

Release Notes for EX-series Switches and JUNOS Software for EX-series Switches, Release 9.1

Release 9.1R4
13 February 2009

Contents

Features in JUNOS Software for EX-series Switches, Release 9.1	2
Bridging, VLANs, and Spanning Trees	2
Layer 3 Protocols	3
Management and RMON	3
Outstanding and Resolved Issues in JUNOS 9.1 for EX-series Switches	3
Resolved Issues	3
Access Control and Port Security	4
Class of Service	4
Firewall Filters	4
Infrastructure	5
Interfaces	5
Layer 3 Protocols	5
Outstanding Issues	5
Access Control and Port Security	6
Bridging, VLANs, and Spanning Trees	6
Class of Service	6
Firewall Filters	7
Infrastructure	7
Interfaces	8
Layer 3 Protocols	8
Virtual Chassis	9
List of EX-series Guides for JUNOS 9.1	9
Getting Support	10
Revision History	10

Features in JUNOS Software for EX-series Switches, Release 9.1

Date: 13 February 2009

This page describes the features in Release 9.1 of JUNOS software for EX-series switches.

Bridging, VLANs, and Spanning Trees

- **BPDU protection**—A loop-free network in a spanning-tree topology is supported through the exchange of a special type of frame called bridge protocol data unit (BPDU). Receipt of BPDUs on certain interfaces in an STP, RSTP, or MSTP topology, however, can lead to network outages. Enable BPDU protection on those interfaces to prevent these outages.

Enable BPDU protection on STP interfaces and non-STP interfaces to prevent spoofed BPDU packets from entering a domain. When a BPDU-protected interface receives BPDUs, it transitions to a BPDU inconsistent state, disabling an interface and preventing it from forwarding traffic. The interface can be returned to service again automatically by configuring a timer or manually using the operational mode command `clear ethernet-switching bpd-error`. For more information, see Understanding BPDU Protection for STP, RSTP, and MSTP on EX-series Switches.

- **Root protection**—Root protection lets network administrators manually enforce the root bridge placement in the network. Enable root protection on interfaces that should not receive superior BPDUs from the root bridge and should not be elected as the root port. If the bridge receives superior STP BPDUs on an interface that has root protection enabled, that interface transitions to a root-prevented STP state (inconsistency state) and the interface is blocked. This blocking prevents a bridge that should not be the root bridge from being elected the root bridge.

After the bridge stops receiving superior STP BPDUs on the interface with root protection, it automatically transitions back to a forwarding state.

When root protection is enabled on an interface, it is enabled for all the STP instances on that interface. The interface is blocked only for instances for which it receives superior BPDUs. Otherwise, it participates in the spanning-tree topology.

An interface can be configured for either root protection or loop protection, but not for both. For more information, see Understanding Root Protection for STP, RSTP, VSTP, and MSTP on EX-series Switches.

- **Loop protection**—STP loop protection provides additional protection against Layer 2 forwarding loops in STP domains. When loop protection is enabled, the spanning-tree topology detects root ports and blocked ports and makes sure both keep receiving BPDUs. If a loop-protection-enabled interface stops receiving BPDUs from its designated port, it reacts as it would react to a problem with the physical connection on this interface. It does not transition the interface to a forwarding state, but instead transitions it to a loop-inconsistent state. The interface recovers and then it transitions back to the spanning-tree blocking state as soon as it receives a BPDU. An interface can be configured for either root protection or loop protection, but not for both. For more information, see

Understanding Loop Protection for STP, RSTP, VSTP, and MSTP on EX-series Switches.

- **Storm control**—Storm control prevents a rogue switch from generating traffic storms that might bring down a LAN. Enable storm control to permit the switch to monitor traffic levels and drop packets when a specified traffic level is exceeded, thus preventing packets from proliferating and degrading the LAN. For more information, see Understanding Storm Control on EX-series Switches.

Layer 3 Protocols

- **IGMP snooping**—Internet Group Management Protocol (IGMP) snooping regulates multicast traffic in a switched network. With IGMP snooping enabled, a LAN switch monitors the IGMP transmissions between a host and multicast router, keeping track of the multicast groups and associated member ports. The switch uses that information to make intelligent multicast-forwarding decisions and forward traffic to the intended destination interfaces. EX-series switches support IGMP versions 1 and 2. Note that EX-series switches do not support IGMPv3. For more information, see IGMP Snooping on EX-series Switches Overview.

Management and RMON

- **Licenses**—Using the License option, you can add, delete, and display license keys for the BGP, GRE, and IS-IS features. For more information, see Managing Licenses for the EX-series Switch (J-Web Procedure).

Related Topics ■ Outstanding and Resolved Issues in JUNOS 9.1 for EX-series Switches on page 3

Outstanding and Resolved Issues in JUNOS 9.1 for EX-series Switches

Date:13 February 2009

This page lists the outstanding issues in the JUNOS Release 9.1R3 software for EX-series switches. It also lists the issues that have been resolved since JUNOS Release 9.0R3.

- Resolved Issues on page 3
- Outstanding Issues on page 5

Resolved Issues

The following issues have been resolved since JUNOS Release 9.0R3 for EX-series switches. The identifier following the description is the tracking number in our bug database.

Access Control and Port Security

- When you configure the MAC limiting **drop** action and then change which VLAN the interface is in, packets are not dropped. As a workaround, clear the Ethernet switching table after enabling MAC limiting. [PR/256877: This issue has been resolved.]
- In multiple supplicant mode, if multiple users with dynamic VLAN movement have authenticated successfully, the **show vlans detail** command displays the interface entry as many times as the number of authentication sessions. [PR/267981: This issue has been resolved.]
- After DHCP has granted a lease to a trusted interface (a trunk port), the DHCP snooping database may show interface as **unknown**. [PR/278119: This issue has been resolved.]
- Occasionally, if you toggle the mode of an interface from **access** to **trunk** and then back to **access**, the switch might not insert the static DHCP binding entries into the DHCP snooping table. [PR/283444: This issue has been resolved.]

Class of Service

- The **show interfaces queue** command for any interface always shows that no forwarding classes and no queues are in use. [PR/270670: This issue has been resolved.]
- On an EX-series switch with aggregated interfaces, when you apply classifiers on interfaces using wildcards (for example, **ge-***) that include the aggregated interface members, occasionally a cosd core is generated in **/var/tmp**. As a workaround, delete the class-of-service configuration, perform a commit, and add the class-of-service configuration again. [PR/276973: This issue has been resolved.]
- If you apply fewer than four scheduler maps to an interface using wildcards (such as **ge-***), you may get a commit error indicating that you are trying to apply more than four different scheduler maps. The workaround is to remove the wildcard and apply the scheduler map to the individual interfaces. [PR/277186: This issue has been resolved.]

Firewall Filters

- If you configure the match conditions **source-port** or **destination-port**, you cannot specify a port value of 61. [PR/268033: This issue has been resolved.]
- TCAM rules installed for DHCP snooping and DAI are not removed when DHCP snooping, DAI, and the corresponding VLANs are deleted at the same time. [PR/270617: This issue has been resolved.]
- When you use the **delete vlan default** command to delete a VLAN, the filter associated with the default VLAN is not removed. To remove the filter on the default VLAN, use the **delete vlan default filter** command instead. [PR/273680: This issue has been resolved.]
- When you restart the firewall process, 802.1X filters installed on the EX-series switch are removed. This happens only when the attribute "filter-id" is used on

the RADIUS server to install the filter for the 802.1X client. [PR/277203: This issue has been resolved.]

- When you delete a filter on a VLAN, DHCP snooping and ARP inspection stop working on that VLAN. [PR/278705: This issue has been resolved.]
- In a firewall filter, the match condition “vlan” might not work on EX-series switches. As a workaround, use the match condition “dot1q-tag.” [PR/282435: This issue has been resolved.]

Infrastructure

- When the analyzer output interface is not part of any VLAN, or when the analyzer output interface is part of a VLAN that contains interfaces other than the analyzer output interface, the analyzer output interface receives switched packets. As a workaround, configure the analyzer output interface to be the only interface in its VLAN. [PR/259820: This issue has been resolved.]
- When an EX-series switch is rebooting, you may see a large number of messages on a syslog server. [PR/276248: This issue has been resolved.]
- If you enable PIM and then perform an SNMP walk on pimNeighborTable, the SNMP walks enters an infinite loop and cannot complete. [PR/277049: This issue has been resolved.]
- When you open the J-Web interface, the font style and sizes may not be the defaults. [PR/279113: This issue has been resolved.]
- When using the J-Web interface, if you select ports that have been configured with different roles and then click on Edit > Port Roles, the Port Configuration screen displays an error. [PR/286297: This issue has been resolved.]
- In an EX-series switch with a 10-Gbps uplink module installed, if you restart the switch and then issue the `show interface xe-fpc/port/0` command, the output shows the uplink module speed as 1000-Mbps. As a workaround, use the `request chassis pic` command to take the PIC offline and then bring it back online. [PR/289106: This issue has been resolved.]

Interfaces

- Currently, EX-series switches allow transit traffic between the out-of-band management interface (me0) and network ports. [PR/279700: This issue has been resolved.]

Layer 3 Protocols

- If you issue the `delete static igmp-snoop mrouter vlan all` command, the static router port might not be deleted. [PR/287455: This issue has been resolved.]

Outstanding Issues

The following issues are outstanding in the JUNOS Release 9.1R3 software for EX-series switches. The identifier following the description is the tracking number in our bug database.

Access Control and Port Security

- If the VLAN associated with a client is not configured on the switch, users are authenticated and the port is placed in the default VLAN. [PR/263719]
- After you deactivate an interface on the switch, LLDP does not send a TLV with a TTL value of zero. Because of this, neighbor switches may not immediately flush the switch details from the LLDP database. The neighbor details are flushed after the TTL value expires. [PR/264368]
- On EX-series switches, if you include the `interface all` statement when configuring the 802.1X protocol in the `[edit protocols dot1x]` configuration hierarchy, dynamic VLAN assignment for 802.1X-authenticated clients is not enabled. As a workaround, enable 802.1X on the individual ports on which you want to use dynamic VLAN assignment. [PR/274265]
- DHCP snooping is not supported for the local DHCP server. [PR/280291]
- In a Virtual Chassis configuration, if the Virtual Chassis undergoes a graceful Routing Engine switchover (GRES), 802.1X authentication might not function properly. [PR/288098]

Bridging, VLANs, and Spanning Trees

- In LLDP-MED TLVs, CoS and DSCP values are always sent as zero. [PR/257327]
- When you configure VRRP on EX-series switches without specifying `accept-data` in the configuration and a VRRP failover occurs, traffic might be lost for about 5 minutes. As a workaround, issue the `clear ethernet-switching table` command on the new VRRP master. [PR/271012]
- After you issue a `clear ospf statistics` command, the OSPF statistics are not updated at regular intervals. [PR/271881]
- When frames are switched from access to trunk interfaces (that is, when incoming frames are not tagged), the priority bits in the 802.1Q header are set to 1 by default. [PR/273079]
- Currently, EX-series switches do not support IGMP snooping on routed VLAN interfaces (RVIs). You should enable IGMP snooping on VLANs that do not include RVIs. [PR/282890]
- In some cases, if you delete and reassign the VoIP configuration for an interface, the Ethernet switching table might not contain static MAC entries for the voice VLAN. [PR/284250]

Class of Service

- In the output of the `show interfaces queue` command, the packets and bytes values displayed for a queue are the count of transmitted in that queue. [PR 259525]
- The `show interfaces queue` command always shows the pps and bps counters as 0 (zero). [PR/263374]

Firewall Filters

- Occasionally, the switch might not be able to retrieve counter statistics for firewall term filters. [PR/284637]

Infrastructure

- The speed/duplex LED on the management Ethernet interface sometimes blinks even when no cable is connected. [PR/257290]
- After you restore the factory default configuration, the previous hostname is still present in the configuration. [PR/263647]
- The J-Web interface does not open in the browser window if a pop-up blocker has been enabled in the installed toolbar (for example, Winamp) or if the toolbar installed in the browser (for example, Megaupload and Firebug) installed in the same browser) does not allow AJAX communication. As a workaround, uninstall these toolbars or disable pop-up blockers and try to start the J-Web interface again. [PR/264741]
- If you remove or delete syslog or traceoptions files and then need to use them again, you must delete and then reconfigure the syslog and traceoptions configuration for the logging to work. [PR/267706]
- Logical interface traffic counters show an extra eight bytes in the output byte statistics. [PR/268667]
- When an SNMP walk or polling is done on the `jnxBoxAnatomy` (`jnx-chassis.mib`), CPU usage remains at 95 to 100 percent until the SNMP walk completes. [PR/270552]
- If you modify the configuration to change the system hostname, the name might not change when you commit the configuration. As a workaround, exit from the terminal session to the switch after you have activated the configuration, then log in again. [PR/272903]
- When you perform an SNMP walk on the switch, the message “unable to create internal request” might be displayed. [PR/274019]
- You cannot use the `rollback rescue` command to revert to a rescue configuration. As a workaround, save a known good configuration to a location from which you can reload it to your switch if needed. [PR/275480]
- When you configure SNMPv3 with SHA authentication, all queries fail. As a workaround, use MD5 authentication. [PR/277599]
- When using the J-Web browser interface, if you close the browser by clicking the browser's X button or by pressing `Alt-F4`, the J-Web session might not terminate properly. To properly terminate J-Web sessions, click `Logout` in the J-Web browser window. [PR/278131]
- If you press any key on the keyboard while the switch is rebooting, the switch enters `uboot` mode instead of rebooting and you see the `uboot` prompt (`=>`). If this occurs, issue the `boot` command at the `=>` prompt to continue the reboot. [PR/280086]
- After receiving an SNMP request, the Ethernet switching process (`eswd`) might stall at `dot1qVlanStaticEntry_next()`. [PR/284153]

- In some cases, you might not be able to disable interfaces that belong to a particular Multiple Spanning Tree Instance (MSTI). [PR/284912]
- In the J-Web interface, the list of interfaces in the following 802.1X configuration screen might be empty: **Configure > 802.1X > Exclusion List > Add/Edit > Exclude if connected through port**. [PR/284966]
- If you reboot an EX-series switch after you have configured the Power over Ethernet (PoE) guard band value, two ports that had been shut down because of their low priority become active again. [PR/285262]
- Occasionally in a Virtual Chassis configuration, after a member switch becomes the master switch, you might see a license error message. If you see this error message, remove the license from the original master switch using the **request system license delete JUNOserial#** command. [PR/285799]
- When using the J-Web interface, if you configure port roles or VLAN options for all the ports and then try to commit the changes, the commit process might fail. [PR/286294]
- After you upgrade or downgrade the software on an EX-series switch (by using either the CLI or the J-Web interface), the Juniper EX-Series Web Device Manager might not function properly until you clear the cache in your Web browser. [PR/286614]
- In an aggregated Ethernet configuration that consists only of 100FX members, if you configure the link speed to be 100-Mbps, the LAG interface might go down. [PR/289497]
- In a multimember Virtual Chassis configuration, after the master has been powered off and the mac-persistence timer has aged out, the Virtual Chassis replies to ARP messages with the MAC address of the new master, but PFE is still programmed with the MAC address of the previous master. [PR/293413]

Interfaces

- Chassis alarms do not work on the management Ethernet interface. [PR/254483]
- When you configure unsupported or invalid interface parameters for speed, full- and half-duplex, and autonegotiation on 10-Gigabit Ethernet or 1-Gigabit Ethernet interfaces, the CLI does not display an error message. [PR/264630]
- The output packet counter on aggregated Ethernet interfaces does not increment correctly. [PR/271057]
- When you enable spanning tree on an autonegotiation port, the default port cost is 20000 and the link type is point to point. [PR/276191]

Layer 3 Protocols

- In some cases, if you issue the **show igmp-snooping membership detail** command after a membership timeout on a port, the command output shows **-1** in the **Receiver count** field. [PR/267781]
- Occasionally, the switch might not remove IGMP snooping entries after you change the IGMP snooping configuration. [PR/268832]

- After the switch receives 8,000 multicast group join messages, the switch might stop processing IGMP membership reports for some groups. [PR/284508]
- IGMP snooping is disabled by default in JUNOS Release 9.1 for EX-series switches. [PR/284543]
- If you issue the `set group snpd protocol igmp-snoop vlan v1 interface <ge-*>` command, you might get an error message saying that `<ge-*>` is an invalid interface type. [PR/285654]
- Occasionally, the multicast snooping process `mcsnoopd` might not be able to process IGMP reports and might trigger an `Invalid interface` error message. [PR/286194]
- After you issue the `clear igmp-snooping static` command, the `invalid` counter and the `timeout` counter might not be cleared. [PR/286495]
- If you issue the `delete igmp-snooping vlan disable` command to enable IGMP snooping, the command might not succeed. Likewise, issuing the `set igmp-snooping vlan disable` and `rollback` commands might not succeed in enabling IGMP snooping. As a workaround, issue the following commands: `deactivate protocol igmp-snooping vlan <vlan-name>`, `commit`, and `activate`. [PR/287584]

Virtual Chassis

- In an EX 4200 Virtual Chassis, the `set mastership priority` command might not work after you renumber the member identifier. [PR/257066]
- When the dates on the members of an EX 4200 Virtual Chassis are not synchronized, a member chassis or backup PFEM might not be able to connect to the master. [PR/278784]
- In some instances, if you change a Virtual Chassis member ID and then issue the `show virtual-chassis member-config member` command, the switch still displays the old member ID. [PR/279387]
- After a Virtual Chassis undergoes a mastership switchover, port mirroring might not function correctly. [PR/287545]

- Related Topics** ■ Features in JUNOS Software for EX-series Switches, Release 9.1 on page 2

List of EX-series Guides for JUNOS 9.1

Title	Description
<i>Complete Hardware Guide for EX 3200 and EX 4200 Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance
<i>Complete Software Guide for JUNOS Software for EX-series Switches, Release 9.1</i>	Software feature descriptions, configuration examples and tasks, and reference pages for configuration statements and operational commands
<i>J-Web User Interface Guide for JUNOS Software for EX-series Switches</i>	How to use the J-Web graphical user interface (GUI) with JUNOS for EX-series software

Title	Description
<i>JUNOS Software for EX-series Switches Release Notes, Release 9.1</i>	Summary of hardware and software features and known problems with the software and hardware

Getting Support

For technical support, open a support case with the Case Manager link at <http://www.juniper.net/support/> or call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

Revision History

- 28 April 2008— Revision 1, JUNOS Software for EX-series Switches, Release 9.1R1
- 2 July 2008— Revision 2, JUNOS Software for EX-series Switches, Release 9.1R2
- 28 October 2008— Revision 3, JUNOS Software for EX-series Switches, Release 9.1R3
- 13 February 2009— Revision 4, JUNOS Software for EX-series Switches, Release 9.1R4

Copyright © 2009, Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.