SR-TE 手動プレファレンス選択

SR-TE 手動プレファレンス選択の設定

このセクションでは、手動プレファレンス選択機能をサポートするために導入された設定および実行コマンドについて説明します。

SR-TE 手動優先順位選択の注意事項と制限事項

次の注意事項と制限事項は、SR-TE 手動優先順位選択機能に適用されます。

- Cisco NX-OS リリース 10.2(2)F 以降、SR-TE の手動優先順位選択機能により、SRTE ポリシーまたはオンデマンド カラー テンプレートの両方でロックダウン、シャットダウン、またはその両方を実行できます（SR-TE ポリシーまたはオンデマンド カラー テンプレートのシャットダウン優先順位）。さらに、この機能により、SR-TE ポリシーに対して特定の優先順位を強制的にアクティブにし、すべてまたは特定の SR-TE ポリシーに対してパスの再最適化を強制することもできます。

  この機能は、Cisco Nexus 9300-EX、9300-FX、9300-FX2、9300-GX、および N9K-C9332D-GX2B プラットフォーム スイッチでサポートされています。

- Cisco NX-OSリリース 10.5(3)F 以降、ルート マップには PBR と NON-PBR の両方の set コマンドを含めることができます。この変更により、同じルートマップ内でのポリシーベースのルーティング コマンドと従来のルーティング コマンドの統合を有効にすることにより、より柔軟なルーティング構成が可能になります。ユーザーは、特定のユースケース要件に基づいて適切な set コマンドが設定されていることを確認する必要があります。

SR-TE 手動設定について：ロックダウンとシャットダウン

Cisco NX-OS リリース 10.2(2)F 以降、必要に応じて次のアクションを実行できます。

- SRTE ポリシーのロックダウン：オンデマンドのカラー テンプレートまたは明示的なポリシーでロックダウンを有効にできます。ロックダウンは、ポリシーのパス設定の自動再最適化を無効にします。ロックダウンされたポリシーに対して新しい優先パスが発生した場合、新しいパスを使用するように自動的に切り替えることはなく、有効になるまで現在のアクティブなパス オプションを使用し続けます。

（注） オンデマンドテンプレートと同じカラーの明示ポリシー構成が存在する場合、ポリシー構成はロックダウンのテンプレート構成よりも優先されます。

例

ポリシーに複数の設定があるシナリオを考えてみましょう。ネットワークの障害により、優先度の高いパスがダウンしたと仮定します。障害は、優先度の高いパスにあるノードの差し迫った障害である可能性があります。障害を調査して修正するとき、運用チームは問題のあるノードをリロードまたは無効にして、これが発生している間の中断を防ぐ必要がある場合があります。次に、優先度の低いパスをロックダウンし、優先度の高いパスに戻らないようにすることは、使用するのに適したオプションです。

- SRTE ポリシーのシャットダウン：オンデマンドのカラー テンプレートまたは明示ポリシーでシャットダウンを有効にすることができます。ポリシーの状態が管理状態ダウンに変わり、ポリシーに関係するすべてのクライアントにポリシー ダウン通知が送信されます。オンデマンドのカラー構成でシャットダウンを無効にすると、ポリシーのパスの有効性に基づいて、ポリシーの状態がアップまたはダウンに変更されます。

（注） オンデマンドテンプレートと同じ色の明示ポリシー設定が存在する場合、シャットダウンのテンプレート構成よりもポリシー構成が優先されます。

- SRTE ポリシーのシャットダウン設定 – オンデマンドのカラー テンプレート構成または明示ポリシー構成のパス設定で、パス設定をシャットダウンできます。これにより、そのパスプリファレンスが無効になり、プリファレンスが解除されるまで、将来のパスの再最適化が開始されなくなります。パスプリファレンスは、設定でシャットダウンされているかシャットダウンされていないかに基づいて、`show srte policy` の出力に管理状態ダウンまたはアップとして表示されます。

SR-TE 手動設定の構成 - ロックダウン/シャットダウン

SR-TEポリシーまたはオンデマンドカラーテンプレートで、ロックダウン、シャットダウン、またはその両方を構成できます。SR-TE ポリシーまたはオンデマンド カラー テンプレートの下で構成をシャットダウンすることもできます。

始める前に

mpls セグメント ルーティング機能が有効になっていることを確認する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します
ステップ 2	**segment-routing**	セグメントルーティング モードを開始します。
ステップ 3	**traffic-engineering**	トラフィック エンジニアリング モードに入ります。
ステップ 4	**on-demand color***color_num* または **policy** *name*	オンデマンド モードを開始し、カラーを構成します または SR-TE ポリシーを個別に構成します。
ステップ 5	（オプション） [**no**] **lockdown**	オンデマンドのカラー テンプレートまたは明示的なポリシー構成でロックダウンを有効にします。 （注） オンデマンド テンプレートと同じ色の明示的なポリシー構成が存在する場合、ポリシー構成がテンプレート構成よりも優先され、ポリシーがロックダウンされます。
ステップ 6	（オプション） [**no**] **shutdown**	必要に応じて、オンデマンド カラー テンプレートまたは構成済みの SR-TE ポリシーから作成されたポリシーをシャットダウンします。 （注） オンデマンド テンプレートと同じ色の明示的なポリシー構成が存在する場合、

	コマンドまたはアクション	目的
		ポリシー構成がテンプレート構成よりも優先され、ポリシーがシャットダウンされます。
ステップ 7	**candidate-paths**	ポリシーの候補パスを指定します。
ステップ 8	**preference** *preference_number*	候補パスの優先順位を指定します。
ステップ 9	（オプション） [**no**] **shutdown**	SR-TEポリシー構成またはオンデマンドカラー テンプレート構成の下でパス プリファレンスをシャットダウンします。

SRTE ポリシーの特定のパス設定を適用する

特定の設定を SRTE ポリシーのアクティブ パス オプションに適用するには、`segment-routing traffic-engineering switch name <policy_name> pref <preference_number>` 実行コマンドを使用します。このコマンドは、有効になるまで設定を使用します。

次のような出力例を示します。

```
NX2# show srte policy Green_White
Policy: 8.8.8.0|801
Name: Green_White
Source: 2.2.2.0
End-point: 8.8.8.0
State: UP
Color: 801
Authorized: Y
Binding-sid Label: 22
Policy-Id: 3
Path type = MPLS Active path option
Path-option Preference:180 ECMP path count: 1
1. PCE Weighted: No
Delegated PCE: 11.11.11.11
Index: 1 Label: 16005
Index: 2 Label: 16008
NX2# segment-routing traffic-engineering switch name Green_White preference 170
NX2(cfg-pref)# show srte policy Green_white detail
Policy: 8.8.8.0|801
Name: Green_White
…..
Path type = MPLS Path options count: 4
Path-option Preference:180 ECMP path count: 1 Admin: UP Forced: No
1. PCE Weighted: No
Delegated PCE: 11.11.11.11
Index: 1 Label: 16005
Index: 2 Label: 16008
Path-option Preference:170 ECMP path count: 1 Admin: UP Forced: Yes Active path option
1. Explicit Weighted: No
Name: Yellow
Index: 1 Label: 16006
Index: 2 Label: 16008
```

この手動で選択した設定を元に戻すには、次のオプションのいずれかを実行します。

- segment-routing traffic-engineering reoptimize name <policy_name> コマンドを使用します。詳細については、SRTE ポリシーまたはすべての SRTE ポリシーのパス再最適化の適用 （5 ページ）を参照してください。
- 別の設定に切り替えます
- このポリシーを閉じます
- 選択した設定を閉じます

SRTE ポリシーまたはすべての SRTE ポリシーのパス再最適化の適用

SRTE ポリシーに複数の設定がある場合、ポリシーを再最適化でき、利用可能な最適なパスを選択できます。

特定の SRTE ポリシーのパスの再最適化を適用するには、segment-routing traffic-engineering reoptimize name <policy_name> コマンドを使用します。<policy_name> は、ポリシー名またはエイリアス名にすることができます。このコマンドは、前のセクションで説明した設定スイッチ コマンドを取り消し、構成されている場合はロックダウンをオーバーライドします。

次のような出力例を示します。

```
NX2# show srte policy Green_White
Policy: 8.8.8.0|801
Name: Green_White
Source: 2.2.2.0
End-point: 8.8.8.0
State: UP
Color: 801
Authorized: Y
Binding-sid Label: 22
Policy-Id: 3
Path type = MPLS Active path option
Path-option Preference:170 ECMP path count: 1
1. Explicit Weighted: Yes Weight: 1
Name: Yellow
Index: 1 Label: 16006
Index: 2 Label: 16008
NX2# segment-routing traffic-engineering reoptimize name Green_White
NX2# show srte policy Green_White
Policy: 8.8.8.0|801
Name: Green_White
Source: 2.2.2.0
End-point: 8.8.8.0
State: UP
Color: 801
Authorized: Y
Binding-sid Label: 22
Policy-Id: 3
Path type = MPLS Active path option
Path-option Preference:180 ECMP path count: 1
1. PCE Weighted: No
Delegated PCE: 11.11.11.11
Index: 1 Label: 16005
Index: 2 Label: 16008
```

すべての SRTE ポリシーのパスの再最適化を強制するには、segment-routing traffic-engineering reoptimize all コマンドを使用して、システムに存在するすべての SRTE ポリシーのパスの再

最適化を適用します。このコマンドは、前のポイントで説明した設定スイッチ コマンドを取り消し、構成されている場合はロックダウンをオーバーライドします。

SRTE フローベース トラフィック ステアリングの構成

この章では、Cisco Nexus 9000-FX、9000-FX2、9000-FX3、9000-GX、および 9300 プラットフォーム スイッチで SRTE フローベースのトラフィック ステアリングを構成する方法について説明します。

SRTE フローベース トラフィック ステアリング

Cisco NX-OS リリース 10.1(2) のフローベースのトラフィック ステアリング機能は、直接的で柔軟な、ステアリングするトラフィックを選択する代替方法を提供します。この方法では、出力ノードではなく、ヘッドエンド ノードでソース ルーティングを直接構成できます。フローベースのトラフィック ステアリングにより、ユーザーは、宛先アドレス、UDP または TCP ポート、DSCP ビット、その他のプロパティなどの着信パケットのフィールドを一致させることにより、SRTEポリシーに誘導されるパケットを選択できます。一致は、パケットをポリシーに導くように ACL をプログラミングすることによって行われます。

トラフィックを一致させて誘導するために、ポリシーベース ルーティング（PBR）機能が拡張され、SRTE ポリシーをサポートするようになりました。現在の PBR 機能には、RPM、ACL Manager、および AclQoS コンポーネントが含まれます。Cisco NX-OS リリース 10.1(2) 以降、SRTE サポートを追加するために、RPM コンポーネントは SRTE および ULIB とも通信し、URIB との通信が強化されています。

したがって、SRTE のフローベースのトラフィック ステアリング機能には、次のものが含まれます。

- MPLS SR データプレーン
- IPv4 トラフィックのステアリングはデフォルト VRF でサポートされ、IPv4 および IPv6 トラフィックのステアリングはデフォルト以外の VRF でサポートされます
- 5 つのタプル フィールド（送信元アドレス、宛先アドレス、プロトコル、tcp/udp 送信元ポート、tcp/udp 宛先ポート）の組み合わせに基づく ACL によるトラフィックの一致
- 一致したトラフィックを SRTE ポリシーに導く
- IPv4 パケットのパケット内の DSCP/TOS ビットのマッチング。Cisco NX-OS リリース 10.3(1)F 以降では、VXLAN パケットの外部ヘッダーの DSCP/TOS ビットのマッチングもサポートされています。
- IPv6 パケットのパケットのトラフィック クラス フィールドの一致
- 期間の定義に基づく ACL の自動有効化および無効化
- VRF ケースをステアリングするとき、ネクスト ホップを指定せずに SRTE ポリシーへのステアリングをサポートします。

- エニーキャスト エンドポイントを使用したオーバーレイ ECMP
- ACL に一致するパケットは、通常のルートよりも優先されます
- ToS/DSCP およびタイマーベースの ACL に基づくフロー選択
- next-hop-ip は、あるエンドポイントから別のエンドポイントへの SRTE ポリシーへのトラフィックのステアリングに使用されます。

SRTE のフローベース トラフィック ステアリングの注意事項と制限事項

次の注意事項と制限事項は、SRTE機能のフローベース トラフィック ステアリングに適用されます。

- Cisco NX-OS リリース 10.1(2) 以降、SRTE のフローベースのトラフィック ステアリング機能は、Cisco Nexus 9000-FX、9000-FX2、9000-FX3、9000-GX、および 9300 プラットフォーム スイッチでサポートされます。
- SRTE ポリシーが VRF のインターフェイスに割り当てられたルート マップに適用されるとき（L3VPN/L3EVPN トラフィックを誘導するため）、set statement のネクスト ホップが BGP プレフィックスに解決され、その BGP プレフィックスがすでに SRTE を使用してトラフィックを誘導し、ルートマップはトラフィックを誘導しません。
- アンダーレイ ECMP は、ポリシー内のアクティブな各 SRTE パス（ECMP メンバー）のラベル スタックが同じ場合にのみサポートされます。9000-GX プラットフォームには、この制限はありません。
- ルートマップ トラッキング機能はサポートされていません。
- SRTE ポリシーを操作する場合、1 つのルート マップ シーケンス エントリに複数の**ネクスト ホップを設定**することはサポートされていません。
- SRTE ポリシーが VRF のインターフェイスに割り当てられたルート マップに適用される場合（L3VPN/L3EVPN トラフィックを誘導するため）、set ステートメントのネクスト ホップが RIB で複数のネクスト ホップを有する BGP ルート（オーバーレイ ルート）に対して解決される場合、 トラフィックはルートの最初のネクスト ホップにのみ誘導され、すべてのネクスト ホップで ECMP は行われません。
- SRTE ポリシー名がルート マップ セット ステートメントで使用されている場合、カラーとエンドポイントではなく、デフォルトの VRF ステアリングにのみ使用できます。そうでない場合は、明示的に定義されている SRTE パスを選択する必要があります。具体的には、これは、ラベルの代わりにポリシーエンドポイント キーワードを含むセグメントリストを使用するように定義された SRTE ポリシーを選択するためには使用できません。
- **set ip next-hop <>** で指定されたネクスト ホップ IP に適用される次のキーワードは、SRTE ポリシーにステアリングするときのルート マップではサポートされません。
  - verify-availability

- drop-on-fail
- force-order
- load-share

- 必要な機能（セグメンティング ルーティング、l3 evpn または l3vpn）がデバイスで有効になっていない場合でも、srte-policy を使用したルート マップをインターフェイスに適用できます。ただし、srte-policy を使用した set-actions は抑制されます。つまり、これらのフローに対してデフォルト ルーティングが実行されます。
- ルート マップには、srte-policy ありおよび srte-policy なしの set コマンドを含めることができます。
- srte-policy 情報のない set-command の場合、ステアリングは next-hop-ip への到達可能性が MPLS ラベルを必要としない場合にのみ実行されます。
- ルート マップがデフォルト以外の VRF のインターフェイスに関連付けられており、そのルート マップにネクスト ホップ IP アドレス **N** と SRTE ポリシーを指定するシーケンスが含まれている場合、そのルートマップ上の他のすべてのシーケンスと、同じネクストホップ IP アドレスを使用する同じ VRF に関連付けられたその他すべてのルート マップにも SRTE ポリシーが必要です。同じネクスト ホップ IP と異なる SRTE ポリシーを使用して、別のルート マップまたはルート マップ シーケンスを同じ VRF に関連付けることはできません。
- 同様に、ルート マップがデフォルト以外の VRF のインターフェイスに関連付けられていて、そのルート マップが SRTE ポリシーを指定していないが、ネクスト ホップ IP アドレス **N** を指定している場合、同じネクスト ホップ IP アドレス N を使用し、SRTE ポリシーを指定する、そのルートマップまたは別のルートマップ内の別のシーケンスは適用されません。
- SRTE フローベースのトラフィック ステアリングは、VXLAN または EoMPLS PBR と同時に使用することはできません。
- SRTE 入力ノードのポリシー ベースのルーティング トラフィックでは、SR ラベル統計はサポートされていません。ただし、ACL リダイレクト統計はサポートされています。
- デフォルト VRF の IPv6 トラフィックは、SRTE ポリシーに誘導できません。MPLS SR アンダーレイは、IPv4 でのみサポートされます。ただし、IPv6 SR アンダーレイが必要な場合は、代わりに SRv6 を使用します。
- 9000-FX、9000-FX2、9000-FX3、および 9300 プラットフォーム ハードウェアは、ECMP メンバーごとに一意のアンダーレイ ラベル スタックをプッシュできず、これらのプラットフォームのアンダーレイ ECMP に影響します。つまり、セグメント リストの最初のホップが異なる SRTE ポリシーに複数のアクティブ セグメント リストがある場合（1 つの設定が複数のセグメント リストで構成されている場合）、そのような構成はサポートされません。このような場合、回避策として、エニーキャスト SID を構成して、すべての ECMP メンバーでラベル スタックが同じになるようにします。

- モジュラ プラットフォームは、Cisco NX-OS リリース 10.1(2) ではサポートされていません。
- Cisco NX-OS リリース 10.2(2)F 以降、SRTE のフローベースのトラフィック ステアリング機能は、Cisco N9K-C9332D-GX2B 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 10.3(1)F 以降、DSCP ベースの SR-TE フロー ステアリング機能により、IP ヘッダーの DSCP フィールドを使用して照合され、SRTE パスに誘導される VXLAN パケットのソースルーティングが可能になります。以下はこの機能の注意事項と制限事項です。
  - この機能は、Cisco Nexus 9300-FX2、9300-FX3、9300-GX、9300-GX2 TOR スイッチでのみサポートされます。
  - VXLAN パケットが終了していない場合、ACL フィルタは VXLAN パケットの外部 IP ヘッダ フィールド（IPv4）に適用されます。
- Cisco NX-OS リリース 10.3(2)F 以降、SRTE 向けフローベース トラフィック ステアリング機能は、Cisco Nexus 9700-FX および 9700-GX ライン カードでサポートされます。以下はこの機能の注意事項と制限事項です。
  - Cisco Nexus 9508 プラットフォーム スイッチが VXLAN EVPN から MPLS SR L3VPN へのハンドオフモードで、MPLS カプセル化パケットが L2 ポートで転送される場合、dot1q ヘッダーは追加されません。
  - Cisco Nexus 9500 プラットフォーム スイッチが EVPN から MPLS SR L3VPN へのハンドオフモードとして設定されている場合、SVI/サブインターフェイスは、コアに面したアップリンク (MPLS または VXLAN) ではサポートされません。
  - DSCP から MPLS EXP へのプロモーションは、DCI モードの FX TOR/ラインカードでは機能しません。MPLS EXP への内部 DSCP 値のコピーは、このハンドオフ モードの FX TOR/ライン カードでは機能しません。MPLS EXP は 0x7 に設定されます。
- Cisco NX-OS リリース 10.3(2)F 以降、DSCP ベースの SRTE フロー ステアリング機能は、Cisco Nexus 9300-FX プラットフォームおよび Cisco Nexus 9700-FX と 9700-GX ライン カードでサポートされます。以下はこの機能の注意事項と制限事項です。
  - Cisco Nexus 9500 プラットフォーム スイッチが VXLAN EVPN から MPLS SR L3VPN へのハンドオフモードで、MPLS カプセル化パケットが L2 ポートで転送される場合、dot1q ヘッダーは追加されません。
  - Cisco Nexus 9500 プラットフォーム スイッチが EVPN から MPLS SR L3VPN へのハンドオフモードとして設定されている場合、SVI/サブインターフェイスは、コアに面したアップリンク (MPLS または VXLAN) ではサポートされません。
  - DSCP から MPLS EXP へのプロモーションは、DCI モードの FX TOR/ラインカードでは機能しません。MPLS EXP への内部 DSCP 値のコピーは、このハンドオフ モードの FX TOR/ライン カードでは機能しません。MPLS EXP は 0x7 に設定されます。

構成プロセス：SRTE フローベース トラフィック ステアリング

SRTE フローベースのトラフィック ステアリング機能の構成プロセスは次のとおりです。

1. 特に IP アクセス リストの基準に一致する IP アクセス リストを構成します。

   詳細については、『*Cisco Nexus Series NX-OS* セキュリティ構成ガイド』の「*IP ACL* の構成」章を参照してください。

2. SRTE ポリシーを定義します。

   SRTE の設定の詳細については、『*Cisco Nexus 9000* シリーズ *NX-OS* ラベル スイッチ構成ガイド』の「トラフィック エンジニアリング用セグメント ルーティングの構成」の章を参照してください。

3. 一致（ステップ 1 で設定した IP アクセス リスト）とアクションをバインドするルートマップを構成します。一致は、パケットで一致するフィールドを参照し、アクションは、どの SRTE ポリシーを誘導するか、および使用する VPN ラベルを参照します（存在する場合）。

ToS/DSCP およびタイマーベース ACL に基づいたフロー選択の構成

SRTE フローベースのトラフィック ステアリング機能では、フロー選択は ToS/DSCP およびタイマー ベースの ACL に基づいています。

デフォルトおよびデフォルト以外の VRF のルート マップを、さまざまな基準によって選択されたポリシーに構成して正しく動作させるには、次の構成手順を実行します。

始める前に

MPLS セグメント ルーティング トラフィック エンジニアリングおよび PBR 機能が有効になっていることを確認する必要があります。

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** | **ipv6**] **access-list** *acl_name*
	例：
	`switch(config)# ip access-list L4_PORT`
	`switch(config)#`
		名前を使用して IP または IPv6 アクセス リストを定義し、 IP または IPv6 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 3	**10 permit ip** *ip_address* **any** 例：	スイッチで構成された IP または IPv6 アクセス リストを表示します。

	コマンドまたはアクション	目的
	`switch(config)# 10 permit ip any 5.5.0.0/16` `switch(config)#`	

ステップ 4	**20 permit tcp** *tcp_address* [**any**]
	例：
	`switch(config)# 20 permit tcp any 5.5.0.0/16`
	`switch(config)#`
		IPv6 アクセス リストに TCP 許可条件を設定します。
		（注）
		any キーワードは、IPv6 にのみ使用されます。

ステップ 5	[**ip** | **ipv6**] **access-list** *dscp_name*
	例：
	`switch(config)# ip access-list dscp`
	`switch(config)#`
		名前を使用して IP または IPv6 アクセス リストの DSCP 定義し、 IP または IPv6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 6	**10 permit tcp any** *tcp_address* **dscp** <*dscp value*>
	例：
	`switch(config)# 10 permit tcp any 5.5.0.0/16 dscp af11`
	`switch(config)#`
		IP または IPv6 アクセス リストの DSCP 値を設定します。
		（注）
		any キーワードは、IPv6 にのみ使用されます。

ステップ 7	[**ip** | **ipv6**] **access-list** *acl_name*
	例：
	`switch(config)# ip access-list acll`
	`switch(config)#`
		名前を使用して IP または IPv6 アクセス リストを定義し、 IP または IPv6 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 8	**10 permit tcp any** *tcp_address* **acl** *acl_name*
	例：
	`switch(config)# 10 permit tcp any 5.5.0.0/16 eq www dscp af11`
	`switch(config)#`
		IPv6 アクセス リストに TCP 許可条件を設定します。
		（注）
		any キーワードは、IPv6 にのみ使用されます。

ステップ 9	[**ip** | **ipv6**] **access-list** *acl_name*
	例：
	`switch(config)# ip access-list acl1`
	`switch(config)#`
		名前を使用して IP または IPv6 アクセス リストを定義し、 IP または IPv6 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 10	**10 permit tcp any** *any time - range tl*
	例：
	`switch(config-acl)# 10 permit tcp any 5.5.0.0/16 eq www dscp af11`
	`switch(config)#`
		IP または IPv6 アクセス リストの TCP の時間範囲を定義する時間範囲値を設定します。
		（注）
		any キーワードは、IPv6 にのみ使用されます。

	コマンドまたはアクション	目的

ステップ 11	**time-range** *name*
	例：
	`switch(config-acl)# time-range t1`
	`switch(config)#`
		名前を使用して、IP または IPv6 アクセス リストの時間範囲を定義します。

ステップ 12	**F2(config-time-range)#** **WOLF2(config-time-range)#** 例： `switch(config-time-range)# 10 absolute start 20:06:56 8 february 2021 end 20:10:56 8 february 2021`	構成の時間範囲を定義します。

フローベース トラフィック ステアリングのデフォルトおよび非デフォルト VRF でのルート マップの構成

次のセクションでは、SRTE フローベースのトラフィック ステアリング機能のデフォルトおよび非デフォルト VRF でルート マップを構成する方法を示します。

カラーおよびエンドポイントによって選択されているポリシーへのデフォルト VRF のルート マップの構成

デフォルト VRF のトラフィックを、色とエンドポイントで選択されたポリシーに導くルート マップを構成するには、次の手順を実行します。

始める前に

MPLS セグメント ルーティング トラフィック エンジニアリングおよび PBR 機能が有効になっていることを確認する必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**route-map FLOW1** *seq_num*
	例：
	`switch(config)# route-map FLOW1 seq 10`
	`switch(config-route-map)#`
		ルート マップに FLOW1 という名前を付けます。

	コマンドまたはアクション	目的

ステップ 2	**match** [**ip** | **ipv6**] **address** *acl_name*
	例：
	`switch(config-route-map)# match ip address L4_PORT`
	`switch(config-route-map)#`
		フィールドを説明する ACL を追加することにより、ルート マップが一致する必要のあるフィールドを指定します。

ステップ 3	**set srte-policy color** *num* **endpoint** *ip address*
	例：
	`switch(config-route-map)# set srte-policy color 121 endpoint 10.0.0.1`
	`switch(config-route-map)#`
		SRTE ポリシー カラーとポリシーのエンド ポイントを構成します。
		（注）
		IPv4 アドレスのみをエンドポイントにできます。

ステップ 4	**interface** *interface-type/slot/port*
	例：
	`switch(config-route-map)# interface ethernet 1/1`
	`switch(config-route-map-if)#`
		インターフェイス設定モードを開始します。

ステップ 5	[**ip** | **ipv6**] **policy route-map FLOW1**
	例：
	`switch(config-route-map-if)# ip policy route-map FLOW1`
	`switch(config-route-map-if)#`
		IP または IPv6 ポリシーベース ルーティングをインターフェイスに割り当てます。これにより、インターフェイスに入力するすべてのトラフィックのルート マップが適用されます。

名前で選択されたポリシーへのデフォルト VRF のルート マップ構成例

デフォルト VRF のトラフィックを名前で選択されたポリシーに導くルート マップを構成するには、次の手順を実行します。

始める前に

MPLS セグメント ルーティング トラフィック エンジニアリングおよび PBR 機能が有効になっていることを確認する必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**route-map FLOW1** *seq_num*
	例：
	`switch(config)# route-map FLOW1 seq 10`
	`switch(config-route-map)#`
		ルート マップに FLOW1 という名前を付けます。

	コマンドまたはアクション	目的

ステップ 2	**match** [**ip** | **ipv6**] **address** *acl_name*
	例：
	`switch(config-route-map)# match ip address L4_PORT`
	`switch(config-route-map)#`
		フィールドを説明する ACL を追加することにより、ルート マップが一致する必要のあるフィールドを指定します。

ステップ 3	**set srte-policy name** *policy-name*
	例：
	`switch(config-route-map)# set srte-policy name policy1`
	`switch(config-route-map)#`
		SRTE ポリシー名を構成します。

ステップ 4	**interface** *interface-type/slot/port*
	例：
	`switch(config-route-map)# interface ethernet 1/1`
	`switch(config-route-map-if)#`
		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 5	[**ip** | **ipv6**] **policy route-map FLOW1**
	例：
	`switch(config-route-map-if)# ip policy route-map FLOW1`
	`switch(config-route-map-if)#`
		IP または IPv6 ポリシーベース ルーティングをインターフェイスに割り当てます。これにより、インターフェイスに入力するすべてのトラフィックのルート マップが適用されます。

ネクストホップ、カラー、およびエンドポイントで選択されたポリシーへのデフォルト以外の VRF のルート マップ構成

デフォルト以外の VRF のトラフィックを、カラーとエンドポイントで選択されたポリシーに導くルートマップを構成するには、次の手順を実行します。この手順では、正しいMPLS VPNラベルがトラフィックに適用されるようにネクストホップを指定します。

始める前に

MPLS セグメント ルーティング トラフィック エンジニアリングおよびPBR 機能が有効になっていることを確認する必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**route-map FLOW1** *seq_num*
	例：
	`switch(config)# route-map FLOW1 seq 10`
	`switch(config-route-map)#`
		ルート マップに FLOW1 という名前を付けます。

	コマンドまたはアクション	目的

ステップ 2	**match** [**ip** | **ipv6**] **address** *acl_name*
	例：
	`switch(config-route-map)# match ip address L4_PORT`
	`switch(config-route-map)#`
		フィールドを説明する ACL を追加することにより、ルート マップが一致する必要のあるフィールドを指定します。

ステップ 3	**set** [**ip** | **ipv6**] **next-hop** *destination-ip-next-hop* **srte-policy color** *num* **endpoint** *ip address*
	例：
	`switch(config-route-map)# set ip next-hop 5.5.5.5 srte-policy color 121 endpoint 10.0.0.1`
	`switch(config-route-map)#`
		srte-policy（カラーおよびエンドポイント）を介して、構成されたネクストホップにパケットをリダイレクトします。

ステップ 4	**exit**
	例：
	`switch(config-route-map)# exit`
	`switch(config)#`
		ルートマップ構成モードを終了し、グローバル構成モードに戻ります。

ステップ 5	**interface** *interface-type/slot/port*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		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 6	**vrf member** *vrf-name*
	例：
	`switch(config-if)# vrf member vrf1`
	`switch(config-if)#`
		このインターフェイスを VRF に追加します。

ステップ 7	[**ip** | **ipv6**] **policy route-map FLOW1**
	例：
	`switch(config-if)# ip policy route-map FLOW1`
	`switch(config-if)#`
		IP または IPv6 ポリシーベース ルーティングをインターフェイスに割り当てます。これにより、インターフェイスに入力するすべてのトラフィックのルートマップが適用されます。

ステップ 8	[**no**] **shutdown**
	例：
	`switch(config-if)# no shutdown`
	`switch(config-if)#`
		インターフェイスをディセーブルにします。

デフォルト以外のVRFのルートマップをネクストホップおよびカラー別に選択されたポリシーに構成する

次の手順を実行し、デフォルト VRF のトラフィックを色とエンドポイントで選択されたポリシーに誘導するルートマップを構成しますが、エンドポイントは明示的に構成されていません。 ネクストホップが指定されているため、正しい MPLS VPN ラベルがトラフィックに適用され、正しい SRTE エンドポイントがネクストホップに一致するルートから取得されます。

始める前に

MPLS セグメント ルーティング トラフィック エンジニアリングおよび PBR 機能が有効になっていることを確認する必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**route-map FLOW1** *seq_num*
	例：
	`switch(config)# route-map FLOW1 seq 10`
	`switch(config-route-map)#`
		ルート マップに FLOW1 という名前を付けます。

ステップ 2	**match** [**ip** | **ipv6**] **address** *acl_name*
	例：
	`switch(config-route-map)# match ip address L4_PORT`
	`switch(config-route-map)#`
		フィールドを説明する ACL を追加することにより、ルート マップが一致する必要のあるフィールドを指定します。

ステップ 3	**set** [**ip** | **ipv6**] **next-hop** *destination-ip-next-hop* **srte-policy color** *num*
	例：
	`switch(config-route-map)# set ip next-hop 5.5.5.5 srte-policy color 121`
	`switch(config-route-map)#`
		srte-policy（カラー）を介して、構成されたネクストホップにパケットをリダイレクトします。

ステップ 4	**exit**
	例：
	`switch(config-route-map)# exit`
	`switch(config)#`
		ルートマップ構成モードを終了し、グローバル構成モードに戻ります。

ステップ 5	**interface** *interface-type/slot/port*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		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。

	コマンドまたはアクション	目的

ステップ 6	**vrf member** *vrf-name*
	例：
	`switch(config-if)# vrf member vrf1`
	`switch(config-if)#`
		このインターフェイスを VRF に追加します。

ステップ 7	[**ip** | **ipv6**] **policy route-map FLOW1**
	例：
	`switch(config-if)# ip policy route-map FLOW1`
	`switch(config-if-route-map)#`
		IP または IPv6 ポリシーベース ルーティングをインターフェイスに割り当てます。これにより、インターフェイスに入力するすべてのトラフィックのルートマップが適用されます。

ステップ 8	[**no**] **shutdown**
	例：
	`switch(config-if-route-map)# no shutdown`
	`switch(config-if-route-map)#`
		インターフェイスをディセーブルにします。

デフォルト以外の VRF のルートマップをネクストホップおよび名前別に選択されたポリシーに構成する

次の手順を実行して、デフォルト以外の VRF のトラフィックを名前別に選択されたポリシーに誘導するルート マップを構成します。ネクストホップは、正しい MPLS VPN ラベルがトラフィックに課されるように指定されます

始める前に

MPLS セグメント ルーティング トラフィック エンジニアリングおよび PBR 機能が有効になっていることを確認する必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**route-map FLOW1** *seq_num*
	例：
	`switch(config)# route-map FLOW1 seq 10`
	`switch(config-route-map)#`
		ルート マップに FLOW1 という名前を付けます。

ステップ 2	**match** [**ip** | **ipv6**] **address** *acl_name*
	例：
	`switch(config-route-map)# match ip address L4_PORT`
	`switch(config-route-map)#`
		フィールドを説明する ACL を追加することにより、ルート マップが一致する必要のあるフィールドを指定します。

	コマンドまたはアクション	目的

ステップ 3	**set** [**ip** | **ipv6**] **next-hop** *destination-ip-next-hop* **srte-policy** *name*
	例：
	`switch(config-route-map)# set ip next-hop 5.5.5.5 srte-policy policy1`
	`switch(config-route-map)#`
		srte-policy（名前）を介して、構成されたネクストホップにパケットをリダイレクトします。

ステップ 4	**exit**
	例：
	`switch(config-route-map)# exit`
	`switch(config)#`
		ルートマップ構成モードを終了し、グローバル構成モードに戻ります。

ステップ 5	**interface** *interface-type/slot/port*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		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 6	**vrf member** *vrf-name*
	例：
	`switch(config-if)# vrf member vrf1`
	`switch(config-if)#`
		このインターフェイスを VRF に追加します。

ステップ 7	[**ip** | **ipv6**] **policy route-map FLOW1**
	例：
	`switch(config-if)# ip policy route-map FLOW1`
	`switch(config-if)#`
		IP または IPv6 ポリシーベース ルーティングをインターフェイスに割り当てます。これにより、インターフェイスに入力するすべてのトラフィックのルートマップが適用されます。

ステップ 8	[**no**] **shutdown**
	例：
	`switch(config-if)# no shutdown`
	`switch(config-if)#`
		インターフェイスをディセーブルにします。

カラーとエンドポイントで選択されたポリシーへのデフォルト以外の VRF のルート マップ構成例

デフォルト以外の VRF のトラフィックを、カラーとエンドポイントで選択されたポリシーに導くルートマップを構成するには、次の手順を実行します。この手順では、指定するネクストホップは必要ありません。VPN ラベルは、ローカル スイッチで VRF に割り当てられたラベルを検索することによって取得されます。 これは、すべてのスイッチの VRF の BGP 割り当てインデックス構成を使用して、すべてのスイッチの VRF に同じラベルが割り当てられている場合にのみ構成可能です。

始める前に

MPLS セグメント ルーティング トラフィック エンジニアリングおよび PBR 機能が有効になっていることを確認する必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**route-map FLOW1** *seq_num*
	例：
	`switch(config)# route-map FLOW1 seq 10`
	`switch(config-route-map)#`
		ルート マップに FLOW1 という名前を付けます。

ステップ 2	**match** [**ip** | **ipv6**] **address** *acl_name*
	例：
	`switch(config-route-map)# match ip address L4_PORT`
	`switch(config-route-map)#`
		フィールドを説明する ACL を追加することにより、ルートマップが一致する必要のあるフィールドを指定します。

ステップ 3	**set srte-policy color** *num* **endpoint** *ip address*
	例：
	`switch(config-route-map)# set srte-policy color 121 endpoint 10.0.0.1`
	`switch(config-route-map)#`
		SRTE ポリシー カラーとポリシーのエンド ポイントを構成します。
		（注）
		IPv4 アドレスのみをエンドポイントにできます。

ステップ 4	**interface** *interface-type/slot/port*
	例：
	`switch(config-route-map)# interface ethernet 1/1`
	`switch(config-route-map-if)#`
		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 5	**vrf member** *vrf-name*
	例：
	`switch(config-route-map-if)# vrf member vrf1`
	`switch(config-route-map-if)#`
		このインターフェイスを VRF に追加します。

ステップ 6	[**ip** | **ipv6**] **policy route-map FLOW1**
	例：
	`switch(config-route-map-if)# ip policy route-map FLOW1`
	`switch(config-route-map-if)#`
		IP または IPv6 ポリシーベース ルーティングをインターフェイスに割り当てます。これにより、インターフェイスに入力するすべてのトラフィックのルート マップが適用されます。

ステップ 7	[**no**] **shutdown** 例：	インターフェイスをディセーブルにします。

	コマンドまたはアクション	目的
	`switch(config-route-map-if)# no shutdown` `switch(config-route-map-if)#`	

ステップ 8	**exit**
	例：
	`switch(config-route-map)# exit`
	`switch(config)#`
		ルートマップ構成モードを終了し、グローバル構成モードに戻ります。

ステップ 9	**feature bgp**
	例：
	`switch(config)# feature bgp`
	`switch(config)#`
		BGP 機能を開始します。

ステップ 10	**router bgp as-number**
	例：
	`switch(config)# router bgp 1.1`
	`switch(config-router)#`
		BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。

ステップ 11	**vrf** *vrf-name*
	例：
	`switch(config-router)# vrf vrf1`
	`switch(config-router-vrf)#`
		BGP プロセスを VRF に関連付けます。

ステップ 12	**allocate-index** *index* 例： `switch(config-router-vrf)# allocate-index 10`	VRF にインデックスを割り当てます。これにより、VRF にスタティック MPLS ローカル VPN ラベルを割り当てるように BGP に指示されます。VRF に割り当てられた MPLS VPN ラベルは、指定された値から取得されます。インデックスは、MPLS ラベル値の特別な範囲へのオフセットとして使用されます。 指定されたインデックス値の場合、同じローカル ラベルが常に許可されます。

名前で選択されたポリシーへのデフォルト以外のルートマップ構成例

次の手順を実行して、デフォルト以外の VRF のトラフィックを名前別に選択されたポリシーに誘導するルートマップを構成します。この手順では、指定するネクストホップは必要ありません。VPN ラベルは、ローカル スイッチで VRF に割り当てられたラベルを検索することによって取得されます。 これは、すべてのスイッチの VRF の BGP 割り当てインデックス構成を使用して、すべてのスイッチの VRF に同じラベルが割り当てられている場合にのみ構成可能です。

始める前に

MPLS セグメント ルーティング トラフィック エンジニアリングおよび PBR 機能が有効になっていることを確認する必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**route-map FLOW1** *seq_num*
	例：
	`switch(config)# route-map FLOW1 seq 10`
	`switch(config-route-map)#`
		ルート マップに FLOW1 という名前を付けます。

ステップ 2	**match** [**ip** | **ipv6**] **address** *acl_name*
	例：
	`switch(config-route-map)# match ip address L4_PORT`
	`switch(config-route-map)#`
		フィールドを説明する ACL を追加することにより、ルートマップが一致する必要のあるフィールドを指定します。

ステップ 3	**set srte-policy** *name*
	例：
	`switch(config-route-map)# set srte-policy policy1`
	`switch(config-route-map)#`
		SRTE ポリシー名を構成します。

ステップ 4	**interface** *interface-type/slot/port*
	例：
	`switch(config-route-map)# interface ethernet 1/1`
	`switch(config-route-map-if)#`
		インターフェイス設定モードを開始します。

ステップ 5	**vrf member** *vrf-name*
	例：
	`switch(config-route-map-if)# vrf member vrf1`
	`switch(config-route-map-if)#`
		このインターフェイスを VRF に追加します。

ステップ 6	[**ip** | **ipv6**] **policy route-map FLOW1**
	例：
	`switch(config-route-map-if)# ip policy route-map FLOW1`
	`switch(config-route-map-if)#`
		IP または IPv6 ポリシーベース ルーティングをインターフェイスに割り当てます。これにより、インターフェイスに入力するすべてのトラフィックのルート マップが適用されます。

ステップ 7	[**no**] **shutdown** 例：	インターフェイスをディセーブルにします。

	コマンドまたはアクション	目的
	`switch(config-route-map-if)# no shutdown` `switch(config-route-map-if)#`	

ステップ 8	**exit**
	例：
	`switch(config-route-map)# exit`
	`switch(config)#`
		ルートマップ構成モードを終了し、グローバル構成モードに戻ります。

ステップ 9	**feature bgp**
	例：
	`switch(config)# feature bgp`
	`switch(config)#`
		BGP 機能を開始します。

ステップ 10	**router bgp as-number**
	例：
	`switch(config)# router bgp 1.1`
	`switch(config-router)#`
		BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。

ステップ 11	**vrf** *vrf-name*
	例：
	`switch(config-router)# vrf vrf1`
	`switch(config-router-vrf)#`
		BGP プロセスを VRF に関連付けます。

ステップ 12	**allocate-index** *index* 例： `switch(config-router-vrf)# allocate-index 10`	VRF にインデックスを割り当てます。これにより、VRF にスタティック MPLS ローカル VPN ラベルを割り当てるように BGP に指示されます。VRF に割り当てられた MPLS VPN ラベルは、指定された値から取得されます。インデックスは、MPLS ラベル値の特別な範囲へのオフセットとして使用されます。 指定されたインデックス値の場合、同じローカル ラベルが常に許可されます。

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。