



Nexus Data Broker の設定

この章の内容は、次のとおりです。

- [トポロジの表示, 1 ページ](#)
- [ポート定義の設定, 1 ページ](#)
- [モニタリング デバイスの設定, 5 ページ](#)
- [サービス ノードの追加, 6 ページ](#)
- [フィルタの追加, 6 ページ](#)
- [接続の追加, 13 ページ](#)
- [リダイレクションの追加, 16 ページ](#)
- [統計情報の表示, 20 ページ](#)
- [SPAN セッションの追加, 21 ページ](#)

トポロジの表示

トポロジを表示するには、左側のフレームにある [Topology] タブをクリックします。

ポート定義の設定

GUI で [Port Definition] タブをクリックすると、[Port Definition] 画面が表示されます。ポートを設定するには、ドロップダウン リストからスイッチを選択します。

[Port Definition] 画面には、次の 2 つのタブが表示されます。

- ポート設定
- SPAN Definition

[Port Configuration] タブをクリックすると、次のタブが表示されます。

- Configure Multiple Ports
- Remove port Configuration
- Add Service Node
- Add Monitoring Device

[Configure Multiple Ports] タブをクリックすると、[Configure Multiple Ports] ウィンドウが表示されます。

ポートを削除するには、削除するポートを選択して [Remove port Configuration] タブをクリックします。

サービス ノードを追加するには、[Add Service Node] をクリックします。

モニタリング デバイスを追加するには、[Add Monitoring Device] をクリックします。

[Port Configuration] 画面には、選択したノードに関する次のポート詳細が表示されます。

- Serial Number
- Status (ステータス)
- ポート名
- タイプ
- In Use
- Port ID
- Action : [Configure] をクリックすると、[Configure Ports] ウィンドウが表示されます。

[SPAN Destination] タブには、次の詳細が表示されます。

- SPAN Destination Name
- SPAN 宛先
- Node Connector
- monitor Port Type
- 説明

ポートの設定

ステップ 1 [Port Configuration] 画面で、ポートの詳細を設定するスイッチを選択します。

ステップ 2 [Action] の下にある [Configure] をクリックします。
[Configure Ports] ウィンドウが表示されます。

ステップ 3 [Configure Ports] ウィンドウで、[Select a port type] ドロップダウン リストから次のいずれかのオプションを選択してポート タイプを設定します。

- Add Monitoring Device
- Edge Port-SPAN
- Edge Port-TAP
- Production Port

[Monitoring Device]: トラフィックをキャプチャするモニタリング デバイスを作成し、対応する配信ポートを設定します。

[Edge Port-SPAN]: SPAN 宛先として設定されたアップストリーム スイッチに接続された着信トラフィックのエッジポートを作成します。

[Edge Port-TAP]: 物理 TAP ポートに接続された着信トラフィックのエッジポートを作成します。

[Production Port]: 入力および出力トラフィックの実稼動ポートを作成します。

(注) Cisco Nexus Data Broker で実稼動ポートが Q-in-Q に対して有効になっている必要があり、各実稼動ポートに一意的な VLAN を割り当てる必要があります。この VLAN には、実稼動の VLAN 番号と重複していないものを選択する必要があります。

ポートタイプを選択するとウィンドウのタイトルが [Manage Configure Ports] に変わります。

- ステップ 4** (任意) [Port Description] フィールドに、ポートの説明を入力します。
ポートの説明には 1 ~ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「|」、ピリオド「.」、およびアットマーク「@」です。
- ステップ 5** ポートの VLAN ID を入力します。
ポートは dot1q として設定され、実稼働の VLAN 情報を維持するように設定されています。VLAN ID は、トラフィックの送信元ポートを特定するために使用します。
- ステップ 6** (任意) APIC が使用可能な場合は、ACI 側ポートを選択し、そのポートを SPAN 宛先ポートとして指定できます。
- ステップ 7** [Enable Packet Truncation] フィールドに、パケット長を入力します。
- ステップ 8** [Block Tx] の横にチェックボックスが表示されます。このチェックボックスはエッジ SPAN のみに適用され、オンにするとエッジ SPAN インターフェイスから送信されたトラフィックをブロックできます。
- ステップ 9** [Submit] をクリックして設定を保存するか、[Clear] をクリックして詳細をクリアします。
ポートを設定した後は、[Port Configuration] 画面の [Action] の下にある [Edit] をクリックしてポートの詳細を編集できます。また、[Port Configuration] 画面の [Action] の下にある [Remove] をクリックするとポートの詳細をクリアできます。

SPAN 宛先の追加

エッジ SPAN ポートとして構成したポートが API 側に接続されると、ACI 側からポッド、ノード、およびポートを選択して、ポートを SPAN 宛先として設定できるようになります。



(注) SPAN 宛先を追加できるのは、APIC がネットワークに正常に追加された後だけです。

-
- ステップ 1** [Port Configuration] 画面で、ポートの詳細を設定するスイッチを選択します。
- ステップ 2** [Action] の下にある [Configure] をクリックします。
[Configure Ports] ウィンドウが表示されます。
- ステップ 3** [Configure Ports] ウィンドウで、[Select a port type] ドロップダウン リストから次のいずれかのオプションを選択してポートタイプを設定します。
- Add Monitoring Device
 - Edge Port-SPAN
 - Edge Port-TAP
 - Production Port
- [Monitoring Device] : トラフィックをキャプチャするモニタリング デバイスを作成し、対応する配信ポートを設定します。
- [Edge Port-SPAN] : SPAN 宛先として設定されたアップストリーム スイッチに接続された着信トラフィックのエッジポートを作成します。
- [Edge Port-TAP] : 物理 TAP ポートに接続された着信トラフィックのエッジポートを作成します。
- [Production Port] : 入力および出力トラフィックの実稼動ポートを作成します。
- ポートタイプを選択するとウィンドウのタイトルが [Manage Configure Ports] に変わります。
- ステップ 4** [SPAN DESTINATION] ペインの [Pod] ドロップダウン リストからポッドを選択します。
- ステップ 5** [Leaf] ドロップダウン リストから ACI リーフを選択します。
- ステップ 6** [Port] ドロップダウン リストで ACI 側のポートを選択し、インターフェイスを SPAN 宛先として設定します。
- ステップ 7** [Submit] をクリックして、設定を保存します。
選択したポートが SPAN 宛先ポートとして設定され、[Port Definition] 画面に表示されます。
-

複数のポートの設定

1 つのノードに複数のポートを設定できます。

- ステップ 1 [Port Configuration] 画面で [Configure Multiple Ports] をクリックします。[Configure Multiple Ports] ウィンドウが表示されます。
- ステップ 2 CTRL+SHIFT キーを使用し、[Select Ports] フィールドで複数のポートを選択します。
- ステップ 3 [Select Port Type] フィールドのドロップダウンリストでポートのタイプを選択します。
- ステップ 4 [Submit] をクリックして、設定を保存します。

モニタリング デバイスの設定

- ステップ 1 [Configuration] の下にある [Monitoring Devices] タブに移動します。
- ステップ 2 [+ Monitoring Device] をクリックします。
- ステップ 3 [Monitoring Device] ウィンドウで、次のフィールドに値を入力します。

名前	説明
Monitoring Device Name	サービス ノード名を追加します。
Select Switch Node	スイッチ ノードを選択します。
Select Port	ポートを選択します。
アイコン	モニタリング デバイスのアイコンを選択します。
Block Rx	モニタリング ツールからのトラフィックの受信をブロックします。このオプションは、デフォルトで選択されます。このオプションを無効にするには、チェックボックスをオフにします。

- ステップ 4 [Save (保存)] をクリックします。

サービスノードの追加

- ステップ 1 [Configuration] の下にある [Service Nodes] タブに移動し、[+ Service Node] をクリックします。
- ステップ 2 [Add Service Node] ウィンドウでサービスノードの名前を入力します。
- ステップ 3 [Service Node Ingress Port] ドロップダウンリストからサービスノードの入力ポートを選択します。
- ステップ 4 [Service Node Egress Port] ドロップダウンリストからサービスノードの出力ポートを選択します。
- ステップ 5 表示されたオプションからサービスノードのアイコンを選択します。
- ステップ 6 [Save (保存)] をクリックします。

フィルタの追加

- ステップ 1 フィルタを追加するには、[Filters] タブで [+ Filter] をクリックします。[Add Filter] ウィンドウが表示されます。
- ステップ 2 [Add Filter] ウィンドウの [Filter Description] セクションで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	フィルタの名前。名前には 1 ~ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「 」、ピリオド「.」、およびアットマーク「@」です。 (注) 一度保存した名前は後から変更できません。
[Bidirectional] チェックボックス	送信元 IP アドレス、送信元ポート、または送信元 MAC アドレスから宛先 IP アドレス、宛先ポート、または宛先 MAC アドレスへのトラフィックに関する情報、および宛先 IP アドレス、宛先ポート、または宛先 MAC アドレスから送信元 IP アドレス、送信元ポート、または送信元 MAC アドレスへのトラフィックに関する情報をフィルタでキャプチャするには、このチェックボックスをオンにします。

- ステップ 3 [Add Filter] ウィンドウの [Layer 2] セクションで、次のフィールドに値を入力します。

[Ethernet Type] フィールド	<p>必須です。レイヤ 2 トラフィックのイーサネットタイプ。表示されるデフォルト値は IPv4 ですが、次のいずれかを選択することもできます。</p> <ul style="list-style-type: none"> • IPv6 • 『ARP』 • LLDP • Predefined EtherTypes • All EtherTypes • Enter Ethernet Type : タイプとして [Enter Ethernet Type] を選択する場合は、イーサネットタイプを 16 進数形式で入力します。 [Predefined EtherTypes] を選択する場合は、config.in ファイルに含まれるすべての事前定義済みイーサネットタイプがルールに関連付けられるため、その他のパラメータを設定しないようにする必要があります。 <p>(注) これにより、1 つのフィルタに対して複数のユーザ定義イーサネットタイプを設定できるようになります。任意の数のイーサネットタイプを「,」で区切って指定すると、1 つのフィルタを複数のトラフィックタイプに対して設定できます。</p>
[VLAN Identification Number] フィールド	<p>レイヤ 2 トラフィックの VLAN ID。単一の VLAN ID、VLAN ID 値の範囲、またはカンマで区切られた VLAN ID 値と VLAN ID 範囲（たとえば、1-4,6,8,9-12）を入力できます。</p> <p>(注) NX-API を使用する場合、レイヤ 3 アドレスを含む VLAN ID はサポートされません。レイヤ 3 アドレスを含む VLAN ID を設定すると、フローの矛盾が発生します。その場合は、フローのトラブルシューティングと修正が必要になります。</p>
[VLAN Priority] フィールド	レイヤ 2 トラフィックの VLAN のプライオリティ。
[Source MAC Address] フィールド	レイヤ 2 トラフィックの送信元 MAC アドレス。
[Destination MAC Address] フィールド	レイヤ 2 トラフィックの宛先 MAC アドレス。

ステップ 4 [Add Filter] ウィンドウの [Layer 3] セクションで、次のフィールドを更新します。

名前	説明
[Source IP Address] フィールド	<p>レイヤ 3 トラフィックの送信元 IP アドレス。次のいずれかになります。</p> <ul style="list-style-type: none"> • ホスト IP アドレス (たとえば、10.10.10.10) • 不連続の送信元 IP アドレス (例 : 10.10.10.10、10.10.10.11、10.10.10.12) • IPv4 アドレスの範囲 (例 : 10.10.10.10-10.10.10.15) • IPv4 サブネット (例 : 10.1.1.0/24) • IPv6 形式のホスト IP アドレス (例 : 2001::0) <p>(注)</p> <ul style="list-style-type: none"> • [Source IP Address] フィールドに IPv6 アドレスの範囲を入力することはできません。 • レイヤ 3 の送信元 IP アドレスの範囲を設定する場合、レイヤ 4 の送信元ポートまたは宛先ポートの範囲を設定することはできません。 • レイヤ 3 の送信元 IP アドレスの範囲を設定する場合、レイヤ 2 の VLAN ID の範囲を設定することはできません。

名前	説明
[Destination IP Address] フィールド	<p>レイヤ 3 トラフィックの宛先 IP アドレス。次のいずれかになります。</p> <ul style="list-style-type: none"> • ホスト IP アドレス（たとえば、10.10.10.11） • IPv4 アドレスの範囲（例： 10.10.10.11-10.10.10.18） • IPv4 サブネット（例：10.1.1.0/24） • IPv6 形式のホスト IP アドレス（例：2001::4） • サブネット（例：10.0.0.0/25） <p>(注)</p> <ul style="list-style-type: none"> • [Destination IP Address] フィールドに IPv6 アドレスの範囲を入力することはできません。 • レイヤ 3 の送信元 IP アドレスの範囲を設定する場合、レイヤ 4 の送信元ポートまたは宛先ポートの範囲を設定することはできません。 • レイヤ 3 の送信元 IP アドレスの範囲を設定する場合、レイヤ 2 の VLAN ID の範囲を設定することはできません。
[Protocol] ドロップダウン リスト	<p>レイヤ 3 トラフィックのインターネット プロトコルを選択します。次のいずれかになります。</p> <ul style="list-style-type: none"> • ICMP • TCP • UDP • Enter Protocol <p>タイプとして [Enter Protocol] を選択した場合は、10 進形式のプロトコル番号を入力します。</p>
[ToS Bits] フィールド	<p>レイヤ 3 IP ヘッダー内の Type of Service (ToS) ビット。Differentiated Services Code Point (DSCP) 値だけが使用されます。</p>

ステップ 5 [Add Filter] ダイアログボックスの [Layer 4] セクションで、次のフィールドを入力します。

名前	説明
[Source Port] ドロップダウンリスト	<p>レイヤ 4 トラフィックの送信元ポートを選択します。次のいずれかになります。</p> <ul style="list-style-type: none"> • FTP (Data) • FTP (Control) • SSH • TELNET • HTTP • HTTPS • Enter Source Port <p>[Enter Source Port] を選択する場合は、単一のポート番号または送信元ポート番号の範囲を入力します。</p> <p>(注)</p> <ul style="list-style-type: none"> • レイヤ 4 の送信元ポートの範囲を設定する場合、レイヤ 3 の送信元 IP アドレスまたは宛先 IP アドレスの範囲を設定することはできません。 • レイヤ 4 の送信元ポートの範囲を設定する場合、レイヤ 2 の VLAN ID の範囲を設定することはできません。

名前	説明
[Destination Port] ドロップダウン リスト	<p>レイヤ4トラフィックの宛先ポートを選択します。次のいずれかになります。</p> <ul style="list-style-type: none"> • FTP (Data) • FTP (Control) • SSH • TELNET • HTTP • HTTPS • Enter Destination Port <p>[Enter Destination Port] を選択する場合は、単一のポート番号または宛先ポート番号の範囲を入力します。</p> <p>(注)</p> <ul style="list-style-type: none"> • レイヤ4の宛先ポートの範囲を設定する場合、レイヤ3の送信元IPアドレスまたは宛先IPアドレスの範囲を設定することはできません。 • レイヤ4の宛先ポートの範囲を設定する場合、レイヤ2のVLAN IDの範囲を設定することはできません。

ステップ 6 [Add Filter] ダイアログボックスの [Layer 7] セクションで、次のフィールドを入力します。

名前	説明
[HTTP Method] フィールド	<p>照合する HTTP メソッドを設定し、そのメソッドに基づくトラフィックをリダイレクトできます。1つのフィルタ内で照合するメソッドを1つまたは複数選択します。このオプションは、宛先ポートが HTTP または HTTPS である場合にのみ使用できます。</p> <ul style="list-style-type: none"> • Connect • Delete • get • Head • 投稿 • Put • トレース <p>(注) レイヤ7の照合は NX-API モードでのみサポートされ、OpenFlow ではサポートされません。</p> <p>(注) レイヤ7トラフィックのいずれかのメソッドを選択すると、[TCP Option Length] が有効になります。</p>
[TCP Option Length] フィールド	<p>TCP オプション長をテキストボックスで指定することによりフィルタ設定を拡張できます。このテキストボックスのデフォルト値は 0 です。同じオプション長がフィルタ内のすべてのメソッドに適用されます。</p> <p>TCP オプション長を入力する際には 10 進形式を使用します。</p> <p>(注) このテキストボックスの値は 0 ~ 40 の間で4の倍数に設定する必要があります。</p>

ステップ7 [Add Filter] をクリックします。

接続の追加

はじめる前に

- 接続に割り当てるフィルタを追加します。
- モニタリング デバイスを設定します（オプション）。
- 1つまたは複数のエッジ ポートを設定します（オプション）。

ステップ 1 [Connections] タブで、[+ Connection] をクリックします。[Add Connections] ウィンドウが表示されます。

ステップ 2 [Add Connections] ウィンドウの [Connection Details] 領域で、接続の [Connection Name] と [Priority] を追加できます。

フィールド	説明
Connection Name	接続の名前。 名前には 1～256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「 」、ピリオド「.」、およびアットマーク「@」です。
説明	新しい接続の作成時に説明を入力します。
プライオリティ	接続に適用するプライオリティ。 デフォルトは 100 で、有効な範囲は 0～10000 です。

ステップ 3 [Allow Matching Traffic] 領域で、次のフィールドを修正します。

フィールド	説明
[Allow Filters] ドロップダウン リスト	一致するトラフィックを許可するために使用するフィルタを選択します。 (注) [Traffic Drop Filters] と同じフィルタを [Allow Filters] で選択することはできません。
[Set VLAN] フィールド	接続に設定する VLAN ID。

フィールド	説明
[Strip VLAN at delivery port] チェックボックス	<p>配信ポートに到達する前にパケットから VLAN タグを除去するには、このチェックボックスをオンにします。</p> <p>(注) [Strip VLAN at delivery port] の処理は、1つのノードにつき、1つのエッジポートおよび1つまたは複数の配信デバイスとの接続に対してのみ適用されます。</p>
[Destination Devices] リスト	<p>フィルタに関連付けるモニタリング デバイス。名前の横にあるチェックボックスをオンにすることで、1つ以上のデバイスを選択できます。</p>
[Traffic Drop Filters] ドロップダウン リスト	(注)

ステップ 4 [Drop Matching Traffic] 領域で、次のフィールドに値を入力します。

フィールド	説明
[Traffic Drop] フィルタ	<p>デフォルトの [Default-Match-all] フィルタを選択するか、一致するトラフィックを破棄するために使用するその他のフィルタを選択します。</p> <p>(注) [Allow Filters] と同じフィルタを [Traffic Drop Filters] で選択することはできません。</p>

ステップ 5 [Source Ports (Optional)] 領域で、次のフィールドに値を入力します。

フィールド	説明
[Select Source Node] ドロップダウン リスト	<p>割り当てる送信元ノードを選択します。</p> <p>(注) 送信元ノードを選択しないと、any-to-multipoint のループフリーの転送パス オプションが使用され、すべての非配信ポートからのトラフィックがフィルタに対して評価されます。</p> <p>(注) 新しいリダイレクションを設定すると、各入力ポートに含まれるフローの数を表示できます。ポート番号をクリックすると、フローの詳細が表示されます。</p>

フィールド	説明
[Select Source Port] ドロップダウン リスト	<p>割り当てる送信元ノードのポートを選択します。</p> <p>(注) エッジポートのみを送信元ポートとして使用できます。</p> <p>(注) 新しい接続を追加する際に送信元ポートを選択しなかった場合は、次の警告メッセージが表示されます。No source port is selected. Connection will be setup from all configured Edge-SPAN and Edge-TAP ports. 接続のインストールと作成を続行するには、[OK] をクリックします。この場合、any-to-multipoint 接続はインストールされず、既存のトラフィックは中断されません。接続のセットアップ ページに移動するには、[Cancel] をクリックします。</p>

(注) トポロジ内の各スイッチの上に表示されるエッジタップポートやSPANポートの数と同様に、スイッチの上にマウスのポインタを合わせると、特定のモニタリングツールを使用している転送ルールが表示されます。ポップアップテーブルに、モニタリングツールを使用しているルール（接続）の名前が表示されます。

ステップ 6 次のいずれかを実行します。

- 接続の保存のみを行い、後でインストールする場合は、[Save Connection] をクリックします。
- 接続の保存とインストールを同時に行う場合は、[Install Connection] をクリックします。
- 接続を保存せずに閉じる場合は、[Close] をクリックします

[Connection Setup] 画面に、次のフィールドが表示されます。

- 名前
- Allow Filters
- Deny Filters
- 送信元ポート
- デバイス
- プライオリティ
- Last Modified By
- 説明

リダイレクションの追加



(注) リダイレクション設定機能は、リリース 6.0(2)U5(2) のみが稼働している Cisco Nexus 3000 シリーズスイッチと、リリース 7.x および OpenFlow が稼働している Cisco Nexus 9300 スイッチでサポートされます。

はじめる前に

- リダイレクションに割り当てるフィルタを追加します。
- モニタリングデバイスを設定します (オプション)。
- 1 つまたは複数のエッジポートを設定します (オプション)。
- 実稼働の入力ポート、実稼働の出力ポート、およびサービスノードは、同じリダイレクションスイッチ上に配置してください。

ステップ 1 [Redirections] タブで、[+ Redirection] をクリックします。[Add Redirection] ウィンドウが表示されます。

ステップ 2 [Add Redirection] ウィンドウの [Redirection Details] 領域で、リダイレクションの [Redirection Name] と [Priority] を追加できます。

フィールド	説明
Redirection Name	リダイレクションの名前。 名前には 1 ~ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「 」、ピリオド「.」、およびアットマーク「@」です。 (注) 一度保存したリダイレクションの名前は後で変更できません。
説明	新しいリダイレクションの作成時に説明を入力します。
[Set Auto Priority] チェックボックス	リダイレクションの自動プライオリティを有効にするには、このオプションをオンにします。リダイレクションのプライオリティは、選択した入力ポートにインストールされた既存のリダイレクションに基づいて設定されます。
プライオリティ	リダイレクションに適用するプライオリティ。有効な値の範囲は 0 ~ 10000 です。デフォルトは 100 です。

フィールド	説明
[Automatic Fail-safe] チェックボックス	このチェックボックスをオンにすると、リダイレクションのフェールセーフ機能が有効になります。この機能を有効にすると、実稼働の入力ポートおよび出力ポートから直接のフローが作成され、これはすべての低プライオリティの EtherType トラフィックに一致します。

ステップ 3 [Matching Traffic] 領域で、次のフィールドを修正します。

フィールド	説明
[Filters] ドロップダウン リスト	一致するトラフィックを許可するために使用するフィルタを選択します。 (注) フィルタに同じリダイレクションを選択することはできません。

ステップ 4 [Redirection Switch] 領域で、次のフィールドを修正します。

フィールド	説明
[Select Redirection Switch] ドロップダウン リスト	割り当てるリダイレクションスイッチを選択します。

(注) 1 台のリダイレクションスイッチに割り当てられる入力ポートと出力ポートはそれぞれ 1 つのみです。

ステップ 5 [Service Nodes (OPTIONAL)] 領域で、次のフィールドに値を入力します。

フィールド	説明
[Select Service Node] ドロップダウン リスト	割り当てるリダイレクションサービスノードを選択して、[Add Service Node] をクリックします。

(注) 複数のサービスノードを追加する場合は、パケットが移動する順番に従ってサービスノードを追加する必要があります。

ステップ 6 [Production Ports] 領域で、次のフィールドに値を入力します。

フィールド	説明
[Select Production Ingress Port] ドロップダウン リスト	<p>割り当てる実稼働の入力ポートを選択します。</p> <p>(注) 選択できる実稼働入力ポートは1つだけです。複数の入力ポートを選択することはできません。同じポートを入力ポートおよび出力ポートとして使用することはできません。</p> <p>(注) 新しいリダイレクションを設定すると、各入力ポートに含まれるフローの数を表示できます。ポート番号をクリックすると、フローの詳細が表示されます。</p>
[Select Production Egress Port] ドロップダウン リスト	<p>割り当てる実稼働出力ポートを選択します。</p> <p>(注) 選択できる実稼働出力ポートは1つだけです。複数の出力ポートを選択することはできません。同じポートを入力ポートおよび出力ポートとして使用することはできません。</p>

ステップ 7 [Delivery Devices to copy traffic (OPTIONAL)] 領域で、次のフィールドに値を入力します。

フィールド	説明
[Select Device] ドロップダウン リスト	<p>割り当てるデバイス（スイッチなど）をドロップダウンリストから選択し、[Add Device] をクリックします。</p> <p>(注) 1つのリダイレクションに対して複数の配信デバイスを選択することもできます。</p>

ステップ 8 次のいずれかを実行します。

- リダイレクションの保存のみを行い、後でインストールする場合は、[Save Redirection] をクリックします。
- リダイレクションの保存とインストールを同時に行う場合は、[Install Redirection] をクリックします。
- リダイレクションを保存せずに閉じる場合は、[Close] をクリックします。

ステップ 9 [Install Redirection] をクリックしてリダイレクションを保存し、同時にそれをインストールする場合、リダイレクションスイッチのリダイレクションパスは実稼働の入力ポート、サービス ノード、および実稼働の出力ポートに表示されます。

ステップ 10 リダイレクションスイッチのフロー統計情報を表示するには、[Flow Statistics] をクリックします。次のフィールドにフロー統計情報が表示されます。

- [In Port] フィールド：トラフィックの照合が行われる入力ポート。アスタリスク (*) は任意の入力ポートを表します。
- [DL Drc] フィールド：着信トラフィックに対して照合される送信元 MAC アドレス。アスタリスク (*) は任意の送信元 MAC アドレスを表します。
- [DL Dst] フィールド：着信トラフィックに対して照合される宛先 MAC アドレス。アスタリスク (*) は任意の宛先 MAC アドレスを表します。
- [DL Type] フィールド：着信トラフィックに対して照合される EtherType。たとえば、「IPv4」または「IPv6」は、すべての IP トラフィック タイプに使用されます。
- [DL VLAN] フィールド：着信トラフィックに対して照合される VLAN ID。アスタリスク (*) は任意の VLAN ID を表します。
- [VLAN PCP] フィールド：着信トラフィックに対して照合される VLAN プライオリティ。このフィールドには、ほとんど常にアスタリスク (*) が表示されます。
- [NW Src] フィールド：着信トラフィックに対して照合される IPv4 または IPv6 送信元アドレス。アスタリスク (*) は IPv4 または IPv6 EtherType に基づく任意の送信元アドレスを表します。
- [NW Dst] フィールド：着信トラフィックに対して照合される IPv4 または IPv6 宛先アドレス。アスタリスク (*) は IPv4 または IPv6 EtherType に基づく任意の宛先アドレスを表します。
- [NW Proto] フィールド：着信トラフィックに対して照合されるネットワークプロトコル。たとえば、「6」は TCP プロトコルを表します。
- [TP Src] フィールド：着信トラフィックに対して照合されるネットワークプロトコルに関連付けられた送信元ポート。アスタリスク (*) は任意のポート値を表します。
- [TP Dst] フィールド：着信トラフィックに対して照合されるネットワークプロトコルに関連付けられた宛先ポート。アスタリスク (*) は任意のポート値を表します。
- [Action] フィールド：指定された条件に一致するトラフィックに対して実行される出力アクション（「OUTPUT = OF2」など）。
- [Byte Count] フィールド：指定されたフロー接続に一致する集約トラフィックの量（バイト数）。
- [Packet Count] フィールド：指定されたフロー接続に一致する集約トラフィックの量（パケット数）。
- [Duration Seconds] フィールド：特定のフロー接続がスイッチにインストールされてからの時間（ミリ秒）。
- [Idle Timeout] フィールド：フロー テーブルから削除される前にフローをアイドル状態にできる時間（ミリ秒）。
- [Priority] フィールド：フローに割り当てられたプライオリティ。最も高いプライオリティ値を持つフローが最も優先されます。

ステップ 11 フロー統計情報表示ウィンドウを閉じるには、[Close] をクリックします。

統計情報の表示

ステップ 1 [Configuration] の下にある [Statistics] タブに移動し、ドロップダウンリスト内のノードをクリックすると、そのノードのフローとポートの統計情報が表示されます。

別のスイッチの統計情報に切り替えるには、ドロップダウン ボックスでスイッチを選択します。

表示されるフロー統計情報には次の項目が含まれます。

- Flow Name
- In Port
- DL Source
- DL Destination
- DL Type
- DL VLAN
- VLAN PCP
- NW Source
- NW Destination
- NW Proto
- TP Source
- TP Destination
- AP HttpMd
- AP TcpOptLn
- Actions
- Byte Count
- Packet Count
- Duration Seconds
- Idle Timeout
- プライオリティ

ステップ 2 ポートの統計情報を確認するには、[Ports] タブをクリックします。

表示されるポート統計情報には次の項目が含まれます。

- Port Name
- Rx Packets
- Tx Packets

- Rx Bytes
- Tx Bytes
- Rx Rate (kbps)
- Tx rate (kbps)
- Rx Drops
- Tx Drops
- Rx Errors
- Tx Errors
- Rx Frame Errors
- Rx Overrun Errors
- Rx CRC Errors
- Collisions

SPAN セッションの追加

[SPAN Sessions] タブには、次のフィールドが表示されます。

- SPAN セッション
- フィルタ
- デバイス
- SPAN 送信元
- SPAN Definition

SPAN セッションは ACI に追加できます。

-
- ステップ 1** SPAN セッションを追加するには、[+ SPAN Session] をクリックします。[Add SPAN Session] ウィンドウが表示されます。
 - ステップ 2** [Add SPAN Session] ウィンドウの [SPAN Session Name] フィールドにセッション名を追加します。
 - ステップ 3** (任意) [Select Connections] フィールドで接続を選択します。
 - ステップ 4** [Actions] ペインで、SPAN セッションのプライオリティを選択します。
 - ステップ 5** [Rule Filter] フィールドのドロップダウンリストを使用してルールを選択します。[Default-Match-IP] (デフォルトのフィルタ ルール) を選択するか、ドロップダウンリストから別のフィルタを選択します。

選択可能なフィルタールールは、[Default-Match-IP]、[Match-HTTP]、[Match-vlan]、および [Default-Match-all] です。

ステップ 6 トラフィックの送信先となる宛先デバイスを選択します。

ステップ 7 [SPAN SOURCES] ペインで、[+Add SPAN Source] をクリックします。リーフポートを追加して複数のリーフポートからのトラフィックをキャプチャするには、同じペインで [+Add Leaf Ports] をクリックします。あるいは、[+Add EPG] をクリックして EPG 送信元を追加することもできます。次のフィールドに値を入力します。

- a) [Add Leaf Ports] ウィンドウで、[POD] フィールドのドロップダウン リストを使用してポッドを選択します。
- b) [Node] フィールドのドロップダウン リストを使用してノードを選択します。
- c) [Port] フィールドのドロップダウン リストを使用してポートを選択します。
- d) [Add Leaf Ports] をクリックします。
- e) [SPAN SOURCES] ペインで、[Incoming]、[Outgoing]、または [Both] オプションの中から適切な方向を選択します。
選択した SPAN 送信元が、[Span Source] フィールドに表示されます。
- f) [+Add EPG] を選択して EPG 送信元を追加した場合は、[Add EPG] ウィンドウの [Tenant] フィールドのドロップダウン リストを使用してテナントを選択します。
- g) [Profile] フィールドのドロップダウン リストを使用してプロファイルを選択します。
- h) [EPg] フィールドのドロップダウン リストを使用して、テナントに関連付けられている EPG を選択します。
選択した [SPAN Source] が表示されます。
- i) [Add EPG] をクリックします。

ステップ 8 [SPAN Destination] フィールドで、SPAN 宛先を選択できます。

(注) SPAN 宛先は、SPAN 送信元が選択されているリーフと同じにする必要があります。

ステップ 9 [Add SPAN Session] をクリックします。

SPAN セッションを追加する場合は、確認を求めるメッセージボックスに「Are you sure you want to add SPAN session?」と表示されます。

ステップ 10 [OK] をクリックします。

その結果、ACI で SPAN セッションが設定されます。また、Cisco Nexus Data Broker でも同じ SPAN セッション名を使用して自動的に接続が設定されます。この接続により、指定された送信元ポートからモニタリング デバイスにトラフィックがリダイレクトされます。

(注) 各リーフには最大 4 つの SPAN セッションを設定できません。

したがって、追加の SPAN セッションを設定することもできます。また、既存の接続に新しい SPAN セッションを追加することもできます。その場合は、[Add SPAN Session] ウィンドウで新しい SPAN セッションを選択し、以前に作成した接続を使用し、別のリーフポートから新しい SPAN 送信元を選択し、SPAN 宛先を選択し、SPAN セッションを追加します。

これにより、新しいセッションが ACI に作成されますが、Cisco Nexus Data Broker 側では既存の接続に新しいトラフィックが追加されます。

既存の SPAN セッションを編集または複製することもできます。SPAN セッションを削除する場合は、削除するセッションをクリックし、[Remove SPAN Session(s)] をクリックします。表示されている SPAN セッションを削除するかどうかの確認を求めるメッセージボックスに「Remove the following sessions?」と表示されます。削除する場合は、[Remove SPAN Sessions] をクリックします。その SPAN セッションで既存の接続が使用されている場合は、変更結果が自動的に接続に反映されます。その接続が SPAN セッションに関連付けられている最後の接続である場合、その接続は削除されます。
