

# JUNOS 4.1 Internet Software Release Notes

**Release 4.1R4**  
**2 February 2001**  
**Part No. 530-003083-01**  
**Revision 5**

These release notes accompany Release 4.1 of the JUNOS Internet software. They describe the documentation for the router and known problems with the software.

You can also find these release notes on the Juniper Networks technical documentation Web page, which is located at <http://www.juniper.net/techpubs/>.

<b>Contents</b>	Product Documentation .....	1
	Release 4.1 Features .....	2
	Current Software Release .....	4
	Resolved Issues .....	4
	Outstanding Issues .....	6
	Previous Software Releases .....	8
	Release 4.1R3 .....	8
	Release 4.1R2 .....	9
	Errata .....	10
	Upgrade to Release 4.1 .....	11
	Upgrade from Release 3.3 or 3.4 .....	11
	Upgrade from Release 4.0R1 or Later .....	12
	Contact Juniper Networks .....	12
	Revision History .....	13

## Product Documentation

The following documentation describes the JUNOS Internet software, which is the software that runs on Juniper Networks routers:

*JUNOS Internet Software Configuration Guide: Installation and System Management* —Provides an overview of the JUNOS Internet software and describes how to install and upgrade the software. This manual also describes how to configure system management functions, including user accounts, passwords, and SNMP.

*JUNOS Internet Software Configuration Guide: Interfaces and Chassis* —Provides an overview of routing interfaces and describes how to configure routing interfaces, router chassis, firewalls, and CoS.

*JUNOS Internet Software Configuration Guide: MPLS Applications* —Provides an overview of MPLS, LDP, and RSVP concepts and describes how to configure these protocols.

*JUNOS Internet Software Configuration Guide: Routing and Routing Protocols*—Provides an overview of routing concepts and describes how to configure routing, routing policy, and unicast and multicast routing protocols.

*JUNOS Internet Software Command Reference*—Describes the JUNOS Internet software commands you use to monitor and troubleshoot Juniper Networks routers.

The JUNOS Internet software runs on Juniper Networks routers, which are described in the following manuals:

*M5 and M10 Internet Backbone Routers Hardware Installation Guide*

*M20 Internet Backbone Router Hardware Installation Guide*

*M40 Internet Backbone Router Hardware Installation Guide*

*M160 Internet Backbone Router Hardware Installation Guide*

## Release 4.1 Features

The following features have been added to JUNOS Release 4.1:

M5 and M10 Internet Backbone Router support—New entry-level Internet Backbone Routers, the M5 router can support up to four PICs and the M10 router can support up to eight PICs. New show chassis commands have been added to support these routers.

Support for E1 and T1 Physical Interface Cards (PICs) is available. Note that the E1 PIC does not support Channel Associated Signaling (CAS).

Support for the one-port OC-48 SR PIC for the M5, M10, M20, and M40 routers is available. This PIC is a four-slot PIC.

Support for the DS-3, E3, and Fast Ethernet PICs on the M160 router is available.

LDP on top of RSVP-engineered tunnels—Supports two-level label stacks and provides support for a traffic-engineered core with LDP at the edge of the network.

MSDP mesh groups—Allows groups of peers to be configured in a full-mesh topology, such that when a Source Active message is received from a mesh group peer, the Source Active message is not flooded to the other peers in the mesh group. The Source Active message is flooded to peers outside of the mesh group, including members of other mesh groups. If a Source Active message is received from a peer in the same mesh group, the message is always accepted.

Traffic policing—Using firewall filters, classifies a stream of packets into groups and performs an action on each packet based on its state: either accepting, discarding, or marking the packet by setting the PLP bit or the output queue. Various kinds of policing are supported: on a per-interface basis, on a per-class basis within a logical interface, and on a Layer 4 profile (to control protocol traffic). For example, you can rate-limit an interface to less than line rate without having to change the configuration of lower-layer devices, such as DSUs. You can also rate-limit ICMP traffic.

Cflowd aggregation—When sampling traffic, you can now export the data in cflowd format, providing the ability to aggregate sampled traffic flows and send them in cflowd format to a remote host. The JUNOS software supports cflowd Version 5 and Version 8. To interpret the flows, use software from CAIDA (<http://www.caida.org/tools/measurement/cflowd>).

Manual synchronization of redundant Routing Engines—On routers that have two Routing Engines, you can copy files between Routing Engines and load a package from one Routing Engine onto another. To activate this feature, you must install the JUNOS 4.1 software from a PCMCIA card or LS-120 floppy.

Policy arithmetic—Within a routing policy, you can add or subtract values from the metric, preference, tag, color, or local preference values.

AS path range expressions—Within a regular expression, you can specify a range of AS path numbers wherever you can specify a single AS number.

Prefix lists—You can configure a list of prefixes to use in a routing policy (for route filtering) or in a firewall filter (for source address verification).

Disable damping policy—You can disable the default BGP route damping behavior based on policy.

Multipoint ATM VC and Frame Relay DLCI statistics—You can display these statistics with the show interface statistics detail command.

SNMP MIB support:

Host MIB support—The following groups defined in RFC 2790, *Host Resources MIB*, are supported:

hrSystem

hrSWInstalled

E1/T1 MIB support—RFC 1406, *Definitions of Managed Objects for the DS1 and E1 Interface Types* is supported, except for dsx1FarEndConfigTable, dsx1FarEndCurrentTable, dsx1FarEndIntervalTable, dsx1FarEndTotalTable, and dsx1FracTable.

IGMPv2 MIB support—The IGMPv2 MIB, as defined in *Internet Group Management Protocol (IGMP) MIB*, Internet draft draft-ietf-idmr-igmp-mib-13.txt, is supported.

Ethernet interface MIB support—The etherStatsTable of the Remote Network Monitoring MIB, as defined in RFC 1757, *Remote Network Monitoring Management Information Base*, is supported.

Air filter alarm trap—A proprietary alarm MIB is available, which includes a trap for the air filter alarm.

Chassis MIB updates—The proprietary chassis MIB supports the M5 and M10 routers as well as the new PICs.

## Current Software Release

The current software release is Release 4.1R4. For information about obtaining the software packages, see the Juniper Networks Web page, <http://www.juniper.net/techpubs/>.

For upgrade instructions, see the section “Upgrade to Release 4.1” on page 11.

## Resolved Issues

The following issues have been resolved since JUNOS Release 4.1R3. The identifier following the description is the tracking number in our bug database.

### Software Installation

Immediately after a software upgrade, the system configuration database, `/var/db/juniper.data`, might have been missing, thereby preventing the router from activating the committed configuration. A workaround was to create the `/var/db/juniper.data` file, enter configuration mode, and issue the commit command. [PR/10413]

### Platform and Forwarding

When you issued the ping command for an unreachable host and an ICMP unreachable message was not received, when you tried to end the session by typing Ctrl-C, the CLI stopped operating. [PR/8070]

If you used the traceroute command on MPLS LSPs, it might have caused random kernel panic on transit routers only. A workaround was to disable MPLS ICMP replies by typing the following command at a UNIX prompt: `sysctl -w net.tag.icmpreply=0`. However, the only certain way to prevent crashes is by upgrading software. [PR/10761]

On rare occasions, a race condition within the virtual memory process in the JUNOS kernel might have caused the kernel to panic. To identify this condition, you would have seen the following kernel panic message on the console: “vm\_object\_deallocate: object deallocated too many times”. [PR/11665]

### User Interface and Configuration

Issuing a command to deactivate the first route-filter entry within a from clause might have caused all instances of route-filter to be deactivated. [PR/10752]

### Interfaces and Chassis

If the receive side of the protect circuit failed, APS might have malfunctioned. There was no workaround. [PR/10023]

If you deleted a VRRP configuration from a logical interface and changed the IP address to the virtual IP address within a single commit, the router might have failed. A workaround was to delete the IP address (and the associated details) from the logical interface, commit the change, and then reconfigure the IP address with the virtual IP address and commit again. [PR/10655]

The flow sequence number field in cflowd packets might have contained the packet sequence number instead of the flow sequence number. [PR/10670]

For Gigabit Ethernet interfaces only, if you configured VLAN tagging with a unit number higher than 4095, it caused an error. Unit numbers can range from 0 to 16384. [PR/10844]

If you configured packet sampling and the number of packets sampled was large, the sampling process might have consumed large amounts of CPU time and memory. [PR/11036]

	For SONET/SDH interfaces only, a UDP port used for APS support remained open when APS was not in use. [PR/11174]
	If you installed a Gigabit Ethernet LH PIC, which is not supported in Release 4.2 and earlier, the show chassis hardware command output not only included an entry for it, but also displayed it as a Gigabit Ethernet LX PIC. [PR/11610]
	It was possible for the syslog file on an M160 router to fill up with the following message: "chassisd[PID]: CHASSISD_SENSOR_REREAD: HPS 0 temperature sensor reporting 127 overtemp, rereading". [PR/12087]
<b>Simple Network Management Protocol</b>	The MIB-II object ifOutDiscards did not increment when packets were dropped. [PR/9964]
	If you configured tunnel interfaces, such as PIM encapsulation, IP-IP, or GRE interfaces, the SNMP objects ifSpeed or ifHighSpeed should have returned zero. [PR/10399]
<b>General Routing</b>	AS path regular expressions of the form () N N+1 did not commit properly. A workaround was to rewrite the expression to place the () alternation at the end: N N+1 (). [PR/11286]
<b>Routing Protocols</b>	RIP metrics did not appear in the show route command output. Also, BGP did not set its MED correctly. [PR/9617]
	In a network with a large number of LSPs, IS-IS might have generated CSNPs that were too long. [PR/9796]
	On passive MSDP connections, blocking conditions might have occurred. [PR/10330]
	For routers with established OSPF peers, authentication failures might have occurred occasionally. [PR/10654]
	If you configured a route reflector and an export policy to an IBGP neighbor, the routing protocol process (rpd) might have dumped core. [PR/10758]
	If you used wildcards in a configuration group and you configured a routing policy for an IBGP neighbor, the routing protocol process (rpd) might have dumped core. [PR/10759]
	The clear rip command, which clears RIP statistics, should have required clear permissions to issue it. [PR/10815]
	When RIP was configured, the error message "task_receive_packet: RIP rcvfrom/rcvmsg: Bad file descriptor" appeared in the log file periodically if more than one RIP update packet was received at the same moment; however, RIP was working normally. This could have happened if updates from different neighbors synchronized with each other or if a neighbor sent more than one update. [PR/11041]
	In certain network topologies, the OSPF area border router might have failed to install routes or propagate network summary LSAs. [PR/11103]
	If a RIP group name was 16 characters or more, the routing protocol process (rpd) might have suddenly terminated. [PR/11110]
	When IGMP membership changes occurred, PIM dense mode might not have updated multicast forwarding cache entries correctly. [PR/11267]
	IGMP group membership leaves were not reported to PIM correctly. [PR/11275]

Nonconforming SAP packets might have caused the routing protocol process (rpd) to terminate abnormally. [PR/11358]

A route reflector might have failed to reflect a path originating from one of its clients to other route reflector clients. The route reflector might have failed in this way when the reflector learned of an alternate (worse) path from a nonclient. Additionally, the reflector's peering with the originating client might have gone down and come back with the route reflector queueing but not yet transmitting an advertisement of the alternate path to the originator, at the same time that the originator readvertised the better path to the reflector. [PR/11425]

On a large IS-IS network, it was possible for the JUNOS software to transmit LSPs with smaller sequence numbers than the purged one. This could have caused the IS-IS SPF calculation to take a long time. [PR/11651]

**MPLS Applications**

LDP sent 2 extra bytes at the end of status messages and expected other implementations to do so, causing interoperability problems. There was no workaround. [PR/10226]

If you configured the no-decrement-ttl statement for an LSP, a transit router might have decremented the TTL counter anyway. [PR/10824]

If you configured fast reroute in a topology with overlapping detours, detours might not have come up. [PR/10882]

When byte counter increments over an LSP are extremely large ( $2^{61}$  or larger), RSVP might have dumped core as a result of floating-point overflow while collecting traffic statistics. [PR/11734]

Primary and secondary paths of the same LSP should refrain from sharing links, but they might have been criss-crossing the same links. [PR/12098]

**Outstanding Issues**

This section lists outstanding issues with this release of the JUNOS software. The identifier following the description is the tracking number in our bug database.

**Software Installation**

During a software upgrade, the management process might log errors about a database schema mismatch. These errors are cosmetic. The system operates normally after being rebooted. [PR/10618]

**Platform and Forwarding**

If a route entry has accounting enabled and the outbound interface for the route has an outbound filter specified, the route entry counter might not function correctly. There is no workaround. [PR/9005]

If you do not configure NTP, the NTP process (xntpd) should close its UDP listener port. [PR/11175]

When the router's memory is being heavily utilized, it might run out of mbufs, which could cause the router to reset. [PR/12263]

**User Interface and Configuration**

In some circumstances, the CLI displays a > before a completion option that does not contain future options. [PR/9885]

**Interfaces and Chassis**

The APS process (apsd) signals 1+ 1 APS instead of the correct 1:1 APS in the K2 SONET/SDH overhead. This most likely has no operational impact. [PR/8607]

- If you configure the revert timer only on the protect circuit, forced reversion does not work. [PR/8932]
- If you have configured firewall filters and you issue the show firewall filter command, the packet count and byte count fields might show values twice as large as the actual values. [PR/9952]
- If you configure the icmp-type time-exceeded statement at the [edit firewall filter *filter-name* term *term-name* from] hierarchy level, thereby explicitly allowing ICMP time exceeded messages to pass through, the firewall filter might still block the messages anyway. [PR/10090]
- If you configure APS and the protect router reboots, APS might unnecessarily switch to protect state. [PR/10944]
- General Routing**
  - Routing policy term matching for next-hop interfaces considers only the first next-hop interface. This is inconsistent with policy term matching for next-hop addresses, which considers all next-hop addresses. [PR/8640]
- Routing Protocols**
  - You cannot set reference bandwidth, which is used as a scaling factor in computation of OSPF metrics, to values over 4 GB. [PR/7264]
  - On unnumbered point-to-point links and virtual links, OSPF advertises an incorrect destination prefix length. Conforming implementations should ignore this field, but some implementations validate it. [PR/9056]
  - While MSDP is running, the routing protocol process (rpd) might terminate abnormally. [PR/9228]
  - If you apply a routing policy to an internal BGP neighbor level, it causes all other internal BGP sessions to reset, although the specific neighbor is not reset. This occurs only the first time you perform the action; if you apply the policy a second time, it takes effect in the normal way. [PR/10365]
  - While processing an IS-IS IIH PDU, the routing protocol process (rpd) might terminate abnormally. [PR/10664]
  - If you configure PIM dense groups and a sparse mode join is received for a dense group, routing might terminate abnormally when the join message is sent upstream. [PR/10735]
  - Before implementing DVMRP, please contact customer support.
- MPLS Applications**
  - When LDP is trying to reestablish a connection, it always uses an exponential backoff algorithm. It should not use this algorithm when the connection simply fails or is shut down gracefully. [PR/7972]
  - LDP does not respond to loop-prevention TLVs. [PR/9174]
  - LDP installs only routes that have a prefix length of 32. There is no workaround. [PR/10375]
  - LDP advertises all addresses on all interfaces. [PR/10379]
  - If LDP receives a label withdrawal message followed quickly by a label map, LDP might not be able to send an intervening label release message, thereby causing LDP to close the connection. The connection recovers on its own. [PR/10436]

## Previous Software Releases

### **Release 4.1R3**

The following issues have been resolved since JUNOS Release 4.1R2. The identifier following the description is the tracking number in our bug database.

#### **Platform and Forwarding**

When converting interfaces from point-to-point to multipoint and back again, the NTP process (xntpd) displayed the error message "SIOCGIFBRDADDR fails." The workaround was to restart xntpd. [PR/783]

If you configured CCC connections on an M160 router and then took an SFM offline and back online again, the CCC connections belonging to that SFM contained incorrect next hops, preventing the packets belonging to the affected CCC connections from reaching their destination. [PR/10464]

#### **User Interface and Configuration**

NTP broadcast could be configured on only one address and thus on only one interface. There was no workaround. [PR/10382]

#### **Interfaces and Chassis**

When you unconfigured loopback mode on a SONET/SDH interface, the show interface command showed that the link flags still showed "loop detected". To clear the link flags, you had to take the PIC offline and bring it online again. [PR/9032]

If an FPC containing the active circuit for APS failed or was removed, APS did not switch to the other circuit. There was no workaround for this problem. [PR/10099]

Removing the master and only SSB in an M20 router without pressing the offline button might have caused the subsequently inserted SSB to become active even though the other SSB was the master and this SSB was the backup. [PR/10253]

When firewall filter logging was enabled, or when firewall counters were added to a filter configuration and the logs were polled or the counters were polled, packet buffer leaks occurred. [PR/10394]

APS did not support the exercise request. If an exercise request was received, the circuit might have been protection switched. There was no workaround. [PR/10439]

Pressing the FPC online button multiple times could have caused multiple connection timeout requests to be queued and then subsequently overwritten. When the timers timed out, the FPC mistakenly was placed into diagnostic mode. [PR/10501]

#### **General Routing**

The command show route *prefix* all did not show a hidden route if it was the longest match for the prefix. [PR/10549]

#### **Routing Protocols**

When the system received a BGP update containing new next-hop information for a prefix, and the next hop used for forwarding purposes remained unchanged, the system might have failed to update the next hop that was being advertised by BGP. [PR/8815]

Intra-area routes learned over virtual links in the backbone area might not have been updated to the inet.0 routing table and hence in the forwarding table. The workaround was to clear the OSPF database using the clear ospf database command. [PR/10306]

#### **MPLS Applications**

If you configured a strict hop along an LSP, the CSPF load-balancing algorithm (least fill, most fill, and random) did not function properly. [PR/10170]

LDP might have closed sessions randomly depending on the protocol traffic load at that point in time. There was no workaround. [PR/10214]

If you configured the no-cspf statement and multiple, equal-cost paths toward the egress router existed, an LSP might have blackholed traffic. [PR/10236]

## Release 4.1R2

The following issues have been resolved since JUNOS Release 4.1R1. The identifier following the description is the tracking number in our bug database.

### Platform and Forwarding

In rare cases, a write to the rotating media or flash failed and the system might have retried the write forever, causing the writing process to stop, instead of detecting the write error. [PR/9361]

On an M160 router, in rare cases, the SFM might have failed to come online and the Routing Engine might not have received the resynchronize message from the SFM, causing the Routing Engine to never mark the SFM as online. [PR/9822]

### Interfaces and Chassis

If an OC-192 PIC had been up continuously for 49 days, ADC timeout messages were displayed. These messages, and this condition, did not affect proper operation of the board. [PR/10046]

When the chassis was not over the temperature limit, the system intermittently generated an alarm about the temperature of the chassis being over the shutdown limit and cleared the alarm 5 seconds later. [PR/8949]

When APS was configured on SDH interfaces, if the working router detected signal failure, the protect router did not respond appropriately. There was no workaround. [PR/9413]

The show interface at-x/x/x switch-id command displayed extraneous characters. [PR/9425]

If the sum of the configured priority costs for the VRRP-tracked interfaces exceeded the VRRP group's priority, the VRRP process might have dumped core. This misconfiguration is now detected when you commit configuration changes. [PR/9806]

The show chassis routing-engine command incorrectly displayed the value of the temperature probe on the Routing Engine. [PR/9837]

### General Routing

When interfaces disappeared and reappeared while the routing protocols process (rpd) was experiencing heavy load, rpd never noticed that the interfaces disappeared and reappeared. This might have led to incorrect next hops. [PR/9255]

In an AS-path regular expression, the plus (+) operator might not have worked correctly if it appeared in the middle of the expression. [PR/9534]

When an ATM interface was configured the same way as another interface in the router that was disabled, the ATM interface might have appeared to be up but did not transmit locally generated packets. [PR/9659]

If you issued the show route community *community-id* command simultaneously in two different sessions, the routing subsystem might have restarted. The workaround was to not issue this command in two sessions at the same time. [PR/9745]

**Routing Protocols**

The show route <prefix> hidden command did not show the hidden route that was the longest match for the prefix. [PR/9871]

If you issued the following sequence of commands in rapid succession, the routing process might have restarted:

```
user@host> set protocols isis interface interface-name level level-number disable
user@host> commit
user@host> delete protocols isis interface interface-name level level-number disable
user@host> commit
```

The workaround was to allow for a 10-second delay between commits. [PR/6684]

IS-IS did not truncate the metric for interface routes to 63 when advertising them even if the value was set to a higher value and even if the wide-metrics-only statement was configured. [PR/9506]

When a PIM null register was received at the RP and MSDP peers were configured, the router incorrectly sent a source active message with the pseudo-IP header as data. [PR/9672]

Triggered PIM joins were not sent out in a timely manner. [PR/9764]

On rare occasions, OSPF might have crashed if an interface went down while performing its SPF computation, especially if the only change in the LSA database was to summary or external LSAs. [PR/9845]

The show isis database detail command displayed an incorrect value for the remaining LSP lifetime. A workaround was to use the non-detail version of the command to discern the lifetime. [PR/9890]

**MPLS Applications**

CSPF might have computed a valid path that appeared to contain loops, causing RSVP not to establish the path. [PR/6335]

When two IS-IS routers shared the same router ID (which is a configuration error), the TED database might have asserted and the routing protocol process (rpd) might have dumped core. [PR/9737]

LDP did not work correctly if the neighbor negotiated a maximum PDU size of less than 2085 bytes. [PR/9954]

LDP placed parts of messages in the wrong order. Some other vendors' implementations might have been confused by this. There was no workaround. [PR/9985]

**Errata**

This section lists outstanding issues with the documentation:

The mtrace command is not supported in Release 4.1.

## Upgrade to Release 4.1



### Note

Before upgrading, you might want to back up the currently running and active file system so that you can recover to a known, stable environment in case something goes wrong with the upgrade:

```
user@host> request system snapshot
```

## Upgrade from Release 3.3 or 3.4

To upgrade to Release 4.1, you remove the Release 3.3 or 3.4 bundle and install the Release 4.0 base software packages.

To upgrade to Release 4.1, follow these steps:

1. Delete the software packages that are currently installed:

```
user@host> request system software delete jroute-3
user@host> request system software delete jpf-3
user@host> request system software delete jkernel-3
```

If you are deleting a Release 3.3 package, specify `jpfe_m40-3` in place of `jpfe-3`.

2. Add the JUNOS Release 4.0 base software.



### Note

When upgrading from any version of JUNOS Release 3 to Release 4.1, you must install the JUNOS 4.0 base software.

For customers in the United States and Canada, use the following command:

```
user@host> request system software add path/jbase-4.0R1-domestic.tgz
```

*path* is the full path name to the base software. To download the software from the Juniper Networks FTP site, specify *path* as `ftp://ftp.juniper.net/private/junos/4.1R4`.

For all other customers, use the following command:

```
user@host> request system software add path/jbase-4.0R1-export.tgz
```

*path* is the full path name to the base software. To download the software from the Juniper Networks FTP site, specify *path* as `ftp://ftp.juniper.net/private/junos/4.1R4`.

3. Add the new package:

```
user@host> request system software add path/jbundle-4.1R4.tgz
```

*path* is the full path name to the file. To download the software from the Juniper Networks FTP site, specify *path* as  
ftp://ftp.juniper.net/private/junos/4.1R4/packages/All.

4. Reboot the router to start the new software:

```
user@host> request system reboot
```

## **Upgrade from Release 4.0R1 or Later**

To upgrade to Release 4.1 from Release 4.0R1 or later, install the JUNOS 4.1 software packages on top of the Release 4.0 operating system base (jbase). You do not need to upgrade the base software or delete the previous packages. To upgrade to Release 4.1, follow these steps:

1. Add the new package:

```
user@host> request system software add path/jbundle-4.1R4.tgz
```

*path* is the full path name to the file. To download the software from the Juniper Networks FTP site, specify *path* as  
ftp://ftp.juniper.net/private/junos/4.1R4/packages/All.

2. Reboot the router to start the new software:

```
user@host> request system reboot
```

## Contact Juniper Networks

For technical support, contact Juniper Networks at support@juniper.net.

If you are reporting a software problem, please issue the following command from the CLI before contacting support:

```
user @host> request support information | save filename
```

For documentation issues, contact Juniper Networks at tech-doc@juniper.net.

To provide a core file to Juniper Networks for analysis, gzip the file, rename the file to include your company name, copy it to ftp.juniper.net:pub/incoming, and then send the filename, along with software version information (the output of the show version command) and the configuration, to support@juniper.net.

## Revision History

- 2 February 2001—Release 4.1R4.
- 16 October 2000—Release 4.1R3.
- 1 September 2000—Release 4.1R2.
- 11 August 2000—Added restriction to the manual synchronization of redundant Routing Engines feature; added support for the DS-3, E3, and Fast Ethernet PICs on the M160 router.
- 2 August 2000—Initial release notes, Release 4.1R1.

Juniper Networks is a registered trademark of Juniper Networks, Inc. Internet Processor, Internet Processor II, JUNOS, JUNOScript, M5, M10, M20, M40, and M160 are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks may be the property of their respective owners. All specifications are subject to change without notice.

Copyright © 2000-2001, Juniper Networks, Inc.  
All rights reserved. Printed in USA.

