ループ検出ガードの設定

ループ検出ガードの制約事項

ループ検出ガードは、レイヤ2物理インターフェイスでのみ設定できます。ポートチャネル、スイッチ仮想インターフェイス（SVI）、トンネルなどのレイヤ 3 ポートおよび仮想インターフェイスはサポートされません。

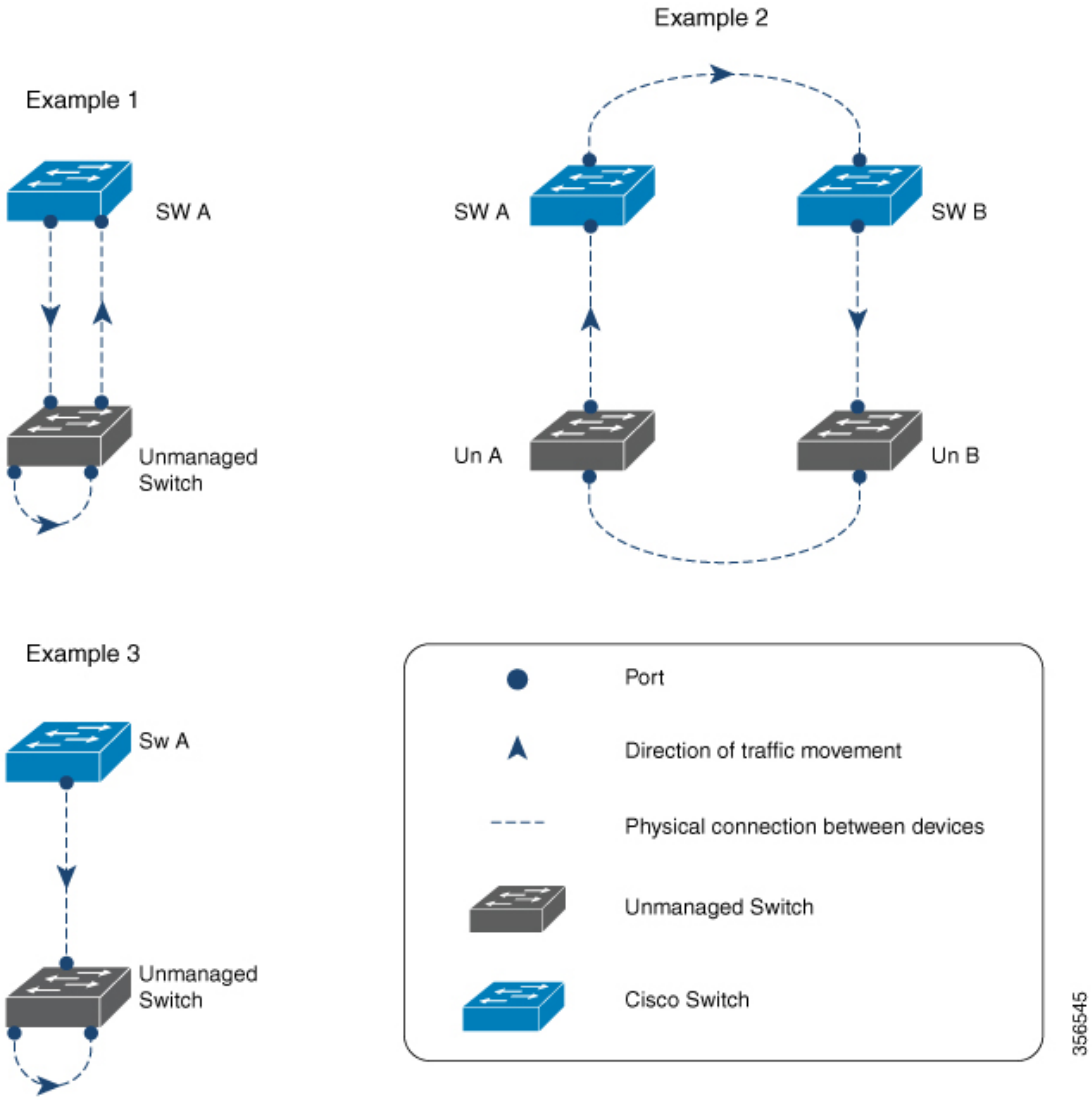
ループ検出ガードについて

コンピュータネットワークでは、2つのエンドポイント間に複数のレイヤ 2 パスがあるネットワークループが発生する可能性があります。ネットワーク内の2つのスイッチ間に複数の接続がある場合、または同じスイッチ上の2つのポートが相互に接続されている場合が考えられます。次の図に、ネットワークループの例をいくつか示します。

例 1：ネットワーク内にあるスイッチ SW A は、1 つのポートでアンマネージドスイッチにトラフィックを送信し、別のポートで同じアンマネージドスイッチからのトラフィックを受信しています。アンマネージドスイッチでは、トラフィックを受信するポートが、ネットワーク内の SW A にトラフィックを送信するポートに接続されているため、ネットワークループが発生しています。

例 2：この例では、ネットワーク内の 2 台のスイッチ（SW A と SW B）と 2 台のアンマネージドスイッチ（Un A と Un B）の 4 台のスイッチを含むネットワークループを示します。トラフィックは、SW A から SW B、Un A から Un B、そして SW A に戻る順に移動するため、ネットワークループが発生しています。

例3：アンマネージドスイッチの2つのポートが相互に接続されているため、ネットワークループが発生しています。



通常、この目的（ネットワークループを防ぐ）のために設定されるプロトコルはスパニングツリープロトコル（STP）ですが、STP を認識しないネットワーク内にアンマネージドスイッチが存在する場合や、STP がネットワーク上で設定されていない状況では、ループ検出ガードが適しています。

ループ検出ガードは、インターフェイスレベルでイネーブルです。ループを検出するため、システムはインターフェイスからループ検出フレームを事前に設定された間隔で送信します。ループが検出されると、設定されたアクションが実行されます。

デフォルトでは、ループ検出ガードはディセーブルになっています。この機能をイネーブルにすると、次のいずれかのアクションを設定できます。

- トラフィックを送信するポートをエラーディセーブルにします。
- トラフィックを受信するポートをエラーディセーブルにします（デフォルト）。

- エラーメッセージを表示し、ポートをディセーブルにしません。

ポートがエラーディセーブルになっている場合、そのポートでトラフィックは送受信されません。

ループ検出ガードと他の機能の連携動作

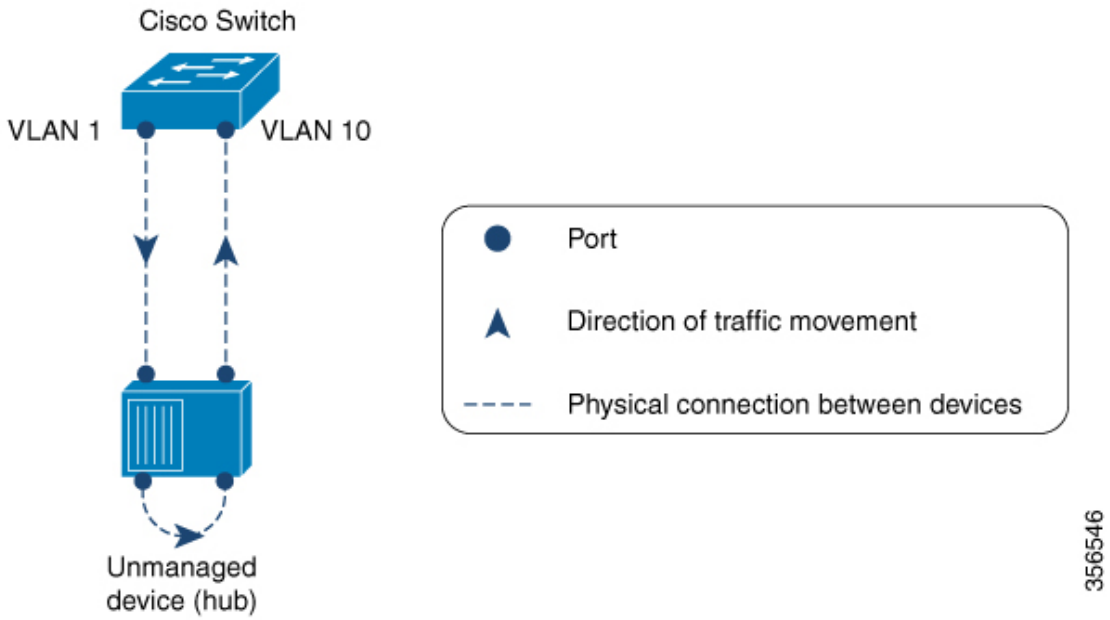
スパニング ツリー プロトコルとループ検出ガード

デバイスでループ検出ガードと STP の両方が有効になっている場合、STP がネットワークのループモニタリングを引き継ぎます。この場合、ループ検出パケットはネットワークで受信も処理もされません。

VLAN およびループ検出ガード

以下の理由から、ハブに接続されているスイッチでこの機能を設定することは推奨されません。ハブは、すべてのインターフェイスにトラフィックをフラッディングします。ネットワーク内のスイッチが同じハブからのトラフィックを異なる VLAN のポートで受信している場合は、これらの宛先ポートを誤ってエラーディセーブルにする可能性があります。次の図は、このような状況を示します。VLAN 1 のポートがハブにトラフィックを送信しています。スイッチはまた、同じハブからのトラフィックを、異なる VLAN（VLAN 10）のポートで受信します。ループ検出ガードを設定した場合（および宛先ポートをエラーディセーブルにするデフォルトアクションを設定した場合）、VLAN 10 のポートはブロックされます。（ポートをエラーディセーブルにする代わりに）メッセージを表示するオプションを設定することも推奨されません。これは、ハブに設定されたインターフェイスの数と同じ数だけメッセージが表示されるため、CPU が過負荷になるためです。

図 *1:* 管理対象外ネットワーク ハブに接続されたスイッチ



ループ検出ガードの設定方法

ループ検出ガードのイネーブル化と必要なポートのエラーディセーブル化

この機能はデフォルトで無効に設定されています。ループ検出ガードを有効にして、ループが検出されたときにシステムに実行させるアク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。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	**interface** {*interface-id* | *subinterface-id* | *vlan-id*}
	例：
	`Device(config)# interface tengigabitethernet 1/0/20`
	`Device(config-if)#`
		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。デバイスでループ検出ガードを設定するには、物理インターフェイスのみを指定します。PortChannel、スイッチ仮想インターフェイス（SVI）、トンネルなどのレイヤ 3 ポートおよび仮想インターフェイスはサポートされません。

ステップ 4	［**no**］**loopdetect** 例： `Device(config-if)# loopdetect`	デバイスでループ検出ガードをイネーブルにします。設定されたインターフェイスからループ検出フレームが送信されます。ループ検出ガードをイネーブルにするには、キーワードを指定せずに **loopdetect** コマンドを使用します。 この機能を無効化するには、このコマンドの **no** 形式を使用します。 （注） トランクポートでこの機能をイネーブルにすることはできますが、次の理由により、警告メッセージが表示されます。トランクポートが複数の VLAN のトラフィックを同時に伝送する。1つの VLAN でループが検出されると、トランクポートに関連付けられたすべての VLAN トラフィックがエラーディセーブルになる。
ステップ 5	［**no**］**loopdetect** {*time* | **action syslog** | **source-port**} 例： `Device(config-if)# loopdetect 7`	ループ検出フレームが送信される頻度と、ループが検出されたときにシステムが実行するアクションを指定します。アクションを指定しない場合、宛先ポートはデフォルトでエラーディセーブルになります。 次の設定を行えます。 • *time*：ループ検出フレームを送信する時間間隔（秒単位）。範囲は 0 ～ 10 です。デフォルトは 5 分です。

	コマンドまたはアクション	目的
		• **action syslog**：システムメッセージを表示し、どのポートもエラーディセーブルにしません。このコマンドの **no** 形式を使用すると、システムは最後に設定されたオプションに戻ります。 • **source-port**：ポートをエラーディセーブルにします。このコマンドの **no** 形式を使用すると、宛先ポートはエラーディセーブルになります。 左側の設定例（`Device(config-if)# loopdetect 7`）では、インターフェイスは7秒ごとにループ検出フレームを送信し、ループが検出された場合は宛先ポートをエラーディセーブルに設定するように設定されます（**action syslog** オプションも **source-port** オプションも設定されていないため、デフォルトが適用される）。
ステップ **6**	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ **7**	**show loopdetect** 例： `Device# show loopdetect`	ループ検出ガードがイネーブルになっているすべてのインターフェイス、ループ検出パケットが送信される頻度、および物理インターフェイスのステータスを表示します。

ループ検出ガードの設定に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9300 Series Switches)* の「Layer 2/3 Commands」の項を参照してください

ループ検出ガードの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Amsterdam 17.2.1	ループ検出ガード	ループ検出ガードは、STPが設定されていないネットワーク、またはSTPが設定されているネットワーク内の管理対象外デバイスのネットワークループを防止します。

Cisco Feature Navigatorを使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigatorには、http://www.cisco.com/go/cfn [英語] からアクセスします。

翻訳について
このドキュメントは、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。