ワーストケースの障害による影響の評価

シミュレーション分析ツールでは、多数の障害シナリオのシミュレーション結果が組み合わされます。これらの結果は、障害発生時の輻輳や高遅延に対してネットワークがどの程度脆弱であるかを判断するのに役立ち、そのため、特定の障害シナリオに対して十分なキャパシティをプランニングすることができます。

シミュレーション分析は、選択されたオブジェクト（回線など）とトラフィックレベルを含む一連の障害シナリオにわたって実行されます。Cisco Crosswork Planning は、すべてのサービスクラスにわたって、これらの障害シナリオを計算します。各シナリオがシミュレートされ、次のような分析結果が得られます。これらは、ネットワークに QoS パラメータがあるかどうかや、シミュレーションの実行時に選択されたオプションによって異なります。

- ワーストケースのトラフィック使用率の特定 （2 ページ）（サービスクラスごとにインターフェイスにおいて）
- （オプション）VPN のワーストケースの使用率と遅延
- （オプション）ワーストケースのデマンド遅延の特定 （6 ページ）
- [障害影響（Failure impact）] ビューでのネットワークの可視化 （13 ページ）（障害が発生した各オブジェクトがネットワーク全体のインターフェイス使用率に与える影響を分析）

完了すると、レポートウィンドウが開き、各分析のサマリーと、実行されたシミュレーションのリストが表示されます。シミュレーションを実行するたびに、この情報が更新（置換）されます。

シミュレーション分析は、障害後のネットワーク回復のどの段階を調査するかに応じて、さまざまなシミュレーション コンバージェンス モード（高速再ルーティング、IGP および LSP 再コンバージェンス、自動帯域幅コンバージェンス、および自動帯域幅コンバージェンス（障害を含む））で実行できます。デフォルトのシミュレーションモードは IGP および LSP 再コンバージェンスであり、特に明記されていない限り、このシミュレーションモードについて説明します。

ここでは、次の内容について説明します。

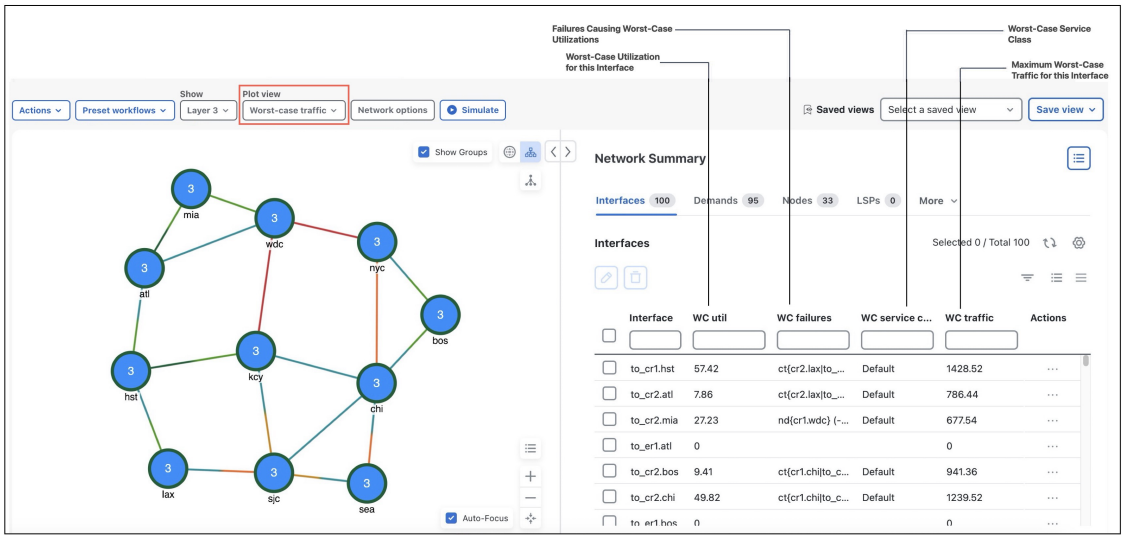
ワーストケースのトラフィック使用率の特定

「ワーストケース」は、選択したすべての障害セットおよびトラフィックレベルで特定のインターフェイスにおいて発生する使用率の最大値です。Cisco Crosswork Planning は、このワーストケースの使用率を引き起こす障害の組み合わせを決定します。

デフォルトの分析では、ネットワークに含まれる各インターフェイスでのワーストケースの使用率について、最大 10 個の障害が特定されます。または、ワーストケースの使用率の指定されたパーセンテージ以内の使用率を引き起こした障害を記録できます。障害シナリオを調査するときに Cisco Crosswork Planning が並行して処理するスレッドの数を制御するには、[スレッドの最大数（Maximum number ofthreads）] フィールドを設定します。シミュレーション分析の実行方法の詳細については、シミュレーション分析の実行 （8 ページ）を参照してください。

分析が完了すると、Cisco Crosswork Planning は、[ワーストケースのトラフィック（Worst-Case traffic）] ビューに切り替え、プロットを更新して、すべてのインターフェイスでのワーストケースの使用率を同時に表示します。

図 *1:* すべてのインターフェイスでのワーストケースのトラフィック使用率



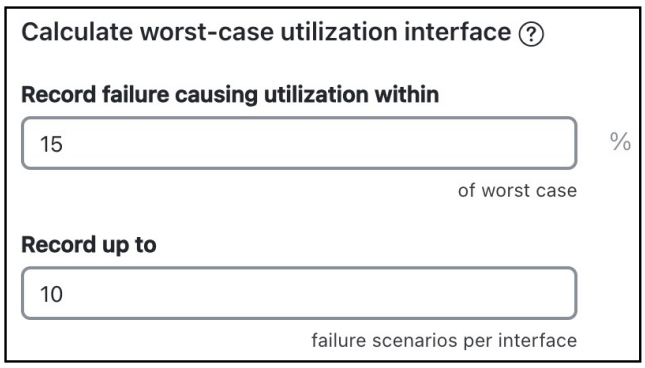
プロットビューの変更に加えて、シミュレーション分析の完了時には [インターフェイス（Interfaces）] テーブルと [回線（Circuits）] テーブルの次の列も更新されます。

- [ワーストケースの使用率（WC util）]：そのインターフェイスでのワーストケースの使用率。回線のワーストケースは、2 つの構成インターフェイスでのワーストケースのうち、使用率が大きくなる方として定義されます。そのため、回線の場合、この値は、回線に含

まれる 2 つのインターフェイスに関する [ワーストケースの使用率（WC util）] の値の大きい方になります。

- [ワーストケースのトラフィック（WC traffic）]：ワーストケースのシナリオでインターフェイスを通過する実際のトラフィック（Mbps）。
- [ワーストケースのトラフィックレベル（WC traff level）]：このワーストケースのシナリオを引き起こすトラフィックレベル。
- [ワーストケースの障害（WC failure）]：回線のワーストケースの障害を引き起こす 1 つ以上の障害のリスト。このリストを簡単に確認するには、インターフェイスを選択し、 ••• > [ワーストケースを引き起こす障害（Fail to WC）] を使用します。

  ワーストケースの特定パーセンテージ以内の使用率を引き起こした障害を記録する場合、この列には、QoS 違反がパーセンテージとして表示されます。（ワーストケースの QoS 違反の特定 （3 ページ） を参照。）数値が正の場合、割り当てられたキャパシティを超えています。負の場合は、キャパシティを超えていません。たとえば、回線のキャパシティが 10,000 Mbps であり、3 つの異なる障害の結果として回線上のトラフィック量が 11,000 Mbps、8000 Mbps、および 4000 Mbps になる場合、使用率はそれぞれ 10%、-20%、および -60% になります（降順に表示）。



- [ワーストケースのサービスクラス（WC service class）]：このワーストケースのシナリオを引き起こすサービスクラス。

QoS を使用したシミュレーション分析の実行については、ワーストケースの QoS 違反の特定 （3 ページ） を参照してください。

VPN のワーストケースの計算については、VPN のシミュレーションを参照してください。

ワーストケースの QoS 違反の特定

Cisco Crosswork Planning には、ワーストケースの計算の一部として、QoS 境界（使用可能な最大キャパシティ）が含まれます。QoS パラメータが設定されていない場合、QoS 境界は 100% であり、使用率がその 100% を超えると違反が発生します。ただし、サービスクラスにワーストケースポリシーが設定されている場合、またはインターフェイスキューのパラメータが設定されている場合は、ワーストケースの QoS 違反が計算されます。このような場合、Cisco

Crosswork Planning は、QoS 違反のパーセンテージが最も高いインターフェイスを、ワーストケースの可能性として識別します。

それに応じて、次の列が更新されます。

- [ワーストケースのQoS境界（WC QoS bound）]：これらの QoS 要件に違反することなく使用可能なワーストケースのインターフェイスキャパシティ。この値は、使用可能なキャパシティ、トラフィック使用率、サービスクラスに設定されたワーストケースポリシー、およびインターフェイスキューのパラメータに基づきます。

  [ワーストケースのQoS境界（%）（WC QoS bound (%)）] 列は、この同じ値を、合計キャパシティのパーセンテージとして識別します。

- [ワーストケースのQoS違反（WC QoS violation）]：ワーストケースのトラフィックからワーストケースの許容キャパシティを引いた値（[ワーストケースのQoS境界（WC QoS bound）]）。サービスクラスのワーストケースポリシーによって割り当てられた QoS キャパシティを超えた場合、またはインターフェイスキューのパラメータによって割り当てられた QoS キャパシティを超えた場合、違反が発生します。[ワーストケースのQoS違反（WC QoS violation）]列に表示される数値が正の場合、割り当てられたキャパシティを超えています。負の場合は、キャパシティを超えていません。

  [ワーストケースのQoS違反（%）（WC QoS violation (%)）]列は、この同じ値を、合計キャパシティのパーセンテージとして識別します。

  ワーストケースの QoS 違反の原因を確認するには、回線を選択して、 ••• >[ワーストケースを引き起こす障害（Fail to WC）] を使用します。表示されるページには、この回線のワーストケースの使用率とワーストケースの QoS 違反について、そのすべての原因が一覧表示されます。表示するワーストケースの障害を選択し、[送信（Submit）] をクリックします。

- [ワーストケースのサービスクラス（WC service class）]：ワーストケースの QoS 違反を引き起こしたサービス。

次の詳細情報	参照先
• QoS パラメータと QoS 計算 • サービスクラスへのワーストケースポリシーの設定 • インターフェイスキューのパラメータの設定	Quality of Service（QoS）のシミュレーション
VPN のワーストケースの QoS 計算	VPN のシミュレーション

ワーストケースの使用率を引き起こす回線の障害化

シミュレーション分析を実行（シミュレーション分析の実行 （8 ページ）を参照）した後、単一のインターフェイスでワーストケースの使用率またはワーストケースの QoS 違反を引き起こす各障害シナリオを選択的に表示するオプションがあります。

ワーストケースの障害に関して複数の可能性がある場合、またはワーストケースの障害のパーセンテージ（[ワーストケースの障害（WC failures）] 列に示される）以内に障害の範囲がある場合、[ワーストケースを引き起こす障害（Fail to WC）]ページに、各障害、そのワーストケースの使用率（パーセンテージ）、およびその QoS 違反（パーセンテージ）が一覧表示されます（図 2 : ワーストケースを引き起こす 1 つの回線の障害 （6 ページ）を参照）。

（注） インターフェイスを選択すると、実際には、関連する回線で、そのワーストケースを引き起こす障害が発生します。

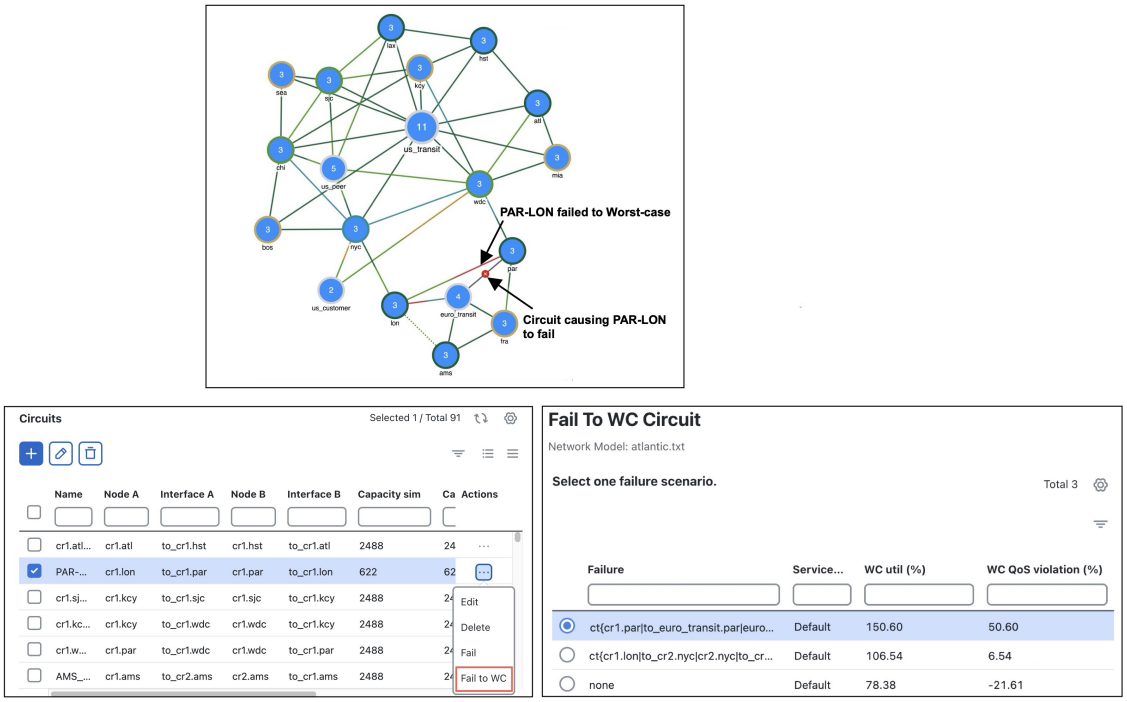
インターフェイス/回線で、ワーストケースを引き起こす障害を発生させるには、次の手順を実行します。

1. [ワーストケースのトラフィック（Worst-case traffic）] ビューで、それぞれのテーブルから目的のインターフェイスまたは回線を選択します。
2. [アクション（Actions）] 列から、 ··· > [ワーストケースを引き起こす障害（Fail to WC）] の順に選択します。

   [ワーストケースのインターフェイス（または回線）を引き起こす障害（Fail to WC Interface (or Circuit)）] ページが表示されます。
3. 目的の障害シナリオを選択します（図 2 : ワーストケースを引き起こす 1 つの回線の障害 （6 ページ）を参照）。
4. [送信（Submit）] をクリックします。

ネットワークプロットが変更され、この特定の障害シナリオが表示されます（図 2 : ワーストケースを引き起こす 1 つの回線の障害 （6 ページ）を参照）。

図 *2:* ワーストケースを引き起こす *1* つの回線の障害



ワーストケースのデマンド遅延の特定

シミュレーション分析を実行する場合（シミュレーション分析の実行 （8ページ）を参照）、プランの各デマンドについてワーストケースの遅延をシミュレートするオプションがあります。Cisco Crosswork Planning は、選択した障害シナリオでの各デマンドの最大遅延を計算します。デマンドルーティングはそれらのプランから独立しているため、結果は、サービスクラスまたはトラフィックレベルに依存しません。シミュレーションでは、この最大遅延を引き起こす障害も記録されます。

[デマンド（Demands）]テーブルの次の列は、シミュレーション分析ツールの実行中に、[デマンドのワーストケースの遅延を計算（Calculate demand worst-case latency）] チェックボックスをオンにすると更新されます。

- [ワーストケースの遅延（WC latency）]：分析対象のすべての障害シナリオにおける最大デマンド遅延。
- [ワーストケースの遅延の障害（WC latency failures）]：このワーストケースの遅延を引き起こした障害。最大 10 個の障害が特定されます。

Cisco Crosswork Planning は、次の 2 つのオプションを使用して、シミュレーション分析に含まれる各障害ケースのデマンドごとの遅延をキャプチャします。

- [ワーストケースの__%以内のデマンド遅延を引き起こす障害を記録（Record failures causing demand latency within __% of worst case）]：ワーストケース遅延の指定されたパーセンテー

ジ範囲内のデマンド遅延を引き起こす障害を記録します。デフォルトは 0 です。0 を入力すると、ワーストケースの遅延障害のみが記録されます。

- [デマンド遅延における__件までの障害シナリオを記録（Record up to __ failure scenarios on demand latency）]：デマンドごとに記録される障害シナリオの最大数。デフォルトは 1 です。

ワーストケースの特定割合内のデマンド遅延を引き起こす障害を記録した場合、[ワーストケースの遅延の障害（WC latency failures）] 列には、障害シナリオとともにワーストケースの遅延が表示されます。

ワーストケースの遅延を引き起こすデマンドの障害化

シミュレーション分析を実行して（シミュレーション分析の実行 （8 ページ）を参照）デマンドのワーストケースの遅延を計算した後、1 つのデマンドに障害を発生させて、そのワーストケースの遅延を引き起こすことができます。

（注） シミュレーション分析の実行中に [デマンドのワーストケースの遅延を計算（Calculate demand worst-case latency）] チェックボックスをオンにしておらず、[プロットビュー（Plot view）] が [ワーストケースのトラフィック（Worst-case traffic）] でない場合、デマンドに障害を発生させてそのワーストケースの遅延を引き起こすオプションは表示されません。

ワーストケースの遅延を引き起こす障害シナリオは、[デマンド（Demands）] テーブルの [ワーストケースの遅延の障害（WC latency failures）] 列に一覧表示されます。

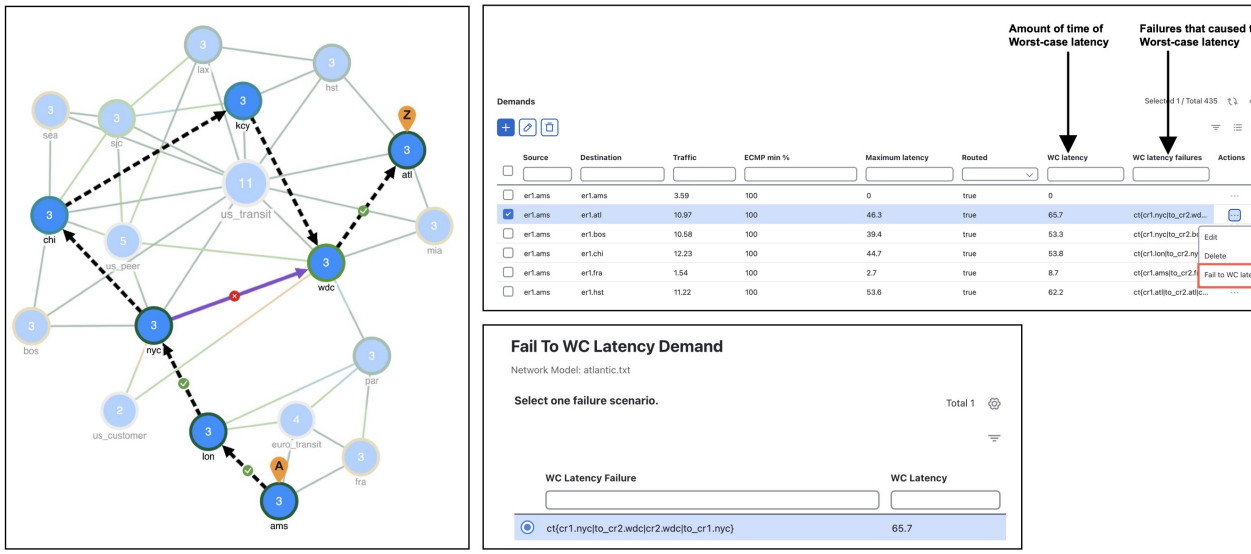
デマンドに障害を発生させてワーストケースの遅延を引き起こすには、次の手順を実行します。

1. [ワーストケースのトラフィック（Worst-case traffic）] ビューで、[デマンド（Demands）] テーブルから目的のデマンドを選択します。
2. [アクション（Actions）] 列から、 ••• > [ワーストケースの遅延を引き起こす障害（Fail to WC latency）] の順に選択します。

   [ワーストケースの遅延デマンドを引き起こす障害（Fail to WC Latency Demand）] ページが表示されます。
3. 目的の障害シナリオを選択します（図 3 : ワーストケースのデマンド遅延の例 （8 ページ）を参照）。
4. [送信（Submit）] をクリックします。

ネットワークプロットが変更され、この特定の障害シナリオが表示されます（図 3 : ワーストケースのデマンド遅延の例 （8 ページ）を参照）。

図 *3:* ワーストケースのデマンド遅延の例



シミュレーション分析の実行

シミュレーション分析ツールは、4 つの障害分析オプション（インターフェイスでのワーストケースの使用率、ワーストケースの VPN の使用率と遅延、ワーストケースのデマンド遅延、および障害の影響）の基礎となります。

（注） ワーストケースのデマンド遅延または VPN のワーストケースの使用率を記録すると、ワーストケースの分析の実行にかかる時間が長くなります。

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。

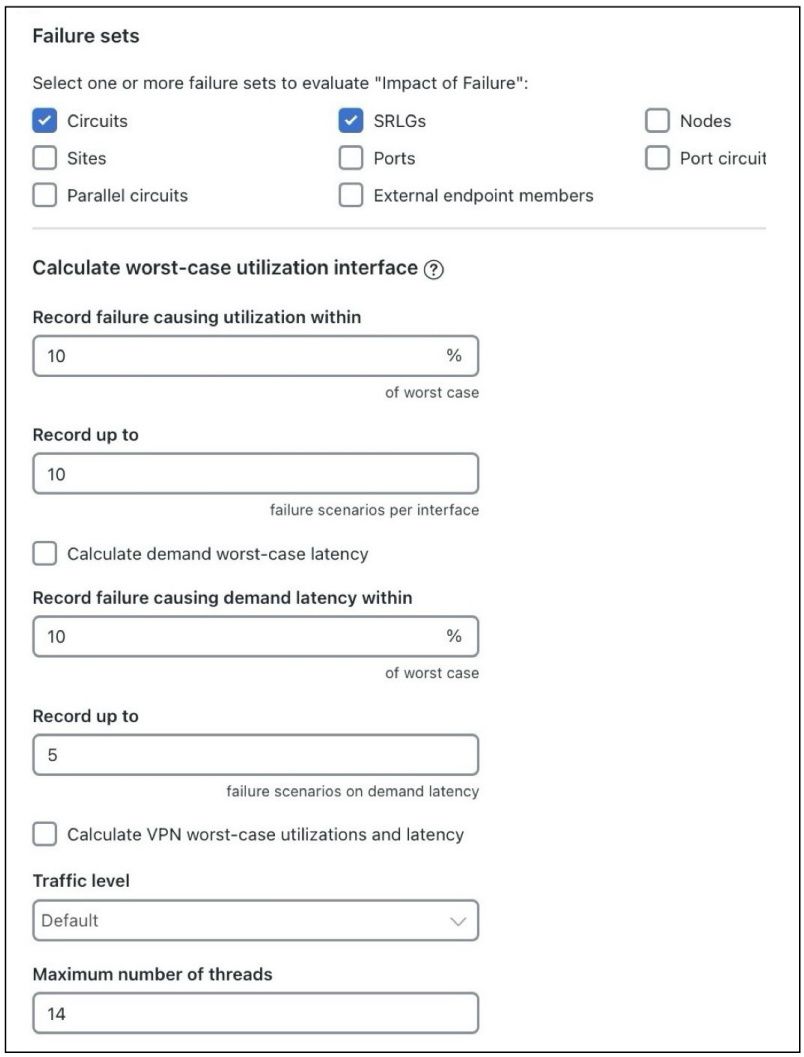
ステップ 2 ツールバーから、次のいずれかのオプションを選択します。

- [プリセットワークフロー（Preset workflows）] > [障害の影響の評価（Evaluate impact of failures）]

  または

- [アクション（Actions）] > [ツール（Tools）] > [シミュレーション分析（Simulation analysis）]

図 *4*: シミュレーション分析の設定



ステップ 3 [障害セット（Failure sets）] セクションで、1 つ以上の障害セットを選択します。

ステップ 4 [ワーストケースの__%以内の使用率を引き起こす障害を記録（Record failures causing utilizations within __% of worst case）] フィールドで、0 を入力して、ワーストケースの障害のみを記録するか、数値を入力して、ワーストケースの障害のパーセンテージ範囲内の使用率を引き起こすすべての障害を検索します。

ステップ 5 [インターフェイスごとに__件までの障害シナリオを記録（Record up to __ failure scenarios per interface）] フィールドに、インターフェイスごとに記録する障害シナリオの最大数を入力します。デフォルトは 10 です。

例：ワーストケースの 10% 以内の使用率を引き起こす障害を記録するときに、インターフェイスのワーストケースの使用率が 90% の場合、Cisco Crosswork Planning は、このインターフェイスで 81%（90 - （90/10））以上の使用率を引き起こす障害を記録します。この同じシナリオで、インターフェイスごとに 10 個の障害シナリオを記録するときに、90%、85%、82%、および 76% のインターフェイス使用率を引き起こす可能性のある障害がある場合、Cisco Crosswork Planning は、76% の使用率を引き起こす障害を記録しません。

ステップ 6 [デマンドのワーストケースの遅延を計算（Calculate demand worst-case latency）] チェックボックスを使用して、デマンドのワーストケース遅延の計算を記録するかどうかを選択します。

ステップ 7 [ワーストケースの__%以内のデマンド遅延を引き起こす障害を記録（Record failures causing demand latency within __% of worst case）] フィールドで、0 を入力して、ワーストケース遅延障害のみを記録するか、数値を入力して、ワーストケースの遅延のパーセンテージ範囲内のデマンド遅延を引き起こすすべての障害を検索します。

ステップ 8 [デマンド遅延における__件までの障害シナリオを記録（Record up to __ failure scenarios on demand latency）] フィールドに、デマンドごとに記録される障害シナリオの最大数を入力します。デフォルトは 1 です。

例：ワーストケースの 10% 以内のデマンド遅延を引き起こす障害を記録するときに、ワーストケースのデマンドの遅延が 100 ミリ秒である場合、Cisco Cisco Crosswork Planning は、このデマンドに対して 90 ミリ秒（100 -（100/10））以上の遅延を引き起こす障害シナリオを記録します。この同じシナリオで、デマンド遅延ごとに 5 つの障害シナリオを記録するときに、92 ミリ秒、95 ミリ秒、98 ミリ秒、および 80 ミリ秒のデマンド遅延を引き起こす可能性のある障害がある場合、Cisco Cisco Crosswork Planning は、80 ミリ秒のデマンド遅延を引き起こす障害を記録しません。

ステップ 9 [VPNのワーストケースの使用率と遅延を計算（Calculate VPN worst-case utilizations and latency）] チェックボックスを使用して、VPN のワーストケースの使用率と遅延を記録するかどうかを選択します。詳細については、VPN のシミュレーションを参照してください。

ステップ 10 [スレッドの最大数（Maximum number of threads）] フィールドにスレッドの最大数の値を入力します。

ステップ 11 [次へ（Next）] をクリックします。

ステップ 12 [実行設定（Run Settings）] ページで、タスクを今すぐ実行するか、後で実行するようにスケジュールするかを選択します。次の [実行（Execute）] オプションから選択します。

- [今すぐ（Now）]：ジョブをすぐに実行するには、このオプションを選択します。ツールが実行され、変更がネットワークモデルにすぐに適用されます。また、サマリーレポートが表示されます。**[アクション（Actions）] > [レポート（Reports）] > [生成されたレポート（Generated reports）]** オプションを使用して、後でいつでもレポートにアクセスできます。
- [スケジュールされたジョブとして（As a scheduled job）]：タスクを非同期ジョブとして実行するには、このオプションを選択します。このオプションを選択した場合は、タスクの優先順位を選択し、ツールを実行する時間を設定します。ツールは、スケジュールされた時間に実行されます。[Job Manager] ウィンドウを使用して、いつでもジョブのステータスを追跡できます（メインメニューから、[Job Manager] を選択）。ジョブが完了したら、出力ファイル（.tar ファイル）をダウンロードして解凍し、更新されたプランファイルをユーザースペースにインポートしてアクセスします（詳細については、ローカルマシンからのプランファイルのインポートを参照）。

  （注）
  ジョブをスケジュールする前に、必ず、プランファイルを保存してください。スケジュールされたジョブとしてツールを実行する場合、プランファイルの保存されていない変更は考慮されません。

ステップ 13 [送信（Submit）] をクリックします。

[ワーストケースのトラフィック（Worst-case traffic）] ビュー（[プロットビュー（Plot view）] ドロップダウンから [ワーストケースのトラフィック（Worst-case traffic）] を選択）を使用して、ワーストケースのトラフィック使用率、ワーストケースの QoS 違反、およびワーストケー

スの遅延情報を分析できるようになりました。ここでは、インターフェイスとノードに障害を発生させてワーストケースを引き起こし、デマンドに障害を発生させてワーストケースの遅延を引き起こすこともできます。[障害影響（Failure impact）] ビューでのネットワークの可視化（13 ページ） ビューを使用して、ワーストケースのトラフィック輻輳の原因となっている回線を特定することも可能です。

オブジェクトの保護

シミュレーション分析の実行時に失敗したオブジェクトのリストからオブジェクトを除外するには、そのオブジェクトの[編集（Edit）] ウィンドウでそのオブジェクトを[保護（Protected）] としてマークします。たとえば、コアノードでのみシミュレーション分析を実行する場合は、最初にすべてのエッジノードを保護できます。

ノード、サイト、回線ポート、ポート回線、外部エンドポイントメンバー、および並列回線を保護できます。

（注） インターフェイスを選択すると、実際には、関連する回線が保護されます。

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 それぞれのテーブルから 1 つ以上の類似オブジェクトを選択します。

ステップ 3 をクリックします。

（注）
単一のオブジェクトを編集している場合は、[アクション（Actions）] 列の下にある ··· > [編集（Edit）] オプションを使用することもできます。

ステップ 4 [状態（State）] フィールドで、[保護（Protected）] チェックボックスをオンにします。

ステップ 5 [保存（Save）] をクリックします。

シミュレーション分析レポートの分析

シミュレーション分析を実行するたびに、レポートが自動的に生成されます。この情報には、[アクション（Actions）] > [レポート（Reports）] > [生成されたレポート（Generated reports）] の順に選択し、右側のパネルで[シミュレーション分析（Simulation Analysis）] リンクをクリックすることで、いつでもアクセスできます。以前のレポートは新しいレポートに置き換わることに注意してください。

[オプション（Options）]タブには、シミュレーション分析に使用される入力パラメータが表示されます。

[サマリー（Summary）]タブには、分析で使用されるオプションの詳細情報が表示され、特定された最も重要な問題（QoS 違反や遅延境界違反など）が要約されます。

[最大使用率（Max Utilization）]タブには、最大使用率に対する障害の影響が円グラフの形式で表示されます。

[シミュレーション（Simulations）]テーブルには、シミュレーション分析で実行された各シミュレーションが一覧表示されます（表 1 : シミュレーション分析レポートの [シミュレーション（Simulations）] テーブル （12 ページ））。

表 *1 :* シミュレーション分析レポートの *[*シミュレーション（*Simulations*）*]* テーブル

シミュレーションデータ ポイント	説明
[失敗（Failure）]	分析で使用された障害シナリオ。
サービス クラス	分析で使用されたサービスクラス。
[トラフィック レベル（Traffic level）]	分析で使用されたトラフィック レベル。
[ネットワーク ブレークポイント（Network breakpoint）]	このシミュレーションにおいて障害が原因でネットワークが切断されているかどうかを識別します。複数のネットワーク ブレークポイントが発生した場合は、最も重大なブレークポイントが示されます。 • [はい（合計）（Yes (Total)）]：ネットワークを 2 つ以上の切断されたセクションに完全に分割する切断が存在します。 • [はい（AS）（Yes (AS)）]：AS を 2 つ以上のセクションに完全に分割する切断が存在します。ただし、他の AS を経由する AS のセクション間にはルートが存在します。 • [はい（OSPFエリア0）（Yes (OSPF Area 0)）]：OSPF を実行する AS のエリア 0 を完全に分割する切断が存在します。OSPF では、AS のゼロ以外のエリアを通過するパスが使用可能であっても、トラフィックをパーティション間でルーティングできません。 • [いいえ（No）]：ネットワークの切断はありません。
[ルーティングされていないデマンドの数（Num unrouted demands）]	ネットワーク ブレークポイントで特定された理由のいずれかにより、この障害下でルーティングできないデマンドの数。

シミュレーションデータ ポイント	説明
[ルーティングされていないトラフィック（Unrouted traffic）]	ネットワーク ブレークポイントで特定されたいずれかの理由により、この障害下でルーティングできないデマンドトラフィックの総量。
[最大使用率（Max util）]	このシミュレーションに含まれるすべてのインターフェイスにわたる最大使用率。使用率は、インターフェイスを通過するトラフィックを、インターフェイスのキャパシティのパーセンテージで表したものです。
[最大QoS境界パーセンテージ（Max QoS bound percent）]	QoS 境界に違反することなく使用可能なワーストケースのキャパシティ。総キャパシティのパーセンテージとして表されます。
[QoS違反の数（Num QoS violations）]	QoS 境界違反の回数。QoS 境界は、サービスクラスポリシーとインターフェイス キュー パラメータによって設定されます。
[遅延境界違反（Latency bound violations）]	デマンドに指定された遅延境界を超える最大遅延を持つデマンドの数。
[ルーティングされていないLSPの数（Num unrouted LSPs）]	分析に含まれるルーティングされていない非高速再ルーティング（FRR）LSP の数。
[ルーティングされていないFRR LSPの数（Num unrouted FRR LSPs）]	分析に含まれるルーティングされていない FRR LSP の数。

[障害影響（Failure impact）] ビューでのネットワークの可視化

シミュレーション分析の実行時には、[障害影響（Failure impact）] ビューを使用できます（図 5 : 障害の影響の例 （15 ページ））。このビューのプロットにより、ノードまたは回線に障害が発生した場合にネットワーク内の他の場所で発生する最大使用率レベルに従って、ノードと回線が色分けされます。この色は、結果として生じる使用率と輻輳のシビラティ（重大度）を示します。

例：[障害影響（Failure impact）] ビューでは、sjc-lax 回線の使用率は 90 ～ 100% であり、赤に近いオレンジ色で表示されています。これは、sjc-lax に障害が発生した場合、1 つ以上のインターフェイスが 90% 使用率レベルを超える反応を示し、それに対応してプロットで赤に近いオレンジ色になることを意味します。

[ノード（Node）]、[インターフェイス（Interface）]、および[回線（Circuit）]テーブルには、[障害影響（Failure impact）] 列と [障害影響インターフェイス（Failure impact interface）] 列が含まれています。[インターフェイス（Interfaces）]テーブルの情報は、インターフェイスを含む回線の障害の影響を示しています。

- [障害影響（Failure impact）]：各ノードまたは回線の障害の影響。たとえば、この値が 80% の場合は、このノードまたは回線に障害が発生したときに、1 つ以上のインターフェイスで結果として生じるトラフィック使用率が 80% を超えることを意味します。
- [障害影響インターフェイス（Failure impact interface）]：ノードまたは回線がダウンした結果として使用率が最も高くなるインターフェイス。

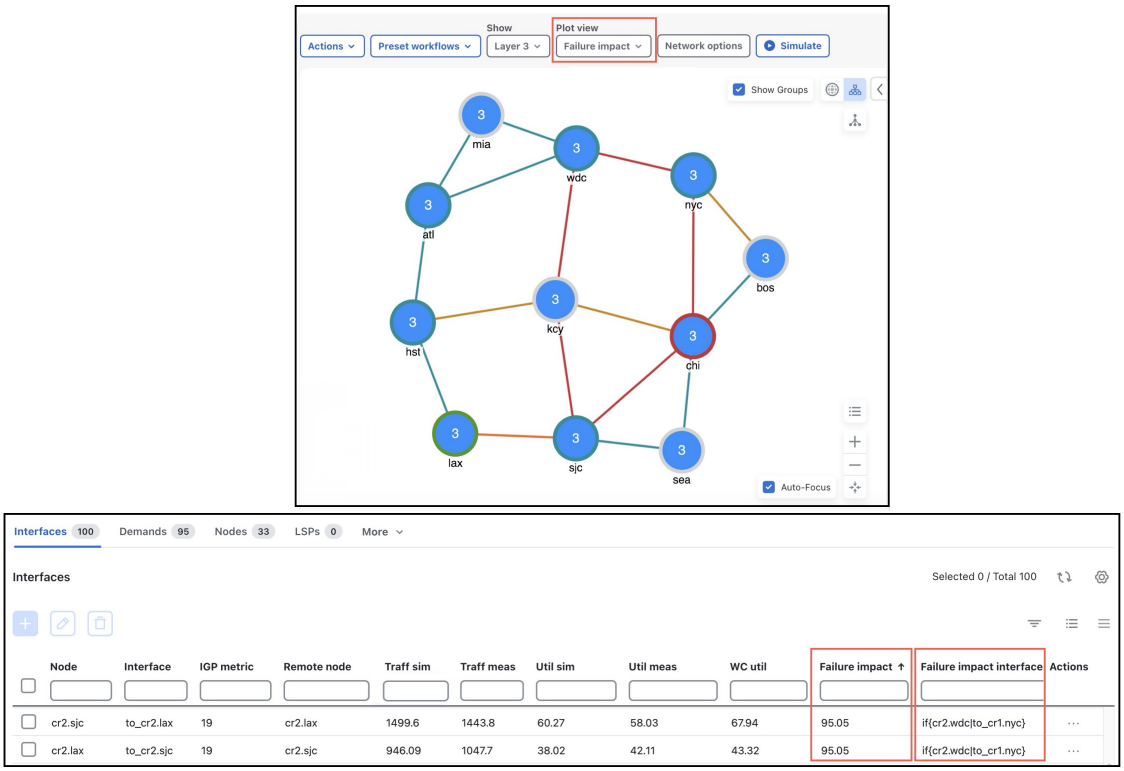
形式 = if{Node|Interface}

例：if{cr2.sjc|to_cr1.kcy} は、回線がダウンした場合、cr2.sjc から cr1.kcy へのインターフェイスに対するトラフィックの影響が最も大きいことを意味します。

ネットワークプロットでは、サイトの境界線は、その中のノードに障害が発生した場合またはその中のサイト内回線に障害が発生した場合に、ネットワーク内の他の場所で発生する最大使用率レベルを示します。

（注） [障害影響（Failure impact）] ビューには、回線およびノードの障害の影響のみが表示されます。他のオブジェクトの障害は表示されません。

図 *5* : 障害の影響の例



並列化

シミュレーション分析ツールを使用すると、計算を並列化できるため、大規模なネットワークモデルでより迅速に結果を得られます。

たとえば、ネットワークモデルに10000の回線があり、10の異なるエンジンが使用可能である場合、このツールを使用してネットワークモデルを10のパーティションに分割します。各パーティションでは1000の障害シナリオが処理されます。これにより、10の異なる結果ファイルが作成されます。これらの独立した各実行の結果はマージされ、最終結果が得られます。

並列化の実行：

CLIツールを使用して並列化を実行します。詳細については、CLIを使用したツールまたはイニシャライザの実行を参照してください。

1. メインメニューから [Job Manager] を選択します。
2. > [CLIの使用（Using CLI）] の順にクリックします。
3. [シミュレーション分析（Simulation analysis）] を選択し、[次へ（Next）] をクリックします。

4. シミュレーション分析を実行するネットワークモデルを選択し、[次へ（Next）] をクリックします。
5. [シミュレーション分析の入力オプション（Simulation Analysis input options）] フィールドで、次のコマンド使用します。

```
-failure-sets <failure-sets> -num-partitions <number-of-partitions> -num-threads
<number-of-threads> -partition-index <partition-index> -result-file <result-filename>
```

ここで

- **-num-partitions**：障害シナリオのパーティションの数。各パーティションは、関連する一連の障害シナリオを持ち、0 から、パーティション数から 1 を引いた数までのインデックスによって識別されます。デフォルトは 1 です。
- **-partition-index**：指定されたパーティションに属する一連の障害シナリオをシミュレートします。デフォルトは 0 です。
- **-result-file**：指定した場合、シミュレーション分析レポートの結果がこのファイルに書き込まれます。*.txt ファイルまたは *.db ファイルを指定できます。

CLI を使用したツールとイニシャライザの実行の詳細については、CLI を使用したツールまたはイニシャライザの実行を参照してください。

結果のマージ：

結果をマージするには、Python スクリプトを使用して merge_sim_analysis CLI を呼び出します。スクリプトの実行の詳細については、外部スクリプトの実行を参照してください。

サンプルスクリプト（run_cli_merge.py）：

```
import os
import sys

cmd = "merge_sim_analysis -plan-file {0} -partial-results {1} -out-file out-plan.txt
".format( sys.argv[1], sys.argv[2])
print(cmd)
os.system(cmd)
```

ここで

- **-plan-file**：入力プランファイル。
- **-out-file**：出力プランファイル。
- **-partial-results**：各パーティションのシミュレーション分析結果を含むファイルのカンマ区切りリスト。これらは、プランファイルか、シミュレーション分析 CLI ツールの実行中に **-result-file** オプションを使用して生成されたファイルである可能性があります。
- **-partial-result-paths-file**：各パーティションのシミュレーション分析結果を含むファイルのリスト（1 行に 1 つずつ）を含むファイル。これらは、プランファイルか、シミュレーション分析 CLI ツールの実行中に **-result-file** オプションを使用して生成されたファイルである可能性があります。**-partial-results** オプションが指定されている場合、これは無視されます。

Job Manager で、スクリプト（run_cli_merge.py）の実行時に次の引数を入力します。

```
run_cli_merge.py input_planfile.pln res_0.txt,res_1.txt,res_2.txt
```

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。