# 2024年9月18日リリース
# Mist 新機能のご紹介

ジュニパーネットワークス株式会社

JUNIPer driven by Mist AI

# はじめに

❖ 本ドキュメントは以下のリリースノートを抄訳したものです

https://www.mist.com/documentation/september-18th-2024-updates/

本ドキュメントは2024年9月時点のMist cloudのGUIを使用しております

❖ 実際の画面と表示が異なる場合がございます

❖ 内容について不明な点、ご質問等がございましたら担当営業までお問い合わせください

# 本リリースで追加された機能一覧（1/2）

**Marvis**
- MQLで表示されるスイッチリストへの項目の追加

**Simplified Operations**
- OAuth 2.0を用いたWebhook

**Wireless Assurance**
- 6GHz帯のチャネル割り当てロジックの改良
- PSK生成のためのデフォルトURLの上書き
- アクセスポイントのラベル生成機能の拡張

**Mist Edge**
- IPv6サポート
- Mist Edgeノート

**Wired Assurance**
- キャンパスファブリックでのIPv6サポート
- キャンパスファブリックにおけるスイッチ間の最小接続数の変更
- システム定義のポートプロファイルの削除
- スタンドアロンスイッチとVCメンバースイッチの位置の確認
- スイッチポートプロファイルの再認証間隔
- スイッチやゲートウェイ機器へのリモートシェルアクセスの無効化
- RSTPエッジポート
- ポートリスト内でのトランシーバ情報の表示
- リモートシェル経由でのスイッチログのダウンロード

# 本リリースで追加された機能一覧（2/2）

**WAN Assurance**

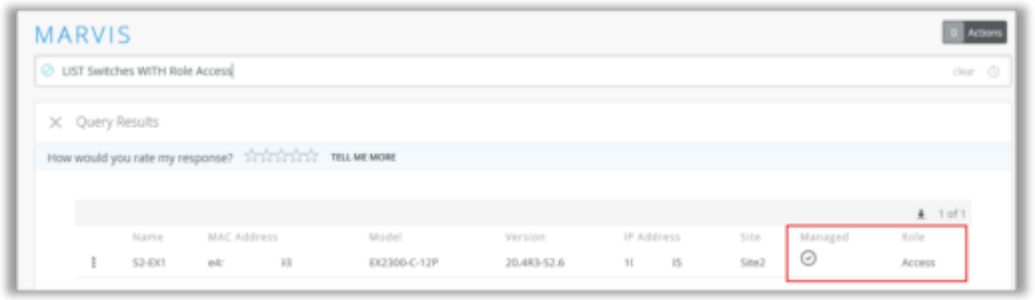
- SRX4300のサポート
- ゲートウェイ帯域幅SLE（SRX）
- アプリケーション経路インサイト機能の拡張
- カスタムアプリケーションのヘルスチェック（SSR）
- セッションテストツール機能の拡張（SSR）
- アプリケーションポリシー適用回数の表示
- ポートリセットテストツール（SSR）

**Support**

- 新規導入に関するサポートチケット分類の追加

# Marvis

# MQLで表示されるスイッチリストへの項目の追加



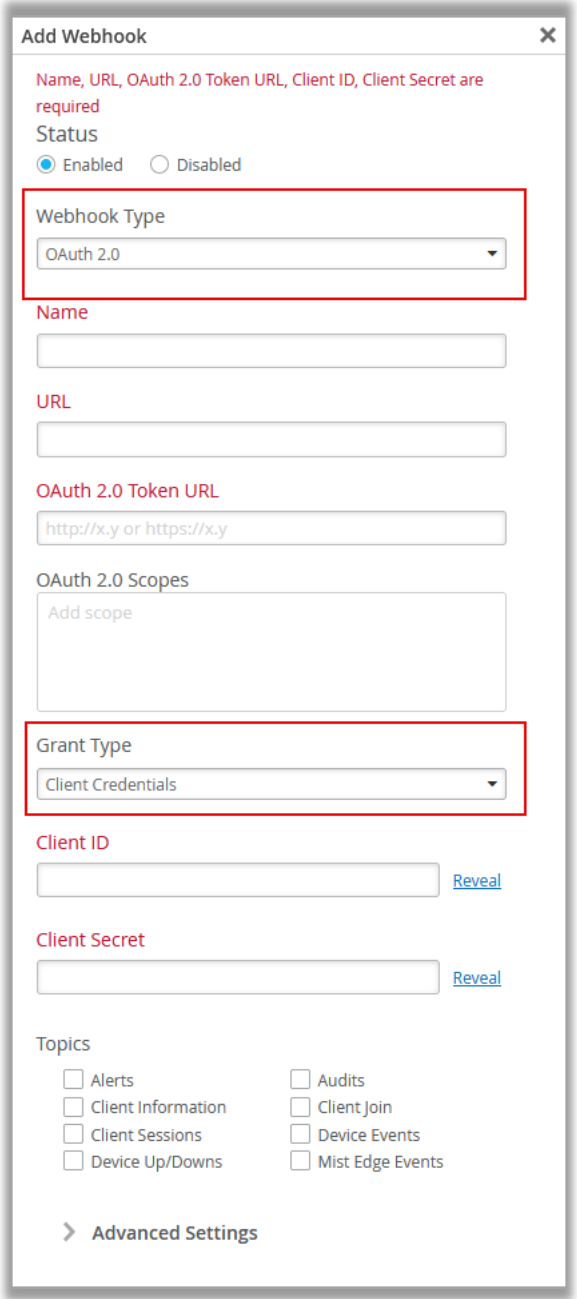

- Marvisクエリで呼び出されるスイッチリストに以下の2つの項目を追加しました（左図）
  - Role：

    スイッチの役割
  - Managed：

    スイッチがMistによって（設定を含めて）管理されているかどうか
- 追加された項目を見るにはMarvis > Marvis Actionsページの右上部にある「Ask a Question」機能を用いてMavisクエリを実行し、スイッチリストを表示させます

# Simplified Operations

# OAuth 2.0を用いたWebhook




- Webhookの認証でOAuth 2.0をサポートしました（左図）
- OAuth 2.0を有効にした場合、MistクラウドはOAuth 2.0のクライアントとして動作し、認証サーバに対して認証を行い、トークンを取得します
- トークンはWebhook認証ヘッダに追加されます
- 顧客システムからアクセストークンをリクエストする以下の2種類の方法（許可種別、グラントタイプ）をサポートしています
  - パスワード：

    顧客システム所有者のユーザ名とパスワードが必要です
  - クライアント認証：

    OAuth IDPが提供するクライアントIDとクライアントシークレットが必要です
- Webhookは組織レベル（Organization > Settings）またはサイトレベル（Organization > Site Configuration）で設定できます

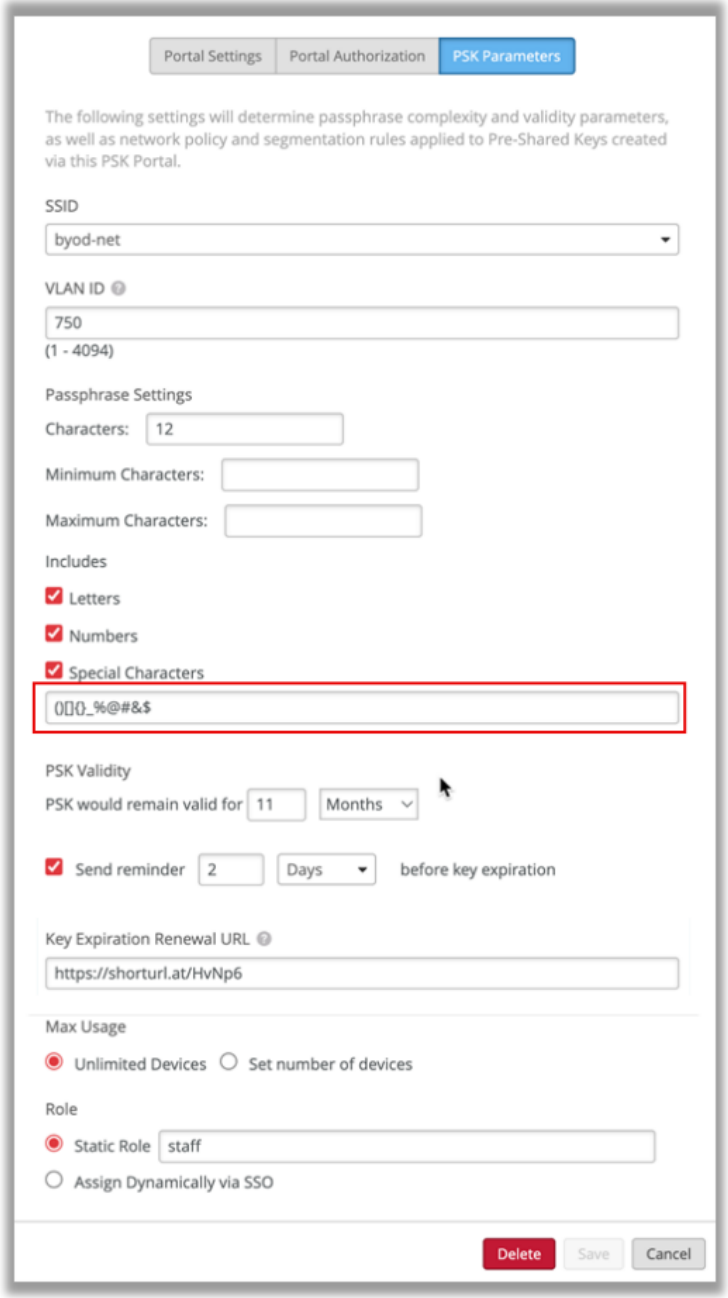
# Wireless Assurance

# 6GHz帯のチャネル割り当てロジックの改良

- 電波自動調整機能（RRM）が6GHz帯の優先スキャンチャネル（PSC）と非PSCを割り当てるようになりました
  - これまでは手動で全チャネルを有効にしないかぎり、6GHz帯のPSCのみを割り当てていました
- 異なるチャネル幅に対する6GHz帯のチャネル割り当てロジックは以下のとおりです
  - 20MHz/40MHz：
    - 全てのチャネル（PSC、非PSC含む）がプライマリチャネルとして使用されます
  - 80MHz/160MHz：
    - PSCチャネルがプライマリチャネルとして使用されます

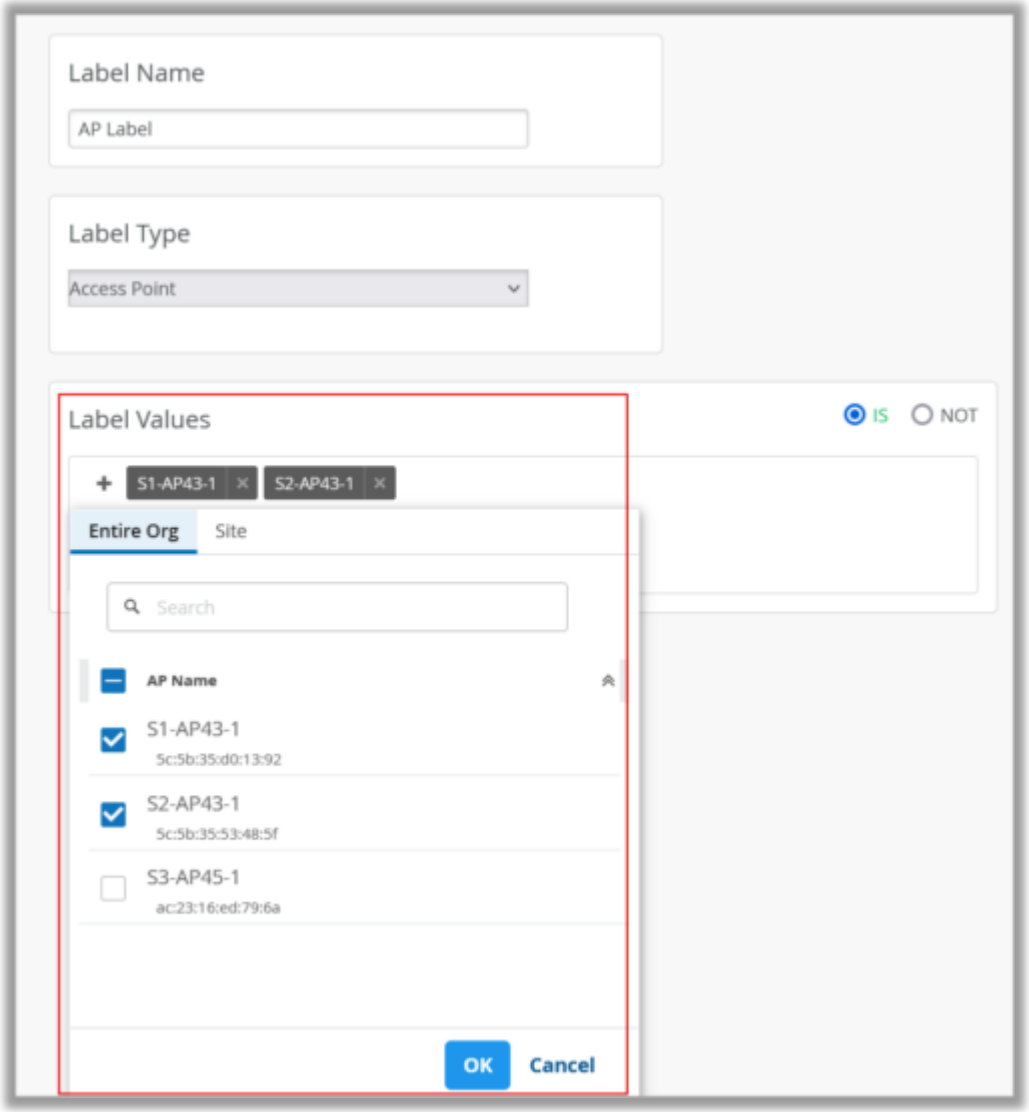
- テスト環境と広範なデプロイメントでの検証を通じて、クライアントが通常Reduced Neighbor Report (RNR)や11k Neighbor Report等のアウトバウンド方式を介して非PSCを効率的に発見することを確認したため、6GHz帯の非PSCの使用に関するガイダンスを修正するにいたりました

# PSK生成のためのデフォルトURLの上書き




- クライアントオンボーディングを使用して無線ネットワークにアクセスしているユーザの再認証に用いられるURLをカスタマイズしたものに変更できるようになりました
- ユーザが使用している事前共有鍵（PSK）の有効期限が切れる際にMistクラウドは再認証のためのURLをユーザに送信します
- 送られたURLを用いてユーザは再認証し、新規PSKを生成します
- このURLをカスタマイズしたURL（例：SSO URL）に変更することができます
- Add/Edit PSK Portalページ（Organization > Client Onboarding > Add/Edit PSK Portal）内のPSK Parametersタブにある「Key Expiration Renew URL」項目にカスタマイズされたURLを入力します（左図）
- カスタマイズされたURLを設定した場合、Mistクラウドは有効期限のお知らせメールにPSK再更新のためのカスタマイズURLを含めます（下図）
- 「Key Expiration Renew URL」項目は「Send Reminders」オプションを有効にした場合に表示されます

# アクセスポイントのラベル生成機能の拡張

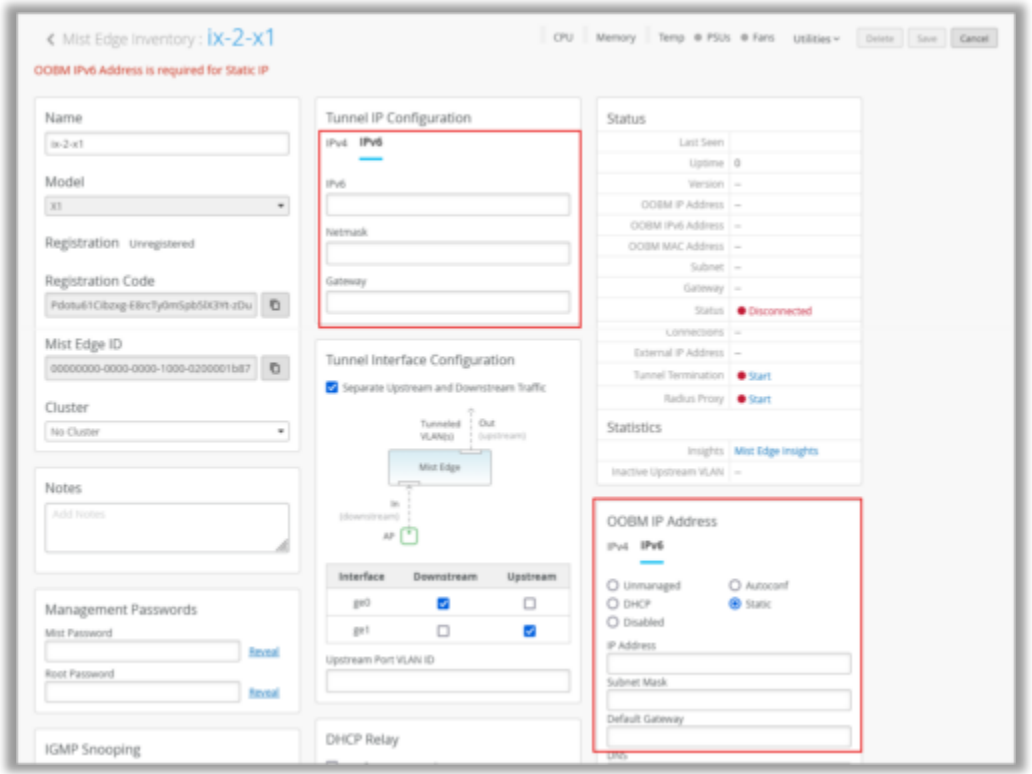



- アクセスポイント（AP）のラベル生成時に、ラベルに含めるAPを複数選択できるようになりました
- この機能はOrganizationレベル（Organization > Labels > Add Label）とサイトレベル（Site > Labels > Add Label）のAPラベル生成ページで使用できます
- ラベルに含めるAPを選択するには、「+」アイコンをクリックします
- Organizationレベルおよびサイトレベルでは、APを選択する際にMACアドレスまたはAP名でAPをフィルタリングできる検索フィルが含まれています
- Organizationレベルでは上記に加え特定のサイトまたはOrganization全体でAPを検索するオプションがあります（左図）

- APを複数選択できる機能はWLANページ（Site > WLANs > Add WLAN）やAP詳細ページ（Access Points > アクセスポイント名）でも使用することができます

# Mist Edge

# IPv6サポート

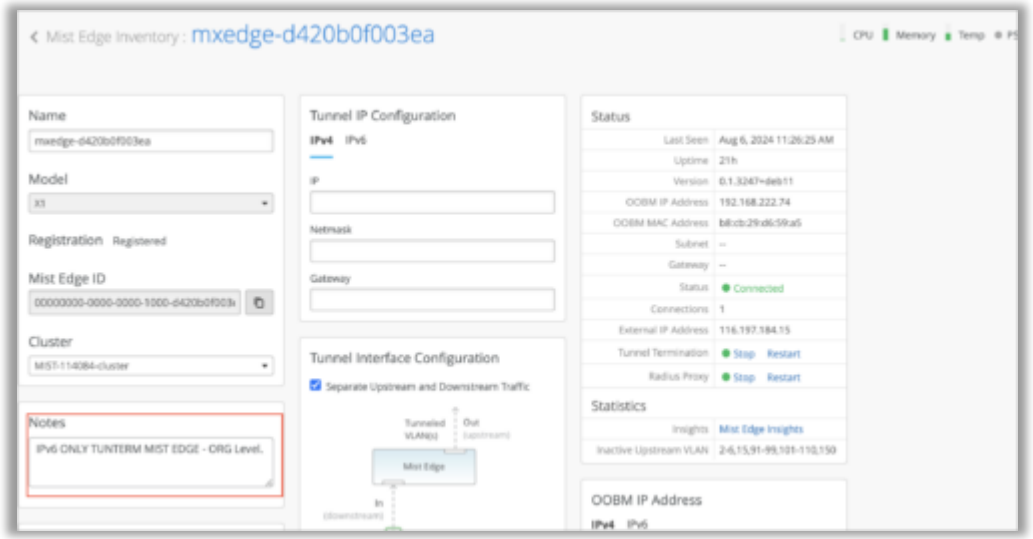



- Mist EdgeでIPv6アドレスを設定できるようになりました（左図）
- Mist Edgeの設定ページの以下のセクションでIPv6アドレスを設定できます
  - OOBM IPアドレス：
    - IPv6設定用のタブが追加されました
    - IPアドレス、サブネットマスク、デフォルトゲートウェイ、DNSを設定できます
    - IPv4またはIPv6の動的アドレス割り当てを無効にするオプションを追加しました
  - トンネルIP：
    - IPv6設定用のタブが追加されました
    - IPアドレス、サブネットマスク、デフォルトゲートウェイを設定できます
- Mist Edgeのクラスタページでは、以下の既存の設定項目でIPv6アドレスを設定できるようになりました
  - RADIUS認証サーバ
  - RADIUSアカウンティングサーバ
  - COA/DMサーバ
  - トンネル終端サービス（Tunnel Termination Service）
  - APサブネット
  - アップストリームリソースモニタリング

# IPv6サポート（続き）

- サイト設定ページ（Organization > Site Configuration）内のMistトンネルの設定でもIPv6を設定できます
- インサイト、アラート、Marvisクエリページでも以下の項目に設定されたIPv6アドレスを確認することができます
  - OOBMインタフェース
  - Mistトンネル
  - RADIUSサーバ
  - AP

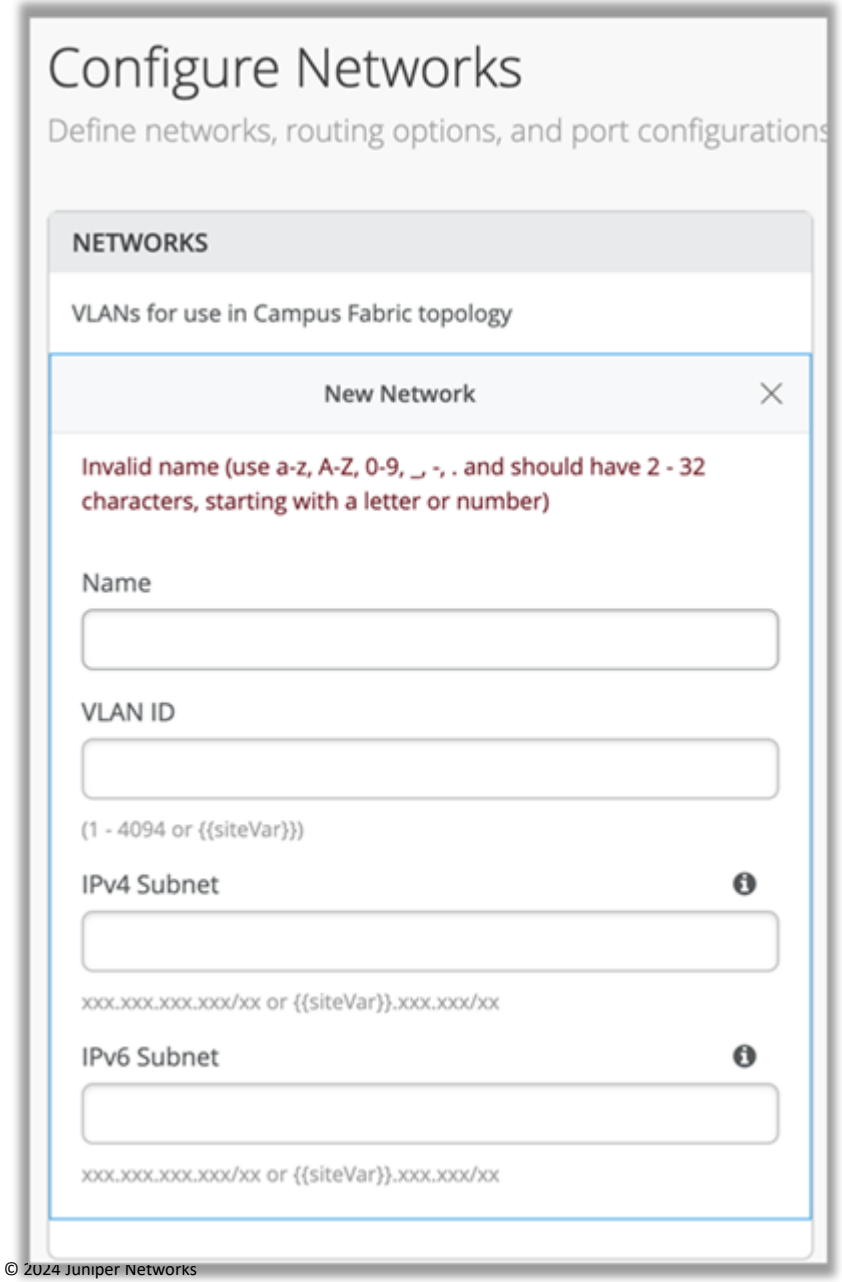
# Mist Edgeノート




- 機器固有のメモを入力するオプションが追加されました（左図）
- 機器に関する追加情報を記載することが可能です

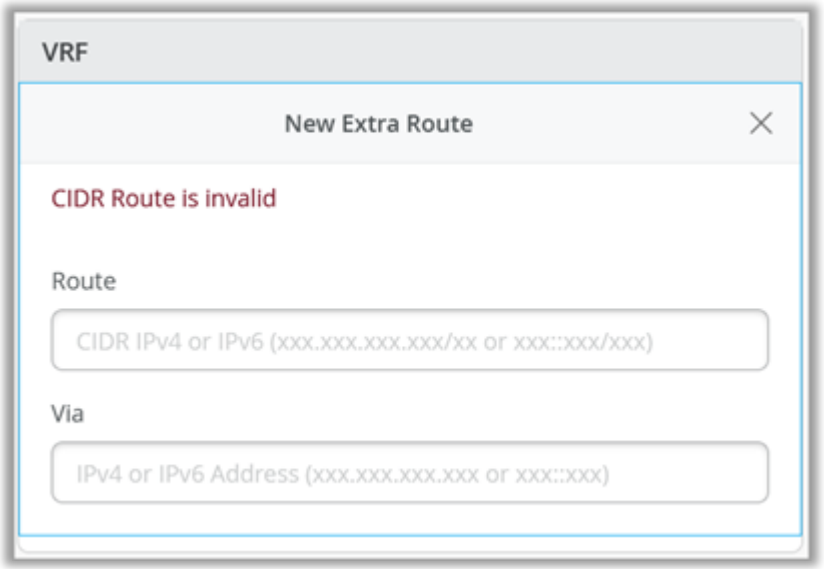
# Wired Assurance

# キャンパスファブリックでのIPv6サポート



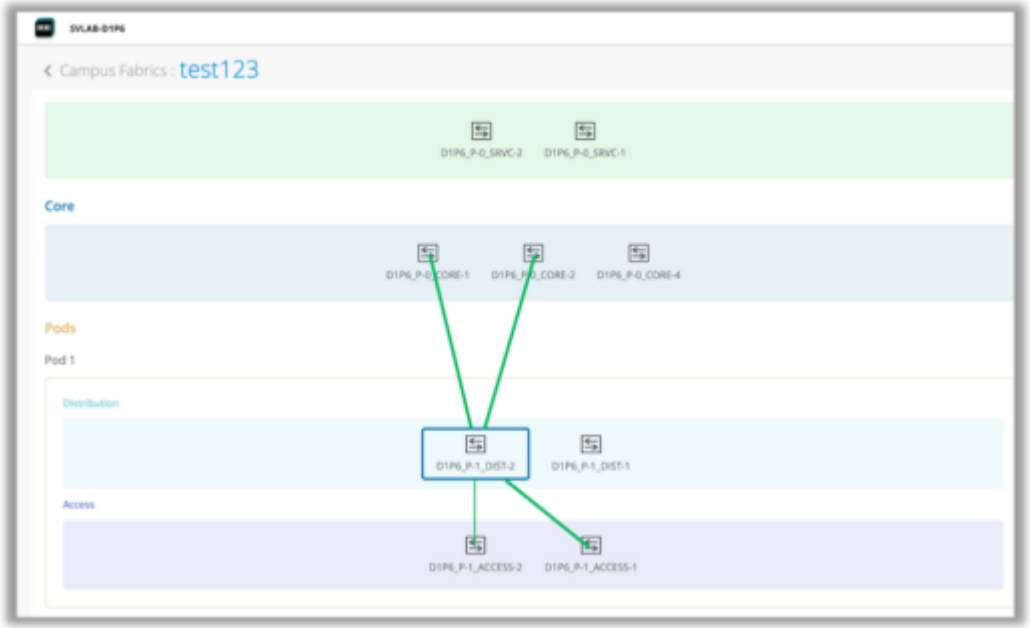

- キャンパスファブリック構成において、以下のスイッチ設定項目でIPv6アドレスを設定できるようになりました
  - ネットワーク（Networks）
  - その他IP設定（Other IP Configuration）
  - VRF
  - DCHPリレー/サーバ（DHCP relay or server）
  - 静的経路（Static Route）
    - 宛先およびネクストホップアドレスでIPv6を設定できます
  - IPおよび追加のIP設定項目（IP and Additional IP Configuration）
    - IPアドレスとサブネットマスクでIPv6を設定できます
  - ポート設定内のL3インタフェースとL3サブインタフェース（L3 interface and L3 subinterface in Port Configuration）
    - IPアドレスとサブネットマスクでIPv6を設定できます
- ネットワーク等の設定では、IPv6アドレスを設定する専用の入力フィールドがあります（左図）

# キャンパスファブリックでのIPv6サポート（続き）



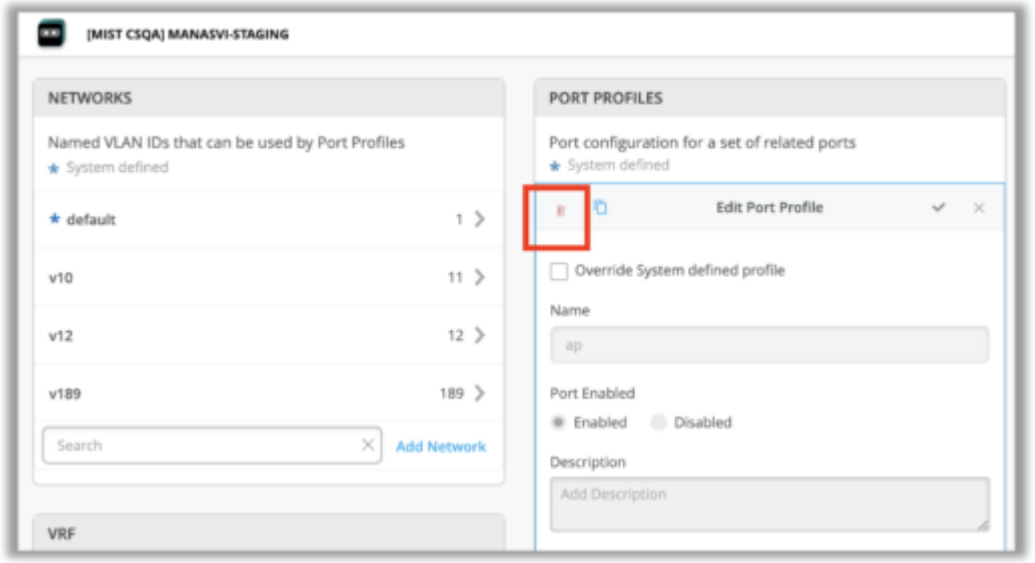

- VRF等の設定では、既存のIPアドレス設定フィールドでIPv4アドレスとIPv6アドレスの両方を設定できます（左図）
- IPv4とIPv6を両方設定したい場合、1つを設定、保存した後、もう1つを設定ください

# キャンパスファブリックにおけるスイッチ間の最小接続数の変更



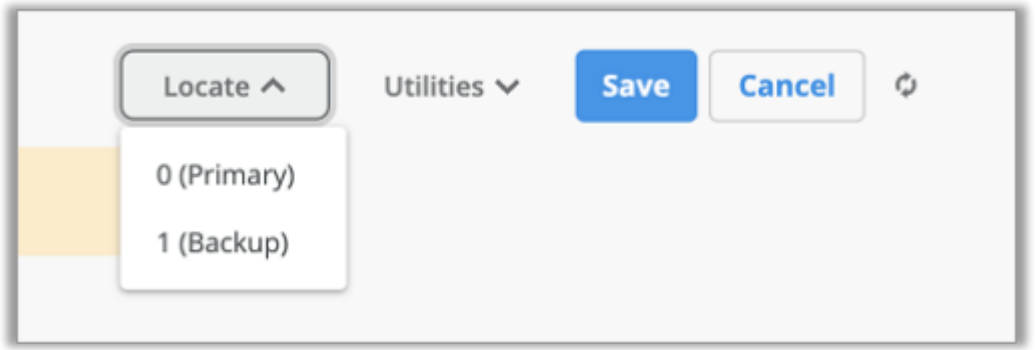

- キャンパスファブリックのメンバースイッチ間に必要な最小接続数を引き下げました
- ポッドとコアスイッチ間の接続が1本ですみます（左図）
  - これまでは、ポッド内の各ディストリビューションスイッチが全てのコアスイッチと接続する必要がありました
- コア-ディストリビューション構成（CRBまたはERB）では、各コアに対し、ディストリビューションスイッチのペア構成から1本の接続しか必要ありません
- IP Clos構成では、各コアとディストリビューションスイッチペア間、および各ディストリビューションスイッチとアクセススイッチペア間の接続は1本しか必要ありません

# システム定義のポートプロファイルの削除



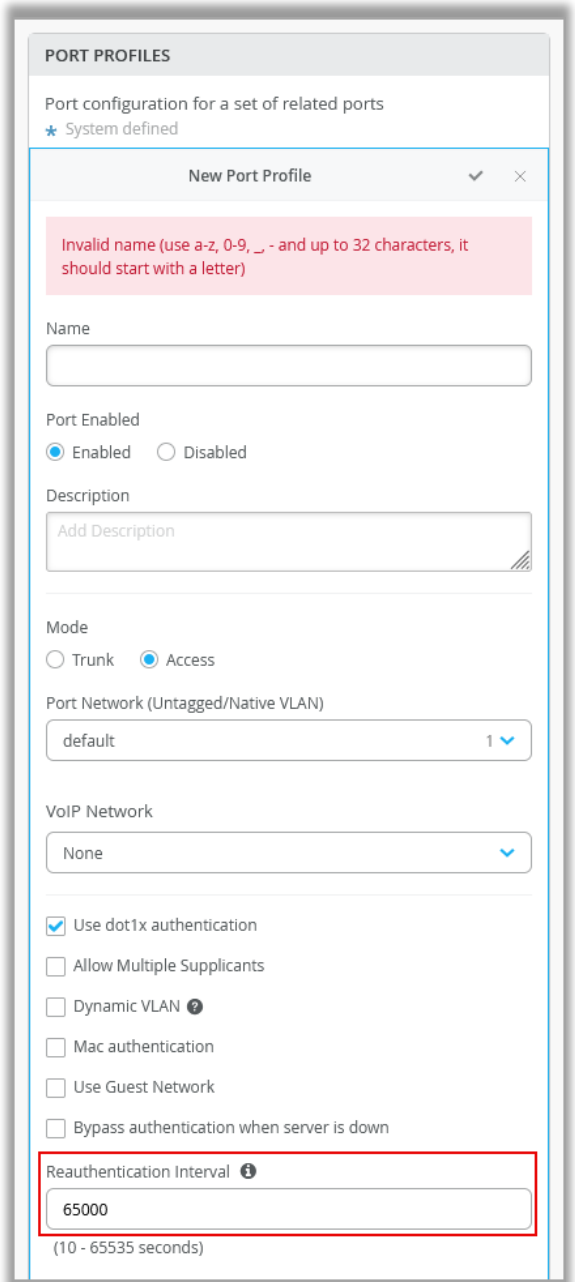

- デフォルトで存在した、以下のシステム定義のポートプロファイルが削除できるようになりました
  - ap
  - iot
  - uplink
- スイッチテンプレートで削除することができます
  - スイッチテンプレート内のポートプロファイル項目から削除したいポートプロファイルを開き、削除アイコンをクリックします（左図）
- 以下のシステム定義のポートプロファイルは削除できません
  - default
  - disabled
- 既存の設定で使用されているap、iot、uplinkプロファイルを削除した場合、defaultプロファイルに置き換えられます

# スタンドアロンスイッチとVCメンバースイッチの位置の確認



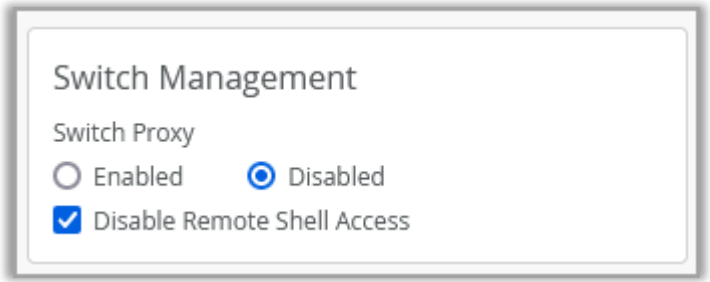

- スタンドアロンスイッチまたは仮想シャーシ（VC）メンバースイッチの物理的な場所を確認できるようになりました
- スイッチの場所を確認するには、スイッチダッシュボード（スイッチ名をクリックした後の詳細ページ）にある「Locate」ボタンをクリックします
- 「Locate」ボタンをクリックすると、スイッチのLEDが一定時間点滅します
- VCスイッチでは、プライマリ、バックアップ、またはラインカートメンバースイッチを確認できます（左図）
- 一度に位置確認できるメンバースイッチは1台のみです

# スイッチポートプロファイルの再認証間隔



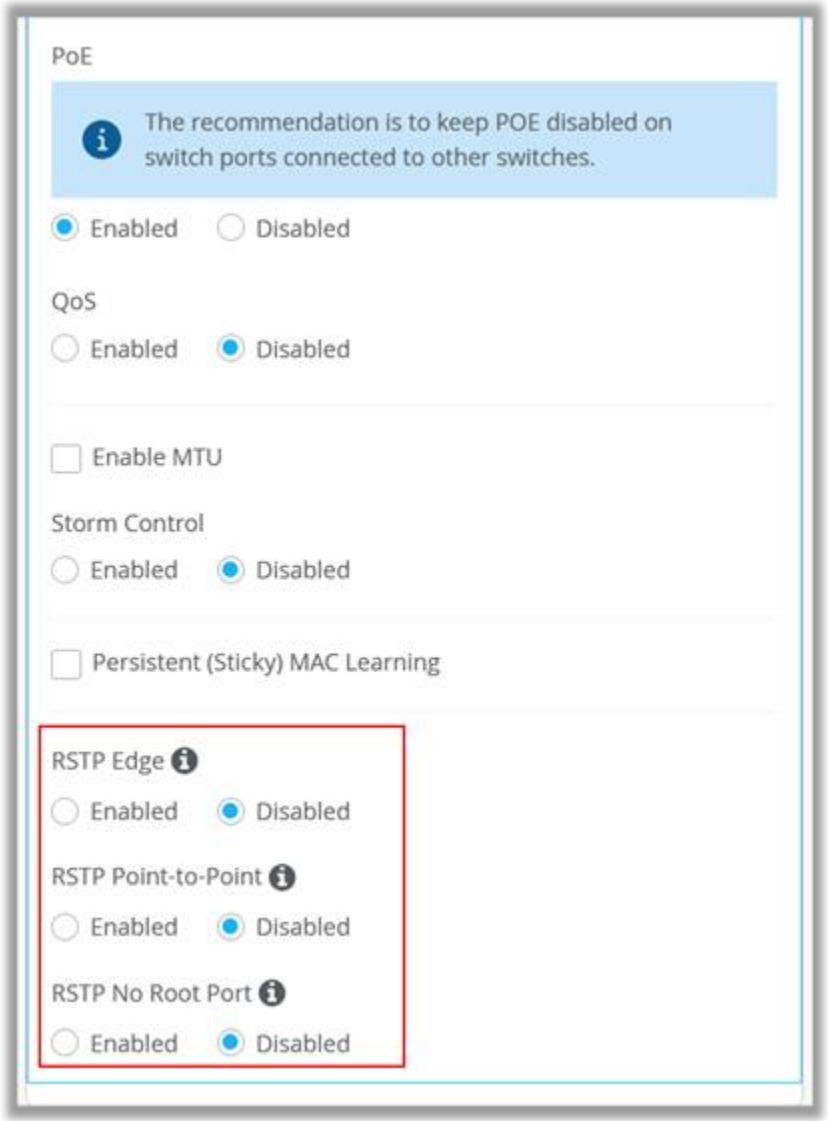

- dot1x認証を使用するスイッチポートプロファイルで、クライアントがRADIUSサーバで再認証される頻度を設定できるようになりました（左図）
- クライアントが認証されてから再認証されるまでの時間を設定できます
- 推奨値は6～12時間（21600 ～ 43200秒）です
- デフォルト値は65000秒です

# スイッチやゲートウェイ機器へのリモートシェルアクセスの無効化




- Organization内のスイッチやゲートウェイ機器へのリモートシェルアクセスを無効にすることができるようになりました
- Organizationレベルで設定が可能です
- アクセスを無効にするには、Organization ＞ Settingsページ内のSwitch Management項目で「Disable Remote Shell Access」をチェックします（左図）

# RSTPエッジポート

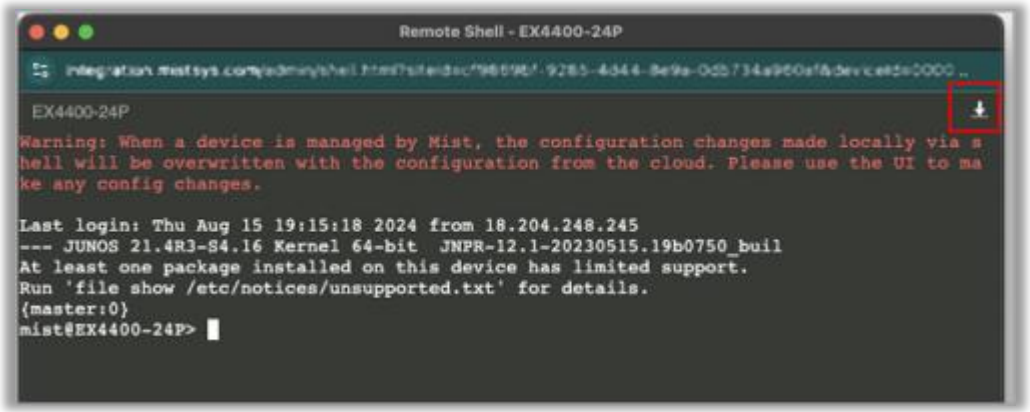



- RSTPに参加しないクライアントが接続されているポートでRapid Spanning Tree Protocol（RSTP）エッジを有効にできるようになりました
  - 接続クライアント例：
    - BPDUを送信しないはずのクライアント
      - PC
      - VoIP電話
- スイッチポートプロファイルで設定できます（左図）
- RSTPエッジを設定したポートでBPDUを受信した場合、RSTPによりブロックされます
- アップリンクポートにRSTPエッジを有効にしないでください
- RSTPエッジは基本のSTPエッジを置き換えます
- Organizationレベル、サイトレベルで以下のRSTPリンクをサポートします
  - RSTP Point-to-Point:
    - インタフェースモードをポイントツーポイントに変更します
      - ポイントツーポイント：
        - 2つのネットワークノードやスイッチ間を接続する専用リンク
  - RSTP No Root Port:
    - インタフェースがルートポートとなるのを防ぎます

# ポートリスト内でのトランシーバ情報の表示


- スイッチダッシュボード（スイッチ詳細ページ）のポートリストでポートで使用されているトランシーバの以下の情報を表示するようになりました（左図）
  - トランシーバ：
    - トランシーバの製造元
  - シリアル番号：
    - トランシーバのシリアル番号
  - トランシーバモデル：
    - トランシーバのモデル

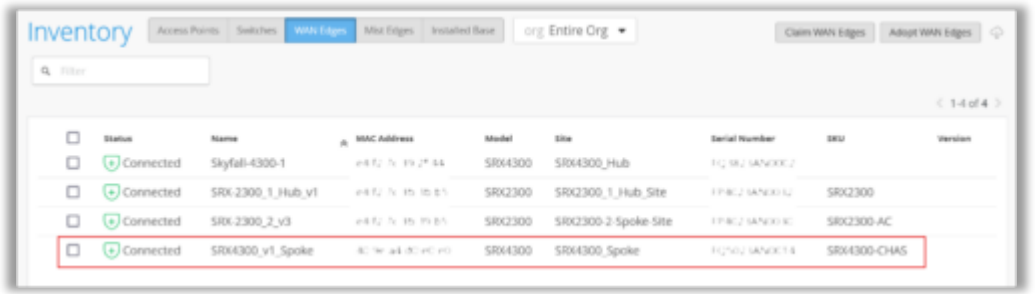
# リモートシェル経由でのスイッチログのダウンロード




- リモートシェルで実施した内容をログとしてダウンロードできるようになりました
- トラブルシューティング目的で活用できます
- ダウンロードするには、リモートシェル画面の右上にあるダウンロードボタンを使用します（左図）

# WAN Assurance

# SRX4300のサポート




- SRX4300をサポートしました
- WANエッジとして登録、設定、管理できます
- インベントリページ（Organization > Inventory > WAN Edges）にある「Adapt WAN Edges」ワークフローを使用して登録します
- 登録されたSRXはWANエッジのインベントリページとWANエッジページ（WAN Edges > WAN Edges）で表示されます（左図）
- Mistポータルでサポートされるには、SRX4300、SRX1600、SRX2300はJunos OSバージョン24.2R1.17を使用している必要があります

# ゲートウェイ帯域幅SLE（SRX）


- ゲートウェイ機器の帯域幅がしきい値を満たしているかどうかをゲートウェイ帯域幅SLEで確認できるようになりました（左図）
- ゲートウェイ機器の帯域幅がしきい値を満たさない場合、以下の分類子に問題を原因を分類します
  - アップリンクの輻輳（Congestion Uplink）：
    - アップリンクの輻輳が原因でゲートウェイ帯域幅SLEがしきい値を満たさなかった時間（パーセント）
  - 帯域幅Headroom（Bandwidth Headroom）：
    - 帯域幅ヘッドルームのしきい値を超えたことによりゲートウェイ帯域幅SLEがしきい値を満たさなかった時間（パーセント）
      - 帯域幅ヘッドルーム：
        - WANの利用可能な帯域幅を予測した値です
        - 過去14日間で最も多く使用された帯域幅を基準値としています
    - 現在の帯域幅使用量が基準値を超えた場合に帯域幅ヘッドルームの分類子に分類されます
    - SLEでは、利用率の最も高いキューがDistributionタブに表示されます

# アプリケーション経路インサイト機能の拡張


- 経路切り替えの詳細を提供するために、アプリケーション経路インサイトに以下の機能拡張を追加しました（左図）
  - 経路ステータスバー：
    - 経路の状態に関する情報をタイムライン上に表示します
    - 経路の状態に関するイベントを異なる色でハイライトします
      - 緑色：経路のアップに関するイベント
      - 赤色：経路のダウンに関するイベント
    - ハイライトされた部分にマウスのカーソルを合わせると、経路の状態に関するイベントの概要が表示されます
    - バーをクリックすると、経路の状態に関するさらなるインサイトを確認するためのイベントビューが表示されます
  - 経路状態イベントの概要：
    - アプリケーション経路インサイトの左側に直近の経路の状態に関するイベントの概要を表示します
  - アクティブ、インアクティブポリシーの表示：
    - 「Policies」ドロップダウンリストに選択した時間範囲のアクティブポリシー（トラフィックが発生したポリシー）とインアクティブポリシー（トラフィックが発生しなかったポリシー）が含まれます

# カスタムアプリケーションのヘルスチェック（SSR）


- カスタムアプリケーションのヘルスSLEデータのみを表示できるようになりました（左図）
  - 例：

    POS機器をカスタムアプリケーションとして登録した場合、POS機器に対するアプリケーションヘルスを確認することができます
- カスタムアプリケーションのヘルスSLEのみを表示するには以下の手順を実施します
  1. Monitor > Service LevelsのWANタブをクリック
  2. SLE項目の上部にある「Show Custom Apps」をクリックして機能をオンにします（青色）
- 全てのアプリケーションのデータを表示させたい場合は「 Show Custom Apps」をクリックして機能をオフにします（グレー）

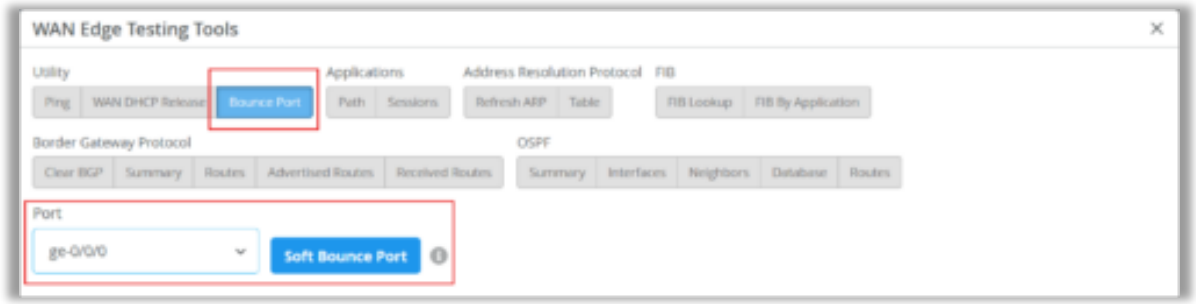
# セッションテストツール機能の拡張（SSR）

- WANエッジ機器のトラブルシューティングを支援するために、セッションテストツール機能を拡張しました
- セッションの詳細を表示します
- 必要に応じてセッションを削除することができます

# アプリケーションポリシー適用回数の表示


- WANエッジ機器ページのアプリケーションポリシー項目で、各ポリシールールが適用された回数を表示できるようになりました（左図）
- 今回の新機能リリース時点では、SRXシリーズでのみ本機能が利用可能です
- 将来的にSSRシリーズへも適用予定です

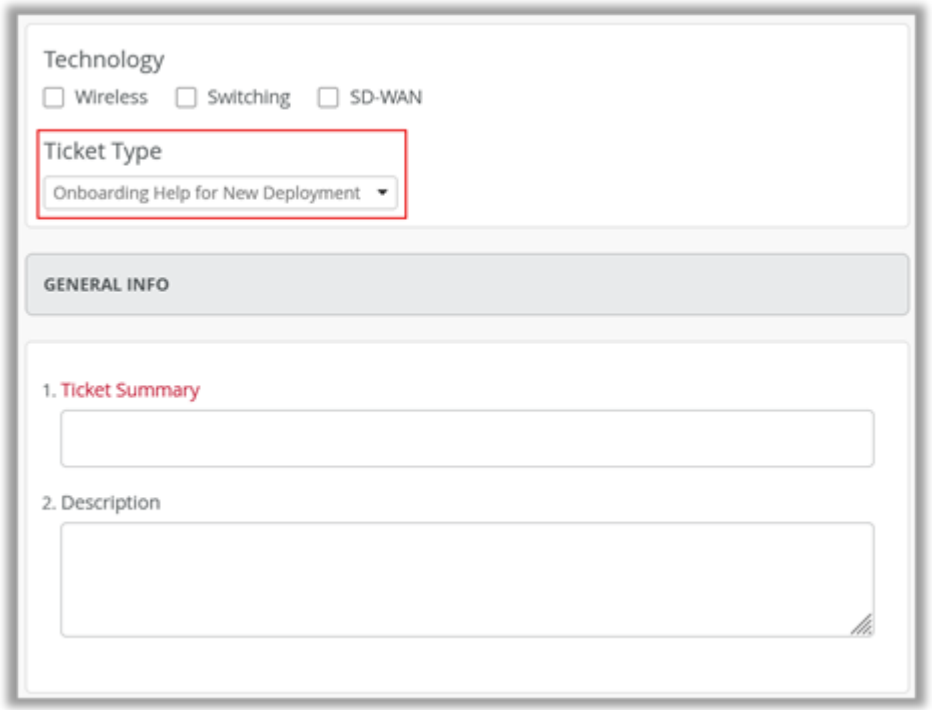
# ポートリセットテストツール（SSR）




- SSRのポートをソフトリセット（Bounce Port）するテストを実施できるようになりました（左図）
- ソフトリセットのテストでは、一時的にポートをダウンさせ、その後アップさせることで機器内部でのポートの状態を変化させます
- ソフトリセットによって外部の物理リンクの状態が変更されることはありません
- SSRに接続された機器はリンクの状態変化を認識することはありません
- ソフトリセットする手順は以下となります
  1. WANエッジ機器ページ上部の「Utilities」ボタンから「Testing Tools」をクリックします
  2. 「Utility」の項目で「Bounce Port」を選択します
  3. 「Port」項目でソフトリセットしたいポートをリストから選択し、「Soft Bounce Port」をクリックします

# Support

# 新規導入に関するサポートチケット分類の追加




- 「新規導入のためのオンボーディングヘルプ（Onboarding Help for New Deployment）」という新規サポートチケットの分類を追加しました（左図）
- Juniper Mistをご利用のお客様はこのチケット分類を使用して、円滑な導入を目的とした初期セットアップ、設定、基本的なトラブルシューティングに関するサポートをリクエストできます
- このチケット分類は以下の技術分野に関して使用できます
  - 無線（Wireless）
  - スイッチング（Switching）
  - SD-WAN
- このチケット分類の対応範囲には、ネットワーク設計関連のサポートは含まれません
- このチケット分類はサポートが必要となる少なくとも48時間前までにケースオープンする必要があります


Thank you
JUNIPER
driven by Mist AI