

Chapter 1

JUNOS Software Overview

The JUNOS 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 Network and Services Interfaces Command Reference* and the *JUNOS Protocols, Class of Service, and System Basics Command Reference*.

This chapter discusses the following topics:

Routing Engine Software Components on page 4

Software Installation Overview on page 11

Tools for Accessing and Controlling the Software on page 11

Software Configuration Overview on page 12

Using Software Monitoring Tools on page 13

Router Security on page 14

Supported Software Standards on page 19

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 41). This section describes the Routing Engine components:

Routing Protocol Process on page 4

VPNs on page 9

Interface Process on page 9

Chassis Process on page 9

SNMP and MIB II Processes on page 10

Management Process on page 10

Routing Engine Kernel on page 10

For information about Routing Engine software components and Routing Engine functions in a routing matrix, see the *TX Matrix Platform Hardware Guide*.

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:

IPv4 Routing Protocols on page 5

IPv6 Routing Protocols on page 6

Routing and Forwarding Tables on page 7

Routing Policy on page 8

IPv4 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 Multiprotocol Label Switching (MPLS) applications protocols:

Unicast routing protocols:

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.

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

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.

Multicast routing protocols:

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

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

MSDP—Multicast Source Discovery Protocol allows multiple Protocol Independent Multicast (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.

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.

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

MPLS applications protocols:

LDP—The Label Distribution Protocol provides a mechanism for distributing labels in nontraffic-engineered applications. LDP allows routers to establish label-switched paths (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 Resource Reservation Protocol (RSVP).

MPLS—Multiprotocol Label Switching, formerly known as tag switching, allows you to manually or dynamically configure 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—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 LSPs.

IPv6 Routing Protocols

The JUNOS software implements IP routing functionality, providing support for IP version 6 (IPv6). The routing protocols have been developed to provide the scale and control necessary for the Internet core.

The software supports the following unicast routing protocols:

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

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

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

OSPF version 3 (OSPFv3) supports IPv6. The fundamental mechanisms of OSPF such as flooding, designated router (DR) election, area-based topologies, and the SPF calculations remain unchanged. Some differences exist either due to changes in protocol semantics between IPv4 and IPv6, or to handle the increased address size of IPv6.

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.

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 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 41 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. BGP, IS-IS, OSPF, and RIP 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. BGP, IS-IS, OSPF, and RIP 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 (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.

VPNs

The JUNOS software supports several types of virtual private networks (VPNs):

Layer 2 VPNs—A Layer 2 VPN links a set of sites sharing common routing information, and whose connectivity is controlled by a collection of policies. A Layer 2 VPN is not aware of routes within a customer's network. It simply provides private links between a customer's sites over the service provider's existing public Internet backbone.

Layer 3 VPNs—A Layer 3 VPN links a set of sites that share common routing information, and whose connectivity is controlled by a collection of policies. A Layer 3 VPN is aware of routes within a customer's network, requiring more configuration on the part of the service provider than a Layer 2 VPN. The sites that make up a Layer 3 VPN are connected over a service provider's existing public Internet backbone.

Inter-provider VPNs—An inter-provider VPN supplies connectivity between two VPNs in separate autonomous systems (ASs). This functionality could be used by a VPN customer with connections to several various Internet service providers (ISPs), or different connections to the same ISP in various geographic regions.

Carrier-of-carrier VPNs—Carrier-of-carrier VPNs allow a VPN service provider to supply VPN service to a customer who is also a service provider. The latter service provider supplies Internet or VPN service to an end customer.

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 Flexible PIC Concentrator [FPC] is installed in and which location on the FPC the Physical Interface Card [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 daemon (chassisd) on the Routing Engine communicates directly with its peer processes running on the Packet Forwarding Engine.

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, version 2 (also known as version 2c, or v2c), and version 3 (SNMPv3). 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 Management Information Base II (MIB II) processes, which consist of an SNMP master agent and various subagents. For information about SNMP, see the *JUNOS Network Management Configuration Guide*.

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 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 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 drive. 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 PC 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 drive, then finally the hard disk. Normally, you want the router to boot from the flash drive.

To upgrade the software, you copy a set of software images over the network to the router's flash drive 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 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 megabits-per-second (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 12

Configuring the Software on page 12

Activating a Configuration on page 13

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 up a router, the system prompts you to log in. Log in as the user “root” (with no password) and configure a password for the user “root.” Then configure the router’s name, domain name, and the Internet address of at least one interface on the router.

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.

Using 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 in to 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.

Router Security

Router security consists of three major elements: physical security of the router, operating system security, and security that can be effected through configuration. Physical security involves restricting access to the router. Exploits that can easily be prevented from remote locations are extremely difficult or impossible to prevent if an attacker can gain access to the router's management port or console. The inherent security of the JUNOS operating system also plays an important role in router security. The JUNOS software is extremely stable and robust. The JUNOS software also provides features to protect against attacks, allowing you to configure the router to minimize vulnerabilities.

In designing your router configuration, you can increase router security by *hardening* the configuration, using the JUNOS features to apply sound security policies. In this way, virtually any router configuration should be capable of secure operation. Likewise, misconfiguring the JUNOS software can increase router vulnerability.

This section discusses some JUNOS software features available to improve router security:

JUNOS Default Settings on page 15

Router Access on page 16

User Authentication on page 16

Specifying Plain-Text Passwords on page 17

Routing Protocol Security Features on page 18

Firewall Filters on page 19

Auditing for Security on page 19

JUNOS Default Settings

Immediately after installation and configuration of a root account password, the JUNOS software presents a hardened target by virtue of its default software settings. The following are some common router security weaknesses that the JUNOS software addresses in the default software settings:

The JUNOS software does not forward directed broadcast messages. Directed broadcast services send ping requests from a spoofed source address to a broadcast address and can be used to attack other Internet users. For example, if broadcast ping messages were allowed on the 200.0.0.0/24 network, a single ping request could result in up to 254 responses, all aimed at the supposed source of the ping. The result would be that the source actually becomes the victim of a denial of service (DoS) attack.

Only console access to the router is enabled by default. Remote management access to the router and all management access protocols, including Telnet, FTP, and SSH (secure shell), are disabled by default.

The JUNOS software does not support the SNMP set capability for editing configuration data. While the software does support the SNMP set capability for monitoring and troubleshooting the network, this support exposes no known security issues. (You can configure the software to disable this SNMP set capability.)

The JUNOS software ignores martian addresses that contain the following prefixes: 0.0.0.0/8, 127.0.0.0/8, 128.0.0.0/16, 191.255.0.0/16, 192.0.0.0/24, 223.255.55.0/24, and 240.0.0.0/4. Martian addresses are reserved host or network addresses about which all routing information should be ignored.

Router Access

When you first install the JUNOS software, all remote access to the router is disabled, thereby ensuring that remote access is possible only if deliberately enabled by an authorized user. You can establish remote communication with a router in one of the following ways:

Out-of-band management—Allows connection to the router through an interface dedicated to router management. Juniper Networks routers support out-of-band management with a dedicated management Ethernet interface (fxp0), as well as EIA-232 console and auxiliary ports. The management Ethernet interface connects directly to the Routing Engine. No transit traffic is allowed through this interface, providing complete separation of customer and management traffic and ensuring that congestion or failures in the transit network do not affect the management of the router.

Inband management—Allows connection to the routers using the same interfaces through which customer traffic flows. While this approach is simple and requires no dedicated management resources, it has some disadvantages:

Management flows and transit traffic flows are mixed together. Any attack traffic that is mixed with the normal traffic can affect the communication with the router.

The links between the router might not be totally trustworthy, leading to the possibility of wiretapping and replay attacks.

For management access to the router, the standard ways to communicate with the router from a remote console are with telnet and the secure shell (ssh). ssh provides secure encrypted communications and is therefore useful for inband router management. Telnet provides unencrypted, and therefore less secure, access to the router.

User Authentication

On a route, you can create local user login accounts to control who can log into the router and the access privileges they have. A password, either an ssh key or a Message Digest 5 (MD5) password, is associated with each login account. To define access privileges, you create login classes in to which you group users with similar jobs or job functions. You use these classes to explicitly define what commands their users are and are not allowed to issue while logged in to the router.

The management of multiple routers by many different personnel can create a user account management problem. One solution is to use a central authentication service to simplify account management, creating and deleting user accounts only on a single, central server. A central authentication system also simplifies the use of one-time password systems such as SecureID, which offer protection against password sniffing and password replay attacks (attacks in which someone uses a captured password to pose as a router administrator).

The JUNOS software supports two protocols for central authentication of users on multiple routers—Remote Authentication Dial In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+). RADIUS is a multivendor IETF standard whose features are more widely accepted than those of TACACS+ or other proprietary systems. All one-time-password system vendors support RADIUS.

The JUNOS software also supports the following:

Internet Protocol Security (IPSec). IPSec architecture provides a security suite for the IPv4 and IPv6 network layers. The suite provides such functionality as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. In addition to IPSec, the JUNOS software also supports the Internet Key Exchange (IKE), which defines mechanisms for key generation and exchange, and manages security associations (SAs). For more information about IPSec, see the *JUNOS Services Interfaces Configuration Guide* and “Security Services” on page 617.

MD5 authentication of MSDP peering sessions. This authentication provides protection against spoofed packets being introduced into a peering session. For more information about SNMPv3, see the *JUNOS Multicast Protocols Configuration Guide*.

SNMPv3 authentication and encryption. SNMPv3 uses the user-based security model (USM) for message security and the view-based access control model (VACM) for access control. USM specifies authentication and encryption. VACM specifies access-control rules. For more information about SNMPv3, see the *JUNOS Network Management Configuration Guide*.

Specifying Plain-Text Passwords

The JUNOS software has special requirements when you create plain-text passwords on a routing platform:

The password must be at least 6 characters long.

You can include most character classes in a password (alphabetic, numeric, and special characters), except control characters.

Valid passwords must contain at least one change of case or character class.

You can include the plain-text-password statement at the [edit system diag-port-authentication], [edit system pic-console-authentication], [edit system root-authentication], and [edit system login user *username* authentication] hierarchy levels.

Table 2 lists error messages that display when you enter an invalid plain-text password.

Table 2: Plain-text Password Error Messages

Problem with password	Resulting error message
Too few characters; for example, "abc".	Minimum password length is 6
Does not include a change of case, numeric, or special character; for example, "abcdefg".	Require change of case, digits or punctuation
Does not match the original password.	Passwords are not equal; aborting

For more information about how to create plain-text passwords, see “Configuring the Root Password” on page 355, “Configuring User Accounts” on page 387, and “Configuring the Password on the Diagnostics Port” on page 435.

Routing Protocol Security Features

The main task of a router is to forward user traffic toward its intended destination based on the information in the router’s routing and forwarding tables. You can configure routing policies that define the flows of routing information through the network, controlling which routes the routing protocols place in the routing tables and which routes they advertise from the tables. You can also use routing policies to change specific route characteristics, change the BGP route flap-damping values, perform per-packet load balancing, and enable class of service (CoS).

Attackers can send forged protocol packets to a router with the intent of changing or corrupting the contents of its routing table or other databases, which in turn could degrade the functionality of the router. To prevent such attacks, you must ensure that routers form routing protocol peering or neighboring relationships with trusted peers. One way to do this is by authenticating routing protocol messages. The JUNOS BGP, IS-IS, OSPF, RIP, and RSVP protocols support HMAC-MD5 authentication, which uses a secret key combined with the data being protected to compute a hash. When the protocols send messages, the computed hash is transmitted with the data. The receiver uses the matching key to validate the message hash.

The JUNOS software supports the IPSec security suite for the IPv4 and IPv6 network layers. The suite provides such functionality as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. The JUNOS software also supports IKE, which defines mechanisms for key generation and exchange, and manages SAs.

Firewall Filters

Firewall filters allow you to control packets transiting the router to a network destination and packets destined for and sent by the router. You can configure firewall filters to control which data packets are accepted on and transmitted from the physical interfaces, and which local packets are transmitted from the physical interfaces and to the Routing Engine. Firewall filters provide a means of protecting your router from excessive traffic. Firewall filters that control local packets can also protect your router from external aggressions, such as DoS attacks.

To protect the Routing Engine, you can configure a firewall filter only on the router's loopback interface. Adding or modifying filters for each interface on the router is not necessary. You can design firewall filters to protect against ICMP and Transmission Control Protocol (TCP) connection request (SYN) floods and to rate-limit traffic being sent to the Routing Engine.

Auditing for Security

The JUNOS software logs significant events that occur on the router and within the network. Although the logging of events and actions does not increase router security, you can use the system logs to monitor the effectiveness of your security policies and router configurations. You can also use the logs when reacting to a continued and deliberate attack as a means of identifying the source address, router, or port of the attacker's traffic. You can configure the logging of different levels of events, from only critical events to all events, including informational events. You can then inspect the contents of the system log files either in real time or at a later time.

Debugging and troubleshooting is much easier when the timestamps in the system log files of all routers are synchronized, because events that span the network might be correlated with synchronous entries in multiple logs. The JUNOS software supports the Network Time Protocol (NTP), which you can enable on the router to synchronize the system clocks of routers and other networking equipment. By default, NTP operates in an unauthenticated mode. You can configure various types of authentication, including an HMAC-MD5 scheme.

Supported Software Standards

This section lists the standards supported by the JUNOS software:

Supported Internet RFCs and Drafts on page 20

Supported ISO Standards on page 36

Supported SDH and SONET Standards on page 36

Other Supported Standards on page 37

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:

Asynchronous Transfer Mode (ATM) on page 21

BGP on page 21

Challenge Handshake Authentication Protocol (CHAP) on page 22

Firewall Filters on page 22

Frame Relay on page 22

Generalized MPLS (GMPLS) on page 22

Generalized Routing Encapsulation (GRE) and IP-IP Encapsulation on page 23

Integrated Local Management Interface (ILMI) on page 23

IP Multicast on page 23

IPSec and IKE on page 25

IPv6 on page 25

IS-IS on page 26

LDP on page 27

Link Management Protocol (LMP) on page 27

Layer 2 Tunneling Protocol (L2TP) on page 28

MIBs on page 28

MPLS on page 31

Network Address Translation (NAT) on page 33

OSPF on page 33

Point-to-Point Protocol (PPP) on page 33

RIP on page 33

RSVP on page 34

Secure Sockets Layer (SSL) on page 34

TCP/IP v4 on page 34

Voice Services on page 35

VPNs on page 35

Asynchronous Transfer Mode (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)

Internet draft draft-martini-l2circuit-encap-mpls-07.txt, *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks* (expires December 2004)

The JUNOS software has the following exceptions:

A packet with a sequence number of 0 is treated as out of sequence.

Any packet which does not have the next incremental sequence number is considered out of sequence.

When out-of-sequence packets arrive, the expected sequence number for the neighbor is set to the sequence number in the Layer 2 circuit control word.

Internet draft draft-martini-l2circuit-trans-mpls-09.txt, *Transport of Layer 2 Frames Over MPLS*

BGP

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

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

RFC 1965, *Autonomous System Confederations for BGP*

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 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*

RFC 2796, *BGP Route Reflection*

RFC 2858, *Multiprotocol Extensions for BGP-4*

RFC 3065, *Autonomous System Confederations for BGP*

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

Internet draft draft-ramachandra-bgp-ext-communities-09.txt, *BGP Extended Communities A ttribute*

Internet draft draft-ietf-l3vpn-rfc2547bis-03.txt, *BGP/MPLS IP VPNs*

Internet draft draft-kato-bgp-ipv6-link-local-00.txt, *BGP4+ Peering Using IPv6 Link-local Address*

Internet draft draft-ietf-idr-cap-neg-01.txt, *Capabilities Negotiation with BGP4* (expires February 1998)

Internet draft draft-ietf-idr-restart-10.txt, *Graceful Restart Mechanism f or BGP* (expires December 2004)

Internet draft draft-ietf-mpls-bgp-mpls-restart-03.txt *Graceful Restart Mechanism f or BGP with MPLS* (expires August 2004)

Internet draft draft-ietf-ngtrans-bgp-tunnel-04.txt, *Connecting IPv6 Islands across IPv4 Clouds with BGP* (only multiprotocol-BGP [MP-BGP] over IPv4 approach) (expires July 2002)

Challenge Handshake Authentication Protocol (CHAP)

RFC 1994, *PPP Challenge Handshak e Authentication Pr otocol (CHAP)*

Firewall Filters

RFC 2474, *Definition of the Differ entiated Services (DS) Field*

RFC 2475, *An Architecture for Differentiated Services*

RFC 2597, *Assured Forwarding PHB*

RFC 2598, *An Expedited F orwarding PHB*

Frame Relay

RFC 1490, *Multiprotocol Inter connect o ver Frame Relay*

Generalized MPLS (GMPLS)

RFC 3471, *Generalized Multi-Protocol Label Swit ching (GMPLS)-Signaling Functional Description*. The JUNOS software supports only the following areas:

Generalized label request (only bandwidth encoding)

Generalized label (only suggested label)

Bidirectional LSPs (only upstream label)

Control channel separation

RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions* (only Section 9, “Fault Handling”)

Internet draft draft-ietf-ccamp-gmpls-sonet-sdh-08.txt, *GMPLS Extensions for SONET and SDH Control* (only SUKLM labels and SONET traffic parameters)

Internet draft draft-ietf-mpls-generalized-rsvp-te-06.txt, *Generalized MPLS Signaling - RSVP-TE Extensions*. The JUNOS software supports only the following areas:

- Generalized label request object

- Generalized label object (only suggested labeled type)

- Bidirectional LSPs (only upstream label)

- Control channel separation (only IF-ID Hop object and IF-ID ErrSpec object)

- New addressing for Path and PathTear messages

Internet draft draft-ietf-ccamp-ospf-gmpls-extensions-09.txt, *OSPF Extensions in Support of Generalized MPLS* (interface switching only)

Internet draft draft-ietf-mpls-bundle-04.txt, *Link Bundling in MPLS Traffic Engineering*

Internet draft draft-ietf-ccamp-gmpls-routing-06.txt, *Routing Extensions in Support of Generalized MPLS*

Generalized Routing Encapsulation (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*

RFC 2890, *Key and Sequence Number Extensions to GRE*. The JUNOS software supports the key field, but not the sequence number field.

Integrated Local Management Interface (ILMI)

ILMI Management Information Base MIB (only the atmMYIPNmAddress and atmPortMyIfname objects). For more information about the ILMI MIB, see the *JUNOS Network Management Configuration Guide* and the ATM Forum at <http://www.atmforum.com/>.

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*

RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*

RFC 2858, *Multiprotocol Extensions for BGP-4*

RFC 2974, *Session Announcement Protocol*

RFC 3208, *PGM Reliable Transport Protocol Specification*

RFC 3376, *Internet Group Management Protocol, Version 3* (source-specific multicast [SSM] include mode only)

RFC 3446, *Anycast Rendezvous Point (RP) Mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*

RFC 3569, *An Overview of Source-Specific Multicast (SSM)*

RFC 3590, *Source Address Selection for Multicast Listener Discovery Protocol* (SSM include mode only)

RFC 3618, *Multicast Source Discovery Protocol (MSDP)*

Internet draft draft-ietf-pim-sm-bsr-03.txt, *Bootstrap Router (BSR) Mechanism for PIM Sparse Mode* (expired August 2003)

Internet draft draft-ietf-idmr-dvmrp-v3-11.txt, *Distance Vector Multicast Routing Protocol* (expired April 2004)

Internet draft draft-rosen-vpn-mcast-06.txt, *Multicast in MPLS/BGP VPNs, Option 2* (expired April 2004)

Internet draft draft-ietf-pim-sm-v2-new-10.txt, *Protocol Independent Multicast—Sparse Mode (PIM-SM): Protocol Specification (Revised)* (expires January 2005)

Internet draft draft-ietf-pim-dm-new-v2-05.txt, *Protocol Independent Multicast Version 2 Dense Mode Specification* (expires December 2004)

Internet draft draft-ietf-ssm-arch-06.txt, *Source-Specific Multicast for IP* (expires March 2005)

Internet draft draft-ietf-mboned-ssm232-08.txt, *Source-Specific Protocol Independent Multicast in 232/8* (expires September 2004)

Internet draft draft-holbrook-idmr-igmpv3-ssm-07.txt, *Using IGMPv3 and MLDv2 for Source-Specific Multicast* (expires December 2004)

Internet draft draft-raggarwa-l3vpn-2547-mvpn-00.txt, *Base Specification for Multicast in BGP/MPLS VPNs* (expires December 2004)

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*
- RFC 2403, *The Use of HMAC-MD5-96 within ESP and AH*
- RFC 2404, *The Use of HMAC-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*
- RFC 3706, *A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers*

IPv6

- 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 1981, *Path MTU Discovery for IP version 6*
- RFC 2080, *RIPng for IPv6*

RFC 2081, *RIPng Protocol Applicability Statement*

RFC 2283, *Multiprotocol Extensions for BGP-4*

RFC 2373, *IP Version 6 Addressing Architecture*

RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*

RFC 2461, *Neighbor Discovery for IP Version 6 (IPv6)*

RFC 2462, *IPv6 Stateless Address Autoconfiguration*

RFC 2463, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*

RFC 2464, *Transmission of IPv6 Packets over Ethernet Networks*

RFC 2472, *IP Version 6 over PPP*

RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*

RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*

RFC 2578, *Structure of Management Information Version 2 (SMIPv2)*

RFC 2740, *OSPF for IPv6*

RFC 2878, *PPP Bridging Control Protocol*

RFC 2893, *Transition Mechanisms for IPv6 Hosts and Routers*

Internet draft draft-kato-bgp-ipv6-link-local-00.txt, *BGP4+ Peering Using IPv6 Link-local Address* (expires April 2002)

Internet draft draft-ietf-dhc-dhcpv6-16.txt, *Dynamic Host Configuration Protocol for Ipv6* (expires May 2001)

Internet draft draft-ietf-ngtrans-bgp-tunnel-04.txt, *Connecting IPv6 Islands across IPv4 Clouds with BGP* (only MP-BGP over IPv4 approach)

Internet draft draft-ietf-isis-ipv6-02.txt, *Routing IPv6 with IS-IS*

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*

Internet draft draft-ietf-katz-ward-bfd-02.txt, *Bidirectional Forwarding Detection* (except the transmission of echo packets) (expires January 2005)

Internet draft draft-ietf-isis-hmac-03.txt, *IS-IS Cryptographic Authentication* (expires January 2002)

Internet draft draft-ietf-isis-traffic-04.txt, *IS-IS Extensions for Traffic Engineering* (expires February 2002)

Internet draft draft-ietf-isis-wg-multi-topology-04.txt, *M-ISIS: Multi Topology (MT) Routing in IS-IS* (expires December 2004)

Internet draft draft-ietf-isis-snp-checksum-02.txt, *Optional Checksums for IS-IS* (expires 2001)

Internet draft draft-ietf-isis-igp-p2p-over-lan-03.txt, *Point-to-point operation over LAN in link-state routing protocols* (expires February 2004)

Internet draft draft-ietf-isis-restart-05.txt, *Restart signaling for IS-IS* (expires February 2002)

Internet draft draft-ietf-isis-ipv6-02.txt, *Routing IPv6 with IS-IS* (expires September 2001)

Internet draft draft-ietf-isis-3way-03.txt, *Three-Way Handshake for IS-IS Point-to-Point Adjacencies* (expires January 2001)

LDP

RFC 3036, *LDP Specification*. The JUNOS software does not support the following areas:

Label distribution control mode: ordered (only independent)

Label retention mode: liberal (only conservative)

Label advertisement mode: downstream unsolicited (only downstream on demand)

Loop detection

Constraint-Based Routed LDP (CR-LDP)

Internet draft draft-ietf-mpls-ldp-restart-06.txt, *Graceful Restart Mechanism for LDP*

Link Management Protocol (LMP)

Internet draft draft-ietf-ccamp-lmp-09.txt, *Link Management Protocol (LMP)*

Layer 2 Tunneling Protocol (L2TP)

RFC 2661, *Layer Two Tunneling Protocol "L2TP"*

RFC 2866, *Radius Accounting*

MIBs

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

Only the following are supported:

dot3adAggPortTable, dot3adAggPortListTable, dot3adAggTable, and dot3adAggPortStatsTable

dot3adAggPortDebugTable (only dot3adAggPortDebugRxState, dot3adAggPortDebugMuxState, dot3adAggPortDebugActorSyncTransitionCount, dot3adAggPortDebugPartnerSyncTransitionCount, dot3adAggPortDebugActorChangeCount, and dot3adAggPortDebugPartnerChangeCount)

dot3adTablesLastChanged

RFC 1155, *Structure and Identification of Management Information for TCP/IP-based Internets*

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

RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments* (only isisSystem, isisMANAreaAddr, isisAreaAddr, isisSysProtSupp, isisSummAddr, isisCirc, isisCircLevel, isisPacketCount, isisISAdj, isisISAdjAreaAddr, isisAdjIPAddr, isisISAdjProtSupp, isisRa, and isisIPRA)

RFC 1212, *Concise MIB Definitions*

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, *IP Forwarding Table MIB*])

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

RFC 1406, *Definitions of Managed Objects for the DS1 and E1 Interface Types* (T1 MIB is supported)

RFC 1407, *Definitions of Managed Objects for the DS3/E3 Interface Type* (T3 MIB is supported)

RFC 1657, *Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIPv2*

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 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 SMIPv2*

RFC 2012, *SNMPv2 Management Information Base for the Transmission Control Protocol using SMIPv2*

RFC 2013, *SNMPv2 Management Information Base for the User Datagram Protocol using SMIPv2*

RFC 2096, *IP Forwarding Table MIB*

RFC 2115, *Management Information Base for Frame Relay DTEs Using SMIPv2*

RFC 2287, *Definitions of System-Level Managed Objects for Applications* (only sysApplInstallPkgTable, sysApplInstallElmtTable, sysApplElmtRunTable, and sysApplMapTable)

RFC 2465, *Management Information Base for IP Version 6: Textual Conventions and General Group* (except IPv6 or ICMP version 6 [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 2571, *An Architecture for Describing SNMP Management Frameworks* (read-only access)

RFC 2576, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*

RFC 2578, *Structure of Management Information Version 2 (SMIPv2)*

RFC 2579, *Textual Conventions for SMIPv2*

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

RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol* (except row creation, set operation, and the object vrrpStatsPacketLengthErrors)

RFC 2790, *Host Resources MIB*

Only the hrStorageTable. The file systems /, /config, /var, and /tmp will always return the same index number. When SNMP restarts, the index numbers for the remaining file systems might change.

Only the objects of the hrSystem and hrSWInstalled groups.

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

RFC 2863, *The Interfaces Group MIB*

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*

RFC 2933, *Internet Group Management Protocol (IGMP) MIB*

RFC 2934, *Protocol Independent Multicast MIB for IPv4*

RFC 3413, *Simple Network Management Protocol (SNMP) Applications* (except for the proxy MIB)

RFC 3414, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*

RFC 3415, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*

RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*

RFC 3498, *Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures* (implemented under the Juniper Networks enterprise branch)

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

ESO Consortium MIB, which can be found at <http://www.snmp.com/eso/>

Internet draft draft-ietf-idr-bgp4-mibv2-04.txt, *Definitions of Managed Objects for the Fourth Version of Border Gateway Protocol (BGP-4), Second Version* (only jnxBgpM2PrefixInPrefixes, jnxBgpM2PrefixInPrefixesAccepted, and jnxBgpM2PrefixInPrefixesRejected objects) (June 12, 2004)

Internet draft draft-reeder-snmipv3-usm-3desede-00.txt, *Extension to the User-Based Security Model (USM) to Support Triple-DES EDE in 'Outside' CBC Mode*

Internet draft draft-ietf-ppvpn-mpls-vpn-mib-05.txt, *MPLS/BGP Virtual Private Network Management Information Base Using SMIPv2* (only mplsVpnScalars, mplsVpnVrfTable, mplsVpnVrfPerfTable, and mplsVpnVrfRouteTargetTable)

Internet draft draft-ietf-isis-wg-mib-16.txt, *Management Information Base for IS-IS* (only isisISAdjTable, isisISAdjAreaAddrTable, isisISAdjIPAddrTable, and isisISAdjProtSuppTable) (expires January 2005)

Internet draft draft-ietf-msdp-mib-08.txt, *Multicast Source Discovery protocol MIB* (except msdpEstablished, msdpBackwardTransition, and msdpRequestsTable) (expires April 2004)

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 2858, *Multiprotocol Extensions for BGP-4*

RFC 3031, *Multiprotocol Label Switching Architecture*

RFC 3032, *MPLS Label Stack Encoding*

RFC 3208, *PGM Reliable Transport Protocol Specification* (only the network element)

RFC 3270, *Multi-Protocol Label Switching (MPLS) Support of Differentiated Services (e-lsps only)*

RFC 3443, *Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks*

RFC 3469, *Framework for Multi-Protocol Label Switching (MPLS)-based Recovery*

RFC 3478, *Graceful Restart Mechanism for Label Distribution Protocol*

RFC 3564, *Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering*

Internet draft draft-ietf-l3vpn-rfc2547bis-03.txt, *BGP/MPLS IP VPNs*

Internet draft draft-ietf-mpls-lsp-ping-version-05.txt, *Detecting MPLS Data Plane Failures* (only the LDP IPv4 prefix type, length, and value [TLV], RSVP IPv4 Session Query TLV, and VPN IPv4 prefix TLV)

Internet draft draft-raggarwa-mpls-p2mp-te-02.txt, *Establishing Point to Multipoint MPLS TE LSPs*, (except nonadjacent signaling for branch LSPs, make-before-break and fast reroute, and LSP hierarchy using point-to-point LSPs)

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

Internet draft draft-ietf-mpls-rsvp-lsp-fastreroute-03.txt, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels* (except node protection in facility backup)

Internet draft draft-ietf-tewg-diff-te-mam-03.txt, *Maximum Allocation Bandwidth Constraints Model for Diff-Serv-aware MPLS Traffic Engineering* (except overbooking)

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

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

Internet draft draft-ietf-mpls-soft-preemption-00.txt, *MPLS Traffic Engineering Soft preemption*

Internet draft draft-ietf-ccamp-ospf-gmpls-extensions-09.txt, *OSPF Extensions in Support of Generalized MPLS* (interface switching only)

Internet draft draft-ietf-tewg-diff-te-proto-06.txt, *Protocol extensions for support of Diff-Serv-aware MPLS Traffic Engineering*

Internet draft draft-marques-ppvpn-ibgp-00.txt, *RFC2547bis networks using internal BGP as PE-CE*

Internet draft draft-ietf-ccamp-gmpls-routing-06.txt, *Routing Extensions in Support of Generalized MPLS* (interface switching only)

Internet draft draft-ietf-tewg-diff-te-russian-06.txt, *Russian Dolls Bandwidth Constraints Model for Diff-Serv-aware MPLS Traffic Engineering*

Internet draft draft-martini-l2circuit-trans-mpls-14.txt, *Transport of Layer 2 Frames Over MPLS*

Network Address Translation (NAT)

RFC 3022, *Traditional IP Network Address Translator (Traditional NAT)*

OSPF

RFC 1587, *The OSPF NSS A Option*

RFC 2328, *OSPF Version 2*

RFC 2740, *OSPF for IPv6*

RFC 3623, *OSPF Graceful Restart*

Internet draft draft-ietf-katz-ward-bfd-02.txt, *Bidirectional Forwarding Detection* (except the transmission of echo packets)

Internet draft draft-ietf-isis-igp-p2p-over-lan-03.txt, *Point-to-point operation over LAN in link-state routing protocols* (expires February 2004)

Internet draft draft-katz-yeung-ospf-traffic-01.txt, *Traffic Engineering Extensions to OSPF* (expires April 2000)

Internet draft draft-ietf-ccamp-ospf-gmpls-extensions-12.txt, *OSPF Extensions in Support of Generalized MPLS* (except link local/remote identifiers, link protection type, shared risk link group [SRLG], and implications of graceful restart) (expires April 2004)

Point-to-Point Protocol (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 1877, *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*

RFC 1990, *The PPP Multilink Protocol (MP)*

RFC 2615, *PPP over SONET/SDH*

RIP

RFC 1058, *Routing Information Protocol*

RFC 2082, *RIP-2 MD-5 Authentication*

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*

RFC 2961, *RSVP Refresh Overhead Reduction Extensions*

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

Internet draft draft-ietf-mpls-generalized-rsvp-te-09.txt, *Generalized MPLS Signaling - RSVP-TE Extensions* (fault handling only)

Secure Sockets Layer (SSL)

RFC 1319, *The MD2 Message-Digest Algorithm*

RFC 1321, *The MD5 Message-Digest Algorithm*

RFC 2246, *The TLS Protocol Version 1.0*

RFC 2459, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*

TCP/IP v4

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 Internetworks*

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 1948, *Defending Against Sequence Number Attacks*

RFC 2338, *Virtual Router Redundancy Protocol*

RFC 3246, *An Expedited Forwarding PHB (Per-Hop Behavior)*

Voice Services

RFC 2508, *Compressing IP/UDP/RTP Headers for Low-Speed Serial Links*

VPNs

RFC 2283, *Multiprotocol Extensions for BGP4*

RFC 2547, *BGP/MPLS VPNs*

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

Internet draft draft-ietf-l3vpn-rfc2547bis-03.txt, *BGP/MPLS IP VPNs*

Internet draft draft-kompella-l2ppvpn-version.txt, *MPLS based Layer 2 VPNs*

Internet draft draft-martini-l2circuit-encap-mpls-07.txt, *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*

The JUNOS software has the following exceptions:

A packet with a sequence number of 0 is treated as out of sequence.

Any packet which does not have the next incremental sequence number is considered out of sequence.

When out-of-sequence packets arrive, the expected sequence number for the neighbor is set to the sequence number in the Layer 2 circuit control word.

Internet draft draft-kompella-ppvpn-vpls-01.txt, *Virtual Private LAN Service*

Internet draft draft-ietf-l2vpn-vpls-bgp-02.txt, *Virtual Private LAN Service*

Internet draft draft-martini-l2circuit-trans-mpls-14.txt, *Transport of Layer 2 Frames Over MPLS*

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 Multiple x 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

The following sections describe other standards supported by JUNOS software:

ATM on page 37

Ethernet on page 37

Frame Relay on page 38

Serial on page 38

T3 on page 38

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: 5 1,840 kbits/s operation*

Ethernet

IEEE 802.3ad, *Link Aggregation (Aggregation of Multiple Link Segments and Link Aggregation Control Protocol only)*

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

IEEE 802.1Q, *Virtual LANs*

Frame Relay

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

FRF.12, *Frame Relay Fragmentation Implementation Agreement*

FRF.15, *End-to-End Multilink Frame Relay Implementation Agreement*

FRF.16.1, *Multilink Frame Relay UNI/NNI Implementation Agreement*

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

Internet draft draft-martini-frame-encap-mpls-01.txt (except translation of the command/response bit and sequence numbers and padding), *Frame Relay Encapsulation over Pseudo-Wires* (expires June 2002)

Serial

ITU-T Recommendation V.35, *Data Transmission at 48 kbit/s Using 60-108 kHz Group Band Circuits*



NOTE: The Juniper Networks Serial PIC supports V.35 interfaces with speeds higher than 48 kilobits per second (Kbps).

ITU-T Recommendation X.21, *Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment for Synchronous Operation on Public Data Networks*

TIA/EIA Standard 530, *High-Speed 25-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment*

TIA/EIA Standard 232, *Interface between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange*

T3

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