Engineering
Simplicity

# Juniper Mist Edge Design Guide

Published
2024-10-15

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

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

*Juniper Mist Edge Design Guide*

The information in this document is current as of the date on the title page.

## 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

# Table of Contents

# About the Guide

Juniper Mist™ Edge Design Guide is for administrators who want to learn about the Juniper Mist™ Edge architecture, deployment choices, and understand the configuration choices that are available through the Juniper Mist™ cloud portal.

1

CHAPTER

# Overview

# Juniper Mist Edge Overview

IN THIS SECTION

Juniper Mist leverages Juniper Mist Edge appliance when an organization needs to retain a centralized datapath architecture for campus or branch deployments. The Juniper Mist Edge appliance provides a centralized datapath for user traffic, a task that legacy wireless controllers traditionally performed. Additionally, the appliance keeps all the control and management functions in the Juniper Mist cloud.

Juniper Mist Edge can be a hardware or virtual appliance. Just like the APs, the hardware appliance comes with a claim-code. To add the device to an organization inventory, you can claim the device through the Juniper Mist Portal. You can also scan the claim code by using Mist AI app. For information on onboarding the Mist Edge device and to set up the initial configuration, see Juniper Mist Edge Quick Start Guide.

Juniper Mist Edge solution offers several key benefits:

- Agility—Rapidly develop and deploy new microservices.
- Scalability—Meet the demands of small and large campuses.
- Simplicity—Ease deployment and management with zero-touch configuration and cloud management.

## Features

The Juniper Mist Edge solution offers the following features:

### Tunneling Microservice

With tunneling microservice, you can seamlessly transition from the existing centralized data plane with legacy controller architectures to the modern Juniper Mist microservices cloud architecture. The access points (APs) leverage standards-based L2TPv3 technology to tunnel VLAN traffic to and from the Juniper Mist Edge for selected wireless LANs (WLANs).

### Flexible Traffic Redirection

The Juniper Mist microservices architecture provides the flexibility to form multiple tunnels to different Juniper Mist Edge appliances to meet the wireless configuration requirements. A Juniper Mist Edge deployment can support both locally bridged and tunneled WLANs. For example, you can:

- Locally bridge one site of the WLAN.
- Tunnel a guest WLAN to the Juniper Mist Edge deployment at the DMZ.
- Tunnel the corporate service set identifier (SSID) to the Juniper Mist Edge deployment at the data center.

With SSID tunneling, the Juniper Mist Edge solution can access corporate resources.

### High Availability and Clustering

Juniper Mist Edge supports an elastically scalable cluster that has an unlimited number of nodes. The support also includes :

- Backup clusters
- Meeting throughput expectations
- Optimizing the aggregate capacity for APs and clients

In case of a catastrophic network failure, Juniper Mist Edge supports multiple layers of redundancy to ensure WLAN survivability. If an entire cluster goes offline within a data center, Juniper Access Points can fail over to a different cluster hosted in a different data center to ensure network survivability.

## Use Cases and Benefits

The following are some of the typical use cases for a Juniper Mist Edge deployment:

### Centralized Datapath Architecture for Campus or Branch Deployment

With a simple, on-premises deployment of Juniper Mist Edge, you can establish a centralized data plane. The Juniper Mist Edge appliance provides a centralized datapath for user traffic, a task that legacy wireless controllers traditionally performed. Additionally, the appliance keeps all the control and management functions in the Juniper Mist cloud, while providing micro services architecture to the campus. Juniper Mist Edge solution provids access to corporate resources, while extending visibility into user network experience and streamlining IT operations through cloud management. This use case offers the following benefits:

- - Agility
    - Network management with minimal effort —Leverage Marvis® Virtual Network Assistant and manage network performance with analytics about Juniper Mist service-level exception (SLE) metrics.
    - Firmware independence—Remove firmware dependency between an AP and Juniper Mist Edge. You can independently update the Juniper Mist Edge services in less than 3 seconds.
  - Security
    - Traffic isolation—The level of traffic control is similar to the level in the original wireless LAN controller architecture. Enable transparent movement of user traffic to a single central location, isolating the traffic from your access switches.
    - Automated security—Enable machine-driven site deployment without any credential exposure.
    - Secure WebSocket to communicate to the cloud.
    - Provide IPsec tunnel support for remote workers.
  - Resiliency
    - Support high availability, fail over, automatic preemption, and load balancing.
  - Scalability
    - Support scaling from a few branches to thousands of branches.
    - Support any campus with AP count ranging from a few hundreds to a few thousands.
    - Support up to 10,000 APs and 100,000 clients on a single Juniper Mist Edge (X-10).
    - Support unlimited horizontal scaling within a cluster, that is, with this capability, dozens of Juniper Mist Edge appliances can exist within a cluster.

### Remote Worker Use Case

Juniper Mist Edge extends virtual LANs (VLANs) to distributed branches and telecommuters to replace remote virtual private network (VPN) technology. It also provides dynamic traffic segmentation for IoT devices. Split tunneling allows for guest access and corporate traffic.This use case offers the following benefits:

- - Agility
    - Zero-touch Provisioning—Remove the need for prior staging of an AP.

- Network management with minimal effort—Leverage Marvis and manage network performance with analytics about Juniper Mist SLE metrics.

- Security

  - Traffic isolation—Maintain the same level of traffic control as you maintain on-premises.

  - Automated Security—Enable machine-driven site deployment without any credential exposure.

  - Endpoint protection—Easily secure wireless and wired endpoints through Power Over Ethernet (PoE)-out.

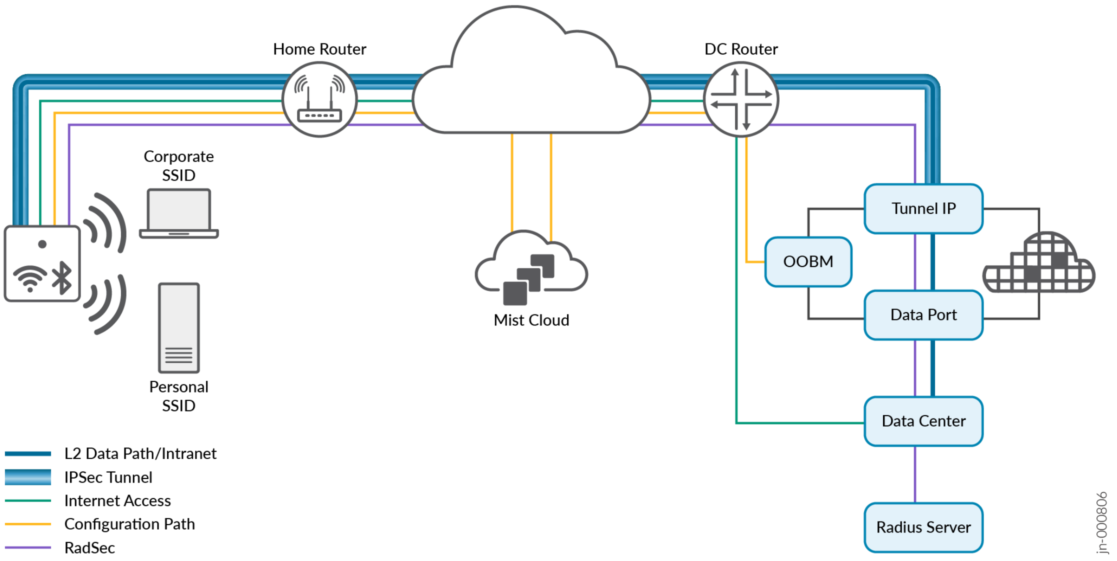
- Flexibility

  - Reuse hardware.

  - Support flexible all-home coverage with secure mesh capabilities.

  - Enable employees to self-manage their home SSID.

The following image illustrates the Juniper Mist Teleworker solution:



## Switch Proxy Service

The switch proxy service in Juniper Mist™ Edge enables you to proxy all the data packets received from the Juniper EX series switches to the Juniper Mist™ cloud. You can benefit from this service when switches are behind an HTTP proxy, a firewall with port 2200 blocked, or when the switch cannot access the Internet. If a firewall exists between the Juniper Mist Edge device and the switch, you need to allow outbound access on TCP port 2222 (configurable) to the management port of the switch.

### RADIUS Proxy Service

In a Juniper Mist™ network, you can use access points (APs) as the source of Remote Authentication Dial-In User Service (RADIUS) Access-Request messages. If your network requires a centralized source of RADIUS requests, then you can benefit from the RADIUS proxy service on Juniper Mist Edge. The RADIUS proxy acts as a RadSec (Secure Radius) server toward the wireless AP (acting as NAS - Network access server) and as a client toward the RADIUS servers.

When you enable RADIUS proxy service on Mist Edge, instead of adding each AP in the site as individual RADIUS clients, you just need to add only one IP (the RADIUS proxy).

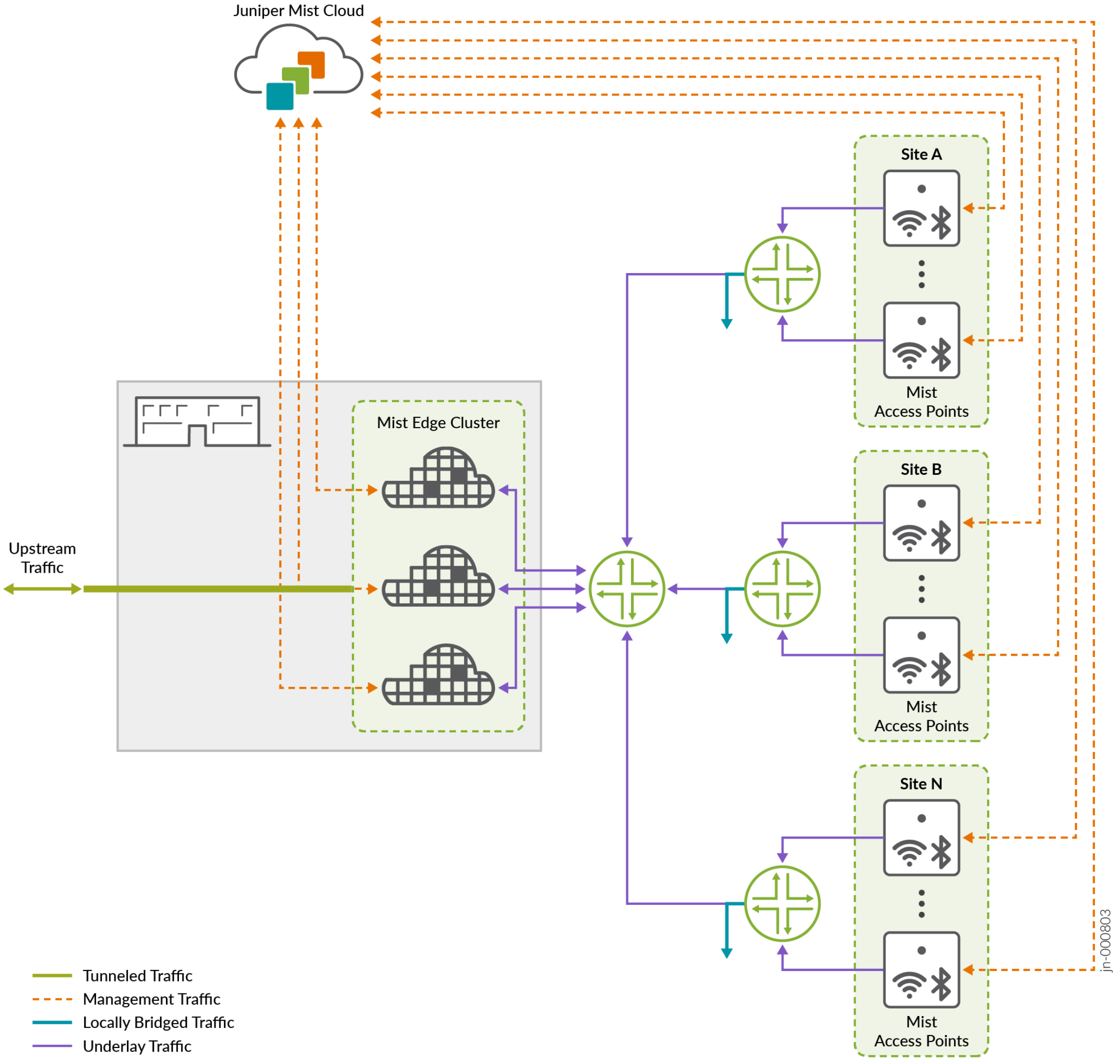
# Juniper Mist Edge Architecture

The components of the Juniper Mist Edge centralized architecture solution include the following:

- Juniper Access Points
- Juniper Mist Edge appliances

Figure 1 on page 7 illustrates the architecture of Juniper Mist Edge and the configuration components.

**Figure 1: Juniper Mist Edge Centralized Architecture**



The Juniper Mist Edge architecture includes the following configuration components:

- Juniper Mist Edge—This component includes the hardware or virtual appliance. Within the Juniper Mist Edge configuration, you can configure the tunnel IP or hostname to which the access points (APs) form a tunnel.
- Juniper Mist Edge cluster—You can configure cluster at the Org level and at the Site level.
    - Org Level —You can configure an Org level cluster, when APs from multiple sites are required to tunnel to a centralized location (DC).

  A cluster can have a single edge to multiple edges. Juniper Mist Edge must be a part of a cluster to actively terminate tunnels from the AP. Under normal operation, the members within a cluster are in active/active mode and load-balance all the AP tunnels.

  - Site Level —You can configure Juniper Mist Edge as a Site Edge, for deployments when :

    - You want the traffic to be tunneled at each site due to the underlying network constraints or security concerns

    - You have many sites with site-specific Juniper Mist Edge appliances and you want to reuse a WLAN template for ease of operation

    - Only APs from a single site need to be tunneled to a Juniper Mist Edge

- Juniper Mist tunnels—The tunnel configuration decides the primary cluster and the secondary cluster for AP tunnel termination. The Juniper Mist tunnel object contains the attributes that determine the tunnel protocol, endpoints, tunneled VLANs, tunnel failover timers, automatic preemption, and other features.

- Juniper Mist WLAN template—A WLAN template is a collection of WLAN policies, tunneling policies and WxLAN policies. Instead of repeating a given configuration across multiple service set identifiers (SSIDs), with WLAN templates you can set it once and then attach APs to the template to automatically inherit the setting.

2

CHAPTER

# When to Consider Juniper Mist Edge for your network

# Deployment Considerations

Juniper Mist leverages Juniper Mist Edge appliance when an organization needs to retain a centralized datapath architecture for campus or branch deployments. Juniper Mist Edge provides increased network flexibility and operational efficiency. By deploiyng Juniper Mist Edge in your network, you can :

- Retain the centralized datapath if you are migrating from legacy controller based architecture.
- Effectively manage broadcast and multicast traffic, prevent excessive flooding, and to avoid MAC table overflow.
- Extend VLANs to distributed branches and telecommuters to replace remote VPN technology.
- Separate guest access and corporate traffic.
- Provide dynamic traffic segmentation for IoT devices.
- Expand microservices on the campus for scalable and resilient wireless operations,management, troubleshooting, and analytics.
- Deploy networks with an expected number of wireless clients exceeding 2000 in a segment (across all VLANs).

3

CHAPTER

# How to Choose a Juniper Mist Edge Model

# Access Point Scale Considerations

Juniper Mist Edge supports an elastically scalable cluster that has an unlimited number of nodes. The scalable cluster includes options for backup clusters. The Juniper Mist Edge cluster design for the tunneling microservice depends on the aggregate capacity considerations for several access points (APs) and clients, and on throughput expectations.

The Juniper Mist cloud solution can scale to manage, configure, and monitor thousands of APs without an on-premises controller-managed topology. You can choose the appropriate edge for your deployment by referring to the metrics mentioned in Table 1 on page 12.

**NOTE**: For medium and large campus deployments, we recommend the Mist Edge X6 device with 80 percent maximum AP capacity considering failover as well as growth.

**Table 1: Juniper Mist Edge Models with Metrics**

| Key Metrics | Mist Edge – X1-M | Mist Edge – X5 | Mist Edge – X5-M | Mist Edge – X10 | Mist Edge-X6 |
|---|---|---|---|---|---|
| Number of Access Points | 500 | 5000 | 5000 | 10,000 | 5000 |
| Number of Clients | 5000 | 50,000 | 50,000 | 100,000 | 100,000 |
| Maximum Throughput | 4 Gbps | 20 Gbps | 40 Gbps | 40 Gbps | 100 Gbps |

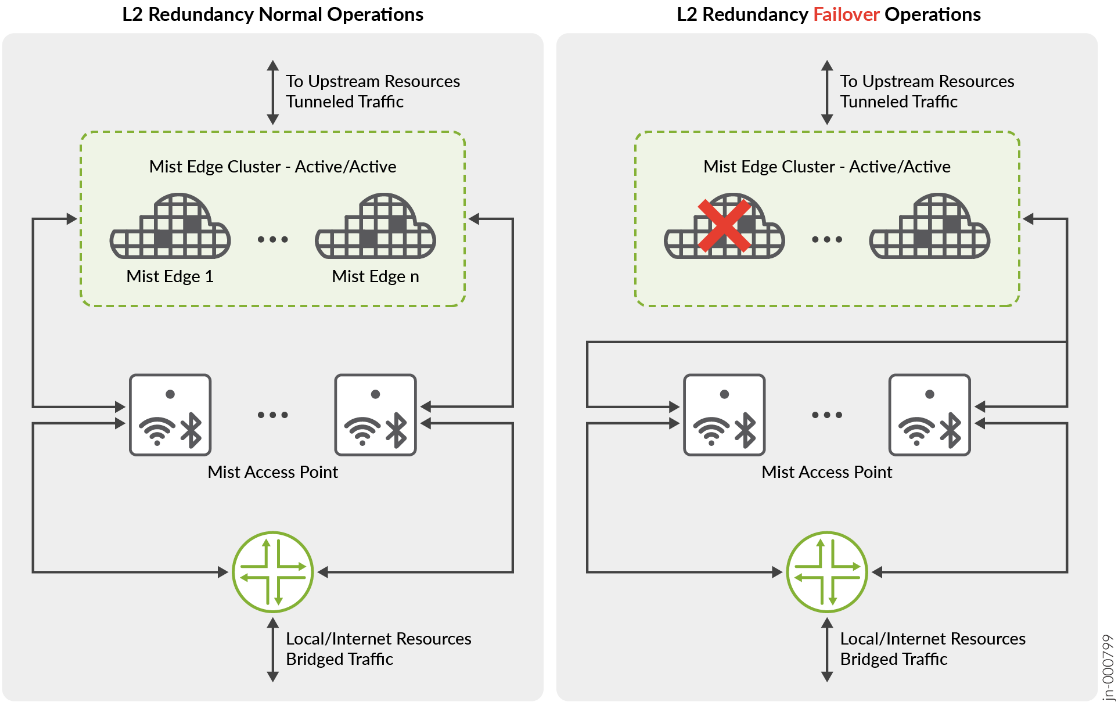
4

CHAPTER

# How to Design the Deployment of Juniper Mist Edge

# Layer 2 Redundancy Design Consideration

APs located at multiple sites can terminate tunnels to Juniper Mist Edge devices that belong to the same cluster. The Juniper Mist tunnel configuration determines the primary cluster where APs perform tunnel termination. To ensure Layer 2 redundancy, the cluster must consist of a minimum of two Juniper Mist Edge devices.. This arrangement provides robust network coverage and enhances overall system reliability. Additionally, regardless of the number of Juniper Mist edges in a cluster, all the edges are active and ensures load-balance of AP tunnels across the edges. The Juniper Mist cloud sends a list of Juniper Mist Edge devices to APs for tunnel termination. Each AP receives a list with a different order of Juniper Mist Edge devices. This order determines the preferred Juniper Mist Edge device for each AP. The following illustration depicts Layer 2 redundancy normal operations and failover operations in a Layer 2 redundancy deployment.



If multiple Juniper Mist Edge devices reside on the same Layer 2 segment in your network, we recommend you to:

- Add the Juniper Mist Edge devices to the same cluster in the active/active mode.
- Design for 80 percent capacity of the total number of tunnels on Juniper Mist Edge to keep additional capacity for failover.

For example, plan for 4000 AP tunnels (which is 80 percent of the maximum number of tunnels), for an ME-X5-M SKU, which supports a maximum of 5000 AP tunnels.

- Temporarily oversubscribe the tunnel service only when multiple Juniper Mist Edge devices disconnect from the network.

When multiple sites tunnel traffic to a cluster with more than one Juniper Mist Edge device, APs from within a site may terminate tunnels on different edge devices. This behavior achieves optimal load balancing and is therefore the default and recommended behavior. However, you can tunnel traffic from a particular site to terminate on the same Mist edge by configuring **Tunnel Host Selection** under the Juniper Mist Clusters in the Juniper Mist portal. You can select:

- Shuffle—Default option.
- Shuffle by Site—Configure APs on a single site to terminate on a same edge device within a cluster. If you select this option, remember to plan for the capacity of the edge device based on the largest AP site.

Figure 2 on page 15 illustrates the tunnel selection in a campus deployment when you select **Shuffle** option.

**Figure 2: Tunnel Host Selection-Shuffle**

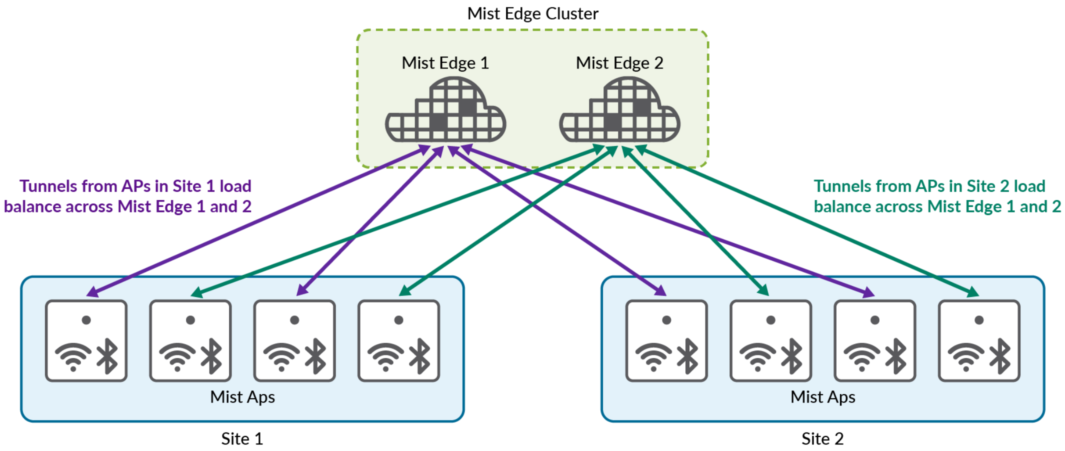
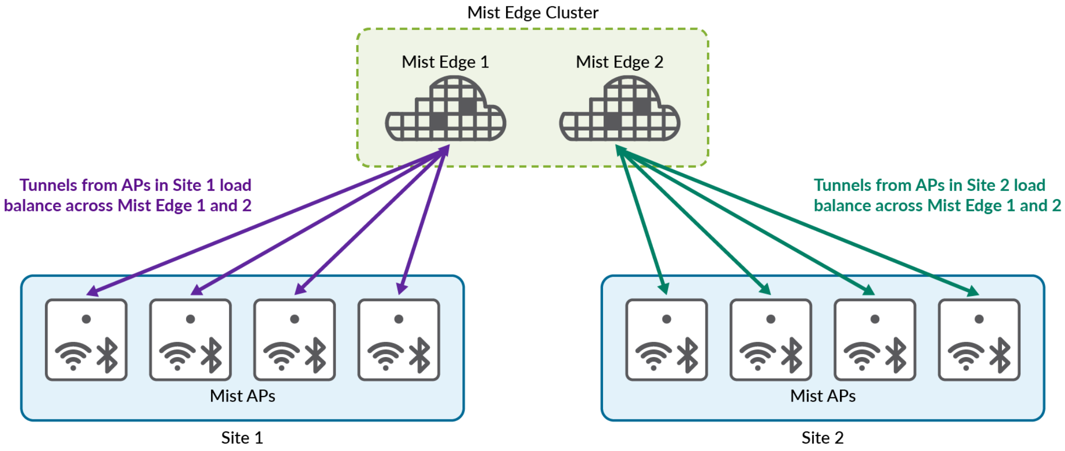

Mist Edge Cluster
Mist Edge 1
Mist Edge 2
Tunnels from APs in Site 1 load balance across Mist Edge 1 and 2
Tunnels from APs in Site 2 load balance across Mist Edge 1 and 2
Mist Aps
Site 1
Mist Aps
Site 2

Figure 3 on page 16 illustrates tunnel selection in a campus deployment when you select **Shuffle by Site**.

**Figure 3: Tunnel Host Selection-Shuffle by Site**


Mist Edge Cluster
Mist Edge 1
Mist Edge 2
Tunnels from APs in Site 1 load balance across Mist Edge 1 and 2
Tunnels from APs in Site 2 load balance across Mist Edge 1 and 2
Mist APs
Site 1
Mist APs
Site 2

# Layer 3 (Data Center) Considerations

When you design data center redundancy or traffic separation between the Layer 3 data centers, separate the Juniper Mist Edge devices into primary and secondary clusters. Juniper Mist Edge devices in primary cluster are in an active mode and edge devices in secondary cluster are in standby mode. This arrangement is an active-standby deployment. Each cluster in the distributed data centers may have one or more edges.

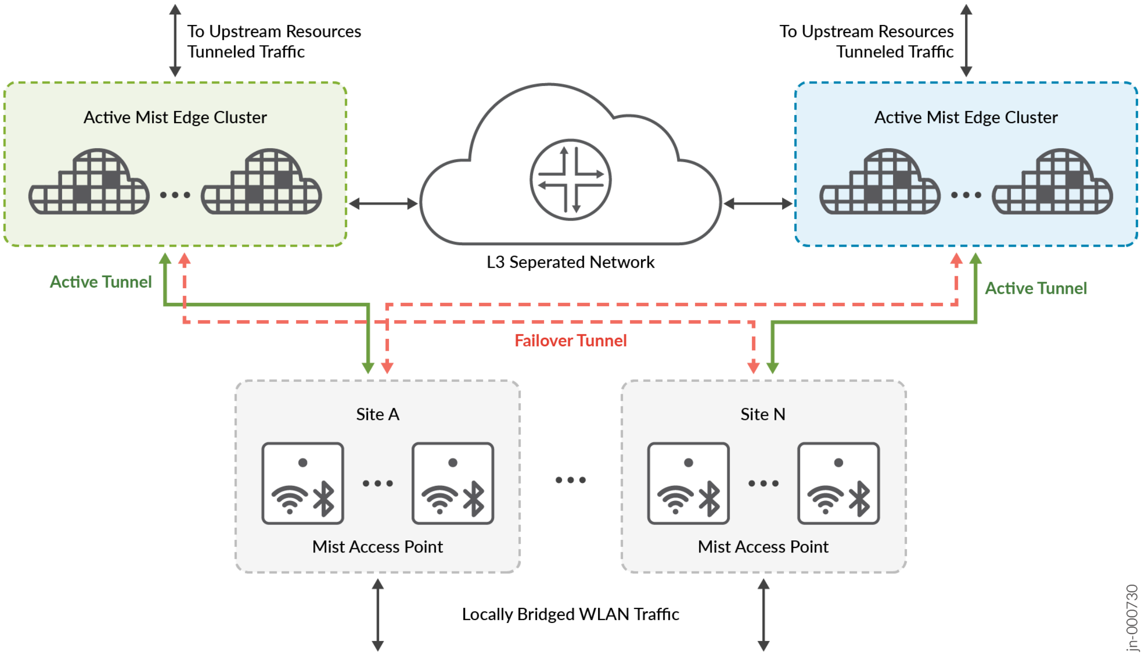
You can also achieve Layer 3 redundancy with one edge device each in the primary and secondary clusters. However, having more than one edge in each cluster provides maximum benefit by achieving both same cluster as well as across cluster redundancy.

You can use the Juniper Mist portal to handle up to two cluster failovers. With this capability, you ensure optimal network management in your campus deployment. However, if you need additional levels of failover protection, Juniper Mist API provides you more flexibility to customize the configuration.

To maximize the resource utilizations and balance the load across the datacenter, you can configure multiple Mist Tunnels from WLAN on APs, where one Mist Edge cluster is primary (active) for one set of tunnels and secondary (standby) for remaining set of tunnels.

See the following illustration and configuration. The left part marked in green depicts a primary cluster and the right part marked in blue. depicts a secondary cluster. Note that the AP does not form concurrent tunnels to a secondary cluster member, dotted lines are for illustration only.

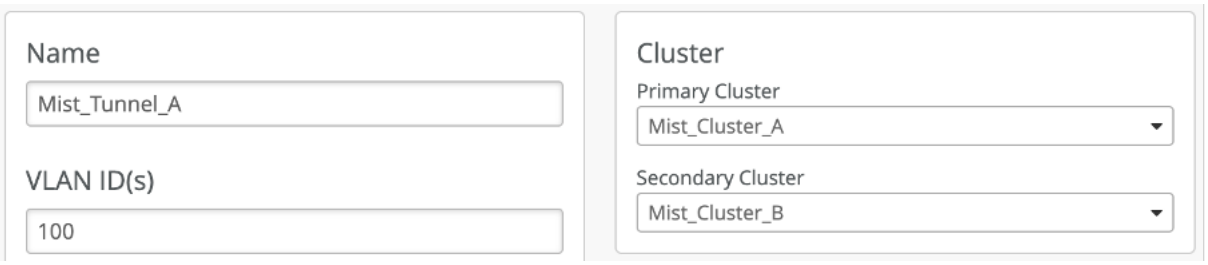
**Figure 4: Data Center Redundancy or Separation in Layer 3**



You can achieve a similar configuration as illustrated in Figure 4 on page 17 by using the options on the Juniper Mist Tunnel page, which is accessible from the Juniper Mist portal.

To achieve this configuration, you select and configure the **Primary Cluster** and **Secondary Cluster** options on the Juniper Mist Tunnel page. You can use the same tunnel object for mapping the tunneled WLAN in the WLAN configuration at multiple sites. The tunnel object must have **Mist Cluster A** as the preferred cluster and **Mist Cluster B** for Layer 3 redundancy. Juniper Access Points do not support simultaneous active and standby tunnels.

**Figure 5: Tunnel Configuration in Sites A, B, and C**



Name

Mist_Tunnel_A

VLAN ID(s)

100

Cluster

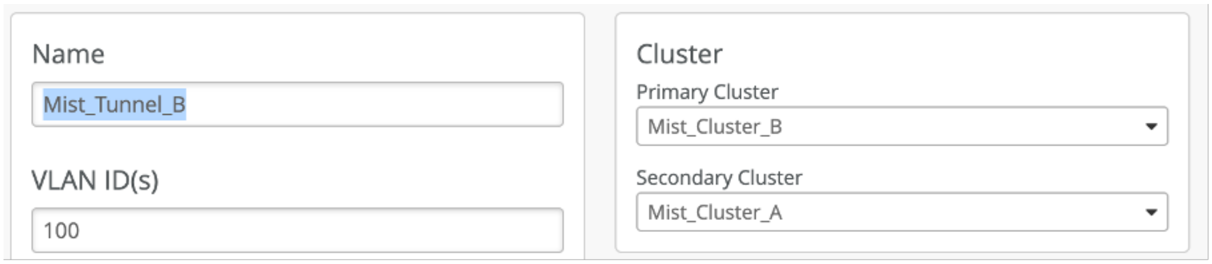
Primary Cluster

Mist_Cluster_A

Secondary Cluster

Mist_Cluster_B

Figure 6: Tunnel Configuration in Sites D, E, and F



Name

Mist_Tunnel_B

VLAN ID(s)

100

Cluster

Primary Cluster

Mist_Cluster_B

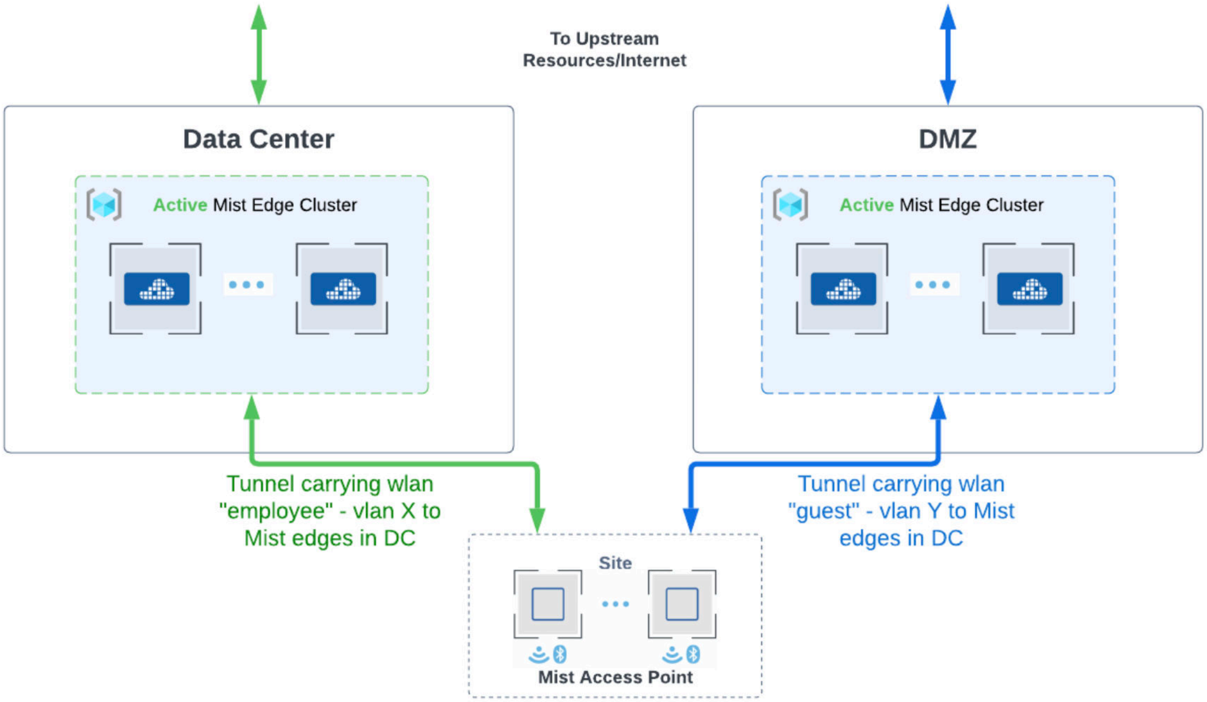
Secondary Cluster

Mist_Cluster_A

# Dual Tunnel

You can configure Juniper Mist APs to tunnel traffic to two different Juniper Mist Edge Clusters that are geographically or L3 separated in the WLAN configuration page. This is the recommended architecture for customers migrating from legacy controller architecture that do anchor tunnel or site to site tunnels.

Figure 7: Architecture for Dual Tunnels


To Upstream Resources/Internet
Data Center
Active Mist Edge Cluster
DMZ
Active Mist Edge Cluster
Tunnel carrying wlan "employee" - vlan X to Mist edges in DC
Tunnel carrying wlan "guest" - vlan Y to Mist edges in DC
Site
Mist Access Point

In case you cannot implement the architecture illustrated in Figure 7 on page 18 due to the underlying network limitations, Juniper Mist Edges support Anchor Tunnels for Site to DMZ tunnels.

# Failover Tunnel Timers

You can use the failover timer to determine the time span for which an access point (AP) waits before it fails over to another Juniper Mist Edge device.

APs tunnel traffic to multiple edge devices, by adjusting the failover timers for each tunnel. You can therefore fine-tune the performance of the VLANs that carry application-sensitive data between the AP and the Juniper Mist Edge device.

**NOTE**: Do not configure a very aggressive failover timer if the network experiences latency and packet loss.

You can refer to the following table to configure tunnel timers for a Juniper Mist tunnel.

**Table 2: Recommended Timers**

| Timers | Hello Interval | Retries | Total Time before Failover (Worst Case) |
|---|---|---|---|
| Aggressive | 15 | 4 | Approximately 30 seconds<br>(15 seconds +1+2+4+8) |
| Default | 30 | 4 | Approximately 45 seconds<br>(30 seconds+1+2+4+8) |

Hello interval is used as a heartbeat to detect if a tunnel is alive. It ranges from 0.5 second through 300 seconds. The default vlaue for the hello interval is 60 seconds.

# Port and IP Address Configuration Requirements

IN THIS SECTION

Each Juniper Mist™ Edge device requires a minimum of two IP addresses. Juniper Mist Edge IP address and port configuration requirements are as follows:pane

- Out-of-Band Management (OOBM) port and IP—The port is also known as the Mist port on the appliance. The OOBM port is a dedicated interface for the Juniper Mist Edge device to communicate with the Juniper Mist cloud. Through this port, the device receives configuration information and sends telemetry and status updates for services that run on the network edge. By default, the interface receives a Dynamic Host Configuration Protocol (DHCP)-assigned IP address and has network access to the Juniper Mist cloud. With this access, the interface can successfully complete zero-touch provisioning (ZTP). After you configure the Juniper Mist Edge device, on the Juniper Mist portal, you can change the OOBM IP address mode to a static IP address.

  We recommend using the DHCP-assigned IP address for the OOBM interface to complete the initial ZTP process. However, in cases where the DHCP server is unavailable, you can log in to Juniper Mist Edge using the credentials and manually assign the IP address.

- Tunnel (Data) port and IP—An interface to which access points (APs) form a tunnel. The tunnel IP can be configure as a static IP. You can configure the tunnel IP address in the Tunnel IP Configuration page of the Juniper Mist portal.

  You can configure the data (tunnel) port as a single-arm or a dual-arm port. Depending on the number of ports selected, the Juniper Mist Edge automatically forms port channel.

  Downstream traffic is the tunneled (encapsulated) traffic that originates from the AP. Upstream data is the client (after de-encapsulation) traffic that moves toward the upstream resources in your data center.

- **NOTE**: The OOBM port and the tunnel port have different IP addresses, and these addresses must be from different subnets.

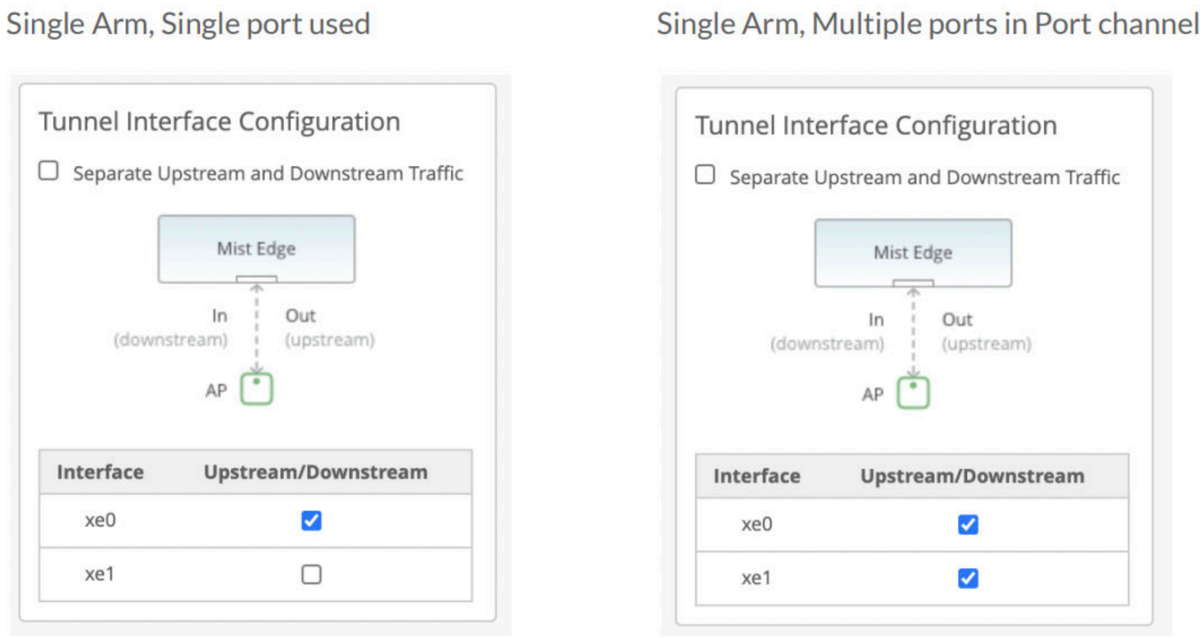
## Tunnel Port—Single-Arm and Dual-Arm Configuration

Juniper Mist Edge has multiple tunnel (data) ports. You can configure the tunnel port as a single-arm or a dual-arm port.

- A dual-arm tunnel port carries upstream and downstream traffic on two different ports. You can configure one more ports in each upstream and downstream direction. These ports automatically detect and form two LACP bundles. For dual-arm deployments, Juniper Mist Edge automatically configures each upstream data port as a trunk port. Juniper Mist Edge adds the VLANs that you configure for the Juniper Mist Tunnels as tagged VLANs. The downstream port is untagged and you must connect the port to the tunnel IP network.
- A single-arm tunnel port carries both upstream and downstream traffic. You can configure one or more ports in a single arm and these ports can automatically detect and form a Link Aggregation Control Protocol (LACP) bundle. For single-arm deployments, Juniper Mist Edge automatically configures the data port as a trunk with tunnel IP as its untagged or native VLAN. Trunk adds the VLANs that you configure under the Juniper Mist Tunnels as tagged VLANs.

The following illustration depicts the different configurations.

**Figure 8: Examples for Single-Arm Deployment**



Single Arm, Single port used

Tunnel Interface Configuration

□ Separate Upstream and Downstream Traffic

| Interface | Upstream/Downstream |
|---|---|
| xe0 | ☑ |
| xe1 | □ |

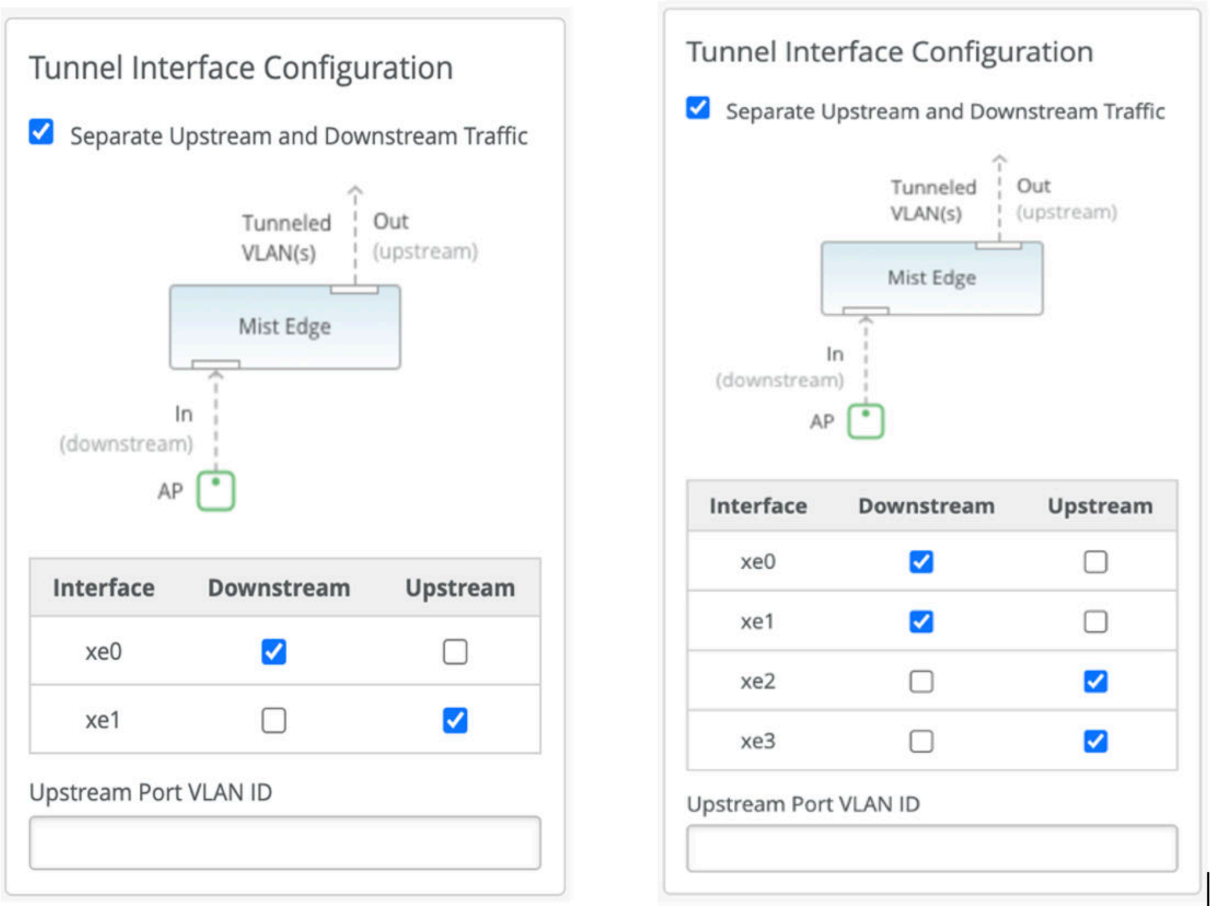
Single Arm, Multiple ports in Port channel

Tunnel Interface Configuration

□ Separate Upstream and Downstream Traffic

| Interface | Upstream/Downstream |
|---|---|
| xe0 | ☑ |
| xe1 | ☑ |

**Figure 9: Examples for Dual-Arm Deployment**



Tunnel Interface Configuration

☑ Separate Upstream and Downstream Traffic

| Interface | Downstream | Upstream |
|---|---|---|
| xe0 | ☑ | □ |
| xe1 | □ | ☑ |

Upstream Port VLAN ID

Tunnel Interface Configuration

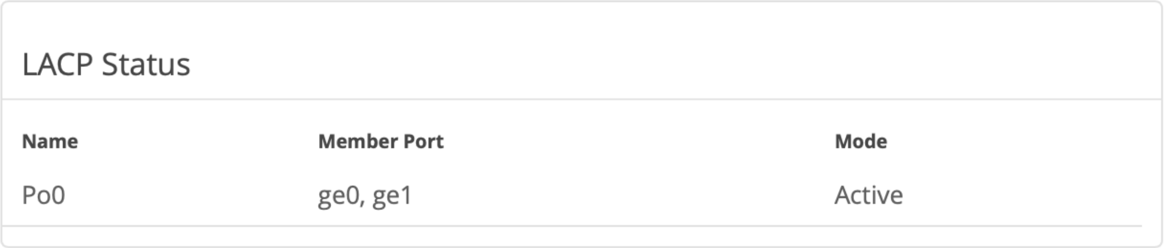
☑ Separate Upstream and Downstream Traffic

| Interface | Downstream | Upstream |
|---|---|---|
| xe0 | ☑ | □ |
| xe1 | ☑ | □ |
| xe2 | □ | ☑ |
| xe3 | □ | ☑ |

Upstream Port VLAN ID

You can monitor the LACP status on the Mist Edge Insights page on the Juniper Mist portal. You can see a sample LACP status report in the following illustration.

**Figure 10: LACP Status Report**



LACP Status

| Name | Member Port | Mode |
|---|---|---|
| Po0 | ge0, ge1 | Active |

# Additional Features and Services

IN THIS SECTION

This document describes the additional features and services that you can configure on a Juniper Mist™ Edge appliance.

## Autopreemption

An access point (AP) will failover to the next Edge appliance within the Layer 2 (L2) cluster or to its backup Layer 3 (L3) cluster in the following instances:

- During a temporary network disruption
- When an AP is unable to reach or exchange hellos successfully with its preferred edge

Autopreemption is a mechanism through which APs are nudged to terminate the tunnels on the preferred peer, assuming that the peer is reachable.

The feature is disabled by default. With the default presets, if an AP tunnel fails over to a nonpreferred Edge appliance, the AP continues forwarding traffic to that appliance. You can move these AP tunnels manually by preempting or disconnecting the tunnels through the API or the Juniper Mist portal.

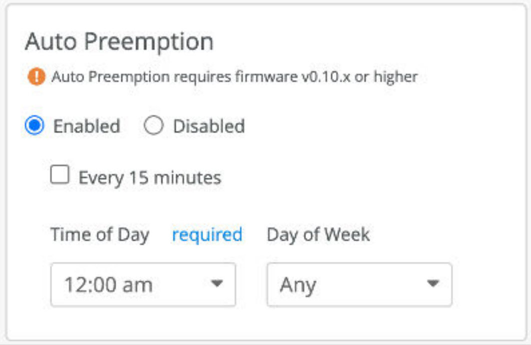
You can configure preemption at individual Mist tunnels. When you enable this feature, the cloud orchestrates the preemption and slowly moves the AP tunnels to preferred Edge appliances to cause the least traffic disruption. A service running in the cloud monitors for any APs that have failed over from a preferred Edge appliance, given that the appliance is up and healthy.

Based on the options selected from the following list, the cloud nudges the AP to disconnect from the current Edge appliance and move to the preferred peer. Clients on the AP are not deauthenticated.

- **Every 15 minutes**—If the connectivity between the APs and the Mist Edge cluster is jittery, AP tunnels may end up failing over to a Mist Edge from a secondary cluster. This failover may cause clients to do get renewed IP addresses from the DHCP server, if the secondary edge is in an L3-separated data center with a different IP schema. In such cases, we recommend that you use the option of Every 15 minutes.

> **NOTE**: In most cases you do not need this setting of Every 15 minutes. We recommend you to use Time of the day for off hours.

- **Time of the day**—You can specify a time of the day during which you want to move APs back to the preferred edge, if the APs have failed over between the specified times. We recommend choosing a day and time of day when your network is least busy.



Auto Preemption

! Auto Preemption requires firmware v0.10.x or higher

● Enabled ○ Disabled

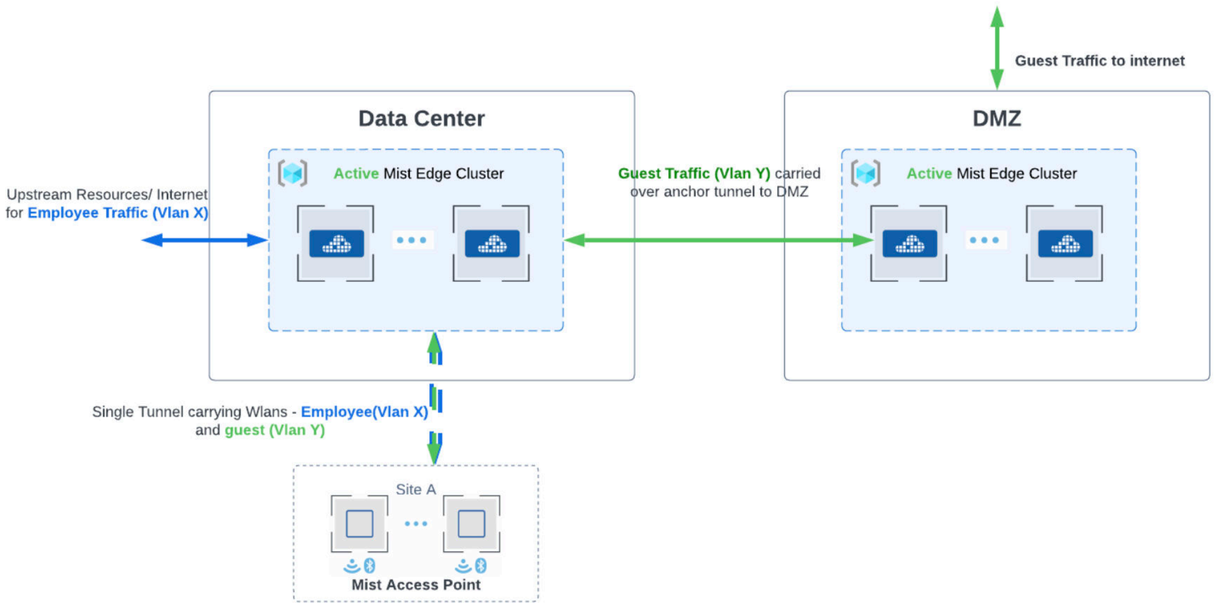
□ Every 15 minutes

Time of Day required: 12:00 am

Day of Week: Any

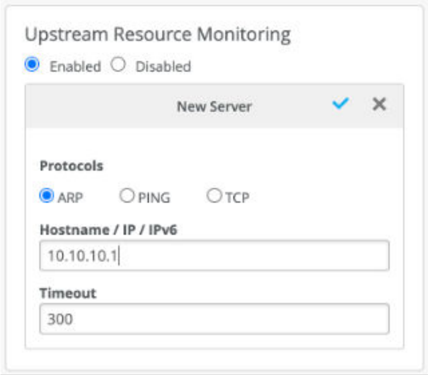
## Anchor Tunnel

In specific deployments where traffic must be tunneled to a DMZ area deeper in the data centers, you can use anchor tunnels. Anchor tunnels enable you to configure Juniper Mist Edge to carry all traffic to DMZ and to tunnel specific traffic to another Mist Edge. You configure an anchor tunnel from the Mist Tunnel page.


Guest Traffic to internet
Data Center
DMZ
Active Mist Edge Cluster
Active Mist Edge Cluster
Upstream Resources/ Internet
for Employee Traffic (Vlan X)
Guest Traffic (Vlan Y) carried
over anchor tunnel to DMZ
Single Tunnel carrying Wlans - Employee(Vlan X)
and guest (Vlan Y)
Site A
Mist Access Point

## Critical Resource Monitoring (CRM)

You can configure Juniper Mist Edge to monitor the health of the upstream resources. This configuration helps determine the reachability of those resources from the Juniper Mist Edge data ports. If the health check of the upstream resource fails, the Juniper Mist Edge prompts the APs to failover to the next member and shuts down the tunnel terminator service temporarily. The shutdown continues until the upstream resources are healthy and reachable again.



Upstream Resource Monitoring

● Enabled ○ Disabled

New Server ✓ ✕

Protocols

● ARP ○ PING ○ TCP

Hostname / IP / IPv6

10.10.10.1

Timeout

300

You can configure the upstream resource monitoring on the **Mist Cluster** page. The option is disabled by default. Protocols to monitor a resource include ARP, PING, and TCP. You can configure multiple resources using different protocols to monitor the health check. Even if one of the health checks fails, the Juniper Mist Edge prompts the APs to failover to another edge. Commonly used health checks are ARPing or PINGing the default gateways.

# Alerts

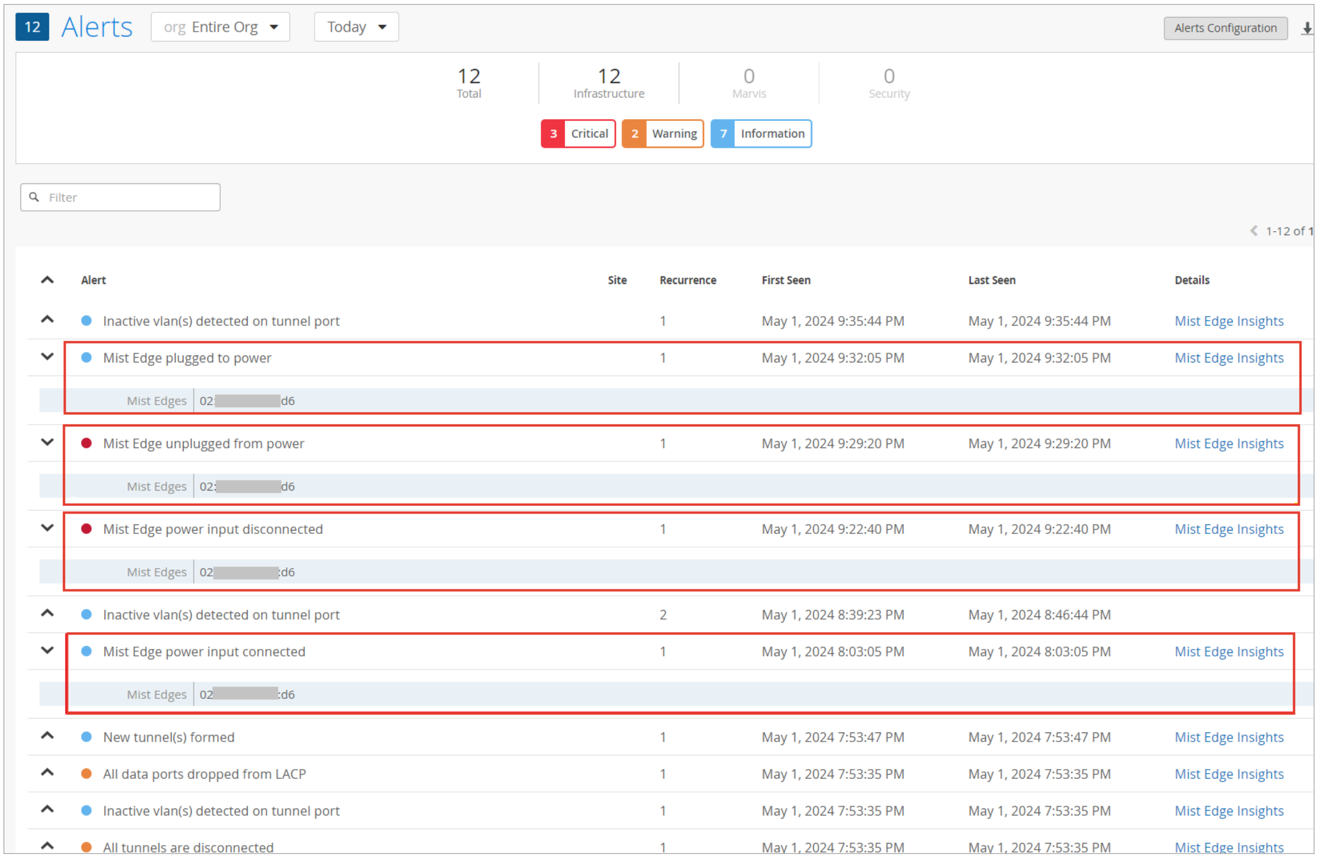
The Alerts Dashboard gives you visibility into issues with Mist Edge devices deployed across your sites. The dashboard provides information about all alerts that you enable on the Alerts Configuration page. You can also enable e-mail notifications for issues that you want to monitor closely or forward the alerts as webhooks. For information about configuring alerts, see Configure Alerts and Email Notifications. For information about webhook alerts, see Webhooks and Alerts.

You can configure alerts to monitor:

- Resource usage
- Cloud connection status
- PSU status
- Power cable status
- Service status

For a list of alerts that you can enable for your Mist Edge device, see Juniper Mist Alert Types.

Here is a sample screenshot that shows the alerts for Mist Edges:



| Alert | Site | Recurrence | First Seen | Last Seen | Details |
|---|---|---|---|---|---|
| ● Inactive vlan(s) detected on tunnel port | | 1 | May 1, 2024 9:35:44 PM | May 1, 2024 9:35:44 PM | Mist Edge Insights |
| ● Mist Edge plugged to power | | 1 | May 1, 2024 9:32:05 PM | May 1, 2024 9:32:05 PM | Mist Edge Insights |
| Mist Edges 02[redacted]d6 | | | | | |
| ● Mist Edge unplugged from power | | 1 | May 1, 2024 9:29:20 PM | May 1, 2024 9:29:20 PM | Mist Edge Insights |
| Mist Edges 02:[redacted]d6 | | | | | |
| ● Mist Edge power input disconnected | | 1 | May 1, 2024 9:22:40 PM | May 1, 2024 9:22:40 PM | Mist Edge Insights |
| Mist Edges 02[redacted]:d6 | | | | | |
| ● Inactive vlan(s) detected on tunnel port | | 2 | May 1, 2024 8:39:23 PM | May 1, 2024 8:46:44 PM | |
| ● Mist Edge power input connected | | 1 | May 1, 2024 8:03:05 PM | May 1, 2024 8:03:05 PM | Mist Edge Insights |
| Mist Edges 02[redacted]:d6 | | | | | |
| ● New tunnel(s) formed | | 1 | May 1, 2024 7:53:47 PM | May 1, 2024 7:53:47 PM | Mist Edge Insights |
| ● All data ports dropped from LACP | | 1 | May 1, 2024 7:53:35 PM | May 1, 2024 7:53:35 PM | Mist Edge Insights |
| ● Inactive vlan(s) detected on tunnel port | | 1 | May 1, 2024 7:53:35 PM | May 1, 2024 7:53:35 PM | Mist Edge Insights |
| ● All tunnels are disconnected | | 1 | May 1, 2024 7:53:35 PM | May 1, 2024 7:53:35 PM | Mist Edge Insights |

## QoS

By default, Mist Edge tunnels the packets by preserving the inner packet's DSCP by copying it onto the outer L2TP packet. Juniper Mist Edge can also run DHCP Proxy and IGMP snooping services that are configured under the specific Juniper Mist Edge page.