Juniper Networks | Engineering Simplicity

Distributed Branch EX Series — Juniper Validated Design (JVD)

Published
2025-11-26

Table of Contents

Distributed Branch EX Series — Juniper Validated Design (JVD)

Juniper Networks Validated Designs provide you with a comprehensive, end-to-end blueprint for deploying Juniper solutions in their network. These designs are created by Juniper's expert engineers and tested to ensure they meet your requirements. Using a validated design, you can reduce the risk of costly mistakes, save time and money, and ensure that their network is optimized for maximum performance.

About this Document

This document discusses the approach and best practices when deploying and managing Juniper Networks® EX Series Switches at the branch using the Juniper Mist™ cloud. At the branch, EX Series Switches can be used as traditional standalone switches or as a Virtual Chassis combining up to ten switches and managing them as a single device. For higher scale deployments at the branch, topologies including distribution switches between access switches and WAN devices have been tested and presented as part of this JVD.

The integration of other typical elements at the branch, such as access points and WAN routers have also been tested. Instructions integrating them have been added to the appendix section of this JVD.

Solution Benefits and Overview

Juniper Mist™ Wired Assurance brings cloud management and Mist AI™ to campus fabrics. It sets a new standard for network management by moving your campus deployment toward AI-driven operations, which helps deliver better experiences to connected devices. The Juniper Mist cloud streamlines deployment and management of your campus fabric, while Mist AI simplifies operations and improves visibility into the performance of connected devices.

Wired Assurance helps IT teams reduce mean time to repair (MTTR) and deliver a new generation of experience-first networking. EX Series Switches combined with Mist AI deliver insights into switch health and pre- and post-connection service-level metrics.

Key Features

- Onboard, configure, and manage EX Series Switches from the Juniper Mist cloud

- Build and deploy campus fabric architectures in minutes based on intent
- Leverage open APIs for third-party integration and automation across multivendor environments
- Use AI-driven insights to learn exactly how switches are performing
- Configure sites and switches using templates and port profiles
- Get proactive root-cause identification and enable self-driving actions

Simple Switch Provisioning

Configure and troubleshoot cloud-ready, zero-touch provisioning (ZTP)-enabled EX Series Switches with an activation code for plug-and-play capabilities. You'll minimize onboarding errors, save time, and streamline efficiencies. Once templates and profiles are established, you can implement colorless ports, so devices automatically inherit the right configurations.

Intent-Based Config Models

Create consistent, streamlined configurations and universal templates and profiles from the cloud. Easily build and manage campus fabric architectures in a few clicks based on intent. This structure helps standardize deployments while offering the flexibility to tweak specific site or switch attributes.

AI-Driven Switch Insights

Learn how your wired switches perform across a timeline with detailed device-level metrics, such as CPU and memory utilization and Virtual Chassis status. At the port level, see the number of bytes transferred, traffic utilization levels, and power draw.

Manage Switch Health

Ensure optimal switch operations with key health metrics such as firmware compliance, missing VLANs, and switch-Wi-Fi access point (AP) affinity in multivendor environments, when paired with Juniper wireless APs.

Open APIs

Harness the power of 100% open and programmable APIs to fully automate the switch activation, onboarding, and configuration processes. You can integrate with third-party systems like ServiceNow and Splunk, which support APIs for automated ticketing, troubleshooting, and more.

Better Align Resources

You can analyse up to 30 days of data to help simplify the process of extracting network insights across your enterprise to better align your resources with changing requirements.

View details of Juniper Mist Wired Assurance from the datasheet here: Juniper Mist Wired Assurance Datasheet

Use Case and Reference Architecture

The architectures for EX Series Switches and other elements such as APs and WAN routers at a branch are rather simple by nature. Either you have:

Network designs covered in this JVD:

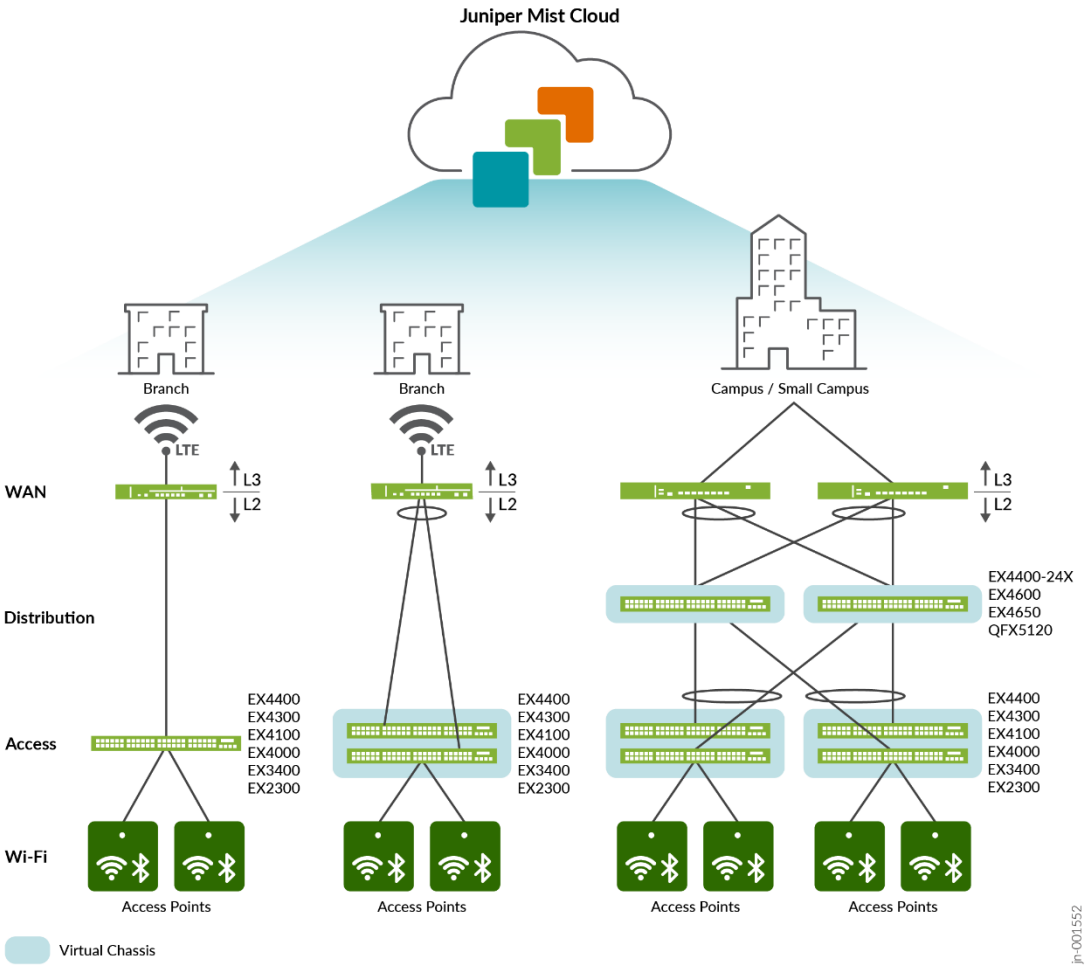
- One or more standalone switches connected to a WAN router. Access points are then connected to the switch (usually also using PoE). The WAN router is usually connected via a single non-redundant uplink to save costs.
- Two or more switches that form a Virtual Chassis connected to a WAN router. Access points are then connected to the Virtual Chassis (usually also using PoE). Here, we recommend using multiple links for the uplink by adding an IEEE 802.3ag link aggregation configuration for redundancy.
- For larger branches those Virtual Chassis then might be cascaded and then you have an access and a distribution Layer. This design may even be comprised having two link aggregation groups (LAGs) or bundles depending on the WAN router capabilities.

Network designs not covered in this JVD:

- A small campus fabric such as EVPN multihoming. This has a separate JVD found here.
- An AP directly connected to a WAN router.

Figure 1 on page 4 shows the three main architectures that were tested end-to-end with EX Series Switches managed by Juniper Mist cloud as part of this JVD.

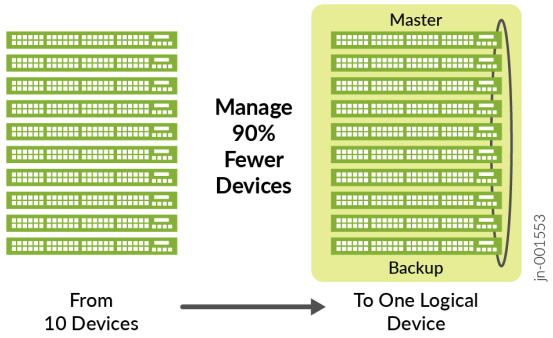
Figure 1: Branch Architectures with EX Switches



NOTE: You may find references using a routing protocol such as OSPF between the distribution switch (as Virtual Chassis) and WAN router. Such designs are seldom used today because designs such as campus fabric EVPN multihoming are more popular in this case.

In addition to multiple standalone switches, Juniper Networks provides Virtual Chassis as a technology which combines multiple switches and manages them as one logical unit.

Figure 2: Virtual Chassis



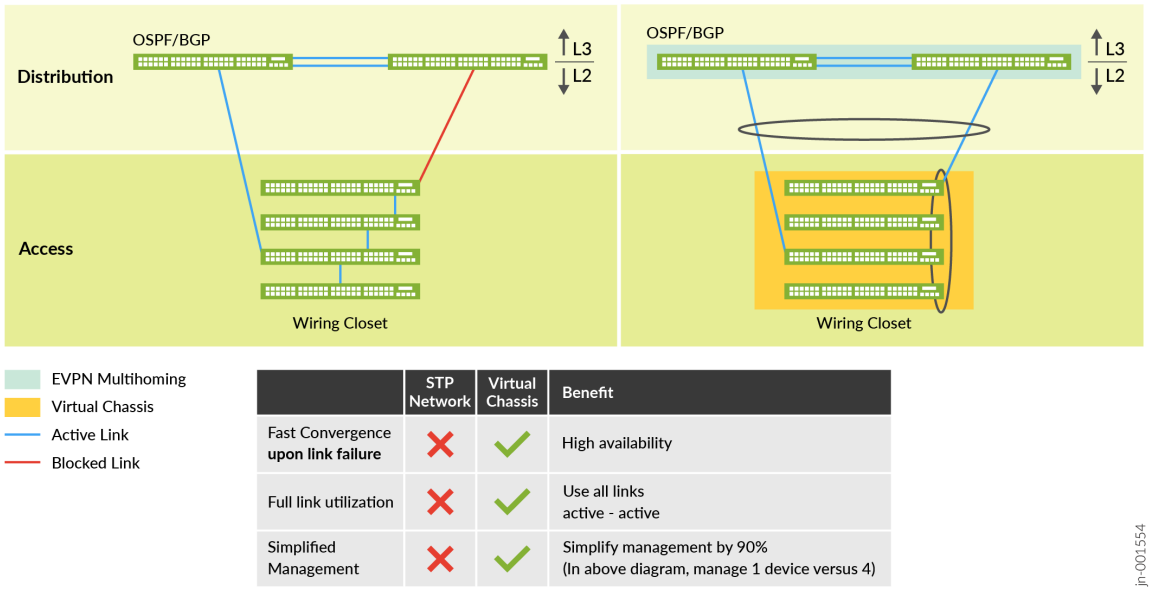
Implementing Virtual Chassis has the following major advantages:

- A Virtual Chassis is managed as a single switch.
- The convergence time on link failure is faster than with the traditional spanning tree approach.
- All uplinks can be active at the same time using link aggregation. With spanning-tree protocols, only one link can be active at the same time.

NOTE: Not a subject of this JVD but, should you consider using Virtual Chassis in a Juniper Mist cloud-managed campus fabric, the Virtual Chassis can only be deployed at the access layer.

Figure 3 on page 6 highlights the general advantage of using Virtual Chassis versus a traditional spanning tree method.

Figure 3: Virtual Chassis in Access



Most EX Series Switches attempt to form a Virtual Chassis automatically from factory state when they are powered on. Hence, there is no manual intervention needed during installation. The connection toward the Juniper Mist cloud to manage the device may use a dedicated management port or use the preferred in-band management through any revenue port.

Table 1 on page 6 shows which EX Series Switch models support which Virtual Chassis formation method:

Table 1: Switch Models and Virtual Chassis Formation Methods

Switch Model Used in Virtual Chassis	VC Connections Made Through	VC Formation Support
EX3400, EX4100, EX4100-F, EX4300, EX4400 & EX4600	Special Backplane connectors called VCP Ports	Automatic on boot (ZTP support)
EX4000, EX4100-H	Predefined Uplink-Ports on Front Pannel	Automatic on boot (ZTP support)
EX2300, EX4650 and QFX5120	Uplink-Ports on Front Pannel	Pre-staging needed
EX4400-24X	Front Pannel-Ports (after they are converted to HGoE)	Pre-staging needed

Uplinks to the WAN router should utilize an IEEE 802.3ad LAG with active LACP. The WAN router must support a feature such as “force-up” on at least one interface to build a LAG between the WAN router and the switch. The details are explained in the "Best practices when using Link Aggregation on the uplink Interfaces" on page 48 section.

Validation Framework

IN THIS SECTION

Test Bed

The test topology used for the evaluation of this JVD is documented in Figure 4 on page 8:

Figure 4: Test Bed for Phase 1+ 2 of this JVD

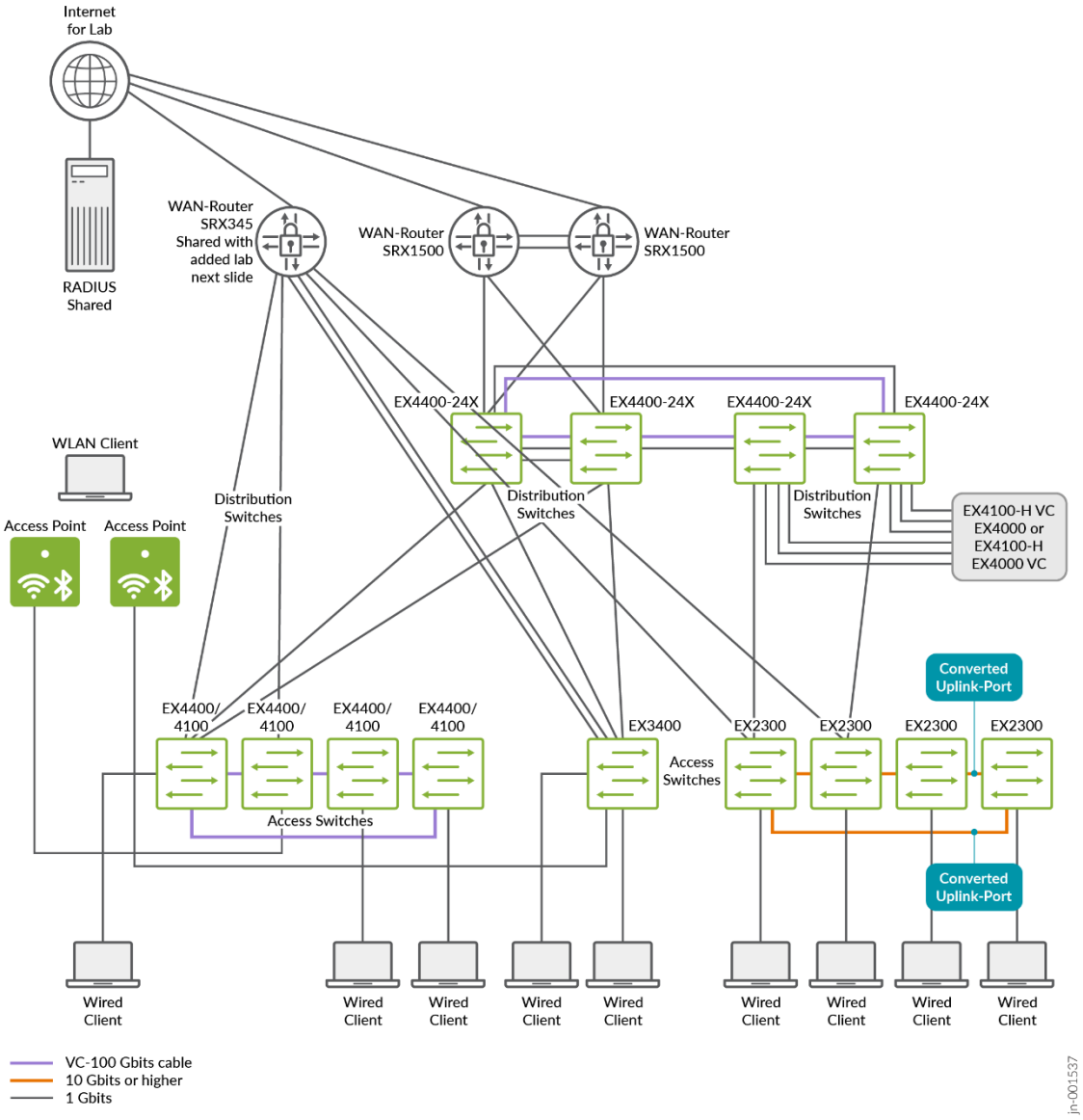
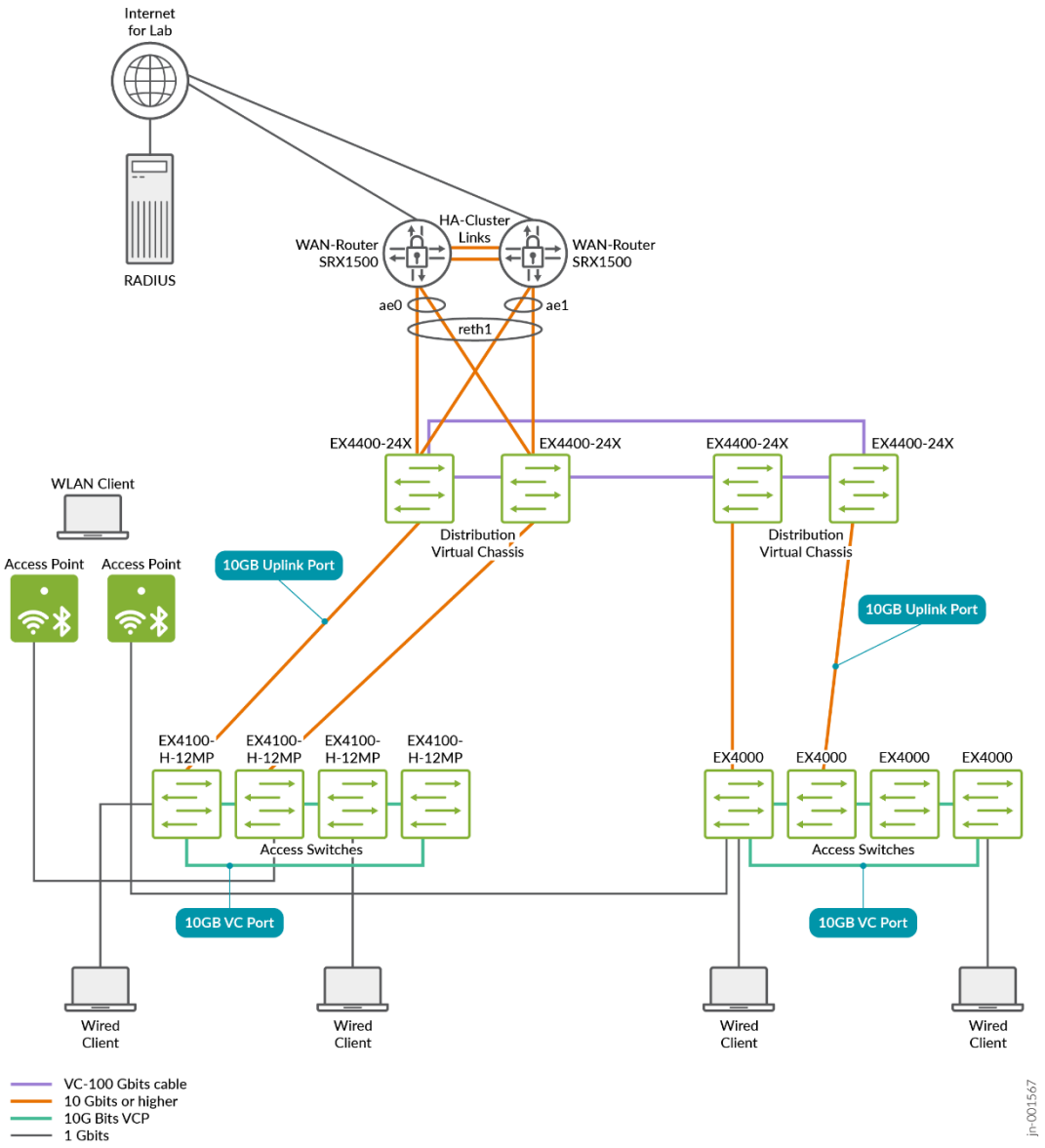


Figure 5: Lab extension to test EX4000 and EX4100-H



The current lab design includes the following:

- Branch use cases:
  - Single standalone switch (Juniper Networks® EX3400 Switch) attached directly to WAN router.
  - Single standalone switch (Juniper Networks® EX4000 Switch or Juniper Networks® EX4100-H Switch) attached directly to WAN router.
  - One four-member Virtual Chassis access switch based on Juniper Networks® EX4400 Switch or EX4100 Switch.

    - One four-member Virtual Chassis access switch based on Juniper Networks® EX2300 Switch.
    - One four-member Virtual Chassis access switch based on EX4000 Switch.
    - One four-member Virtual Chassis access switch based on EX4100-H Switch.
    - One four-member Virtual Chassis distribution switch based on Juniper Networks® EX4400-24X Switch.
    - Two access points for limited Wi-Fi testing.
- EVPN multihoming campus fabric (not within the scope of this JVD):
    - Two redundant distribution switches acting as a collapsed core.
        - One four-member Virtual Chassis access switch acting as a leaf.
        - One standalone access switch acting as a leaf.
    - Four distribution switches acting as collapsed core in a ring.
        - Four four-member Virtual Chassis Access Switch acting as a leaf.
        - Two standalone access switches acting as a leaf.
- WAN router integration:
    - Layer 3 gateways on the WAN router.
        - IEEE 802.3ad LAG-based trunks.
    - Attached to
        - Distribution switches.
        - Directly to the access switches.
    - Redundant WAN router design
        - Two Juniper SRX firewalls in a high availability configuration.
    - The WAN router is also managed by the Juniper Mist cloud (WAN edge SRX operating in standalone mode).
    - The DHCP server is located on the WAN router or the WAN router is performing DHCP relay.
- Wireless access points
    - Locally attached to the access switches with PoE.
    - Various wireless clients.
    - Basic wireless roaming.

- Wired clients
  - Virtual machines or testing equipment attached to the access switches.
- RADIUS server
  - Server location
    - Local server attached to the underlay or VPN network.
    - Juniper Mist™ Access Assurance via public cloud.
  - Authentication for the following clients:
    - Wired clients attached to access switches.
    - Wi-Fi clients using the access points.
  - Authentication based on clients:
    - MAC address.
    - 802.1X EAP authentication.
  - Dynamic authorization profiles via RADIUS:
    - Single VLAN assigned.
    - Multiple VLANs assigned.
    - Assigns Filter-ID of manually configured ACL.
- Testing switch features such as:
  - Protect RE-filter
  - DHCP snooping
  - Storm control
  - MAC address limit with aging
  - Dynamic port configuration
  - Voice VLAN
  - SNMP
  - Syslog
  - Port mirroring
  - DNS

    - NTP
- Day 0 Features:
    - Claim and ZTP all Virtual Chassis and standalone switches.
    - Switch management via outbound-ssh (Pyagent) or HTTPS (CloudX).
    - Switch adoption (not a test case).
- Day 1 Features:
    - Site variables
    - Switch templates and configuration hierarchy.
    - Additional Junos OS CLI.
- Day 2 Features:
    - Firmware upgrades of all Virtual Chassis.
    - Swapping an existing VC member with a new switch.
    - Adding a new Virtual Chassis member.
    - Deleting a Virtual Chassis member.
    - On-demand and Dynamic Packet Capture
- Monitoring:
    - Switch insights.
    - Wired client insights.
    - Wired Assurance alerts (via e-mail).
    - Wired SLE monitoring.
    - Marvis® Virtual Network Assistant.

From the one global lab topology suggested, two major designs for EX Series branch testing can be derived and tested depending on which links they use, and which device is active at the time the lab is executed:

- A design with a standalone switch and all Virtual Chassis in the access layer that are then directly connected to the WAN router.

Figure 6: Test Bed without Distribution Layer Virtual Chassis

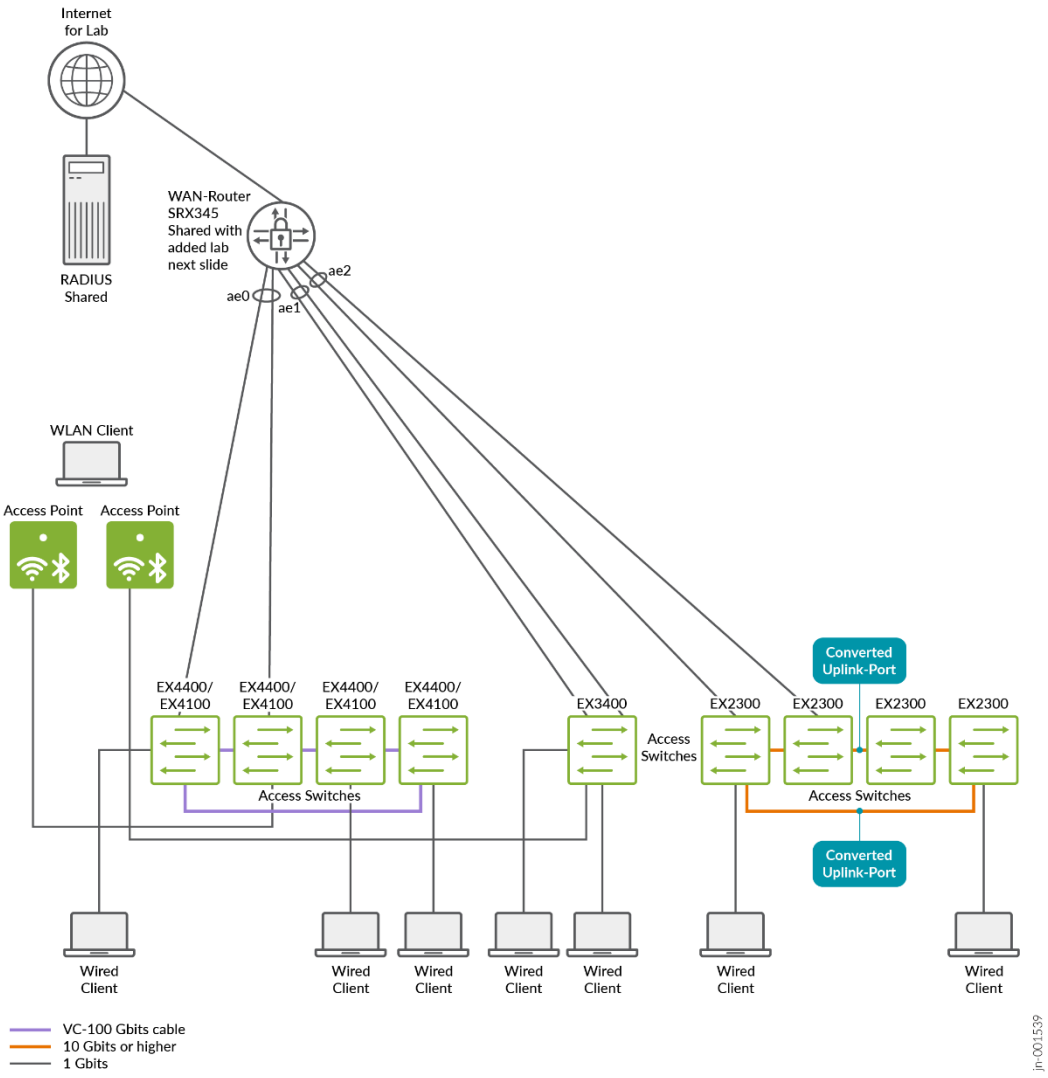
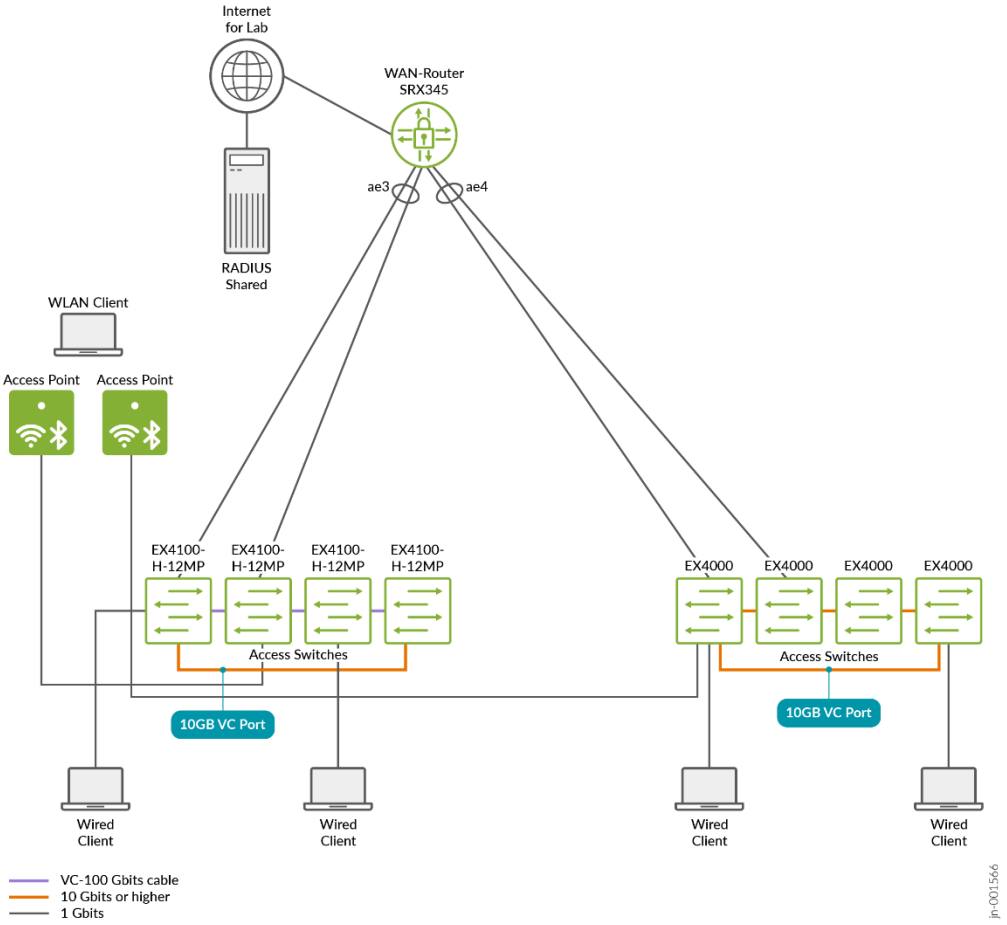


Figure 7: Test Bed without Distribution Layer Virtual Chassis with Phase2 added devices



- A design where the standalone switch and all Virtual Chassis in the access layer are connected to a Virtual Chassis in the distribution layer. That distribution layer then has the final connection to the WAN router. This is usually suggested when a customer wants to deploy five or more Virtual Chassis in the access layer.

Figure 8: Test Bed with Distribution Layer Virtual Chassis

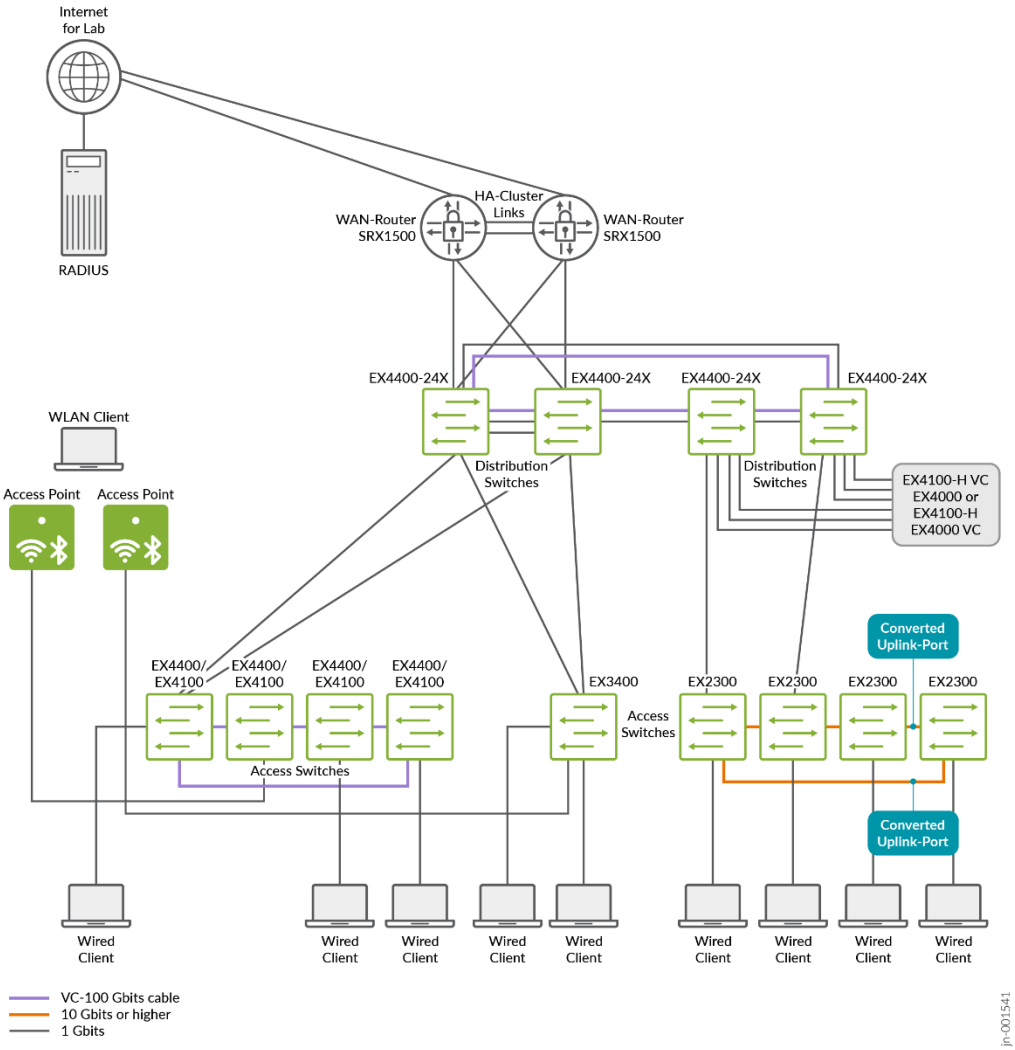
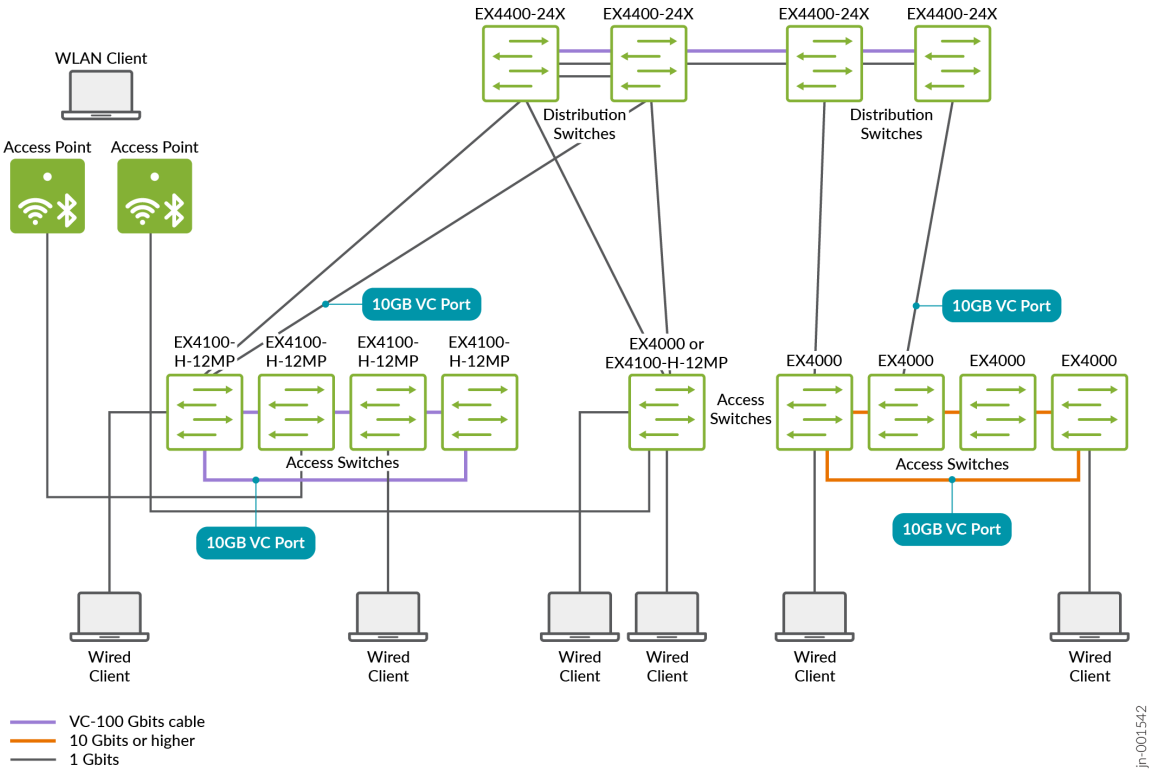


Figure 9: Test Bed with Distribution Layer Virtual Chassis and added Phase2 access switches



Platforms / Devices Under Test (DUT)

Testing was performed with a focus on the EX Series Switches using the following Junos OS versions:

Table 2: Devices Under Test

Devices Under Test		
Platform	**Device**	**Junos OS Release**
EX4400 (added in Phase2)	Access switch (standalone)	24.4R2
EX4100	Access switch VC	24.4R2
EX2300	Access switch VC	24.4R2

Table 2: Devices Under Test *(Continued)*

Devices Under Test		
Platform	**Device**	**Junos OS Release**
EX4400-24X	Distribution switch	24.4R2
EX3400	Access switch (standalone)	24.4R2
EX4000 (added in Phase2)	Access switch VC	24.4R2
EX4100-H (added in Phase2)	Access switch VC	24.4R2
SRX345	WAN router	23.4R2-S5
SRX1500	WAN router	23.4R2-S5

Test Bed Configuration

The appendix section of this document shares information on exactly how some of the tests were performed. Contact your Juniper account representative to obtain the full archive of the test bed configurations used for this JVD.

Test Objectives

IN THIS SECTION

Test Goals

The testing for this JVD was performed with the following goals in mind (Please consult the Test Report for more information):

- Build a production-grade lab design where all branch links are at minimum 10 Gbps when technically possible.
- **Test with Dualstack IPv4 and IPv6 wired and wireless client connections via WAN-Router.**
- Day 0 Features
  - Planning the deployment selecting the right option to manage EX switches remotely via Mist cloud.
  - Switch templates and configuration hierarchy.
  - Site variables
  - Additional Junos OS CLI
- Day 1 Installation of the WAN-Router:
  - As standalone Router with a single downlink towards access switches.
  - As standalone Router with LAG towards the access switches.
  - As high-availability cluster with two LAG's towards a distribution Virtual Chassis.
- Day 1 single switch claim and ZTP towards Mist cloud (outbound-ssh or CloudX)
- Day 1 Test with all permutations building Virtual Chassis through claim and ZTP when:
  - EX4100 or EX4400 that automatically built a Virtual Chassis when connected through backport.
  - EX4000 and EX4100-H that automatically built a Virtual Chassis when connected through dedicated 10Gbit/s Frontports.
  - EX2300 that needs to be prepared building Virtual Chassis via Front Port.
  - EX4400-24X requiring console to be prepared building Virtual Chassis via HGOE.
- Day 1 Installation and claim of Juniper Access Point attached to access switch.
- Day 1 Features simultaneously enabled such as:
  - Protect RE-filter
  - DHCP snooping
  - Storm control

    - MAC address limit with aging
    - Voice VLAN
    - QoS profile
    - RADIUS-based assignments of single VLAN, multiple VLANs and Filter-ID
    - Dynamic Port Configuration
    - SNMP
    - Syslog
    - Port mirroring
- Day 2 Monitoring
    - Switch Insights.
    - Wired client insights.
    - Wired Assurance alerts (via e-mail).
    - Wired SLE monitoring.
    - Marvis VNA
    - Perform On-demand and dynamic Packet captures.
- Day 2 Test of the three Virtual Chassis permutations where on each one must perform:
    - A Junos OS software update on the entire Virtual Chassis.
    - An RMA replacement of the primary member of a Virtual Chassis.
    - Adding a new member to each Virtual Chassis.
    - Deleting a member from each Virtual Chassis.
- Perform scale testing with 50 VLANs and 2000 wired clients.
- Perform extensive PoE testing.

Test Exclusions

The testing for this JVD was not performed on the following items:

- Large scale switch testing and multiple building testing. Juniper Networks offers technologies such as campus fabric for these use cases which are not typically used at the branch.
- Extensive testing of wireless and roaming. Wireless networking is not the focus of this JVD.
- Juniper Mist™ Edge integration for wireless scaling. Mist Edge is not usually part of a branch. It is usually placed at the corporate headquarters or at the data center.
- Testing with Juniper Networks® SSR Series Routers was not included in this JVD, as a separate JVD dedicated to WAN Edge for SSR had been published shortly beforehand. The integration of SSR WAN routers with branch EX Series Switches was already covered in that earlier testing process.
- Extensive testing of third party RADIUS vendors. If one works such as FreeRADIUS, the others are believed to work as well.
- Testing a routing protocol such as OSPF or BGP between the distribution layer and the WAN router. This is because most of the deployments terminate all VLANs at the WAN router for the sake of simplicity.
- DHCP relay testing. This is part of the campus fabric. At the branch, the DHCP relay function is usually on the WAN router.
- Testing of virtual routing functions (VRF). All Layer 3 functions are located on the WAN router.

Recommendations

The following list of recommendations summarizes those recommendations covered throughout this document:

- Check how you connect the WAN router to the EX Series Switch and what features it supports. When using a LAG between the two devices, features like active LACP and “force-up” will help you manage the attached EX Series Switch more effectively using in-band management.
- Use switch templates for efficient configuration management. Configuration errors and unnecessary additional work can be avoided this way.
  - Use the template hierarchy from organization-level templates to site-level templates. Making changes to individual switches should be done as a last resort.
  - Rather than making change to individual switches, leverage the use of site variables for unique configuration settings within templates.
  - Do not duplicate templates to make unique configuration settings. Having many templates may cause you to lose sight over time. Leverage features like site variables and roles instead.

    - For added security we recommend either to disable unused ports or at least define and use a quarantine VLAN on all unused ports. Please review the example here.

- When designing and using Virtual Chassis:
    - When designing Virtual Chassis, it is not recommended using the maximum of supported Virtual Chassis Members stated in the "Virtual Chassis Overview (Juniper Mist)" on page 23 . Roughly cut the stated maximum members to a half. This is to avoid oversubscription of the bandwidth of the Virtual Chassis port (VCP) linkshave when building the Ring between the Virtual Chassis members.
    - Create and assign individual Templates for Virtual Chassis with the same amount of members. Avoid configuring the same port configurations on all kinds of sizes of Virtual Chassis. This helps the system to apply your configuration changes straight without needing to detect each time if Template specified ports are really avail in your local Virtual Chassis configuration.
    - All Virtual Chassis configurations should be done via the Mist-Cloud and the Modify Virtual Chassis-dialogue. CLI or Additional CLI should not be used for managing a Virtual Chassis.
- Juniper recommends enabling the **protection of the Routing Engine** .
- When needing to decide how to manage port configuration dynamically:
    - Assigning VLANs and filters via RADIUS/NAC infrastructure is the recommended approach. Especially for those customers using Juniper Mist Access Assurance.
    - Using Dynamic Port Configuration is less preferred.
- When using Dynamic Port Configuration:
    - Avoid matching by MAC-Address if the device supports LLDP.
    - Don’t match by MAC-Address if ports are enabled with dot1x.
    - The use of a Filter-Id should be avoided. Usually there is no need to do that if the ports are dot1x enabled a one can apply a dynamic VLAN via RADIUS.
    - Avoid a high number of port flaps for a DPC-configured port.
    - Refer switch insights to ascertain the individual configuration is applied.
- Try to avoid using additional Junos OS CLI commands if possible.
- For the recommended version for Juniper products, see **Recommended Junos OS Releases.**

Revision History

Table 3: Revision History

Date	Version	Description
November 2025	JVD-ENTWIRED-DISTENT-02-01	Switch management via CloudX/JMA On-Demand and Dynamic Packet capture Added EX4000 and EX4100-H Junos OS 24.4R2
September 2024	JVD-ENTWIRED-DISTENT-01-01	Initial publish Junos OS 22.R3

Appendix: Day-0 Plan

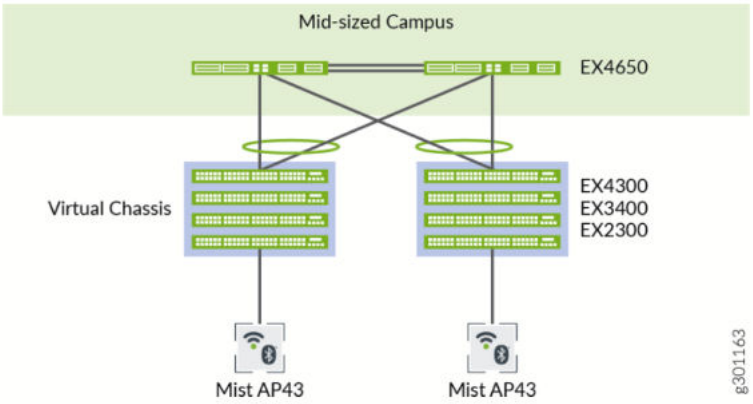
IN THIS SECTION

Building a Virtual Chassis

Virtual Chassis Overview (Juniper Mist)

The Virtual Chassis technology enables you to connect multiple individual switches together to form one logical unit and to manage them as a single unit. You can configure and manage a Virtual Chassis using the Juniper Mist™ portal. The switches you add to a Virtual Chassis are called members. In a Virtual Chassis setup, VCPs connect the member switches and are responsible for passing the data and control traffic between member switches.

Figure 10: A Typical Virtual Chassis Setup



A Virtual Chassis helps you mitigate the risk of loops. It also eliminates the need for legacy redundancy protocols such as spanning-tree protocols (STPs) and Virtual Router Redundancy Protocol (VRRP). In core and distribution deployments, you can connect to the Virtual Chassis using link aggregation group (LAG) uplinks. These uplinks ensure that the member switches in a Virtual Chassis have device-level redundancy.

A Virtual Chassis can include from two to ten switches. Such a physical configuration can provide better resilience if a member switch goes down. One possible disadvantage of combining several switches into a Virtual Chassis is that this configuration requires more space and power than a single device requires.

Link to video: Virtual Chassis Overview

You can create a Virtual Chassis using the Form Virtual Chassis option on the portal. The Form Virtual Chassis option applies only to the Juniper Networks® EX4650 Switches, Juniper Networks® QFX5120 Switches, and EX2300 Switches, as these switches don't have dedicated VCPs. This option is not available to the Juniper Networks® EX4100-F Switch, Juniper Networks® EX4300 Switch, Juniper Networks® EX4600 Switch, EX3400, EX4100, and EX4400 Switches as they come with dedicated VCPs.

Table 4 on page 24 shows the switch models along with the maximum number of member switches allowed in a Virtual Chassis configuration.

Table 4: Maximum Number of Member Switches Allowed in a Virtual Chassis Configuration

Switch Model	Maximum Number of Members
EX2300	4
EX4650	4
EX3400	10
EX4000	6
EX4100	10
EX4100-F	10
EX4100-H	6
EX4300	10
EX4400	10

Table 4: Maximum Number of Member Switches Allowed in a Virtual Chassis Configuration *(Continued)*

Switch Model	Maximum Number of Members
EX4400-24X	10
EX4600	10
QFX5120-32C,QFX5120-48T, QFX5120-48Y	2
QFX5120-48YM	4
QFX5110	10

Juniper Mist supports only preprovisioned Virtual Chassis configuration. It doesn't support non-provisioned configuration. The preprovisioned configuration enables the deterministic control of the roles and member IDs assigned to the member switches when creating and managing a Virtual Chassis. The preprovisioned configuration distinguishes member switches by associating their serial numbers with the member ID.

For more information, see Virtual Chassis Overview for Switches.

Mixed and Non-Mixed Virtual Chassis

A Virtual Chassis that includes switches of the same model can operate as a non-mixed Virtual Chassis. However, a Virtual Chassis that includes different models of the same switch (for example, two or more types of EX Series switches) must operate in mixed mode because of architecture differences between the different switch models.

Table 5: Supported Combination of Switches in a Mixed-Mode Virtual Chassis

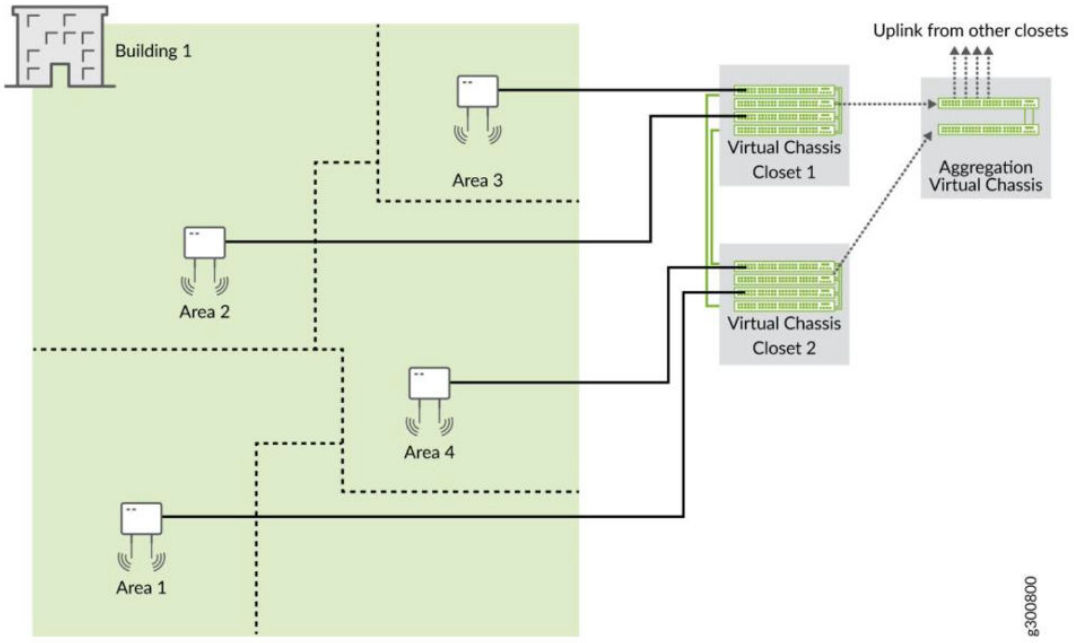
Allowed Routing Engine Members	Allowed Linecard Members
EX4300	EX4300 and EX4600
EX4300-48MP	EX4300-48MP and EX4300 (excludes EX4600)
EX4600	EX4600 and EX4300 (excludes EX4300-48MP)

For more information about the combination of switches that a mixed or a non-mixed Virtual Chassis configuration supports, see Understanding Mixed EX Series and QFX Series Virtual Chassis.

Design Considerations for Virtual Chassis

We recommend that you physically distribute your Juniper access points across a floor in the network operations center (NOC) so that they connect to multiple switches in a Virtual Chassis. Doing so provides better redundancy and is a more robust design for handling power supply-related hardware failure.

Figure 11: Virtual Chassis Setup in a NOC



For example, let's say you want to deploy a solution that includes 96 ports. The two main options for doing so are:

- Use two EX4300-48P Switches, with one switch serving as the primary and one as backup. The advantages here are a compact footprint and cost effectiveness. The main disadvantage is that the loss of one switch can impact 50 percent of your users.
- Use four EX4300-24P Switches, with one switch serving as the primary, one as backup, and two switches serving as line cards. The advantages here are higher availability (the loss of one switch only affects 25 percent of users), and the fact that uplinks are not affected by a switch failure (provided

that the failed switch did not include any uplinks). The main disadvantage is that you need more space, power, and cost to support the equipment. Regardless of the options you go with, if you do plan to leverage one or more Virtual Chassis in your deployment, we recommend that you configure the primary and backup switches in the Virtual Chassis so that they are in different physical locations. The member devices of the Virtual Chassis should likewise be distributed so that no more than half are dependent on the same power supply or other single point of failure, and they should be evenly spaced by a member hop in the Virtual Chassis.

Workflow for VC Formation With Mist for EX3400, EX4000, EX4100, EX4100-F, EX4100-H, EX4300, EX4400 and EX4600 Switches

The EX3400, EX4000, EX4100, EX4100-F, EX4100-H, EX4300, and EX4400 Switches come with dedicated VCPs. A dedicated VCPs can be either a 100Gbit/s port on the back of the switch or a dedicated 10Gbit/s port on the front of the switch depending on the switch model. To create a Virtual Chassis using these switches, you only need to connect them to each other using VCPs. The **Form Virtual Chassis** option on the **Switches** page on the Juniper Mist portal is not applicable to these switches. However, once a Virtual Chassis is created with these switches, you can use the **Modify Virtual Chassis** option on the switch details page to modify and manage the Virtual Chassis. The Virtual Chassis workflow for these switches involves the following two steps:

1. Virtual Chassis formation by connecting the switches using the dedicated VCPs and powering on them.

2. (Optional but highly recommended) Preprovisioning the Virtual Chassis using the Modify Virtual Chassis option on the Juniper Mist portal. Juniper Mist supports only the preprovisioned Virtual Chassis configuration. The preprovisioned configuration specifies the chassis serial number, member ID, and role for both member switches in the Virtual Chassis. When a new member router joins the Virtual Chassis, Junos OS compares its serial number against the values specified in the preprovisioned configuration. Preprovisioning prevents any accidental role assignments, or the accidental addition of a new member to the Virtual Chassis. Each role, member ID, addition or removal of members, is under the control of the configuration.

NOTE: Juniper Mist automatically upgrades a Virtual Chassis linecard member if it is running a Junos OS version different from that of the primary member. The linecard member will be upgraded to the same version as the primary member if the following conditions are met:

- The switch must form a Virtual Chassis with three or more members—that is, a primary, a backup, and a linecard member.

- The Junos OS version on the linecard member is different from that on the primary member.
- The linecard member must be in Inactive state. Note that a linecard member will be upgraded only if it is inactive and running a clearly different Junos OS version. Minor version differences, such as different spin numbers, will not trigger an upgrade.
- Only the Junos OS versions listed on the Juniper Mist portal are available for upgrade.

In addition to creating a Virtual Chassis, you can renumber, replace, or add a member to an existing Virtual Chassis, by using the **Modify Virtual Chassis** option on the Switch Details page.

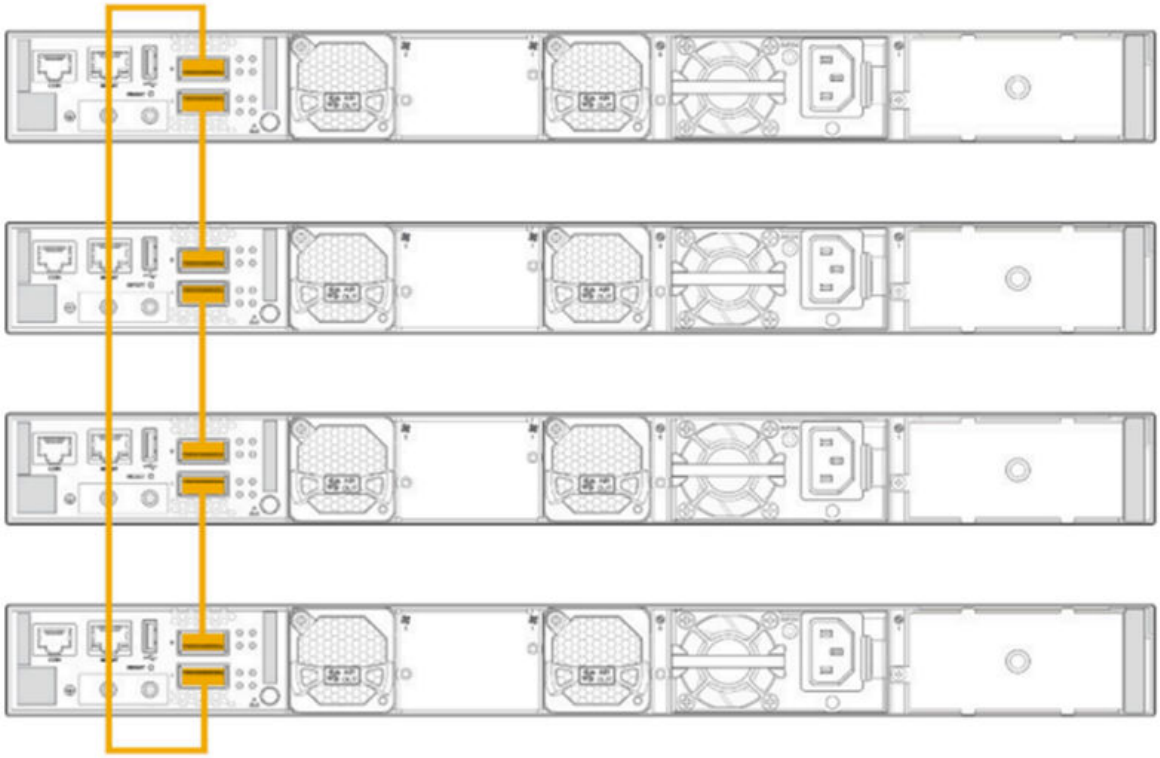
NOTE: The **Modify Virtual Chassis** option is available for switches that have the configuration management enabled in Juniper Mist.

You can configure the Virtual Chassis in mixed mode or non-mixed mode. A Virtual Chassis that includes switches of the same model operates as a non-mixed Virtual Chassis. However, a Virtual Chassis that includes different models of the same switch operates in mixed mode because of architecture differences between the different switch models. For more information, see "Mixed and Non-Mixed Virtual Chassis" on page 25.

To configure a Virtual Chassis using EX3400, EX4000, EX4100, EX4100-F, EX4100-H, EX4300, or EX4400 Switches:

1. Ensure that all the switches that you want to include in the Virtual Chassis are onboarded to the Juniper Mist cloud and assigned to the same site. To onboard a new switch (greenfield deployment), see Onboard Switches to Mist Cloud. To onboard an existing switch (brownfield deployment), see Onboard a Brownfield Switch.
2. Power off the switches that you want to include in the Virtual Chassis.
3. Connect the switches to each other using the dedicated VCPs, preferably in a full ring topology, as shown below. The following is a sample image. The location of the VCPs will vary depending on the switch models.

Figure 12: Virtual Chassis VCP connection as Ring



4. Power on the switches.
5. Wait for the MST LED on the primary and backup switches to come up. The LED appears solid on the primary switch. On the backup switch, the LED stays in a blinking state.

   NOTE: The MST LED remains off on the switches elected as the linecard members in a Virtual Chassis.

6. A Virtual Chassis is now physically formed but not preprovisioned.

   Connect the Virtual Chassis to the Juniper Mist cloud by connecting the uplink port on the primary switch to the upstream switch.

   We recommend connecting the uplink port only after the Virtual Chassis has formed. Wait for the MST LEDs to come up (LED appears solid on the primary member and blinking on the backup member), then connect the uplink ports on those members.

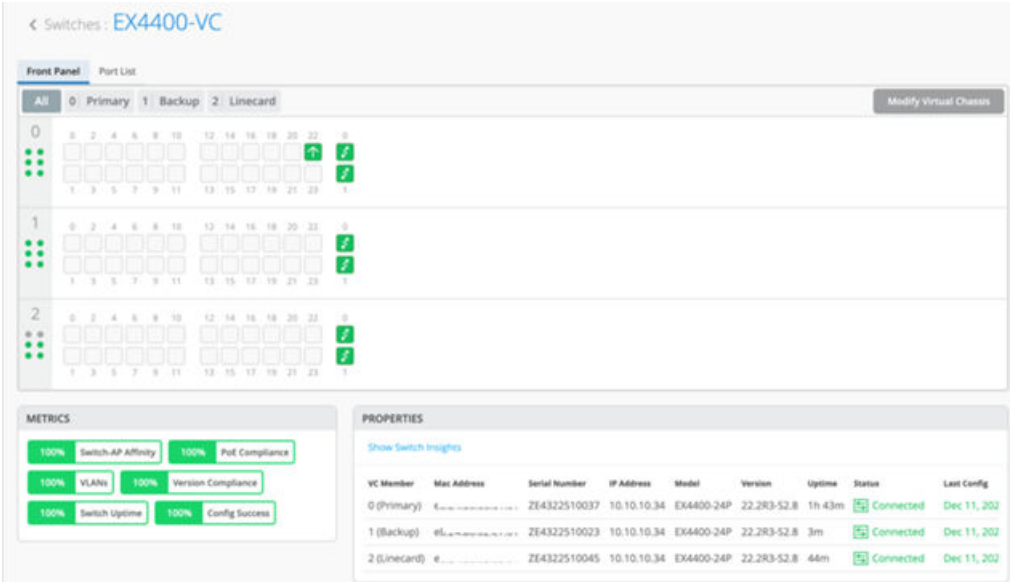
   This step initiates a ZTP process on the Virtual Chassis and connects it to the Juniper Mist cloud.

   After a Virtual Chassis connects to the Juniper Mist cloud for the first time, it may take 5 to 10 minutes for the Virtual Chassis stats to appear on the Juniper Mist cloud for all the members.

7. Click **Switches > Switch Name** to go to the Virtual Chassis page (the switch details page) to verify the details.

   The switches appear as a single Virtual Chassis as shown below:

Figure 13: Virtual Chassis in Mist GUI



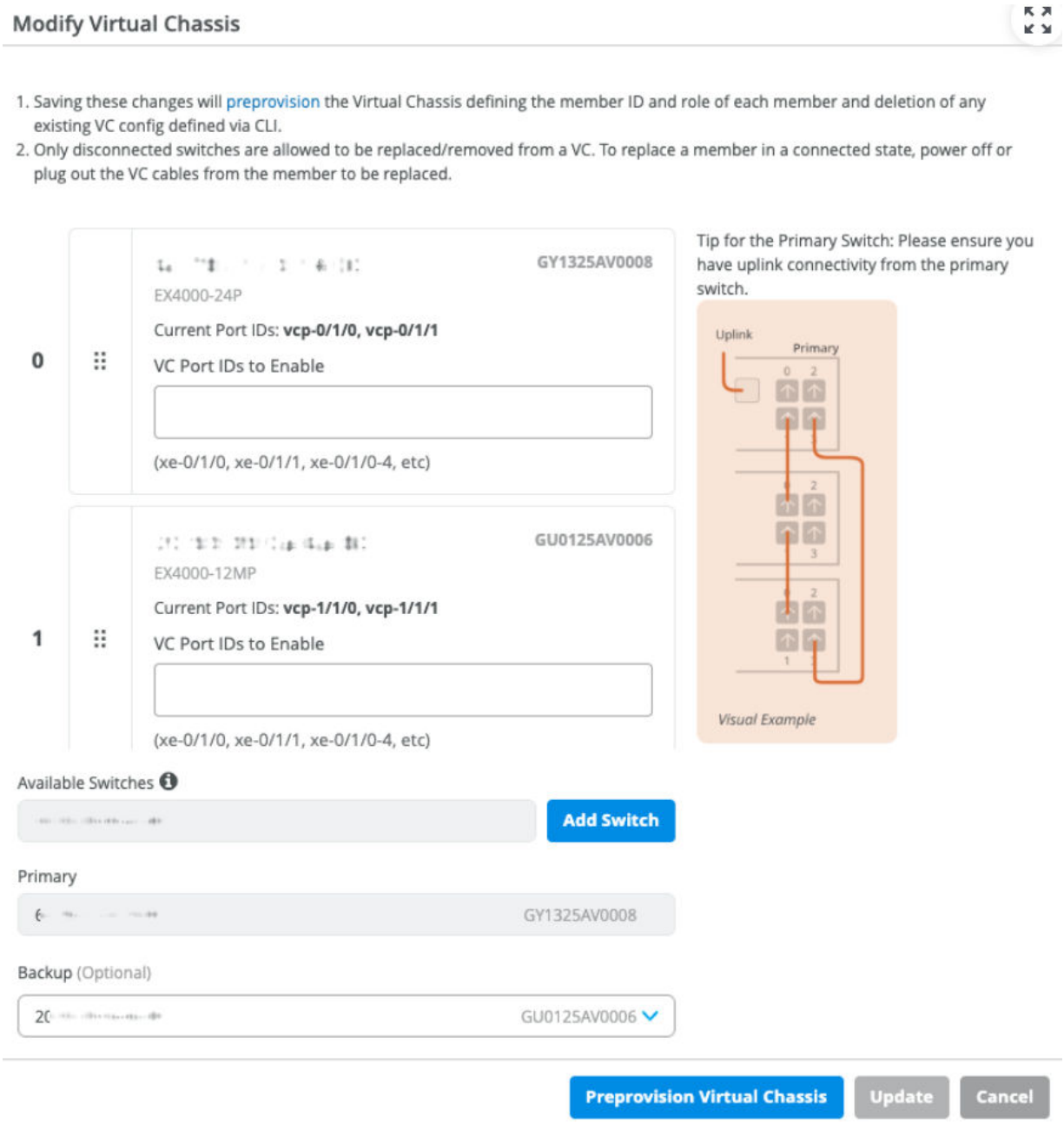
8. After the Virtual Chassis is connected to the Juniper Mist cloud, preprovision it. Preprovisioning allows users to define the roles and renumber appropriately. To preprovision the Virtual Chassis, follow the steps below:

   a. On the switch details page, click **Modify Virtual Chassis**.

      The Modify Virtual Chassis page appears.

   b. On the Modify Virtual Chassis page, click **Preprovision Virtual Chassis**. See a sample Modify Virtual Chassis page below:

Figure 14: Modify Virtual Chassis dialogue



This step pushes the preprovisioned Virtual Chassis configuration to the device and overwrites the old autoprovision Virtual Chassis configuration pushed to the device during the ZTP process. This option assumes the current positioning of the members and preprovisions them as is.

NOTE: If you make any changes on the Modify Virtual Chassis page, such as moving the members around or adding or removing members, the Preprovision Virtual Chassis button is disabled and the Update button is enabled. In this case, click the **Update** button to effect the changes made and preprovision the Virtual Chassis.

All configurations are pushed instantly after you preprovision the Virtual Chassis. The stats could take up to 15 minutes to appear on the Juniper Mist dashboard.

Workflow for Virtual Chassis Formation With Juniper Mist for EX2300, EX4650 and QFX5120

NOTE: Virtual Chassis formation on the following EX Series Switches cannot be executed without preprovisioning. You may need to enable this in a lab or staging environment where you have proper access to the Juniper Mist cloud managing the devices so that they appear on the **Inventory** page. This must be done before you can execute the Virtual Chassis creation.

The EX2300, EX4650, and QFX5120 Switches do not form a Virtual Chassis by default, as these switches don't have dedicated VCPs. Therefore, to create a Virtual Chassis with these switches, you need to use the Form Virtual Chassis option on the Juniper Mist™ portal. The **Form Virtual Chassis** option applies only to the EX2300, EX4650, and QFX5120 switches. This workflow creates a preprovisioned Virtual Chassis configuration. Juniper Mist supports only the preprovisioned Virtual Chassis configuration.

The procedure to configure a Virtual Chassis using the EX3400, EX4000, EX4100, EX4100-F, EX4100-H, EX4300, or EX4400 switches is different, as those switches have dedicated VCPs. For more information, see "Workflow for VC formation with Mist for EX3400, EX4000, EX4100, EX4100-F, EX4100-H, EX4300, EX4400 & EX4600" on page 27.

To configure a Virtual Chassis using EX2300, EX4650, or QFX5120 switches:

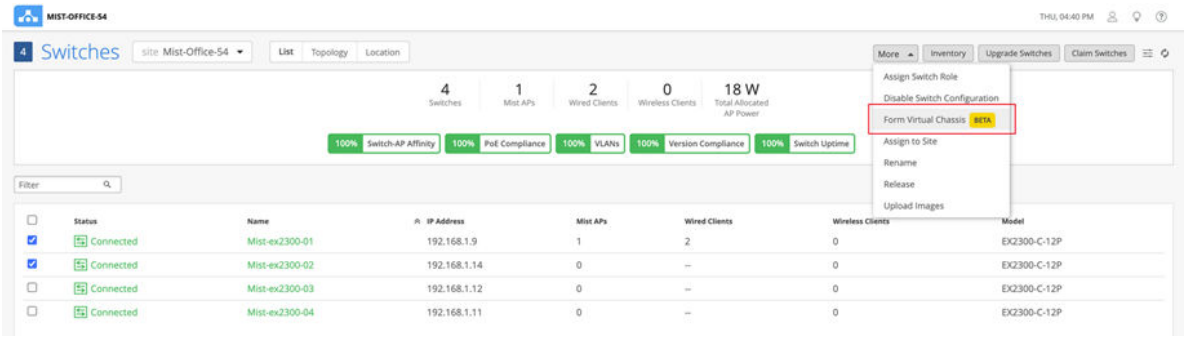
1. Connect the switches to the Juniper Mist cloud. Ensure that you have an uplink connection directly to the switch.
2. Ensure that all the switches that you want to include in the Virtual Chassis are onboarded to the Juniper Mist cloud and assigned to the same site. Also, ensure that configuration management is enabled on the switches.
3. Click the **Switches** tab on the left to navigate to the Switches page.

4. Select the switches that you want to include in the Virtual Chassis.

   An EX2300 switch variant can form a Virtual Chassis with any EX2300 switch variants. An EX4650 variant switch can form a Virtual Chassis with any EX4650 switch variants. A QFX5120 switch variant can form a Virtual Chassis only with the same QFX5120 switch variant. Therefore, the **Form Virtual Chassis** option is available only if you select the right switch models for a Virtual Chassis.

5. Click **More > Form Virtual Chassis**.

Figure 15: Form Virtual Chassis

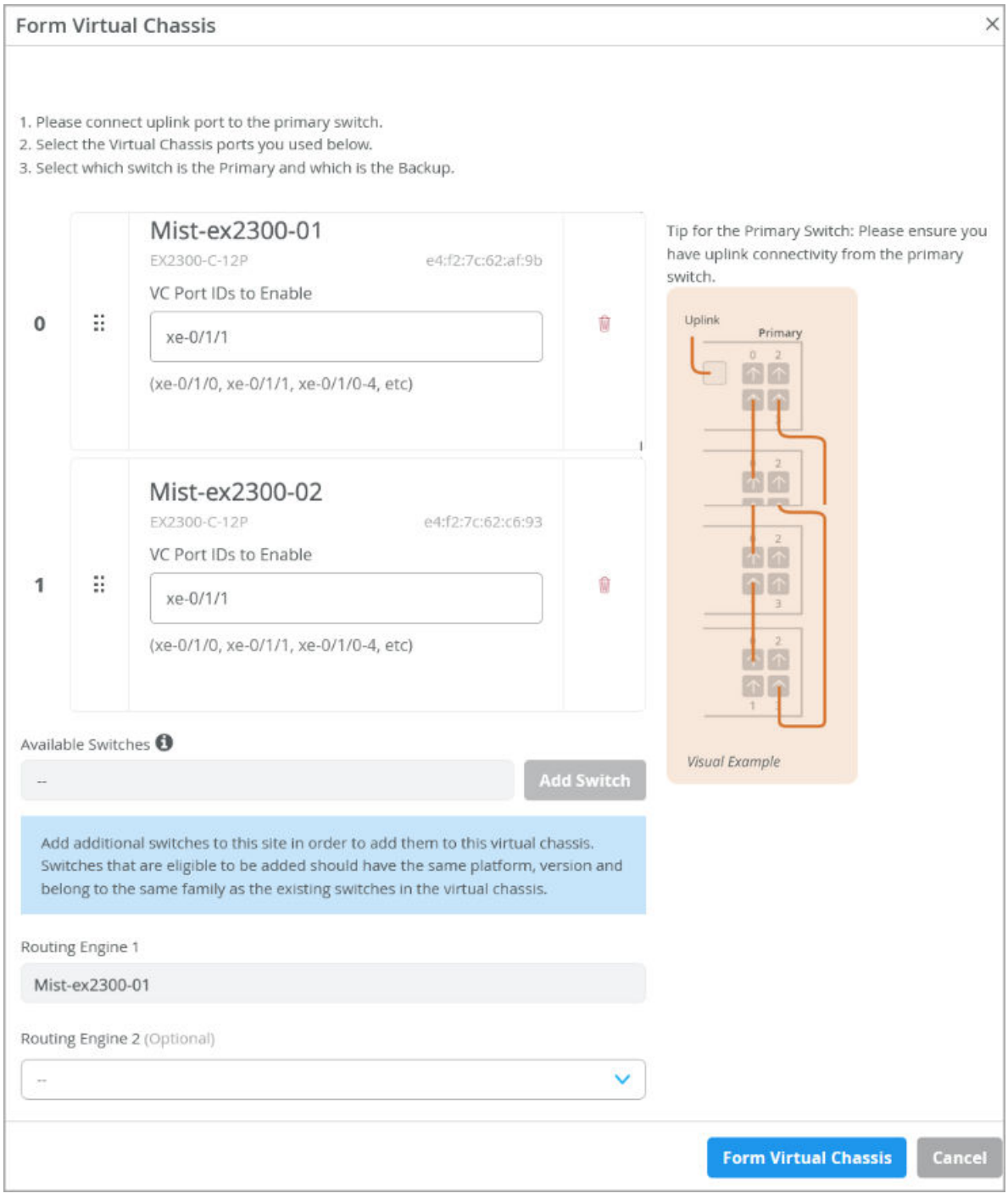


NOTE: You can see the **Form Virtual Chassis** option only if:The selected switches are running the same Junos OS version and have the configuration management option enabled.All the selected switch models are supported by the Virtual Chassis.

You can also create Virtual Chassis from the switch details page by using the **Utilities > Form Virtual Chassis** option.

The Form Virtual Chassis window appears, as shown in the following example.

Figure 16: Utilities option



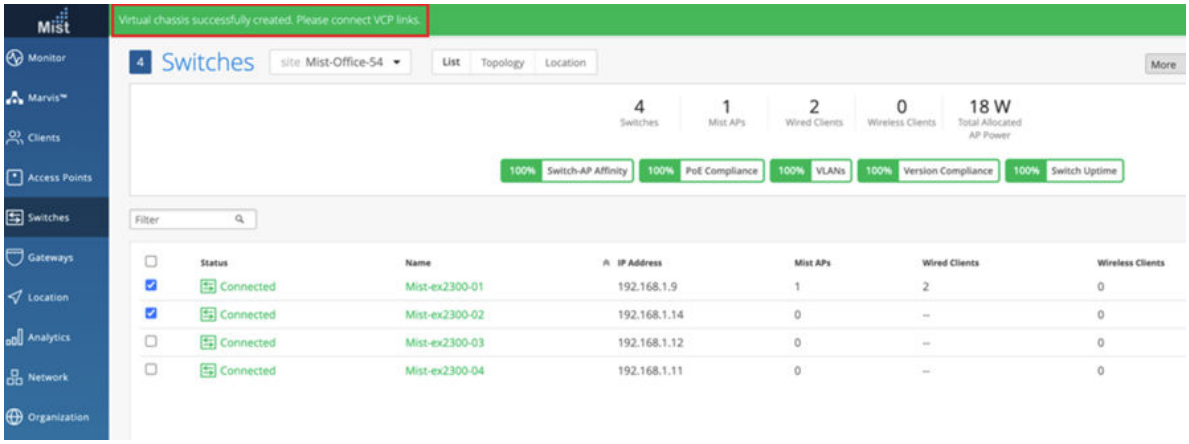
> **NOTE**: This example shows two switches included in the Virtual Chassis. A Virtual Chassis device created using EX2300 or EX4650 switches supports up to 4 switches. All switches, except those assigned Routing Engine roles, function as linecard members.

6. On the Form Virtual Chassis window, specify the following:
   a. **Port IDs** for the switches. These are IDs for the VCPs. This window displays all the switches you selected from the Switches page.
   b. The **Routing Engine 1** switch. The switch that you selected first is shown as the Routing Engine 1 switch by default. You can modify that.
   c. The **Routing Engine 2** switch. This configuration is optional. If you don't select a switch to function in the Routing Engine 2 role, Mist assigns the linecard role to that switch.

      > **NOTE**: Juniper Mist automatically upgrades a Virtual Chassis linecard member if it is running a Junos OS version different from that of the primary member. The linecard member will be upgraded to the same version as the primary member if the following conditions are met:The switch must form a Virtual Chassis with three or more members—that is, a primary, a backup, and a linecard member.The Junos OS version on the linecard member is different from that on the primary member.The linecard member must be in Inactive state. Note that a linecard member will be upgraded only if it is inactive and running a clearly different Junos OS version. Minor differences, such as different spin numbers, will not trigger an upgrade.Only the Junos OS versions listed on the Juniper Mist portal are available for upgrade.

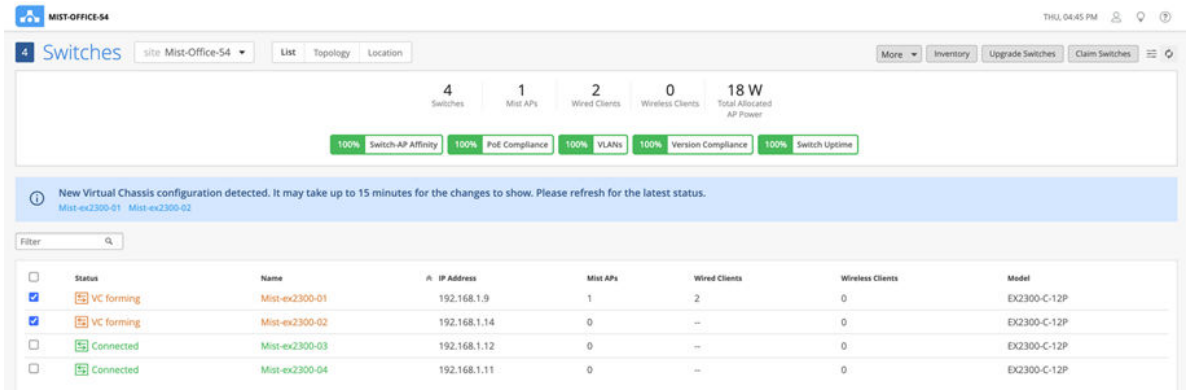
      This operation converts the ports to VCPs and also preprovisions the Virtual Chassis.

7. Click **Form Virtual Chassis** and wait for the Virtual Chassis to be created.
   The Switches page shows a message indicating that you must connect the switches to each other using the VCPs.

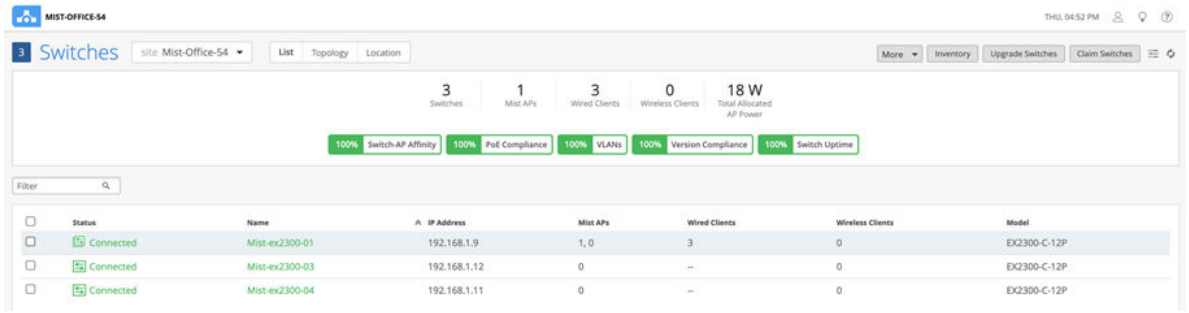


8. Connect the switches to each other using the configured VCPs.

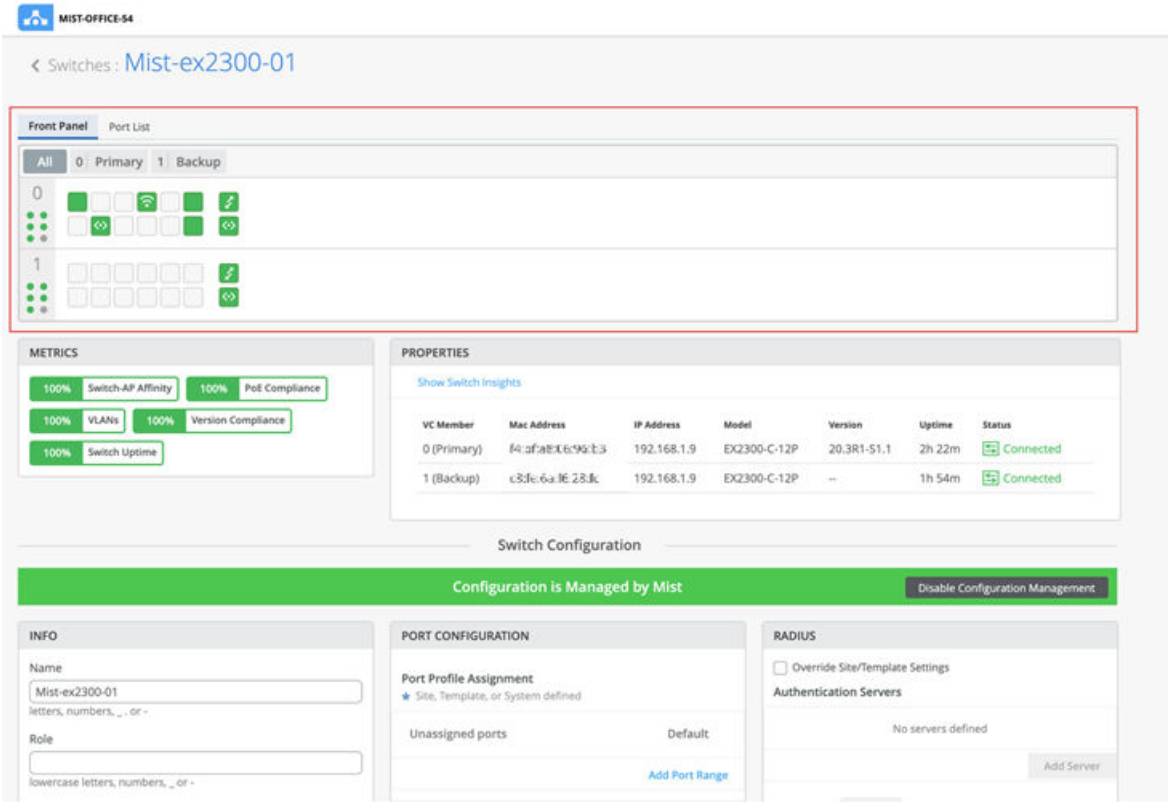
   When the Virtual Chassis formation is in progress, the Switches page shows the switch status as **VC forming**.



After the Virtual Chassis formation is successful, the Switches page displays only one entry for the Virtual Chassis with the name of the primary switch. However, the **Mist APs** column displays one AP for each Virtual Chassis member in a comma-separated format.



The switch details page displays the front panel of all the Virtual Chassis members.



NOTE: Once the Virtual Chassis is formed, if you need only one uplink to the Virtual Chassis, maintain the uplink to the primary switch and remove uplinks from the other switches.

You can use the **Modify Virtual Chassis** option on the switch details page to renumber and replace Virtual Chassis members and add members to a Virtual Chassis connected to the Juniper Mist cloud. For more information, see "Manage a Virtual Chassis Using Mist (Add, Delete, Replace, and Modify Members)" on page 203 .

Workflow for VC formation With Juniper Mist for EX4400-24X

NOTE: Virtual Chassis formation on the following EX Series Switches cannot be executed without preprovisioning. You may need to enable this in a lab or staging environment where you have proper access to the Juniper Mist cloud managing the devices so that they appear on the Inventory page. For EX4400-24X switches, plan to have serial console access when preprovisioning the Virtual Chassis.

1. Unbox and power on the EX4400-24X switches.

2. Cloud reachability — Connect the 10GbE front panel ports or plug in a relevant uplink module on the EX4400-24X from each member of the Virtual Chassis to each of the upstream device(s) such as the WAN router and make sure the links come up as connected and able to reach the Juniper Mist cloud.

3. Onboard the switch on the Juniper Mist dashboard:

   a. Claim method (Preferred): Please review the chapter ""Activating a Greenfield Switch via claim and ZTP-based installation" on page 109" below using QR-Code and Mist App / Mist dashboard.

   b. Adopt method: Please review the chapter ""Activating a Brownfield Switch via Adoption Code-Based Installation" on page 112" below.

4. When using the claim method, the devices should appear in the Inventory of the Juniper Mist cloud automatically as part of the process. Using the adopt method, the switches may appear immediately or after the Virtual Chassis has been formed.

   The steps below detail forming a Virtual Chassis from the two EX4400-24X switches as an example:

5. Connect the VCPs on EX4400-24X using DAC Cables — 40G/100G. The VCPs are located on the front panel on the EX4400-24X (as indicated in the figure below) and only support the HGoE protocol for Virtual Chassis formation.

6. Using either remote console or a serial console cable connected directly to the first switch that will become the primary switch of your Virtual Chassis, login to the Junos OS CLI and enter the following command: `request virtual-chassis mode hgoe <reboot>`

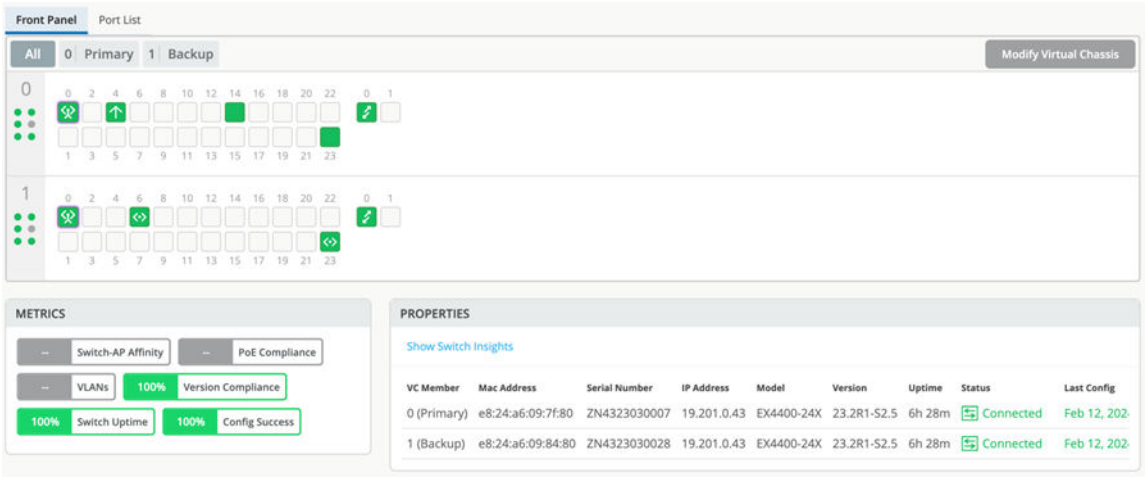
7. This CLI command is needed to convert the two front panel ports on the EX4400-24X switches from network ports to VCPs to enable Virtual Chassis formation. See an example in the figure below.

```
mist@e824a6097f80> request virtual-chassis mode hgoe
fpc0:
--------------------------------------------------------------------------
Mode set to 'Virtual Chassis with hgoe mode enabled'.  (Reboot required)
```

8. Make sure the switch reboots now.

9. Repeat the command on your backup switch followed by a reboot. Also repeat the command and reboot any optional linecard switches.

10. Once the devices come up after the reboot, they should be in Virtual Chassis mode and seen as a single device on the Juniper Mist dashboard:

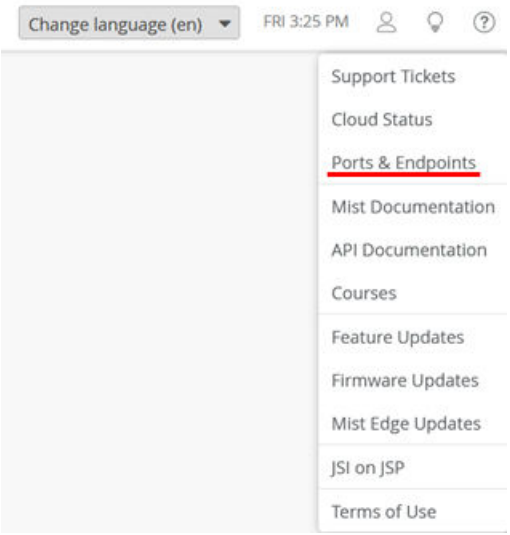


11. OPTIONAL: Check the Virtual Chassis state using remote shell as shown in the figure below:

```
mist@EX4400-24x_VC> show virtual-chassis

Virtual Chassis ID: 0c5a.2d83.7aaa
Virtual Chassis Mode: Enabled
                                                Mstr           Mixed Route Neighbor List
Member ID  Status   Serial No    Model          prio  Role      Mode  Mode ID  Interface
0 (FPC 0)  Prsnt    ZN4323030007 ex4400-24x     128   Master*      N  VC   1  vcp-255/1/1
1 (FPC 1)  Prsnt    ZN4323030028 ex4400-24x     128   Backup       N  VC   0  vcp-255/1/0

Member ID for next new member: 2 (FPC 2)

{master:0}
```

How Does an EX Series Switch Connect to the Juniper Mist Cloud to Get Managed?

When an EX Series Switch must be managed by the Juniper Mist cloud, it must have a way to exchange data with the nearest reachable Juniper Mist cloud. You can't use an EX Series Switch in air-gapped environments that do not provide Internet access. Should there be a firewall between the EX Series Switch and the Juniper Mist cloud, please check the link in your Mist account for "Ports & Endpoints" to configure the firewall to allow this traffic.



To avoid needing to use a console connection to pre-stage the device to apply a configuration, the switch should get a DHCP lease from the local network like any other wired or wireless client. Typically, the local WAN router runs a DHCP server configured to provide DHCP leases and access towards the Juniper Mist cloud for the attached switch.

Below, we show the factory default configuration that is expected to be on the switch when powering it on for the first time.

```
root@access1> edit
root@access1# load factory-default
warning: activating factory configuration
.
root@access1# show
system {
.
    phone-home {
        server https://redirect.juniper.net;
        rfc-compliant;
    }
    ## Warning: missing mandatory statement(s): 'root-authentication'
}
.
interfaces {
    ge-0/0/0 {
        unit 0 {
            family ethernet-switching {
                storm-control default;
            }
```

```
        }
    }
.
# we skipped showing the configuration of the other revenue interfaces
.
    irb {
        unit 0 {
            family inet {
                dhcp;
            }
        }
    }
    vme {
        unit 0 {
            family inet {
                dhcp;
            }
        }
    }
}
forwarding-options {
    storm-control-profiles default {
        all;
    }
}
protocols {
    lldp {
        interface all;
    }
    lldp-med {
        interface all;
    }
    igmp-snooping {
        vlan default;
    }
    rstp {
        interface all;
    }
}
poe {
    interface all;
}
vlans {
```

```
    default {
        vlan-id 1;
        l3-interface irb.0;
    }
}
```

In its factory default configuration, the switch is set to obtain a DHCP lease through various interfaces, install a default route, and attempt to connect to the Juniper Mist cloud for management. The switch automatically initiates communication with the Juniper Mist cloud, operating under the assumption that source NAT is applied somewhere along the network path to the cloud. With the default DHCP lease obtained, the switch is managed by two major methods of operation:

- The DHCP lease can be obtained by the dedicated out-of-band management port (may be labeled differently on the QFX Series and EX9200 line of Switches). This port is referred to as “me0” in Junos OS and the DHCP lease will be assigned to the virtual interface called “vme” (it’s referred to as “fxp0” on the EX9200 line of Switches). The usage of dedicated out-of-band management ports is designed for and typically used by campus fabric setups.

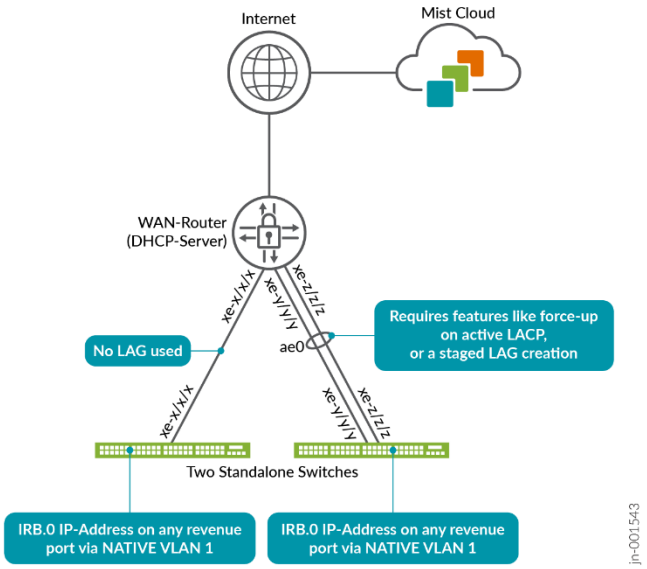
- The DHCP lease can be obtained by any regular revenue port on the switch. The factory-default configuration configures a native default VLAN on all revenue ports and maps that VLAN into the integrated routing and bridging (IRB) interface called “irb.0”. The DHCP lease is then assigned to this virtual interface. All other VLANs are assumed to use the same interface as trunked VLANs with IEEE 802.1q tags assigned. This in-band management method is very popular in branch deployments as you do not need extra cables just to manage the switch itself. Instead, you multiplex the upstream traffic into the same link and separate by means of regular VLANs.

A standalone switch for the recommended in-band management method can be attached to the WAN router via:

- A single link which is not redundant. The native VLAN over which the switch is managed from the Juniper Mist cloud is there as an initial link where the WAN router side might just be an access VLAN when starting. Over time you can change the two sides without losing the ability to manage the switch as long as you have a VLAN natively configured that continues to have the managed switch providing connection towards the Juniper Mist cloud.

- Multiple links that are redundant. It’s assumed in this case that both sides are able to configure IEEE 802.ad link aggregation and active LACP to detect outages of any configured link. As the link aggregation is not configured initially on the EX Series Switch, you must first ensure that it is able to get a successful connection towards the Juniper Mist cloud and then reconfigure the links as a LAG with active LACP. There are multiple options of how you can achieve this which are explained in the next chapter “"Best practices when using Link Aggregation on the uplink Interfaces" on page 48”.

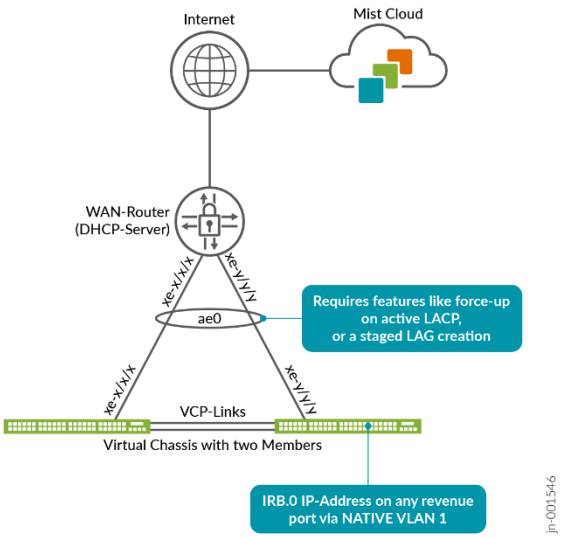
Figure 17: Switch In-Band Management



For a Virtual Chassis that uses in-band management, we recommend avoiding relying on a single uplink, even if it is technically supported. Instead, use multiple uplinks combined into a LAG with active LACP enabled. Ideally, each uplink should be connected to a different member switch within the Virtual Chassis, as illustrated below.

Since link aggregation is not configured by default, you must first ensure that the Virtual Chassis can successfully connect to the Juniper Mist cloud before reconfiguring the uplinks into a LAG with active LACP. Several methods can be used to accomplish this, which are described in the next chapter, "Best practices when using Link Aggregation on the uplink Interfaces" on page 48.

Figure 18: Virtual In-Band Management




```
root@EX3400> show interfaces terse
Interface               Admin Link Proto    Local                 Remote
ge-0/0/0                up    down
ge-0/0/0.0              up    down eth-switch
ge-0/0/1                up    up
ge-0/0/1.0              up    up   eth-switch
ge-0/0/2                up    up
ge-0/0/2.0              up    up   eth-switch
ge-0/0/3                up    up
ge-0/0/3.0              up    up   eth-switch
.
irb                     up    up
irb.0                   up    up   inet     10.33.33.11/24
.
vme                     up    up
vme.0                   up    up   inet
.
.
root@EX3400> show arp
MAC Address       Address         Name                    Interface               Flags
ee:38:73:9a:d4:a5 10.33.33.1      10.33.33.1              irb.0 [ge-0/0/1.0]      none
.
root@EX3400> show route
```

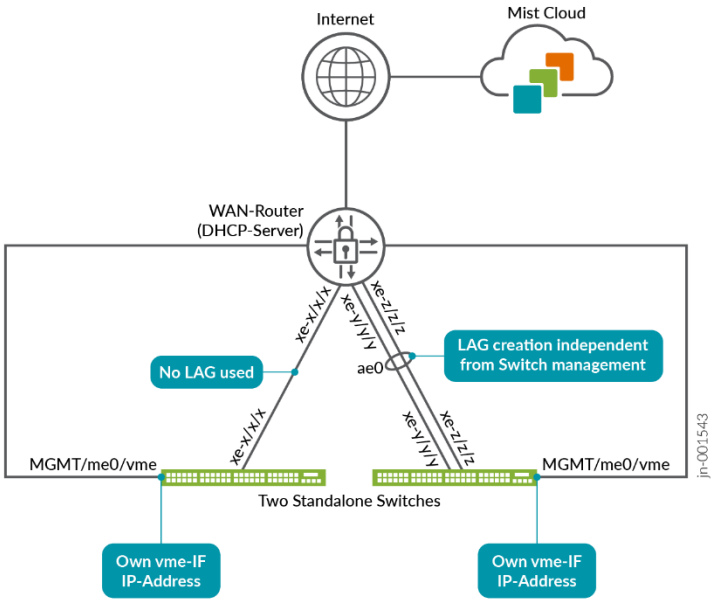
```
.
inet.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
Limit/Threshold: 32768/32768 destinations
+ = Active Route, - = Last Active, * = Both
0.0.0.0/0          *[Access-internal/12] 00:01:34, metric 0
                    >  to 10.33.33.1 via irb.0
10.33.33.0/24      *[Direct/0] 00:01:35
                    >  via irb.0
10.33.33.11/32     *[Local/0] 00:01:35
                       Local via irb.0
```

Even though it is seldom used at the branch, one may still use out-of-band management. Here, we assume for cost reasons that a branch has an out-of-band management network set up only inside a single branch and not stretched across multiple branches.

A standalone switch, when using the out-of-band management method, can be attached to the WAN router using the switch's dedicated management port. The WAN router then must provide the DHCP lease (one for each standalone switch, and one for each Virtual Chassis). Once the lease is obtained, the EX Series Switch can connect to the Juniper Mist cloud through the Internet and get managed by Mist. You have the same choice in terms of uplink to the WAN router:

- A single link which is not redundant. The management port is always configured as an access VLAN and the WAN router's port configuration does not change over time. Hence, you are free to configure the uplink at any time between the WAN router and EX Series Switch without the fear of losing the ability to manage the switch.
- Multiple links that are redundant. It's assumed in this case that both sides are able to configure IEEE 802.ad link aggregation and active LACP to detect outages of any configured link. The management port is always configured as an access VLAN, and the WAN router's port configuration does not change over time. Hence, you are free to configure the uplink at any time between the WAN router and EX Series Switch without the fear of losing the ability to manage the switch.

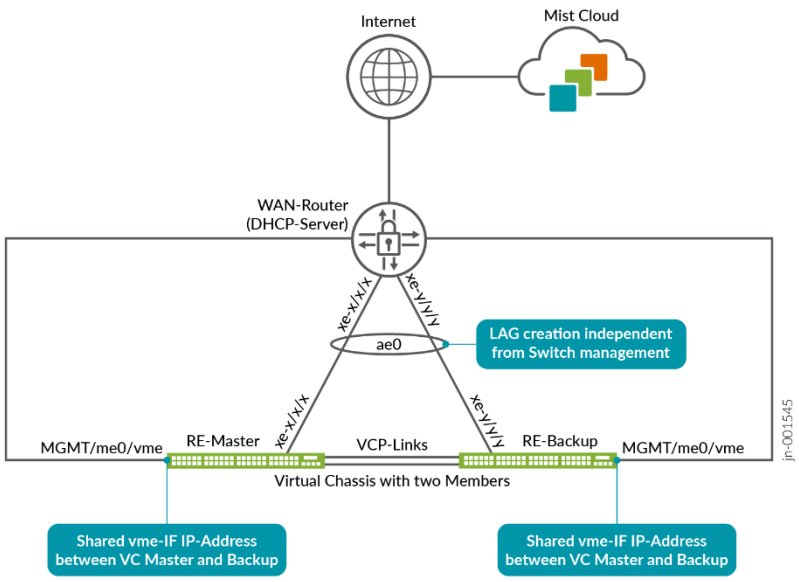
Figure 19: Switch Out-of-Band Management



For a Virtual Chassis using in-band management, we recommend avoiding using a single uplink, even though it may be technically supported. Instead, use multiple uplinks combined into a LAG with active LACP enabled.

Unlike a standalone switch, a Virtual Chassis uses only one DHCP lease for the entire system, even when it includes up to ten member switches. This is achieved through the virtual “vme” interface, which holds the DHCP lease and can move between the Primary and Backup switches as needed. Member (linecard) switches within the Virtual Chassis do not obtain their own individual DHCP leases.

Figure 20: Virtual Chassis Out-of-Band Management



When using the switch management port to perform out-of-band management, the physical port is referred to as “me0” and a virtual port named “vme” is assigned the DHCP lease in order to connect to the Juniper Mist cloud as shown below.

```
root@access1> show interfaces terse
Interface               Admin Link Proto    Local                 Remote
.
.
me0                     up    up
me0.0                   up    up   eth-switch
.
.
vme                     up    up
vme.0                   up    up   inet     192.168.10.205/24
.
.
root@access1> show route
inet.0: xyz destinations, xyz routes (xyz active, 0 holddown, 0 hidden)
Limit/Threshold: 32768/32768 destinations
+ = Active Route, - = Last Active, * = Both
0.0.0.0/0          *[Access-internal/12] 1d 02:11:06, metric 0
                    >  to 192.168.10.1 via vme.0
.
```

```
.
192.168.10.0/24    *[Direct/0] 1d 02:11:06
                    >  via vme.0
192.168.10.205/32  *[Local/0] 1d 02:11:06
                       Local via vme.0
```

Independent of whichever method of managing the switch you are using, it is assumed that the DHCP lease also contains a DNS server assignment. Hence, ICMP pings using DNS resolution like the one shown below are expected to work.

```
root@access1> ping www.google.com inet
PING www.google.com (172.217.12.100): 56 data bytes
64 bytes from 172.217.12.100: icmp_seq=0 ttl=113 time=2.750 ms
64 bytes from 172.217.12.100: icmp_seq=1 ttl=113 time=2.711 ms
64 bytes from 172.217.12.100: icmp_seq=2 ttl=113 time=2.678 ms
```

Best practices When Using Link Aggregation on the Uplink Interfaces

When creating a LAG on an EX Series Switch, whether operating as a standalone device or part of a Virtual Chassis, two main benefits are gained:

- Link redundancy is provided, so if one or more links fail, the remaining links in the bundle continue to operate without interruption.
- Higher overall throughput is achieved when multiple traffic flows are present, as these flows can be distributed across all links in the bundle. The specific load-balancing method used depends on the configuration and is not discussed in detail here.

To maximize redundancy and achieve optimal throughput, we assume both sides support the following:

- Link aggregation according to IEEE 802.3ad.
- Dead link detection when both ends of the connection have active LACP configured on each link within the bundle. Simply creating a LAG without LACP and relying on the physical layer to detect link failure is not sufficient. For example, if a LAG includes two fiber links and one of them fails, one side might still detect its interface as physically “up,” even though communication is no longer bidirectional. Using a protocol like LACP provides continuous monitoring of link status, allowing the system to quickly identify failures and maintain proper operation. It also helps trigger rebalancing of the ECMP load distribution when network topology changes occur.

This isn't a concern when using out-of-band management since the LAG link setup is independent from the device management connection to the Juniper Mist cloud. However, when using in-band management, you need to avoid losing the management connection to the switch when forming the LAG between the WAN router and the EX Series Switch. This is because when configuring active LACP for a particular side, there will be no communication on that link before the remote side has configured active LACP and exchanged LACP packets to unblock this link for communication. This leads to a kind of chicken and egg problem between the WAN router and attached EX Series Switch. You cannot have one side activating active LACP on the bundle without losing the other side. To overcome this problem, you have the following options:

- The recommended method is: Some devices (like the Juniper Networks® SRX Series Firewalls) support special features like the so called "force-up" feature. This relaxes the strict active LACP checking on one link of the WAN router's bundle. Hence, the EX Series Switch can use this link to communicate with the Juniper Mist cloud before the LAG is formed on both sides. The following describes the workflow to set this up:
  1. On the WAN router, configure the entire LAG bundle with all member links. One member link is configured with the "force-up" feature.
  2. The EX Series Switch attach comes up initially. Communication to the Juniper Mist cloud will only be possible over the WAN router link which has the force-up option set.
  3. Now you can configure the LAG bundle on the EX Series Switch with all members included. As the WAN router already has a valid configuration, the entire LAG between the two should automatically come up.
  4. Once both sides have built the LAG with active LACP running on all member links, you can remove the "force-up" feature on the WAN router side.
- If such a "force-up" feature or similar is not supported by the WAN router, then consider the next method when building the LAG:
  1. Configure the link bundle excluding one link on the EX Series Switch and let the Juniper Mist cloud push the configuration.
  2. Configure the link bundle excluding one opposite link on the WAN router and apply the configuration.
  3. Both devices should now build an LAG link with active LACP on both sides, with communication remaining on the single untouched link between the two.
  4. Now you can update the LAG bundle on the EX Series Switch with all members included. Device management is expected to now failover to the LAG bundle and continue.
  5. You can update the LAG bundle on the WAN router with all members included to reach the final state.

- The last alternative method is to pre-stage the LAG configuration on the EX Series Switch. This will ensure the needed configuration is already there and the device is already known to the Juniper Mist cloud.
  - Pre-stage the device in a lab or staging environment before shipping it on-site. You may also use this opportunity to refresh the Junos OS firmware on the device.
  - While on-site with proper instructions to the person performing the installation, consider doing out-of-band management for a short while until the LAG is configured.

The figure below shows the example configuration on an SRX as a WAN router utilizing the recommended “force-up” feature.

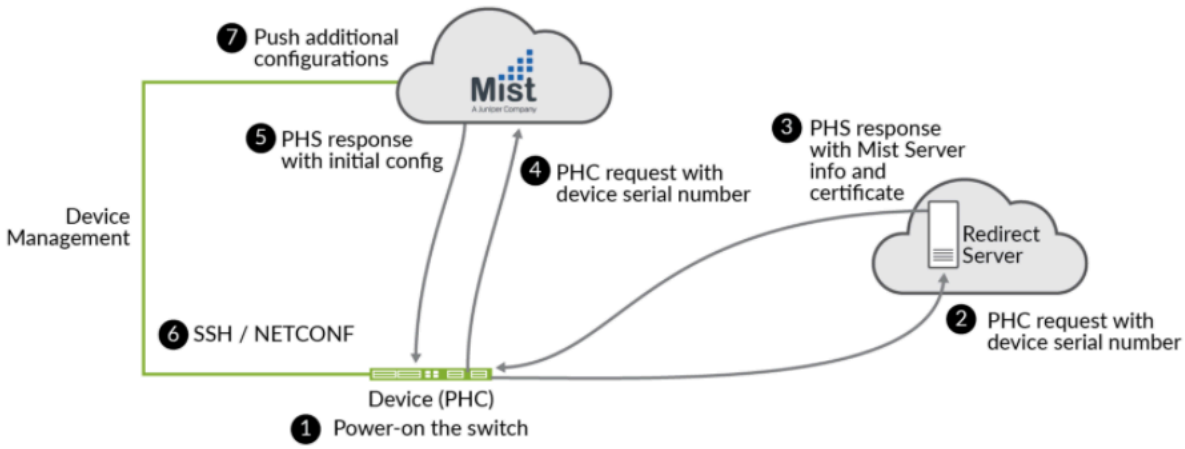
NOTE: The methods that have been presented here for connecting a WAN router and a directly connected EX Series Switch works the same in respect to a larger topology with distribution and access switches. It can be used when you build the connection between the WAN router and distribution switch and then start deploying the access switches. The “force-up” feature is available on EX Series Switches so you can use it on the distribution switches when configuring the downlinks to the access switches.

Overview of the ZTP Process

NOTE: The ZTP process described here is not to be mistaken with an older ZTP method that is described in documentation and that is also supported. That method always needs a local DHCP server that delivers special DHCP attributes within the DHCP lease to the local EX Series Switch to inform the switch where to fetch the initial configuration and other items (usually via TFTP). The ZTP method described here is free of such constraints. The local DHCP server just needs to provide regular IP address, gateway and DNS server information like that provided for any other wired or wireless client.

Once a cloud-ready switch is connected to the internet and powered on for the first time, it triggers an onboard phone-home client (PHC) to get configuration updates from the phone-home server (PHS) as shown in Figure 21 on page 51. The default behavior is for the PHC to connect to a redirect server, which then redirects it to a phone home server where the switch can get the configuration or software image. This enables the switch to obtain the most recent Junos OS configuration or software image securely and automatically, with no intervention other than physically connecting the switch to the network. Alternatively, you can configure the switch to use a DHCP server configured with the necessary ZTP options to complete the ZTP process. To revert to the ZTP default, you need to boot from factory default state (or you can issue the Junos OS `request system zeroize` command to reset the configuration).

Figure 21: Zero-Touch Provisioning Steps



Juniper ZTP follows IETF RFC 8071 as a standards-based method. The switch must be “cloud-ready” to be able to perform this operation out of the box without any additional pre-configuration needed. The Juniper Networks® Cloud-Ready Switches come ready to install and manage using the portal at https://manage.mist.com. Your switch is cloud-ready if it has a QR claim code on the front or back panel.

Figure 22: Location of Claim Code on Switch

NOTE: The onboarding procedures described in this guide apply only to cloud-ready EX and QFX switches. See Juniper Mist Supported Hardware for a list of cloud-ready EX and QFX switches.

Switch Connectivity Towards the Juniper Mist Cloud

When a switch is managed by the Juniper Mist cloud, it must initiate a connection to the cloud in order to be controlled and configured remotely. This approach is necessary because the switch typically resides behind an enterprise firewall. In most environments, several switches may be located behind the same firewall, and requiring inbound connections from the cloud would force IT staff to manually configure port forwarding for each device.

- Instead, it is more efficient for the switch to establish the outbound connection to the Juniper Mist cloud. This allows standard source NAT on the enterprise firewall or broadband router to automatically permit the connection. Once the connection is active, all communication between the switch and the cloud—including configuration updates, commands, and monitoring data—is securely multiplexed through this single, bidirectional connection. Apply the device configuration through NETCONF pushed by Juniper Mist cloud.
- Collect interface statistics and log files from the device and upload them to Juniper Mist cloud.
- Allow a remote shell using Juniper Mist portal or Websocket.
- Issue Junos OS commands on the device.

- Trigger firmware update commands on the device.

Outbound SSH Towards Juniper Mist Cloud

The capability for Junos OS devices to initiate an outbound SSH connection to a cloud-based management system has been available for several years and is not a new feature. Originally, management through the Juniper Mist cloud involved sending event scripts to the device, which were then executed locally. This approach has since been replaced with a more advanced model.

Today, once the connection to the Juniper Mist cloud is established, the cloud deploys a PyAgent to the device. This agent handles management tasks directly and offers the following advantages over the previous event script method, providing greater flexibility, reliability, and efficiency in communication and configuration management:

- Push model
- Reduced CPU load when compared with event scripts
- Better WAN utilization
- Faster event framework
- Switch statistics collection interval is 180 seconds.

Outbound SSH utilizes a destination TCP connection towards port 2200 implemented in Juniper Mist cloud initiated by the switch.

NOTE: A newer method exists that the switch can now also utilize. Read about CloudX below.

CloudX HTTPS Connectivity

Juniper CloudX, integrated natively into Junos OS, is an advanced architecture that ensures faster and secure communication between Juniper switches and the Juniper Mist cloud. It is responsible for creating a secure connection between the switch and the Juniper Mist cloud. CloudX-enabled switches can be monitored and managed by cloud services.

CloudX applies to both new and existing switches. It enables the new switches to communicate directly over HTTPS 443 when they are onboarded to Juniper Mist cloud using ZTP. With CloudX enabled, the existing switches that are connected to the Juniper Mist cloud over TCP port 2200 will have their connection switched to CloudX with no impact on the data plane. For switches to connect and communicate using CloudX over TCP 443, the following firewall port must be opened: jma-terminator.[xx].mist.com(TCP 443). The variable [xx] should be replaced by the environment name.

Benefits of CloudX:

- Keeps the data on the cloud up to date. Events are sent to the cloud every 10-15 seconds and stats are updated every 60 seconds.
- Leverages the Junos Telemetry Interface (JTI), which ensures asynchronous and faster communication by bypassing any polling from the cloud to the switch.
- Enables switches to connect to the cloud over HTTPS port 443, like Juniper APs. You do not need to open any non-standard ports on the firewall.
- Enables switches to communicate with the Juniper Mist cloud through a proxy server. You can statically define a proxy server or dynamically send proxy server details through DHCP option 43. For more information, see Connect a Switch to Mist Cloud via a Proxy Server Using CloudX.
- Offers packet capture for switches on the Juniper Mist cloud. You can initiate packet capture on a single switch port or a range of ports. You can leverage the on-demand packet capture feature in Mist to view transit traffic or control traffic. For more information, refer to "Packet capture examples" on page 225.

Availability of CloudX

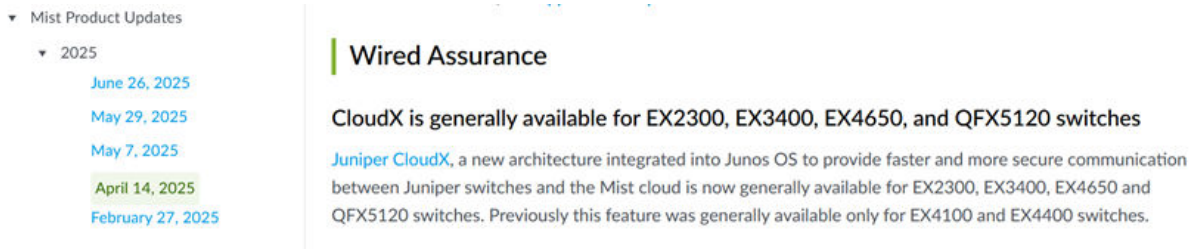
The following table lists the platforms that support CloudX in different Junos OS releases. The table lists multiple Junos OS versions for each platform. Different models (variants) within each platform are also supported. So, the EX4100-F and EX4100-H variant of the EX4100 Series is also supported. We recommend that you upgrade the switch to a Junos suggested release for the CloudX support.

NOTE: For CloudX to work, you must ensure that the firewall port towards jma-terminator.xx.mist.com is open and SSL encryption is disabled on the firewall (for more information, refer to Juniper Mist Firewall Ports and IP Addresses for Firewall Configuration). To check if your switch is communicating with Juniper Mist cloud by using CloudX, refer to the steps listed in Troubleshooting Juniper CloudX. If you still don't see CloudX enabled on your switch even after upgrading it to a supported Junos OS release, contact Juniper support.

Table 6: CloudX-Supported Platforms

Platforms	Supported Junos OS Release	CloudX Availability
EX2300/EX3400	23.4R2-S4 and above 24.2R1-S2 and above	Generally Available
EX4000	24.4R1 and above 24.4R1-S2 and above	Generally Available
EX4400/EX4100	22.4R2-S1 and above 22.4R3 and above 23.4R2 and above 24.2R1 and above	Generally Available
EX4650/QFX5120	23.4R2-S4 and above 24.2R1-S2 and above	Generally Available

Since April 2025, CloudX is also automatically activated on EX2300, EX3400, EX4650 and QFX5120 switches as mentioned in the announcement below:



Additional changes when CloudX is used:

- While CloudX enables the ability to perform packet captures and send the results towards the Juniper Mist cloud, not all platforms support that ability in hardware. Presently, only the EX4000, EX4100 and EX4400 support packet captures.
- When CloudX is enabled, the way dynamic port configuration is maintained is changed. Please review "When do we use Dynamic Port Profiles and when do we use a NAC Infrastructure?" on page 143 for more information.

Design a Switch Template

A key feature of switch management through the Juniper Mist cloud is the ability to use configuration templates and a hierarchical model to group the switches and make bulk updates. Templates provide uniformity and convenience, while the hierarchy (organization, site, and switch) provides both scale and granularity.

What templates, and the hierarchical model, means in practice is that you can create a template configuration and then apply those settings to all the devices in each group. When a conflict occurs, for example, when there are settings at both the site and organizational levels that apply to the same device, the narrower settings (in this case, the site hierarchy) override the broader settings defined at the organization level.

Individual switches, at the bottom of the hierarchy, can inherit all or part of the configuration defined at the organization level, and again at the site level. Of course, individual switches can also have their own unique configurations.

You can include individual CLI commands at any level of the hierarchy, which are then appended to all the switches in that group on an “AND” basis —that is, individual CLI settings are appended to the existing configuration (existing settings are not replaced).

We recommend that all switches in an organization be managed exclusively through the Juniper Mist cloud, and not from the device’s CLI.

The process of configuring a switch with Juniper Mist Wired Assurance involves two main steps: creating a switch configuration template and applying it to one or multiple sites. The configuration settings linked to a particular site will be applied to the switches within that site. This allows you to manage and apply consistent and standardized configurations across your network infrastructure, making the configuration process more efficient and streamlined.

For a quick overview of switch templates, watch the following video.

To configure a switch, you need to have a Super User role assigned to you. This role grants you the necessary permission to make changes and customize the switch settings. Other roles may just allow you to change a port or only to review a configuration without the ability to change it.

Create a Switch Configuration Template

Switch configuration templates make it easy to apply the same settings to switches across your sites. Whether it's one site or multiple sites, you can use the template to quickly configure new switches. When you assign a switch to a site, it automatically adopts the configuration from the associated template.

NOTE: Configuration done on the switch through the Juniper Mist dashboard overrides any configuration done through the device CLI. The switch details page doesn't display any configuration changes you make directly on the switch through the switch CLI.

To create a switch configuration template:

1. Open the portal and click **Organization > Switch Templates**.
2. Click **Create Template**, enter a name for the template in the **Template Name** field, and then click **Create**. The **Switch Templates: <Template Name>** page appears.

   NOTE: You have the flexibility to import the template settings from a JSON file instead of manually entering the information. To import the settings, click **Import Template**. To get a JSON file with the configuration settings that can be customized and imported, open an existing configuration template of your choice, and click **Export**.

3. In the **All Switches** configuration section, configure basic settings for the switches. Use the tips on the screen to configure the settings.

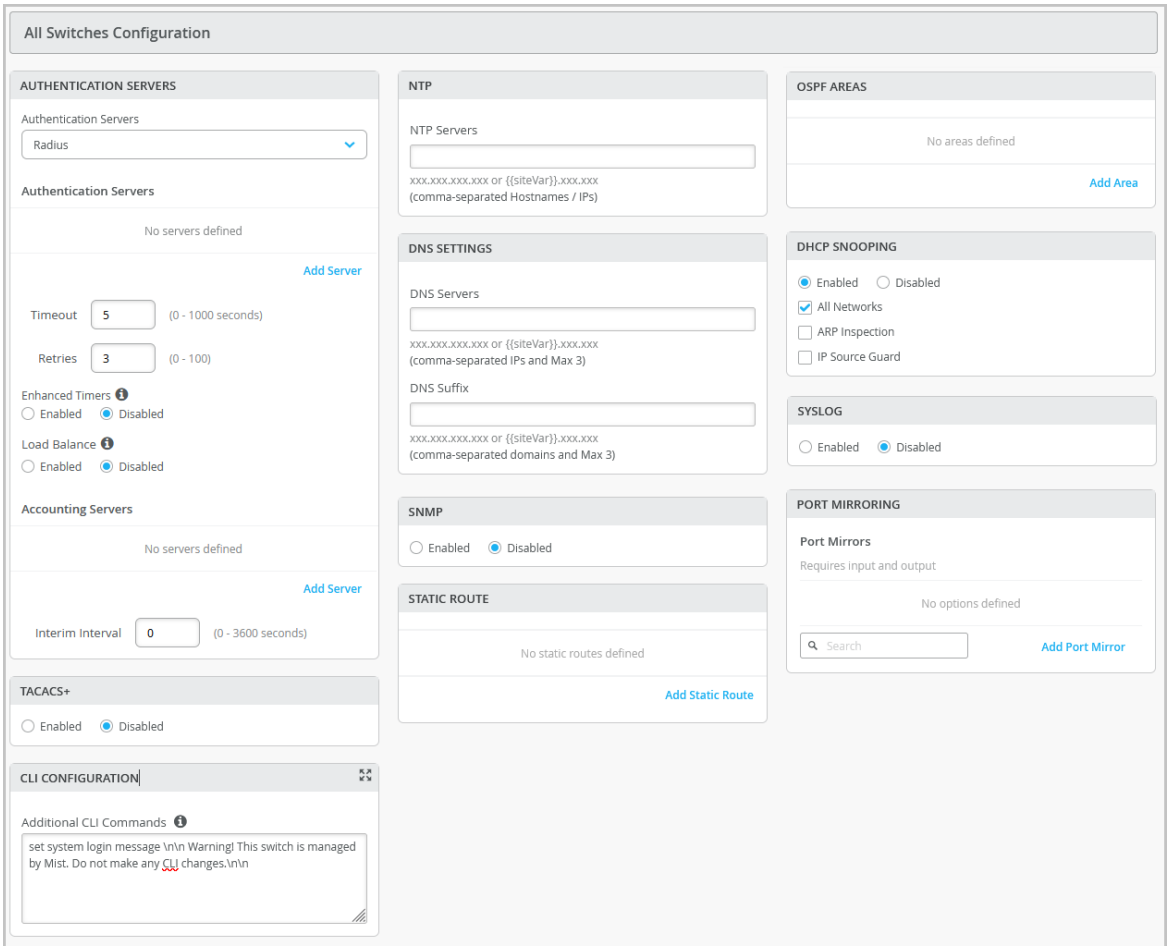

All Switches Configuration
AUTHENTICATION SERVERS
Authentication Servers
Radius
Authentication Servers
No servers defined
Add Server
Timeout
5
(0 - 1000 seconds)
Retries
3
(0 - 100)
Enhanced Timers
Enabled
Disabled
Load Balance
Enabled
Disabled
Accounting Servers
No servers defined
Add Server
Interim Interval
0
(0 - 3600 seconds)
TACACS+
Enabled
Disabled
CLI CONFIGURATION
Additional CLI Commands
set system login message \n\n Warning! This switch is managed by Mist. Do not make any CLI changes.\n\n
NTP
NTP Servers
xxx.xxx.xxx.xxx or {{siteVar}}.xxx.xxx
(comma-separated Hostnames / IPs)
DNS SETTINGS
DNS Servers
xxx.xxx.xxx.xxx or {{siteVar}}.xxx.xxx
(comma-separated IPs and Max 3)
DNS Suffix
xxx.xxx.xxx.xxx or {{siteVar}}.xxx.xxx
(comma-separated domains and Max 3)
SNMP
Enabled
Disabled
STATIC ROUTE
No static routes defined
Add Static Route
OSPF AREAS
No areas defined
Add Area
DHCP SNOOPING
Enabled
Disabled
All Networks
ARP Inspection
IP Source Guard
SYSLOG
Enabled
Disabled
PORT MIRRORING
Port Mirrors
Requires input and output
No options defined
Search
Add Port Mirror

Table 7: All Switch Configuration Field Descriptions

Field	Description
RADIUS	Choose an authentication server for validating usernames and passwords, certificates, or other authentication factors provided by users. • Mist Auth—Select this option if you want to configure Juniper Mist Access Assurance, a cloud-based authentication service from Mist, on your switch. For this option to work, you also need to use a port with dot1x or MAB authentication. Note: Mist Auth on wired switches require Junos OS 20.4R3-S7 or above, 22.3R3 or above, 22.4R2 or above, or 23.1R1 or above. To configure Juniper Mist Access Assurance features such as authentication policies, policy label, certificates, and identity providers, navigate to **Organization > Access**. • RADIUS—Select this option to configure a RADIUS authentication server and an accounting server, for enabling dot1x port authentication at the switch level. For the dot1x port authentication to work, you also need to create a port profile that uses dot1x authentication, and you must assign that profile to a port on the switch. The default port numbers are: • port 1812 for the authentication server • port 1813 for the accounting server **NOTE**: If you want to set up dot1x authentication for switch management access (for the switch CLI login), you need to include the following CLI commands in the **Additional CLI Commands** section in the template: `set system authentication-order radiusset system radius-server <radius-server-IP> port 1812set system radius-server <radius-server-IP> secret <secret-code>set system radius-server <radius-server-IP> source-address <radius-Source-IP>`
TACACS+	Configure TACACS+ for centralized user authentication on network devices. Additionally, you can enable TACACS+ accounting on the device to gather statistical data about user logins and logouts on a LAN and send this data to a TACACS+ accounting server. The port range supported for TACACS+ and accounting servers is 1 to 65535.
NTP	Specify the IP address or hostname of the Network Time Protocol (NTP) server. NTP is used to synchronize the clocks of the switch and other hardware devices on the Internet.
DNS SETTINGS	Configure the domain name server (DNS) settings. You can configure up to three DNS IP addresses and suffixes in comma separated format.

Table 7: All Switch Configuration Field Descriptions *(Continued)*

Field	Description
SNMP	Configure Simple Network Management Protocol (SNMP) on the switch to support network management and monitoring. You can configure the SNMPv2 or SNMPv3. Here are the SNMP options that you can configure: **Options under SNMPv2 (V2)** • General—Specify the system's name, location, administrative contact information, and a brief description of the managed system. When using SNMPv2, you have the option to specify the source address for SNMP trap packets sent by the device. If you don't specify a source address, the address of the outgoing interface is used by default. • Client—Define a list of SNMP clients. You can add multiple client lists. This configuration includes a name for the client list and IP addresses of the clients (in comma separated format). Each client list can have multiple clients. A client has a prefix with a /32 mask. • Trap Group—Create a named group of hosts to receive the specified trap notifications. At least one trap group must be configured for SNMP traps to be sent. The configuration includes the following fields: • Group Name—Specify a name for the trap group. • Categories—Choose from the following list of categories. You can select multiple values as there are: authentication, chassis, configuration, link, remote-operations, routing, services, startup and vrrp-events • Targets—Specify the target IP addresses. You can specify multiple targets. • Version—Specify the version number of SNMP traps. • Community—Define an SNMP community. An SNMP community is used to authorize SNMP clients by their source IP address. It also determines the accessibility and permissions (read-only or read-write) for specific MIB objects defined in a view. You can include a client list, authorization information, and a view in the community configuration. • View (Applicable to both SNMPv2 and SNMPv3)—Define a MIB view to identify a group of MIB objects. Each object in the view shares a common object identifier (OID) prefix. MIB views allow an agent to have more control over access to specific branches and objects within its MIB tree. A view is made up of a name and a collection of SNMP OIDs, which can be explicitly included or excluded. **Options under SNMPv3 (V3)**

Table 7: All Switch Configuration Field Descriptions *(Continued)*

Field	Description
	• General—Specify the system's name, location, administrative contact information, and a brief description of the managed system. When using SNMPv2, configure an engine ID, which serves as a unique identifier for SNMPv3 entities. • USM—Configure the user-based security model (USM) settings. This configuration includes a username, authentication type, and an encryption type. You can configure a local engine or a remote engine for USM. If you select a remote engine, specify an engine identifier in hexadecimal format. This ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host. If you specify the Local Engine option, the engine ID specified on the General tab is considered. If no engine ID is specified, local mist is configured as the default value. • VACM—Define a view-based access control model (VACM). A VACM lets you set access privileges for a group. You can control access by filtering the MIB objects available to read, write, and notify operations using a predefined view (you must define the required views first from the Views tab). Each view can be associated with a specific security model (v1, v2c, or usm) and security level (authenticated, privacy, or none). You can also apply security settings (you have the option to use already defined USM settings here) to the access group from the Security to Group settings. • Notify—Select SNMPv3 management targets for notifications and specify the notification type. To configure this, assign a name to the notification, choose the targets or tags that should receive the notifications, and indicate whether it should be a trap (unconfirmed) or an inform (confirmed) notification. • Target—Configure the message processing and security parameters for sending notifications to a particular management target. You can also specify the target IP address here. View (Applicable to both SNMPv2 and SNMPv3)—Define a MIB view to identify a group of MIB objects. Each object in the view shares a common object identifier (OID) prefix. MIB views allow an agent to have more control over access to specific branches and objects within its MIB tree. A view is made up of a name and a collection of SNMP OIDs, which can be explicitly included or excluded.

Table 7: All Switch Configuration Field Descriptions *(Continued)*

Field	Description
STATIC ROUTE	Configure static routes. The switch uses static routes when: • It doesn't have a route with a better (lower) preference value. • It can't determine the route to a destination. • It needs to forward packets that can't be routed. Types of static routes supported: • Subnet—Includes the IP addresses for the destination network and the next hop. • Network—Includes a VLAN (containing a VLAN ID and a subnet) and the next hop IP address.

CLI CONFIGURATION	For any additional settings that are not available in the template's GUI, you can still configure them using **set** CLI commands.
	For instance, you can set up a custom login message to display a warning to users, advising them not to make any CLI changes directly on the switch. Here's an example of how you can do it:
	`set system login message "\n\n Warning! This switch is managed by Mist. Do not make any CLI changes."`
	To delete a CLI command that was already added, use the delete command, as shown in the following example:
	`delete system login message "\n\n Warning! This switch is managed by Mist. Do not make any CLI changes."`
	NOTE: Ensure that you enter the complete CLI command for the configuration to be successful.

OSPF AREAS	Define an Open Shortest Path First (OSPF) area, if required. OSPF is a link-state routing protocol used to determine the best path for forwarding IP packets within an IP network. OSPF divides a network into areas to improve scalability and control the flow of routing information.

Table 7: All Switch Configuration Field Descriptions *(Continued)*

Field	Description
DHCP SNOOPING	Enable the DHCP snooping option to monitor DHCP messages from untrusted devices connected to the switch. DHCP snooping creates a database to keep track of these messages. This helps prevent the acceptance of DHCPOFFER packets on untrusted ports, assuming they originate from unauthorized DHCP servers. DHCP configuration has the following options: • All Networks— Select the All Networks check box to enable DHCP snooping on all VLANs. • Networks—If you want to enable DHCP snooping only on specific networks, click Add (+) in the Networks box and add the required VLANs. • Address Resolution Protocol (ARP) Inspection—Enable this feature to block any man-in-the-middle attacks. ARP Inspection examines the source MAC address in ARP packets received on untrusted ports. It validates the address against the DHCP snooping database. If the source MAC address does not have a matching entry (IP-MAC binding) in the database, it drops the packets. You can check ARP statistics by using the following CLI commands: show dhcp-security arp inspection statistics , and show log messages | match DAI . The device logs the number of invalid ARP packets that it receives on each interface, along with the sender's IP and MAC addresses. You can use these log messages to discover ARP spoofing on the network. • IP Source Guard—IP source guard validates the source IP and MAC addresses received on untrusted ports against entries in the DHCP snooping database. If the source addresses do not have matching entries in the database, IP Source Guard discards the packet. Note: IP Source Guard works only with single-supplicant 802.1X user authentication mode. Note: • If you have a DHCP server connected to an untrusted access port, DHCP won't function properly. In such cases, you may need to make adjustments to ensure that DHCP works as intended. By default, DHCP considers all trunk ports as trusted and all access ports as untrusted. • You need to enable VLAN on the switch for the DHCP snooping configuration to take effect. So, you need to apply port profiles (described later in this document) to the ports.

Table 7: All Switch Configuration Field Descriptions *(Continued)*

Field	Description
	A device with a static IP address might not have a matching MAC-IP binding in the DHCP snooping database, if you have connected the device to an untrusted port on the switch. To check the DHCP snooping database on your switch and view the bindings, use the CLI command show dhcp-security binding. This command will provide you with information about the DHCP bindings recorded in the snooping database. Note: You need to enable this feature if you want to view the DHCP issues for the switch under the Successful Connect SLE metric.
SYSLOG	Configure SYSLOG settings to set up how system log messages are handled. You can configure settings to send the system log messages to files, remote destinations, user terminals, or to the system console. Here are the configuration options available for SYSLOG settings: • Files—Send log messages to a named file. • Hosts—Send log messages to a remote location. This could be an IP address or hostname of a device that will be notified whenever those log messages are generated. • Users—Notify a specific user of the log event. • Console—Send log messages of a specified class and severity to the console. Log messages include priority information, which provide details about the facility and severity levels of the log messages. • Archive—Define parameters for archiving log messages. • General—Specify general information such as a time format, routing instance, and source address for the log messages.

Table 7: All Switch Configuration Field Descriptions *(Continued)*

Field	Description
PORT MIRRORING	Configure port mirroring. Port mirroring is the ability of a router to send a copy of a packet to an external host address or a packet analyzer for analysis. In the port mirroring configuration, you can specify the following: • Input: The source (an interface or network) of the traffic to be monitored. Along with the input, you can specify whether you want Mist to monitor the ingress traffic or the egress traffic for an interface. If you want both ingress and egress traffic to be monitored, add two input entries for the same interface - one with the ingress flag and the other with the egress flag. • Output: The destination interface to which you want to mirror the traffic. You cannot specify the same interface or network in both the input and output fields.

4. In the **Management** section of the Switch Template Configuration page, configure the following:

   a. Configuration Revert Timer—This feature helps restore connectivity between a switch and the Juniper Mist cloud if a configuration change causes the switch to lose connection. It automatically reverts the changes made by a user and reconnects to the cloud within a specified time duration. By default, this time duration is set to 10 minutes for EX Series Switches. You can specify a different time duration here.

   b. Root password—A plain-text password for the root-level user (whose username is root).

   c. Protection of Routing Engine—Enable this feature to ensure that the Routing Engine accepts traffic only from trusted systems. This configuration creates a stateless firewall filter that discards all traffic destined for the Routing Engine, except SSH and BGP protocol packets from specified trusted sources.

5. In the **Shared Elements** section, configure the following:

   a. In the **Networks** tile, click **Add Network** and configure the VLANs to be used in the port profiles. The settings include a Name, VLAN ID, and a Subnet.

   b. In the **Port Profiles** tile, choose a predefined port profile or click **Add Profile** to create a new profile and assign a network to it. Port profiles provide a way to automate provisioning of multiple switch interfaces. Use the tips on the screen to configure the port profile settings. Table 8 on page 66 for tips about key fields in the port profile.

NOTE: This table does not include basic fields such as Name, Enabled, Disabled, Description, and so on.

Table 8: Port Profile Fields

Field	Description
Mode	Trunk—Trunk interfaces typically connect to other switches, APs, and routers on the LAN. In this mode, the interface can be in multiple VLANs and can multiplex traffic between different VLANs. Specify the Port Network, VoIP Network (if applicable), and Trunk Networks. Access—Default mode. Access interfaces typically connect to network devices, such as PCs, printers, IP phones, and IP cameras. In this mode, the interface can be in a single VLAN only. Specify the Port Network and the VoIP Network (if applicable).

Table 8: Port Profile Fields *(Continued)*

Field	Description
Use dot1x authentication	Select this option to enable IEEE 802.1X authentication for Port-Based Network Access Control. 802.1X authentication is supported on interfaces that are members of private VLANs (PVLANs). The following options are available if you enable dot1x authentication on a port: Allow Multiple Supplicants—Select this option to allow multiple end devices to connect to the port. Each device is authenticated individually. Dynamic VLAN—Specify dynamic VLANs that will be returned by the RADIUS server attribute 'tunnel-private-group-ID' or 'Egress-VLAN-Name'. This configuration enables a port to perform dynamic VLAN assignment. MAC authentication—Select this option to enable MAC authentication for the port. When this option is selected, you can also specify an Authentication Protocol. If you specify a protocol, it must be used by supplicants to provide authentication credentials. Use Guest Network—Select this option to use a guest network for authentication. Then select a Guest Network from the drop-down list. Bypass authentication when server is down—If you select this option, clients can join the network without authentication if the server is down. You need to also do the following for dot1x authentication to work: • Configure a RADIUS server for dot1x authentication from the Authentication Servers tile in the All Switches Configuration section of the template. • Assign a dot1x port profile to a switch port for the RADIUS configuration to be pushed to the switch. You can do this from the Port Config tab in the Select Switches Configuration section of the template.
MAC Limit	Configure the maximum number of MAC addresses that can be dynamically learned by an interface. When the interface exceeds the configured MAC limit, it drops the frames. A MAC limit also results in a log entry. The default value: 0 Supported range: 0 through 16383
PoE	Enable the port to support power over Ethernet (PoE).

Table 8: Port Profile Fields *(Continued)*

Field	Description
STP Edge	Configure the port as a Spanning Tree Protocol (STP) edge port, if you want to enable Bridge Protocol Data Unit (BPDU) guard on a port. This setting ensures that the port is treated as an edge port and guards against the reception of BPDUs, which are control messages in the STP. If you plug a non-edge device into a port configured with STP Edge, the port is disabled. In addition, the Switch Insights page generates a Port BPDU Blocked event. The Front Panel on the Switch Details will also display a BPDU Error for this port. You can clear the port of the BPDU error by selecting the port on the Front Panel and then clicking **Clear BPDU Errors**. You can also configure STP Edge at the switch level, from the Port Profile section on the switch details page.
QoS	Enable Quality of Service (QoS) for the port to prioritize latency-sensitive traffic, such as voice, over other traffic on a port. Note: For optimal results, it's important to enable Quality of Service (QoS) for both the downstream (incoming) and upstream (outgoing) traffic. This ensures that the network can effectively prioritize and manage traffic in both directions, leading to improved performance and better overall quality of service. You have the option to override the QoS configuration on the WLAN settings page (**Site > WLANs > <WLAN name>**). To override the QoS configuration, select the Override QoS check box and choose a wireless access class. The downstream traffic (AP > client) gets marked with the override access class value specified. The override configuration doesn't support upstream traffic (client > AP).
Storm Control	Enable storm control to monitor traffic levels and automatically drop broadcast, multicast, and unknown unicast packets when the traffic exceeds a traffic level (specified in percentage). This specified traffic level is known as the storm control level. This feature actively prevents packet proliferation and maintains the performance of the LAN. When you enable Storm Control, you can also choose to exclude broadcast, multicast, and unknown unicast packets from monitoring.

Table 8: Port Profile Fields *(Continued)*

Field	Description

Persistent (Sticky) MAC Learning	Enable Persistent (Sticky) MAC to stop unauthorized devices from connecting to your network. When enabled, the switch learns the MAC addresses of devices that arrive on the port and saves them in memory. If the number of MAC addresses learned exceeds the 'MAC Limit' specified above, the port drops the frames. Also, you will see a 'MAC Limit Exceeded' event on the Insights page.
	
	You can hover over the port from the front panel on the switch details page to see the MAC Limit and the MAC Count (the number of MAC addresses that the port learned dynamically).
	
	NOTE: You cannot enable this feature on a Trunk port or on a port with 802.1X authentication, as Junos OS does not support this combination. Enable this feature for static wired clients. Do not enable it for Juniper AP interfaces.
	The portal does not show the MAC addresses that an interface has learned. It shows only the maximum MAC address count. To view the MAC addresses that an interface learned, select the **Utilities > Remote Shell** option on the switch details page and run the following commands:
	
	`show ethernet-switching table persistent-learning`
	
	`show ethernet-switching table persistent-learning interface`
	
	The MAC Count value remains on the port until you clear it from the front panel on the switch details or until you disable the Persistent (Sticky) MAC Learning feature. To clear the MAC addresses that a port learned, select the port on the switch front panel and then click Clear MAC [Dynamic/Persistent]. This action generates a MAC Limit Reset event on the Switch Insights page.

c. In the VRF tile, configure Virtual Routing and Forwarding (VRF).

d. With VRF, you can divide an EX Series switch into multiple virtual routing instances, effectively isolating the traffic within the network. You can define a name for the VRF, specify the networks associated with it, and include any additional routes needed.

> **NOTE**: You can't assign the default network (VLAN ID = 1) to a VRF.

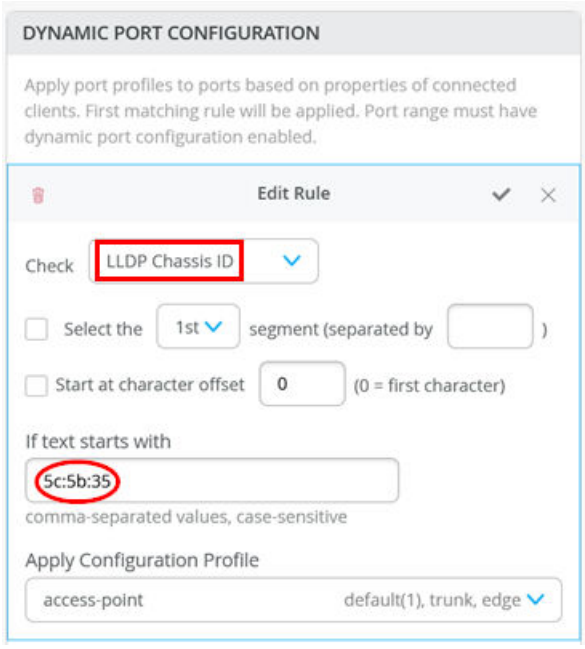
6. In the **Dynamic Port Configuration** tile, set up rules for dynamically assigning port profiles. When a user connects a client device to a switch port with this feature enabled, the switch identifies the device and assigns a suitable port profile to the port. Dynamic port profiling utilizes a set of device

properties of the client device to automatically associate pre-configured port and network settings to the interface. You can configure a dynamic port profile based on the following parameters:

- LLDP System Name
- LLDP Description
- LLDP Chassis ID
- Radius Username
- Radius Filter-ID
- MAC (Ethernet MAC address)

> **NOTE**: Avoid using Dynamic Port Configuration if the port experiences a huge number of port flaps. Each port flap will trigger a configuration change on the switch (Junos commit). In such a case it is better to apply dynamic VLAN configuration through RADIUS.

Here's an example of a rule that automatically assigns the port profile "`access-point`" to a Juniper AP. As per this rule, when the port identifies a device with a chassis ID that starts with "`5c:5b:35`", it assigns the "`access-point`" profile to the connected device.

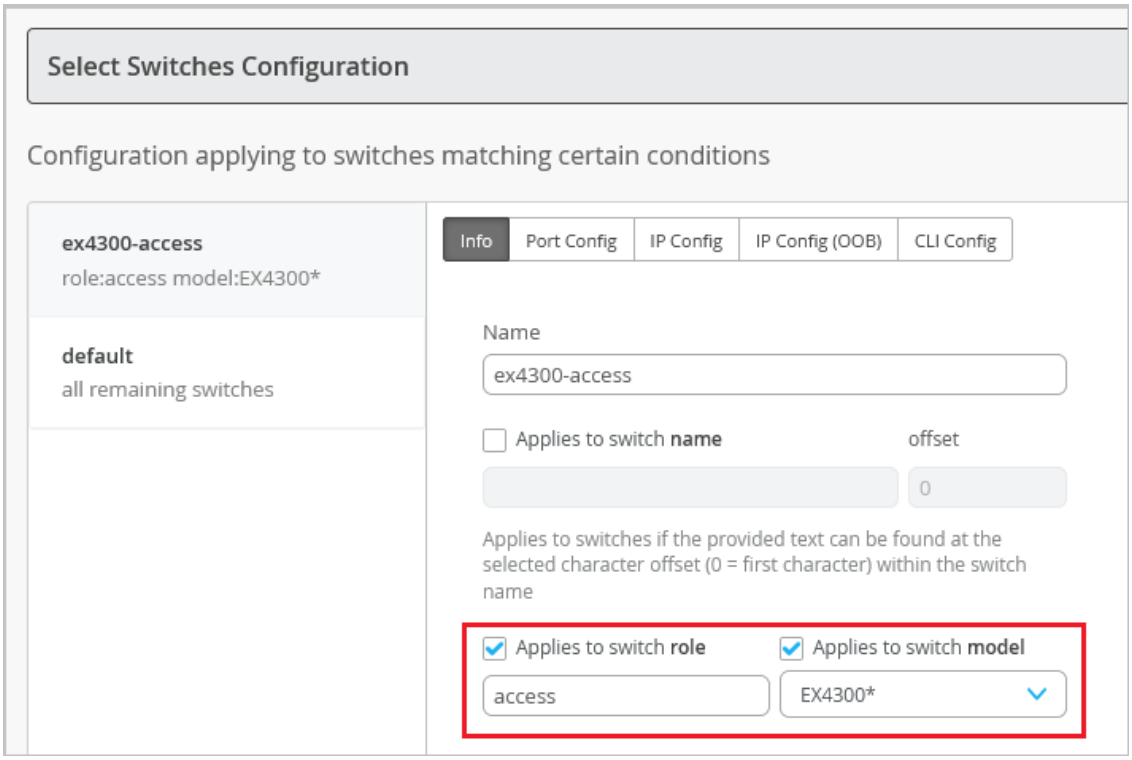


7. For your dynamic port configurations to take effect, you also need to specify the ports that you want to function as dynamic ports. You can do this by selecting the **Enable Dynamic Configuration** check box on the **Port Config** tab in the **Select Switches** section of the switch template. You can also do this at the switch level, from the **Port Configuration** section on the **Switch Details** page.

NOTE: It takes a couple minutes for a port profile to be applied to a port after a client is recognized, and a couple of minutes after that for the port profile assignment status to appear on the portal.In case of switch reboots or a mass link up or down event affecting all ports on a switch, it takes approximately 20 minutes for all the ports to be assigned to the right profile (assuming that dynamic port configuration is enabled on all the ports).

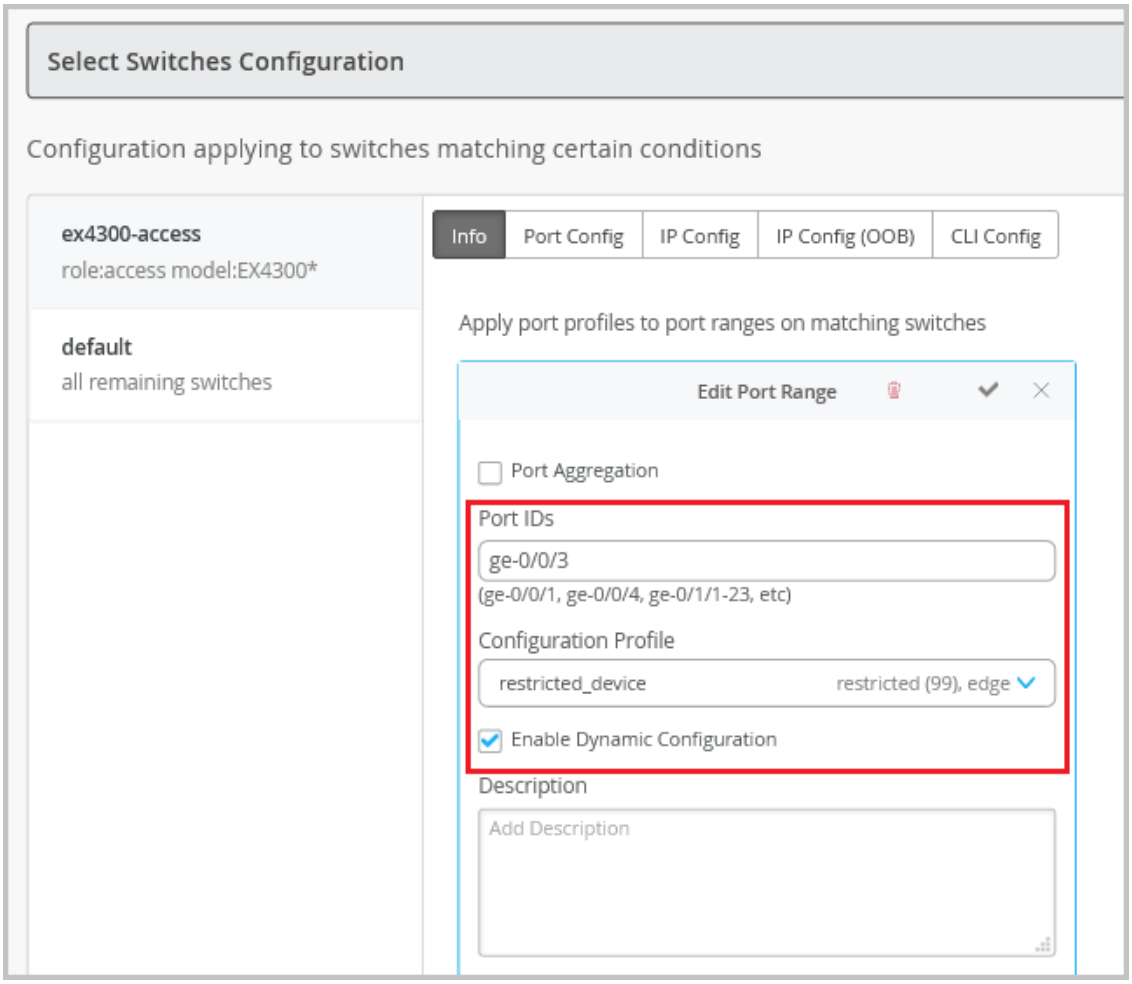
8. In the **Select Switches Configuration** section, configure the following:

   a. On the **Info** tab, create a rule to associate the shared elements with your switch. Here's an example of how to add a rule that maps the EX4300 switch to an "access" role.



9. On the **Port Config** tab, click **Add Port Range** to associate a port profile with a port. Here, you also have the following key options:

   a. Enable Dynamic Configuration on the port. Dynamic port profiling allows you to assign a dynamic profile to a connected device based on defined attributes. If the device matches the attributes, Mist assigns a matching dynamic profile to the device. But if the device doesn't match the attributes, it will be placed in a specified VLAN. In the following example, the port is enabled with dynamic port allocation and is assigned with a restricted VLAN. In this case, if the connected device doesn't match the dynamic profiling attributes, it will be placed into a restricted VLAN such as a non-routable VLAN or a guest VLAN. Interfaces enabled with Port Aggregation don't support dynamic port configuration.



b. Enable Port Aggregation. Port aggregation or link aggregation enables you to group Ethernet interfaces to form a single link layer interface. This interface is also known as a link aggregation group (LAG) or bundle. The number of interfaces that you can group into a LAG and the total number of LAGs that a switch supports vary depending on the switch model. You can use LAG with or without LACP enabled. If the device on the other end doesn't support LACP, you can disable LACP here. You can also configure the LACP force-up state for the switch. This configuration sets the state of the interface as up when the peer has limited LACP capability. You can also configure an LACP packet transmission interval. If you configure the LACP Periodic Slow option on an AE interface, the LACP packets are transmitted every 30 seconds. By default, the interval is set to fast in which the packets are transmitted every second. The following example shows the use of LAG in an uplink port configuration:

Auto

PoE

Enabled Disabled

MTU

Enabled Disabled

Description

Add Description

Up / Down Port Alerts

Enabled Disabled

Manage Alert Types in Alerts Page

Port Aggregation

Enabled Disabled

LACP

Enabled Disabled

LACP Force-UP

Enabled Disabled

LACP Periodic Slow

Enabled Disabled

AE Index (0 - 255)

Allow switch port operator to modify port profile

Yes No

c. Configure alerts and email notifications for the interface up and down events on specified ports of a switch. To configure a switch port to support alerts, select the Enable “Up/Down Port” Alerts check box. Also, on the Monitor > Alerts > Alerts Configuration page, you must select from the following check boxes to enable alerts for the ports.

   i. Critical WAN Edge Port Up

   ii. Critical WAN Edge Port Down

   iii. Critical Switch Port Up

   iv. Critical Switch Port Down

d. On the **IP Config** tab, you can specify a network for in-band management traffic.

e. On the **IP Config (OOB)** tab, you can enable a dedicated management virtual routing and forwarding (VRF) instance on the switch. Enabling this feature confines the management interface (em0/me0/fxp0,vme) to a non-default VRF instance. This feature works for standalone devices and Virtual Chassis systems running Junos OS version 21.4 or later. With the dedicated management VRF instance in place, management traffic does not have to share a routing table with other control traffic or protocol traffic.

f. On the **CLI Config** tab, include CLIs (in the set format) to configure any additional rule-based settings for which the template doesn’t provide a GUI option.

> **NOTE**: For this JVD, the section on Group-Based Policy (GBP) configuration and Switch Policies using GBP has been removed. These features are applicable only in Campus Fabric deployments with an IP Clos architecture and are not relevant for Branch network designs.

10. Click **Save** to save the switch template.

    The **Confirm changes** window appears.

11. Click **Save** on the **Confirm changes** window.

    The template is saved. To view the new template, go to **Organization > Switch Templates**.

Assign a Template to Sites

After creating a switch configuration template, you need to assign it to the relevant sites. This ensures that the configuration settings are applied to the devices within those sites. You have the flexibility to apply the template to a single site or multiple sites, depending on your specific requirements.

To assign a template to one or multiple sites:

1. Click **Organization > Switch Templates**.
   a. The Switch Templates page appears.
2. Click the template that you want to assign to sites.
   a. The Switch Templates: Template-Name page appears.
3. Click **Assign to Sites**.
   a. The **Assign Template to Sites** window appears.
4. Select the sites to which you want to apply the template and then click **Apply**.

Alternatively, you can apply a template to a site from the Site Configuration page, using the following steps:

1. Click **Site > Switch Configuration**.
2. Click a site from the list to open it.
3. Select a template from the Configuration Template field, and then click **Save**.

Precedence and Hierarchy of Configuration and Templates

Configuration templates have a hierarchy of assignments that you need to keep in mind when using them:

- All configs are inherited from a template to a site. All switches assigned to a site inherits the corresponding config.
- Each config element has an override option at both Site and Device levels making the configuration model extremely flexible.
- The precedence for configuration:
  - The configuration highest level is applied on the Switch (Device) itself > Network (Site) > Template (Org).

Configuration Hierarchy of Templates

Figure 23: Configuration Model

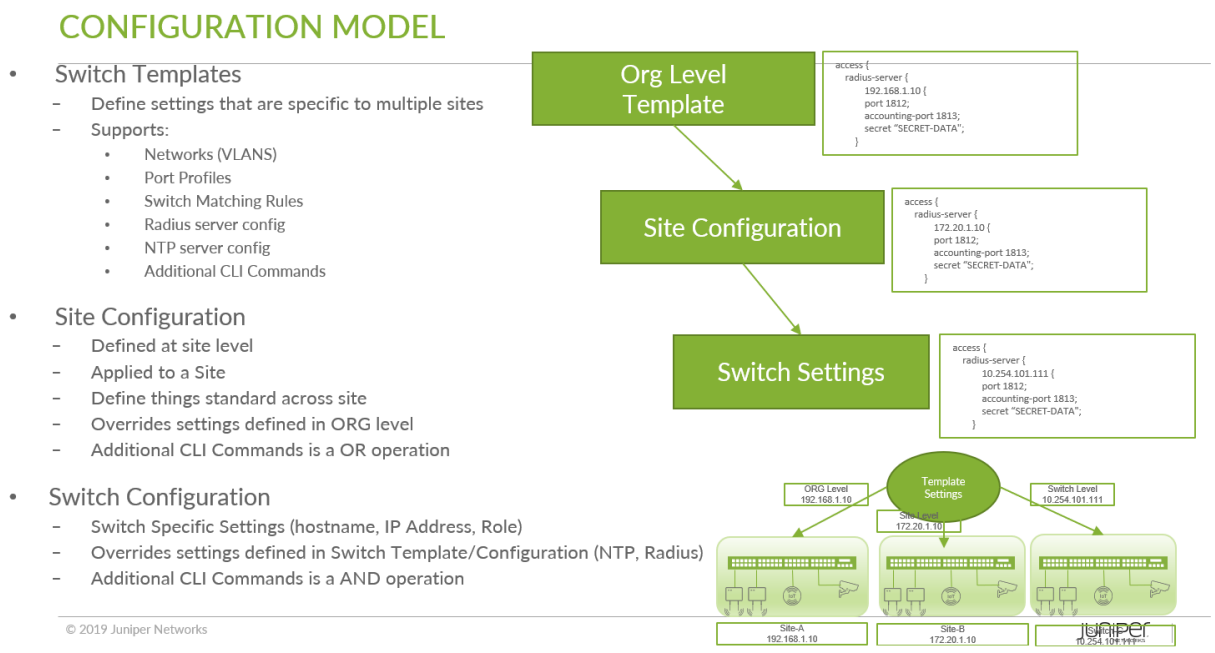
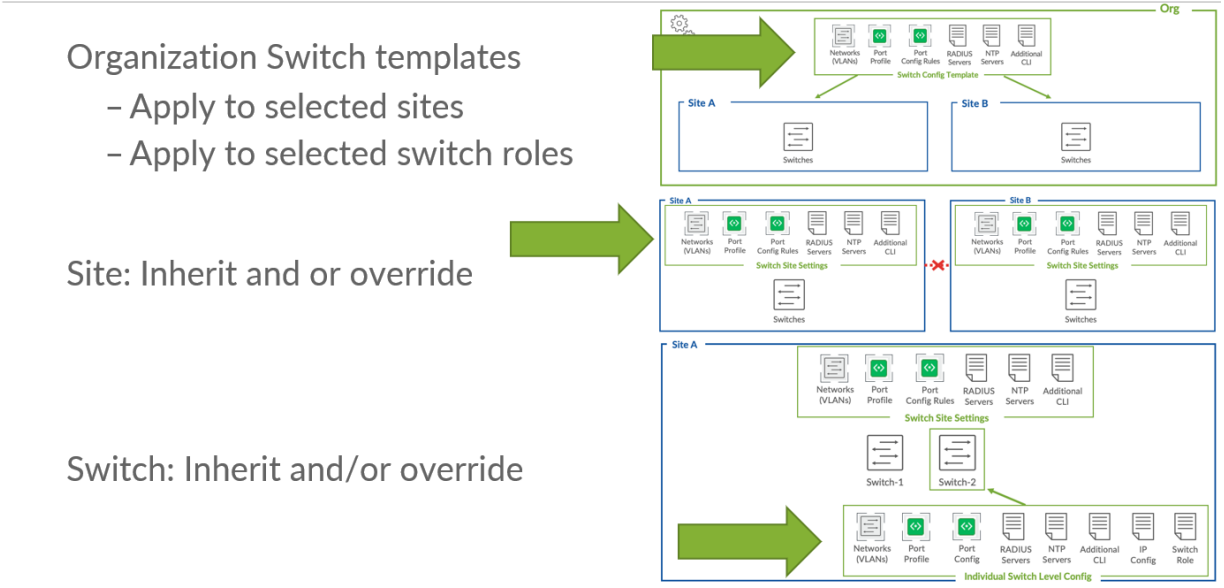


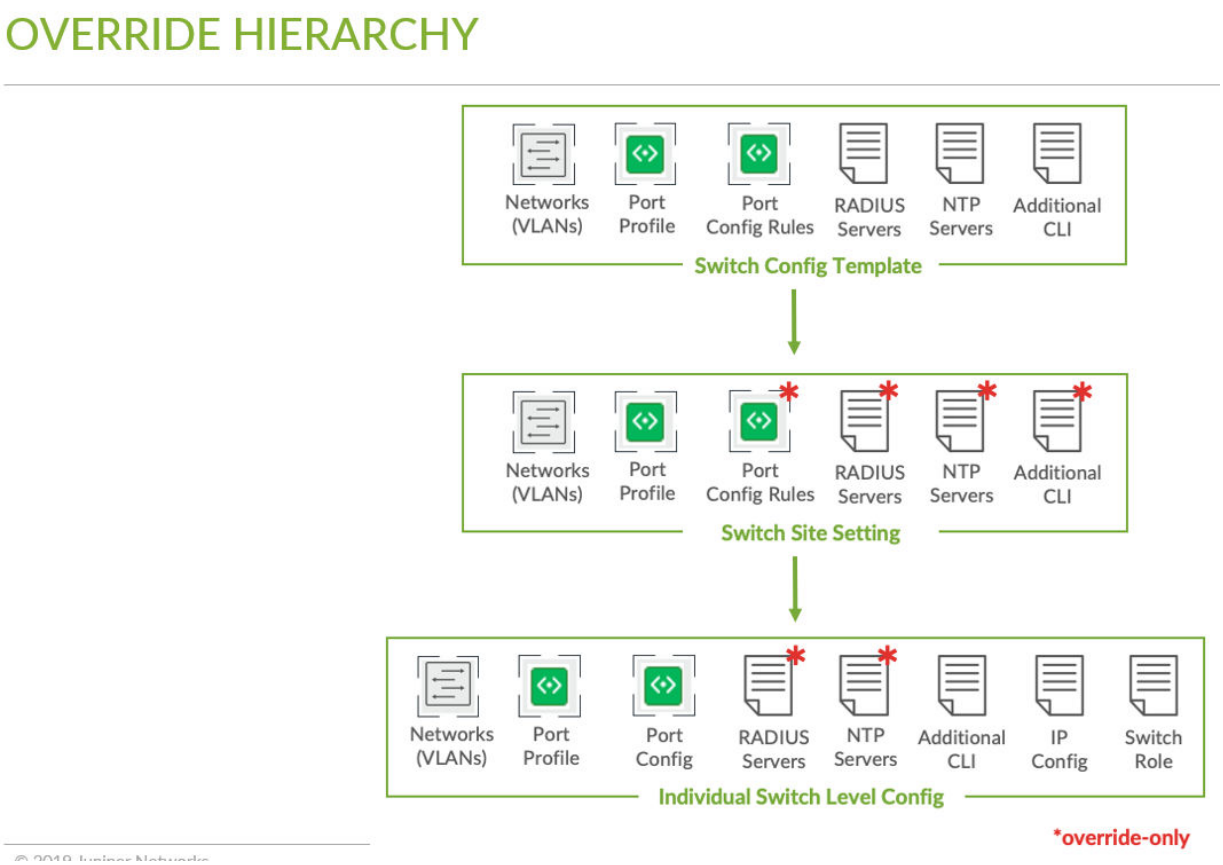
Figure 24 on page 76 shows an example of the configuration hierarchy:

Figure 24: Configuration Hierarchy



It is possible to override the configuration from upper levels in the hierarchy to create more individualized configuration in case it is needed. Figure 25 on page 77 shows an example:

Figure 25: Configuration Override Hierarchy



NOTE: Unless required, it is recommended not to override at the network/site configuration. You could use site variables instead, which are explained below.

Site Variables

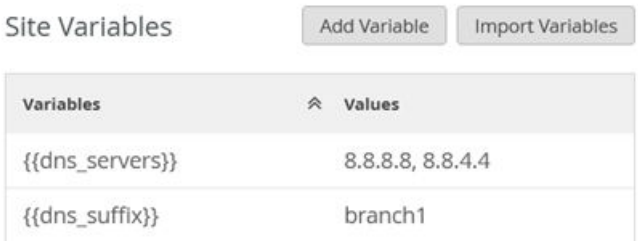
To minimize the number of configuration overrides at the site level, we could use the concept of site variables.

The following is an example of using site variables where we want to individually configure the DNS servers and DNS suffixes to be used:

1. Go to **Organization > Site Configuration** and select an existing site or create a new one.
2. Create a variable containing your DNS servers as a string.
3. Create a variable containing your DNS suffix as a string.

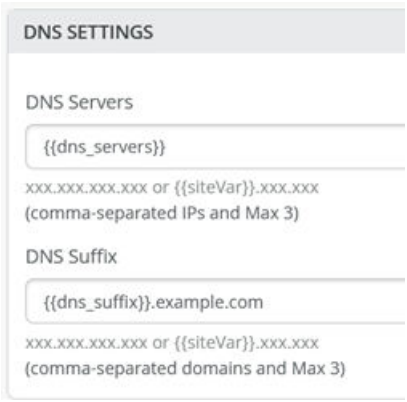
4. **Save** the site setting.

   Your two example variables should now look like the below figure:



5. Go to **Organization > Switch Templates** and select an existing template or create a new one.
6. Under DNS Settings:
   a. For DNS Servers=`{{dns_servers}}`
   b. For DNS Suffix=`{{dns_suffix}}.example.com`
7. Make sure the template is assigned to this site.
8. **Save** the site setting.

Your two example configuration fields should now look like the below figure so that the right values are substituted:



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

Appendix: Day-1 Deploy

IN THIS SECTION

WAN Router Installation

In this chapter, we share configuration examples for Juniper WAN routers that are also managed by the Juniper Mist cloud. Such a solution is called a “Full Stack” solution as it enables you to manage all network devices located at a branch within a single pane of glass. Those devices can be either SSR or SRX based.

Juniper SSR as WAN Router Managed by Juniper Mist Cloud

Testing with SSR WAN routers was not included in this JVD, as a separate JVD dedicated to WAN Edge for SSR had been published shortly beforehand. The integration of SSR WAN routers with branch EX Series Switches was already covered in that earlier testing process.

Refer to the JVD for WAN Edge on SSR or the SRX section in this document and take note of the following required changes:

- SSR Routers do not need the special AppID license to be installed. This is only required for SRX Series Firewalls.
- Juniper Networks® SSR Series Routers support LAG interfaces (starting with release V6.2.0) along with the suggested LACP “force-up” option starting with release V6.3.0. As it’s suggested using both when building a LAG and wanting in-band management of the switch please **consider starting your deployment release V6.3.0 or higher**.
- SSR Routers do not support sharing VLANs across multiple standalone interfaces or multiple LAGs. Unlike the SRX3xx Series Firewalls, this limitation must be considered during network design, or a distribution switch should be used to accommodate the required VLAN structure. It is important to review how VLANs are distributed to branch access switches, particularly when supporting wireless client roaming in scenarios where local bridging at the access point is used for breakout traffic.
- When applying the application policies, do not configure traffic steering towards the LAN as required for the SRX Series Firewalls. For SSR Routers, please implement Table 9 on page 80 as shown below.

Table 9: Application Policies for SSR

Serial Number	Rule Name	Network	Action	Destination	Steering
1	Inside_Branch_hairpin	VLAN1033, VLAN1099, VLAN1088	Pass	Branch-VLANs	**N/A**
2	Internet	VLAN1033, VLAN1099, VLAN1088	Pass	any	wan

- You must enable configuration management straight when assigning an SSR to the Site.

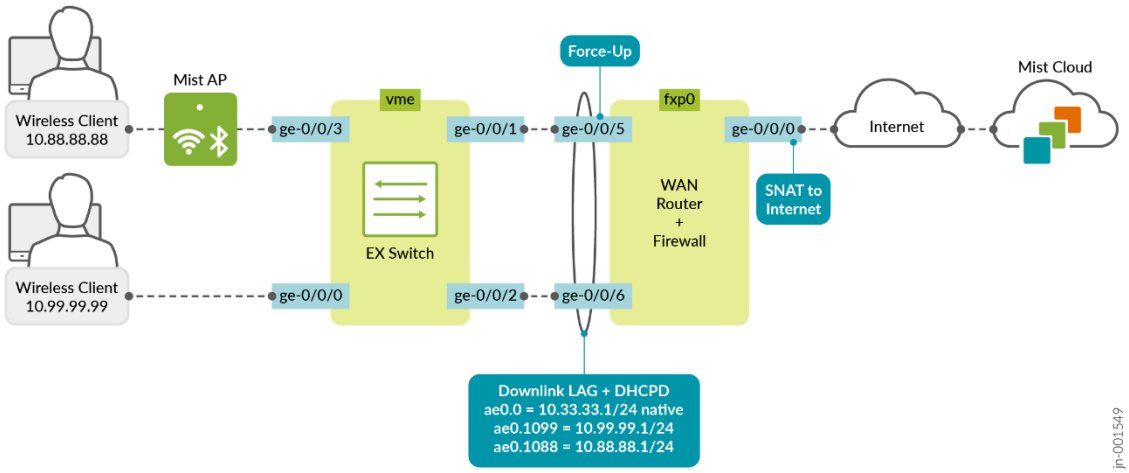
Juniper SRX as WAN Router Managed by Juniper Mist Cloud

NOTE: Make sure the SRX Series Firewall has an AppID license or else it cannot be managed by Juniper Mist cloud. This is independent of whether you use it as a standalone firewall or as an SD-WAN router managing your VPN.

With the example below, we are sharing the minimum requirements with a standalone WAN router and a standalone EX Series Switch to establish a simple branch with in-band management of the switch over

a LAG interface. You can extend this by having the EX Series Switch form a Virtual Chassis or have the WAN router form a high availability cluster pair. Unfortunately, we cannot describe all possible permutations here, so we just cover the basics.

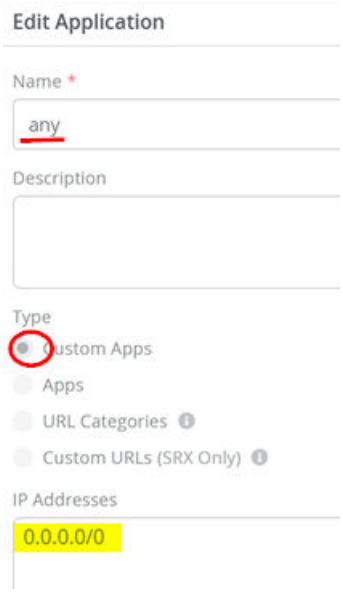
Figure 26: Branch Topology of Juniper SRX as WAN Router



NOTE: Should your design have multiple LAGs from the WAN router towards the access switches, then you have the following options:1. When using a Juniper SRX 3xx Series Firewall, VLANs can be shared across multiple LAGs. In this setup, the Juniper Mist cloud can automatically configure IRB interfaces to support this functionality.2. When using a Juniper SRX 1500 Series Firewall or higher, you need to define a unique set of VLANs per LAG or utilize a distribution layer architecture with high availability configuration in cluster mode.

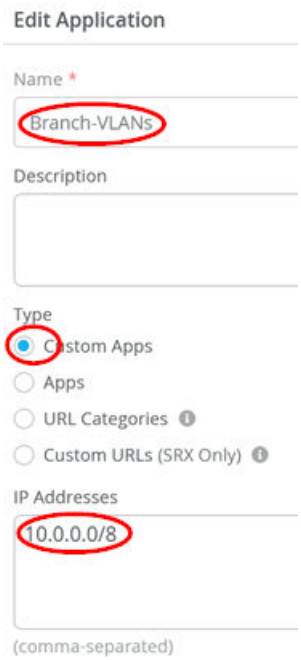
Go to **Organization > Applications** and check that there is an existing application with the following settings:

- Name=`any`
- Type=`Custom Apps`
- IP Addresses=`0.0.0.0/0`

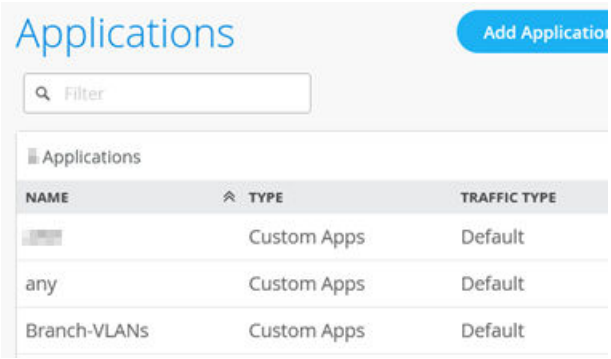


Add another application with the following settings:

- Name=`Branch-VLANs`
- Type=`Custom Apps`
- IP Addresses=`10.0.0.0/8`

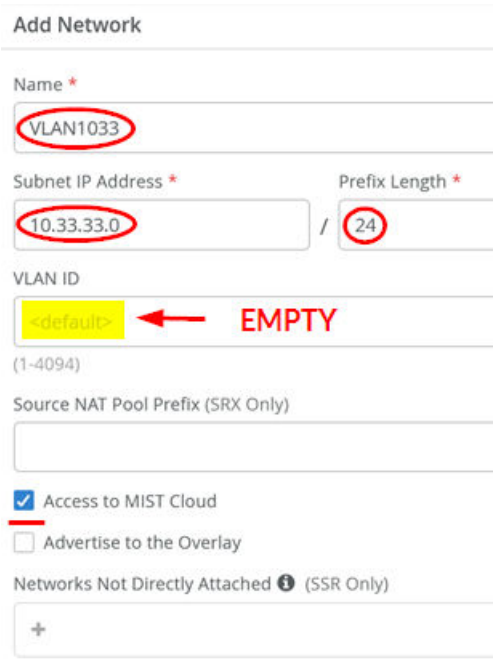


You should now see the two applications listed as shown below:



Go to **Organization > Networks** and add the first VLAN:

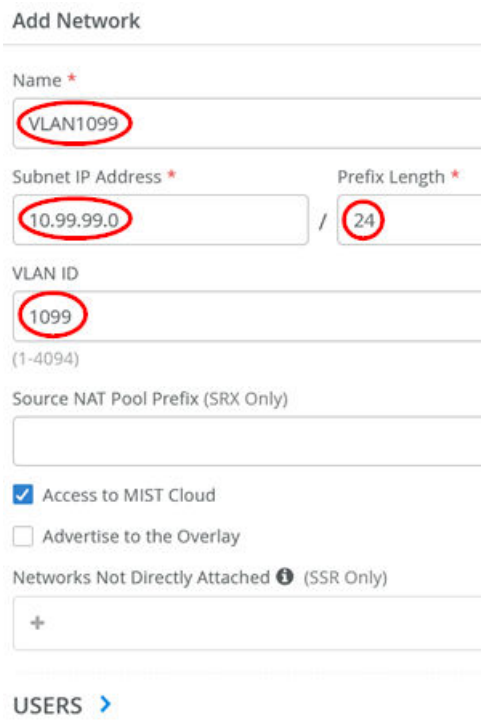
- Name=`VLAN1033`
- Subnet IP Address=`10.33.33.0`
- Prefix Length=`24`
- VLAN ID=Leave this field empty. This is the native VLAN used for in-band management of the attached EX Series Switch as well as the AP.
- Access to Mist Cloud=`Enabled`. This must be enabled for the attached switches and AP to be managed by the Juniper Mist cloud.



Then, add the second VLAN (in our topology we use this for wired clients):

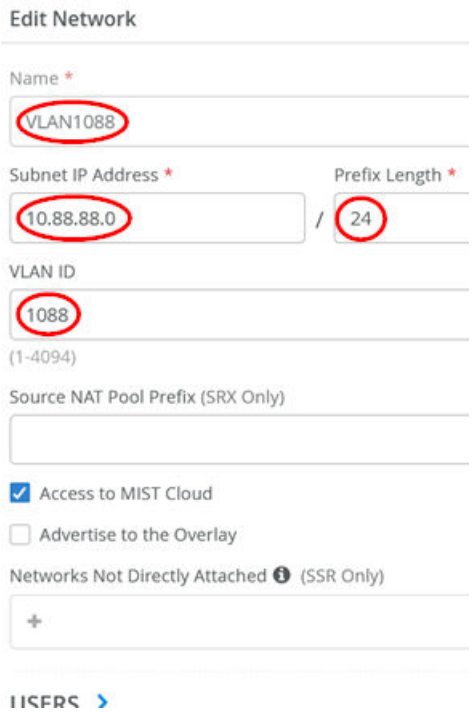
- Name=`VLAN1099`

- Subnet IP Address=`10.99.99.0`
- Prefix Length=`24`
- VLAN ID=`1099`

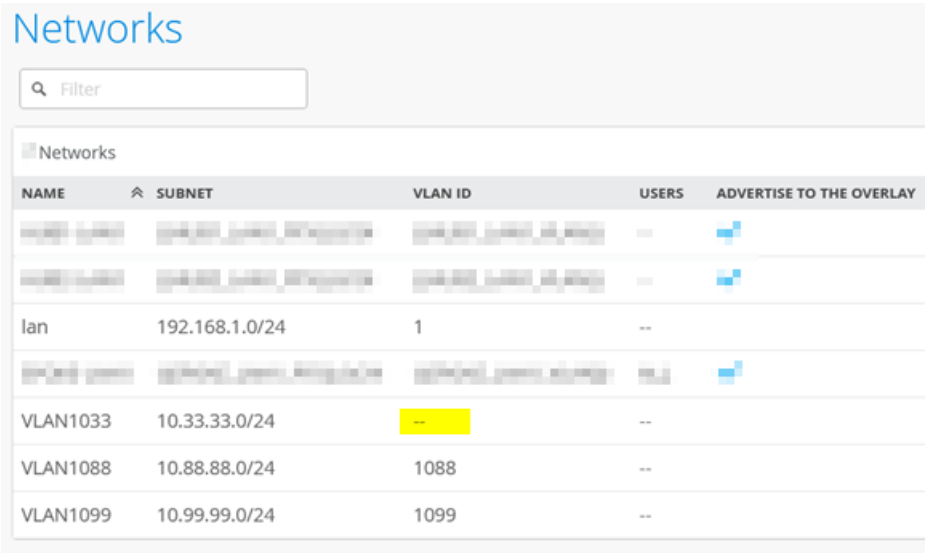


Then, add the third VLAN (in our topology, we use it for wireless clients attached through AP)

- Name=`VLAN1088`
- Subnet IP Address=`10.88.88.0`
- Prefix Length=`24`
- VLAN ID=`1088`



Review the three networks and verify that no VLAN ID is set for the switch and AP management network, since this is a native VLAN on the downlink trunk.



The following JSON template may be used to configure the branch WAN router. Alternatively, manual configuration steps for the branch WAN router are listed immediately after the JSON template.

```
{
  "type": "standalone",
  "port_config": {
```

```
    "ge-0/0/0": {
      "usage": "wan",
      "name": "wan",
      "ip_config": {
        "type": "dhcp"
      }
    },
    "ge-0/0/15": {
      "usage": "wan",
      "name": "wan2",
      "ip_config": {
        "type": "dhcp"
      }
    },
    "cl-1/0/0": {
      "usage": "wan",
      "name": "lte",
      "wan_type": "lte",
      "ip_config": {
        "type": "dhcp"
      }
    },
    "ge-0/0/5-6": {
      "usage": "lan",
      "aggregated": true,
      "ae_disable_lacp": false,
      "ae_lacp_force_up": true,
      "ae_idx": 0,
      "redundant": false,
      "critical": false,
      "disabled": false,
      "networks": [
        "VLAN1033",
        "VLAN1099",
        "VLAN1088"
      ]
    }
  },
  "ip_configs": {
    "VLAN1033": {
      "type": "static",
      "ip": "10.33.33.1",
      "netmask": "/24"
```

```
    },
    "VLAN1099": {
      "type": "static",
      "ip": "10.99.99.1",
      "netmask": "/24"
    },
    "VLAN1088": {
      "type": "static",
      "ip": "10.88.88.1",
      "netmask": "/24"
    }
  },
  "dhcpd_config": {
    "VLAN1033": {
      "type": "local",
      "ip_start": "10.33.33.10",
      "ip_end": "10.33.33.250",
      "gateway": "10.33.33.1",
      "dns_servers": [
        "8.8.8.8",
        "9.9.9.9"
      ],
      "options": {}
    },
    "VLAN1099": {
      "type": "local",
      "ip_start": "10.99.99.10",
      "ip_end": "10.99.99.250",
      "gateway": "10.99.99.1",
      "dns_servers": [
        "8.8.8.8",
        "9.9.9.9"
      ],
      "options": {}
    },
    "VLAN1088": {
      "type": "local",
      "ip_start": "10.88.88.10",
      "ip_end": "10.88.88.250",
      "gateway": "10.88.88.1",
      "dns_servers": [
        "8.8.8.8",
        "9.9.9.9"
```

```
      ],
      "options": {}
    }
  },
  "path_preferences": {
    "wan": {
      "paths": [
        {
          "type": "wan",
          "name": "wan"
        }
      ]
    },
    "LAN": {
      "strategy": "ordered",
      "paths": [
        {
          "type": "local",
          "networks": [
            "VLAN1033"
          ]
        },
        {
          "type": "local",
          "networks": [
            "VLAN1099"
          ]
        },
        {
          "type": "local",
          "networks": [
            "VLAN1088"
          ]
        }
      ]
    }
  },
  "service_policies": [
    {
      "name": "inside_Branch_hairpin",
      "tenants": [
        "VLAN1033",
        "VLAN1088",
```

```
        "VLAN1099"
      ],
      "services": [
        "Branch-VLANs"
      ],
      "action": "allow",
      "path_preference": "LAN",
      "idp": {
        "enabled": false
      }
    },
    {
      "name": "Internet",
      "tenants": [
        "VLAN1033",
        "VLAN1099",
        "VLAN1088"
      ],
      "services": [
        "any"
      ],
      "action": "allow",
      "path_preference": "wan",
      "idp": {
        "enabled": false
      }
    }
  ],
  "bgp_config": {},
  "routing_policies": {},
  "extra_routes": {},
  "vrf_instances": {},
  "tunnel_configs": {},
  "oob_ip_config": {
    "type": "dhcp",
    "node1": {
      "type": "dhcp"
    }
  },
  "ntp_servers": [
    "time.google.com"
  ],
  "dns_servers": [
```

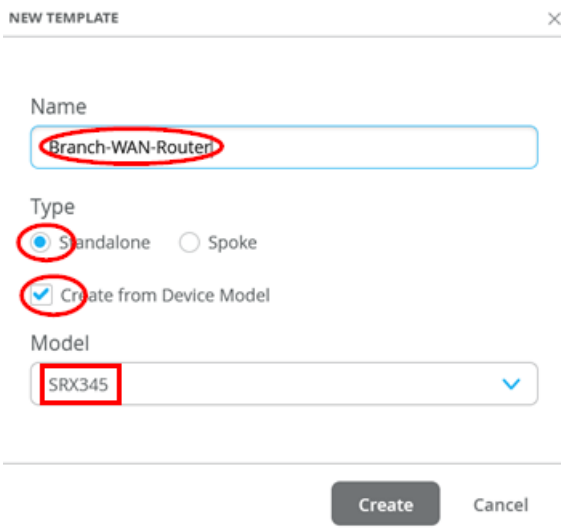
```
    "8.8.8.8",
    "9.9.9.9"
  ],
  "tunnel_provider_options": {
    "jse": {},
    "zscaler": {}
  },
  "additional_config_cmds": [
    "set security zones security-zone VLAN1033 host-inbound-traffic system-services ping",
    "set security zones security-zone VLAN1099 host-inbound-traffic system-services ping",
    "set security zones security-zone VLAN1088 host-inbound-traffic system-services ping"
  ],
  "name": "Branch-WAN-Router"
}
```

When not using the JSON template, execute the following steps instead to configure the branch WAN router:

Go to **Organization > WAN Edge Templates**

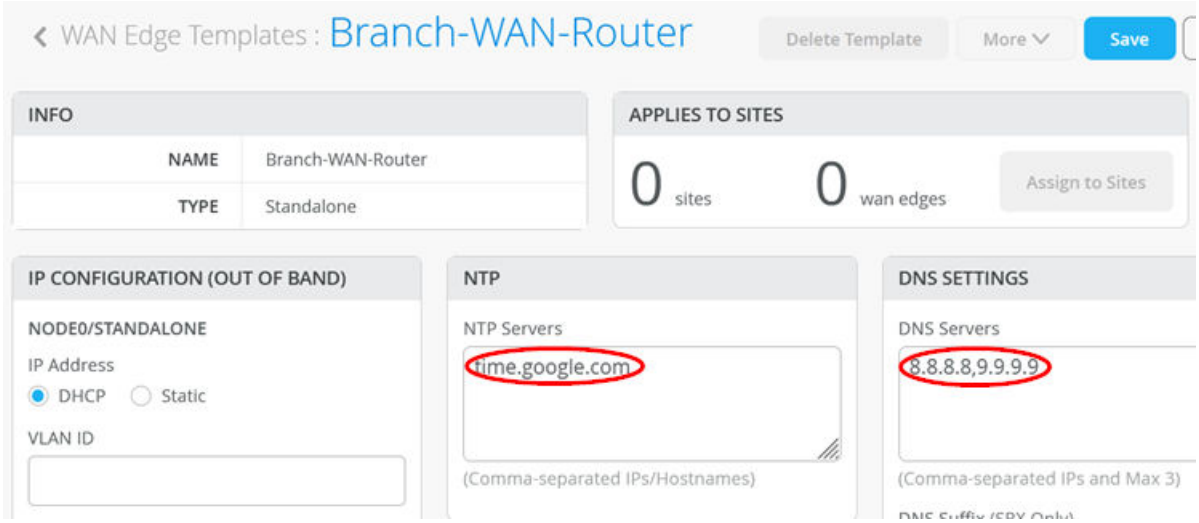
Create a new template with the following parameters:

- Name=`Branch-WAN-Router`
- Type=`Standalone`
- Create from Device Model=`Checked`
- Model=`<Select your Model>`

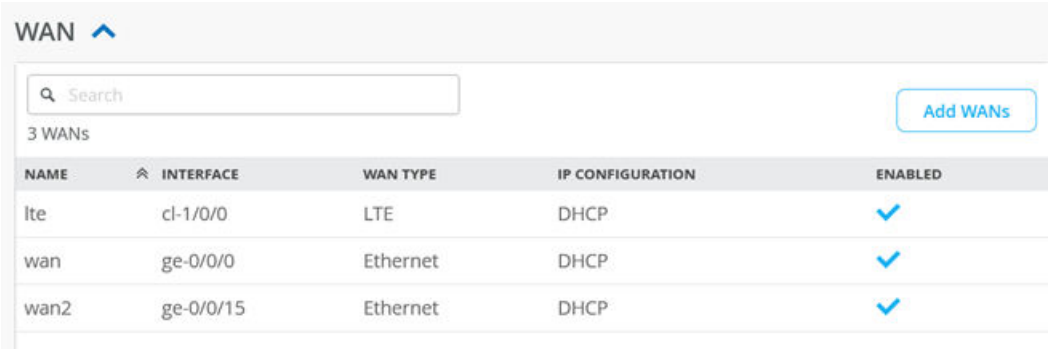


After the template has been created, start with basic configuration settings based on your environment such as the following:

- NTP=`time.google.com`
- DNS Servers=`8.8.8.8, 9.9.9.9`



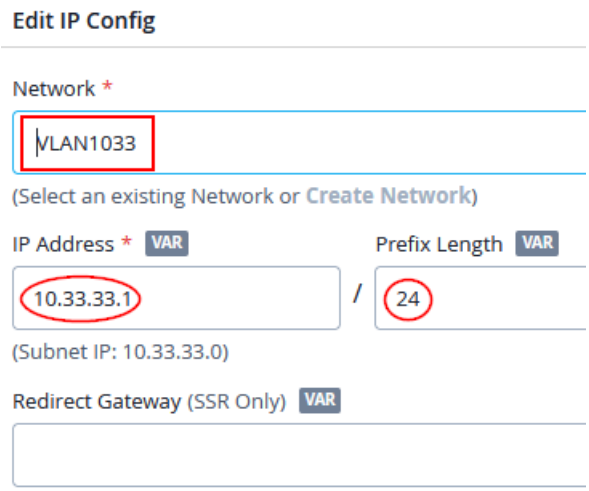
When you check the template, you should see the following preconfigured WAN interfaces. We are going to use the "`wan`" ge-0/0/0 interface to obtain a DHCP lease from the broadband router.



We are going to modify the LAN interfaces of this template. Delete the preconfigured “lan” interface (not shown here).

Then, create a first LAN network (native for our device management) with the following IP config:

- Network=`VLAN1033`
- IP Address=`10.33.33.1`
- IP-Prefix Length=`24`



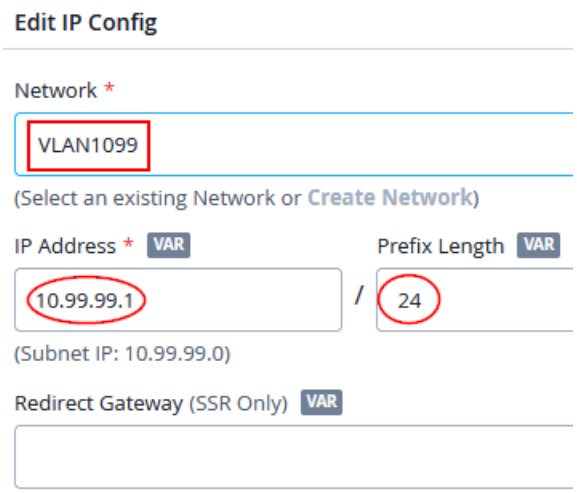
Configure with the following DHCP config:

- Network=`VLAN1033`
- DHCP=`Server`
- IP Start=`10.33.33.10`
- IP End=`10.33.33.250`
- Gateway=`10.33.33.1`

- DNS Servers=`8.8.8.8, 9.9.9.9`

Then, create a second LAN network (trunked for our wired clients) with the following IP config:

- Network=`VLAN1099`
- IP Address=`10.99.99.1`
- IP-Prefix Length=`24`

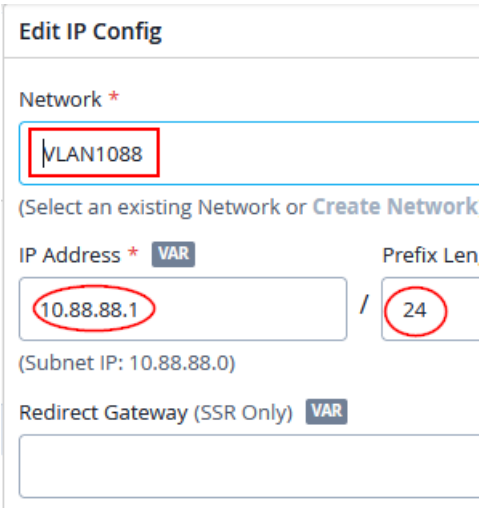


Configure with the following DHCP config:

- Network=`VLAN1099`
- DHCP=`Server`
- IP Start=`10.99.99.10`
- IP End=`10.99.99.250`
- Gateway=`10.99.99.1`
- DNS Servers=`8.8.8.8, 9.9.9.9`

Then, create a third LAN network (trunked for our wireless clients) with the following IP config:

- Network=`VLAN1088`
- IP Address=`10.88.88.1`
- IP-Prefix Length=`24`

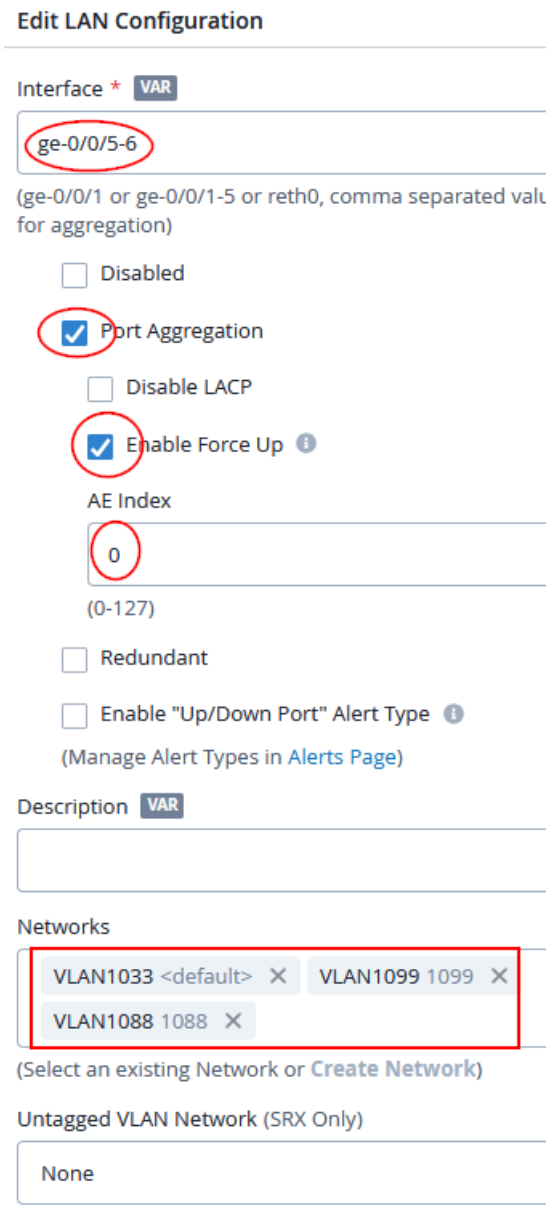


Configure with the following DHCP config:

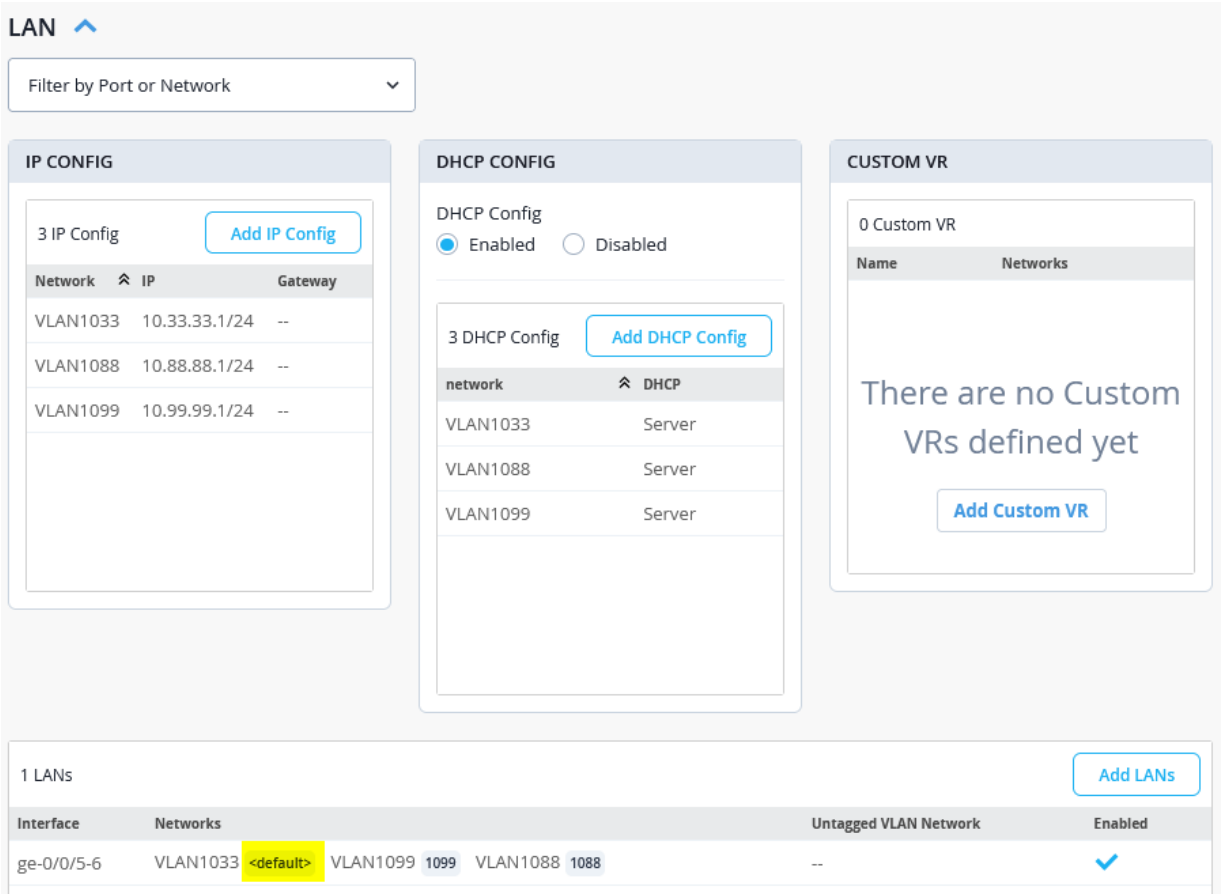
- Network=`VLAN1088`
- DHCP=`Server`
- IP Start=`10.88.88.10`
- IP End=`10.88.88.250`
- Gateway=`10.88.88.1`
- DNS Servers=`8.8.8.8, 9.9.9.9`

Finally, configure the LAN interfaces with LAG and the Force-Up option binding the three networks together:

- Interface=`ge-0/0/5-6`
- Port aggregation=`Enabled`
- Disable LACP=`Unchecked` (default)
- Enable Force Up=`Enabled`
- AE Index=`0`
- Network=`VLAN1033` and `VLAN1099` and `VLAN1088`

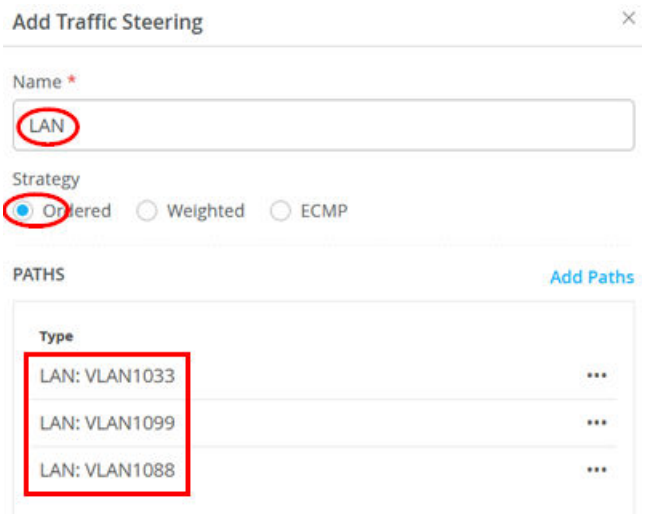


The final LAN interface table should look like the figure below:

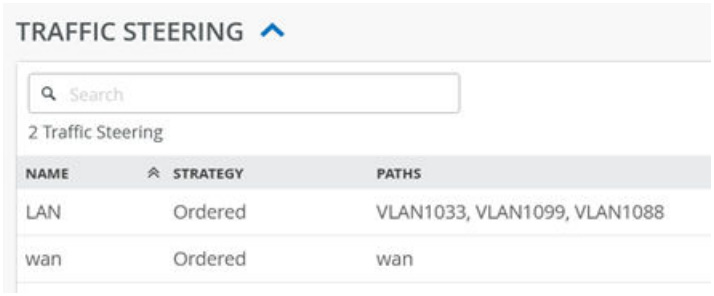


Next step is adding a new destination to the traffic steering policy. This is required to enable communication between the local VLANs which we want to happen in our example. Add a new traffic steering policy using the following settings:

- Name=`LAN`
- Strategy=`Ordered`
- Paths:
  - Type=`LAN: VLAN1033`
  - Type=`LAN: VLAN1099`
  - Type=`LAN: VLAN1088`



You should see the following for traffic steering destinations now:

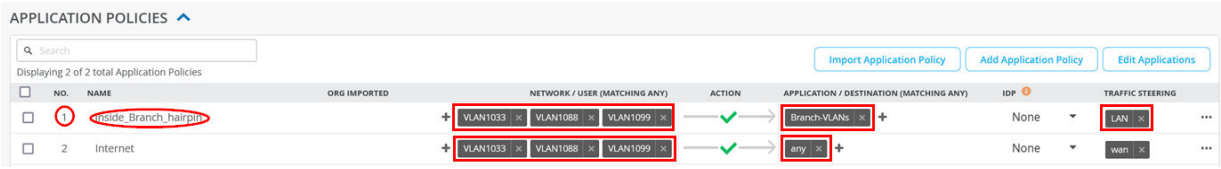


Implement Table 10 on page 100 for application policies when your device is an SRX Series Firewall. Parts should already exist that you only need to modify.

Table 10: Application Policies for SRX

Serial Number	Rule Name	Network	Action	Destination	Steering
1	Inside_Branch_hairpin	VLAN1033, VLAN1099, VLAN1088	Pass	Branch-VLANs	LAN
2	Internet	VLAN1033, VLAN1099, VLAN1088	Pass	any	wan

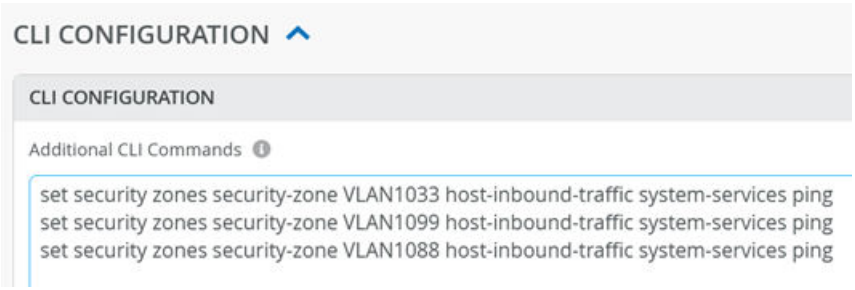
You should see the following configuration for application policies now after the implementation of the above table:



In the current version, clients on the LAN side cannot get an answer when sending ICMP pings to the WAN router as their local gateway. However, receiving pings is crucial for any local debugging. Hence, it is highly recommended that you add some additional Junos OS CLI commands to enable ping for any wired or wireless clients towards the WAN router as the local gateway of the VLAN they are attached to. See the example below:

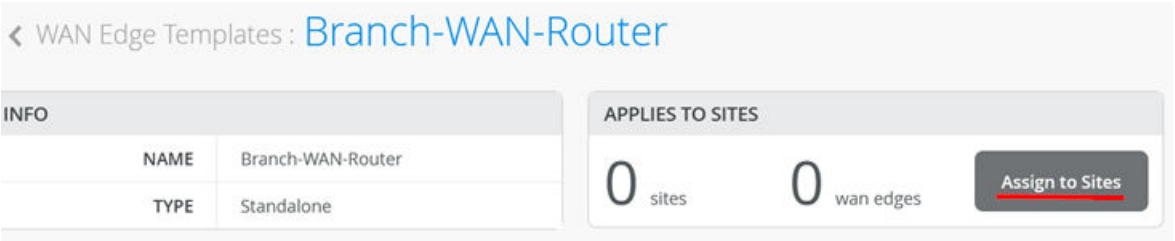
```
set security zones security-zone VLAN1033 host-inbound-traffic system-services ping
set security zones security-zone VLAN1099 host-inbound-traffic system-services ping
set security zones security-zone VLAN1088 host-inbound-traffic system-services ping
```

In the portal, it should look like the figure below:

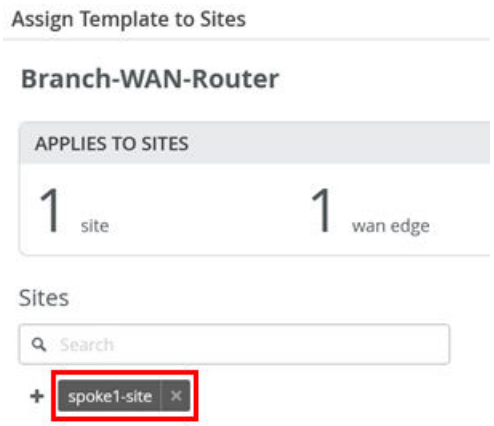


Click **Save** to save the template now.

You must assign a site for this template or else it won't be used on any device.



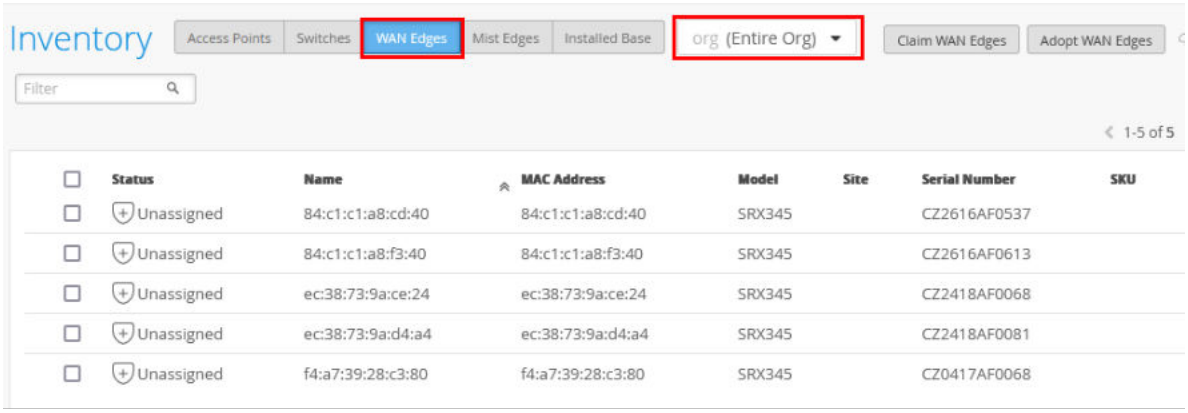
Here, we add the Spoke1 site to the template, which is where our switches are located.



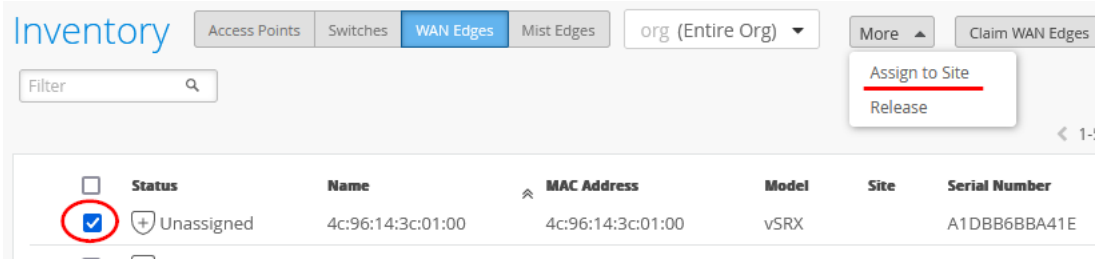
To assign your SRX Series Firewall devices to sites, the devices must be present in the Juniper Mist inventory. You can claim or adopt your SRX Series Firewall to onboard it in the Juniper Mist cloud. After the device is onboarded, the organization inventory shows the device.

To assign an SRX Series Firewall to a site:

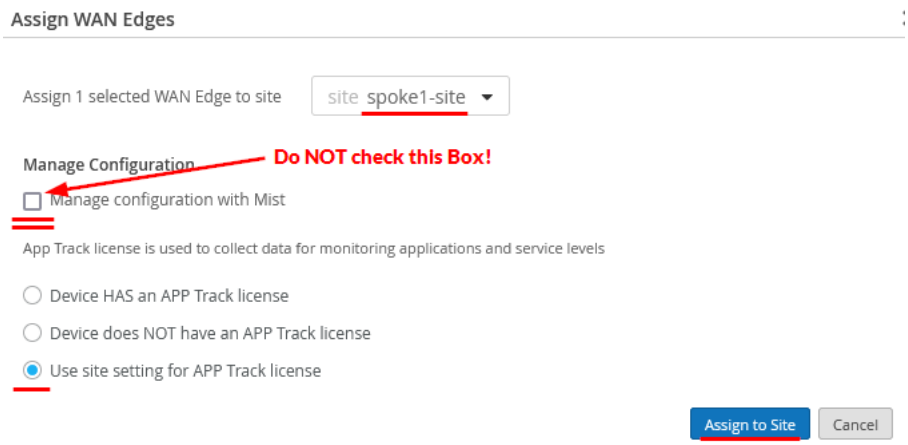
- In the portal, click **Organization > Admin > Inventory**.
- Refresh your browser and check under **WAN Edges** to find out if your SRX Series Firewall is part of the inventory.



- Assign each SRX Series Firewall to an individual site using the **Assign to Site** option.

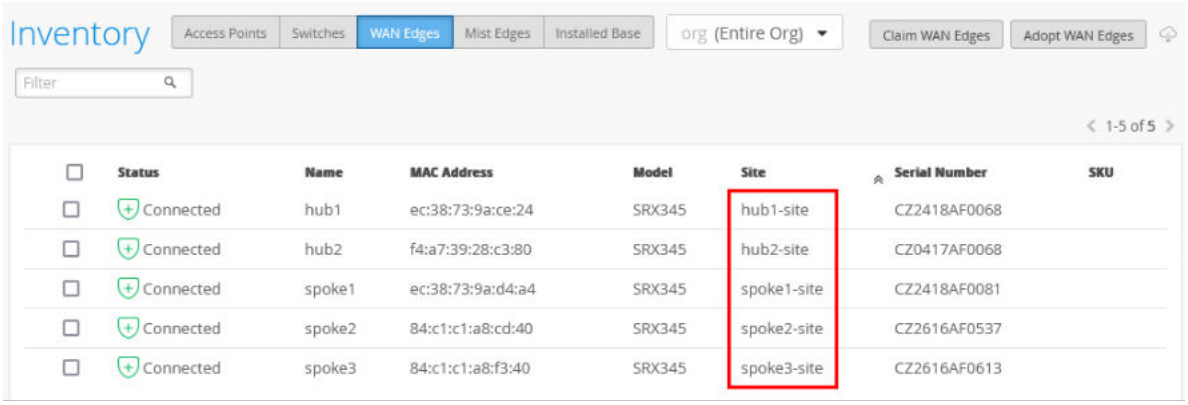


- On the **Assign WAN Edges** page, select the site you want to assign from the list of available sites.

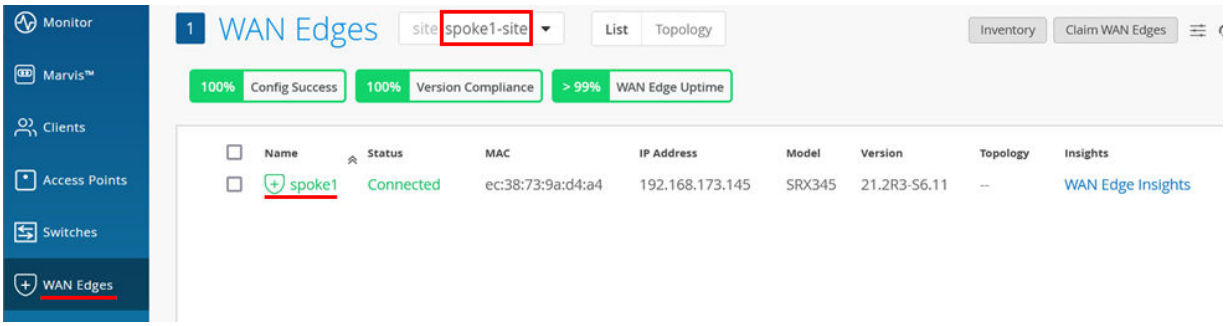


- Do not select the **Manage configuration with Mist** option. If you do, you may see unwanted changes to the configuration on your SRX Series Firewall. You can enable the option later if required, after you've assigned the device to the site.
- Check the **Use site setting for APP Track license** option if you have a valid Application Security license, and then click **Assign to Site**.

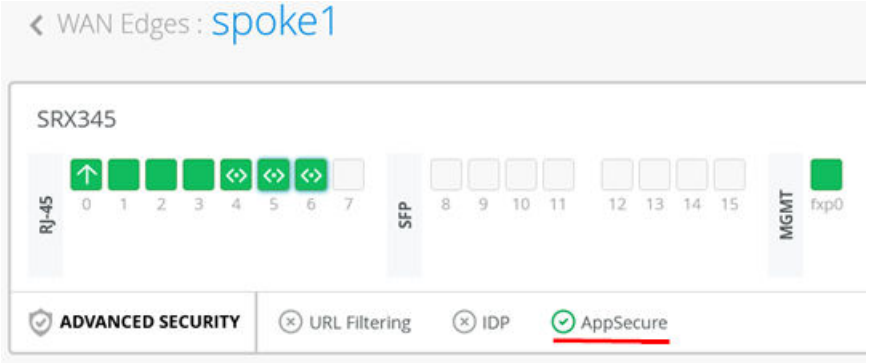
The figure below shows changes in the inventory once you assign the device to the site:



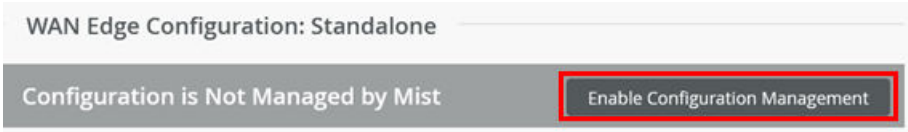
- After the device is onboarded, on the **WAN Edges** tab, select **<your site>** and then click on the device.



- Check the device and AppSecure status:



- Now click **Enable Configuration Management** to activate it as the last step so that Mist can configure the device:



- OPTIONAL: Use a remote console to verify the device configuration and status after Juniper Mist cloud takes over management of the device. In our example, you see the below output:

```
root@spoke1> show interfaces terse
Interface               Admin Link Proto    Local                 Remote
ge-0/0/0                up    up
ge-0/0/0.0              up    up   inet     192.168.173.145/24
.
ge-0/0/5                up    up
ge-0/0/5.0              up    up   aenet    --> ae0.0
ge-0/0/5.1088           up    up   aenet    --> ae0.1088
ge-0/0/5.1099           up    up   aenet    --> ae0.1099
ge-0/0/5.32767          up    up   aenet    --> ae0.32767
ge-0/0/6                up    up
ge-0/0/6.0              up    up   aenet    --> ae0.0
ge-0/0/6.1088           up    up   aenet    --> ae0.1088
ge-0/0/6.1099           up    up   aenet    --> ae0.1099
ge-0/0/6.32767          up    up   aenet    --> ae0.32767
.
ae0                     up    up
ae0.0                   up    up   inet     10.33.33.1/24
ae0.1088                up    up   inet     10.88.88.1/24
ae0.1099                up    up   inet     10.99.99.1/24
```

```
ae0.32767               up    up
.
root@spoke1> show lacp interfaces
Aggregated interface: ae0
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      ge-0/0/5 FUP    Actor   No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-0/0/5 FUP  Partner   No   Yes    No   No  Yes   Yes     Fast   Passive
      ge-0/0/6       Actor    No   Yes    No   No   No   Yes     Fast    Active
      ge-0/0/6     Partner    No   Yes    No   No   No   Yes     Fast   Passive
    LACP protocol:        Receive State  Transmit State          Mux State
      ge-0/0/5 FUP              Current   Fast periodic Collecting distributing
      ge-0/0/6                Defaulted   Fast periodic           Detached
```

The moment you attach the EX Series Switch and power it up, it should obtain a DHCP lease from the WAN router which you can verify as shown below. From time to time, you should also see the Phone Home Client on the switch trying to contact the redirect server as in our example:

```
root@spoke1> show dhcp server binding detail
Client IP Address:  10.33.33.11
     Hardware Address:             04:5c:6c:6b:13:42
     State:                        BOUND(LOCAL_SERVER_STATE_BOUND)
     Protocol-Used:                DHCP
     Lease Expires:                2024-03-07 17:02:09 UTC
     Lease Expires in:             85474 seconds
     Lease Start:                  2024-03-06 17:02:09 UTC
     Last Packet Received:         2024-03-06 17:02:09 UTC
     Incoming Client Interface:    ae0.0
     Client Interface Vlan Id:     1
     Server Identifier:            10.33.33.1
     Session Id:                   2
     Client Pool Name:             VLAN1033
root@spoke1> show security flow session source-prefix 10.0.0.0/8
Session ID: 249108247036, Policy name: 01_Internet/20, State: Stand-alone, Timeout: 854, Valid
  In: 10.33.33.11/59874 --> 44.231.144.179/443;tcp, Conn Tag: 0x0, If: ae0.0, Pkts: 8, Bytes:
1278,
  Out: 44.231.144.179/443 --> 192.168.173.145/8983;tcp, Conn Tag: 0x0, If: ge-0/0/0.0, Pkts: 18,
Bytes: 13734,
Total sessions: 1
```

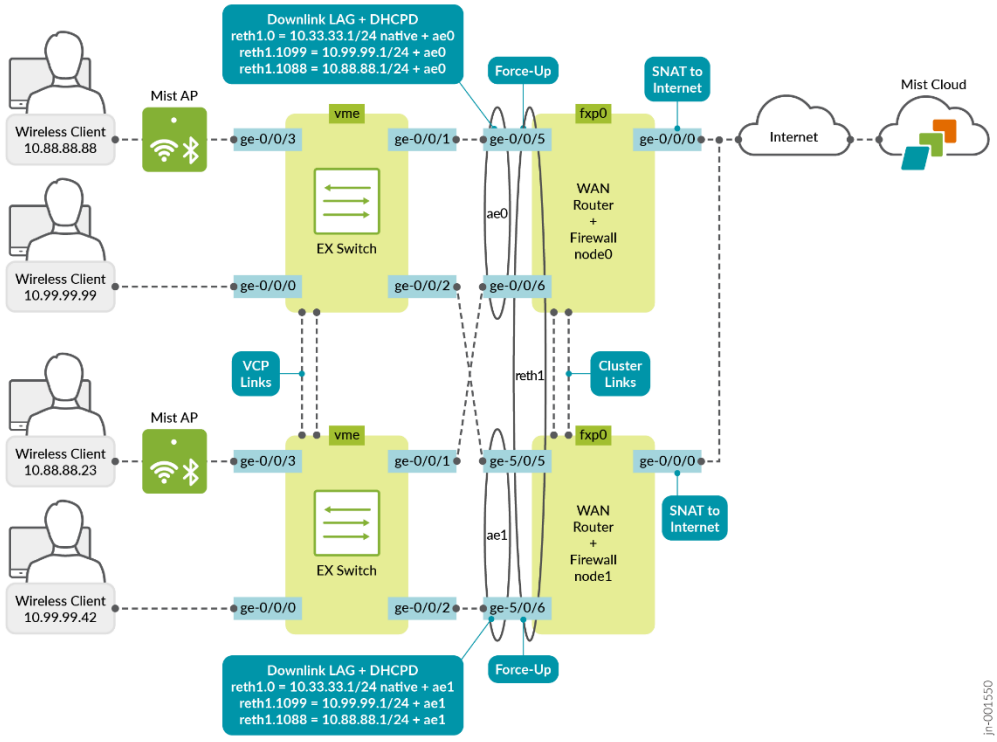
The example below illustrates the use of SRX Series Firewalls in a redundant cluster configuration. At the time this JVD was created, the required configuration could not be fully completed through the GUI. Therefore, a hybrid approach was used: redundant Ethernet interfaces were configured through the GUI,

while the LAG interfaces—with the “force-up” option—were manually added via the CLI within the same template.

SRX Chassis Cluster

When using SRX Series Firewalls in chassis cluster mode, you need to configure a minimum of 4 links when using LAGs as it is not possible to span a single aggregate Ethernet bundle across the two redundant cluster nodes. Instead, you form individual aggregate Ethernet bundles on each local cluster node and bind those together through a redundant Ethernet interface called a “reth” interface. You can find an example topology in Figure 27 on page 106:

Figure 27: Branch Topology of Juniper SRX Chassis Cluster as WAN Router

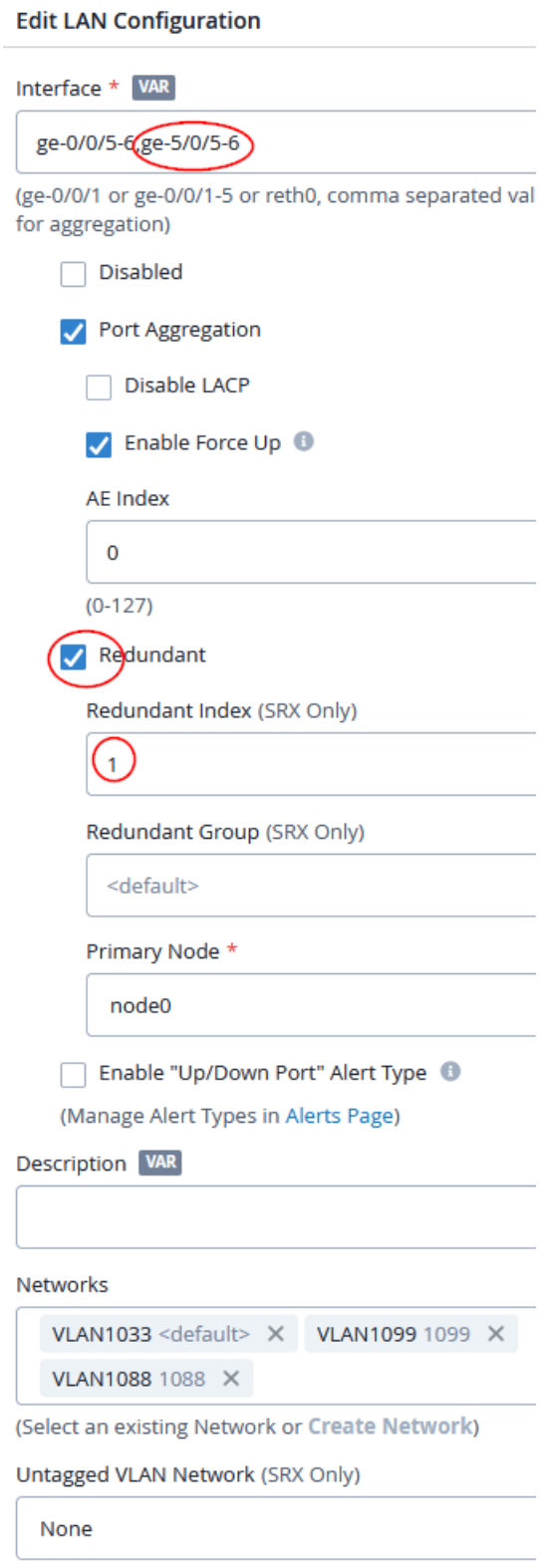


When changing the configuration :

- The **Interface** field must have all four interface names that are distributed across all cluster nodes. On node1, the interface name is always renamed when the cluster is built. What the exact new interface name will be is device specific and you can review more information here.
- You need to add the redundant interface option to your existing LAG configuration.

In the example below, we added the following configuration:

- Interface=`ge-0/0/5-6, ge-5/0/5-6`
- Redundant=`Enabled`
  - Redundant Index=`1`
  - Redundant Group=`empty` (default)
  - Primary Node=`Node0`


Edit LAN Configuration
Interface * VAR
ge-0/0/5-6,ge-5/0/5-6
(ge-0/0/1 or ge-0/0/1-5 or reth0, comma separated val
for aggregation)
Disabled
Port Aggregation
Disable LACP
Enable Force Up
AE Index
0
(0-127)
Redundant
Redundant Index (SRX Only)
1
Redundant Group (SRX Only)
<default>
Primary Node *
node0
Enable "Up/Down Port" Alert Type
(Manage Alert Types in Alerts Page)
Description VAR
Networks
VLAN1033 <default>
VLAN1099 1099
VLAN1088 1088
(Select an existing Network or Create Network)
Untagged VLAN Network (SRX Only)
None

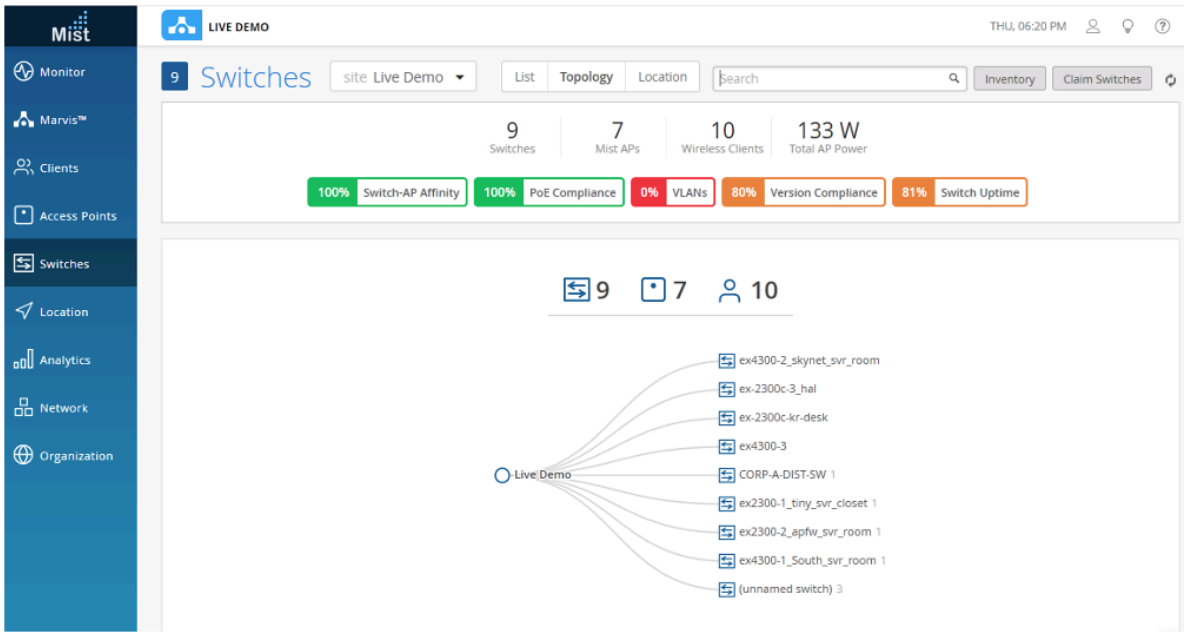
Activating a Greenfield Switch via Claim and ZTP-Based Installation

A switch-specific QR code is set up at the time of purchase. The switch will arrive in a box with the cloud-ready logo, and a sticker with a QR code will be on the back of the switch near the fan exhaust and interfaces.

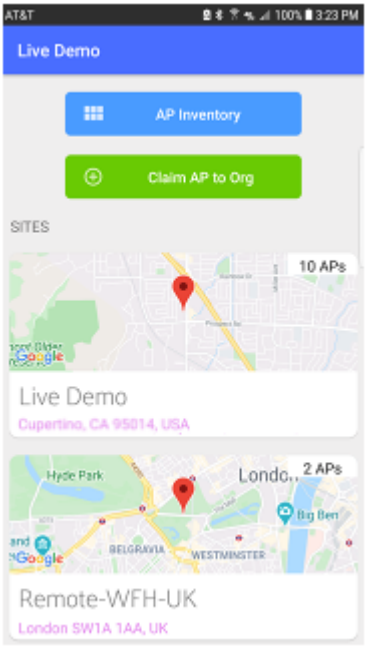
Using the MistAI App to add a cloud-ready switch to the Juniper Mist cloud

Step-by-Step Procedure:

1. Download and install the MistAI app to your phone.
2. Unbox your switch, connect the management port to the Internet, and power it on. As part of the ZTP process, the switch will automatically access the PHC server (or the DHCP server if you have set this up instead) and then connect to the Juniper Mist cloud for configuration updates.
3. Using a web browser, log in to your Juniper Mist account. The **Monitor** screen appears, showing an overview of the Juniper Mist cloud and any APs and clients that are already connected. In the menu on the left, click **Switches** to open that screen. Once the ZTP process resolves, the switch will automatically appear here (if the switch doesn't appear after a few minutes, despite refreshing the web page, log out and then log back in, or go to the troubleshooting section below to find out how to confirm whether the device is connecting to the cloud.



4. While the switch is being resolved in the Juniper Mist cloud, find the QR code on the front of the switch.
5. On your phone, open the MistAI app and log into your Juniper Mist cloud account. Tap the **Claim AP to Org** button that appears.



6. Point the QR code viewer at the QR code on your switch. Once the QR code comes into focus (that is, your camera is held at the right distance), the app automatically claims the device and adds it to your organization's inventory in the portal.

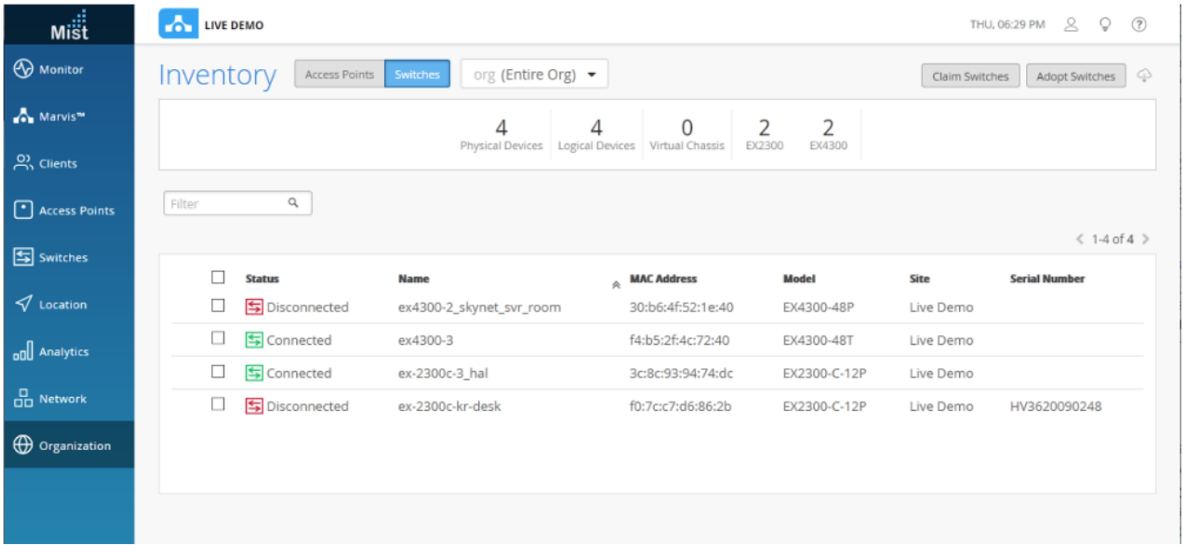
Manually Adding a Cloud-Ready Switch to the Juniper Mist Cloud

Step-by-Step Procedure:

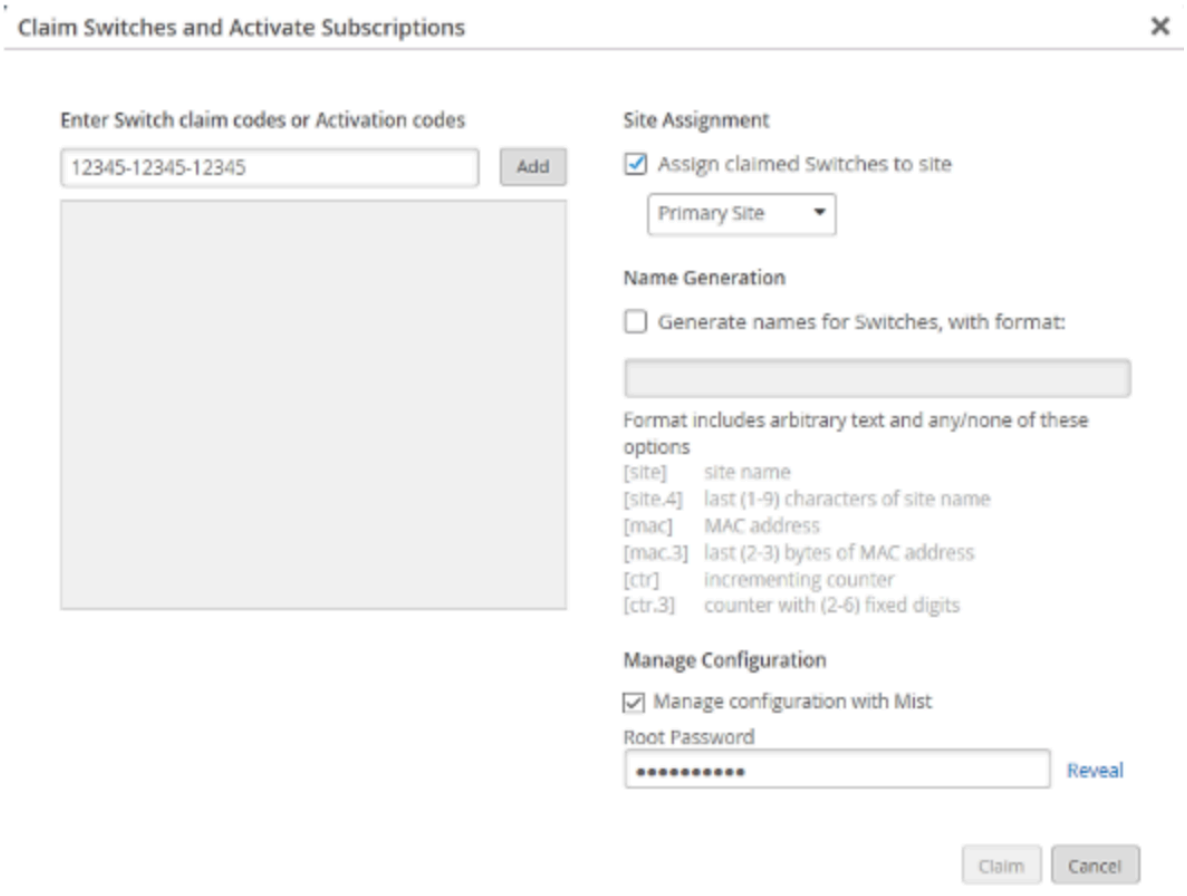
To adopt a cloud-ready switch manually, you need an activation code for the switch (these are sent via email to the address on record at the time of purchase, or they can be obtained by contacting the Juniper Mist Customer Engagement team). Using the activation code will adopt the switch and any Juniper APs that are part of the purchase order, as well as claiming any subscriptions that are included in your purchase.

1. Start by unboxing your switch, connecting the management port to the Internet, and powering it on. As part of the ZTP process, the switch will automatically access the PHC server (or the DHCP server if you have set this up instead) and then connect to the Juniper Mist cloud for configuration updates.

2. Using a web browser, log in to your Juniper Mist account. The **Monitor** screen appears, showing an overview of the Juniper Mist cloud and any Juniper APs and clients that are already connected. In the menu on the left, click **Organization > Inventory** to open that screen.



3. Choose the Switches tab at the top of the Inventory screen, and then click the **Claim Switches** button and enter the claim code or activation code for the switch.



4. Fill out the other fields on the screen as you like. Note that if you deselect **Assign claimed switches to site**, the switch will not be listed in the Switches page. To see your switch on the Switches page, you

must first assign the switch to the site from the **Inventory** page. Check **Manage configuration with Juniper Mist** and then enter a root password for the switch. Note that this choice puts the switch under the management of Mist, and as such, Juniper recommends that local configuration using the CLI be restricted to prevent conflicts (for example, you may want to create a system login message on the switch to warn against making configuration changes locally, from the CLI).

5. Once the ZTP process resolves, the switch will automatically appear on the **Inventory** screen. If the switch doesn't appear after a few minutes despite refreshing the web page, log out and then log back in, or go to the troubleshooting section below to find out how to confirm whether the device is connecting to the cloud.

Activating a Brownfield Switch via Adoption Code-Based Installation

> **NOTE**: It is important to backup your existing Junos OS configuration on the switch before activating a brownfield switch, because when the switch is adopted for management from the Juniper Mist cloud, as described below, the old configuration will be replaced. Do this by running the `request system software configuration-backup <path>` command, which saves the currently active configuration and any installation-specific parameters.

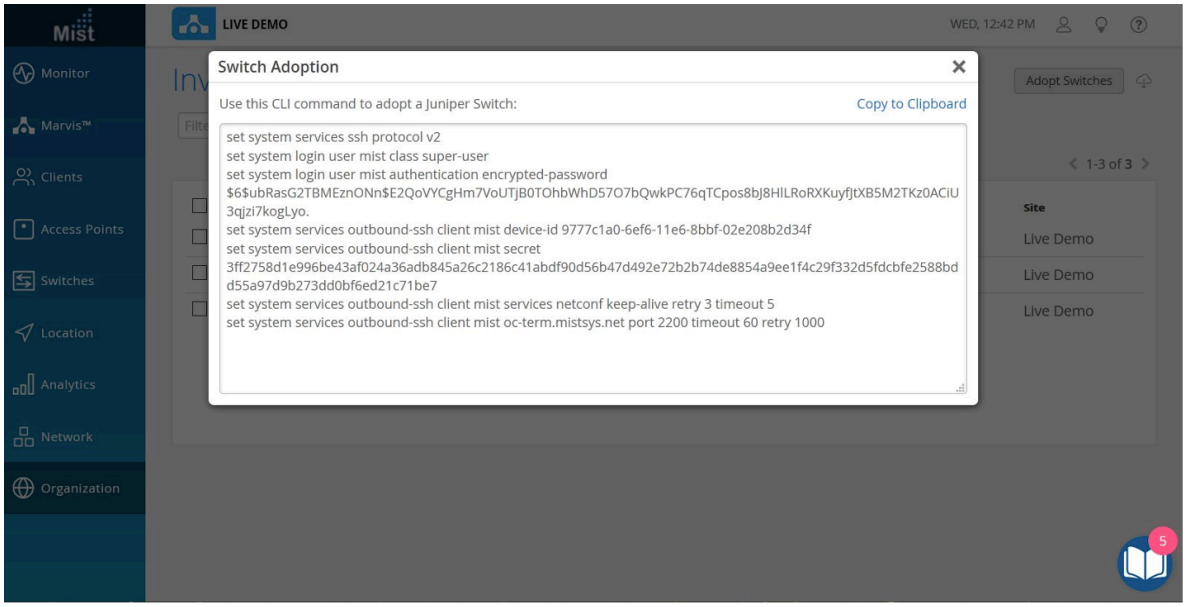
To prevent users from using the Junos OS CLI to configure the switch after it has been adopted into the Juniper Mist cloud, you may want to create a system login message on the switch to warn against making configuration changes, or to restrict their management access altogether by changing the password or placing restrictions on the Junos OS CLI user accounts.

> **NOTE**: Switch adoption will always use outbound SSH initially. Even if one has a CloudX ready switch with JMA installed the system is unable to know that upfront. The least common determinator is outbound-ssh for all switches that should be managed by Mist cloud. Once the Switch is fully managed by Mist Cloud, and JMA installed, the outbound-ssh capability may be deactivated and CloudX via HTTPS used from then on.

This procedure describes how to set up a secure connection between a supported EX Series Switch running a supported version of Junos OS. In it, you will make a few configuration changes on the portal as well as some on the switch using the Junos OS CLI. Be sure you can log on to both systems.

1. Log in to your organization on the Juniper Mist cloud and then click **Organization > Inventory** in the menu.

2. Choose **Switches** at the top of the screen that appears, and then click the **Adopt Switch** button in the upper right corner to generate the Junos OS CLI commands needed for the interoperability. The commands create a Juniper Mist user account, and a SSH connection to the Juniper Mist cloud over TCP port 2200 (the switch connection is from a management interface and is used for configuration settings and sending telemetry data).



3. In the window that appears, click **Copy to Clipboard** to get the commands from the Juniper Mist cloud.

4. At the Junos OS CLI, type “edit” to start configuration mode, and then paste the commands you just copied (type “top” if you are not already at the base level of the hierarchy).

5. Back in the portal, click **Organization > Inventory > Switches** and select the switch you just added.

6. Click the **More** drop-down at the top of the screen, and then the **Assign to Site** button to continue making your selections as prompted.

7. Confirm your updates on the switch by running show commands at the system services level of the hierarchy, and again at the system login user juniper-mist level of the hierarchy.

```
cli
show configuration system services
ssh {
    protocol-version v2;
}
netconf {
    ssh;
}
```

```
outbound-ssh {
    client mist {
        device-id 3634a49d-3e20-46d6-b0c9-0b0d6a314690;
        secret "trimmed"; ## SECRET-DATA
        keep-alive {
            retry 12;
            timeout 5;
        }
        services netconf;
        oc-term.mistsys.net {
            port 2200;
            retry 1000;
            timeout 60;
        }
    }
}
show configuration system login user mist
full-name mist;
uid 63157;
class super-user;
authentication {
    encrypted-password "trimmed"; ## SECRET-DATA
    ssh-rsa "trimmed"; ## SECRET-DATA
}
```

NOTE: The Junos OS CLI for adoption is unique to the Mist organization itself. Once retrieved, you can use it on other EX Series Switches that belong to the same organization. After first contacting the Juniper Mist cloud, the default passwords are going to be changed to unique passwords per device.

Add the Switch to the Juniper Mist Portal and View Details

Now that the switch is able to register with the portal, the next steps are to add the switch to the appropriate site and to assign APs. You do this from the portal.

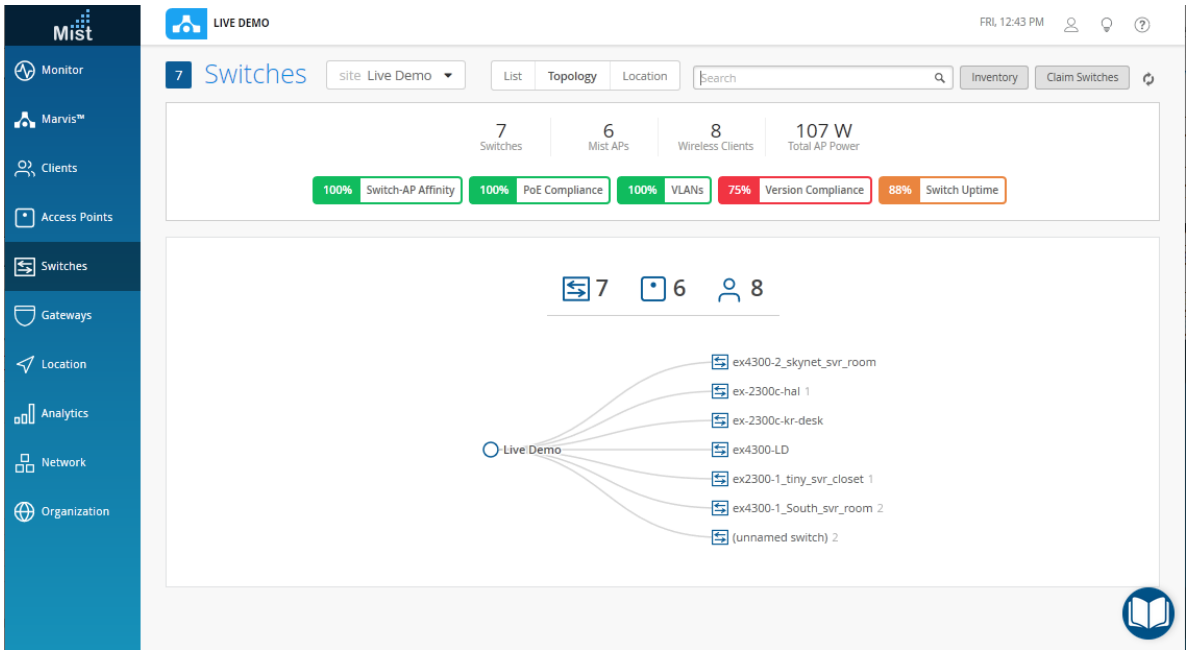
Step-by-Step Procedure:

1. To add the switch to a site, click **Organization > Inventory** in the Juniper Mist menu and then the **Switches** tab at the top of the screen that appears. Select the switch you just added, and then click

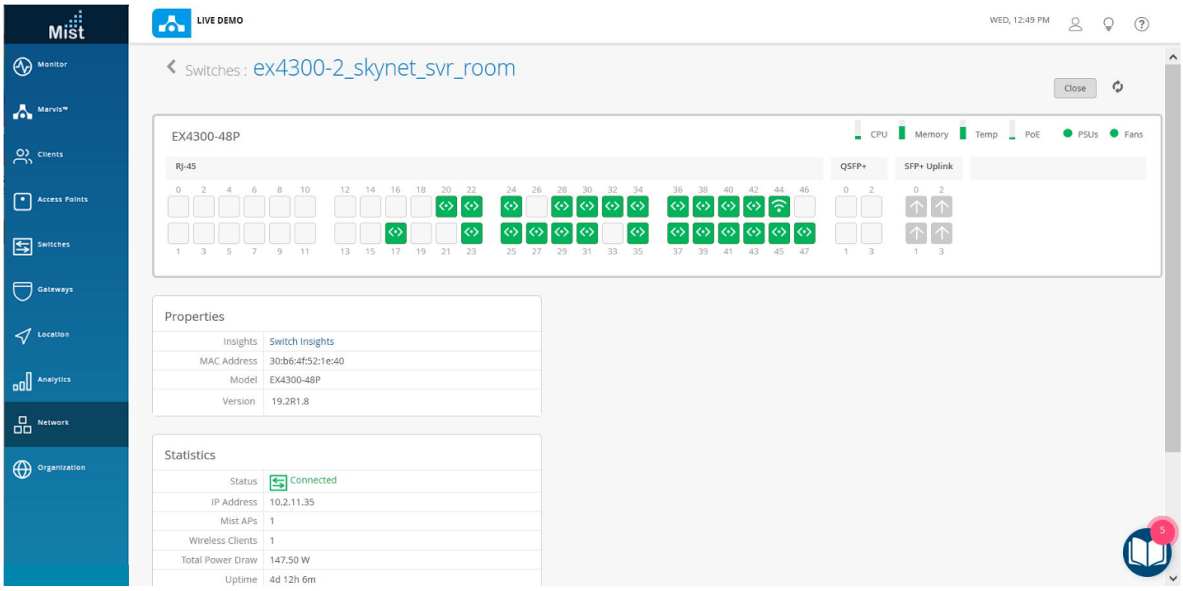
the **More** button, **Assign to Site**, and then choose a site from the drop-down list that appears in the **Assign Switches** window. Click the **Assign to Site** button to complete the action.

2. Click **Access Points** to see a list of **unassigned APs**.

3. Click **Switches** to see the list of switches. You can choose a switch from the list to confirm that it and the portal are correctly provisioned. Note that the PoE compliance you set up earlier on the switch interfaces is shown with the switch, as are the VLANs and other details.



4. From the Switches page, click a switch name to drill down into a detailed view of that switch, including connected APs and clients. For each switch on the list, you can view various properties, including the version, model number, CPU and memory utilization, bytes transferred, power drawn by the PoE devices, and port errors.



5. Finally, as the stepping off point of this JVD, open a Junos OS shell from the portal by selecting the switch you just added and then clicking Open Shell in the upper right corner of the Switches screen. From here, you have full read and write access to the switch for any further configuration changes you wish to make.

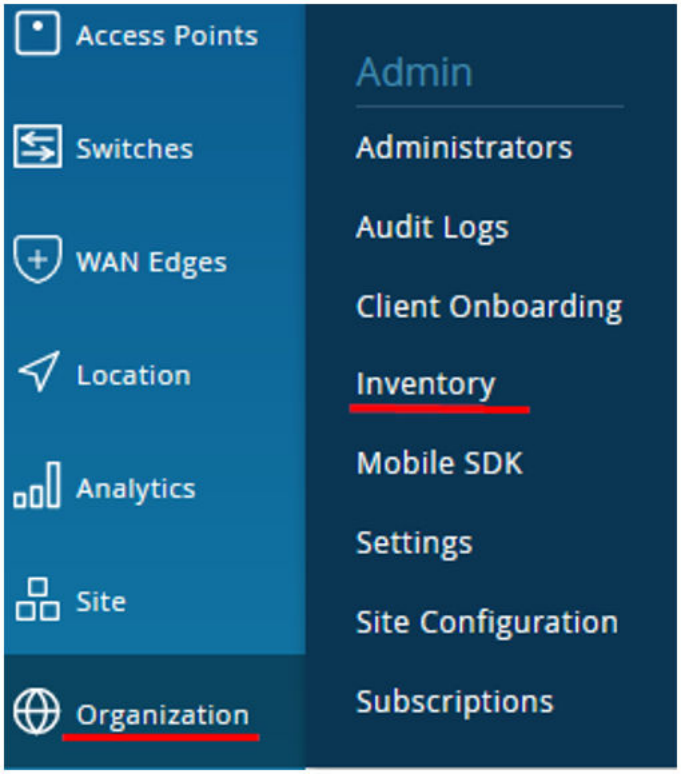
EX Series Switch Behind a WAN Router

Now it is time to onboard your switch and add it to your infrastructure. We assume in this example that we form a LAG with the WAN router and that we use the force-up method described in the previous chapter "Best practices when using Link Aggregation on the uplink Interfaces" on page 48.

To assign a switch to a site:

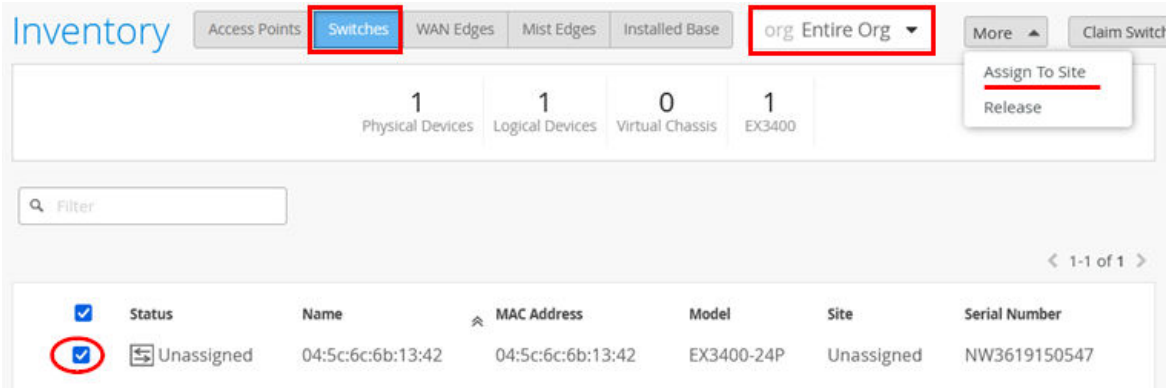
1. In the portal, click **Organization > Admin > Inventory**.

Figure 28: Navigating to Inventory



2. In the Inventory page, ensure the inventory view is set to org (Entire Org) and refresh your browser until you see all of your devices.

Figure 29: EX Series Switch in Inventory



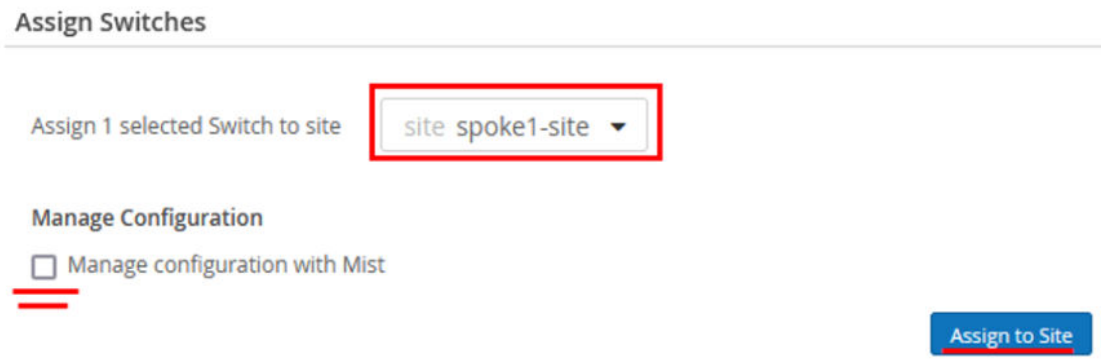
3. Select your new switch and click **Assign to Site**.

4. On the **Assign Switches** page:

a. Select `spoke1-site`.

b. **Disable Manage configuration with Mist** option. You can enable this option at a later stage, if required.

Figure 30: Selecting Site for Assigning Switch

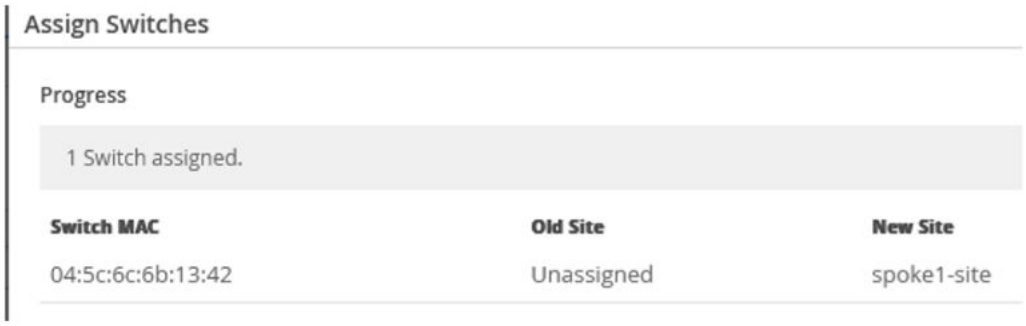


5. Click **Assign to Site**.

6. Confirm the changes in the inventory once you assign the device to the site.

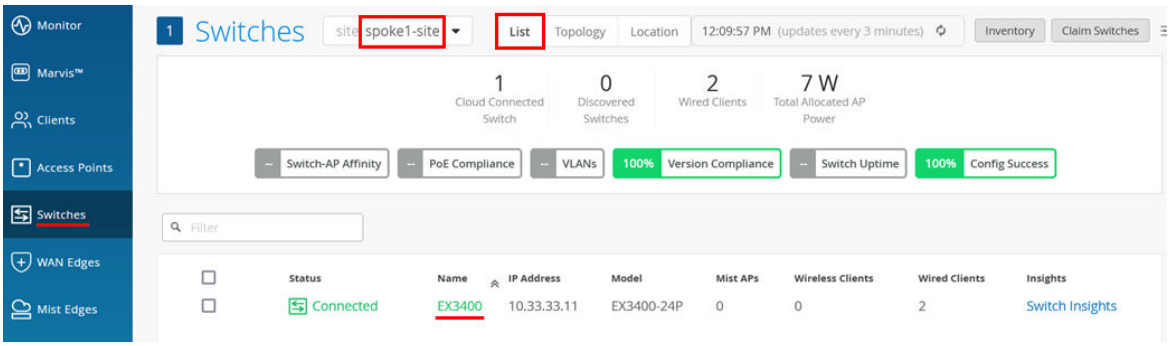
7. You can see `spoke1-site` under New Site.

Figure 31: Assigned Switch to Site Details



8. In the portal, go to Switches and select spoke1-site.

Figure 32: Selecting Assigned Switch for Modification

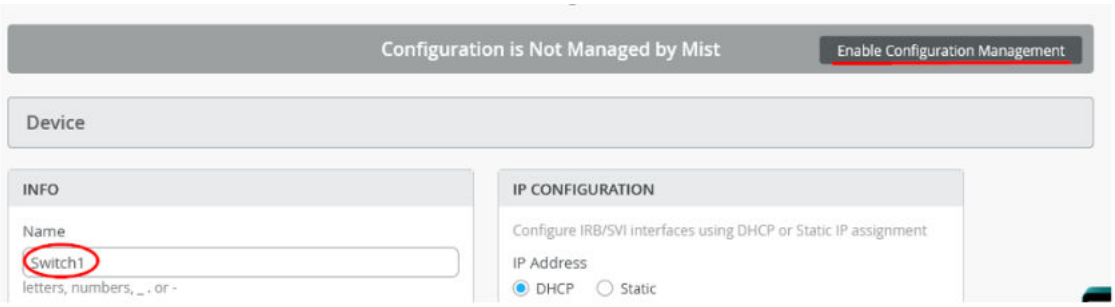


The page displays the list of switches assigned to the site.

9. Click the required switch to open the switch configuration page.

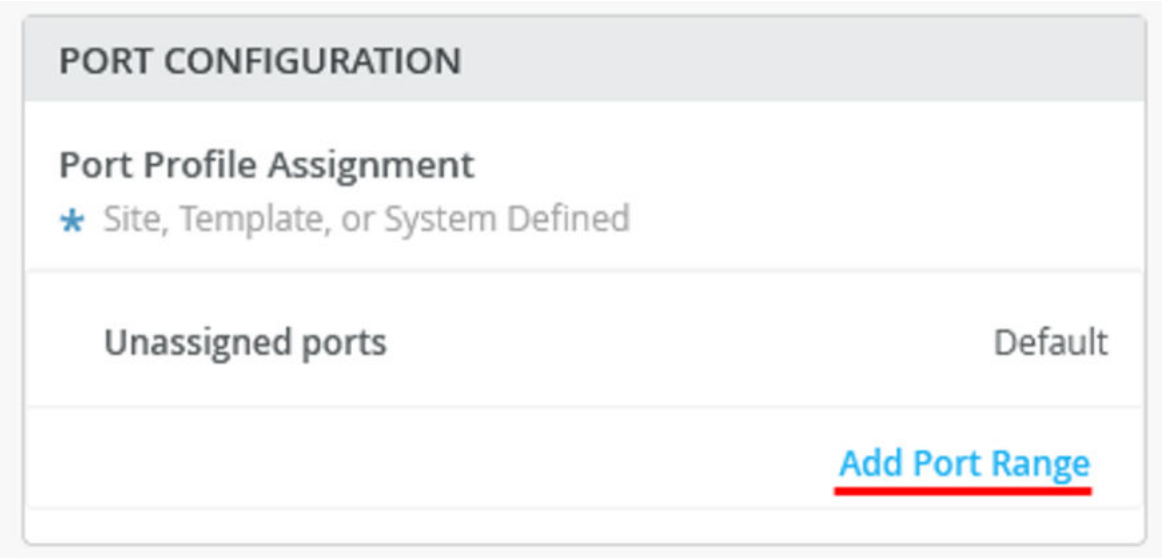
10. Verify the device name, then scroll down to the **Switch Configuration** section and check **Enable Configuration Management**.

Figure 33: Configuration of Assigned Switch



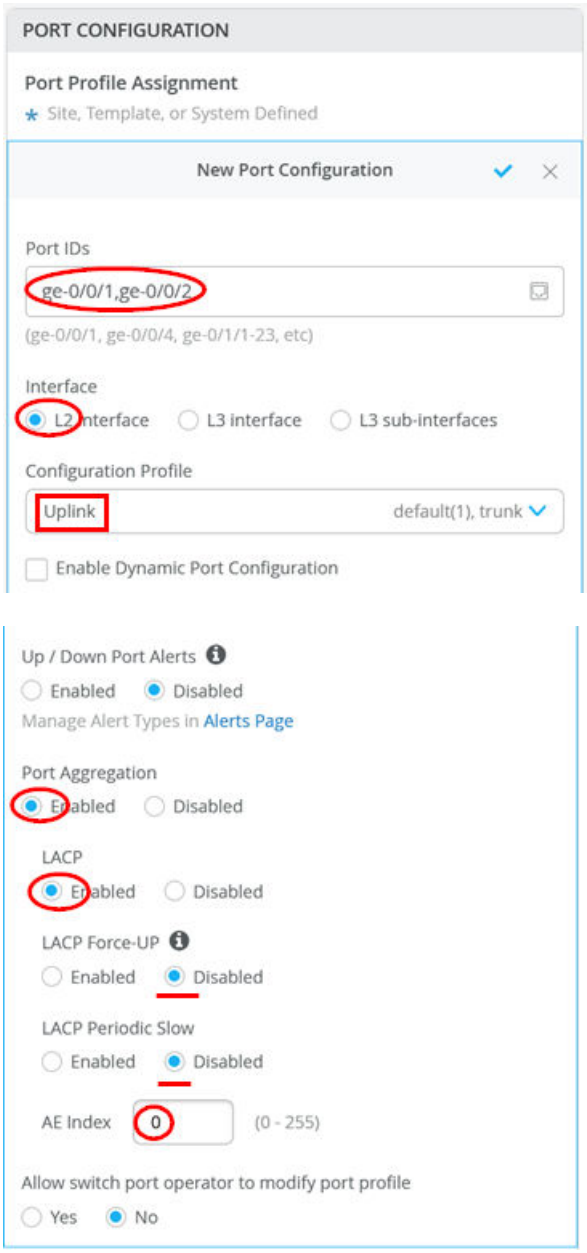
11. Under Port Configuration, click **Add Port Range**.

Figure 34: Port Configuration of Assigned Switch



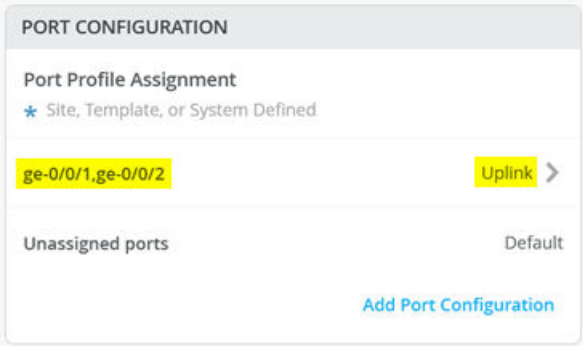
12. On the **New Port Range** page, configure the following options:
    a. Set the **Port IDs** as `ge-0/0/1` and `ge-0/0/2` (two ports for the LAG).
    b. For the interface, select the default "`L2 Interface`".
    c. Select the existing Configuration Profile as "`Uplink`".
    d. Enable Port Aggregation.
    e. Enable LACP to detect a failed or broken link.
    f. Disable force-up. You need to enable this option only on the WAN router or if this is a distribution switch where you configure a downlink towards an access switch.
    g. Leave LACP periodic slow disabled.
    h. Set the AE Index to 0 to ensure that the AE index is the same on both sides.

Figure 35: Port Configuration of Assigned Switch



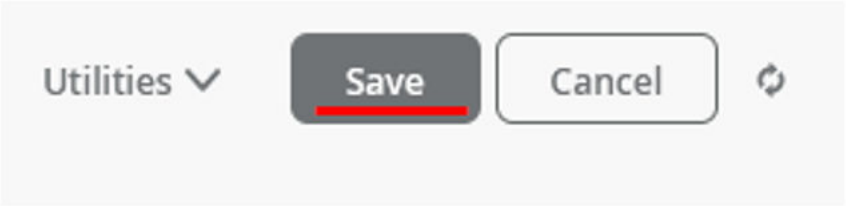
13. The figure below shows the summary of the port configuration.

Figure 36: Port Configuration of Assigned Switch



14. **Save** your changes.

Figure 37: Save Changes



You've now added a new EX Series Switch to your Juniper Mist Wired Assurance deployment.

Optionally, you can confirm that your switch has the two links up by using remote shell as shown in the following sample output:

```
              show lacp interfaces
Aggregated interface: ae0
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      ge-0/0/1       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-0/0/1     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-0/0/2       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
      ge-0/0/2     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      ge-0/0/1                  Current   Fast periodic Collecting distributing
      ge-0/0/2                  Current   Fast periodic Collecting distributing
```

Troubleshooting Tips

In this chapter, we share more information about the connection between the switch and Juniper Mist cloud. Please also review the article "How does an EX Series Switch connect to the Juniper Mist Cloud to get managed?" on page 39 where we introduced these methods in case you skipped it.

In case you encounter any issue with the onboarding process with the Juniper Mist cloud, taking the steps below may help with resetting a device and ensure further communication to the Juniper Mist cloud. An external reference is available through the following link: https://www.mist.com/documentation/troubleshooting-switches/

Check Any Firewall Between EX Series Switch and Mist Cloud Communication

We assume that you have implemented the protocols and port openings on your firewall as described here. For EX Series Switch management, the three most important protocols and port openings are:

- **For Outbound SSH connections towards Juniper Mist cloud:** TCP to destination port 2200. The EX Series Switch establishes an outbound SSH session to pass a source NAT towards the Internet which works in the following way:
  - The device uses a raw socket for a TCP connection to the Juniper Mist cloud.
  - Once the TCP connection is established, the device sends a special DMI message so that the Juniper Mist cloud gathers information such as the device serial number to determine which devices need to be managed.
  - If the Juniper Mist cloud has identified the device based on the DMI, it uses the existing TCP connection to establish a reverse SSH session back to the device with the credentials known for SSH login.
  - It is critical that the firewall vendor does not attempt to apply any kind of further application-level management looking deeper into the session. It can be assumed that the special DMI message and reverse SSH login are unknown applications. This TCP 2200 port session must not be inspected deeper and must be treated as raw all the time.
- **For Claim and ZTP of the Switch:** An HTTPS TLS-encrypted session towards destination port 443 towards FQDN `redirect.juniper.net`. This is required for the ZTP process to work and for the device to retrieve the initial config to attach to the correct Juniper Mist cloud. If for some reason this is not possible, consider the brownfield adoption method instead.
- **For CloudX connections towards Juniper Mist cloud:** You need to open an HTTPS TLS-encrypted session towards destination port 443 towards the Juniper Mist cloud. Here, the firewall vendor can apply application-level management for the TLS session. The destination FQDN is usually `jma-terminator.<cloud>.mist.com`

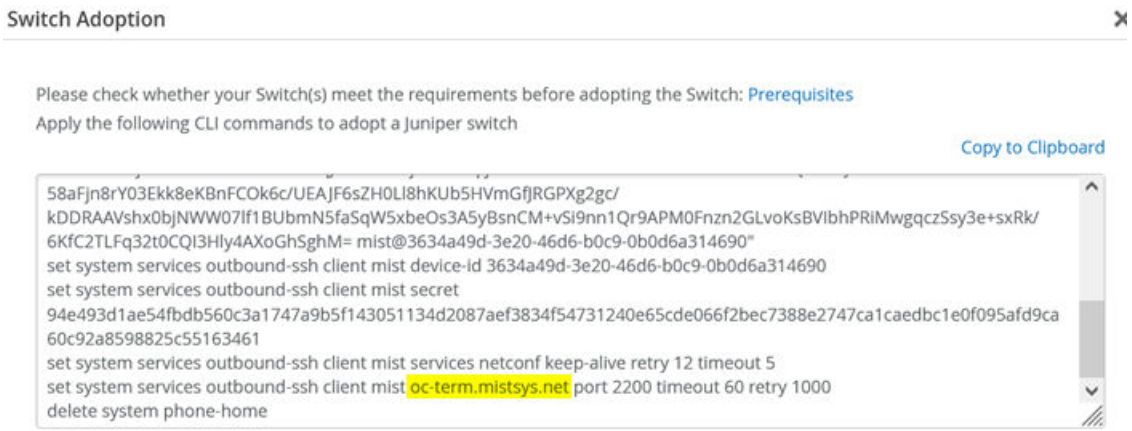
NOTE: The recommendation is that you open both ports required for outbound SSH and CloudX operation. When unboxing a new switch, you may not have the JMA client installed as part of the factory-installed Junos OS version. Also, the adoption method uses outbound SSH initially to manage the device.

If you have console access to the device you can try the following check:

```
# test you can ping a site in the internet
root> ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=53 time=5.371 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=53 time=5.175 ms
# test DNS working as well
root> ping www.google.com inet
PING www.google.com (142.251.32.36): 56 data bytes
64 bytes from 142.251.32.36: icmp_seq=0 ttl=112 time=24.966 ms
64 bytes from 142.251.32.36: icmp_seq=1 ttl=112 time=18.031 ms
64 bytes from 142.251.32.36: icmp_seq=2 ttl=112 time=9.661 ms
64 bytes from 142.251.32.36: icmp_seq=3 ttl=112 time=8.440 ms
```

Switches Using Outbound SSH as the Connection Towards Juniper Mist Cloud

For the next step, you need to know the FQDN of the management instance of the Juniper Mist cloud. You get this information by going to **Organization > Inventory** and then selecting **Switches** and then clicking **Adopt Switches**.



In the above example, the device is managed by FQDN “oc-term.mistsys.net” so we can try to open a telnet session to port 2200.

```
# test that a telnet session can be established
root> telnet oc-term.mistsys.net port 2200
Trying 52.53.57.207...
Connected to a4119aeb75a5342119e38dd3c475aff9-99130767d4e77d46.elb.us-west-1.amazonaws.com.
Escape character is '^]'.
^C
```

If the telnet session can be successfully established, it is a positive indication, but it does not guarantee full connectivity. This is because a test telnet session cannot replicate the complete connection process. Some firewalls that perform application-level inspection may still terminate the session later. Therefore, the next step is to verify that the session remains active and stable over time without unexpected interruptions.

```
# test that an outbound ssh session can be established
root> show system connections | match 2200 | match ESTA
tcp4       0      0  192.168.10.205.60913    52.53.57.207.2200  ESTABLISHED
# see for a longer time that the connection stays really up
root> show system connections | match 2200 | match ESTA | refresh 5
---(refreshed at 2024-02-29 14:49:49 UTC)---
tcp4       0      0  192.168.10.205.60913    52.53.57.207.2200  ESTABLISHED
---(refreshed at 2024-02-29 14:49:54 UTC)---
tcp4       0      0  192.168.10.205.60913    52.53.57.207.2200  ESTABLISHED
---(refreshed at 2024-02-29 14:49:59 UTC)---
tcp4       0      0  192.168.10.205.60913    52.53.57.207.2200  ESTABLISHED
---(refreshed at 2024-02-29 14:50:04 UTC)---
tcp4       0      0  192.168.10.205.60913    52.53.57.207.2200  ESTABLISHED
---(refreshed at 2024-02-29 14:50:09 UTC)---
tcp4       0      0  192.168.10.205.60913    52.53.57.207.2200  ESTABLISHED
---(refreshed at 2024-02-29 14:50:14 UTC)---
tcp4       0      0  192.168.10.205.60913    52.53.57.207.2200  ESTABLISHED
---(refreshed at 2024-02-29 14:50:19 UTC)---
tcp4       0      0  192.168.10.205.60913    52.53.57.207.2200  ESTABLISHED
---(refreshed at 2024-02-29 14:50:24 UTC)---
tcp4       0      0  192.168.10.205.60913    52.53.57.207.2200  ESTABLISHED
---(refreshed at 2024-02-29 14:50:29 UTC)---
tcp4       0      0  192.168.10.205.60913    52.53.57.207.2200  ESTABLISHED
---(refreshed at 2024-02-29 14:50:34 UTC)---
tcp4       0      0  192.168.10.205.60913    52.53.57.207.2200  ESTABLISHED
```

```
---(refreshed at 2024-02-29 14:50:39 UTC)---
tcp4       0      0  192.168.10.205.60913    52.53.57.207.2200  ESTABLISHED
---(refreshed at 2024-02-29 14:50:44 UTC)---
tcp4       0      0  192.168.10.205.60913    52.53.57.207.2200  ESTABLISHED
---(refreshed at 2024-02-29 14:50:49 UTC)---
tcp4       0      0  192.168.10.205.60913    52.53.57.207.2200  ESTABLISHED
---(refreshed at 2024-02-29 14:50:54 UTC)---
tcp4       0      0  192.168.10.205.60913    52.53.57.207.2200  ESTABLISHED
---(*more 100%)---[abort]
```

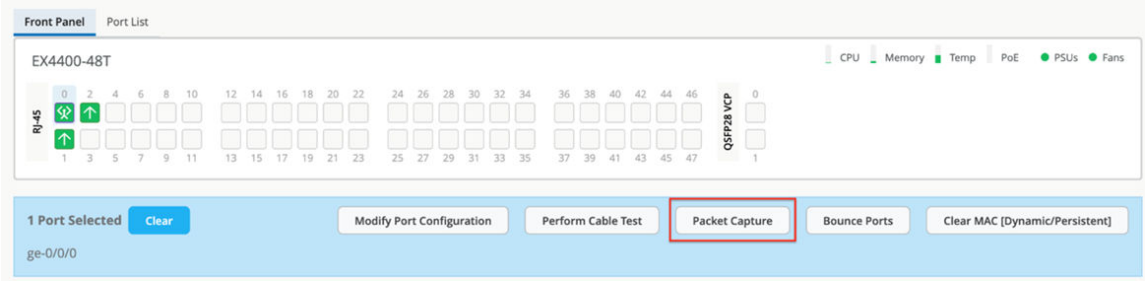
Switches Using CloudX as the Connection Towards Juniper Mist Cloud

To check if a switch can communicate with Juniper Mist cloud using CloudX:

1. Run the below CLI commands on the switch:

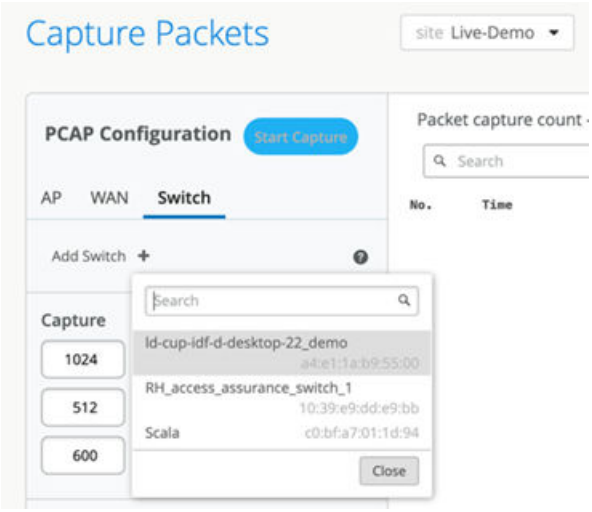
```
user@switch> show version | match mist
JUNOS Mist Agent [v1.0.2205-2]
.
user@switch> show system connections | grep 443
tcp4       0      0  192.168.2.52.62957
52.52.102.40.443                       ESTABLISHED
```

2. To verify CloudX through the Juniper Mist portal, you can use the steps below:
   a. Log in to the Juniper Mist portal (manage.mist.com).
   b. Click **Switches > switch name** to go to the switch detail page.
   c. Click any port or a range of ports.
      If CloudX is running, the **Packet Capture** button is enabled; otherwise, the button is grayed out.



You can also check if CloudX is enabled on multiple switches by using the Juniper Mist portal.

To do that, click **Site > Switch Packet Captures > Add Switch**.



The switches listed here are all CloudX-enabled.

3. Verify that Juniper Mist cloud daemon (mcd) and Junos Mist daemon (jmd) is running.

   The mcd process is responsible for enabling communication between the switch and the cloud. It maintains a secure WebSocket connection to the terminator in the cloud.

   The jmd process is used for:

   - Generating periodic statistics for the device.
   - Applying device configuration.
   - Gathering device events.
   - Initiating device functions (such as packet capture and software updates).
   - Returning results from requested functions (such as files and streamed data).

   To verify that jmd and mcd are running, use the following CLIs:

```
user@switch> set cli screen-width 400
user@switch> start shell
% ps aux | grep jmd
root   21408   0.0  0.4 1246080  32200  -  S    Fri23      15:17.51 /var/run/scripts/jet/jmd -
mcd-socket /var/run/mist_mcd.ipc
mist    3706   0.0  0.0   11136   2516  0  S+   07:14       0:00.00 grep jmd
%
%
% ps aux | grep mcd
root   21319   0.0  0.3 1242924  22256  -  I    Fri23       8:18.00 /var/run/scripts/jet/mcd
root   21408   0.0  0.4 1246080  32200  -  S    Fri23      15:17.53 /var/run/scripts/jet/jmd -
```

```
mcd-socket /var/run/mist_mcd.ipc
mist    3708   0.0  0.0   11136   2516  0  S+   07:14       0:00.00 grep mcd
%
```

4. Check the jmd and mcd logs for any errors by using the CLI commands below. Typically, jmd logs show issues related to configuration or stats. The mcd logs report issues related to the connectivity between the switch and the cloud.

```
user@switch> show log jmd.log | last 10
[jmd] 2024/11/04 07:12:02 collector.go:850: total stats collection time = 10s
[jmd] 2024/11/04 07:12:02 app_states.go:355: app sending stats to mist cloud (26171 bytes)
[jmd] 2024/11/04 07:12:02 app_states.go:360: successfully sent ipc stats:
[jmd] 2024/11/04 07:12:02 app.go:282: processing app state "STEADY"
[jmd] 2024/11/04 07:12:12 app.go:339: sending ipc keep-alive
[jmd] 2024/11/04 07:12:22 app.go:339: sending ipc keep-alive
[jmd] 2024/11/04 07:12:32 app.go:339: sending ipc keep-alive
[jmd] 2024/11/04 07:12:42 app.go:339: sending ipc keep-alive
[jmd] 2024/11/04 07:12:52 app.go:339: sending ipc keep-alive
[jmd] 2024/11/04 07:12:52 collector.go:417: collecting periodic stats, interval 60
```

.

```
user@switch> show log mcd.log | last 10
[mcd] 2024/11/04 07:09:31 app.go:967: successfully sent msg to cloud: ep-telemetry
[mcd] 2024/11/04 07:10:02 ipc_server.go:414: rx ipc request: send cloud telemetry
[mcd] 2024/11/04 07:10:02 ipc_server.go:447: forwarding ipc telemetry to "junos-stats-"
(26167 bytes)
[mcd] 2024/11/04 07:11:02 ipc_server.go:414: rx ipc request: send cloud telemetry
[mcd] 2024/11/04 07:11:02 ipc_server.go:447: forwarding ipc telemetry to "junos-stats-"
(26171 bytes)
[mcd] 2024/11/04 07:12:01 app.go:967: successfully sent msg to cloud: ep-telemetry
[mcd] 2024/11/04 07:12:02 ipc_server.go:414: rx ipc request: send cloud telemetry
[mcd] 2024/11/04 07:12:02 ipc_server.go:447: forwarding ipc telemetry to "junos-stats-"
(26171 bytes)
[mcd] 2024/11/04 07:13:02 ipc_server.go:414: rx ipc request: send cloud telemetry
[mcd] 2024/11/04 07:13:02 ipc_server.go:447: forwarding ipc telemetry to "junos-stats-"
(26171 bytes)
```

5. If jmd or mcd are not running for some reason, try restarting them, as shown in the sample below.

```
user@switch> request extension-service restart-daemonize-app mcd
Extension-service application 'mcd' with pid: 92502 exited with return: -1
Extension-service application restarted successfully
```

> **NOTE**: If you are using a Junos OS 22.4xx version, use the command `request extension-service daemonize-restart mcd`.

6. If the switch is not connecting to the cloud, check its reachability by using ping and curl tests. These tests will help you check if the required ports are allowed through the firewall.

The cloud endpoints are not set up to respond to ping tests; however, running a ping test will ensure that DNS resolves FQDN. Here is a sample ping test:

```
user@switch> ping jma-terminator-staging.mistsys.net
PING a8481a00030ad459aac15af07d5f2c5b-75855524.us-east-1.elb.amazonaws.com (3.210.247.53): 56
data bytes
^C
--- a8481a00030ad459aac15af07d5f2c5b-75855524.us-east-1.elb.amazonaws.com ping statistics ---
1 packets transmitted, 0 packets received, 100% packet loss
```

Here is a sample curl test:

```
user@switch> start shell
% curl -k https://jma-terminator.mistsys.net/test
Welcome to MIST
%
```

A valid response from the curl test proves that the jma-terminator in the Juniper Mist cloud is reachable. A lack of response or receipt of an error will indicate that the path between the switch and the cloud is blocking these ports, likely because of the firewall. The URLs used in the test are the same as those in firewall ports and differ between cloud instances.

Recover a Root Password

When you need to recover your root password, you must have a local console connection to the device and then follow the instructions here: https://www.juniper.net/documentation/us/en/software/junos/user-access/topics/topic-map/recovering-root-password.html.

Remove a Virtual Chassis

If you experience an issue with a Virtual Chassis setup, in some cases you may want to reset the entire system to factory settings. The CLI output below is based on the excellent demonstration video on YouTube.

```
# Login on first Switch and do
request virtual-chassis vc-port set interface vcp-255/1/0 disable
request virtual-chassis vc-port set interface vcp-255/1/1 disable
# added interfaces for EX4400
request virtual-chassis vc-port set interface vcp-255/1/2 disable
request virtual-chassis vc-port set interface vcp-255/1/3 disable
```

After entering the above commands on the primary switch, the primary switch will disconnect from the Virtual Chassis. Any further commands entered on this switch now go to the dedicated console port for this switch. The system will elect a new primary so try the next console port and repeat this process until all switches are finally disconnected from the Virtual Chassis and you have a dedicated console connection to all switches.

Next, access each switch and run the appropriate commands based on its member ID:

```
# delete any exiting pre-provision config first
edit
delete virtual-chassis pre-provision
commit and-quit
.
# When indicated by the ":1" member ID do the following
{master:1}
request virtual-chassis recycle member-id 0
request virtual-chassis renumber member-id 1 new-member-id 0
yes
.
# When indicated by the ":0" member ID do the following
{master:0}
request virtual-chassis recycle member-id 1
.
# In case the switch went into linecard-mode do this and then login again
request virtual-chassis reactivate
```

As a last step, ensure all your switches display “Master” as their role (ignore the master priority for now) and don’t see any other switch as connected before you leave the lab.

```
              show virtual-chassis
.
Virtual Chassis ID: 3d2d.5316.b4c3
Virtual Chassis Mode: Enabled
.                                                 Mstr           Mixed Route Neighbor List
Member ID  Status   Serial No    Model          prio  Role      Mode  Mode ID  Interface
0 (FPC 0)  Prsnt    NX0216330306 ex3400-48t     128   Master*      N  VC
#
# Make sure there is no other memebr displayed here
#
.
Member ID for next new member: 1 (FPC 1)
```

Factory Reload of a Single Device

To get an EX Series Switch back to the initial factory configuration, execute the commands shown below and then afterwards, check that it can contact the Juniper Mist cloud.

```
              cli
              edit
              load factory-default
              delete chassis auto-image-upgrade
              set system root-authentication plain-text-password
# we are adding the below as a best practice
set system name-server 8.8.8.8
              set interfaces irb unit 0 family inet dhcp force-discover
              set interfaces vme unit 0 family inet dhcp force-discover
              commit and-quit
              show configuration | save /config/recovery.conf
# now check that you got a DHCP-lease and have a default route
show route
inet.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
Limit/Threshold: 32768/32768 destinations
+ = Active Route, - = Last Active, * = Both
0.0.0.0/0          *[Access-internal/12] 00:01:34, metric 0
                    >  to 10.33.33.1 via irb.0
10.33.33.0/24      *[Direct/0] 00:01:35
```

```
                    >  via irb.0
10.33.33.11/32     *[Local/0] 00:01:35
                       Local via irb.0
# test you can ping a site in the internet
ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=53 time=5.371 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=53 time=5.175 ms
# test DNS working as well
ping www.google.com inet
PING www.google.com (142.251.32.36): 56 data bytes
64 bytes from 142.251.32.36: icmp_seq=0 ttl=112 time=24.966 ms
64 bytes from 142.251.32.36: icmp_seq=1 ttl=112 time=18.031 ms
64 bytes from 142.251.32.36: icmp_seq=2 ttl=112 time=9.661 ms
64 bytes from 142.251.32.36: icmp_seq=3 ttl=112 time=8.440 ms
```

Check the Device RTC Clock When Having ZTP Issues.

The longer a device remains in storage, the more its internal clock can drift. During the phone-home ZTP process, the device verifies the server certificate, and if the local clock is significantly incorrect—such as being set to 1970—the verification will fail. As a best practice, an NTP server should always be used to synchronize the device's time. The Juniper Mist cloud automatically configures this once the device is under its management. However, during the initial factory default state when starting ZTP, this configuration is not yet in place. If this issue occurs, you can either configure an NTP server or manually set the system clock, as shown below:

```
# optional: set a local NTP server of this lab
cli
edit
set system ntp boot-server 216.239.35.0
set system ntp server 216.239.35.0
commit and-quit
# check current time else ZTP CA-Certificates may be rejected
show system uptime
Current time: 2024-01-08 14:16:34 UTC
.
.
# In case the date is below Year 2024 manually adjust the local time
# set date YYYYMMDDhhmm.ss
# or check if you already have enough connctivity to do that via our lab ntp
# set date ntp 216.239.35.0
restart phone-home-client
```

```
Phone home client daemon signalled but still running, waiting 28 seconds more
Phone home client daemon still running, sending another terminate signal
Phone home client daemon started, pid 7197
```

Juniper Access Point Attached to EX Series Switch

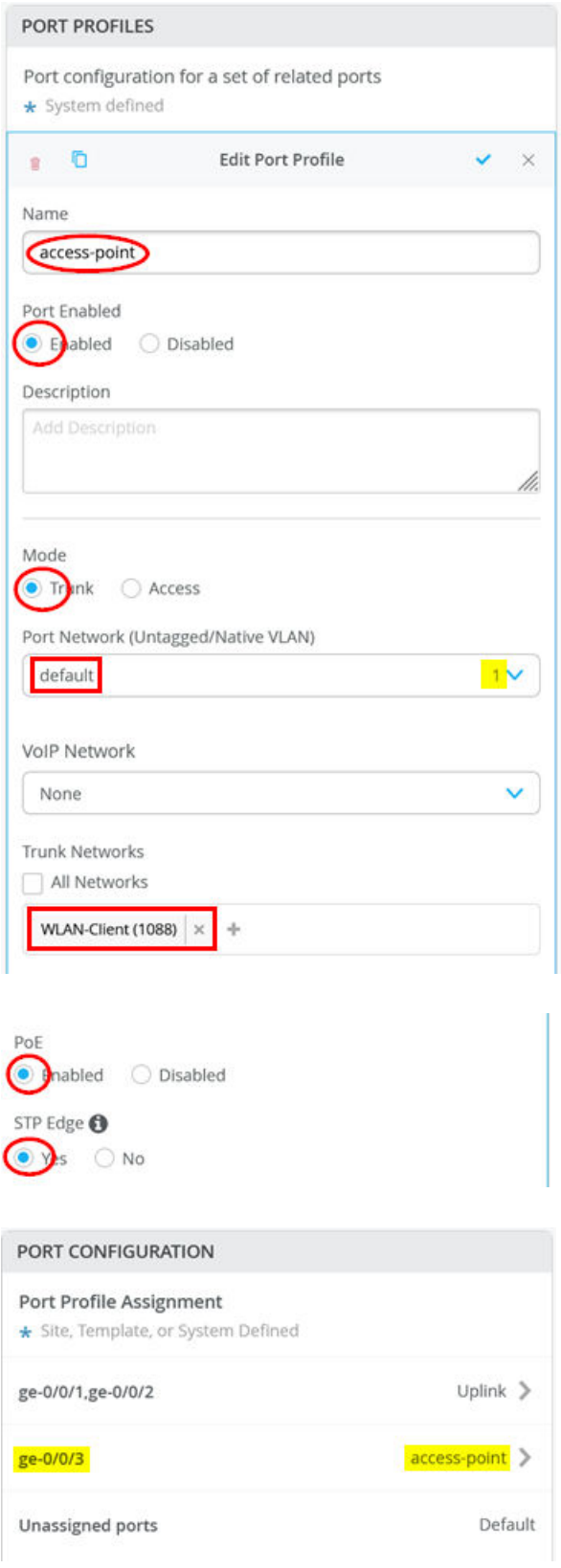
Here, we integrate the next element to complete the branch installation which is attaching the AP to the switch to support wireless clients.

Pre-Conditions That Must Be Met for AP Onboarding

To be able to execute this lab, we assume that the following conditions are met:

- The AP is cabled to our EX Series Switch and has power (through an external power supply or through PoE).
- If PoE is being used, the switch must have sufficient available PoE power and support at least IEEE 802.3af or IEEE 802.3at standards, depending on the AP model.
- LLDP should be enabled on switches and routers to assist with troubleshooting, although it is not strictly required.
- You have completely followed the instructions from the above chapters as those include instructions for the following:
  - A DHCP server is configured for the AP management VLAN 1033 subnet 10.33.33.0/24 in this branch. In our example, that is done on the WAN router.
  - An additional VLAN 1088 subnet 10.88.88.0/24 is used for WLAN clients.
  - An additional VLAN 1099 subnet 10.99.99.0/24 is used for wired clients.
  - On the WAN router, a LAG is formed to the switch containing native VLAN 1033 and VLANs 1088 and 1099 as trunk. Keep in mind that without further changes, the native VLAN from the uplink gets assigned to VLAN 1 on the switch where irb.0 for in-band management is assigned. Providing that management VLAN then to a downstream device such as an AP needs then to reference this VLAN 1.
  - On the port where the switch is attached, the default VLAN 1 is native and VLAN 1088 is trunked. We did not add 1099 for wired clients again as the port does not need to support it.
  - The WAN router must implement some form of source NAT on the WAN interfaces to allow management traffic towards the Juniper Mist cloud.

Below is just a reminder about the minimal configuration on the switch (apart from the uplink):

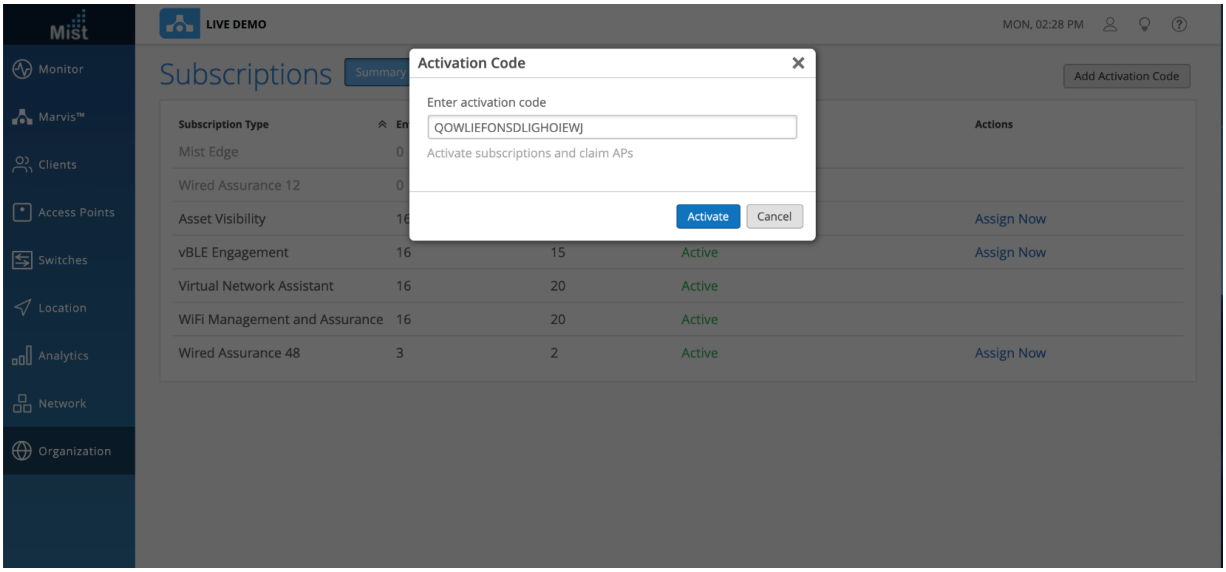


How to Claim APs to an Organization

APs can be claimed to any organization by using either an activation code, claim code, or QR code.

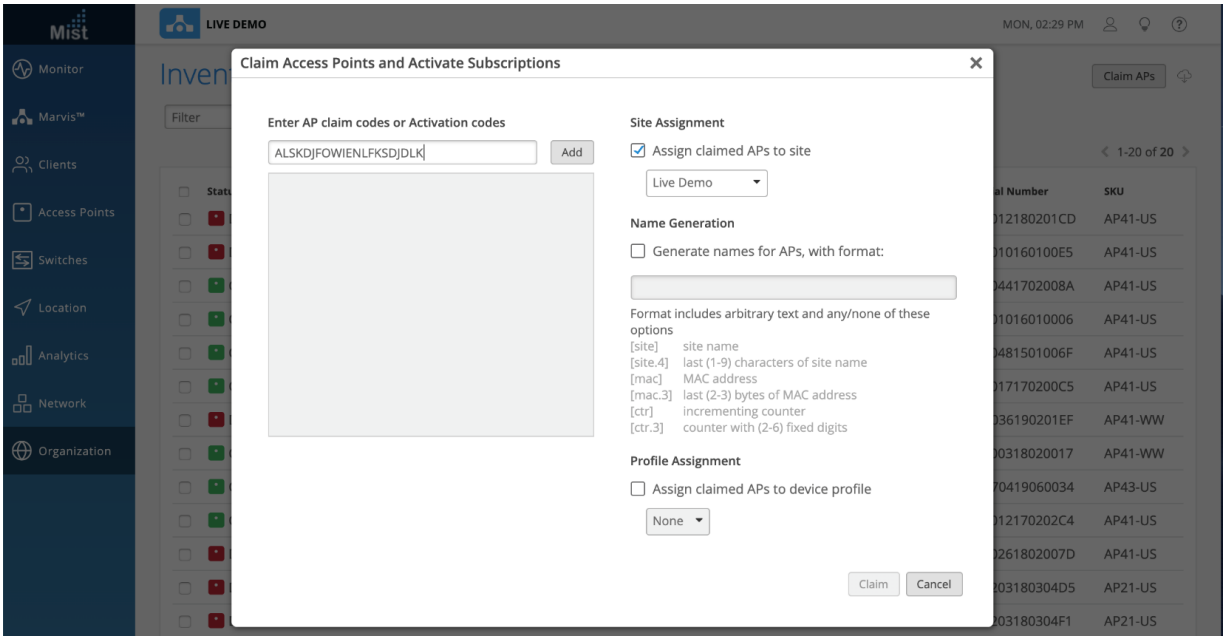
Activation Code

Whenever you order APs, our Sales Operations team will send you an activation code which can be used for claiming the APs and subscriptions as per the order. You can use this activation code to claim APs in one go. To claim the APs, go to the **Organization > Subscriptions** page and select **Add Activation Code** button in the upper-right corner. Once the activation code is added and activated, all the APs will automatically get claimed to the organization. You can see the list of APs on the **Inventory** page (**Organization > Inventory**).



AP Claim Code

You can individually claim APs to your organization by navigating to **Organization > Inventory > Claim APs** and entering in the claim code found on the back of each AP.



AP QR Code

Using our MistAI mobile app, you can scan the QR code printed on the back of our APs to claim APs to your organization. Our app is compatible with both iOS and Android devices. Read more about it here: https://www.mist.com/documentation/mist-ai-mobile-app/

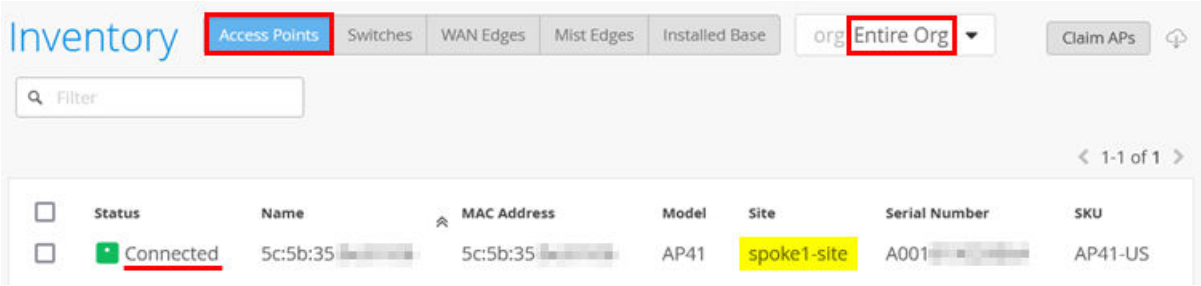
Where Can I Get the Claim Codes for the APs in My Organization?

The claim code of the AP is written on the backside of the AP where the QR code of the AP is printed.

Figure 38: Photo of a Claim Code

Troubleshoot: Bringing the AP Online as “Connected” Into the Inventory

We assume in this step you have used any of the methods above to claim the AP into the inventory. When you refresh the browser window after 3-5 minutes, the AP should appear automatically in the “Connected” state in the Inventory such as seen in the figure below:



If your AP shows as “Connected”, you can skip this section, as the following instructions cover troubleshooting if the AP is not connecting.

The troubleshooting of Juniper APs is explained in detail here: https://www.mist.com/documentation/category/troubleshooting/. This section will focus on what to troubleshoot on the EX Series Switch side to help bring the AP into the “`Connected`” state in the Inventory.

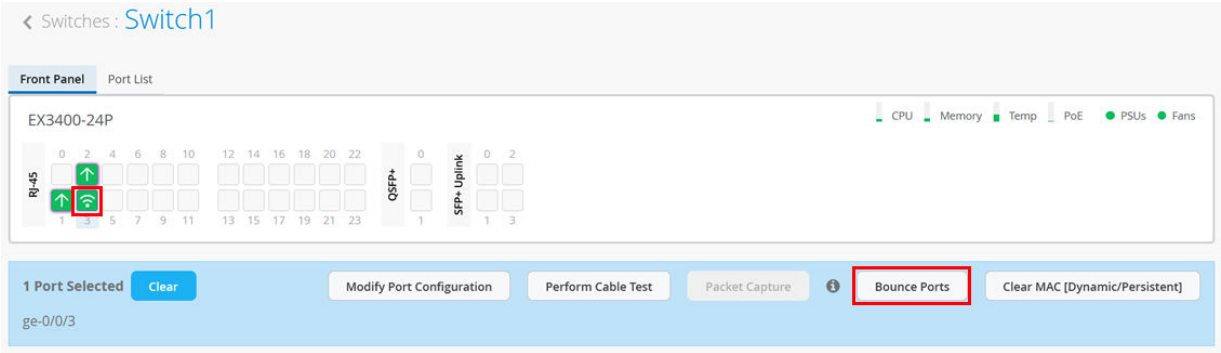
> **NOTE**: If the AP is not assigned to a site, it will always appear in the “Disconnected” state irrespective of its connectivity to the cloud. Remember that along with claiming the AP, assigning the AP to a site is mandatory.

If you are local to the site, check the AP’s status LED since its blinking code may indicate an error.

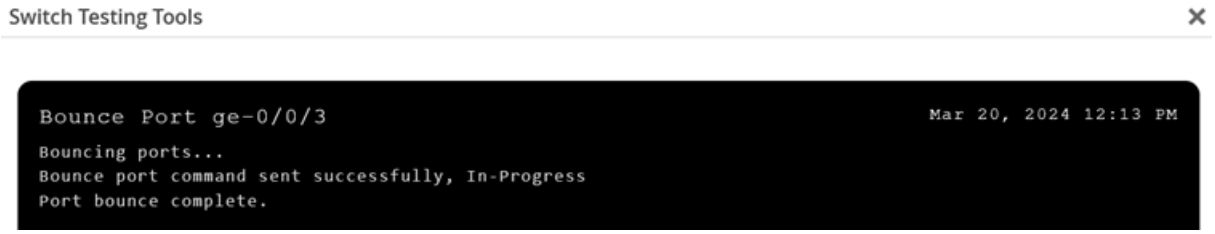
Figure 39: LED Blink Patterns

The first thing to do is to understand the source of the error by viewing the AP's status LED. If you can't see the LED on the AP, reboot it. If the AP is powered by PoE, then you can do that using one of two methods:

- Use the **Bounce Ports** option on the portal. Selecting the port where the AP is attached opens a pane where you can directly select to bounce a particular port which will also power cycle the attached AP.



You will see a new window with information about the bounce port status as shown in the figure below:



NOTE: Bouncing a port may take several minutes since two Junos OS configuration commits must happen as part of the process.

- Change the PoE interface configuration using remote shell (This option is not recommended).

```
cli
edit
set poe interface ge-0/0/3 disable
commit
# wait >20seconds
delete poe interface ge-0/0/3 disable
commit and-quit
exit
```

If the AP is powered by an external power supply, then you must ask someone to unplug it for a while and then power it on again. The AP has no console connection like the switches.

The next step is to use a remote console to the switch to review items such as:

- Is the port that the AP is connected to showing as “Up”?
- Is the port that the AP is connected to correctly configured and forwarding packets?

- Does the MAC address of the AP appear on the expected port?
- Do you see the AP appearing as an LLDP neighbor?
- Assuming the AP is powered by PoE, what's the actual power draw?

The following example output shows an AP that is attached to interface ge-0/0/3:

- Check if the port is administratively "up" and a physical link detected.

```
root@Switch1> show interfaces terse
Interface               Admin Link Proto    Local                 Remote
ge-0/0/0                up    down
ge-0/0/0.0              up    down eth-switch
ge-0/0/1                up    up
ge-0/0/1.0              up    up   aenet    --> ae0.0
ge-0/0/2                up    up
ge-0/0/2.0              up    up   aenet    --> ae0.0
ge-0/0/3                up
              up
ge-0/0/3.0              up    up   eth-switch
ge-0/0/4                up    down
ge-0/0/4.0              up    down eth-switch
.
```

- Then, check that the port is in forwarding mode and that it is configured with the expected VLAN (the default VLAN in this example) and is in access mode. Also, verify that the VLAN assigned is the same VLAN that the WAN router uses for DHCP lease handouts for AP management.

```
root@Switch1> show ethernet-switching interface ge-0/0/3
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
                         LH - MAC limit hit, DN - interface down,
                         MMAS - Mac-move action shutdown,  AS - Autostate-exclude enabled,
                         SCTL - shutdown by Storm-control, MI - MAC+IP limit hit)
Logical         Vlan                  TAG   MAC    MAC+IP STP         Logical
Tagging
interface       members                     limit  limit  state       interface flags
ge-0/0/3.0                                  32768  0                                tagged
                WLAN-Client           1088  32768  0      Forwarding                tagged
                default               1     32768  0      Forwarding
untagged
```

- Next, check if the MAC address (also printed on the QR code) of the AP appears on the switch's interface as expected.

```
root@Switch1> show ethernet-switching table
MAC flags (S - static MAC, D - dynamic MAC, L - locally learned, P - Persistent static, C -
Control MAC
           SE - statistics enabled, NM - non configured MAC, R - remote PE MAC, O - ovsdb MAC)
Ethernet switching table : 2 entries, 2 learned
Routing instance : default-switch
    Vlan                MAC                 MAC         Age    Logical
NH        RTR
    name                address             flags              interface
Index     ID
    default             5c:5b:35:be:81:06   D             -    ge-0/0/3.0
0         0
    default             ee:38:73:9a:d4:a5   D             -    ae0.0
0         0
```

NOTE: At this point, it is appropriate to check the port authorization status of the AP as well. Sometimes it is intended that the AP authorizes itself to the switch it is attached to and sometimes this is not required, and someone accidentally applies a port profile with authentication enabled.

- Next, check if you see the AP's MAC address appearing as an LLDP neighbor Chassis ID. The port info may be different based on the AP model you have; however, the system name may help you determine more about the state of the AP:
  - When no LLDP system name is reported, then the AP has a connection issue. For example, it cannot receive a DHCP lease.
  - When the LLDP system name is "Mist", like in the example below, then the AP is usually up but not assigned to an inventory.
  - When the LLDP system name is the MAC address of the AP or the inventory name, then it should already be in the "Connected" state in the inventory of your organization and you can start applying more configuration.

```
root@Switch1> show lldp neighbors
Local Interface    Parent Interface    Chassis Id          Port info          System Name
ge-0/0/1           ae0                 ec:38:73:9a:d5:24   ge-0/0/5           spoke1
ge-0/0/2           ae0                 ec:38:73:9a:d5:24   ge-0/0/6           spoke1
```

```
ge-0/0/3           -                  5c:5b:35:be:81:06   ETH0               Mist
```

- Should you have PoE running on the switch, you should also check the power consumption of the AP. The PoE mode negotiated depends on the AP model (usually 802.3af on 802.3at) and can be verified in the datasheet. Depending on the configuration state and radio usage, you should see differences in the actual “power consumed” report.

```
root@Switch1> show poe interface
.
.
root@Switch1> show poe interface ge-0/0/3
PoE interface status:
PoE interface                :  ge-0/0/3
Administrative status        : Enabled
Operational status           :   ON
Power limit on the interface : 19.5W (L)
Priority                     : High
Power consumed               : 7.3W
Class of power device        :        4
PoE Mode                     :   802.3at
  (L) LLDP-negotiated value on the port.
```

- The following checks should be done on the WAN router. In our example, we use a remote console session to an SRX Series Firewall acting as WAN router. You should look for the DHCP lease requests from the AP and verify that you see two sessions towards port 443 for TCP/UDP towards the Juniper Mist cloud as shown in the example below.

```
root@spoke1> show dhcp server binding
IP address        Session Id  Hardware address   Expires     State      Interface
10.33.33.12       3           04:5c:6c:6b:13:42  54553       BOUND      ae0.0
10.33.33.15       6           5c:5b:35:be:81:06  48923       BOUND      ae0.0
.
root@spoke1> show arp interface ae0.0
MAC Address       Address         Name                      Interface              Flags
04:5c:6c:6b:13:42 10.33.33.12     10.33.33.12               ae0.0                  permanent
5c:5b:35:be:81:06 10.33.33.15     10.33.33.15               ae0.0                  permanent
Total entries: 2
.
root@spoke1> show security flow session source-prefix 10.33.33.15
Session ID: 34359960425, Policy name: 01_Internet/20, State: Stand-alone, Timeout: 60, Valid
```

```
  In: 10.33.33.15/40267 --> 44.204.233.81/443;udp, Conn Tag: 0x0, If: ae0.0, Pkts: 45026,
Bytes: 8408428,
  Out: 44.204.233.81/443 --> 192.168.173.145/23463;udp, Conn Tag: 0x0, If: ge-0/0/0.0, Pkts:
5524, Bytes: 407857,
.
Session ID: 34359962715, Policy name: 01_Internet/20, State: Stand-alone, Timeout: 1794, Valid
  In: 10.33.33.15/37165 --> 54.144.163.241/443;tcp, Conn Tag: 0x0, If: ae0.0, Pkts: 8997,
Bytes: 4866046,
  Out: 54.144.163.241/443 --> 192.168.173.145/28185;tcp, Conn Tag: 0x0, If: ge-0/0/0.0, Pkts:
5063, Bytes: 421001,
Total sessions: 2
```

When Do We Use Dynamic Port Profiles and When Do We Use a NAC Infrastructure?

Port profiles can be assigned statically or dynamically based on the detected wired client. Both have their advantages and downsides which we do not discuss here. When you choose a dynamic approach, an EX Series Switch managed by Juniper Mist cloud offers the following two options:

- Dynamic VLAN/filter assignment by RADIUS/NAC infrastructure. In this case, you usually configure a static VLAN into a quarantine network that has limited access to the Internet and corporate resources and assign it as default VLAN in the port profile to be used. This is for fall through configuration in case the RADIUS authentication fails and you can't afford all clients not being able to access the network. You then also activate 802.1x authentication for the port or 802.1x authentication and MAB (MAC address-based authentication). When the wired client then logs in to the port, the RADIUS server receives several attributes about the client such as:
  - Authentication parameters like a username or a certificate.
  - Switch name and port.
  - Wired client MAC address.

The backend RADIUS server can include several authorization parameters in the access-accept message, specifying what should be dynamically assigned to the port, such as:

- - A single access VLAN for the client.
  - Several VLANs where one is native, and the others are tagged VLANs. This is also called colorless port assignment in the literature. This is usually used when the attached device is an AP.
  - A filter ID string that can be used to apply the following:

    - An ACL-based filter for local firewalling.
    - A GBP tag to be assigned to a wired client. (Only applicable in IP Clos fabrics. This option is not relevant for this JVD discussing branch designs).

- Dynamic Port Configuration (DPC) by Juniper Mist cloud for colorless ports. As the name indicates, this feature is limited to EX Series Switches which are managed by Juniper Mist cloud and does not work elsewhere. When a user connects a client device to a switch port with this feature enabled, the switch identifies the device and assigns a suitable port profile to the port. Dynamic port profiling utilizes a set of device properties of the client device to automatically associate pre-configured port and network settings to the interface. You can configure a dynamic port profile based on the following parameters:
    - LLDP System Name
    - LLDP Description
    - LLDP Chassis ID
    - Radius Username
    - Radius Filter ID
    - MAC (Ethernet MAC address) also MAC OUI.

> **NOTE**: We recommend using dynamic VLAN/filter assignment by RADIUS/NAC infrastructure whenever possible. Especially when using Juniper Mist Access Assurance as your RADIUS/NAC infrastructure where this becomes an easy to manage task.

Let's review these use cases and how they work:

- Use case 1: RADIUS/NAC Infrastructure present in the network

  Usually – there are two goals with enabling authentication on a port:

    - Making the system zero trust
    - Assign the devices to their relevant network segments.

In networks utilizing a RADIUS infrastructure, we recommend all ports be set to an access port with a dot1x + MAB port profile enabled. We rely on RADIUS transactions to get the network/VLAN assignments as well as assign the ports as access or trunk based on the use case. Clients could be a combination of devices that are capable of dot1x (802.1x EAP-authenticated supplicants) or all device MAC addresses are available in the RADIUS database. Please be sure to configure RADIUS servers with enhanced timers in the switch template. (Enhanced timers reduce the default fallback time from dot1x

to MAB from ~120-180 seconds to ~10-15 seconds, which is highly recommended for a good client experience).

Let's discuss the different use cases for return attributes (AVP) from RADIUS that we recommend being sent as part of the access-accept message:

- Clients that need to be assigned to a specific VLAN while the port remains an access port. Here, you use the AVP=Tunnel-Private-Group-ID. See the example configuration below:

```
001094001123 Cleartext-Password := "001094001123"
    Tunnel-Type = VLAN,
    Tunnel-Medium-Type = IEEE-802,
    Tunnel-Private-Group-ID = "VLAN1099",
```

- Clients that need to be assigned to multiple VLANs and need to be moved to a trunk port. Here, you use the AVP=Egress-VLAN-ID or Egress-VLAN-Name. See the example configuration below:

```
# 4Byte tagged VLAN =   0x31+<000000padding>-<VLAN-ID in Hex>
# 4Byte untagged VLAN = 0x32+<000000padding>-<VLAN-ID in Hex>
001094001177 Cleartext-Password := "001094001177"
    Tunnel-Type = VLAN,
    Tunnel-Medium-Type = IEEE-802,
    Egress-VLANID += 0x32000001,
    Egress-VLANID += 0x31000440,
.
# first char of string 1 = Tagged , 2 = native/untagged
001094001144 Cleartext-Password := "001094001144"
    Tunnel-Type = VLAN,
    Tunnel-Medium-Type = IEEE-802,
    Egress-VLAN-Name += "2default",
    Egress-VLAN-Name += "1VLAN1088",
```

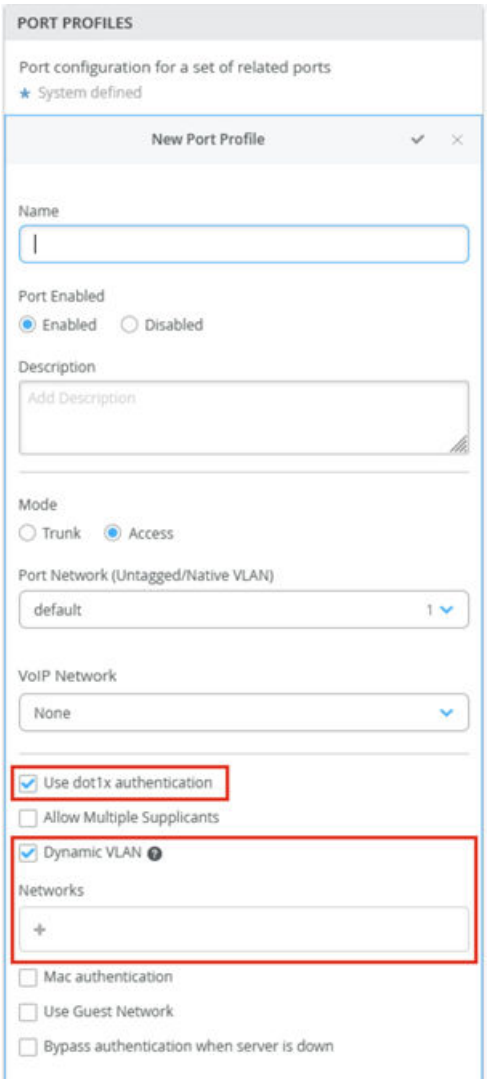
- Clients that need to be assigned to a policy as firewall-filter/ACL (In addition to either of the above two AVPs). Here, you use the AVP=Filter-Id.

```
001094001142 Cleartext-Password := "001094001142"
    Tunnel-Type = VLAN,
    Tunnel-Medium-Type = IEEE-802,
    Tunnel-Private-Group-ID = "1099",
    Filter-Id = "filter1"
```

Keep in mind that before you can use a particular filter ID, you must create a filter on the switch itself. Here is an example using additional CLI:

```
set firewall family ethernet-switching filter filter1 term supplicant1 from source-mac-
address 00:10:94:00:11:42
set firewall family ethernet-switching filter filter1 term supplicant2 from source-mac-
address 00:10:94:00:11:66
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1k
set firewall policer p1 then discard
set firewall family ethernet-switching filter filter1 term supplicant1 then cosunt counter1
set firewall family ethernet-switching filter filter1 term supplicant1 then policer p1
set firewall family ethernet-switching filter filter1 term supplicant2 then count counter2
```

- Another way is to assign the Dynamic VLAN based on a port profile but still requiring the authentication through RADIUS at least to be performed for the wired client. Hence, the RADIUS server in this case is not required to send back any of the above-mentioned RADIUS AVPs as part of the final access-accept message. Only the access-accept message is required and the VLAN configuration will be derived from the port profile. The figure below shows where this optional configuration can be made.



NOTE: We do not recommend adding DPC in any of the above scenarios, hence do not turn on DPC on any of the ports in this scenario as well. This is the most preferred scenario in case you have a RADIUS/NAC infrastructure.

- Use case 2: Usage of RADIUS/NAC infrastructure but augmenting some devices with DPC for the reasons mentioned below:

  All of the above AVPs listed in use case 1 still hold true. Juniper DPC, however, extends functionality by using LLDP information and MAC OUI (the vendor portion of a MAC address) as identifiers for port configuration. This level of identification is typically not available when relying solely on a traditional RADIUS or NAC-based management system.

  Motivation for this approach:

- - Avoid adding a lot of MACs (APs and cameras are usually volume devices) to the RADIUS user database and use LLDP and MAC OUI instead.
  - Reduce the cost of RADIUS/NAC infrastructure, since it involves client count.

Juniper recommends enabling an additional layer of security, such as 802.1X or MAB, when using VLAN assignment through DPC on certain ports. The remaining ports should continue to use 802.1X or MAB for authentication, but without incorporating DPC.

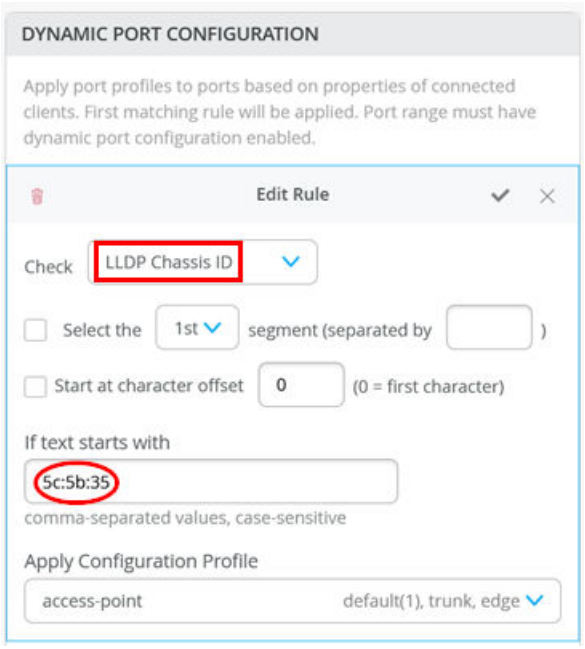
In case you cannot predict where selected devices will be plugged in to the network, all ports need to enabled for DPC and 802.1x or MAB which is the less recommended approach.

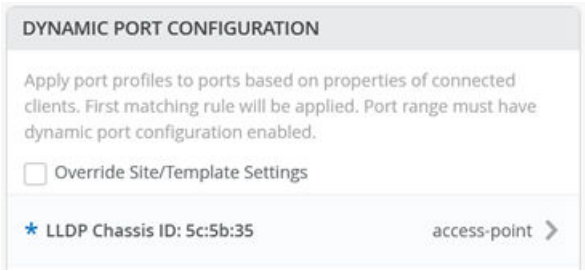
NOTE: For both use case 1 and use case 2, when 802.1x and MAB are enabled on all ports, it is critical to note that no MAC addresses will be learned until the authentication is successful. Hence, DPC using MAC-based rules will not work and should not be configured. We only recommend using DPC with LLDP-based rules when ports are enabled for 802.1x and MAB.

- Use case 3: No RADIUS/NAC infrastructure, DPC + static assignment of port profiles.
  - In the absence of a RADIUS/NAC Infrastructure, DPC could be used either with LLDP or MAC-based rules to provision ports. The preferred approach is if one is aware of the ports that are allocated for DPC eligible devices, one should enable DPC only on those ports. The rest of the ports are to be statically assigned.
  - The less preferred approach is if one is not aware of the ports where DPC eligible devices will be plugged in, enable DPC on all ports.
  - We also recommend the default profile where the DPC is enabled, to be pointing to a dummy (or at least a quarantine) VLAN, so no devices get IPs when they are plugged and do not match any DPC rules.

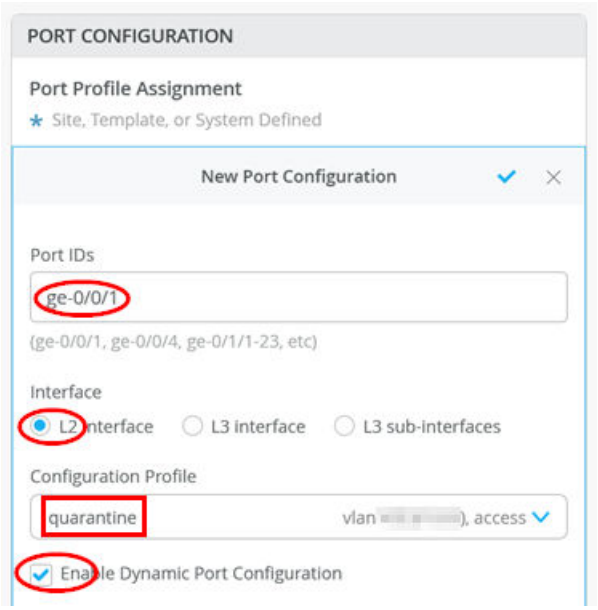
NOTE: Avoid using DPC if the port experiences a large number of port flaps. Each port flap will trigger a configuration change on the switch (Junos OS commit). In such a case, it is better to apply dynamic VLAN configuration through RADIUS.

The figure below illustrates an example where DPC identifies a Juniper AP using the vendor MAC OUI part of the LLDP chassis ID.





Do not forget that you must activate DPC for the port by using the checkbox as indicated by the image below:



NOTE: It takes a couple of minutes for a port profile to be applied to a port after a client is recognized, and a couple of minutes after that for the port profile assignment status to appear on the portal. In case of switch reboots or a mass link up or down event affecting all ports on a switch, it takes approximately 20 minutes for all the ports to be assigned to the right profile (assuming that DPC is enabled on all ports).

When the Switch Utilizes CloudX Towards Juniper Mist Cloud

The following changes to the operation of DPC need to be kept in mind when the Switch uses CloudX for communication towards the Juniper Mist cloud.

- CloudX leverages an ephemeral database in Junos for DPC and the port bounce feature instead of the conventional static configuration database that is usually used.
- Any interfaces enabled with DPC are moved to an ephemeral database from the static configuration database. This includes any Spanning Tree Protocol (STP) configuration as well.
- Ephemeral database commits are faster. The commits take 1-2 seconds even on a large VC compared to the static configuration database.
- When looking at the static configuration database, you will not see the changes made in the ephemeral database. So, do not get confused thinking your DPC configuration was not applied. To review the configuration in the ephemeral database, run the following Junos OS CLI commands through a console or remote shell session as shown below

  ```
  show ephemeral-configuration instance mist-dpc
  ```

```
{master:0}
mist@ld-cup-idf-bbb> show ephemeral-configuration instance mist-dpc
## Last changed: 2025-04-10 19:53:28 UTC
interfaces {
    mge-0/0/2 {
        native-vlan-id 1;
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members all;
                }
            }
        }
    }
    mge-0/0/3 {
        unit 0 {
            family ethernet-switching {
                vlan {
                    members default;
                }
            }
        }
    }
    mge-0/0/4 {
        native-vlan-id 1;
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members all;
                }
```

NOTE: Using a combination of DPC and 802.1X configuration through additional Junos OS CLI commands is not supported. When CloudX is enabled, DPC relies on the ephemeral database, and mixing it with static configuration from additional CLI results in inconsistencies between the static settings and the interface configurations stored in the ephemeral database.

Configure DHCP Snooping for Switches

DHCP snooping enables a switch to examine all the DHCP traffic initiated from the untrusted ports on the network. When DHCP snooping is enabled on a VLAN, the system examines DHCP messages sent from untrusted hosts associated with the VLAN and extracts their IP addresses and lease information. This information is used to build and maintain the DHCP snooping database. Only hosts that can be verified using this database are allowed access to the network. More detailed information about this security feature and how it operates can be found here https://www.juniper.net/documentation/us/en/software/junos/security-services/topics/concept/port-security-dhcp-snooping-els.html.

NOTE: By default, access ports are treated as untrusted ports and trunk ports are treated as trusted ports.

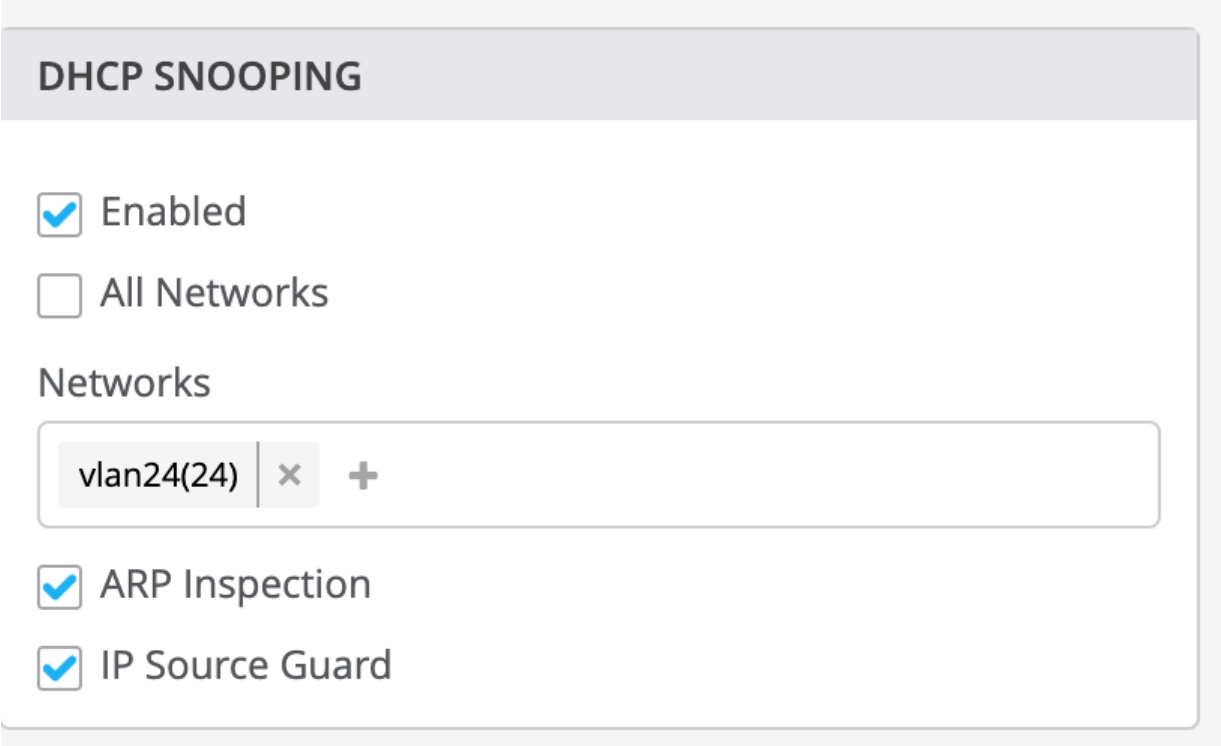
There are three places where you can configure the DHCP Snooping/ARP Inspection/IP Source Guard in the portal:

- **Switch Device Details** page.
- **Site > Switch Configuration** page
- **Organization > Switch Templates**.

Configuration is applied in the following order of priority: first from the **Switch Device Details** page, followed by the **Site > Switch Configuration** page, and finally from the **Organization > Switch Templates**, which has the lowest priority.

Below is an example where you can enable the above configuration for a single network. There are two options you can enable for all networks / single network as per your requirement.

In the example below, we are enabling DHCP snooping for a single network > Vlan24 (vlan-id-24).



The VLAN must exist on the switch for the configuration to take effect. For this reason, the port needs to be associated with a port profile. In an access port profile, you can specify whether the port is trusted

or untrusted; if this setting is not defined, it defaults to the standard behavior (untrusted). The port network can be configured as either a standard data network or a VoIP network. By default, trunk ports are always considered trusted.

In the example below, we make the access port trusted:

PORT PROFILES

Port configuration for a set of related ports

* System defined

Edit Port Profile

Name

vlan24_template

Port Enabled

(•) Enabled ( ) Disabled

Mode

( ) Trunk (•) Access

Port Network (Untagged/Native VLAN)

vlan24 24

VoIP Network

None

(•) Trusted Port ( ) Untrusted Port ( ) Default

[ ] Use dot1x authentication

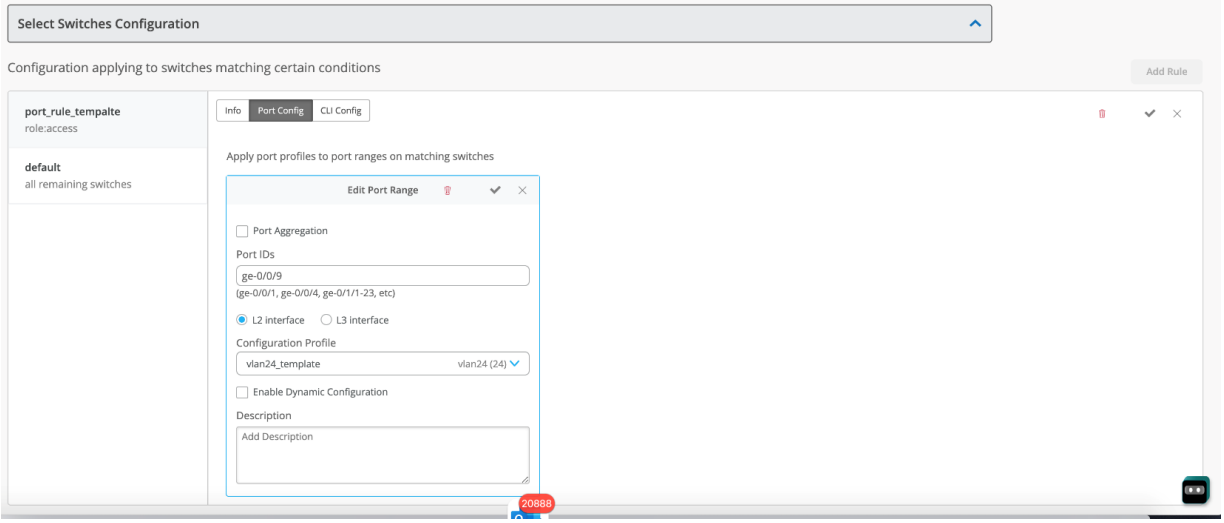
Speed

Auto

Duplex

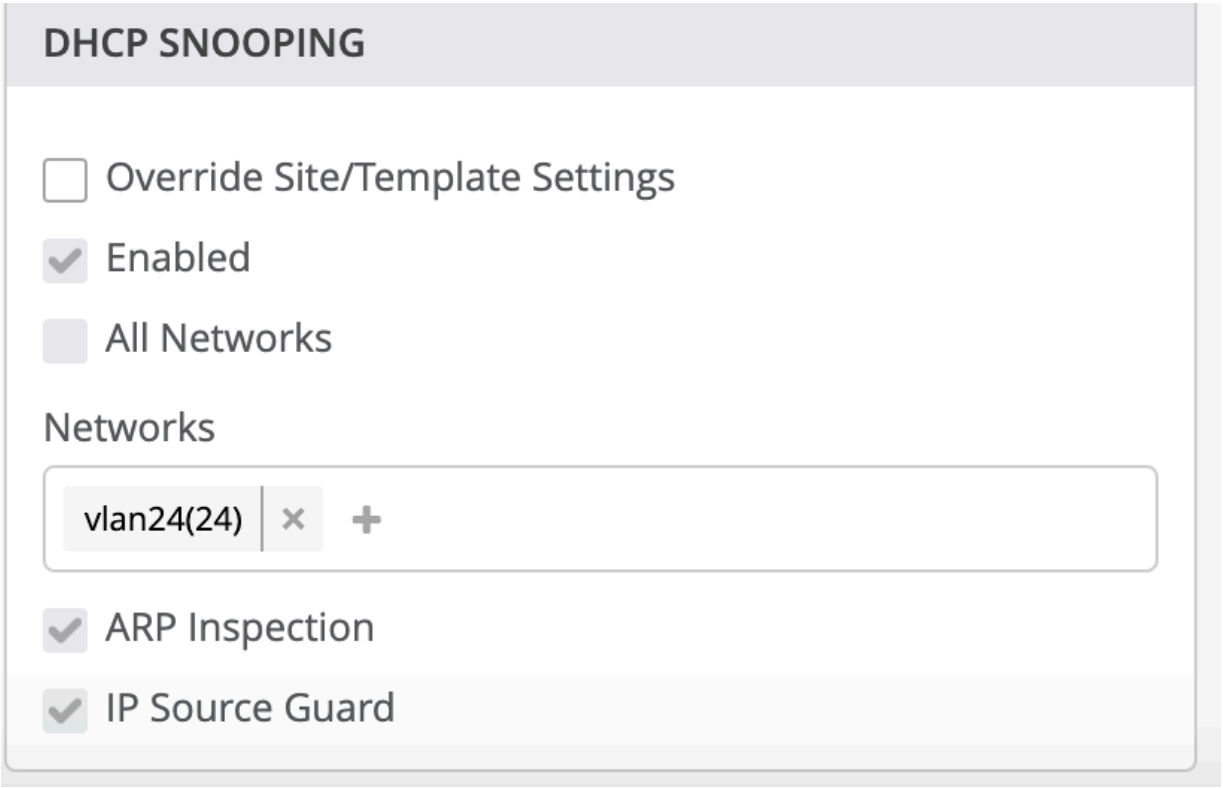
Auto

The port profile to the port would be as below:



We have the option for the override site/template settings for DHCP snooping from the site settings and device settings:

Site settings:



We have the options for overriding the trusted/untrusted/default options for port profile from the site settings and device settings.

Site settings:

PORT PROFILES

Port configuration for a set of related ports

* Template or System defined

Edit Port Profile

Override Template or System defined profile

Name

vlan24_template

Port Enabled

Enabled Disabled

Mode

Trunk Access

Port Network (Untagged/Native VLAN)

vlan24 24

VoIP Network

None

Trusted Port Untrusted Port Default

Use dot1x authentication

Speed

Auto

Device settings:

PORT PROFILES

Port configuration for a set of related ports

* Site, Template, or System Defined

Edit Port Profile

Override Site, Template, or System Defined profile

Name

vlan24_template

Port Enabled

Enabled Disabled

Mode

Trunk Access

Port Network (Untagged/Native VLAN)

vlan24 24

VoIP Network

None

Trusted Port Untrusted Port Default

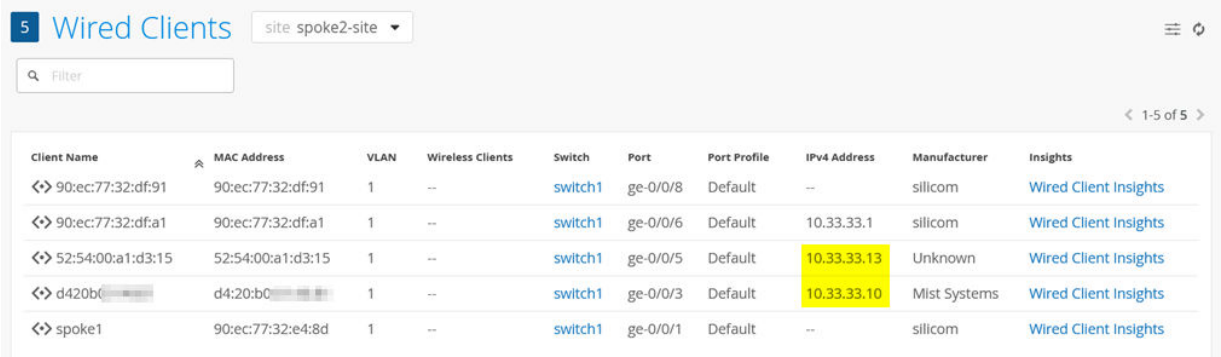
Use dot1x authentication

Speed

Auto

Duplex

Enabling DHCP snooping will allow the Juniper Mist cloud to show IP Address information when reviewing the clients table. Unlike a campus fabric deployment, the switch has no VRF configuration and is a pure Layer 2 forwarder. Hence, the switch is usually not enabled for ARP resolution as a default gateway and would not be able to gather such information automatically and report it to the Juniper Mist cloud.



Command to configure DHCP snooping:

```
set vlans default forwarding-options dhcp-security
```

Command to check the DHCP snooping table locally on the switch like in the example below:

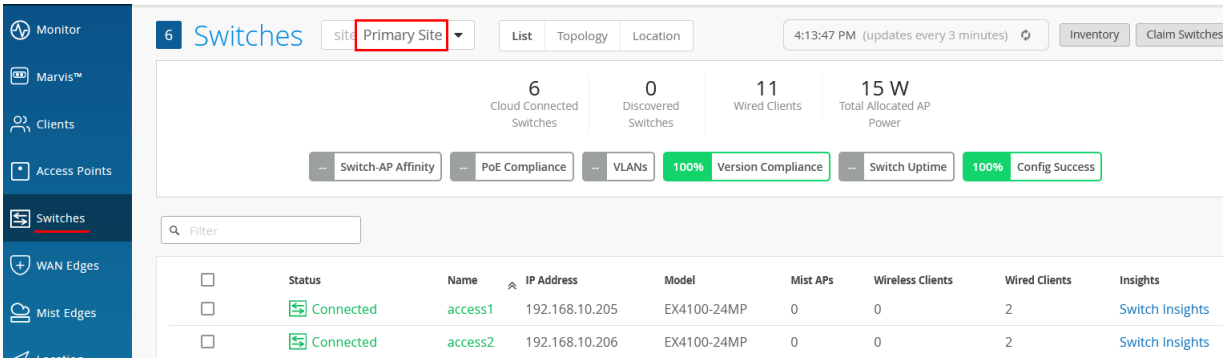
```
                show dhcp-security binding
IP address        MAC address         Vlan     Expires State    Interface
10.33.33.10       d4:20:b0:xx:yy:zz   default  0       REQUESTING ge-0/0/3.0
10.33.33.13       52:54:00:a1:d3:15   default  0       BOUND    ge-0/0/5.0
```

Appendix: Day-2 Operate

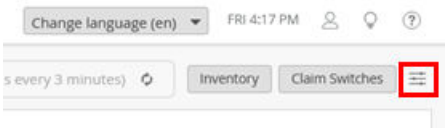
IN THIS SECTION

Switch Information Page

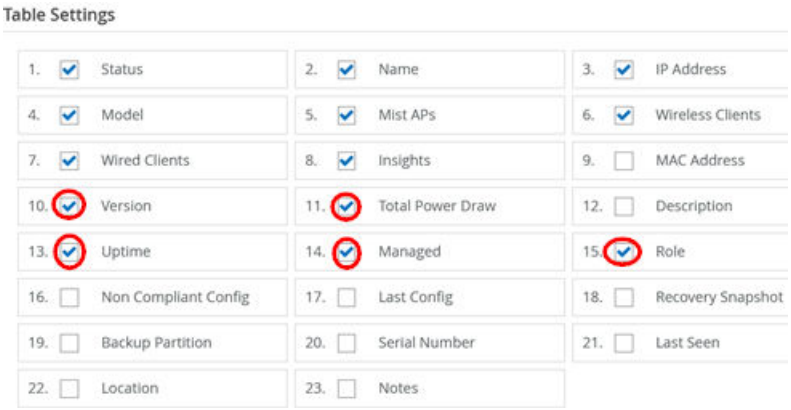
To get to the basic switch monitoring page, click **Switches**, select a site, and then click on the device itself similar to what is shown below:



Not obvious but very useful is this hamburger-button at the right side which allows you to modify what is displayed on this page:



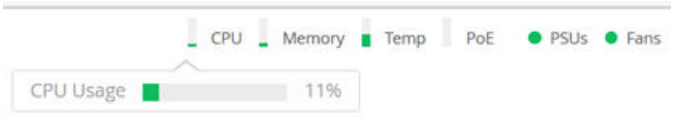
A typical example of adding displayed items is shown below:



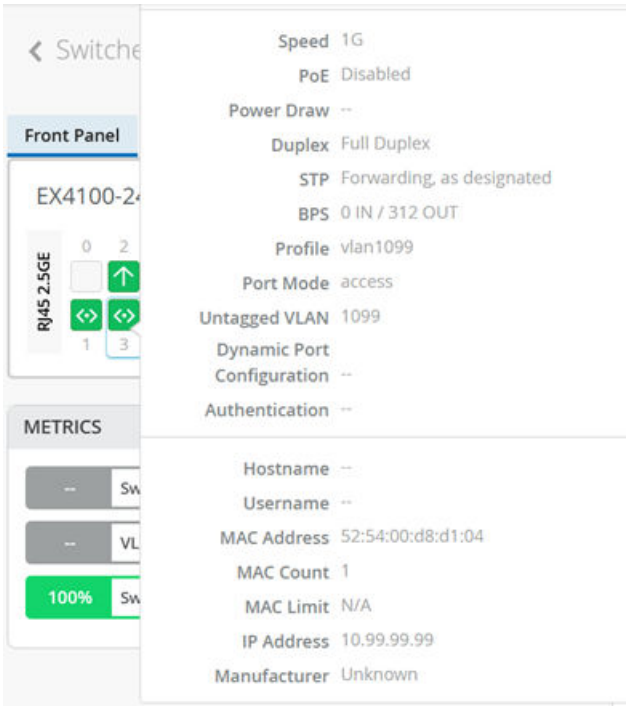
Resulting in this new view:

Going further, click on the switch name you want to inspect (here, we select "access1"). At the top of the device information page, you see a graphical front view of the device, its ports and some baseline status information.

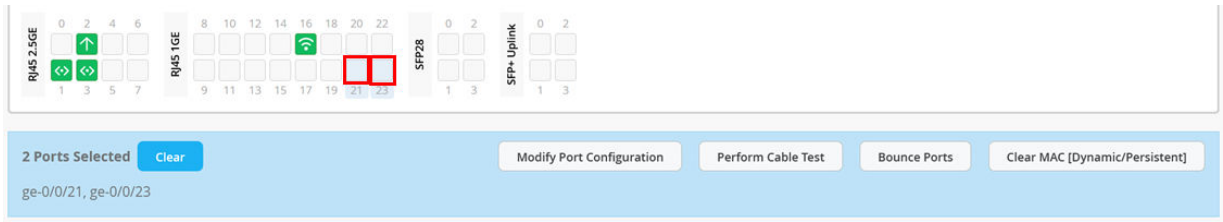
Hover your mouse over each status icon for **CPU**, **Memory**, **Temperature**, **PoE**, **PSUs** and **Fans** to see the current status for each category.



Next, hover your mouse over some of the ports of the device to review what is configured and detected there. In our example, you also see at the bottom that our lab switch has a wired client (a test VM) that is attached to the port.

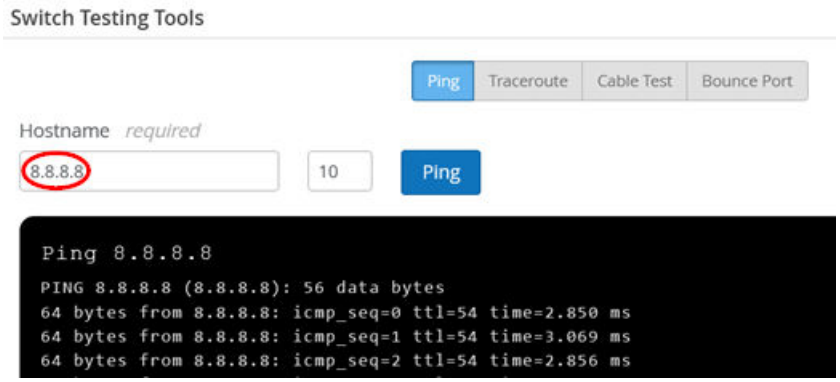


Clicking on one or more ports gives you access to the commands shown below:

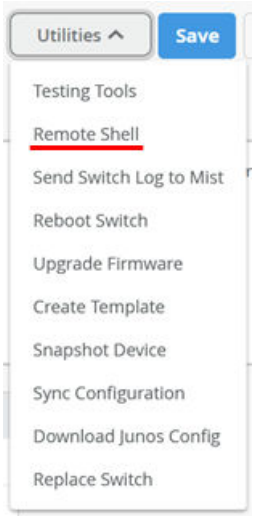


Then, select the **Utilities** tab available for the device and click on **Testing Tools** to see what tests are available to run.

The testing tools allow you to issue ICMP pings, traceroutes and to bounce a port, for example:



Besides the testing tools, one of the most useful utilities is the ability to open a direct SSH shell to the device just by clicking a button.

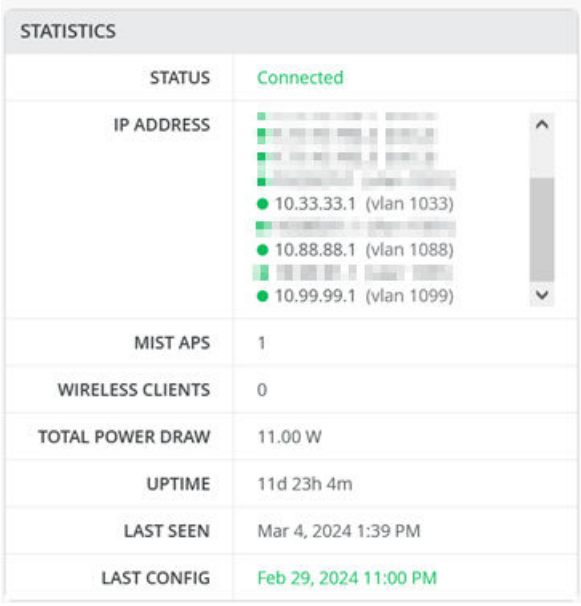


This will open a new window with the ability to run CLI commands on the device remotely.

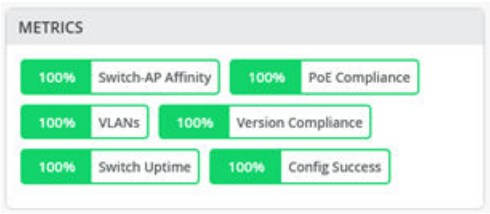
A new option is **Sync Configuration** which will immediately push a synced configuration to the device based on what is configured on the Juniper Mist portal (and reviewable using the **Download Junos Config** option). Consider this option when:

- You made use of the additional CLI commands option and want to revoke previously made configurations without “delete” commands.
- Somebody made a local change on the device without proper configuration through the Juniper Mist portal and you want to remove these changes.
- There was a prior configuration push that failed, and you want to try again.

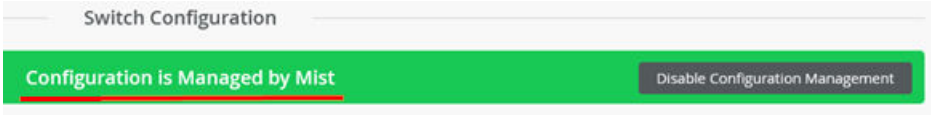
Back on the device information page, review the **Statistics** pane for information.



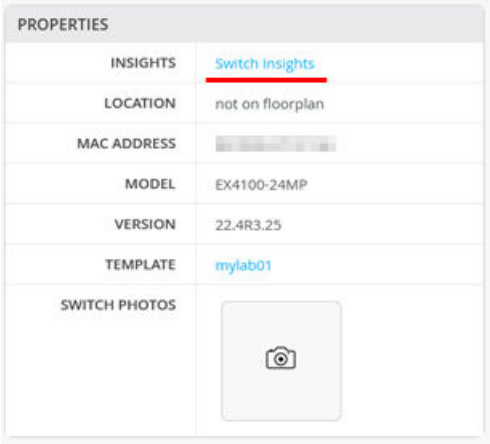
Also review the **Metrics** pane to confirm all is well.



Then, review the configuration for the device. Usually, it should be inherited by the templates or profiles you used. However, if you need to, you can make individual changes to the configuration to be pushed to the device. Ensure that your switch is managed by Mist now:

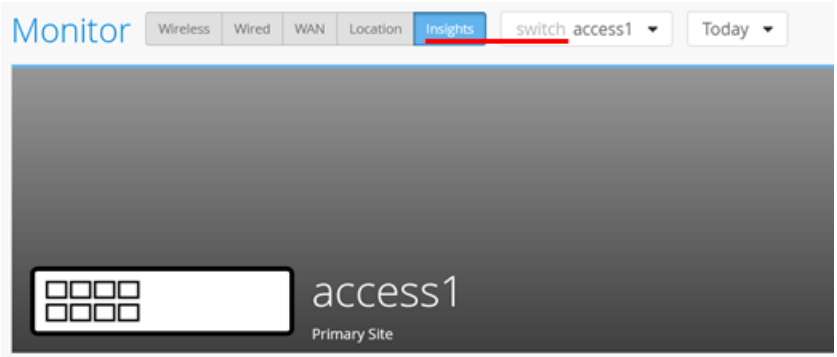


Finally, review the **Properties** pane for information and then click on **Switch Insights** for the next level of information about this device:

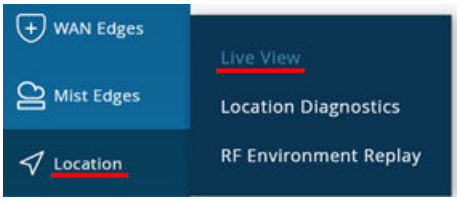


Switch Insights Page

At the top of the **Switch Insights** page, you should see your switch.

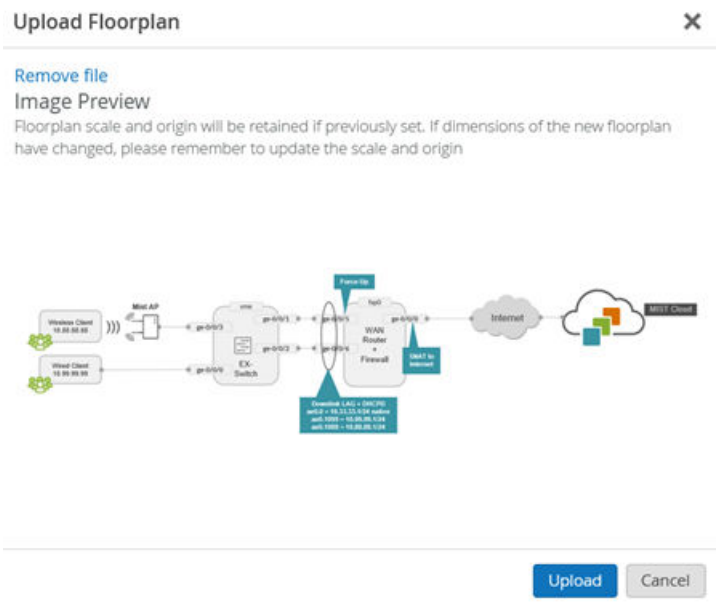


In our example, you do not see the location of the access switch, hence the dark background. Optionally, you can add this information using a location configuration as shown below. Go to **Location > Live View**:

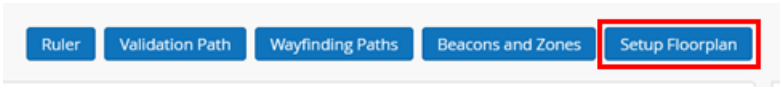


Add a new floorplan:

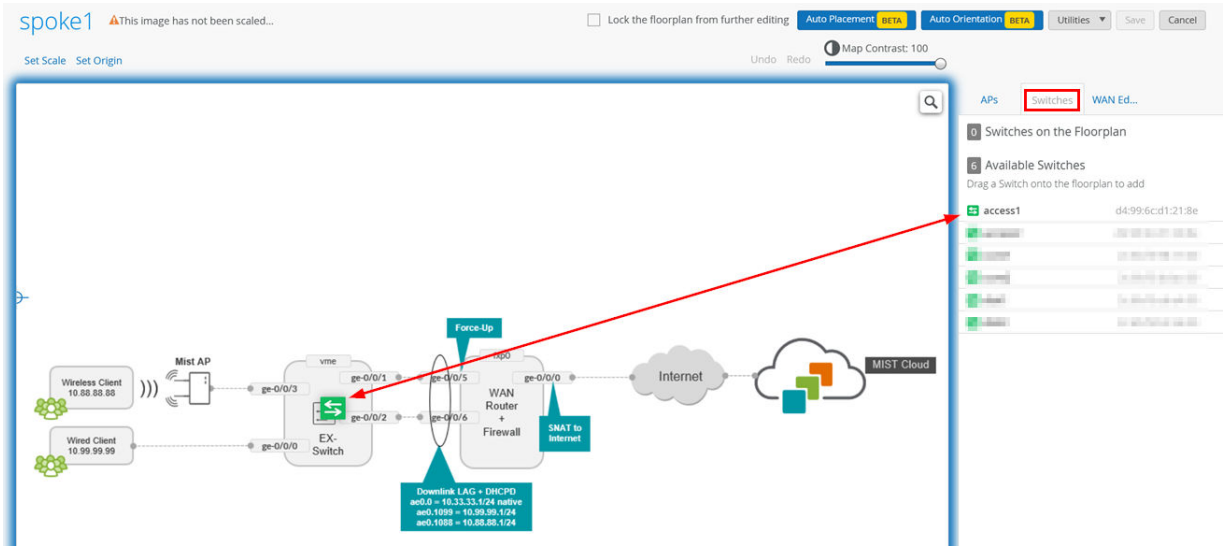
Upload the picture of your topology:



Click on **Setup Floorplan**:

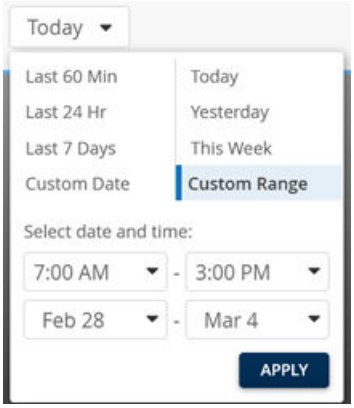


Select **Switches** and drag the switch itself to the position on the topology/floorplan:

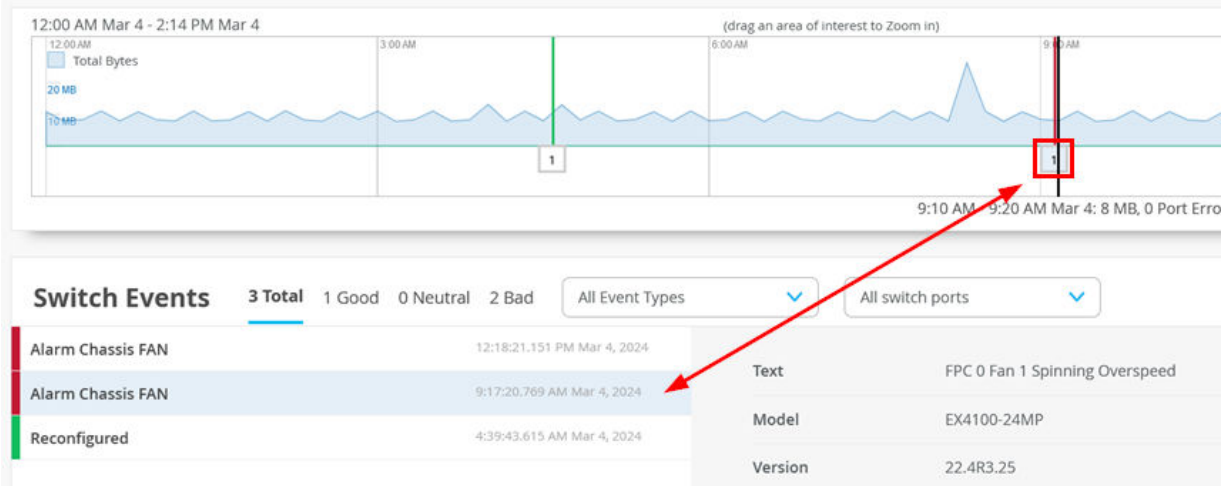


Click **Save** and return to the **Switch Insights** page to see the topology:

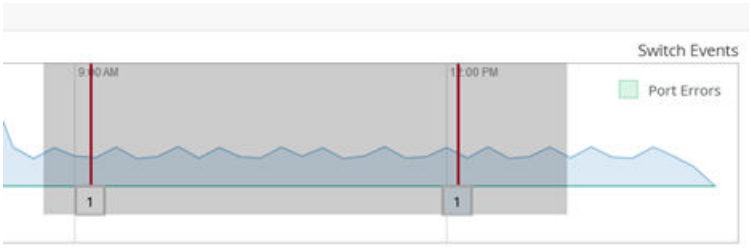
On the **Switch Insights** page, at the top of the page, you can see the time range for the information you want to see (the default is “Today”). Below, you can see how you can modify that range:



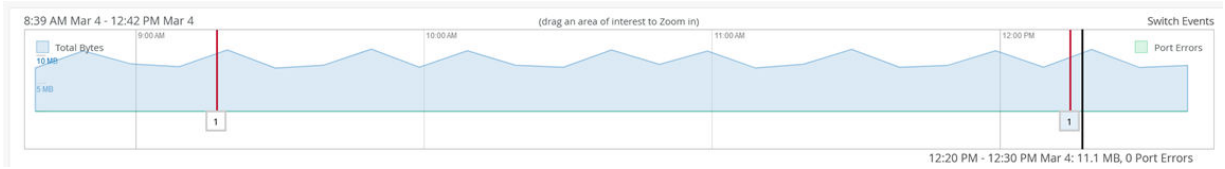
Below the device, you can see events over time (and the traffic through the device at that time). With your mouse cursor, you can select an event to review which will then automatically be selected in the events reports below:



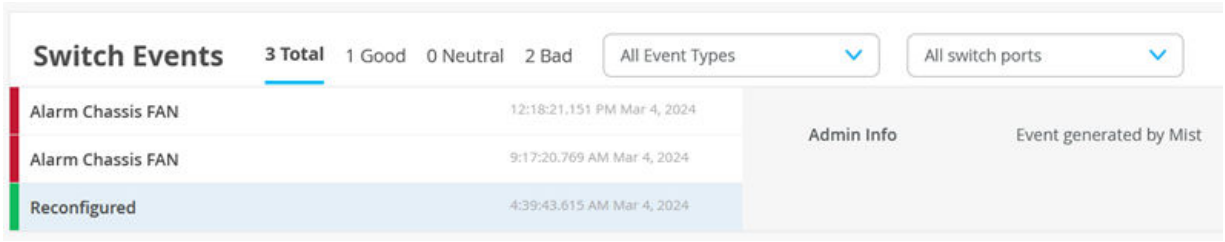
You can also zoom in by left-clicking with the mouse and dragging to select an area in the timeline (make sure it's not too short).



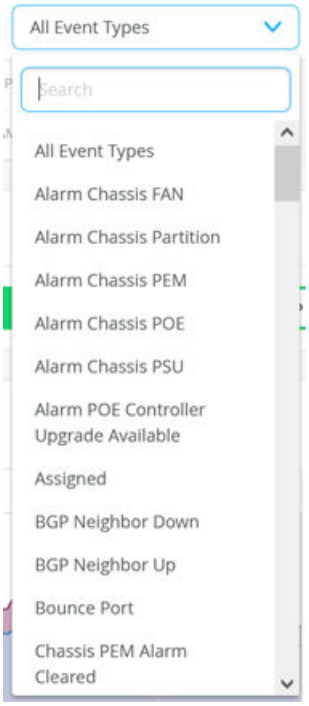
To then get to a more detailed view of the time range, selected before:



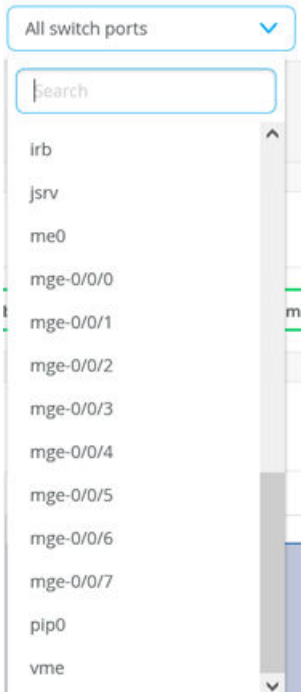
Then, review the **Switch Events** pane:



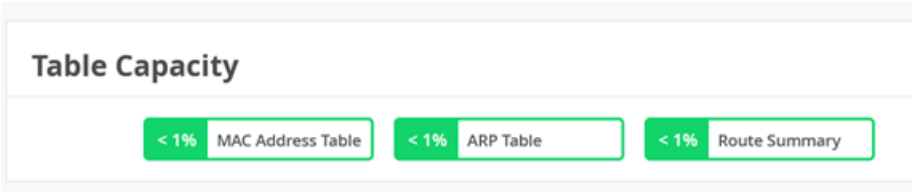
You can limit the events displayed by selecting specific events as shown below:



You can limit the events displayed by selecting specific ports as shown below:

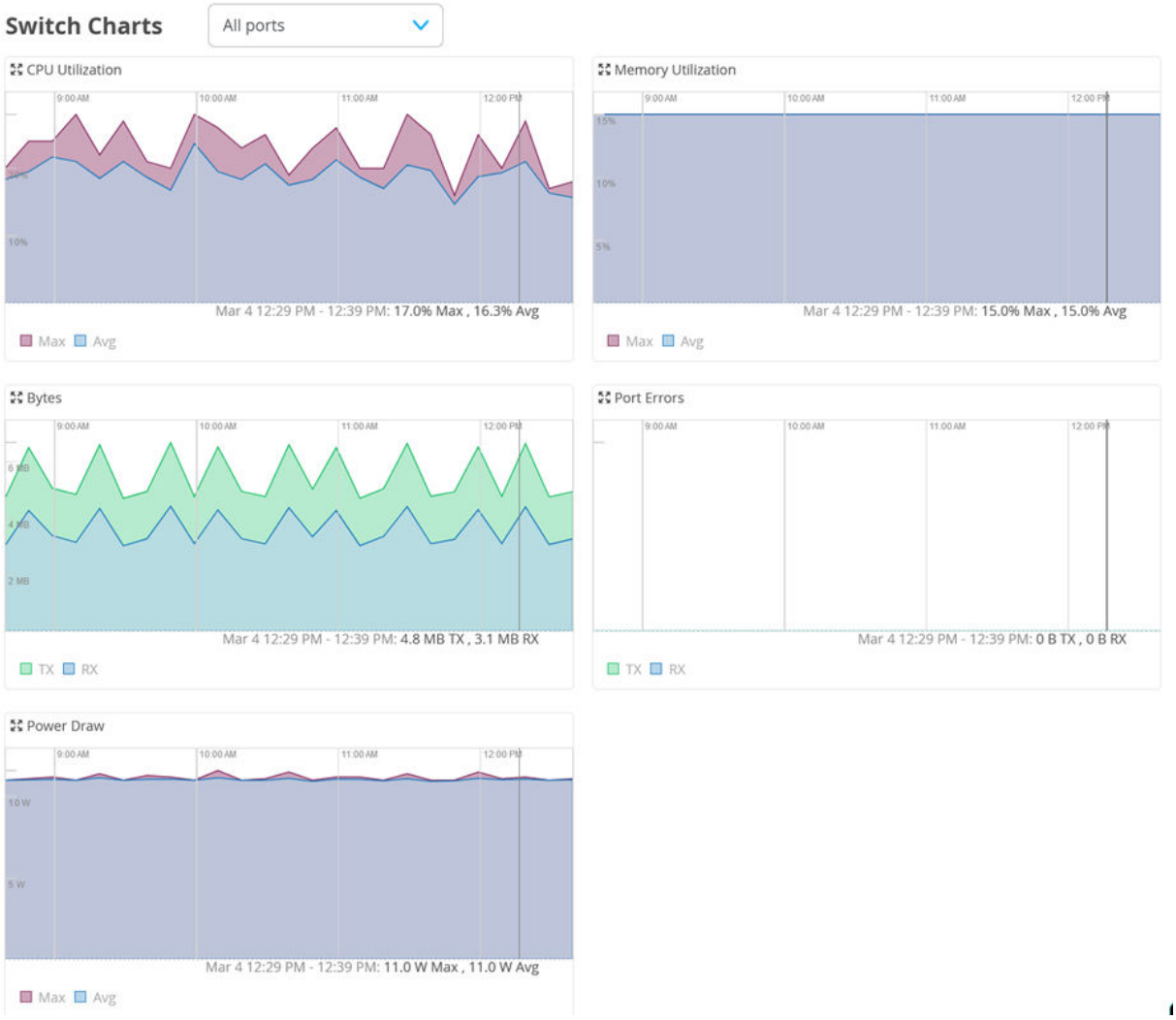


Another item you can review is **Table Capacity** like the example shown below:

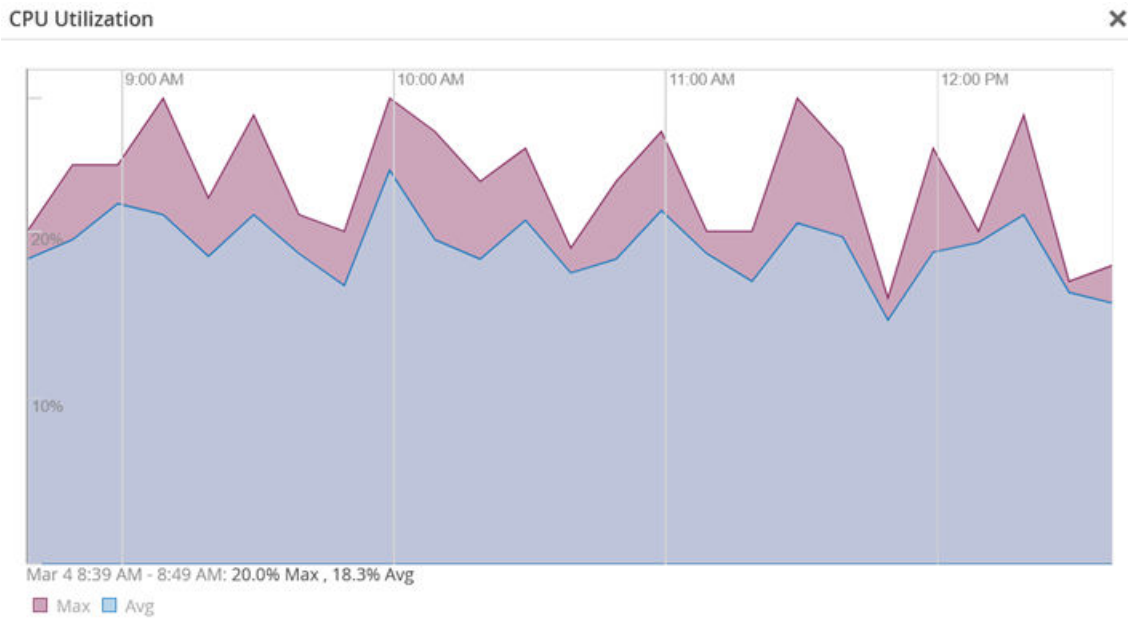


Next, is the **Switch Charts** pane with the following five charts:

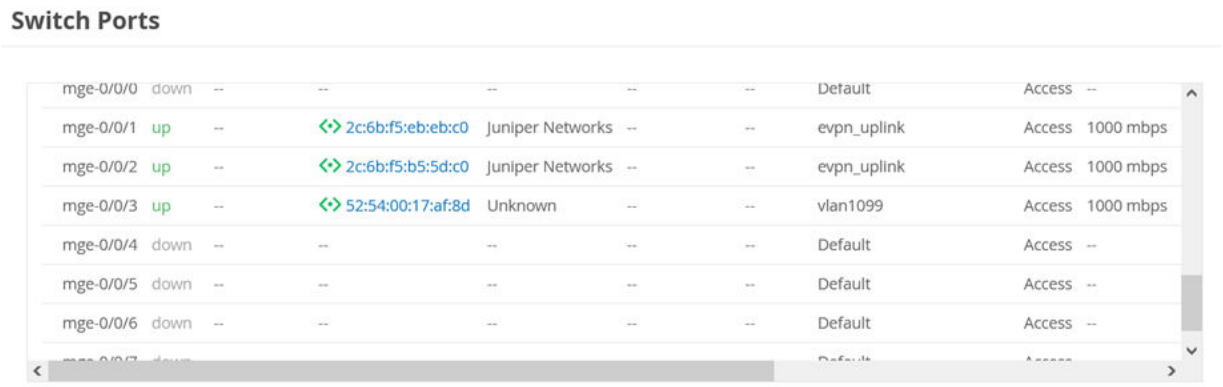
- CPU Utilization
- Memory Utilization
- RX+TX Bytes
- Port Errors
- Power Draw



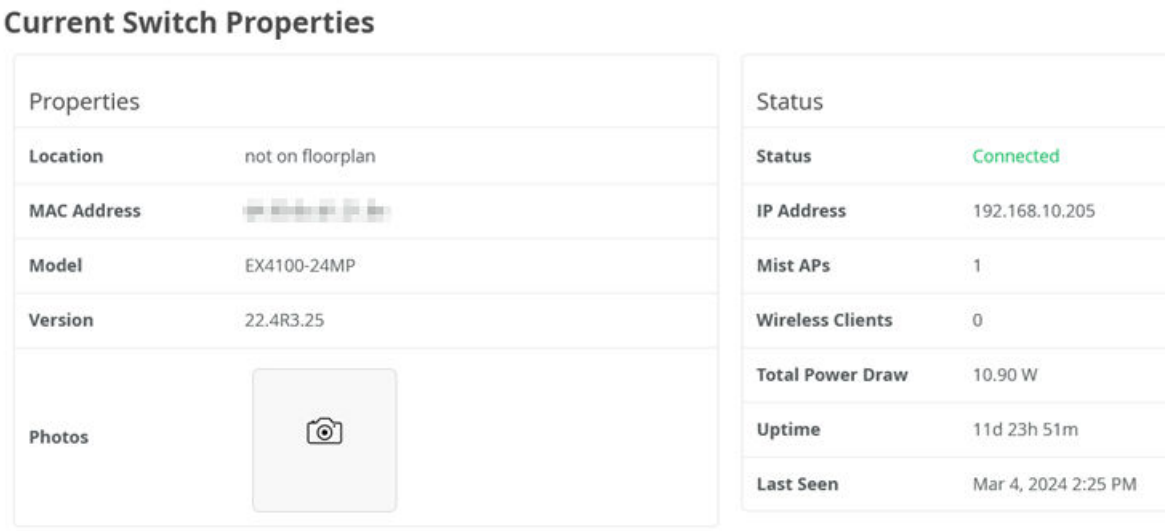
You can expand the chart by clicking on the symbol marked below:



You can then review the switch ports again to figure out what is attached to each:

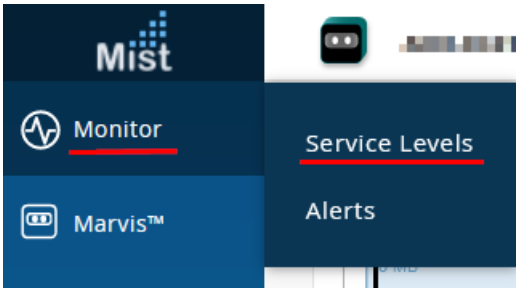


Then, the last pane on this page is **Current Switch Properties**:

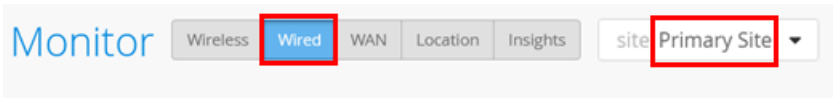


Wired SLE Monitor Page

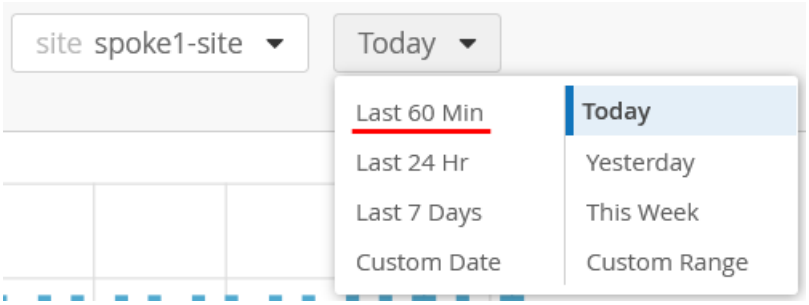
The next level of information involves Switch SLE monitoring. To review those, click **Monitor > Service Levels**.



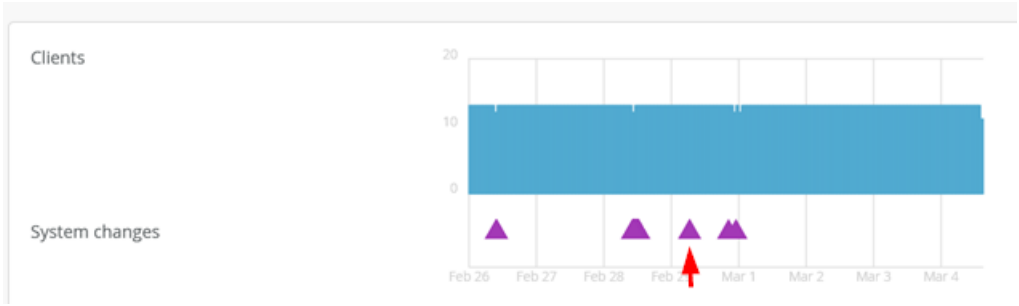
Then, select a site for inspection and select **Wired**.



Be aware that all Wired SLE metrics are about monitoring a device for a longer period of time. They may not display much after you've just onboarded a device as not much data has been collected yet. In a production environment, expect to need to collect a full week of data from the device. You can try to change the period to "Last 60 min", but it may not present much information.



The first pane gives you a relationship between the number of connected clients within that time range and the system events that occurred. A purple triangle denotes when something changed. Also, familiarize yourself with the ability to see what is reported in the lower-right corner of the pane.



Currently, there are three Wired SLE measurements displayed with different classifiers together for each SLE:

- Throughput SLE
- Successful Connect SLE
- Switch Health SLE
- Switch Bandwidth

NOTE: It is critical to understand that the metrics and reports for each SLE are based on Mist AI utilizing a tensor flow network. This means:

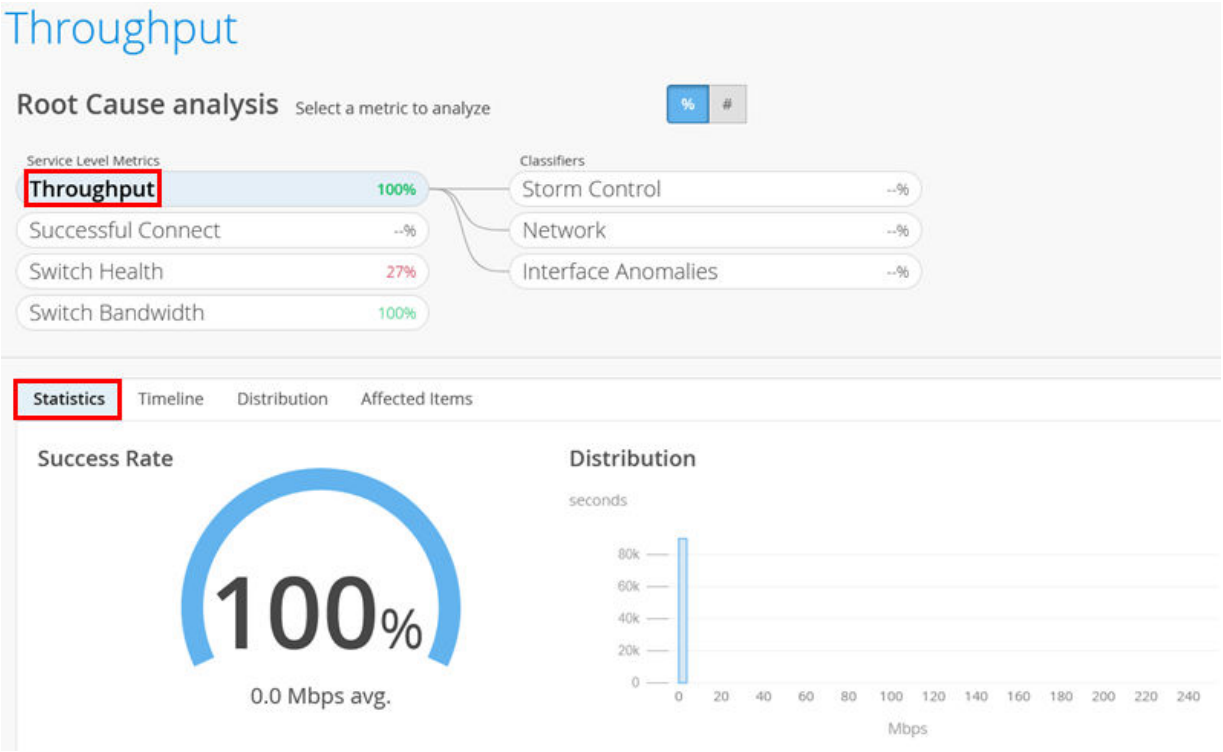
1. As with all AIs, Mist AI requires large amounts of data about your network to provide useful analysis. We recommend waiting a week after the switch has been installed and traffic has been running though it before inspecting this information.

2. Unlike traditional monitoring tools that simply display charts and leave interpretation to the user, Juniper Mist uses AI to assess the overall health of the network and highlights only items that may be at risk. Therefore, if no reports are shown, it indicates that everything is functioning normally and no further review is needed.

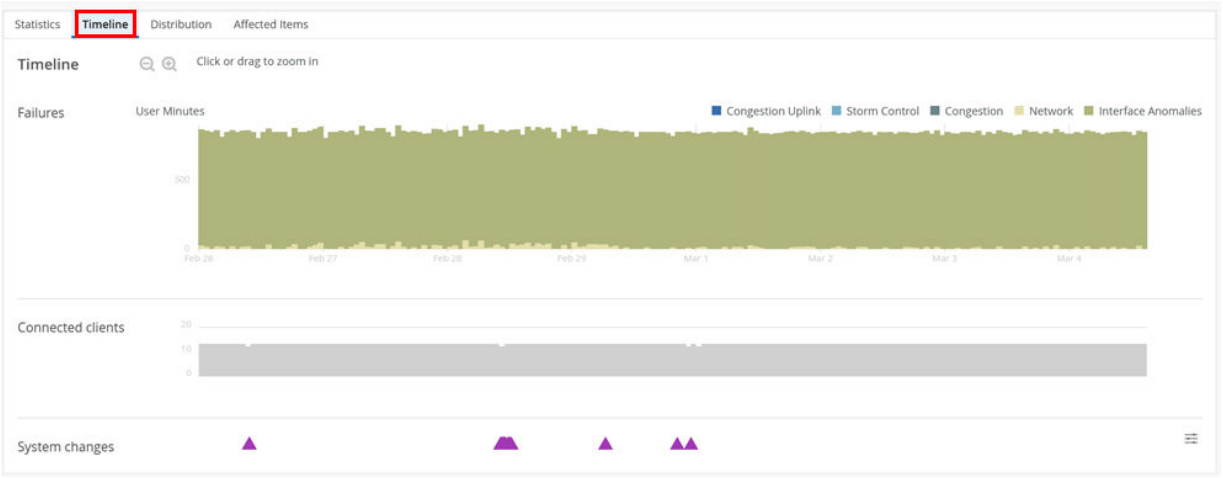
Let's focus on the reports you can get through each SLE now. The SLE for throughput with accompanying classifiers:

- Storm Control
- Network with sub-classifiers:
  - Latency
  - Jitter
- Interface Anomalies with sub-classifiers:
  - Cable Issues
  - MTU Mismatch
  - Negotiation Failed

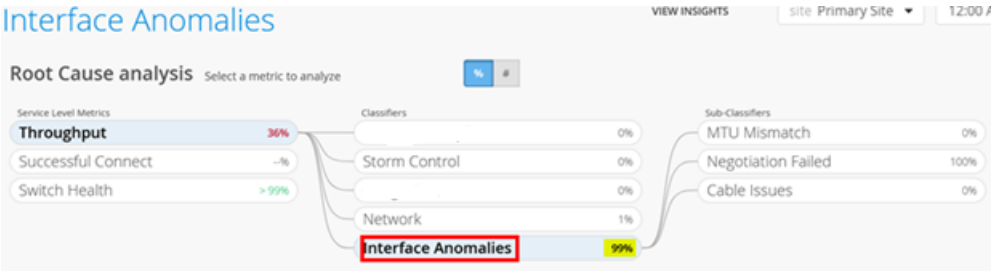
It is best practice to start inspecting the SLE through the **Statistics** tab first:



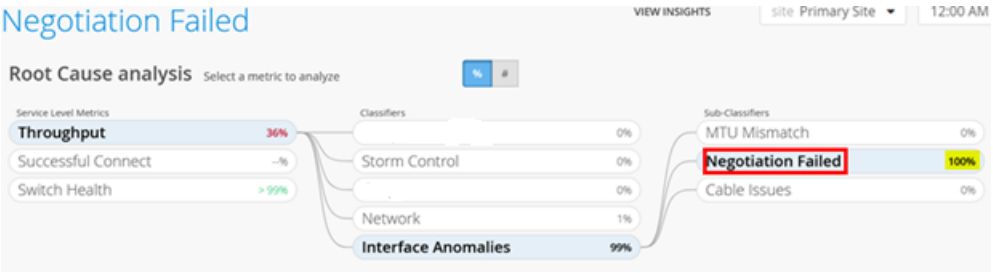
You may select the next tab named **Timeline**, if needed.



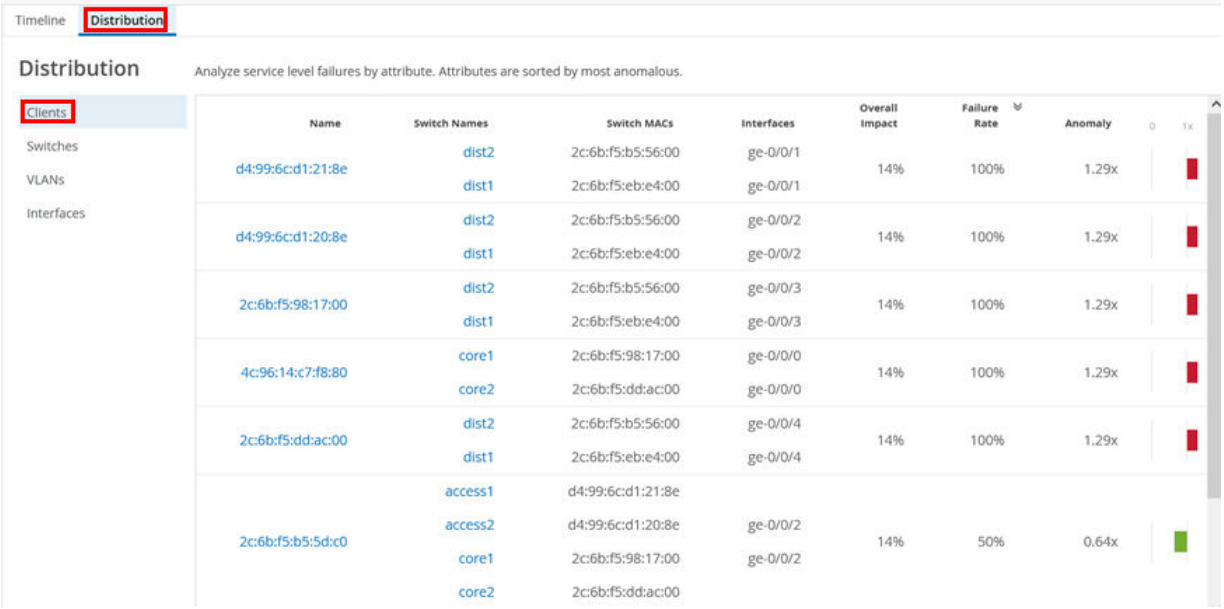
Then, you should review the next classifier, drilling deeper into the issue. In the example below, we select the classifier having the most impact:



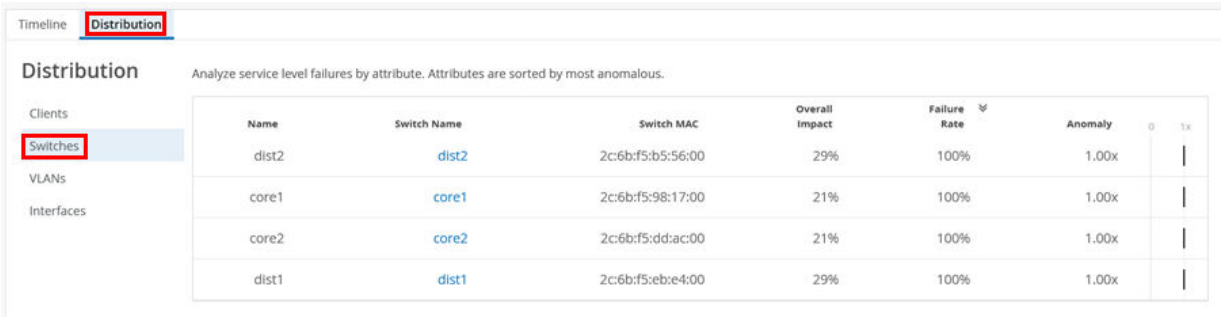
As this SLE classifier has sub-classifiers, we then select the sub-classifier with the most impact:

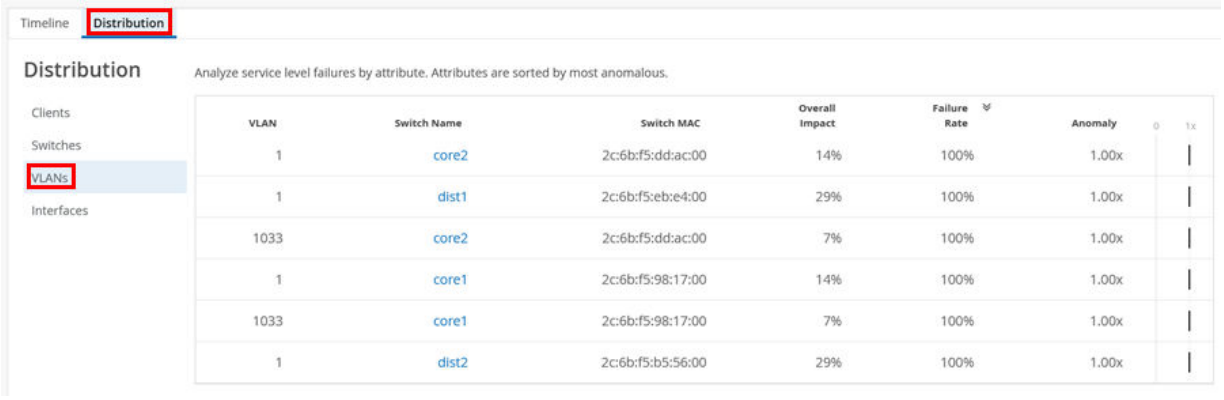


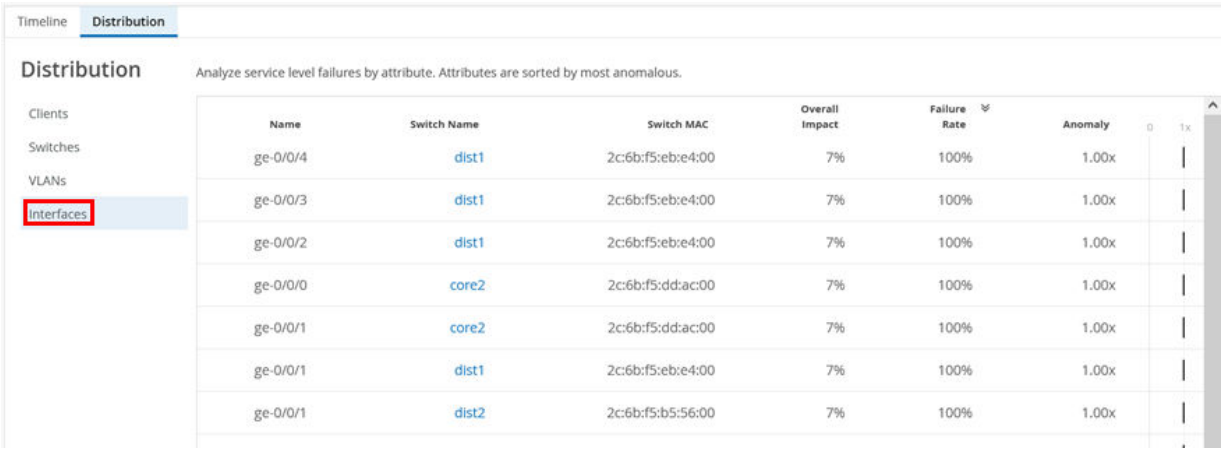
In this example, it's best to inspect the **Distribution** tab next. Here, we start with **Clients**:



Below, we review the affected switches, for example:

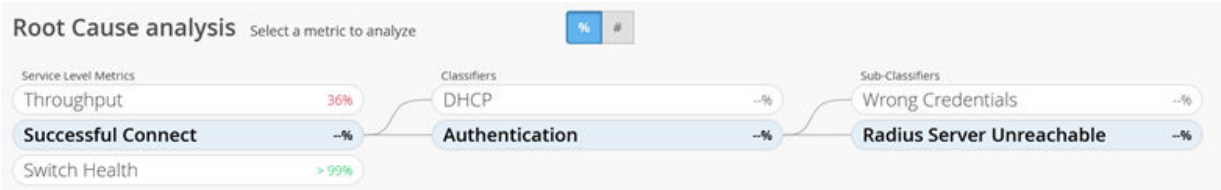






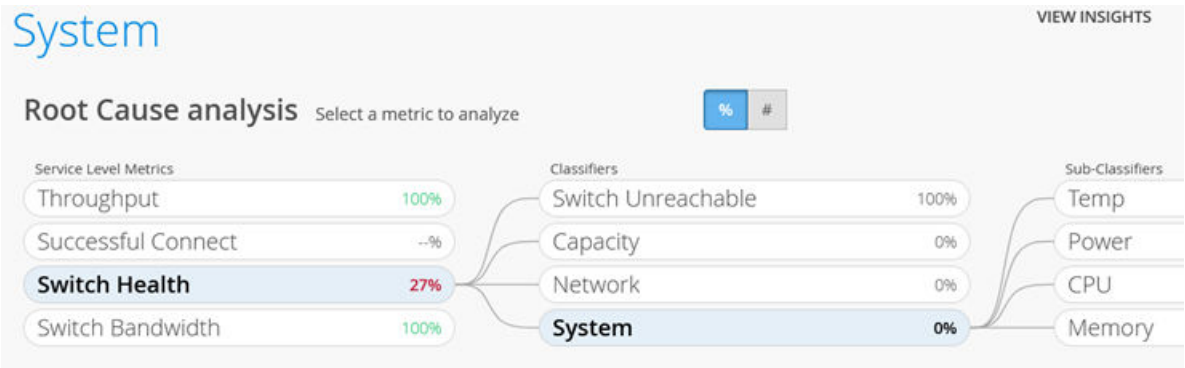
Next comes the Successful Connect SLE with its classifiers:

- DHCP
- Authentication with sub-classifiers:
  - Wrong Credentials
  - Radius Server Unreachable



Next comes the Switch Health SLE with its classifiers:

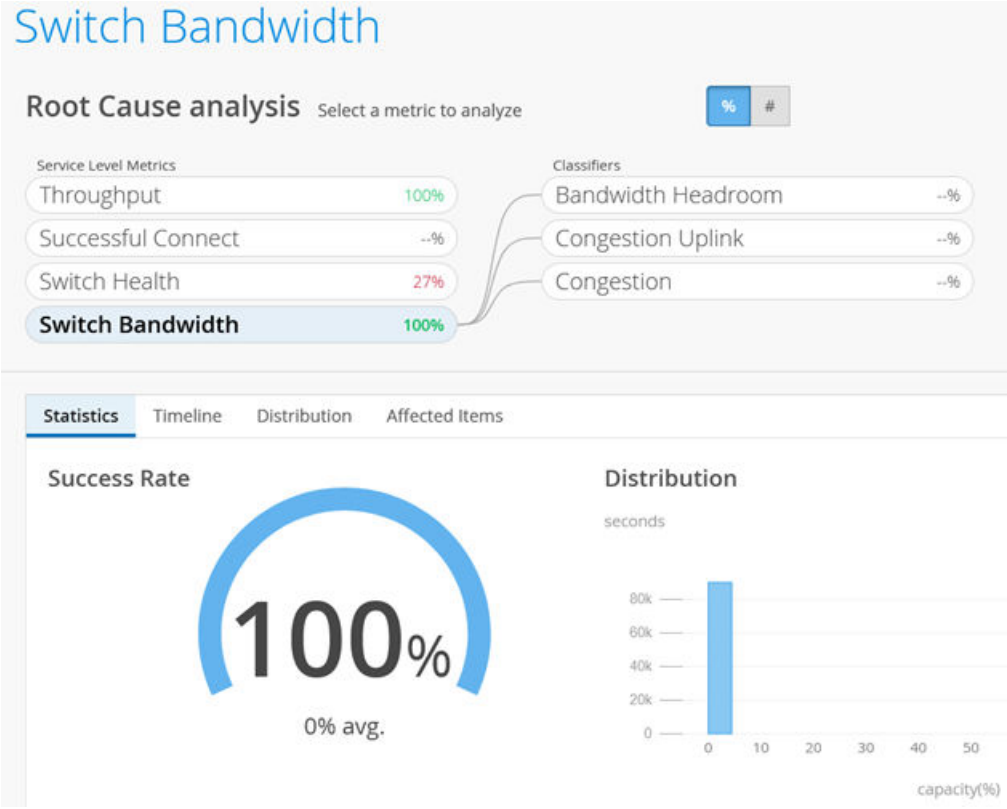
- Switch Unreachable
- Capacity with sub-classifiers:
  - Mac Address Table
  - ARP Table
  - Route Table
- Network with sub-classifiers:
  - WAN Jitter
  - WAN Latency
- System with sub-classifiers:
  - Temp
  - Power
  - CPU
  - Memory



Finally, the Switch Bandwidth SLE with its classifiers:

- Bandwidth Headroom
- Congestion Uplink

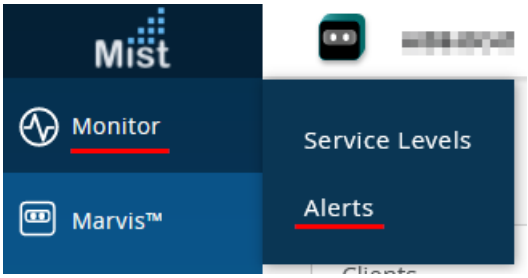
- Congestion



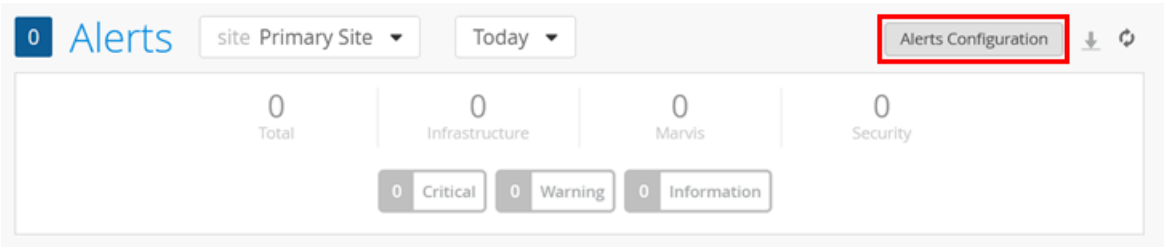
NOTE: Reports on SLEs are only made visible if there is a concern and you need to review something. If you want charts on raw data without the benefit of an AI-based analysis, please visit the "Switch Insights Page" on page 166.

Alarms Page

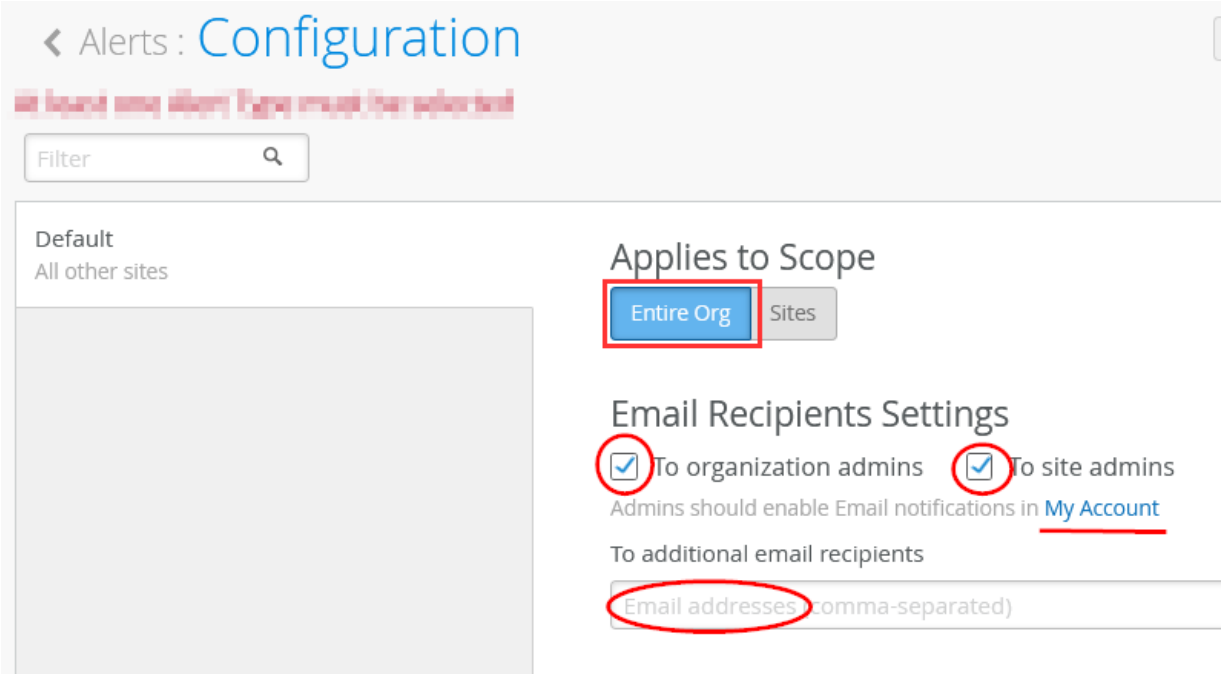
With this test case, we demonstrate the ability to see alarms for switches and optionally, to get those alarms sent as emails to the administrator. Go to **Monitor > Alarms**:



Review the current page and open the Alerts Configuration:

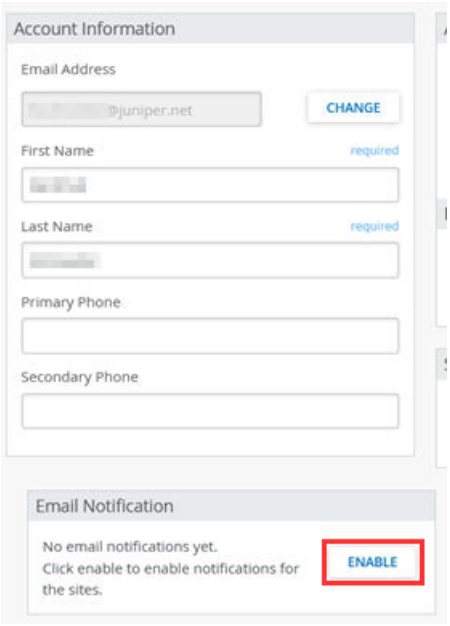


Under the configuration, keep the scope as the default **Entire Org**, and email recipients as organization and site admins. Then, you can optionally add your email address to the "`To additional email recipients`" field and click on the "`My Account`" link to verify your own settings.

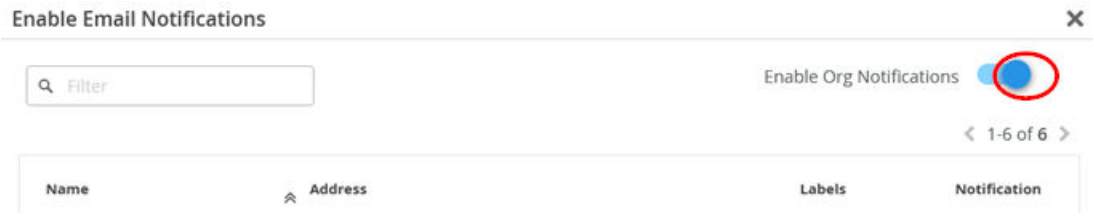


NOTE: If you are an admin, the default setting is to not send you any emails so you must enable this now.

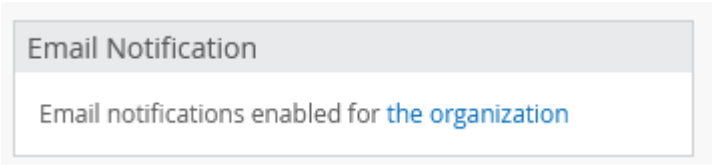
If you have followed the "`My Account`" link above, you can now select **enable** under the **Email Notification** section.



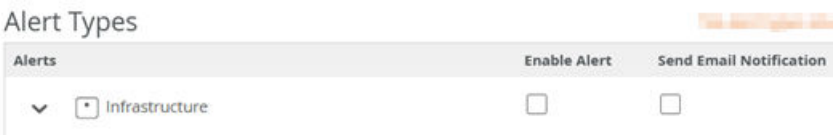
You can enable notifications on a site-by-site basis, but for now enable them for the entire organization as indicated below:

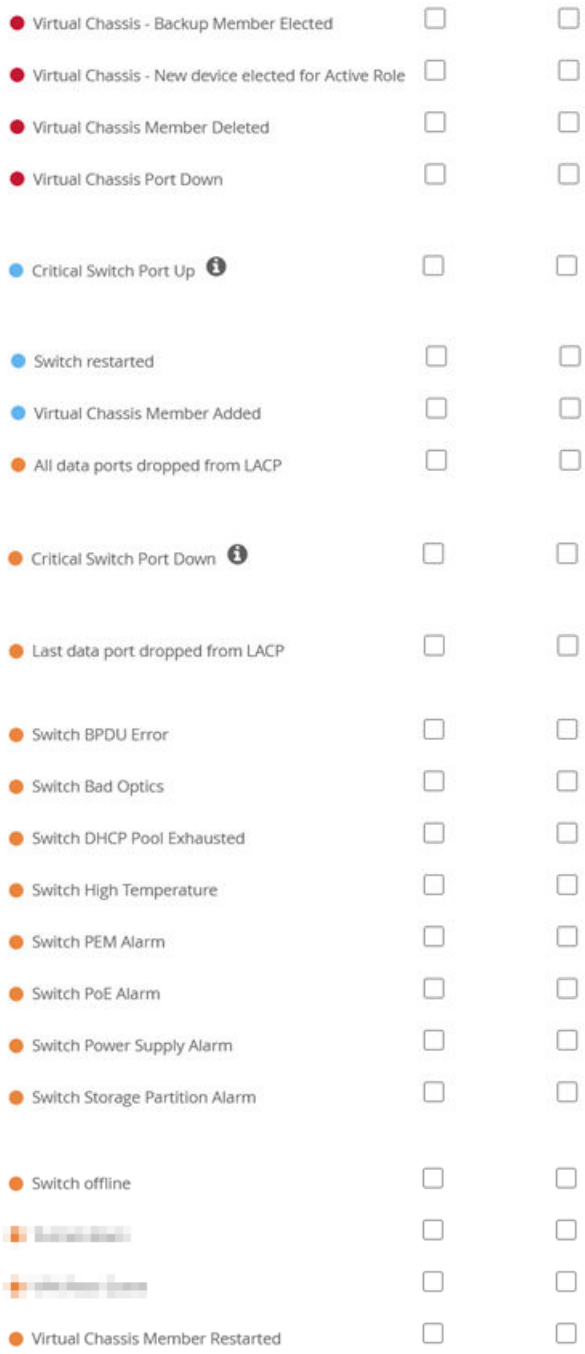


Your account email notification setting should now look like this:

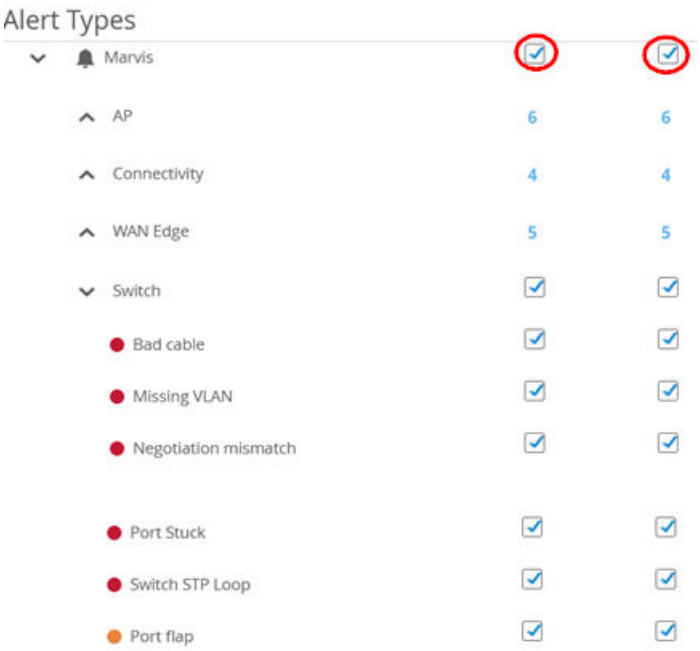


Now, enable the switch alerts and email notifications for infrastructure as the options below indicate:

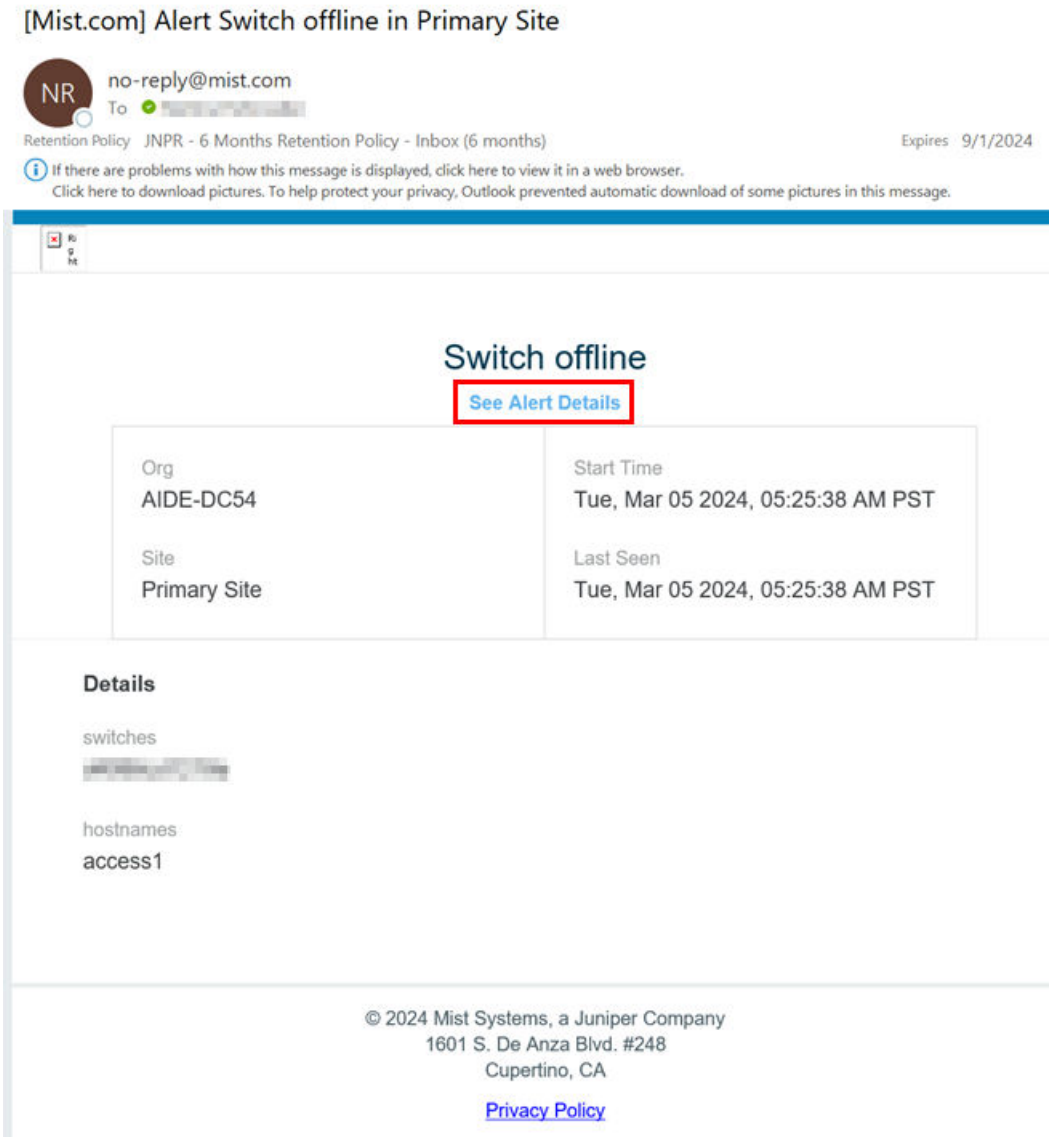




We recommend enabling the Marvis switch alerts and email notifications as well.



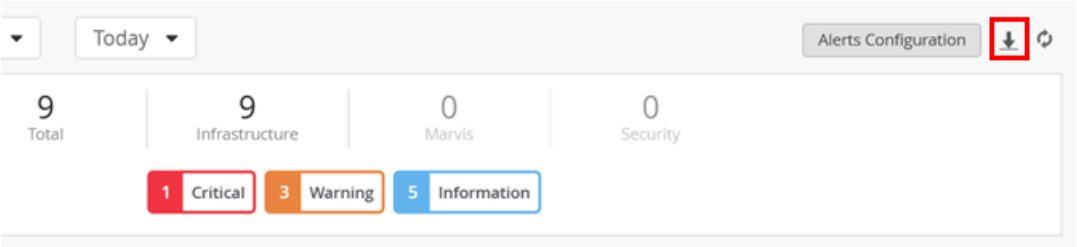
As an example, if you were to reboot a switch, you would receive the following email and others after a couple of minutes:



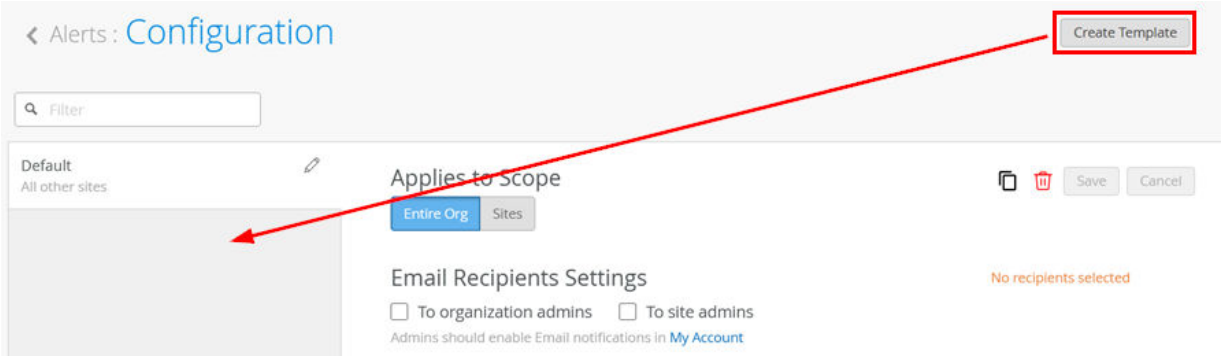
The link in the above image redirects you to the alarms page, which shows the event information similar to what is shown below:

Alert	Recurrence	First Seen	Last Seen	Details
Device restarted	1	Mar 5, 2024 2:32 PM	Mar 5, 2024 2:32 PM	Device Insights
Device reconnected	1	Mar 5, 2024 2:32 PM	Mar 5, 2024 2:32 PM	Device Insights
Switch reconnected	1	Mar 5, 2024 2:31 PM	Mar 5, 2024 2:31 PM	Switch Insights
BGP Neighbor Up	8	Mar 5, 2024 2:30 PM	Mar 5, 2024 2:30 PM	Site Insights
Virtual Chassis - New device elected for Active Role	1	Mar 5, 2024 2:28 PM	Mar 5, 2024 2:28 PM	Switch Insights
Device offline	1	Mar 5, 2024 2:26 PM	Mar 5, 2024 2:26 PM	Device Insights
Switch offline	1	Mar 5, 2024 2:25 PM	Mar 5, 2024 2:25 PM	Switch Insights
BGP Neighbor State Changed	12	Mar 5, 2024 2:25 PM	Mar 5, 2024 2:30 PM	Site Insights
BGP Neighbor Down	4	Mar 5, 2024 2:25 PM	Mar 5, 2024 2:25 PM	Site Insights

There is also a button to download the events as a CSV-based table:



Large organizations tend to use templates for alarms. Alarm templates allow for more granular assignments of alerts to the persons needing them based on the sites they manage or based on other needs.

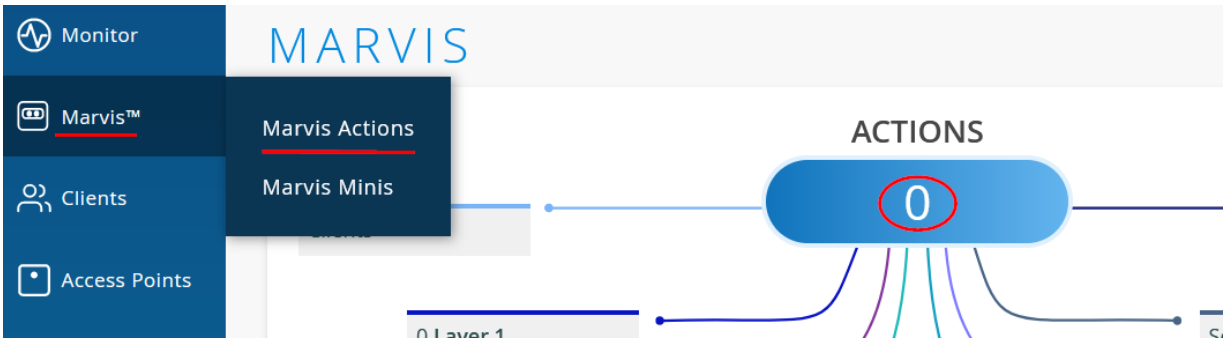


Marvis Actions

Marvis Actions is a feature of the Juniper Mist AI-driven operations platform that provides proactive and reactive troubleshooting capabilities. It leverages Mist AI to identify network issues, recommend actions,

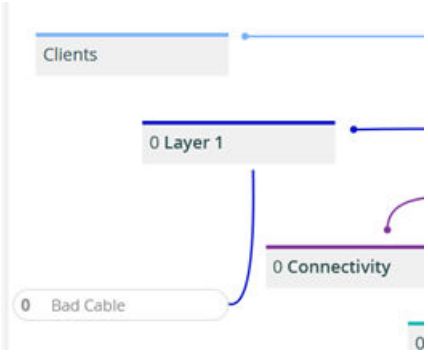
and provides insights into the root causes of these issues. The Marvis Actions dashboard displays high-impact network issues across wired, WAN, and wireless networks at different levels (MSP, organization, site). It allows users to track firmware compliance, detect WAN link outages, identify bad cables, and more. With real-time AI-driven insight, Marvis Actions enables proactive issue detection and resolution, reducing troubleshooting effort and time. More details to be found here https://www.mist.com/documentation/switch-actions/

Marvis Actions are reachable by navigating to **Marvis > Marvis Actions**. Should there be any outstanding actions needed on the network, they will be identified here.



The Marvis Actions you may see with concerns to switch infrastructure are currently:

- Marvis Switch Actions
  - Missing VLAN
  - Negotiation Mismatch
  - Loop Detected
  - Port Flap
  - High CPU
  - Port Stuck
  - Traffic Anomaly
- Marvis Layer 1 Action
- Bad Cable



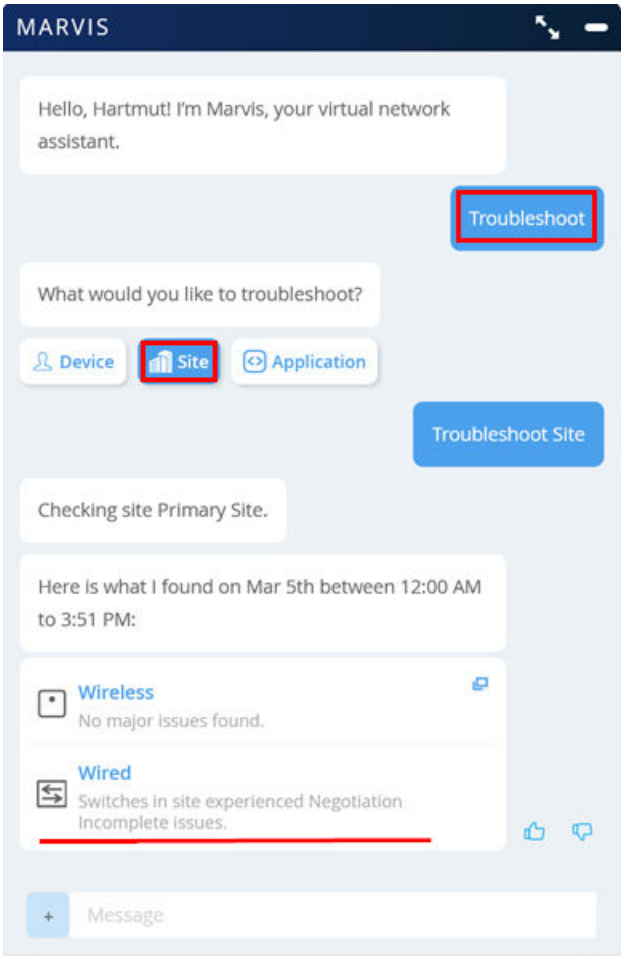
NOTE: The Marvis "Missing VLAN" action is not triggered by the switch itself as with all others shown. It needs a Juniper AP to inspect the LLDP-Media information reported by the switch. This should contain all configured VLANs on the switch where the AP is attached. When a wireless client attaches to the AP, and the SSID the client connects to is configured for a particular VLAN, the AP checks if the switch has the same VLAN configured. If that is not the case, a Marvis action is triggered.

Marvis Conversational Assistant

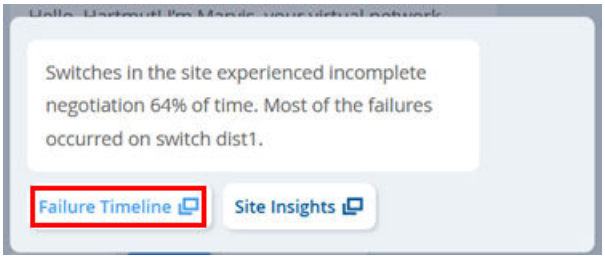
> **NOTE**: Remember that the recommendation is to have traffic running for at least a week for the AI to be able to collect enough data for processing.

The Marvis Conversational Assistant is in the lower-right corner of your browser window.

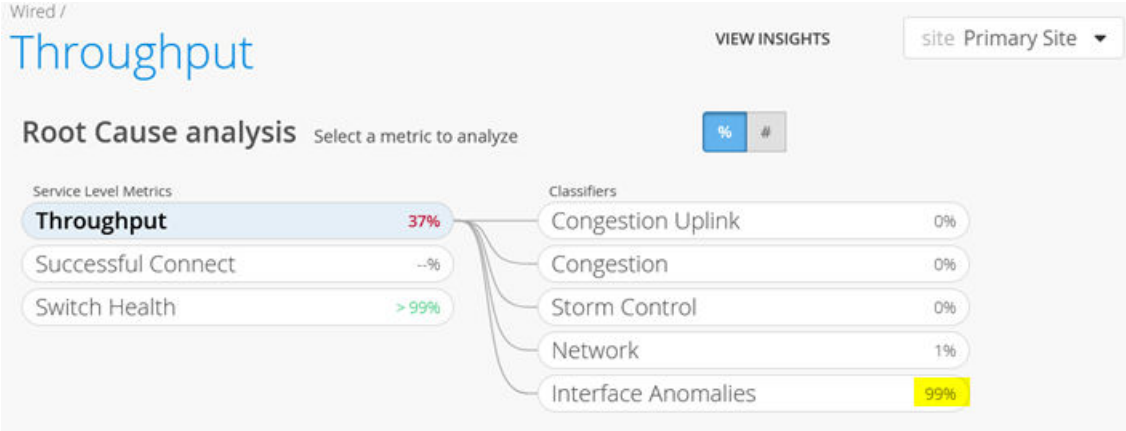
After selecting the Marvis Conversational Assistant icon, the window that appears allows you to enter questions and lists predefined topics. Enter (or click as below) here "`Troubleshoot Site`" to limit the search to issues related only the current site.



When clicking on **Wired** in our example, you can see the following report:



In this case, the link points to the **Wired SLE Monitor** page as shown in one of the chapters above.



Switch Firmware Upgrade

With Juniper Mist, you can now upgrade switches directly from the cloud.

Please refer to EX4400 – BIOS and Junos Upgrade Recommendations.

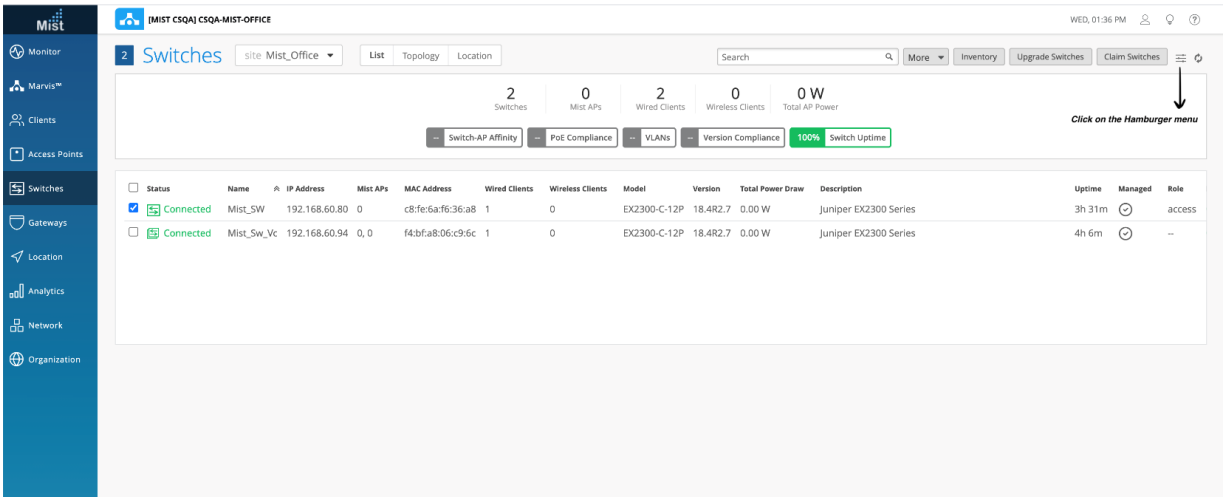
Preconditions

- Ensure stable SSH connectivity from switch to the cloud
- Ensure enough space on the switch (more details below)

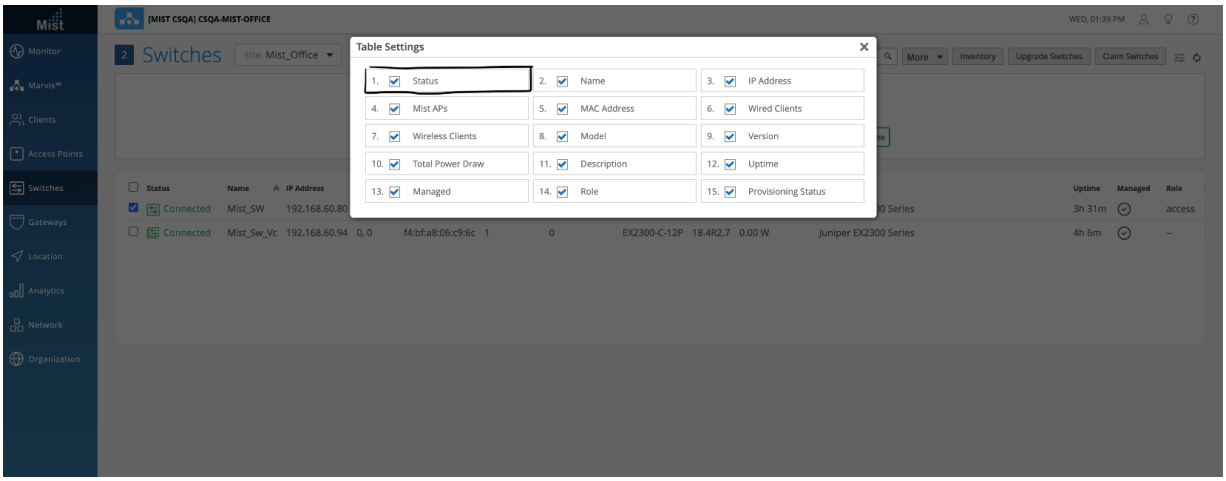
Enabling Status Column from the Menu

Make sure the status column is enabled to see the switch upgrade option.

The hamburger menu option is visible on top of the right side in the switch list view:

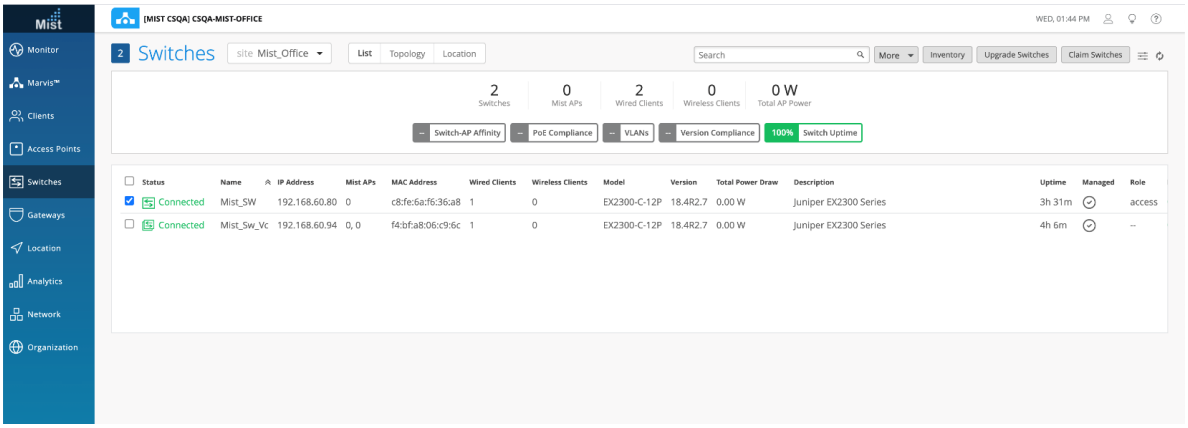


Ensure the status option is checked:

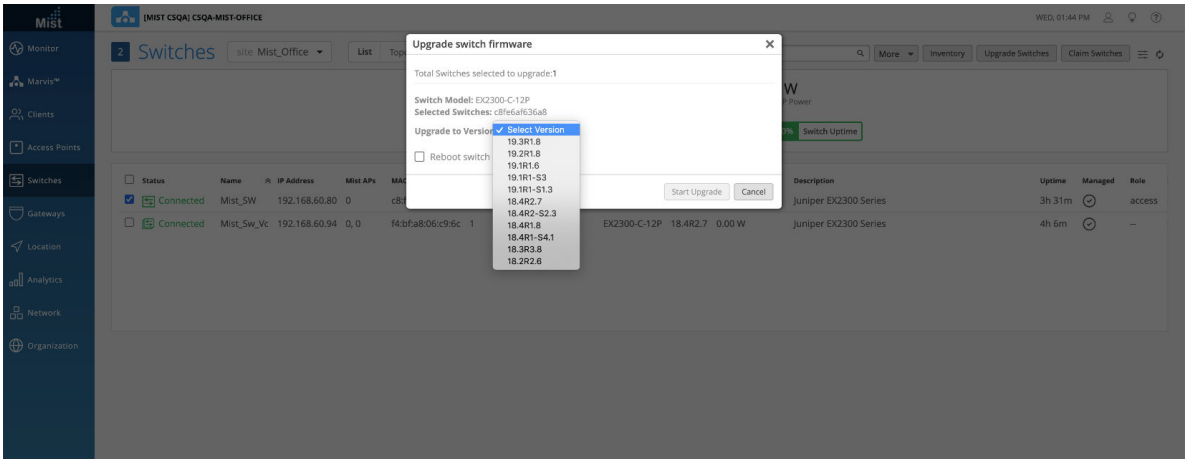


Steps to perform the switch upgrade:

1. Select the switch to upgrade, and the **Upgrade Switches** option will become visible in the upper-right corner.

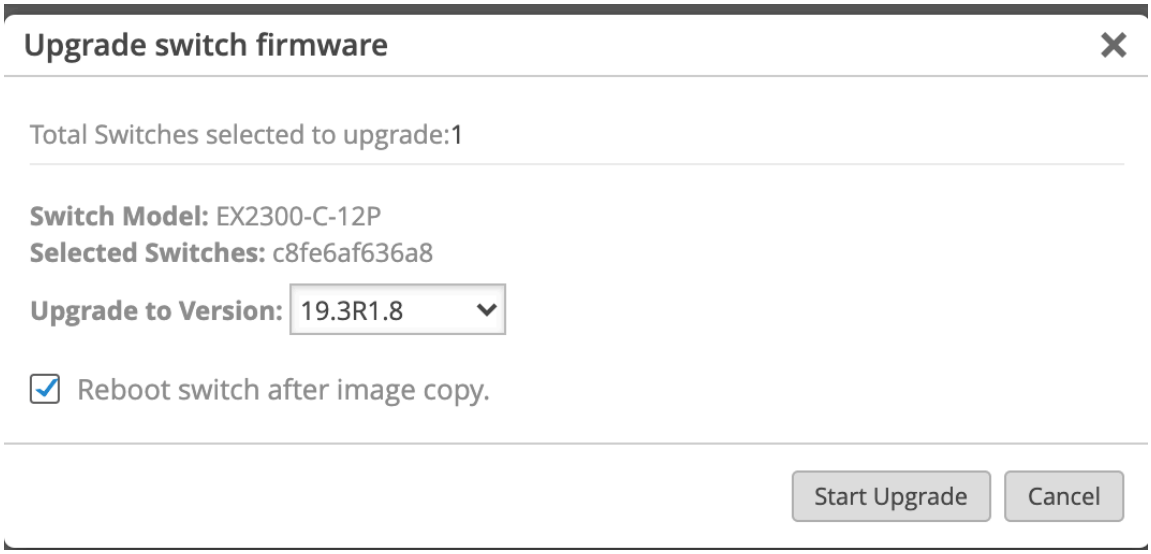


2. Click **Upgrade Switches > Upgrade switch firmware** and then select the firmware of choice.

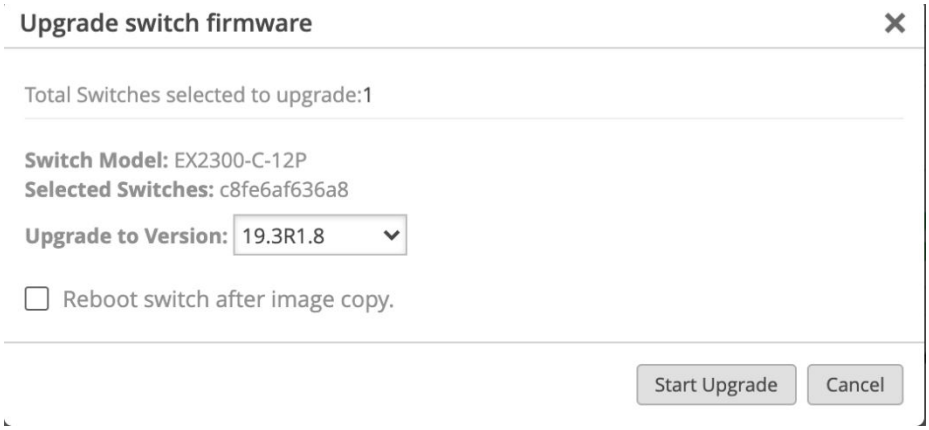


3. You are presented with two options:

   a. Reboot switch after image copy—By checking this box, the switch will automatically reboot after the image copy procedure is completed so that the switch will boot up with the new image.



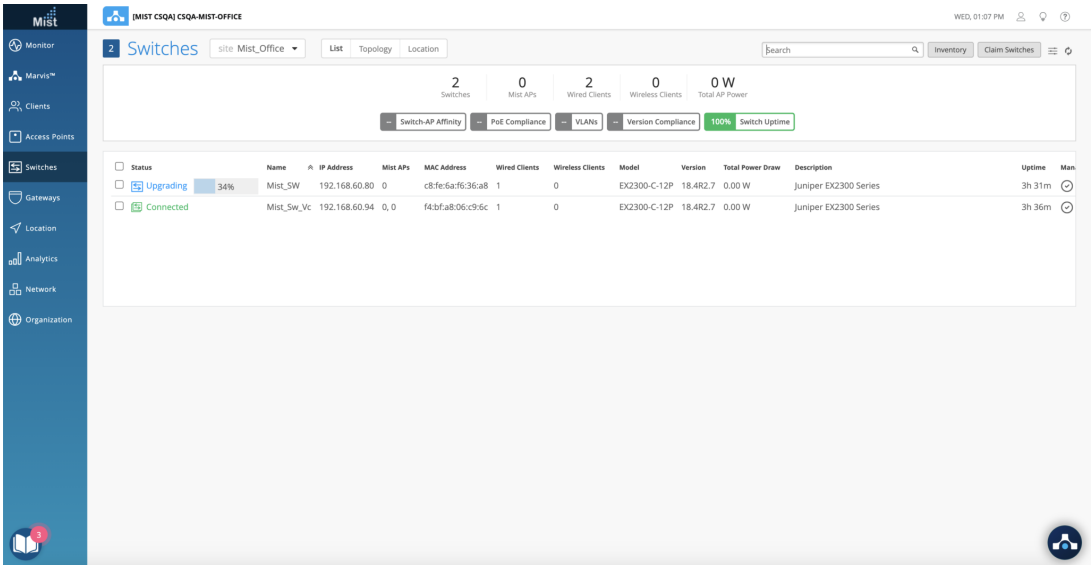
   b. If left unchecked—The image will be copied to the switch and will be in a state of pending reboot. To complete the upgrade of the switch, select **Utilities > Reboot Switch** when you are ready.



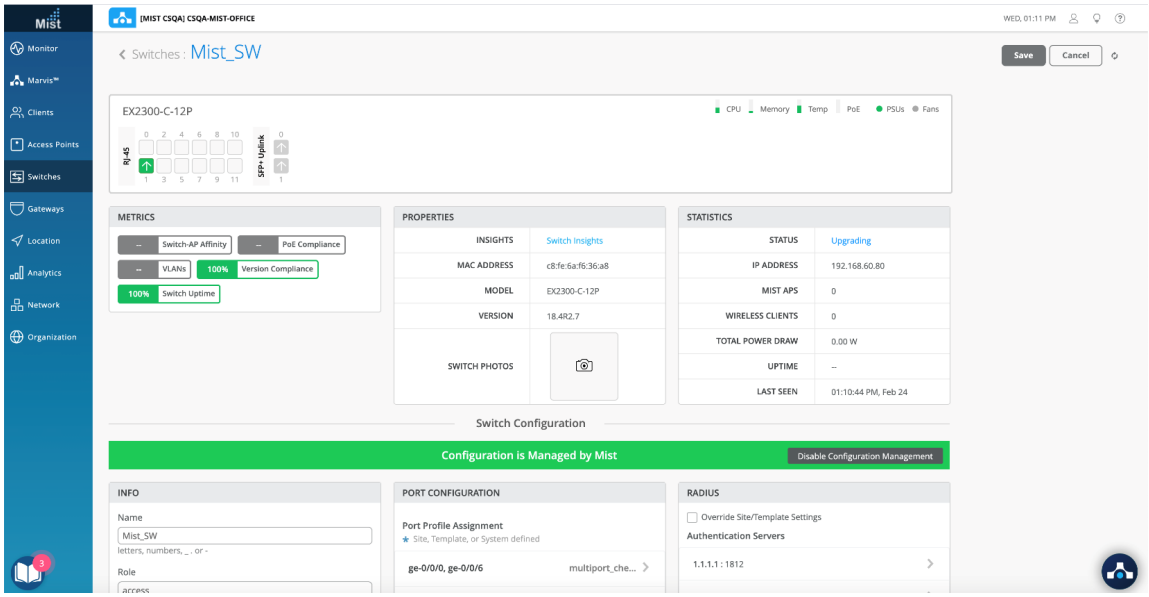
   c. The Upgrade Process:

      i. Once the upgrade starts, the progress of the upgrade will be indicated in the switch list view, switch details view (will show as “Upgrading”) and from the **Switch Insights** view:

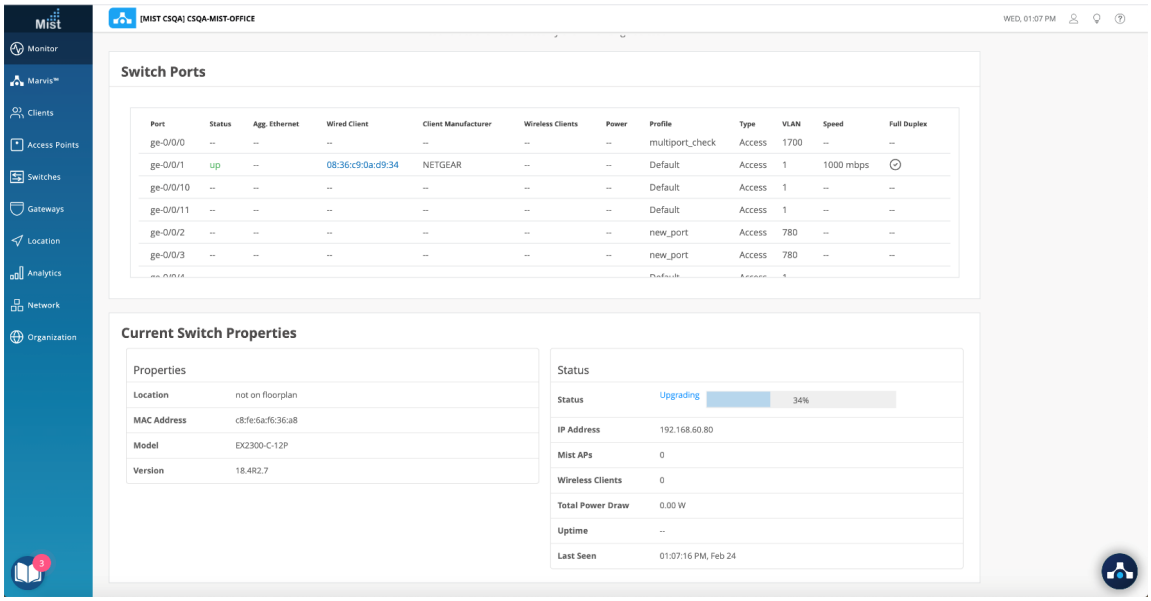
      ii. Switch List View:



d. Switch details view:

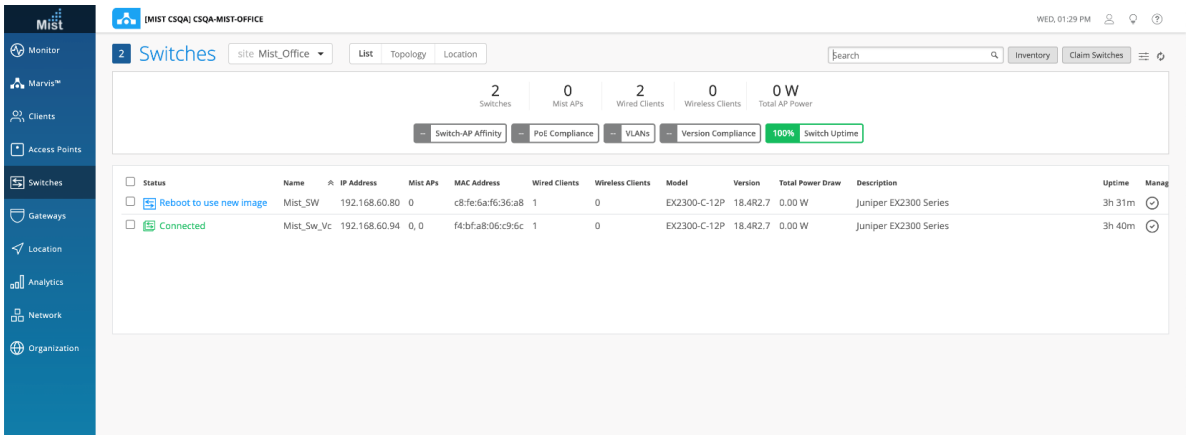


e. **Switch Insights** view:



4. Once the copy process is complete, if the “Reboot after image copy” option was chosen, the switch will reboot automatically, and the switch upgrade will be complete.

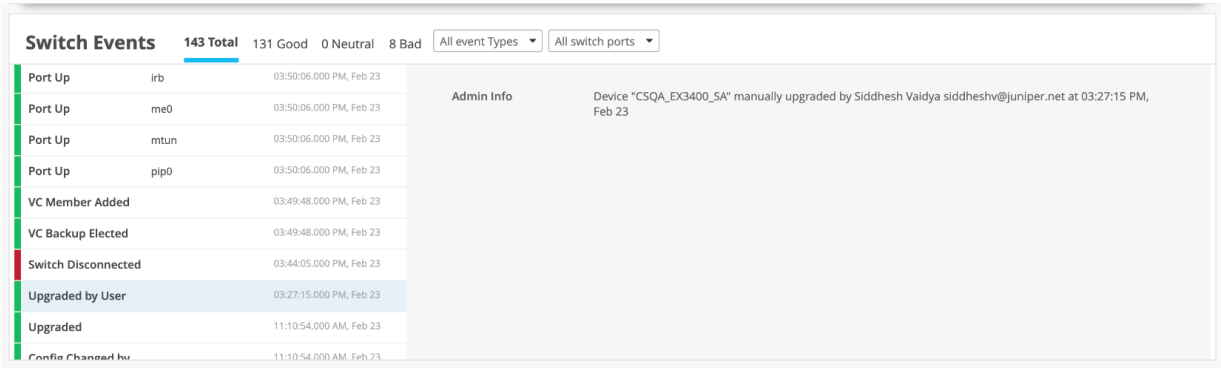
5. If the option “Reboot after image copy” was unchecked, the portal will indicate that the switch needs to “Reboot to use new image”.



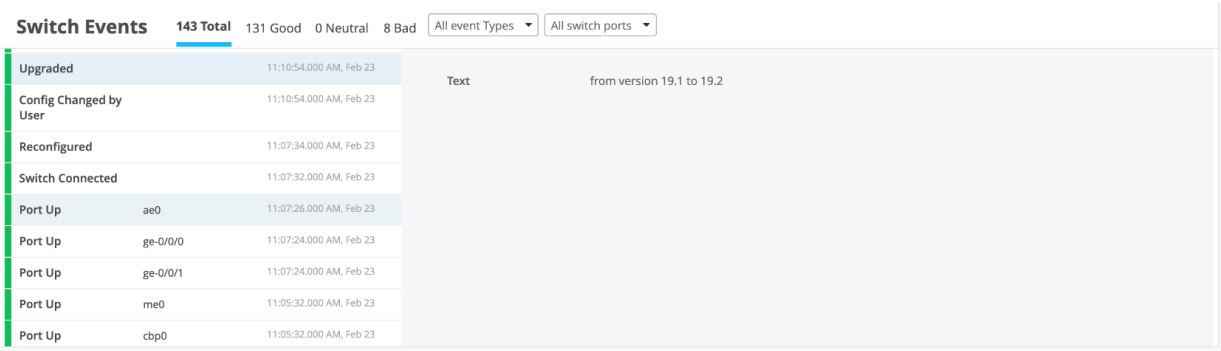
Upgrade Event

Upgrade events are visible on the portal. Clicking on **Switch Insights** will redirect to the switch upgrade events. The following events will appear when choosing **Reboot after image copy**:

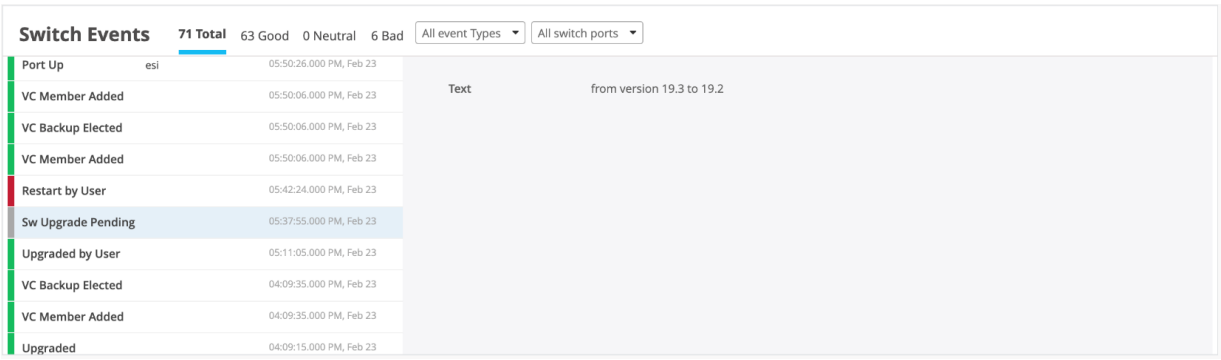
- “`Upgraded by User`” (Meaning the user has initiated the upgrade from the portal)



- "Upgraded" (After the switch has rebooted and was upgraded to the image from the portal)

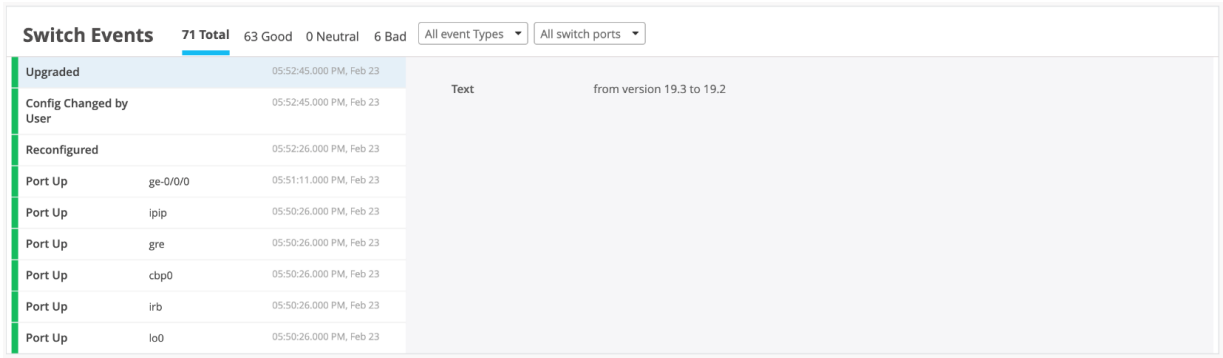


- If the option **Reboot after image copy** is unchecked, the "Sw Upgrade Pending" event is visible as a manual reboot is required to complete the switch upgrade to the desired version:



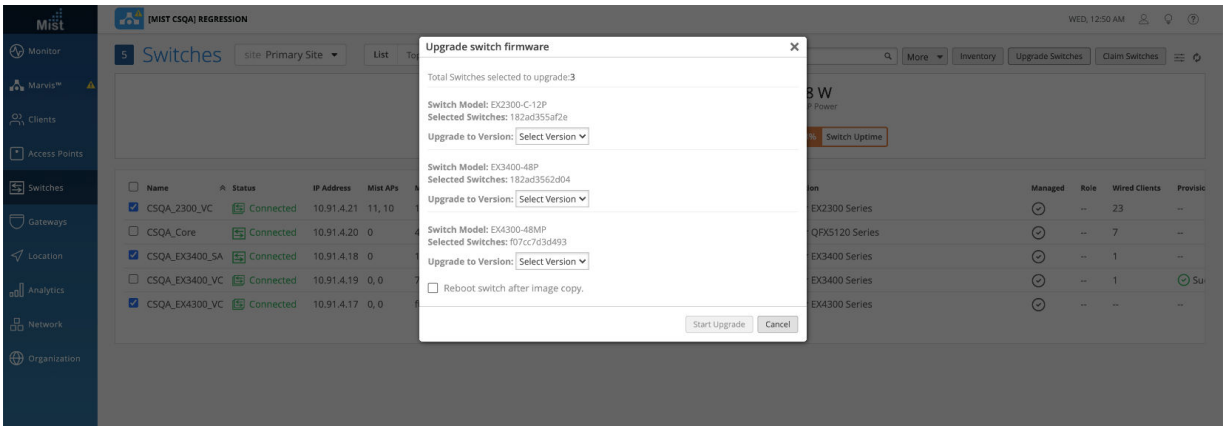
- The "Restart by User" event is visible here as a manual reboot was needed for the software upgrade to take effect:

Once the switch is upgraded, the "Upgraded" event is visible on the portal:



Multi-Switch Upgrade Support

Juniper Mist provides options to upgrade multiple platforms simultaneously from the switch list view (With different switch model combinations):



Virtual-chassis upgrade support

Mist supports the upgrade of Virtual Chassis. This support does not include NSSU.

NOTE: The switch upgrade is implemented in a way that it uses the "`request system storage cleanup`" Junos OS CLI command before any upgrade to make sure the space is available so that the image can be copied into the /var/tmp folder onto the switch.

Replace a Single Switch

Overview

- You can replace a switch without disrupting network service by retaining the existing configuration of the switch.
- Also note that this topic does not apply to replacing a switch in a Virtual Chassis.

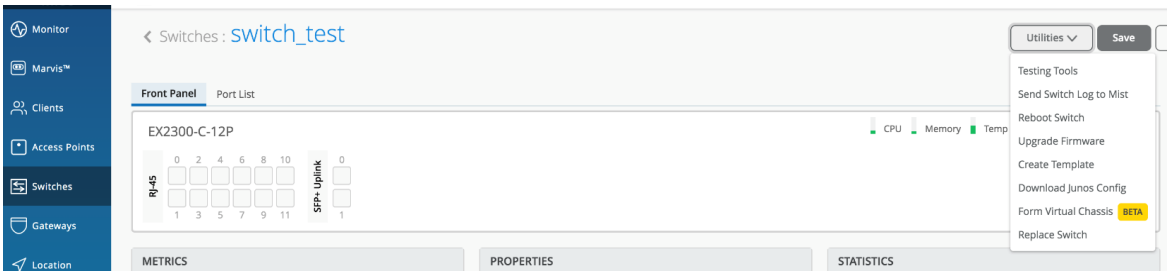
Replace a Switch through the Juniper Mist Portal

Prerequisites

- The switch being replaced must already be claimed or adopted in the organization and assigned to a site.
- The switch can be in either a "connected" or "disconnected" state.
- The new switch that will replace the old switch should be in an "unassigned" state (that is, not assigned to any site in the organization) and seen on the **Inventory** page.

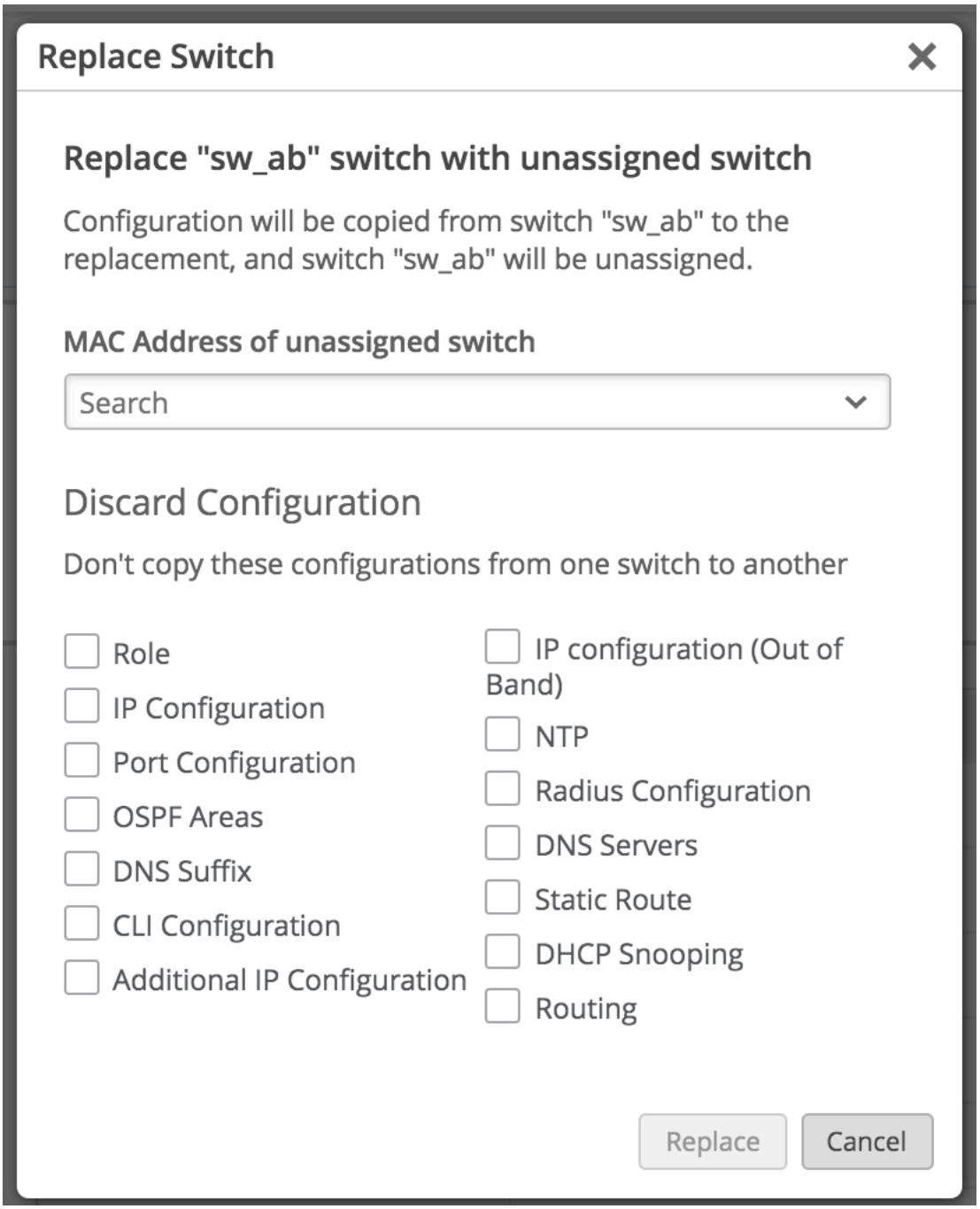
Steps

1. Go to the **Switch** tab on the dashboard and click on the switch details view.
2. Click on the **Utilities** button in the upper-right corner of the page.
3. In the **Utilities** dropdown menu, the **Replace Switch** option is seen as shown in the image below.



4. Click on the **Replace Switch** option.

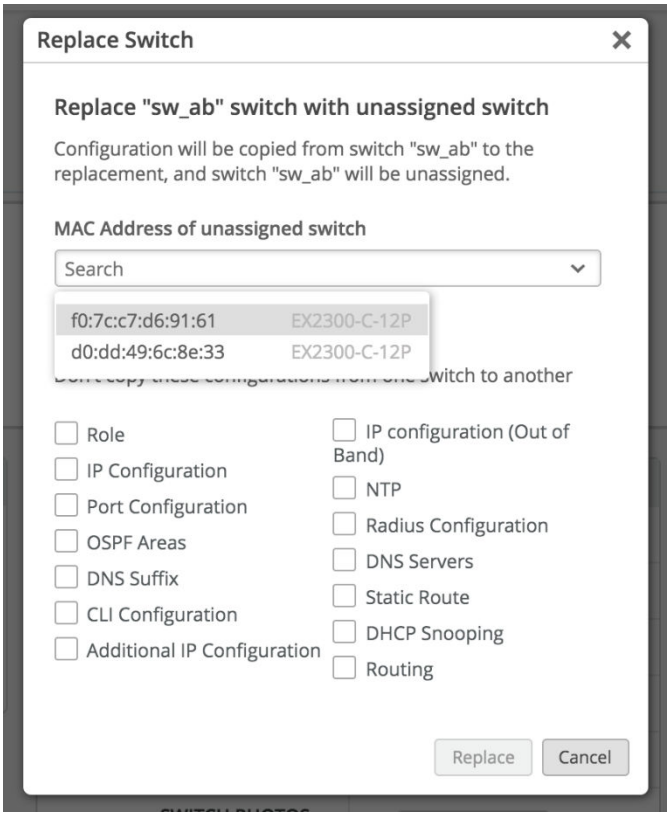
5. A **Replace Switch** window opens up as shown below:



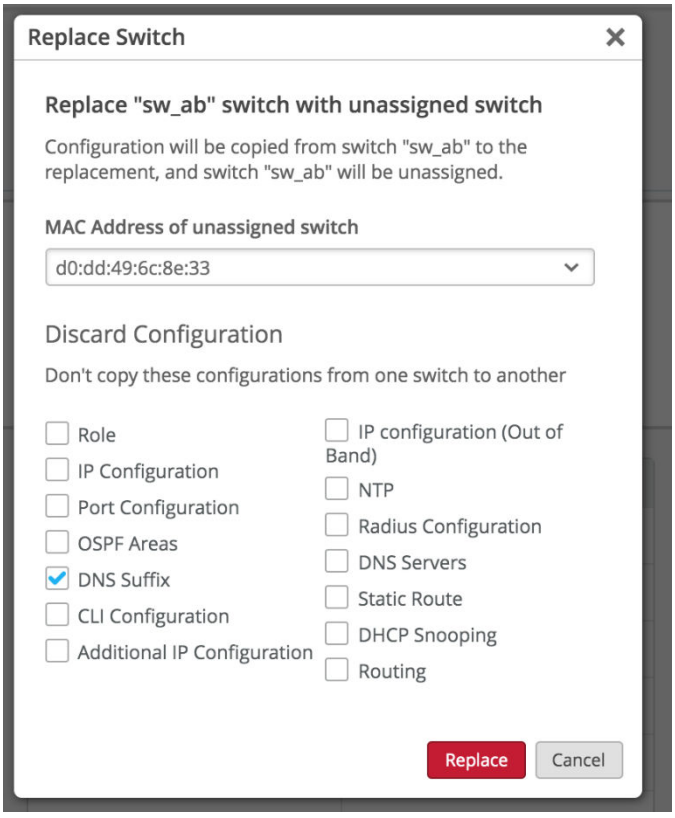
6. Make sure that there is at least one switch (non-Virtual Chassis) in an “unassigned” state on the **Inventory** page of that organization.

7. Also note that existing EX Series Switches can only be replaced with another EX Series Switch and not by QFX Series nor SRX Series devices.

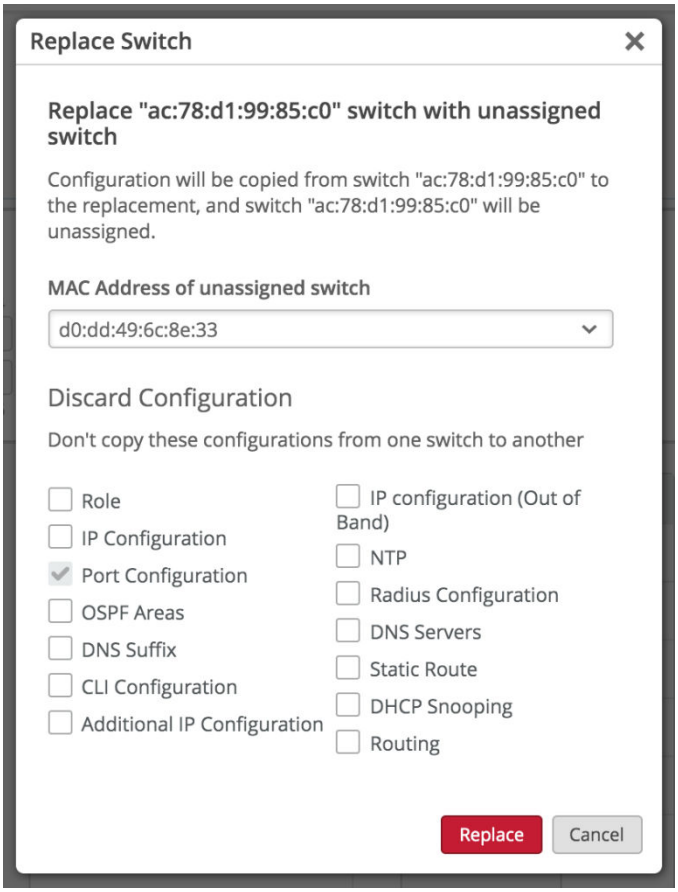
8. Search for the MAC address of the new switch in the search box as seen below:



9. Click on the checkboxes of any of the listed configuration items from the old switch that you don't want to copy to the new switch, as seen below:



10. If a switch with a higher number of ports is getting replaced with a switch with a lower number of ports, then by default the portal will discard the port configurations. Hence, the **Port Configuration** checkbox will always be checked by default in such scenarios, as seen below:



11. Click the **Replace** button.
12. Notice that the switch is replaced—the new switch takes the place of the old switch.
13. The old switch is set to an “Unassigned” state under the **Inventory** page.

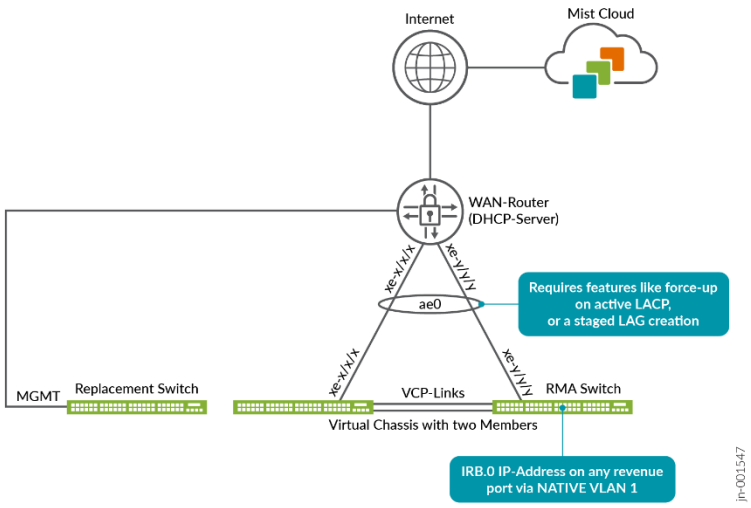
Manage a Virtual Chassis Using Juniper Mist (Add, Delete, Replace, and Modify Members)

Independent of the device type used in the Virtual Chassis, you must always do a preprovisioning of the new switch that will replace an existing switch in the current Virtual Chassis. The Juniper Mist cloud needs to know about and update the Junos OS firmware on the switch that will be added to the Virtual Chassis as well as configure the new device before you can add it to the Virtual Chassis. If the replacement switch arrives at the site, you can leverage one of two methods to be able to image and preprovision the switch before adding it to the Virtual Chassis.

One method is to use a temporary OOBM connection towards the new switch to be able to preprovision it like in the figure shown below. After this switch has joined the Virtual Chassis and all is

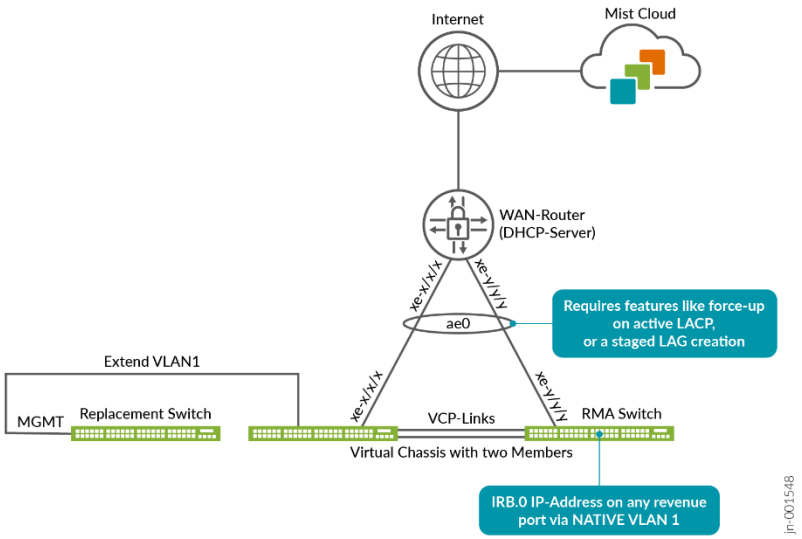
working again as expected, you can remove the temporary link. If possible, it is recommended to use the same VLAN on the OOBM connection as on the in-band management connection over the LAG.

Figure 40: VC In-Band Management Pre-Stage Using Temporary OOBM



The other option is to daisy chain the in-band management capabilities between an existing (not to be replaced) switch and the new switch using a patch cable between the revenue port on the existing switch and the MGMT port on the new switch:

Figure 41: VC In-Band Management Pre-Stage Using Daisy Chain



NOTE: It is NOT RECOMMENDED to daisy chain between the existing switch and the new switch using the revenue ports on both sides! This method has the potential to cause a loop in case someone forgets to remove this cable after the Virtual Chassis is formed again and STP is subsequently removed from these ports.

You can use the **Modify Virtual Chassis** option on the switch details page to manage your Virtual Chassis. The operations you can perform include renumbering and replacing the Virtual Chassis members and adding new members to a Virtual Chassis.

The modify virtual chassis workflow leverages the Junos OS preprovisioning method which configures the role and serial number of all members in a Virtual Chassis.

NOTE: The **Modify Virtual Chassis** option is available for switches that have the configuration management enabled in Juniper Mist.

The preprovisioned configuration specifies the chassis serial number, member ID, and role for both member switches in the Virtual Chassis. When a new member switch joins the Virtual Chassis, Junos OS compares its serial number against the values specified in the preprovisioned configuration. Preprovisioning prevents any accidental role assignment to a Routing Engine, or any accidental addition of a new member to the Virtual Chassis. Role assignments, member ID assignments, and additions or deletions of members in Virtual Chassis are under the control of a preprovisioned configuration.

- The **Modify Virtual Chassis** option is available:
  - To Super Users and Network Admins.
  - For switches that have their configuration managed by Juniper Mist.
- This workflow applies to all the EX Series and QFX Series platforms that support Virtual Chassis.
- To delete a member whose MAC address is used as the Virtual Chassis device ID, trash and replace it with an existing member in the Virtual Chassis. To verify if any Virtual Chassis member is used as the device identifier, look for the device ID on the **Switch Details** page (Virtual Chassis page) or on the switch list.
- The **Add Switch** dropdown only shows the switches that:
  - Are part of the same site. Models with dedicated VCPs can be in connected or disconnected state. However, to modify the EX2300, EX4650, or QFX5120 Virtual Chassis, the members should be in the connected state as these switches don't have dedicated VCPs.
  - Have configuration management enabled in Mist.
  - Are not currently part of the same or another Virtual Chassis.
  - Are of the same model family. For example, an EX4100-F switch can be part of a Virtual Chassis with an EX4100-48MP switch.
- The **Modify Virtual Chassis** button is disabled when the **Configuration Management** option is disabled for the switch.
- When a Virtual Chassis configuration is in progress, you cannot make any changes inside the **Modify Virtual Chassis** page.

Prerequisites

Before you perform any modification to a Virtual Chassis, you must remove all the additional CLI commands specific to Virtual Chassis (the virtual-chassis commands) from the associated device or site template. The additional CLI commands take precedence over other types of configurations. If a Virtual Chassis configuration is detected under the **Additional CLI Commands** section, you cannot make any changes using the **Modify Virtual Chassis** option. When you attempt to modify a Virtual Chassis, the

Juniper Mist dashboard displays a message to indicate that the additional CLI commands (if present) need to be removed and saved.

Convert a Virtual Chassis to Use a Virtual Device ID (Using the API)

When a Virtual Chassis device is represented in Juniper Mist by the MAC address of one of its member switches, managing it can become challenging. Especially replacing or removing a member switch may cause inconsistencies in how the Virtual Chassis is represented, potentially disrupting connectivity.

Therefore, we recommend that you convert any existing Virtual Chassis device that uses a member MAC address as its device ID to use a virtual device ID. Moving to a virtual device ID provides a consistent and centralized way to represent and manage a Virtual Chassis as a single logical entity, making future operations cleaner and more reliable.

A virtual device ID starts with the value of 0200. A device ID that starts with any other value is assumed to be based on a member MAC address.

To convert a virtual chassis (using the API):

1. Locate the site where the Virtual Chassis is deployed and identify the site ID. To do that, use the steps below:
   a. Navigate to **Organization > Site Configuration**.
   b. Select the site to open it. You can find the site ID on the **Information** tile on this page.
2. Identify the current device ID of the Virtual Chassis that is represented using a member MAC address. To do that, use the steps below:
   a. Click **Switches** to navigate to the switches page and locate the Virtual Chassis that needs to be converted.
   b. Click the Virtual Chassis device to open the Virtual Chassis (switch) details page. Look for the device ID in the URL. A MAC address-based device ID typically starts with a value other than '0200'.
3. Perform the conversion by issuing a POST request to the API endpoint below using your Site ID and Device ID.

API Endpoint:

```
https://api.<cloud_env>.mist.com/api/v1/sites/<site_id>/devices/<device_id>/vc/
convert_to_virtualmac
```

Example:

```
POST https://api.mist.com/api/v1/sites/978c48e6-6ef6-11e6-8bbf-02e208b2d34f/devices/
00000000-0000-0000-1000-a4e11a000000/vc/convert_to_virtualmac
```

Following this action, the existing device (represented by a member MAC) is disconnected from the Juniper Mist cloud, and a new device along with a virtual device ID is created and displayed. A virtual device ID typically starts with '0200'.

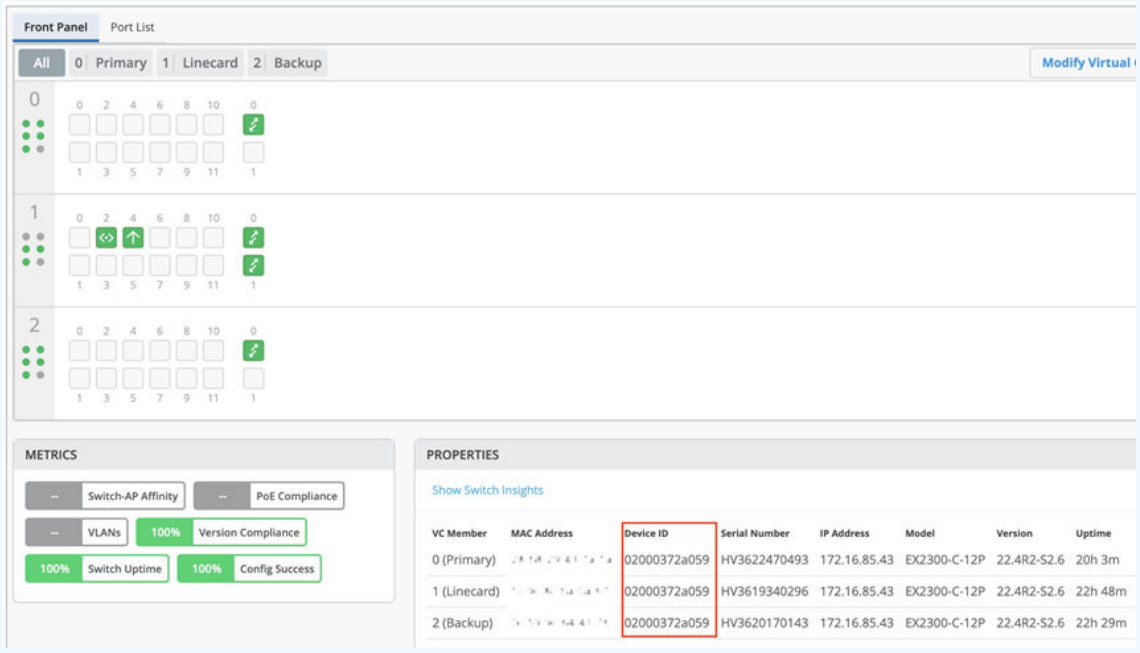
NOTE:

- Converting a Virtual Chassis device to use a virtual device ID will permanently erase all the events and stats previously stored for this device in the Juniper Mist cloud.
- The newly created Virtual Chassis may initially show as disconnected on the switch list page. However, within a few minutes, it will automatically reconnect and appear on the switch list as connected.
- The conversion does not impact the data plane—switching functionality continues uninterrupted.

Replace a Virtual Chassis Member

NOTE: Instructions in this topic apply to any Virtual Chassis device that has a device ID starting with '0200', as shown in the image below. If the Virtual Chassis uses a member MAC address as its device identifier, you must follow the instructions in **Replace a Member Whose MAC Address is Used as Virtual Chassis Device ID** to avoid any connectivity disruptions during the process.

You can find the device ID on the switch details page (Virtual Chassis page).



Replacing a Virtual Chassis member switch involves deleting the old member and adding a new member. Before replacing a member switch, you must ensure that:

- The new switch is of the same model family as the other members in the Virtual Chassis.
- The new switch is connected to the Virtual Chassis.
- The new switch is assigned to the same site as the other members in the Virtual Chassis.

To replace a Virtual Chassis member that has a device ID starting with '0200':

1. Onboard the replacement switch to the Juniper Mist cloud and assign it to the same site as the other members in the Virtual Chassis. To onboard the switch, use the **Claim Switch** or **Adopt Switch** option on the **Inventory** page (**Organization > Inventory**). You can also use the MistAI mobile app to claim a switch.

   During the switch onboarding, remember to enable the configuration management for the switch by selecting the **Manage Configuration with Mist** option.

   For the adopt switch workflow, the **Manage Configuration with Mist** option is available during the site assignment step. For more information on the adopt switch workflow, see Onboard a Brownfield Switch.

   For the claim switch workflow, the **Manage Configuration with Mist** option is available on the Claim Switches and Activate Subscription page. For more information about the claim switch workflow, see Onboard Switches to Mist Cloud.

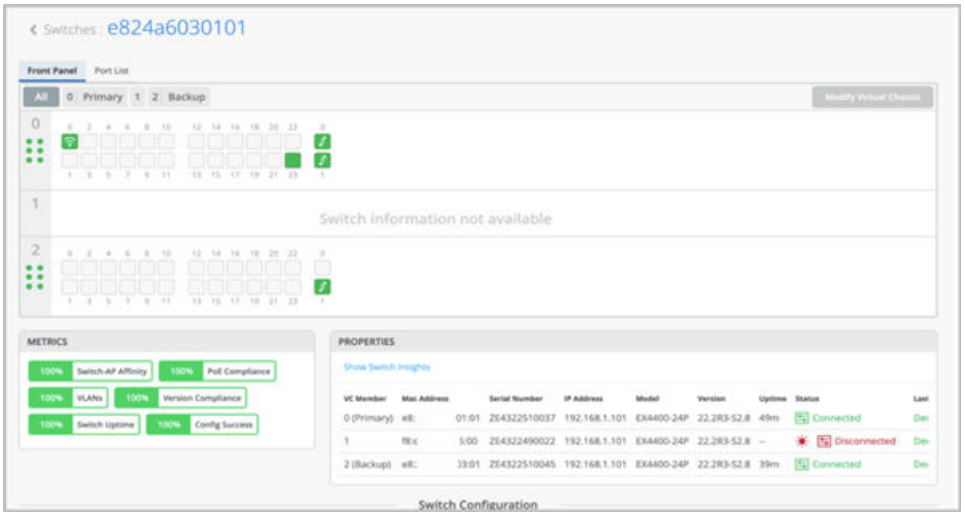
2. If you are replacing the primary member, that is, the Routing Engine of the Virtual Chassis, perform a graceful switchover from the primary role to the backup role. To do this, log in to the remote shell and run the following CLI command: `request chassis routing-engine master switch`.

3. When the backup becomes the new primary, power off the original primary member (the member to be replaced). Or remove the VCP cables from this member.

4. Connect the Virtual Chassis cables from the existing Virtual Chassis members to the new replacement switch.

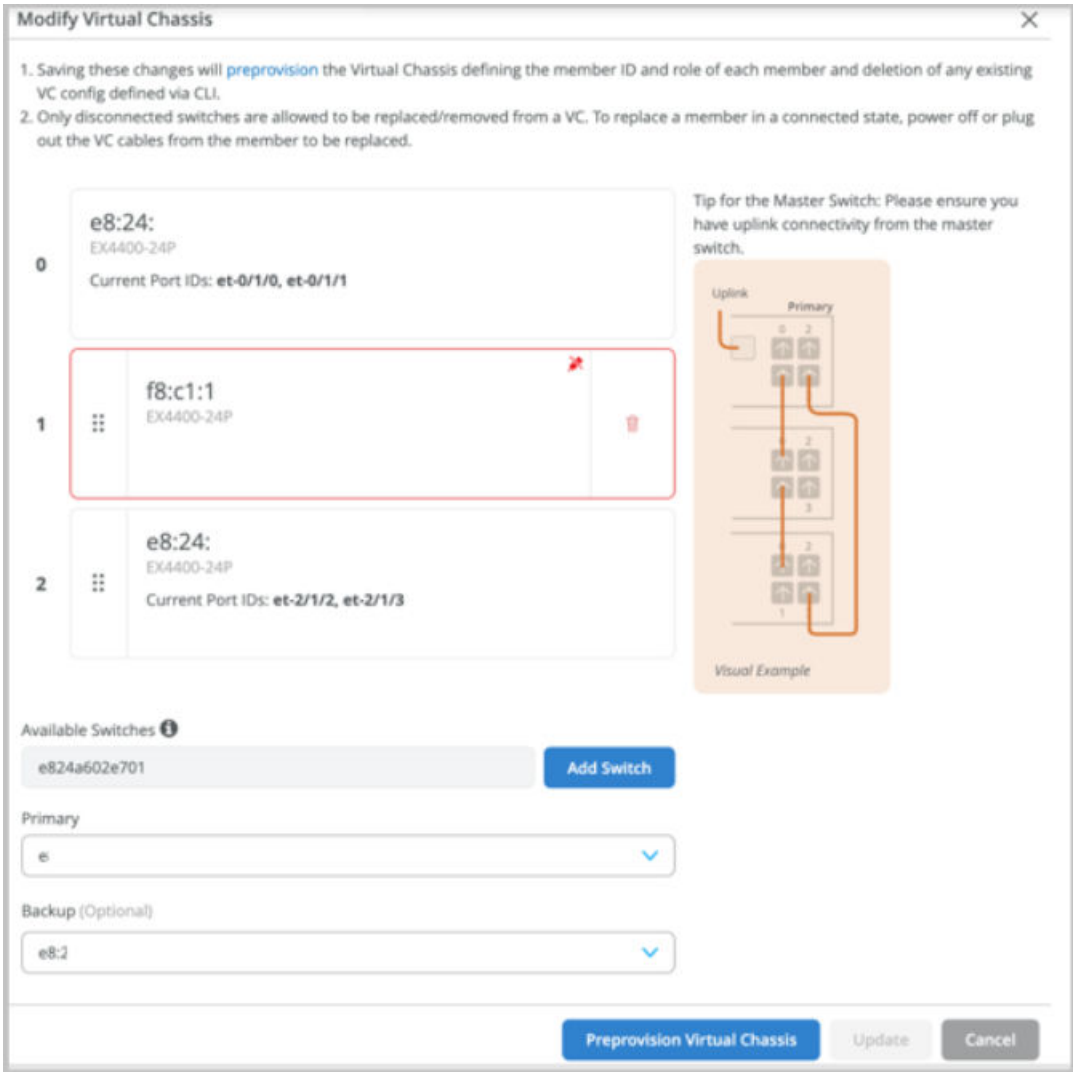
5. On the Juniper Mist portal, navigate to the switch (Virtual Chassis) details page by clicking **Switches > <Switch Name>**.

6. Wait for the switch details page to display the member switch to be replaced as offline, as shown below:

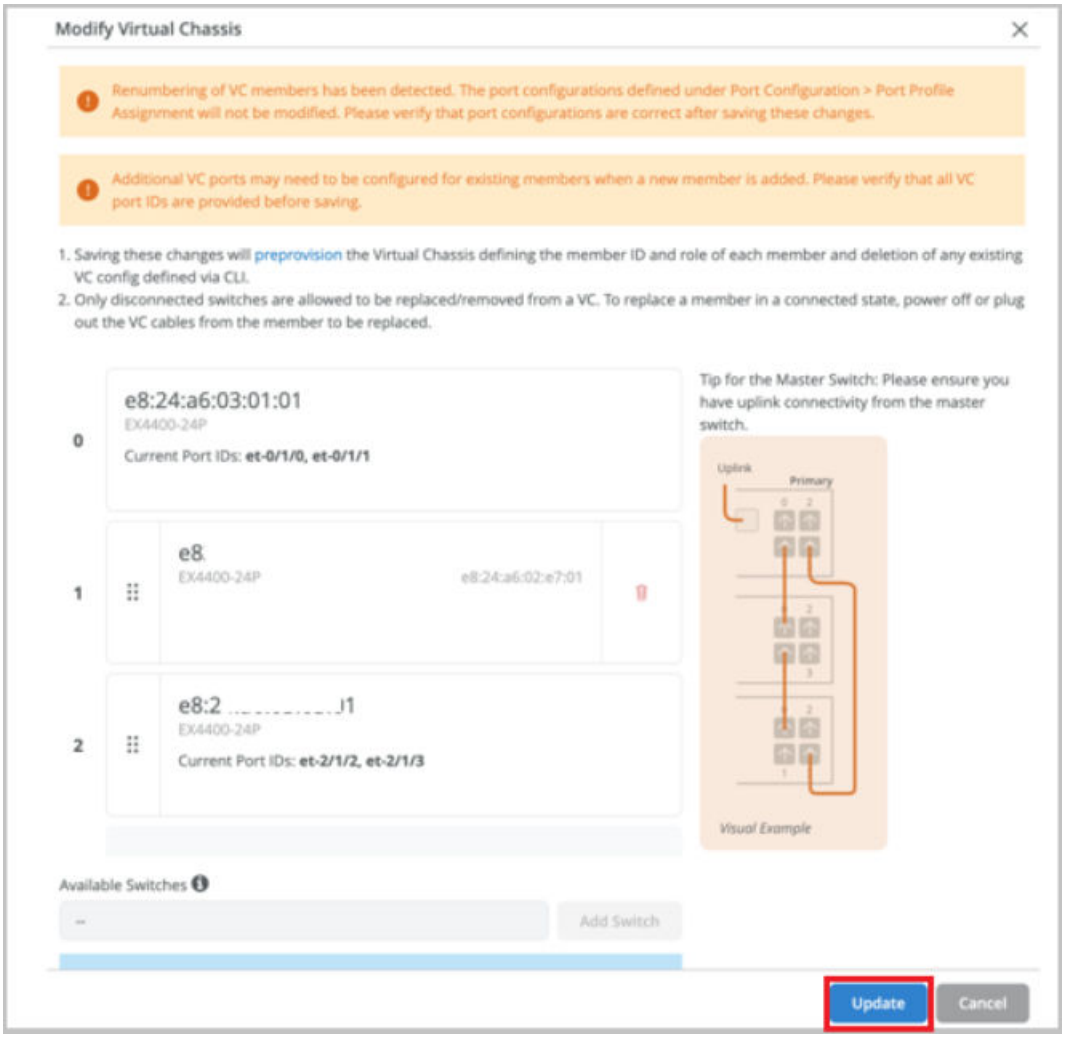


7. Click **Modify Virtual Chassis**.

   Because you removed the VCP connection from the member switch being replaced, the Modify Virtual Chassis window displays a broken link for this member switch along with a delete (trash) icon.



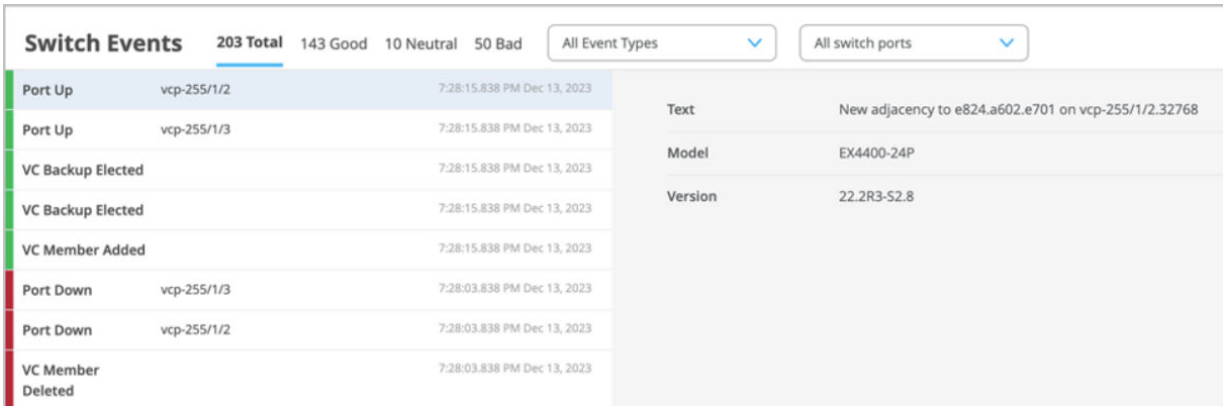
8. Delete the member to be replaced by clicking the trash icon.
9. Click **Add Switch** to add the new replacement member.
10. Renumber the new switch by dragging and dropping it into the appropriate slot.
11. Edit the MAC address of the primary or backup switch if you are replacing one of them.
12. Click **Update**.



13. Ensure that the replacement switch, which is onboarded, is powered on.

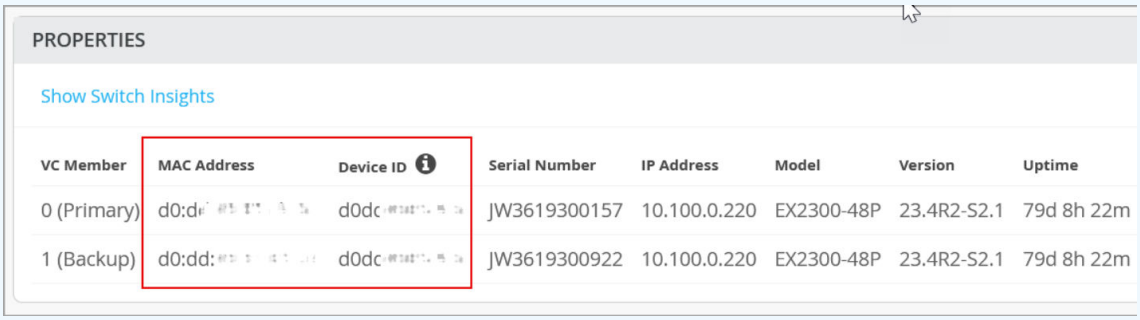
14. Wait for Virtual Chassis formation to be complete.

The Switch Events page displays all the Virtual Chassis update events.



Replace a Member Whose MAC Address is Used as Virtual Chassis Device ID

NOTE: Instructions in this topic apply to any Virtual Chassis device that uses a member MAC address as its device identifier, as shown in the image below. If the Virtual Chassis that has a device ID starting with 0200, you must follow the instructions in Replace a Virtual Chassis Member to replace its members. You can find the device ID on the switch details page (Virtual Chassis page).



If a Virtual Chassis uses the MAC address of a member (typically the FPC0) as the device identifier, you cannot replace that member in a single operation as it is used to communicate to the Juniper Mist cloud. You need to carry out the replacement in a 2-step process that includes adding the new replacement switch and then removing the switch to be replaced. In such cases, you should carry out the member replacement operation in a maintenance window as this operation can impact the traffic to the clients connected.

NOTE: Replacing an FPC member that is used as the device ID will freshly assign the Virtual Chassis with a new device ID that is no longer tied to any FPC member.

Before replacing a member switch, you must ensure that:

- The new switch is of the same model family as the other members in the Virtual Chassis.
- The new switch is connected to the Virtual Chassis.
- The new switch is assigned to the same site as the other members in the Virtual Chassis.
- The Virtual Chassis is preprovisioned. For a 2-member VC, the split and merge feature is disabled by default (no-split-detection) if the Virtual Chassis is provisioned by the cloud.

To replace a member (FPC0, for example) whose MAC address is used as the Virtual Chassis device ID:

1. Remove the uplink connection (in-band or OOB) from the FPC0 member (if an uplink is present). Ensure the connectivity to the Juniper Mist cloud is maintained after the removal of the uplink. If this is the only uplink, connect it to another member that can provide the uplink connectivity.

2. If the FPC0 is a primary member, that is, the Routing Engine of the Virtual Chassis, perform a graceful switchover from the primary role to the backup role. To do this, log in to a remote shell and run the following CLI command: `request chassis routing-engine master switch`.

3. Power off the FPC0 member to be replaced. Or, remove the VCP cable from it.

4. Claim the new member switch, assign it to the same site, and enable configuration management on the switch.

   If this member switch belongs to a model (such as the EX2300, EX4000-8P, EX4650, or QFX5120) that does not have a dedicated VC port, you should connect it to the Juniper Mist cloud. For information on how to claim a switch, refer to "Activating a Greenfield Switch via claim and ZTP-based installation" on page 109.

5. Connect the VCP cable to the new member on the same ports.

   The new member is added to the Virtual Chassis.

   Now, the Virtual Chassis status in Junos OS will look like that shown below:

   - fpc0 - Not present
   - fpc1 – Present
   - fpc2 - Non-provisioned because the fpc0 and fpc1 were already preprovisioned.

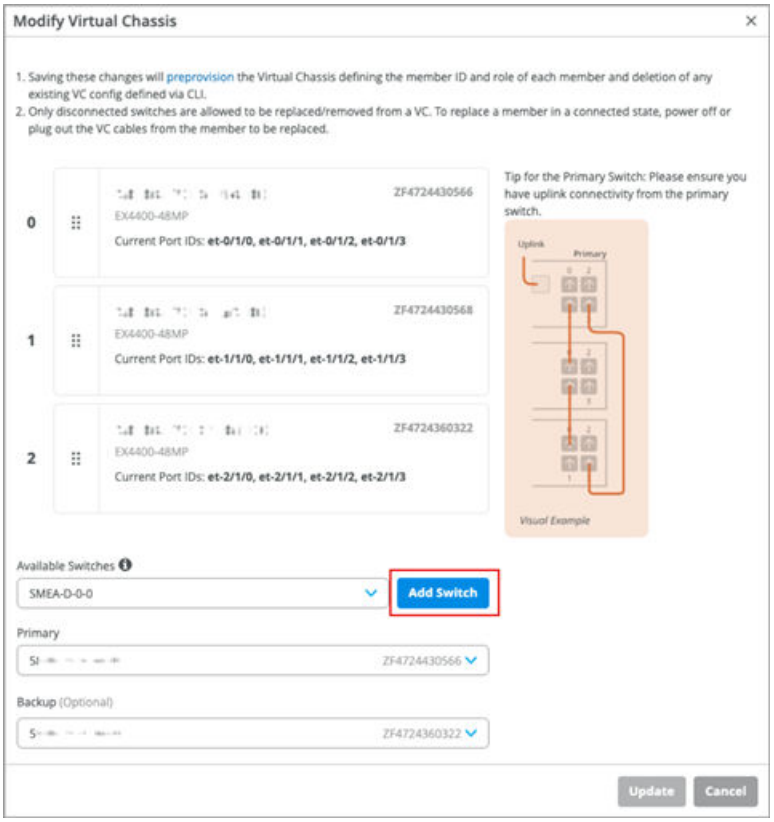
```
user@switch> show virtual-chassis
.
Preprovisioned Virtual Chassis
Virtual Chassis ID: 19e4.0553.ff90
Virtual Chassis Mode: Enabled
                                                  Mstr           Mixed Route Neighbor List
Member ID  Status   Serial No    Model          prio  Role      Mode  Mode ID  Interface
0 (FPC 0)  NotPrsnt EZ0524AX0140
1 (FPC 1)  Prsnt    FA1024AX0329 ex4100-48p     129   Master*      N  VC
-          Unprvsnd FJ1123AV0214 ex4100-f-12p
```

6. In the Juniper Mist portal, click **Switches > Switch Name** to go to the switch details page of the Virtual Chassis to be modified.

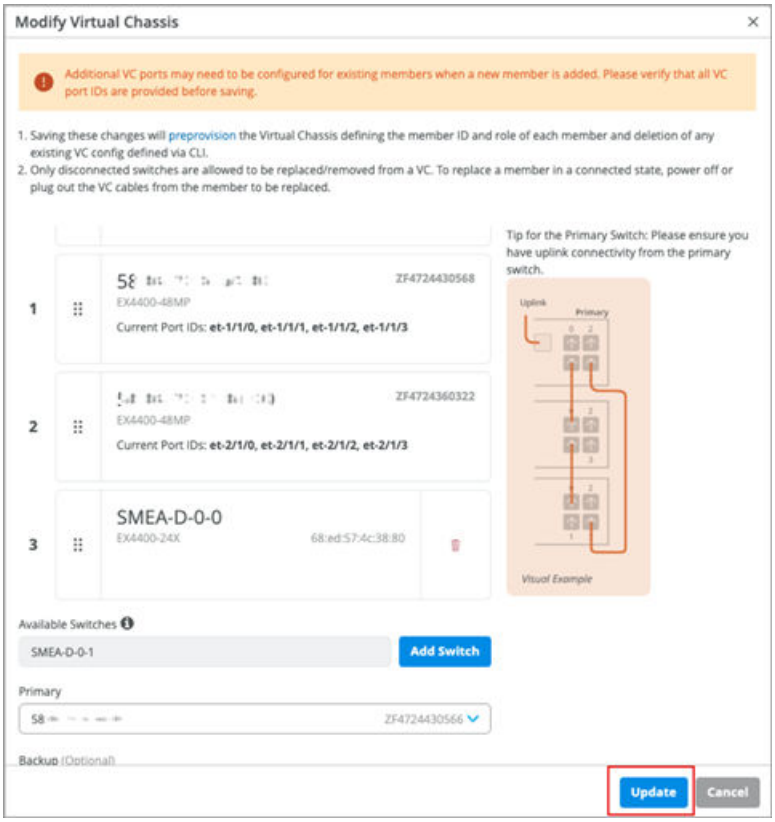
7. Click **Modify Virtual Chassis**.

   The Modify Virtual Chassis window appears.

8. On the Modify Virtual Chassis window, click **Add Switch** and add the replacement switch to the Virtual Chassis as a new member.



9. Click **Update**.



10. Wait 5 to 10 minutes for the data to synchronize and appear on the Juniper Mist portal.

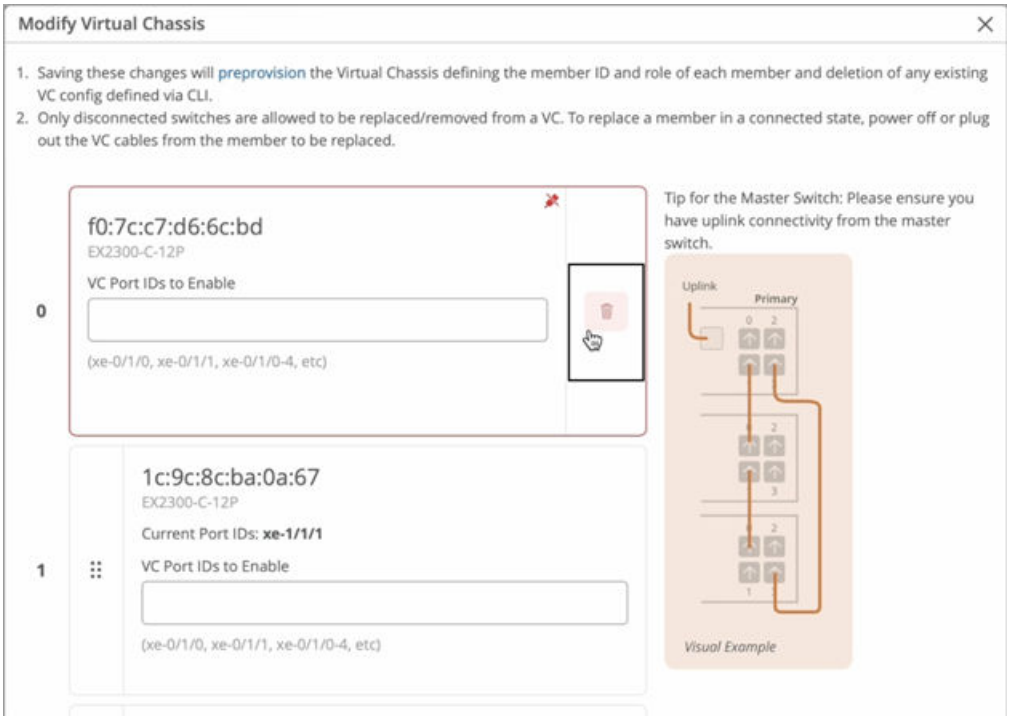
11. Click **Modify Virtual Chassis** again.

    Because you removed the VCP connection from the FPC0 being replaced, the Modify Virtual Chassis window displays a broken link against this member switch along with a delete (trash) icon.

12. Delete the member to be replaced by clicking the trash icon.

    The Modify Virtual Chassis window displays a message indicating that FPC0 is required.

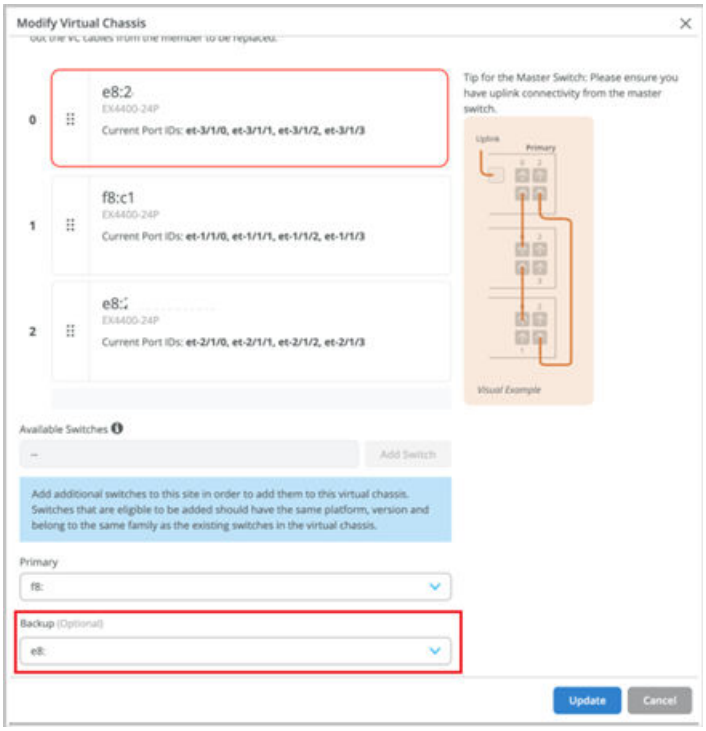
13. Move the FPC2 member to slot 0 (the FPC0 slot) by dragging and dropping.



NOTE: Ensure that no role change is performed.

14. Click **Update**.

15. Update the **Backup** field with the MAC address of the new switch, as shown below:



16. Click **Update**.

Renumber the Virtual Chassis Members

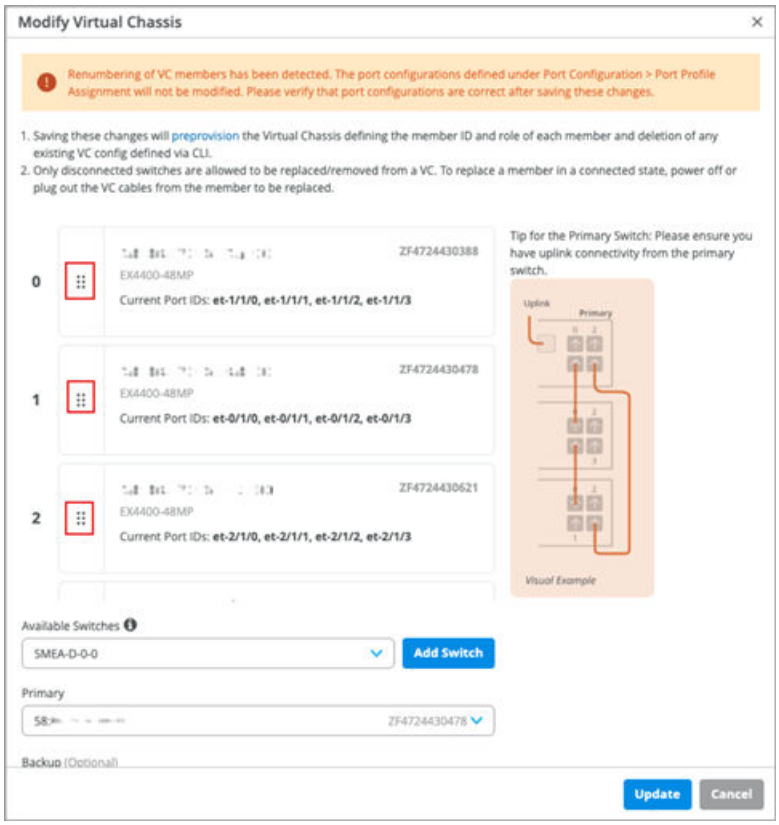
If you prefer to see the Virtual Chassis members on the Juniper Mist portal in the same order as they are physically stacked, you need to reorder the switches (after they are powered on and connected to Virtual Chassis) using the **Modify Virtual Chassis** option.

You can modify the member switches' order on the Juniper Mist portal by renumbering the members. On the Modify Virtual Chassis window, accessible from the switch details page, you can move around the port panel of a switch to change the order of the member. The order is incremental. The first entry is member 0, the second is member 1, and so on. You are required to specify the FPC0.

To renumber the switches in a preprovisioned Virtual Chassis:

1. Click the **Switches** tab on the left to navigate to the Switches page.
2. Click the Virtual Chassis in which you want to renumber the members.
   The switch details page appears.
3. On the switch details page, click **Modify Virtual Chassis**.
   The Modify Virtual Chassis window appears.
4. On the Modify Virtual Chassis screen, drag and drop the port panel of a switch to different slots to change the switch number. The order is incremental. The first entry is member 0, the second is

member 1, and so on. In the example below, the FPC1 has been renumbered as FPC2 and the FPC2 has been renumbered as FPC1.



NOTE: Within a Virtual Chassis that uses the MAC address of a member (typically FPC0) as the device ID, you cannot renumber or move around that member unless it is disconnected.Renumbering the members within a Virtual Chassis does not renumber the port configurations and port profile assignment. When you renumber a VC, Mist displays the following warning (as shown in the picture above): "Renumbering of VC members has been detected. The port configurations defined under Port Configuration > Port Profile Assignment will not be modified. Please verify that port configurations are correct after saving these changes."

So, ensure that these changes are taken care of before or after renumbering the members in the Virtual Chassis.

5. After you have made the changes, click **Update**.

   The members are renumbered.

Reassign Virtual Chassis Member Roles

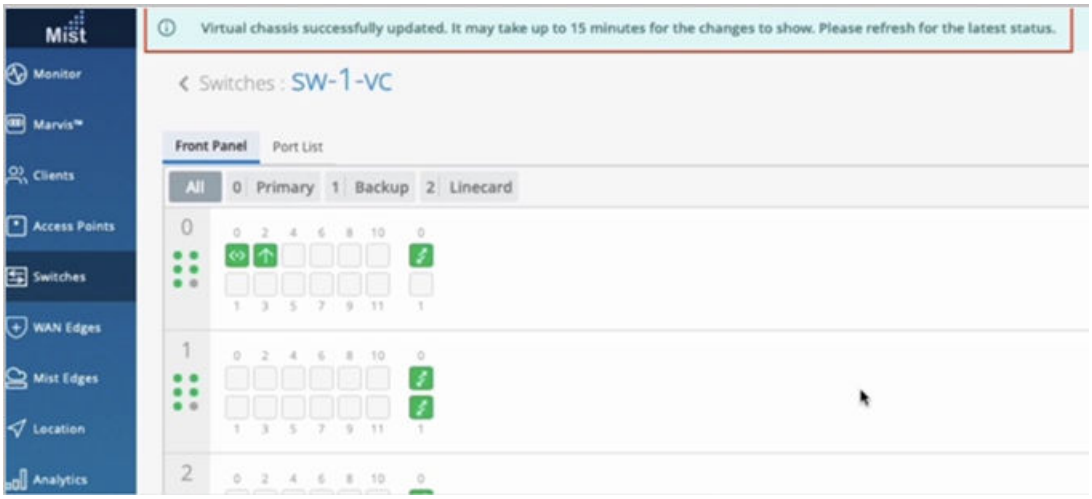
A Virtual Chassis configuration in a Juniper Mist™ network has two switches in the Routing Engine role — one in the primary Routing Engine role, and the other in the backup Routing Engine role. The

remaining member switches operate in the linecard role. You can change the role of a switch from primary to backup or backup to linecard or linecard to primary.

To change the role of Virtual Chassis members:

1. Click the **Switches** tab on the left to navigate to the Switches page.
2. Click the Virtual Chassis in which you want to change the member roles.
   The switch details page appears.
3. On the switch details page, click **Modify Virtual Chassis**.
   The Modify Virtual Chassis window appears.
4. On the Modify Virtual Chassis screen, specify a primary switch and a backup switch (optional) from the Primary and Backup drop-down list. All the other switches assume a linecard role.
5. After you have made the changes, click **Update**.
   The member roles are changed.

You will see the updated status about the role change on the switches page on the Juniper Mist portal. The role change will take some time (approximately 15 minutes) to appear on the Juniper Mist portal. You can see a banner message at the top after every change that you make, as shown below:

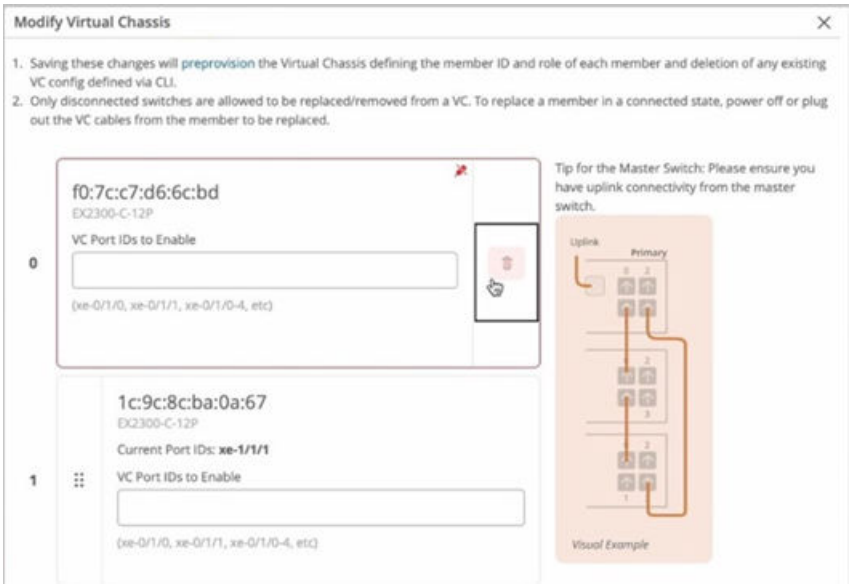


Delete Virtual Chassis Members

You can delete the member switches from the Virtual Chassis by clicking the delete (trash) icon on the Modify Virtual Chassis window. Before deleting any member switch, you must ensure that the switch to be removed is disconnected from the Virtual Chassis. If the switch is connected, power it off or remove the VCP connection from it.

To delete a member switch from Virtual Chassis:

1. If you are removing a primary member, that is, the Routing Engine of the Virtual Chassis, perform a graceful switchover from the primary role to the backup role. To do this, log in to the Remote Shell and run the following CLI command: `request chassis routing-engine master switch`
2. Power off the member to be removed. Or remove the VCP cable from it.
3. On the Juniper Mist portal, click the **Switches** tab on the left to navigate to the Switches page.
4. Click the Virtual Chassis from which you want to delete a member switch.
   The switch details page appears.
5. On the switch details page, click **Modify Virtual Chassis**.
   The Modify Virtual Chassis window appears. Because you have removed the VCP connection from the member switch, the Modify Virtual Chassis window displays a broken link for the member switch along with a delete icon.
6. Click the delete icon and then click **Update**.



Mist removes the member switch from the Virtual Chassis.

Add a Member Switch to a Virtual Chassis

You can add one or more member switches to a Virtual Chassis from the Modify Virtual Chassis window. Before adding a new member switch to a Virtual Chassis, ensure the following:

- The new switch is of the same model family as the other members in the Virtual Chassis.
- The new switch is connected to the network (applicable to EX2300, EX4650, and QFX5120).
- The new switch is assigned to the same site as the other members in the Virtual Chassis.

Juniper Mist automatically upgrades a Virtual Chassis linecard member if it is running a Junos OS version different from that of the primary member. The linecard member will be upgraded to the same version as the primary member if the following conditions are met:

- The switch must form a Virtual Chassis with three or more members—that is, a primary, a backup, and a linecard member.
- The Junos OS version on the linecard member is different from that on the primary member.
- The linecard member must be in Inactive state.

  Note that a linecard member will be upgraded only if it is inactive and running a clearly different Junos OS version. Minor differences, such as different spin numbers, will not trigger an upgrade.
- Only the Junos OS versions listed on the Mist portal are available for upgrade.

To add a new member switch to the Virtual Chassis:

1. Onboard the new switch to the Juniper Mist cloud and assign it to the same site as the other members in the Virtual Chassis. To onboard the switch, use the **Claim Switch** or **Adopt Switch** option on the Inventory page (Organization > Inventory). You can also use the MistAI mobile app to claim a switch.

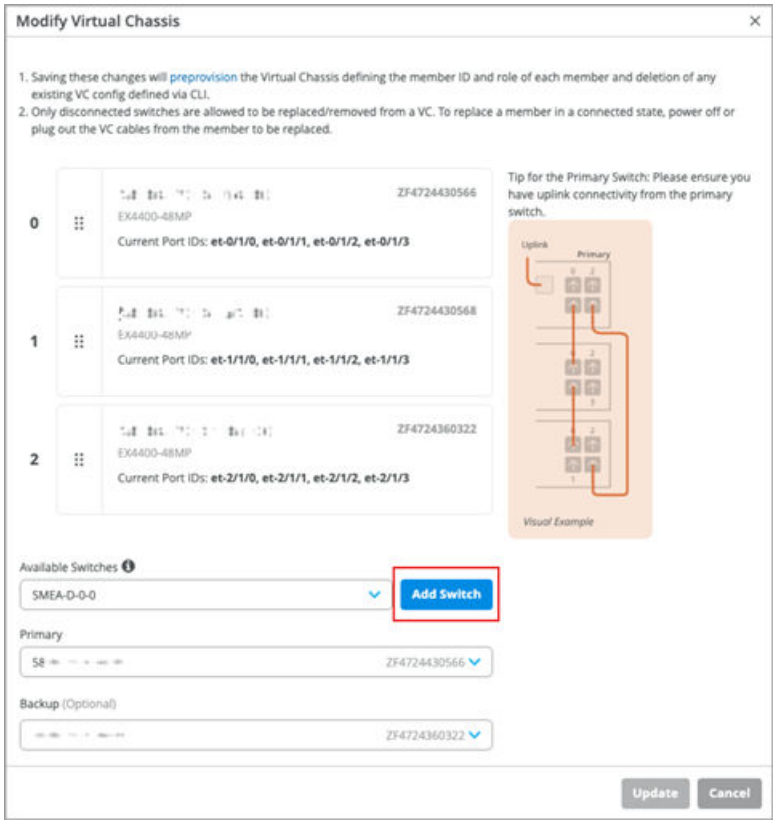
   During the switch onboarding, remember to enable the configuration management for the switch by selecting the **Manage configuration with Mist** option.

   For the adopt switch workflow, the **Manage configuration with Mist** option is available during the site assignment step. For more information on the adopt switch workflow, see "Activating a Greenfield Switch via claim and ZTP-based installation" on page 109 .

   For the claim switch workflow, the **Manage configuration with Mist** option is available on the Claim Switches and Activate Subscription page. For more information about the claim switch workflow, see "Activating a Brownfield Switch via Adoption Code-Based Installation" on page 112 .
2. On the Juniper Mist portal, click the **Switches** tab on the left to navigate to the Switches page.
3. Click the Virtual Chassis to which you want to add the new member switch.

   The switch details page appears.
4. On the switch details page, click **Modify Virtual Chassis**.

   The Modify Virtual Chassis window appears.
5. On the Modify Virtual Chassis window, click **Add Switch**.

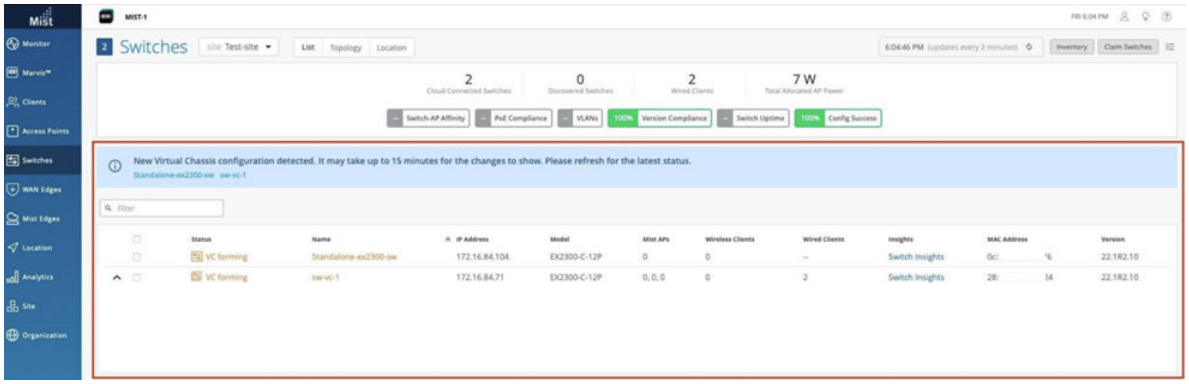


6. Specify the VC port ID for the switch, if needed (the port ID configuration applies to the EX2300, EX4650, and QFX5120 switches).

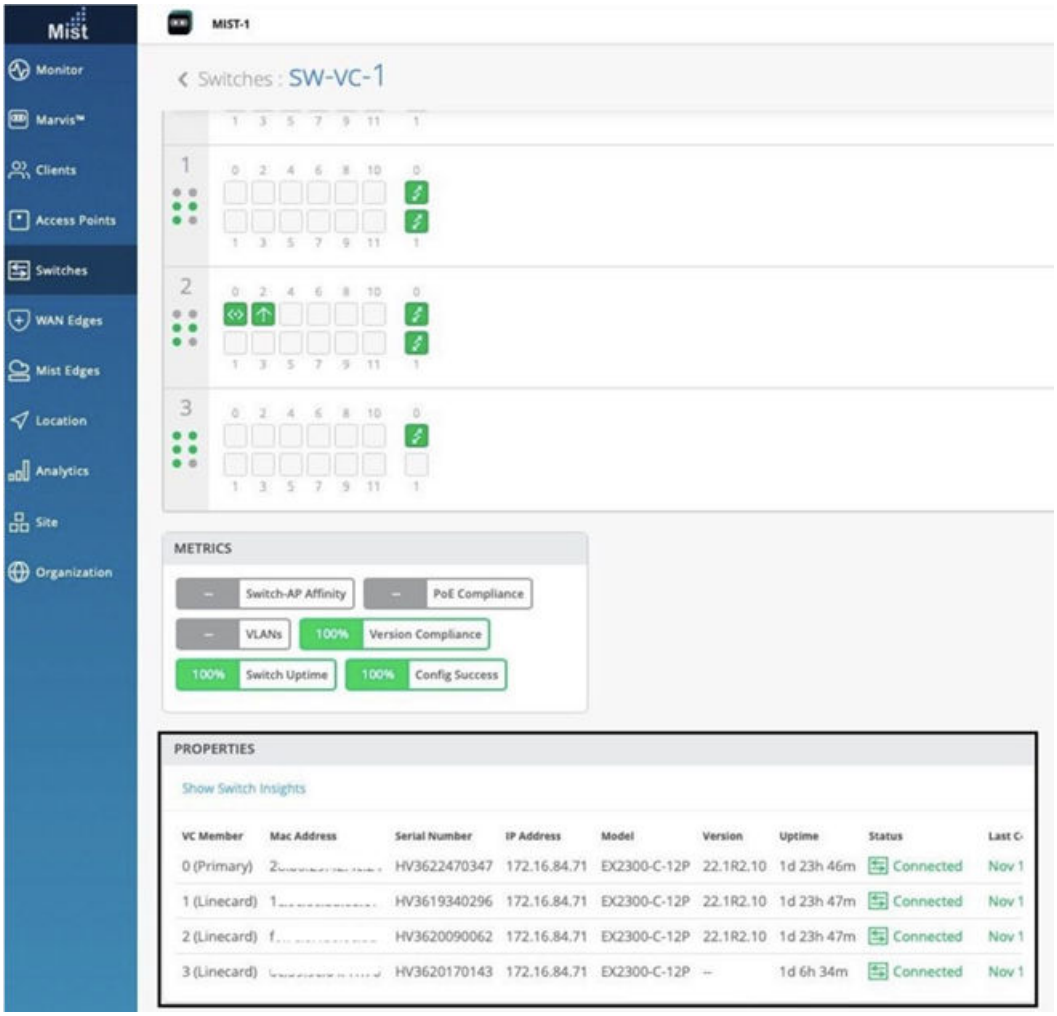
7. Click **Update**.

8. Connect the VCPs as specified on the Modify Virtual Chassis window and wait for 3 to 5 minutes for virtual chassis to be updated.

   While the Virtual Chassis is forming, the switches page displays the status as 'VC Forming'.



9. After Mist updates the Virtual Chassis, the switch details page displays the front panel of all the three Virtual Chassis members.



Preprovision a Virtual Chassis

Before modifying any Virtual Chassis, we recommend that you ensure it is preprovisioned.

The preprovisioned configuration specifies the chassis serial number, member ID, and role for the member switches in a Virtual Chassis. When a new member switch joins the Virtual Chassis, Junos OS compares its serial number against the values specified in the preprovisioned configuration. Preprovisioning prevents any accidental role assignments, or the accidental addition of a new member to the Virtual Chassis. Each role, member ID, addition or removal of members, is under the control of the configuration.

To preprovision a Virtual Chassis:

1. Navigate to the Switches page (switch list) and review the preprovisioning status in the **Preprovisioned VC** column. The Virtual Chassis devices that are not preprovisioned are highlighted with an 'x' mark in red.

2. Click to open the Virtual Chassis that has not been preprovisioned.

The Virtual Chassis (switch) details page appears with a warning message indicating that the device is not yet preprovisioned.

3. Click the **Preprovision** button on the right side of the warning message to go to the Modify Virtual Chassis window.

4. On the Modify Virtual Chassis window, click **Preprovision Virtual Chassis**.
   This action pushes the preprovisioned Virtual Chassis configuration to the device and overwrites the old autoprovision Virtual Chassis configuration pushed to the device during the ZTP process. This option assumes the current positioning of the members and preprovisions them as is.

Packet Capture Examples

Packet capture (PCAP) is a tool that helps you to analyze network traffic and troubleshoot network problems. The packet capture tool captures real-time data packets traveling over the network for monitoring and logging.

You can enable on-demand PCAP on switches that have CloudX running. For the list of switches that support CloudX, refer to "Switch Connectivity Towards Juniper Mist cloud" on page 52.

The PCAP feature captures both control traffic (the traffic handled by the device CPU) and transit traffic (the traffic forwarded by network processors) that pass through switches at a site.

> **NOTE**: To capture transit traffic, a switch must have the secure PCAP feature enabled. Currently, only the EX4400, EX4100, EX4000 switches support this feature. PCAPs capture **only ingress transit traffic**, not egress traffic.

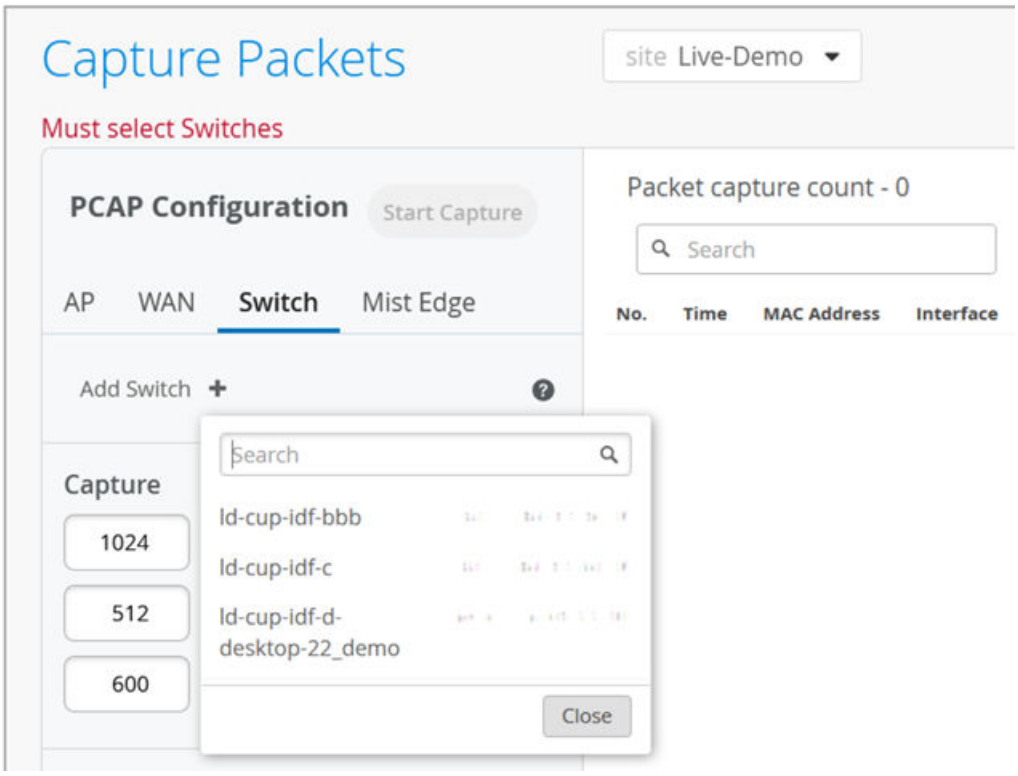
Packets are captured as binary data, without modification. You can read the packet information offline with a packet analyzer such as Wireshark or tcpdump.

To enable PCAP on a switch:

1. Select **Site > Wired > Switch Packet Captures**.

2. Select a site from the **Site** drop-down list.

3. Click the + icon next to the **Add Switch** field and select the switch on which you want to enable packet capture.

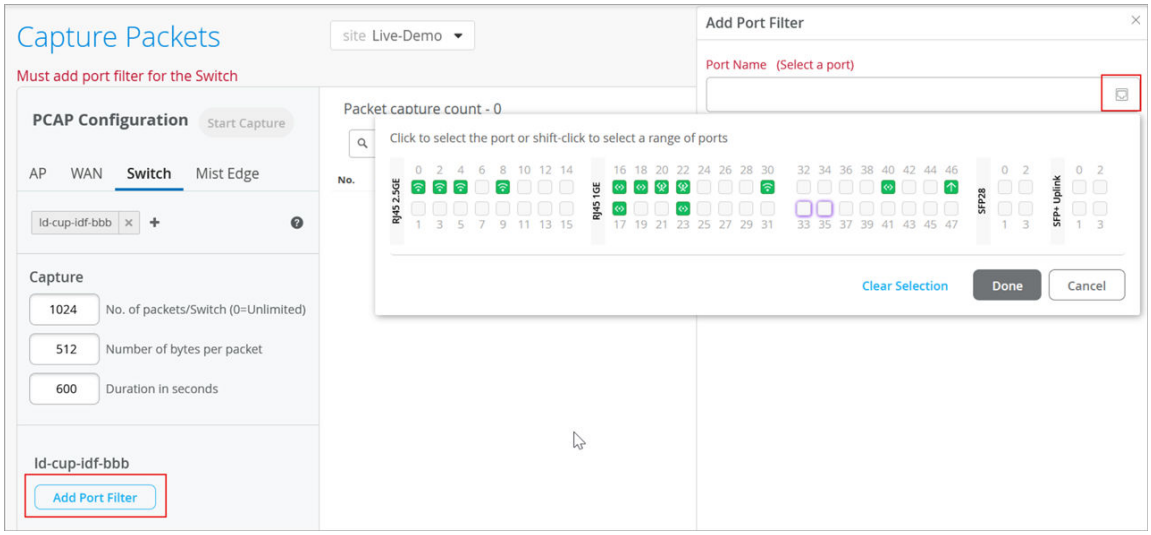


You can select multiple switches for a single packet capture operation.

4. Specify the number of packets captured per switch, packet size in bytes, and the duration of the capture session in seconds.

> **NOTE**: If you specify 0 in the No. of packets/Switch field, unlimited number of packets will be captured.

5. Configure a port filter for packet capture. To do that follow the steps below:
   a. Click **Add Port Filter**.
   b. Click the port icon in the **Port Name** field, select a port on which you want to enable packet capture, and then click **Done**.



NOTE: You can select multiple ports from multiple switches in a single packet capture configuration.

If you want to capture traffic on CPU, select the **Capture Traffic on CPU** check box.

c. Under Advanced filters, specify filters using a tcpdump expression if required.
You can also use the expression builder to build the expression.

d. Click **Save**.

6. Click **Start Capture** to enable packet capture on the selected port.

After the packet capture is complete, you can download the file for inspection. To do that, click **Captured File** on the upper right of the screen. Note that the upload and availability in Juniper Mist cloud can take a few minutes.

For more details about how to view the packet capture in Wireshark, refer to Configure IEEE 802.11 on Wireshark and View Wireless Packet Captures in Wireshark.