Juniper Networks | Engineering Simplicity

Midsize Branch Solution with Juniper Mist Cloud

Published
2021-03-22

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

1

CHAPTER

Using Juniper Mist Cloud to connect Juniper EX switches in a branch office

Midsize Branch Office Overview

IN THIS SECTION

About This Network Configuration Example

This Network Configuration Example (NCE) describes how you can set up the networking and security infrastructure for a midsize branch office. Our solution combines a security gateway, switches, and access points to meet all the requirements for a resilient WAN, LAN, and Wireless LAN (WLAN) connectivity, a secure network, and other services in the branch office. This NCE provides step-by-step configuration for the initial onboarding and provisioning of basic services, such as a DHCP Server, traffic separation in virtual local area networks (VLANs), EX series switch, and Mist-based WLAN configuration. In addition, we cover a plethora of advanced SD-WAN and security services such as advanced policy-based routing (APBR), AppQoE, and SkyATP.

Use Case Overview

The proliferation of 4G LTE cellular networks along with the decreased form factor and affordability of LTE-capable devices are contributing to the rapid deployment of new branch offices. LTE networks provide broadband access to the Internet and help you to avoid the cost of building redundant physical infrastructure at remote office sites. You can also leverage the connectivity of 4G cellular networks as backup connections to locations that already have primary wired connections.

Enterprise networks respond to IT innovations and show their business agility by quickly adopting the software-defined WAN (SD-WAN) technology. The financial benefits of SD-WAN include automated provisioning to improve operational efficiency, lower WAN operational expenditures (OpEx), and lower capital expenditures (CapEx). You can use SD-WAN to optimize application experiences and network performance by prioritizing business-critical applications on the network links that guarantee Quality-of-service (QoS).

Juniper Networks solutions satisfy the following business needs for branch site deployments:

- A solid and cost-effective business continuity plan that ensures continuous business operations even when WAN connectivity is interrupted.
- Data integrity and confidentiality protection.
- Segregated networks for guest and internal users.
- Basic wireless—by using a site survey, you can determine the quantity and placement of wireless access points throughout the office to ensure adequate wireless coverage.
- PoE+ support for desk phones, smart cameras, and wireless access points
- Support up to 50 active client (guests and employees) devices at any given time.
- Manage the connectivity for guest and employee devices. Employees may have multiple devices, like a desk phone, laptop, and smartphone.

Benefits for a Midsize Branch Office Solution.

The midsize branch office solution from Juniper Networks offers a low-cost, low-maintenance, and secure solution using an SRX Series device to provide security, EX4300 family of switches to provide versatility, and Mist access points to provide a stellar wireless experience.

Technical Overview

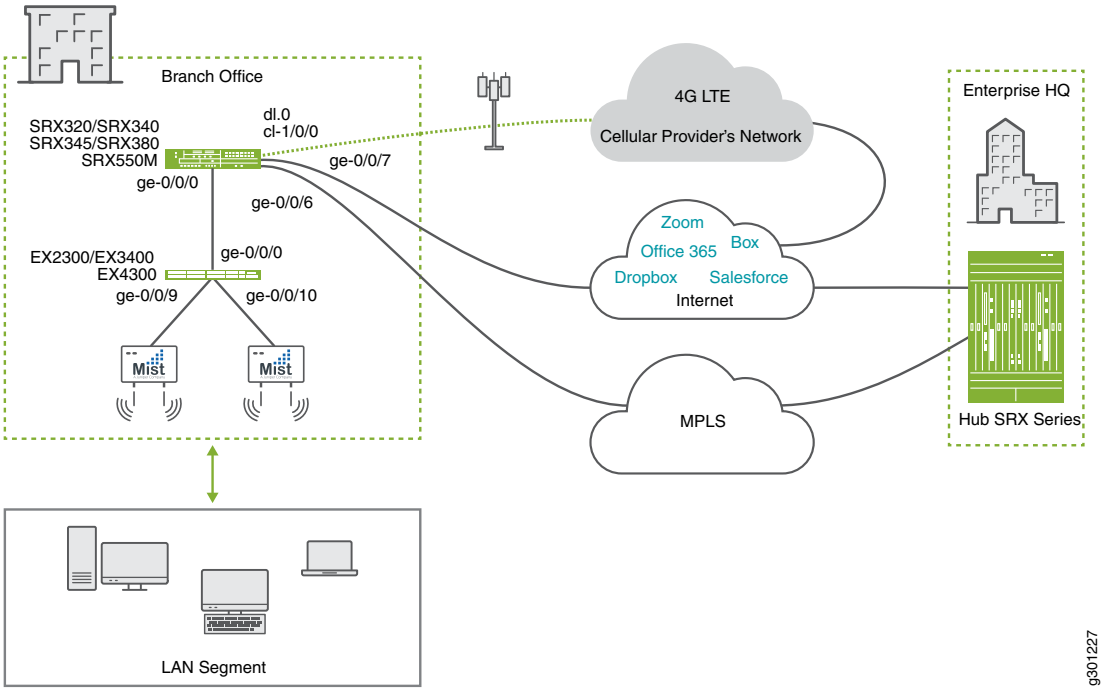
The EX4300 family of switches is a versatile platform that satisfies the demands of an enterprise's campus and branch locations. They support IEEE 802.3af Power over Ethernet (PoE) and IEEE 802.3af PoE+ ports up to 30W. You can interconnect the switches as a single logical device in a virtual chassis to add Ethernet ports as needed and still keep the simplicity of managing a single networking switch. The platform delivers a cost-effective solution for 1GbE or mixed 1GbE/10GbE/40GbE environments that you can tailor to the specific demands of each location.

MIST access points provide the wireless network of tomorrow today. Their built-in AI capabilities enable a self-driving wireless network, which continuously evaluates the state of the network and proactively resolves issues that may jeopardize the stellar user experience.

The SRX Series device brings the next-generation firewall capabilities, 4G LTE, and advanced SD-WAN capabilities. With Junos OS, you can manage all the wired networking equipment using one CLI. Furthermore, Junos OS supports AppQoE, the industry-leading application that monitors primary and secondary wired links on an SRX Series Services Gateway in the branch. If traffic performance in the primary link falls below the acceptable levels specified in the SLA, traffic automatically switches to the secondary link. For added reliability, you can also configure an additional backup cellular wireless LTE connection to the Internet to ensure business continuity if both the primary and secondary links fail.

Figure 1 on page 7 shows a typical branch office setup with connections to corporate headquarters starting from an SRX Series Services Gateway and going over the internet to the headquarters.

Figure 1: Branch Office with Redundant Internet Connectivity



A typical branch office has three independent connections to the Internet.

- Wired connection to the corporate headquarters with guaranteed QoS link. The link is built on an MPLS network.
- Local broadband Internet access.
- Wireless connection with 2G, 3G, or 4G LTE.

The connection to the branch terminates on an SRX Series Services Gateway. The SRX Series Services Gateways provide next-generation firewall (NGFW) capability along with wired and wireless services to onsite employees that include:

- SD-WAN driven access to the Internet
- Next-generation firewall protection
- Antivirus protection
- Enhanced web filtering
- Intrusion prevention
- Advanced application visibility and control

The throughput capacity of the three Internet links is not equal. The primary link (MPLS) provides a lower throughput at a guaranteed quality of service (QoS) compared to the broadband Internet link. The LTE link delivers lower throughput compared to the broadband Internet connection, and it does not have the guaranteed QoS of the MPLS link.

Business-critical applications have priority over all other traffic. They will predominantly use the primary MPLS link which has QoS guarantees. The non-critical applications will use any remaining throughput capacity on the primary and secondary links. LTE is configured as a backup link and becomes active only when both primary and secondary links are down or unavailable. Configurations of the MPLS link and WAN technology are similar to Asymmetric digital subscriber line (ADSL), very-high-bit-rate digital subscriber line (VDSL), and T1/E1 and is beyond the scope of this document.

How to Configure a Midsize Branch Office using Juniper Mist Cloud

Requirements

This example shows how to configure a WAN link in Active/Active mode with an LTE backup link on the SRX300. You'll need the following hardware and software components:

- One SRX300 Series device (SRX320, SRX340, SRX345, SRX380 or SRX550M): Software version: Junos OS Version 19.4R1.
- One EX Series ethernet switch (EX2300, EX3400, or EX4300): Software version: Junos OS Version 19.4R1.
- Two MIST access points (AP12, AP41, AP43, AP61, or AP32).
- One LTE Mini-PIM for the SRX300.
- One SIM card with a subscription for data services.

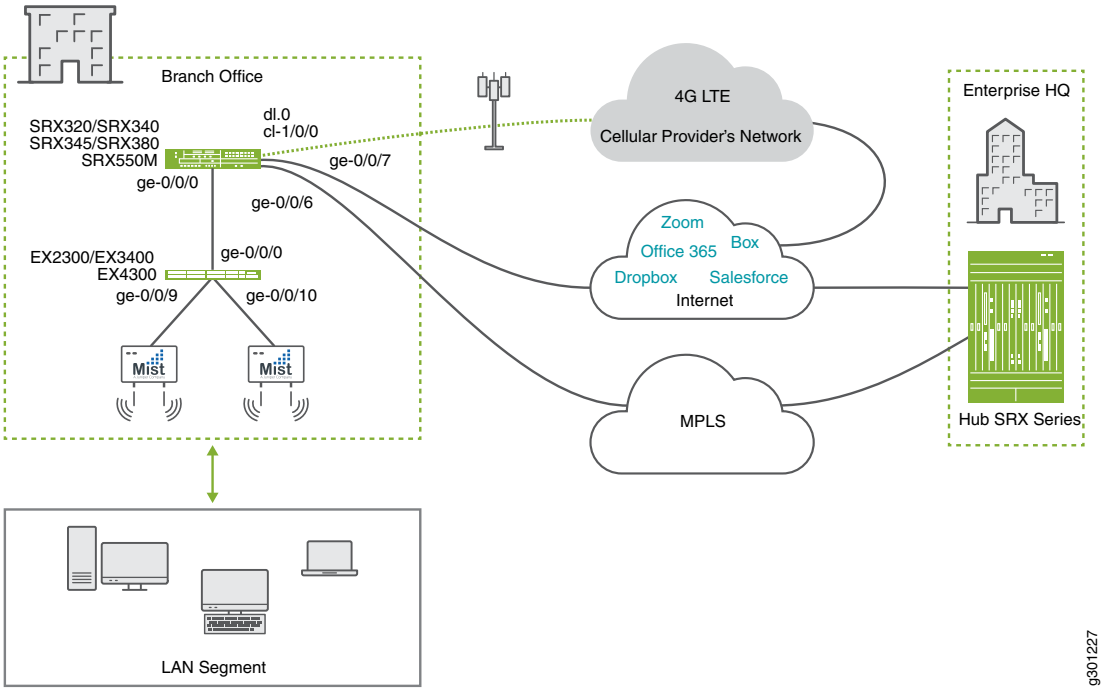
Overview

In this example, we configure an SRX320 to provide the wired and wireless connections for on-site employees to the Internet and Intranet and wireless Internet access to guest devices. The primary link is on an MPLS network, the secondary link is broadband Internet over Ethernet, and the backup link uses an LTE network. The primary and secondary links are configured in Active/Active mode. Traffic is not routed

through the LTE modem unless both the primary and secondary links go down. The switch connects to the SRX device and provides the Layer 2 functionality and ports for the branch. Moreover, you can configure a virtual chassis (VC) with multiple EX2300, EX3400, and EX4300 switches to provide higher port density for the branch. For wireless access, we connect two Juniper access points to an EX switch.

Figure 2 on page 9 shows the branch office topology.

Figure 2: Branch Office with Redundant Internet Connectivity



Our topology has the following hardware layout on the SRX Series device:

- The LTE Mini-PIM is installed in slot 1 on the SRX Series device.
- The SIM card is installed in slot 1 of the LTE Mini-PIM.
- The primary MPLS link is connected to ge-0/0/6 interface.
- The broadband Internet link is connected to interface ge-0/0/7.
- The interface cl-1/0/0 identifies the slot for the modem Mini-PIM.
- The link over the cellular network terminates on interface dl.0.
- The wired ports ge-0/0/6 and ge-0/0/7 receive their IP address, network mask, and default gateway via DHCP.
- The cellular service provider assigns the IP address, network mask, default gateway to the LTE interfaces (cl-1/0/0 and dl.0).

On the EX switch, we have the following layout:

- Interface ge-0/0/0 on the EX switch is connected to interface ge-0/0/0 of the SRX.
- The access points are connected to ports ge-0/0/9 and ge-0/0/10 of the EX switch.

We will configure two security zones, a trusted security zone named **trust** and an untrusted security zone named **untrust**, on the SRX device. By having interfaces in different security zones, we can separate the traffic and mitigate the risks on the corporate intranet. Security zones are used to implement clear and simplified security policies. We host interfaces with access to the Internet in the **untrust** zone and internal interfaces that access the corporate Intranet in the **trust** zone. While there are six VLANs listed, only four are routable. Specifically, we configure four interfaces (VLAN and IP interfaces)—one for each of the four types of devices that are connected in the branch office along with the default VLAN. The VLANs are as follows:

- VLAN1 is the default VLAN used by the SRX device and is configured on all access ports on the switch.
- VLAN10 is used by all wireless traffic, including all of the management traffic of the Juniper access points.
- VLAN20 is used by the IoT devices that are commonly found in buildings, such as lighting and HVAC controllers.
- VLAN30 is used by the surveillance cameras in the office.
- VLAN40 is the wired VLAN used by employee computers and is routed to the corporate Intranet.
- VLAN99 is a wired VLAN that we use as a restricted VLAN for all ports where dynamic profiling is enabled in the switch. It is a non-routable VLAN. Devices initially connect to VLAN99 and once the device is identified by the SRX, it assigns the device to an appropriate VLAN and port.

See Figure 3 on page 10 and Table 1 on page 11 for information on the interfaces, security zones, and security policies that are configured on the SRX for this example.

Figure 3: Security Zones

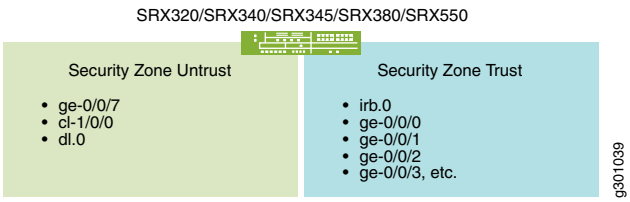


Table 1 on page 11 lists the security policy that you should define and the expected behavior for traffic flows between the trusted and untrusted zones.

Table 1: Security Policies for Zones

From Zone	To Zone	Security Policy Behavior to Allow Traffic
trust	trust	No
untrust	untrust	No
trust	untrust	Yes
untrust	trust	Trust-initiated only.

Table 2 on page 11 lists the VLAN and the IP address information for the interfaces.

Table 2: VLAN and IP Address on the Interfaces

Interface	VLAN ID	IP Address	Network Mask
dl.0	—	DHCP	—
ge-0/0/6	—	DHCP	255.255.255.0
ge-0/0/7	—	DHCP	—
Irb.0	1	192.168.1.1	255.255.255.0
ge-0/0/0.10	10	10.10.10.1	255.255.255.0
ge-0/0/0.20	20	10.10.20.1	255.255.255.0
ge-0/0/0.30	30	10.10.30.1	255.255.255.0
ge-0/0/0.40	40	10.10.40.1	255.255.255.0

Table 3 on page 11 lists the VLANs, usage, and port type used in this example. All other ports on the SRX Series device and EX switch are untagged VLAN ports.

Table 3: VLAN Usage

VLAN	VLAN ID	Name	SRX to EX Port Type	Usage
vlan1	1	Default	untagged	Used by the SRX device and all access ports.

Table 3: VLAN Usage *(continued)*

VLAN	VLAN ID	Name	SRX to EX Port Type	Usage
vlan10	10	WLAN	tagged	Used for wireless traffic. This includes all management traffic for the Juniper access points.
vlan20	20	IoT	tagged	Used by all IoT devices.
vlan30	30	Security	tagged	Used by the surveillance cameras.
vlan40	40	Corporate	tagged	VLAN on the wired Ethernet used by employees.
vlan99	99	Restricted	—	Used in switch ports where a dynamic profile assigns a default restricted VLAN.

Configure the SRX Series Device

Overview

This section shows how to configure the SRX Series device starting logically from the lower layers to the upper layers of the network. We start our configuration on a SRX device with its factory default configuration. Alternatively, you can use the zeroize command to reset the SRX to its factory-default settings.

1. Set the hostname and password for the SRX device. In this example. we use **Mist-SRX-GW** as the hostname

```
set system host-name Mist-SRX-GW
set system root-authentication plain-text-password
```

2. Configure the time zone on the SRX device and add a DNS and NTP server. In this example, we set the time zone to **America/Los_Angeles** and use an IP address of 8.8.8.8 for the DNS server and 216.239.35.12 for the NTP server.

```
set system time-zone America/Los_Angeles
set system name-server 8.8.8.8
set system ntp server 216.239.35.12
```

3. Create the four VLANs for the four types of branch office devices that will connect to the corporate intranet and the VLAN for the access points. See Table 3 on page 11.

```
set vlans vlan10 vlan-id 10
set vlans vlan20 vlan-id 20
set vlans vlan30 vlan-id 30
set vlans vlan40 vlan-id 40
```

4. Configure the interface (ge-0/0/7) as the primary Internet link and set the interface to be a DHCP client.

```
set interfaces ge-0/0/7 unit 0 description "WAN Interface 1 - Primary"
set interfaces ge-0/0/7 unit 0 family inet dhcp vendor-id Juniper-srx320
```

5. Configure the modem interface (LTE-MPIM) and activate the slot seated with the SIM card.

```
set interfaces cl-1/0/0 description “WAN Interfaces 2 – Backup”
set interfaces cl-1/0/0 dialer-options pool 1 priority 100
set interfaces cl-1/0/0 act-sim 1
set interfaces cl-1/0/0 cellular-options sim 1 radio-access automatic
```

6. Configure the dialer interface.

```
set interfaces dl0 unit 0 family inet negotiate-address
set interfaces dl0 unit 0 family inet6 negotiate-address
set interfaces dl0 unit 0 dialer-options pool 1
set interfaces dl0 unit 0 dialer-options dial-string “*99”
```

7. Create a security policy to allow traffic between the trusted and untrusted zones. Be sure to include the desired network segments and applications in the policy.

```
set security policies from-zone trust to-zone untrust policy allow-in-zone match
 source-address 192.168.1.0/24
set security policies from-zone trust to-zone untrust policy allow-in-zone match
 source-address 10.10.10.0/24
```

```
set security policies from-zone trust to-zone untrust policy allow-in-zone match
 source-address 10.10.20.0/24
set security policies from-zone trust to-zone untrust policy allow-in-zone match
 source-address 10.10.30.0/24
set security policies from-zone trust to-zone untrust policy allow-in-zone match
 source-address 10.10.40.0/24
set security policies from-zone trust to-zone untrust policy allow-in-zone match
 destination-address any
set security policies from-zone trust to-zone untrust policy allow-in-zone match
 application any
set security policies from-zone trust to-zone untrust policy allow-in-zone then
 permit
```

8. Configure the SRX device to allow the EX switch to obtain an IP address from the DHCP pool and to connect to the Internet. This allows the EX switch to connect to Juniper Mist Cloud. Modify the security policy to allow ICMP ECHO (ping) and DHCP service messages in the trusted security zone and add the irb.0 interface to the security zone.

   NOTE: We configure DHCP services later in the document as part of the"Application Quality of Experience on a SD-WAN" on page 39.

```
set security zones security-zone LAN-NETs host-inbound-traffic system-services
 ping
set security zones security-zone trust host-inbound-traffic system-services dhcp

set security zones security-zone LAN-NETs interfaces irb.0
 set interfaces irb unit 0 family inet address 192.168.1.1/24
```

9. Configure the system logs that we will need to collect from the SRX device. In this example, we set the maximum size of the Syslog to 100KB, keep the 3 most recent files only, set the files readable by all users, and add all emergency log messages related to users to the syslog.

   In addition, we configure other system logs to capture interactive commands and session status using the following syslog messages:

Messages	Syslog file Name	File Size
Severity level messages from all facilities Severity level messages from the authorization facility	LOG-Messages	100 KB

Messages	Syslog file Name	File Size
Any severity level message from the interactive commands facility	LOG-Interactive-Commands	
RT_FLOW_SESSION_CREATE events	LOG-Accepted-Traffic	1 MB
RT_FLOW_SESSION_DENY	LOG-Blocked-Traffic	1 MB
RT_FLOW	LOG-Sessions	1 MB

```
set system syslog archive size 100k
set system syslog archive files 3
set system syslog archive world-readable
set system syslog user * any emergency
set system syslog file LOG-Messages any notice
set system syslog file LOG-Messages authorization info
set system syslog file LOG-Interactive-Commands interactive-commands any
set system syslog file LOG-Accepted-Traffic any any
set system syslog file LOG-Accepted-Traffic match RT_FLOW_SESSION_CREATE
set system syslog file LOG-Accepted-Traffic archive size 1m
set system syslog file LOG-Accepted-Traffic archive files 3
set system syslog file LOG-Blocked-Traffic any any
set system syslog file LOG-Blocked-Traffic match RT_FLOW_SESSION_DENY
set system syslog file LOG-Blocked-Traffic archive size 1m
set system syslog file LOG-Blocked-Traffic archive files 3
set system syslog file LOG-Sessions any any
set system syslog file LOG-Sessions match RT_FLOW
set system syslog file LOG-Sessions archive size 1m
set system syslog file LOG-Sessions archive files 3
```

10. Commit the configuration

```
commit and-quit
```

11. Set the Access Point Name (APN) for the SIM in the modem (LTE-MPIM).

```
request modem wireless create-profile profile-id 10 access-point-name broadband
 cl-1/0/0 slot 1
```

At this point, the SRX device is providing Internet access to the EX switch and the Juniper access points. Once the EX switch and Juniper access points are configured, we will modify the configuration on the SRX to accommodate the trunk ports that are connected to the EX switch.

Results

WARNING: To avoid using an additional cable during configuration, you must follow the instructions as detailed. When we configure the SRX interfaces as trunk ports to the EX switch, the switch will lose access to the Internet. We restore the Internet connection on the SRX later in this document.

Configure the EX Series Switch in the Juniper Mist Cloud

Overview

With Juniper Mist cloud services, you can use Juniper Mist Wired Assurance to centrally manage all your Juniper switches. Juniper Mist Wired Assurance gives you full visibility on the devices that comprise your network's access layer.. The Juniper Mist portal provides a user interface to access your architecture through the AI-driven cloud services with your Juniper Mist account. You can monitor, measure, and get alerts on key compliance metrics on the wired network including switch version compliance, PoE compliance, switch-AP affinity, and VLANs insights. Juniper switches and Juniper access points (APs) combine to support dense, heavily utilized networks that can host a large number of mobile devices, and provide end-user security with reliable performance.

We group the adoption and management of EX Series Switches into three categories:

- **Day 0** represents zero-touch and single-click activation for adopting new and existing switches into the Juniper Mist Cloud.
- **Day 1** represents template-based configuration for managing switch configurations across the organization, multiple site, or individual switches.
- **Day 2** represents ongoing switch insights and intelligence, leveraging the Marvis Virtual Network Assistant driven by Mist AI.

How to Activate a Greenfield Switch

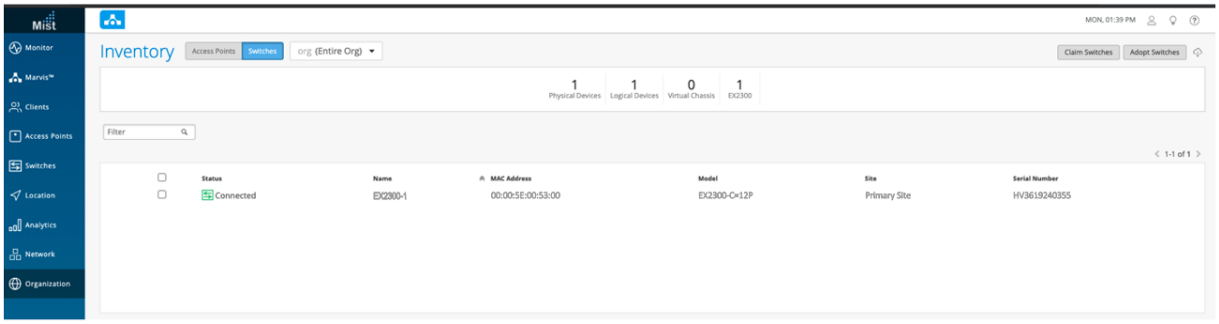
To adopt a cloud-ready switch (greenfield switch) manually, you need an activation code for the switch. Activation codes are sent by e-mail to the address on record at the time of purchase. You can also contact the Juniper Mist Customer Engagement team to get your activation code. Using the activation code adopts the switch and any Juniper access points that are part of the purchase order, as well as claims any subscriptions that are included in your purchase. A cloud-ready switch comes with the claim code and cloud ready sticker on the packaging box and with a QR code on the front or back of the switch depending on the model type.

Figure 4: Cloud-ready switch and QR code

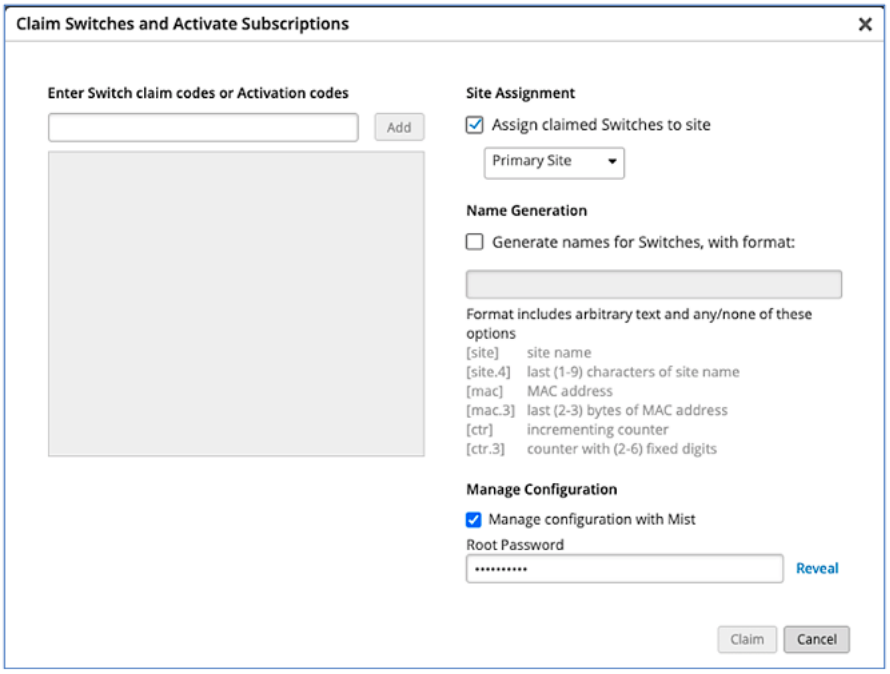
Step-by-Step Procedure

This procedure describes how to manually add a cloud-ready switch to the Juniper Mist Cloud.

1. Use a Web browser to log in to your Juniper Mist account. The Monitor page appears, showing an overview of the Juniper Mist cloud and any Juniper access points and clients that are already connected. Click on **Organization > Inventory** in the menu on the left to open the Juniper Mist Inventory Screen.



2. Select **Switches** at the top of the Inventory screen, and click the **Claim Switches** button and enter the activation code or claim code for the switch.



3. Complete the fields on the screen. Select the **Manage configuration with Mist** check box and enter a root password for the switch. Note that this choice puts the switch under the management of the Juniper Mist portal. As such, we recommend that local configuration using the CLI be restricted to prevent conflicts (for example, you might want to create a system login message on the switch to warn against making configuration changes locally, from the CLI).

NOTE:

4. Unbox your switch, connect the management port of the switch to the Internet, and power it on. As part of the zero touch provisioning (ZTP) process, the switch automatically accesses the phone home server (PHS) and connects to the Juniper Mist Cloud for configuration updates.

   Once the ZTP process resolves, the switch automatically appears in the Inventory page. If the switch does not appear after a few minutes, despite refreshing the web page, try logging out and then logging back in. If you still do not see the switch, see "Troubleshooting" on page 21 for information about how to confirm whether the device is connected to the cloud.

How to Activate a Brownfield Switch

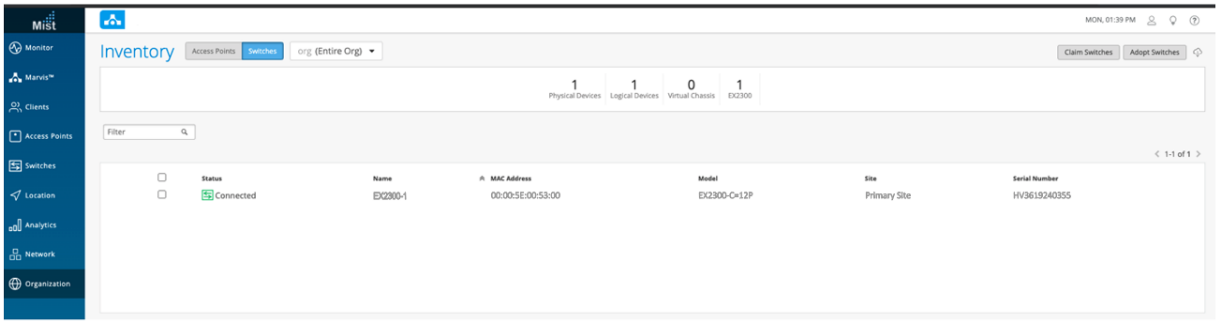
Brownfield switches are switches being brought into the Juniper Mist Cloud from a previous deployment. We recommend that you back up the existing configuration on the switch before getting started. To prevent users from using the CLI to configure the switch after it has been adopted into the Juniper Mist Cloud, you may also want to create a system login message on the switch to warn against making configuration changes, or you can restrict their management access altogether by changing the password or placing restrictions on the CLI user accounts.

How to Manually Add a Brownfield Switch to the Juniper Mist Cloud

Step-by-Step Procedure

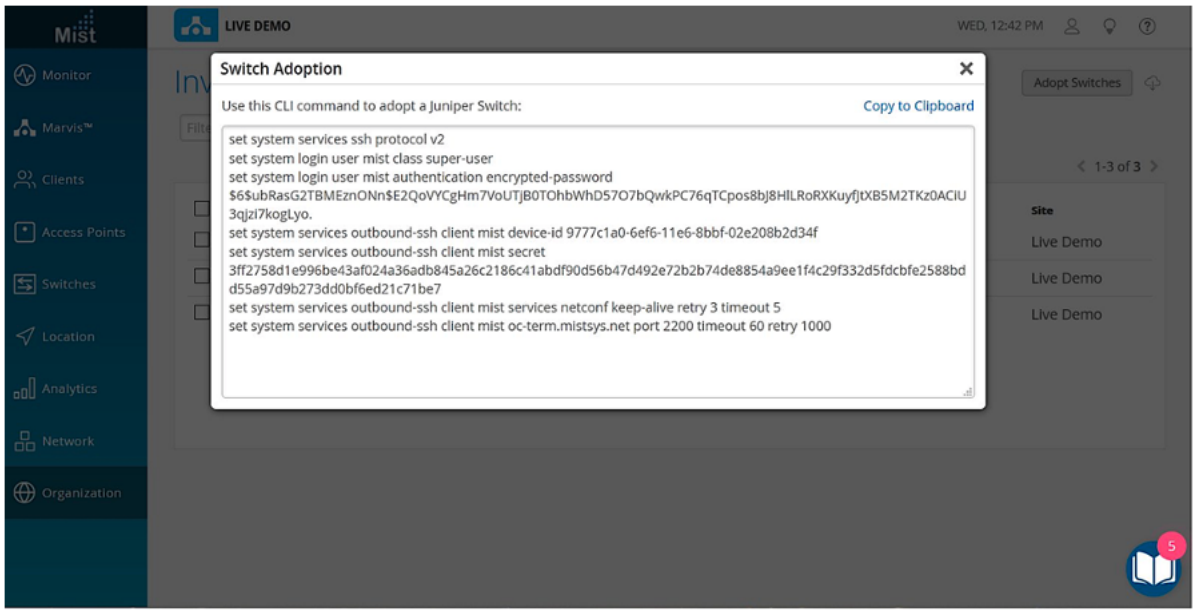
This procedure describes how to set up a secure connection between a supported EX Series switch running a supported version of Junos OS. Be sure you can log in to both the Juniper Mist portal and the switch since you will be making configuration changes to both systems.

1. Log in to your organization on Juniper Mist Cloud Click **Organization > Inventory** to open the Inventory screen.



2. Select **Switches** at the top of the Inventory screen and then click **Adopt Switches** 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 an SSH connection to the Juniper Mist Cloud over TCP port 2200 (This is the TCP port value used for the management session that is used for configuration updates and sending telemetry data).



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

4. On the console of the switch, type **configuration** to enter 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. On the Juniper Mist portal, click **Organization > Inventory > Switches** and select the switch you just added.

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

7. Confirm your connection from the switch to the Juniper Mist Cloud in the Junos CLI by typing **show system connections**.

```
user@host> show system connections | grep 2200
0
tcp4  0 0 10.10.70.89.63208  <ip-address>.2200  ESTABLISHED
```

The output shows that the switch established a connection to the Juniper Mist Cloud. It includes the IP Address of the management interface, the IP address of the Juniper Mist Cloud and the connection status.

Troubleshooting

Confirm your connection from the switch to the Juniper Mist Cloud by running the Junos OS command below on your switch console.

```
user@host> show system connections | grep 2200
```

The command output shows the switch connection to the Juniper Mist Cloud. It includes the IP address of the management interface on the switch, the destination IP address of the Juniper Mist Cloud, and the connection result.

```
tcp4  0 0 10.10.70.89.63208  <ip-address>.2200   ESTABLISHED
```

If you do not see the switch in the Inventory list, the SRX may be blocking the acknowledgment messages for the initial connection request. If the SRX is blocking the inbound packets over TCP port 2200, add a firewall rule to enable communication on port 2200. The switch will appear in **Organization > Inventory > Switches**.

Day 1: Use a Template-Based Configuration with Device and Port Profile

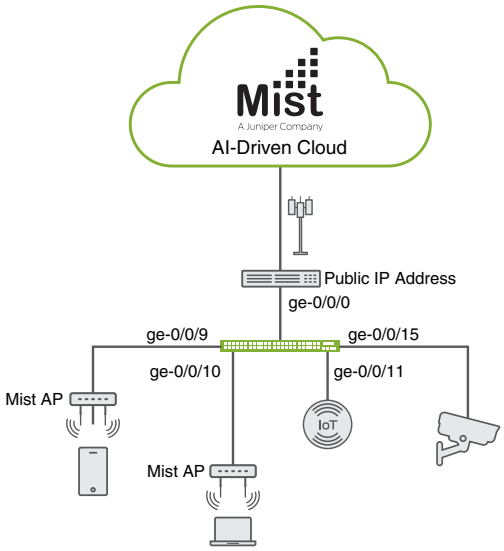
Overview

A key feature of switch management through the Juniper Mist Cloud is the ability to use configuration templates and a hierarchical model to group switches and to make bulk updates. Using templates allows you to have consistent configurations across the organization and to conveniently apply them with granularity to a particular switch as well as at scale across your entire network.

You can create a template configuration and then apply those settings to all the devices in a group. When a conflict occurs, the more narrow settings override the broader settings. For example, when there are settings at both the branch and organizational levels that apply to the same device, the more narrow settings (in this case, branch) override the broader settings that are defined at the organization level.

Figure 5 on page 22 shows the configured network behind the SRX device.

Figure 5: Network Behind the SRX Device



Devices	Ports	VLAN
Mist AP	ge-0/0/0-10	10, 11, 12
IOT Devices	ge-0/0/11-14	20
Camera	ge-0/0/15-18	30
Access Ports	ge-0/0/19-20	40
Uplink	ge-0/0/0	Trunk
Switch Management	ge-0/0/23	99

g301242

Procedure

The following procedure configures the EX switch based on this configuration example.

Step-by-Step Procedure

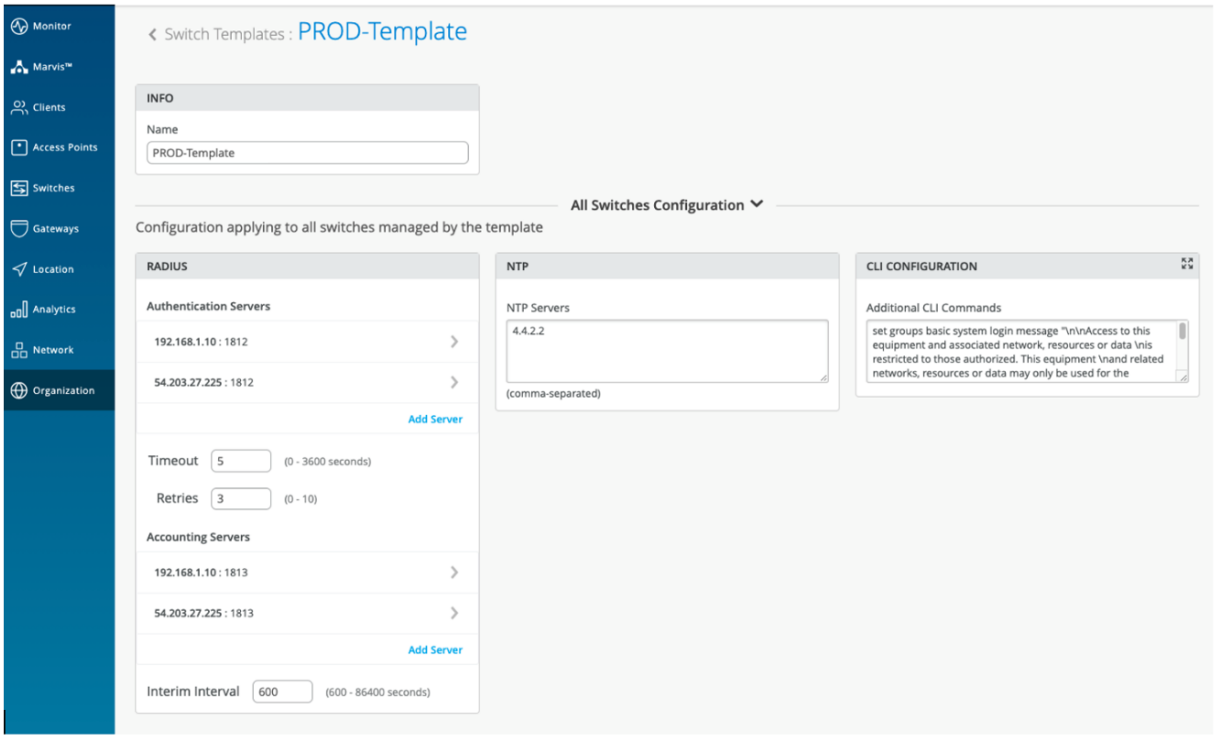
1. To create a Switch Configuration template, click on **Organization > Switch Template** in the menu on the left. In the Switch Configuration template, we define the standard configurations that are used for all the switches in the branch. For this example, we will take the following actions:

   Click on the headings (All Switches Configuration, Shared Elements, and Select Switches Configuration) to expand the configuration and the down arrow to collapse the configuration.

   a. Under All Switches Configuration, we will add the following:

      - Under RADIUS, add a RADIUS server for the organization or branch.

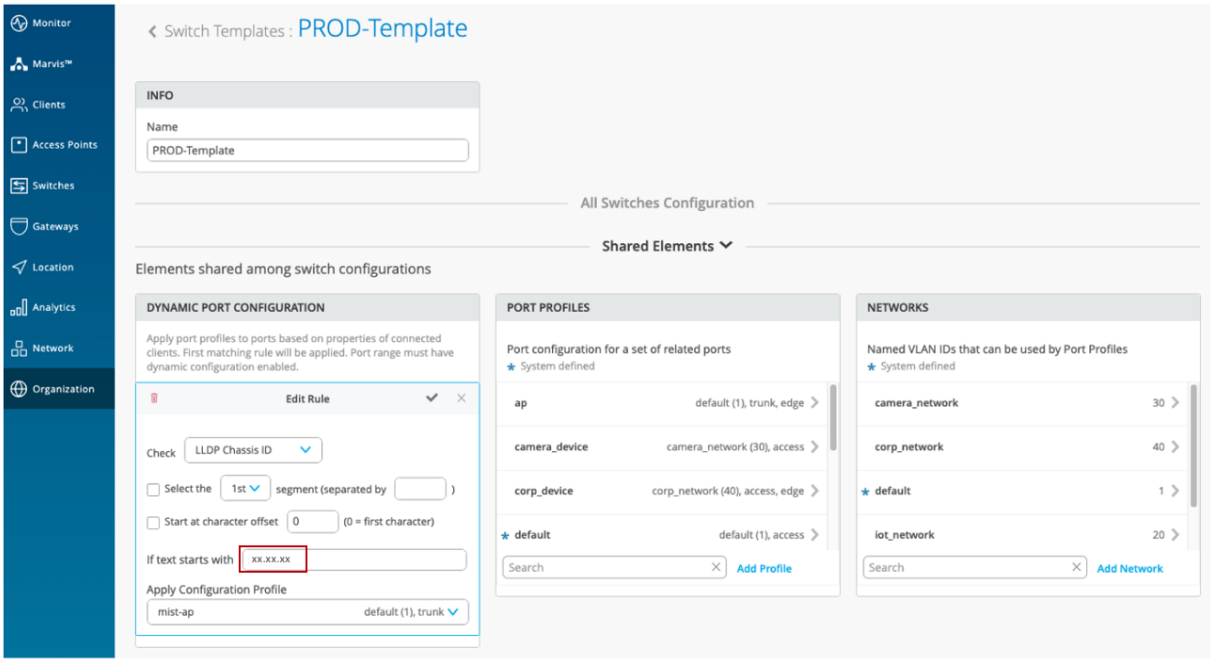
- Under NTP, add the NTP server for the branch.



b. Under Shared Elements, we will add the following:

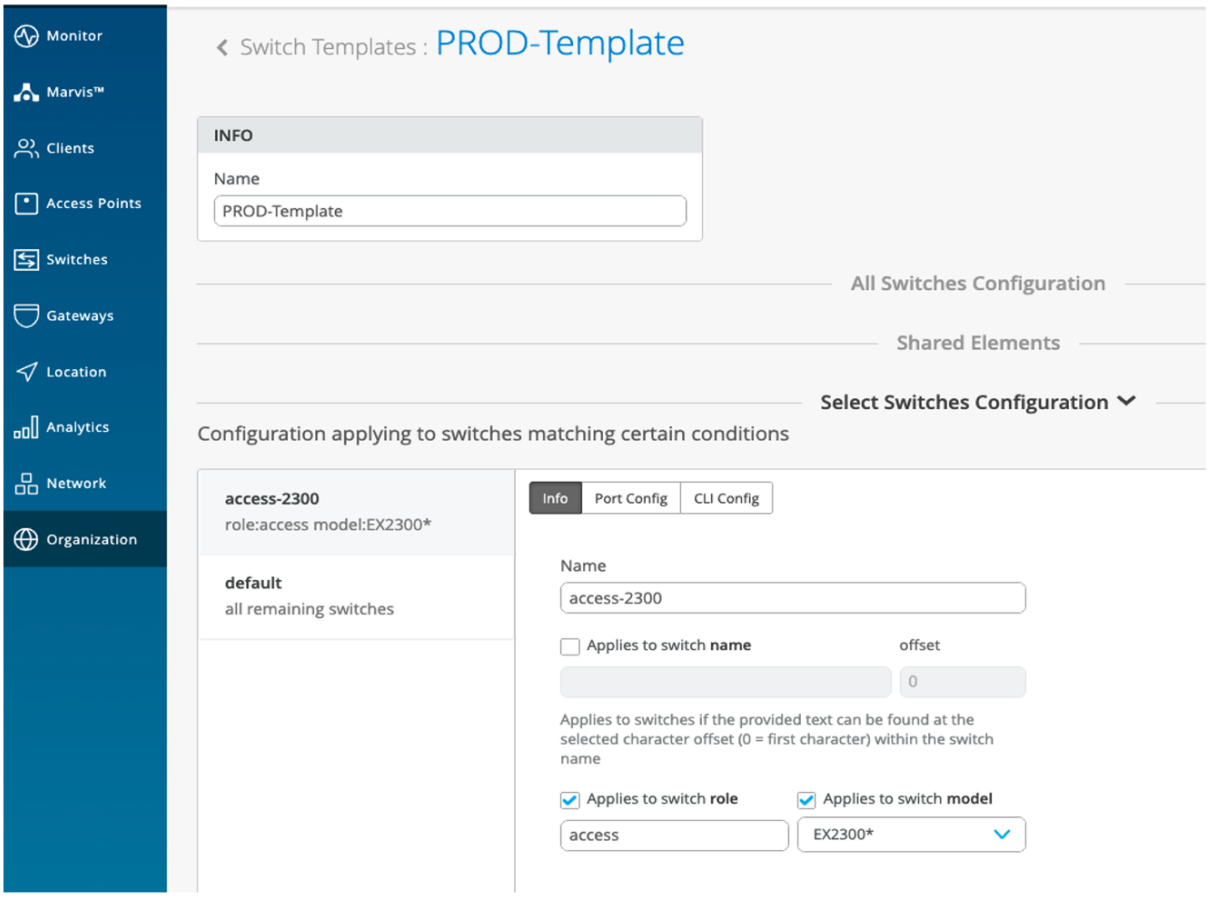
- Under Networks, add the VLANs for the branch—vlan10 (native VLAN for access points), vlan20 (IoT network), vlan30 (Security Network), vlan40 (Corporate Network) and vlan99 (Restricted).
- Under Port Profiles, create the new port profiles, such as ”mist_ap”, camera_device” and “corp_device,” for the related port and map the port profiles to the above VLAN.
- Under Dynamic Port Configuration, create a rule that assigns the port profile “mist_ap” to Juniper access points automatically. Our rule uses LLDP to detect the chassis ID and when it identifies a device where the first three octets of the MAC addresses match our Juniper access points, it

assigns the device to the Juniper access point profile that was created. In the figure below, we use “xx-xx-xx” as an example.

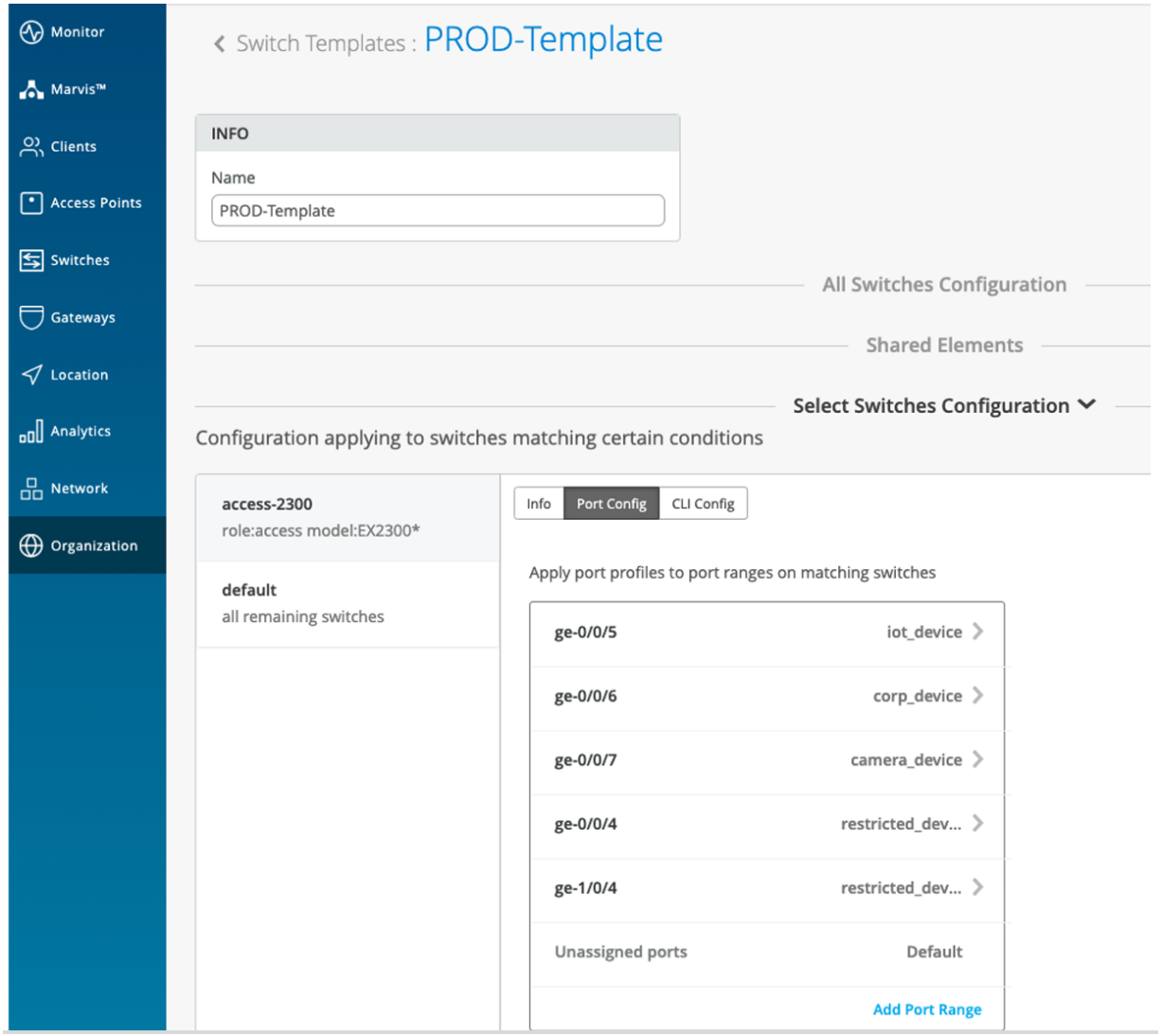


c. Under Select Switches Configurations, we will add the following:

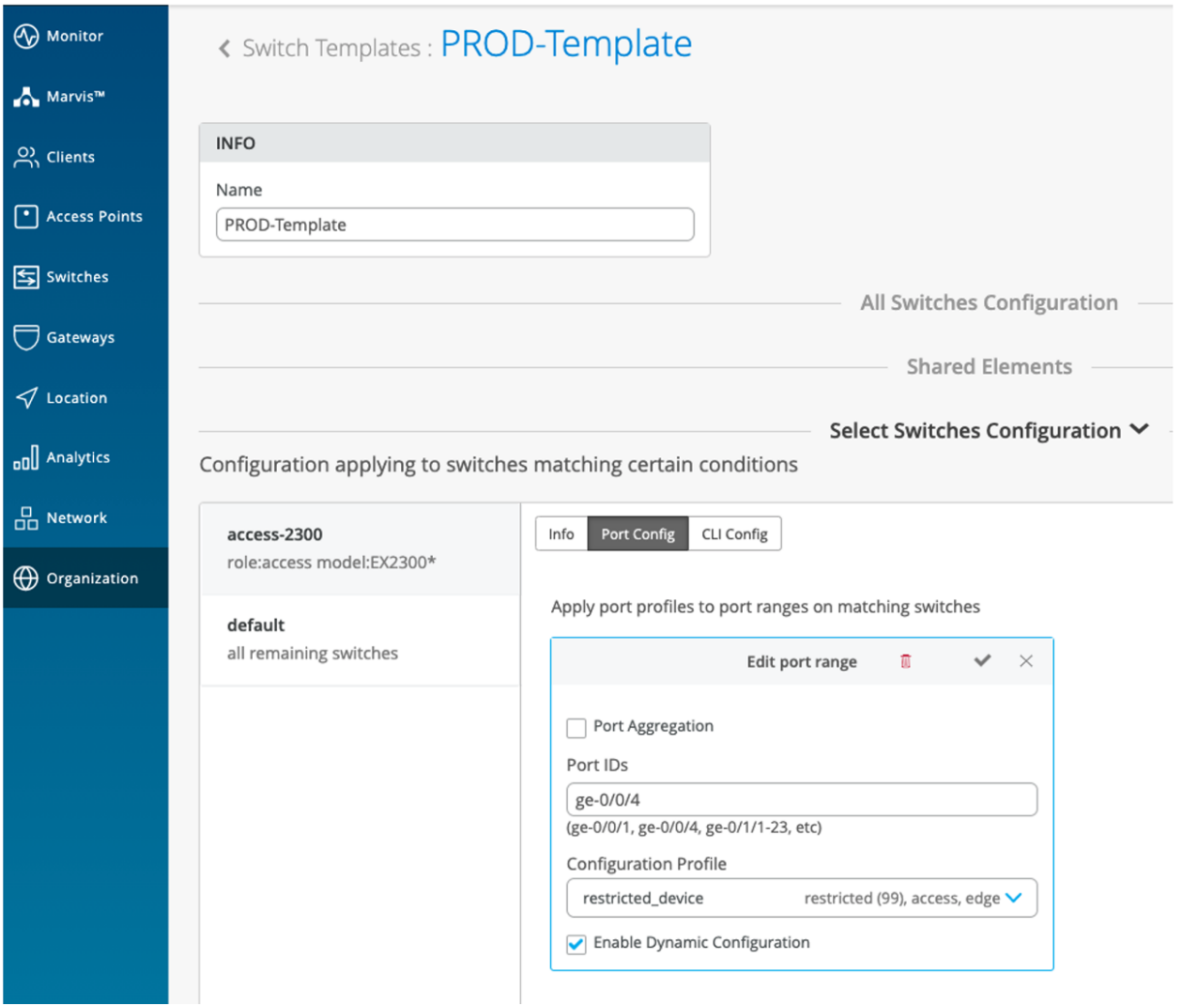
- Under Port Configuration Rules, define the port configuration rules and map the port profiles to the physical ports in the switch. Create a rule to associate the port profile with your switches, in the example we have an EX2300 switch with a role of “access.”



- Map the port profiles to physical ports in the switch

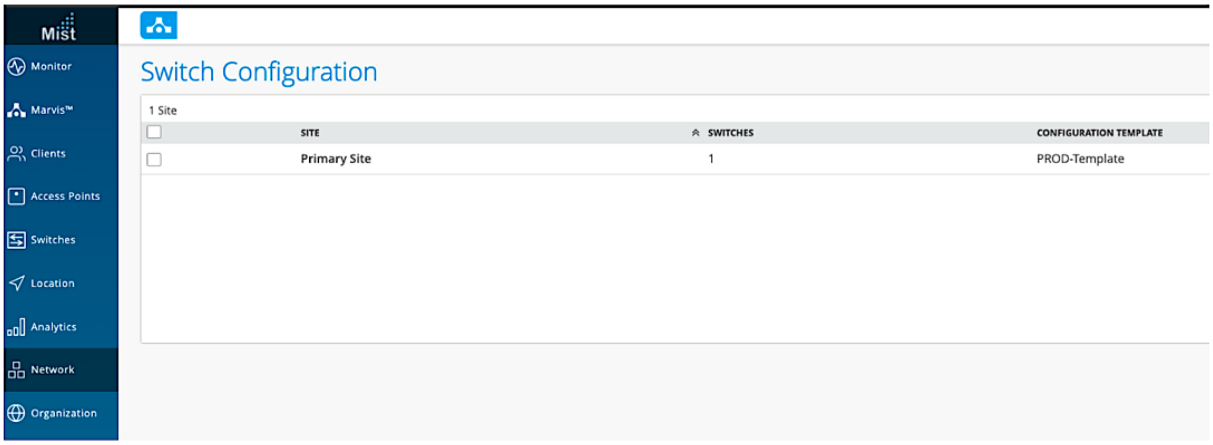


- Enable the dynamic port profile assignment by mapping the switch port to a “restricted_device” profile. This maps a port profile to a VLAN with restricted access and enables “Dynamic Configuration.”

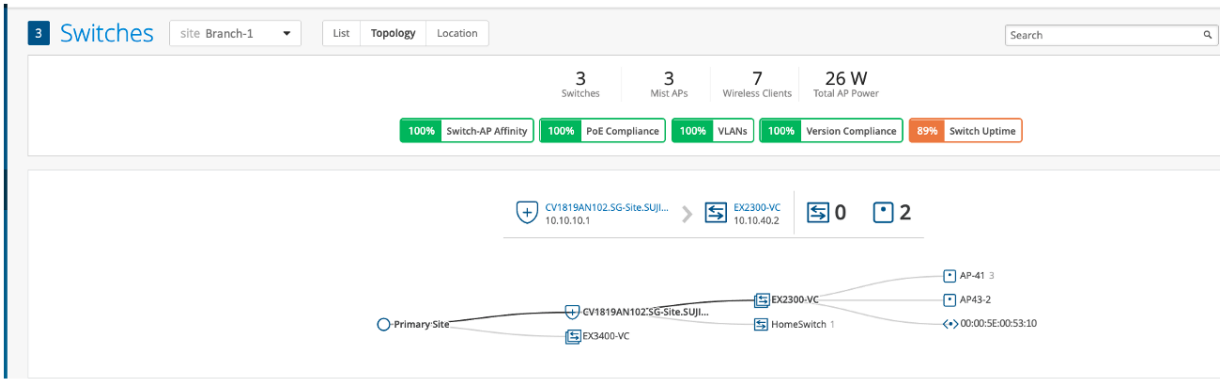


If you have features that are not supported on the Juniper Mist Cloud, you can include the statements in the CLI configuration text box.

2. To map the switch template that you created to your site, click **Network > Switch Configuration** in the menu on the left. Select the check box next to your site and click the **Assign to Template** link to map the “PROD-Template” to your site.

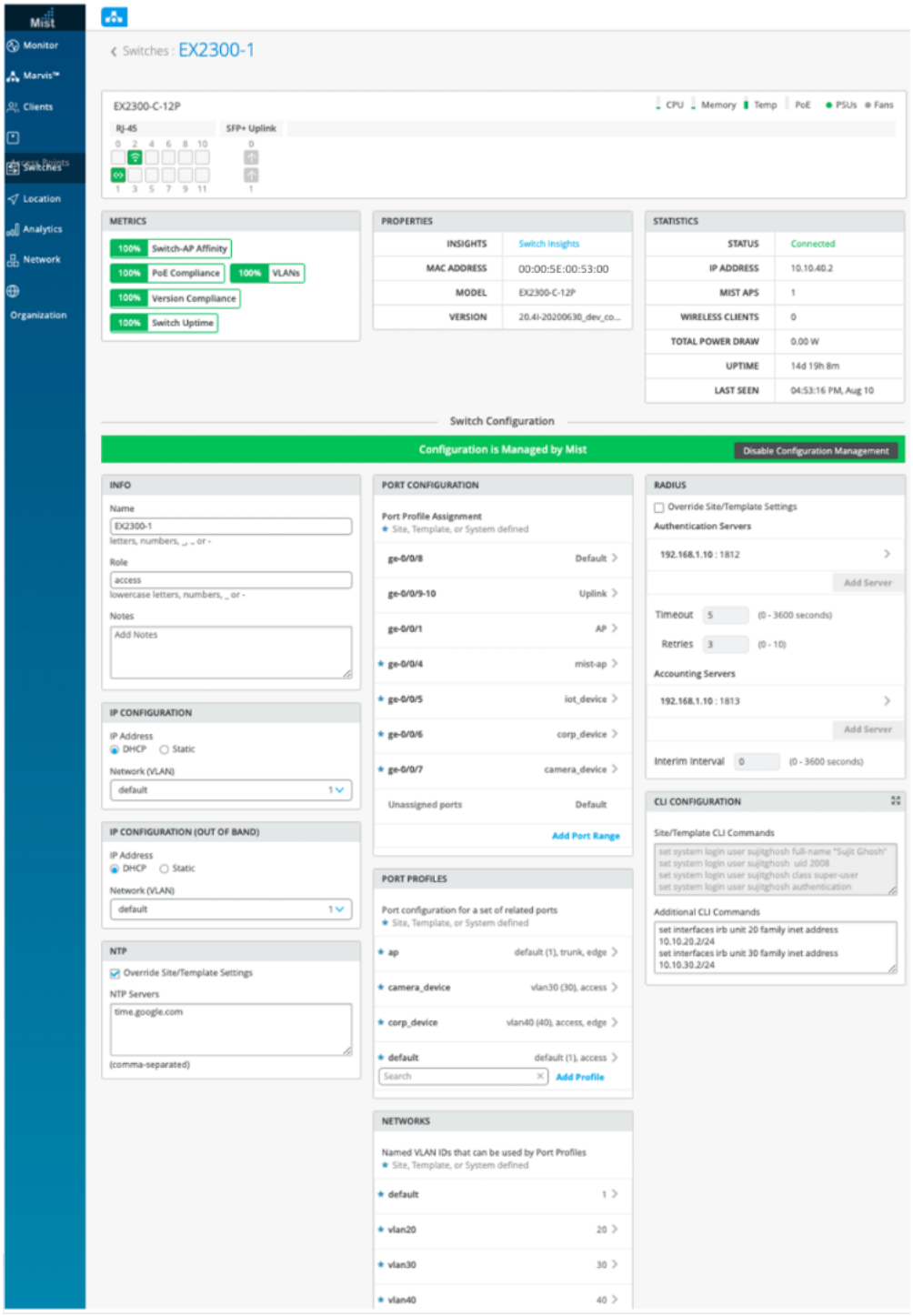


3. To configure devices at the branch office, click **Switches** in the menu on the left, select **Primary Site** and add the switch to the primary site. In this example, the Primary Site is the branch office.



Click on each switch for more details. The switch inherits its configuration from the template. If you want to override any of the settings, you can include additional CLI commands at the switch level.

Additional CLI commands are combined with the template configuration commands and then sent to the switch.



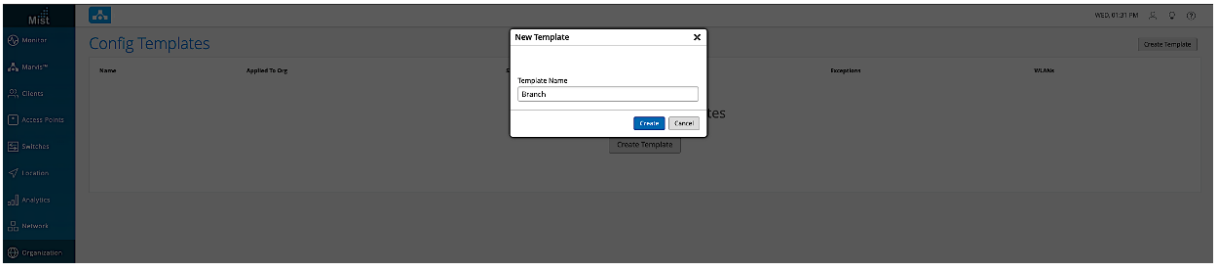
Wireless Configuration on the Juniper Mist Cloud

Juniper Mist Wi-Fi Assurance, driven by machine learning on Juniper Mist, replaces manual troubleshooting tasks with automated wireless operations. This subscription service makes WLANs predictable, reliable, and measurable with unique visibility into user service levels. You can set up and track service-level thresholds for key wireless criteria connection metrics, such as time to connect, capacity, coverage, and throughput.

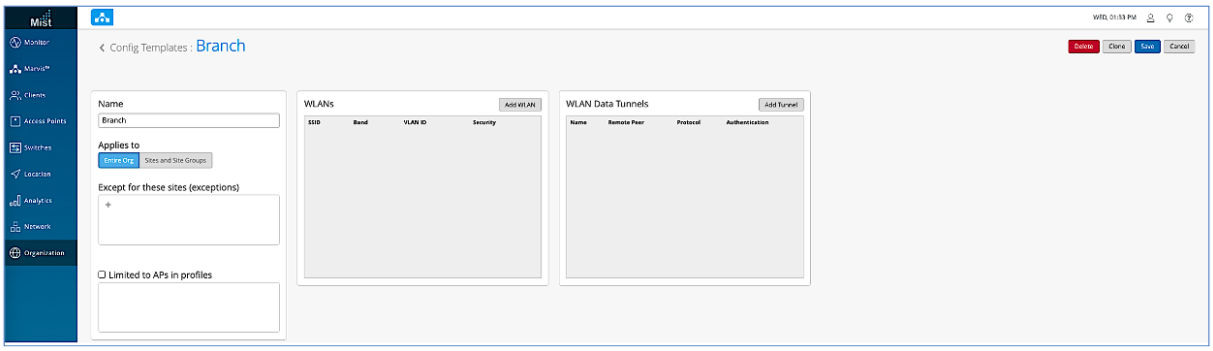
Juniper Mist Wi-Fi Assurance provides the industry's most scalable guest access solution with flexible options including multiple language support, customizable branding, social login, external captive portal integration, and AAA/RADIUS integration.

Step-by-Step Procedure

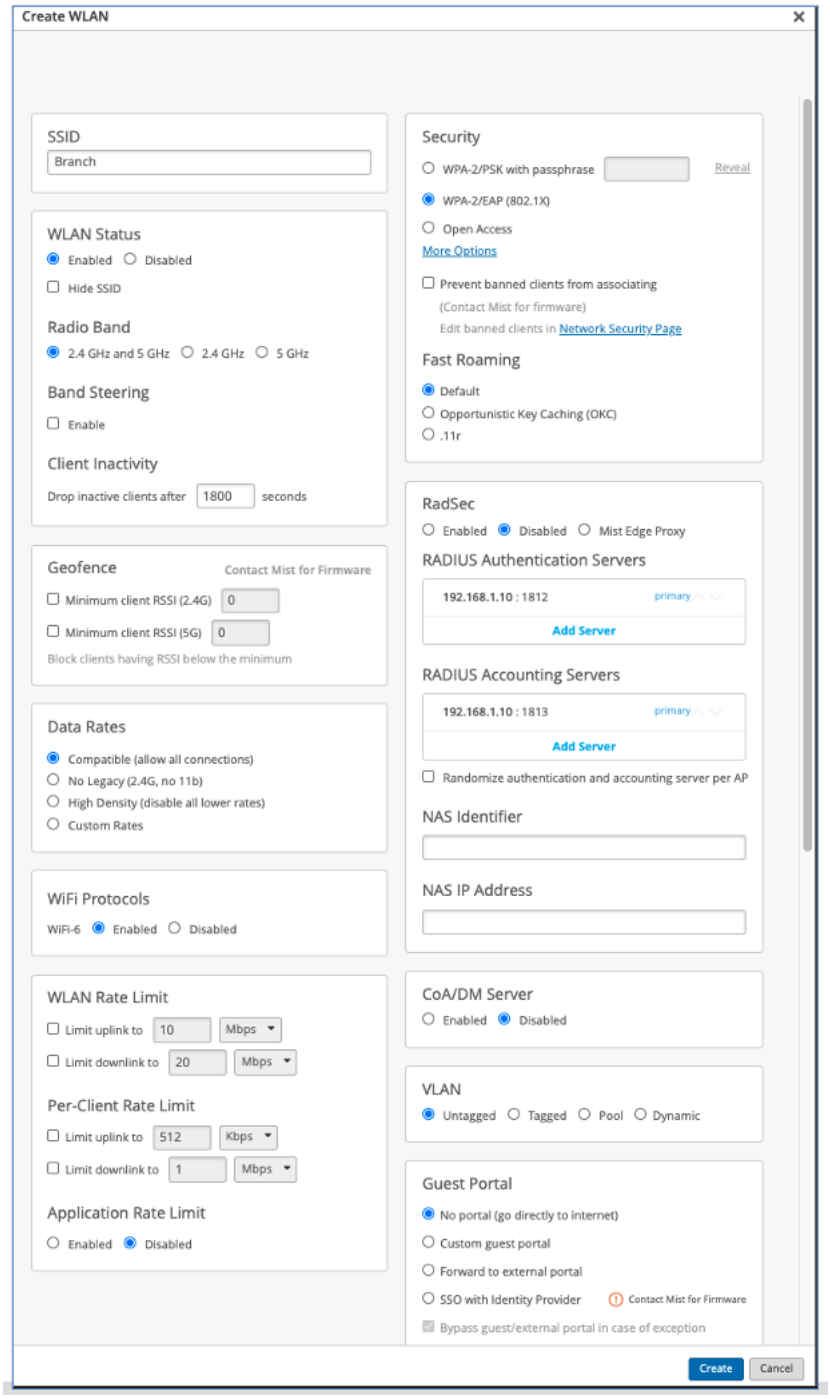
1. To create the templates for the branch office, click **Organization > Config Templates** in the menu on the left.



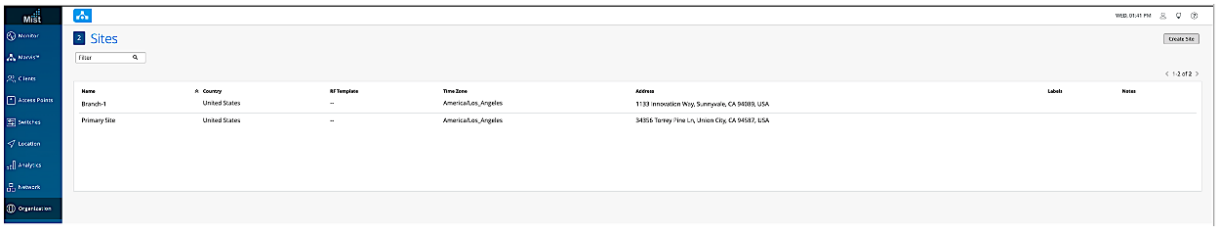
2. Select whether you want to apply the template to the entire organization or to specific sites. For this example, we apply our configuration to the entire organization.



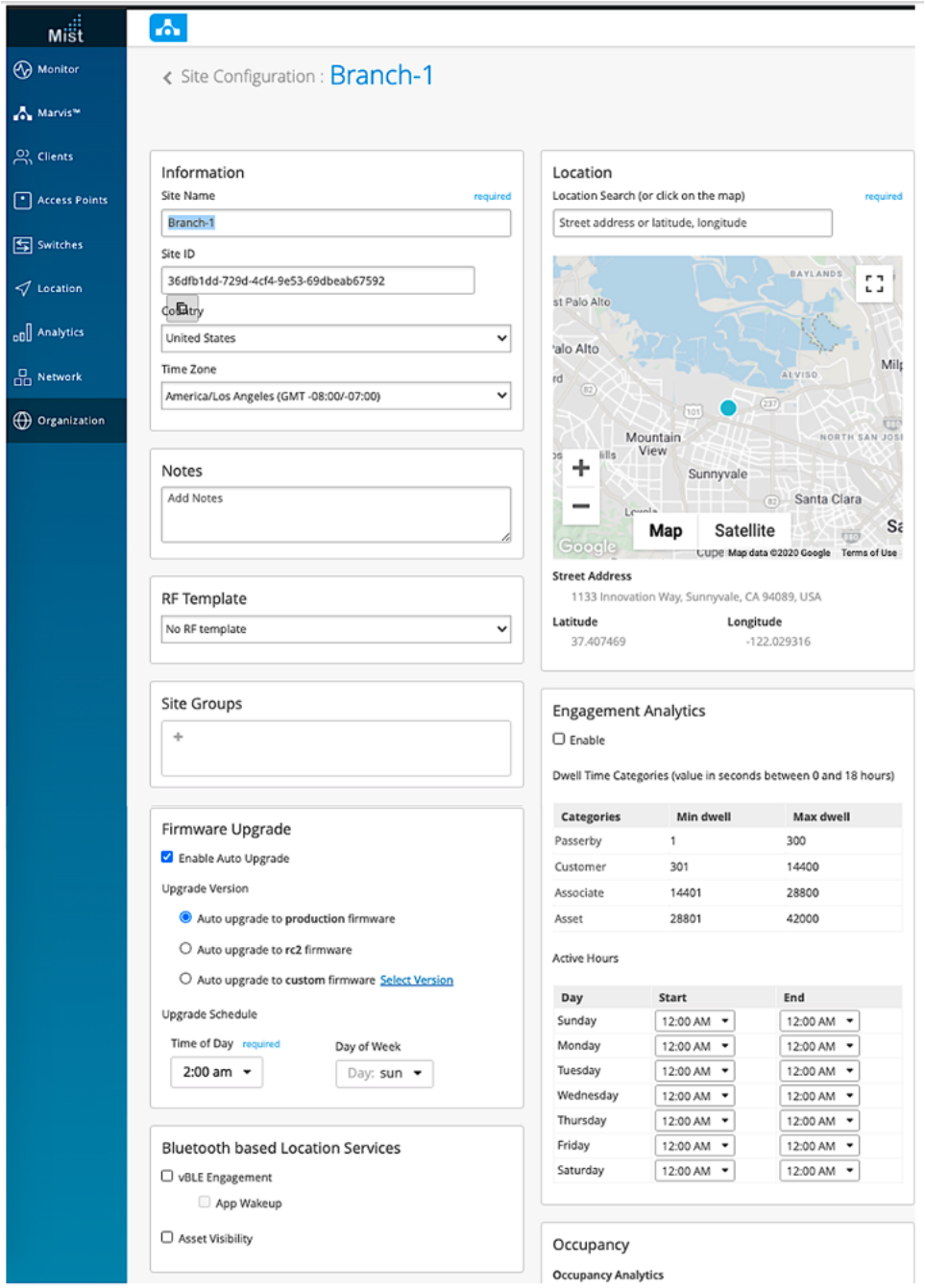
3. Create the WLAN template for this branch. We will use this template to create the SSIDs (WLANs) needed for the branch. For our example, we enabled 802.1x authentication with the RADIUS server for security and selected **Untagged** as the supported VLAN type.



4. To create a site for “Branch-1”, click on **Organization >Site Configuration** in the menu on the left and select **Create Site**.



5. Enter all relevant information for this site.



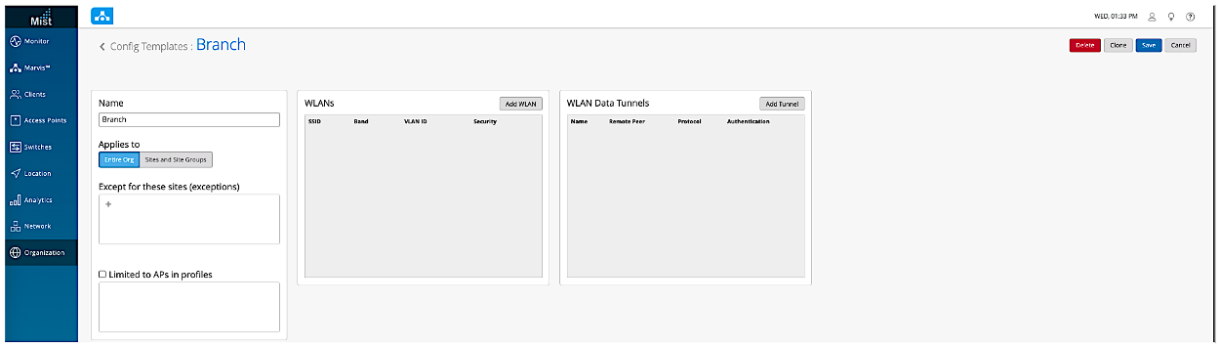
6. You can assigned access points to the switch on the branch site. To claim an access point for the branch site click on **Access point > Claim AP** in the menu on the left.

Additional SSID Configuration

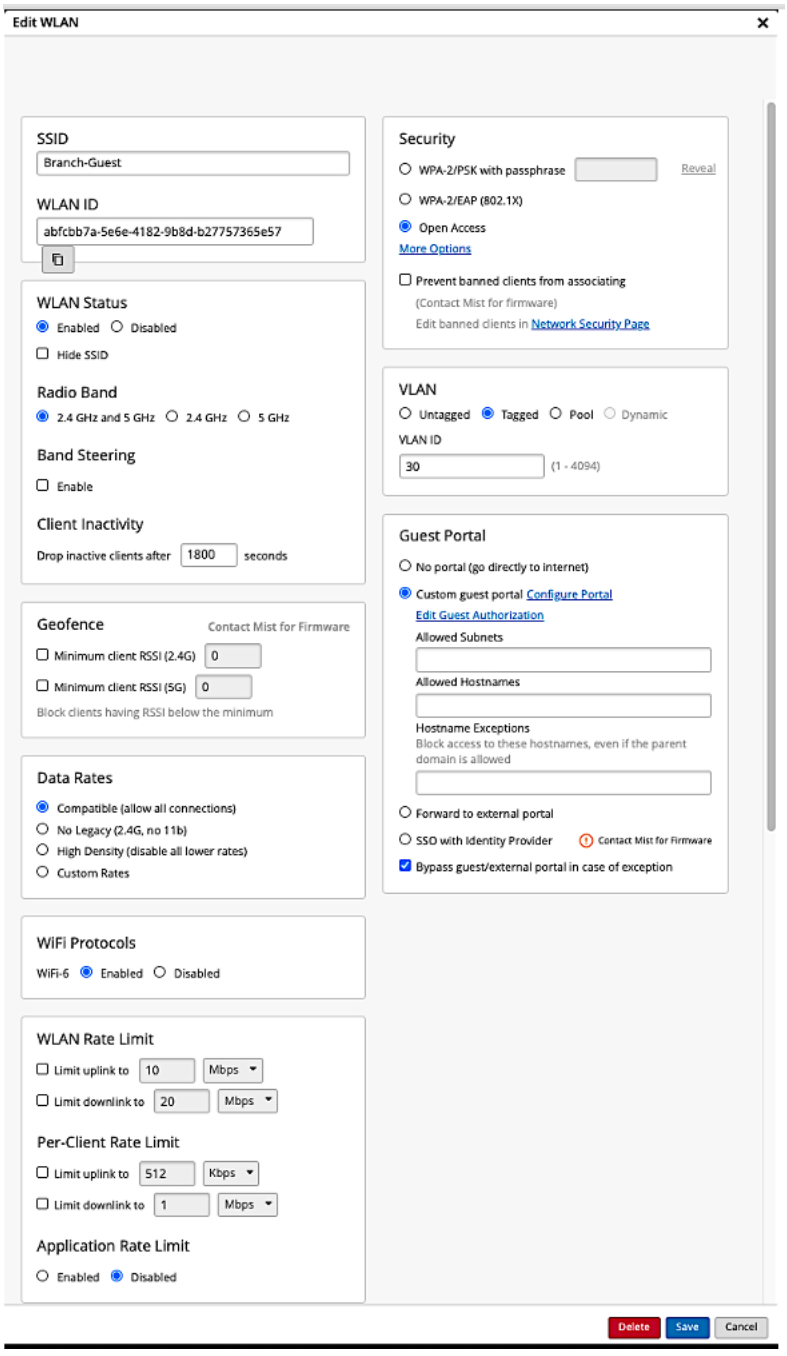
In midsize branch offices, you often find multiple SSIDs and WLANs for different VLAN groups with different security. In our configuration, we configure the SRX switch port as a trunk port with **native-vlan-id** enabled for the management of the access points. In the procedure below, we will update our branch site to include WLAN networks for guest access and IOT devices.

Step-by-Step Procedure

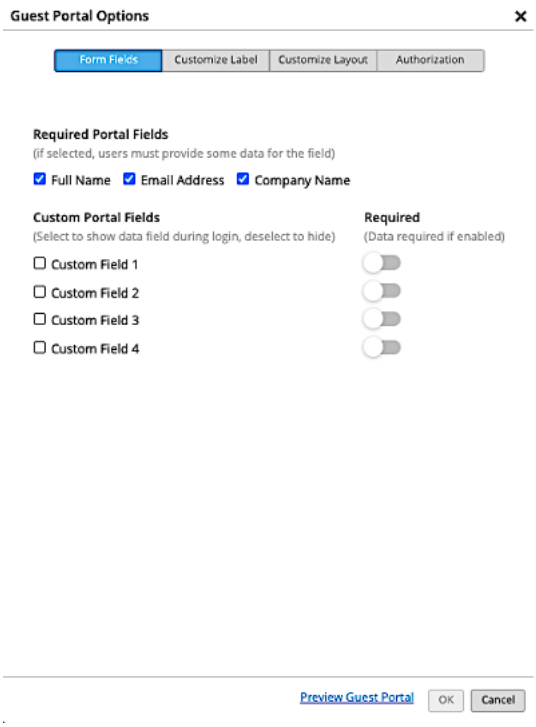
1. To edit the template for the branch office, click **Organization > Config Templates** in the menu on the left.



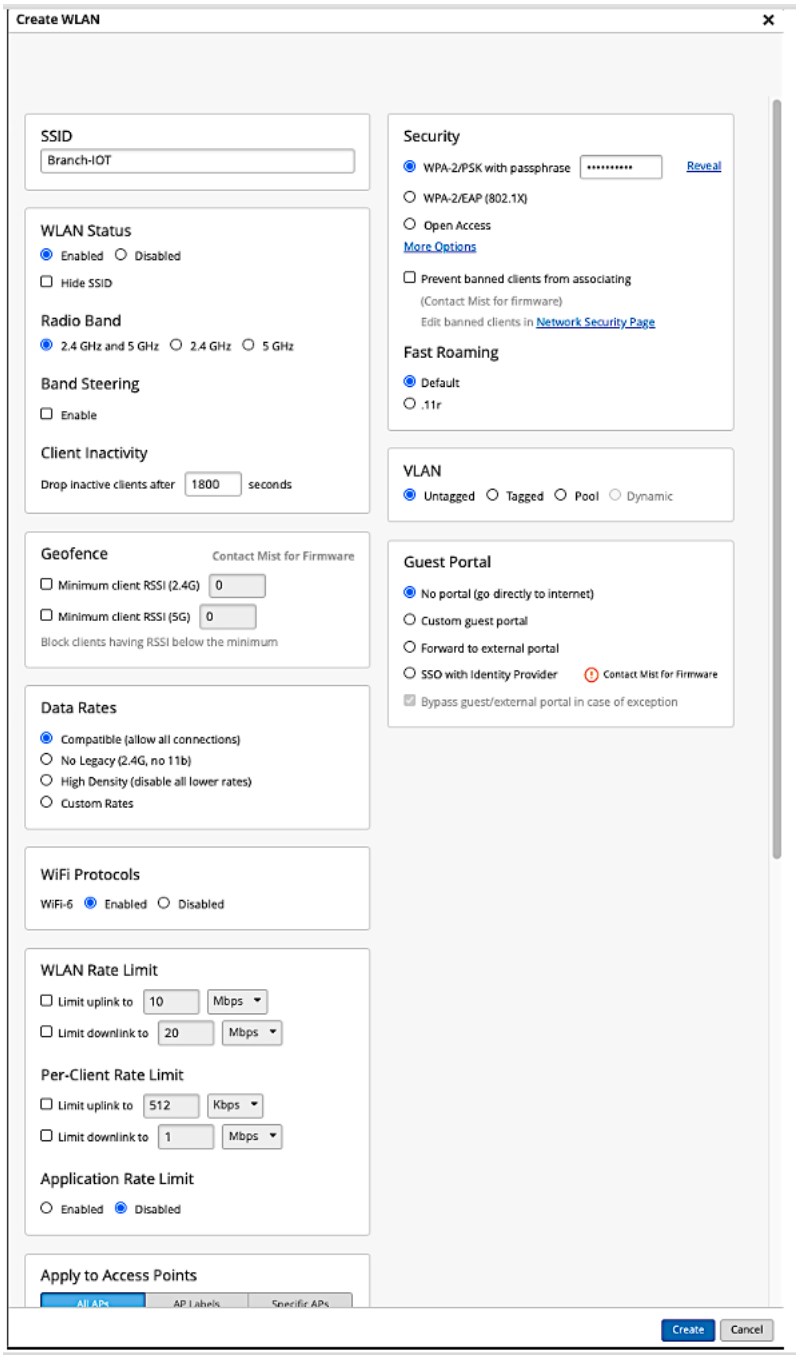
2. To create additional WLANs for the branch office, click **Add WLAN**. We start by creating a WLAN with an SSID for guest access on VLAN30. To assign the VLAN ID, click **Tagged** and enter the VLAN ID.


Edit WLAN
SSID
Branch-Guest
WLAN ID
abfcbb7a-5e6e-4182-9b8d-b2757365e57
WLAN Status
Enabled
Disabled
Hide SSID
Radio Band
2.4 GHz and 5 GHz
2.4 GHz
5 GHz
Band Steering
Enable
Client Inactivity
Drop inactive clients after
1800
seconds
Geofence
Contact Mist for Firmware
Minimum client RSSI (2.4G)
0
Minimum client RSSI (5G)
0
Block clients having RSSI below the minimum
Data Rates
Compatible (allow all connections)
No Legacy (2.4G, no 11b)
High Density (disable all lower rates)
Custom Rates
WiFi Protocols
WiFi-6
Enabled
Disabled
WLAN Rate Limit
Limit uplink to
10
Mbps
Limit downlink to
20
Mbps
Per-Client Rate Limit
Limit uplink to
512
Kbps
Limit downlink to
1
Mbps
Application Rate Limit
Enabled
Disabled
Security
WPA-2/PSK with passphrase
Reveal
WPA-2/EAP (802.1X)
Open Access
More Options
Prevent banned clients from associating
(Contact Mist for firmware)
Edit banned clients in Network Security Page
VLAN
Untagged
Tagged
Pool
Dynamic
VLAN ID
30
(1 - 4094)
Guest Portal
No portal (go directly to internet)
Custom guest portal
Configure Portal
Edit Guest Authorization
Allowed Subnets
Allowed Hostnames
Hostname Exceptions
Block access to these hostnames, even if the parent domain is allowed
Forward to external portal
SSO with Identity Provider
Contact Mist for Firmware
Bypass guest/external portal in case of exception
Delete
Save
Cancel

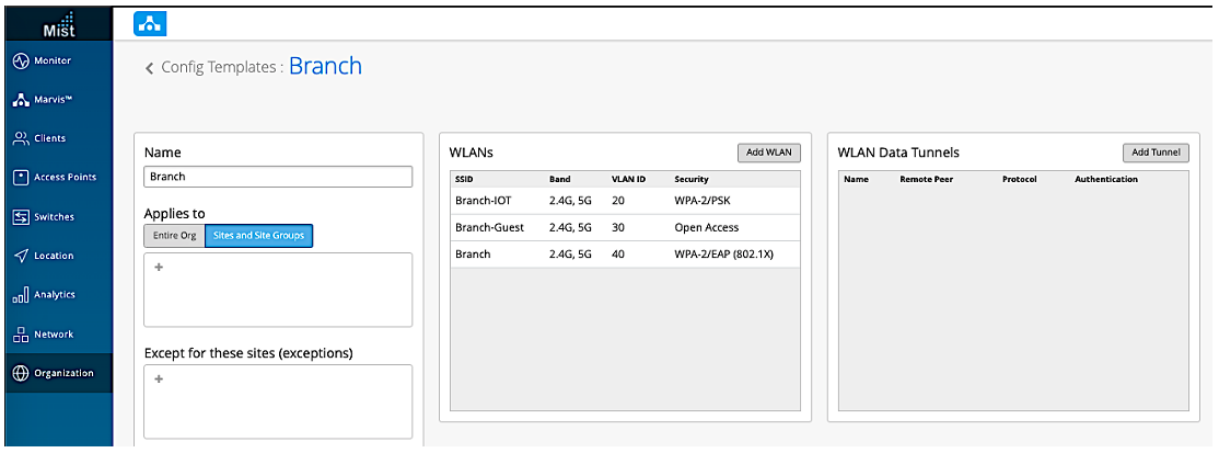
3. In the Guest Portal workarea, click **Custom guest portal** to customize a WLAN for guest access.



4. Create an SSID (WLAN) and the corresponding VLAN that will be used by the different types of devices. We create the SSID for IOT on VLAN20 and assign PSK enabled SSID for security. To assign the VLAN ID, click **Tagged** and enter the VLAN ID.


Create WLAN
SSID
Branch-IOT
WLAN Status
Enabled
Disabled
Hide SSID
Radio Band
2.4 GHz and 5 GHz
2.4 GHz
5 GHz
Band Steering
Enable
Client Inactivity
Drop inactive clients after
1800
seconds
Geofence
Contact Mist for Firmware
Minimum client RSSI (2.4G)
0
Minimum client RSSI (5G)
0
Block clients having RSSI below the minimum
Data Rates
Compatible (allow all connections)
No Legacy (2.4G, no 11b)
High Density (disable all lower rates)
Custom Rates
WiFi Protocols
WiFi-6
Enabled
Disabled
WLAN Rate Limit
Limit uplink to
10
Mbps
Limit downlink to
20
Mbps
Per-Client Rate Limit
Limit uplink to
512
Kbps
Limit downlink to
1
Mbps
Application Rate Limit
Enabled
Disabled
Apply to Access Points
All APs
AP Labels
Specific APs
Security
WPA-2/PSK with passphrase
Reveal
WPA-2/EAP (802.1X)
Open Access
More Options
Prevent banned clients from associating
(Contact Mist for firmware)
Edit banned clients in Network Security Page
Fast Roaming
Default
.11r
VLAN
Untagged
Tagged
Pool
Dynamic
Guest Portal
No portal (go directly to internet)
Custom guest portal
Forward to external portal
SSO with Identity Provider
Contact Mist for Firmware
Bypass guest/external portal in case of exception
Create
Cancel

When you are done, the SSIDs that you configured are displayed.



Repeat the procedure for the other VLANs. We are finished with the configuration on the EX switch and the access points and will now complete the configuration for the SRX.

Application Quality of Experience on a SD-WAN

Overview

Application Quality Experience (AppQoE) improves the user experience at the application level by constantly monitoring the quality of service parameters and Service Level Agreement (SLA) compliance of application traffic. It ensures that the application data is sent over the most SLA-compliant link available. We enable and configure AppQoE on the SRX device.

Let us consider the applications listed in Table 4 on page 39. For illustrative purposes, let us assume that the applications Office365, Salesforce, and Zoom are business-critical for the organization and these critical applications will be routed predominantly through the MPLS link. We will prioritize these applications on the LTE link as well. The remaining applications use the broadband Internet access link as the primary link. Finally, we reserve the LTE backup link only for business-critical applications. The noncritical applications are inaccessible when we only have the LTE connection available.

Table 4: Typical Applications Used in a Branch Office

Applications	Primary Link	Secondary Link	Critical Application?
Office365	MPLS	Broadband Internet	Yes
Salesforce	MPLS	Broadband Internet	Yes

Table 4: Typical Applications Used in a Branch Office *(continued)*

Applications	Primary Link	Secondary Link	Critical Application?
Zoom	MPLS	Broadband Internet	Yes
Slack	Broadband Internet	MPLS	No
GoToMeeting	Broadband Internet	MPLS	No
Dropbox	Broadband Internet	MPLS	No
Skype	Broadband Internet	MPLS	No
Youtube	Broadband Internet	MPLS	No

1. Configure the interface that connects the SRX to the EX. Add vlan1 as the native VLAN and add the VLAN interfaces according to Table 2 on page 11.

```
set interfaces ge-0/0/0  flexible-vlan-tagging
set interfaces ge-0/0/0 native-vlan-id 1
set interfaces ge-0/0/0 unit 1 vlan-id 1
set interfaces ge-0/0/0 unit 10 family inet address 10.10.10.1/24
set interfaces ge-0/0/0 unit 10 vlan-id 10
set interfaces ge-0/0/0 unit 20 vlan-id 20
set interfaces ge-0/0/0 unit 20 family inet address 10.10.20.1/24
set interfaces ge-0/0/0 unit 30 vlan-id 30
set interfaces ge-0/0/0 unit 30 family inet address 10.10.30.1/24
set interfaces ge-0/0/0 unit 40 vlan-id 40
set interfaces ge-0/0/0 unit 40 family inet address 10.10.40.1/24
```

2. Add the VLAN interfaces to the security zone named “trust”.

```
set security zones security-zone trust interfaces ge-0/0/0.10
set security zones security-zone trust interfaces ge-0/0/0.20
set security zones security-zone trust interfaces ge-0/0/0.30
set security zones security-zone trust interfaces ge-0/0/0.40
```

3. Create a DHCP server and an IP address pool for assigning to devices on vlan10. Configure the interface ge-0/0/0.10 to be a DHCP Server.

```
set system services dhcp-local-server group CORP-NET interface ge-0/0/0.10
set access address-assignment pool AP-NET_DHCP-POOL family inet network
10.10.10.0/24
set access address-assignment pool AP-NET_DHCP-POOL family inet range
AP-NET_DHCP-POOL---IP-RANGE low 10.10.10.10
set access address-assignment pool AP-NET_DHCP-POOL family inet range
AP-NET_DHCP-POOL---IP-RANGE high 10.10.10.100
set access address-assignment pool AP-NET_DHCP-POOL family inet dhcp-attributes
 domain-name MyMistLAB.com
set access address-assignment pool AP-NET_DHCP-POOL family inet dhcp-attributes
 name-server 8.8.8.8
set access address-assignment pool AP-NET_DHCP-POOL family inet dhcp-attributes
 router 10.10.10.1
```

4. Create a DHCP server and an IP address pool for assigning to devices on vlan20. Configure the interface ge-0/0/0.20 to be a DHCP Server address

```
 set system services dhcp-local-server group IOT-NET_DHCP-POOL interface
ge-0/0/0.20
set access address-assignment pool IOT-NET_DHCP-POOL family inet network
10.10.20.0/24
set access address-assignment pool IOT-NET_DHCP-POOL family inet range
IOT-NET_DHCP-POOL---IP-RANGE low 10.10.20.10
set access address-assignment pool IOT-NET_DHCP-POOL family inet range
IOT-NET_DHCP-POOL---IP-RANGE high 10.10.20.100
set access address-assignment pool IOT-NET_DHCP-POOL family inet dhcp-attributes
 domain-name MyMistLAB.com
set access address-assignment pool IOT-NET_DHCP-POOL family inet dhcp-attributes
 name-server 8.8.8.8
set access address-assignment pool IOT-NET_DHCP-POOL family inet dhcp-attributes
 router 10.10.20.1
```

5. Create a DHCP server and an IP address pool for assigning to devices on vlan30. Configure the interface ge-0/0/0.30 to be a DHCP Server address

```
set system services dhcp-local-server group CAMERA-NET_DHCP-POOL interface
ge-0/0/0.30
set access address-assignment pool CAMERA-NET_DHCP-POOL family inet network
10.10.30.0/24
set access address-assignment pool CAMERA-NET_DHCP-POOL family inet range
CAMERA-NET_DHCP-POOL---IP-RANGE low 10.10.30.10
set access address-assignment pool CAMERA-NET_DHCP-POOL family inet range
```

```
CAMERA-NET_DHCP-POOL---IP-RANGE high 10.10.30.100
set access address-assignment pool CAMERA-NET_DHCP-POOL family inet
dhcp-attributes domain-name MyMistLAB.com
set access address-assignment pool CAMERA-NET_DHCP-POOL family inet
dhcp-attributes name-server 8.8.8.8
set access address-assignment pool CAMERA-NET_DHCP-POOL family inet
dhcp-attributes router 10.10.30.1
```

6. Create a DHCP server and an IP address pool for assigning to devices on vlan40. Configure the interface ge-0/0/0.40 to be a DHCP Server address

```
set system services dhcp-local-server group CORPORATE-NET_DHCP-POOL interface
ge-0/0/0.40
set access address-assignment pool CORPORATE-NET_DHCP-POOL family inet network
 10.10.40.0/24
set access address-assignment pool CORPORATE-NET_DHCP-POOL family inet range
CORPORATE-NET_DHCP-POOL---IP-RANGE low 10.10.40.10
set access address-assignment pool CORPORATE-NET_DHCP-POOL family inet range
CORPORATE-NET_DHCP-POOL---IP-RANGE high 10.10.40.100
set access address-assignment pool CORPORATE-NET_DHCP-POOL family inet
dhcp-attributes domain-name MyMistLAB.com
set access address-assignment pool CORPORATE-NET_DHCP-POOL family inet
dhcp-attributes name-server 8.8.8.8
set access address-assignment pool CORPORATE-NET_DHCP-POOL family inet
dhcp-attributes router 10.10.40.1
```

7. Commit the configuration.

```
commit and quit
```

   The EX switch and Access points are now connected on the trunk port and Internet access is restored on the EX switch.

8. Create time-performance monitoring probes for each application and link specified in Table 4 on page 39. We set up a probe to test the connectivity to an IP address used by Office365, specifically 40.97.223.114. The probe test runs 5 times, 6 seconds apart. We also configure the thresholds that should not be violated, such as the loss of 5 successive tests or return transmit time (RTT) of 300000 microseconds. The IP address of the gateway on interface ge-0/0/6 is 192.168.220.1.

```
set services rpm probe office365_rpm_primary test office365_test_primary
probe-type icmp-ping
set services rpm probe office365_rpm_primary test office365_test_primary target
 address 40.97.223.114
set services rpm probe office365_rpm_primary test office365_test_primary
probe-count 5
set services rpm probe office365_rpm_primary test office365_test_primary
probe-interval 6
set services rpm probe office365_rpm_primary test office365_test_primary
thresholds successive-loss 5
set services rpm probe office365_rpm_primary test office365_test_primary
thresholds rtt 300000
set services rpm probe office365_rpm_primary test office365_test_primary
destination-interface ge-0/0/6.0
set services rpm probe office365_rpm_primary test office365_test_primary next-hop
 192.168.220.1
```

9. Create the second probe for the same application to probe the secondary link using the secondary interface. The IP address of the default gateway on the broadband Internet link is 10.10.10.1.

```
set services rpm probe office365_rpm_secondary test office365_test_secondary
probe-type icmp-ping
set services rpm probe office365_rpm_secondary test office365_test_secondary
target address 40.97.223.114
set services rpm probe office365_rpm_secondary test office365_test_secondary
probe-count 5
set services rpm probe office365_rpm_secondary test office365_test_secondary
probe-interval 6
set services rpm probe office365_rpm_secondary test office365_test_secondary
thresholds successive-loss 5
set services rpm probe office365_rpm_secondary test office365_test_secondary
thresholds rtt 300000
set services rpm probe office365_rpm_secondary test office365_test_secondary
destination-interface ge-0/0/7.0
set services rpm probe office365_rpm_secondary test office365_test_secondary
next-hop 10.10.10.1
```

10. We also create two probes for the Skype application. Because we have higher link guarantees for this application, we set a shorter probe interval of 1 second, and a shorter RTT of 60000 microseconds.

NOTE: We set up the primary and secondary probes on the interface based on whether the application is a business critical application. The interface and the IP address for the primary probe for noncritical applications (Skype) is different than the probe for the critical application (Office365).

```
set services rpm probe skype_rpm_primary test skype_test_primary probe-type
icmp-ping
set services rpm probe skype_rpm_primary test skype_test_primary target address
 13.107.8.2
set services rpm probe skype_rpm_primary test skype_test_primary probe-count 5

set services rpm probe skype_rpm_primary test skype_test_primary probe-interval
 1
set services rpm probe skype_rpm_primary test skype_test_primary thresholds
successive-loss 5
set services rpm probe skype_rpm_primary test skype_test_primary thresholds rtt
 60000
set services rpm probe skype_rpm_primary test skype_test_primary
destination-interface ge-0/0/7.0
set services rpm probe skype_rpm_primary test skype_test_primary next-hop
10.10.10.1
set services rpm probe skype_rpm_secondary test skype_test_secondary probe-type
 icmp-ping
set services rpm probe skype_rpm_secondary test skype_test_secondary target
address 13.107.8.2
set services rpm probe skype_rpm_secondary test skype_test_secondary probe-count
 5
set services rpm probe skype_rpm_secondary test skype_test_secondary
probe-interval 1
set services rpm probe skype_rpm_secondary test skype_test_secondary thresholds
 successive-loss 5
set services rpm probe skype_rpm_secondary test skype_test_secondary thresholds
 rtt 60000
```

11. We configure probes for the remaining applications using a similar pattern.

```
set services rpm probe salesforce_rpm_primary test salesforce_test_primary
probe-type icmp-ping
set services rpm probe salesforce_rpm_primary test salesforce_test_primary target
 address 96.43.144.26
```

```
set services rpm probe salesforce_rpm_primary test salesforce_test_primary
probe-count 5
set services rpm probe salesforce_rpm_primary test salesforce_test_primary
probe-interval 6
set services rpm probe salesforce_rpm_primary test salesforce_test_primary
thresholds successive-loss 5
set services rpm probe salesforce_rpm_primary test salesforce_test_primary
thresholds rtt 300000
set services rpm probe salesforce_rpm_primary test salesforce_test_primary
destination-interface ge-0/0/6.0
set services rpm probe salesforce_rpm_primary test salesforce_test_primary
next-hop 192.168.220.1
set services rpm probe salesforce_rpm_secondary test salesforce_test_secondary
 probe-type icmp-ping
set services rpm probe salesforce_rpm_secondary test salesforce_test_secondary
 target address 96.43.144.26
set services rpm probe salesforce_rpm_secondary test salesforce_test_secondary
 probe-count 5
set services rpm probe salesforce_rpm_secondary test salesforce_test_secondary
 probe-interval 6
set services rpm probe salesforce_rpm_secondary test salesforce_test_secondary
 thresholds successive-loss 5
set services rpm probe salesforce_rpm_secondary test salesforce_test_secondary
 thresholds rtt 300000
set services rpm probe salesforce_rpm_secondary test salesforce_test_secondary
 destination-interface ge-0/0/7.0
set services rpm probe salesforce_rpm_secondary test salesforce_test_secondary
 next-hop 10.10.10.1
set services rpm probe dropbox_rpm_primary test dropbox_test_primary probe-type
 icmp-ping
set services rpm probe dropbox_rpm_primary test dropbox_test_primary target
address 162.125.248.1
set services rpm probe dropbox_rpm_primary test dropbox_test_primary probe-count
 5
set services rpm probe dropbox_rpm_primary test dropbox_test_primary
probe-interval 1
set services rpm probe dropbox_rpm_primary test dropbox_test_primary thresholds
 successive-loss 5
set services rpm probe dropbox_rpm_primary test dropbox_test_primary thresholds
 rtt 200000
set services rpm probe dropbox_rpm_primary test dropbox_test_primary
destination-interface ge-0/0/7.0
set services rpm probe dropbox_rpm_primary test dropbox_test_primary next-hop
10.10.10.1
```

```
set services rpm probe dropbox_rpm_secondary test dropbox_test_secondary
probe-type icmp-ping
set services rpm probe dropbox_rpm_secondary test dropbox_test_secondary target
 address 162.125.248.1
set services rpm probe dropbox_rpm_secondary test dropbox_test_secondary
probe-count 5
set services rpm probe dropbox_rpm_secondary test dropbox_test_secondary
probe-interval 1
set services rpm probe dropbox_rpm_secondary test dropbox_test_secondary
thresholds successive-loss 5
set services rpm probe dropbox_rpm_secondary test dropbox_test_secondary
thresholds rtt 200000
set services rpm probe dropbox_rpm_secondary test dropbox_test_secondary
destination-interface ge-0/0/6.0
set services rpm probe dropbox_rpm_secondary test dropbox_test_secondary next-hop
 192.168.220.1
set services rpm probe zoom_rpm_primary test zoom_test_primary probe-type
icmp-ping
set services rpm probe zoom_rpm_primary test zoom_test_primary target address
3.80.20.128
set services rpm probe zoom_rpm_primary test zoom_test_primary probe-count 5
set services rpm probe zoom_rpm_primary test zoom_test_primary probe-interval
1
set services rpm probe zoom_rpm_primary test zoom_test_primary thresholds
successive-loss 5
set services rpm probe zoom_rpm_primary test zoom_test_primary thresholds rtt
60000
set services rpm probe zoom_rpm_primary test zoom_test_primary
destination-interface ge-0/0/6.0
set services rpm probe zoom_rpm_primary test zoom_test_primary next-hop
192.168.220.1
set services rpm probe zoom_rpm_secondary test zoom_test_secondary probe-type
icmp-ping
set services rpm probe zoom_rpm_secondary test zoom_test_secondary target address
 3.80.20.128
set services rpm probe zoom_rpm_secondary test zoom_test_secondary probe-count
 5
set services rpm probe zoom_rpm_secondary test zoom_test_secondary probe-interval
 1
set services rpm probe zoom_rpm_secondary test zoom_test_secondary thresholds
successive-loss 5
set services rpm probe zoom_rpm_secondary test zoom_test_secondary thresholds
rtt 60000
set services rpm probe zoom_rpm_secondary test zoom_test_secondary
```

```
destination-interface ge-0/0/7.0
set services rpm probe zoom_rpm_secondary test zoom_test_secondary next-hop
10.10.10.1
set services rpm probe gotomeeting_rpm_primary test gotomeeting_test_primary
probe-type icmp-ping
set services rpm probe gotomeeting_rpm_primary test gotomeeting_test_primary
target address 216.115.208.241
set services rpm probe gotomeeting_rpm_primary test gotomeeting_test_primary
probe-count 5
set services rpm probe gotomeeting_rpm_primary test gotomeeting_test_primary
probe-interval 1
set services rpm probe gotomeeting_rpm_primary test gotomeeting_test_primary
thresholds successive-loss 5
set services rpm probe gotomeeting_rpm_primary test gotomeeting_test_primary
thresholds rtt 60000
set services rpm probe gotomeeting_rpm_primary test gotomeeting_test_primary
destination-interface ge-0/0/7.0
set services rpm probe gotomeeting_rpm_primary test gotomeeting_test_primary
next-hop 10.10.10.1
set services rpm probe gotomeeting_rpm_secondary test gotomeeting_test_secondary
 probe-type icmp-ping
set services rpm probe gotomeeting_rpm_secondary test gotomeeting_test_secondary
 target address 216.115.208.241
set services rpm probe gotomeeting_rpm_secondary test gotomeeting_test_secondary
 probe-count 5
set services rpm probe gotomeeting_rpm_secondary test gotomeeting_test_secondary
 probe-interval 1
set services rpm probe gotomeeting_rpm_secondary test gotomeeting_test_secondary
 thresholds successive-loss 5
set services rpm probe gotomeeting_rpm_secondary test gotomeeting_test_secondary
 thresholds rtt 60000
set services rpm probe gotomeeting_rpm_secondary test gotomeeting_test_secondary
 destination-interface ge-0/0/6.0
set services rpm probe gotomeeting_rpm_secondary test gotomeeting_test_secondary
 next-hop 192.168.220.1
set services rpm probe youtube_rpm_primary test youtube_test_primary probe-type
 http-get
set services rpm probe youtube_rpm_primary test youtube_test_primary target url
 https://youtube.com
set services rpm probe youtube_rpm_primary test youtube_test_primary probe-count
 5
set services rpm probe youtube_rpm_primary test youtube_test_primary
probe-interval 10
set services rpm probe youtube_rpm_primary test youtube_test_primary thresholds
```

```
 successive-loss 5
set services rpm probe youtube_rpm_primary test youtube_test_primary thresholds
 rtt 150000
set services rpm probe youtube_rpm_primary test youtube_test_primary
destination-interface ge-0/0/7.0
set services rpm probe youtube_rpm_primary test youtube_test_primary next-hop
10.10.10.1
set services rpm probe youtube_rpm_secondary test youtube_test_secondary
probe-type http-get
set services rpm probe youtube_rpm_secondary test youtube_test_secondary target
 url https://youtube.com
set services rpm probe youtube_rpm_secondary test youtube_test_secondary
probe-count 5
set services rpm probe youtube_rpm_secondary test youtube_test_secondary
probe-interval 10
set services rpm probe youtube_rpm_secondary test youtube_test_secondary
thresholds successive-loss 5
set services rpm probe youtube_rpm_secondary test youtube_test_secondary
thresholds rtt 150000
set services rpm probe youtube_rpm_secondary test youtube_test_secondary
destination-interface ge-0/0/6.0
set services rpm probe youtube_rpm_secondary test youtube_test_secondary next-hop
 192.168.220.1
set services rpm probe slack_rpm_primary test slack_test_primary probe-type
icmp-ping
set services rpm probe slack_rpm_primary test slack_test_primary target address
 216.115.208.241
set services rpm probe slack_rpm_primary test slack_test_primary probe-count 5
set services rpm probe slack_rpm_primary test slack_test_primary probe-interval
 1
set services rpm probe slack_rpm_primary test slack_test_primary thresholds
successive-loss 5
set services rpm probe slack_rpm_primary test slack_test_primary thresholds rtt
 60000
set services rpm probe slack_rpm_primary test slack_test_primary
destination-interface ge-0/0/7.0
set services rpm probe slack_rpm_primary test slack_test_primary next-hop
10.10.10.1
set services rpm probe slack_rpm_secondary test slack_test_secondary probe-type
 icmp-ping
set services rpm probe slack_rpm_secondary test slack_test_secondary target
address 216.115.208.241
set services rpm probe slack_rpm_secondary test slack_test_secondary probe-count
 5
```

```
set services rpm probe slack_rpm_secondary test slack_test_secondary
probe-interval 1
set services rpm probe slack_rpm_secondary test slack_test_secondary thresholds
 successive-loss 5
set services rpm probe slack_rpm_secondary test slack_test_secondary thresholds
 rtt 60000
set services rpm probe slack_rpm_secondary test slack_test_secondary
destination-interface ge-0/0/6.0
set services rpm probe slack_rpm_secondary test slack_test_secondary next-hop
192.168.220.1
```

12. Create a routing instance for each application. We configure an application's primary link route with a lower preference value than the other links. Routes with lower preference value have preference over higher value routes. We will configure the LTE backup interface only for the business-critical applications.

    For the routing instance for the Office365 application, we use a primary MPLS link. We set a preference value of 10 to the gateway of this link (most preferred route), a preference value of 20 for the gateway of the broadband Internet link (next preferred route), and a preference value of 30 for the LTE backup link (least preferred route).

```
set routing-instances office365_RInstance instance-type forwarding
set routing-instances office365_RInstance routing-options static route 0/0
qualified-next-hop 192.168.220.1 preference 10
set routing-instances office365_RInstance routing-options static route 0/0
qualified-next-hop 10.10.10.1 preference 20
set routing-instances office365_RInstance routing-options static route 0/0
qualified-next-hop dl0.0 preference 30
```

13. Configure the routing instances for the remaining applications in a similar pattern.

```
set routing-instances skype_RInstance instance-type forwarding
set routing-instances skype_RInstance routing-options static route 0/0
qualified-next-hop 10.10.10.1 preference 10
set routing-instances skype_RInstance routing-options static route 0/0
qualified-next-hop 192.168.220.1 preference 20
set routing-instances salesforce_RInstance instance-type forwarding
set routing-instances salesforce_RInstance routing-options static route 0/0
qualified-next-hop 192.168.220.1 preference 10
set routing-instances salesforce_RInstance routing-options static route 0/0
qualified-next-hop 10.10.10.1 preference 20
set routing-instances salesforce_RInstance routing-options static route 0/0
qualified-next-hop dl0.0 preference 30
```

```
set routing-instances dropbox_RInstance instance-type forwarding
set routing-instances dropbox_RInstance routing-options static route 0/0
qualified-next-hop 10.10.10.1 preference 10
set routing-instances dropbox_RInstance routing-options static route 0/0
qualified-next-hop 192.168.220.1 preference 20
set routing-instances slack_RInstance instance-type forwarding
set routing-instances slack_RInstance routing-options static route 0/0
qualified-next-hop 10.10.10.1 preference 10
set routing-instances slack_RInstance routing-options static route 0/0
qualified-next-hop 192.168.220.1 preference 20
set routing-instances zoom_RInstance instance-type forwarding
set routing-instances zoom_RInstance routing-options static route 0/0
qualified-next-hop 192.168.220.1 preference 10
set routing-instances zoom_RInstance routing-options static route 0/0
qualified-next-hop 10.10.10.1 preference 20
set routing-instances zoom_RInstance routing-options static route 0/0
qualified-next-hop dl0.0 preference 30
set routing-instances gotomeeting_RInstance instance-type forwarding
set routing-instances gotomeeting_RInstance routing-options static route 0/0
qualified-next-hop 10.10.10.1 preference 10
set routing-instances gotomeeting_RInstance routing-options static route 0/0
qualified-next-hop 192.168.220.1 preference 20
set routing-instances youtube_RInstance instance-type forwarding
set routing-instances youtube_RInstance routing-options static route 0/0
qualified-next-hop 10.10.10.1 preference 10
set routing-instances youtube_RInstance routing-options static route 0/0
qualified-next-hop 192.168.220.1 preference 20
```

14. Configure IP monitoring policies for all applications. The goal of the policies is to dynamically change the metric of the routes that were created in the routing instances in the previous step. The policies are created on a per-probe basis.

    In this step, we create the IP monitoring policy for the Office365 application. For Office365, we configure two probes and create two policies—one for each probe. When the probe detects that the application traffic has violated the configured threshold on a link, the policy changes the preference of the routes. The policy decreases the metric for the second best link to 2 and reroutes the application traffic to the link.

    For example, when the probe identifies that the primary link for Office365, the MPLS link, does not meet the requirements for RTT and loss, the policy changes the metric of the gateway for the broadband Internet link (next preferred route) to a value of 2.

```
set services ip-monitoring policy office365_ipm_primary match rpm-probe
office365_rpm_primary
```

```
set services ip-monitoring policy office365_ipm_primary then preferred-route
routing-instances office365_RInstance route 0/0 next-hop 10.10.10.1
set services ip-monitoring policy office365_ipm_primary then preferred-route
routing-instances office365_RInstance route 0/0 preferred-metric 2
```

15. Configure the IP monitoring policy for the secondary probe for Office365.

> **NOTE:** The next-hop address is the IP address for the primary MPLS link.

```
set services ip-monitoring policy office365_ipm_secondary match rpm-probe
office365_rpm_secondary
set services ip-monitoring policy office365_ipm_secondary then preferred-route
 routing-instances office365_RInstance route 0/0 next-hop 192.168.220.1
set services ip-monitoring policy office365_ipm_secondary then preferred-route
 routing-instances office365_RInstance route 0/0 preferred-metric 2
```

16. Configure IP monitoring policy for the remaining applications in a similar pattern.

```
set services ip-monitoring policy skype_ipm_primary match rpm-probe
skype_rpm_primary
set services ip-monitoring policy skype_ipm_primary then preferred-route
routing-instances skype_RInstance route 0/0 next-hop 192.168.220.1
set services ip-monitoring policy skype_ipm_primary then preferred-route
routing-instances skype_RInstance route 0/0 preferred-metric 2
set services ip-monitoring policy skype_ipm_secondary match rpm-probe
skype_rpm_secondary
set services ip-monitoring policy skype_ipm_secondary then preferred-route
routing-instances skype_RInstance route 0/0 next-hop 10.10.10.1
set services ip-monitoring policy skype_ipm_secondary then preferred-route
routing-instances skype_RInstance route 0/0 preferred-metric 2
set services ip-monitoring policy salesforce_ipm_primary match rpm-probe
salesforce_rpm_primary
set services ip-monitoring policy salesforce_ipm_primary then preferred-route
routing-instances salesforce_RInstance route 0/0 next-hop 10.10.10.1
set services ip-monitoring policy salesforce_ipm_primary then preferred-route
routing-instances salesforce_RInstance route 0/0 preferred-metric 2
set services ip-monitoring policy salesforce_ipm_secondary match rpm-probe
salesforce_rpm_secondary
set services ip-monitoring policy salesforce_ipm_secondary then preferred-route
 routing-instances salesforce_RInstance route 0/0 next-hop 192.168.220.1
```

```
set services ip-monitoring policy salesforce_ipm_secondary then preferred-route
 routing-instances salesforce_RInstance route 0/0 preferred-metric 2
set services ip-monitoring policy dropbox_ipm_primary match rpm-probe
dropbox_rpm_primary
set services ip-monitoring policy dropbox_ipm_primary then preferred-route
routing-instances dropbox_RInstance route 0/0 next-hop 192.168.220.1
set services ip-monitoring policy dropbox_ipm_primary then preferred-route
routing-instances dropbox_RInstance route 0/0 preferred-metric 2
set services ip-monitoring policy dropbox_ipm_secondary match rpm-probe
dropbox_rpm_secondary
set services ip-monitoring policy dropbox_ipm_secondary then preferred-route
routing-instances dropbox_RInstance route 0/0 next-hop 10.10.10.1
set services ip-monitoring policy dropbox_ipm_secondary then preferred-route
routing-instances dropbox_RInstance route 0/0 preferred-metric 2
set services ip-monitoring policy slack_ipm_primary match rpm-probe
slack_rpm_primary
set services ip-monitoring policy slack_ipm_primary then preferred-route
routing-instances slack_RInstance route 0/0 next-hop 192.168.220.1
set services ip-monitoring policy slack_ipm_primary then preferred-route
routing-instances slack_RInstance route 0/0 preferred-metric 2
set services ip-monitoring policy slack_ipm_secondary match rpm-probe
slack_rpm_secondary
set services ip-monitoring policy slack_ipm_secondary then preferred-route
routing-instances slack_RInstance route 0/0 next-hop 10.10.10.1
set services ip-monitoring policy slack_ipm_secondary then preferred-route
routing-instances slack_RInstance route 0/0 preferred-metric 2
set services ip-monitoring policy zoom_ipm_primary match rpm-probe
zoom_rpm_primary
set services ip-monitoring policy zoom_ipm_primary then preferred-route
routing-instances zoom_RInstance route 0/0 next-hop 10.10.10.1
set services ip-monitoring policy zoom_ipm_primary then preferred-route
routing-instances zoom_RInstance route 0/0 preferred-metric 2
set services ip-monitoring policy zoom_ipm_secondary match rpm-probe
zoom_rpm_secondary
set services ip-monitoring policy zoom_ipm_secondary then preferred-route
routing-instances zoom_RInstance route 0/0 next-hop 192.168.220.1
set services ip-monitoring policy zoom_ipm_secondary then preferred-route
routing-instances zoom_RInstance route 0/ preferred-metric 2
set services ip-monitoring policy gotomeeting_ipm_primary match rpm-probe
gotomeeting_rpm_primary
set services ip-monitoring policy gotomeeting_ipm_primary then preferred-route
 routing-instances gotomeeting_RInstance route 0/0 next-hop 192.168.220.1
set services ip-monitoring policy gotomeeting_ipm_primary then preferred-route
 routing-instances gotomeeting_RInstance route 0/0 preferred-metric 2
```

```
set services ip-monitoring policy gotomeeting_ipm_secondary match rpm-probe
gotomeeting_rpm_secondary
set services ip-monitoring policy gotomeeting_ipm_secondary then preferred-route
 routing-instances gotomeeting_RInstance route 0/0 next-hop 10.10.10.1
set services ip-monitoring policy gotomeeting_ipm_secondary then preferred-route
 routing-instances gotomeeting_RInstance route 0/0 preferred-metric 2
set services ip-monitoring policy youtube_ipm_primary match rpm-probe
youtube_rpm_primary
```

17. Configure an advanced policy-based routing (APBR) profile. APBR profile matches all of our eight applications and redirects the traffic for each and every one of them to their respective routing instance. The profile is divided into rules with each rule covering one application and one routing instance. For this example, we configure a rule named office365_rule to match all the traffic for the application named junos:OFFICE365-CREATE-CONVERSATION" and redirect the traffic to the routing instance named office365_RInstance.

> **NOTE:** To maintain application continuity and not impact users, we are not allowing mid-session path changes for the ongoing sessions, so we set the **max-route-change** parameter to 0.

```
set security advance-policy-based-routing tunables max-route-change 0
set security advance-policy-based-routing profile apbr_profile rule office365_rule
 match dynamic-application junos:OFFICE365-CREATE-CONVERSATION
set security advance-policy-based-routing profile apbr_profile rule office365_rule
 then routing-instance office365_RInstance
set security advance-policy-based-routing profile apbr_profile rule skype_rule
 match dynamic-application junos: SKYPE
set security advance-policy-based-routing profile apbr_profile rule skype_rule
 then routing-instance skype_RInstance
set security advance-policy-based-routing profile apbr_profile rule
salesforce_rule match dynamic-application junos:SALESFORCE
set security advance-policy-based-routing profile apbr_profile rule
salesforce_rule then routing-instance salesforce_RInstance
set security advance-policy-based-routing profile apbr_profile rule dropbox_rule
 match dynamic-application junos: DROPBOX
set security advance-policy-based-routing profile apbr_profile rule dropbox_rule
 then routing-instance dropbox_RInstance
set security advance-policy-based-routing profile apbr_profile rule slack_rule
 match dynamic-application junos:SLACK
```

```
set security advance-policy-based-routing profile apbr_profile rule slack_rule
 then routing-instance slack_RInstance
set security advance-policy-based-routing profile apbr_profile rule zoom_rule
match dynamic-application junos:ZOOM
set security advance-policy-based-routing profile apbr_profile rule zoom_rule
then routing-instance zoom_RInstance
set security advance-policy-based-routing profile apbr_profile rule
gotomeeting_rule match dynamic-application junos: GOTOMEETING
set security advance-policy-based-routing profile apbr_profile rule
gotomeeting_rule then routing-instance gotomeeting_RInstance
set security advance-policy-based-routing profile apbr_profile rule youtube_rule
 match dynamic-application junos:YOUTUBE
set security advance-policy-based-routing profile apbr_profile rule youtube_rule
 then routing-instance youtube_RInstance
```

18. Configure a protocol-independent group of routing tables. The allows a group to import the routing tables of each dedicated instances from the main routing table.

```
set routing-options interface-routes rib-group inet apbr_group
set routing-options rib-groups apbr_group import-rib inet.0
set routing-options rib-groups apbr_group import-rib office365_RInstance.inet.0

set routing-options rib-groups apbr_group import-rib skype_RInstance.inet.0
set routing-options rib-groups apbr_group import-rib salesforce_RInstance.inet.0

set routing-options rib-groups apbr_group import-rib dropbox_RInstance.inet.0
set routing-options rib-groups apbr_group import-rib slack_RInstance.inet.0
set routing-options rib-groups apbr_group import-rib zoom_RInstance.inet.0
set routing-options rib-groups apbr_group import-rib gotomeeting_RInstance.inet.0

set routing-options rib-groups apbr_group import-rib youtube_RInstance.inet.0
```

19. Add the newly created profile apbr_profile to the security zone trust. This configuration applies the profile to the traffic in the zone.

```
set security zones security-zone trust advance-policy-based-routing-profile
apbr_profile
```

20. Create a security policy that allows traffic between the trust zone and untrust zone. Be sure to include the desired network segments and applications in the policy.

```
set security policies from-zone trust to-zone untrust policy allow-in-zone then
 permit application-services application-traffic-control rule-set critical_app_rs
```

21. Commit the configuration.

```
commit and quit
```

Validation

Verifying Detection of Mini-PIM Modules by Junos OS

Purpose

Verify that the Junos OS detects the Mini-PIM modules.

Action

On the SRX Series device, verify that the LTE Mini-PIM was installed.

`user@host>` **show chassis hardware**

```
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                CX0916AF0004      SRX320-POE
Routing Engine   REV 0x05 650-065041   CX0916AF0004      RE-SRX320-POE
FPC 0                                                    FPC
  PIC 0                                                  6xGE,2xGE SFP Base PIC
FPC 1            REV 02   650-073958   AH06074206        FPC
  PIC 0                                                  LTE for AE
Power Supply 0
```

Meaning

The device shows that the LTE Mini-PIM was installed and is recognized by the system.

Verifying the Firmware Version of the Mini-PIM

Purpose

Check the firmware version of the Mini-PIM.

Action

On the SRX Series device, verify the firmware version of the LTE Mini-PIM module.

`user@host>`**show system firmware**

```
Part             Type              Tag Current              Available
  Status
                                       version              version
FPC 1
PIC 0            MLTE_FW           1   17.1.80             0
 OK
Routing Engine 0 RE BIOS           0   3.0                  3.6
  OK
Routing Engine 0 RE BIOS Backup    1   3.0                  3.6
  OK
```

Meaning

The output shows the firmware version of the Mini-PIM as 17.1.80. Update the firmware if required. For more information on upgrading the firmware on the LTE, see *LTE Mini-Physical Interface Module*.

Verifying APBR Rule Effectiveness

Purpose

Check the statistic for the APBR.

Action

Verify the traffic handling details after the APBR rule is applied.

`user@host>`**show security advance-policy-based-routing statistics**

```
Advance Profile Based Routing statistics:
  Sessions Processed                        5611
  App rule hit on cache hit                 1
  App rule hit on HTTP Proxy/ALG            0
  Midstream disabled rule hit on cache hit  0
  URL cat rule hit on cache hit             0
  DSCP rule hit on first packet             0
  App and DSCP hit on first packet          0
```

```
App rule hit midstream                    0
Midstream disabled rule hit midstream     0
URL cat rule hit midstream                0
App and DSCP rule hit midstream           0
DSCP rule hit midstream                   0
Route changed on cache hits               1
Route changed on HTTP Proxy/ALG           0
Route changed midstream                   0
Zone mismatch                             0
Drop on zone mismatch                     0
Next hop not found                        0
Application services bypass               0
```

Meaning

The output displays the statistical details collected for APBR including the number of sessions processed for the application-based routing rule, the number of times the application traffic matches the APBR profile (rule hit) and the number of times APBR is applied for the session, such as in a route change.