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

ERSPAN は、IPv4 または IPv6 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 ー 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 ー 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

（注） SPAN/ERSPAN をサポートする他のすべてのスイッチは、TCAM カービングを使用する必要があります。

- フィルタ アクセス グループの統計情報はサポートされていません。
- ERSPAN セッションのアクセス グループ フィルタは、vlan-accessmap として設定する必要があります。
- スーパーバイザによって生成されたコントロール プレーン パケットは、ERSPAN カプセル化または ERSPAN アクセス コントロール リスト（ACL）によるフィルタ処理をすることはできません。
- ERSPAN は、管理ポートではサポートされません。
- ERSPAN は、レイヤ 3 ポート チャネル サブインターフェイスの宛先をサポートしません。
- 送信元としての VLAN は、R シリーズ ライン カードおよび N3K-C36180YC-R、N3KC36480LD-R2、および N3K-C3636C-R プラットフォーム スイッチの ERSPAN 設定ではサポートされません。
- VLAN は、ERSPAN 送信元またはフィルタとして使用される場合、属することができるのは 1 つのセッションだけです。
- VLAN ERSPAN がモニタするのは、VLAN のレイヤ 2 ポートを出入りするトラフィックだけです。
- vPC で ERSPAN をイネーブルにし、ERSPAN パケットが vPC を介して宛先にルーティングされなければならない場合は、vPC ピア リンクを通過するパケットはキャプチャできません。
- ERSPAN は、VXLAN オーバーレイではサポートされません。
- マルチキャスト パケットの ERSPAN コピーは、書き換え前に作成されます。したがって、TTL、VLAN ID、出力ポリシーによる再マーキングなどは ERSPAN コピーにキャプチャされません。
- ERSPAN タイプ III セッションのタイムスタンプの粒度は、CLI では設定できません。100 ピコ秒で、PTP を介して駆動されます。
- ERSPAN はデフォルトおよびデフォルト以外の VRF で動作しますが、ERSPAN マーカー パケットはデフォルト VRF でのみ動作します。
- 同じ送信元は、複数のセッションの一部にすることができます。

次の注意事項と制約事項が （Tx）ERSPAN に適用されます。

- 不明ユニキャストでフラッディングされたパケットのルーティング後のフローは ERSPAN セッションに置かれますが、これはフローが転送されるポートをモニタしないよう ERSPAN セッションが設定されている場合であっても同様です。この制限は、ネットワーク フォ

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 ERSPAN Tx 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。
- IPv6 経由の ERSPAN 宛先には、次の注意事項と制約事項が適用されます。
  - Cisco NX-OS リリース 10.2(1)F 以降、IPv6 機能経由の ERSPAN は Cisco Nexus 9300-GX2、9300-GX、9300-FXP、9300-FX2、9300-EX、9300-FX3、9300-FX3S、および 9300-FX3P プラットフォーム スイッチ、 N9K-X9716D-GX、N9K-X9736C-EX、N9K-X9732C-EX（X86_64 Atom）、N9K-X9732C-EXM、N9K-X97160YC-EX、および N9K-X9736C-FX ライン カードでサポートされています。
  - この機能は、出力ポート チャネル メンバーと出力 ECMP パス間のロード バランシングではサポートされません。
  - この機能は、ヘッダータイプ 3、フィルタ ACL の udf、およびマーカー パケットではサポートされません。
  - この機能は、IPv6 の ERSPAN 送信元としての FEX ホスト インターフェイスではサポートされません。

- Cisco NX-OS リリース 10.2(3)F 以降、IPv6 機能経由の ERSPAN 接続先/終端先は Cisco Nexus 9300-GX2、9300-GX、9300-FXP、9300-FX2、9300-EX、9300-FX3、9300-FX3S、および 9300-FX3P プラットフォーム スイッチ、 N9K-X9716D-GX、N9K-X9736C-EX、N9K-X9732C-EX（X86_64 Atom）、N9K-X9732C-EXM、N9K-X97160YC-EX、および N9K-X9736C-FX ライン カードでサポートされています。
- 次の注意事項と制限事項が適用されます。
  - VRF デフォルトのみがサポートされています。
  - スイッチごとに設定できる IPv6 アドレスは 1 つだけです。
  - この機能は、ほかのトンネル機能ではサポートされていません。
  - 一度に 4 つの ERSPAN 宛先セッションを起動できます。
  - ERSPAN ID はセッションごとに一意で、範囲は 1～32 です。

- Cisco NX-OS リリース 10.3(1)F 以降、Cisco Nexus 9808 プラットフォーム スイッチで ERSPAN のサポートが提供されます。
  - ERSPAN では RX のみがサポートされています。
  - タイプ 3 ヘッダーはサポートされていません。

- ERSPAN 接続先/終端 はサポートされていません。

- Cisco NX-OS リリース 10.4(1)F 以降、ERSPAN は次のスイッチおよびライン カードでサポートされます。
  - Cisco Nexus 9332D-H2R スイッチ
  - Cisco Nexus 9804 スイッチ
    - タイプ 3 ヘッダーはサポートされていません
    - ERSPAN 接続先/終端 はサポートされていません
  - Cisco Nexus X98900CD-A および X9836DM-A ラインカードと Cisco Nexus 9808 および 9804 スイッチ

- Cisco NX-OS リリース 10.4(2)F 以降、Cisco Nexus 9300-H2R プラットフォーム スイッチは、ERSPAN 送信元セッションの入力方向の ACL ドロップで SPAN をサポートします。
- Cisco NX-OS リリース 10.4(2)F 以降、ERSPAN 送信元および宛先としてのレイヤ 3 ポート チャネル インターフェイスは 9804 および 9808 プラットフォーム スイッチでサポートされます。ただし、次の注意事項と制限事項が適用されます。
  - ポート チャネルでのミラー トラフィックのロード バランシングはサポートされていません。i
  - セッション間での同じ送信元ポートまたはインターフェイスの共有はサポートされていません。
  - 一度に最大 10 台のモニタ セッションがサポートされます。
  - 一度に 10 個のアクティブ SPAN セッションがサポートされます。
  - ERSPAN MTU 切り捨ては、FCS を除き、9804 および 9808 スイッチ では 343 バイトでのみサポートされます。
  - ERSPAN タイプ 3 ヘッダーはサポートされていません。
  - ERSPAN 接続先/終端 はサポートされていません。
  - ERSPAN レイヤ 2 インターフェイス（スイッチ ポート）および送信元としての VLAN はサポートされていません。
  - UDF ベースの ERSPAN はサポートされていません。
  - ERSPAN ミラー パケットには個別の SPAN 出力キューがなく、デフォルト キューが使用されます。
  - ポート チャネル インターフェイス（複数のメンバー ポートを持つ）が ERSPAN 宛先として構成されている場合、1 つのメンバー インターフェイスだけがミラーリングされたトラフィックの送信に使用されます。

- メンバーの選択はソフトウェアで行われるため、メンバーシップが変更されるとパケット損失が発生します。

- Cisco NX-OS リリース 10.4(2)F 以降、ERSPAN は Cisco Nexus 93400LD-H1 プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(3)F 以降、ERSPAN は Cisco Nexus 9364C-H1 プラットフォーム スイッチ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。

手順の概要

1. **configure terminal**
2. **monitor erspan origin ip-address** *ip-address* **global** or **monitor erspan origin ipv6-address** *ipv6-address* **global**
3. **no monitor session** {*session-number* | **all**}
4. **monitor session** {*session-number* | **all**} **type erspan-source** [**shut**]

5. **description** *description*
6. **source** {**interface** *type* [**tx** | **rx** |**both**] **vlan** {**number** | **range**} [**rx**]}
7. （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。
8. **filter vlan** {*number* | *range*}
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。
10. （任意） **filter access-group** *acl-filter*
11. **destination ip** *ip-address*
12. **erspan-id** *erspan-id*
13. **vrf** *vrf-name*
14. （任意） **ip ttl** *ttl-number*
15. （任意） **ip dscp** *dscp-number*
16. **no shut**
17. **exit**
18. （任意） **show monitor session** {**all** | *session-number* | **range** *session-range*} [**brief**]
19. （任意） **show running-config monitor**
20. （任意） **show startup-config monitor**
21. （任意） **copy running-config startup-config**

手順の詳細

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** *ip-address* **global** or **monitor erspan origin ipv6-address** *ipv6-address* **global** 例： `switch(config)# monitor erspan origin ip-address 10.0.0.1 global` `switch(config)# monitor erspan origin ipv6-address 2001:DB8:1::1 global`	ERSPAN のグローバルな送信元 IPv4 または IPv6 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。

	コマンドまたはアクション	目的
ステップ 4	**monitor session** {*session-number* | **all**} **type erspan-source** [**shut**] 例： `switch(config)# monitor session 3 type erspan-source` `switch(config-erspan-src)#`	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	**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 sup-eth 0 rx` 例： `switch(config-erspan-src)# source vlan 3, 6-8 rx` 例： `switch(config-erspan-src)# source interface ethernet 101/1/1-3`	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。コピーするト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。 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 7	（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

	コマンドまたはアクション	目的
		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、*Cisco Nexus 9000* シリーズ *NX-OS* 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。） （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** *ip-address* 例： `switch(config-erspan-src)# destination ip 10.1.1.1` `switch(config-erspan-src)# destination ipv6 2001:DB8:1::1`	**destination ipv6** *ipv6-address* ERSPAN セッションの宛先 IPv4 または IPv6 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 IPv4 または IPv6 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 13	**vrf** *vrf-name* 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** *ttl-number* 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。

	コマンドまたはアクション	目的
ステップ 15	（任意） **ip dscp** *dscp-number* 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。
ステップ 18	（任意） **show monitor session** {**all** | *session-number* | **range** *session-range*} [**brief**] 例： `switch(config)# show monitor session 3`	ERSPAN セッション設定を表示します。
ステップ 19	（任意） **show running-config monitor** 例： `switch(config)# 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。
ステップ 20	（任意） **show startup-config monitor** 例： `switch(config)# 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。
ステップ 21	（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 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。

手順の概要

1. **configure terminal**
2. **monitor session** {*session-range* | **all**} **shut**
3. **no monitor session** {*session-range* | **all**} **shut**
4. **monitor session** *session-number* **type erspan-source**
5. **shut**
6. **no shut**
7. **exit**
8. （任意） **show monitor session all**
9. （任意） **show running-config monitor**
10. （任意） **show startup-config monitor**
11. （任意） **copy running-config startup-config**

手順の詳細

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 session** {*session-range* | **all**} **shut** 例： `switch(config)# monitor session 3 shut`	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 shut`	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。 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	**monitor session** *session-number* **type erspan-source** 例： `switch(config)# monitor session 3 type erspan-source` `switch(config-erspan-src)#`	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。

	コマンドまたはアクション	目的
ステップ 5	**shut** 例： `switch(config-erspan-src)# shut`	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 7	**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。
ステップ 9	（任意） **show running-config monitor** 例： `switch(config)# 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。
ステップ 10	（任意） **show startup-config monitor** 例： `switch(config)# 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。
ステップ 11	（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 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。

手順の概要

1. **configure terminal**
2. **ip access-list** *acl-name*
3. [*sequence-number*] {**permit** | **deny**} *protocol source destination*
4. **vlan access-map erpsan-acl** *map name* [*sequence-number*]
5. **match ip address** *acl-name*
6. **action forward**
7. **exit**

8. **monitor session** [*session-number*| **all**] **type erspan-source** [**shut**]
9. **filter access_group** *name*
10. （任意） **copy running-config startup-config**

手順の詳細

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** *acl-name* 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。*acl-name* 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* 例： `switch(config-acl)# permit ip 192.168.2.0/24 any` 例： `switch(config)# ip access-list match_11_pkts` `switch(config-acl)# permit ip 10.0.0.0/24 any` `switch(config-acl)# exit`	ERSPAN ACL 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。 **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。
ステップ 4	**vlan access-map erpsan-acl** *map name* [*sequence-number*] 例： `switch(config)# vlan access-map erspan_filter`	指定した VLAN アクセス マップの VLAN アクセス マップ コンフィギュレーション モードを開始します。VLAN アクセス マップが存在しない場合は、デバイスによって作成されます。 シーケンス番号を指定しなかった場合、デバイスによって新しいエントリが作成され、このシーケンス番号はアクセス マップの最後のシーケンス番号よりも 10 大きい番号となります。
ステップ 5	**match ip address** *acl-name* 例： `switch(config-access-map)# match ip address erspan-acl`	アクセス マップ エントリに ACL を指定します。
ステップ 6	**action forward** 例：	ACL に一致したトラフィックにデバイスが適用する処理を指定します。

	コマンドまたはアクション	目的
	`switch(config-access-map)# action forward`	
ステップ 7	**exit** 例： `switch(config-access-map)# exit`	VLAN アクセスマップ コンフィギュレーション モードを終了します。
ステップ 8	**monitor session** [*session-number*| **all**] **type erspan-source** [**shut**] 例： `switch(config)# monitor session 1 type erspan-source`	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 9	**filter access_group** *name* 例： `switch(config-erspan-src)# filter access_group erspan_filter`	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、*Cisco Nexus 9000* シリーズ *NX-OS* セキュリティ構成ガイドを参照してください。）
ステップ 10	（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。

ERSPAN ACL 構成の確認

ERSPAN ACL 構成を表示するには、次の表に示す適切な show コマンドを実行します。

コマンド	目的
show ip access-lists *name* 例： `switch(config-acl)# show ip access-lists erpsan-acl`	ERSPAN ACL の設定を表示します。
show vlan access-map *name* 例： `switch(config-acl)# show vlan access-map erspan_filter`	VLAN アクセス マップに関する情報を表示します。
show monitor session {**all** | *session-number* | **range** *session-range*} [**brief**] 例： `switch(config-acl)# show monitor session 1`	ERSPAN セッション設定を表示します。

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。

手順の概要

1. **configure terminal**
2. **udf** *udf-name offset-base offset length*
3. **hardware access-list tcam region** {**racl | ifacl | vacl** }**qualify udf** *udf-names*
4. **copy running-config startup-config**
5. **reload**
6. **ip access-list** *erspan-acl*
7. 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*
8. （任意） **copy running-config startup-config**

手順の詳細

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	**udf** *udf-name offset-base offset length* 例： `switch(config)# udf udf-x packet-start 12 1` `switch(config)# udf udf-y header outer l3 20 2`	次のように UDF を定義します。 • *udf-name*：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。 • *offset-base*：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

	コマンドまたはアクション	目的
		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** {**l3** | **l4**}}. • 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 access-list tcam region** {**racl** | **ifacl** | **vacl** }**qualify udf** *udf-names* 例： `switch(config)# hardware access-list tcam region racl qualify udf udf-x udf-y`	次のいずれかの TCAM リージョンに UDF を付加します。 • 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。 （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。

	コマンドまたはアクション	目的
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 7	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： `switch(config-acl)# permit udf udf-x 0x40 0xF0 udf-y 0x1001 0xF00F` 例： `switch(config-acl)# permit ip 10.0.0.0/24 any udf udf-x 0x02 0x0F udf-y 0x1001 0xF00F`	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） 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。

手順の概要

1. **configure terminal**
2. **monitor session** *session-number* **type erspan-source**
3. **source interface** *type slot*/*port* [**rx** | **tx** | **both**]
4. **mtu** *size*
5. **destination interface** *type slot*/*port*
6. **no shut**
7. （任意） **show monitor session** *session*

8. **copy running-config startup-config**

手順の詳細

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)#`	グローバル設定モードを開始します。
ステップ 2	**monitor session** *session-number* **type erspan-source** 例： `switch(config)# monitor session 10 type erspan-source` `switch(config-erspan-src)#`	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。
ステップ 3	**source interface** *type slot/port* [**rx** | **tx** | **both**] 例： `switch(config-erspan-src)# source interface ethernet 1/5 both`	送信元インターフェイスを設定します。
ステップ 4	**mtu** *size* 例： `switch(config-erspan-src)# mtu 512` 例： `switch(config-erspan-src)# mtu ?` `<512-1518> Enter the value of MTU truncation size for ERSPAN packets (erspan header + truncated original packet)`	MTU の切り捨てサイズを設定します。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 パケットの切り捨てのMTU範囲は次のとおりです。 • Cisco Nexus 9300-EX シリーズ スイッチの MTU サイズの範囲は 512ー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ー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ー1518 バイトです。 • Cisco Nexus 9808 および 9804 プラットフォーム スイッチの MTU サイズは 343 バイトです（FCS を除く）。
ステップ 5	**destination interface** *type slot/port* 例： `switch(config-erspan-src)# destination interface Ethernet 1/39`	イーサネット ERSPAN 宛先ポートを設定します。

	コマンドまたはアクション	目的
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 7	（任意） **show monitor session** *session* 例： `switch(config-erspan-src)# show monitor session 5`	ERSPAN の設定を表示します。
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。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot/port*[*-port*]
3. **switchport**
4. **switchport mode** [**access** | **trunk**]
5. **switchport monitor**
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。
7. **no monitor session** {*session-number* | **all**}
8. **monitor session** {*session-number* | **all**} **type erspan-destination**
9. **description** *description*
10. **source ip** *ip-address*
11. **destination** {[**interface** [*type slot/port*[*-port*]]] [**port-channel** *channel-number*]]}
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。
13. **erspan-id** *erspan-id*
14. **no shut**
15. **exit**
16. **exit**
17. （任意） **show monitor session** {**all** | *session-number* | **range** *session-range*}

18. （任意） **show running-config monitor**
19. （任意） **show startup-config monitor**
20. （任意） **copy running-config startup-config**

手順の詳細

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** *slot/port*[*-port*] 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	**switchport** 例： `switch(config-if)# switchport`	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	**switchport mode** [**access** | **trunk**] 例： `switch(config-if)# switchport mode trunk`	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	**switchport monitor** 例： `switch(config-if)# switchport monitor`	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 7	**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	**monitor session** {*session-number* | **all**} **type erspan-destination** 例：	ERSPAN 宛先セッションを設定します。

	コマンドまたはアクション	目的
	`switch(config-if)# monitor session 3 type erspan-destination` `switch(config-erspan-dst)#`	
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	**source ip** *ip-address* 例： `switch(config-erspan-dst)# source ip 10.1.1.1` `switch(config-erspan-dst)# source ipv6 2001:DB8:1::1`	**source ipv6** *ipv6-address* ERSPAN セッションの宛先 IPv4 または IPv6 アドレスを構成します。送信元 IPv4 または IPv6 アドレスは、ローカルに構成された IPv4 または IPv6 アドレスです。ERSPAN 宛先セッションの送信元 IPv4 または IPv6 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 IPv4 または IPv6 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 IPv4 または IPv6 アドレスのみがサポートされます。 （注） IPv6 は、Cisco NX-OS リリース 10.2(3)F からサポートされています。
ステップ 11	**destination** {[**interface** [*type slot/port*[*-port*]]] [**port-channel** *channel-number*]]} 例： `switch(config-erspan-dst)# destination interface ethernet 2/5`	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。

	コマンドまたはアクション	目的
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。
ステップ 17	（任意） **show monitor session** {**all** | *session-number* | **range** *session-range*} 例： `switch(config)# show monitor session 3`	ERSPAN セッション設定を表示します。
ステップ 18	（任意） **show running-config monitor** 例： `switch(config-erspan-src)# 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。
ステップ 19	（任意） **show startup-config monitor** 例： `switch(config-erspan-src)# 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。
ステップ 20	（任意） **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 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
show monitor session {**all** | *session-number* | **range** *session-range*} [**brief**]	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

IPv6 経由の ERSPAN 送信元セッションの設定例

次に、IPv6 経由の ERSPAN 送信元セッションを設定する例を示します。

```
switch# configure terminal
switch(config)# monitor erspan origin ipv6-address 2001::10:0:0:9 global
switch(config)# moni session 10 type erspan-source
switch(config-erspan-src)# erspan-id 10
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# source interface ethernet 1/64
switch(config-erspan-src)# destination ip 10.1.1.2
```

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 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(config-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
destination-ip    : 10.1.1.2
ip-ttl            : 16
ip-dscp           : 5
header-type       : 3
origin-ip         : 172.28.15.250 (global)
source intf       :
    rx            : Eth1/15
    tx            : Eth1/15
    both          : Eth1/15
    rx            :
marker-packet     : enabled
packet interval   : 100
packet sent       : 25
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：0xFFFFFFFF

```
udf udf_pktsig_msb header outer l3 26 2
udf udf_pktsig_lsb header outer l3 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 ERSPAN 接続先セッションの構成例

次に、IPv4 上で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
```

IPv6 上の ERSPAN 接続先セッションの構成例

次に、IPv6 上で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 ipv6 2001:DB8:1::1
switch(config-erspan-dst)# destination interface eth1/1
```

```
switch(config-erspan-dst)# no shut
switch(config-erspan-dst)# exit
```

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。