Junos OS 11.3 Product and Feature Descriptions

Published: 2011-09-21
Part Number: , Revision 1

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos OS 11.3 Product and Feature Descriptions

Revision History
September 2011—R1 Junos OS 11.3

The information in this document is current as of the date listed in the revision history.

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 http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Tables

PART 1

Product Description

CHAPTER 1

Product Description

Junos OS Product Description

The Junos OS from Juniper Networks includes IP routing protocol software, as well as software for management of interfaces, networks, and chassis. The Junos OS runs on the following Juniper Networks devices:

- EX Series Ethernet Switches
- J Series Services Routers
- LN Series Mobile Secure Routers
- M Series Multiservice Edge Routers
- MX Series Ethernet Services Routers
- QFX Series
- SRX Series Services Gateways
- T Series Core Routers

Juniper Networks routers use two types of processing engine:

- Routing Engine—Maintains routing tables and controls routing protocols.
- Packet Forwarding Engine—Forwards network traffic, which is processed by application-specific integrated circuits (ASICs) and other components.

Juniper Networks offers three versions of the Junos OS:

- Canada and United States version, which incorporates cryptographic functionality and is therefore subject to export controls. When used in combination with an ES PIC, the strong cryptographic functionality in the Canada and U.S. version of the Junos OS substantially supports IP Security (IPsec). The software also supports secure remote network management sessions (using SSH and Secure Sockets Layer [SSL]), and secure transmission of control traffic between Routing Engines (using SSH).
- Worldwide version, which omits most cryptographic functionality, including support for IPsec with the ES PIC.
- Junos-FIPS version, which meets the requirements of Federal Information Processing Standard (FIPS) PUB 140-2.

Related Documentation

- User Interfaces to the Junos OS on page 6

Configuration Features in the Junos OS

This topic describes the configuration features available in the Junos OS. For more information about displaying and changing router configuration, see the *Junos OS CLI User Guide*.

Configuration Operations

To configure a Juniper Networks device that runs the Junos OS, you define a hierarchy of configuration statements, either by typing them in Junos OS command-line interface (CLI) configuration mode, or by loading a text file that contains the statements in formatted ASCII.

You can also write an application that uses the Junos XML management protocol or NETCONF management protocol to add, modify, or delete configuration information; for more information, see "User Interfaces to the Junos OS" on page 6.

In CLI configuration mode, you issue commands to perform the following operations:

- Activate (commit) a configuration
- Display the current configuration
- Globally search and replace text; you can use regular expressions to locate and replace identifiers and values
- Insert, copy, and delete statements
- Issue operational mode commands
- List the commands that were previously issued during the session

- List the users currently editing the configuration
- Move among the levels of the configuration hierarchy
- Save a configuration to a file
- Verify the syntactic correctness of a configuration before activating it

When you load a text file that contains a configuration, you can commit it immediately to activate the configuration on the router, or you can alter it in CLI configuration mode and commit it later. When loading the file, you can specify that it overwrite the entire configuration or portions of it, or that nonoverlapping portions be merged with the existing configuration.

You can include comments in the configuration to identify or explain particular statement or subhierarchies.

You can copy the contents of currently active file system partitions on the router to standby partitions that are not active.

Configuration Versions

When you change the configuration in CLI configuration mode, your changes are stored in a copy of the currently active configuration. The copy is called the *candidate configuration*. By default, multiple users can edit the candidate configuration at the same time, and all users immediately see the changes made by everyone. Alternatively, you can lock other users out of the candidate configuration as you enter CLI configuration mode, making them unable to change the candidate configuration until you release the lock. For finer-grained control, you can also allow multiple users each to edit nonoverlapping portions of the configuration and to commit only their own changes.

For the candidate configuration to become the *active* configuration running on the router, you must commit it. The candidate file is checked for proper syntax, activated, and saved to a file as the currently active configuration. If the candidate configuration is committed while multiple users are editing it, all changes made by all the users take effect.

In addition to saving the candidate and active configurations, the CLI saves the previous 49 configurations that were committed. You can *roll back* to any of the saved previous versions, making it the candidate configuration and then committing it if desired.

Configuration Groups

Junos *configuration groups* are named collections of configuration statements that are defined at the **[edit groups]** level of the hierarchy and referenced at other locations in the hierarchy. The statements in the configuration group are said to be *inherited* at the referring location and apply at that location as though they were actually typed there. You can apply the same group in multiple locations in the configuration, and apply different sections of one group to different locations.

Related Documentation

- User Interfaces to the Junos OS on page 6
- Configuration Mode Commands in the Junos OS
- Notational Conventions Used in Junos OS Configuration Hierarchies

User Interfaces to the Junos OS

The Junos OS provides several user interfaces, including a *command-line interface* (*CLI*), the Junos XML management protocol, the NETCONF management protocol, and the J-Web graphical user interface. They are described in the following sections. For more information about the user interfaces, see the *Junos OS CLI User Guide*.

CLI

The Junos CLI is the user interface available when a user logs in to a router through the console or auxiliary port, or logs in remotely. The CLI has two modes: operational mode, which provides commands for monitoring the Junos OS, routing protocols, network interfaces and connectivity, and router hardware; and configuration mode, which provides commands for configuring the Junos OS.

The Junos CLI provides the following functionality:

- Context-sensitive name completion for commands, configuration statements, and other text strings, such as filenames and usernames. When you type only the initial part of a name and press the Tab key or the Spacebar, the CLI automatically adds the remainder of the name if there is only one possible completion. If multiple completions are possible, the CLI lists them and displays a short description of each.

  Similarly, if you type a question mark (**?**) after the starting portion of a term (word) in a command or configuration statement, or after a complete term and a following space, the CLI displays the terms that can be specified at that position in the command or statement, along with a short description of each.

- Keyword search for commands and configuration statements (similar to the UNIX **apropos** command). The **help apropos** ***topic*** command displays all commands or configuration statements that include the specified ***topic*** word or phrase in their names or short description. In configuration mode, this feature is context-sensitive—the CLI displays only the matching terms that are valid at or below the current level in the configuration hierarchy.

- Automatic display of one screen at a time when command output or the list of possible completions is longer than the screen length (similar to the effect of the UNIX **more** utility). You can scroll backward and forward through the screen output and search for text strings in it.

- Keyboard sequences for editing the command line and moving the cursor on it, and for scrolling through a list of recently executed commands. The keyboard sequences

are the same as those used in the UNIX editor Emacs. For example, when you type Ctrl+b, the cursor moves backward one character.

- Tracking of commands issued during the current CLI session. To display them, issue the **show cli history** command.

You can customize your CLI environment in the following ways:

- Define the terminal type as ANSI, VT100, or regular or small xterm.
- Disable command completion.
- Display helpful hints about how to use the CLI.
- Enable an automatic prompt for the user to restart the router after a software upgrade. Restarting is required for the new software to take effect.
- Set the CLI prompt.
- Set the duration that a login session can be idle before it is terminated.
- Set the screen length, width, or both.

You can apply filters to command output to change the CLI's standard display behavior in the following ways:

- Count the number of lines in the output instead of displaying the actual output.
- Display only text that matches or does not match a pattern. The Junos OS supports the use of extended (modern) regular expressions as defined in POSIX 1003.2.
- Display all output at once (override the default behavior of displaying one screen of output at a time).
- Display only the final lines of output.
- Suppress redisplay of the CLI prompt at the end of command output.
- Save (redirect) the screen output to a file.

When displaying the current configuration, you can filter the output in the following ways in addition to those in the preceding list:

- Compare the current configuration with a previously saved configuration.
- Display additional information about the configuration, including the version of the Junos OS under which the configuration was created.

You can also apply multiple filters in sequence, and write scripts that customize the output in ways not provided by the CLI. For information about scripting, see the *Junos OS Configuration and Operations Automation Guide*.

For detailed information about the CLI features described in this section, see the *Junos OS CLI User Guide*.

Junos XML API, Junos XML Management Protocol, and NETCONF Management Protocol

The *Junos Extensible Markup Language (XML) application programming interface (API)* defines XML tag elements that correspond to all Junos configuration statements and many operational commands. XML is a language for defining a set of markers (tag elements) that are applied to a data set or document to describe the function of individual elements and codify the hierarchical relationships between them.

The *Junos XML management protocol* enables client applications to exchange information with Juniper Networks devices. The Junos XML management protocol defines XML tag elements that retrieve and change Junos configuration objects, which are represented by the XML tag elements in the Junos XML API.

The *NETCONF management protocol* is similar in function to the Junos XML management protocol and is defined in RFC 4741, *NETCONF Configuration Protocol*. The NETCONF server and client applications use the SSH protocol for communication in accordance with RFC 4742, *Using the NETCONF Configuration Protocol over Secure SHell (SSH)*.

J-Web User Interface

The *J-Web* user interface is a graphical user interface that enables you to configure and monitor Juniper Networks devices through an Internet browser. The J-Web interface includes the following features:

- Quick Configuration pages for performing basic configuration operations
- Monitoring tools that display system status, routes, and statistics
- Diagnostic tools
- A View Events page that displays system log messages
- File utilities for managing configuration files, licenses, and temporary files

Related Documentation

- Junos OS Product Description on page 3
- Configuration Features in the Junos OS on page 4
- Configuration Mode Commands in the Junos OS

PART 2

Feature Descriptions

CHAPTER 2

Chassis and System Features

Chassis Configuration Features in the Junos OS

The Junos OS enables you to configure several properties of the router chassis, including the following:

- Conditions that activate the red and yellow alarm LEDs on the router's craft interface
- SONET/SDH framing and concatenation properties for individual PICs
- Source for clock synchronization
- Synchronization of the system Stratum 3 clock to an external source (M40e, M120, and M320 routers only)

Network Management Features in the Junos OS

The Junos OS substantially supports SNMP version 1, version 2c, and version 3. The Junos SNMP agent software accepts both IP version 4 (IPv4) and IP version 6 (IPv6) addresses.

The Junos OS provides numerous enterprise MIBs, including the following:

- Alarm
- Asynchronous Transfer Mode (ATM)
- ATM class of service (CoS)
- BGP4 version 2
- Chassis
- Chassis definitions for router model
- Chassis forwarding
- CoS
- Configuration management

- Destination class usage
- Dynamic flow capture
- Ethernet media access control (MAC)
- Experimental
- Firewall
- Flow collector services
- Host resources
- IP Security (IPsec) monitoring
- IPv4
- IPv6 and ICMPv6
- LDP
- MPLS
- Passive monitoring
- RSVP traffic engineering
- Reverse path forwarding
- Services PIC
- SONET Automatic Protection Switching (APS)
- SONET/SDH interface management
- Source class usage
- Structure of Management Information (SMI)
- Virtual private network (VPN)

For more information about MIBs, see the *Junos OS Network Management Configuration Guide*.

The Junos OS supports the use of scripts and event-triggered policies that you write to automate network management. The functions you can perform with these utilities include the following:

- Automatically detect, diagnose, and fix network problems. When it detects a problem, the script can issue a command that includes options appropriate to the current situation, and then interpret the command output to determine the next appropriate command or action.
- Periodically check for alarms or other indicators of network or chassis problems, and perform specific actions if they exist.
- Respond automatically to the occurrence of events and conditions that also trigger system log messages or SNMP traps.
- Verify that the router's configuration includes only statements you deem appropriate for your network, and automatically add or remove statements as necessary.

- Automatically change the router's configuration in response to network problems or conditions you specify.
- Generate custom error, warning, or system log messages.

For more information about scripts and event policies, see the *Junos OS Configuration and Operations Automation Guide*.

In addition, the Junos OS provides extensions to the interface, ping, remote monitoring (RMON) events and alarms, and traceroute MIBs.

For some traps, a message is directed to the system log when the trap condition occurs, even if the SNMP agent does not send the trap to a network management system (NMS).

Related Documentation

- Supported Network Management Standards

Services PIC and DPC Features in the Junos OS

On routers equipped with one or more Adaptive Services PICs (both standalone and integrated versions) or Multiservices PICs or DPCs, the Junos OS provides the following services:

- CoS—Traffic filtering based on class-of-service features. The Junos OS substantially supports the standards listed in Supported CoS Standards.
- Dynamic flow capture—Tools for forwarding passively monitored traffic that matches filter criteria to one or more destinations. The Junos OS substantially supports the standards listed in Supported DTCP Standard.
- Flow monitoring and discard accounting—Tools for sampling traffic, gathering detailed information about traffic flows, and performing discard accounting. On routers with one or more Monitoring Services PICs, Adaptive Services PICs, or Multiservices PICs or DPCs, the Junos OS substantially supports the standards listed in Supported Flow Monitoring and Discard Accounting Standards.
- Intrusion detection services (IDS)—Tools for detecting, redirecting, and preventing certain kinds of network attack and intrusion.
- IPsec—Tools for configuring manual or dynamic security associations (SAs) for encryption of data traffic.

  The Canada and U.S. version of the Junos OS substantially supports the IPsec architecture, which provides a security suite for the IP version 4 (IPv4) and IP version 6 (IPv6) network layers for traffic destined to or originating at the Routing Engine. The Canada and U.S. version of the software also substantially supports Internet Key Exchange (IKE), which defines mechanisms for key generation and exchange, and manages security associations (SAs). The Junos OS supports manual and dynamic SAs. The Canada and U.S. version of the Junos OS substantially supports the standards listed in Supported IPsec and IKE Standards.
- Layer 2 Tunneling Protocol (L2TP) client services—Services that enable support for tunneling Point-to-Point Protocol (PPP) traffic across a network. The Junos OS substantially supports the standards listed in Supported L2TP Standards.

- Link services—System for providing multiple independent links between two systems. The Junos OS substantially supports the standards listed in Supported Link Services Standards.
- Network Address Translation (NAT)—Security-enhancement procedure that hides the IP addresses of hosts on a private network by substituting publicly visible addresses for them. NAT services support Session Initiation Protocol (SIP) dialogs and UDP/IPv4 transport of SIP messages. The Junos OS substantially supports the standards listed in Supported NAT and SIP Standards.
- Real-time performance monitoring (RPM)—Tools for configuring active probes to track and monitor traffic. The Junos OS substantially supports the standards listed in Supported RPM Standard.
- Stateful firewall—Type of firewall filter that considers state information derived from previous communications and other applications when evaluating traffic. Stateful firewall services support SIP dialogs and UDP/IPv4 transport of SIP messages, and the Junos OS substantially supports RFC 3261, *SIP: Session Initiation Protocol*.
- Tunnel services—Method for transmitting traffic along a secure path in a public network. The Junos OS substantially supports the tunneling standards listed in Supported GRE and IP-IP Interface Standards.
- Voice services—Utility for transporting packetized voice traffic over an IP network infrastructure. The Junos OS substantially supports the standards listed in Supported Voice Services Standards.

Related Documentation

- Supported CoS Standards
- Supported DTCP Standard
- Supported Flow Monitoring and Discard Accounting Standards
- Supported GRE and IP-IP Interface Standards
- Supported IPsec and IKE Standards
- Supported L2TP Standards
- Supported Link Services Standards
- Supported NAT and SIP Standards
- Supported RPM Standard
- Supported Voice Services Standards
- Accessing Standards Documents on the Internet

CHAPTER 3

Packet Processing Features

CoS Features in the Junos OS

For interfaces that carry IP version 4 (IPv4), IP version 6 (IPv6), or MPLS traffic, the Junos OS includes class-of-service (CoS) features that provide multiple classes of service for different applications. You can configure multiple forwarding classes for transmitting packets, defining which packets are placed into each output queue, scheduling the transmission service level for each queue, and managing congestion using a Random Early Detection (RED) algorithm.

The CoS features in the Junos OS include the following:

- Classifiers—Assign incoming packets to a forwarding class and loss priority, and direct packets to output queues based on the forwarding class. Two general types of classifiers are supported:
  - Behavior aggregate (BA) or code point traffic classifiers—Determine each packet's forwarding class and loss priority. BA classifiers allow setting of the forwarding class and loss priority of a packet based on Differentiated Services (DiffServ) code point (DSCP) bits, IP precedence bits, MPLS EXP bits, and IEEE 802.1p bits. The default classifier is based on IP precedence bits.
  - Multifield traffic classifiers (also referred to as "MF traffic classifiers")—Set a packet's forwarding class and loss priority based on packet filter rules.
- DiffServ—Implemented as six bits of the type-of-service (ToS) byte in the IP header. The Junos OS uses DSCPs in the IP type of service (ToS) field to determine the forwarding class associated with each packet.
- Forwarding classes—Determine the forwarding, scheduling, and marking policies applied to packets as they transit the router. Four forwarding classes are supported: best effort, assured forwarding, expedited forwarding, and network control. Together with loss priority, the forwarding class defines the per-hop behavior.
- Forwarding policy options—Associate forwarding classes with next hops. Also enable creation of classification overrides, which assign forwarding classes to sets of prefixes.

- Layer 2 to Layer 3 CoS mapping—Set a Layer 3 packet's forwarding class and loss priority value based on information in the Layer 2 packet header. Output involves mapping the forwarding class and loss priority value to a Layer 2-specific marking. You can configure the Junos OS to mark the Layer 2 and Layer 3 headers simultaneously.
- Loss priorities—Set a packet's priority to be discarded. Typically, packets exceeding some service level are marked with a high loss priority. Loss priority affects the scheduling of a packet. Loss priority is set by configuring a classifier or a policer.
- MPLS EXP—Map MPLS EXP bit settings to forwarding classes and vice versa.
- Oversubscription of interface bandwidth (Gigabit Ethernet IQ and Channelized IQ PICs)—Configures shaping rates so that their sum exceeds the physical Ethernet bandwidth.
- Rewrite markers—Change the code-point value of outgoing packets. Rewriting, or marking, outbound packets is useful when the router is at the border of a network and must alter the code points to meet the policies of the targeted peer.
- Simple filters for metropolitan Ethernet applications (4-port and 8-port Gigabit Ethernet IQ2 PICs only)—Classify IPv4 traffic based on noncomplex filters.
- Transmission scheduling and rate control—Provides a variety of tools to manage traffic flows:
  - Fabric schedulers (T Series routers only)—Identify a packet as high or low priority based on its forwarding class.
  - Policers—Limit traffic of a certain class to a specified bandwidth and burst size. Packets exceeding the policer limits can be discarded, or can be assigned to a different forwarding class, to a different loss priority, or to both. Policers are defined with filters that can be associated with either input or output interfaces.
  - Schedulers—Define the priority, bandwidth, delay buffer size, rate control status, and RED drop profiles to be applied to a particular forwarding class for packet transmission.
- Two-rate tricolor marking—For T Series routers with Enhanced II Flexible PIC Concentrators (FPCs), configures traffic policing using two-rate tricolor marking (trTCM), which provides three levels of drop precedence (also called packet loss priority [PLP]). Two-rate TCM is a "color-aware" method of traffic policing—high, medium, and low loss priorities are mapped to the colors red, yellow, and green. The color of a packet, which is used or set by the TCM policer, corresponds to the packet's loss priority. trTCM is defined in RFC 2698, *A Two Rate Three Color Marker*.
- Virtual channels and virtual channel groups (J Series Services Routers and SRX Series Services Gateways)—Direct traffic into a virtual channel and apply bandwidth limits to the channel.
- VPN outer label marking—Set outer label EXP bits based on MPLS EXP mapping.

The Junos OS supports CoS features on all interface types except the following:

- **cau4**—Channelized STM1 IQ interface (configured on the Channelized STM1 IQ PIC)
- **ce1**—Channelized E1 IQ interface (configured on the Channelized E1 IQ PIC or Channelized STM1 IQ PIC)
- **coc1**—Channelized OC1 IQ interface (configured on the Channelized OC12 IQ PIC)
- **coc12**—Channelized OC12 IQ interface (configured on the Channelized OC12 IQ PIC)
- **cstm-1**—Channelized STM1 IQ interface (configured on the Channelized STM1 IQ PIC)
- **ct1**—Channelized T1 IQ interface (configured on the Channelized DS3 IQ PIC or Channelized OC12 IQ PIC)
- **ct3**—Channelized T3 IQ interface (configured on the Channelized DS3 IQ PIC or Channelized OC12 IQ PIC)
- **dsc**—Discard interface
- **fxp**—Management and internal Ethernet interfaces
- **lo**—Loopback interface, which is internally generated
- **pd**—Interface that de-encapsulates packets on a Platform Independent Multicast (PIM) rendezvous point (RP) router
- **pe**—Interface on a first-hop RP that encapsulates packets destined for the RP router
- **vt**—Virtual loopback tunnel interface

Related Documentation

- Supported CoS Standards

High Availability and Virtualization Features in the Junos OS

In support of high-availability router functioning, the Junos OS includes the following features:

- Graceful restart—Enables a routing protocol, before it restarts, to inform its adjacent neighbors and peers of its condition. Most Junos routing protocols support graceful restart.
- Graceful Routing Engine switchover—On routers with dual Routing Engines, enables switching of mastership between Routing Engines without interruption to packet forwarding.

  For routers in which Adaptive Services, Multiservices, or Tunnel Services PICs or DPCs are installed, features that rely on their services are interrupted momentarily during a Routing Engine switchover. Features that do not use the services continue uninterrupted. After switchover, all features are restored and packet forwarding continues.

The Junos OS supports these virtualization features:

- Unicast reverse-path forwarding.
- Routing instances, which enable you to create multiple instances of BGP, IS-IS, OSPF, PIM, RIP, and static routes.
- Logical systems, which enables you to create multiple logical routing devices within a single router.

Packet Filtering Features in the Junos OS

You can configure filters in the Junos OS that examine characteristics of incoming and outgoing packets, including the following:

- Bit fields in the packet header, including IP fragmentation flags, IP options, and TCP flags
- IP version 4 (IPv4) numeric range, including destination port, DiffServ code point (DSCP) value, fragment offset, Internet Control Message Protocol (ICMP) code, ICMP packet type, interface group, IP precedence, packet length, protocol, and TCP and UDP source and destination port
- IP version 6 (IPv6) numeric range, including CoS priority, destination address, destination port, ICMP code, ICMP packet type, interface group, IP address, next header, packet length, source address, source port, and TCP and UDP source and destination port
- Source and destination address and prefix list

You can configure filters to perform certain actions when packets match specified characteristics, including the following actions:

- Accept the packets
- Apply a policer
- Classify the packets based on their source address
- Discard the packets
- Evaluate the next term in the filter
- Increment a packet counter
- Reject the packets
- Sample the packets
- Set the packets' loss priority
- Specify a forwarding class
- Specify an IPsec SA
- Specify the forwarding path that the packets follow within the router
- Write an alert or message to the system log

Related Documentation

- Supported Packet Filtering Standards

CHAPTER 4

Routing Features

IS-IS Features in the Junos OS

The Junos OS supports authentication for IS-IS protocol exchanges (HMAC-MD5 or simple authentication), link-state packets, sequence-number packets (complete sequence number PDU [CSNP] and partial sequence number PDU [PSNP]), and IS-IS hello packets (IIH).

The Junos OS supports the advertisement of MPLS label-switched paths into IS-IS.

Related Documentation

- Supported IS-IS Standards

OSPF Features in the Junos OS

The Junos OS supports the following features for OSPF:

- Authentication for protocol exchanges (simple authentication)
- Extensions to support MPLS traffic engineering
- Advertisement of MPLS label-switched paths (LSPs) into OSPF

Related Documentation

- Supported OSPF and OSPFv3 Standards

Routing Policy Features in the Junos OS

The Junos OS provides a routing policy language that enables you to control the transfer of routing information between the routing protocols and the routing tables, and between the routing tables and the forwarding table.

You can configure policies that examine characteristics of incoming and outgoing routes, including the following:

- Address family
- Aggregate route contributors
- BGP AS path, AS path group, community, and origin attributes
- Destination prefix
- IP address or list of addresses
- IS-IS level
- Metric
- Multicast source address
- Neighbor (peer)
- Next-hop address
- OSPF area identifier
- OSPF external route and tags
- Preference
- Protocol from which route was learned
- Router interface
- Routing instance
- Routing table

You can configure policies to perform certain actions when routes match specified characteristics, including the following actions:

- Accept the routes
- Add, delete, or set the BGP community
- Add or delete a BGP local preference
- Apply BGP route-damping parameters
- Apply CoS parameters
- Choose a next hop to install into the forwarding table
- Create a forwarding class
- Evaluate the next term in the policy
- Evaluate the next policy in a policy chain
- Extract the last AS number from an AS path
- Maintain packet counts based on source and destination address
- Modify the metric value

- Modify the preference value
- Perform per-packet load balancing
- Prepend an AS path
- Reject the routes
- Set the BGP MED and origin attribute
- Set the external metric type
- Set the next hop
- Specify or modify OSPF tags

Routing Table Features in the Junos OS

The Junos OS maintains two databases for routing information:

- Routing table—Contains all the routing information learned by all routing protocols. (Some vendors refer to this kind of table as a routing information base [RIB].)
- Forwarding table—Contains the routes actually used to forward packets. (Some vendors refer to this kind of table as a forwarding information base [FIB].)

By default, the Junos OS maintains three routing tables: one for IP version 4 (IPv4) unicast routes, a second for multicast routes, and a third for MPLS. You can configure additional routing tables.

The Junos OS maintains separate routing tables for IPv4 and IP version 6 (IPv6) routes.

The Junos OS installs all active routes from the routing table into the forwarding table. The active routes are routes that are used to forward packets to their destinations. The Junos operating system kernel maintains a master copy of the forwarding table. It copies the forwarding table to the Packet Forwarding Engine, which is the component responsible for forwarding packets.

The Junos routing protocol process generally determines the active route by selecting the route with the lowest preference value. The Junos OS provides support for alternate and tiebreaker preferences, and some of the routing protocols, including BGP and MPLS, use these additional preferences.

You can add martian addresses and static, aggregate, and generated routes to the Junos routing tables, configuring the routes with one or more of the properties shown in Table 1 on page 23.

Table 1: Routing Table Route Properties

Description	Static	Aggregate	Generated
Destination address	X	X	X
Default route to the destination	X	X	X

Table 1: Routing Table Route Properties *(continued)*

Description	Static	Aggregate	Generated
IP address or interface of the next hop to the destination	X	–	–
Label-switched path (LSP) as next hop	X	–	–
Drop the packets, install a reject route for this destination, and send Internet Control Message Protocol (ICMP) unreachable messages	X	X	X
Drop the packets, install a reject route for this destination, but do not send ICMP unreachable messages	X	X	X
Cause packets to be received by the local router	X	–	–
Associate a metric value with the route	X	X	X
Type of route	X	X	X
Preference values	X	X	X
Additional preference values	X	X	X
Independent preference (**qualified-next-hop** statement)	X	–	–
BGP community information to associate with the route	X	X	X
Autonomous system (AS) path information to associate with the route	X	X	X
OSPF tag strings to associate with the route	X	X	X
Do not install active static routes into the forwarding table	X	–	–
Install the route into the forwarding table	X	–	–
Permanently retain a static route in the forwarding table	X	–	–
Include only the longest common leading sequences from the contributing AS paths	–	X	–
Include all AS numbers for a specific route	–	X	–
Retain an inactive route in the routing and forwarding tables	X	X	X
Remove an inactive route from the routing and forwarding tables	X	X	X
Active policy to associate with the route	–	X	X

Table 1: Routing Table Route Properties *(continued)*

Description	Static	Aggregate	Generated
Specify that a route is ineligible for readvertisement	X	–	–
Specify route to a prefix that is not a directly connected next hop	X	–	–

PART 3

Index

Index

