ローカル SPAN および ERSPAN の設定

この章は、次の項で構成されています。

ERSPAN に関する情報

Cisco NX-OS システムは、発信元および宛先ポートの両方で Encapsulated Remote Switching Port Analyzer（ERSPAN）機能をサポートします。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。

ERSPAN は、ERSPAN 送信元セッション、ルーティング可能な ERSPAN Generic Routing Encapsulation（GRE）カプセル化トラフィック、および ERSPAN 宛先セッションで構成されています。異なるスイッチで ERSPAN 送信元セッションおよび宛先セッションを個別に設定することができます。ACL を使用し、入力トラフィックをフィルタ処理するように ERSPAN 送信元セッションを設定することもできます。

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 ポートおよびポート チャネル。

- VLAN：VLAN が ERSPAN 送信元として指定されている場合、VLAN でサポートされているすべてのインターフェイスが ERSPAN 送信元となります。

ERSPAN 送信元ポートには、次の特性があります。

- 送信元ポートとして設定されたポートを宛先ポートとしても設定することはできません。
- 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ーしません。
- ACL を使用して送信元ポートで入力トラフィックをフィルタし、ACL 基準に一致する情報のパケットのみがミラーリングされるようにすることができます。

マルチ ERSPAN セッション

最大 18 個の ERSPAN セッションを定義できますが、同時に作動できるのは最大 4 個の ERSPAN または SPAN セッションのみです。受信ソースと送信ソースの両方が同じセッションに設定されている場合、同時に作動できるのは 2 つの ERSPAN または SPAN セッションのみです。未使用の ERSPAN セッションはシャットダウンもできます。

（注） Cisco Nexus 34180YC プラットフォーム スイッチは、スイッチに設定されている合計で 32 セッションの SPAN および ERSPAN セッションをサポートします。32 すべてのセッションを同時にアクティブにできます。

ERSPAN セッションのシャットダウンについては、ERSPAN セッションのシャットダウンまたはアクティブ化 （19 ページ）を参照してください。

高可用性

ERSPAN 機能はステートレス およびステートフル リスタートをサポートします。リブートまたはスーパーバイザ スイッチオーバー後に、実行コンフィギュレーションが適用されます。

ERSPAN の前提条件

ERSPAN の前提条件は、次のとおりです。

•所定の ERSPAN 設定をサポートするには、まず各デバイス上でポートのイーサネット インターフェイスを設定する必要があります。詳細については、お使いのプラットフォームのインターフェイス コンフィギュレーション 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

ERSPAN 設定時の注意事項と制限事項は次のとおりです。

- 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。
- 複数の ACL フィルタは、同じ送信元でサポートされます。
- 2 つの ERSPAN 宛先セッションは、Cisco Nexus 3000、3100、および 3200 プラットフォーム スイッチではサポートされていません。
- Cisco Nexus 34180YC プラットフォーム スイッチには次の制限が適用されます。
  - ERSPAN では、PortChannel は宛先インターフェイスとしてサポートされていません。
  - ACL フィルタと VLAN フィルタはサポートされていません。
  - ERSPAN UDF ベースの ACL サポートはサポートされていません
  - Cisco Nexus 34180YC プラットフォーム スイッチは、スイッチに設定されている合計で 32 セッションの SPAN および ERSPAN セッションをサポートします。32 すべてのセッションを同時にアクティブにできます。
  - **filter access-group** コマンドは、Cisco Nexus 34180YC プラットフォーム スイッチでサポートされていません。
  - スーパーバイザに対する ERSPAN はサポートされていません。
  - ERSPAN での IPv6 ベースのルーティングおよび IPv6 UDF はサポートされていません。
- ERSPAN は次をサポートしています。
  - 4 ～ 6 個のトンネル
  - トンネルなしパケット
  - IP-in-IP トンネル
  - IPv4 トンネル（制限あり）
  - Cisco Nexus 3000 シリーズ スイッチでは、ERSPAN 送信元セッションと一致するパケットのスパニングに汎用 GRE ERSPAN ヘッダー形式を使用します。この形式は、Cisco ERSPAN タイプ 1/2/3 ヘッダー形式に準拠していません。Cisco ASIC ベースのプラットフォームでは、Cisco ERSPAN カプセル化形式タイプに準拠した ERSPAN パケットに対してのみ ERSPAN 終端およびカプセル化解除がサポートされます。したがって、Cisco Nexus 3000 シリーズ スイッチから CISCO ASIC ベース スイッチのローカル宛先 IP アドレスに対して発信される ERSPAN パケットは ERSPAN 終端フィルタと一致しません。宛先 IP アドレスが Cisco ASIC プラットフォーム上のローカル IP アドレスでもある場合、ERSPAN パケットはソフトウェアに送信され、ソフトウェアでドロップされます。

  - ERSPAN 宛先セッション タイプ（ただし、ERSPAN パケットのカプセル化を解除するためのサポートは使用できません。カプセル化されたパケット全体は、ERSPAN 終端ポイントの前面パネル ポートにスパンされます）。

- ERSPAN パケットは、カプセル化されたミラー パケットがレイヤ 2 MTU のチェックに失敗した場合、ドロップされます。
- 出力カプセルでは 112 バイトの制限があります。この制限を超えるパケットはドロップされます。このシナリオは、トンネルとミラーリングが混在する場合に発生することがあります。
- ERSPAN セッションは複数のローカル セッションで共有されます。最大 18 セッションが設定できます。ただし、同時に動作できるのは最大 4 セッションのみです。受信ソースと送信ソースの両方が同じセッションで設定されている場合、2 セッションのみが動作できます。
- NX-OS 5.0(3)U2(2) をインストールして ERSPAN を設定し、その後でソフトウェアを以前のバージョンにダウングレードすると、ERSPAN の設定は失われます。これは、ERSPAN が NX-OS 5.0(3)U2(2) よりも前のバージョンでサポートされていないためです。

  同様の SPAN の制約事項については、SPAN の注意事項および制約事項を参照してください。
- ERSPAN および ERSPAN（ACL フィルタリングあり）は、スーパーバイザが生成したパケットではサポートされません。
- ACL フィルタリングは、Rx ERSPAN に対してのみサポートされます。Tx ERSPAN は、送信元インターフェイスで出力されるすべてのトラフィックをミラーリングします。
- ACL フィルタリングは、TCAM 幅の制限があるため、IPv6 および MAC ACL ではサポートされません。
- 同じ送信元が複数の ERSPAN セッションで設定されていて、各セッションに ACL フィルタが設定されている場合、送信元インターフェイスは、最初のアクティブ ERSPAN セッションに対してのみプログラムされます。その他のセッションに属する ACE には、この送信元インターフェイスはプログラムされません。
- 同じ送信元を使用するように ERSPAN セッションおよびローカル SPAN セッション（filter access-group および allow-sharing オプションを使用）を設定する場合は、設定を保存してスイッチをリロードすると、ローカル SPAN セッションがダウンします。
- モニター セッションの filter access-group を使用する VLAN アクセスマップ設定では、ドロップ アクションはサポートされていません。モニター セッションでドロップ アクションのある VLAN アクセスマップに filter access-group が設定されている場合、モニターセッションはエラー状態になります。
- 許可 ACE と拒否 ACE は、どちらも同様に処理されます。ACE と一致するパケットは、ACL の許可エントリまたは拒否エントリを含んでいるかどうかに関係なく、ミラーリングされます。
- ERSPAN は、管理ポートではサポートされません。

- 宛先ポートは、一度に 1 つの ERSPAN セッションだけで設定できます。
- ポートを送信元ポートと宛先ポートの両方として設定することはできません。
- 1 つの ERSPAN セッションに、次の送信元を組み合わせて使用できます。
  - イーサネット ポートまたはポート チャネル（サブ インターフェイスを除く）。
  - ポート チャネル サブインターフェイスに割り当てることのできる VLAN またはポート チャネル。
  - コントロール プレーン CPU へのポート チャネル。

（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ーしません。

- 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。
- ERSPANセッションに、送信方向または送受信方向でモニターされている送信元ポートが含まれている場合、パケットが実際にはその送信元ポートで送信されなくても、これらのポートを受け取るパケットが ERSPAN の宛先ポートに複製される可能性があります。送信元 ポート上でのこの動作の例を、次に示します。
  - フラッディングから発生するトラフィック
  - ブロードキャストおよびマルチキャスト トラフィック
- 入力と出力の両方が設定されている VLAN ERSPAN セッションでは、パケットが同じ VLAN 上でスイッチングされる場合に、宛先ポートから 2 つのパケット（入力側から 1 つ、出力側から 1 つ）が転送されます。
- VLAN ERSPAN がモニターするのは、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。
- Cisco Nexus 3000 シリーズ スイッチが ERSPAN 宛先の場合、GRE ヘッダーは、終端ポイントからミラー パケットが送信される前には削除されません。パケットは、GRE パケットである GRE ヘッダー、および GRE ペイロードである元のパケットとともに送信されます。
- ERSPAN 送信元セッションの出力インターフェイスは、**show monitor session <session-number>** CLI コマンドの出力に表示されるようになりました。出力インターフェイスには、物理ポートまたは port-channel を指定できます。ECMP の場合、ECMP メンバー内の 1 つのインターフェイスが出力に表示されます。この特定のインターフェイスがトラフィックの出力に使用されます。
- SPAN/ERSPAN ACL 統計情報は、**show monitor filter-list** コマンドを使用して表示できます。このコマンドの出力には、SPAN TCAM の統計情報とともにすべてのエントリが表示されます。ACL 名は表示されず、エントリのみ出力に表示されます。統計情報は、**clear monitor filter-list statistics** コマンドを使用してクリアできます。出力は、**show ip access-list**

コマンドの出力と同様です。Cisco Nexus 3000 シリーズ スイッチは、ACL レベルごとの統計情報をサポートしていません。この機能強化は、ローカル SPAN および ERSPAN の両方でサポートされています。

- CPU とやりとりされるトラフィックはスパニングされます。その他のインターフェイス SPAN に似ています。この機能強化は、ローカル SPAN でのみサポートされています。ACL 送信元ではサポートされていません。Cisco Nexus 3000 シリーズ スイッチは、CPU から送信される（RCPU.dest_port != 0）ヘッダー付きのパケットはスパニングしません。
- SPAN 転送ドロップ トラフィックの場合、フォワーディング プレーンにおけるさまざまな原因でドロップされるパケットのみ SPAN されます。この機能強化は、ERSPAN 送信元セッションでのみサポートされています。SPAN ACL、送信元 VLAN、および送信元インターフェイスとともにはサポートされません。SPAN のドロップ トラフィックには、3 つの ACL エントリがインストールされます。ドロップ エントリに優先度を設定して、その他のモニター セッションの SPAN ACL エントリや VLAN SPAN エントリよりも高いまたは低い優先度にすることができます。デフォルトでは、ドロップエントリの優先度の方が高くなります。
- SPAN UDF（ユーザー定義フィールド）ベースの ACL サポート
  - パケットの最初の 128 バイトのパケット ヘッダーまたはペイロード（一定の長さ制限あり）を照合できます。
  - 照合のために、特定のオフセットと長さを指定して UDF を定義できます。
  - 1 バイトまたは 2 バイトの長さのみ照合できます。
  - 最大 8 個の UDF がサポートされます。
  - 追加の UDF 一致基準が ACL に追加されます。
  - UDF 一致基準は、SPAN ACL に対してのみ設定できます。この機能強化は、その他の ACL 機能（RACL、PACL、および VACL）ではサポートされていません。
  - ACE ごとに最大 8 個の UDF 一致基準を指定できます。
  - UDF および HTTP リダイレクト設定を、同じ ACL に共存させることはできません。
  - UDF 名は、SPAN TCAM に適合している必要があります。
  - UDF は、SPAN TCAM によって認定されている場合のみ有効です。
  - UDF 定義の設定および SPAN TCAM での UDF 名の認定では、**copy r s** コマンドを使用して、リロードする必要があります。
  - UDF の照合は、ローカル SPAN と ERSPAN 送信元セッションの両方でサポートされています。
  - UDF 名の長さは最大 16 文字です。
  - UDF のオフセットは 0（ゼロ）から始まります。オフセットが奇数で指定されている場合、ソフトウェアの 1 つの UDF 定義に対して、ハードウェアで 2 つの UDF が使用

されます。ハードウェアで使用している UDF の数が 8 を超えると、その設定は拒否されます。

- UDF の照合では、SPAN TCAM リージョンが倍幅になる必要があります。そのため、その他の TCAM リージョンのサイズを減らして、SPAN の領域を確保する必要があります。
- SPAN UDF は、タップ アグリゲーション モードではサポートされていません。

- erspan-src セッションに sup-eth 送信元インターフェイスが設定されている場合、acl-span を送信元としてそのセッションに追加することはできません（その逆も同様）。
- ERSPAN 送信元および ERSPAN 宛先セッションでは、専用のループバック インターフェイスを使用する必要があります。そのようなループバック インターフェイスには、どのようなコントロール プレーン プロトコルも使用しません。
- ERSPAN マーケットパケット UDP データ ペイロードは、Cisco Nexus 3000 シリーズ スイッチで 58 バイトです。

ERSPAN のデフォルト設定

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

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。

送信元には、イーサネット ポート、ポート チャネル、および VLAN を指定できます。単一の ERSPAN セッションには、イーサネット ポートまたは VLAN を組み合わせた送信元を使用できます。

（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# config t`
	`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** 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	**monitor session** {*session-number* | **all**} **type erspan-source**
	例：
	`switch(config)# monitor session 3 type erspan-source`
	`switch(config-erspan-src)#`
		ERSPAN 送信元セッションを設定します。

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	**filter access-group** *acl-name* 例： `switch(config-erspan-src)# filter access-group acl1`	ACL リストに基づいて、送信元ポートで入力トラフィックをフィルタリングします。アクセスリストに一致するパケットのみがスパニングされます。*acl-name* には、IP アクセス リストを指定できますが、アクセスマップは指定できません。
ステップ 7	**source** { **interface** *type* [**rx** [**allow-pfc**] | **tx** | **both**] | **vlan** {*number* | *range*} [**rx**] | **forward-drops rx** [**priority-low**]} 例： `switch(config-erspan-src)# source interface ethernet 2/1-3, ethernet 3/1 rx`	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。イーサネット ポート範囲、ポート チャネル、または VLAN 範囲を入力できます。

	コマンドまたはアクション	目的

	例：
	`switch(config-erspan-src)# source interface port-channel 2`
	例：
	`switch(config-erspan-src)# source interface sup-eth 0 both`
	例：
	`switch(config-monitor)# source interface ethernet 101/1/1-3`
		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。最大 128 のインターフェイスを指定できます。VLAN の範囲については、『*Cisco Nexus 3000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。
		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。デフォルトは双方向です。
		allow-pfc オプションは、ポートで受信されるプライオリティ フロー制御（PFC）フレームのスパニングを開始します。PFC フレームは、ドロップされずに入力パイプラインで許可されます。該当ポートに ERSPAN が設定されている場合、それらの PFC フレームは適切な出力インターフェイスにスパニングされます。このオプションを指定して設定されているポートは、通常のデータ トラフィックもスパニングできます。
		インターフェイスまたは VLAN を ERSPAN 送信元として設定する代わりに、入力パイプラインで可能な最大数のフォワードパケット ドロップをスパニングするように ERSPAN 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。デフォルトでは、**source forward-drops rx** コマンドは、ネットワーク転送モジュールのすべてのポートのパケット ドロップをキャプチャします。**priority-low** オプションを指定すると、この ERSPAN アクセス コントロール エントリ（ACE）の一致ドロップ条件は、標準インターフェイスや VLAN ERSPAN ACL によって設定されている

	コマンドまたはアクション	目的
		その他の ERSPAN ACE よりも優先度が低くなります。
ステップ 8	（任意） ステップ 6 を繰り返して、すべての ERSPAN 送信元を設定します。	—
ステップ 9	**destination ip** *ip-address* **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。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 10	（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。
ステップ 11	（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 12	**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。 （**注**） 同時に実行できる ERSPAN 送信元セッションは 2 つだけです。
ステップ 13	（任意） **show monitor session** {**all** | *session-number* | **range** *session-range*} **例：** `switch(config-erspan-src)# show monitor session 3`	ERSPAN セッション設定を表示します。
ステップ 14	（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 15	（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。

	コマンドまたはアクション	目的
ステップ 16	（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 送信元セッションの SPAN 転送ドロップ トラフィックの設定

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# config t`
	`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-number* | **all**} **type erspan-source**
	例：
	`switch(config)# monitor session 1 type erspan-source`
	`switch(config-erspan-src)#`
		ERSPAN 送信元セッションを設定します。

ステップ 3	**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 VRF を設定します。
ステップ 4	**destination ip** *ip-address* 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。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 5	**source forward-drops rx** [*priority-low*] 例： `switch(config-erspan-src)# source forward-drops rx [priority-low]`	ERSPAN 送信元セッションの SPAN 転送ドロップ トラフィックを設定します。低い優先度に設定されている場合、このSPAN ACEの一致ドロップ条件は、ACL SPAN またはVLAN ACL SPAN インターフェイスによって設定されているその他の SPAN ACE よりも優先度が低くなります。priority-low キーワードを指定しない場合、これらのドロップ ACE は、標準インターフェイスや VLAN SPAN ACL よりも優先度が高くなります。優

	コマンドまたはアクション	目的
		先度は、パケットの一致ドロップ ACE およびインターフェイス/VLAN SPAN ACL が設定されている場合のみ問題になります。
ステップ 6	**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。 （注） 同時に実行できる ERSPAN 送信元セッションは 2 つだけです。
ステップ 7	（任意） **show monitor session** {**all** | *session-number* | **range** *session-range*} 例： `switch(config-erspan-src)# show monitor session 3`	ERSPANセッション設定を表示します。

例

```
switch# config t
  switch(config)# monitor session 1 type erspan-source
  switch(config-erspan-src)# vrf default
  switch(config-erspan-src)# destination ip 40.1.1.1
  switch(config-erspan-src)# source forward-drops rx
  switch(config-erspan-src)# no shut
  switch(config-erspan-src)# show monitor session 1

switch# config t
  switch(config)# monitor session 1 type erspan-source
  switch(config-erspan-src)# vrf default
  switch(config-erspan-src)# destination ip 40.1.1.1
  switch(config-erspan-src)# source forward-drops rx  priority-low
  switch(config-erspan-src)# no shut
  switch(config-erspan-src)# show monitor session 1
```

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** *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* [**set-erspan-dscp** *dscp-value*] [**set-erspan-gre-proto** *protocol-value*] 例： `switch(config-acl)# permit ip 192.168.2.0/24 any set-erspan-dscp 40 set-erspan-gre-proto 5555`	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。 **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 値でモニター 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 またはモニター 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 つの宛先モニター セッションを使用します。ERSPAN ACL ごとに、これらのアクションのいずれかが

	コマンドまたはアクション	目的
		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 がある 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 アクションと 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 がある 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た 1 つの ACE がある ACL が設定されている最大 2 つの ERSPAN セッション
ステップ 4	（任意） **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。
ステップ 5	（任意） **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。
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。

ユーザー定義フィールド（UDF）ベースの ACL サポートの設定

Cisco Nexus 3000 シリーズ スイッチにユーザー定義フィールド（UDF）ベースの ACL のサポートを設定できます。次の手順を参照して、UDF に基づく ERSPAN を設定します。詳細については、「ERSPAN の注意事項および制約事項」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	switch# **configure terminal**	グローバル設定モードを開始します。

ステップ 2	switch(config)# **udf** < *udf -name*> <*packet start*> <*offset*> <*length*>
	例：
	`(config)# udf udf1 packet-start 10 2`
	`(config)# udf udf2 packet-start 50 2`
		UDF を定義します。
		（注） 複数の UDF を定義できますが、必要な UDF のみ設定することを推奨します。UDF は、TCAM カービング時（ブートアップ時）にリージョンの修飾子セットに追加されるため、この設定は、UDF を TCAM リージョンにアタッチして、ボックスを再起動した後でのみ有効になります。

ステップ 3	switch(config)# **udf** < *udf -name*> header <*Layer3/Layer4*> <*offset*> <*length*>
	例：
	`(config)# udf udf3 header outer l4 0 1`
	`(config)# udf udf3 header outer l4 10 2`
	`(config)# udf udf3 header outer l4 50 1`
		UDF を定義します。

ステップ 4	switch(config)# **hardware profile tcam region span qualify udf** <*name1*>…… <*name8*>
	例：
	`(config)# hardware profile tcam region span qualify udf udf1 udf2 udf3 udf4 udf5`
	`[SUCCESS] Changes to UDF qualifier set will be applicable only after reboot. You need to 'copy run start' and 'reload'`
	`config)#`
		SPAN TCAM に UDF 認定を設定します。TCAM カービング時（ブートアップ時）に UDF を TCAM リージョンの修飾子セットに追加します。この設定では、SPAN リージョンにアタッチできる最大 4 つの UDF を許可できます。UDF はすべて、リージョンの単一コマンドでリストされます。リージョンの新しい設定により、既存の設定が置き換わりますが、設定を有効にするには再起動する必要があります。

	コマンドまたはアクション	目的
		UDF 修飾子が SPAN TCAM に追加されると、TCAM リージョンはシングル幅から倍幅に拡大します。拡大に使用できる十分な空き領域（128 以上のシングル幅エントリ）があることを確認します。十分な領域がない場合、コマンドは拒否されます。未使用リージョンの TCAM 領域を削減して領域を確保したら、コマンドを再入力します。**no hardware profile tcam region span qualify udf <name1> ..<name8>** コマンドを使用して UDF が SPAN/TCAM リージョンからデタッチされると、SPAN TCAM リージョンはシングル幅エントリであると見なされます。

ステップ 5	switch(config)# **permit** …… <*regular ACE match criteria*> **udf** <*name1*> < *val* > <*mask*> .....<*name8*> < *val* > <*mask*>
	例：
	`(config)# ip access-list test`
	`10 permit ip any any udf udf1 0x1234 0xffff udf3 0x56 0xff`
	`30 permit ip any any dscp af11 udf udf5 0x22 0x22`
	`config)#`
		UDF と一致する ACL を設定します。

ステップ 6	switch(config)# **show monitor session** <*session-number*>
	例：
	`(config)# show monitor session 1`
	`session 1`
	`---------------`
	`type : erspan-source`
	`state : up`
	`vrf-name : default`
	`destination-ip : 40.1.1.1`
	`ip-ttl : 255`
	`ip-dscp : 0`
	`acl-name : test`
	`origin-ip : 100.1.1.10 (global)`
	`source intf :`
	`rx : Eth1/20`
	`tx : Eth1/20`
	`both : Eth1/20`
	`source VLANs :`
	`filter VLANs : filter not specified`
	`rx :`
	`source fwd drops :`
	`egress-intf : Eth1/23`
		show monitor session <session-number> コマンドを使用して、ACL を表示します。BCM SHELL コマンドを使用して、SPAN TCAM リージョンがカービングされているかどうかを確認できます。

	コマンドまたはアクション	目的
	switch# config)#	

ERSPAN での IPv6 ユーザー定義フィールド（UDF）の設定

Cisco Nexus 3000 シリーズ スイッチでは ERSPAN で IPv6 ユーザー定義フィールド（UDF）を設定できます。次の手順を参照して、IPv6 UDF に基づく ERSPAN を設定します。詳細については、「ERSPAN の注意事項および制約事項」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	switch# **configure terminal**	グローバル設定モードを開始します。

ステップ 2	switch(config)# **udf** < *udf -name*> <*packet start*> <*offset*> <*length*>
	例：
	`(config)# udf udf1 packet-start 10 2`
	`(config)# udf udf2 packet-start 50 2`
		UDF を定義します。
		（注） 複数の UDF を定義できますが、必要な UDF のみ設定することを推奨します。UDF は、TCAM カービング時（ブートアップ時）にリージョンの修飾子セットに追加されるため、この設定は、UDF を TCAM リージョンにアタッチして、ボックスを再起動した後でのみ有効になります。

ステップ 3	switch(config)# **udf** < *udf -name*> header <*Layer3/Layer4*> <*offset*> <*length*>
	例：
	`(config)# udf udf3 header outer l4 0 1`
	`(config)# udf udf3 header outer l4 10 2`
	`(config)# udf udf3 header outer l4 50 1`
		UDF を定義します。

ステップ 4	switch(config)# **hardware profile tcam region ipv6-span-l2 512**
	例：
	`(config)# hardware profile tcam region ipv6-span-l2 512`
	`Warning: Please save config and reload the system for the`
		レイヤ 2 ポートの UDF で IPv6 を設定します。リージョンの新しい設定により既存の設定が置き換わりますが、設定を有効にするにはスイッチを再起動する必要があります。

	コマンドまたはアクション	目的
	configuration to take effect. config)#	
ステップ 5	switch(config)# **hardware profile tcam region ipv6-span 512** 例： (config)# **hardware profile tcam region ipv6-span 512** Warning: Please save config and reload the system for the configuration to take effect. config)#	レイヤ 3 ポートの UDF で IPv6 を設定します。リージョンの新しい設定により既存の設定が置き換わりますが、設定を有効にするにはスイッチを再起動する必要があります。
ステップ 6	switch(config)# **hardware profile tcam region span spanv6 qualify udf** *<name1>*…… *<name8>* 例： (config)# **hardware profile tcam region spanv6 qualify udf udf1** [SUCCESS] Changes to UDF qualifier set will be applicable only after reboot. You need to 'copy run start' and 'reload' config)#	レイヤ 3 ポートの SPAN に UDF 認定を設定します。これにより、ipv6-span TCAM リージョンの UDF 照合が有効になります。TCAM カービング時（ブートアップ時）に UDF を TCAM リージョンの修飾子セットに追加します。この設定では、SPAN リージョンにアタッチできる最大 2 つの IPv6 UDF を許可できます。UDF はすべて、リージョンの単一コマンドでリストされます。リージョンの新しい設定により、既存の設定が置き換わりますが、設定を有効にするには再起動する必要があります。
ステップ 7	switch(config)# **hardware profile tcam region span spanv6-12 qualify udf** *<name1>*…… *<name8>* 例： (config)# **hardware profile tcam region spanv6-l2 qualify udf udf1** [SUCCESS] Changes to UDF qualifier set will be applicable only after reboot. You need to 'copy run start' and 'reload' config)#	レイヤ 2 ポートの SPAN に UDF 認定を設定します。これにより、ipv6-span-12 TCAM リージョンの UDF 照合が有効になります。TCAM カービング時（ブートアップ時）に UDF を TCAM リージョンの修飾子セットに追加します。この設定では、SPAN リージョンにアタッチできる最大 2 つの IPv6 UDF を許可できます。UDF はすべて、リージョンの単一コマンドでリストされます。リージョンの新しい設定により、既存の設定が置き換わりますが、設定を有効にするには再起動する必要があります。
ステップ 8	switch (config-erspan-src)# **filter** …… *ipv6 access-group….<aclname>….<allow-sharing>* 例：	SPAN および ERSPAN モードで IPv6 ACL を設定します。1 つのモニターセッションには「filter ip access-group」

	コマンドまたはアクション	目的
	(config-erspan-src)# **ipv6 filter access-group test** (config)#	または「filter ipv6 access-group」 のいずれか 1 つだけを設定できます。同じ送信元インターフェイスが IPv4 と IPv6 ERSPAN ACL モニターセッションの一部である場合は、モニターセッションの設定で「allow-sharing」に「filter [ipv6] access-group」を設定する必要があります。
ステップ 9	switch(config)# **permit** …… <*regular ACE match criteria*> **udf** <*name1*> < *val* > <*mask*> .....<*name8*> < *val* > <*mask*> 例： (config-erspan-src)# **ipv6 access-list test** (config-ipv6-acl)# **permit ipv6 any any udf udf1 0x1 0x0**	UDF と一致する ACL を設定します。
ステップ 10	switch(config)# **show monitor session** <*session-number*> 例： (config)# **show monitor session 1** session 1 ----------	**show monitor session <session-number>** コマンドを使用して、ACL を表示します。

```
type              : erspan-source
state             : up
vrf-name          : default
destination-ip    : 40.1.1.1
ip-ttl            : 255
ip-dscp           : 0
acl-name          : test
origin-ip         : 100.1.1.10
(global)
source intf       :
    rx            : Eth1/20
    tx            : Eth1/20
    both          : Eth1/20
source VLANs      :
filter VLANs      : filter not
specified
    rx            :
source fwd drops  :
egress-intf       : Eth1/23
switch#
config)#
```

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。同時に実行できる ERSPAN セッション数は限定されているため、ある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することによって、別のセッションが使用で

きるようになります。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	**configuration terminal**
	例：
	`switch# configuration 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。セッションの範囲は 1 ～ 18 です。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。単方向の 4 つのセッション、または双方向の 2 つのセッションを同時にアクティブにすることができます。 （注） • Cisco Nexus 5000 および 5500 プラットフォームでは、2 つのセッションを同時に実行できます。 • Cisco Nexus 5600 および 6000 プラットフォームでは、16 のセッションを同時に実行できます。
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。セッションの範囲は 1 ～ 18 です。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。単方向の 4 つのセッション、または双方向の 2 つのセッションを同時にアクティブにすることができます。

	コマンドまたはアクション	目的
		（注） モニター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。

ステップ 5	**monitor session** *session-number* **type erspan-destination** 例： `switch(config-erspan-src)# monitor session 3 type erspan-destination`	ERSPAN 宛先タイプのモニター コンフィギュレーション モードを開始します。
ステップ 6	**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 7	**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 8	（任意） **show monitor session all** 例： `switch(config-erspan-src)# 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-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 10	（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。

	コマンドまたはアクション	目的
ステップ 11	（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 の設定情報を確認するには、次のコマンドを使用します。

コマンド	目的
show monitor session {**all** | *session-number* | **range** *session-range*}	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

ERSPAN 送信元セッションの設定例

次に、ERSPAN 送信元セッションを設定する例を示します。

```
switch# config t
switch(config)# interface e14/30
switch(config-if)# no shut
switch(config-if)# exit
switch(config)# monitor erspan origin ip-address 3.3.3.3 global
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# filter access-group acl1
switch(config-erspan-src)# source interface e14/30
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 9.1.1.2
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_11_pkts
switch(config-acl)# permit ip 11.0.0.0 0.255.255.255 any
switch(config-acl)# exit
switch(config)# ip access-list match_12_pkts
switch(config-acl)# permit ip 12.0.0.0 0.255.255.255 any
switch(config-acl)# exit
switch(config)# vlan access-map erspan_filter 5
switch(config-access-map)# match ip address match_11_pkts
switch(config-access-map)# action forward
switch(config-access-map)# exit
switch(config)# vlan access-map erspan_filter 10
switch(config-access-map)# match ip address match_12_pkts
switch(config-access-map)# action forward
switch(config-access-map)# exit
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# filter access_group erspan_filter
```

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
```

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
ERSPAN コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト、使用上の注意事項、および例	ご使用プラットフォームの『*Cisco Nexus NX-OS System Management Command Reference*』。

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。