

ERSPAN の設定

この章は、カプセル化リモートスイッチドポートアナライザ(ERSPAN)を Cisco NX-OS デバイスの IP ネットワークでミラーリングされたトラフィックを転送するように設定する方法 について説明します。

- ERSPAN について (1 ページ)
- ERSPAN の前提条件 (3 ページ)
- ERSPAN の注意事項および制約事項 (3ページ)
- ・デフォルト設定 (8ページ)
- ERSPAN の設定 (8 ページ)
- ERSPAN 設定の確認 (23 ページ)
- ERSPAN の設定例 (24 ページ)

ERSPAN について

ERSPANは、IPネットワークでミラーリングされたトラフィックを転送して、ネットワーク内で複数のスイッチのリモートモニタリングを提供します。トラフィックは、送信元ルータでカプセル化され、ネットワーク間を転送されます。パケットは宛先ルータでカプセル化解除され、宛先インターフェイスに送信されます。もう1つの方法は、パケットを解析して内部(SPAN コピー)フレームにアクセスするために、ERSPANカプセル化形式を理解する必要があるアナライザ自体を宛先とする方法です。

ERSPAN 送信元

トラフィックをモニタできるモニタ元インターフェイスのことをERSPAN送信元と呼びます。 送信元では、監視するトラフィックを指定し、さらに入力、出力、または両方向のトラフィッ クをコピーするかどうかを指定します。ERSPAN送信元には次のものが含まれます。

- イーサネットポート(ただしサブインターフェイスではない)
- •ポートチャネル
- ・コントロールプレーン CPU への帯域内インターフェイス。

(注) SPAN送信元としてスーパーバイザインバンドインターフェイス を指定すると、デバイスはスーパーバイザCPUにより送信された すべてのパケットをモニタします。

(注) スーパーバイザインバンドインターフェイスを SPAN 送信元として使用する場合、スーパーバイザハードウェア(出力)によって生成されたすべてのパケットがモニタされます。

Rx は ASIC の観点から見たものです(トラフィックはインバンド を介してスーパーバイザから出力され、ASIC / SPAN で受信され ます)。

VLAN

- VLAN が ERSPAN 送信元として指定されている場合は、VLAN 内でサポートされて いるすべてのインターフェイスが ERSPAN 送信元になります。
- VLANは、Cisco Nexus 9300-EX/-FX/-FX2/-FX3/-GX シリーズプラットフォームスイッ チおよび -EX/-FX ラインカードを備えた Cisco Nexus 9500 シリーズプラットフォームスイッチを除き、入力方向でのみ ERSPAN 送信元にすることができます。

(注)

1つの ERSPAN セッションに、上述の送信元を組み合わせて使用できます。

ERSPANの宛先

宛先ポートは ERSPAN 送信元からコピーされたトラフィックを受信します。宛先ポートは、 リモートモニタリング (RMON) プローブなどのデバイス、あるいはコピーされたパケットを 1つまたは複数の送信元ポートから受信したり、解析することができるセキュリティデバイス に接続されたポートです。宛先ポートはスパニングツリーインスタンスまたはレイヤ3プロト コルに参加しません。

Cisco Nexus 9200、9300-EX、9300-FX、および 9300-FX2 プラットフォーム スイッチは、GRE ヘッダー トラフィック フローを使用して、スイッチポート モードの物理インターフェイスま たはポートチャネルインターフェイスで設定された ERSPAN 宛先セッションをサポートしま す。送信元 IP アドレスは、デフォルト VRF で設定する必要があります。複数の ERSPAN 宛先 セッションを同じ送信元 IP アドレスで設定する必要があります。

ERSPAN セッション

モニタする送信元を指定する ERSPAN セッションを作成できます。

ローカライズされた ERSPAN セッション

すべての送信元インターフェイスが同じラインカード上にある場合、ERSPAN セッションは ローカライズされます。

(注) VLAN 送信元の ERSPAN セッションはローカライズされません

ERSPANの切り捨て

Cisco NX-OS Release 7.0(3)I7(1) 以降では、MTU のサイズに基づいて各 ERSPAN セッションの 送信元パケットの切り捨てを設定できます。切り捨てにより、モニタするパケットのサイズを 減らすことで、ERSPAN の帯域幅を効果的に軽減できます。設定された MTU サイズよりも大 きい ERSPAN パケットはすべて、設定されたサイズに切り捨てられます。ERSPAN では、 ERSPAN ヘッダータイプに応じて、切り捨てられたパケットに 54 ~ 166 バイトの ERSPAN ヘッダーが追加されます。たとえば、MTU を 300 バイトに設定すると、ERSPAN ヘッダー タ イプの設定に応じて、パケットは 354 ~ 466 バイトの ERSPAN ヘッダーサイズで複製されま す。

ERSPAN 切り捨てはデフォルトでは無効です。切り捨てを使用するには、個々のERSPANセッションで有効にしておく必要があります。

ERSPAN の前提条件

ERSPAN の前提条件は、次のとおりです。

各デバイス上で、まず所定の ERSPAN 設定をサポートするポートを設定する必要があります。詳細については、『Cisco Nexus 9000 シリーズ NX-OS インターフェイス設定ガイド』を参照してください。

ERSPAN の注意事項および制約事項



(注) スケールの情報については、リリース特定の『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』を参照してください。

ERSPAN 設定時の注意事項と制限事項は次のとおりです。

・ERSPAN セッション(Rx および Tx、Rx、または Tx)ごとに最大 48 の送信元インター フェイスがサポートされます。

- ERSPAN 宛先は、プラットフォームに基づいて MTU のジャンボ フレームを異なる方法で 処理します。次の Cisco Nexus 9300 プラットフォーム スイッチおよびサポート ラインカー ドを備えた Cisco Nexus 9500 プラットフォーム スイッチの場合、ERSPAN 宛先はジャンボ フレームをドロップします。
 - Cisco Nexus 9332PQ
 - Cisco Nexus 9372PX
 - Cisco Nexus 9372PX-E
 - Cisco Nexus 9372TX
 - Cisco Nexus 9372TX-E
 - Cisco Nexus 93120TX
 - ・次のライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ
 - Cisco Nexus 9564PX
 - Cisco Nexus 9464TX
 - Cisco Nexus 9464TX2
 - Cisco Nexus 9564TX
 - Cisco Nexus 9464PX
 - Cisco Nexus 9536PQ
 - Cisco Nexus 9636PQ
 - Cisco Nexus 9432PQ

次の Cisco Nexus 9200 プラットフォーム スイッチおよびサポート ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチの場合、ERSPAN はポート MTU でパケット を切り捨て、TX 出力エラーを発行します。

- Cisco Nexus 92160YC-X
- Cisco Nexus 92304QC
- Cisco Nexus 9272Q
- Cisco Nexus 9232C
- Cisco Nexus 9236C
- Cisco Nexus 92300YC
- Cisco Nexus 93108TC-EX
- Cisco Nexus 93180LC-EX
- Cisco Nexus 93180YC-EX
- ・次のライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチ
 - Cisco Nexus 9736C-EX

- Cisco Nexus 97160YC-EX
- Cisco Nexus 9732C-EX
- Cisco Nexus 9732C-EXM
- ACL フィルタを使用した、親インターフェイスでの ERSPAN サブインターフェイストラ フィックは、Cisco Nexus 9200 プラットフォームスイッチではサポートされません。
- ACL フィルタを使用した、親インターフェイスでの ERSPAN サブインターフェイストラ フィックは、Cisco Nexus 9300-EX/FX/FX2/FX3/GX プラットフォームスイッチではサポー トされません。
- ERSPAN ミラーリングは、PBR トラフィックではサポートされません。
- タイプ3ヘッダをもつ ERSPAN は、Cisco NX-OS リリース9.3(3) ではサポートされません。
- ・ERSPAN セッションの制限については、『Cisco Nexus 9000 シリーズ NX-OS 検証スケーラ ビリティ ガイド』を参照してください。
- ラインカードごとの ERSPAN セッションの数は、同じインターフェイスが複数セッションの双方向送信元として設定されている場合は、2 に減少します。
- 同じ送信元インターフェイスで2つの SPAN または ERSPAN セッションを1つのフィル タだけで設定することはできません。同じ送信元が複数のSPAN または ERSPAN セッションで使用されている場合は、すべてのセッションに異なるフィルタを設定するか、セッションにフィルタを設定しないでください。
- Cisco NX-OS リリース 9.3(5) 以降、次の ERSPAN 機能は Cisco Nexus 9300-GX プラット フォーム スイッチでサポートされています。
 - ・ERSPAN タイプ III ヘッダー
 - ERSPAN 宛先サポート
- FCS エラーがあるパケットは、ERSPAN セッションでミラーリングされません。
- TCAM カービングは、次のライン カードの SPAN/ERSPAN には必要ありません。
 - Cisco Nexus 9636C-R
 - Cisco Nexus 9636Q-R
 - Cisco Nexus 9636C-RX
 - Cisco Nexus 96136YC-R
 - Cisco Nexus 9624D-R2



ワーディングエンジン(NFE)と NFE2対応 EOR スイッチおよび ERSPAN セッションで Tx ポートの送信元を持つものに適用されます。

- レイヤ2のERSPANTxマルチキャストの場合、ERSPANコピーはマルチキャストレプリケーションとは無関係に作成されます。このため、マルチキャストとSPANパケットでは、VLANタグ(入力インターフェイス VLAN ID)の値が異なります。
- •次の注意事項と制約事項が (Rx) ERSPAN に適用されます。
 - •VLAN 送信元は Rx 方向のみがサポートされます。
 - セッションフィルタリング機能(VLANまたはACLフィルタ)は、Rx送信元でのみ サポートされます。
 - VLAN は、ERSPAN 送信元として入力方向でのみサポートされます。
- ・プライオリティフロー制御(PFC) ERSPANには、次の制約事項と制約事項があります。
 - フィルタとは共存できません。
 - 物理または port-channel インターフェイスの Rx 方向でのみサポートされています。
 VLAN インターフェイスの Rx 方向、または Tx 方向ではサポートされていません。
- ・次の注意事項および制約事項が FEX ポートに適用されます。
 - 双方向 ERSPAN セッションで使用される送信元が同じ FEX からのものである場合、 ハードウェア リソースは2つの ERSPAN セッションに制限されます。
 - FEXポートは、ERSPANとしてすべてのトラフィックに対して入力方向でサポートされ、既知のレイヤ2ユニキャストトラフィックには出力方向のみがサポートされます。
 - Cisco Nexus 9300 プラットフォーム スイッチは、FEX インターフェイスに接続されて いる ERSPAN 宛先をサポートしていません。ERSPAN 宛先は、前面パネル ポートに 接続する必要があります。
 - VLAN および ACL フィルタは FEX ポートではサポートされません。フィルタとは共存できません。
- ERSPAN 宛先には、次の注意事項と制約事項が適用されます。
 - Cisco Nexus 9200、9300-EX、9300-FX、および 9300-FX2 プラットフォーム スイッチ は、GRE ヘッダートラフィックフローを使用して、スイッチポートモードの物理イ ンターフェイスまたはポートチャネルインターフェイスで設定された ERSPAN 宛先 セッションをサポートします。
 - ERSPAN 宛先は、Cisco Nexus 9200、9300、9300-EX、9300-FX、および 9300-FX2 プ ラットフォーム スイッチの MPLS や VXLAN などの他のトンネル機能と共存できま せん。
 - Cisco Nexus 9300-GX スイッチでは、ERSPAN 宛先セッションがアクティブであるデ バイスを通過する dot1q タグ付きブロードキャストまたはマルチキャストパケット

は、ハードウェアの制限により、正しい VLAN ではなくネイティブ VLAN でタグ付 けされます。

- ・ERSPAN 宛先セッションは、デフォルトの VRF のみをサポートします。
- Cisco Nexus 9300-EX/FX スイッチは、Cisco Nexus 3000 および非 EX/FX Cisco Nexus 9000 スイッチの ERSPAN 宛先として機能できません。
- Cisco NX-OS リリース 10.1 (2) 以降、ERSPAN は Cisco Nexus N9K-X9624D-R2 ライン カー ドでサポートされます。

デフォルト設定

次の表に、ERSPAN パラメータのデフォルト設定を示します。

表 1: デフォルトの ERSPAN パラメータ

パラメータ	デフォルト
ERSPAN セッション	シャットステートで作成されます

ERSPANの設定



(注) この機能の Cisco NX-OS コマンドは、Cisco IOS のコマンドとは異なる場合があるので注意してください。

ERSPAN 送信元セッションの設定

ERSPANセッションを設定できるのはローカルデバイス上だけです。デフォルトでは、ERSPAN セッションはシャット ステートで作成されます。



(注) ERSPAN は送信元に関係なく、スーパーバイザによって生成されるパケットをモニタしません。

手順

	コマンドまたはアクション	目的
ステップ1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ2	monitor erspan origin ip-address <i>ip-address</i> global or 例: switch(config)# monitor erspan origin ip-address 10.0.0.1 global	ERSPAN のグローバルな送信元 IP アド レスを設定します。
ステップ 3	no monitor session {session-number all} 例: switch(config)# no monitor session 3	指定した ERSPAN セッションの設定を 消去します。新しいセッション コン フィギュレーションは、既存のセッ ションコンフィギュレーションに追加 されます。
ステップ4	<pre>monitor session {session-number all} type erspan-source [shut] 例: switch(config)# monitor session 3 type erspan-source switch(config-erspan-src)#</pre>	ERSPAN タイプ II 送信元セッションを 設定します。デフォルトでは、セッ ションは双方向です。オプションの shut キーワードは、選択したセッションに 対して shut ステートを指定します。
ステップ5	description description 例: switch(config-erspan-src)# description erspan_src_session_3	セッションの説明を設定します。デ フォルトでは、説明は定義されませ ん。説明には最大32の英数字を使用で きます。
ステップ6	<pre>source {interface type [tx rx both] vlan {number range} [rx]} 例: switch(config-erspan-src)# source interface ethernet 2/1-3, ethernet 3/1 rx 例: switch(config-erspan-src)# source interface port-channel 2 例: switch(config-erspan-src)# source interface switch(config-erspan-src)# source interface</pre>	送信元およびパケットをコピーするト ラフィックの方向を設定します。一定 範囲のイーサネットポート、ポート チャネル、インバンドインターフェイ ス、または一定範囲の VLAN、または Cisco Nexus 2000 シリーズファブリッ クエクステンダ (FEX) 上のサテライ トポートまたはホストインターフェイ スポート チャネルを入力できます。 送信元は1つ設定することも、または カンマで区切った一連のエントリとし て、または番号の範囲として、複数設 定することもできます コピーすスト

I

	コマンドまたはアクション	目的
	例: switch(config-erspan-src)# source vlan	ラフィックの方向には、入力、出力、 または両方を指定できます。
	3, 6-8 rx 例: switch(config-erspan-src)# source interface ethernet 101/1/1-3	単一方向のセッションには、送信元の 方向はセッションで指定された方向に 一致する必要があります。 (注)
		送信元 VLAN は、入力方向でのみサ ポートされます。送信元 FEX ポート は、すべてのトラフィックに対して入 力方向でサポートされ、既知のレイヤ 2ユニキャストトラフィックには出力 方向のみがサポートされます。
		送信元としてのスーパーバイザは、Rx 方向でのみサポートされます。
ステップ 1	(任意)ステップ7を繰り返して、す べてのERSPAN送信元を設定します。	
ステップ8	filter vlan {number range} 例: switch(config-erspan-src)# filter vlan 3-5, 7	設定された送信元から選択する VLAN を設定します。VLAN は1 つ設定する ことも、またはカンマで区切った一連 のエントリとして、または番号の範囲 として、複数設定することもできま す。VLAN の範囲については、『Cisco Nexus 9000 シリーズ NX-OS レイヤ 2 スイッチング設定ガイド』を参照して ください。 (注) ERSPAN送信元として設定された FEX ポートは VLAN フィルタをサポートし ません。
ステップ 9	(任意) ステップ9を繰り返して、す べての送信元 VLAN のフィルタリング を設定します。	
ステップ 10	(任意) filter access-group acl-filter 例: switch(config-erspan-src)# filter access-group ACL1	ACL を ERSPAN セッションにアソシ エートします。(標準の ACL 設定プロ セスを使用して ACL を作成できます。 詳細については、 <i>Cisco Nexus 9000 シ</i> リーズ <i>NX-OS</i> セキュリティ コンフィ ギュレーションガイドを参照してくだ さい。)

	コマンドまたはアクション	目的
		(注) このコマンドを実行する前に、ipアク セスリストおよび関連する vlan アク セスマップを構成します。ERSPAN ACL の構成を参照してください。
ステップ 11	destination ip <i>ip-address</i> 例: switch(config-erspan-src)# destination ip 10.1.1.1	 ERSPAN セッションの宛先 IP アドレス を設定します。 (注) ERSPAN 送信元セッションごとに1つ の宛先 IP アドレスのみがサポートされます。
ステップ 12	erspan-id erspan-id 例: switch(config-erspan-src)# erspan-id 5	ERSPAN 送信元セッションの ERSPAN ID を設定します。ERSPAN の範囲は 1 ~ 1023 です。
ステップ1 3	vrf <i>vrf-name</i> 例: switch(config-erspan-src)# vrf default	ERSPAN 送信元セッションがトラ フィックの転送に使用する仮想ルー ティングおよびフォワーディング (VRF) インスタンスを設定します。 VRF名は、32文字以内の英数字のスト リング (大文字と小文字を区別) で指 定します。
ステップ14	(任意) ip ttl <i>ttl-number</i> 例: switch(config-erspan-src)# ip ttl 25	ERSPAN トラフィックの IP 存続可能時 間(TTL)値を設定します。範囲は 1 ~ 255 です。
ステップ 15	(任意) ip dscp <i>dscp-number</i> 例: switch(config-erspan-src)# ip dscp 42	ERSPAN トラフィックのパケットの DiffServ コードポイント(DSCP)値を 設定します。範囲は 0 ~ 63 です。
ステップ16	no shut 例: switch(config-erspan-src)# no shut	ERSPAN 送信元セッションをイネーブ ルにします。デフォルトでは、セッ ションはシャットステートで作成され ます。
ステップ 17	exit 例: switch(config-erspan-src)# exit switch(config)#	モニタ設定モードを閉じます。

示しま
レーショ
ュンフィ
0
を、ス イーション

ERSPAN セッションのシャットダウンまたはアクティブ化

ERSPAN セッションをシャットダウンすると、送信元から宛先へのパケットのコピーを切断で きます。1セッションをシャットダウンしてハードウェアリソースを解放し、別のセッション を有効にできます。デフォルトでは、ERSPAN セッションはシャット ステートで作成されま す。

ERSPAN セッションをイネーブルにすると、送信元から宛先へのパケットのコピーをアクティ ブ化できます。すでにイネーブルになっていて、動作状況がダウンの ERSPAN セッションを イネーブルにするには、そのセッションをいったんシャットダウンしてから、改めてイネーブ ルにする必要があります。ERSPAN セッション ステートをシャットダウンおよびイネーブル にするには、グローバルまたはモニタ コンフィギュレーション モードのいずれかのコマンド を使用できます。

手順

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

	コマンドまたはアクション	目的
	<pre>switch# configure terminal switch(config)#</pre>	
ステップ 2	<pre>monitor session {session-range all} shut 例: switch(config)# monitor session 3 shut</pre>	指定の ERSPAN セッションをシャット ダウンします。デフォルトでは、セッ ションはシャットステートで作成され ます。
ステップ3	no monitor session {session-range all} shut 例: switch(config)# no monitor session 3	指定の ERSPAN セッションを再開(イ ネーブルに)します。デフォルトで は、セッションはシャットステートで 作成されます。
	shut	モニタセッションがイネーブルで動作 状況がダウンの場合、セッションをイ ネーブルにするには、最初に monitor session shut コマンドを指定してから、 no monitor session shut コマンドを続け る必要があります。
ステップ4	<pre>monitor session session-number type erspan-source 例: switch(config)# monitor session 3 type erspan-source switch(config-erspan-src)#</pre>	ERSPAN 送信元タイプのモニタ コン フィギュレーションモードを開始しま す。新しいセッション コンフィギュ レーションは、既存のセッションコン フィギュレーションに追加されます。
ステップ5	<pre>shut 例: switch(config-erspan-src)# shut</pre>	ERSPAN セッションをシャットダウン します。デフォルトでは、セッション はシャットステートで作成されます。
ステップ6	no shut 例: switch(config-erspan-src)# no shut	ERSPAN セッションをイネーブルにし ます。デフォルトでは、セッションは シャット ステートで作成されます。
ステップ1	exit 例: switch(config-erspan-src)# exit switch(config)#	モニタ設定モードを閉じます。
ステップ8	(任意) show monitor session all 例: switch(config)# show monitor session all	ERSPAN セッションのステータスを表示します。

	コマンドまたはアクション	目的
ステップ9	(任意) show running-config monitor	ERSPAN の実行コンフィギュレーショ
	例:	ンを表示します。
	<pre>switch(config)# show running-config monitor</pre>	
ステップ10	(任意) show startup-config monitor	ERSPAN のスタートアップ コンフィ
	例:	ギュレーションを表示します。
	<pre>switch(config)# show startup-config monitor</pre>	
ステップ 11	(任意) copy running-config startup-config	実行コンフィギュレーションを、ス タートアップコンフィギュレーション
	例:	にコピーします。
	<pre>switch(config)# copy running-config startup-config</pre>	

ERSPAN ACL の設定

デバイスに IPv4 ERSPAN ACL を作成して、ルールを追加できます。

始める前に

DSCP 値または GRE プロトコルを変更するには、新しい宛先モニタ セッションを割り当てる 必要があります。最大 4 つの宛先モニタ セッションがサポートされます。

手順

	コマンドまたはアクション	目的
ステップ1	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ2	ip access-list <i>acl-name</i> 例: switch(config)# ip access-list erspan-acl switch(config-acl)#	ERSPAN ACL を作成して、IP ACL コン フィギュレーション モードを開始しま す。 <i>acl-name</i> 引数は 64 文字以内で指定 します。
ステップ3	[sequence-number] { permit deny } protocol source destination [set-erspan-dscp dscp-value] [set-erspan-gre-proto protocol-value] 例:	ERSPANACL内にルールを作成します。 多数のルールを作成できます。 sequence-number 引数には、1~ 4294967295 の整数を指定します。

 コマンドまたはアクション	目的
 <pre>switch(config-acl)# permit ip 192.168.2.0/24 any set-erspan-dscp 40 set-erspan-gre-proto 5555</pre>	permit コマンドと deny コマンドには、 トラフィックを識別するための多くの方 法が用意されています。
例: switch(config)# ip access-list match_11_pkts switch(config-acl)# permit ip 10.0.0.0/24 any switch(config-acl)# exit	set-erspan-dscpオプションは、ERSPAN 外部 IP ヘッダーに DSCP 値を設定しま す。DSCP 値の範囲は 0 ~ 63 です。 ERSPAN ACL に設定された DSCP 値で、 モニタ セッションに設定されている値 が上書きされます。ERSPAN ACL にこ のオプションを含めない場合、0または モニタ セッションで設定されている DSCP 値が設定されます。
	set-erspan-gre-proto オプションは、 ERSPAN GRE ヘッダーにプロトコル値 を設定します。プロトコル値の範囲は0 ~ 65535 です。ERSPAN ACL にこのオ プションを含めない場合、ERSPAN カ プセル化パケットの GRE ヘッダーのプ ロトコルとしてデフォルト値の 0x88be が設定されます。
	set-erspan-gre-proto または set-erspan-dscp アクションが設定されて いる各アクセス コントロール エントリ (ACE)は、1つの宛先モニタセッショ ンを消費します。ERSPANACLごとに、 これらのアクションのいずれかが設定さ れている最大3つの ACE がサポートさ れます。たとえば、次のいずれかを設定 できます。
	 set-erspan-gre-protoまたは set-erspan-dscpアクションが設定された最大3つのACEを持つACLが設定されている、1つのERSPAN セッション
	 set-erspan-gre-proto または set-erspan-dscp アクションが設定され、1つの追加のローカルまたは ERSPAN セッションが設定された 2 つの ACE を持つ ACL が設定され ている、1 つの ERSPAN セッショ ン

	コマンドまたはアクション	目的
		 set-erspan-gre-proto または set-erspan-dscp アクションが設定さ れた1つの ACE を持つ ACL が設定 されている、2 つの ERSPAN セッ ションのうち大きなもの
ステップ4	<pre>show ip access-lists name 例 : switch(config-acl)# show ip access-lists erpsan-acl</pre>	ERSPAN ACL の設定を表示します。
ステップ5	<pre>show monitor session {all session-number range session-range} [brief] 何]: switch(config-acl)# show monitor session 1</pre>	ERSPANセッション設定を表示します。
ステップ6	(任意) copy running-config startup-config 例: switch(config-acl)# copy running-config startup-config	実行コンフィギュレーションを、スター トアップ コンフィギュレーションにコ ピーします。

UDF ベース ERSPANの設定

外部または内部パケットフィールド(ヘッダまたはペイロード)のユーザ定義フィールド (UDF)で照合し、一致するパケットを ERSPAN 宛先に送信するようにデバイスを設定でき ます。そのように設定することで、ネットワークのパケットドロップを分析して、分離するこ とができます。

始める前に

UDF ベース ERSPAN をイネーブルにするのに十分な空き領域を確保するために、hardware access-list tcam region コマンドを使用して適切な TCAM リージョン (racl、ifacl、または vacl) が設定されていることを確認します。詳細については、Cisco Nexus 9000 シリーズ NX-OS セキュリティ設定ガイドの『ACL TCAM リージョン サイズの設定』セクションを参照してください。

手順

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

I

	コマンドまたはアクション	目的
	<pre>switch# configure terminal switch(config)#</pre>	
ステップ2	udf udf-name offset-base offset length	次のように UDF を定義します。
	次、,、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、	 <i>udf-name</i>: UDF の名前を指定しま す。名前には最大 16 文字の英数字 を入力できます。 <i>offset-base</i>: UDF オフセットベース を以下のように指定します。ここで header は、オフセットのために考 慮に入れるべきパケット ヘッダー です: packet-start header {outer inner {I3 I4}}.
		 オフセット:オフセットベースからのオフセットバイト数を指定します。オフセットベース(レイヤ3/レイヤ4ヘッダー)の最初のバイトを照合するには、オフセットを0に設定します。
	 長さ:オフセットからバイトの数 を指定します。1または2バイトの みがサポートされています。追加の バイトに一致させるためには、複数 の UDF を定義する必要がありま す。 	
		複数の UDF を定義できますが、シスコ は必要な UDF のみ定義することを推奨 します。
ステップ3 hardware acces ifacl vacl } qua 例: switch(config tcam region racl qualify	hardware access-list tcam region {racl ifacl vacl }qualify udf udf-names	次のいずれかの TCAM リージョンに UDF を付加します。
	例: switch(config)# hardware access-list tcam region racl qualify udf udf-x udf-y	• racl:レイヤ3ポートに適用しま す:レイヤ2およびレイヤ3ポート に適用します。
		• ifacl:レイヤ2ポートに適用しま す。
		• vacl:送信元 VLAN に適用します。
		UDF は TCAM リージョンに最大 8 個ま で付加できます。

	コマンドまたはアクション	目的
		 (注) UDF 修飾子が追加されると、TCAM リージョンはシングル幅から倍幅に拡 大します。十分な空きスペースがある ことを確認してください。それ以外の 場合このコマンドは拒否されます。必 要な場合、未使用のリージョンから TCAM スペースが減りますので、この コマンドを再入力します。詳細につい ては、Cisco Nexus 9000 シリーズ NX-OS セキュリティ設定ガイドの『ACL TCAM リージョンサイズの設定』セク ションを参照してください。
		(注) このコマンドの no 形式は、UDF を TCAM リージョンから切り離し、リー ジョンをシングル幅に戻します。
ステップ4	必須: copy running-config startup-config 例: switch(config)# copy running-config startup-config	リブートおよびリスタート時に実行コン フィギュレーションをスタートアップ コンフィギュレーションにコピーして、 変更を継続的に保存します。
ステップ5	必須: reload 例 : switch(config)# reload	デバイスがリロードされます。 (注) UDF 設定は copy running-config startup-config + reload を入力した後の み有効になります。
ステップ6	ip access-list erspan-acl 例: switch(config)# ip access-list erspan-acl-udf-only switch(config-acl)#	IPv4 アクセス コントロール リスト (ACL)を作成して、IP アクセス リス 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1	次のいずれかのコマンドを入力します。 • permit udf udf-name value mask • permit ip source destination udf udf-name value mask 例 ·	ACLを設定し、UDF(例1)でのみ、ま たは外部パケットフィールドについて 現在のアクセスコントロールエントリ (ACE)と併せて UDF で一致させるよ うに設定します(例2)
	switch(config-acl)# permit udf udf-x 0x40 0xF0 udf-y 0x1001 0xF00F	シングル ACL は、UDFがある場合とな い場合の両方とも、ACE を有すること

	-	·
	コマンドまたはアクション	目的
	例: switch(config-acl)# permit ip 10.0.0.0/24 any udf udf-x 0x02 0x0F udf-y 0x1001 0xF00F	ができます。各ACEには一致する異なるUDFフィールドがあるか、すべてのACEをUDFの同じリストに一致させることができます。
ステップ8	(任意) copy running-config startup-config 例: switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スター トアップ コンフィギュレーションにコ ピーします。

ERSPAN 切り捨ての設定

切り捨ては、ローカルおよび ERSPAN 送信元セッションに対してのみ設定できます。

手順

	コマンドまたはアクション	目的
ステップ1	configure terminal	グローバル設定モードを開始します。
	例:	
	switch# configure terminal switch(config)#	
ステップ2	monitor session session-number type erspan-source	指定された ERSPAN セッションのモニ タ設定モードに入ります。
	例: switch(config)# monitor session 10 type erspan-source switch(config-erspan-src)#	
ステップ3	source interface <i>type slot/port</i> [rx tx both]	送信元インターフェイスを設定します。
	例:	
	<pre>switch(config-erspan-src)# source interface ethernet 1/5 both</pre>	
ステップ4	mtu size	MTUの切り捨てサイズを設定します。
	例:	設定された MTU サイズよりも大きい
	switch(config-erspan-src)# mtu 512	EKSPAN ハケットはすべて、設定され たサイズに切り捨てられます FRSPAN
	例:	パケットの切り捨てのMTU範囲は次の
	<pre>switch(config-erspan-src)# mtu ?</pre>	とおりです。
	<512-1518> Enter the value of MTU	

	コマンドまたはアクション	目的
	ERSPAN packets (erspan header + truncated original packet)	 Cisco Nexus 9300-EX シリーズス イッチの MTU サイズの範囲は 512 ~1518 バイトです。 Cisco Nexus 9300-FX シリーズス イッチの MTU サイズの範囲は 64~ 1518 バイトです。 9700-EX および 9700-FX ラインカー ドを搭載した Cisco Nexus 9500 プ ラットフォーム スイッチの場合、 MTU サイズの範囲は 512~1518 バ
		イトです。
ステップ5	destination interface type slot/port	イーサネット ERSPAN 宛先ポートを設
	例:	定します。
	<pre>switch(config-erspan-src)# destination interface Ethernet 1/39</pre>	
ステップ6	no shut	ERSPAN セッションをイネーブルにし
	例: switch(config-erspan-src)# no shut	ます。デフォルトでは、セッションは シャット ステートで作成されます。
ステップ7	(任意) show monitor session session	ERSPAN の設定を表示します。
	例:	
	<pre>switch(config-erspan-src)# show monitor session 5</pre>	
ステップ 8	copy running-config startup-config 例: switch(config-erspan-src)# copy running-config startup-config	実行コンフィギュレーションを、スター トアップ コンフィギュレーションにコ ピーします。

ERSPAN 宛先セッションの設定

送信元 IP アドレスからローカル デバイス上の宛先ポートにパケットをコピーするように ERSPAN 宛先セッションを設定できます。デフォルトでは、ERSPAN 宛先セッションはシャッ トステートで作成されます。

始める前に

スイッチポート モニタ モードで宛先ポートが設定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	configure terminal 例: switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します
ステップ 2	interface ethernet <i>slot/port</i> [- <i>port</i>] 例: switch(config)# interface ethernet 2/5 switch(config-if)#	選択したスロットおよびポートまたは ポート範囲で、インターフェイスコン フィギュレーションモードを開始しま す。
ステップ3	<pre>switchport 例: switch(config-if)# switchport</pre>	選択したスロットおよびポートまたは ポート範囲でスイッチポートパラメー タを設定します。
ステップ4	<pre>switchport mode [access trunk] 例: switch(config-if)# switchport mode trunk</pre>	選択したスロットおよびポートまたは ポート範囲で次のスイッチポートモー ドを設定します。 ・アクセス ・トランク
ステップ5	<pre>switchport monitor 例: switch(config-if)# switchport monitor</pre>	ERSPAN 宛先としてスイッチポートイ ンターフェイスを設定します。
ステップ6	ステップ2~5を繰り返して、追加の ERSPAN 宛先でモニタリングを設定し ます。	
ステップ1	no monitor session {session-number all} 例: switch(config-if)# no monitor session 3	指定した ERSPAN セッションの設定を 消去します。新しいセッション コン フィギュレーションは、既存のセッ ションコンフィギュレーションに追加 されます。
ステップ8	<pre>monitor session {session-number all} type erspan-destination 例: switch(config-if)# monitor session 3 type erspan-destination switch(config-erspan-dst)#</pre>	ERSPAN 宛先セッションを設定しま す。

I

	コマンドまたはアクション	目的
ステップ9	description description 例: switch(config-erspan-dst)# description erspan_dst_session_3	セッションの説明を設定します。デ フォルトでは、説明は定義されませ ん。説明には最大32の英数字を使用で きます。
ステップ 10	<pre>source ip ip-address 例 : switch(config-erspan-dst)# source ip 10.1.1.1</pre>	ERSPAN セッションの宛先 IP アドレ スを構成します。送信元 IP アドレス は、ローカルに構成されたIP アドレス です。ERSPAN 宛先セッションの送信 元 IP アドレスは、カプセル化された データの受信元である ERSPAN 送信元 セッションで構成された宛先 IP アド レスと一致する必要があります。 ERSPAN 送信元セッションごとに1つ の宛先 IP アドレスのみがサポートさ れます。
ステップ 11	<pre>destination {[interface [type slot/port[-port]]] [port-channel channel-number]]} 何]: switch(config-erspan-dst)# destination interface ethernet 2/5</pre>	コピーする送信元パケットの宛先を設 定します。宛先インターフェイスを設 定できます。 (注) 宛先ポートをトランクポートとして設 定できます。
ステップ 12	(任意) ステップ 11 を繰り返して、 すべての ERSPAN 宛先を設定します。	
ステップ 13	erspan-id erspan-id 例: switch(config-erspan-dst)# erspan-id 5	ERSPAN セッションの ERSPAN ID を 設定します。指定できる範囲は1~ 1023 です。
ステップ 14	no shut 例: switch(config-erspan-dst)# no shut	ERSPAN 宛先セッションを有効にしま す。デフォルトでは、セッションは シャット ステートで作成されます。
ステップ 15	exit 例: switch(config-erspan-dst)# exit	モニタ設定モードを閉じます。
ステップ16	exit 例: switch(config)# exit	グローバル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 17	(任意) show monitor session { all <i>session-number</i> range <i>session-range</i> }	ERSPAN セッション設定を表示しま す。
	例:	
	switch(config)# show monitor session 3	
ステップ 18	(任意) show running-config monitor	ERSPAN の実行コンフィギュレーショ
	例:	ンを表示します。
	<pre>switch(config-erspan-src)# show running-config monitor</pre>	
ステップ 19	(任意) show startup-config monitor	ERSPAN のスタートアップ コンフィ
	例:	ギュレーションを表示します。
	switch(config-erspan-src)# show startup-config monitor	
ステップ 20	(任意) copy running-config startup-config	実行コンフィギュレーションを、ス タートアップコンフィギュレーション
	例:	にコピーします。
	<pre>switch(config-erspan-src)# copy running-config startup-config</pre>	

ERSPAN 設定の確認

ERSPAN 設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
<pre>show monitor session {all session-number range session-range} [brief]</pre>	ERSPAN セッション設定を表示します。
show running-config monitor	ERSPAN の実行コンフィギュレーションを表示します。
show startup-config monitor	ERSPAN のスタートアップ コンフィギュレー ションを表示します。

ERSPANの設定例

単一方向 ERSPAN セッションの設定例

次に、単一方向 ERSPAN セッションを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 14/30
switch(config-if)# no shut
switch(config-if)# exit
switch(config)# no monitor session 3
switch(config)# monitor session 3 rxswitch(config-erspan-src)# source interface ethernet
2/1-3 rx
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 10.1.1.2
switch(config-erspan-src)# no shut
switch(config-erspan-src)# exit
switch(config)# show monitor session 1
```

ERSPAN ACL の設定例

次に、ERSPAN ACL を設定する例を示します。

```
switch# configure terminal
switch(config)# ip access-list match_10_pkts
switch(config-acl)# permit ip 10.0.0.0/24 any
switch(config-acl)# exit
switch(config)# ip access-list match_172_pkts
switch(config-acl)# permit ip 172.16.0.0/24 any
switch(config-acl)# exit
```

定義済みの ACL フィルタに基づいて対象トラフィックが選択されるさまざまな ERSPAN 接続 先の場合、最後に設定されたセッションが常に高い優先順位を持ちます。

たとえば、モニター セッション1が構成されているとします。次に、モニター セッション2 が構成されます。この場合、ERSPAN トラフィックフィルタは意図したとおりに機能します。 ただし、ユーザーがモニター セッション1に戻り、既存の構成行の1つを再適用した場合(構 成に新しい変更はありません)。その後、スパンされたトラフィックはモニター セッション1 に戻ります。

マーカー パケットの設定例

次に、2秒間隔で ERSPAN マーカー パケットを有効にする例を示します。

```
switch# configure terminal
switch(config)# monitor erspan origin ip-address 172.28.15.250 global
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# header-type 3
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
```

```
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 10.1.1.2
switch(confiq-erspan-src)# source interface ethernet 1/15 both
switch(config-erspan-src)# marker-packet 100
switch(config-erspan-src)# no shut
switch(config-erspan-src)# show monitor session 1
session 1
_____
type
                 : erspan-source
state
                : up
granularity
                : nanoseconds
erspan-id
                : 1
vrf-name
                 : default
               : 10.1.1.2
destination-ip
ip-ttl
                 : 16
ip-dscp
                : 5
header-type
                : 3
origin-ip
                : 172.28.15.250 (global)
source intf
                 :
                : Eth1/15
   rx
   tx
                : Eth1/15
   both
                : Eth1/15
   rx
marker-packet : enabled
packet interval : 100
               : 25
packet sent
packet failed
                : 0
egress-intf
                 :
```

UDF ベース ERSPAN の設定例

次に、以下の一致基準を使用して、カプセル化された IP-in-IP パケットの内部 TCP フラグで照 合する UDF ベース ERSPAN を設定する例を示します。

- ・外部送信元 IP アドレス: 10.0.0.2
- 内部 TCP フラグ:緊急 TCP フラグを設定
- ・バイト: Eth Hdr(14) + 外部 IP(20) + 内部 IP(20) + 内部 TCP(20、ただし、13 番目の バイトの TCP フラグ)
- パケットの先頭からのオフセット:14+20+20+13=67
- UDF の照合値: 0x20
- UDF マスク: 0xFF

```
udf udf_tcpflags packet-start 67 1
hardware access-list tcam region racl qualify udf udf_tcpflags
copy running-config startup-config
reload
ip access-list acl-udf
permit ip 10.0.0.2/32 any udf udf_tcpflags 0x20 0xff
monitor session 1 type erspan-source
source interface Ethernet 1/1
filter access-group acl-udf
```

次に、以下の一致基準を使用して、レイヤ4ヘッダーの先頭から6バイト目のパケット署名 (DEADBEEF)と通常のIPパケットを照合するUDFベース ERSPAN を設定する例を示しま す。

- ・外部送信元 IP アドレス: 10.0.0.2
- 内部 TCP フラグ: 緊急 TCP フラグを設定
- バイト: Eth Hdr (14) + IP (20) + TCP (20) + ペイロード: 112233445566DEADBEEF7788
- レイヤ4ヘッダーの先頭からのオフセット:20+6=26
- UDFの照合値: 0xDEADBEEF(2バイトのチャンクおよび2つの UDF に分割)
- UDF マスク: 0xFFFFFFF

```
udf udf_pktsig_msb header outer 13 26 2
udf udf_pktsig_lsb header outer 13 28 2
hardware access-list tcam region racl qualify udf udf_pktsig_msb udf_pktsig_lsb
copy running-config startup-config
reload
ip access-list acl-udf-pktsig
permit udf udf_pktsig_msb 0xDEAD 0xFFFF udf udf_pktsig_lsb 0xBEEF 0xFFFF
monitor session 1 type erspan-source
source interface Ethernet 1/1
filter access-group acl-udf-pktsig
```

ERSPAN 切り捨ての設定例

次に、MPLS ストリッピングで使用する ERSPAN 切り捨てを設定する例を示します。

```
mpls strip
ip access-list mpls
  statistics per-entry
  20 permit ip any any redirect Ethernet1/5
interface Ethernet1/5
  switchport
  switchport mode trunk
 mtu 9216
 no shutdown
monitor session 1
  source interface Ethernet1/5 tx
 mtu 64
 destination interface Ethernet1/6
 no shut
monitor session 21 type erspan-source
 description "ERSPAN Session 21"
 header-type 3
 erspan-id 21
  vrf default
  destination ip 10.1.1.2
 source interface Ethernet1/5 tx
 mtu 64
 no shut
monitor session 22 type erspan-source
 description "ERSPAN Session 22"
 erspan-id 22
```

```
vrf default
destination ip 10.2.1.2
source interface Ethernet1/5 tx
mtu 750
no shut
monitor session 23 type erspan-source
description "ERSPAN Session 23"
header-type 3
marker-packet 1000
erspan-id 23
vrf default
destination ip 10.3.1.2
source interface Ethernet1/5 tx
mtu 1000
no shut
```

IPv4 上の構成例

次に、ERSPAN 接続先セッションを構成する例を示します。

destination interface eth1/1 はスイッチポート モニタ モードです。このインターフェイスは、 mpls strip、tunnel、nv Overlay、vn-segment-vlan-based、mpls segment-routing、mpls evpn、mpls static、mpls oam、mpls l3vpn、mpls ldp、および nv overlay evpn 機能と共存できません。

```
switch# monitor session 1 type erspan-destination
switch(config)# erspan-id 1
switch(config-erspan-dst)# source ip 10.1.1.1
switch(config-erspan-dst)# destination interface eth1/1
switch(config-erspan-dst)# no shut
switch(config-erspan-dst)# exit
```

I

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。