SPAN の設定

この章では、Cisco NX-OS デバイス上のポート間のトラフィックを分析するようにイーサネット スイッチド ポート アナライザ（SPAN）を設定する方法について説明します。

この章の内容は、次のとおりです。

- SPAN の概要，1 ページ
- SPAN のライセンス要件，5 ページ
- SPAN の前提条件，5 ページ
- SPAN の注意事項および制約事項，5 ページ
- SPAN のデフォルト設定，8 ページ
- SPAN の設定，8 ページ
- SPAN の設定確認，16 ページ
- SPAN のコンフィギュレーション例，16 ページ
- その他の参考資料，19 ページ

SPAN の概要

SPAN は、外付けアナライザが接続された宛先ポートに SPAN セッション トラフィックを送ることで、送信元ポート間のすべてのトラフィックを分析します。

ローカル デバイス上で、SPAN セッションでモニタする送信元と宛先を定義できます。

SPAN ソース

トラフィックを監視できる監視元インターフェイスのことを SPAN 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。SPAN 送信元には次のものが含まれます。

- イーサネット ポート(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 ハードウェアに入力方向に到達したすべてのパケットをモニタします。

- VLANs

（注） VLAN を SPAN 送信元として指定すると、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 SPAN 送信元になります。

（注） VLAN ポートは、入力方向にのみ SPAN 送信元となることができます。

- Cisco Nexus 2000 シリーズ ファブリック エクステンダ（FEX）のサテライト ポートおよびホスト インターフェイス ポート チャネル

（注） これらのインターフェイスは、レイヤ 2 アクセス モードおよびレイヤ 2 トランク モードでサポートされます。これらはレイヤ 3 モードではサポートされず、レイヤ 3 サブインターフェイスはサポートされません。

（注） FEX ポートが SPAN 送信元としてサポートされるのは、入力方向についてはすべてのトラフィックに対してですが、出力方向については既知のレイヤ 2 ユニキャスト トラフィックだけです。

（注） 1 つの SPAN 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。

送信元ポートの特性

SPAN 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。
- スーパーバイザ帯域内インターフェイスを SPAN 送信元として使用する場合、次のパケットがモニタされます。

- スーパーバイザ ハードウェアに着信するすべてのパケット（入力）
- スーパーバイザ ハードウェアによって生成されるすべてのパケット（出力）

SPAN 宛先

SPAN 宛先とは、送信元ポートを監視するインターフェイスを指します。宛先ポートは SPAN 送信元からコピーされたトラフィックを受信します。SPAN 宛先には、次のものが含まれます。

- アクセス モードまたはトランク モードのイーサネット ポート
- アクセス モードまたはトランク モードのポート チャネル
- Cisco Nexus 9300 シリーズ スイッチのアップリンク ポート
- Cisco Nexus 9200 シリーズ スイッチの CPU（Cisco NX-OS リリース 7.0(3)I4(1) 以降）

（注） FEX ポートは SPAN 宛先ポートとしてサポートされません。

宛先ポートの特性

SPAN 宛先元ポートには、次の特性があります。

- 宛先ポートとして設定されたポートを送信元ポートとしても設定することはできません。
- 宛先ポートは、一度に 1 つの SPAN セッションだけで設定できます。
- 宛先ポートはスパニングツリー インスタンスに関与しません。SPAN 出力にはブリッジ プロトコル データ ユニット（BPDU）スパニングツリー プロトコル hello パケットが含まれます。

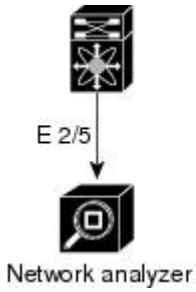
SPAN セッション

モニタする送信元と宛先を指定する SPAN セッションを作成できます。

サポートされる SPAN セッション数に関する情報については、『*Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*』を参照してください。

この図では、SPAN の設定を示します。3 つのイーサネット ポート上のパケットが宛先ポートのイーサネット 2/5 にコピーされます。コピーされるのは、指定した方向のトラフィックだけです。

図 *1*：*SPAN* の設定



Source Port	Direction	Destination Ports
E 2/1	Rx	E 2/5
E 2/2	Rx, Tx	
E 2/3	Tx	

186383

ローカライズされた SPAN セッション

SPANセッションがローカライズされるのは、すべての送信元インターフェイスが同じライン カードにある場合です。セッションの宛先インターフェイスは、任意のライン カードとすることが可能です。

（注） VLAN 送信元の SPAN セッションはローカライズされません。

ACL TCAM リージョン

ハードウェアの ACL Ternary Content Addressable Memory（TCAM）リージョンのサイズを変更できます。SPAN セッションで使用される TCAM リージョンの詳細については、『*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*』の「Configuring IP ACLs」の章を参照してください。

ハイ アベイラビリティ

SPAN 機能はステートレス リスタート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を適用します。ハイ アベイラビリティの詳細については、『*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

SPAN のライセンス要件

製品	ライセンス要件
Cisco NX-OS	SPAN にはライセンスは不要です。ライセンス パッケージに含まれていない機能は nx-os イメージにバンドルされており、無料で提供されます。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

SPAN の前提条件

SPAN 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 SPAN 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 Series NX-OS Interfaces Configuration Guide*』を参照してください。

SPAN の注意事項および制約事項

SPAN には、次の注意事項と制限事項があります。

- SPAN セッションの制限については、『*Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*』を参照してください。
- ライン カードごとの SPAN 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。
- 1 つのフォワーディング エンジン インスタンスで 4 つの SPAN セッションがサポートされます。Cisco Nexus 9300 シリーズ スイッチの場合は、最初の 3 つのセッションに双方向送信元が含まれていると、4 番目のセッションのハードウェア リソースは Rx 送信元専用になります。この制限は、SPAN 送信元のフォワーディング エンジン インスタンス マッピングに応じて、Cisco Nexus 9500 シリーズ スイッチにも適用される場合があります。
- SPAN は、管理ポートではサポートされません。
- Cisco Nexus 9300 シリーズ スイッチは、Tx SPAN を 40G アップリンク ポートでサポートしません。
- Cisco Nexus 9300 シリーズ スイッチ 40G アップリンク インターフェイスの SPAN コピーは、Rx 方向にスパンする際に dot1q 情報を取り逃がします。
- スイッチ インターフェイスのアクセス ポートの出力 SPAN コピーには、常に dot1q ヘッダーがあります。

- VLAN は、SPAN 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 送信元は Rx 方向でのみスパンします。
- スーパーバイザ生成の Stream Of Bytes Module Header（SOBMH）パケットには、インターフェイスから出力されるための情報がすべて含まれており、SPAN および ERSPAN を含めた、ハードウェア内部でのフォワーディング ルックアップはすべてバイパス可能です。パケットのブリッジ プロトコル データ ユニット（BPDU）クラスおよびレイヤ 3 インターフェイスでの CPU 生成のフレームは、SOBMH を使用して送信されます。
- ポート チャネルが SPAN の宛先として使用される場合、これらがロード バランシング用に使用するメンバーは 8 未満です。
- フィルタ アクセス グループの統計情報はサポートされません。
- SPAN セッションでの access-group フィルタは、vlan-accessmap として設定する必要があります。
- 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。
- すべてのスパンのレプリケーションはハードウェアで行われます。スーパーバイザ CPU は関与しません。
- 1 つの SPAN セッションには 1 つの宛先ポートのみを設定できます。
- 宛先ポートは、一度に 1 つの SPAN セッションだけで設定できます。
- ポートをソース 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。
- SPAN は、N9K-X9408PC-CFP2 ライン カード ポートの宛先をサポートしません。
- SPAN 宛先ポートへの VLAN ACL リダイレクトはサポートされません。
- 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。
- 双方向 SPAN セッションで使用される送信元が同じ FEX から出されている場合、ハードウェア リソースは 2 つの SPAN セッションに限定されます。
- SPAN セッションに、送信方向または送信および受信方向でモニタ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 SPAN の宛先ポートに複製される可能性があります。ソース 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
- 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 SPAN 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 SPAN 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 SPAN 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。

- VLAN SPAN がモニタするのは、VLAN のレイヤ 2 ポートが受信するトラフィックだけです。
- VLAN は、入力方向のみの SPAN 送信元としてサポートされます。
- FEX ポートが SPAN 送信元としてサポートされるのは、入力方向についてはすべてのトラフィックに対してですが、出力方向については既知のレイヤ 2 ユニキャスト トラフィックだけです。
- SPAN 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。
- SPAN はレイヤ 3 モードでサポートされます。ただし、SPAN は、レイヤ 3 サブインターフェイスやレイヤ 3 ポート チャネル サブインターフェイスではサポートされません。
- Cisco NX-OS は、送信元インターフェイスがホスト インターフェイス ポート チャネルでないときは、リンク層検出プロトコル（LLDP）またはリンク集約制御プロトコル（LACP）パケットをスパンしません。
- SPAN セッションは、セッションの送信元がスーパーバイザのイーサネット インバンド インターフェイスの場合、ARP 要求および Open Shortest Path First（OSPF）プロトコル hello パケットのようなスーパーバイザに到達するブロードキャストまたはマルチキャスト MAC アドレスを持つパケットをキャプチャできません。これらのパケットをキャプチャするには、SPAN セッションの送信元として物理インターフェイスを使用する必要があります。
- Cisco NX-OS リリース 7.0(3)I4(1) 以降では、同じ送信元が複数のセッションに属することができます。
- Cisco NX-OS リリース 7.0(3)I4(1) 以降では、Cisco Nexus 9300 および 9500 シリーズ スイッチで同じ送信元の複数の ACL フィルタをサポートします。
- 次の注意事項と制約事項は、Cisco Nexus 9200 シリーズ スイッチに適用されます。
  - UDF ベース SPAN は、Cisco NX-OS リリース 7.0(3)I4(1) 以降でサポートされます。
  - Tx SPAN は、マルチキャスト、未知のマルチキャスト、およびブロードキャスト トラフィックではサポートされません。
  - SPAN 送信元と宛先が同じスライスにあり、スライスに転送インターフェイスがない場合、Rx SPAN はマルチキャストでサポートされません。これがサポートされるのは、スライスに転送インターフェイスがあるか、あるいは SPAN の送信元と宛先が異なるスライスにある場合です。
  - 同じスライスにある複数の出力ポートで出力 SPAN トラフィックの輻輳が生じると、これらの出力ポートではライン レートを得られません。
  - ACL フィルタを使用した、親インターフェイスでのサブインターフェイス トラフィックのスパンは、サポートされません。
  - CPU SPAN 送信元は、Rx 方向（CPU からの SPAN パケット）でのみ追加できます。
  - 複数の ACL フィルタは、同じ送信元ではサポートされません。
  - CPU への SPAN パケットはレート制限されており、インバンド パスでドロップされます。レート制限の変更は、**hardware rate-limiter span** コマンドで行えます。スーパーバ

イザの SPAN コピーの分析は、**ethanalyzer local interface inband mirror detail** コマンドで行えます。

SPAN のデフォルト設定

次の表に、SPAN パラメータのデフォルト設定を示します。

パラメータ（Parameters）	デフォルト
SPAN セッション	シャット ステートで作成されます。

SPAN の設定

（注） この機能の Cisco NX-OS コマンドは、Cisco IOS のコマンドと異なる場合があります。

SPAN セッションの設定

SPAN 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、SPAN セッションはシャット ステートで作成されます。

（注） 双方向性の従来のセッションでは、トラフィックの方向を指定せずにセッションを設定できます。

はじめる前に

アクセス モードまたはトランク モードで宛先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 Series NX-OS Interfaces Configuration Guide*』を参照してください。

手順の概要

1. **configure terminal**
2. **interface***interface slot*/*port*
3. **switchport**
4. **switchport monitor**
5. （任意） ステップ 2 ～ 4 を繰り返して、追加の SPAN 宛先でモニタリングを設定します。
6. **no monitor session***session-number*
7. **monitor session***session-number* [**rx** | **tx**] [**shut**]
8. **description***description*
9. **source** {**interface***type* [**rx** | **tx** | **both**] | **vlan** {*number* | *range*} [**rx**]}
10. （任意） ステップ 9 を繰り返して、すべての SPAN 送信元を設定します。
11. （任意） **filter vlan** {*number* | *range*}
12. （任意） ステップ 11 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。
13. （任意） **filter access-group***acl-filter*
14. **destination interface***typeslot*/*port*
15. **no shut**
16. （任意） **show monitor session** {**all** | *session-number* | **range***session-range*} [**brief**]
17. （任意） **copy running-config startup-config**

手順の詳細

	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***interface slot*/*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上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 monitor** 例： `switch(config-if)# switchport monitor`	SPAN 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。

	コマンドまたはアクション	目的
ステップ 5	ステップ 2 ～ 4 を繰り返して、追加の SPAN宛先でモニタリングを設定します。	（任意） —
ステップ 6	**no monitor session***session-number* 例： `switch(config)# no monitor session 3`	指定した SPAN セッションのコンフィギュレーションを消去します。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 7	**monitor session***session-number* [**rx** | **tx**] [**shut**]
	
	例：
	`switch(config)# monitor session 3 rx`
	`switch(config-monitor)#`
	
	例：
	`switch(config)# monitor session 3 tx`
	`switch(config-monitor)#`
	
	例：
	`switch(config)# monitor session 3 shut`
	`switch(config-monitor)#`
		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。デフォルトでは、セッションが shut ステートで作成されます。このセッションは、ローカル SPAN セッションです。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 8	**description***description* 例： `switch(config-monitor)# description my_span_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 9	**source** {**interface***type* [**rx** | **tx** | **both**] | **vlan** {*number* | *range*} [**rx**]}
	
	例：
	`switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx`
	
	例：
	`switch(config-monitor)# source interface port-channel 2`
	
	例：
	`switch(config-monitor)# source interface sup-eth 0 both`
	
	例：
	`switch(config-monitor)# source vlan 3, 6-8 rx`
	
	例：
	`switch(config-monitor)# 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、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方向を、入力（rx）、出力（tx）、または両方向（both）として指定できます。
		
		（注） 送信元 VLAN は、入力方向に限りサポートされます。送信元 FEX ポートがサポートされるのは、入力方向についてはすべてのトラフィックに対してですが、出力方向については既知のレイヤ 2 ユニキャスト トラフィックだけです。
		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。

	コマンドまたはアクション	目的
ステップ 10	ステップ 9 を繰り返して、すべての SPAN 送信元を設定します。	（任意） —
ステップ 11	**filter vlan** {*number* | *range*} 例： `switch(config-monitor)# filter vlan 3-5, 7`	（任意） 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。 （注） SPAN 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 12	ステップ 11 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。	（任意） —
ステップ 13	**filter access-group***acl-filter* 例： `switch(config-monitor)# filter access-group ACL1`	（任意） ACL を SPAN セッションにアソシエートします。

ステップ 14	**destination interface***typeslot/port*
	
	例：
	`switch(config-monitor)# destination interface ethernet 2/5`
	
	例：
	`switch(config-monitor)# destination interface sup-eth 0`
		コピーされたソース パケットの宛先を設定します。
		（注） SPAN 宛先ポートはアクセス ポートまたはトランク ポートを指定する必要があります。
		（注） 宛先ポートでモニタ モードをイネーブルにする必要があります。
		Cisco NX-OS リリース 7.0(3)I4(1) 以降では、Cisco Nexus 9200 シリーズ スイッチだけの SPAN 宛先として CPU を設定できます。そのためには、インターフェイス タイプとして **sup-eth 0** を入力します。

ステップ 15	**no shut** 例： `switch(config-monitor)# no shut`	SPAN 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 16	**show monitor session** {**all** | *session-number* | **range***session-range*} [**brief**] 例： `switch(config-monitor)# show monitor session 3`	（任意） SPAN 設定を表示します。
ステップ 17	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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 SPAN の設定

デバイスの設定では、外部または内部パケット フィールド（ヘッダーまたはペイロード）のユーザ定義フィールド（UDF）と照合させ、一致したパケットを SPAN の宛先に送信させるようにできます。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。

はじめる前に

UDF ベース SPAN 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 Series NX-OS Security Configuration Guide』の「Configuring ACL TCAM Region Sizes」の項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***span-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

	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 ベースを次のように指定しますが、ここでの **header** はオフセットを考慮したパケット ヘッダーです。**packet-start** | **header** {**outer** | **inner** {**l3** | **l4**}}。

	コマンドまたはアクション	目的
		• *offset*：オフセット ベースからオフセットさせる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）からの先頭バイトに一致させるには、オフセットを 0 に設定します。 • *length*：オフセットからのバイト数を指定します。1 バイトまたは 2 バイトだけがサポートされます。追加のバイト数に一致させるには、複数の UDF の定義が必要です。 複数の UDF を定義できますが、必要な UDF のみを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。 • **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ダブル幅になります。十分な空き領域があることを確認してください。そうでない場合、このコマンドは拒否されます。必要であれば、未使用リージョンでの TCAM スペースを削減してから、このコマンドを再入力することもできます。詳細については『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』の「Configuring ACL TCAM Region Sizes」の項を参照してください。 （注） このコマンドの **no** 形式を使用すると、UDF の TCAM リージョンへの付加は解除され、リージョンはシングル幅に戻ります。
ステップ 4	**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	**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** を入力した後にのみ有効になります。

	コマンドまたはアクション	目的

ステップ 6	**ip access-list***span-acl*
	
	例：
	`switch(config)# ip access-list span-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、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./24 any udf udf-x 0x02 0x0F udf-y 0x1001 0xF00F`
		ACL を UDF でのみ一致させるか（例 1）、あるいは外部パケット 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）。
		1 つの ACL には、UDF の有無にかかわらず、同時に複数の ACE を持たせることができます。各 ACE ごとに異なる UDF フィールドで一致させることもできれば、すべての ACE で同じリストの UDF で一致させることもできます。

ステップ 8	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

SPAN セッションのシャットダウンまたは再開

SPAN 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することができます。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、別のセッションをイネーブルにできます。デフォルトでは、SPAN セッションはシャット ステートで作成されます。

SPAN セッションを再開（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再開できます。すでにイネーブルになっていて、動作状況がダウンの SPAN 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。

SPAN セッションのシャット ステートおよびイネーブル ステートは、グローバルまたはモニタ コンフィギュレーション モードのどちらのコマンドでも設定できます。

手順の概要

1. **configure terminal**
2. [**no**] **monitor session** {*session-range* | **all**} **shut**
3. **monitor session***session-number*
4. [**no**] **shut**
5. （任意） **show monitor**
6. （任意） **copy running-config startup-config**

手順の詳細

	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	[**no**] **monitor session** {*session-range*	**all**} **shut** 例： `switch(config)# monitor session 3 shut`	指定の SPAN 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。 コマンドの **no** 形式は、指定された SPAN 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。 （注） 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 3	**monitor session***session-number*
	
	例：
	`switch(config)# monitor session 3`
	`switch(config-monitor)#`
		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 4	[**no**] **shut** 例： `switch(config-monitor)# shut`	SPAN 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。 コマンドの **no** 形式は SPAN 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 5	**show monitor** 例： `switch(config-monitor)# show monitor`	（任意） SPAN 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 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

SPAN の設定確認

SPAN の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**]	SPAN セッションの設定を表示します。

SPAN のコンフィギュレーション例

SPAN セッションのコンフィギュレーション例

SPAN セッションを設定する手順は、次のとおりです。

手順の概要

1. アクセス モードで宛先ポートを設定し、SPAN モニタリングをイネーブルにします。
2. SPAN セッションを設定します。

手順の詳細

ステップ 1 アクセス モードで宛先ポートを設定し、SPAN モニタリングをイネーブルにします。

例：

```
switch# configure terminal
switch(config)# interface ethernet 2/5
switch(config-if)# switchport
switch(config-if)# switchport monitor
switch(config-if)# no shut
switch(config-if)# exit
```

```
switch(config)#
```

ステップ 2 SPAN セッションを設定します。

例：

```
switch(config)# no monitor session 3
switch(config)# monitor session 3
switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-monitor)# source interface port-channel 2
switch(config-monitor)# source interface sup-eth 0 both
switch(config-monitor)# source vlan 3, 6-8 rx
switch(config-monitor)# source interface ethernet 101/1/1-3
switch(config-monitor)# filter vlan 3-5, 7
switch(config-monitor)# destination interface ethernet 2/5
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 3
switch(config)# copy running-config startup-config
```

単一方向 SPAN セッションの設定例

単一方向 SPAN セッションを設定するには、次の手順を実行します。

手順の概要

1. アクセス モードで宛先ポートを設定し、SPAN モニタリングをイネーブルにします。
2. SPAN セッションを設定します。

手順の詳細

ステップ 1 アクセス モードで宛先ポートを設定し、SPAN モニタリングをイネーブルにします。

例：

```
switch# configure terminal
switch(config)# interface ethernet 2/5
switch(config-if)# switchport
switch(config-if)# switchport monitor
switch(config-if)# no shut
switch(config-if)# exit
switch(config)#
```

ステップ 2 SPAN セッションを設定します。

例：

```
switch(config)# no monitor session 3
switch(config)# monitor session 3 rx
switch(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx
switch(config-monitor)# filter vlan 3-5, 7
switch(config-monitor)# destination interface ethernet 2/5
```

```
switch(config-monitor)# no shut
switch(config-monitor)# exit
switch(config)# show monitor session 3
switch(config)# copy running-config startup-config
```

SPAN ACL の設定例

次に、SPAN 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 span_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 span_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
switch(config-erspan-src)# filter access_group span_filter
```

UDF ベース SPAN 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 SPAN 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
  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 SPAN 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
  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
ACL TCAM リージョン	『*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*』
FEX	『*Cisco Nexus 2000 Series NX-OS Fabric Extender Software Configuration Guide for Cisco Nexus 9000 Series Switches*』