

## IN FOCUS

---

# Junos<sup>®</sup> OS Release 19.4

Published  
2019-12-23

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

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.

*IN FOCUS Junos<sup>®</sup> OS Release 19.4*

Copyright © 2019 Juniper Networks, Inc. All rights reserved.

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

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

## **Start Here with Junos OS Release 19.4**

**What You Need to Know About the In Focus Guide | 7**

**Important Features in Junos OS Release 19.4 | 7**

2

## **Junos Multi-Access User Plane**

**Junos Multi-Access User Plane | 11**

Junos Multi-Access User Plane Overview | 12

Benefits of Junos Multi-Access User Plane | 14

3

## **Protect and Reroute Traffic Using BGP Labeled Unicast**

**How to Protect and Reroute Traffic Using BGP Labeled Unicast | 19**

How BGP Prefix Independent Convergence Work? | 19

BGP PIC Edge over BGP Labeled Unicast Overview | 20

Key Benefits of BGP PIC Edge Using BGP Labeled Unicast Transport Protocol | 21

4

## **Wi-Fi Mini-PIM**

**Wi-Fi Mini-PIM Configuration | 25**

Wi-Fi Mini-Physical Interface Module Overview | 25

Features Supported on the Wi-Fi Mini-PIM | 26

Benefits of Using the Wi-Fi Mini-PIM | 27

# 1

CHAPTER

## Start Here with Junos OS Release 19.4

---

[What You Need to Know About the In Focus Guide | 7](#)

[Important Features in Junos OS Release 19.4 | 7](#)

---



# What You Need to Know About the In Focus Guide

Use this guide to quickly learn about important features in this Junos OS Release 19.4 and how you can deploy them in your network.

You might also be interested in seeing the complete list of features in the [Release Notes for Junos OS Release 19.4](#). In addition to this guide, you can find detailed information on concepts, configuration, and examples in the [Junos OS documentation](#).

Want to tell us what you think about this guide? E-mail us at [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net).

## Important Features in Junos OS Release 19.4

For details on these features, go to the other chapters in this guide or click the link in the feature description below.

- **Inline monitoring services (MX Series with MPCs excluding MPC10E and MPC11E linecards)**—Starting in Junos OS Release 19.4R1, you can configure a new monitoring technology that provides the flexibility to monitor different streams of traffic at different sampling rates on the same interface. You can also export the packet up to the configured clip length to a collector in an IP Flow Information Export (IPFIX) format. The IPFIX format includes important metadata information about the monitored packets for further processing at the collector.

The inline monitoring services overcome the limitations of traditional sampling technologies, such as JFlow, sFlow, and port mirroring, thereby providing you the benefit of effective sampling and troubleshooting processes.

[See *How to Configure Inline Monitoring Services*.]

- **Integrating RIFT protocol into Junos OS (MX Series, QFX Series, and VMX virtual routers)**—Starting in Junos OS Release 19.4R1, you can integrate a new IGP protocol, Routing in Fat Tree (RIFT), into Junos OS to route packets in variants of CLOS-based and fat tree network topologies (also called the spine and leaf model).

The RIFT protocol is capable of automatic construction of fat-tree topologies, providing you the benefit of having a close to zero necessary configuration. RIFT makes networks resilient, extensively traceable, and simpler to manage, thereby overcoming the deployment limitations of evolving IP fabrics.

[See *How to Integrate RIFT protocol into Junos OS*.]

- **Junos Multi-Access User Plane (MX240, MX480, MX960)**—With Junos OS Release 19.4R1, we introduce Junos Multi-Access User Plane, a software solution that turns your MX router into a high-capacity user plane function called a System Architecture Evolution Gateway-User Plane (SAEGW-U). This MX

SAEGW-U interoperates with a third-party SAEGW-C (control plane function), per 3GPP Release 14 Control User Plane Separation (CUPS) architecture, to provide high-throughput 4G and 5G fixed-wireless access service with support for 5G non-stand-alone (NSA) mode. CUPS enables independent scaling of the user and control planes, network architecture flexibility, operational flexibility, and an easier migration path from 4G to 5G services. The CUPS architecture is optional for 4G but inherent in 5G architecture.

To transform your MX240, MX480, or MX960 router into an SAEGW-U, all you need is at least one MPC7 linecard, a routing engine with at least 32GB memory, and Junos OS Release 19.4R1.

[See [“Junos Multi-Access User Plane” on page 11.](#)]

- **Microsoft Azure Key Vault (HSM) integration (vSRX 3.0)**—Starting in Junos OS Release 19.4R1, vSRX 3.0 is integrated with Microsoft Azure Key Vault hardware security module (HSM). With the integration of Microsoft Azure Key vault HSM, vSRX can protect and manage sensitive data such as private cryptographic keys, passwords, and configurations.

[See *Deployment of Microsoft Hardware Security Module on vSRX 3.0.*]

- **Support for BGP PIC Edge with BGP labeled unicast (MX Series and PTX Series)**—Starting with Junos OS Release 19.4R1, MX Series and PTX Series routers support BGP PIC Edge with BGP labeled unicast as the transport protocol. BGP PIC Edge using the BGP labeled unicast transport protocol helps to protect and reroute traffic when border nodes (ABR and ASBR) failures happen in multi-domain networks. Multi-domain networks are typically used in Metro Ethernet aggregation and Mobile Backhaul networks designs.

[See [“How to Protect and Reroute Traffic by Configuring BGP PIC Edge Using BGP Labeled Unicast as the Transport Protocol” on page 19.](#)]

- **Support for flexible algorithm in IS-IS for segment routing–traffic engineering (MX Series and PTX Series)**—Starting in Junos OS Release 19.4R1, you can thin slice a network by defining flexible algorithms that compute paths using different parameters and link constraints based on your requirements. For example, you can define a flexible algorithm that computes a path to minimize IGP metric and define another flexible algorithm to compute a path based on SPF calculation type to divide the network into separate planes. This feature allows networks without a controller to configure traffic engineering and utilize segment routing capability of a device.

To define a flexible algorithm, include **flex-algorithm** statement at the **[edit routing-options]** hierarchy level.

To configure participation in a flexible algorithm include the **flex-algorithm** statement at the **[edit protocols isis segment routing]** hierarchy level.

[See *How to Configure Flexible Algorithm in IS-IS for Segment Routing Traffic Engineering.*]

- **Wi-Fi Mini-Physical Interface Module (SRX320, SRX340, SRX345, and SRX550M)**—In Junos OS Release 19.4R1, we introduce the Wi-Fi Mini-Physical Interface Module (Mini-PIM) for SRX320, SRX340, SRX345, and SRX550M. For retail and small offices, the Wi-Fi Mini-PIM provides secure wireless LAN connectivity to endpoint devices. The Wi-Fi Mini-PIM supports 802.11ac wave 2 wireless standards.

[See [Wi-Fi Mini-Physical Interface Module Overview.](#)]

# 2

CHAPTER

## Junos Multi-Access User Plane

---

Junos Multi-Access User Plane | 11

---





# Junos Multi-Access User Plane

## SUMMARY

With Junos OS Release 19.4R1, we introduce Junos Multi-Access User Plane, a software solution that turns your MX router into a high-capacity user plane function called a System Architecture Evolution Gateway-User Plane (SAEGW-U). This MX SAEGW-U interoperates with a third-party SAEGW-C (control plane function), per 3GPP Release 14 Control User Plane Separation (CUPS) architecture, to provide high-throughput 4G and 5G fixed-wireless access service with support for 5G non-stand-alone (NSA) mode. CUPS enables independent scaling of the user and control planes, network architecture flexibility, operational flexibility, and an easier migration path from 4G to 5G services. The CUPS architecture is optional for 4G but inherent in 5G architecture.

## IN THIS SECTION

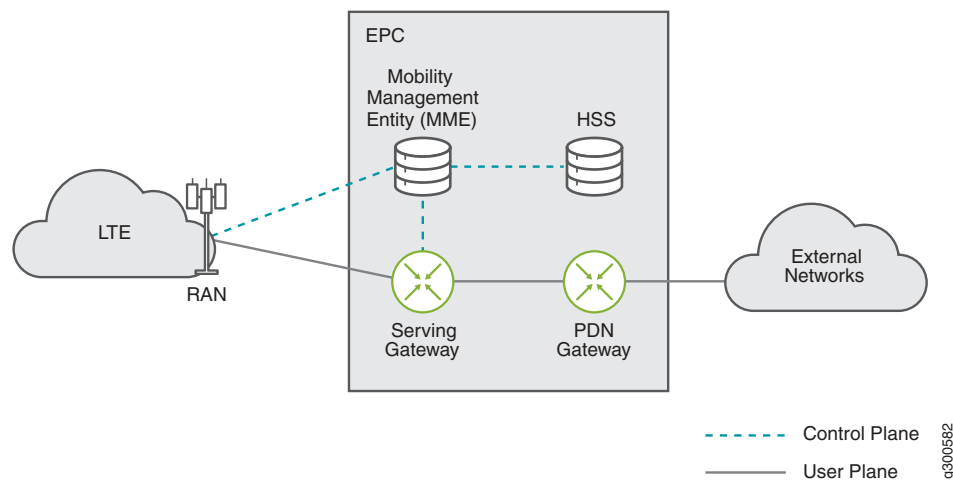
- [Junos Multi-Access User Plane Overview | 12](#)

## Junos Multi-Access User Plane Overview

The 3GPP Release 8 introduced the Evolved Packet Core (EPC) for core network architecture. As [Figure 1 on page 12](#) shows, the four main EPC network elements are:

- Serving Gateway
- Packet Data Network (PDN) Gateway
- Mobility Management Entity
- Home Subscriber Server

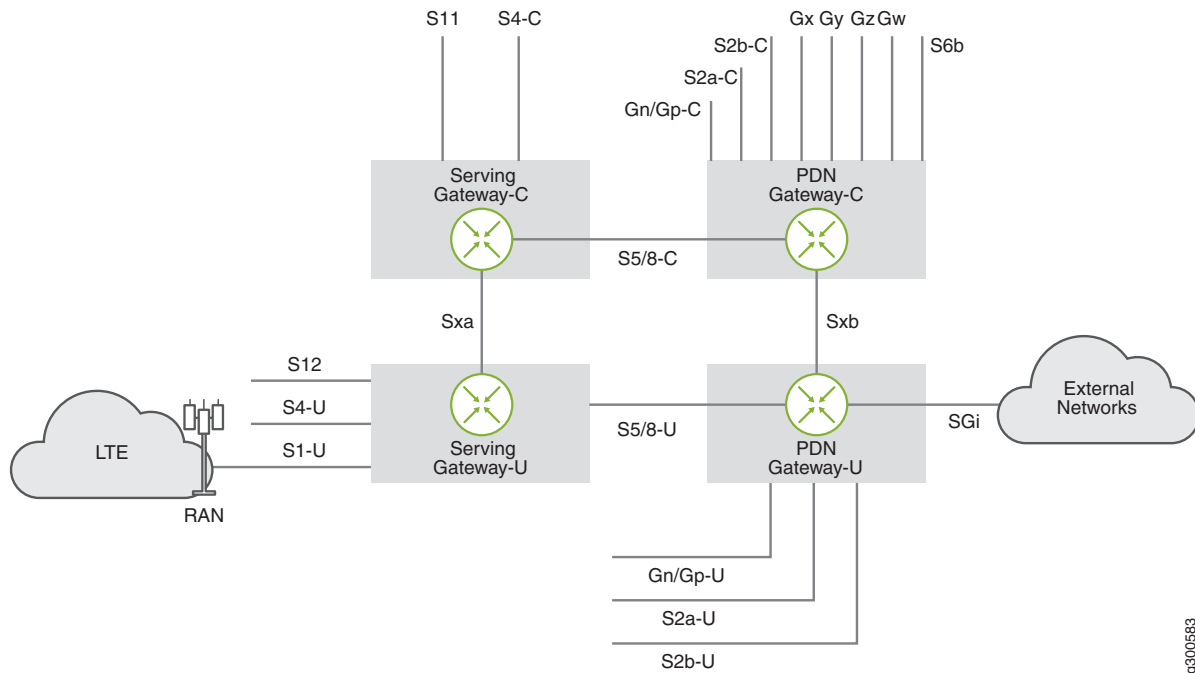
Figure 1: 3GPP Release 8 Evolved Packet Core Architecture



User Equipment (UE) has control and data path connectivity to the EPC network elements over eNodeB base stations. The EPC provides data connectivity to external networks such as the Internet.

3GPP Release 14 introduced CUPS. CUPS stands for Control and User Plane Separation, providing the architecture enhancements for the separation of functionality in the EPC's serving gateway (SGW) and PDN gateway (PGW). As [Figure 2 on page 13](#) shows, both the serving gateway and the PDN gateway of the EPC can be separated into their control plane and user plane functions. CUPS introduces new interfaces, Sxa and Sxb, between the control plane and user plane functions of the SGW and PGW, respectively. CUPS enables control plane and user plane functions to be deployed, scaled and operated separately while integrated over a standard reference interface.

Figure 2: 3GPP Release 14 CUPS Architecture



The control plane provides the following functionality:

- Receives traffic rules and actions
- Triggers accounting (volume and time of traffic)
- Makes session level announcements
- Receives usage information
- Receives user plane status information
- Northbound integration with the signaling plane

The user plane provides the following functionality:

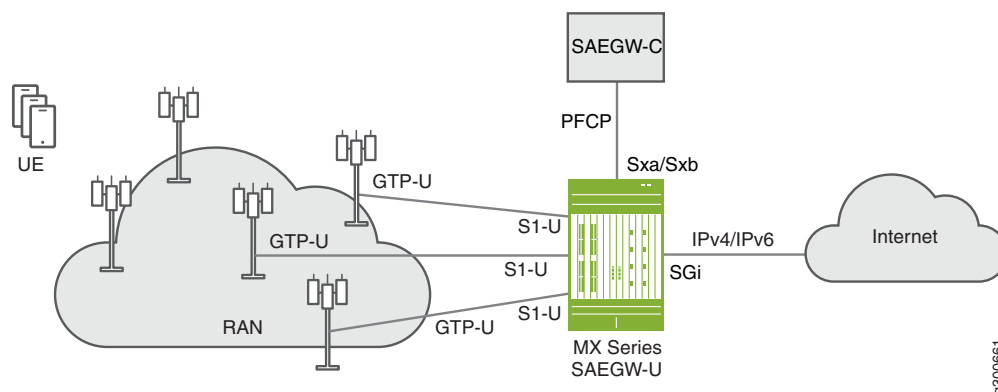
- Subscriber tunnel encapsulations (GTP-U)
- Packet routing and forwarding
- QoS and buffering
- Policy enforcement
- Statistics gathering and reporting
- Optional advanced services

The Junos Multi-Access User Plane solution is to provide a combined SGW user plane (SGW-U) and PGW user plane (PGW-U) in a single MX series router (see [Figure 3 on page 14](#)). The combined SGW-U/PGW-U

is referred to as a SAEGW-U (System Architecture Evolution Gateway-User Plane). Juniper's MX SAEGW-U can interoperate with a third-party combined SGW-C/PGW-C, hereafter referred to as SAEGW-C, through a combined Sxa/Sxb interface.

**NOTE:** Juniper's MX SAEGW-U communicates with the third-party SAEGW-C over the Sxa/Sxb interface through Packet Forwarding Control Protocol (PFCP) as specified in 3GPP TS 29.244.

**Figure 3: Junos Multi Access User Plane SAEGW-U**



### Benefits of Junos Multi-Access User Plane

With this functional separation, the control plane and user plane have very distinct deployment requirements and can be in different physical locations. While the control plane function is very complex, the user plane function simply requires high packet processing capability and rich policy enforcement. The user plane can be more distributed than the control plane and located closer to end-user access points, such as a radio access network (RAN), enabling higher bandwidth per user while delivering lower latency. Control plane and user plane separation provides the following benefits:

- Independent scaling of the user and control planes.
- Network architecture flexibility including:
  - Ability to deploy from the edge to the core.
  - Ability to segregate different traffic types and services across different user planes while maintaining a common or single control plane.
- Operational flexibility
- Easier migration path from 4G to 5G services. CUPS is optional for 4G, but is an integral part of the 5G network architecture.

## WHAT'S NEXT

For more information and full instructions on how to configure Junos Multi-Access User Plane, see [Junos Multi-Access User Plane User Guide](#).

# 3

CHAPTER

## Protect and Reroute Traffic Using BGP Labeled Unicast

---

How to Protect and Reroute Traffic Using BGP Labeled Unicast | 19

---





# How to Protect and Reroute Traffic Using BGP Labeled Unicast

## SUMMARY

Learn how to protect and reroute traffic to the destination network if a border node fails in a multi-domain network.

## IN THIS SECTION

- [How BGP Prefix Independent Convergence Work? | 19](#)
- [BGP PIC Edge over BGP Labeled Unicast Overview | 20](#)

## How BGP Prefix Independent Convergence Work?

### SUMMARY

This section talks about how BGP Prefix Independent Convergence (PIC) improves BGP convergence on network node failures.

BGP PIC creates and stores primary and backup paths for the indirect next hop on the Routing Engine and also provides the indirect next hop route information to the Packet Forwarding Engine. When a network node failure occurs, the Routing Engine signals the Packet Forwarding Engine that an indirect next hop has failed, and that the traffic is rerouted to a pre-calculated equal-cost or backup path without modifying BGP prefixes. Routing the traffic to the destination prefix continues by using the backup path to reduce traffic loss until the global convergence through BGP is resolved.

BGP convergence is applicable to both core and edge network node failures. In the case of BGP PIC Core, adjustments to the forwarding chains are made as a result of node or core link failures. In the case of BGP PIC Edge, adjustments to the forwarding chains are made as a result of edge node or edge link failures.

## BGP PIC Edge over BGP Labeled Unicast Overview

### SUMMARY

This section talks about BGP PIC Edge using the BGP labeled unicast as the transport protocol.

### IN THIS SECTION

- [Key Benefits of BGP PIC Edge Using BGP Labeled Unicast Transport Protocol | 21](#)

BGP PIC Edge using the BGP labeled unicast transport protocol helps to protect and reroute traffic when border nodes (ABR and ASBR) failures happen in multi-domain networks. Multi-domain networks are typically used in metro-aggregation and mobile backhaul networks designs.

On Juniper Networks MX Series and PTX Series routers, BGP PIC Edge supports IPv4, IPv6, BGP labeled unicast, and Layer 3 VPN services. These BGP services are multipath (learnt from multiple PEs) and resolved through BGP labeled unicast routes, which could again be a multipath learnt from other ABRs. Transport protocols supported over BGP PIC Edge are RSVP, LDP, OSPF, and ISIS.

The following BGP service routes are supported:

- IPv6 Layer 3 VPN services over IPv4 BGP labeled unicast
- IPv4 services over IPv4 BGP labeled unicast
- IPv4 Layer 3 VPN services over IPv4 BGP labeled unicast
- IPv6 BGP labeled unicast service over IPv4 BGP labeled unicast

Starting with Junos OS Release 19.4R1, MX Series and PTX Series routers support BGP PIC Edge with BGP labeled unicast as the transport protocol.

**Key Benefits of BGP PIC Edge Using BGP Labeled Unicast Transport Protocol**

- Provides traffic protection in case of border (ABR and ASBR) node failures in multi-domain networks.
- Provides faster restoration of network connectivity and reduces traffic loss if the primary path becomes unavailable.

WHAT'S NEXT

For an example on configuring BGP PIC over BGP labeled unicast, see [Example: Protecting IPv4 Traffic over Layer 3 VPN Running BGP Labeled Unicast](#).  
For more information on configuring BGP PIC and load balancing, see [Load Balancing for a BGP Session](#).

Release History Table

| Release                | Description  |
|------------------------|--|
| <a href="#">19.4R1</a> | Starting with Junos OS Release 19.4R1, MX Series and PTX Series routers support BGP PIC Edge with BGP labeled unicast as the transport protocol. |

# 4

CHAPTER

## Wi-Fi Mini-PIM

---

Wi-Fi Mini-PIM Configuration | 25

---



# Wi-Fi Mini-PIM Configuration

## SUMMARY

The Wi-Fi Mini-Physical Interface Module (Mini-PIM) for SRX Series devices provides an integrated wireless access point (or wireless LAN) solution along with routing, switching, and security in a single device.

## IN THIS SECTION

- [Wi-Fi Mini-Physical Interface Module Overview | 25](#)

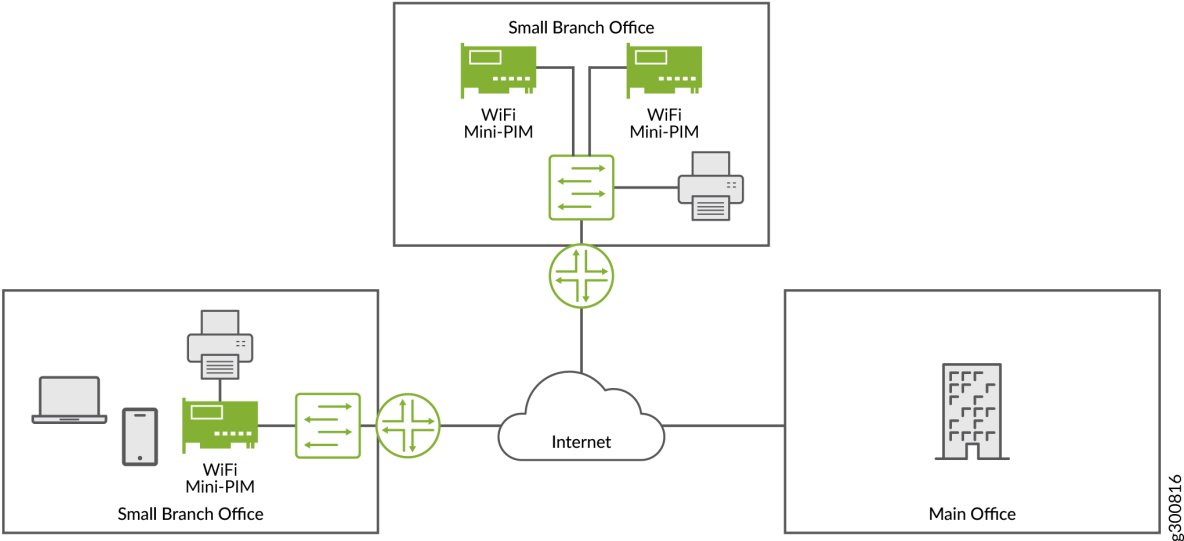
## Wi-Fi Mini-Physical Interface Module Overview

Wi-Fi Mini-Physical Interface Module (Wi-Fi Mini-PIM) for SRX320, SRX340, SRX345, and SRX550M provides an integrated wireless access point —or wireless LAN— along with routing, switching, and security in a single device. Mini-PIM supports the 802.11ac Wave 2 wireless standards and is backward compatible with 802.11a/b/g/n. The Wi-Fi Mini-PIM can coexist with other Mini-PIMs supported on the SRX Series device. [Table 1 on page 26](#) provides a summary of the features supported on Mini-PIM.

Typical deployments for Wi-Fi Mini-PIM solution include:

- Secure wireless LAN connectivity to endpoint devices of corporate users at remote branch offices as seen in Figure.... 802.11ac, WPA2, 802.1X, and SSID-to-VLAN mapping features provide secure Wireless LAN connectivity.
- Direct network connectivity to the enterprise Internet of Things (IoT) devices. The security features on the SRX Series devices secure the IoT devices.

The Mini-PIM inserted onto the SRX series device provides a secure wireless access point connection to multiple clients in a remote location. The following figure illustrates the secure LAN connectivity of Wi-Fi Mini-PIM.



See [How to Install the Wi-Fi Mini-PIM for SRX Series Services Gateways](#) for more information about how to install the Wi-Fi Mini-PIM.

**Features Supported on the Wi-Fi Mini-PIM**

[Table 1 on page 26](#) lists the key features supported on the Wi-Fi Mini-PIM.

**Table 1: Wi-Fi Mini-PIM Features**

| Feature     | Description  |
|-------------|--|
| 2x2 MU-MIMO | Enables transmission of data to multiple clients simultaneously.   |
| Dual radios | Both radios of 2.4 GHz and 5 GHz bands are simultaneously supported. The maximum supported speed is upto 1.2 Gbps. |
|             |  |

Table 1: Wi-Fi Mini-PIM Features (*continued*)

| Feature  | Description  |
|--|--|
| Virtual access points (VAPs) and VLAN features | <ul style="list-style-type: none"> <li>• Allows you to segment the WLAN into multiple broadcast domains that are the wireless equivalents of Ethernet VLANs. A single access point is segregated into multiple individual VAPs, simulating multiple access points in a single system.</li> <li>• An access point supports multiple VLANs, which can be distributed across VAPs and radios.</li> <li>• You can configure up to eight VAPs per radio. You can map up to 16 extended service set identifiers (ESSIDs) to individual VLANs.</li> <li>• The VLANs from the Mini-PIM software map to VLANs on Junos OS.</li> </ul> |
| Co-existence of interfaces                     | The Wi-Fi Mini-PIM coexists with 4G LTE, VDSL, T1, and serial interfaces.  |
| Client authentication methods                  | Client authentication methods supported are Wi-Fi Protected Access (WPA) Enterprise (WPA2 standards) and Wi-Fi Protected Access (WPA) Personal (AES-CCMP cipher suits and WPA2 standards).   |

### Benefits of Using the Wi-Fi Mini-PIM

- Provides advanced security capabilities (WPA personal and WPA enterprise authentication methods).
- Simplifies network design, and provides unified management.
- Supports end-to-end segmentation from user to applications with ESSID-to-VLAN mapping.

### WHAT'S NEXT

For more information on configuring Wi-Fi Mini-PIM, see [How to Install the Wi-Fi Mini-PIM for SRX Series Services Gateways](#).