2024年3月29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/march-29th-2024-updates/

本ドキュメントは2024年3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）

Simplified Operations
- Mistポータルの多言語化対応
- Super Observer権限
- 英国への新規クラウドインスタンス
- ゲストポータル利用者の個人データ保存に明示的な許可を求めるオプション
- アクティベーション前のサブスクリプションの移動（MSPポータル）

Marvis
- Marvisクエリ言語でのMist Edgeサポート

Wireless Assurance
- WPA3-Enterprise 192ビットセキュリティ
- クライアントへの割り当てVLAN設定の上書き
- 承認SSIDへのワイルドカード使用

Wired Assurance
- スイッチ管理専用のVRFインスタンス（Out of Band）
- スイッチテンプレートでのインバンド管理ネットワーク設定
- VRFサブネット毎のループバック要件の変更
- サイトレベルのキャンパスファブリックでのポッド構成
- 802.1X認証でのダイナミックVLAN割り当て
- 専用ボーダーノードを持つIP Clos構成でのシングルコアスイッチのサポート
- ポートリストへのトランシーバ列の追加

本リリースで追加された機能一覧（2/2）

WAN Assurance

- WANエッジでのOSPFのサポート
- VRFルートリーク
- WANリンク速度のテスト（SSR）
- WANエッジポートの無効化
- サイト変数をサポートする項目の明確化

Behavior Changes

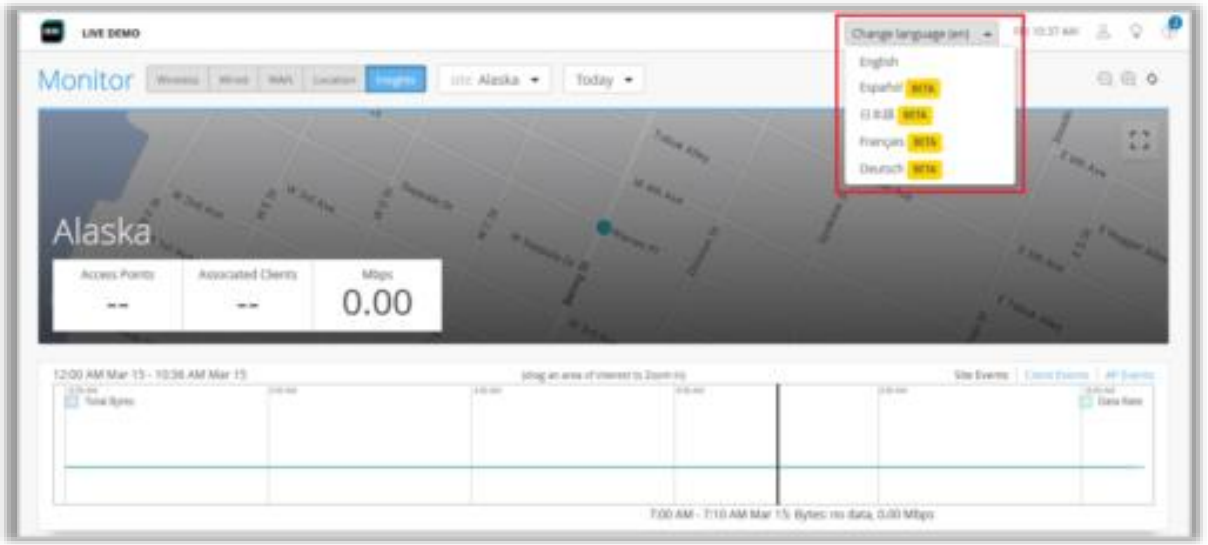
- サイトレベルでのユーザ権限継承の変更
- /self APIの変更（MSPユーザ）

Feature Deprecation

- Webhookトピックasset-rawの廃止

Simplified Operations

Mistポータルの多言語化対応



- Mistダッシュボードの利便性向上のため、Mistポータルが複数の言語に対応しました
- 現時点では英語に加え、以下の言語に対応しています
  - 日本語
  - ドイツ語
  - フランス語
  - スペイン語
- Mistポータルの言語ドロップダウンリストから言語を選択できます（左図）

Super Observer権限

図1

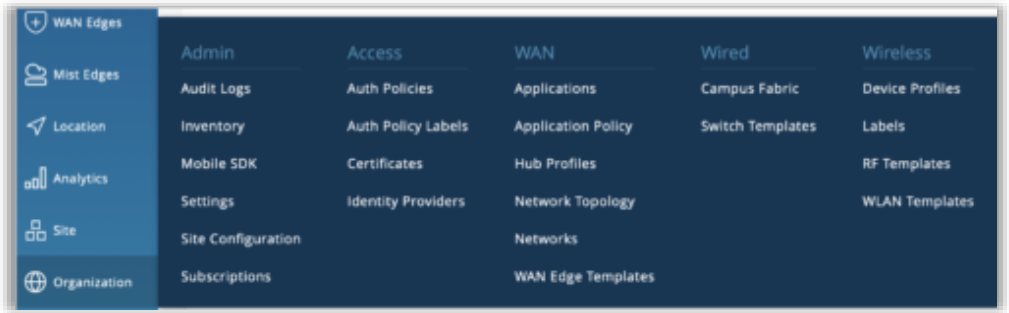


図2

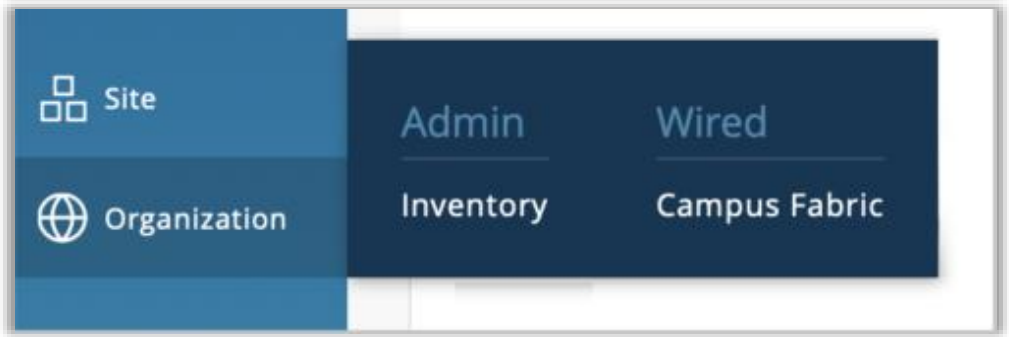
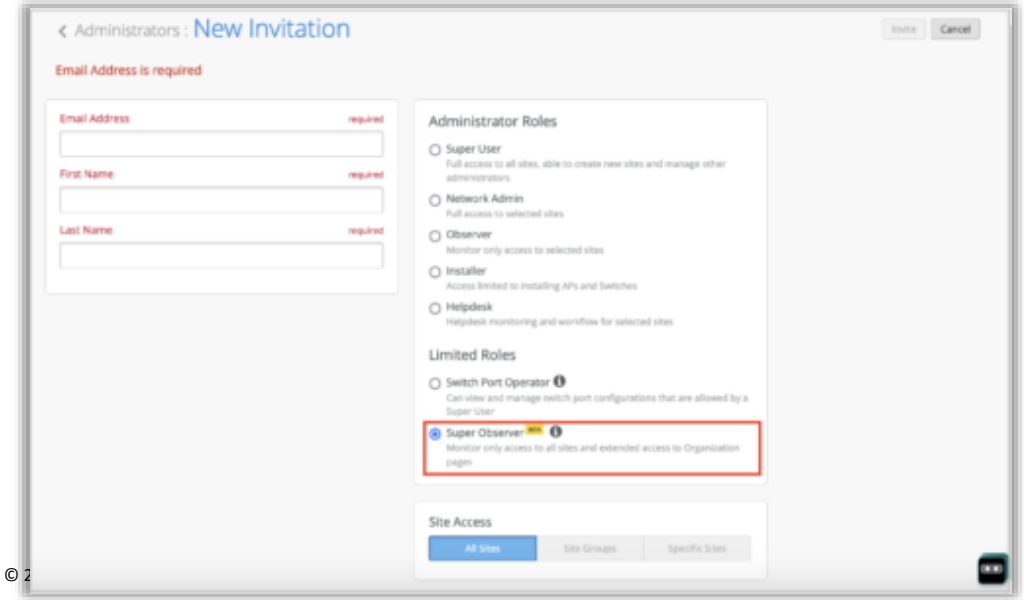


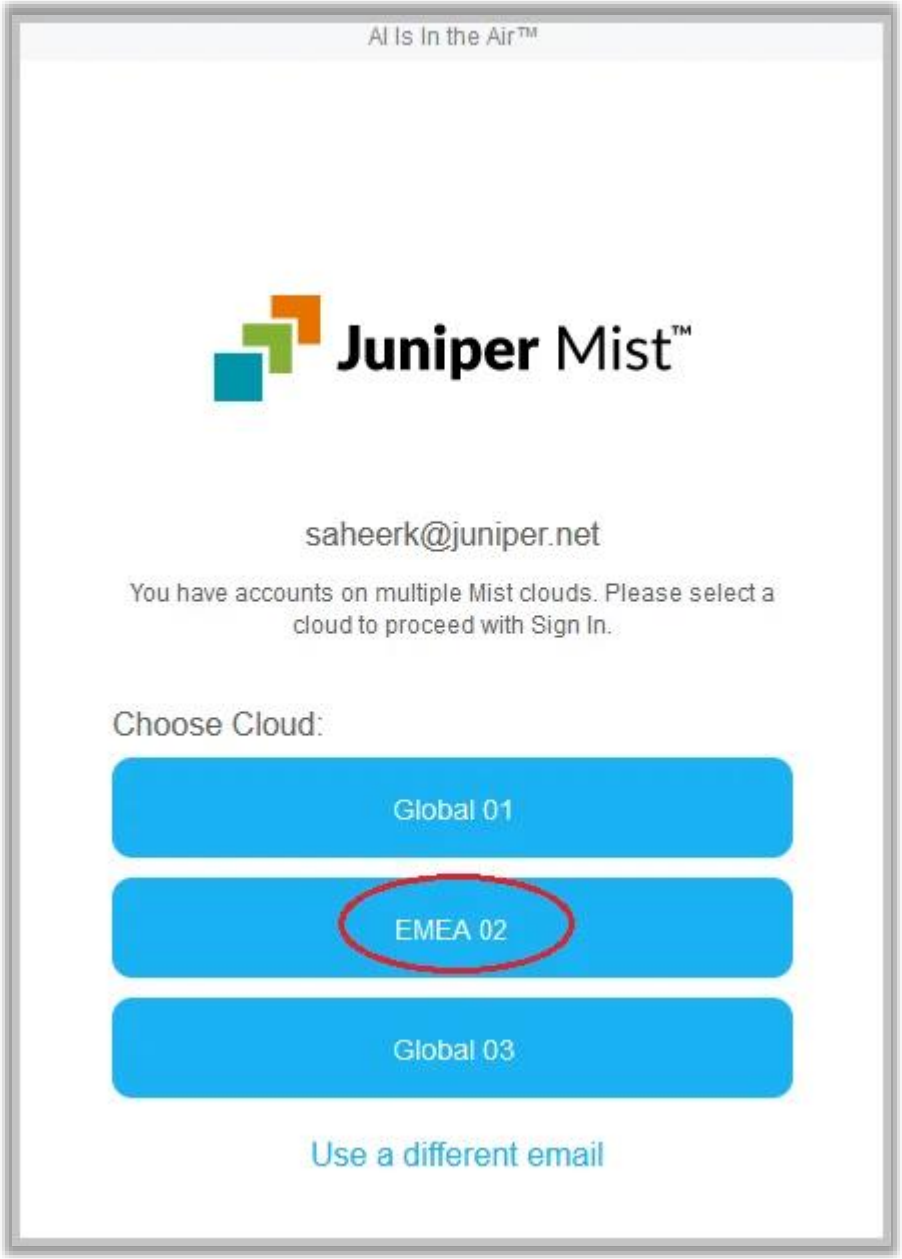
図3



- Organizationタブ配下にあるテンプレートやその他のページを含む、Organization全体（全サイト）の情報を閲覧できるアクセス権限となる、Super Observerという権限を追加しました
- この権限はObserverの権限を拡張したものになります
  - Observer：

    サイトレベルのページ（アクセス権限があるサイトのみ）、インベントリ、キャンパスファブリックページ（全サイトへのアクセス権限がある場合のみ）へのアクセスが可能な権限
- Super ObserverはObserverと同じレベルのAPIアクセス権限を持っています
- Super ObserverはAdministratorsページへのアクセス権限はありません
- Super ObserverはAdministratorsの除くAdmin列、Access列、WAN列、Wired列、Wireless列の内容を閲覧することができます（図1）
- Observerが閲覧できるOrganizationタブは図2となります
- Super Userの権限を持つユーザがNew Invitationページ（Administrators > Invite Administrators）でユーザにSuper Observerの権限を付与することができます（図3）

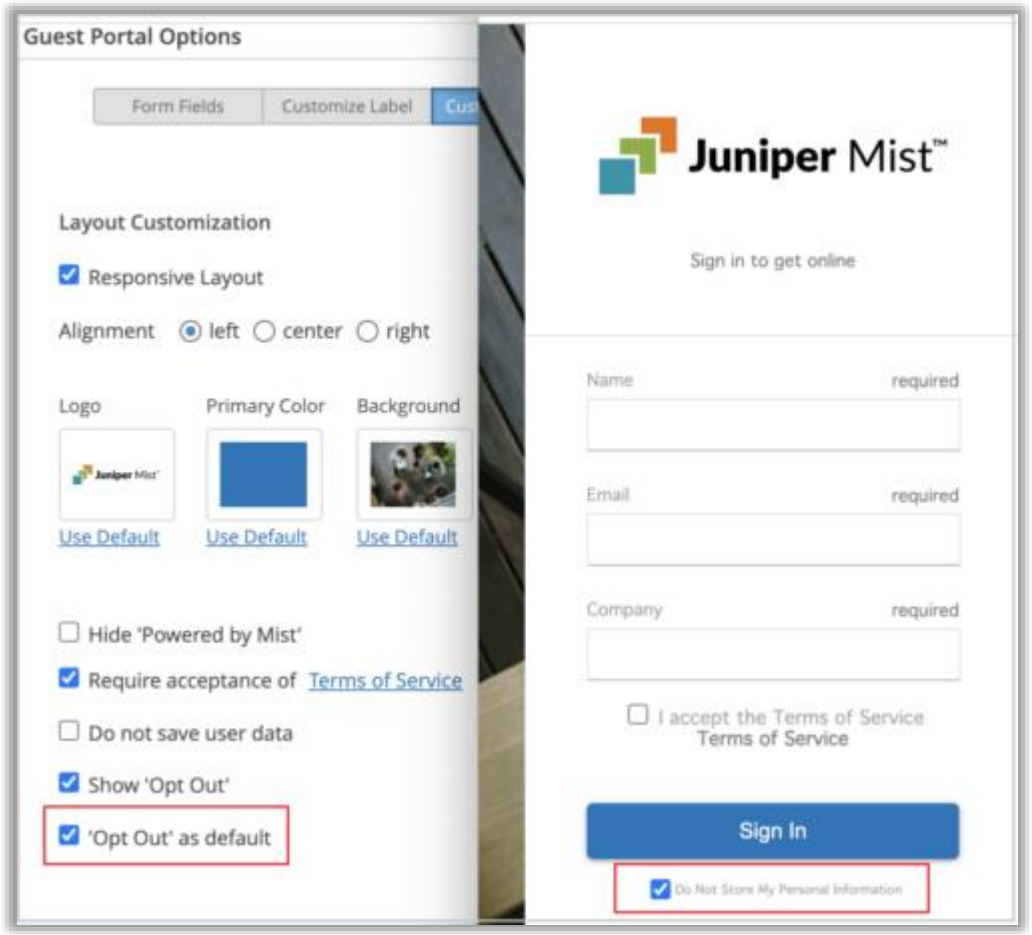
英国への新規クラウドインスタンス



- 英国に新しいMistクラウドインスタンスを追加しました
- 新しいクラウドインスタンス名はEMEA 02となります（左図）
- これまでEurope 01という名称だったクラウドインスタンスはEMEA 01という名称に変更になりました
  - Mistログインページのクラウド選択画面ではEMEA 01と出力されます
- Mistクラウドの詳細に関しましては以下のページをご覧ください

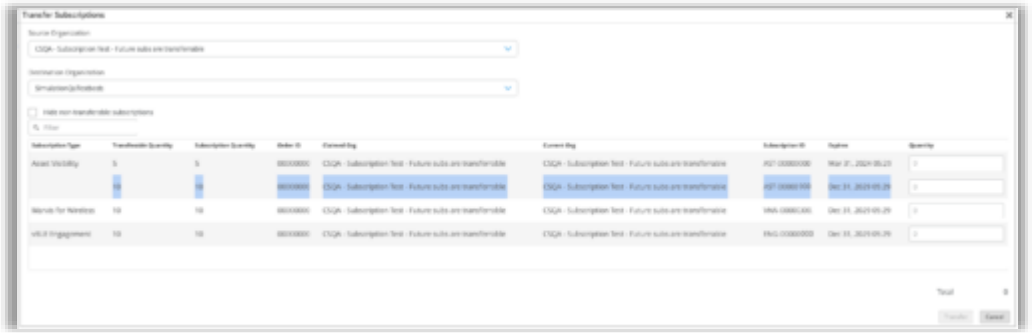
  https://www.juniper.net/documentation/us/en/software/mist/mist-management/topics/ref/firewall-ports-to-open.html

ゲストポータル利用者の個人データ保存に明示的な許可を求めるオプション



- ユーザの明示的な許可無しでユーザの個人情報が保存されないように、Mistゲストポータルを設定できるようになりました
- WLANsのカスタムゲストポータル設定ページのCustomize Layoutタブ内の「'Opt Out' as default」を選択します（左図）
- 「'Opt Out' as default」を選択すると、ゲストログインページで「Do not store my personal information」がデフォルトで選択されるようになります（左図）
- ユーザがポータルに入力した情報を保存させたい場合は、明示的にチェックボックスからチェックを外す必要があります
- 「'Opt Out' as default」項目は「Show 'Opt Out'」項目を選択した場合に出力されます
- 「Show 'Opt Out'」のみを選択した際にユーザが個人データの保存を望まない場合は、ユーザは明示的に「Do not store my personal information」をチェックする必要があります

アクティベーション前のサブスクリプションの移動（MSPポータル）

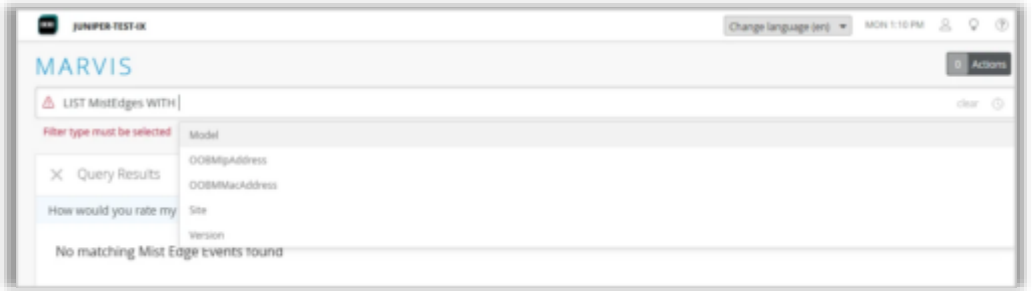


- MSPダッシュボードで管理者ユーザが、アクティベーション前のサブスクリプションをOrganization間で移動できるようになりました（左図）
- MSPポータルのOrganizationページ内にある「Transfer Subscription」オプションでサブスクリプションの移動が可能です
- 移動したいサブスクリプションの数を入力するとTransferボタンがクリックできるようになります
- 移動できる数やサブスクリプション数を超えた数を入力すると、Transferボタンは無効のままとなります
- 以下のページも併せてご覧ください

  https://www.juniper.net/documentation/us/en/software/mist/mist-msp/topics/task/transfer-subscriptions.html

Marvis

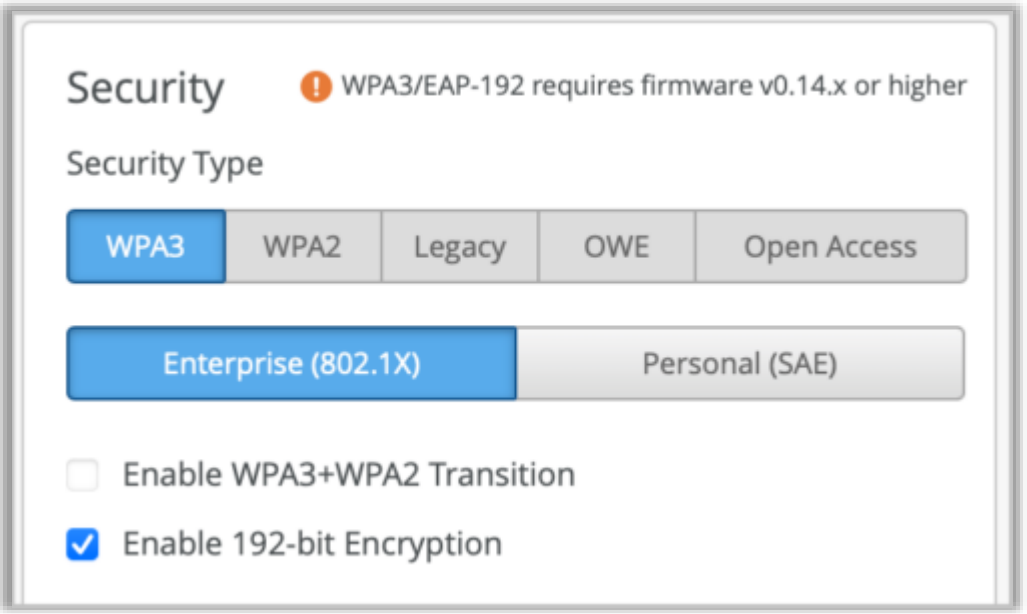
Marvisクエリ言語でのMist Edgeサポート



- Marvisクエリ言語でMist Edgeをサポートしました
- Marvisクエリ言語を用いてMist EdgeやMist Edgeに関連したイベントを確認することができます
- Marvisクエリ言語でサポートされているMist Edge関連のクエリは以下となります
  - OOBM IPアドレス、OOBM MACアドレス、モデル、サイト情報、バージョンを用いたMist Edgeの検索、リスト表示
  - サイト、Mist Edge名、Mist Edgeイベントの種類を用いたMist Edgeイベントの検索、リスト表示
  - Mist Edge名/ID、MXトンネルのUp/Downを用いたAPの検索、リスト表示
  - OOBM IPアドレス、OOBM MACアドレス、モデル、サイト情報、バージョンを用いたMist Edge数のカウント
  - サイト、Mist Edge名、Mist Edgeイベントの種類を用いたMist Edgeイベント数のカウント
  - Mist Edge名/IDを用いたAP数のカウント
  - トンネル数によるMist Edgeのランキング
  - Mist Edgeイベント数によるMist Edgeのランキング
  - バージョン別のMist Edge数ランキング
  - モデル別のMist Edge数ランキング
- クエリを開始するにはMarvisページの右上部にある「Ask a Question」をクリックします（左上図）
- 左下図がMarvisクエリでMist Edgeを調査する例となります

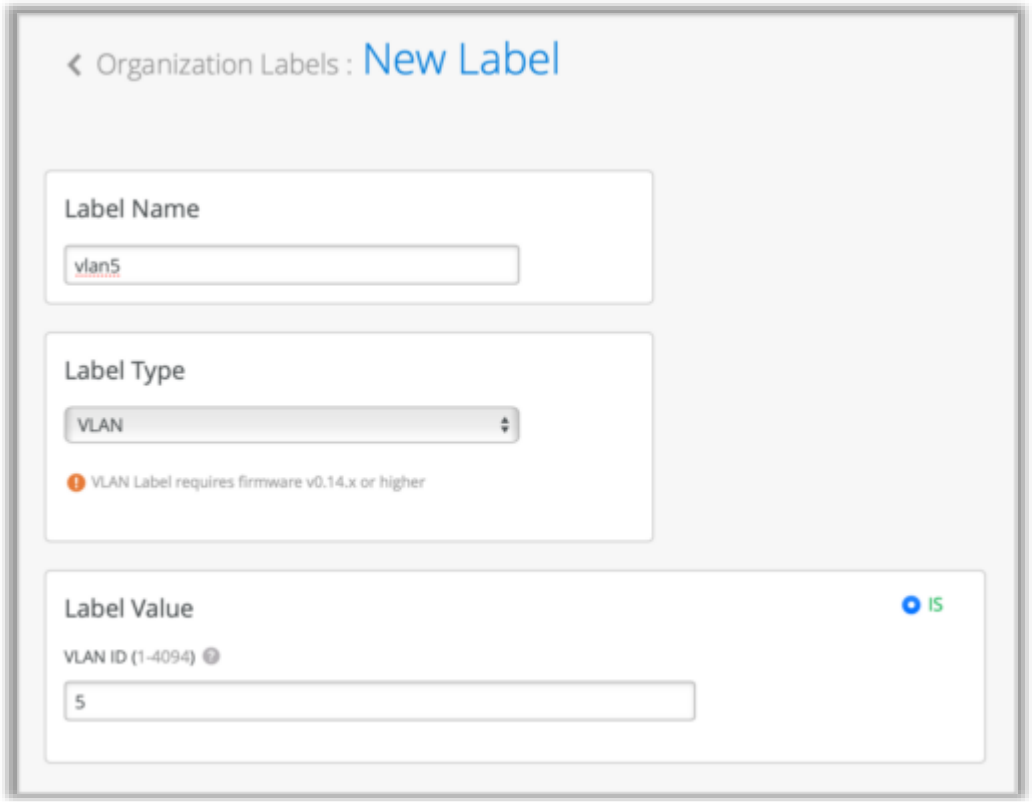
Wireless Assurance

WPA3-Enterprise 192ビットセキュリティ



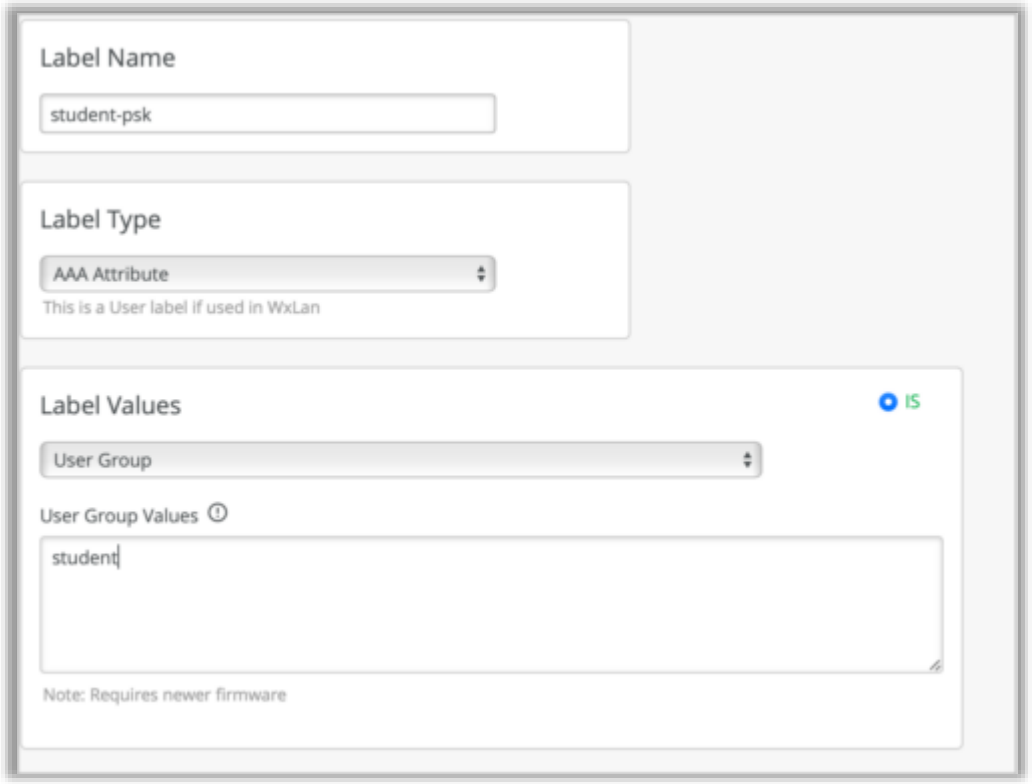
- WLANセキュリティにWPA3-Enterprise 192ビットセキュリティを追加しました
- この設定ではGCMP-256の暗号化と、より安全な証明書を必要とすることで、最高レベルの802.1Xセキュリティをwi-Fiで提供します
- サイト、またはWLANテンプレート内のセキュリティ項目でWPA3-Enterpriseを設定し、「Enable 192-bit Encryption」をチェックすることで設定できます（左図）
- WPA3-Enterprise 192ビットセキュリティでは、移行モード（transition mode）と802.11r高速ローミングはサポートしないのでご留意ください
- RADIUS側で必要な要件は以下となります
  - EAP-TLSを使用します
    - WPA3-Enterprise 192ビットセキュリティ使用時にAccess AssuranceではEAP-TLSをサポートします
  - 以下のいづれかのEAP暗号を使用します
    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- WPA3-Enterprise 192ビットセキュリティを使用するには、アクセスポイントは0.14.29091以降のファームウェアバージョンを使用する必要があります
- より高いセキュリティが必要で、デバイス側でのサポートが確認されている場合に、WPA3-Enterprise 192ビットをデフォルトとすることを推奨します
- WPA3-Enterprise 192ビットの欠点としては802.11r高速ローミングできない点となります

クライアントへの割り当てVLAN設定の上書き



- クライアントVLANを上書きするWxLANポリシーを設定できるようになりました
- 想定している使用ケースは、mPSKでサイト毎にVLANを柔軟に設定する場合です
  - 例：
    - サイトAではPSK AにVLAN A、PSK BにVLAN Bを使用
    - サイトXではPSK AにVLAN X、PSK BにVLAN Yを使用
- WxLANポリシーを使用することにより、AAA属性のユーザグループラベルを使用するPSKの役割に基づいてクライアントへVLANを割り当てることができます
- WxLANによるVLAN割り当ては、RADIUSから受信したダイナミックVLANによるクライアントへのVLAN割り当て等、その他のVLAN割り当ての設定を上書きすることができます
- 本機能を使用するには、WxLANポリシーで割り当てるVLANが既にWLAN設定に存在する必要があります
- 以下の手順で設定が可能です
  1. Label Type にVLANを用いてWxLANポリシーラベルを作成します（Organization/Site > Labels > Add Label）（左図）
     - VLAN IDを指定する必要があります
     - Organizationラベルを作成する場合、「{{*}}」形式のVLAN変数を使用し、サイトレベル、またはデバイスプロファイルレベルで変数を解決することができます

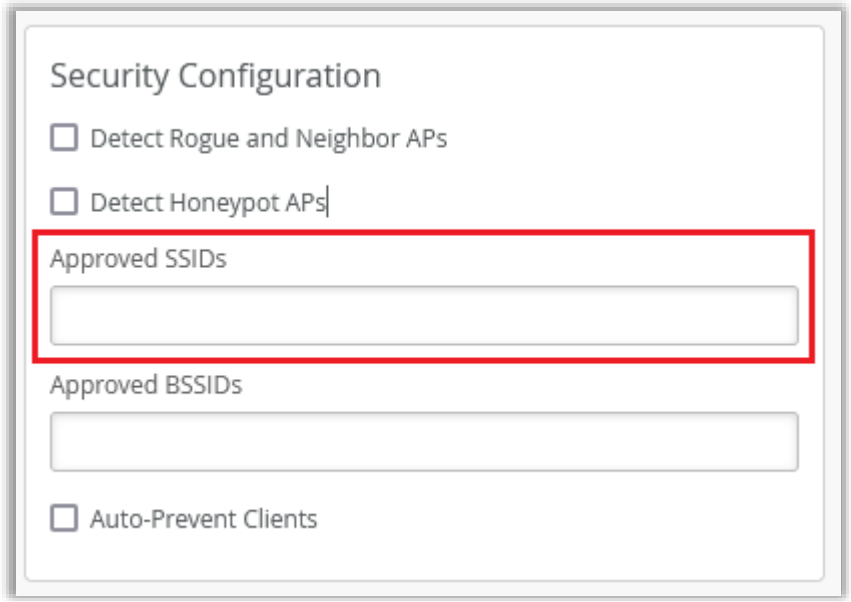
クライアントへの割り当てVLAN設定の上書き（続き）



2. PSKの役割に一致するAAA属性のユーザグループラベルを作成します（左上図）
   - クライアントラベルも作成できますが、規模に応じてAAA属性のラベルを使用することを推奨します
3. WxLANポリシーを作成し、 Resourceフィールドに VLANラベルを追加します（Organization > WLAN Templates > Policy、またはSite > Policy > Add Rule）（左下図）
   - ポリシーに一致するユーザは指定されたVLANに割り当てられます

- 本機能はRADIUS AVP（Tunnel-Private-GroupIdやAirespace-Interface-Name）やmPSKに設定されたVLANなど、ポリシーによってユーザにVLANを割り当てる通常の方法に加えて使用することができます
- 本機能を使用するにはアクセスポイントのファームウェアバージョンが0.14.29091以降である必要があります

承認SSIDへのワイルドカード使用



- 「Approved SSID（承認されたSSID）」項目でワイルドカードと部分一致を使用できるようになりました（左図）
  - Approved SSID（承認されたSSID）：

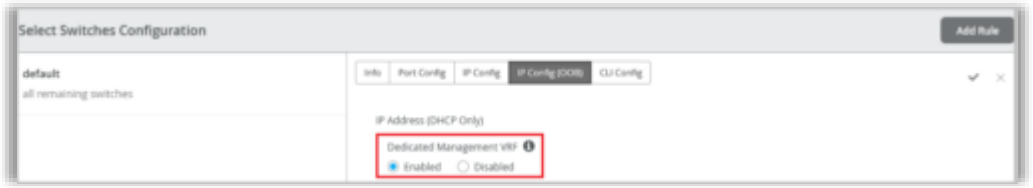
    サイト設定（Organization > Site Configuration）内のセキュリティ設定となり、ここに入力したSSIDは不正SSID、ハニーポット検出から除外されます
- 同じSSID命名規則を使用している複数のSSIDがある場合に有効な機能となります
  - 例：

    SSID「DIRECT-roku-755-22DDFF」を承認したい場合：

    「Approved SSID（承認されたSSID）」に「direct*」のみを入力するだけで、「direct」から始まる全てのSSIDが承認されます
- 「Approved BSSID（承認されたBSSID）」では既に部分一致がサポートされています
  - 例：「cc-73-*」、「cc:82:*」など

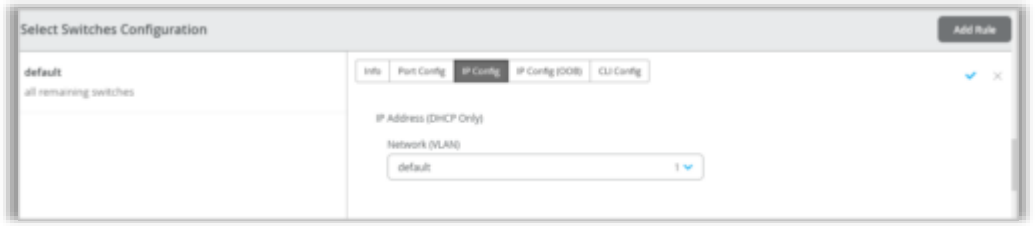
Wired Assurance

スイッチ管理専用のVRFインスタンス（Out of Band）



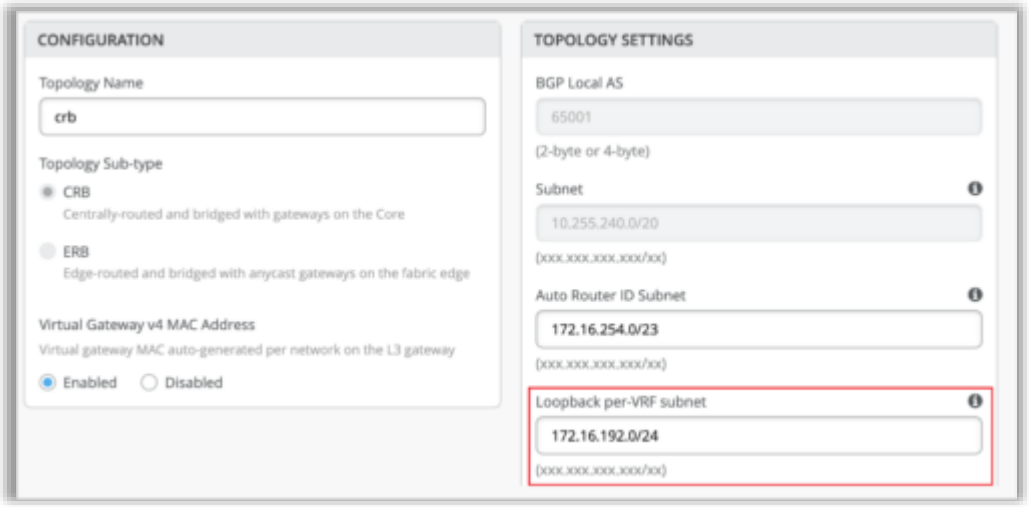
- 管理専用のVRF（Virtual Routing and Forwarding）を設定できるようになりました
- 本機能を有効にすると、管理インタフェース（em0/me0/fxp0、vme）がデフォルト以外のVRFインスタンス内に限定されます（左図）
- Junos OSバージョン21.4以降で起動しているスタンドアロンのスイッチとVC（仮想シャーシ）システムで使用できます
- 管理専用のVRFにより、管理トラフィックは他の管理トラフィックやプロトコルのトラフィックとルーティングテーブルを共有する必要が無くなります
  - デフォルトではインバンドのプロトコルの管理トラフィックを含め、すべてのトラフィックがinet.0ルーティングテーブルを用いています
- 以下のいづれかの項目で管理専用VRFを設定できます
  - Organizationレベル（Organization > Switch Templates）のスイッチテンプレート内の「Select Switches Configuration」項目内にある「IP Config（OOB）」タブ
  - サイトレベル（Sites > Switch Configuration）のスイッチテンプレート内の「Select Switches Configuration」項目内にある「IP Config（OOB）」タブ
  - スイッチ詳細ページ（Switches > スイッチ名）

スイッチテンプレートでのインバンド管理ネットワーク設定



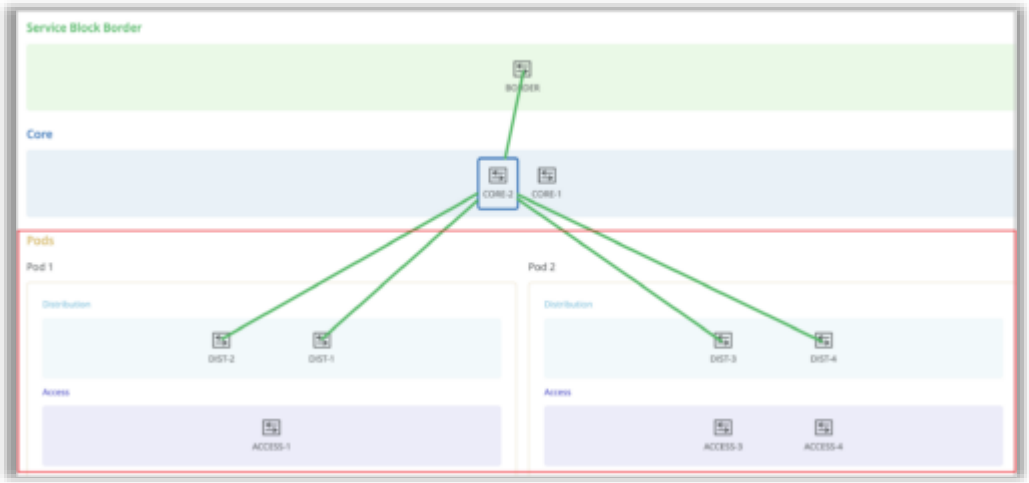
- インバンドの管理トラフィックを設定できるようになりました
- 以下のいづれかの箇所で設定できます（左図）
  - Organizationレベル（Organization > Switch Templates）のスイッチテンプレート内の「Select Switches Configuration」項目内の「IP Config」タブ
  - サイトレベル（Sites > Switch Configuration）のスイッチテンプレート内の「Select Switches Configuration」項目内の「IP Config」タブ
- スイッチレベル（Switches > スイッチ名）では本機能は既に使用可能です

VRFサブネット毎のループバック要件の変更



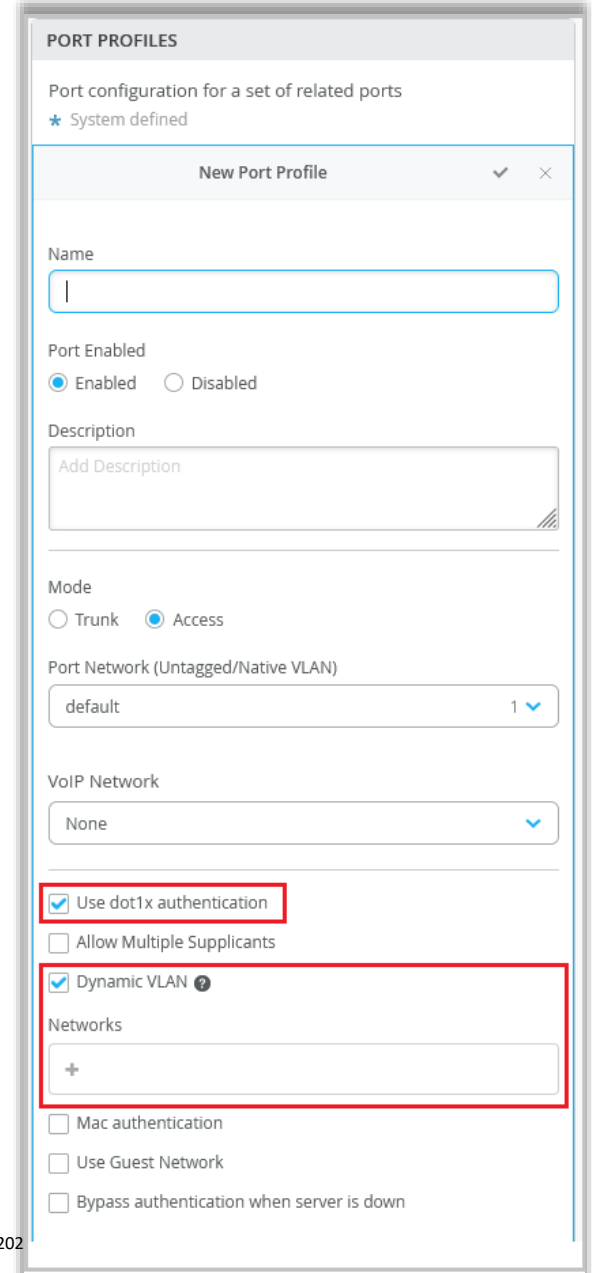
- キャンパスファブリック設定（コアディストリビューション、IP Clos構成）に含まれる設定「Loopback per-VRF subnet」項目で/19以下のサブネットを設定できるようになりました（左図）
  - これまでは/19サブネットのみ、使用することができました
- 新規のキャンパスファブリック構成を設定する際に、デフォルト値だった172.16.192.0/19を、172.16.192.0/24に変更しました
  - 既存のキャンパスファブリック構成では変更されません
  - 設定されたサブネットを使用して、DHCP リレーなどのサービスに使用するループバックインタフェース（lo0.x）をVRFインスタンス単位で自動的に設定します

サイトレベルのキャンパスファブリックでのポッド構成



- ポッド構成をサポートすることにより、サイトレベルでのキャンパスファブリックの拡張性が向上しました
- キャンパスファブリック構成において、アクセス層とディストリビューション層の機器をグループ化できるようになります（左図）
  - 例：
    - サイトの建物毎にポッドを作成し、そのポッド内のアクセス層とディストリビューション層の機器を接続させます
      - アクセス層の機器セットを異なる建物にあるディストリビューション層の機器に接続する必要が無くなります
- 以下のいづれかのネットワーク構成でポッド構成をサポートします
  - キャンパスファブリックのコアディストリビューション構成
  - キャンパスファブリックのIP Clos構成

802.1X認証でのダイナミックVLAN割り当て

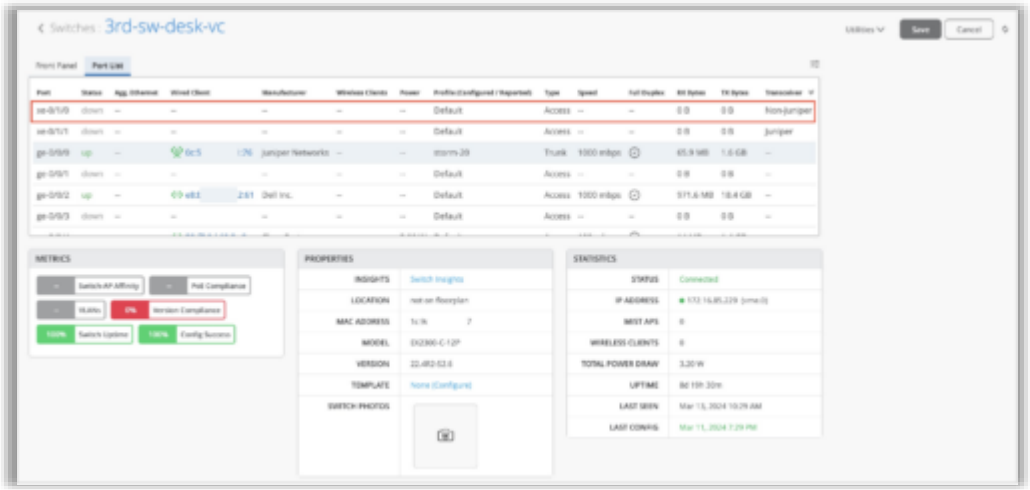


- 802.1Xが設定されたスイッチのポートでダイナミックVLANの割り当てができるようになりました
  - 認証中、RADIUSサーバはRADIUS　access-acceptメッセージでVLAN属性（Tunnel-Private-Group-IDまたはEgress-VLAN-Name）を返すことがあります
  - ダイナミックVLANを割り当てるために、このVLAN属性がスイッチポートに設定されたVLANにマッピングされます
- RADIUSサーバから返されるVLAN情報をオプションでポートプロファイル内の「Dynamic VLAN」項目に設定することができます
  - IP Clos構成の場合、定義したVLANがスイッチにプッシュされるために、VLAN情報を「Dynamic VLAN」項目に入力することが必須となります
- 設定の手順は以下となります
  1. スイッチテンプレート、またはスイッチ詳細ページ内のポートプロファイル設定を開く（Organization > Switch Templates > テンプレート名、Site > Switch Configuration > サイト名、またはSwitches > スイッチ名）
  2. 「Use dot1x authentication」のチェックボックスをチェックする（左図）
  3. 「Dynamic VLAN」チェックボックスをチェックする
  4. Networksドロップダウンリストから VLANプールに追加したいVLANを選択する
  5. ポートプロファイルを保存し、ダイナミックVLANを設定したいスイッチポートにポートプロファイルを割り当てる

専用ボーダーノードを持つIP Clos構成でのシングルコアスイッチのサポート

- 専用スイッチ（ボーダーノード）を用いてサービスブロック機能を実現しているIP Closキャンパスファブリック構成の場合に必要なコアスイッチの最小台数を、2台から1台に削減しました
  - ボーダーノード：
    - ファイアウォール、ルータ、重要な機能を持つ機器などの外部の機器と接続するためのスイッチです
    - 外部のサービスや機器（例：DHCPやRADIUSサーバ）はボーダーノードを経由してキャンパスファブリックに接続します
- この変更はコアスイッチがサービスブロック機能も提供している構成には適用されません

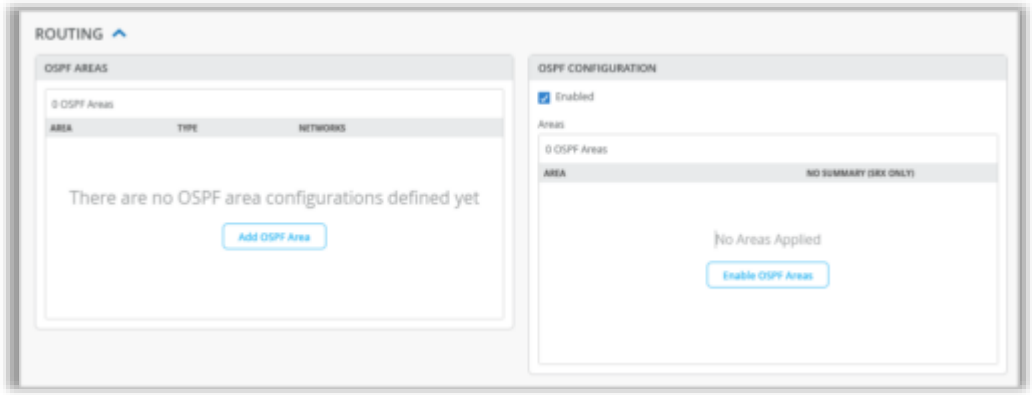
ポートリストへのトランシーバ列の追加



- スイッチ詳細ページのポートリストで、使用中トランシーバがジュニパーでサポートされるかどうかを表示することができるようになりました
- 新しく追加された「トランシーバ（Transceiver）」列で以下の情報を表示します（左図）
  - Juniper：ジュニパーでサポートされるトランシーバ
  - Non-Juniper：ジュニパーでサポートされないトランシーバ

WAN Assurance

WANエッジでのOSPFのサポート



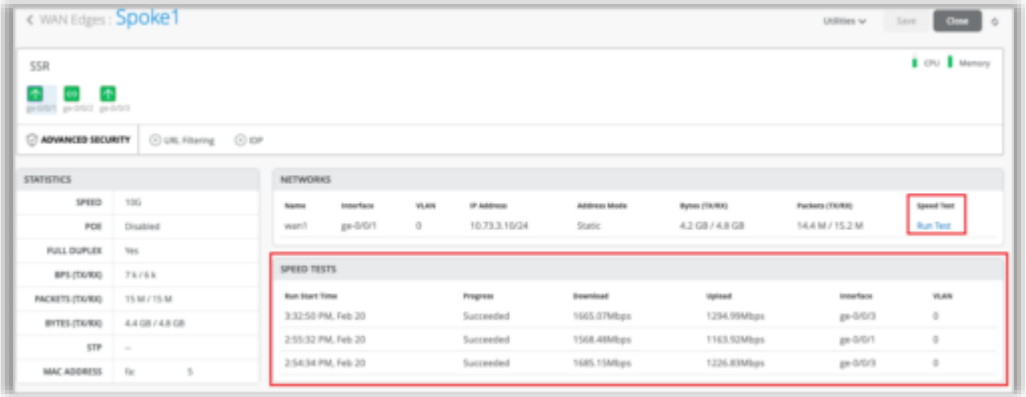
- WANエッジ機器でOSPFがサポートされました
- 以下のいづれかの場所で設定が可能です
  - WANエッジテンプレートのルーティング項目（Organization > WAN Edge Templates）
  - ハブプロファイルのルーティング項目（Organization > Hub Profiles）
  - WANエッジ設定ページ（WAN Edges > WAN Edges > WANエッジ名）
- OSPFは以下の手順で設定できます（左図）
  1. OSPF AREAS項目でOSPFエリアを定義します
  2. OSPF CONFIGRATION項目で設定したOSPFエリアをWANエッジ機器に適用します
- OSPFエリアに関しての詳細は以下のページをご覧ください

  https://www.juniper.net/documentation/us/en/software/junos/ospf/topics/topic-map/configuring-ospf-areas.html

VRFルートリーク

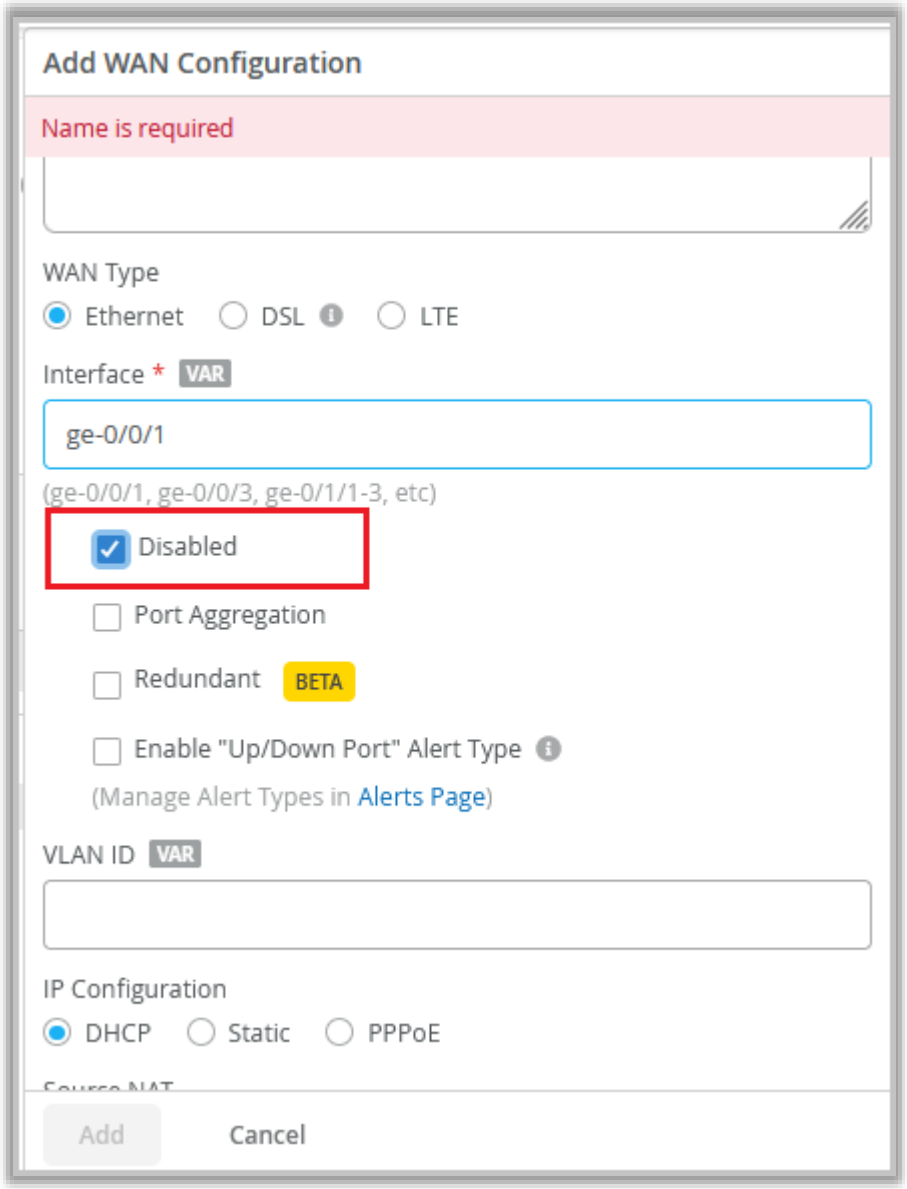
- WANエッジ機器でVRFルートリークをサポートしました
  - ルートリーク：VRFインスタンス間で経路情報を共有する機能
- 機器内のVRF間や、複数の機器間で経路を共有できます
- SSRでVRFルートリークを設定する手順は以下となります
  1. 共有する経路（プレフィックス）のルーティングポリシーを作成し、その中に対象のVRFを含めます
     - ハブ・スポーク構成の場合、このポリシーはハブに関連付けられることが一般的です
     - WANエッジテンプレート、ハブプロファイル、WANエッジ設定で設定できます
  2. ハブとなる機器で宛先項目に経路（ルーティングポリシーに含まれるプレフィックス）を指定したアプリケーションポリシーを設定します
     - スポークとスポークに接続されているスイッチ間に適切がBGPポリシーが無い場合にのみ、スポーク側でアプリケーションポリシーが必要となります
- SRXの場合、ルートリークはインテント構成モデルの一部であり、アプリケーションポリシーで有効にすることができます

WANリンク速度のテスト（SSR）



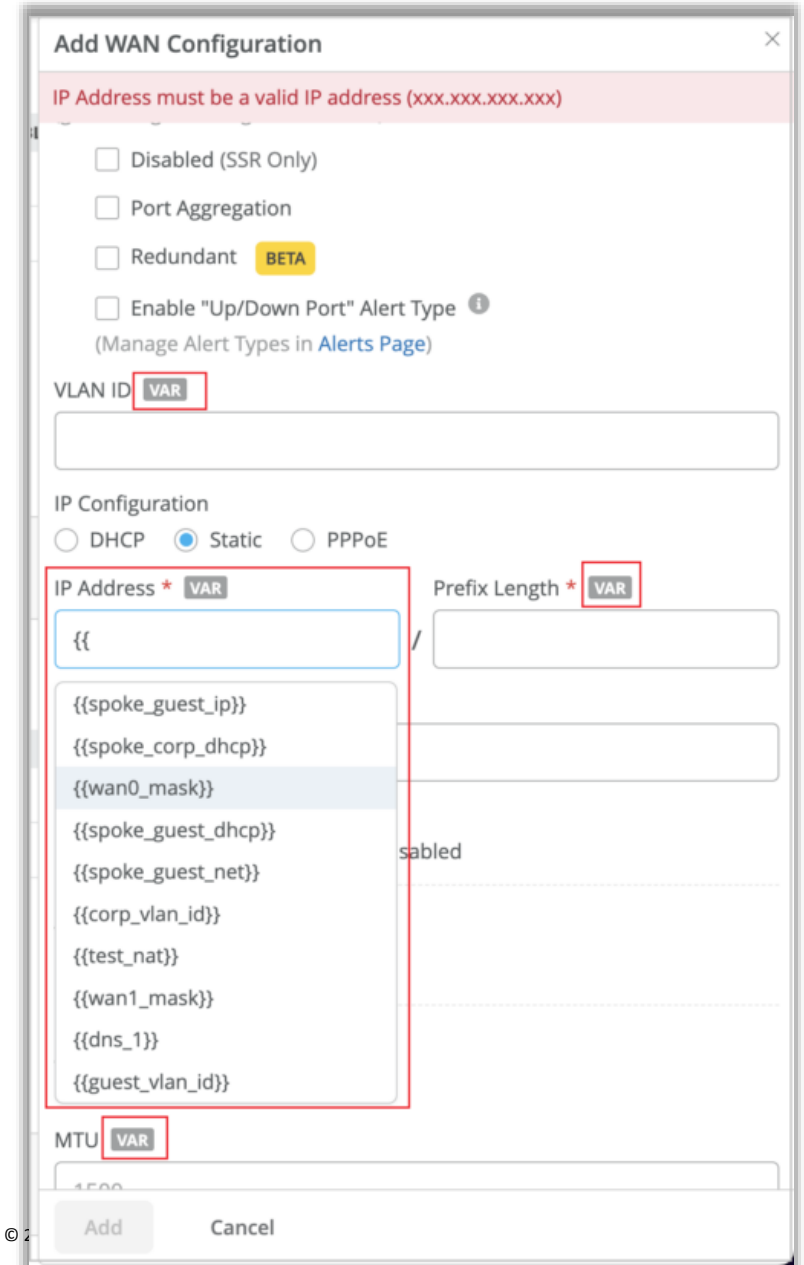
- Mist管理のSSRでWANリンクの速度をテストすることができるようになりました
- 以下のような状況で活用できます
  - 新しいリンクの適正チェック
  - リンク速度の低下がリンクの問題を引き起こしていると思われる場合のオンデマンド速度テスト
- SSRのWANエッジ詳細ページ（WAN Edges > WAN Edges > WANエッジ名）で速度テストをしたいポートをポートパネルから選択します（左図）
- 過去に実施したオンデマンド、または計画的に実行された速度テストの結果はWANエッジ詳細ページで確認できます（左図）
- 速度テストの実施前に、WANリンクがインターネットに接続しており、速度テストで使用する環境に到達できることを確認ください
- SSRクラスタの場合、アクティブなWANリンクでのみ、速度テストが実施できます
- 速度テスト機能を使用するために、SSRのファームウェアバージョンのアップデートは必要ありません

WANエッジポートの無効化



- LANポート、WANポートを無効にすることができるようになりました
- WANエッジテンプレート（Organization > WAN Edge Templates）、またはWANエッジ設定ページ（WAN Edges > WAN Edges > WANエッジ名）で無効に設定できます
- WANエッジポートを無効にするにはLAN、またはWAN設定項目で指定したインタフェースの下部にある「Disabled」チェックボックスをチェックします（左図）

サイト変数をサポートする項目の明確化



- WANエッジ設定内で、サイト変数を利用することができる項目には「VAR」ラベルが表示されるようになりました（左図）
- このラベルにより、どの項目でサイト変数を利用できるかが分かりやすくなりました
- 項目にサイト変数を入力しようとした場合、入力した文字列に一致するサイト変数を表示します（既にサイト変数が設定済みの場合）（左図）
- サイト変数の詳細については以下のページをご覧ください

  https://www.juniper.net/documentation/us/en/software/mist/mist-management/topics/task/site-variables.html

Behavior Changes

サイトレベルでのユーザ権限継承の変更

- ユーザに付与される権限は、スコープ（MSP、Organization、サイト）で最も高い権限にマッピングされるようになります
  - MSPとOrganizationの場合、既に同様の仕組みとなっています
- Organizationとサイトの場合に一貫性を持たせることができるようになります
- ローカルユーザとSSOユーザでも同じ動作となります
- Organizationレベルで設定された権限は、サイトレベルで設定された権限を上書きできるようになります
- 留意点：
  - Mistポータルからは複数のOrganization、サイト権限の設定はできませんが、APIからは可能です

	Organization 1で設定された権限	サイト 1で設定された権限	サイト 1で実際に割り当てられる権限
2024年5月6日までの挙動	Super User	Helpdesk	Helpdesk
2024年5月7日以降の挙動	Super User	Helpdesk	Super User

/self APIの変更（MSPユーザ）

- 2024年5月7日より、/self APIはMSPで設定したユーザ権限情報のみを取得します
- ユーザの継承された権限は取得されません
- Organizationレベルで継承された権限を確認したい場合は、MSPレベルで「/msps/:msp_id/orgs」のGET APIクエリを実行する必要があります
- サイトレベルで継承された権限を確認するには、Organizationレベルで「/orgs/:org_id/sites」のGET APIクエリを実行します

Feature Deprecation

Webhookトピックasset-rawの廃止

- 2024年6月30日より、asset-rawのWebhookトピックを廃止します
- asset-raw-rssiに代替されます
- Webhookの詳細は以下のセクションをご覧ください（Mistユーザアカウントが必要となります）
  https://api.mist.com/api/v1/docs/Site#webhooks


Thank you
JUNIPER
driven by Mist AI