	Interface
IP_CAMERA_INTERFACE_TEMPLATE	Built-in	dynamic	Gi1/0/30
AP_INTERFACE_TEMPLATE	Modified-Built-in	dynamic	Gi1/0/7

ASP から Autoconf への移行

始める前に

show running-config | include macro auto global コマンドを使用して、AutoSmart ポート (ASP) マクロが実行されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。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： Device# 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 macro auto global processing 例： Device(config)# no macro auto global processing	グローバルレベルで ASP を無効にします。
ステップ 4	exit 例： Device(config)# exit	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	clear macro auto configuration all 例： Device# clear macro auto configuration all	すべてのインターフェイスのマクロ設定をクリアします。
ステップ 6	configure terminal 例： Device# 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	autoconf enable 例：	Autoconf 機能を有効にします。

	コマンドまたはアクション	目的
	<code>Device(config)# autoconf enable</code>	
ステップ 8	end 例： <code>Device(config)# end</code>	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

プラットフォーム タイプ フィルタの設定

次のタスクでは、クラスマップおよびパラメータマップのプラットフォーム タイプ フィルタを設定する方法を示します。

クラスマップのプラットフォーム タイプ フィルタの設定

制御クラスは、制御ポリシーのアクションが実行される条件を定義します。制御ポリシーのアクションを実行するためには、すべての条件を評価する必要があるか、いずれかの条件を評価する必要があるか、または評価しないかを定義する必要があります。プラットフォームタイプは、制御ポリシーで指定されたプラットフォーム名に基づいて評価されます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： <code>Device> enable</code>	特権 EXEC モードを有効にします。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： <code>Device# configure terminal</code>	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	class-map type control subscriber {match-all match-any match-none} <i>control-class-name</i> 例： <code>Device (config)# class-map type control subscriber match-all DOT1X_NO_AGENT</code>	制御クラスを作成し、制御クラスマップ フィルタ モードを開始します。 <ul style="list-style-type: none"> • match-all : 制御クラスのすべての条件に一致する必要があります。 • match-any : 制御クラスの少なくとも 1 つの条件に一致する必要があります。 • match-none : 制御クラスのどの条件にも一致しない必要があります。

	コマンドまたはアクション	目的
ステップ 4	match platform-type <i>platform-name</i> 例： Device (config-filter-control-classmap) # match platform-type C3850	指定されたプラットフォームタイプに基づいて制御クラスを評価する条件を作成します。
ステップ 5	end 例： Device (config-filter-control-classmap) # end	制御クラスマップフィルタモードを終了し、特権 EXEC モードに戻ります。
ステップ 6	show class-map type control subscriber { all name control-class-name } 例： Device# show class-map type control subscriber all	(任意) すべてのクラスマップまたは特定のクラスマップの制御ポリシーに関する情報を表示します。

パラメータマップのプラットフォームタイプフィルタの設定

パラメータマップを使用することを推奨します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。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： Device# 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	parameter-map type subscriber attribute-to-service <i>parameter-map-name</i> 例： Device (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、パラメータマップ フィルタ モードを開始します。
ステップ 4	map-index map platform-type {{ eq not-eq regex } <i>filter-name</i> } 例： Device (config-parameter-map-filter) # 10 map platform-type eq C9xxx	プラットフォームタイプにパラメータマップ属性フィルタ基準を指定します。

	コマンドまたはアクション	目的
ステップ 5	end 例 : Device (config-parameter-map-filter-submode) # end	パラメータマップ フィルタ モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	show parameter-map type subscriber attribute-to-service {all name parameter-map-name} 例 : Device# show parameter-map type subscriber attribute-to-service	(任意) パラメータマップ属性を表示します。

Autoconf の設定例

次のセクションに Autoconf 機能の設定例を示します。

例：エンドデバイスへの組み込みテンプレートの適用

次に、インターフェイスに接続されたエンドデバイスに組み込みテンプレートを適用する例を示します。

```
Device> enable
Device(config)# configure terminal
Device(config)# autoconf enable
Device(config)# end
Device# show device classifier attached interface Gi3/0/26
Device# show template binding target GigabitEthernet 3/0/26
```

例：エンドデバイスへの変更された組み込みテンプレートの適用

次に、変更された組み込みテンプレートをエンドデバイスに適用し、設定を確認する例を示します。

```
Device> enable
Device(config)# configure terminal
Device(config)# template AP_INTERFACE_TEMPLATE
Device(config-template)# switchport access vlan 20
Device(config-template)# description modifiedAP
Device(config-template)# exit
Device(config)# autoconf enable
Device(config)# end
Device# show template interface binding all
```

例 : ASP マクロから Autoconf への移行

次に、ASP から Autoconf に移行する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# no macro auto global processing
Device(config)# exit
Device# clear macro auto configuration all
Device# configure terminal
Device(config)# autoconf enable
Device(config)# end
```

例 : プラットフォームタイプフィルタの設定

次の例では、クラスマップのプラットフォームタイプフィルタを設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# class-map type control subscriber match-all DOT1X_NO_AGENT
Device(config-filter-control-classmap)# match platform-type C9xxx
Device(config-filter-control-classmap)# end
Device#
```

次の例では、パラメータマップのプラットフォームタイプフィルタを設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type subscriber attribute-to-service Aironet-Policy-para
Device(config-parameter-map-filter)# 10 map platform-type eq C9xxx
Device(config-parameter-map-filter-submode)# end
Device#
```

Autoconf のその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco identity-based networking services コマンド	『Cisco IOS Identity-Based Networking Services Command Reference』
インターフェイス テンプレート	『Identity-Based Networking Services Configuration Guide』 の「Interface Templates」の章。

標準および RFC

標準/RFC	タイトル
IEEE 802.1X	「Port Based Network Access Control」

シスコのテクニカル サポート

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

Autoconf の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 2: Autoconf の機能情報

機能名	リリース	機能情報
[Autoconf]	Cisco IOS XE Fuji 16.9.1	この機能が導入されました。 autoconf enable 、 map attribute-to-service (autoconf) 、 map device-type (service-template) 、 parameter-map type subscriber (service-template) 、 show parameter-map type subscriber attribute-to-service all 、 show template interface の各コマンドが追加または変更されました。
AutoConfによるデバイス設定をシスコスイッチのPIDまで細分化	Cisco IOS XE Gibraltar 16.12.1	クラスマップとパラメータマップの設定用に platform type フィルタオプションが追加されました。



第 2 章

Cisco プラグ アンド プレイの設定

- [Cisco プラグ アンド プレイの設定 \(21 ページ\)](#)

Cisco プラグ アンド プレイの設定

プラグ アンド プレイの設定方法については、次を参照してください。

- [Cisco プラグ アンド プレイ機能ガイド](#)
- [Configuration Guide for Cisco Network Plug and Play on APIC-EM](#)



第 3 章

Cisco Discovery Protocol の設定

Cisco Discovery Protocol は、シスコデバイス上で動作し、ネットワーキングアプリケーションが直接接続された付近のデバイスに関して学習できるようにする、メディア独立型かつネットワーク独立型のレイヤ2プロトコルです。このプロトコルによってシスコデバイスが検出されてその設定状態が特定され、異なるネットワーク層プロトコルを使用するシステムが相互に学習できるようになることで、デバイスの管理が容易になります。

このモジュールでは、Cisco Discovery Protocol バージョン 2 とその SNMP での動作について説明します。

- [Cisco Discovery Protocol について \(23 ページ\)](#)
- [Cisco Discovery Protocol の設定方法 \(24 ページ\)](#)
- [Cisco Discovery Protocol のモニタリングとメンテナンス \(31 ページ\)](#)
- [Cisco Discovery Protocol の機能情報 \(33 ページ\)](#)

Cisco Discovery Protocol について

ここでは、Cisco Discovery Protocol について説明します

Cisco Discovery Protocol のデフォルト設定

次の表に、Cisco Discovery Protocol のデフォルト設定を示します。

機能	デフォルト設定
Cisco Discovery Protocol グローバル状態	イネーブル
Cisco Discovery Protocol インターフェイス状態	イネーブル
Cisco Discovery Protocol タイマー (パケット更新頻度)	60 秒
Cisco Discovery Protocol 保持時間 (廃棄前)	180 秒
Cisco Discovery Protocol バージョン 2 アドバタイズメント	イネーブル

Cisco Discovery Protocol の概要

Cisco Discovery Protocol 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、既知のデバイスのネイバーであるシスコデバイスを検出することができます。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、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。

Cisco Discovery Protocol 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。Cisco Discovery Protocol 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。

Cisco Discovery Protocol 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 Cisco Discovery Protocol 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。

Cisco Discovery Protocol はデバイス上で 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。デバイスは Cisco Discovery Protocol を使用してクラスタ候補を検出し、クラスタメンバ、およびコマンドデバイスから最大 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。

次の内容は、デバイスおよび接続されたエンドポイントデバイスに当てはまります。

- Cisco Discovery Protocol は、デバイスと直接通信する接続されたエンドポイントを識別します。
- ネイバーデバイスのレポートが重複しないように、1 つの有線デバイスだけがロケーション情報をレポートします。
- 有線デバイスとエンドポイントは、ロケーションの送信と受信の両方を行います。

Cisco Discovery Protocol の設定方法

ここでは、Cisco Discovery Protocol の設定方法について説明します。

Cisco Discovery Protocol の特性の設定

次の Cisco Discovery Protocol の特性を設定できます。

- Cisco Discovery Protocol アップデートの頻度
- 破棄するまで情報を保持する時間の長さ

- バージョン 2 アドバタイズメント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。

次の手順に従って、Cisco Discovery Protocol の特性を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configureterminal 例： Device# configure terminal	
ステップ 3	cdp timer seconds 例： Device(config)# cdp timer 20	(任意) Cisco Discovery Protocol 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： Device(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： Device(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 Cisco Discovery Protocol 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： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 7	show running-config 例：	入力を確認します。

	コマンドまたはアクション	目的
	Device# <code>show running-config</code>	
ステップ 8	copy running-config startup-config 例： Device# <code>copy running-config startup-config</code>	(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。

次のタスク

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

Cisco Discovery Protocol のディセーブル化

Cisco Discovery Protocol はデフォルトでイネーブルになっています。



- (注) デバイスクラスタと他のシスコデバイス (Cisco IP Phone など) は、Cisco Discovery Protocol メッセージを定期的に交換します。Cisco Discovery Protocol 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。

Cisco Discovery Protocol 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

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> <code>enable</code>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none">パスワードを入力します (要求された場合)。
ステップ 2	configureterminal 例： Device# <code>configure terminal</code>	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： Device(config)# <code>no cdp run</code>	Cisco Discovery Protocol を無効にします。

	コマンドまたはアクション	目的
ステップ 4	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 6	copy running-config startup-config 例 : Device# 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。

次のタスク

Cisco Discovery Protocol を使用するには、再度有効にする必要があります。

Cisco Discovery Protocol の有効化

Cisco Discovery Protocol はデフォルトでイネーブルになっています。



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

ディセーブルになっている Cisco Discovery Protocol をイネーブルにするには、次の手順を実行します。

始める前に

Cisco Discovery Protocol がディセーブルになっていないと、イネーブルにはできません。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 :	特権 EXEC モードを有効にします。

■ インターフェイス上で Cisco Discovery Protocol をディセーブルにします。

	コマンドまたはアクション	目的
	Device> enable	<ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configureterminal 例： Device# 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： Device(config)# cdp run	Cisco Discovery Protocol がディセーブルになっている場合にイネーブルにします。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	show running-config 例： Device# show running-config	入力を確認します。
ステップ 6	copy running-config startup-config 例： Device# 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。

次のタスク

Cisco Discovery Protocol がイネーブルになっていることを表示するには、**show run all** コマンドを使用します。**show run** を入力しただけでは、Cisco Discovery Protocol がイネーブルになっていることが表示されない場合があります。

インターフェイス上で Cisco Discovery Protocol をディセーブルにします。

Cisco Discovery Protocol は、Cisco Discovery Protocol 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でデフォルトで有効になっています。



- (注) デバイスクラスタと他のシスコデバイス (Cisco IP Phone など) は、Cisco Discovery Protocol メッセージを定期的に交換します。Cisco Discovery Protocol 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。



- (注) Discovery Protocol バイパスはサポートされていないため、ポートが `err-disabled` ステートになる場合があります。

ポートで Cisco Discovery Protocol をディセーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configureterminal 例 : Device# 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 : Device(config)# interface gigabitethernet 1/0/1	Cisco Discovery Protocol 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 : Device(config-if)# no cdp enable	ステップ 3 で指定したインターフェイス上で Cisco Discovery Protocol をディセーブルにします。
ステップ 5	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例 : Device# 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： Device# 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。

インターフェイス上での Cisco Discovery Protocol のイネーブル化

Cisco Discovery Protocol は、Cisco Discovery Protocol 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でデフォルトで有効になっています。



- (注) デバイスクラスタと他のシスコデバイス (Cisco IP Phone など) は、Cisco Discovery Protocol メッセージを定期的に交換します。Cisco Discovery Protocol 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。



- (注) Discovery Protocol バイパスはサポートされていないため、ポートが `err-disabled` ステートになる場合があります。

ポートでディセーブルになっている Cisco Discovery Protocol をイネーブルにするには、次の手順を実行します。

始める前に

Cisco Discovery Protocol をイネーブルにしようとしているポートでは、Cisco Discovery Protocol がディセーブルになっている必要があります。そうでないと、イネーブルにできません。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configureterminal 例： Device# 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	interface interface-id 例： Device(config)# interface gigabitethernet1/0/1	Cisco Discovery Protocol 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： Device(config-if)# cdp enable	ディセーブルになっているインターフェイスで Cisco Discovery Protocol をイネーブルにします。
ステップ 5	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例： Device# show running-config	入力を確認します。
ステップ 7	copy running-config startup-config 例： Device# 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。

Cisco Discovery Protocol のモニタリングとメンテナンス

表 3: Cisco Discovery Protocol 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	ネイバーに関する情報の Cisco Discovery Protocol 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。

コマンド	説明
show cdp entry <i>entry-name</i> [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 Cisco Discovery Protocol 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 [<i>interface-id</i>]	Cisco Discovery Protocol がイネーブルになっているインターフェイスに関する情報を表示します。 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 [<i>interface-id</i>] [<i>detail</i>]	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	Cisco Discovery Protocol カウンタ（送信済み/受信済みパケット数とチェックサムエラー数を含む）を表示します。
show ap cdp neighbors	アクセスポイントの Cisco Discovery Protocol ネイバーに関する情報を表示します。
show ap cdp neighbors detail	アクセスポイントの Cisco Discovery Protocol ネイバーに関する詳細情報を表示します。
show ap name <i>ap-name</i> cdp neighbors	アクセスポイントの Cisco Discovery Protocol 情報を表示します。
show ap name <i>ap-name</i> cdp neighbors detail	Cisco Discovery Protocol を使用している特定のアクセスポイントのネイバーに関する詳細情報を表示します。

Cisco Discovery Protocol の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレーンで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 4: Cisco Discovery Protocol の機能情報

リリース	機能情報
Cisco IOS XE Fuji 16.9.2	この機能が導入されました。



第 4 章

Cisco Discovery Protocol バイパスの設定

Cisco Discovery Protocol バイパス モードでは、Cisco Discovery Protocol パケットを受け取り、そのまま送信します。受信パケットは処理されません。パケットは生成されません。このモードでは、Bump-In-The-Wire (BITW) 動作が Cisco Discovery Protocol パケットに適用されます。これは Cisco Discovery Protocol のサポートがない場合に等しい下位互換モードです。

- [Cisco Discovery Protocol バイパスの制約事項 \(35 ページ\)](#)
- [Cisco Discovery Protocol バイパスについて \(35 ページ\)](#)
- [Cisco Discovery Protocol バイパスの設定方法 \(36 ページ\)](#)
- [Cisco Discovery Protocol バイパスの設定例 \(38 ページ\)](#)
- [Cisco Discovery Protocol バイパスの機能情報 \(39 ページ\)](#)

Cisco Discovery Protocol バイパスの制約事項

Cisco Discovery Protocol バイパスは、スイッチポート上の標準 ACL をサポートしていません。

Cisco Discovery Protocol バイパスについて

Cisco IP Phone が音声 VLAN とシングルホスト モードで設定されたポートに接続されている電話機は、Cisco Discovery Protocol バイパス機能によりネットワークに暗黙的に許可されます。Cisco Discovery Protocol メッセージで適切な TLV (Type Length Value) を送信する電話機 (またはデバイス) が音声 VLAN へのアクセスを許可されます。

Cisco Discovery Protocol バイパス モードでは、Cisco Discovery Protocol パケットを受け取り、そのまま送信します。受信パケットは処理されません。パケットは生成されません。このモードでは、Bump-In-The-Wire (BITW) 動作が Cisco Discovery Protocol パケットに適用されます。これは Cisco Discovery Protocol のサポートがない場合に等しい下位互換モードです。

Cisco Discovery Protocol バイパス モードでは、認証セッションが IP フォンのシングルホストモードとマルチポストモードで確立されます。ただし、インターフェイスポートの音声 VLAN と 802.1x が有効になっている場合は、ホストモードがシングルホストモードまたはマルチポストモードに設定されているときに Cisco Discovery Protocol バイパスが有効になります。

Cisco Discovery Protocol バイパス機能の代わりに、より優れたアクセス制御、可視性、および許可を提供する Multi-Domain Authentication (MDA) 機能を使用できます。



(注) デフォルトでは、ホストモードはレガシーモードの場合はシングルモード、エッジモードの場合はマルチ認証に設定されます。

2番目のポートの切断の場合の Cisco Discovery Protocol の機能拡張：電話機の背後からプラグが抜かれホストが切断されたときに Cisco IP Phone は Cisco Discovery Protocol メッセージをスイッチに送信できます。ホストが直接接続され、リンクダウンイベントを検出した場合と同様に、スイッチは間接的に接続されたホストの認証済みセッションをクリアできます。これは最新の IP 電話機でサポートされています。

Cisco Discovery Protocol バイパスは、サードパーティ製の電話機ではサポートされていません。Cisco Discovery Protocol バイパスが動作するのはシスコ製の電話機に限られます。

Cisco Discovery Protocol バイパスの設定方法

Cisco Discovery Protocol バイパスを有効にするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： > enable	特権 EXEC モードを有効にします。 • 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： # 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： (config)# interface GigabitEthernet1/0/12	物理ポートを指定し、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。 • 指定できるインターフェイスは、物理ポートです。
ステップ 4	switchport mode access 例： (config-if)# switchport mode access	インターフェイスがアクセスモードになるように指定します。

	コマンドまたはアクション	目的
ステップ 5	switchport access vlan <i>vlan id</i> 例 : <pre>(config-if)# switchport access vlan 10</pre>	同じ VLAN 内のすべてのポートをスタティック アクセス ポートとして割り当てます。 <ul style="list-style-type: none"> • ポートをスタティックアクセスポートとして設定する場合は、ポートを1つのVLANにのみ割り当ててください。指定できる範囲は1～4094です。
ステップ 6	switchport voice vlan <i>vlan-id</i> 例 : <pre>(config-if)# switchport voice vlan 3</pre>	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、Cisco IP Phone に指示します。デフォルトでは、Cisco IP Phone は 802.1Q プライオリティ 5 を使用して音声トラフィックを転送します。 有効な VLAN ID の範囲は、拡張ソフトウェア イメージ (EI) がインストールされている場合は 1～4094 で、標準ソフトウェア イメージ (SI) がインストールされている場合は 1～1001 です。先行ゼロは入力しないでください。
ステップ 7	authentication port-control auto 例 : <pre>(config-if)# authentication port-control auto</pre>	ポートでの 802.1x 認証をイネーブルにします。
ステップ 8	authentication host-mode {single-host multi-host} 例 : <pre>(config-if)# authentication host-mode single multi-host</pre>	キーワードにより、次のものが許可されます。 <ul style="list-style-type: none"> • single-host : IEEE 802.1X 認可ポートの単一ホスト (クライアント) が許可されます。 • multi-host : 単一ホストの認証後に 802.1X 認可ポートの複数ホストが許可されます。
ステップ 9	dot1x pae authenticator 例 : <pre>(config-if)# dot1x pae authenticator</pre>	ポート上でデフォルト設定の 802.1X 認証をイネーブルにします。

Cisco Discovery Protocol バイパスの設定例

例 : Cisco Discovery Protocol バイパスの有効化

「Authentication port-control auto」が dotx1 または MAB で設定されるか、または音声 VLAN が シングル/マルチポストモードとともにインターフェイスに設定されている場合、Cisco Discovery Protocol バイパスがデフォルトで有効になります。

次に、認証で MAB を使用している場合の Cisco Discovery Protocol バイパスの設定例を示します。

```
(config)# interface GigabitEthernet1/0/12
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# switchport voice vlan 3
(config-if)# authentication port-control auto
(config-if)# mab
```

Cisco Discovery Protocol ネイバーの無効化

次に、Cisco Discovery Protocol ネイバーを表示する設定例を示します。

```
# show cdp neighbors g1/0/37 detail
Device ID: SEP24B657B038DF
Entry address(es):
Platform: Cisco IP Phone 9971, Capabilities: Host Phone Two-port Mac Relay
Interface: GigabitEthernet1/0/37, Port ID (outgoing port): Port 1
Holdtime : 157 sec
Second Port Status: Down <<<<<<<<<<
Version :
sip9971.9-1-1SR1
advertisement version: 2
Duplex: full
Power drawn: 12.804 Watts
Power request id: 57146, Power management id: 4
Power request levels are:12804 0 0 0 0
Total cdp entries displayed : 1
```

例 : Cisco Discovery Protocol バイパスの無効化

Cisco Discovery Protocol バイパスを無効にするには、インターフェイスから「Authentication port-control auto」を削除する必要があります。

Cisco Discovery Protocol バイパスの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 5: Cisco Discovery Protocol バイパスの機能情報

リリース	機能情報
Cisco IOS XE Fuji 16.9.2	この機能が導入されました。



第 5 章

簡易ネットワーク管理プロトコルの設定

- [SNMP の前提条件](#) (41 ページ)
- [SNMP の制約事項](#) (43 ページ)
- [SNMP に関する情報](#) (44 ページ)
- [SNMP の設定方法](#) (49 ページ)
- [SNMP の例](#) (58 ページ)
- [SNMP ステータスのモニタリング](#) (59 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](#) (60 ページ)

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 6: 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	未対応	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	未対応	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	未対応	ユーザ名の照合を使用して認証します。

モデル	レベル	認証	暗号化	結果
SNMPv3	authNoPriv	Message Digest 5 (MD5) または Secure Hash Algorithm (SHA)	なし	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。
SNMPv3	authPriv	MD5 または SHA	データ暗号規格 (DES) または Advanced Encryption Standard (AES)	<p>HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。</p> <p>次の暗号化アルゴリズムで、User-based Security Model (USM) を指定できます。</p> <ul style="list-style-type: none"> • CBC-DES (DES-56) 規格に基づく認証に加えた DES 56 ビット暗号化 • 3DES 168 ビット暗号化 • AES 128 ビット暗号化、192 ビット暗号化、または 256 ビット暗号化

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

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。

SNMPv3 認証は、次のシナリオではサポートされません。

- スイッチ優先順位の変更後にスタックリロードが発生した場合。
- 低い MAC アドレスを持つデバイスがスタックに追加された場合、スタック内のすべてのスイッチの優先順位が同じであれば、そのデバイスがアクティブスイッチとして選択されます。

SNMPv3 認証の失敗を回避するには、SNMPv3 ユーザを設定する前に、デバイスで SNMP engineID を手動で設定する必要があります。これにより、ユーザは engineID に関連付けられているためデバイスを管理できます。

SNMP に関する情報

ここでは、SNMP の概要について説明します。

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。エージェントと MIB はネットワークデバイス上に存在します。デバイスに SNMP を設定するには、マネージャとエージェントの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 7: 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。 ¹

動作	説明
get-bulk-request ²	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。

¹ 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。

² get-bulk コマンドを使用できるのは、SNMPv2 以上に限られます。



(注) パフォーマンスに関連する問題を回避するために、SNMP マネージャで **ciscoFlashFileDate** MIB オブジェクトをクエリから除外することを推奨します。これは、**ciscoFlashFileDate** オブジェクトが MIB で公開されていても、製品ではサポートされていないためです。

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、スパンニングツリートポロジが変更された場合、認証に失敗した場合などがあります。

SNMP コミュニティ スtring

SNMP コミュニティ スtring は、MIB オブジェクトへのアクセスを認証し、組み込みパスワードとして機能します。NMS がデバイスにアクセスするには、NMS 上のコミュニティ スtring 定義がデバイス上の 3 つのコミュニティ スtring 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tring の属性は、次のいずれかです。

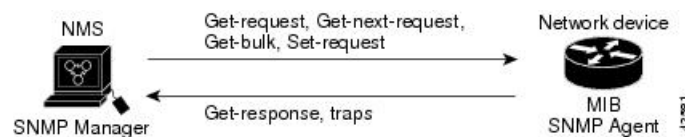
- 読み取り専用 (RO) : コミュニティストリングを除き MIB 内のすべてのオブジェクトに、許可された管理ステーションに対する読み取りアクセス権を与えますが、書き込みアクセスは許可しません。
- 読み取り-書き込み (RW) : MIB 内のすべてのオブジェクトに、許可された管理ステーションに対する読み取りおよび書き込みアクセス権を与えますが、コミュニティストリングへのアクセスは許可しません。
- クラスタを作成すると、コマンドデバイスがメンバデバイスと SNMP アプリケーション間のメッセージ交換を管理します。Network Assistant ソフトウェアは、コマンドデバイス上で最初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

SNMP MIB 変数アクセス

NMS の例として、Cisco Prime Infrastructure ネットワーク管理ソフトウェアがあります。Cisco Prime Infrastructure ソフトウェアは、デバイス 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 1: 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、デバイスから 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を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、デバイス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デバイスのメモリ上のトラフィックが問題になる場合で、なおかつ通知が不要な場合は、トラップを使用してください。

SNMP ifIndex MIB オブジェクト値

SNMP エージェントの IF-MIB モジュールがリポート後すぐに起動されます。さまざまな物理インターフェイス ドライバが IF-MIB モジュールの登録を初期化されているように、「インデックス番号をください」と示します。IF-MIB モジュールが先着順で使用可能な次の ifIndex 番号を割り当てます。つまり、1つのリポートから他のリポートへのドライバの初期化順序のマイナーな違いが、同じ物理インターフェイスにリポートを行う以前のものとは別のインデックス番号を取得する可能性があるということです (インデックス持続が有効化されていない限り)。

SNMP と Syslog、IPv6 による

IPv4 と IPv6 の両方をサポートするには、IPv6 のネットワーク管理で IPv4 および IPv6 のトランスポートが必要になります。IPv6 による Syslog は、このトランスポートのアドレス データタイプをサポートします。

Simple Network Management Protocol (SNMP) と IPv6 を介した syslog は、次の機能を提供します。

- IPv4 と IPv6 両方のサポート
- SNMP に対する IPv6 トランスポート、および SNMP 変更による IPv6 ホストのトラップのサポート
- IPv6 アドレス指定をサポートするための SNMP および Syslog に関連する MIB
- IPv6 ホストをトラップ レシーバとして設定

IPv6に関連するサポートでは、SNMPは既存のIPトランスポートマッピングを変更して、IPv4とIPv6を同時にサポートします。次のSNMP動作は、IPv6トランスポート管理をサポートします。

- デフォルト設定のユーザデータグラムプロトコル (UDP) SNMPソケットを開く
- `SR_IPV6_TRANSPORT` と呼ばれる新しいトランスポートメカニズムを提供
- IPv6トランスポートによるSNMP通知の送信
- IPv6トランスポートのSNMP名のアクセスリストのサポート
- IPv6トランスポートを使用したSNMPプロキシ転送のサポート
- SNMPマネージャ機能とIPv6トランスポートの連動確認

設定手順を含む、IPv6によるSNMPについては、Cisco.comで『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

設定手順を含む、IPv6によるSyslogについては、Cisco.comで『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

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 ³
SNMP トラップ レシーバ	未設定
SNMP トラップ	TCP接続のトラップ (tty) 以外は、イネーブルではありません。
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。

³ これは、デバイスが起動し、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

デバイスが起動し、デバイス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 エージェントは有効になります。

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 グループを設定するときには、次の注意事項に従ってください。

- SNMP グループを設定するときは、通知ビューを指定しません。**snmp-server host** グローバル コンフィギュレーション コマンドがユーザの通知ビューを自動生成し、そのユーザに関連付けられてい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、デバイスは **auth** (**authNoPriv**) および **priv** (**authPriv**) の認証レベルの情報を送信しません。
- SNMP エンジン ID の値を変更すると、重大な影響が生じます。(コマンドラインで入力された) ユーザのパスワードは、パスワードおよびローカル エンジン ID に基づいて、MD5 または SHA セキュリティダイジェストに変換されます。コマンドラインのパスワードは、RFC 2274 の規定に従って廃棄されます。このようにパスワードが廃棄されるため、エンジン ID 値を変更した場合は、SNMPv3 ユーザのセキュリティダイジェストが無効となり、**snmp-server user username** グローバル コンフィギュレーション コマンドを使用して、SNMP ユーザを再設定する必要があります。エンジン ID を変更した場合は、同様の制限によってコミュニティ スtring も再設定する必要があります。

SNMP の設定方法

ここでは、SNMP の設定方法について説明します。

SNMP コミュニティ スtring

SNMP コミュニティ スtring は、MIB オブジェクトへのアクセスを認証し、組み込みパスワードとして機能します。NMS がデバイスにアクセスするには、NMS 上のコミュニティ スtring 定義がデバイス上の 3 つのコミュニティ スtring 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tring 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tring 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 String へのアクセスは許可しません。
- クラスタを作成すると、コマンドデバイスがメンバデバイスと 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、コマンドデバイス上で最初に設定された RW および RO コミュニティ String にメンバデバイス番号 (@esN、N はデバイス番号) を追加し、これらの String をメンバデバイスに伝播します。

SNMP グループおよびユーザの設定

デバイス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。

デバイス上の 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

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • 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 : Device# 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 : Device(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。 • <i>engineid-string</i> は、SNMP のコピー名を指定する 24 文字の ID String 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、

	コマンドまたはアクション	目的
		<p>12340000000000000000000000000000 のエンジン ID を設定します。</p> <ul style="list-style-type: none"> • 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 <i>ip-address</i> 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。
<p>ステップ 4</p>	<p>snmp-server group <i>group-name</i> {v1 v2c v3 {auth noauth priv}} [read readview] [write writeview] [notify notifyview] [access access-list]</p> <p>例 :</p> <pre>Device(config)# snmp-server group public v2c access lmnop</pre>	<p>リモート デバイス上で新しい SNMP グループを設定します。</p> <p><i>group-name</i> には、グループの名前を指定します。</p> <p>次のいずれかのセキュリティ モデルを指定します。</p> <ul style="list-style-type: none"> • v1 は、最も安全性の低いセキュリティ モデルです。 • v2c は、2 番目に安全性の低いセキュリティ モデルです。標準の 2 倍の幅で情報および整数を送送できます。 • v3最も安全な場合には、次の認証レベルの1つを選択する必要があります。 <p>auth : Message Digest 5 (MD5) およびセキュア ハッシュ アルゴリズム (SHA) によるパケット認証を可能にします。</p> <p>noauth : noAuthNoPriv セキュリティ レベルを可能にします。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。</p> <p>priv : データ暗号規格 (DES) によるパケット暗号化 (プライバシーともいう) を可能にします。</p> <p>(任意) read readview とともに、エージェントの内容を表示できるビュー名を</p>

	コマンドまたはアクション	目的
		<p>表す文字列（64 文字以内）を入力します。</p> <p>（任意） write writeview とともに、データを入力し、エージェントの内容を表示できるビュー名を表す文字列（64 文字以内）を入力します。</p> <p>（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名を表す文字列（64 文字以内）を入力します。</p> <p>（任意） access access-list とともに、アクセスリスト名の文字列（64 文字以内）を入力します。</p>
ステップ 5	<p>snmp-server user <i>username group-name</i> {remote <i>host</i> [udp-port <i>port</i>] } {v1 [access <i>access-list</i>] v2c [access <i>access-list</i>] v3 [encrypted] [access <i>access-list</i>] [auth { md5 sha } <i>auth-password</i>] } [priv { des 3des aes { 128 192 256 } } <i>priv-password</i>]</p> <p>例 :</p> <pre>Device(config)# snmp-server user Pat public v2c</pre>	<p>SNMP グループに対して新規ユーザを追加します。</p> <p><i>username</i> は、エージェントに接続するホスト上のユーザ名です。</p> <p><i>group-name</i> は、ユーザが関連付けられているグループの名前です。</p> <p>remote を入力して、ユーザが所属するリモート SNMP エンティティおよびそのエンティティのホスト名または IP アドレスとともに、任意で UDP ポート番号を指定します。デフォルトは 162 です。</p> <p>SNMP バージョン番号 (v1、v2c、または v3) を入力します。v3 を入力する場合は、次のオプションを追加します。</p> <ul style="list-style-type: none"> • encrypted は、パスワードを暗号化形式で表示するように指定します。このキーワードは、v3 キーワードが指定されている場合にのみ使用できます。 • auth では、認証レベルを設定します。HMAC-MD5-96 (md5) または HMAC-SHA-96 (sha) 認証レベルを指定できます。また、<i>auth-password</i> でパスワードの文字

	コマンドまたはアクション	目的
		<p>列を指定する必要があります（最大 64 文字）。</p> <p>v3 を入力すると、次のキーワードを使用して（64 文字以内）、プライベート（priv）暗号化アルゴリズムおよびパスワード文字列 <i>priv-password</i> を設定することもできます。</p> <ul style="list-style-type: none"> • priv は、ユーザベースセキュリティモデル（USM）を指定します。 • des 56 ビット DES アルゴリズムを使用する場合に指定します。 • 3des 168 ビット DES アルゴリズムを使用する場合に指定します。 • aes DES アルゴリズムを使用する場合に指定します。128 ビット暗号化、192 ビット暗号化、または 256 ビット暗号化のいずれかを選択する必要があります。 <p>（任意） access <i>access-list</i> とともに、アクセスリスト名の文字列（64 文字以内）を入力します。</p>
ステップ 6	<p>end</p> <p>例：</p> <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 7	<p>show running-config</p> <p>例：</p> <pre>Device# show running-config</pre>	入力を確認します。
ステップ 8	<p>copy running-config startup-config</p> <p>例：</p> <pre>Device# copy running-config startup-config</pre>	（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 通知

SNMPを使用すると、特定のイベントが発生した場合に、デバイスから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を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、デバイス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デバイス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。

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

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code> 例： Device> <code>enable</code>	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	<code>configure terminal</code> 例： Device# <code>configure terminal</code>	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 contact <i>text</i> 例： Device(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 <i>text</i> 例： Device(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： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例： Device# show running-config	入力を確認します。
ステップ 7	copy running-config startup-config 例： Device# 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

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • 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：	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
	Device# <code>configure terminal</code>	
ステップ 3	snmp-server tftp-server-list access-list-number 例 : Device(config)# <code>snmp-server tftp-server-list 44</code>	SNMP を介したコンフィギュレーション ファイルのコピーに使用する TFTP サー バを、アクセス リストのサーバに限定 します。 <i>access-list-number</i> には、1 ~ 99 および 1300 ~ 1999 の標準 IP アクセス リス ト 番号を入力します。
ステップ 4	access-list access-list-number {deny permit} source [source-wildcard] 例 : Device(config)# <code>access-list 44 permit 10.1.1.2</code>	標準アクセス リストを作成し、コマン ドを必要な回数だけ実行します。 <i>access-list-number</i> には、ステップ 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。 <i>source</i> には、デバイスにアクセスできる TFTP サーバの IP アドレスを入力しま す。 (任意) <i>source-wildcard</i> には、 <i>source</i> に 適用されるワイルドカードビットをドッ ト付き 10 進表記で入力します。無視す るビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに 対する暗黙の拒否ステートメントが常に 存在します。
ステップ 5	end 例 : Device(config)# <code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例 : Device# <code>show running-config</code>	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 : Device# 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 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。

始める前に

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

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • 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 : Device# 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 : Device (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 :	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
	Device(config)# end	
ステップ 5	show running-config 例： Device# show running-config	入力を確認します。
ステップ 6	copy running-config startup-config 例： Device# 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、デバイスはトラップを送信しません。

```
Device(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。デバイスはさらに、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。

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

```
Device(config)# snmp-server community comaccess ro 4
Device(config)# snmp-server enable traps snmp authentication
Device(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 行目で、デバイス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** ホストコマンドを無効にします。

```
Device(config)# snmp-server enable traps entity
Device(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* に送信するようにデバイスをイネーブルにする例を示します。

```
Device(config)# snmp-server enable traps
Device(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 モードの際に **auth** (**authNoPriv**) 認証レベルで情報を送信する例を示します。

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

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 8: 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。
	デバイスに設定されているローカル SNMP エンジンおよびすべてのリモート エンジンに関する情報を表示します。
show snmp group	ネットワーク上の各 SNMP グループに関する情報を表示します。
show snmp pending	保留中の SNMP 要求の情報を表示します。
show snmp sessions	現在の SNMP セッションの情報を表示します。
show snmp user	SNMP ユーザ テーブルの各 SNMP ユーザ名に関する情報を表示します。 (注) このコマンドは、 auth noauth priv モードの SNMPv3 設定情報を表示する際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。

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 Fuji 16.9.2	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。

- [SLA の制約事項 \(61 ページ\)](#)
- [サービスレベル契約に関する情報 \(61 ページ\)](#)
- [IP SLA 動作の設定方法 \(67 ページ\)](#)
- [IP SLA 動作のモニタリング \(81 ページ\)](#)
- [IP SLA 動作のモニタリングの例 \(82 ページ\)](#)
- [その他の参考資料 \(83 ページ\)](#)
- [サービスレベル契約の機能情報 \(84 ページ\)](#)

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。

- デバイスは、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。

サービスレベル契約に関する情報

ここでは、サービスレベル契約について説明します。

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します。

- 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

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。

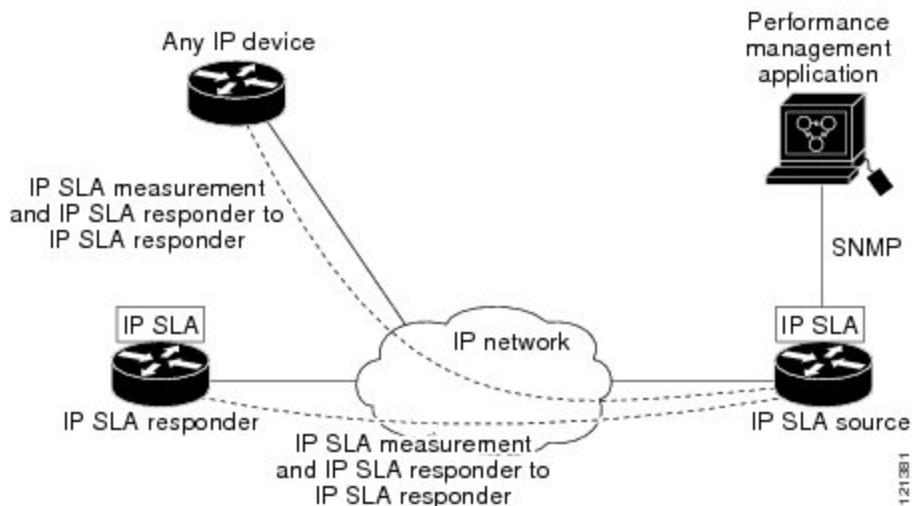
- 端末間のネットワーク アベイラビリティをモニタリングして、ネットワーク リソースをあらかじめ検証し接続をテストできる（たとえば、ビジネス上の重要なデータを保存する NFS サーバのネットワーク アベイラビリティをリモート サイトから確認できる）。
- 問題をすぐに認識し、トラブルシューティングにかかる時間を短縮できる一貫性のある信頼性の高い測定によるネットワーク動作のトラブルシューティング。
- マルチプロトコル ラベル スイッチング (MPLS) パフォーマンス モニタリングとネットワークの検証を行う（デバイスが MPLS をサポートする場合）。

Cisco IOS IP SLA でのネットワーク パフォーマンスの測定

IPSLA 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監視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。

図 2: Cisco IOS IP SLA 動作

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。

IP SLA レスポンダおよび IP SLA 制御プロトコル

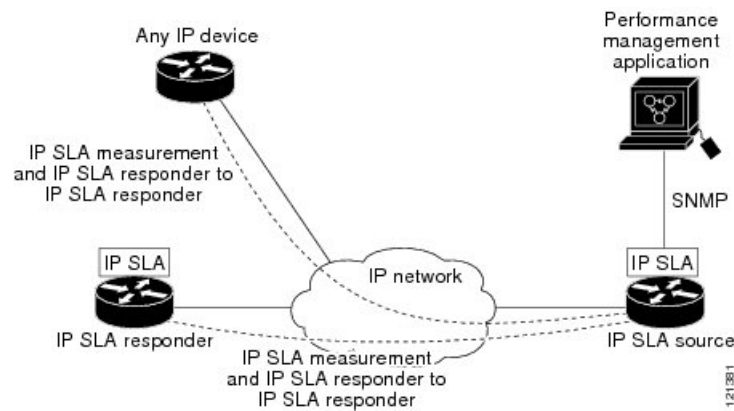
IP SLA レスポンダは宛先 Cisco デバイスに組み込まれたコンポーネントで、システムが IP SLA 要求パケットを予想して応答します。Responder は専用プローブなしで正確な測定を行います。レスポンダは、受信および応答するポートが通知されるメカニズムを Cisco IOS IP SLA コントロール プロトコルを通じて実現します。



(注) IP SLA レスポンダはレスポンダ設定可能なデバイスである 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有効にします。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 パケットに回答した後または指定の時間が経過したら ポートを無効にします。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 認証が利用できません。

図 3: 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 Responder では必要ありません。

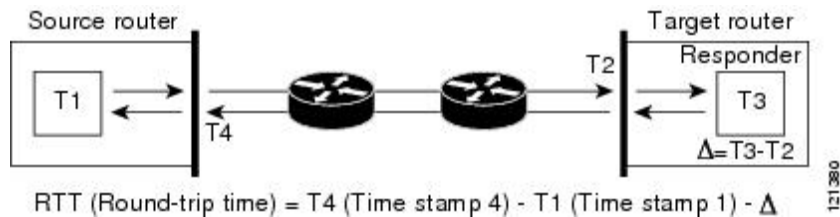
IP SLA の応答時間の計算

スイッチ、コントローラ、ルータは、他の高優先度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 レスポンダが有効の場合、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。

図 4: Cisco IOS IP SLA レスポンダ タイムスタンプ

次の図に、レスポнда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нда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。



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。1度に1つの IP SLA 動作をスケジューリングしたり、グループの動作をスケジューリングすることもできます。

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。

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。

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、『[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](#)』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デバイスでサポートされないものもあります。デバイスでは、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。

```
Device# 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

IPSLA 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 デバイスも含まれます。

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

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。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： Device# config t	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：	デバイスを 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。

	コマンドまたはアクション	目的
	<pre>Device(config)# ip sla responder udp-echo 172.29.139.134 5000</pre>	<ul style="list-style-type: none"> • tcp-connect : Responder 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。 <p>(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。</p>
ステップ 4	<p>end</p> <p>例 :</p> <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 5	<p>end</p> <p>例 :</p> <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 6	<p>show running-config</p> <p>例 :</p> <pre>Device# show running-config</pre>	入力を確認します。
ステップ 7	<p>copy running-config startup-config</p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	(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

デバイス上で 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。

始める前に

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

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> 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： Device# config t	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： Device(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 { <i>destination-ip-address</i> <i>destination-hostname</i> } <i>destination-port</i> [source-ip { <i>ip-address</i> <i>hostname</i> }] [source-port <i>port-number</i>] [control { enable disable }] [num-packets <i>number-of-packets</i>] [interval <i>interpacket-interval</i>] 例： Device(config-ip-sla)# udp-jitter 172.29.139.134 5000	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）。 <ul style="list-style-type: none"> 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。 (任意) source-ip {<i>ip-address</i> <i>hostname</i>} : 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

	コマンドまたはアクション	目的
		<p>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。</p> <ul style="list-style-type: none"> • (任意) source-port <i>port-number</i> : 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有効または無効にします。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 <i>number-of-packets</i> : 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 <i>inter-packet-interval</i> : 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 <i>seconds</i> 例 : <pre>Device(config-ip-sla-jitter)# frequency 45</pre>	(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 <i>milliseconds</i> 例 : <pre>Device(config-ip-sla-jitter)# threshold 200</pre>	(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 :	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

	コマンドまたはアクション	目的
	Device(config-ip-sla-jitter)# exit	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	<p>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]</p> <p>例 :</p> <pre>Device(config)# ip sla schedule 10 start-time now life forever</pre>	<p>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。</p> <ul style="list-style-type: none"> • 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、特定の秒数 (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	<p>end</p> <p>例 :</p>	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
	Device(config)# end	
ステップ 10	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 11	copy running-config startup-config 例 : Device# 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。

```

Device(config)# ip sla 10
Device(config-ip-sla)# udp-jitter 172.29.139.134 5000
Device(config-ip-sla-jitter)# frequency 30
Device(config-ip-sla-jitter)# exit
Device(config)# ip sla schedule 10 start-time now life forever
Device(config)# end
Device# 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:

```

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 ジッター動作を設定するには、次の手順を実行します。

始める前に

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

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • 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： Device# config t	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： Device(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 { <i>destination-ip-address</i> <i>destination-hostname</i> } <i>destination-port</i> [source-ip { <i>ip-address</i> <i>hostname</i> }] [source-port <i>port-number</i>] [control { enable disable }] [num-packets <i>number-of-packets</i>] [interval <i>interpacket-interval</i>] 例： Device(config-ip-sla)# udp-jitter 172.29.139.134 5000	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。 • <i>destination-ip-address</i> <i>destination-hostname</i> : 宛先 IP アドレスまたはホスト名を指定します。 • <i>destination-port</i> : 宛先ポート番号を 1 ~ 65535 の範囲で指定します。 • (任意) source-ip { <i>ip-address</i> <i>hostname</i> } : 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

	コマンドまたはアクション	目的
		<p>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。</p> <ul style="list-style-type: none"> （任意） source-port <i>port-number</i> : 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有効または無効にします。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 <i>number-of-packets</i> : 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 <i>inter-packet-interval</i> : 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 <i>seconds</i> 例 : Device (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 : Device (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 <i>operation-number</i> [life { forever <i>seconds</i> }] [start-time { <i>hh:mm</i> [: <i>ss</i>] [<i>month day</i> <i>day month</i>] pending	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。

	コマンドまたはアクション	目的
	<p>now after hh:mm:ss] [ageout seconds] [recurring]</p> <p>例 :</p> <pre>Device(config)# ip sla schedule 10 start-time now life forever</pre>	<ul style="list-style-type: none"> • 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、特定の秒数 (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	<p>end</p> <p>例 :</p> <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 9	<p>show running-config</p> <p>例 :</p>	入力を確認します。

	コマンドまたはアクション	目的
	Device# show running-config	
ステップ 10	copy running-config startup-config 例 : Device# 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。

```

Device(config)# ip sla 10
Device(config-ip-sla)# udp-jitter 172.29.139.134 5000
Device(config-ip-sla-jitter)# frequency 30
Device(config-ip-sla-jitter)# exit
Device(config)# ip sla schedule 10 start-time now life forever
Device(config)# end
Device# 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:

```

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。

始める前に

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

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • 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： Device# config 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： Device(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 { <i>destination-ip-address</i> <i>destination-hostname</i> } [source-ip { <i>ip-address</i> <i>hostname</i> } source-interface <i>interface-id</i>] 例： Device(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。 • <i>destination-ip-address</i> <i>destination-hostname</i> : 宛先 IP アドレスまたはホスト名を指定します。 • (任意) source-ip { <i>ip-address</i> <i>hostname</i> } : 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 <i>interface-id</i> : 動作に対する送信元インターフェイスを指定します。

	コマンドまたはアクション	目的
ステップ 5	frequency seconds 例 : <pre>Device(config-ip-sla-echo)# frequency 30</pre>	(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 : <pre>Device(config-ip-sla-echo)# exit</pre>	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。
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 : <pre>Device(config)# ip sla schedule 10 start-time now life forever</pre>	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。 <ul style="list-style-type: none"> • 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、特定の秒数 (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 と入力すると、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

	コマンドまたはアクション	目的
		<p>す。デフォルトは0秒（いつまでも保存する）です。</p> <ul style="list-style-type: none"> （任意） recurring : 毎日、動作を自動的に実行します。
ステップ 8	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 9	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 10	copy running-config startup-config 例 : Device# 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。

```

Device(config)# ip sla 10
Device(config-ip-sla)# icmp-echo 172.29.139.134
Device(config-ip-sla-echo)# frequency 30
Device(config-ip-sla-echo)# exit
Device(config)# ip sla schedule 10 start-time now life forever
Device(config)# end
Device# 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:

```

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 9: 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 [<i>entry-number</i>]	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 [<i>entry-number</i>]	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 [<i>entry-number</i> 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。

```
Device# 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。

```
Device# 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

その他の参考資料

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/c/en/us/td/docs/ios-xml/ios/mdata/configuration/15-sy/mdata-15sy-book/metadata-framework.pdf
Cisco Media Services Proxy Configuration Guide	http://www.cisco.com/c/en/us/td/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/c/en/us/td/docs/ios-xml/ios/media_monitoring/configuration/15-mt/mm-15-mt-book/mm-mediatrace.html

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	<p>選択したプラットフォーム、Cisco IOS リリース、およびフィードバックに関する 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。</p> <p>http://www.cisco.com/go/mibs</p>

シスコのテクニカル サポート

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

サービスレベル契約の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 10: サービスレベル契約の機能情報

リリース	機能情報
Cisco IOS XE Fuji 16.9.2	この機能が導入されました。



第 7 章

SPAN および RSPAN の設定

- SPAN および RSPAN の前提条件 (85 ページ)
- SPAN および RSPAN の制約事項 (85 ページ)
- SPAN および RSPAN について (87 ページ)
- SPAN および RSPAN の設定 (99 ページ)
- SPAN および RSPAN の設定方法 (100 ページ)
- SPAN および RSPAN 動作のモニタリング (127 ページ)
- SPAN および RSPAN の設定例 (127 ページ)
- SPAN および RSPAN の機能の履歴と情報 (130 ページ)

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

SPAN の制約事項は次のとおりです。

- 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 のトラフィックを監視できます。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。
- デバイスポートを SPAN 宛先ポートとして設定すると、通常のデバイスポートではなくなります。SPAN 宛先ポートを通過するのは、監視対象トラフィックのみになります。
- SPAN コンフィギュレーション コマンドを入力しても、前に設定した SPAN パラメータは削除されません。設定されている SPAN パラメータを削除するには、**no monitor session {session_number | all | local | remote}** グローバル コンフィギュレーション コマンドを入力する必要があります。
- ローカル SPAN では、**encapsulation replicate** キーワードが指定されている場合、SPAN 宛先ポートを経由する発信パケットは元のカプセル化ヘッダー（タグなし、ISL、または IEEE 802.1Q）を伝送します。このキーワードが指定されていない場合、パケットはネイティブ形式で送信されます。
- 無効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 が有効になってからです。
- 単一の SPAN セッションに、送信元 VLAN とフィルタ VLAN を混在させることはできません。

SPAN セッションのトラフィック監視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。
- Wireshark は、出力スパンがアクティブな場合は出力パケットをキャプチャしません。
- 同じデバイスまたはデバイススタック内で、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。デバイスまたはデバイススタックは、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つのデバイス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 セッションがデバイス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 のポートをトラフィック監視するなど、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 が有効の場合、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 を監視すると、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。
- ディゼ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。
- デバイスは、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。
 - 同じデバイスまたはデバイススタック上で、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。
- デバイスで DHCP スヌーピングが有効になっている場合、SPAN セッションは Dynamic Host Configuration Protocol (DHCP) 入力パケットのみをキャプチャします。

RSPAN

RSPAN の制約事項は次のとおりです。

- RSPAN は、BPDU パケットモニタリングまたは他のレイヤ 2 デバイス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デバイスで 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、デバイスはスパンされたトラフィックを監視しないため、デバイスの 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グディングが防止されます。
- RSPAN VLAN をネイティブ VLAN として設定しないことをお勧めします。

SPAN および RSPAN について

ここでは、SPAN および RSPAN について説明します。

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、そのデバイス上、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デバイス上のポートにトラフィックのコピーを送信します。SPAN は送信元ポート上または送信元 VLAN 上で受信、送信、または送受信されたトラフィックを宛先ポートにコピー（ミラーリング）して、解析します。SPAN は送信元ポートまたは VLAN 上のネットワークトラフィックのスイッチングには影響しません。宛先ポートは SPAN 専用にする必要があります。SPAN または RSPAN セッションに必要なトラフィック以外、宛先ポートがトラフィックを受信したり転送したりすることはありません。

SPAN を使用してモニタできるのは、送信元ポートを出入りするトラフィックまたは送信元 VLAN に入り出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 つのデバイス内の 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、同じデバイスまたはデバイス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。

ローカル SPAN は 1 つのスイッチ内の SPAN セッション全体をサポートします。すべての送信元ポートおよび宛先ポートは、同じスイッチ内にあります。ローカル SPAN は、1 つ以上の送信元ポートからのトラフィックを、解析のため宛先ポートにコピーします。

図 5: 単一デバイスでのローカル SPAN の設定例

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

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。

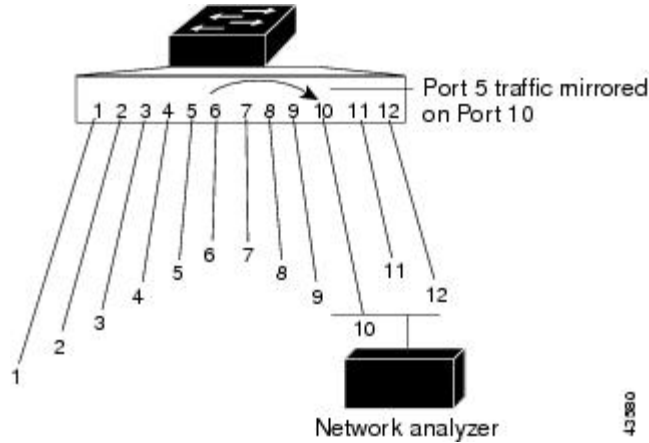
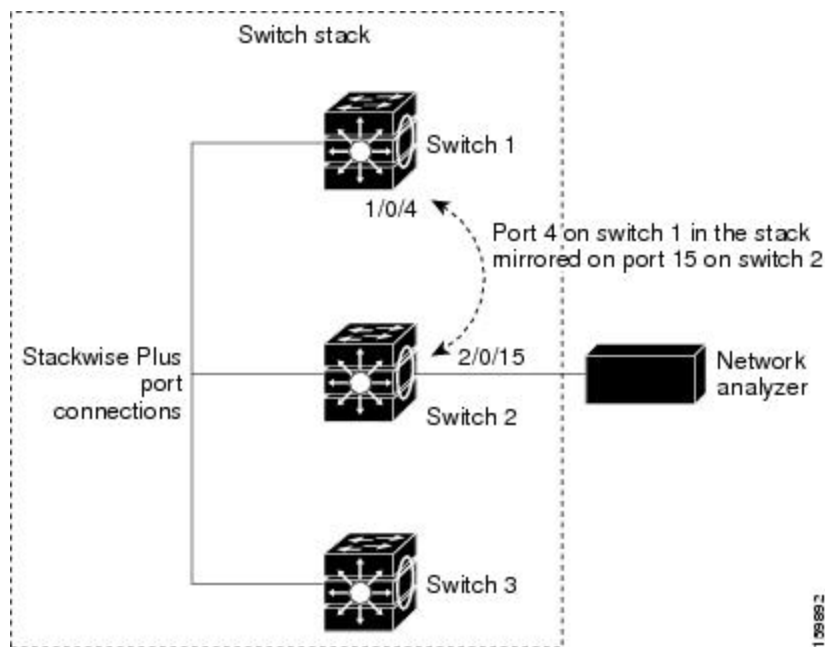


図 6: デバイスタックでのローカル SPAN の設定例

これは、デバイ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。



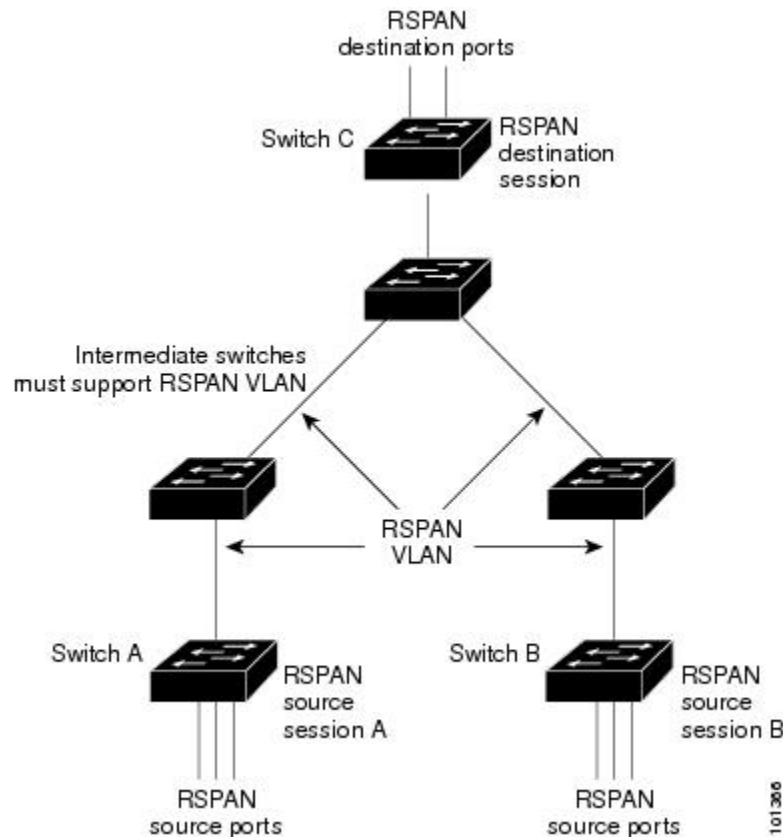
リモート SPAN

RSPAN は、異なるデバイス（または異なるデバイスタック）上の送信元ポート、送信元 VLAN、および宛先ポートをサポートしているため、ネットワーク上で複数のデバイスをリモート監視できます。

図 7: RSPAN の設定例

下の図にデバイス A とデバイス B の送信元ポートを示します。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デバイスの 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 を監視する宛先セッションに転送されます。各 RSPAN 送信元デバイスには、ポートまたは VLAN のいずれかが RSPAN 送信元として必要です。図中のデバイス C のように、宛先は常に物理ポートになります。



SPAN と RSPAN の概念および用語

SPAN セッション

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

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

RSPAN は少なくとも1つの RSPAN 送信元セッション、1つの RSPAN VLAN、および少なくとも1つの RSPAN 宛先セッションで構成されています。RSPAN 送信元セッションと RSPAN 宛先セッションは、異なるネットワーク デバイス上に別々に設定します。デバイスに RSPAN

送信元セッションを設定するには、一連の送信元ポートまたは送信元 VLAN を RSPAN VLAN に関連付けます。このセッションの出力は、RSPAN VLAN に送信される SPAN パケットのストリームです。別のデバイスに RSPAN 宛先セッションを設定するには、宛先ポートを RSPAN VLAN に関連付けます。宛先セッションは RSPAN VLAN トラフィックをすべて収集し、RSPAN 宛先ポートに送信します。

RSPAN 送信元セッションは、パケットストリームが転送される点を除き、ローカル SPAN セッションに非常に似ています。RSPAN 送信元セッションでは、SPAN パケットに RSPAN VLANID 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デバイスに転送されます。

RSPAN 宛先セッションは RSPAN VLAN 上で受信されたすべてのパケットを取得し、VLAN のタグングを除去し、宛先ポートに送ります。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。

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。
- 同じデバイスまたはデバイススタック内で、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。デバイスまたはデバイススタックは、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 つのデバイス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 セッションがデバイス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 のポートをトラフィック監視するなど、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 が有効の場合、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。
- ディゼ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。
- デバイスは、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。
 - 同じデバイスまたはデバイススタック上で、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。

モニタ対象トラフィック

SPAN セッションは、次のトラフィック タイプを監視できます。

- 受信 (Rx) SPAN : 受信 (または入力) SPAN は、デバイス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、デバイス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。

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。

デバイスの輻輳により、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。
- デバイスの輻輳が原因でドロップされた出力パケットは、出力 SPAN からで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 モニタ用とポート 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 からデバイスに入ってポート 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（別名モニタ側ポート）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。

デバイスは、任意の数の送信元ポート（デバイス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。

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デバイスまたはデバイススタックに存在する必要があります。RSPAN セッションの場合は、RSPAN 宛先セッションを含むデバイス上にあります。RSPAN 送信元セッションのみを実行するデバイスまたはデバイススタックには、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 (ON モードのみ)。
- 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。
- デバイスまたはデバイス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、すべての中間デバイスを手動で設定する必要があります。

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

SPAN および RSPAN と他の機能の相互作用

SPAN は次の機能と相互に作用します。

- ルーティング：SPAN はルーテッドトラフィックを監視しません。VSPAN が監視するのはデバイス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、デバイスが別の 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 セッションが無効になると、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、デバイス間で 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できます。グループが SPAN 送信元として設定されている場合、グループ全体が監視されます。

監視対象の 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。監視対象の 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監視されます。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 グループおよび監視対象ポート 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監視できます。出力ポートおよび入力ポートの監視では、未編集の packets が 1 つだけ SPAN 宛先ポートに送信されます。マルチキャスト packets の送信回数は反映されません。
- プライベート VLAN ポートは、SPAN 宛先ポートには設定できません。
- セキュア ポートを SPAN 宛先ポートにすることはできません。

SPAN セッションでは、入力転送が宛先ポートで有効の場合、出力を監視しているポートでポートセキュリティを有効にしないでください。RSPAN 送信元セッションでは、出力を監視しているポートでポートセキュリティを有効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 を有効にできますが、SPAN 宛先としてこのポートを削除するまで、IEEE 802.1x は無効に設定されます。

SPAN セッションでは、入力転送が宛先ポートで有効の場合、出力を監視しているポートで IEEE 802.1x を有効にしないでください。RSPAN 送信元セッションでは、出力を監視しているポートで IEEE 802.1x を有効にしないでください。

SPAN と RSPAN とデバイス スタック

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

フローベースの SPAN

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

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

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

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

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

スタックに設定された VLAN ベースの FSPAN セッションが 1 つまたは複数のデバイス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デバイス上でアンロードされたものとして処理され、デバイスでの 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デバイスの 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。

SPAN および RSPAN のデフォルト設定

表 11: 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

機能	デフォルト設定
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

SPAN および RSPAN の設定

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 {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** 形式を使用すると、**encapsulation** オプションは無視されます。
- トランクポート上のすべての VLAN をモニタするには、**no monitor session session_number filter** グローバル コンフィギュレーション コマンドを使用します。

RSPAN 設定時の注意事項

- すべての SPAN 設定時の注意事項が RSPAN に適用されます。
- RSPAN VLAN には特性があるので、RSPAN VLAN として使用するためにネットワーク上の VLAN をいくつか確保し、それらの VLAN にはアクセス ポートを割り当てないでおく必要があります。
- RSPAN トラフィックに出力 ACL を適用して、特定の packets を選択的にフィルタリングまたはモニタできます。RSPAN 送信元内の 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タスになります。
- 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で RSPAN がサポートされている。

FSPAN および FRSPAN 設定時の注意事項

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

SPAN および RSPAN の設定方法

ここでは、SPAN および RSPAN の設定方法について説明します。

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（監視対象）ポートまたは VLAN、および宛先（監視側）ポートを指定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • 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： Device# 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	<p>no monitor session {<i>session_number</i> all local remote}</p> <p>例 :</p> <pre>Device(config)# no monitor session all</pre>	<p>セッションに対する既存の SPAN 設定を削除します。</p> <ul style="list-style-type: none"> • <i>session_number</i> の範囲は、1 ~ 66 です。 • all : すべての SPAN セッションを削除します。 • local : すべてのローカルセッションを削除します。 • remote : すべてのリモート SPAN セッションを削除します。
ステップ 4	<p>monitor session <i>session_number</i> source {interface <i>interface-id</i> / vlan <i>vlan-id</i>} [, -] [both rx tx]</p> <p>例 :</p> <pre>Device(config)# monitor session 1 source interface gigabitethernet1/0/1</pre>	<p>SPAN セッションおよび送信元ポート (モニタ対象ポート) を指定します。</p> <ul style="list-style-type: none"> • <i>session_number</i> の範囲は、1 ~ 66 です。 • <i>interface-id</i> には、モニタリングする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポートチャネル論理インターフェイス (port-channel <i>port-channel-number</i>) があります。有効なポートチャネル番号は 1 ~ 48 です。 • <i>vlan-id</i> には、監視する送信元 VLAN を指定します。指定できる範囲は 1 ~ 4094 です (RSPAN VLAN は除く)。 <p>(注) 1つのセッションに、一連のコマンドで定義された複数の送信元 (ポートまたは VLAN) を含めることができます。ただし、1つのセッション内では送信元ポートと送信元 VLAN を併用できません。</p> <ul style="list-style-type: none"> • (任意) [, -] には、一連のインターフェイスまたはインターフェイスの

	コマンドまたはアクション	目的
		<p>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。</p> <ul style="list-style-type: none"> • (任意) both rx tx : 監視するトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、送信元インターフェイスは送信トラフィックと受信トラフィックの両方を送信します。 <ul style="list-style-type: none"> • both : 受信トラフィックと送信トラフィックの両方を監視します。 • 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。 <p>(注) monitor session session_number source コマンドを複数回使用すると、複数の送信元ポートを設定できます。</p>
ステップ 5	<pre>monitor session session_number destination { interface interface-id [, -] [encapsulation replicate dot1q]} 例 :</pre> <pre>Device(config)# monitor session 1 destination interface gigabitethernet1/0/2 encapsulation replicate</pre>	<p>SPANセッションおよび宛先ポート（監視側ポート）を指定します。設定変更が有効になると、ポートのLEDがオレンジ色に変わります。LEDはSPAN宛先の設定を削除した後にのみ、元の状態（緑色）に戻ります。</p> <p>(注) ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。</p> <ul style="list-style-type: none"> • session_number には、ステップ 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。

	コマンドまたはアクション	目的
		<p>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。</p> <ul style="list-style-type: none"> • (任意) [,-]には、一連のインターフェイスまたはインターフェイスの範囲を指定します。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。 <p>(任意) encapsulation replicate には、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。</p> <p>(任意) encapsulation dot1q は宛先インターフェイスが IEEE 802.1Q カプセル化の送信元インターフェイスの着信パケットを受け入れるように指定します。</p> <p>(注) monitor session session_number destination コマンドを複数回使用すると、複数の送信元ポートを設定できます。</p>
ステップ 6	<p>end</p> <p>例 :</p> <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 7	<p>show running-config</p> <p>例 :</p> <pre>Device# show running-config</pre>	入力を確認します。
ステップ 8	<p>copy running-config startup-config</p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	(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。

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

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • 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： Device# 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 { <i>session_number</i> all local remote } 例： Device(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。 • <i>session_number</i> の範囲は、1～66 です。 • all : すべての SPAN セッションを削除します。 • local : すべてのローカルセッションを削除します。 • remote : すべてのリモート SPAN セッションを削除します。
ステップ 4	monitor session <i>session_number</i> source { interface <i>interface-id</i> vlan <i>vlan-id</i> } [, -] [both rx tx] 例： Device(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 <i>session_number</i> destination { interface <i>interface-id</i> [, -] [encapsulation replicate] [ingress { dot1q vlan <i>vlan-id</i> untagged vlan <i>vlan-id</i> vlan <i>vlan-id</i> }]}	SPAN セッション、宛先ポート、パケットカプセル化、および入力 VLAN とカプセル化を指定します。

	コマンドまたはアクション	目的
	<p>例 :</p> <pre>Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate ingress dot1q vlan 6</pre>	<ul style="list-style-type: none"> • <i>session_number</i> 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。 • <i>interface-id</i> には、宛先ポートを指定します。 宛先インターフェイスには物理ポートを指定する必要があります。 EtherChannel や VLAN は指定できません。 • (任意) <i>[, -]</i> : 一連のインターフェイスまたはインターフェイスの範囲を指定します。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 には、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。 • (任意) encapsulation dot1q は宛先インターフェイスが IEEE 802.1Q カプセル化の送信元インターフェイスの着信パケットを受け入れるように指定します。 • ingress 宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定します。 <ul style="list-style-type: none"> • dot1q vlan vlan-id : デフォルトの VLAN として指定した VLAN で、IEEE 802.1Q でカプセル化された着信パケットを受け入れます。 • untagged vlan vlan-id または vlan 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

	コマンドまたはアクション	目的
		た着信パケットを受け入れます。
ステップ 6	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 7	show running-config 例： Device# show running-config	入力を確認します。
ステップ 8	copy running-config startup-config 例： Device# 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。

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

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • 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： Device# 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 { <i>session_number</i> all local remote } 例：	セッションに対する既存の SPAN 設定を削除します。 • <i>session_number</i> の範囲は、1 ~ 66 です。

	コマンドまたはアクション	目的
	<pre>Device(config)# no monitor session all</pre>	<ul style="list-style-type: none"> • 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	<p>monitor session <i>session_number</i> source interface <i>interface-id</i></p> <p>例 :</p> <pre>Device(config)# monitor session 2 source interface gigabitethernet1/0/2 rx</pre>	<p>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。</p> <ul style="list-style-type: none"> • <i>session_number</i> の範囲は、1 ~ 66 です。 • <i>interface-id</i> には、モニタリング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	<p>monitor session <i>session_number</i> filter vlan <i>vlan-id</i> [, -]</p> <p>例 :</p> <pre>Device(config)# monitor session 2 filter vlan 1 - 5 , 9</pre>	<p>SPAN 送信元トラフィックを特定の VLAN に制限します。</p> <ul style="list-style-type: none"> • <i>session_number</i> 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。 • <i>vlan-id</i> に指定できる範囲は 1 ~ 4094 です。 • (任意) カンマ (,) を使用して一連の VLAN を指定するか、ハイフン (-) を使用して VLAN 範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 6	<p>monitor session <i>session_number</i> destination {interface <i>interface-id</i> [, -] [encapsulation replicate] }</p> <p>例 :</p> <pre>Device(config)# monitor session 2 destination interface gigabitethernet1/0/1</pre>	<p>SPAN セッションおよび宛先ポート（モニタ側ポート）を指定します。</p> <ul style="list-style-type: none"> • <i>session_number</i> 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。 • <i>interface-id</i> には、宛先ポートを指定します。

	コマンドまたはアクション	目的
		<p>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。</p> <ul style="list-style-type: none"> • (任意) [,-]には、一連のインターフェイスまたはインターフェイスの範囲を指定します。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) encapsulation replicate には、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 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 8	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 9	copy running-config startup-config 例 : Device# 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

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • 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： Device# 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： Device(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： Device(config-vlan)# remote-span	VLAN を RSPAN VLAN として設定します。
ステップ 5	end 例： Device(config-vlan)# end	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例： Device# show running-config	入力を確認します。
ステップ 7	copy running-config startup-config 例： Device# 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。

次のタスク

RSPAN に参加するすべてのデバイスに 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 つのデバイスに RSPAN VLAN を作成し、VTP がこの RSPAN VLAN を VTP ドメイン内の他のデバイス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デバイス、および中間デバイスに 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

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none">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： Device# 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 { <i>session_number</i> all local remote } 例： Device(config)# no monitor session 1	セッションに対する既存の SPAN 設定を削除します。 <ul style="list-style-type: none"><i>session_number</i> の範囲は、1～66 です。all：すべての SPAN セッションを削除します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • 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	<p>monitor session <i>session_number</i> source {interface <i>interface-id</i> vlan <i>vlan-id</i>} [, -] [both rx tx]</p> <p>例 :</p> <pre>Device(config)# monitor session 1 source interface gigabitethernet1/0/1 tx</pre>	<p>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。</p> <ul style="list-style-type: none"> • <i>session_number</i> 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。 <ul style="list-style-type: none"> • <i>interface-id</i> には、モニタリングする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポートチャネル論理インターフェイス (port-channel <i>port-channel-number</i>) があります。有効なポートチャネル番号は 1 ~ 48 です。 • <i>vlan-id</i> には、モニタする送信元 VLAN を指定します。指定できる範囲は 1 ~ 4094 です (RSPAN VLAN は除く)。 <p>1つのセッションに、一連のコマンドで定義された複数の送信元 (ポートまたはVLAN) を含めることができます。ただし、1つのセッション内で送信元ポートと送信元 VLAN を併用することはできません。</p> <ul style="list-style-type: none"> • (任意) [, -] : 一連のインターフェイスまたはインターフェイスの範囲を指定します。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 : 監視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

	コマンドまたはアクション	目的
		<p>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。</p> <ul style="list-style-type: none"> • both : 受信トラフィックと送信トラフィックの両方を監視します。 • 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	<p>monitor session session_number destination remote vlan vlan-id</p> <p>例 :</p> <pre>Device(config)# monitor session 1 destination remote vlan 100</pre>	<p>RSPAN セッション、宛先 RSPAN VLAN、および宛先ポートグループを指定します。</p> <ul style="list-style-type: none"> • <i>session_number</i> には、ステップ 4 で指定した番号を入力します。 • <i>vlan-id</i> には、モニタリングする送信元 RSPAN VLAN を指定します。
ステップ 6	<p>end</p> <p>例 :</p> <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 7	<p>show running-config</p> <p>例 :</p> <pre>Device# show running-config</pre>	入力を確認します。
ステップ 8	<p>copy running-config startup-config</p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	(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。

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

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> 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 : Device# 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 : Device (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。 <ul style="list-style-type: none"> session_number の範囲は、1 ～ 66 です。 all : すべての SPAN セッションを削除します。 local : すべてのローカルセッションを削除します。 remote : すべてのリモート SPAN セッションを削除します。
ステップ 4	monitor session session_number source interface interface-id 例 : Device (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。 <ul style="list-style-type: none"> 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。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。

	コマンドまたはアクション	目的
ステップ 5	monitor session <i>session_number</i> filter vlan <i>vlan-id</i> [, -] 例 : <pre>Device(config)# monitor session 2 filter vlan 1 - 5 , 9</pre>	SPAN 送信元トラフィックを特定の VLAN に制限します。 <ul style="list-style-type: none"> • <i>session_number</i> 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。 • <i>vlan-id</i> に指定できる範囲は 1 ~ 4094 です。 • (任意) , -カンマ (,) を使用して一連の VLAN を指定するか、ハイフン (-) を使用して VLAN 範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 6	monitor session <i>session_number</i> destination remote vlan <i>vlan-id</i> 例 : <pre>Device(config)# monitor session 2 destination remote vlan 902</pre>	RSPAN セッションおよび宛先リモート VLAN (RSPAN VLAN) を指定します。 <ul style="list-style-type: none"> • <i>session_number</i> には、ステップ 4 で指定したセッション番号を入力します。 • <i>vlan-id</i> には、宛先ポートにモニタ対象トラフィックを伝送する RSPAN VLAN を指定します。
ステップ 7	end 例 : <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 8	show running-config 例 : <pre>Device# show running-config</pre>	入力を確認します。
ステップ 9	copy running-config startup-config 例 : <pre>Device# copy running-config startup-config</pre>	(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、別のデバイスまたはデバイススタック（送信元セッションが設定されていないデバイスまたはデバイススタック）に設定します。

このデバイス上で 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

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • 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： Device# 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： Device(config)# vlan 901	送信元デバイスで作成された 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。 両方のデバイスが 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： Device(config-vlan)# remote-span	VLAN を RSPAN VLAN として識別します。
ステップ 5	exit 例： Device(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 6	no monitor session {session_number all local remote} 例： Device(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。 • <i>session_number</i> の範囲は、1～66 です。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • 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 : <pre>Device(config)# monitor session 1 source remote vlan 901</pre>	RSPAN セッションと送信元 RSPAN VLAN を指定します。 <ul style="list-style-type: none"> • session_number の範囲は、1 ~ 66 です。 • vlan-id には、モニタリングする送信元 RSPAN VLAN を指定します。
ステップ 8	monitor session session_number destination interface interface-id 例 : <pre>Device(config)# monitor session 1 destination interface gigabitethernet2/0/1</pre>	RSPAN セッションと宛先インターフェイスを指定します。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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 : <pre>Device(config)# end</pre>	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 10	show running-config 例： Device# show running-config	入力を確認します。
ステップ 11	copy running-config startup-config 例： Device# 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

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • 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： Device# 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： Device (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。 • <i>session_number</i> の範囲は、1 ~ 66 です。 • all : すべての SPAN セッションを削除します。 • local : すべてのローカル セッションを削除します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • 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	<p>monitor session <i>session_number</i> source remote vlan <i>vlan-id</i></p> <p>例 :</p> <pre>Device(config)# monitor session 2 source remote vlan 901</pre>	<p>RSPAN セッションと送信元 RSPAN VLAN を指定します。</p> <ul style="list-style-type: none"> • <i>session_number</i> の範囲は、1 ~ 66 です。 • <i>vlan-id</i> には、モニタリングする送信元 RSPAN VLAN を指定します。
ステップ 5	<p>monitor session <i>session_number</i> destination {interface <i>interface-id</i> [, -] [ingress { dot1q vlan <i>vlan-id</i> untagged vlan <i>vlan-id</i> vlan <i>vlan-id</i> }]}</p> <p>例 :</p> <pre>Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress vlan 6</pre>	<p>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。</p> <ul style="list-style-type: none"> • <i>session_number</i> には、ステップ 5 で指定した番号を入力します。 <p>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。</p> <ul style="list-style-type: none"> • <i>interface-id</i> には、宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。 • encapsulation replicate はコマンドラインのヘルプストリングに表示されますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。 • (任意) [, -] には、一連のインターフェイスまたはインターフェイスの範囲を指定します。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。 • 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

	コマンドまたはアクション	目的
		<p>を追加のキーワードと一緒に入力します。</p> <ul style="list-style-type: none"> • dot1q vlan <i>vlan-id</i> : デフォルトの VLAN として指定した VLAN で、IEEE 802.1Q でカプセル化された着信パケットを転送します。 • untagged vlan <i>vlan-id</i> または vlan <i>vlan-id</i> : デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを転送します。
ステップ 6	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 7	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 8	copy running-config startup-config 例 : Device# 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。

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（モニター側）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

	コマンドまたはアクション	目的
ステップ 1	enable 例 :	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	Device> enable	<ul style="list-style-type: none"> 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： Device# 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： Device(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。 <ul style="list-style-type: none"> session_number の範囲は、1～66 です。 all：すべての SPAN セッションを削除します。 local：すべてのローカルセッションを削除します。 remote：すべてのリモート SPAN セッションを削除します。
ステップ 4	monitor session session_number source { interface interface-id vlan vlan-id} [, -] [both rx tx] 例： Device(config)# monitor session 2 source interface gigabitethernet1/0/1	SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 <ul style="list-style-type: none"> 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。 vlan-idには、監視する送信元 VLAN を指定します。指定できる範囲は 1～4094 です（RSPAN VLAN は除く）。

	コマンドまたはアクション	目的
		<p>(注) 1つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1つのセッション内では送信元ポートと送信元 VLAN を併用できません。</p> <ul style="list-style-type: none"> • (任意) <code>[, -]</code>：一連のインターフェイスまたはインターフェイスの範囲を指定します。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) <code>[both rx tx]</code>：モニタリングするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、SPAN は送信トラフィックと受信トラフィックの両方をモニタします。 <ul style="list-style-type: none"> • both：送信トラフィックと受信トラフィックの両方を監視します。これはデフォルトです。 • rx：受信トラフィックをモニタします。 • tx：送信トラフィックをモニタします。 <p>(注) monitor session <i>session_number</i> <i>source</i> コマンドを複数回使用すると、複数の送信元ポートを設定できます。</p>
ステップ 5	<p>monitor session <i>session_number</i> <i>destination</i> {<i>interface interface-id</i> [, -] [<i>encapsulation replicate</i>]}</p> <p>例：</p>	<p>SPANセッションおよび宛先ポート（監視側ポート）を指定します。</p> <ul style="list-style-type: none"> • <i>session_number</i> 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。

	コマンドまたはアクション	目的
	<pre>Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate</pre>	<ul style="list-style-type: none"> • destination では、次のパラメータを指定します。 <ul style="list-style-type: none"> • interface-id には、宛先ポートを指定します。 宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 • (任意) [, -] には、一連のインターフェイスまたはインターフェイスの範囲を指定します。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) encapsulation replicate には、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 <p>(注) ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。</p> <p>monitor session session_number destination コマンドを複数回使用すると、複数の送信元ポートを設定できます。</p>
ステップ 6	<pre>monitor session session_number filter {ip ipv6 mac} access-group {access-list-number name}</pre> <p>例 :</p> <pre>Device(config)# monitor session 2 filter ipv6 access-group 4</pre>	<p>SPAN セッション、フィルタリングするパケットのタイプ、および FSPAN セッションで使用する ACL を指定します。</p> <ul style="list-style-type: none"> • 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。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • <i>access-list-number</i> には、トラフィックのフィルタリングに使用したい ACL 番号を指定します。 • <i>name</i> には、トラフィックのフィルタリングに使用する ACL の名前を指定します。
ステップ 7	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 8	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 9	copy running-config startup-config 例 : Device# 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。

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

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • 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 : Device# 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	<p>no monitor session {<i>session_number</i> all local remote}</p> <p>例 :</p> <pre>Device(config)# no monitor session 2</pre>	<p>セッションに対する既存の SPAN 設定を削除します。</p> <ul style="list-style-type: none"> • <i>session_number</i> の範囲は、1 ~ 66 です。 • all : すべての SPAN セッションを削除します。 • local : すべてのローカルセッションを削除します。 • remote : すべてのリモート SPAN セッションを削除します。
ステップ 4	<p>monitor session <i>session_number</i> source {interface <i>interface-id</i> vlan <i>vlan-id</i>} [, -] [both rx tx]</p> <p>例 :</p> <pre>Device(config)# monitor session 2 source interface gigabitethernet1/0/1</pre>	<p>SPAN セッションおよび送信元ポート (モニタ対象ポート) を指定します。</p> <ul style="list-style-type: none"> • <i>session_number</i> の範囲は、1 ~ 66 です。 • <i>interface-id</i> には、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ンネル論理インターフェイス (port-channel <i>port-channel-number</i>) があります。有効なポートチャンネル番号は 1 ~ 48 です。 • <i>vlan-id</i> には、監視する送信元 VLAN を指定します。指定できる範囲は 1 ~ 4094 です (RSPAN VLAN は除く)。 <p>(注) 1つのセッションに、一連のコマンドで定義された複数の送信元 (ポートまたは VLAN) を含めることができます。ただし、1つのセッション内では送信元ポートと送信元 VLAN を併用できません。</p>

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

	コマンドまたはアクション	目的
ステップ 8	exit 例 : Device(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 : Device(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。 <ul style="list-style-type: none"> • <i>session_number</i> 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。 • <i>access-list-number</i> には、トラフィックのフィルタリングに使用したい ACL 番号を指定します。 • <i>name</i> には、トラフィックのフィルタリングに使用する ACL の名前を指定します。
ステップ 10	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 11	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 12	copy running-config startup-config 例 : Device# 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。

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モニタするために使用するコマンドについて説明します。

表 12: SPAN および RSPAN 動作のモニタリング

コマンド	目的
<code>show monitor</code>	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

次のセクションに SPAN および RSPAN の設定例を示します

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。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 1
Device(config)# monitor session 1 source interface gigabitethernet1/0/1
Device(config)# monitor session 1 destination interface gigabitethernet1/0/2
encapsulation replicate
Device(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。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 1 source interface gigabitethernet1/0/1
Device(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。

```
Device> enable
Device# configure terminal
Device(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。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 source vlan 1 - 3 rx

Device(config)# monitor session 2 destination interface gigabitethernet1/0/2
Device(config)# monitor session 2 source vlan 10
Device(config)# end
```

次に、SPAN セッション 2 の既存の設定を削除し、ギガビットイーサネットソース送信元ポート 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、そのトラフィックを送信元ポートと同じ出力カプセル化方式の宛先ギガビットイーサネットポート 2 に送信し、デフォルト入力 VLAN として VLAN 6 を使用した入力転送をイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 source gigabitethernet0/1 rx
Device(config)# monitor session 2 destination interface gigabitethernet0/2 encapsulation
    replicate ingress vlan 6
Device(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。

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

例 : RSPAN VLAN の作成

この例は、RSPAN VLAN 901 の作成方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# vlan 901
Device(config-vlan)# remote span
Device(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。


```
Device> enable
Device# configure terminal
Device(config)# no monitor session 1
Device(config)# monitor session 1 source interface gigabitethernet1/0/1 tx
Device(config)# monitor session 1 source interface gigabitethernet1/0/2 rx
Device(config)# monitor session 1 source interface port-channel 2
Device(config)# monitor session 1 destination remote vlan 901
Device(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。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Device(config)# monitor session 2 filter vlan 1 - 5 , 9
Device(config)# monitor session 2 destination remote vlan 902
Device(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。

```
Device> enable
Device# configure terminal
Device(config)# monitor session 1 source remote vlan 901
Device(config)# monitor session 1 destination interface gigabitethernet2/0/1
Device(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GigabitEthernet2を宛先インターフェイスとして設定し、VLAN6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。

```
Device> enable
Device# configure terminal
Device(config)# monitor session 2 source remote vlan 901
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress
vlan 6
Device(config)# end
```

SPAN および RSPAN の機能の履歴と情報

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	<p>スイッチポートアナライザ (SPAN) : スニファアやアナライザまたは RMON プロブを使用してポートまたは VLAN のデバイスのトラフィックを監視できます。</p> <p>この機能が導入されました。</p>
Cisco IOS XE Fuji 16.9.2	<p>フローベースのスイッチポートアナライザ (SPAN) : 指定されたフィルタを使用してエンドホスト間の必要なデータのみをキャプチャする手段を提供します。フィルタは、IPv4、IPv6 または IPv4 と IPv6、あるいは指定された送信元と宛先アドレス間の IP トラフィック (MAC) 以外を制限するアクセスリストの観点から定義されます。</p> <p>この機能が導入されました。</p>
Cisco IOS XE Fuji 16.9.2	<p>スイッチポートアナライザ (SPAN) - 分散型出力</p> <p>SPAN : ラインカードにすでに分散された入力 SPAN とともにラインカードに出力 SPAN 機能を分散させます。出力 SPAN 機能をラインカードに分散させることで、システムのパフォーマンスが向上します。</p> <p>この機能が導入されました。</p>



第 8 章

パケット キャプチャの設定

- [パケットキャプチャ設定の前提条件](#) (131 ページ)
- [組み込みパケット キャプチャの制約事項](#) (132 ページ)
- [パケット キャプチャについて](#) (133 ページ)
- [組み込みパケット キャプチャの実装方法](#) (134 ページ)
- [組み込みパケット キャプチャの設定例](#) (136 ページ)
- [パケットキャプチャ設定の機能履歴と情報](#) (139 ページ)

パケットキャプチャ設定の前提条件

パケット キャプチャは Cisco Catalyst 9200 シリーズ スイッチでサポートされています。ここでは、パケットキャプチャの設定に関する前提条件について説明します。

組み込みパケットキャプチャ設定の前提条件

組み込みパケット キャプチャ (EPC) のソフトウェア サブシステムは、その動作で CPU とメモリ リソースを消費します。さまざまなタイプの操作を行うために十分なシステム リソースを準備する必要があります。システムリソースを使用するためのガイドラインを以下の表に示します。

表 13: EPC サブシステムのシステム要件

システム リソース	要件
ハードウェア	CPU 利用率の要件は、プラットフォームによって異なります。
メモリ	パケット バッファは DRAM に保存されます。パケット バッファのサイズは、ユーザが指定します。
ディスクスペース	パケットは外部のデバイスにエクスポートできます。フラッシュ ディスクでの中間保管は必要ありません。

組み込みパケットキャプチャの制約事項

- レイヤ 2 EtherChannels はサポートされません。
- 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。
- 組み込みパケットキャプチャ (EPC) は、ポートチャネル、スイッチ仮想インターフェイス (SVI)、およびサブインターフェイスを含む論理ポートではサポートされません。物理ポート上でのみサポートされます。
- ユーザがスイッチポートからルーテッドポート (レイヤ 2 からレイヤ 3) へ、またはその逆へインターフェイスを変更した場合、インターフェイスが再び起動したときに、そのキャプチャポイントを削除し、新しいファイルを作成する必要があります。キャプチャポイントの停止/開始が機能しません。
- 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、デバイスの書き換えによって行われた変更 (TTL、VLAN タグ CoS、チェックサム、および MAC アドレス、DSCP、プレジデント、UP など) が反映されないこともあります。
- パケットキャプチャの最小設定可能期間は 1 秒ですが、パケットキャプチャは少なくとも 2 秒間機能します。
- キャプチャがすでにアクティブである、または開始されている場合、キャプチャポイントパラメータを変更することはできません。
- EPC は、入力のマルチキャストパケットのみをキャプチャし、出力の複製パケットはキャプチャしません。
- 入力および出力の両方のパケットの書き換え情報はキャプチャされません。
- 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。
- コントロールプレーンパケットは、レート制限とパフォーマンスへの影響はありません。コントロールプレーンパケットのキャプチャを制限するフィルタを使用してください。
- Control and Provisioning of Wireless Access Points (CAPWAP) などのプロトコルのデコードは、DNA Advantage でサポートされています。
- 最大 8 つ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。
- MAC フィルタは、MAC アドレスに一致しても IP パケットをキャプチャしません。これは、すべてのインターフェイス (レイヤ 2 スwitchポート、レイヤ 3 ルーテッドポート) に適用されます。
- 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。

- MAC フィルタは、レイヤ 3 インターフェイスとレイヤ 2 パケット (ARP) をキャプチャすることはできません。
- IPv6 ベースの ACL は VACL ではサポートされません。

パケット キャプチャについて

パケットキャプチャ機能は、オンボードのパケットキャプチャファシリティです。ネットワーク管理者がデバイスを出入りするかデバイスを通るパケットをキャプチャすることで、パケットをローカルで分析したり、Embedded Packet Capture (EPC) を使用するオフライン分析に向けてパケットを保存してエクスポートしたりできるようにするものです。この機能は、デバイスがネットワークの管理と操作にアクティブに参加できるようにすることによって、ネットワーク操作を簡略化します。この機能は、パケットの形式に関する情報を収集することによって、トラブルシューティングを容易にします。また、アプリケーションの分析とセキュリティも容易にします。

組み込みパケットキャプチャについて

EPCは、パケットのトレースとトラブルシューティングに役立つ組み込みシステム管理機能を提供します。この機能を使用すると、ネットワーク管理者は、シスコデバイスを出入りするか通過するデータパケットをキャプチャできます。ネットワーク管理者は、キャプチャバッファサイズとタイプ (循環またはリニア) およびキャプチャする各パケットの最大バイト数を定義する場合があります。パケット キャプチャ レートは、詳細な管理制御を使用してスロットリングできます。たとえば、アクセス コントロール リストを使用してキャプチャ対象パケットをフィルタリングするオプションや、最大パケット キャプチャ レートまたはサンプリング間隔の指定などの詳細な定義を行うオプションが利用できます。

組み込みパケット キャプチャの利点

- デバイスで IPv4 および IPv6 パケットをキャプチャでき、MAC フィルタを使用したり、MAC アドレスをマッチさせたりして、非 IP パケットもキャプチャ可能。
- パケット キャプチャ ポイントを有効にする拡張可能なインフラストラクチャキャプチャ ポイントは、パケットがキャプチャされ、バッファと関連付けられるトラフィック トランジット ポイントです。
- 外部ツールを使用した分析に適したパケットキャプチャファイル (PCAP) 形式でパケット キャプチャをエクスポートする機能。
- さまざまな詳細レベルでキャプチャされたデータ パケットをデコードする方法。

パケット データ キャプチャ

パケット データ キャプチャは、バッファに格納されるデータ パケットのキャプチャです。パケット データ キャプチャは、一意の名前とパラメータを入力することによって定義します。

こうしたキャプチャでは、次のアクションを実行できます。

- インターフェイスでのキャプチャのアクティブ化。
- キャプチャポイントへのアクセスコントロールリスト (ACL) やクラスマップの適用。



(注) Network Based Application Recognition (NBAR) と MAC スタイルのクラスマップは、サポートされていません。

- キャプチャの破棄。
- サイズやタイプなどのバッファストレージパラメータの指定。サイズの範囲は 1 ~ 100 MB です。デフォルトのバッファは線形です。もう 1 つのバッファオプションは循環です。
- プロトコル、IP アドレス、ポートアドレスに関する情報を含む一致基準の指定。

組み込みパケットキャプチャの実装方法

次のセクションでは EPC の導入方法について説明します。

パケットデータキャプチャの管理

バッファモードでパケットデータキャプチャを管理するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 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 access-list access-list-name 例： Device# monitor capture mycap access- list v4acl	アクセスリストをパケットキャプチャのコアフィルタとして指定し、モニタキャプチャを設定します。
ステップ 3	monitor capture capture-name limit duration seconds 例：	モニタキャプチャの制限を設定します。

	コマンドまたはアクション	目的
	<code>Device# monitor capture mycap limit duration 1000</code>	
ステップ 4	monitor capture <i>capture-name</i> interface <i>interface-name</i> both 例： <code>Device# monitor capture mycap interface GigabitEthernet 0/0/1 both</code>	接続ポイントおよびパケット フロー方向を指定して、モニタ キャプチャを設定します。
ステップ 5	monitor capture <i>capture-name</i> buffer circular size <i>bytes</i> 例： <code>Device# monitor capture mycap buffer circular size 10</code>	パケット データをキャプチャするようにバッファを設定します。
ステップ 6	monitor capture <i>capture-name</i> start 例： <code>Device# monitor capture mycap start</code>	トラフィック トレース ポイントでパケットデータのバッファへのキャプチャを開始します。
ステップ 7	monitor capture <i>capture-name</i> stop 例： <code>Device# monitor capture mycap stop</code>	トラフィック トレース ポイントでパケットデータのキャプチャを停止します。
ステップ 8	monitor capture <i>capture-name</i> export <i>file-location/file-name</i> 例： <code>Device# monitor capture mycap export tftp://10.1.88.9/mycap.pcap</code>	分析のためにキャプチャされたデータをエクスポートします。
ステップ 9	end 例： <code>Device# end</code>	特権 EXEC モードに戻ります。

キャプチャされたデータのモニタリングとメンテナンス

キャプチャされたパケットデータのモニタリングとメンテナンスを行うには、次の作業を実行します。キャプチャ バッファの詳細とキャプチャ ポイントの詳細を表示します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	show monitor capture capture-buffer-name buffer dump 例： Device# show monitor capture mycap buffer dump	（任意）キャプチャパケットの 16 進数ダンプおよびそのメタデータを表示します。
ステップ 3	show monitor capture capture-buffer-name parameter 例： Device# show monitor capture mycap parameter	（任意）キャプチャを指定するために使用されたコマンドのリストを表示します。
ステップ 4	debug epc capture-point 例： Device# debug epc capture-point	（任意）パケットキャプチャポイントのデバッグを有効にします。
ステップ 5	debug epc provision 例： Device# debug epc provision	（任意）パケットキャプチャプロビジョニングのデバッグを有効にします。
ステップ 6	end 例： Device(config)# end	特権 EXEC モードに戻ります。

組み込みパケットキャプチャの設定例

例：パケットデータキャプチャの管理

次の例では、パケットデータキャプチャを管理する方法を示します。

```
Device> enable
Device# monitor capture mycap access-list v4acl
Device# monitor capture mycap limit duration 1000
```



```
Device# monitor capture mycap interface GigabitEthernet 0/0/1 both
Device# monitor capture mycap buffer circular size 10
Device# monitor capture mycap start
Device# monitor capture mycap export tftp://10.1.88.9/mycap.pcap
Device# monitor capture mycap stop
Device# end
```

例：キャプチャされたデータのモニタリングとメンテナンス

次の例は、ASCII 形式でパケットをダンプする方法を示しています。

```
Device# show monitor capture mycap buffer dump
Starting the packet display ..... Press Ctrl + Shift + 6 to exit

0
0000: 01005E00 00020000 0C07AC1D 080045C0 ..^.....E.
0010: 00300000 00000111 CFDC091D 0002E000 .0.....
0020: 000207C1 07C1001C 802A0000 10030AFA .....*.....
0030: 1D006369 73636F00 0000091D 0001 ..example.....
1
0000: 01005E00 0002001B 2BF69280 080046C0 ..^.....+.....F.
0010: 00200000 00000102 44170000 0000E000 . .....D.....
0020: 00019404 00001700 E8FF0000 0000 .....
2
0000: 01005E00 0002001B 2BF68680 080045C0 ..^.....+.....E.
0010: 00300000 00000111 CFDB091D 0003E000 .0.....
0020: 000207C1 07C1001C 88B50000 08030A6E .....n
0030: 1D006369 73636F00 0000091D 0001 ..example.....
3
0000: 01005E00 000A001C 0F2EDC00 080045C0 ..^.....E.
0010: 003C0000 00000258 CE7F091D 0004E000 .<.....X.....
0020: 000A0205 F3000000 00000000 00000000 .....
0030: 00000000 00D10001 000C0100 01000000 .....
0040: 000F0004 00080501 0300
```

次の例は、mycap という名前のキャプチャの設定に使用するコマンドのリストを表示する方法を示しています。

```
Device# show monitor capture mycap parameter
monitor capture mycap interface GigabitEthernet 1/0/1 both
monitor capture mycap match any
monitor capture mycap buffer size 10
monitor capture mycap limit pps 1000
```

次の例は、キャプチャ ポイントをデバッグする方法を示しています。

```
Device# debug epc capture-point
EPC capture point operations debugging is on

Device# monitor capture mycap start
*Jun 4 14:17:15.463: EPC CP: Starting the capture cap1
*Jun 4 14:17:15.463: EPC CP: (brief=3, detailed=4, dump=5) = 0
*Jun 4 14:17:15.463: EPC CP: final check before activation
*Jun 4 14:17:15.463: EPC CP: setting up c3pl infra
*Jun 4 14:17:15.463: EPC CP: Setup c3pl acl-class-policy
*Jun 4 14:17:15.463: EPC CP: Creating a class
*Jun 4 14:17:15.464: EPC CP: Creating a class : Successful
*Jun 4 14:17:15.464: EPC CP: class-map Created
*Jun 4 14:17:15.464: EPC CP: creating policy-name epc_policy_cap1
*Jun 4 14:17:15.464: EPC CP: Creating Policy epc_policy_cap1 of type 49 and client type
21
*Jun 4 14:17:15.464: EPC CP: Storing a Policy
```

例：キャプチャされたデータのモニタリングとメンテナンス

```

*Jun 4 14:17:15.464: EPC CP: calling ppm_store_policy with epc_policy
*Jun 4 14:17:15.464: EPC CP: Creating Policy : Successful
*Jun 4 14:17:15.464: EPC CP: policy-map created
*Jun 4 14:17:15.464: EPC CP: creating filter for ANY
*Jun 4 14:17:15.464: EPC CP: Adding acl to class : Successful
*Jun 4 14:17:15.464: EPC CP: Setup c3pl class to policy
*Jun 4 14:17:15.464: EPC CP: Attaching Class to Policy
*Jun 4 14:17:15.464: EPC CP: Attaching epc_class_cap1 to epc_policy_cap1
*Jun 4 14:17:15.464: EPC CP: Attaching Class to Policy : Successful
*Jun 4 14:17:15.464: EPC CP: setting up c3pl qos
*Jun 4 14:17:15.464: EPC CP: DBG> Set packet rate limit to 1000
*Jun 4 14:17:15.464: EPC CP: creating action for policy_map epc_policy_cap1 class_map
epc_class_cap1
*Jun 4 14:17:15.464: EPC CP: DBG> Set packet rate limit to 1000
*Jun 4 14:17:15.464: EPC CP: Activating Interface GigabitEthernet1/0/1 direction both
*Jun 4 14:17:15.464: EPC CP: Id attached 0
*Jun 4 14:17:15.464: EPC CP: inserting into active lists
*Jun 4 14:17:15.464: EPC CP: Id attached 0
*Jun 4 14:17:15.465: EPC CP: inserting into active lists
*Jun 4 14:17:15.465: EPC CP: Activating Vlan
*Jun 4 14:17:15.465: EPC CP: Deleting all temp interfaces
*Jun 4 14:17:15.465: %BUFCAP-6-ENABLE: Capture Point cap1 enabled.
*Jun 4 14:17:15.465: EPC CP: Active Capture 1

Device# monitor capture mycap1 stop
*Jun 4 14:17:31.963: EPC CP: Stopping the capture cap1
*Jun 4 14:17:31.963: EPC CP: Warning: unable to unbind capture cap1
*Jun 4 14:17:31.963: EPC CP: Deactivating policy-map
*Jun 4 14:17:31.963: EPC CP: Policy epc_policy_cap1
*Jun 4 14:17:31.964: EPC CP: Deactivating policy-map Successful
*Jun 4 14:17:31.964: EPC CP: removing provision feature
*Jun 4 14:17:31.964: EPC CP: Found action for policy-map epc_policy_cap1 class-map
epc_class_cap1
*Jun 4 14:17:31.964: EPC CP: cleaning up c3pl infra
*Jun 4 14:17:31.964: EPC CP: Removing Class epc_class_cap1 from Policy
*Jun 4 14:17:31.964: EPC CP: Removing Class from epc_policy_cap1
*Jun 4 14:17:31.964: EPC CP: Successfully removed
*Jun 4 14:17:31.964: EPC CP: Removing acl mac from class
*Jun 4 14:17:31.964: EPC CP: Removing acl from class : Successful
*Jun 4 14:17:31.964: EPC CP: Removing all policies
*Jun 4 14:17:31.964: EPC CP: Removing Policy epc_policy_cap1
*Jun 4 14:17:31.964: EPC CP: Removing Policy : Successful
*Jun 4 14:17:31.964: EPC CP: Removing class epc_class_cap1
*Jun 4 14:17:31.965: EPC CP: Removing class : Successful
*Jun 4 14:17:31.965: %BUFCAP-6-DISABLE: Capture Point cap1 disabled.
*Jun 4 14:17:31.965: EPC CP: Active Capture 0

```

次の例は、組み込みパケットキャプチャ（EPC）のプロビジョニングをデバッグする方法を示しています。

```

Device# debug epc provision
EPC provisioning debugging is on

Device# monitor capture mycap start
*Jun 4 14:17:54.991: EPC PROV: No action found for policy-map epc_policy_cap1 class-map
epc_class_cap1
*Jun 4 14:17:54.991: EPC PROV:
*Jun 4 14:17:54.991: Attempting to install service policy epc_policy_cap1
*Jun 4 14:17:54.992: EPC PROV: Attached service policy to epc idb subblock
*Jun 4 14:17:54.992: EPC PROV: Successful. Create feature object
*Jun 4 14:17:54.992: EPC PROV:
*Jun 4 14:17:54.992: Attempting to install service policy epc_policy_cap1
*Jun 4 14:17:54.992: EPC PROV: Successful. Create feature object
*Jun 4 14:17:54.992: %BUFCAP-6-ENABLE: Capture Point cap1 enabled.

```

```
Device# monitor capture mycap stop
*Jun 4 14:18:02.503: EPC PROV: Successful. Remove feature object
*Jun 4 14:18:02.504: EPC PROV: Successful. Remove feature object
*Jun 4 14:18:02.504: EPC PROV: Destroyed epc idb subblock
*Jun 4 14:18:02.504: EPC PROV: Found action for policy-map epc_policy_cap1 class-map
epc_class_cap1
*Jun 4 14:18:02.504: EPC PROV: Deleting EPC action
*Jun 4 14:18:02.504: EPC PROV: Successful. CLASS_REMOVE, policy-map epc_policy_cap1,
class epc_class_cap1
*Jun 4 14:18:02.504: %BUFCAP-6-DISABLE: Capture Point cap1 disabled.
```

パケットキャプチャ設定の機能履歴と情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 14: パケットキャプチャ設定の機能情報

機能名	リリース	機能情報
パケット キャプチャの設定	Cisco IOS XE Gibraltar 16.10.1	この機能が導入されました。
ダウン状態または管理状態のインターフェイスでの EPC の設定。	Cisco IOS XE Amsterdam 17.2.1	ダウン状態または管理ダウン状態のいずれかのインターフェイスで EPC を設定しても、インターフェイスがアップ状態に変化した後のパケットキャプチャには影響しません。



第 9 章

Flexible NetFlow の設定

- [Flexible NetFlow の前提条件](#) (141 ページ)
- [Flexible Netflow に関する制約事項](#) (142 ページ)
- [Flexible NetFlow に関する情報](#) (144 ページ)
- [Flexible NetFlow の設定方法](#) (163 ページ)
- [Flexible NetFlow の監視](#) (174 ページ)
- [Flexible NetFlow の設定例](#) (174 ページ)
- [Flexible NetFlow の機能情報](#) (177 ページ)

Flexible NetFlow の前提条件

- 次のコマンドで定義される Flexible NetFlow の key フィールドについてよく理解していること。
 - **match flow**
 - **match interface**
 - **match {ipv4 | ipv6}**
 - **match routing**
 - **match transport**
- 次のコマンドで定義される Flexible NetFlow の nonkey フィールドについてよく理解していること。
 - **collect counter**
 - **collect flow**
 - **collect interface**
 - **collect {ipv4 | ipv6}**
 - **collect routing**
 - **collect timestamp sys-uptime**

- **collect transport**

- ネットワーキング デバイスで、Flexible NetFlow がサポートされた Cisco リリースが稼働していること。
- レイヤ 3 ポートチャネル メンバポートの 1 つに適用された Flexible NetFlow 設定は、同じデバイス内の他のすべてのメンバポートにも適用されます。スタックの一部として、または StackWise Virtual を使用して設定されたデバイスの場合、ポートチャネルインターフェイスで Flexible NetFlow を設定することを推奨します。

IPv4 トラフィック

- ネットワーキング デバイスが IPv4 ルーティング用に設定されていること。
- Cisco Express Forwarding または distributed Cisco Express Forwarding のいずれかが、デバイスおよび Flexible NetFlow を有効化するすべてのインターフェイスで有効化されていること。

IPv6 トラフィック

- ネットワーキング デバイスが、IPv6 ルーティング用に設定されていること。
- Cisco Express Forwarding IPv6 または分散型 Cisco Express Forwarding のいずれかが、デバイスおよび Flexible NetFlow を有効化するすべてのインターフェイスで有効化されていること。

Flexible Netflow に関する制約事項

次に、Flexible NetFlow に関する制約事項を示します。

- Flexible NetFlow は、レイヤ 2 ポートチャネル インターフェイスではサポートされませんが、レイヤ 2 ポートチャネル メンバポートではサポートされます。
- Flexible NetFlow は、レイヤ 3 ポートチャネル インターフェイスとメンバポートでサポートされますが、同じトラフィックタイプと方向の両方に対して同時にサポートされることはありません。
- 複数の Flexible NetFlow 設定は、ポートチャネル インターフェイスまたはポートチャネル メンバポートのいずれかでサポートされますが、両方ではサポートされません。
- Traditional NetFlow のアカウンティングはサポートされていません。
- Flexible NetFlow バージョン 9 およびバージョン 10 のエクスポートフォーマットがサポートされています。ただし、エクスポートプロトコルが設定されていない場合は、バージョン 9 のエクスポートフォーマットがデフォルトで適用されます。
- 有線 Application Visibility and Control (AVC) トラフィックの場合、システム上の 1 つ以上のレイヤ 2 またはレイヤ 3 の物理インターフェイスに設定できるフローモニタは 1 つのみです。

- Flexible NetFlow および NBAR は同じインターフェイスで同時に設定できません。
- レイヤ 2、IPv4、および IPv6 のトラフィック タイプがサポートされています。異なるトラフィック タイプの複数のフロー モニタを、指定したインターフェイスと方向に適用できます。同じトラフィック タイプの複数のフロー モニタを指定したインターフェイスと方向には適用できません。
- デバイスはトンネルをサポートしていません。ただし、レイヤ 2、レイヤ 3、VLAN、および SVI インターフェイスがサポートされています。
- スイッチのタイプに応じて、スイッチには 1 個または 2 個の転送 ASIC があります。上の表に示されている容量は、コア単位または ASIC 単位です。
- スイッチにはシングルコア ASIC があり、サポートされる合計フロー数は 16K フロー（入力方向と出力方向ごとに 8K）です。TCAM の制限は、方向ごとに 128 エントリです。
- NetFlow テーブルは個別のコンパートメントにあり、組み合わせることはできません。パケットを処理したコアに応じて、対応したコアのテーブルにフローが作成されます。
- NetFlow ハードウェアの実装では、4 台のハードウェア サンプラーがサポートされています。1/2 ~ 1/1024 のサンプラー レートを選択できます。ランダム サンプリングと確定的サンプリングの両方のモードがサポートされています。
- NetFlow ハードウェアの内部では、ハッシュテーブルが使用されています。ハードウェア内でハッシュ衝突が発生する場合があります。したがって、内部の連想メモリ（CAM）でオーバーフローが発生しても、実際の NetFlow テーブルの使用率は約 80 % しかない場合があります。
- フローに使用されるフィールドによって異なりますが、単一のフローは 2 個の連続したエントリを取得できます。IPv6 フローとデータリンク フローも 2 個のエントリを取得します。この場合、NetFlow エントリを効果的に使用すれば、テーブルサイズの半分で済みます。これは、上記のハッシュ衝突の制限とは別です。
- デバイスは、最大 15 個のフローモニタをサポートしています。
- NetFlow ソフトウェアの実装では、分散 NetFlow エクスポートがサポートされるため、フローが作成された同じデバイスからフローがエクスポートされています。
- 入力フローは最初にフローのパケットを受信した ASIC にあります。出力フローは、パケットが実際にデバイスセットアップを残した ASIC にあります。
- バイトカウントフィールドのレポート値（「bytes long」と呼ばれる）は、レイヤ 2 パケットサイズの 18 バイトです。従来のイーサネットトラフィック（802.3）の場合、これは正確です。他のすべてのイーサネットタイプの場合、このフィールドは正確ではありません。「bytes layer2」フィールドを使用すると、常に正確なレイヤ 2 パケットサイズが報告されます。サポートされる Flexible NetFlow フィールドについては、トピック「Supported Flexible NetFlow Fields」を参照してください。
- AVC フロー モニタの IPFIX エクスポートの設定はサポートされていません。

- Flexible NetFlow エクスポートは、イーサネット管理ポート（GigabitEthernet 0/0）ではサポートされていません。
- フローレコードに送信元グループタグ（SGT）と宛先グループタグ（DGT）のフィールド（またはこの2つのいずれかのフィールド）だけが含まれる場合、両方の値を適用できないとしても、SGT と DGT に値ゼロを設定したフローが作成されます。フローレコードには、SGT および DGT フィールドと一緒に、送信元および宛先 IP アドレスが含まれる必要があります。
- Cisco TrustSec 以外のインターフェイスでは、SGT 値がゼロの場合、コマンドヘッダーがないことを意味します。Cisco TrustSec インターフェイスでは、SGT 値がゼロの場合、不明タグであることを意味します。
- Quality of Service（QoS）のマークが付けられたパケットが入力方向に NetFlow が設定されているインターフェイスで受信されると、パケットの QoS 値が NetFlow コレクタによってキャプチャされます。ただし、パケットが出力方向に NetFlow が設定されているインターフェイスで受信されると、パケットの QoS 値はコレクタによってキャプチャされます。
- IPv6 フローモニタの場合、送信元グループタグ（SGT）フィールドと宛先グループタグ（DGT）フィールドは、MAC アドレスフィールドと共存できません。
- NetFlow レコードは、マルチプロトコルラベルスイッチング対応（MPLS 対応）インターフェイスをサポートしません。
- フローモニタは、レイヤ3物理インターフェイスと論理インターフェイス（レイヤ3ポートチャンネルインターフェイス、レイヤ3ポートチャンネルメンバ、スイッチ仮想インターフェイス（SVI）など）間で共有することはできませんが、論理インターフェイス間またはレイヤ3物理インターフェイス間で共有できます。

Flexible NetFlow に関する情報

ここでは、Flexible Netflow について説明します。

Flexible NetFlow の概要

Flexible NetFlow ではフローを使用して、アカウントリング、ネットワークモニタリング、およびネットワークプランニングに関連する統計情報を提供します。

フローは送信元インターフェイスに届く単方向のパケットストリームで、キーの値は同じです。キーは、パケット内のフィールドを識別する値です。フローを作成するには、フローレコードを使用して、フロー固有のキーを定義します。

デバイスは、ネットワークの変則性とセキュリティの高度な検出を可能にする Flexible NetFlow 機能をサポートします。フレキシブル NetFlow 機能を使用すると、大量の定義済みフィールドの集合からキーを選択することで、そのアプリケーションに最適なフローレコードを定義できます。

1 つのフローと見なされるパケットでは、すべてのキー値が一致している必要があります。フローは、設定したエクスポートレコードバージョンに基づいて、関係のある他のフィールドを集めることもあります。フローは Flexible NetFlow キャッシュに格納されます。

エクスポートを使用して Flexible NetFlow がフローのために収集するデータをエクスポートし、Flexible NetFlow コレクタなどのリモートシステムにこのデータをエクスポートできます。Flexible NetFlow コレクタは、IPv4 アドレスを使用できます。

モニタを使用してフローのために収集するデータのサイズを定義します。モニタで、フローレコードおよびエクスポートを Flexible NetFlow キャッシュ情報と結合します。

Cisco IOS XE 16.12.1 リリース以降、Flexible NetFlow 上の送信元グループタグ (SGT) および宛先グループタグ (DGT) フィールドは、IPv6 トラフィックでサポートされます。

以前の NetFlow と Flexible NetFlow の利点

Flexible NetFlow ではフローをユーザが定義できます。次に、Flexible NetFlow の利点を示します。

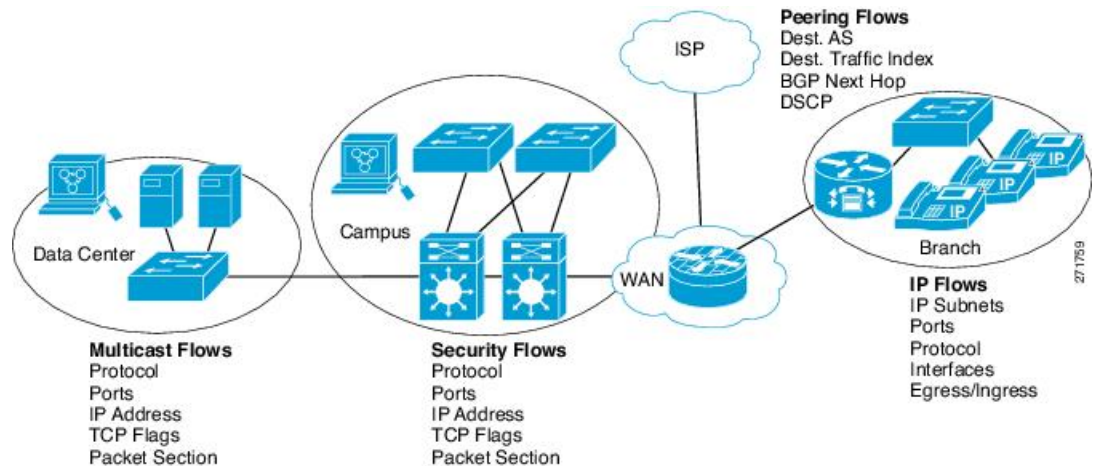
- スケーラビリティ、フロー情報の集約などの、大容量フロー認識。
- セキュリティの監視と dDoS の検出および識別のための拡張されたフローインフラストラクチャ。
- フロー情報をネットワーク内の特定のサービスまたはオペレーションに適応させるパケットからの新しい情報。利用できるフロー情報は、Flexible NetFlow ユーザがカスタマイズ可能。
- Cisco の柔軟で拡張可能な NetFlow Version 9 の活用。
- IP アカウンティング、ボーダー ゲートウェイ プロトコル (BGP) ポリシー アカウンティング、永続的キャッシュなどの多数のアカウント機能置換のために使用できる包括的な IP アカウンティング機能。

Flexible NetFlow では、ネットワークの動作を、ネットワーク内で使用されるさまざまなサービスに合わせた特定のフロー情報とともに、より効率的に理解できます。次に、Flexible NetFlow 機能用の適用例を示します。

- Flexible NetFlow は Cisco NetFlow をセキュリティ監視ツールとして拡張します。たとえば、ユーザがネットワーク内で特定のタイプの攻撃を検索できるように、パケット長や MAC アドレスのために新しいフロー キーを定義することができます。
- Flexible NetFlow を使用すると、TCP アプリケーションまたは UDP アプリケーションをパケット内のサービスクラス (CoS) ごとに明確に追跡することによって、ホスト間で送信されるアプリケーショントラフィックの量を迅速に識別できます。
- サービスクラスごとに各ネクストホップのマルチプロトコルラベルスイッチング (MPLS) か IP コア ネットワーク、およびその宛先を入力するトラフィックのアカウント機能。この機能では、エッジ間のトラフィックマトリクスを構築できます。

次の表に、Flexible NetFlow をネットワークに導入する方法の例を示します。

図 8: Flexible NetFlow の通常の導入



Flexible NetFlow のコンポーネント

Flexible NetFlow は、いくつかのバリエーションと一緒に使用して、トラフィック分析およびデータ エクスポートに使用できるコンポーネントで構成されます。Flexible NetFlow のユーザ定義のフローレコードおよびコンポーネントの構造では、最小限の数のコンフィギュレーション コマンドで、ネットワーク デバイスでのトラフィック分析およびデータ エクスポートのためのさまざまなコンフィギュレーションの作成が容易になります。各フロー モニタに、フローレコード、フロー エクスポータ、および キャッシュ タイプの固有の組み合わせを設定できます。フロー エクスポータの宛先 IP アドレスなどのパラメータを変更する場合、フロー エクスポータを使用するすべてのフロー モニタに対して自動的に変更されます。同じフロー モニタを複数のフロー サンプラと組み合わせると、さまざまなインターフェイス上でさまざまな速度の同じタイプのネットワークトラフィックをサンプリングできます。ここでは、Flexible NetFlow コンポーネントのその他の情報を提供します。

フローレコード

Flexible NetFlow では、キー フィールドと非キー フィールドの組み合わせをレコードと呼びます。Flexible NetFlow のレコードは Flexible NetFlow フロー モニタに割り当てられ、フロー データの格納に使用されるキャッシュが定義されます。Flexible NetFlow には、Flexible NetFlow の使用を開始する際に役立ついくつかの事前定義済みのレコードが含まれています。

フローレコードでは、フロー内のパケットを識別するために Flexible NetFlow で使用するキーとともに、Flexible NetFlow がフローについて収集する他の関連フィールドを定義します。キーと関連フィールドを任意の組み合わせで指定して、フローレコードを定義できます。デバイスは、幅広いキーセットをサポートします。フローレコードでは、フロー単位で収集するカウンタのタイプも定義します。64 ビットのパケットまたはバイトカウンタを設定できます。デバイスは、フローレコードの作成時に、デフォルトとして次の match フィールドを有効にします。

- **match datalink**— レイヤ 2 属性

- **match flow direction**— フローの方向を識別するフィールドとの一致を指定します。
- **match interface**— インターフェイス属性
- **match ipv4**— IPv4 属性
- **match ipv6**— IPv6 属性
- **match transport** : トランスポート層フィールド
- **match flow cts**— Cisco TrustSec フィールド

NetFlow の事前定義済みのレコード

Flexible NetFlow には事前定義済みのレコードがいくつか含まれ、それを使用してネットワークトラフィックの監視を開始できます。事前定義済みのレコードは、Flexible NetFlow を迅速に導入するために役立ち、ユーザ定義のフローレコードよりも簡単に使用できます。ネットワークモニタリングのニーズを満たす定義済みのレコードのリストから選択できます。Flexible NetFlow が改良されると、一般的なユーザ定義のフローレコードを事前定義済みレコードとして使用でき、簡単に導入できるようになります。



(注) 事前定義されたレコードは、Cisco Catalyst 9000 シリーズスイッチの通常の Flexible NetFlow ではサポートされません。

ユーザ定義レコード

Flexible NetFlow では、**key** および **nonkey** フィールドを指定し、実際の要件に合わせてデータ収集をカスタマイズすることで、Flexible NetFlow フローモニタキャッシュ用の独自のレコードを定義できます。Flexible NetFlow フローモニタキャッシュに対して独自のレコードを定義する場合、ユーザ定義レコードと呼ばれます。**nonkey** フィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。**nonkey** フィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、**nonkey** フィールドの値はフロー内の最初のパケットからのみ取得されます。Flexible NetFlow を使用すると、**nonkey** フィールドとして、フロー内のバイト数やパケット数などのカウンター値をキャプチャできます。

ユーザ定義レコードは、QoS および帯域幅監視、アプリケーションとユーザのトラフィックプロファイリング、dDoS 攻撃に対するセキュリティ監視などのアプリケーション用に作成できます。Flexible NetFlow のユーザ定義レコードでは、ユーザが設定可能なサイズのパケットの連続するセクションを監視する機能を利用でき、**key** フィールドまたは **nonkey** フィールドとしてパケットのその他のフィールドや属性とともにフローレコード内で使用します。セクションにはパケットのレイヤ3データが含まれる場合があります。パケットフィールドの分析機能によって、さらに詳細なトラフィック監視が可能になるため、dDoS 攻撃の調査に役立ち、URL 監視など他のセキュリティアプリケーションの実装が可能になります。

bytes 値は、フローレコードのこれらのフィールドのサイズ (バイト単位) です。パケットの対応フラグメントが要求されたセクションサイズよりも小さい場合、Flexible NetFlow はフロー

レコード内の残りのセクションフィールドを 0 で埋めます。パケットタイプが要求されたセクションタイプと一致しなかった場合、Flexible NetFlow はフローレコード内のセクションフィールド全体を 0 で埋めます。

Flexible NetFlow では、ヘッダーおよびパケットセクションのタイプに新しいバージョン 9 エクスポートフォーマットフィールドタイプが追加されます。Flexible NetFlow は NetFlow コレクタに、対応するバージョン 9 エクスポートテンプレートフィールドで設定されたセクションサイズを通知します。ペイロードセクションには、対応する長さフィールドがあり、収集されるセクションの実際のサイズを収集するために使用できます。

Flexible NetFlow の match パラメータ

次の表で、Flexible NetFlow の match パラメータについて説明します。フローレコードごとに、次の match パラメータを 1 つ以上設定する必要があります。

表 15: match パラメータ

コマンド	目的
match datalink {dot1q ethertype mac vlan }	データリンクまたはレイヤ 2 フィールドとの一致を指定します。次のコマンドオプションが使用可能です。 <ul style="list-style-type: none"> • dot1q : dot1q フィールドと一致します。 • ethertype : パケットの ethertype と一致します。 • mac : 送信元または宛先の MAC フィールドと一致します。 • vlan : パケットが配置される VLAN と一致します (入力または出力)。
match flow direction	フローを識別するフィールドとの一致を指定します。
match interface {input output}	インターフェイスフィールドとの一致を指定します。次のコマンドオプションが使用可能です。 <ul style="list-style-type: none"> • input : 入力インターフェイスと一致します。 • output : 出力インターフェイスと一致します。

コマンド	目的
match ipv4 { destination protocol source tos ttl version }	<p>IPv4 フィールドとの一致を指定します。次のコマンド オプションが使用可能です。</p> <ul style="list-style-type: none"> • destination : IPv4 宛先アドレス ベースのフィールドと一致します。 • protocol : IPv4 プロトコルと一致します。 • source : IPv4 送信元アドレス ベースのフィールドと一致します。 • tos : IPv4 タイプ オブ サービス フィールドと一致します。 • ttl : IPv4 存続時間フィールドと一致します。 • version : IPv4 ヘッダーの IP バージョンと一致します。
match ipv6 { destination hop-limit protocol source traffic-class version }	<p>IPv6 フィールドとの一致を指定します。次のコマンド オプションが使用可能です。</p> <ul style="list-style-type: none"> • destination : IPv6 宛先アドレス ベースのフィールドと一致します。 • hop-limit : IPv6 ホップリミットフィールドと一致します。 • protocol : IPv6 ペイロードプロトコルフィールドと一致します。 • source : IPv6 送信元アドレス ベースのフィールドと一致します。 • traffic-class : IPv6 トラフィック クラスと一致します。 • version : IPv6 ヘッダーの IP バージョンと一致します。

コマンド	目的
match transport { destination-port igmp icmp source-port }	<p>トランスポート層フィールドとの一致を指定します。次のコマンドオプションが使用可能です。</p> <ul style="list-style-type: none"> • destination-port : 転送先ポートと一致します。 • icmp : ICMP IPv4 および IPv6 フィールドを含む ICMP フィールドと一致します。 • igmp : IGMP フィールドと一致します。 • source-port : 転送元ポートと一致します。

Flexible NetFlow の collect パラメータ

次の表で、Flexible NetFlow の collect パラメータについて説明します。

表 16: collect パラメータ

コマンド	目的
collect counter { bytes { layer2 { long } long } packets { long } }	カウンタ フィールドの合計バイト数と合計パケット数を収集します。
collect interface { input output }	入力または出力インターフェイスからフィールドを収集します。
collect timestamp absolute { first last }	最初のパケットが確認された絶対時間、または最新のパケットが最後に確認された絶対時間のフィールドを収集します (ミリ秒)。

コマンド	目的
collect transport tcp flags	<p>次の転送 TCP フラグを収集します。</p> <ul style="list-style-type: none"> • ack : TCP 確認応答フラグ • cwr : TCP 輻輳ウィンドウ縮小フラグ • ece : TCP ECN エコー フラグ • fin : TCP 終了フラグ • psh : TCP プッシュ フラグ • rst : TCP リセット フラグ • syn : TCP 同期フラグ • urg : TCP 緊急フラグ <p>(注) デバイスでは、収集する TCP フラグを指定できません。転送 TCP フラグの収集のみ指定できます。すべての TCP フラグはこのコマンドで収集されます。</p>
collect counter bytes	フローの確認されたバイト数を非キー フィールドとして設定し、フローの合計バイト数を収集します。
collect counter packets	フローで確認されるパケット数を非キーフィールドとして設定し、フローから合計パケット数を収集します。

フロー エクスポート

フローエクスポートでは、フロー モニタ キャッシュ内のデータをリモートシステム（たとえば、分析および保管のために NetFlow コレクタを実行するサーバ）にエクスポートします。フローエクスポートは、コンフィギュレーションで別のエンティティとして作成されます。フローエクスポートは、フローモニタにデータエクスポート機能を提供するためにフローモニタに割り当てられます。複数のフローエクスポートを作成して、1つまたは複数のフローモニタに適用すると、いくつかのエクスポート先を指定することができます。1つのフローエクスポートを作成し、いくつかのフローモニタに適用することができます。

NetFlow データ エクスポート フォーマットのバージョン 9

NetFlow の基本出力はフローレコードです。NetFlow が改良され、フローレコードのいくつかのフォーマットが向上しました。NetFlow エクスポート フォーマットの最新の進化は、バージョン 9 と呼ばれます。NetFlow Version 9 エクスポート フォーマットの識別機能は、テンプレートがベースとなります。テンプレートは、レコードフォーマットの設計を拡張可能なもの

にします。NetFlow サービスが将来拡張されても、基本フローレコードフォーマットを変更し続ける必要がありません。テンプレートを使用すると、次のいくつかの利点があります。

- NetFlow のコレクタを提供したり、サービスを表示したりするアプリケーションを作成するサードパーティ ビジネス パートナーは、新規の NetFlow 機能が追加されるたびにアプリケーションを再コンパイルする必要はありません。代わりに、既知のテンプレートフォーマットを記述する外部のデータ ファイルを使用することができます。
- 新規機能は、現在の導入環境を損ねることなく、NetFlow に迅速に追加できます。
- バージョン9フォーマットは新しいプロトコルや開発中のプロトコルに適応できるため、NetFlow はこれらのプロトコルに対して「将来的に対応」します。

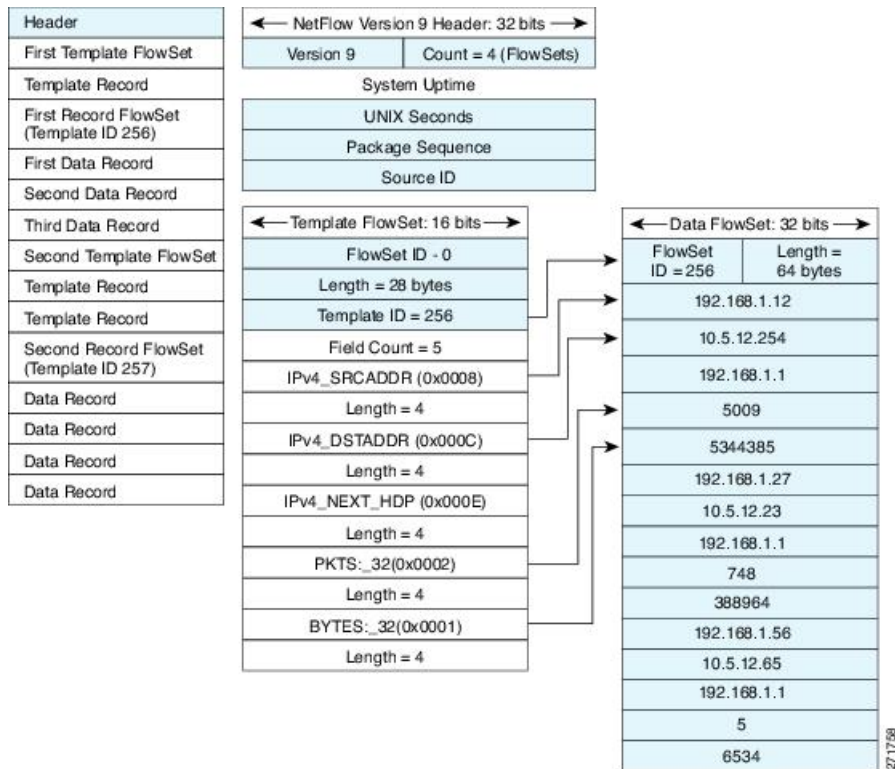
バージョン9のエクスポートフォーマットは、パケットヘッダーとそれに続く1つ以上のテンプレートフローセットまたはデータフローセットで構成されています。テンプレートフローセットでは、将来のデータフローセットに表示されるフィールドの説明が提供されます。このようなデータフローセットは、後で同じエクスポートパケットまたは後続のエクスポートパケットで発生する可能性があります。テンプレートフローセットおよびデータフローセットは、次の図に示すように、単一のエクスポートパケットに混在させることができます。

図9:バージョン9エクスポートパケット



NetFlow Version 9 では、送信されるデータを NetFlow コレクタが理解できるように、テンプレートデータを定期的にはエクスポートします。また、テンプレートのデータフローセットもエクスポートします。Flexible NetFlow の主な利点は、ユーザがフローレコードを設定すると、バージョン9テンプレートに効率的に変換され、コレクタに転送されることです。下の図に、ヘッダー、テンプレートフローセットおよびデータフローセットを含めて、NetFlow Version 9 エクスポートフォーマットの詳細な例を示します。

図 10: NetFlow バージョン 9 エクスポート フォーマットの詳細例



バージョン 9 エクスポート フォーマットの詳細については、ホワイト ペーパー『Cisco IOS NetFlow Version 9 Flow-Record Format』を参照してください。次の URL から入手できます。
http://www.cisco.com/en/US/tech/tk648/tk362/technologies_white_paper09186a00800a3db9.shtml

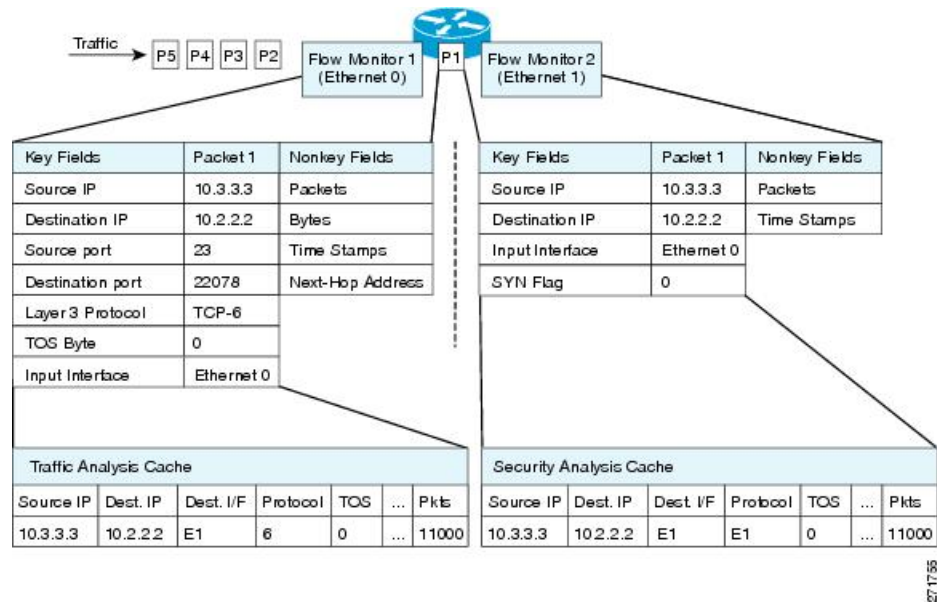
フロー モニタ

フロー モニタは Flexible NetFlow のネットワーク トラフィックの監視を実行するコンポーネントで、インターフェイスに適用されます。

フロー データはネットワーク トラフィックから収集され、フロー レコードの key フィールドおよび nonkey フィールドに基づいて監視プロセス中にフロー モニタ キャッシュに追加されます。

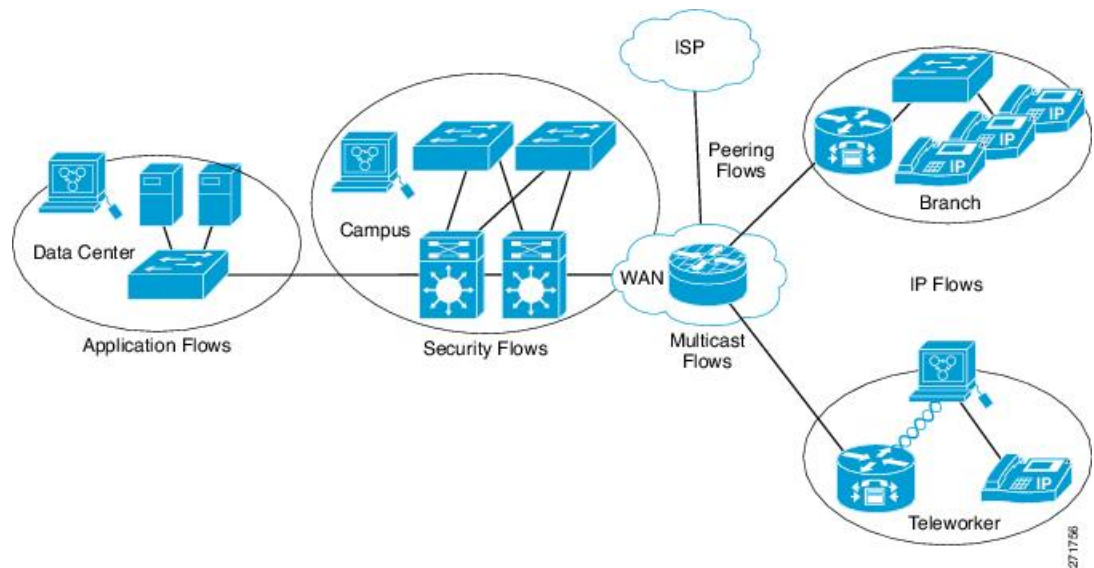
Flexible NetFlow は、同じトラフィックのさまざまなタイプの分析を実行するために使用できます。下の図では、入力インターフェイス上の標準トラフィック分析のために設計されたレコードと、出力インターフェイス上のセキュリティ分析のために設計されたレコードを使用してパケット 1 が分析されます。

図 11: 2つのフロー モニタを使用した同じトラフィックの分析例



下の図に、カスタム レコードを使用して複数のタイプのフロー モニタを適用するより複雑な方法の例を示します。

図 12: カスタム レコードでの複数のタイプのフロー モニタの複雑な使用例



標準

デフォルトのキャッシュタイプは「normal」です。このモードでは、キャッシュ内のエントリが timeout active 設定と timeout inactive 設定に従って期限切れになります。キャッシュ エントリは、期限切れになるとキャッシュから削除され、設定されている何らかのエクスポートによってエクスポートされます。

フロー サンプラー

フローサンプラーは、ルータのコンフィギュレーションで別のコンポーネントとして作成されます。フローサンプラーは、分析用に選択されるパケットの数を制限することで、Flexible NetFlow を実行しているデバイス上の負荷を減らすために使用されます。

フロー サンプリングでは、ルータのパフォーマンスに対するモニタリング精度が交換されます。サンプラーをフロー モニタに適用すると、フロー モニタが分析する必要のあるパケット数が減少するため、ルータでフロー モニタを実行するためのオーバーヘッド負荷が低下します。フロー モニタで分析されるパケット数が減少すると、フロー モニタのキャッシュに格納される情報の精度が、それに応じて低下します。

ip flow monitor コマンドを使用してインターフェイスに適用される場合、サンプラーはフロー モニタと組み合わせて使用されます。

サポートされている Flexible NetFlow フィールド

次の表では、さまざまなトラフィックタイプおよびトラフィック方向について、Flexible NetFlow (FNF) でサポートされるフィールドの統合リストを提供しています。



(注) パケットに VLAN フィールドがある場合、その長さは考慮されません。

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPv4 Out	IPv6 In	IPv6 Out	注意
Key または Collect フィールド							

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPv4 Out	IPv6 In	IPv6 Out	注意
インターフェイス入力	対応	—	対応	—	対応	—	<p>フロー モニタを入力方向に適用する場合：</p> <ul style="list-style-type: none"> • match キーワードを使用し、入力インターフェイスを key フィールドとして使用します。 • collect キーワードを使用し、出力インターフェイスを collect フィールドとして使用します。このフィールドはエクスポートされるレコードに含まれますが、値は0になります。
インターフェイス出力	—	対応	—	対応	—	対応	<p>フロー モニタを出力方向に適用する場合：</p> <ul style="list-style-type: none"> • match キーワードを使用し、出力インターフェイスを key フィールドとして使用します。 • collect キーワードを使用し、入力インターフェイスを collect フィールドとして使用します。このフィールドはエクスポートされるレコードに含まれますが、値は0になります。
フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPv4 Out	IPv6 In	IPv6 Out	注意
Key フィールド							

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPv4 Out	IPv6 In	IPv6 Out	注意
フロー方向	対応	対応	対応	対応	対応	対応	
Ethertype	対応	対応	—	—	—	—	
VLAN 入力	対応	—	対応	—	対応	—	スイッチポートでのみサポートされています。
VLAN 出力	—	対応	—	対応	—	対応	スイッチポートでのみサポートされています。
dot1q VLAN 入力	対応	—	対応	—	対応	—	スイッチポートでのみサポートされています。
dot1q VLAN 出力	—	対応	—	対応	—	対応	スイッチポートでのみサポートされています。
dot1q 優先度	対応	対応	対応	対応	対応	対応	スイッチポートでのみサポートされています。
MAC 送信元アドレス入力	対応	対応	対応	対応	対応	対応	

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPv4 Out	IPv6 In	IPv6 Out	注意
MAC 送信元アドレス出力	—	—	—	—	—	—	
MAC 宛先アドレス入力	対応	—	対応	—	対応	—	
MAC 送信先アドレス出力	—	対応	—	対応	—	対応	
IPv4 バージョン	—	—	対応	対応	対応	対応	
IPv4 TOS	—	—	対応	対応	対応	対応	
IPv4 プロトコル	—	—	対応	対応	対応	対応	送信元/宛先ポート、ICMP コード/タイプ、IGMP タイプ、TCP フラグのいずれかが使用されている場合に使用する必要があります。
IPv4 TTL	—	—	対応	対応	対応	対応	
IPv4 TTL	—	—	対応	対応	対応	対応	IPv4 TTL と同じです。

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPv4 Out	IPv6 In	IPv6 Out	注意
IPv4 プロトコル	—	—	対応	対応	対応	対応	IPv4 プロトコルと同じです。送信元/宛先ポート、ICMP コード/タイプ、IGMP タイプ、TCP フラグのいずれかが使用されている場合に使用する必要があります。
IPv4 発信元アドレス	—	—	対応	対応	—	—	
IPv4 宛先アドレス	—	—	対応	対応	—	—	
ICMP IPv4 タイプ	—	—	対応	対応	—	—	
ICMP IPv4 コード	—	—	対応	対応	—	—	
IGMP タイプ	—	—	対応	対応	—	—	
フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPv4 Out	IPv6 In	IPv6 Out	注意
Key フィールド (続き)							

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPv4 Out	IPv6 In	IPv6 Out	注意
IPv6 バージョン	—	—	対応	対応	対応	対応	IP バージョンと同じです。
IPv6 プロトコル	—	—	対応	対応	対応	対応	IP プロトコルと同じです。送信元/宛先ポート、ICMP コード/タイプ、IGMP タイプ、TCP フラグのいずれかが使用されている場合に使用する必要があります。
IPv6 送信元アドレス	—	—	—	—	対応	対応	
IPv6 宛先アドレス	—	—	—	—	対応	対応	
IPv6 トラフィッククラス	—	—	対応	対応	対応	対応	IP TOS と同じです。
IPv6 ホップリミット	—	—	対応	対応	対応	対応	IP TTL と同じです。
ICMP IPv6 タイプ	—	—	—	—	対応	対応	
ICMP IPv6 コード	—	—	—	—	対応	対応	

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPv4 Out	IPv6 In	IPv6 Out	注意
source-port	—	—	対応	対応	対応	対応	
dest-port	—	—	対応	対応	対応	対応	
フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPv4 Out	IPv6 In	IPv6 Out	注意
Collect フィールド							
バイト長	対応	対応	対応	対応	対応	対応	パケットサイズ = (FCS を含むイーサネットフレームサイズ - 18 バイト) 推奨 : このフィールドを回避し、Bytes layer2 long を使用します。
パケット長	対応	対応	対応	対応	対応	対応	
Timestamp absolute first	対応	対応	対応	対応	対応	対応	
Timestamp absolute last	対応	対応	対応	対応	対応	対応	
TCP フラグ	対応	対応	対応	対応	対応	対応	すべてのフラグを収集します。

フィールド	レイヤ 2 In	レイヤ 2 Out	IPv4 In	IPv4 Out	IPv6 In	IPv6 Out	注意
Bytes layer2 long	対応	対応	対応	対応	対応	対応	

デフォルト設定

次の表は、デバイスに対する Flexible NetFlow のデフォルト設定を示します。

表 17: デフォルトの *Flexible NetFlow* 設定

設定	デフォルト
フロー アクティブ タイムアウト	1800 秒
フロー タイムアウトの非アクティブ化	15 秒

Autonomous System Number

自律システム番号スペースは、4,294,967,296 個の一意的な値を持つ 32 ビットのフィールドで、インターネットのパブリックドメイン間ルーティングシステムをサポートするために使用できます。

自律システム番号 (AS 番号) は、主にボーダー ゲートウェイ プロトコルで使用される IANA によって割り当てられる特別な番号です。一意のルーティングポリシーを持つ単一の技術管理下にあるネットワーク、またはパブリックインターネットにマルチホーム接続されているネットワークを一意的に識別します。この自律システム番号は、ピアリングポイントのインターネット サービスプロバイダーとインターネット エクスチェンジ (IX) の間で、BGP およびピアをインターネット サービスプロバイダーと実行するために必要です。AS 番号はグローバルに一意的である必要があります。これにより、BGP が検出してルーティングできる一意の場所から IP アドレスブロックが送信されるようになります。BGP は、プレフィックスと自律システムパス (AS パス) を使用して、プレフィックスが存在する宛先への最短パスを決定します。

NetFlow V9 および IPFIX エクスポートタイプは、32 ビット AS 番号をサポートします。NetFlow V5 は、固定 16 ビットの送信元および宛先 AS 形式に従うため、この 32 AS フィールドをサポートしません。

NetFlow では、次の BGP パラメータをエクスポートできます。

- BGP 送信元起源またはピア AS 番号
- BGP 宛先起源またはピア AS 番号

設定

AS 番号システムを設定するには、次のコマンドを使用します。

```
[no] collect routing { destination | source } as [[4-octet] peer] [4-octet]
```

Flexible NetFlow の設定方法

Flexible Netflow を設定するには、次の一般的な手順に従います。

1. フローにキー フィールドおよび非キー フィールドを指定して、フロー レコードを作成します。
2. プロトコルを指定して任意のフロー エクスポートを作成し、宛先ポート、宛先、およびその他のパラメータを転送します。
3. フロー レコードおよびフロー エクスポートに基づいて、フロー モニタを作成します。
4. 任意のサンプラーを作成します。
5. レイヤ 2 ポート、レイヤ 3 ポート、または VLAN にフロー モニタを適用します。

フロー レコードの作成

カスタマイズしたフロー レコードを設定するには、次のタスクを実行します。

カスタマイズしたフロー レコードは、特定の目的でトラフィック データを分析するために使用します。カスタマイズしたフロー レコードには、key フィールドとして使用する **match** 基準が 1 つ以上必要です。通常は **nonkey** フィールドとして使用する **collect** 基準が 1 つ以上あります。

カスタマイズしたフロー レコードの順列は、数百もの可能性があります。このタスクでは、可能性のある順列の 1 つを作成するための手順について説明します。必要に応じて当該タスクの手順を変更し、要件に合わせてカスタマイズしたフロー レコードを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • 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： Device# 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	flow record <i>record-name</i> 例 : <pre>Device(config)# flow record FLOW-RECORD-1</pre>	フロー レコードを作成し、Flexible NetFlow フロー レコード コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> このコマンドでは、既存のフロー レコードを変更することもできます。
ステップ 4	description <i>description</i> 例 : <pre>Device(config-flow-record)# description Used for basic traffic analysis</pre>	(任意) フロー レコードの説明を作成します。
ステップ 5	match {ip ipv6} {destination source} address 例 : <pre>Device(config-flow-record)# match ipv4 destination address</pre>	(注) この例では、IPv4 宛先アドレスをレコードの key フィールドとして設定します。
ステップ 6	必要に応じてステップ 5 を繰り返し、レコードの追加 key フィールドを設定します。	—
ステップ 7	end 例 : <pre>Device(config-flow-record)# end</pre>	Flexible NetFlow フロー レコード コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。
ステップ 8	show flow record <i>record-name</i> 例 : <pre>Device# show flow record FLOW_RECORD-1</pre>	(任意) 指定したフロー レコードの現在のステータスが表示されます。
ステップ 9	show running-config flow record <i>record-name</i> 例 : <pre>Device# show running-config flow record FLOW_RECORD-1</pre>	(任意) 指定したフロー レコードの設定が表示されます。

フロー エクスポートの作成

フロー エクスポートを作成して、フローのエクスポート パラメータを定義できます。



(注) フローエクスポートごとに、1つの宛先のみがサポートされます。複数の宛先にデータをエクスポートする場合は、複数のフローエクスポートを設定してフロー モニタに割り当てる必要があります。

IPv4 アドレスを使用して宛先にエクスポートできます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • 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： Device(config)# 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	flow exporter name 例： Device(config)# flow exporter ExportTest	フローエクスポートを作成し、フローエクスポ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 4	description string 例： Device(config-flow-exporter)# description ExportV9	(任意) 最大63文字で、このフローの説明を指定します。
ステップ 5	destination {ipv4-address} 例： Device(config-flow-exporter)# destination 192.0.2.1 (IPv4 destination)	このエクスポートに IPv4 宛先アドレスまたはホスト名を設定します。
ステップ 6	dscp value 例： Device(config-flow-exporter)# dscp 0	(任意) DSCP (DiffServ コードポイント) 値を指定します。範囲は0～63です。デフォルトは0です。

	コマンドまたはアクション	目的
ステップ 7	source { <i>ip</i> } 例 : Device(config-flow-exporter) # source gigabitEthernet1/0/1	(任意) 設定された宛先で NetFlow コネクタに到達するために使用するインターフェイスを指定します。送信元として次のインターフェイスを設定できます。
ステップ 8	transport udp <i>number</i> 例 : Device(config-flow-exporter) # transport udp 200	(任意) NetFlow コレクタに到達するために使用する UDP ポートを指定します。
ステップ 9	ttl <i>seconds</i> 例 : Device(config-flow-exporter) # ttl 210	(任意) エクスポートによって送信されるデータグラムの存続可能時間 (TTL) 値を設定します。範囲は 1 ~ 255 秒です。デフォルトは 255 です。
ステップ 10	export-protocol { <i>netflow-v9</i> } 例 : Device(config-flow-exporter) # export-protocol netflow-v9	エクスポートで使用する NetFlow エクスポートプロトコルのバージョンを指定します。
ステップ 11	end 例 : Device(config-flow-exporter) # end	特権 EXEC モードに戻ります。
ステップ 12	show flow exporter [<i>name record-name</i>] 例 : Device# show flow exporter ExportTest	(任意) NetFlow のフロー エクスポート情報を表示します。
ステップ 13	copy running-config startup-config 例 : Device# 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。

次のタスク

フロー レコードおよびフロー エクスポートに基づいて、フロー モニタを定義します。

カスタマイズしたフロー モニタの作成

カスタマイズしたフロー モニタを作成するには、この必須のタスクを実行します。

各フロー モニタには、専用のキャッシュが割り当てられています。フロー モニタごとに、キャッシュエントリの内容およびレイアウトを定義するレコードが必要です。これらのレコードフォーマットは、事前定義済みのレコードフォーマットのいずれか、またはユーザ定義にすることができます。上級のユーザであれば **flow record** コマンドを使用して、カスタマイズしたフォーマットを作成することもできます。

始める前に

Flexible NetFlow の事前定義済みレコードの代わりにカスタマイズしたレコードを使用する場合は、このタスクを実行する前に、カスタマイズしたレコードを作成する必要があります。データをエクスポートするためにフロー エクスポートをフロー モニタに追加する場合は、このタスクを完了する前にエクスポートを作成する必要があります。



- (注) フローモニタで **record** コマンドのパラメータを変更する前に、**no ip flow monitor** コマンドを使用して、すべてのインターフェイスから適用済みのフローモニタを削除する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • 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： Device# 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	flow monitor monitor-name 例： Device(config)# flow monitor FLOW-MONITOR-1	フロー モニタを作成し、Flexible NetFlow フロー モニタ コンフィギュレーション モードを開始します。 • このコマンドでは、既存のフロー モニタを変更することもできません。
ステップ 4	description description 例：	(任意) フローモニタの説明を作成します。

	コマンドまたはアクション	目的
	Device(config-flow-monitor)# description Used for basic ipv4 traffic analysis	
ステップ 5	record { <i>record-name</i> netflow-original netflow { ipv4 ipv6 } <i>record</i> [<i>peer</i>]} 例 : Device(config-flow-monitor)# record FLOW-RECORD-1	フロー モニタのレコードを指定しま す。
ステップ 6	cache { timeout { active inactive update } <i>seconds</i> type normal } 例 : Device(config-flow-monitor)# cache type normal Device(config-flow-monitor)# cache timeout active	(任意) フロー モニタ キャッシュ パ ラメータ (タイムアウト値、キャッ シュタイプなど) を変更します。指定 したフロー モニタとフロー キャッシュ を関連付けます。
ステップ 7	必要に応じてステップ 6 を繰り返して、このフロー モニタのキャッシュ パ ラメータの変更を完了します。	—
ステップ 8	statistics packet protocol 例 : Device(config-flow-monitor)# statistics packet protocol	(任意) Flexible NetFlow モニタのプロ トコル分散統計情報の収集をイネー ブルにします。
ステップ 9	statistics packet size 例 : Device(config-flow-monitor)# statistics packet size	(任意) Flexible NetFlow モニタのサイ ズ分散統計情報の収集をイネーブルに します。
ステップ 10	exporter exporter-name 例 : Device(config-flow-monitor)# exporter EXPORTER-1	(任意) 事前に作成されたエクスポー タの名前を指定します。
ステップ 11	end 例 : Device(config-flow-monitor)# end	Flexible NetFlow フロー モニタ コンフィ ギュレーションモードを終了して、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 flow monitor [[name] <i>monitor-name</i>] [cache [format {csv record table}]] [statistics]] 例 : Device# show flow monitor FLOW-MONITOR-2 cache	(任意) Flexible NetFlow フロー モニタのステータスおよび統計情報が表示されます。
ステップ 13	show running-config flow monitor <i>monitor-name</i> 例 : Device# show running-config flow monitor FLOW_MONITOR-1	(任意) 指定したフローモニタの設定が表示されます。
ステップ 14	copy running-config startup-config 例 : Device# 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。

フローサンプラーの作成

フロー サンプラーを設定して有効化するには、この必須のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> 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 : Device# 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	sampler <i>sampler-name</i> 例 : Device(config)# sampler SAMPLER-1	サンプラーを作成し、サンプラーコンフィギュレーションモードを開始します。 <ul style="list-style-type: none"> このコマンドでは、既存のサンプラーを変更することもできます。

	コマンドまたはアクション	目的
ステップ 4	description <i>description</i> 例 : Device(config-sampler)# description Sample at 50%	(任意) フローサンプラーの説明を作成します。
ステップ 5	mode {random} 1 out-of <i>window-size</i> 例 : Device(config-sampler)# mode random 1 out-of 2	サンプラーモードおよびフローサンプラーのウィンドウ サイズを指定します。 • <i>window-size</i> 引数の範囲は、0 ~ 1024 です。
ステップ 6	exit 例 : Device(config-sampler)# exit	サンプラー 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	interface <i>type number</i> 例 : Device(config)# interface GigabitEthernet 0/0/0	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 8	{ip ipv6} flow monitor <i>monitor-name</i> [[sampler] <i>sampler-name</i>] { input output } 例 : Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input	作成したフローモニタおよびフローサンプラーをインターフェイスに割り当て、サンプリングをイネーブルにします。
ステップ 9	end 例 : Device(config-if)# end	インターフェイス コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。
ステップ 10	show sampler <i>sampler-name</i> 例 : Device# show sampler SAMPLER-1	設定し有効化したフローサンプラーのステータスおよび統計情報を表示します。

インターフェイスへのフローの適用

フロー モニタおよびオプションのサンプラーをインターフェイスに適用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • 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： Device(config)# 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 type 例： Device(config)# interface GigabitEthernet1/0/1	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、インターフェイスを設定します。 Flexible NetFlow は、L2 ポートチャネル インターフェイスではサポートされませんが、L2 ポートチャネルメンバーポートではサポートされます。 Flexible NetFlow は、L3 ポートチャネル インターフェイスとメンバーポートでサポートされますが、両方に対して同時にサポートされることはありません。
ステップ 4	{ip flow monitor ipv6 flow monitor datalink flow monitor} name [sampler name] {input output} 例： Device(config-if)# ip flow monitor MonitorTest input	入力または出力パケットに対応するインターフェイスに、IPv4、IPv6、データリンクフローモニタ、およびオプションのサンプラーを関連付けます。 ip flow monitor – Flexible NetFlow で IPv4 トラフィックを監視できます。 ipv6 flow monitor – Flexible NetFlow で IPv6 トラフィックを監視できます。 datalink flow monitor – Flexible NetFlow で非IPのトラフィックを監視できます。
ステップ 5	end 例： Device(config-flow-monitor)# end	特権 EXEC モードに戻ります。
ステップ 6	show flow interface [interface-type number] 例：	(任意) インターフェイスの NetFlow 情報を表示します。

	コマンドまたはアクション	目的
	Device# <code>show flow interface</code>	
ステップ 7	copy running-config startup-config 例： Device# <code>copy running-config startup-config</code>	(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。

VLAN 上でのブリッジ型 NetFlow の設定

フロー モニタおよびオプションのサンプラーを VLAN に適用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> <code>enable</code>	特権 EXEC モードを有効にします。 • 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： Device(config)# <code>configure terminal</code>	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 [configuration] vlan-id 例： Device(config)# <code>vlan configuration 30</code> Device(config-vlan-config)#	VLAN または VLAN 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	ip flow monitor monitor name [sampler sampler name] { input } 例： Device(config-vlan-config)# <code>ip flow monitor MonitorTest input</code>	入力パケットに対応する VLAN に、フロー モニタおよびオプションのサンプラーを関連付けます。
ステップ 5	copy running-config startup-config 例： Device# <code>copy running-config</code>	(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
	<code>startup-config</code>	

レイヤ 2 NetFlow の設定

Flexible NetFlow レコード内でレイヤ 2 キーを定義できます。このレコードを使用して、レイヤ 2 インターフェイスのフローをキャプチャできます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • 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： Device(config)# 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	flow record name 例： Device(config)# flow record L2_record Device(config-flow-record)#	フロー レコード 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	match datalink {dot1q ethertype mac vlan} 例： Device(config-flow-record)# match datalink ethertype	レイヤ 2 属性をキーとして指定します。
ステップ 5	end 例： Device(config-flow-record)# end	特権 EXEC モードに戻ります。
ステップ 6	show flow record [name] 例： Device# show flow record	(任意) インターフェイスの NetFlow 情報を表示します。

	コマンドまたはアクション	目的
ステップ 7	copy running-config startup-config 例 : Device# 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。

Flexible NetFlow の監視

次の表にあるコマンドを使用して、Flexible NetFlow をモニタリングできます。

表 18: Flexible NetFlow のモニタリング コマンド

コマンド	目的
show flow exporter [broker export-ids name name statistics templates]	NetFlow のフロー エクスポート情報と統計情報を表示します。
show flow exporter [name exporter-name]	NetFlow のフロー エクスポート情報と統計情報を表示します。
show flow interface	NetFlow インターフェイスに関する情報を表示します。
show flow monitor [name exporter-name]	NetFlow のフロー モニタ情報と統計情報を表示します。
show flow monitor statistics	フロー モニタの統計情報を表示します。
show flow monitor cache format { table record csv }	指定された形式でフロー モニタのキャッシュの内容を表示します。
show flow record [name record-name]	NetFlow のフローレコード情報を表示します。
show sampler [broker name name]	NetFlow サンプラーに関する情報を表示します。

Flexible NetFlow の設定例

例：フローの設定

フローを作成し、そのフローをインターフェイスに適用する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Device(config)# flow export export1
Device(config-flow-exporter)# destination 10.0.101.254
Device(config-flow-exporter)# transport udp 2055
Device(config-flow-exporter)# exit
Device(config)# flow record record1
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match ipv4 protocol
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# match transport destination-port

Device(config-flow-record)# collect counter byte long
Device(config-flow-record)# collect counter packet long
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# exit
Device(config)# flow monitor monitor1
Device(config-flow-monitor)# record record1
Device(config-flow-monitor)# exporter export1
Device(config-flow-monitor)# exit
Device(config)# interface tenGigabitEthernet 1/0/1
Device(config-if)# ip flow monitor monitor1 input
Device(config-if)# end
```

例：IPv4 入カトラフィックのモニタリング

次の例は、IPv4 入カトラフィックをモニタする方法を示しています（int g1/0/11 は、int g1/0/36 および int g3/0/11 にトラフィックを送信します）。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# flow record fr-1
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match interface input
Device(config-flow-record)# collect counter bytes long
Device(config-flow-record)# collect counter packets long
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# collect counter bytes layer2 long
Device(config-flow-record)# exit

Device(config)# flow exporter fe-ipfix6
Device(config-flow-exporter)# destination 2001:0:0:24::10
Device(config-flow-exporter)# source Vlan106
Device(config-flow-exporter)# transport udp 4739
Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow exporter fe-ipfix
Device(config-flow-exporter)# description IPFIX format collector 100.0.0.80
Device(config-flow-exporter)# destination 100.0.0.80
```

例：IPv4 出カトラフィックのモニタリング

```

Device(config-flow-exporter)# dscp 30
Device(config-flow-exporter)# ttl 210
Device(config-flow-exporter)# transport udp 4739
Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow exporter fe-1
Device(config-flow-exporter)# destination 10.5.120.16
Device(config-flow-exporter)# source Vlan105
Device(config-flow-exporter)# dscp 32
Device(config-flow-exporter)# ttl 200
Device(config-flow-exporter)# transport udp 2055

Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow monitor fm-1
Device(config-flow-monitor)# exporter fe-ipfix6
Device(config-flow-monitor)# exporter fe-ipfix
Device(config-flow-monitor)# exporter fe-1
Device(config-flow-monitor)# cache timeout inactive 60
Device(config-flow-monitor)# cache timeout active 180
Device(config-flow-monitor)# record fr-1
Device(config-flow-monitor)# end

Device# show running-config interface g1/0/11
Device# show running-config interface g1/0/36
Device# show running-config interface g3/0/11
Device# show flow monitor fm-1 cache format table

```

例：IPv4 出カトラフィックのモニタリング

```

Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# flow record fr-1 out
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match interface output
Device(config-flow-record)# collect counter bytes long
Device(config-flow-record)# collect counter packets long
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# exit

Device(config)# flow exporter fe-1
Device(config-flow-exporter)# destination 10.5.120.16
Device(config-flow-exporter)# source Vlan105
Device(config-flow-exporter)# dscp 32
Device(config-flow-exporter)# ttl 200
Device(config-flow-exporter)# transport udp 2055
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow exporter fe-ipfix6
Device(config-flow-exporter)# destination 2001:0:0:24::10
Device(config-flow-exporter)# source Vlan106
Device(config-flow-exporter)# transport udp 4739

```



```

Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow exporter fe-ipfix
Device(config-flow-exporter)# description IPFIX format collector 100.0.0.80
Device(config-flow-exporter)# destination 100.0.0.80
Device(config-flow-exporter)# dscp 30
Device(config-flow-exporter)# ttl 210
Device(config-flow-exporter)# transport udp 4739
Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow monitor fm-1-output
Device(config-flow-monitor)# exporter fe-1
Device(config-flow-monitor)# exporter fe-ipfix6
Device(config-flow-monitor)# exporter fe-ipfix
Device(config-flow-monitor)# cache timeout inactive 50
Device(config-flow-monitor)# cache timeout active 120
Device(config-flow-monitor)# record fr-1-out
Device(config-flow-monitor)# end

Device# show flow monitor fm-1-output cache format table

```

Flexible NetFlow の機能情報

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	この機能が導入されました。
Cisco IOS XE Gibraltar 16.12.1	IPv6 トラフィックについて、FNF の SGT フィールドと DGT フィールドのサポートが導入されました。

