

# Chapter 2

## JUNOS Software Overview

The JUNOS Internet software runs on the router's Routing Engine. It consists of software processes that support Internet routing protocols, control the router's interfaces and the router chassis itself, and allow router system management. All these processes run on top of a kernel that enables communication among all the processes and has a direct link to the Packet Forwarding Engine software. You use the JUNOS software to configure the routing protocols that should run on the router and to configure properties of the router's interfaces. Afterward, you use the JUNOS software to monitor the router and to troubleshoot protocol and network connectivity problems. For more information about monitoring the router and troubleshooting problems, see the *JUNOS Internet Software Operational Mode Command Reference*.

This chapter discusses the following topics:

- Routing Engine Software Components on page 9
- Software Installation Overview on page 14
- Tools for Accessing and Controlling the Software on page 14
- Software Configuration Overview on page 15
- Software Monitoring Tools on page 16
- Supported Software Standards on page 16

### Routing Engine Software Components

The Routing Engine software consists of several software processes that control router functionality and a kernel that provides the communication among all the processes (see Figure 1 on page 5). This section describes the Routing Engine components:

- Routing Protocol Process on page 10
- Interface Process on page 13
- Chassis Process on page 13
- SNMP and MIB II Processes on page 13
- Management Process on page 14
- Routing Engine Kernel on page 14

## **Routing Protocol Process**

The routing protocol process controls the routing protocols that run on the router. It starts all configured routing protocols and handles all routing messages. It maintains one or more routing tables, which consolidate the routing information learned from all routing protocols into common tables. From this routing information, the routing protocol process determines the active routes to network destinations and installs these routes into the Routing Engine's forwarding table. Finally, it implements routing policy, which allows you to control the routing information that is transferred between the routing protocols and the routing table. Using routing policy, you can filter routing information so that only some of it is transferred, and you also can set properties associated with the routes.

This section discusses the following topics:

Routing Protocols on page 10

Routing and Forwarding Tables on page 12

Routing Policy on page 12

## **Routing Protocols**

The JUNOS software implements full IP routing functionality, providing support for IP Version 4 (IPv4). The routing protocols are fully interoperable with existing IP routing protocols, and they have been developed to provide the scale and control necessary for the Internet core.

The software provides the following routing and MPLS applications protocols:

Unicast routing protocols

IS-IS—Intermediate System-to-Intermediate System is a link-state interior gateway protocol (IGP) for IP networks that uses the shortest-path-first (SPF) algorithm, which also is referred to as the Dijkstra algorithm, to determine routes. The JUNOS IS-IS software is a new and complete implementation of the protocol, addressing issues of scale, convergence, and resilience.

OSPF—Open Shortest Path First, Version 2, is an IGP that was developed for IP networks by the Internet Engineering Task Force (IETF). OSPF is a link-state protocol that makes routing decisions based on the SPF algorithm. The JUNOS OSPF software is a new and complete implementation of the protocol, addressing issues of scale, convergence, and resilience.

RIP—Routing Information Protocol, Version 2, is an IGP for IP networks based on the Bellman-Ford algorithm. RIP is a distance-vector protocol. RIP dynamically routes packets between a subscriber and a service provider without the subscriber having to configure BGP or to participate in the service provider's IGP discovery process.

ICMP—Internet Control Message Protocol router discovery allows hosts to discover the addresses of operational routers on the subnet.

BGP—Border Gateway Protocol, Version 4, is an exterior gateway protocol (EGP) that guarantees loop-free exchange of routing information between routing domains (also called autonomous systems). BGP, in conjunction with JUNOS routing policy, provides a system of administrative checks and balances that can be used to implement peering and transit agreements.

#### Multicast routing protocols

DVMRP—Distance Vector Multicast Routing Protocol is a dense-mode (flood-and-prune) multicast routing protocol.

PIM sparse mode and dense mode—Protocol-Independent Multicast is a multicast routing protocol. PIM sparse mode routes to multicast groups that might span wide-area and interdomain internets. PIM dense mode is a flood-and-prune protocol.

MSDP—Multicast Source Discovery Protocol allows multiple PIM sparse mode domains to be joined. A rendezvous point (RP) in a PIM sparse mode domain has a peer relationship with an RP in another domain, enabling it to discover multicast sources from other domains.

IGMP—Internet Group Management Protocol, Versions 1 and 2, is used to manage membership in multicast groups.

SAP/SDP—Session Announcement Protocol and Session Description Protocol handle conference session announcements.

#### MPLS applications protocols

MPLS—Multiprotocol Label Switching, formerly known as tag switching, allows you to manually or dynamically configure label-switched paths (LSPs) through a network. It lets you direct traffic through particular paths rather than rely on the IGP's least-cost algorithm to choose a path.

RSVP—The Resource Reservation Protocol, Version 1, provides a mechanism for engineering network traffic patterns that is independent of the shortest path decided upon by a routing protocol. RSVP itself is not a routing protocol; it operates with current and future unicast and multicast routing protocols. The primary purpose of the JUNOS RSVP software is to support dynamic signaling for MPLS label-switched paths (LSPs).

LDP—The Label Distribution Protocol provides a mechanism for distributing labels in nontraffic-engineered applications. LDP allows routers to establish LSPs through a network by mapping network-layer routing information directly to data-link layer switched paths. LSPs created by LDP can also traverse LSPs created by RSVP.

## Routing and Forwarding Tables

A major function of the JUNOS routing protocol process is to maintain the Routing Engine's routing tables and from these tables to determine the active routes to network destinations. The routing protocol process then installs these routes into the Routing Engine's forwarding table. The JUNOS kernel then copies this forwarding table to the Packet Forwarding Engine. Refer to Figure 1 on page 5 for an illustration of the interrelationships between the routing and forwarding tables.

The routing protocol process maintains multiple routing tables. By default, it maintains the following three routing tables. You can configure additional routing tables to suit your requirements.

**Unicast routing table**—Stores routing information for all unicast routing protocols running on the router. IS-IS, OSPF, RIP, and BGP all store their routing information in this routing table. You can configure additional routes, such as static routes, to be included in this routing table. IS-IS, OSPF, RIP, and BGP use the routes in this routing table when advertising routing information to their neighbors.

**Multicast routing table (cache)**—Stores routing information for all the running multicast protocols. DVMRP and PIM both store their routing information in this routing table, and you can configure additional routes to be included in this routing table.

**MPLS routing table**—Stores MPLS path and label information.

With each routing table, the routing protocol process uses the collected routing information to determine active routes to network destinations.

For unicast routes, the routing protocol process determines active routes by choosing the most preferred route, which is the route with the lowest preference value. By default, the route's preference value is simply a function of how the routing protocol process learned about the route. You can modify the default preference value using routing policy and with software configuration parameters.

For multicast traffic, the routing protocol process determines active routes based on traffic flow and other parameters specified by the multicast routing protocol algorithms. The routing protocol process then installs one or more active routes to each network destination into the Routing Engine's forwarding table.

## Routing Policy

By default, all routing protocols place their routes into the routing table. When advertising routes, the routing protocols by default advertise only a limited set of routes from the routing table. Specifically, each routing protocol exports only the active routes that were learned by that protocol. In addition, the IGP's (IS-IS, OSPF, and RIP) export the direct (interface) routes for the interfaces on which the protocol is explicitly configured.

You can control the routes that a protocol places into each table and the routes from that table that the protocol advertises. You do this by defining one or more routing policies and then applying them to the specific routing protocol.

Routing policies applied when the routing protocol places routes into the routing table are referred to as *import policies* because the routes are being imported into the routing table. Policies applied when the routing protocol is advertising routes that are in the routing table are referred to as *export policies* because the routes are being exported from the routing table. In other words, the terms *import* and *export* are used with respect to the routing table.

Routing policy allows you to control (filter) which routes a routing protocol imports into the routing table and which routes a routing protocol exports from the routing table. Routing policy also allows you to set the information associated with a route as it is being imported into or exported from the routing table. Filtering imported routes allows you to control the routes used to determine active routes. Filtering routes being exported from the routing table allows you to control the routes that a protocol advertises to its neighbors.

You implement routing policy by defining policies. A policy specifies the conditions to use to match a route and the action to perform on the route when a match occurs. For example, when a routing table imports routing information from a routing protocol, a routing policy might modify the route's preference, mark the route with a color to identify it and allow it to be manipulated at a later time, or prevent the route from even being installed in a routing table. When exporting routes from a routing table into a routing protocol, a policy might assign metric values, modify the BGP community information, tag the route with additional information, or prevent the route from being exported altogether. You also can define policies for redistributing the routes learned from one protocol into another protocol.

## ***Interface Process***

The JUNOS interface process allows you to configure and control the physical interface devices and logical interfaces present in a router. You can configure various interface properties such as the interface location (that is, which slot the FPC is installed in and which location on the FPC the PIC is installed in), the interface encapsulation, and interface-specific properties. You can configure the interfaces that currently are present in the router, as well as interfaces that currently are not present but that you may be adding at a future time.

The JUNOS interface process communicates, through the JUNOS kernel, with the interface process in the Packet Forwarding Engine, thus enabling the JUNOS software to track the status and condition of the router's interfaces.

## ***Chassis Process***

The JUNOS chassis process allows you to configure and control the properties of the router, including conditions that trigger alarms and clock sources. The chassis process communicates directly with a chassis process in the JUNOS kernel.

## ***SNMP and MIB II Processes***

The JUNOS software supports the Simple Network Management Protocol (SNMP), which helps administrators monitor the state of a router. The software supports SNMP Version 1 and Version 2 (also known as Version 2c, or v2c). The JUNOS implementation of SNMP does not include any of the security features that were originally included in the IETF SNMP drafts but were later dropped because of the inability to standardize on a particular method. The SNMP software is controlled by the JUNOS SNMP and MIB II processes, which consist of an SNMP master agent and various subagents.

## **Management Process**

Within the JUNOS software, a process-controlling process starts and monitors all the other software processes. It also starts the command-line interface (CLI), which is the primary tool you use to control and monitor the JUNOS Internet software. This management process starts all the software processes and the CLI when the router boots. If a software process terminates, the management process attempts to restart it.

## **Routing Engine Kernel**

The Routing Engine kernel provides the underlying infrastructure for all JUNOS software processes. In addition, it provides the link between the routing tables and the Routing Engine's forwarding table. It is also responsible for all communication with the Packet Forwarding Engine, which includes keeping the Packet Forwarding Engine's copy of the forwarding table synchronized with the master copy in the Routing Engine.

## Software Installation Overview

The JUNOS Internet software is preinstalled on the router. Once the router is powered on, it is ready to be configured. The primary copy of the software is installed on a nonrotating flash disk. Two backup copies are included, one on the router's rotating hard disk and a second on the removable media (either an LS-120 floppy disk [a 120-MB disk] or a PCMCIA card) that is shipped with the router.

When the router boots, it first attempts to start the software image from the removable media if one is installed in the router. If this fails, the router next tries the flash disk, then finally the hard disk. Normally, you want the router to boot from the flash disk.

To upgrade the software, you copy a set of software images over the network to the router's flash disk using SCP or another similar utility. The JUNOS software set consists of three images, one for the software processes, a second for the kernel, and the third for the Packet Forwarding Engine. You normally upgrade all images simultaneously.

## Tools for Accessing and Controlling the Software

The primary means of accessing and controlling the JUNOS software is the CLI.

The router provides three ports on the craft interface for connecting external management devices to the Routing Engine and the JUNOS Internet software:

Console port—Connects a system console using an RS-232 serial cable.

Auxiliary port—Connects a laptop or modem using an RS-232 serial cable.

Ethernet management port—Connects the Routing Engine to a management LAN (or any other device that plugs into an Ethernet connection) for out-of-band management of the router. The Ethernet port is 10/100 Mbps autosensing and requires an RJ-45 connector.

The CLI is the interface to the JUNOS software that you use whenever you access the router from the console or through a remote network connection. The CLI provides commands that perform various tasks, including configuring the JUNOS software, and monitoring and troubleshooting the software, network connectivity, and the router hardware.

The CLI is a straightforward command interface. You type commands on a single line, and the commands are executed when you press the Enter key. The CLI provides command help and command completion; it also provides Emacs-style keyboard sequences that allow you to move around on a command line and scroll through a buffer that contains recently executed commands.

## Software Configuration Overview

To configure the JUNOS software, you specify a hierarchy of configuration statements that define the preferred software properties. You can configure all properties of the JUNOS software, including interfaces, general routing information, routing protocols, and user access, as well as some system hardware properties. After you have created a candidate configuration, you commit the configuration to be evaluated and activated by the JUNOS software.

This section discusses the following topics:

Methods of Configuring the Software on page 15

Configuring the Software on page 15

Activating a Configuration on page 16

## ***Methods of Configuring the Software***

There are two basic ways to configure the JUNOS software:

You can create the configuration for the router interactively, working in the CLI on the router.

You can load an ASCII file containing a router configuration that you created earlier, either on this system or on another system. You can then activate and run the configuration file as is or you can edit it using the CLI and then activate it.

## ***Configuring the Software***

When you initially boot a router, the system prompts you for the minimal information needed to configure the router, including the router's name, domain name, and the Internet address of at least one interface on the router. After the router finishes this initial boot, you log in as the user "root" (with no password) and configure a password for the user "root."

After completing this initial minimal configuration, you can configure software properties. If you configure the software interactively using the CLI, you enter software configuration statements to create a candidate configuration that contains a hierarchy of statements. At any hierarchy level, you generally can enter statements in any order. While you are configuring the software, you can display all or portions of the candidate configuration, and you can insert or delete statements. Any changes you make affect only the candidate configuration, not the active configuration that is running on the router.

The configuration hierarchy logically groups related functions, which results in configuration statements that have a regular, consistent syntax. For example, you configure routing protocols, routing policies, interfaces, and SNMP management in their own separate portions of the configuration hierarchy.

At each level of the hierarchy, you can display a list of the statements available at that level, along with short descriptions of the statements' functions. To have the CLI complete the statement name if it is unambiguous or to provide a list of possible completions, you can type a partial statement name followed by a space or tab.

More than one user can edit a router's configuration simultaneously. All changes made by all users are visible to everyone editing the configuration.

## Activating a Configuration

To have a candidate configuration take effect, you commit the changes. At this point, the candidate file is checked for proper syntax, activated, and marked as the current, operational software configuration file. If multiple users are editing the configuration, when you commit the candidate configuration, all changes made by all the users take effect.

The CLI always maintains a copy of previously committed versions of the software configuration. If you need to return to a previous configuration, you can do this from within the CLI.

## Software Monitoring Tools

The primary method of monitoring and troubleshooting the software, routing protocols, network connectivity, and the router hardware is to enter commands from the CLI. The CLI enables you to display information in the routing tables and routing protocol-specific data, and to check network connectivity using ping and traceroute commands.

The JUNOS software includes SNMP software, which allows you to manage routers. The SNMP software consists of an SNMP master agent and a MIB II agent, and supports MIB II SNMP version 1 traps and version 2 notifications, SNMP version 1 Get and GetNext requests, and version 2 GetBulk requests.

The software also supports tracing and logging operations so that you can track events that occur in the router—both normal router operations and error conditions—and track the packets that are generated by or pass through the router. Logging operations use a syslog-like mechanism to record systemwide, high-level operations, such as interfaces' going up or down and users' logging into or out of the router. Tracing operations record more detailed messages about the operation of routing protocols, such as the various types of routing protocol packets sent and received, and routing policy actions.

## Supported Software Standards

This section lists the standards supported by the JUNOS software:

Supported Internet RFCs and Drafts on page 17

Supported ISO Standards on page 25

Supported SDH and SONET Standards on page 25

Other Supported Standards on page 26

To access Internet RFCs and drafts, go to the IETF web site: <http://www.ietf.org>.

## **Supported Internet RFCs and Drafts**

This section lists the supported Internet RFCs and drafts.

### **ATM**

RFC 1483, *Multiprotocol Encapsulation over ATM Adaptation Layer 5* (routed Protocol Data Units only)

RFC 2225, *Classical IP and ARP over ATM* (responses only)

RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5* (routed Protocol Data Units and ethernet bridged protocol data units only)

### **BGP**

RFC 1771, *A Border Gateway Protocol 4 (BGP-4)*

RFC 1772, *Application of the Border Gateway Protocol in the Internet*

RFC 1966, *BGP Route Reflection—An Alternative to Full-Mesh IBGP*

RFC 1997, *BGP Communities Attribute*

RFC 2270, *Using a Dedicated AS for Sites Homed to a Single Provider*

RFC 2283, *Multiprotocol Extensions for BGP-4*

RFC 2385, *Protection of BGP Sessions via the TCP MD5 Signature Option*

RFC 2439, *BGP Route Flap Damping*

RFC 3065, *Autonomous System Confederations for BGP*

RFC 3107, *Carrying Label Information in BGP-4*

*BGP/MPLS VPNs*, Internet Draft draft-ietf-ppvpn-rfc2547bis-00.txt

*Capabilities Negotiation with BGP4*, Internet Draft draft-ietf-idr-cap-neg-01

### **CHAP**

RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*

### **Frame Relay**

RFC 1490, *Multiprotocol Interconnect over Frame Relay*

## **GRE and IP-IP Encapsulation**

RFC 1701, *Generic Routing Encapsulation (GRE)*

RFC 1702, *Generic Routing Encapsulation over IPv4 Networks*

RFC 2003, *IP Encapsulation within IP*

## **IP Multicast**

RFC 1112, *Host Extensions for IP Multicasting* (defines IGMP Version 1)

RFC 2236, *Internet Group Management Protocol, Version 2*

RFC 2327, *SDP: Session Description Protocol*

RFC 2362, *Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*

RFC 2365, *Administratively Scoped IP Multicast*

RFC 2547, *BGP/MPLS VPNs*

*Anycast RP Mechanism using PIM and MSDP*, Internet Draft  
draft-ietf-mboned-anycast-rp-05.txt

*Bootstrap Router (BSR) Mechanism for PIM Sparse Mode*, Internet draft  
draft-ietf-pim-sm-bsr-02.txt

*Distance Vector Multicast Routing Protocol*, Internet Draft  
draft-ietf-idmr-dvmrp-v3-07.txt

*Internet Group Management Protocol, Version 3*, Internet Draft  
draft-ietf-idmr-igmp-v3-07.txt (only SAP, Version 0 and 1)

*Multicast in MPLS/BGP VPNs*, Internet Draft draft-rosen-vpn-mcast-00.txt

*Multicast Source Discovery Protocol (MSDP)*, Internet Draft draft-ietf-msdp-spec-01.txt

*Protocol Independent Multicast-Version 2 Dense Mode Specification*, Internet Draft  
draft-ietf-pim-v2-dm-03.txt

*SAP: Session Announcement Protocol*, Internet Draft draft-ietf-mmusic-sap-00.txt

*Source-Specific Multicast for IP*, Internet Draft draft-holbrook-ssm-arch-02.txt

## **IPSec and IKE**

RFC 2085, *HMAC-MD5 IP Authentication with Replay Prevention*

RFC 2401, *Security Architecture for the Internet Protocol*

RFC 2402, *IP Authentication Header (except for ESP/PIC)*

RFC 2403, *The Use of HMAC-MD5-96 within ESP and AH*

RFC 2404, *The Use of HMAC C-SHA-1-96 within ESP and AH*

RFC 2405, *The ESP DES-CBC Cipher Algorithm With Explicit IV*

RFC 2406, *IP Encapsulation Security Payload*

RFC 2407, *The Internet IP Security Domain of Interpretation for ISAKMP*

RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*

RFC 2409, *Internet Key Exchange*

RFC 2410, *The NULL Encryption Algorithm and Its Use With IPsec*

RFC 2412, *The OAKLEY Key Determination Protocol*

## **IPv6**

ISO/IEC 10589, *Information technology, Telecommunications and information exchange between systems, Intermediate system to intermediate system intradomain routing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)*

RFC 1157, *A Simple Network Management Protocol (SNMP)*

RFC 1213, *Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II*

RFC 1215, *A Convention for Defining Traps for Use with SNMP*

RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*

RFC 1771, *A Border Gateway Protocol 4 (BGP-4)*

RFC 1772, *Application of the Border Gateway Protocol in the Internet*

RFC 1901, *Introduction to Community-based SNMPv2*

RFC 1902, *Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)*

RFC 1905, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*

RFC 1965, *Autonomous System Confederations for BGP*

RFC 1966, *BGP Route Reflection: An Alternative to Full-Mesh IBGP*

RFC 1997, *BGP Communities Attribute*

RFC 2080, *RIPng for IPv6*

RFC 2081, *RIPng Protocol Applicability Statement*

RFC 2270, *Using a Dedicated AS for Sites Homed to a Single Provider*

- RFC 2283, *Multiprotocol Extensions for BGP-4*
- RFC 2373, *IP Version 6 Addressing Architecture*
- RFC 2385, *Protection of BGP Sessions via the TCP MD5 Signature Option*
- RFC 2439, *BGP Route Flap Damping*
- RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*
- RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*
- RFC 2461, *Neighbor Discovery for IP Version 6 (IPv6)*
- RFC 2464, *Transmission of IPv6 Packets over Ethernet Networks*
- RFC 2472, *IP Version 6 over PPP*
- RFC 2578, *Structure of Management Information Version 2 (SMIv2)*
- RFC 2763, *Dynamic Hostname Exchange Mechanism for IS-IS*
- RFC 2893, *Transition Mechanisms for IPv6 Hosts and Routers*
- *Routing IPv6 with IS-IS*, Internet Draft draft-ietf-isis-ipv6-02.txt
- *Capabilities Negotiation with BGP-4*, Internet Draft draft-ietf-idr-cap-neg-01.txt
- *BGP Extended Communities Attribute*, Internet Draft draft-ramachandra-bgp-ext-communities-09.txt

## **IS-IS**

- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*
- RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*
- RFC 2763, *Dynamic Hostname Exchange Mechanism for IS-IS*
- RFC 2966, *Domain-wide Prefix Distribution with Two-Level IS-IS*
- RFC 2973, *IS-IS Mesh Groups*
- *IS-IS Extensions for Traffic Engineering*, Internet Draft draft-ietf-isis-traffic-02.txt
- *Three-Way Handshake for IS-IS Point-to-Point Adjacencies*, Internet draft draft-ietf-isis-3way-03.txt

## **LDP**

- *Label Distribution Protocol (LDP)—Version 1 Functional Specification*, (draft-ietf-mpls-ldp-06.txt)

**MIBs**

IEEE, 802.3ad, *Aggregation of Multiple Link Segments* (only the objects dot3adAggMACAddress, dot3adAggAggregateOrIndividual, dot3adAggPortListPorts, and dot3adTablesLastChanged)

RFC 1157, *A Simple Network Management Protocol (SNMP)*

RFC 1213, *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*. (except for ipRouteTable, which has been replaced by ipCidrRouteTable (RFC 2096)

RFC 1215, *Convention for Defining Traps for Use with the SNMP* (only MIB II SNMP version 1 traps and version 2 notifications)

RFC 1657, *Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIV2*

RFC 1850, *OSPF Version 2 Management Information Base* (except for the ospfOriginateNewLsas and ospfRxNewLsas objects, the Host Table, and the traps ospfOriginateLSA, ospfLsdbOverflow, and ospfLsdbApproachingOverflow)

RFC 1901, *Introduction to Community-based SNMPv2*

RFC 1902, *Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)*

RFC 1905, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*

RFC 1907, *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)*

RFC 2011, *SNMPv2 Management Information Base for the Internet Protocol using SMIV2*

RFC 2012, *SNMPv2 Management Information Base for the Transmission Control Protocol using SMIV2*

RFC 2013, *SNMPv2 Management Information Base for the User Datagram Protocol using SMIV2*

RFC 2096, *IP Forwarding Table MIB*

RFC 2115, *Management Information Base for Frame Relay DTEs Using SMIV2*

RFC 2233, *The Interfaces Group MIB-II using SMIV2* (except ifRcvAddressTable)

RFC 2287, *Definitions of System-Level Managed Objects for Applications* (only sysAppInstallPkgTable, sysAppInstallElmtTable, sysAppElmtRunTable, and sysAppMapTable)

RFC 2465, *Management Information Base for IP Version 6: Textual Conventions and General Group* (except IPv6 or ICMPv6 statistics)

RFC 2495, *Definitions of Managed Objects for the DS1, E1, DS2, and E2 Interface Types* (except for dsx1FarEndConfigTable, dsx1FarEndCurrentTable, dsx1FarEndIntervalTable, dsx1FarEndTotalTable, and dsx1FracTable)

RFC 2496, *Definitions of Managed Objects for the DS3/E3 Interface Type* (except dsx3FarEndConfigTable, dsx3FarEndCurrentTable, dsx3FarEndIntervalTable, dsx3FarEndTotalTable, and dsx3FracTable)

RFC 2515, *Definitions of Managed Objects for ATM Management* (except atmVpCrossConnectTable, atmVcCrossConnectTable, and aal5VccTable)

RFC 2558, *Definitions of Managed Objects for the SONET/SDH Interface Type*

RFC 2665, *Definitions of Managed Objects for the Ethernet-like Interface Types*

RFC 2790, *Host Resources MIB* (only the objects of the hrSystem and hrSWInstalled groups)

RFC 2819, *Remote Network Monitoring Management Information Base* (the etherStatsTable for Ethernet interfaces only, and only the objects alarmTable, eventTable, and logTable)

RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations* (only the objects pingCtlTable, pingResultsTable, pingProbeHistoryTable, pingMaxConcurrentRequests, traceRouteCtlTable, traceRouteResultsTable, traceRouteProbeHistoryTable, and traceRouteHopsTable)

RFC 2932, *IPv4 Multicast Routing MIB*

*IANAiftype Textual Convention MIB*, Internet Assigned Numbers Authority (referenced by RFC 2233, available at <ftp://ftp.isi.edu/mib/ianaiftype.mib>)

*Internet Group Management Protocol (IGMP) MIB*, Internet draft draft-ietf-idmr-igmp-mib-13.txt

*Protocol Independent Multicast (PIM) MIB*, Internet Draft draft-ietf-idmr-pim-mib-09.txt

## **MPLS**

RFC 2205, *Resource ReSerVation Protocol (RSVP)—Version 1 Functional Specification*

RFC 2209, *Resource ReSerVation Protocol (RSVP)—Version 1 Message Processing Rules*

RFC 2210, *The Use of RSVP with IETF Integrated Services*

RFC 2211, *Specification of the Controlled-Load Network Element Service*

RFC 2215, *General Characterization Parameters for Integrated Service Network Elements*

RFC 2216, *Network Element Service Specification Template*

RFC 2702, *Requirements for Traffic Engineering Over MPLS*

RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels*

*BGP/MPLS VPNs*, Internet Draft draft-ietf-ppvpn-rfc2547bis-00.txt

*Fast Reroute Extensions to RSVP-TE for LSP Tunnels*, draft-ietf-mpls-rsvp-lsp-fastreroute-00.txt (except node protection in facility backup)

*ICMP Extensions for Multiprotocol Label Switching*, Internet Draft  
draft-ietf-mpls-icmp-01.txt

*MPLS-based Layer 2 VPNs*, Internet Draft draft-kompella-ppvnp-l2vpn-00.txt

*MPLS Label Stack Encoding*, Internet Draft draft-ietf-mpls-label-encaps-07.txt

*Transport of Layer 2 Frames Over MPLS*, Internet Draft  
draft-martini-l2circuit-trans-mpls-07.txt

## **OSPF**

RFC 1587, *The OSPF NSS A Option*

RFC 2328, *OSPF Version 2*

*Traffic Engineering Extensions to OSPF*, Internet Draft draft-katz-yeung-ospf-traffic-01.txt

## **PPP**

RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*

RFC 1661, *The Point-to-Point Protocol (PPP)*

RFC 1662, *PPP in HDLC-like Framing*

RFC 2615, *PPP over SONET/SDH*

## **RIP**

RFC 1058, *Routing Information Protocol*

RFC 2453, *RIP Version 2*

## **RSVP**

RFC 2205, *Resource ReSerVation Protocol (RSVP), Version 1, Functional Specification*

RFC 2209, *Resource ReSerVation Protocol (RSVP), Version 1, Message Processing Rules*

RFC 2210, *The Use of RSVP with IETF Integrated Services*

RFC 2211, *Specification of the Controlled-Load Network Element Service*

RFC 2212, *Specification of Guaranteed Quality of Service*

RFC 2215, *General Characterization Parameters for Integrated Service Network Elements*

RFC 2216, *Network Element Service Specification Template*

RFC 2747, *RSVP Cryptographic Authentication*

**TCP/IP v4**

RFC 2961, *RSVP Refresh Overhead Reduction Extensions*

RFC 768, *User Datagram Protocol*

RFC 791, *Internet Protocol*

RFC 792, *Internet Control Message Protocol*

RFC 793, *Transmission Control Protocol*

RFC 826, *Ethernet Address Resolution Protocol*

RFC 854, *Telnet Protocol Specification*

RFC 862, *Echo Protocol*

RFC 863, *Discard Protocol*

RFC 896, *Congestion Control in IP/TCP Networks*

RFC 919, *Broadcasting Internet Datagrams*

RFC 922, *Broadcasting Internet Datagrams in the Presence of Subnets*

RFC 959, *File Transfer Protocol*

RFC 1027, *Using ARP to Implement Transparent Subnet Gateways*

RFC 1042, *Standard for the Transmission of IP Datagrams over IEEE 802 Networks*

RFC 1157, *Simple Network Management Protocol (SNMP)*

RFC 1166, *Internet Numbers*

RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*

RFC 1256, *ICMP Router Discovery Messages*

RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation, and Analysis*

RFC 1519, *Classless Inter-Domain Routing (CIDR): An Address Assignment and Aggregation Strategy*

RFC 1812, *Requirements for IP Version 4 Routers*

RFC 2338, *Virtual Router Redundancy Protocol*

## Supported ISO Standards

### IS-IS

ISO/IEC 10589, *Information technology, Telecommunications and information exchange between systems, Intermediate system to intermediate system intradomain routing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)*

## Supported SDH and SONET Standards

ANSI T1.105, *Synchronous Optical Network (SONET) Basic Description Including Multiplex Structures, Rates, and Formats*

ANSI T1.105.02, *Synchronous Optical Network (SONET) Payload Mappings*

ANSI T1.105.06, *SONET: Physical Layer Specifications*

GR-253-CORE, *SONET Transport Systems: Common Generic Criteria*

GR-499-CORE, *Transport System Generic Requirements (TSGR): Common Requirements*

GR-1377-CORE, *SONET OC-192 Transport System Generic Criteria*

ITU-T Recommendation G.691, *Optical interfaces for single channel SDH systems with optical amplifiers, and STM-64 systems*

ITU-T Recommendation G.707 (1996), *Network node interface for the synchronous digital hierarchy (SDH)*

ITU-T Recommendation G.783 (1994), *Characteristics of Synchronous Digital Hierarchy (SDH) equipment functional blocks*

ITU-T Recommendation G.813 (1996), *Timing characteristics of SDH equipment slave clocks (SEC)*

ITU-T Recommendation G.825 (1993), *The control of jitter and wander within digital networks which are based on the Synchronous Digital Hierarchy (SDH)*

ITU-T Recommendation G.826 (1999), *Error performance parameters and objectives for international, constant bit rate digital paths at or above the primary rate*

ITU-T Recommendation G.831 (1993), *Management capabilities of transport networks based on Synchronous Digital Hierarchy (SDH)*

ITU-T Recommendation G.957 (1995), *Optical interfaces for equipment and systems relating to the synchronous digital hierarchy*

ITU-T Recommendation G.958 (1994), *Digital line systems based on the Synchronous Digital Hierarchy for use on optical fibre cables*

ITU-T Recommendation I.432 (1993), *B-ISDN User-Network Interface Physical layer specification*

**Other Supported Standards**

**ATM**

ITU-T Recommendation I.363, B-ISDN ATM adaptation layer sublayers: service-specific coordination function to provide the connection-oriented transport service (JUNOS software conforms only to the AAL5/IP over ATM portion of this standard)

ITU-T Recommendation I.432.3, B-ISDN user-network interface Physical layer specifications: 51,840 kbits/s operation

**Ethernet**

IEEE, 802.3ad, *Aggregation of Multiple Link Segments*

IEEE, 802.3, *Carrier Sense Multiple Access with Collision Detection (CSMA/CD)*

**Frame Relay**

ANSI T1.617-1991, Annex D, Additional procedures for permanent virtual connections (PVCs) using unnumbered information frames

ITU Q.933a, Annex A, Additional Procedures for Permanent Virtual Connections (PVC) status management (using Unnumbered Information frames)

**T3**

ITU-T Recommendation G.703, Physical/electrical characteristics of hierarchical digital interfaces