VPN のシミュレーション

Cisco Crosswork Planning の仮想プライベートネットワーク（VPN）モデルは、ネットワークモデル内の仮想サブネットワークを表します。Cisco Crosswork Planning 内で VPN を表示およびシミュレートすると、多くのネットワークタスクに役立ち、次のような質問に答えることができます。

- ネットワーク上にある VPN はどれか。それらは、どこでどのように設定されているか。
- 輻輳したインターフェイスを使用している VPN はどれか。
- 特定のリストに含まれる障害シナリオのいずれかで輻輳が発生する VPN はどれか。
- VPN のワーストケースの輻輳または遅延を引き起こす障害シナリオはどれか。

VPN にはさまざまな種類があります。たとえば、レイヤ 2（L2）VPN とレイヤ 3（L3）VPN があり、それぞれに含まれるカテゴリは異なっており、ベンダー固有の VPN 実装があります。各 VPN タイプには、固有の設定と用語があります。Cisco Crosswork Planning の VPN モデルは、ルートターゲット接続またはフルメッシュ接続のいずれかに基づいて、これらの VPN タイプを多数サポートしています。

ここでは、次の内容について説明します。

- VPN モデル （2 ページ）
- VPN （3 ページ）
- VPN ノード （6 ページ）
- レイヤ 3 VPN の例 （10 ページ）
- VPN シミュレーション分析 （13 ページ）

VPN モデル

VPN オブジェクト

オブジェクト	説明	例
VPN	相互にデータを交換できる一連の VPN ノード。	• レイヤ 2 VPN：VPN は、仮想スイッチインターフェイス（VSI）を含む個々の VPLS を表します。 • レイヤ 3 VPN：VPN は、相互にトラフィックを転送する一連の VPN ノードに関連付けられた一連の VRF を表します。多くの場合、この一連の VRF は、単一の顧客またはサービスを表します。
VPN ノード	VPN 内の接続ポイント。これらは標準ノードに存在し、各ノードには複数の VPN ノードを含めることができます。1 つの VPN ノードは 1 つの VPN にのみ配置できます。	• レイヤ 2 VPN：VPN ノードは、各ルータで設定された VSI を表します。 • レイヤ 3 VPN：VPN ノードは、各ルータで設定された VRF インスタンスを表します。

VPN のトポロジと接続

Cisco Crosswork Planning の VPN トポロジルート接続は、ルートターゲット（RT）を介して、または VPN ノードのフルメッシュを介して確立されます。[接続（Connectivity）] プロパティは、[VPNの追加/編集（Add/Edit VPN）] ウィンドウで設定されます。

VPN のトポロジと接続を把握することで、Cisco Crosswork Planning は、特定の VPN のトラフィックを伝送する VPN ノード間のデマンドを計算でき、そのため、その VPN のトラフィックを伝送するインターフェイスを計算できます。その後、Cisco Crosswork Planning は、特定の障害および輻輳シナリオに対する VPN の脆弱性を計算できます。

次の条件が満たされている場合、デマンドは VPN に関連付けられます。つまり、その VPN のトラフィックを伝送します。

- 2 つの VPN ノードが同じ VPN 内にある。
- デマンドが VPN と同じサービスクラスにある。
- RT 接続を持つ VPN の場合のみ、1 つの VPN ノードの [RTエクスポート（RT export）] プロパティが別の VPN ノードの [RTインポート（RT import）] プロパティと一致する必要がある。

デマンドが VPN に関連付けられると、この設定により、同じ LAN 上にあるかのようにトラフィックを交換する関連付けられたアクセス回線がシミュレートされます。

VPN に関連付けられたデマンドには、その VPN 向けの他のトラフィックを追加で含めることができることに注意してください。

接続	説明
フルメッシュ	フルメッシュ接続は、VPN 内の VPN ノード間の接続の完全なメッシュであるため、すべてが相互に通信できます。この接続は、すべての VSI が共通の AGI に基づいて相互に識別される VPLS において一般的です。
ルートターゲット（RT）	ルートターゲットは、レイヤ 3 VPN で使用されるより複雑な接続（ハブアンドスポーク ネットワークなど）をモデル化します。ここで、VRF は、各 VPN ノードに設定された [RTエクスポート（RT export）] プロパティと [RTインポート（RT import）] プロパティの照合に基づいて、相互にデータを交換します。 インポート/エクスポートペアがあっても、双方向通信は作成されません。むしろ、トラフィックフローは、ルーティングされるアドバタイズメントとは逆の方向になります。たとえば、ノード A の RT インポートがノード B の RT エクスポートと一致する場合、ノード A から B へのトラフィックフローが可能になります。 ノード B からノード A へのトラフィックフローを実現するには、ノード B に、ノード A の RT エクスポートと一致する RT インポートが必要です。一致するインポートされる RT とエクスポートされる RT のこの組み合わせにより、どの VPN ノードがデータを交換できるかが定義されます。VPN 名により VPN 自体が識別されます。

VPN

各 VPN は、その VPN 内でデータを交換できる一連の VPN ノードで構成されます。VPN には、VPN を一意に識別し、VPN 内のトラフィックのルーティング方法を定義する次のキープロパティがあります。

- [名前（Name）]：VPN の一意の名前。

- [タイプ（Type）]：VPN のタイプ。オプション（VPWS、VPLS、または L3VPN）から選択します。
- [接続（Connectivity）]：Cisco Crosswork Planning が VPN の接続と関連するデマンドを計算する方法を決定します。
  - [フルメッシュ（Full Mesh）]：VPN 内のすべてのノード間に接続が存在します。Cisco Crosswork Planning は、VPN ノードの [RTインポート（RT Import）] プロパティと [RTエクスポート（RT Export）] プロパティを無視します。
  - [RT]：接続は、VPN ノードの [RTインポート（RT Import）] プロパティと [RTエクスポート（RT Export）] プロパティに基づきます。
- [サービスクラス（Service class）]：この VPN に関連付けられたサービスクラス。

VPN が作成されると、VPN ノードの [VPN] ドロップダウンリストに表示されます。

VPN の作成

新しい VPN を作成し、後で VPN ノードを追加することができます（VPN への VPN ノードの追加 （8 ページ）を参照）。

新しい VPN の作成

新しい VPN を作成するには、次の手順を実行します。

手順

ステップ 1 プランファイルを開きます（プランファイルを開くを参照）。[ネットワーク設計（Network Design）] ページに表示されます。

ステップ 2 ツールバーから、**[アクション（Actions）]** > **[挿入（Insert）]** > **[VPN（VPNs）]** > **[VPN]** の順に選択します。

または

右側にある [ネットワークサマリー（Network Summary）] パネルで、[VPN（VPNs）] タブの  をクリックします。

[VPN（VPNs）] タブは、[詳細（More）] タブの下にあります。表示されていない場合は、[テーブルの表示/非表示（Show/hide tables）] アイコン（  ）をクリックし、[VPN（VPNs）] チェックボックスをオンにします。

ステップ 3 [Name] フィールドに、VPN の一意の名前を入力します。

ステップ 4 [タイプ（Type）] ドロップダウンリストから、VPN タイプを選択します。オプションは、[L3VPN]、[VPLS]、および [VPWS] です。

ステップ 5 接続タイプとして [RT] または [フルメッシュ（Full Mesh）] を選択します。

ステップ 6 VPN のサービスクラスを選択します。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 （オプション）新しく作成した VPN に VPN ノードを追加します。詳細については、VPN への VPN ノードの追加 （8 ページ） を参照してください。

[VPN（VPNs）] テーブル

[VPN（VPNs）] テーブルには、VPN のプロパティ、関連するサービスクラス、トラフィック、およびその VPN に含まれる VPN ノードの数が表示されます（表 1 : 通常動作時の [VPN（VPNs）] テーブルの列 （5 ページ））。QoS 測定の詳細については、Quality of Service（QoS）のシミュレーションを参照してください。ここに示されていない [ワーストケース（Worst-Case）] 列については、表 3 : VPN テーブルのシミュレーション分析の列 （14 ページ） を参照してください。

（注） トラフィックおよび QoS の計算は、当該の VPN に指定されたサービスクラス用の、VPN 内のすべてのインターフェイスに基づいているため、プロットビューはテーブルと異なる場合があります。たとえば、音声トラフィックを伝送する VPN が選択されているときに、プロットビューにインターネットトラフィックが表示される場合があります。

（注） すべてのトラフィックおよび QoS 違反は、当該の VPN に定義されたサービスクラス用にその VPN で使用されるすべてのインターフェイスで伝送されるトラフィックに基づきます。

表 *1 :* 通常動作時の *[VPN（VPNs）]* テーブルの列

列	説明
[サービス クラス（Service class）]	この VPN に関連付けられているサービスクラス。テーブル内のすべての値は、このサービスクラスに関連付けられます。
[ノード数（Num nodes）]	この VPN に含まれる VPN ノードの数。
[測定された使用率（Util meas）]	この VPN で使用されるすべてのインターフェイスの測定された最大使用率。
[シミュレートされた使用率（Util sim）]	この VPN で使用されるすべてのインターフェイスのシミュレートされた最大使用率。
[測定された送信元トラフィックの総量（Total src traff meas）]	この VPN で測定された送信元トラフィックの総量。

列	説明
[測定された接続先トラフィックの総量（Total dest traff meas）]	この VPN で測定された接続先トラフィックの総量。
[シミュレートされたQoS違反（QoS violation sim）]	この VPN で使用されるすべてのインターフェイスに関する、シミュレートされたすべてのトラフィックの、通常動作時の最大QoS違反。数値が正の場合、違反があります。
[シミュレートされたQoS違反（%）（QoS violation sim (%)）]	シミュレートされた合計インターフェイス キャパシティのパーセンテージとしての QoS 違反。
[測定されたQoS違反（QoS violation meas）]	この VPN で使用されるすべてのインターフェイスに関する、測定されたすべてのトラフィックの、通常動作時の最大 QoS 違反。数値が正の場合、違反があります。
[測定されたQoS違反（%）（QoS violation meas (%)）]	測定された合計インターフェイス キャパシティのパーセンテージとしての QoS 違反。
[遅延（Latency）]	この VPN で使用されるすべてのデマンドの最大遅延。
[タグ（Tags）]	VPN を簡単にグループ化できるユーザー定義の識別子。

ネットワークプロットから VPN を選択することはできません。VPN はテーブルを介してのみ選択およびフィルタ処理できます。選択すると、VPN に含まれるすべての VPN ノードがプロットで強調表示されます（図 1 : VPN 内の VPN ノード （10 ページ））。

VPN で使用されるインターフェイスの識別

VPN に関連付けられているインターフェイスを表示するには、VPN を選択し、☰ をクリックして、[インターフェイスのフィルタ処理（Filter to interfaces）] を選択します。フィルタ処理されたこれらのインターフェイスをすべて選択すると、ネットワークプロットに VPN の概要が表示されます。

（注） [VPN] テーブルでは、その VPN に関連付けられたサービスクラスの測定値のみが計算されるため、使用率の測定値はテーブル間で異なる場合があります。

VPN ノード

VPN ノードは、ノードが属する VPN と、デマンドのルーティング方法を決定する、次のプロパティによって定義されます。

- [サイト（Site）] : VPN ノードが存在するサイトの名前。

- [ノード（Node）]：VPN ノードが存在するノードの名前。このノード名は、[ノード（Nodes）] テーブルでの名前に対応します。
- [タイプ（Type）]：VPN のタイプ。デフォルト（[VPWS]、[VPLS]、または [L3VPN]）から選択するか、文字列値を入力して新しいタイプを作成することができます。入力すると、新しい VPN タイプがドロップダウンリストに表示され、他の VPN ノードおよび VPN で使用可能になります。
- [名前（Name）]：VPN ノードの名前。
- [VPN]：この VPN ノードが存在する VPN の名前。ドロップダウンリストには、[タイプ（Type）] フィールドで設定されたタイプの既存の VPN が表示されます。VPN を設定せずに VPN ノードを作成できますが、この VPN ノードは VPN のメンバーとしてシミュレーションに含まれません。

  RT 接続をシミュレートするには、[VPN接続（VPN Connectivity）] プロパティを [RT] に設定してから、そこに含まれる個別の VPN ノードで [RTインポート（RT import）] プロパティおよび [RTエクスポート（RT export）] プロパティを設定する必要があります。
- [説明（Description）]：VPN ノードの説明。
- [RTインポート（RT import）] と [RTエクスポート（RT export）]：RT 値のペアリングにより、相互に接続している VPN ノードが識別されます。詳細については、VPN のトポロジと接続 （2 ページ）を参照してください。
- （オプション）[RD]：ルート識別子（RD）は、VRF 内のルートをある VPN または別の VPN に属するものとして一意に識別します。これにより、重複ルートをグローバル ルーティング テーブル内で一意にすることができます。

VPN ノードの作成

手順

ステップ 1 プランファイルを開きます（プランファイルを開くを参照）。[ネットワーク設計（Network Design）] ページに表示されます。

ステップ 2 ツールバーから、**[アクション（Actions）] > [挿入（Insert）] > [VPN（VPNs）] > [VPNノード（VPN node）]** の順に選択します。

または

右側にある [ネットワークサマリー（Network Summary）] パネルで、[VPNノード（VPN nodes）] タブの  をクリックします。

[VPNノード（VPN nodes）] タブは、[詳細（More）] タブの下にあります。表示されていない場合は、[テーブルの表示/非表示（Show/hide tables）] アイコン（  ）をクリックし、[VPNノード（VPN nodes）] チェックボックスをオンにします。

ステップ 3 をクリックします。

ステップ 4 [サイト（Site）] フィールドと [ノード（Node）] フィールドで、VPN ノードが存在するサイトを選択し、VPN ノードが設定されているノードを選択します。

ステップ 5 [タイプ（Type）] ドロップダウンリストから、VPN タイプを選択します。オプションは、[L3VPN]、[VPLS]、および [VPWS] です。

ステップ 6 [名前（Name）] フィールドに、VPN ノードの名前を入力します。一意である必要はありません。

ステップ 7 [VPN] ドロップダウンリストから、この VPN ノードを追加する VPN を選択します。表示されるはずの VPN が表示されない場合は、[タイプ（Type）] ドロップダウンリストで正しい VPN タイプが選択されているかどうかを確認してください。

ステップ 8 （オプション）VPN ノードを識別する説明を入力します。たとえば、カスタマー名が役立つ場合があります。

ステップ 9 VPN の接続が RT の場合は、[RTインポート（RT import）] フィールドと [RTエクスポート（RT export）] フィールドに、該当するルートターゲットを入力します。別の VPN ノードのエクスポート RT と同じインポート RT を持つすべての VPN ノードは、その VPN ノードからトラフィックを受信できます。別の VPN ノードのインポート RT と同じエクスポート RT を持つ VPN ノードは、その VPN ノードにトラフィックを送信できます。

ステップ 10 （オプション）[RD] フィールドに、ルート識別子を入力します。

ステップ 11 [追加（Add）] をクリックします。

VPN への VPN ノードの追加

VPN に VPN ノードを追加するには、次の手順を実行します。

手順

ステップ 1 プランファイルを開きます（プランファイルを開くを参照）。[ネットワーク設計（Network Design）] ページに表示されます。

ステップ 2 右側にある [ネットワークサマリー（Network Summary）] パネルで、[VPNノード（VPN Nodes）] テーブルの 1 つ以上の VPN ノードを選択し、 をクリックします。

（注）
単一の VPN ノードを編集する場合は、[アクション（Actions）] 列の ··· > [編集（Edit）] オプションを使用することもできます。

ステップ 3 [VPN] ドロップダウンリストで、VPN ノードを追加する VPN を選択します。表示されるはずの VPN が表示されない場合は、[タイプ（Type）] ドロップダウンリストで正しい VPN タイプが選択されているかどうかを確認してください。

ステップ 4 [保存（Save）] をクリックします。

[VPNノード（VPN Nodes）] テーブル

[VPNノード（VPN Nodes）] テーブルには、VPN ノードのプロパティと、VPN 内の VPN ノードの関係およびそのトラフィックを識別する列が表示されます。

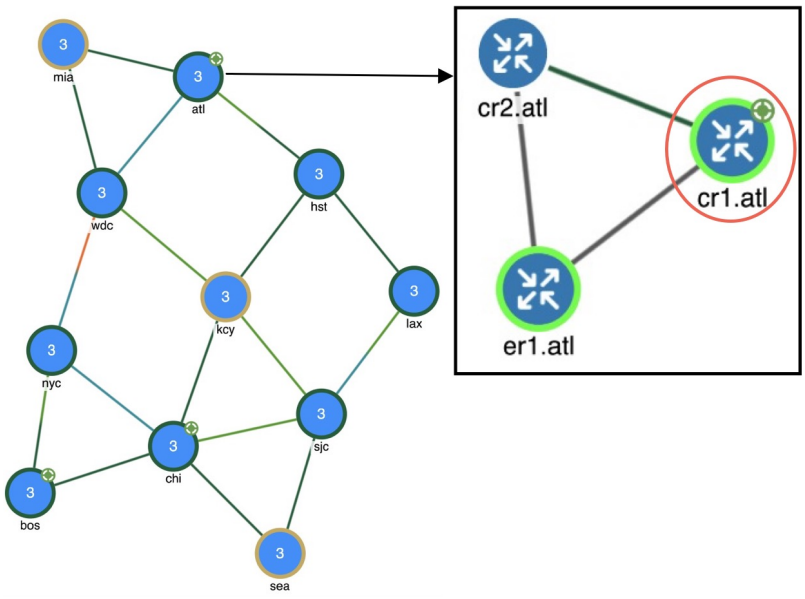
表 2 : [VPNノード（*VPN Nodes*）] テーブル

列	説明
[総接続数（Total connect）]	RT インポートと RT エクスポートのペアリングで定義された、この VPN ノードに接続されている VPN ノードの数。これらは、同じ VPN 内にある場合とない場合があります。
[VPN接続数（VPN connect）]	この VPN ノードに接続され、[VPN] 列で定義されている VPN 内にある VPN ノードの数。
[VPNノード数（Num VPN nodes）]	[VPN] 列で定義されている、この VPN ノードが属する VPN 内のノードの数。VPN ノードが VPN に属していない場合、この値は「na」になります。
[測定された送信元トラフィック（Src traff meas）]	このノードで VPN に入る、測定されたトラフィックの総量（送信元トラフィック）。
[測定された接続先トラフィック（Dest traff meas）]	このノードでVPNから出る、測定されたトラフィックの総量（接続先トラフィック）。
[タグ（Tags）]	VPN ノードを単一の VPN に簡単にグループ化できるユーザー定義の識別子。VPN ノードにタグを付けると、後で VPN を作成するときに、タグを使用して VPN ノードを識別できます。

ネットワークプロットから VPN ノードを選択することはできません。それらはテーブルを介してのみ選択およびフィルタ処理できます。

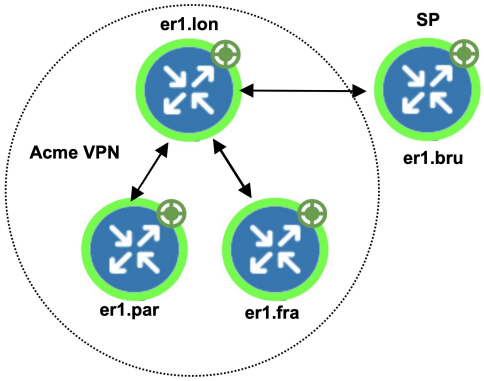
[VPNノード（VPN Nodes）] テーブルまたは [VPN（VPNs）] テーブルから選択すると、関連付けられたサイトとそのサイト内のノードが緑色の円で示されます（図 1 : VPN 内の VPN ノード （10 ページ））。

図 *1 : VPN* 内の *VPN* ノード



レイヤ 3 VPN の例

この例は、Acme 製造会社に 3 つのオフィスがあるが、2 つのブランチオフィス（er1.par および er1.fra）が本社（er1.lon）とのみデータを交換することを許可するシナリオを示しています。



さらに、本社は、Acme VPN にない SP VPN ノード（er1.bur）と通信します。図 2 : RT 接続と Acme VPN フットプリントの例 （11 ページ）は、Acme VPN のフットプリントと、この例に含まれるすべての VPN ノードに設定された RT を示しています。

- VPN の名前は Acme で、[接続（Connectivity）] は [RT]、[タイプ（Type）] は [L3VPN] に設定されています。
- 次に、各ブランチオフィスは Acme VPN に設定されており、[タイプ（Type）] は [L3VPN] です。

- Acme VPN に含まれる他の 2 つの VPN ノードとデータを交換するために、本社（er1.lon）は、オフィスのエクスポートされたルートターゲット 2:1（er1.par）および 3:1（er1.fra）をインポートします。
- 次に、本社（er1.lon）は、ルートターゲット 1:1 をエクスポートします。

これら 3 つの他の VPN ノード（両方のオフィスと SP VPN ノード）はすべて、それをインポートします。

SP VPN ノード（er1.bur）は Acme VPN に含まれていないため、er1.lon との通信は、その VPN のコンテキスト内にはありません。

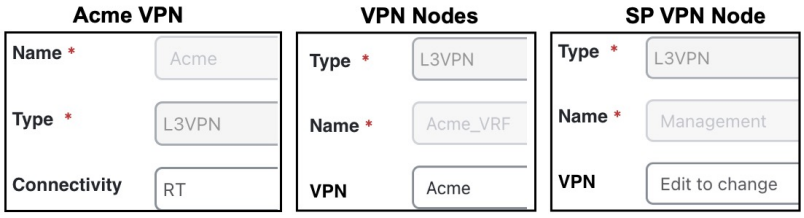


図 2 : RT 接続と Acme VPN フットプリントの例 （11 ページ）の VPN フットプリントは、er1.fra と er1.bur 間の回線で輻輳または障害が発生した場合に VPN が影響を受けることを示しています。ただし、2 つのブランチオフィス間の回線の障害は、影響を受けません。この障害は図 3 : Acme VPN に含まれるブランチオフィス間の障害の例 （12 ページ）に示されています。これは、VPN に関連付けられたデマンドが再ルーティングされていないことを示しています。

図 *2 : RT* 接続と *Acme VPN* フットプリントの例

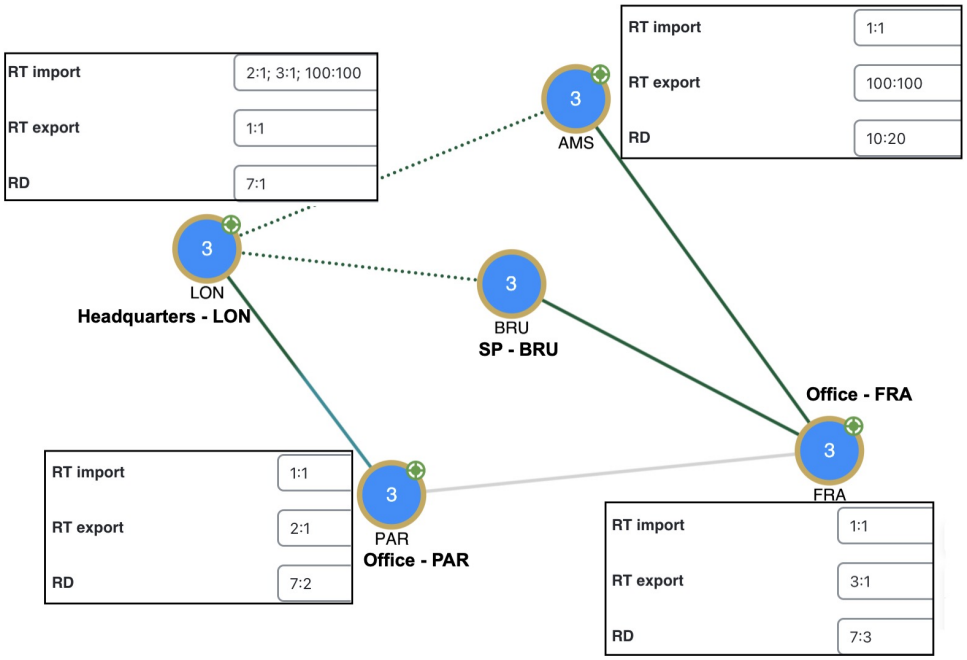
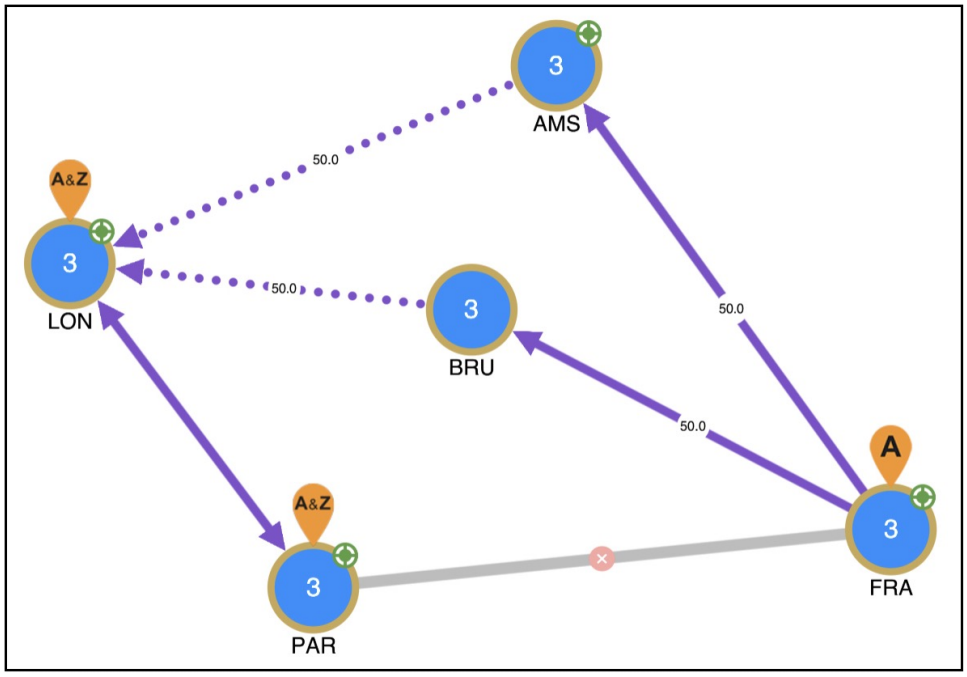


図 *3 : Acme VPN* に含まれるブランチオフィス間の障害の例



この例では、図 4 : Acme VPN に属する VPN ノードと、デマンドに関してフィルタ処理された Acme VPN （13 ページ）は、Acme VPN に属する VPN ノードと、関連するデマンドトラフィックに関する Acme VPN のフィルタ処理を示しています。また、[VPNノード（VPN Nodes）] テーブルの [総接続数（Total connect）] 列と [VPN接続数（VPN Connect）] 列の計算も示しています。

- 本社（er1.lon）に存在する VPN ノードの総接続数は、そのノードが他の 3 つの VPN ノードとデータを交換するため、最大です。

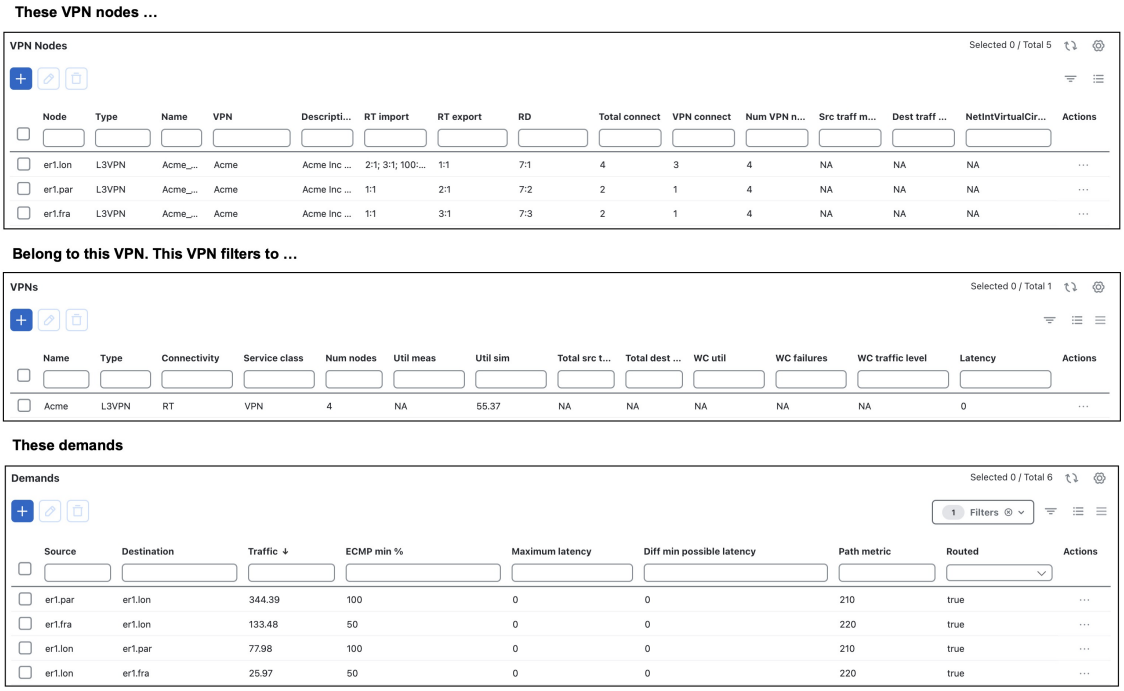
  各オフィスとサービスプロバイダー VPN ノードの [総接続数（Total connect）] 列の値は 2 です。

- 本社（er1.lon）に存在する VPN ノードの VPN 接続数は、そのノードが 2 つのオフィスとデータを交換し、2 つのオフィスと同じ VPN に含まれるため、最大です。3 つの VPN ノードはすべて、同じ VPN 名を共有します。

各オフィスは同じ VPN 内の 1 つの VPN ノードとのみ通信するため、各オフィスの [VPN接続数（VPN connect）] 列の値は 1 です。

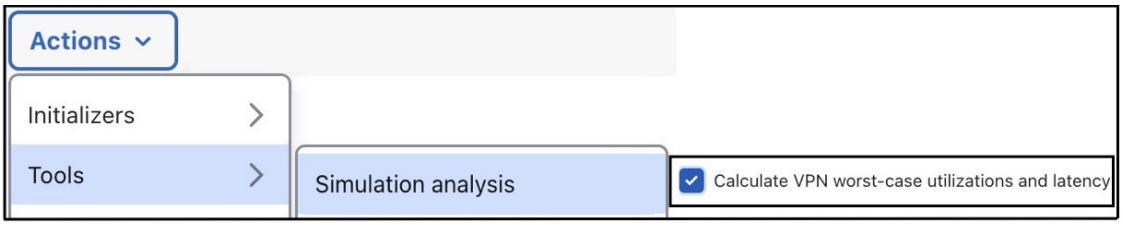
サービスプロバイダー VPN ノード（er1.bur）は、定義された VPN に存在しないため、[VPN接続数（VPN connect）] 列の値は 0 です。

図 *4 : Acme VPN* に属する *VPN* ノードと、デマンドに関してフィルタ処理された *Acme VPN*



VPN シミュレーション分析

シミュレーション分析ツール（ツールバーから、**[アクション（Actions）]**>**[ツール（Tools）]**>**[シミュレーション分析（Simulation analysis）]** の順に選択）を実行すると、VPN のワーストケースの使用率および遅延を VPN テーブルに記録するオプションがあります。その後、 ••• > [ワーストケースを引き起こす障害（Fail to WC）] または [ワーストケースの遅延を引き起こす障害（Fail to WC latency）] オプションをそれぞれ使用して、ワーストケースの使用率またはワーストケースの遅延を引き起こす障害を発生させる VPN を選択できます。



（注） すべての計算は、当該の VPN に定義されたサービスクラス用にその VPN で使用されるすべてのインターフェイスで伝送されるトラフィックに基づいて行われます。

シミュレーション分析が終了すると、[VPN（VPNs）] テーブルで次の列が更新されます。

表 *3 : VPN* テーブルのシミュレーション分析の列

列	説明
[ワーストケースの使用率（WC util）]	すべての障害シナリオにおけるワーストケースの VPN 使用率。
[ワーストケースの障害（WC failures）]	VPN のワーストケースの使用率を引き起こす障害。
[ワーストケースのトラフィックレベル（WC traffic level）]	[ワーストケースの使用率（WC util）]列で特定されたインターフェイスの使用率を引き起こすトラフィックレベル。
[ワーストケースのQoS違反（WC QoS violation）]	この VPN で使用されるすべてのインターフェイスに関するワーストケースの QoS 違反の最大値。QoS 違反は、ワーストケースのトラフィックから、許容されるワーストケースのキャパシティ（ワーストケースの QoS 境界）を引いた値と等しくなります。
[ワーストケースのQoS違反（%）（WC QoS violation (%)）]	総キャパシティのパーセンテージとして表される、この VPN に含まれるすべてのインターフェイスに関するワーストケースの QoS 違反の最高値。
[ワーストケースの遅延（WC latency）]	考慮される障害シナリオにおける最大 VPN 遅延。
[ワーストケースの遅延の障害（WC latency failures）]	ワーストケースの VPN 遅延を引き起こす障害。

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。