# Application-Aware Routing

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます：**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、および **Cisco vSmart** から **Cisco Catalyst SD-WAN Controller** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。



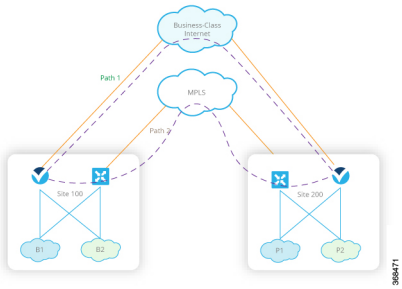
## アプリケーション認識型ルーティングについて

アプリケーション認識型ルーティングは、Cisco IOS XE Catalyst SD-WAN デバイス間のデータプレーントンネルのネットワークとパスの特性を追跡し、収集した情報を使用してデータトラフィックの最適なパスを計算します。対象となる特性には、パケット損失、遅延、ジッター、リンクの負荷、コスト、帯域幅などがあります。ルートプレフィックス、メトリック、リンクステート情報、Cisco IOS XE Catalyst SD-WAN デバイスでのルート削除など、標準のルーティングプロトコルで使用されるパス選択の要因以外を考慮する機能があるため、企業に次のような多くの利点をもたらします。

- 通常のネットワーク運用の場合は、ネットワークを経由するアプリケーション データ トラフィックのパスを最適化できます。アプリケーションの SLA で定義されたパケット損

失、遅延、ジッターに対し、必要なレベルを満たせるようにする WAN リンクにパスを誘導することにより、これを実現します。

- ネットワークの停止またはソフト障害が発生した場合は、パフォーマンスの低下を最小限に抑えることができます。ネットワークとパスの状況をリアルタイムなアプリケーション認識型ルーティングで追跡するので、パフォーマンスの問題をすぐに明らかにし、利用できる最善なパスにデータトラフィックをリダイレクトする戦略を自動的にアクティブ化させます。ネットワークがソフト障害の状態から回復すると、アプリケーション認識型ルーティングはデータトラフィックパスを自動的に再調整します。
- データトラフィックをより効率的にロードバランシングできるため、ネットワークコストを削減できます。
- WAN をアップグレードせずに、アプリケーションのパフォーマンスを向上させることができます。




各 Cisco IOS XE Catalyst SD-WAN デバイスは最大 8 つの TLOC をサポートするので、1 つの Cisco IOS XE Catalyst SD-WAN デバイスを最大 8 つの異なる WAN ネットワークに接続できます。 この機能により、アプリケーション トラフィックにパケット損失と遅延に関するさまざまなニーズがあっても、パスのカスタマイズができるのです。

# マルチキャストプロトコルに対応したアプリケーション認識型ルーティング

**表 *1*: 機能の履歴**

| 機能 | リリース情報 | 説明 |
|---|---|---|
| マルチキャストに対応したアプリケーション認識型ルーティング | Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a<br>Cisco vManage リリース 20.3.1 | これは、送信元と宛先、プロトコル照合、および SLA 要件に基づいて、Cisco IOS XE Catalyst SD-WAN デバイスのマルチキャストトラフィックに、アプリケーション認識型ルーティングポリシーを設定できるようにする機能です。 |

Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a 以降、アプリケーション認識型ルーティングは、Cisco IOS XE Catalyst SD-WAN デバイス上のオーバーレイ マルチキャスト トラフィックをサポートしています。これ以前のリリースでは、アプリケーション ルート ポリシーはユニキャストトラフィックにしか対応していません。

Cisco IOS XE Catalyst SD-WAN デバイスは、グループアドレスに基づいてマルチキャストトラフィックを分類し、SLA クラスを設定します。グループアドレスには、送信元 IP、宛先 IP、送信元プレフィックス、および宛先プレフィックスを指定できます。フォワーディングプレーンでは、グループアドレスのトラフィックは、SLA 要件を満たす TLOC パスのみを使用する必要があります。グループのパス選択は、優先カラー、バックアップカラー、またはデフォルトアクションに基づいて実行できます。

# マルチキャストプロトコルに関する制約事項

Cisco Catalyst SD-WAN Application Intelligence Engine（SAIE）フローを使用する Network-Based Application Recognition（NBAR）は、マルチキャストではサポートされていません。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、SAIE フローはディープ パケット インスペクション（DPI）フローと呼ばれていました。

# アプリケーション認識型ルーティングのコンポーネント

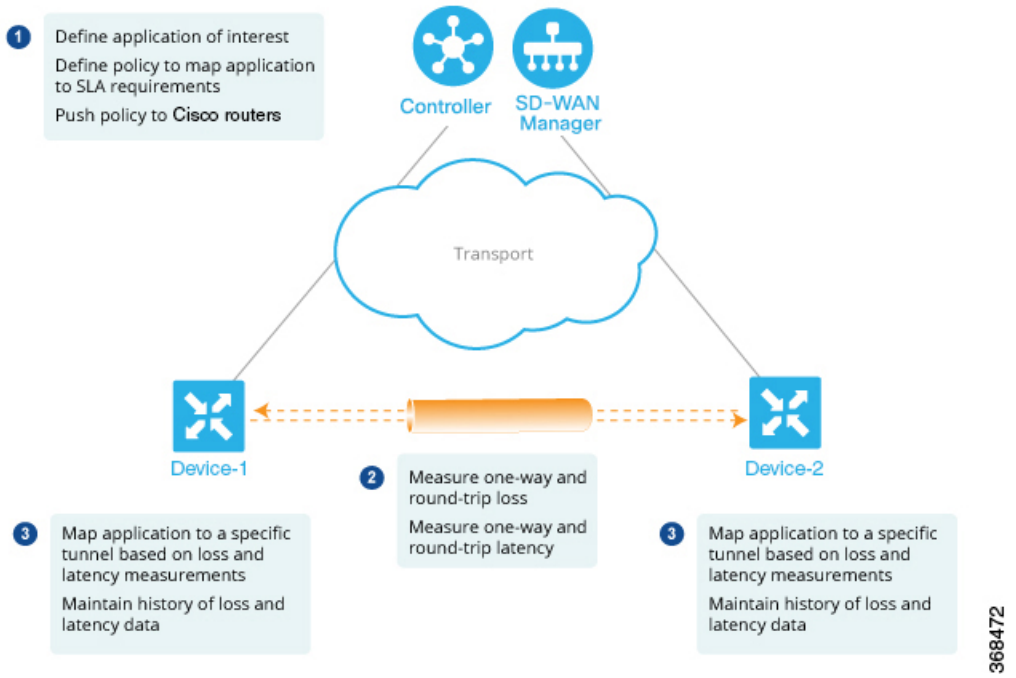
Cisco IOS XE Catalyst SD-WAN アプリケーション認識型ルーティングのソリューションは、次の 3 つの要素で構成されています。

- **識別**：目的のアプリケーションを定義してから、アプリケーションを特定の SLA 要件にマッピングする一元管理型データポリシーを作成します。パケットのレイヤ 3 ヘッダーとレイヤ 4 ヘッダー（送信元と宛先のプレフィックス、ポート、プロトコル、DSCP フィールドなど）を照合して、目的のデータトラフィックを選び出します。すべての一元管理型データポリシーと同様に、Cisco Catalyst SD-WAN コントローラ で設定すると、適切な Cisco IOS XE Catalyst SD-WAN デバイスに渡されます。

- **モニタリングと測定**：Cisco IOS XE Catalyst SD-WAN ソフトウェアでは BFD パケットを使用して、デバイス間のデータプレーントンネル上のデータトラフィックを継続的にモニターし、トンネルのパフォーマンス特性を定期的に測定します。パフォーマンスを測定するために、Cisco IOS XE Catalyst SD-WAN デバイスはトンネルでのトラフィック損失を探し、トンネルを通過するトラフィックの片道時間と往復時間を調べることで遅延を測定します。これらの測定値によって、最適ではないデータトラフィックの状態が示されることもあります。

- **特定のトランスポートトンネルへのアプリケーショントラフィックのマッピング**：最後の手順では、アプリケーションのデータトラフィックを、そのアプリケーションに必要なパフォーマンスを提供するデータプレーントンネルにマッピングします。マッピングの決定は、WAN 接続で実行された測定値から計算されたベストパス基準と、アプリケーション

認識型ルーティングに固有のポリシーで指定された制約という2つの基準に基づいて行われます。




レイヤ7アプリケーション自体に基づいてデータポリシーを作成するには、一元管理型データポリシーを使用して Cisco Catalyst SD-WAN アプリケーション インテリジェンス エンジン（SAIE）フローを設定します。SAIE フローを使用すると、リモート TLOC、リモート TLOC、あるいはその両方に基づいて、トラフィックを特定のトンネルに転送できます。トンネルへのトラフィック転送は、SLA クラスに基づいて行うことはできません。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、SAIE フローはディープ パケット インスペクション（DPI）フローと呼ばれていました。

# SLA クラス

表 *2 :* 機能の履歴

| 機能 | リリース情報 | 説明 |
|---|---|---|
| SLA クラスのサポート | Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r | Cisco SD-WAN コントローラで最大 8 つの SLA クラスを設定できます。この機能を使用すると、アプリケーション認識型ルーティングポリシーに追加のオプションを設定できます。 |
| 各ポリシーで 6 つの SLA クラスのサポート | Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a<br>Cisco vManage リリース 20.3.1 | Cisco IOS XE Catalyst SD-WAN デバイスのポリシーごとに、最大 6 つの SLA クラスを設定できます。この機能拡張により、アプリケーション認識型ルーティングポリシーに追加のオプションを設定できます。 |
| SLA クラスのサポートの拡張機能 | Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a<br>Cisco vManage リリース 20.6.1 | Cisco IOS XE Catalyst SD-WAN デバイスで最大 16 の SLA クラスをサポートするための拡張機能です。 |
| アプリケーション認識型ルーティングおよびデータポリシーの SLA 優先色 | Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a<br>Cisco vManage リリース 20.6.1 | アプリケーション認識型ルーティングポリシーとデータポリシーの両方が設定されている場合、SLA 要件を基に優先色を選択するためのさまざまな動作を提供します。 |

サービスレベル契約（SLA）は、アプリケーション認識型ルーティングで実行されるアクションを決定します。SLA クラスは、Cisco IOS XE Catalyst SD-WAN デバイスのデータプレーントンネルの最大ジッター、最大遅延、最大パケット損失、またはこれらの値の組み合わせを定義します。各データプレーントンネルは、ローカルトランスポートロケータ（TLOC）とリモート TLOC のペアで構成されます。Cisco SD-WAN コントローラの **policy sla-class** コマンド階層で SLA クラスを設定できます。Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r から、最大 8 つの SLA クラスを Cisco SD-WAN Validator で設定できます。ただし、アプリケーション認識ルートポリシーで定義できる一意の SLA クラスは 4 つだけです。Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r より前のリリースでは、最大 4 つの SLA クラスを設定できます。

Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a 以降、Cisco IOS XE Catalyst SD-WAN デバイスのポリシーごとに最大 6 つの SLA クラスを設定できます。

SLA クラスでは、次のパラメータを設定できます。

表 *3 : SLA* コンポーネント

| 説明 | コマンド | 値または範囲 |
|---|---|---|
| データプレーントンネルの最大許容パケットジッター | **ジッター**（ミリ秒） | 1 ～ 1000 ミリ秒 |
| データプレーントンネルの最大許容パケット遅延。 | **遅延**（ミリ秒） | 1 ～ 1000 ミリ秒 |
| データプレーントンネルの最大許容パケット損失 | **損失率**（%） | 1 ～ 100% |

### SLA サポートの機能拡張

Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a および Cisco vManage リリース 20.6.1 以降、Cisco IOS XE Catalyst SD-WAN デバイスのポリシーごとに 6 つ以上の SLA クラスを設定できます。

Cisco IOS XE Catalyst SD-WAN デバイスが最大 16 の SLA クラスをサポートするには、16 GB 以上の RAM が必要です。

この機能拡張により、Cisco SD-WAN コントローラ および SD-WAN エッジデバイスでサポートされる SLA クラスの数が増加します。SLA クラスのサポートの増加により、SLA クラスをマルチプロトコル ラベル スイッチング（MPLS）ネットワーク上の IP 仮想プライベートネットワーク（IP-VPN）に合わせて、グローバルネットワークにトラフィックを転送できます。

SLA の機能拡張はマルチテナントに役立ち、テナントごとに異なる SLA クラスをプッシュできます。マルチテナント機能を使用するには、Cisco SD-WAN コントローラ が 8 つ以上の SLA クラスをサポートする必要があります。SLA クラスを異なるテナントに割り当てるには、ポリシーのグローバル制限を 64 にする必要があります。

（注） デフォルトの SLA は設定できません。デフォルトの SLA は、ユーザー定義の SLA が満たされない場合にトラフィックを転送するよう、すべてのデバイスに設定されます。

表 *4 : Cisco IOS XE Catalyst SD-WAN* デバイスでサポートされる最大 *SLA* クラス数

| サポートするプラットフォームとモデル | **Cisco IOS XE Catalyst SD-WAN** リリース **17.6.1a** より前のユーザー設定可能な **SLA** クラス（**+1** デフォルト **SLA** クラス） | **Cisco IOS XE Catalyst SD-WAN** リリース **17.6.1a** 以降のユーザー設定可能な **SLA** クラス（**+1** デフォルト **SLA** クラス） |
|---|---|---|
| ASR 1001 HX -16GB<br>• vedge-ASR-1001-HX | 6 | 15 |

| サポートするプラットフォームとモデル | **Cisco IOS XE Catalyst SD-WAN** リリース **17.6.1a** より前のユーザー設定可能な **SLA** クラス（**+1** デフォルト **SLA** クラス） | **Cisco IOS XE Catalyst SD-WAN** リリース **17.6.1a** 以降のユーザー設定可能な **SLA** クラス（**+1** デフォルト **SLA** クラス） |
|---|---|---|
| ASR 1002 X -16GB<br>• vedge-ASR-1002-X | 6 | 15 |
| ASR 1002 HX -16GB<br>• vedge-ASR-1002-HX | 6 | 15 |
| ASR 1001 X -16GB<br>• vedge-ASR-1001-X | 6 | 15 |
| ISR 4451 X<br>• vedge-ISR-4451-X | 6 | 7 |
| ISR 4431<br>• vedge-ISR-4431 | 6 | 7 |
| Catalyst 8300 エッジプラットフォーム<br>• vedge-C8300-2N2S-6G<br>• vedge-C8300-2N2S-4G2X<br>• vedge-C8300-1N1S-6G<br>• vedge-C8300-1N1S-4G2X<br>• vedge-C8300-1N1S-6T<br>• vedge-C8300-1N1S-4T2X<br>• vedge-C8300-2N2S-6T<br>• vedge-C8300-2N2S-4T2X | 該当なし | 7 |
| Catalyst 8500 エッジプラットフォーム -16GB<br>• vedge-C8500L-8S4X<br>• vedge-C8500-12X4QC<br>• vedge-C8500-12X | 該当なし | 15 |

| サポートするプラットフォームとモデル | Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a より前のユーザー設定可能な SLA クラス（+1 デフォルト SLA クラス） | Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降のユーザー設定可能な SLA クラス（+1 デフォルト SLA クラス） |
|---|---|---|
| その他の Cisco IOS XE Catalyst SD-WAN デバイス（C11xx、ISR1100、CSR1000v） | 6 | 6 |

### SLA 優先色

Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以降、アプリケーション認識型ルーティングポリシーとデータポリシーの両方を設定し、データフローがアプリケーションルートとデータポリシーのシーケンスに一致する場合、想定される次の動作が発生します。

- アプリケーション認識型ルーティングで設定した優先色が SLA 要件を満たし、これらの優先色にデータポリシーと共通した色が含まれる場合、他の色よりも共通の優先色が転送用に選択されます。（Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a 以前は、データポリシーの優先色が転送され、アプリケーション認識型ルーティングポリシーの推奨は無視されていました）。
- アプリケーション認識型ルーティングの優先色が SLA を満たしていないが、データポリシーと共通する色があり、それらの色がアプリケーション認識型ルーティングの SLA を満たしている場合、これらの色が推奨され、転送用に選択されます。
- アプリケーション認識型ルーティングで SLA を満たすトンネルまたは色がない場合は、データポリシーが推奨され、転送用に選択されます。データポリシーに優先色がある場合は、それらの色が選択されます。それ以外の場合は、データポリシーのすべての色でロードバランスが発生します。

# トンネルの SLA クラスへの分類

アプリケーション認識型ルーティングのためにトンネルを 1 つ以上の SLA クラスに分類するプロセスは、次の 3 つのパートで構成されます。

- トンネルの損失、遅延、ジッター情報の測定。
- トンネルの平均損失、遅延、ジッターの計算。
- トンネルの SLA 分類の決定。

## 損失、遅延、ジッターの測定

オーバーレイネットワークでデータプレーントンネルが確立されると、トンネルで BFD セッションが自動的に開始されます。オーバーレイネットワークでは、各トンネルはローカル TLOC とリモート TLOC 間の特定のリンクを識別する色で識別されます。BFD セッションは、Hello

パケットを定期的に送信してリンクが動作しているかどうかを検出することで、トンネルの稼働状態をモニタリングします。アプリケーション認識型ルーティングでは、BFD Hello パケットを使用して、リンクの損失、遅延、およびジッターを測定します。

デフォルトでは、BFD Hello パケット間隔は 1 秒です。この間隔は、ユーザーが設定できます（**bfd color interval** コマンドを使用）。BFD Hello パケット間隔はトンネルごとに設定できることに注意してください。

## 平均損失、遅延、およびジッターの計算

BFD は、Cisco IOS XE Catalyst SD-WAN デバイス上のすべてのトンネルを定期的にポーリングして、アプリケーション認識型ルーティングで使用するパケット遅延、損失、ジッター、およびその他の統計情報を収集します。アプリケーション認識型ルーティングは、ポーリング間隔ごとに、各トンネルの平均損失、遅延、およびジッターを計算し、各トンネルの SLA を計算または再計算します。各ポーリング間隔は「バケット」とも呼ばれます。

デフォルトでは、ポーリング間隔は 10 分間です。デフォルトの BFD Hello パケット間隔が 1 秒の場合、トンネルの損失、遅延、ジッターを計算するために、1 回のポーリング間隔で約 600 個の BFD Hello パケット情報が使用されることを意味します。ポーリング間隔は、ユーザーが設定できます（**bfd app-route poll-interval** コマンドを使用）。アプリケーション認識型ルーティングのポーリング間隔は、Cisco IOS XE Catalyst SD-WAN デバイスごとに設定できることに注意してください。つまり、デバイスを起点とするすべてのトンネルに適用されるということです。

BFD Hello パケット間隔を短くせずにポーリング間隔を短くすると、損失、遅延、ジッターの計算品質に影響する可能性があります。たとえば、BFD Hello パケット間隔が 1 秒の場合にポーリング間隔を 10 秒に設定すると、トンネルの損失、遅延、ジッターの計算に 10 個の Hello パケットのみが使用されます。

各ポーリング間隔からの損失、遅延、ジッター情報は、6 回のポーリング間隔にわたって保持されます。7 回目のポーリング間隔では、最も早いポーリング間隔の情報が破棄され、最新の情報が優先されます。このように、アプリケーション認識型ルーティングでは、トンネル損失、遅延、ジッター情報のスライディングウィンドウが維持されます。

ポーリング間隔の数（6）は、ユーザーでは設定できません。各ポーリング間隔は、**show app-route statistics** コマンドの出力のインデックス番号（0 ～ 5）によって識別されます。

## SLA 分類の決定

トンネルの SLA 分類を決定するために、アプリケーション認識型ルーティングでは、最新のポーリング間隔に応じて収集された損失、遅延、およびジッター情報を使用します。使用されるポーリング間隔の数は、乗数によって決まります。デフォルトでは、乗数は 6 であるため、すべてのポーリング間隔（特に最後の 6 回のポーリング間隔）を通した情報を使用して分類が決定します。デフォルトのポーリング間隔が 10 分で、デフォルトの乗数が 6 の場合、各トンネルの SLA を分類するときに、直前の 1 時間に収集された損失、遅延、およびジッター情報が考慮されます。これらのデフォルト値は、トンネルの頻繁な再分類（フラッピング）を防ぐ方法として、一種の減衰となるように選択する必要があります。

乗数はユーザーが設定できます（**bfd app-route multiplier** コマンドを使用）。アプリケーション認識型ルーティング乗数は Cisco IOS XE Catalyst SD-WAN デバイスごとに設定できることに注意してください。つまり、デバイスを起点とするすべてのトンネルに適用されるということです。

トンネル特性の変化に迅速に対応する必要がある場合は、乗数を 1 まで減らすことができます。乗数が 1 の場合、そのトンネルが 1 つ以上の SLA 基準を満たすことができるかどうかを判断するために、最新のポーリング間隔での損失と遅延の値のみが使用されます。

トンネル損失と遅延の測定と計算に基づくと、各トンネルが 1 つ以上のユーザー設定の SLA クラスを満たすこともあります。たとえば、平均損失が 0 パケット、平均遅延が 10 ミリ秒のトンネルであれば、最大パケット損失が 5、最小遅延が 20 ミリ秒で定義されたクラスを満たすことになりますが、その上、最大パケット損失 0 、最小遅延が 15 ミリ秒で定義されたクラスも満たすことになります。

トンネルが再分類される速度に関わらず、損失、遅延、およびジッター情報は継続的に測定および計算されます。アプリケーション認識型ルーティングによる変更への対応速度は、ポーリング間隔と乗数を変更することで設定できます。

# クラスごとのアプリケーション認識型ルーティング

**表 *5:* 機能の履歴**

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| クラスごとのアプリケーション認識型ルーティング | Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a<br>Cisco vManage リリース 20.4.1 | この機能により、サービスレベル契約（SLA）の定義に基づいてトラフィックをネクストホップアドレスに転送する機能が強化されます。この SLA 定義と、トラフィックタイプを照合および分類するポリシーを使用することで、特定の Cisco Catalyst SD-WAN トンネルを介してトラフィックを転送できます。SLA の定義は、損失、遅延、ジッターの値で構成されます。これらの値は、2 つのトランスポートロケータ（TLOC）間に存在するBidirectional Forwarding Detection（BFD）チャネルを使用して測定されます。 |

## クラスごとのアプリケーション認識型ルーティングの概要

SLA 定義は、2 つの TLOC 間に存在する BFD チャネルを使用して測定される損失、遅延、およびジッターの値で構成されます。これらの値から、ネットワークと BFD リンクのステータスがまとめて表されます。BFD 制御メッセージは、Differentiated Services Code Point（DSCP）が 48 という高プライオリティで送信されます。

高プライオリティパケットに基づく SLA メトリックには、エッジデバイスを通過する実際のデータによって受信されるプライオリティが反映されません。データは、アプリケーションク

ラスに応じて、ネットワーク内で異なるDSCP値を持つことができます。したがって、ネットワークがこのような測定を使用してトラフィックタイプを適切なトンネルに転送するには、トラフィックプロファイルの損失、遅延、およびジッターをより正確に表現する必要があります。

アプリケーション認識型ルーティングでは、アプリケーションの転送に使用できるパスを制約するポリシーを使用します。こうした制約は通常、SLA クラスに規定された、満たすべき損失、遅延、およびジッターの要件をもとに表現されます。これに沿うには、これらのメトリックを、トラフィックの宛先に向かうすべてのパスで、アクティブプローブまたはパッシブモニタリングを使用して測定する必要があります。

アクティブプローブの方法には、実際のトラフィックとともに注入される合成トラフィックの生成などがあります。この場合、プローブと実際のトラフィックが同じように転送されることが想定されます。BFD プローブ、ICMP、定期的な HTTP 要求、および IP SLA 測定は、アクティブプローブの仕組みを表す例です。Cisco Catalyst SD-WAN ソリューションでは、アクティブな測定にBFDベースのプローブを使用します。パッシブモニタリング方式は、Cisco Catalyst SD-WAN Application Intelligence Engine（SAIE）フローを使用して、実際のトラフィックをモニタリングします。たとえば、RTP/TCP トラフィックは、損失、遅延、およびジッターを確認するためにモニタリングされます。

（注） Cisco vManage リリース 20.7.1 以前のリリースでは、SAIE フローはディープ パケット インスペクション（DPI）フローと呼ばれていました。

## アプリケーション プローブ クラス

アプリケーション プローブ クラス（app-probe-class）は、転送クラス、カラー、および DSCP で構成されます。これによって、転送されるアプリケーションのカラーごとのマーキングが定義されます。カラーまたは DSCP マッピングは、Cisco SD-WAN ネットワークサイトに対してローカルです。ただし、いくつかのカラーと、カラーのDSCPマッピングはサイトごとに変更されません。転送クラスによって、BFDエコー要求を出力トンネルポートでキューイングする場合のQoSキューが決まります。これは、BFDエコー要求パケットにのみ適用されます。BFD パケットのパケット損失優先順位は低に固定されています。BFD パケットが SLA クラスで送信される場合、同じ DSCP 値が使用されます。BFD パケットが SLA クラスとともに app-probe-class を使用して送信される場合、BFD パケットは各 SLA app-probe-class に対してラウンドロビン方式で個別に送信されます。

（注） アプリケーション ルート ポリシーがサイトに適用されると、そのサイトに関連するカラーのみが使用されます。Cisco IOS XE Catalyst SD-WAN デバイスは 6 つの SLA クラスをサポートしているため、app-probe-class も同様に最大 6 つまでサポートされます。

## デフォルトの DSCP 値

DSCP 制御トラフィックで使用されるデフォルトの DSCP 値は 48 です。ただし、エッジデバイスで設定するオプションとともに、デフォルト値を変更するプロビジョニングがあります。すべてのネットワーク サービス プロバイダーが DSCP 48 を使用するとは限りません。

デフォルトの DSCP を持つ BFD パケットは、PMTU などの他の機能にも使用できます。デフォルト DSCP を変更すると、他の機能が変更後のデフォルト DSCP 値に影響を受けます。したがって、サービスプロバイダーが提供する、優先順位の最も高い DSCP マーキングを設定することを推奨します（通常は 48 ですが、サービスプロバイダーの SLA 契約によって異なる場合があります）。色のレベルは、グローバルレベルのデフォルト DSCP マーキングを上書きします。

# アプリケーション認識型ルーティングの設定

**表 *6:* 機能の履歴**

| 機能名 | リリース情報 | 説明 |
|---|---|---|
| IPv6 向けアプリケーション認識型ルーティング | Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a<br>Cisco vManage リリース 20.9.1 | これは、アプリケーション認識型ルーティング（AAR）ポリシーを設定して、IPv6 アプリケーション トラフィックで動作できるようにする機能です。 |

このトピックでは、アプリケーション認識型ルーティングを設定するための一般的な手順について説明します。アプリケーション認識型ルーティングポリシーによって影響を受けるトラフィックは、サービス側（ローカル/WAN 側）から Cisco IOS XE Catalyst SD-WAN デバイスのトンネル（WAN）側に流れるトラフィックのみです。

アプリケーション認識型ルーティングポリシーでは、アプリケーションを SLA と照合します。つまり、アプリケーションのデータトラフィックを送信するために必要なデータプレーントンネルのパフォーマンス特性と照合するということです。アプリケーション認識型ルーティングポリシーの主な目的は、Cisco IOS XE Catalyst SD-WAN デバイスによって送信されるデータトラフィックのパスを最適化することにあります。

アプリケーション認識型ルーティングポリシーは、一元管理型データポリシーの一種です。vSmart コントローラでポリシーを設定すると、コントローラから影響を受ける Cisco IOS XE Catalyst SD-WAN デバイスに自動的にプッシュされます。他のポリシーと同様に、アプリケーション認識型ルーティングポリシーも、一連の番号（順序）が付いたマッチ/アクションペアのシーケンスで構成されています。こうしたペアは、順番に、シーケンス番号の昇順で評価されます。データパケットがいずれかのマッチ条件にマッチすると、SLA アクションがパケットに適用され、そのパケットの送信に使用するデータプレーントンネルが決まります。パケットがどのポリシーシーケンスのパラメータにもマッチせず、default-action に SLA クラスが設定されていない場合、そのパケットは SLA を考慮せずに受け入れられ、転送されます。アプリケーション認識型ルーティングポリシーは、デフォルトでマッチしないトラフィックを受け入れる

ようになっているため、ポジティブポリシーと見なされています。Cisco IOS XE Catalyst SD-WAN ソフトウェアの他のポリシータイプはネガティブポリシーですが、それは、デフォルトでマッチしないトラフィックをドロップするからです。

Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1 以降では、AAR ポリシーとデータポリシーを設定して、マッチアプリケーション、つまり app-list 基準に基づいて IPv6 トラフィックを制御できます。

Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a 以前は、IPv6 トラフィックには、アプリケーション名またはアプリケーションリストに基づいて IPv6 トラフィックを照合し、目的のインテントに基づいて IPv6 トラフィックを誘導する機能がありませんでした。

# Cisco SD-WAN Manager を使用したアプリケーション認識型ルーティングポリシーの設定

アプリケーション認識型ルーティングポリシーを設定するには、Cisco SD-WAN Manager ポリシー構成ウィザードを使用します。一元管理型ポリシーの設定に関する詳細は、「一元管理型ポリシーの設定」を参照してください。このウィザードは、次のような4つのウィンドウが順次開いてポリシーコンポーネントの作成および編集プロセスをガイドするようになっています。

- [アプリケーションまたは対象グループの作成（Create Applications or Groups of Interest）]：関連する項目をグループ化し、ポリシーのマッチやアクションコンポーネントで呼び出すリストを作成します。設定の詳細については、「対象グループの設定」を参照してください。
- [トポロジの設定（Configure Topology）]：ポリシーが適用されるネットワーク構造を作成します。トポロジ設定の詳細については、「トポロジと VPN メンバーシップの設定」を参照してください。
- [トラフィックルールの設定（Configure Traffic Rules）]：ポリシーのマッチ条件とアクション条件を作成します。
- [サイトと VPN にポリシーを適用（Apply Policies to Sites and VPNs）]：ポリシーをオーバーレイネットワークのサイトと VPN に関連付けます。

ポリシー構成ウィザードの最初の3ウィンドウで、ポリシーコンポーネント、つまりブロックを作成します。最後のウィンドウで、オーバーレイネットワークのサイトと VPN にポリシーブロックを適用します。

アプリケーション認識型ルーティングポリシーを有効にするには、ポリシーをアクティブ化する必要があります。

# 最善のトンネルパスの設定

表 *7:* 機能の履歴

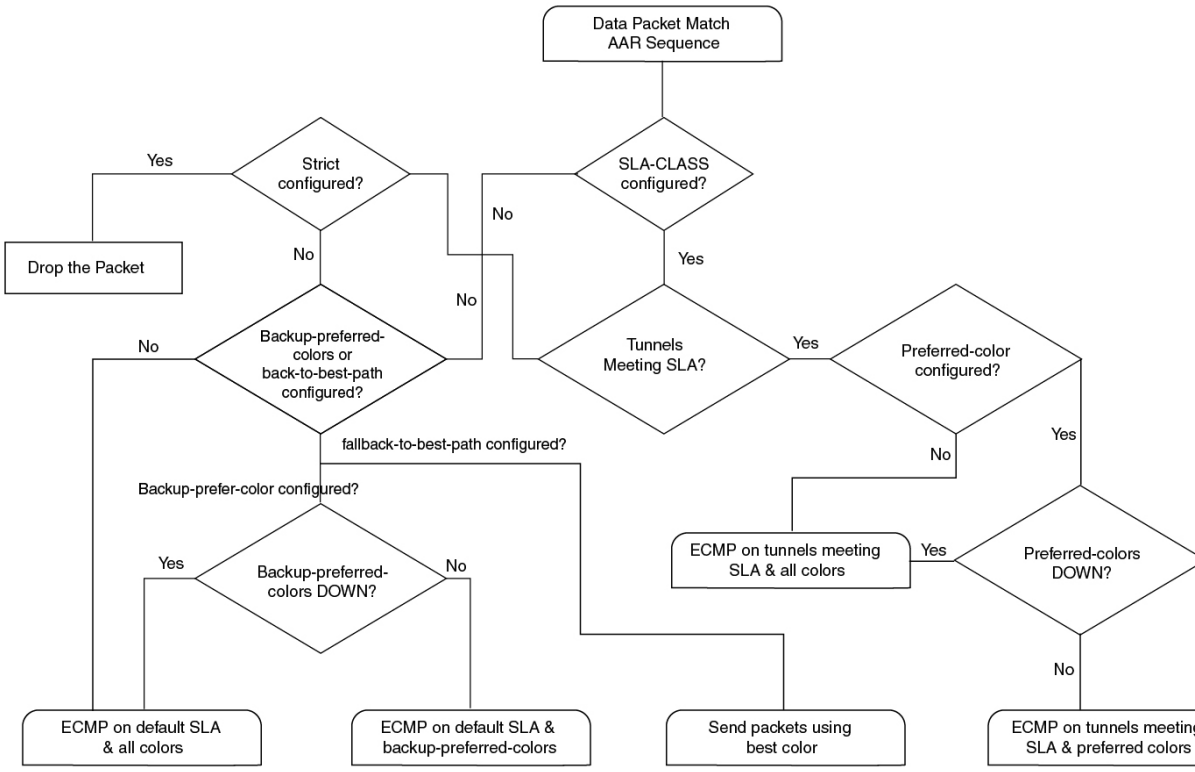
| 機能名 | リリース情報 | 説明 |
|---|---|---|
| ベストオブザワースト（最悪の中の最善、BOW）トンネルの選択 | Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a<br>Cisco vManage リリース 20.5.1 | この機能では、使用可能な色からベストパスや色を選択する新しいポリシーアクション **fallback-to-best-path** を導入しています。<br>データトラフィックが SLA クラスの要件のいずれも満たしていない場合、この機能により、各 SLA クラスの [フォールバックベストトンネル（Fallback Best Tunnel）] オプションを使用して最適なトンネルパスの基準の順序を選択し、パケット損失を回避できます。 |

## 最善のトンネルパスの概要

SLAが満たされていない場合にデータパケット損失を回避し、最適なアプリケーション認識型ルーティングトンネルの選択を設定するために、次のポリシーアクションを設定できます。

- **backup-preferred-color**
- **backup-preferred-color**

図 *1*: アプリケーション認識型ルーティングトンネル選択のフローチャート




## 最善のトンネルパスに向けた推奨事項

- SLA クラスを設定するときに、Cisco SD-WAN Manager で **fallback-to-best-path policy action** ポリシーアクションを設定します。
- トラフィックルールを設定するときに、Cisco SD-WAN Manager で **backup-preferred-color** ポリシーアクションを設定します。

## 最善のトンネルパスに向けたバリアンス設定

Cisco SD-WAN Manager では、SLA クラス要件のいずれも満たすトンネルがない場合に、ベストオブワースト（最悪の中の最善、BOW）機能を使用して最善のトンネルを検索します。

仮にSLA クラスの要件を満たすために規定されている遅延が 100 ミリ秒で、トンネル T1 の遅延が 110 ミリ秒だったとします。トンネル T2 は 111 ミリ秒、トンネル T3 は 112 ミリ秒です。

BOW ロジックによると、最善のトンネルは T1 です。T2 と T3 は、差が数ミリ秒しかないので、同じくらい良いトンネルと言えます。

SLA クラスを設定するときは、Cisco SD-WAN Manager でバリアンスを設定します。バリアンスがあると、最善のトンネル選択の一環として小さな偏差に対応できます。

詳細については、「SLA クラスの設定（Configure SLA Class）」を参照してください。

### 例：バリアンスが設定されていない場合

時刻 t0：T1 は 100 ミリ秒、T2 は 101 ミリ秒、T3 は 102 ミリ秒

時刻 t1：T1 は 101 ミリ秒、T2 は 100 ミリ秒、T3 は 102 ミリ秒

時刻 t3：T1 は 101 ミリ秒、T2 に 112 ミリ秒、T3 に 100 ミリ秒

時刻 t1 で、最善のトンネルが T1 から T2 に変更され、時刻 t2 で、最善のトンネルが T2 から T3 に変更されます。バリアンスが設定されていないと、データパスの再プログラミングとデータトラフィックパスの変更が発生することになります。

代わりに、ミリ秒単位の小さな偏差を減衰するようにバリアンスを設定すると仮定します。

たとえば、バリアンスを 5 ミリ秒に設定すると、最善のトンネル SLA は 100 ミリ秒ということになります。範囲は 100 ～ 105 ミリ秒です。

### 例：バリアンスが設定されている場合

BOW(t0) = {T1、T2、T3}

BOW(t1) = {T1、T2、T3}

BOW(t2) = {T1、T2、T3}

バリアンスが設定されている場合、データパスの再プログラミングやデータトラフィックパスの変更は必要ありません。

## 最善のトンネルパスに向けたバリアンス設定の確認

### 遅延バリアンスの例

```
Device# show sdwan policy from-vsmart
from-vsmart sla-class video
latency                       100
jitter                        150
 fallback-best-tunnel         latency

Tunnel T1: Latency: 110 msec, Loss: 0%, Jitter: 200 msec
Tunnel T2: Latency: 115 msec, Loss: 0%, Jitter: 200 msec
Tunnel T3: Latency: 120 msec, Loss: 0%, Jitter: 200 msec
```

遅延バリアンスがない場合、最適なトンネルは T1 です。

遅延バリアンスが 10 ミリ秒に設定されている場合、T1、T2、T3 が最適なトンネルです。

範囲は 110 ～ 120 ミリ秒です。

最適な遅延 + バリアンスは 110 ミリ秒 + 10 ミリ秒です。

次の式を使用して、遅延バリアンスに最適なトンネルを選択します。

（best_latency、best_latency + Latency_variance）

### ジッターバリアンスの例

```
Device# show sdwan policy from-vsmart
from-vsmart sla-class video
```

```
latency                       100
jitter                        150
 fallback-best-tunnel         jitter

Tunnel T1: Latency: 90 msec, Loss: 0%, Jitter: 160 msec
Tunnel T2: Latency: 80 msec, Loss: 0%, Jitter: 200 msec
Tunnel T3: Latency: 70 msec, Loss: 0%, Jitter: 152 msec
```

ジッターバリアンスがない場合、最適なトンネルは T3 です。

ジッターバリアンスが 10 ミリ秒に設定されている場合、T1、T3 が最適なトンネルです。

範囲は 152 ～ 162 ミリ秒です。

最適なジッター + バリアンスは 152 ミリ秒 + 10 ミリ秒です。

次の式を使用して、ジッターバリアンスに最適なトンネルを選択します。

（best_jitter、best_jitter + Jitter_variance）

### 損失バリアンスの例

```
Device# show sdwan policy from-vsmart
from-vsmart sla-class video
latency                       100
jitter                        1
 fallback-best-tunnel         loss

Tunnel T1: Latency: 110 msec, Loss: 2%, Jitter: 200 msec
Tunnel T2: Latency: 115 msec, Loss: 3%, Jitter: 200 msec
Tunnel T3: Latency: 120 msec, Loss: 4%, Jitter: 200 msec
```

損失バリアンスがない場合、最適なトンネルは T1 です。

損失バリアンスが 1% に設定されている場合、T1 と T2 が最適なトンネルです。

範囲は 2% ～ 3% です。

最適な損失 + バリアンスは 2% です。

次の式を使用して、損失バリアンスに最適なトンネルを選択します。

（best_loss、best_loss + loss_variance）

# SLA クラスの構成

1. Cisco SD-WAN Manager メニューから、**[設定（Configuration）]** > > [ポリシー（Policies）] の順に選択します。[一元管理型ポリシー（Centralized Policy）] がデフォルトで選択され、表示されます。
2. [Add Policy] をクリックします。
3. 対象グループの作成ページの左側のペインで、[SLAクラス（SLA Class）] をクリックし、[新規 SLA クラスリスト（New SLA Class List）] をクリックします。
4. [SLA クラスリスト名（SLA Class List Name）] フィールドに、SLA クラスリストの名前を入力します。

5. SLA クラスのパラメータを定義します。
   1. [損失（Loss）] フィールドに、接続の最大パケット損失を 0 ～ 100% の値で入力します。
   2. [遅延（[Latency）] フィールドに、接続での最大パケット遅延を 1 ～ 1,000 ミリ秒の値で入力します。
   3. [ジッター（Jitter）] フィールドに、接続の最大ジッターを 1 ～ 1,000 ミリ秒の値で入力します。
   4. [アプリケーション プローブ クラス（App Probe Class）] ドロップダウンリストから必要なアプリケーション プローブ クラスを選択します。
6. （オプション）[フォールバックのベストトンネル（Fallback Best Tunnel）] チェックボックスをオンにして、ベストトンネルの基準を有効にします。

   このオプションフィールドは、Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a から利用できるので、SLA が満たされていない場合に、使用可能なカラーからベストパスまたはカラーを選択できます。このオプションを選択すると、ドロップダウンから必要な基準を選択できます。基準には、損失、遅延、およびジッターの値を 1 つ以上組み合わせます。
7. ドロップダウンリストから [基準（Criteria）] を選択します。使用可能な基準は次のとおりです。
   - なし
   - 遅延
   - 損失
   - Jitter
   - 遅延、損失
   - 遅延、ジッター
   - 損失、遅延
   - 損失、ジッター
   - ジッター、遅延
   - ジッター、損失
   - 遅延、損失、ジッター
   - 遅延、ジッター、損失
   - 損失、遅延、ジッター
   - 損失、ジッター、遅延
   - ジッター、遅延、損失

- ジッター、損失、遅延

8. （オプション）選択した基準の**損失バリアンス（%）**、**遅延バリアンス（ミリ秒）**、および**ジッターバリアンス（ミリ秒）**を入力します。

   詳細については、「最善のトンネルパスに向けたバリアンス設定」を参照してください。

9. [Add] をクリックします。

# トラフィックルールの設定

アプリケーション認識型ルーティングポリシーを設定するには、次の手順を実行します。

1. [アプリケーション認識型ルーティング（Application Aware Routing）] をクリックします。
2. [ポリシーの追加（Add Policy）] ドロップダウンリストから、[新規作成（Create New）] を選択します。
3. [シーケンスタイプ（Sequence Type）] をクリックします。**アプリケーションルート**のテキスト文字列を含むポリシーシーケンスが左側のペインに追加されます。
4. **アプリケーションルート**のテキスト文字列をダブルクリックし、ポリシーシーケンスの名前を入力します。ポリシーシーケンスは、コピー、削除、名前の変更ができます。入力した名前は、左側のペインと右側のペインの両方の [シーケンスタイプ（Sequence Type）] リストに表示されます。
5. 右側のペインで、[シーケンスルール（Sequence Rule）] をクリックします。[マッチ/アクション（Match/Actions）] ダイアログボックスを開くと、デフォルトで [マッチ（Match）] が選択されます。使用可能なポリシーマッチ条件は、ダイアログボックスの下に一覧表示されます。
6. [プロトコル（Protocol）] ドロップダウンリストで、次のいずれかのオプションを選択します。
   - **IPv4**
   - **IPv6**
   - **Both**

（注） 選択したプロトコルに応じて、[マッチ（Match）] または [アクション（Match）] の条件が異なる場合があります。

7. 1つ以上の [マッチ（Match）] 条件をクリックして選択します。次の表の説明に従って値を設定します。

表 *8 : Match Conditions*

| 一致条件 | 手順 |
|---|---|
| なし（すべてのパケットに一致） | マッチ条件を指定しないでください。 |
| **アプリケーション/アプリケーションファミリリスト（Application/Application Family List）** | [アプリケーション/アプリケーションファミリリスト（Application/Application Family List）] をクリックし、アプリケーションリストを選択します。<br><br>このマッチ条件は、Cisco IOS XE リリース17.9.1a および Cisco vManage リリース20.9.1 以降の IPv6 トラフィックで使用できます。 |
| **クラウド Saas アプリケーションリスト（Cloud Saas Application List）** | Cisco SD-WAN Manager では、Cisco Catalyst SD-WAN Cloud OnRamp for SaaS が各 Software as a Service（SaaS）アプリケーションのベストパスの選択を決定するために使用できるクラウドアプリケーションのリストが提供されます。<br><br>Cisco Catalyst SD-WAN Cloud OnRamp for SaaS の詳細については、『*Cisco Catalyst SD-WAN Cloud OnRamp Configuration Guide, Cisco IOS XE Release 17.x*』を参照してください。<br><br>（注） [プロトコル（Protocol）] オプションとして [IPv4] を指定すると、[クラウドSaaSアプリケーションリスト（Cloud Saas Application List）] がマッチ条件として表示されます。<br><br>ドロップダウンリストで、[SaaS アプリケーション（SaaS application）] を選択します。 |
| **DNS アプリケーションリスト（DNS Application List）** | ドロップダウンリストで、[アプリケーションファミリ（application family）]を選択します。<br><br>このマッチ条件は、Cisco IOS XE リリース17.9.1a および Cisco vManage リリース20.9.1 以降の IPv6 トラフィックで使用できます。 |
| **Destination Data Prefix** | 宛先プレフィックスのリストと照合するには、ドロップダウンリストから該当するリストを選択します。<br><br>個々の宛先プレフィックスと照合するには、[宛先（Destination）] ダイアログボックスにプレフィックスを入力します。 |

| | |
|---|---|
| **Destination Region**（宛先リージョン） | Cisco Catalyst SD-WAN マルチリージョン ファブリックを使用して、Cisco Catalyst SD-WAN ネットワークの [宛先リージョン（Destination Region）] を使用できます。<br>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ます。<br>• [プライマリ（Primary）] : 宛先サイトが送信元と同じプライマリリージョン（アクセスリージョン）内にある場合にトラフィックを照合します。<br>• [セカンダリ（Secondary）] : 宛先サイトが送信元と同じプライマリリージョン内にはないが、送信元と同じセカンダリリージョン内にある場合にトラフィックを照合します。このトラフィックは、セカンダリリージョンで説明されているように、ダイレクトトンネルを使用して宛先に到達できます。<br>• [その他（Other）] : 宛先サイトが送信元と同じプライマリリージョン内にもセカンダリリージョン内にもない場合にトラフィックを照合します。このトラフィックには、送信元から宛先へのマルチホップパスが必要です。<br>マルチリージョン ファブリックの設定方法の詳細については、『*Cisco Catalyst SD-WAN Multi-Region Fabric*（および *Hierarchical SD-WAN*）*Configuration Guide*』を参照してください。 |
| **宛先ポート** | ポート番号を入力します。単一のポート番号、ポート番号のリスト（スペースで区切られた番号）、またはポート番号の範囲（ハイフン [-] で区切られた 2 つの番号）を指定します。 |
| **トラフィック転送先**（**Traffic To**） | マルチリージョン ファブリックの境界ルータ用のデータポリシーまたはアプリケーション認識型ポリシーを作成する場合、一致基準を使用して、アクセスリージョン、コアリージョン、またはサービス VPN に流れるトラフィックを照合できます。 |
| **DNS**（スプリット DNS を有効にする場合） | DNS アプリケーションの DNS 要求を処理するには、ドロップダウンリストで [要求（Request）] を選択し、アプリケーションの DNS 応答を処理するには [応答（Response）] を選択します。 |
| [DSCP] | DSCP 値を 0 ～ 63 の数値で入力します。 |
| **PLP** | [低（Low）] または [高（High）] を選択します。PLP を [高（High）] に設定するには、[注釈超過（exceed remark）] オプションのあるポリサーを適用します。 |

| | |
|---|---|
| **Protocol** | インターネットプロトコル番号を 0 ～ 255 の数字で入力します。 |
| **ICMP Message** | **プロトコル（IPv4）**の場合、[マッチ条件（Match Conditions）] セクションの [プロトコル（Protocol）] フィールドの値を 1 にすると、[ICMPメッセージ（ICMP Message）] フィールドが表示され、データポリシーに適用する ICMP メッセージを選択できます。<br>**プロトコル（IPv6）**の場合、[マッチ条件（Match Conditions）] セクションの [プロトコル（Protocol）] フィールドの値を 58 にすると、[ICMPメッセージ（ICMP Message）] フィールドが表示され、データポリシーに適用する ICMP メッセージを選択できます。<br>（注） このフィールドは、Cisco IOS XE リリース 17.4.1 または Cisco SD-WAN リリース20.4.1、および Cisco vManage リリース 20.4.1 以降で使用できます。<br>[プロトコル（Protocol）] で [両方（Both）] を選択すると場合、[ICMPメッセージ（ICMP Message）] または [ICMPv6メッセージ（ICMPv6 Message）] フィールドが表示されます。 |
| **Source Data Prefix** | 送信元プレフィックスのリストと照合するには、ドロップダウンリストから該当するリストを選択します。<br>個々の送信元プレフィックスと照合するには、[送信元（Source）] フィールドにプレフィックスを入力します。 |
| **送信元ポート** | ポート番号を入力します。単一のポート番号、ポート番号のリスト（スペースで区切られた番号）、またはポート番号の範囲（ハイフン [-] で区切られた 2 つの番号）を指定します。 |

8. 条件が一致したデータトラフィックのアクションを選択するには、[アクション（Actions）] をクリックします。次の表の説明に従って値を設定します。

表 *9:* アクション

| アクション | 手順 |
|---|---|
| **バックアップSLAの優先カラー** | [バックアップSLAの優先カラー（Backup SLA Preferred Color）] のマッチ条件のポリシーアクションを設定します。SLA に一致するトンネルがない場合は、データトラフィックを特定のトンネルに転送します。そのトンネルインターフェイスが使用できる場合、データトラフィックは設定されたトンネルから送信されます。そのトンネルインターフェイスが使用できない場合、トラフィックは別の使用可能なトンネルに送信されます。1 つ以上の色を指定できます。バックアップ SLA の優先カラーは、厳密なマッチ条件ではなく、緩いマッチ条件です。<br>[バックアップSLAの優先カラー（Backup SLA Preferred Color）] をクリックします。<br>ドロップダウンリストで、1 つ以上の色を選択します。 |
| **カウンタ** | [カウンタ（Counter）] のマッチ条件のポリシーアクションを設定します。<br>[カウンタ（Counter）] をクリックします。<br>[カウンタ名（Counter Name）] フィールドに、パケットカウンタを保存するファイルの名前を入力します。 |
| **Log** | SLA クラスルールに一致するパケットのサンプルセットをシステムログ **(syslog)** ファイルに配置できます。パケットヘッダーが最初にログに記録される際、パケットヘッダーのログの他に、**syslog** メッセージが生成されます。その後もフローがアクティブである限り、 5 分ごとに生成されます。<br>ロギングを有効にするには、[ログ（Log）] をクリックします。 |

| アクション | 手順 |
|---|---|
| **SLAクラスリスト** | [SLAクラスリスト（SLA Class List）] のマッチ条件のポリシーアクションを設定します。SLA クラスの場合、条件が一致するすべてのデータトラフィックは、クラスで定義された SLA パラメータとパフォーマンスが一致するトンネルに送信されます。デバイスは、最初に SLA に一致するトンネルを介してトラフィックを送信しようとします。単一のトンネルが SLA に一致する場合、データトラフィックはそのトンネルを介して送信されます。2つ以上のトンネルが一致する場合、トラフィックはトンネル間で分散されます。SLA に一致するトンネルがない場合、データトラフィックは使用可能なトンネルの 1 つを介して送信されます。<br><br>[SLA Class List] をクリックします。<br><br>[SLAクラス（SLA Class）] ドロップダウンリストで、1 つ以上の SLA クラスを選択します。<br><br>必要に応じて、[優先カラー（Preferred Color）] ドロップダウンリストで、優先するデータプレーントンネルの色を選択します。トラフィックは、すべてのトンネル間でロードバランシングされます。SLA に一致するトンネルがない場合、データトラフィックは使用可能ないずれかのトンネルを介して送信されます。つまり、カラーの設定は厳密な一致ではなく緩い一致です。<br><br>[優先カラー（Preferred Color）]が選択されていない場合、必要に応じて、[優先カラーグループ（Preferred Color Group）] ドロップダウンリストから優先カラーグループを選択できます。優先するデータプレーントンネルの優先カラーグループを選択します。カラーまたはパスの設定に基づいて、最大 3 段階の優先順位を設定できます。このフィールドは、 Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1 以降で使用できます。<br><br>SLA クラスの厳密な照合を実行するには、[厳密/ドロップ（Strict/Drop）] をクリックします。SLA 基準を満たすデータプレーントンネルがない場合、トラフィックはドロップされます。<br><br>パケットドロップを回避するには、[ベストパスへのフォールバック（Fallback to best path）] をクリックして利用可能で最適なトンネルを選択します。<br><br>（注） [ベストパスへのフォールバック（Fallback to best path）] オプションは、Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a および Cisco SD-WAN リリース 20.5.1 以降で使用できます。<br><br>SLA クラスの定義中に、[フォールバックのベストトンネル（Fallback Best Tunnel）] オプションが有効になっている場合にのみ、[ベストパスへのフォールバック（Fallback to best path）] アクションを選択できます。[フォールバックのベストトンネル（Fallback Best Tunnel）] オプションが有効になっていない場合、次のエラーメッセージが Cisco SD-WAN Manager に表示されます。<br><br>`SLA Class selected, does not have Fallback Best Tunnel enabled.`<br>`Please change the SLA class or change to Strict/Drop.`<br><br>すべてのトンネル間でトラフィックの負荷を分散するには、[ロードバランス（Load Balance）] をクリックします。 |
| **クラウドSLA** | **クラウド SLA** により、トラフィックは Cisco Catalyst SD-WAN Cloud OnRamp for SaaS で最適なパス選択を使用できます。<br><br>[クラウドSLA（Cloud SLA）] をクリックします。 |

9. [Save Match and Actions] をクリックします。

10. 必要に応じて、追加のシーケンスルールを作成します。ルールをドラッグアンドドロップして再配置します。
11. [アプリケーション認識型ルーティングポリシーの保存（Save Application Aware Routing Policy）] をクリックします。
12. [次へ（Next）] をクリックして、ウィザードの [サイトとVPNにポリシーを適用（Apply Policies to Sites and VPNs）] に移動します。

# アプリケーション認識型ルーティングポリシーのデフォルトアクション

マッチ条件のいずれにもマッチしないパケットをどう処理するかは、ポリシーのデフォルトアクションで定義します。アプリケーション認識型ルーティングポリシーの場合、デフォルトアクションを設定しないと、すべてのデータパケットは通常のルーティング決定に基づいて受け入れられ、送信されます。SLA は考慮されません。

この動作を変更するには、**default-action sla-class** *sla-class-name* コマンドをポリシーに含め、**policy sla-class** コマンドで定義した SLA クラスの名前を指定します。

ポリシーのデフォルトアクションで SLA クラスを適用する場合、**strict** オプションは指定できません。

デフォルトアクションで SLA クラスを満たすデータプレーントンネルがない場合、Cisco IOS XE Catalyst SD-WAN デバイスは、等しいパス間でロードバランシングを実行することによって、使用可能なトンネルの 1 つを選択します。

データフローが AAR ポリシーとデータポリシーの両方にマッチする場合の予想される動作は以下になります。

1. データポリシーのローカル TLOC アクションが設定されている場合、**App-route preferred-color** および **backup-preferred-color** アクションが無視されます。
2. **sla-class** および **sla-strict** アクションは、アプリケーション ルーティング設定として維持されます。
3. データポリシーの TLOC が優先されます。

**local-tloc-list** アクションがあり、複数のオプションが含まれている場合は、SLA を満たすローカル TLOC を選択します。

- SLA を満たす **local-tloc** がない場合は、**local-tloc-list** を介したトラフィックに等コストマルチパス（ECMP）ルーティングを選択します。
- どの **local-tloc** も稼働していない場合は、稼働している TLOC を選択します。
- どの **local-tloc** も稼働しておらず、データポリシーが制限モードで設定されている場合は、トラフィックをドロップします。

# Cisco Catalyst SD-WAN Manager を介したアプリケーション プローブ クラスの設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。
2. [一元管理型ポリシー（Centralized Policy）] で、[ポリシーの追加（Add Policy）] をクリックします。[対象グループの作成（Create Groups of Interest）] ページが表示されます。
3. 左側のナビゲーションパネルからリストタイプ [アプリケーション プローブ クラス（App Probe Class）] を選択して、対象グループを作成します。
4. [新しいアプリケーションプローブクラス（New App Probe Class）] をクリックします。
5. [プローブクラス名（Prob Class Name）] フィールドにプローブクラス名を入力します。
6. [転送クラス（Forwarding Class）] ドロップダウンリストから必要な転送クラスを選択します。

   転送クラスがない場合は、[カスタム オプション（Custom Options）] メニューの [ローカライズ型ポリシーリスト（Localized Policy Lists）] の下にある [クラスマップ（Class Map）] リストページからクラスを作成します。

   転送クラスを作成するには、次の手順を実行します。

   1. [カスタムオプション（Custom Options）] ドロップダウンで、[ローカライズ型ポリシー（Localized Policy）] オプションから [リスト（Lists）] を選択します。
   2. [リストの定義（Define Lists）] ウィンドウで、左側のナビゲーションパネルからリストタイプとして [クラスマップ（Class Map）] を選択します。
   3. [新しいクラスリスト（New Class List）] をクリックして新しいリストを作成します。
   4. **クラス**を入力して、ドロップダウンリストから [キュー（Queue）] を選択します。
   5. [Save] をクリックします。

7. [エントリ（Entries）]ペインで、[カラー（Color）] ドロップダウンリストから適切なカラーを選択し、**DSCP** 値を入力します。

   **[+]** 記号をクリックして、必要に応じてエントリを追加します。
8. [Save] をクリックします。

## SLA クラスへのアプリケーション プローブ クラスの追加

1. 左側のペインから、[SLAクラス（SLA Class）] を選択します。
2. [新しいSLAクラスのリスト（New SLA Class List）] をクリックします。
3. [SLA クラスリスト名（SLA Class List Name）] フィールドに、SLA クラスリストの名前を入力します。

4. 必要な**損失（%）**、**遅延（ミリ秒）**、**ジッター（ミリ秒）**を入力します。
5. [アプリケーション プローブ クラス（App Probe Class）] ドロップダウンリストから必要なアプリケーション プローブ クラスを選択します。
6. [Add]をクリックします。

   損失、遅延、ジッター、アプリケーション プローブ クラスで作成された新しい SLA クラスがテーブルに追加されます。

## Cisco BFD テンプレートでのデフォルト DSCP の設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]**の順に選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Add template] をクリックします。
4. 左側のペインのデバイスリストから、デバイスを選択します。
5. 右側のペインで、[基本情報（Basic Information）] の下にリストされている BFD テンプレートを選択します。
6. それぞれのフィールドに [テンプレート名（Template Name）] と [説明（Description）] を入力します。
7. [基本設定（Basic Configuration）]ペインで、[乗数（Multiplier）] と [ポーリング間隔（ミリ秒）（Poll Interval (milliseconds)）] を入力します。
8. [BFDパケットのデフォルトDSCP値（Default DSCP value for BFD Packets）] フィールドに、必要なデバイス固有の値を入力するか、DSCP のデフォルト値を選択します。
9. （オプション）[色（Color）]ペインで、ドロップダウンリストから必要な色を選択します。
10. 必要な [Hello間隔（ミリ秒）（Hello Interval (milliseconds)）] と [乗数（Multiplier）]を入力します。
11. [パスMTUディスカバリ（Path MTU Discovery）] 値を選択します。
12. [TLOCカラーのBFDデフォルトDSCP値（BFD Default DSCP value for tloc color）] を入力します。
13. [Add]をクリックします。

    デフォルトの DSCP 値と色の値は、BFD テンプレートで設定されます。

# サイトと VPN へのポリシーの適用

ポリシー構成ウィザードの最後のウィンドウで、前の3つのウィンドウで作成したポリシーブロックを VPN およびオーバーレイネットワーク内のサイトに関連付けます。

オーバーレイネットワークのサイトと VPN にポリシーブロックを適用するには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。[一元管理型ポリシー（Centralized Policy）] がデフォルトで選択され、表示されます。
2. [Add Policy] をクリックします。[アプリケーションまたは対象グループの作成（Create Applications or Groups of Interest）] ページが表示されます。
3. **[Next]** をクリックします。[ネットワークトポロジ（Network Topology）] ウィンドウが開きます。[トポロジ（Topology）] バーで、[トポロジ（Topology）] がデフォルトで選択されています。
4. **[Next]** をクリックします。[トラフィックルールの設定（Configure Traffic Rules）] ウィンドウが開きます。[アプリケーション認識型ルーティング（Application-Aware Routing）] バーで、[アプリケーション認識型ルーティング（Application-Aware Routing）] がデフォルトで選択されています。
5. **[Next]** をクリックします。[サイトとVPNにポリシーを適用（Apply Policies to Sites and VPNs）] ウィンドウが開きます。
6. [ポリシー名（Policy Name）] フィールドに、ポリシーの名前を入力します。このフィールドは必須で、使用できるのは、英大文字と小文字、0 ～ 9 の数字、ハイフン（–）、下線（_）のみです。スペースやその他の文字を含めることはできません。
7. [ポリシーの説明（Policy Description）] フィールドに、ポリシーの説明を入力します。最大2048 文字を使用できます。このフィールドは必須であり、任意の文字とスペースを含めることができます。
8. [トポロジ（Topology）] バーから、ポリシーブロックのタイプを選択します。表には、そのタイプのポリシーブロック用に作成したポリシーが一覧表示されます。
9. [新しいサイトリストを追加（Add New Site List）] と [VPNリスト（VPN list）] をクリックします。1 つ以上のサイトリストを選択し、1 つ以上の VPN リストを選択します。[Add]をクリックします。
10. [プレビュー（Preview）]をクリックして、設定されたポリシーを表示します。ポリシーは CLI 形式で表示されます。
11. [Save Policy] をクリックします。**[設定（Configuration）]** > **[ポリシー（Policies）]** を選択すると、ポリシーテーブルに新しく作成されたポリシーが表示されます。

アプリケーション認識型ルートポリシーを有効にするには、次のようにオーバーレイネットワーク内のサイトのリストに適用します。

```
vSmart(config)# apply-policy site-list list-name app-route-policy policy-name
```

ポリシーを適用する場合は、（インバウンドまたはアウトバウンドのいずれであれ）方向は指定しません。アプリケーション認識型ルーティングポリシーは、Cisco IOS XE Catalyst SD-WAN デバイスのアウトバウンドトラフィックにのみ影響します。

**apply-policy** コマンドで適用するすべての **app-route-policy** ポリシーについて、すべてのサイトリストのサイト ID は一意である必要があります。つまり、サイトリストに重複するサイト ID が含まれていてはなりません。重複するサイト ID の例には、2 つのサイトリスト **site-list 1、site-id 1-100、**および **site-list 2 site-id 70-130** のサイト ID があります。ここでは、サイト 70 ～ 100 が両方のリストに含まれています。これらの 2 つのサイトリストを 2 つの異なる **app-route-policy** ポリシーに適用すると、Cisco Catalyst SD-WAN コントローラ で設定をコミットする試みが失敗します。

同じタイプの制限は、次のポリシーのタイプにも適用されます。

- 一元管理型制御ポリシー（**control-policy**）
- 一元管理型データポリシー（**data-policy**）
- cflowd フローモニタリングに使用される一元管理型データポリシー（**cflowd** アクションを含む **data-policy** および **cflowd-template** コマンドを含む **apply-policy**）

ただし、異なるタイプのポリシーに適用するサイトリストのサイト ID は重複させることができます。たとえば、**app-route-policy** ポリシーと **data-policy** ポリシーのサイトリストでは、サイト ID が重複している可能性があります。したがって、上記 2 つのサイトリストの例（**site-list 1、 site-id 1-100、** および **site-list 2 site-id 70-130**）では、1 つを制御ポリシーに、もう 1 つをデータポリシーに適用できます。

Cisco Catalyst SD-WAN コントローラ で **commit** コマンドを発行して設定を正常にアクティブ化するとすぐ、コントローラは指定されたサイトの Cisco IOS XE Catalyst SD-WAN デバイスにアプリケーション認識型ルーティングポリシーをプッシュします。

Cisco Catalyst SD-WAN コントローラ で設定されたポリシーを表示するには、コントローラで **show running-config** コマンドを使用します。

Cisco Catalyst SD-WAN コントローラ がデバイスにプッシュしたポリシーを表示するには、ルータで **show policy from-vsmart** コマンドを発行します。

デバイスで実行されているアプリケーション認識型アプリケーションのフロー情報を表示するには、ルータで **show app dpi flow** コマンドを発行します。

## アプリケーション認識型ルーティングポリシーを他のデータポリシーと組み合わせて適用する方法

Cisco IOS XE Catalyst SD-WAN デバイスにアプリケーション認識型ルーティングポリシーと他のポリシーを設定すると、そうしたポリシーはデータトラフィックに順次適用されます。

Cisco IOS XE Catalyst SD-WAN デバイスでは、次のタイプのデータポリシーを設定できます。

- 一元管理型データポリシー。Cisco Catalyst SD-WAN コントローラ でこのポリシーを設定すると、ポリシーはデバイスに渡されます。**policy data-policy configuration** コマンドを使

用して設定を定義したら、**apply-policy site-list data-policy** または **apply-policy site-list vpn-membership** コマンドを使用して適用します。

- ローカライズ型データポリシー。一般にアクセスリストと呼ばれます。デバイスでアクセスリストを設定するには、**policy access-list** 構成コマンドを使用します。VPN 内で **vpn interface access-list in** 構成コマンドを使用してインバウンドインターフェイスに適用するか、**vpn interface access-list out** コマンドを使用してアウトバウンドインターフェイスに適用します。
- アプリケーション認識型ルーティングポリシー。アプリケーション認識型ルーティングポリシーによって影響を受けるトラフィックは、 Cisco IOS XE Catalyst SD-WAN デバイスのサービス側（ローカル/LAN 側）からトンネル（WAN）側に流れるトラフィックのみです。アプリケーション認識型ルーティングポリシーを **policy app-route-policy** 構成コマンドを使用して Cisco Catalyst SD-WAN コントローラ で設定し、**apply-policy site-list app-route-policy** コマンドを使用して適用します。設定をコミットすると、ポリシーが該当するデバイスに渡されます。次に、デバイス上のマッチするデータトラフィックが、設定された SLA 条件に従って処理されます。このポリシーの結果としてドロップされないデータトラフィックは、データポリシーに渡されて評価を受けます。データトラフィックがマッチせず、デフォルトアクションが何も設定されていない場合は、SLA を考慮せずにそのデータトラフィックが送信されます。

オーバーレイネットワーク内の単一サイトに適用できるのは、データポリシー 1 つとアプリケーション認識型ルーティングポリシー1つのみです。設定で複数のサイトリストを定義して適用する場合は、単一のデータポリシーまたは単一のアプリケーション認識型ルーティングポリシーが複数のサイトに適用されないようにする必要があります。CLI はこうした状況になっていないかチェックせず、**validate** 構成コマンドは、同じタイプの複数のポリシーが単一のサイトに適用されているかどうかを検出しません。

ルータのサービス側からルータの WAN 側に流れるデータトラフィックの場合、ポリシーによるトラフィック評価は次の順序で行われます。

1. LANインターフェイスで入力アクセスリストを適用。このアクセスリストの結果としてドロップされないデータトラフィックは、アプリケーション認識型ルーティングポリシーに渡されて評価されます。
2. アプリケーション認識型ルーティングポリシーを適用。このポリシーの結果としてドロップされないデータトラフィックは、データポリシーに渡されて評価を受けます。データトラフィックがマッチせず、デフォルトアクションが何も設定されていない場合は、SLA を考慮せずにそのデータトラフィックが送信されます。
3. 一元管理型データポリシーを適用。入力アクセスリストの結果としてドロップされなかったデータトラフィックは、出力アクセスリストに渡されて評価されます。
4. WAN インターフェイスで出力アクセスリストを適用。出力アクセスリストの結果としてドロップされなかったデータトラフィックは、WANインターフェイスから送信されます。

WANからルータを経由してサービス側LANに流入するデータトラフィックの場合、ポリシーによるトラフィック評価は次の順序で行われます。

1. WAN インターフェイスで入力アクセスリストを適用。入力アクセスリストの結果としてドロップされなかったデータトラフィックは、データポリシーに渡されて評価されます。
2. データポリシーを適用。入力アクセスリストの結果としてドロップされなかったデータトラフィックは、出力アクセスリストに渡されて評価されます。
3. LANインターフェイスで出力アクセスリストを適用。出力アクセスリストの結果としてドロップされなかったデータトラフィックは、ローカルサイトの宛先に向けてLANインターフェイスから送信されます。

前述のように、アプリケーション認識型ルーティングポリシーは、Cisco IOS XE Catalyst SD-WANデバイスのサービス側（ローカル/LAN側）からトンネル（WAN）側に流れるトラフィックにのみ影響するため、WANから流入するデータトラフィックはアクセスリストとデータポリシーによってのみ処理されます。

（注） アプリケーション認識型ルーティングとデータポリシーの両方が設定されている場合、データポリシールールにDNSリダイレクト、ネクストホップ、セキュアインターネットゲートウェイ、NAT VPN、またはサービスなどのアクションが含まれていると、それらのルールにマッチするトラフィックはAARポリシーをスキップします。たとえそのトラフィックが、AARポリシーで定義されたルールにマッチしていたとしてもです。 データポリシーアクションは、AARルールをオーバーライドします。

# アプリケーション認識型ルーティングポリシーのアクティブ化

ポリシーをアクティブ化するには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** の順に選択します。[一元管理型ポリシー（Centralized Policy）] がデフォルトで選択され、表示されます。
2. 目的のポリシーについて、[...] をクリックし、[アクティブ化（Activate）] を選択します。[ポリシーのアクティブ化（Activate Policy）] ポップアップが開きます。ポリシーが適用される到達可能な Cisco SD-WAN コントローラ の IP アドレスが一覧表示されます。
3. [Activate] をクリックします。

アプリケーション認識型ルーティングポリシーをアクティブ化すると、接続されているすべての Cisco SD-WAN コントローラ にポリシーが送信されます。

# データプレーントンネルのパフォーマンスのモニター

Bidirectional Forwarding Detection（BFD）プロトコルは、Cisco IOS XE Catalyst SD-WAN デバイス間のすべてのデータプレーントンネルで実行され、トンネルの稼働状態、ネットワークおよびパスの特性をモニタリングします。アプリケーション認識型ルーティングは、BFDによって収集された情報を使用して、トンネルの伝送パフォーマンスを決定します。パフォーマンスは、トンネル上のパケット遅延とパケット損失の観点から報告されます。

BFD は定期的に Hello パケットを送信し、データプレーントンネルの稼働状態をテストして、トンネルの障害をチェックします。これらの Hello パケットは、トンネル上のパケット損失とパケット遅延の測定値を提供します。Cisco IOS XE Catalyst SD-WAN デバイスは、時間のスライディングウィンドウにわたってパケット損失と遅延の統計情報を記録します。BFDは、直近の6つのスライディングウィンドウの統計を追跡し、各統計セットを別々のバケットに配置します。デバイスにアプリケーション認識型ルーティングポリシーを設定する場合、ルータはこれらの統計情報を使用して、データプレーントンネルのパフォーマンスがポリシーの SLA の要件に一致するかどうかを判断します。

スライディングウィンドウのサイズは次のパラメータで決定します。

| パラメータ | デフォルト | コンフィギュレーション コマンド | 範囲 |
|---|---|---|---|
| BFD Hello パケット間隔 | 1 秒 | **bfd color** *color* **hello-interval** *seconds* | 1 ～ 65535 秒 |
| アプリケーション認識型ルーティングのポーリング間隔 | 10 分（600,000 ミリ秒） | **bfd app-route poll-interval** *milliseconds* | 1 ～ 4,294,967（$2^{32}-1$）ミリ秒 |
| アプリケーション認識型ルーティングの乗数 | 6 | **bfd app-route multiplier** *number* | 1 ～ 6 |

これらのパラメータのデフォルト値を使用して、アプリケーション認識型ルーティングの動作について説明します。

- スライディングウィンドウの期間ごとに、アプリケーション認識型ルーティングは 600個の BFD Hello パケットを確認します（BFD Hello 間隔 x ポーリング間隔：1 秒 x 600 秒 = 600 Hello パケット）。これらのパケットは、データプレーントンネルでのパケット損失と遅延の測定値を提供します。
- アプリケーション認識型ルーティングでは、統計情報が 1 時間保持されます（ポーリング間隔 x 乗数：10 分 x 6 = 60 分）。
- 統計情報は、0 ～ 5 の番号でインデックスが付けられた 6 つのバケットにそれぞれ配置されます。バケット 0 には最新の統計情報が、バケット 5 には最も古い統計情報が配置されます。10 分ごとに、最新の統計情報がバケット 0 に配置されます。またバケット 5 の統計情報が破棄され、残りの統計情報が次のバケットに移動します。
- 60 分ごと（1 時間ごと）に、アプリケーション認識型ルーティングが損失と遅延の統計情報に基づいて動作します。すべてのスライディングウィンドウのすべてのバケットの損失および遅延の平均を計算し、この値をトンネルの指定された SLA と比較します。計算された値が SLA を満たす場合、アプリケーション認識型ルーティングは何も行いません。値が SLA を満たさない場合、アプリケーション認識型ルーティングは新しいトンネルを計算します。
- アプリケーション認識型ルーティングは、6 つのバケットすべての値を使用して、データトンネルの平均損失と遅延を計算します。これは、乗数が 6 であるためです。アプリケーション認識は常に 6 つのデータバケットを保持しますが、損失と遅延を計算するために実

際に使用する数は、乗数によって決まります。たとえば、乗数が 3 の場合、バケット 0、1、2 が使用されます。

これらのデフォルト値は1時間ごとにしかアクションを実行しないため、安定したネットワークに適しています。ネットワーク障害をより迅速にキャプチャして、アプリケーション認識型ルーティングが新しいトンネルをより頻繁に計算できるようにするには、これら 3 つのパラメータの値を調整します。たとえば、ポーリング間隔だけを1分（60,000 ミリ秒）に変更した場合、アプリケーション認識型ルーティングはトンネルのパフォーマンス特性を毎分確認しますが、損失と遅延の計算は 60 個の Hello パケットのみに基づいて実行されます。アプリケーション認識型ルーティングが新しいトンネルが必要であると計算した場合、トンネルをリセットするのに 1 分以上かかることがあります。

各データプレーントンネルの統計情報を表示するには、**show sdwan app-route stats** コマンドを使用します。

```
デバイス# show sdwan app-route stats

                                                                                                                TX    RX
                                    SRC    DST    MEAN  MEAN            TOTAL          AVERAGE  AVERAGE  DATA  DATA
SRC IP       DST IP          PROTO  PORT   PORT   LOSS  LATENCY  INDEX  PACKETS  LOSS  LATENCY  JITTER   PKTS  PKTS
-------------------------------------------------------------------------------------------------------------------
192.0.2.1  192.0.2.254  ipsec  12346  12346  0     22       0      596      0     21       2        0     0
                                                          1      596      0     21       2        0     0
                                                          2      596      0     21       2        0     0
                                                          3      597      1     21       2        0     0
                                                          4      596      0     21       2        0     0
                                                          5      596      0     29       4        0     0
192.0.2.1  192.0.2.254  ipsec  12346  12346  0     24       0      596      0     24       3        0     0
                                                          1      596      0     25       3        0     0
                                                          2      596      0     25       3        0     0
                                                          3      596      0     24       3        0     0
                                                          4      596      0     24       3        0     0
                                                          5      596      0     24       3        0     0
192.0.2.1  192.0.2.254  ipsec  12346  34083     0   21      0      596      0     21       3        0     0
                                                          1      596      0     22       3        0     0
                                                          2      596      0     22       3        0     0
                                                          3      596      0     21       3        0     0
                                                          4      596      0     21       3        0     0
                                                          5      596      0     21       3        0     0

192.0.2.1  192.0.2.254  ipsec  12346  36464   0     23       0      596      0     23       3        0     0
                                                          1      596      0     23       3        0     0
                                                          2      596      0     24       3        0     0
                                                          3      596      0     23       4        0     0
                                                          4      596      0     23       4        0     0
                                                          5      596      0     23       4        0     0
...
```

デバイスがサービス側インターフェイスに送信する IP パケットのネクストホップ情報を表示するには、**show policy service-path** コマンドを使用します。ルータが WAN トランスポート トンネルインターフェイスに送信するパケットの類似情報を表示するには、**show policy tunnel-path** コマンドを使用します。

## Cisco IOS XE Catalyst SD-WAN デバイスでのアプリケーションの可視性の有効化

LAN 内のすべての VPN で実行されているすべてのアプリケーションをモニタリングできるように、アプリケーション認識型ルーティングポリシーを設定せずに、Cisco IOS XE Catalyst SD-WANデバイスでアプリケーションの可視性を直接有効にすることができます。これを行うには、ルータでアプリケーションの可視性を設定します。

```
vEdge(config)#  policy app-visibility
```

アプリケーションをモニターするには、デバイスで **show app dpi applications** および **show app dpi supported-applications** コマンドを使用します。

# CLIを使用したアプリケーション認識型ルーティングの設定

次に、アプリケーション認識型ルーティングポリシーの設定手順の概要を示します。

1. アプリケーション認識型ルーティングポリシーを適用するオーバーレイ ネットワーク サイトのリストを作成します（**apply-policy** コマンドを使用）。

   ```
   vSmart(config)# policy
   vSmart(config-policy)# lists site-list list-name
   vSmart(config-site-list)# site-id site-id
   ```

   リストには、必要な数のサイトIDを含めることができます。サイトIDごとに1つの**site-id** コマンドを含めます。連続するサイトIDの場合は、番号をダッシュ（-）で区切って範囲指定できます。必要に応じて、さらにサイトリストを作成します。

2. 次のように、マッチするアプリケーションのデータトラフィックに適用するSLAクラスとトラフィック特性を作成します。

   ```
   vSmart(config)# policy sla-class sla-class-name
   vSmart(config-sla-class)# jitter milliseconds
   vSmart(config-sla-class)# latency milliseconds
   vSmart(config-sla-class)# loss percentage
   vSmart(config-sla-class)# app-probe-class app-probe-class
   vSmart(config-sla-class)# fallback-best-tunnelcriterialatencylossjitter
   ```

3. （ポリシー定義の**match**セクションで）対象のアプリケーションのトラフィックの特定に使用するアプリケーション、IP プレフィックス、およびVPNのリストを作成します。

   ```
   vSmart(config)# policy lists
   vSmart(config-lists)# app-list list-name
   vSmart(config-app-list)# (app application-name | app-family family-name)

   vSmart(config-lists)# prefix-list list-name
   vSmart(config-prefix-list)# ip-prefix prefix/length

   vSmart(config-lists)# vpn-list  list-name
   vSmart(config-vpn-list)# vpn vpn-id
   ```

4. 次のように、アプリケーション認識型ルーティングポリシーのインスタンスを作成し、それをVPNのリストに関連付けます。

   ```
   vSmart(config)# policy app-route-policy policy-name
   vSmart(config-app-route-policy)# vpn-list list-name
   ```

5. ポリシー内で、マッチ/アクションペアの番号付きシーケンスを1つ以上作成します。ここで、マッチパラメータは対象のデータトラフィックとアプリケーションを定義し、アクションパラメータは一致が発生した場合に適用するSLAクラスを指定します。

   1. シーケンスを作成します。

```
vSmart(config-app-route-policy)# sequence number
```

2. データパケットのマッチパラメータを定義します。

```
vSmart(config-sequence)# match  parameters
```

3. 次のように、マッチが発生したときに実行するアクションを定義します。

```
vSmart(config-sequence)# action sla-class sla-class-name [strict]
vSmart(config-sequence)# action sla-class sla-class-name [strict] preferred-color
 colors
vSmart(config-sequence)# <userinput>action backup-sla-preferred-color</userinput>
 <varname>colors</varname>
```

最初の 2 つの**アクション**オプションは、一致するデータトラフィックを、指定された SLA クラスの SLA 特性を満たすトンネルインターフェイスに転送します。

- **sla-class** *sla-class-name*：追加パラメータなしで SLA クラスを指定すると、1 つのトンネルインターフェイスが使用可能である限り、SLA に一致するデータトラフィックが転送されます。ソフトウェアは、最初にSLAに一致するトンネルを介してトラフィックを送信しようとします。単一のトンネルが SLA に一致する場合、データトラフィックはそのトンネルを介して送信されます。2 つ以上のトンネルが一致する場合、トラフィックはトンネル間で分散されます。SLA に一致するトンネルがない場合、データトラフィックは使用可能なトンネルの 1 つを介して送信されます。

- **sla-class** *sla-class-name* **preferred-color** *color*：データトラフィックが SLA クラスと一致する場合に使用する特定のトンネルを設定するには、**preferred-color** オプションを含めて、優先トンネルの色を指定します。複数のトンネルが SLA に一致する場合、トラフィックは優先トンネルに送信されます。優先カラーのトンネルが使用できない場合、トラフィックは SLA クラスに一致するトンネルを介して送信されます。SLA に一致するトンネルがない場合、データトラフィックは使用可能ないずれかのトンネルを介して送信されます。この意味で、色設定は厳密な一致ではなく、緩い一致であると見なされます。これは、データトラフィックは優先色のトンネルが使用可能かどうかに関係なく、常に転送されるためです。

- **sla-class** *sla-class-name* **preferred-color** *colors*：データトラフィックが SLA クラスと一致する場合に使用する複数のトンネルを設定するには、**preferred-color** オプションを含めて、2 つ以上のトンネルの色を指定します。トラフィックは、すべてのトンネル間でロードバランシングされます。

SLA に一致するトンネルがない場合、データトラフィックは使用可能ないずれかのトンネルを介して送信されます。この意味で、色設定は厳密な一致ではなく、緩い一致であると見なされます。これは、データトラフィックは優先色のトンネルが使用可能かどうかに関係なく、常に転送されるためです。SLA に一致するトンネルがない場合は、データトラフィックの処理方法を選択できます。

- **strict**：データトラフィックをドロップします。

- **backup-sla-preferred-color** *colors*：データトラフィックを特定のトンネルに転送します。トンネルインターフェイスが使用可能な場合、データトラフィックは設定されたトンネルから送信されます。そのトンネルが使用できない場合、トラフィッ

クは使用可能な別のトンネルに送信されます。1 つ以上の色を指定できます。**preferred-color** オプションと同様に、バックアップ SLA の優先色は緩い一致です。単一の**アクション**設定では、**strict** オプションと **backup-sla-preferred-color** オプションの両方を含めることはできません。

4. ポリシーに一致するパケットまたはバイトをカウントします。

   ```
   vSmart(config-sequence)# action count counter-name
   ```

5. SLA クラスルールに一致するパケットのサンプルセットを syslog ファイルに配置します。

   ```
   vSmart(config-sequence)# action log
   ```

6. ポリシー内のマッチ/アクションペアは、シーケンス番号に基づいて、番号の小さいものから順に評価されます。マッチした場合は、対応するアクションが実行され、ポリシーの評価が停止します。

6. パケットがいずれかのシーケンスの条件のどれにもマッチしない場合は、デフォルトのアクションが実行されます。アプリケーション認識型ルーティングポリシーの場合、デフォルトのアクションでは、マッチしないトラフィックが受け入れられ、SLA を考慮せずにそのトラフィックがそのまま転送されます。次のようにデフォルトのアクションを設定しておくことで、SLA パラメータをマッチしないパケットに適用することができます。

   ```
   vSmart(config-policy-name)# default-action sla-class sla-class-name
   ```

7. ポリシーを site-list に適用します。

   ```
   vSmart(config)# apply-policy site-list list-name app-route-policy policy-name
   ```

# CLI を使用したアプリケーション プローブ クラスの設定

次の例に示すように、app-probe-class と real-time-video を設定したら、それらを SLA クラスにマッピングします。

```
Device(config)# app-probe-class real-time-video
Device(config)# forwarding-class videofc
Device(config)# color mpls dscp 34
Device(config)# color biz-internet dscp 40
Device(config)# color lte dscp 0


Device(config)# sla-class streamsla
Device(config)# latency 20
Device(config)# loss 10
Device(config)# app-probe-class real-time-video
```

次に示すように、BFD テンプレートを使用して DSCP のデフォルト値を設定します。

```
Device(config)# bfd default-dscp 50
Device(config)# bfd color mpls 15
```

# アプリケーション認識型ルーティングポリシーの設定例

このトピックでは、アプリケーション認識型ルーティングポリシーを設定する簡単な例を示します。この例では、ICMP トラフィックに適用するポリシーを定義し、リンクが使用可能な場合は遅延が 50 ミリ秒以下のリンクにトラフィックを誘導します。

Cisco Catalyst SD-WAN コントローラ にアプリケーション認識型ルーティングポリシーを設定します。設定は以下のハイレベルコンポーネントで構成されます。

- アプリケーションの定義
- アプリケーション プローブ クラスの定義（オプション）
- SLA パラメータの定義
- サイト、プレフィックス、VPN の定義
- アプリケーション認識型ルーティングポリシー自体
- ポリシーが適用されるオーバーレイ ネットワーク サイトの指定

これらのコンポーネントを設定する順序は、CLI の観点からは重要ではありません。ただし、アーキテクチャ設計の観点から見た論理的な順序は、まずアプリケーション認識型ルーティングポリシー自体で呼び出される、またはオーバーレイネットワーク内のさまざまなサイトにポリシーを適用するために使用されるすべてのパラメータを定義することです。次に、アプリケーション認識型ルーティングポリシー自体と、ポリシーを適用するネットワーク サイトを指定します。

Cisco Catalyst SD-WAN コントローラ で、このアプリケーション認識型ルーティングポリシーを設定する手順を次に示します。

1. 一致する ICMP トラフィックに適用する SLA パラメータを定義します。この例では、遅延が 50 ミリ秒以下のリンクに ICMP トラフィックを転送します。

```
vSmart# config
vSmart(config)# policy sla-class test_sla_class latency 50
vSmart(config-sla-class-test_sla_class)#
```

2. アプリケーション認識型ルーティングポリシーを適用するサイトと VPN リストを定義します。

```
vSmart(config-sla-class-test_sla_class)# exit
vSmart(config-sla-class-test_sla_class)# lists vpn-list vpn_1_list vpn 1
vSmart(config-vpn-list-vpn_1_list)# exit
vSmart(config-lists)# site-list site_500 site-id 500
vSmart(config-site-list-site_500)#
```

3. アプリケーション認識型ルーティングポリシーの設定この例では、2 つの異なる方法でアプリケーションにポリシーを適用することに注意してください。シーケンス 1、2、3 では、プロトコル番号を指定しています（プロトコル 1 は ICMP、プロトコル 6 は TCP、プロトコル 17 は UDP）。

```
vSmart(config-site-list-site_500)# exit
vSmart(config-lists)# exit
```

```
vSmart(config-policy)# app-route-policy test_app_route_policy
vSmart(config-app-route-policy-test_app_route_policy)# vpn-list vpn_1_list
vSmart(config-vpn-list-vpn_1_list)# sequence 1 match protocol 6
vSmart(config-match)# exit
vSmart(config-sequence-1)# action sla-class test_sla_class strict
vSmart(config-sequence-1)# exit
vSmart(config-vpn-list-vpn_1_list)# sequence 2 match protocol 17
vSmart(config-match)# exit
vSmart(config-sequence-2)# action sla-class test_sla_class
vSmart(config-sequence-2)# exit
vSmart(config-vpn-list-vpn_1_list)# sequence 3 match protocol 1
vSmart(config-match)# exit
vSmart(config-sequence-3)# action sla-class test_sla_class strict
vSmart(config-sequence-3)# exit
vSmart(config-sequence-4)#
```

4. Cisco IOS XE Catalyst SD-WAN オーバーレイネットワーク内の目的のサイトにポリシーを適用します。

```
vSmart(config-sequence-4)# top
vSmart(config)# apply-policy site-list site_500 app-route-policy test_app_route_policy
```

5. 設定の変更を表示します。

```
vSmart(config-site-list-site_500)# top
vSmart(config)# show config
```

6. 設定にエラーがないことを確認します。

```
vSmart(config)# validate
Validation complete
```

7. 設定を有効にします。

```
vSmart(config)# commit
Commit complete.
```

8. 設定モードを終了します。

```
vSmart(config)# exit
vSmart#
```

設定をすべてまとめると、次のようになります。

```
vSmart# show running-config policy
policy
 sla-class test_sla_class
  latency 50
 !
 app-route-policy test_app_route_policy
  vpn-list vpn_1_list
   sequence 1
    match
     protocol 6
    !
    action sla-class test_sla_class strict
   !
   sequence 2
    match
     protocol 17
    !
    action sla-class test_sla_class
   !
   sequence 3
```

```
    match
     protocol 1
    !
    action sla-class test_sla_class strict
   !
  !
 !
 lists
  vpn-list vpn_1_list
   vpn 1
  !
  site-list site_500
   site-id 500
  !
  site-list site_600
   site-id 600
  !
 !
!
apply-policy
 site-list site_500
  app-route-policy test_app_route_policy
 !
!
```

マルチキャストプロトコルを定義する例を次に示します。

```
policy
!
 sla-class SLA_BEST_EFFORT
  jitter 900
 !
 sla-class SLA_BUSINESS_CRITICAL
  loss    1
  latency 250
  jitter  300
 !
 sla-class SLA_BUSINESS_DATA
  loss    3
  latency 400
  jitter  500
 !
 sla-class SLA_REALTIME
  loss    2
  latency 300
  jitter  60
 !
 app-route-policy policy_multicast
  vpn-list multicast-vpn-list
   sequence 10
    match
     source-ip      10.0.0.0/8
     destination-ip 10.255.255.254/8
    !
    action
     count mc-counter-10
     sla-class SLA_BUSINESS_CRITICAL
    !
   !
   sequence 15
    match
     source-ip      172.16.0.0/12
     destination-ip 172.31.255.254/12
    !
```

```
     action
      count mc-counter-15
      sla-class SLA_BEST_EFFORT
     !
    !
    sequence 20
     match
      destination-ip 192.168.0.1
     !
     action
      count mc-counter-20
      sla-class SLA_BUSINESS_CRITICAL
     !
    !
    sequence 25
     match
      protocol       17
     !
     action
      count mc-counter-25
      sla-class SLA_REALTIME
     !
    !
    sequence 30
     match
      source-ip      192.168.0.0/16
      destination-ip 192.168.255.254
      protocol       17
     !
     action
      count mc-counter-30
      sla-class SLA_BUSINESS_DATA preferred-color lte
     !
    !
    default-action sla-class SLA_BEST_EFFORT
    !
    sequence 35
     match
      source-ip      10.0.0.0/8
      destination-ip 10.255.255.254/8
      protocol       17
     !
     action
      count mc-counter-35
      sla-class SLA_BUSINESS_DATA preferred-color lte
      backup-sla-preferred-color 3g
     !
    !
  lists
   vpn-list multicast-vpn-list
    vpn 1
    vpn 60
    vpn 4001-4010
    vpn 65501-65510
   !
   site-list multicast-site-list
    site-id 1100
    site-id 500
    site-id 600
   !
  !
!
apply-policy
 site-list multicast-site-list
```

```
  app-route-policy policy_multicast
 !
!
```

### ランク付けカラーの優先順位の例

```
app-route-policy SAMPLE _AAR
 vpn-list ONE
  sequence 10
   match
    dscp 46
   !
   action
    sla VOICE_SLA strict preferred-color-group GROUP2_COLORS
   !
  !
  sequence 20
   match
    dscp 34
   !
   action
    sla VOICE_SLA preferred-color-group GROUP1_COLORS
   !
  !
  sequence 30
   match
    dscp 28
   !
   action
    sla VOICE_SLA preferred-color-group GROUP3_COLORS
   !
  !
 !
policy lists
  preferred-color-group GROUP1_COLORS
   primary-preference
    color-preference biz-internet
    path-preference direct-tunnel
   !
   secondary-preference
    color-preference mpls
    path-preference multi-hop-path
   !
   tertiary-preference
    color-preference lte
   !
  !
  preferred-color-group GROUP2_COLORS
   primary-preference
    color-preference mpls
   !
   secondary-preference
    color-preference biz-internet
   !
  !
  preferred-color-group GROUP3_COLORS
   primary-preference
    color-preference mpls biz-internet lte
   !
```

（注） Cisco SD-WAN Manager で [マルチリージョン ファブリック（Multi-Region Fabric）] オプションを有効にしている場合にのみ、path-preference オプションを設定できます。

### IPv6 アプリケーションに対する AAR ポリシーの例

```
policy
  sla-class Default
   jitter 100
   latency 300
   loss 25
  !
 app-route-policy _VPN1_AAR-Policy-for-IPv6-Traffic
  vpn-list VPN1
    sequence 1
     match
      app-list Msft-0365
     !
     action
      sla-class Default  preferred-color public-internet
     !
    !
 !
 lists
  app-list Msft-0365
   app ms-office-web-apps
  !
  site-list SITE-100
   site-id 100
  !
  vpn-list VPN1
   vpn 1
  !
 !
!
apply-policy
 site-list SITE-100
  app-route-policy _VPN1_AAR-Policy-for-IPv6-Traffic
 !
!
```

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。