Junos® 10.3 OS Release Notes for Dell PowerConnect J-SRX Series Services Gateways and J-EX Series Ethernet Switches

Release 10.3R2
22 November 2010

These release notes accompany Release 10.3 of the Juniper Networks Junos operating system (Junos OS) for Dell PowerConnect J-SRX Series Services Gateways and J-EX Series Ethernet Switches. They describe device documentation and known problems with the software.

You can also find these release notes at http://www.support.dell.com/manuals.

Contents

Junos OS Release Notes for Dell PowerConnect J-SRX Series Services Gateways

Powered by Junos OS, Dell PowerConnect J-SRX Series Services Gateways provide robust networking and security services. J-SRX Series Services Gateways range from lower-end devices designed to secure small distributed enterprise locations to high-end devices designed to secure enterprise infrastructure, data centers, and server farms. The J-SRX Series Services Gateways include the J-SRX100, J-SRX210, and J-SRX240 devices.

New Features in Junos OS Release 10.3 for J-SRX Series Services Gateways

The following features have been added to Junos OS Release 10.3. Following the description is the title of the manual or manuals to consult for further information.

Software Features

Security

- **Policy usability**—This feature is supported on all J-SRX Series devices.

  In a Junos OS stateful firewall, security policies enforce rules for transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on the traffic as it passes through the firewall. Periodically, traffic does not pass for a number of reasons. For example, traffic does not match a correct policy configuration or the source of the traffic is incorrect. The source of the problem can sometimes be difficult to identify. The **show security match-policies** command allows you to troubleshoot traffic problems in the five tuples: source port, destination port, source IP address, destination IP address, and protocol. The command works offline to identify where the exact problem in the transit traffic exists. It uses the actual search engine to identify the problem and thus enables you to use the appropriate match policy for the traffic.

Advertising Bandwidth for Neighbors on a Broadcast Link Support

This feature is supported on all J-SRX Series devices.

You can now advertise bandwidth for neighbors on a broadcast link. The network link is a point-to-multipoint (P2MP) link in the OSPFv3 link state database. This feature uses existing OSPF neighbor discovery to provide automatic discovery without configuration. It allows each node to advertise a different metric to every other node in the network to accurately represent the cost of communication. To support this feature, a new interface-type under the OSPFv3 interface configuration has been added to configure the interface as p2mp-over-lan. OSPFv3 then uses LAN procedures for neighbor discovery and flooding, but represents the interface as P2MP in the link state database.

The interface type and router LSA are available under the following hierarchies:

- [**protocols ospf3 area area-id interface interface-name**]
- [**routing-instances routing-instances-name protocols ospf3 area area-id interface interface-name**]

[*LN1000 Mobile Secure Router User Guide*]

Group VPN Interoperability with Cisco's GET VPN

Cisco's implementation of GDOI is called Group Encryption Transport (GET) VPN. While group VPN in Junos OS and Cisco's GET VPN are both based on RFC 3547, *The Group Domain of Interpretation*, there are some implementation differences that you need to be aware of when deploying GDOI in a networking environment that includes both Dell security devices and Cisco routers. This topic discusses important items to note when using Cisco routers with GET VPN and Dell security devices with group VPN.

Group servers and group members on Dell security devices cannot interoperate with Cisco GET VPN members. Group members on Dell security devices can interoperate with Cisco GET VPN servers, with the following caveats:

The group VPN in Release 10.3 of Junos OS has been tested with Cisco GET VPN servers running Version 12.4(22)T and Version 12.4(24)T.

To avoid traffic disruption, do not enable rekey on a Cisco server when the VPN group includes a Dell security device. The Cisco GET VPN server implements a proprietary ACK for unicast rekey messages. If a group member does not respond to the unicast rekey messages, the group member is removed from the group and is not able to receive rekeys. An out-of-date key causes the remote peer to treat IPsec packets as bad SPIs. The Dell security device can recover from this situation by reregistering with the server to download the new key.

Antireplay must be disabled on the Cisco server when a VPN group of more than two members includes a Dell security device. The Cisco server supports time-based antireplay by default. A Dell security device will not be able to interoperate with a Cisco group member if time-based antireplay is used since the timestamp in the IPsec packet is proprietary. Dell security devices are not able to synchronize time with the Cisco GET VPN server and Cisco GET VPN members as the sync payload is also proprietary. Counter-based antireplay can be enabled if there are only two group members.

According to Cisco documentation, the Cisco GET VPN server triggers rekeys 90 seconds before a key expires and the Cisco GET VPN member triggers rekeys 60 seconds before a key expires. When interacting with a Cisco GET VPN server, a Dell security device member would match Cisco behavior.

A Cisco GET VPN member accepts all keys downloaded from the GET VPN server. Policies associated with the keys are dynamically installed. A policy does not have to be configured on a Cisco GET VPN member locally, but a deny policy can optionally be configured to prevent certain traffic from passing through the security policies set by the server. For example, the server can set a policy to have traffic between subnet A and subnet B be encrypted by key 1. The member can set a deny policy to allow OSPF traffic between subnet A and subnet B not be encrypted by key 1. However, the member cannot set a permit policy to allow more traffic to be protected by the key. The centralized security policy configuration does not apply to the Dell security device.

On a Dell security device, the **ipsec-group-vpn** configuration statement in the permit tunnel rule in a scope policy references the group VPN. This allows multiple policies referencing a VPN to share an SA. This configuration is required to interoperate with Cisco GET VPN servers.

Logical key hierarchy (LKH), a method for adding and removing group members, is not supported with group VPN on Dell security devices.

GET VPN members can be configured for cooperative key servers (COOP KSs), an ordered list of servers with which the member can register or reregister. Multiple group servers cannot be configured on group VPN members.

Changes in Default Behavior and Syntax in Junos OS Release 10.3 for J-SRX Series Services Gateways

The following current system behavior, configuration statement usage, and operational mode command usage might not yet be documented in the Junos OS documentation:

Application Layer Gateways (ALGs)

- The **show security alg msrpc object-id-map** CLI command has a chassis cluster node option to permit the output to be restricted to a particular node or to query the entire cluster. The **show security alg msrpc object-id-map node** CLI command options are **<node-id | all | local | primary>**.

AppSecure

- When you create custom application or nested application signatures for Junos OS application identification, the order value must be unique among all predefined and custom application signatures. The order value determines the application matching priority of the application signature.

  

  NOTE: The order value range for predefined signatures is 1 through 32,767. We recommend that you use an order range higher than 32,767 for custom signatures.

  The order value is set with the **set services application-identification application application-name signature order** command. You can also view all signature order values by entering the **show services application-identification | display set | match order** command. You will need to change the order number of the custom signature if it conflicts with another application signature.

- The output of the **show services application-identification application-system-cache** command has been changed. The new output includes the cache statuses and the timeout value for maintaining mapping details for each application as shown in the following sample:

```
user@host> show services application-identification application-system-cache

Application System Cache Configurations:
  application-cache: on
  nested-application-cache: on
  cache-entry-timeout: 3600 seconds
  pic: 2/0
Vsys-ID     IP address        Port     Protocol     Application
  0           5.0.0.1           80       TCP          HTTP

  0           7.0.0.1           80       TCP          HTTP:FACEBOOK
```

Chassis Cluster

- **Removing Control VLAN 4094 in Chassis Cluster**— For J-SRX Series branch devices (J-SRX100, J-SRX210, and J-SRX240), the existing virtual LAN (VLAN) tag used for control-link traffic will be replaced with the use of experimental Ether type *0x88b5*. However, backward compatibility is also supported for devices that have already deployed chassis cluster with VLAN tagging in place.

  - To toggle between VLAN and Ether type modes, use the following command:

    set chassis cluster control-link-vlan enable/disable

    

    NOTE: You must perform a reboot to initialize this configuration change.

  - To show whether control port tagging is enabled or disabled, use the following command:

    set chassis cluster information

  - To view the chassis cluster information, use the following command:

    show chassis cluster information

user@host > show chassis cluster information

The following is a sample output of the command:

```
node0
--------------------------------------------------------
Control link statistics:
    Control link 0:

Fabric link statistics:
    Probes sent: 1248

    Sequence number of last probe received: 0
Chassis cluster LED information:
    Current LED color: Green
Control port tagging:  Disabled

Cold Synchronization:
```

- In a chassis cluster configuration on a J-SRX100, J-SRX210, or J-SRX240 device, the default values of the **heartbeat-threshold** and **heartbeat-interval** options in the **[edit chassis cluster]** hierarchy are 8 beats and 2000 ms, respectively. These values cannot be changed on these devices.

Command-Line Interface (CLI)

- On AX411 Access Points, the possible completions available for the CLI command **set wlan access-point < ap_name > radio < radio_num > radio-options channel number ?** have changed from previous implementations.

  Now this CLI command displays the following possible completions:

  Example 1:
  user@host# set wlan access-point ap6 radio 1 radio-options channel number ?
  Possible completions:
  36 Channel 36
  40 Channel 40
  44 Channel 44
  48 Channel 48
  52 Channel 52
  56 Channel 56
  60 Channel 60
  64 Channel 64
  100 Channel 100
  108 Channel 108
  112 Channel 112
  116 Channel 116
  120 Channel 120
  124 Channel 124
  128 Channel 128
  132 Channel 132
  136 Channel 136
  140 Channel 140
  149 Channel 149
  153 Channel 153
  157 Channel 157
  161 Channel 161
  165 Channel 165
  auto Automatically selected

  Example 2:
  user@host# set wlan access-point ap6 radio 2 radio-options channel number ?
  1 Channel 1
  2 Channel 2
  3 Channel 3
  4 Channel 4
  5 Channel 5
  6 Channel 6
  7 Channel 7
  8 Channel 8
  9 Channel 9
  10 Channel 10
  11 Channel 11
  12 Channel 12

13 Channel 13
14 Channel 14
auto Automatically selected

- On AX411 Access Points, the possible completions available for the CLI command **set wlan access-point mav0 radio 1 radio-options mode?** have changed from previous implementations.

  Now this CLI command displays the following possible completions:

  - Example 1:
    user@host# **set wlan access-point mav0 radio 1 radio-options mode ?**
    Possible completions:
    5GHz Radio Frequency -5GHz-n
    a Radio Frequency -a
    an Radio Frequency -an
    [edit]
  - Example 2:
    user@host# **set wlan access-point mav0 radio 2 radio-options mode ?**
    Possible completions:
    2.4GHz Radio Frequency --2.4GHz-n
    bg Radio Frequency -bg
    bgn Radio Frequency -bgn

- On J-SRX Series devices, the **show system storage partitions** command now displays the partitioning scheme details on J-SRX Series devices.
  - Example 1:
    show system storage partitions (dual root partitioning)
    user@host# **show system storage partitions**
    Boot Media: internal (da0)
    Active Partition: da0s2a
    Backup Partition: da0s1a
    Currently booted from: active (da0s2a)
    Partitions Information:
    Partition Size Mountpoint
    s1a 293M altroot
    s2a 293M /
    s3e 24M /config
    s3f 342M /var
    s4a 30M recovery
  - Example 2:
    show system storage partitions (single root partitioning)
    user@host# **show system storage partitions**
    Boot Media: internal (da0)
    Partitions Information:
    Partition Size Mountpoint
    s1a 898M /
    s1e 24M /config
    s1f 61M /var
  - Example 3:
    show system storage partitions (usb)
    user@host# **show system storage partitions**
    Boot Media: usb (da1)
    Active Partition: da1s1a
    Backup Partition: da1s2a
    Currently booted from: active (da1s1a)
    Partitions Information:
    Partition Size Mountpoint
    s1a 293M /
    s2a 293M altroot
    s3e 24M /config
    s3f 342M /var
    s4a 30M recovery

- On J-SRX100, J-SRX210, and J-SRX240 devices, support for Layer LAG is added in both standalone and cluster mode.

  In cluster mode, the following CLI is now enabled to specify the number of aggregated interfaces.

  set chassis aggregated-devices ethernet device-count xxx

  Support to add multiple links from each chassis to a reth interface is also available. In the below example, 2 links from each chassis is added to reth3.

  set interfaces ge-0/0/8 gigether-options redundant-parent reth3
  set interfaces ge-0/0/9 gigether-options redundant-parent reth3
  set interfaces ge-5/0/8 gigether-options redundant-parent reth3
  set interfaces ge-5/0/9 gigether-options redundant-parent reth3

  The following CLI is used for enabling LACP on reth interface:

  set interfaces reth3 redundant-ether-options lacp active

Configuration

- On J-SRX100, J-SRX210, and J-SRX240 devices, the current Junos OS default configuration is inconsistent with the one in Secure Services Gateways, thus causing problems when users migrate to J-SRX Series devices. As a workaround, users should ensure the following steps are taken:
  - The **ge-0/0/0** interface should be configured as the Untrust port (with the DHCP client enabled).
  - The rest of the on-board ports should be bridged together, with a VLAN IFL and DHCP server enabled (where applicable).
  - Default policies should allow trust->untrust traffic.
  - Default NAT rules should apply interface-nat for all trust->untrust traffic.
  - DNS/Wins parameters should be passed from server to client and, if not available, users should preconfigure a DNS server (required for download of security packages).

Flow and Processing

- On J-SRX Series devices, the factory default for the maximum number of backup configurations allowed is five. Therefore, you can have one active configuration and a maximum of five rollback configurations. Increasing this backup configuration number will result in increased memory usage on disk and increased commit time.

  To modify the factory defaults, use the following commands:

  ```
  root@host# set system max-configurations-on-flash number
  root@host# set system max-configuration-rollbacks number
  ```

  where **max-configurations-on-flash** indicates backup configurations to be stored in the configuration partition and **max-configuration-rollbacks** indicates the maximum number of backup configurations.

- On J-SRX Series devices, when you configure identical IPs on a single interface, you no longer get a warning message; instead, a syslog message appears.

Interfaces and Routing

- On J-SRX Series devices, to minimize the size of system logs, the default logging level in the factory configuration has been changed from **any any** to **any critical**.
- On J-SRX100, J-SRX210, and J-SRX240 devices, the autoinstallation functionality on an interface enables a DHCP client on the interface and remains in the DHCP client mode. In previous releases, after a certain period, the interface changed from being a DHCP client to a DHCP server.
- On T1/E1 Mini-Physical Interface Module installed on J-SRX210 and J-SRX240 devices, the Loopback LED is turned ON based on the Loopback configuration as well as when the FDL loopback commands are executed from the remote-end. The Loopback LED remains OFF when no FDL Loopback commands are executed from the remote-end, even though **remote-loopback-respond** is configured on the HOST.
- On J-SRX100, J-SRX210 and J-SRX240 devices, support for USB auto-installation is added. This feature simplifies the upgrading of Junos OS images in cases where there is no console access to a J-SRX Series device located at a remote site. Allows you to upgrade the Junos OS image with minimum configuration effort by simply inserting a USB flash drive into the USB port of the J-SRX Series device and performing a few simple steps. This feature can also be used for reformatting boot device and recovering J-SRX Series services gateway after a boot media corruption.

J-Web

- **URL separation for J-Web and dynamic VPN**—This feature prevents the dynamic VPN users from accessing J-Web accidentally or intentionally. Unique URLs for J-Web and dynamic VPN add support to the webserver for parsing all the HTTP requests it receives. The webserver also provides access permission based on the interfaces enabled for J-Web and dynamic VPN.
  - **CLI changes:** A new configuration attribute **management-url** is introduced at the **[edit system services web-management]** hierarchy level to control J-Web access when both J-Web and dynamic VPN are enabled on the same interface. The following example describes the configuration of the new attribute:

```
web-management {
    traceoptions {
        level all;
        flag dynamic-vpn;
        flag all;
    }
    management-url my-jweb;
    http;
    https {
        system-generated-certificate;
    }
    limits {
        debug-level 9;
    }
```

```
    session {
      session-limit 7;
    }
  }
```

- **Disabling J-Web:** Dynamic VPN must have the configured HTTPS certificate and the webserver to communicate with the client. Therefore, the configuration at the **[edit system services web-management]** hierarchy level required to start the appweb webserver cannot be deleted or deactivated. To disable J-Web, the administrator must configure a loopback interface of **lo0** for HTTP or HTTPS. This ensures that the webserver rejects all J-Web access requests.

```
  web-management {
    traceoptions {
      level all;
      flag dynamic-vpn;
      flag all;
    }
    management-url my-jweb;
    http {
      interface lo0.0;
    }
    https {
      system-generated-certificate;
    }
    limits {
      debug-level 9;
    }
    session {
      session-limit 7;
    }
  }
```

- **Changes in the Web access behavior:** The following section illustrates the changes in the Web access behavior when J-Web and dynamic VPN do not share and do share the same interface:

  Case 1: J-Web and dynamic VPN do not share the same interface.

Scenario	http(s)://*server host*	http(s)://*server host//configured attribute*	http(s)://*server host//dynamic-vpn*
J-Web is enabled, and dynamic VPN is configured.	Navigates to the J-Web login page on the J-Web enabled interface or to the dynamic VPN login page on the dynamic VPN enabled interface depending on the server host chosen	Navigates to the J-Web login page if the J-Web attribute is configured; otherwise, navigates to the Page Not Found page	Navigates to the dynamic VPN login page

J-Web is not enabled, and dynamic VPN is not configured.	Navigates to the Page Not Found page	Navigates to the Page Not Found page	Navigates to the Page Not Found page
J-Web is enabled, and dynamic VPN is not configured.	Navigates to the J-Web login page	Navigates to the J-Web login page if the J-Web attribute is configured; otherwise, navigates to the Page Not Found page	Navigates to the Page Not Found page
J-Web is not enabled, and dynamic VPN is configured.	Navigates to the dynamic VPN login page	Navigates to the Page Not Found page	Navigates to the dynamic VPN login page

Case 2: J-Web and dynamic VPN do share the same interface.

Scenario	http(s)://*server host*	http(s)://*server host//configured attribute*	http(s)://*server host//dynamic-vpn*
J-Web is enabled, and dynamic VPN is configured.	Navigates to the dynamic VPN login page	Navigates to the J-Web login page if the attribute is configured; otherwise, navigates to the Page Not Found page	Navigates to the dynamic VPN login page
J-Web is not enabled, and dynamic VPN is not configured.	Navigates to the Page Not Found page	Navigates to the Page Not Found page	Navigates to the Page Not Found page
J-Web is enabled, and dynamic VPN is not configured.	Navigates to the J-Web login page	Navigates to the J-Web login page if the J-Web attribute is configured; otherwise, navigates to the Page Not Found page	Navigates to the Page Not Found page
J-Web is not enabled, and dynamic VPN is configured.	Navigates to the dynamic VPN login page	Navigates to the Page Not Found page	Navigates to the dynamic VPN login page

- On J-SRX100, J-SRX210, and J-SRX240 devices, the LED status (Alarm, HA, ExpressCard, Power Status, and Power) shown in the front panel for Chassis View does not replicate the exact status of the device.
- On all J-SRX Series devices, the BIOS version is displayed on system identification on the J-Web dashboard.

NOTE: Delete your browser cookies to view this change.

- J-Web login page is updated with the new Juniper Networks logo and trademark.
- The options to configure the Custom Attacks, Custom Attack Groups, and Dynamic Attack Groups are disabled because they cannot be configured from J-Web.

Multilink

- When data and LFI streams are present, we recommend the following configuration to get less latency for LFI traffic and to avoid out of order transmission of data traffic:

  Configure the following schedulers

  - set class-of-service schedulers S0 buffer-size temporal 20K
  - set class-of-service schedulers S0 priority low
  - set class-of-service schedulers S2 priority high
  - set class-of-service schedulers S3 priority high

  Configure the following scheduler map

  - set class-of-service scheduler-maps lsqlink_map forwarding-class best-effort scheduler S0
  - set class-of-service scheduler-maps lsqlink_map forwarding-class assured-forwarding scheduler S2
  - set class-of-service scheduler-maps lsqlink_map forwarding-class network-control scheduler S3

  Attach scheduler map to all member links

  - set class-of-service interfaces t1-2/0/0 unit 0 scheduler-map lsqlink_map

  Even after this configuration, if Out-of-range sequence number drops are observed on reassembly side, please increase drop-timeout of the bundle to 200ms

PoE

- On J-SRX210 PoE devices, SDK packages might not work.

Security

- Any change in the Unified Access Control's (UAC) contact interval and timeout values in the J-SRX Series device will be effective only after the next reconnection of the J-SRX Series device with the Infranet Controller.
- The maximum size of a redirect payload is 1450 bytes. The size of the redirect URL is restricted to 1407 bytes (excluding a few HTTP headers). If a user accesses a destination URL that is larger than 1407 bytes, the Infranet Controller authenticates the payload, the exact length of the redirect URL is calculated, and the destination URL is trimmed such that it can fit into the redirect URL. The destination URL can be fewer than 1407 bytes based on what else is present in the redirect URL, for example, policy ID. The destination URL in the default redirect URL is trimmed such that the redirect packet payload size is limited to 1450 bytes, and if the length of the payload is larger than

1450 bytes, the excess length is trimmed and the user is directed to the destination URL that has been resized to 1450 bytes.

WLAN

- While configuring the AX411 Access Point on your J-SRX Series devices, you must enter the WLAN admin password using the **set wlan admin-authentication password** command. This command prompts for the password and the password entered is stored in encrypted form.

  NOTE:
  - Without wlan config option enabled, the AX411 Access Points will be managed with the default password.
  - Changing the wlan admin-authentication password when the wlan subsystem option is disabled might result in mismanagement of Access Points . You might have to power cycle the Access Points manually to avoid this issue.
  - The J-SRX Series devices that are not using the AX411 Access Point can optionally delete the wlan config option.

- Accessing the AX411 Access Point through SSH is disabled by default. You can enable the SSH access using the **set wlan access-point < name > external system services enable-ssh** command.

VLAN

- **Native-vlan-id** can be configured only when either **flexible-vlan-tagging** mode or **interface-mode** trunk is configured. The commit error has been corrected, which was previously indicating **vlan-tagging** mode instead of **flexible-vlan-tagging** mode.

Unsupported CLI Statements and Commands

This section lists unsupported CLI statements and commands.

Accounting-Options Hierarchy

- On J-SRX100, J-SRX210, and J-SRX240 devices, the **accounting**, **source-class**, and **destination-class** statements in the **[accounting-options]** hierarchy level are not supported.

AX411 Access Point Hierarchy

- On J-SRX100 devices, there are CLI commands for wireless LAN configurations related to the AX411 Access Point. However, at this time the J-SRX100 devices do not support the AX411 Access Point.

Chassis Hierarchy

- On J-SRX100, J-SRX210, and J-SRX240 devices, the following chassis hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set chassis craft-lockout

set chassis routing-engine on-disk-failure
```

Class-of-Service Hierarchy

- On J-SRX100, J-SRX210, and J-SRX240 devices, the following class-of-service hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set class-of-service classifiers ieee-802.1ad

set class-of-service interfaces interface-name unit 0 adaptive-shaper
```

Ethernet-Switching Hierarchy

- On J-SRX100, J-SRX210, and J-SRX240 devices, the following Ethernet-switching hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set ethernet-switching-options bpdu-block disable-timeout

set ethernet-switching-options bpdu-block interface

set ethernet-switching-options mac-notification

set ethernet-switching-options voip interface access-ports

set ethernet-switching-options voip interface ge-0/0/0.0 forwarding-class
```

Firewall Hierarchy

- On J-SRX100, J-SRX210, and J-SRX240 devices, the following Firewall hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set firewall family vpls filter

set firewall family mpls dialer-filter d1 term
```

Interfaces CLI Hierarchy

On all J-SRX100, J-SRX210, and J-SRX240 devices, the following interface hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

Aggregated Interface CLI

- The following CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
request lacp link-switchover ae0

set interfaces ae0 aggregated-ether-options lacp link-protection

set interfaces ae0 aggregated-ether-options link-protection
```

ATM Interface CLI

- The following CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set interfaces at-1/0/0 container-options

set interfaces at-1/0/0 atm-options ilmi

set interfaces at-1/0/0 atm-options linear-red-profiles

set interfaces at-1/0/0 atm-options no-payload-scrambler

set interfaces at-1/0/0 atm-options payload-scrambler

set interfaces at-1/0/0 atm-options plp-to-clp

set interfaces at-1/0/0 atm-options scheduler-maps
```

```
set interfaces at-1/0/0 unit 0 atm-l2circuit-mode

set interfaces at-1/0/0 unit 0 atm-scheduler-map

set interfaces at-1/0/0 unit 0 cell-bundle-size

set interfaces at-1/0/0 unit 0 compression-device

set interfaces at-1/0/0 unit 0 epd-threshold

set interfaces at-1/0/0 unit 0 inverse-arp

set interfaces at-1/0/0 unit 0 layer2-policer

set interfaces at-1/0/0 unit 0 multicast-vci

set interfaces at-1/0/0 unit 0 multipoint

set interfaces at-1/0/0 unit 0 plp-to-clp

set interfaces at-1/0/0 unit 0 point-to-point

set interfaces at-1/0/0 unit 0 radio-router

set interfaces at-1/0/0 unit 0 transmit-weight

set interfaces at-1/0/0 unit 0 trunk-bandwidth
```

Ethernet Interfaces

- The following CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set interfaces ge-0/0/1 gigether-options ignore-l3-incompletes

set interfaces ge-0/0/1 gigether-options mpls

set interfaces ge-0/0/0 stacked-vlan-tagging

set interfaces ge-0/0/0 native-vlan-id

set interfaces ge-0/0/0 radio-router

set interfaces ge-0/0/0 unit 0 interface-shared-with

set interfaces ge-0/0/0 unit 0 input-vlan-map

set interfaces ge-0/0/0 unit 0 output-vlan-map

set interfaces ge-0/0/0 unit 0 layer2-policer

set interfaces ge-0/0/0 unit 0 accept-source-mac
```

```
set interfaces fe-0/0/2 fastether-options source-address-filter

set interfaces fe-0/0/2 fastether-options source-filtering

set interfaces ge-0/0/1 passive-monitor-mode
```

GRE Interface CLI

- The following CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set interfaces gr-0/0/0 unit 0 ppp-options

set interfaces gr-0/0/0 unit 0 layer2-policer
```

IP Interface CLI

- The following CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set interfaces ip-0/0/0 unit 0 layer2-policer

set interfaces ip-0/0/0 unit 0 ppp-options

set interfaces ip-0/0/0 unit 0 radio-router
```

LSQ Interface CLI

- The following CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set interfaces lsq-0/0/0 unit 0 layer2-policer

set interfaces lsq-0/0/0 unit 0 family ccc

set interfaces lsq-0/0/0 unit 0 family tcc

set interfaces lsq-0/0/0 unit 0 family vpls

set interfaces lsq-0/0/0 unit 0 multipoint

set interfaces lsq-0/0/0 unit 0 point-to-point

set interfaces lsq-0/0/0 unit 0 radio-router
```

PT Interface CLI

- The following CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set interfaces pt-1/0/0 gratuitous-arp-reply

set interfaces pt-1/0/0 link-mode

set interfaces pt-1/0/0 no-gratuitous-arp-reply
```

```
set interfaces pt-1/0/0 no-gratuitous-arp-request

set interfaces pt-1/0/0 vlan-tagging

set interfaces pt-1/0/0 unit 0 radio-router

set interfaces pt-1/0/0 unit 0 vlan-id
```

T1 Interface CLI

- The following CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set interfaces t1-1/0/0 receive-bucket

set interfaces t1-1/0/0 transmit-bucket

set interfaces t1-1/0/0 encapsulation ether-vpls-ppp

set interfaces t1-1/0/0 encapsulation extended-frame-relay

set interfaces t1-1/0/0 encapsulation extended-frame-relay-tcc

set interfaces t1-1/0/0 encapsulation frame-relay-port-ccc

set interfaces t1-1/0/0 encapsulation satop

set interfaces t1-1/0/0 unit 0 encapsulation ether-vpls-fr

set interfaces t1-1/0/0 unit 0 encapsulation frame-relay-ppp

set interfaces t1-1/0/0 unit 0 layer2-policer

set interfaces t1-1/0/0 unit 0 radio-router

set interfaces t1-1/0/0 unit 0 family inet dhcp

set interfaces t1-1/0/0 unit 0 inverse-arp

set interfaces t1-1/0/0 unit 0 multicast-dlci
```

VLAN Interface CLI

- The following CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set interfaces vlan unit 0 family tcc

set interfaces vlan unit 0 family vpls

set interfaces vlan unit 0 accounting-profile

set interfaces vlan unit 0 layer2-policer
```

```
set interfaces vlan unit 0 ppp-options

set interfaces vlan unit 0 radio-router
```

Protocols Hierarchy

- On J-SRX100, J-SRX210, and J-SRX240 devices, the following CLI commands are not supported. However, if you enter these commands in the CLI editor, they will appear to succeed and will not display an error message.

```
set protocols bfd no-issu-timer-negotiation

set protocols bgp idle-after-switch-over

set protocols l2iw

set protocols bgp family inet flow

set protocols bgp family inet-vpn flow

set protocols igmp-snooping vlan all proxy
```

Routing Hierarchy

- On J-SRX100, J-SRX210, and J-SRX240 devices, the following routing hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set routing-instances p1 services

set routing-instances p1 multicast-snooping-options

set routing-instances p1 protocols amt

set routing-options bmp

set routing-options flow
```

Services Hierarchy

- On J-SRX100, J-SRX210, and J-SRX240 devices, the following services hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set services service-interface-pools
```

SNMP Hierarchy

- On J-SRX100, J-SRX210, and J-SRX240 devices, the following SNMP hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set snmp community 90 logical-system
```

```
set snmp logical-system-trap-filter

set snmp trap-options logical-system

set snmp trap-group d1 logical-system
```

System Hierarchy

- On J-SRX100, J-SRX210, and J-SRX240 devices, the following system hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

  ```
  set system diag-port-authentication
  ```

Related Documentation

- New Features in Junos OS Release 10.3 for J-SRX Series Services Gateways on page 4
- Issues in Junos OS Release 10.3 for J-SRX Series Services Gateways on page 29
- Errata and Changes in Documentation for Junos OS Release 10.3 for J-SRX Series Services Gateways on page 42

Known Limitations in Junos OS Release 10.3 for J-SRX Series Services Gateways

AppSecure

- **Junos OS Application Identification**—When you create custom application or nested application signatures for Junos OS application identification, the order value must be unique among all predefined and custom application signatures. The order value determines the application matching priority of the application signature.

  The order value is set with the **set services application-identification application application-name signature order** command. You can also view all signature order values by entering the **show services application-identification | display set | match order** command. You will need to change the order number of the custom signature if it conflicts with another application signature.

Chassis Cluster

- J-SRX100, J-SRX210, and J-SRX240 devices have the following chassis cluster limitations:
  - Virtual Router Redundancy Protocol (VRRP) is not supported.
  - In service software upgrade (ISSU) is not supported.
  - The 3G dialer interface is not supported.
  - On J-SRX Series device failover, access points on the Layer 2 switch reboot and all wireless clients lose connectivity for 4-6 minutes.
  - On VDSL mini-PIM, chassis cluster is not supported for both VDSL and ADSL mode.
  - Queuing on aggregated Ethernet (**ae**) interface is not supported.

  - PoE is not supported in chassis cluster mode.
  - Group VPN is not supported.
  - Sampling features like J-FLow, packet capture, and port mirror on the **reth** interface are not supported.
  - Switching is not supported in chassis cluster mode.
  - The Chassis Cluster MIB is not supported.
  - Any packet-based services like MPLS and CLNS are not supported.
  - lsq-0/0/0—Link services Multilink Point-to-Point Protocol (MLPPP), Multilink Frame Relay (MLFR), and Compressed Real-Time Transport Protocol (CRTP) are not supported.
  - gr-0/0/0—Generic routing encapsulation (GRE) and tunneling are not supported.
  - ip-0/0/0—IP-over-IP (IP-IP) encapsulation is not supported.
  - lt-0/0/0—CoS for real-time performance monitoring (RPM) is not supported.
  - PP0—PPPoE and PPPoEoA are not supported.
- On J-SRX100, J-SRX210, and J-SRX240 devices, UTM is supported only for active/backup chassis cluster configuration with both RG0 and RG1+ active on the same node. It is not supported for active/active chassis cluster configuration.

For other limitations in chassis cluster, see "Limitations of Chassis Clustering" in the *Junos OS Security Configuration Guide*.

Command-Line Interface (CLI)

- On J-SRX210 and J-SRX240 devices, J-Web crashes if more than nine users log in to the device by using the CLI. The number of users allowed to access the device is limited as follows:
  - For J-SRX210 devices: four CLI users and three J-Web users
  - For J-SRX240 devices: six CLI users and five J-Web users

Dynamic VPN

J-SRX100, J-SRX210, and J-SRX240 devices have the following limitations:

- The IKE configuration for the dynamic VPN client does not support the hexadecimal preshared key.
- The dynamic VPN client IPsec does not support the Authentication Header (AH) protocol and the Encapsulating Security Payload (ESP) protocol with NULL authentication.
- When you log in through the Web browser (instead of logging in through the dynamic VPN client) and a new client is available, you are prompted for a client upgrade even

if the **force-upgrade** option is configured. Conversely, if you log in using the dynamic VPN client with the **force-upgrade** option configured, the client upgrade occurs automatically (without a prompt).

Flow and Processing

- On J-SRX Series devices, high CPU utilization triggered due to various reasons like CPU intensive commands, SNMP Walks etc causes the BFD to flap while processing large BGP updates.

For other limitations in flow and processing, see "Limitations of Flow and Processing" in the *Junos OS Security Configuration Guide*.

Interfaces and Routing

- On J-SRX240 High Memory devices, traffic might stop between J-SRX240 device and CISCO switch due to link mode mismatch. As a workaround, Dell recommends setting auto-negotiation parameters on both ends to the same value.
- On J-SRX240 devices, the VLAN range from 3967 to 4094 falls under the reserved VLAN address range, and the user is not allowed any configured VLANs from this range.
- On J-SRX Series devices, the user can use IPsec only on an interface that resides in the routing instance **inet 0**. The user will not be able to assign an internal or external interface to the IKE policy if that interface is placed in a routing instance other than **inet 0**.
- On J-SRX210 devices, the USB modem interface can handle bidirectional traffic of up to 19 Kbps. On oversubscription of this amount (that is, bidirectional traffic of 20 Kbps or above), **keepalives** are not exchanged, and the interface goes down.
- On J-SRX100, J-SRX210, and J-SRX240 devices, on the Layer 3 **ae** interface, the following features are not supported:
  - Encapsulations (Such as CCC, VLAN CCC, VPLS, or PPPOE) on Layer 3 **ae** interfaces
  - J-Web
  - Layer 3 **ae** for 10-Gigabit Ethernet XPIM ports

IPv6 Support

For limitations in IPv6, see "Limitations of IPv6" in the *Junos OS Security Configuration Guide*.

J-Web Browser Support

- **J-Web Browser Support for Your Dell PowerConnect J-Series Devices**—To access the J-Web interface for all platforms, your management device requires the following Windows operating system and browsers:
  - Operating System: Microsoft Windows XP Service Pack 3
  - Browser: Microsoft Internet Explorer version 7.0 or Mozilla Firefox version 3.0

NOTE: Other browser versions may work but are not supported.

NOTE: Only English-version browsers are supported.

NOTE: For both J-SRX and J-EX devices, the browser and the network must support receiving and processing HTTP 1.1 GZIP compressed data.

NOTE: For J-SRX devices, to use the Chassis View, version 9 or later of Adobe Flash Player must be installed. Chassis View is displayed by default on the Dashboard page. You can enable or disable the Chassis View using options in the Dashboard Preference dialog box.

NetScreen-Remote

- On J-SRX Series devices, NetScreen-Remote is not supported in Junos OS Release 10.3.

Network Address Translation (NAT)

- **NAT rule capacity change**—To support the use of large-scale NAT (LSN) at the edge of the carrier network, the device-wide NAT rule capacity has been changed.

  The number of destination and static NAT rules has been incremented as shown in Table 1 on page 28. The limitation on the number of destination-rule-set and static-rule-set has been increased.

  Table 1 on page 28 provides the requirements per device to increase the configuration limitation as well as scale the capacity for each device.

Table 1: Number of Rules on J-SRX Series Devices

NAT Rule Type	J-SRX100	J-SRX210	J-SRX240
Source NAT rule	512	512	1024
Destination NAT rule	512	512	1024
Static NAT rule	512	512	1024

  The restriction on the number of rules per rule set has been increased so that there is only a device-wide limitation on how many rules a device can support. This restriction is provided to help you better plan and configure the NAT rules for the device.

Point-to-Point Protocol over Ethernet (PPPoE)

- On J-SRX240 devices in a chassis cluster, the **reth** interface cannot be used as the underlying interface for Point-to-Point Protocol over Ethernet (PPPoE).

Switching

- On J-SRX100, J-SRX210, and J-SRX240 devices, CoA is not supported with 802.1x.
- On J-SRX100, J-SRX210, and J-SRX240 devices, on the routed VLAN interface, the following features are not supported:
  - IPv6 (family inet6)
  - ISIS (family ISO)
  - Class-of-service

- Encapsulations (Ether CCC, VLAN CCC, VPLS, PPPoE, and so on) on VLAN interfaces
- CLNS
- PIM
- DVMRP
- VLAN interface MAC change
- Gratuitous ARP
- Change VLAN-Id for VLAN interface

VLAN

- On J-SRX100, J-SRX210, and J-SRX240 devices, the IRB (VLAN) interface cannot be used as the underlying interface for Point-to-Point Protocol over Ethernet (PPPoE).

VPNs

- On J-SRX100, J-SRX210, and J-SRX240 devices, while configuring dynamic VPN using PULSE client, when you select the authentication-algorithm as sha-256 in IKE proposal, IPsec session might not get established.

WLAN

- The following are the maximum numbers of access points that can be configured and managed from J-SRX Series devices:
  - J-SRX210—4 access points
  - J-SRX240—8 access points

NOTE: The number of licensed access points can exceed the maximum number of supported access points. However, you can only configure and manage the maximum number of access points.

Related Documentation

- New Features in Junos OS Release 10.3 for J-SRX Series Services Gateways on page 4
- Issues in Junos OS Release 10.3 for J-SRX Series Services Gateways on page 29
- Errata and Changes in Documentation for Junos OS Release 10.3 for J-SRX Series Services Gateways on page 42

Issues in Junos OS Release 10.3 for J-SRX Series Services Gateways

- Outstanding Issues In Junos OS Release 10.3 for J-SRX Series Services Gateways on page 30
- Resolved Issues in Junos OS Release 10.3 for J-SRX Series Services Gateways on page 39

Outstanding Issues In Junos OS Release 10.3 for J-SRX Series Services Gateways

The following problems currently exist in J-SRX Series devices. The identifier following the description is the tracking number in our bug database.

Application Layer Gateways (ALGs)

- On J-SRX210 devices, the SCCP call cannot be set up after disabling and enabling the SCCP ALG. The call does not go through. [PR/409586]
- On J-SRX240 devices, the maximum SCCP calls cannot be made under stress conditions. [PR/490839]
- On J-SRX Series devices, SIP server protection does not work. The **set security alg sip application-screen protect deny** command does not work. [PR/512202]

AX411 Access Point

- On J-SRX210 PoE devices, the access point reboots when 100 clients are associated simultaneously and each one is transmitting 512 bytes packets at 100 pps. [PR/469418]

Chassis Cluster

- On J-SRX Series devices in a chassis cluster, configuring the **set system process jsrp-service disable** command only on the primary node causes the cluster to go into an incorrect state. [PR/292411]
- On J-SRX Series devices in a chassis cluster, using the **set system processes chassis-control disable** command for 4 to 5 minutes and then enabling it causes the device to crash. Do not use this command on a J-SRX Series device in a chassis cluster. [PR/296022]
- On a J-SRX210 device in a chassis cluster, when you upgrade the nodes, sometimes the forwarding process might crash and get restarted. [PR/396728]
- On a J-SRX210 device in a chassis cluster, sometimes the **reth** interface MAC address might not make it to the switch filter table. This results in the dropping of traffic sent to the **reth** interface. As a workaround, restart the Packet Forwarding Engine. [PR/401139]
- On a J-SRX210 device in a chassis cluster, the fabric monitoring option is enabled by default. This can cause one of the nodes to move to a disabled state. You can disable fabric monitoring by using the following CLI command:

  set chassis cluster fabric-monitoring disable

  [PR/404866]
- On a J-SRX210 Low Memory device in a chassis cluster, the firewall filter does not work on the **reth** interfaces. [PR/407336]
- On a J-SRX210 device in a chassis cluster, the restart forwarding method is not recommended because when the control link goes through forwarding, the restart forwarding process causes disruption in the control traffic. [PR/408436]
- On a J-SRX210 device with an FTP session ramp-up rate of 70, either of the following might disable the secondary node:

  - Back-to-back redundancy group 0 failover
  - Back-to-back primary node reboot

    [PR/414663]

- If a J-SRX210 device receives more traffic than it can handle, node 1 either disappears or gets disabled. [PR/416087]
- On J-SRX240 Low Memory and High Memory devices, binding the same IKE policy to a dynamic gateway and a site-to-site gateway is not allowed. [PR/440833]
- On J-SRX240 devices, the cluster might get destabilized when the file system is full and logging is configured on JSRPD and chassisd. The log file size for the various modules should be appropriately set to prevent the file system from getting full. [PR/454926]
- During a manual failover, a system crash might occur if the nodes have not completely recovered from a previous failover. To determine if a device is ready for repeated failovers, perform these recommended best-practice steps before doing a manual failover.

  The best practice we recommend to ensure a proper failover is as follows:

  - Use the **show chassis cluster status** command to verify the following for all redundancy groups:
    - One node is primary; the other node is secondary.
    - Both nodes have nonzero priority values unless a monitored interface is down.
  - Use the **show chassis fpc pic-status** command to verify that the PIC status is **Online**.
  - Use the **show pfe terse** command to verify that the Packet Forwarding Engine status is **Ready** and to verify following:
    - All slots on the RG0 primary node have the status **Online**.
    - All slots on the RG0 secondary node, except the Routing Engine slots, have the status **Valid**.

  [PR/503389 and PR/520093]

Class of Service (CoS)

- On J-SRX Series devices, class-of-service-based forwarding (CBF) does not work. [PR/304830]

Dynamic Host Configuration Protocol (DHCP)

- On J-SRX210 and J-SRX240 devices, when autoinstallation is configured to run on a particular interface and the default static route is set with the options discard, retain, and no-advertise, the DHCP client running on the interface tries fetching the configuration files from the TFTP server. During this process, the UDP data port on the TFTP server might be unreachable. Because of the TFTP server being unreachable, the autoinstallation process might remain in the configuration acquisition state. When autoinstallation is disabled, the TFTP might fail. In this case, you should manually fetch the file from the server or the client through the relay.

  As a workaround, remove the static route options discard, retain, and no-advertise from the configuration.[PR/454189]

Flow and Processing

- On J-SRX Series devices, the **show security flow session** command currently does not display aggregate session information. Instead, it displays sessions on a per-SPU basis. [PR/264439]
- On J-SRX Series devices, when traffic matches a deny policy, sessions will not be created successfully. However, sessions are still consumed, and the **unicast-sessions** and **sessions-in-use** fields shown by the **show security flow session summary** command will reflect this. [PR/284299 and PR/397300]
- On J-SRX Series devices, configuring the flow filter with the **all** flag might result in traces that are not related to the configured filter. As a workaround, use the flow trace flag **basic** with the command **set security flow traceoptions flag**. [PR/304083]
- On J-SRX210 and J-SRX240 devices, after the device fragments packets, the FTP over a GRE link might not perform properly because of packet serialization. [PR/412055]
- On J-SRX240 devices, traffic flooding occurs when multiple multicast (MC) IP group addresses are mapped to the same MAC address because multicast switching is based on the Layer 2 address. [PR/418519]
- On a J-SRX210 onboard Ethernet port, an IPv6 multicast packet received gets duplicated at the ingress. This happens only for IPv6 multicast traffic in ingress. [PR/432834]
- On J-SRX240 PoE devices, the first packet on each multilink class gets dropped on reassembly. [PR/455023]
- On J-SRX210 and J-SRX240 devices, the serial interface goes down for long duration traffic when FPGA 2.3 version is loaded in the device. As a result, the multilink goes down. This issue is not seen when downgrading the FPGA version from 2.3 to 1.14. [PR/461471]
- On J-SRX Series devices, system log messages about interactive commands to the system log server do not work. [PR/511110]

- On J-SRX Series devices, the software upload and install package will not show a warning message when there are pending changes to be committed. [PR/514853]
- On J-SRX240 Low Memory devices, the LSQ interface transmitting both LLQ and non-LLQ traffic drops out-of-profile packets of the LLQ traffic faster than it was dropping them out earlier. [PR/536588]
- On J-SRX240 High Memory devices under continuous high HTTP traffic load, the forwarding daemon might generate a core file. This core file might be seen after more than 24 hours of continuous high load. Forwarding restarts when the forwarding core file is generated; then the device functions normally. [PR/538383]

Hardware

- On J-SRX210 devices, the MTU size is limited to 1518 bytes for the 1-port SFP Mini-PIM. [PR/296498]
- On J-SRX240 devices, the Mini-PIM LEDs glow red for a short duration (1 second) when the device is powered on. [PR/429942]
- On J-SRX240 devices, the file installation fails on the right USB slot when both of the USB slots have USB storage devices attached. [PR/437563]
- On J-SRX240 devices, the combinations of Mini-PIMs cause SFP-Copper links to go down in some instances during bootup, restarting fwdd, and restarting chassisd. As a workaround, reboot the device and the link will be up. [PR/437788]

Interfaces and Routing

- On J-SRX240 devices, when you are configuring the link options on an interface, only the following scenarios are supported:
  - Autonegotiation is enabled on both sides.
  - Autonegotiation is disabled on both sides (forced speed), and both sides are set to the same speed and duplex.

    If one side is set to autonegotiation mode and the other side is set to forced speed, the behavior is indeterminate and not supported. [PR/423632]
- On J-SRX Series devices, the RPM operation will not work for the probe-type tcp-ping when the probe is configured with the option **destination-interface**. [PR/424925]
- On J-SRX Series devices, incorrect Layer 2 circuit replication on the backup Routing Engine might occur when you:
  - Configure nonstop active routing (NSR) and Layer 2 circuit standby simultaneously and commit them
  - Delete the NSR configuration and then add the configuration back when both the NSR and Layer 2 circuits are up

  As a workaround:

  1. Configure the Layer 2 circuit for a nonstandby connection.
  2. Change the configuration to a standby connection.

3. Add the NSR configuration.

[PR/440743]

- On J-SRX210 Low Memory devices, the E1 interface will flap and traffic will not pass through the interface if you restart forwarding while traffic is passing through the interface. [PR/441312]
- On J-SRX240 Low Memory devices and J-SRX240 High Memory devices, the RPM Server operation does not work when the probe is configured with the option **destination-interface**. [PR/450266]
- On J-SRX210 PoE devices, the ATM interface on G.SHDSL interface will not go down when the interface is disabled through the **disable** command. [PR/453896]
- On J-SRX210 devices, the modem moves to the dial-out pending state while connecting or disconnecting the call. [PR/454996]
- On J-SRX100, and J-SRX210 devices, out-of-band dial-in access using a serial modem does not work. [PR/458114]
- On J-SRX100 devices with VDLS2, multiple carrier transitions (three to four) are seen during long duration traffic testing with ALU 7302 DSLAM. There is no impact on traffic except for the packet loss after long duration traffic testing, which is also seen in the vendor CPE. [PR/467912]
- On J-SRX210 devices with VDLS2, remote end ping fails to go above the packet size of 1480 as the packets are get dropped for the default MTU which is 1496 on an interface and the default MTU of the remote host ethernet intf is 1514. [PR/469651]
- On J-SRX210 devices, the G.SHDSL ATM logical interface goes down when ATM CoS is enabled on the interface with OAM. As a workaround, restart the FPC to bring up the logical interface. [PR/472198]
- On J-SRX210 devices with VDLS2, ATM COS VBR related functionality cannot be tested because of lack of support from the vendor. [PR/474297]
- On J-SRX210 High Memory devices, IGMP v2 JOINS messages are dropped on an IRB interface. As a workaround, enable IGMP snooping to use IGMP over IRB interfaces. [PR/492564]
- On J-SRX210 devices, every time the VDSL2 PIM is restarted in the ADSL mode, the first packet passing through the PIM will be dropped. This occurs because there is a bug in the SAR engine, which will not set the ATM connection until the first packet has been dropped because of no ATM connection. [PR/493099]
- On all J-SRX Series devices, the destination and destination-profile options for address and unnumbered-address within family inet and inet6 are allowed to be specified within a dynamic profile but not supported. [PR/493279]
- On J-SRX210-High Memory devices, the physical interface module (PIM) shows time in ADSL2+ ANNEX-M, even though it is configured for ANNEX-M ADSL2. [PR/497129]
- On J-SRX100, J-SRX210, and J-SRX240 devices, whenever **radius-server** is configured under **profile** option radius server is marked as dead permanently if radius times out.

As a workaround, configure **radius-server** outside the **profile** option under access option. [PR/503717]

- On J-SRX100, J-SRX210, and J-SRX240 devices, egress queues are not supported on VLAN or IRB interfaces.[PR/510568]
- On J-SRX240 devices, IGMP reports are flooded on all ports which are part of the same multicast group, instead of sending it just on router interface. [PR/546444]

J-Web

- On J-SRX210 devices, there is no maximum length limit when the user commits the hostname in CLI mode; however, only a maximum of 58 characters are displayed in the J-Web System Identification panel. [PR/390887]
- On J-SRX210 and J-SRX240 devices, the complete contents of the ToolTips are not displayed in the J-Web Chassis View. As a workaround, drag the Chassis View image down to see the complete ToolTip. [PR/396016]
- On J-SRX100, J-SRX210, and J-SRX240 devices, the LED status in the Chassis View is not in sync with the LED status on the device. [PR/397392]
- On J-SRX Series devices, when you right-click **Configure Interface** on an interface in the J-Web Chassis View, the Configure > Interfaces page for all interfaces is displayed instead of the configuration page for the selected interface. [PR/405392]
- On J-SRX210 Low Memory devices, in the rear view of the Chassis viewer image, the image of ExpressCard remains the same whether a 3G card is present or not. [PR/407916]
- On J-SRX Series devices, the CLI Terminal feature does not work in J-Web over IPv6. [PR/409939]
- On J-SRX210 and J-SRX240 devices, when J-Web users select the tabs on the bottom-left menu, the corresponding screen is not displayed fully, so users must scroll the page to see all the content. This issue occurs when the computer is set to a low resolution. As a workaround, set the computer resolution to 1280 x 1024. [PR/423555]
- On J-SRX Series devices, users cannot differentiate between Active and Inactive configurations on the System Identity, Management Access, User Management, and Date & Time pages. [PR/433353]
- On J-SRX210 devices, in Chassis View, right-clicking any port and then clicking Configure Port takes the user to the Link aggregation page. [PR/433623]
- On J-SRX100 devices, in J-Web users can configure the scheduler without entering any stop date. The device submits the scheduler successfully, but the submitted value is not displayed on the screen or saved in the device. [PR/439636]
- On J-SRX100, J-SRX210, and J-SRX240 devices, in J-Web the associated **dscp** and **dscpv6** classifiers for a logical interface might not be mapped properly when the user edits the classifiers of a logical interface. This can affect the Delete functionality as well. [PR/455670]
- On J-SRX100, J-SRX210, and J-SRX240 devices, in J-Web, the options Input filter and Output Filter are displayed in VLAN configuration page. This feature is not supported,

and the user cannot obtain or configure any value under these filter options. [PR/460244]

- On J-SRX100, J-SRX210, and J-SRX240 devices, when you have a large number of static routes configured, and if you have navigated to pages other than to page 1 in the Route Information table in the J-Web interface (Monitor>Routing>Route Information), changing the Route Table to query other routes refreshes the page but does not return you to page 1. For example, if you run the query from page 3 and the new query returns very few results, the Route Information table continues to display page 3 with no results. To view the results, navigate to page 1 manually. [PR/476338]
- On J-SRX210 Low Memory, J-SRX210 High Memory, and J-SRX210 PoE devices, in the J-Web interface, Configuration>Routing>Static Routing does not display the IPv4 static route configured in rib inet.0. [PR/487597]
- On J-SRX100 (low memory and high memory), J-SRX210 (low memory, high memory, and PoE), J-SRX240 (low memory and high memory) devices, CoS feature commits occur without validation messages, even if you have not made any changes. [PR/495603]
- On J-SRX Series devices, in the J-Web interface, there is no support to change the T1 to E1 interface and vise versa. As a workaround, use the CLI to convert from T1 to E1 and vice versa. [PR/504944]
- On J-SRX100, J-SRX210, and J-SRX240 devices, in the J-Web interface running on Firefox 3.0, the resource utilization does not load any data in the dashboard page. [PR/564165]
- On J-SRX100, J-SRX210, and J-SRX240 devices, in the J-Web interface running on Firefox 3.0, Chassis Viewer sometimes fails to appear in J-Web. This behavior is inconsistent. [PR/564166]

Management and Administration

- On J-SRX240 devices, if a timeout occurs during the TFTP installation, booting the existing kernel using the boot command might crash the kernel. As a workaround, use the reboot command from the loader prompt. [PR/431955]
- On J-SRX240 devices, when you configure the system log hostname as 1 or 2, the device goes to the shell prompt. [PR/435570]
- On J-SRX240 devices, the **Scheduler Oinker** messages are seen on the console at various instances with various Mini-PIM combinations. These messages are seen during bootup, restarting fwdd, restarting chassisd, and configuration commits. [PR/437553]

Power over Ethernet (PoE)

- On J-SRX240 and J-SRX210 devices, the output of the PoE operational commands takes roughly 20 seconds to reflect a new configuration or a change in status of the ports. [PR/419920]
- On J-SRX210 PoE devices managing AX411 Access Points, the device might not be able to synchronize time with the configured NTP Server. [PR/460111]
- On J-SRX210 devices, the fourth access point connected to the services gateway fails to boot with the default PoE configuration. As a workaround, configure all the PoE

ports to a maximum power of 12.4 watts. Use the following command to configure the ports:
root#**set poe interface all maximum-power 12.4**
[PR/465307]

- On J-SRX100, J-SRX210, and J-SRX240 devices with factory default configurations, the device is not able to manage the AX411 Access Point. This might be due to the DHCP default gateway not being set. [PR/468090]
- On J-SRX210 PoE devices managing AX411 Access Points, traffic of 64 bytes at speed more than 45 megabits per second (Mbps), might result in loss of keepalives and reboot of the AX411 Access Point. [PR/471357]
- On J-SRX210 PoE devices, high latencies might be observed for the Internet Control Message Protocol (ICMP) pings between two wireless clients when 32 virtual access points (VAPs) are configured. [PR/472131]
- On J-SRX210 PoE devices, when AX411 Access Points managed by the J-SRX Series devices reboot, the configuration might not be reflected onto the AX411 Access Points. As a result, the AX411 Access Points retain the factory default configuration. [PR/476850]

Security

- On J-SRX210, if the Infranet Controller auth table mapping action is configured as **provision auth table as needed**, UAC terminates the existing sessions after Routing Engine failover. You might have to initiate new sessions. Existing sessions will not get affected after Routing Engine failover if the Infranet Controller auth table mapping action is configured as **always provision auth table**. [PR/416843]

Unified Threat Management (UTM)

- On J-SRX210 High Memory devices, content filtering provides the ability to block protocol commands. In some cases, blocking these commands interferes with protocol continuity, causing the session to hang. For instance, blocking the **FETCH** command for the IMAP protocol causes the client to hang without receiving any response. [PR/303584]
- On J-SRX210 High Memory devices, when the content filtering message type is set to **protocol-only**, customized messages appear in the log file. [PR/403602]
- On J-SRX210 High Memory devices, the express antivirus feature does not send a replacement block message for HTTP upload (POST) transactions if the current antivirus status is **engine-not-ready** and the fallback setting for this state is **block**. An empty file is generated on the HTTP server without any **block** message contained within it. [PR/412632]
- On J-SRX240 devices, Outlook Express is sending infected mail (with an EICAR test file) to the mail server (directly, not through DUT). Eudora 7 uses the IMAP protocol to download this mail (through DUT). Mail retrieval is slow, and the EICAR test file is not detected. [PR/424797]
- On J-SRX240 High Memory devices, FTP download for large files (> 4 MB) does not work in a two-device topology. [PR/435366]

- On J-SRX210 and J-SRX240 devices, the Websense server stops taking new connections after HTTP stress. All new sessions get blocked. As a workaround, reboot the Websense server. [PR/435425]
- On J-SRX240 devices, if the device is under UTM stress traffic for several hours, users might get the following error while using a UTM command:

  the utmd subsystem is not responding to management requests.

  As a workaround, restart the **utmd** process. [PR/436029]
- On J-SRX100 High Memory, J-SRX210 High Memory, and J-SRX240 High Memory devices, the antispam requests more than 1500 are not supported due to system limitation. [PR/451329]

Upgrade

- Low-impact ISSU chassis cluster upgrades are not supported in Junos OS Release 10.3. ISSU upgrade to 10.3 might cause loss of configuration. In order to upgrade to 10.3, use the normal upgrade procedure described in the *Junos OS Installation and Upgrade Guide* . [PR/526599 and PR/526829]

USB Modem

- On J-SRX210 High Memory devices, packet loss is seen during rapid ping operations between the dialer interfaces when packet size is more than 512 Kbps. [PR/484507]
- On J-SRX210 High Memory devices, the modem interface can handle bidirectional traffic of up to 19 Kbps. During oversubscription of 20 Kbps or more traffic, the keepalive packets are not exchanged and the interface goes down. [PR/487258]
- On J-SRX210 High Memory devices, IPv6 is not supported on dialer interfaces with a USB modem. [PR/489960]
- On J-SRX210 High Memory devices, http traffic is very slow through the umd0 interface. [PR/489961]
- On J-SRX210 High Memory devices, on multiple resets of the umd0 interface, the umd0 interface keeps flapping if the d10 (dialer) interface on either the dialin or dialout interface goes down because no keepalive packets are exchanged. As a workaround, increase the ATS0 value to 4 or greater. [PR/492970]
- On J-SRX210 High Memory devices, the D10 link flaps during long-duration traffic of 15-Kbps and also when packet size is 256 Kbps or more. [PR/493943]

Virtual LANs (VLANs)

- On J-SRX240 devices, tagged frames on an access port with the same VLAN tag are not dropped. [PR/414856]
- On J-SRX100, J-SRX210, and J-SRX240 devices, the packets are not being sent out of the physical interface when the VLAN ID associated with the VLAN interface is changed. As a workaround, you need to clear the ARP. [PR/438151]
- On J-SRX100 Low Memory, J-SRX100 High Memory, J-SRX210 Low Memory, J-SRX210 High Memory, and J-SRX240 High Memory devices, the Link Layer Discovery Protocol

(LLDP) organization specific Type Length Value (TLV), medium attachment unit (MAU) information always propagates as "Unknown". [PR/480361]

- On J-SRX100 High Memory devices and J-SRX210 Low Memory devices, dot1x unauthenticated ports accept Link Layer Discovery Protocol (LLDP) Protocol Data Units (PDUs) from neighbors. [PR/485845]
- For J-SRX210 High Memory devices, during configuration of access and trunk ports, the individual VLANs from the vlan-range are not listed. [PR/489872]

VPNs

- On J-SRX210 and J-SRX240 devices, concurrent login to the device from a different management systems (for example, laptop or computers) are not supported. The first user session will get disconnected when a second user session is started from a different management system. Also, the status in the first user system is displayed incorrectly as “Connected”. [PR/434447]
- On J-SRX Series devices, the site-to-site policy-based VPNs in a scenario of three or more zones will not work if the policies match the address “any”, instead of specific addresses, and all cross-zone traffic policies are pointing to the single site-to-site VPN tunnel. As a workaround, configure address books in different zones to match the source and destination, and use the address book name in the policy to match the source and destination. [PR/441967]
- On J-SRX100, J-SRX210, and J-SRX240 devices, Routing Engine level redundancy for dynamic VPN fails because the tunnels need to renegotiate after RG0 failover. [PR/513884]
- On J-SRX100, J-SRX210, and J-SRX240 devices, the dynamic VPN server always pushes the last configured dynamic client configuration to the client. If the VPN configuration bound to this dynamic VPN client is not bound to a policy, IKE negotiation will fail when you try to connect to the server. [PR/514033]
- On J-SRX100, J-SRX210, and J-SRX240 devices, the dynamic VPN client does not get downloaded if there is not enough space in the /jail/var directory in the dynamic VPN server. [PR/515261]

WLAN

- On J-SRX210, and J-SRX240 devices, J-Web online Help displays the list of all the countries and is not based on the regulatory domain within which the access point is deployed. [PR/469941]

Resolved Issues in Junos OS Release 10.3 for J-SRX Series Services Gateways

The following are the issues that have been resolved since Junos OS Release 10.3 for J-SRX Series Services Gateways. The identifier following the descriptions is the tracking number in our bug database.

Chassis Cluster

- On a J-SRX210 device in a chassis cluster, there was a loss of about 5 packets with 20 Mbps of UDP traffic on an RG0 failover. [PR/413642: This issue has been resolved.]

- On J-SRX240 devices in chassis cluster active/active preempt mode, the RTSP session broke after a primary node reboot and preempt failover. The following common ALGs were broken: RSH, TALK, PPTP, MSRPC, RTSP, SUNRPC, and SQL. [PR/448870: This issue has been resolved.]

Command-Line Interface (CLI)

- On J-SRX210 High Memory devices, the help description for the **set interface int arp-resp** command incorrectly stated the default value as 'unrestricted'. The default value was actually 'restricted'. [PR/530323: This issue has been resolved.]
- On J-SRX210 devices, packet drop was seen while prioritizing multiple data streams configured with same multilink class on single-member link ML bundles that were configured between the J-SRX Series devices and other types of devices. [PR/539449: This issue has been resolved.]

Flow and Processing

- On J-SRX240 PoE devices, packet drops were seen on the lsq interface when transit traffic with a frame length of 128 bytes was sent. [PR/455714: This issue has been resolved.]

Hardware

- On J-SRX210 devices, the system took between 2 and 5 minutes to initialize. [PR/298635: This issue has been resolved.]
- On J-SRX240 devices, when users swapped the USBs after startup, the chassis-control subsystem did not respond to any chassis-related commands. [PR/437798: This issue has been resolved.]
- On J-SRX210 Low Memory devices, 3G AC402 Live Network Card activation got timed out. [PR/451493: This issue has been resolved.]

Interfaces and Routing

- On J-SRX Series devices, If you configured attributes of an interface unit under both the [**interfaces**] and the [logical-router **logical-router-name interface**] hierarchies, only the configuration at the interfaces level took effect. [PR/447986: This issue has been resolved.]
- On J-SRX210 High Memory devices, the GRE tunnel session was not created properly and the tunnel outgoing interface took a long time to come up. On T1/E1 interfaces of J-SRX100, J-SRX210, and J-SRX240 devices, traffic through the GRE tunnel did not work. [PR/497864: This issue has been resolved.]
- On J-SRX210 and J-SRX240 devices, when you activated or deactivated the ATM interface for the VDSL PIM inserted on slots 2, 3, or 4, a flowd crash occurred because of a bug in the VDSL driver. [PR/505347: This issue has been resolved.]
- On J-SRX240 devices, MAC address changes for VLAN interface were not supported. [PR/518934: This issue has been resolved.]

J-Web

- On J-SRX Series devices, when the user tried to associate an interface to GVRP, a new window appeared. This new window showed multiple move-left and move-right buttons. [PR/305919: This issue has been resolved.]
- On J-SRX100, J-SRX210, and J-SRX240 devices, in J-Web configuration for the routing feature, if you entered double quotation marks in the text boxes that accepted characters (for example, protocol name, filename, and description), then you could not delete the data with double quotation marks through J-Web. [PR/464030: This issue has been resolved.]
- On J-SRX Series devices, in the J-Web interface, the **ui show** or **ui compare** Junos XML protocol RPC commands generated some unnecessary debug messages. [PR/514540: This issue has been resolved.]

Network Address Translation (NAT)

- On J-SRX240 High Memory devices in a chassis cluster, the secondary node could go to **DB>** mode when there were many policies configured and TCP, UDP, and ICMP traffic matched the policies. [PR/493095: This issue has been resolved.]
- On J-SRX Series devices, Remote Procedure Call (RPC) did not work with source NAT configuration. [PR/515455: This issue has been resolved.]
- On J-SRX100 and J-SRX210 High Memory devices, h323/h245 OLC could not pass whether **src nat** or **dst nat**. [PR/538764: This issue has been resolved.]
- On J-SRX100 High Memory devices, for "nat source" with "port no-translation", the configured source-pool IP addresses were divided into half and they were exclusively used on each node. However, when multiple groups of source-pool IP addresses were configured, the half-divided logic did not work properly, and it resulted in an unexpectedly insufficient IP address (from source-pool) for a node. [PR/538769: This issue has been resolved.]

Power over Ethernet (PoE)

- On J-SRX240 PoE devices, during failover, on the secondary node the ADSL Mini-PIM restarted and took about 3-4 minutes to come up. [PR/528949: This issue has been resolved.]

Security

- On J-SRX240 High Memory devices, when you committed a configuration change that added a security policy that contained a DNS address object, the device would core if the DNS address object was unresolved to an IP address. [PR/ 542175: This issue has been resolved.]
- On J-SRX240 high memory devices, the device rebooted unexpectedly after execute 'commit' command with predefined-attack-groups changes that included **Solaris - Services - All** attack group. [PR/546705: This issue has been resolved.]

Virtual LANs (VLANs)

- On J-SRX240 devices, the Layer 3 traffic with VLAN ID 4093 was allowed but did not forward traffic over that interface. [PR/539580: This issue has been resolved.]

VPNs

- On J-SRX Series devices, Remote Procedure Call (RPC) did not work with the policy VPN. VPN tunnel information was not set when resources were created and when uuid was not in the uuid_2_oid table, the ALG would not open a pinhole. [PR/504576: This issue has been resolved.]

WLAN

- On J-SRX Series devices, when WLAN configuration was committed, it took a while before the configuration was reflected on the access point, depending on the number of virtual access points and the number of access points connected. [PR/450230: This issue has been resolved.]

Related Documentation

- New Features in Junos OS Release 10.3 for J-SRX Series Services Gateways on page 4
- Known Limitations in Junos OS Release 10.3 for J-SRX Series Services Gateways on page 24
- Errata and Changes in Documentation for Junos OS Release 10.3 for J-SRX Series Services Gateways on page 42

Errata and Changes in Documentation for Junos OS Release 10.3 for J-SRX Series Services Gateways

Changes to the Junos Documentation Set

This section lists changes in the documentation.

Single Commit on J-Web

The following information pertains to J-SRX Series devices:

- For all J-Web procedures, follow these instructions to commit a configuration:
  - If Commit Preference is **Validate and commit configuration changes**, click **OK**.

- If Commit Preference is **Validate configuration changes**, click **OK** to check your configuration and save it as a candidate configuration, then click **Commit Options**>**Commit**.

J-Web Online Help

- Previously, J-Web online Help instructions were available both in the Help and in the administration and configuration guides. These topics have been removed from the guides and are now only available in the online Help.

Interfaces and Routing Guide

The *Junos OS Interfaces and Routing Guide* has been divided into five smaller guides to make it easier for readers to find information:

- *Junos OS Class of Service Configuration Guide for Security Devices*
- *Junos OS Interfaces Configuration Guide for Security Devices*
- *Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices*
- *Junos OS MPLS Configuration Guide for Security Devices*
- *Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*

The five books above include all of the information that the original *Junos OS Interfaces and Routing Guide* included. The *Junos OS Interfaces and Routing Guide* is itself, however, no longer available as of Junos 10.3.

Errata for the Junos OS Software Documentation

This section lists outstanding issues with the software documentation.

Feature Support Reference for SRX Series and J Series Devices

- The *Feature Support Reference for SRX Series and J Series Devices* on page 9, Table 6 for ALG Support erroneously states that J-SRX100, J-SRX210, and J-SRX240 do not support the DNS, FTP, RTSP, and TFTP ALGs (Layer 2) with chassis clustering feature.
  The correct information for this section is:
  J-SRX100, J-SRX210, and J-SRX240 support the DNS, FTP, RTSP, and TFTP ALGs (Layer 2) with chassis clustering feature.
- The *Feature Support Reference for SRX Series and J Series Devices* on page 12, Table 10 for Chassis Cluster Support erroneously states that only J-SRX100 and J-SRX210 support the Application Layer Gateways (ALGs) feature.
  The correct information for this section is:
  J-SRX100, J-SRX210, and J-SRX240 support the Application Layer Gateways (ALGs) feature.
- The *Feature Support Reference for SRX Series and J Series Devices* on page 16, Table 15 for Ethernet Link Aggregation Support erroneously states that J-SRX100, J-SRX210, and J-SRX240 do not support Link aggregation in chassis cluster mode.
  The correct information for this section is:

J-SRX100, J-SRX210, and J-SRX240 support the Link aggregation in chassis cluster mode feature.

- The *Feature Support Reference for SRX Series and J Series Devices* on page 31, Table 27 for MPLS Support erroneously states that only J-SRX240 supports the Connectionless Network Service (CLNS) feature.
  The correct information for this section is:
  J-SRX100, J-SRX210, and J-SRX240 support the Connectionless Network Service (CLNS) feature.

J-Web

- **J-Web security package update Help page**—The J-Web Security Package Update Help page does not contain information about download status.
- **J-Web pages for stateless firewall filters**—There is no documentation describing the J-Web pages for stateless firewall filters. To find these pages in J-Web, go to **Configure>Security>Firewall Filters**, then select **IPv4 Firewall Filters** or **IPv6 Firewall Filters**. After configuring filters, select **Assign to Interfaces** to assign your configured filters to interfaces.
- **J-Web Configuration Instructions**— Because of ongoing J-Web interface enhancements, some of the J-Web configuration example instructions in the administration and configuration guides became obsolete and thus were removed. For examples that are missing J-Web instructions, use the provided CLI instructions.

Security Configuration Guide

- ALG configuration examples in the *Junos OS Security Configuration Guide* incorrectly show policy-based NAT configurations. NAT configurations are now rule-based.
- The "Verifying the Policy Compilation and Load Status" section of the *Junos OS Security Configuration Guide* has a missing empty/new line before the **IDPD Trace file** heading, in the second sample output.
- When specifying a forwarding target after authentication on a captive portal, use the **?target=** option followed by either the **%dest-url%** variable or a specific URL. The **%dest-url%** variable forwards authenticated users to the protected resource they originally specified. A URL forwards authenticated users to a specific site.

  Note that when entering a URL with the **?target=** option, you must substitute escape characters for any special characters in the URL. Use the following escape characters for these common special characters:

  - Replace **:** with **%3A**
  - Replace **/** with **%2F**
  - Replace **-** with **%2D**
  - Replace **.** with **%2E**

  In the section "Example: Configuring a Redirect URL for Captive Portal (CLI)" in the *Junos OS Security Configuration Guide*, the procedure description states that, after authentication, users will be forwarded to the specified URL. Step 2 of the configuration

procedure, however, is incorrect. This command would forward users to my-website.com before authentication, not after.

To redirect users after authentication, the command must include:

- The IP address of the Infranet Controller to be used for authentication
- The **?target=** option and URL to distinguish a forwarding address to be used after authentication
- Escape characters substituted for any special characters in the URL name

The following text in Step 2 is incorrect:

```
[edit services unified-access-control]
user@host# set captive-portal my-captive-portal-policy redirect-url
  https://my-website.com
```

The correct text for Step 2 is as follows:

```
[edit services unified-access-control]
user@host# set captive-portal my-captive-portal-policy redirect-url
  https://192.168.0.100/?target=my%2Dwebsite%2Ecom
```

- In the “Example: Configuring an IPsec Phase 2 Proposal (CLI)” section of the *Junos OS Security Configuration Guide*, the second paragraph of the first example states that the SA, “. . . terminates after 1800 KB of data pass through it.” It should instead say, “. . . after 1800 seconds.”
- In the “Example: Accommodating End-to-End TCP Communication for J Series Services Routers” section of the *Junos OS Security Configuration Guide*, one CLI command given in the example in both the CLI Quick Configuration and Step-by-Step Procedure is incomplete. The **set security flow tcp-mss all-tcp** command must be followed by the keyword **mss value**. Therefore, the CLI example in both cases should read **set security flow tcp-mss all-tcp mss 1400.**
- In the section "Example: Using NAT and the H.323 ALG to Enable Incoming Calls (CLI)" in the *Junos OS Security Configuration Guide*, the following text is incorrect:
  user@host# set security policy from-zone zone1 to-zone zone2 policy zone1_to_zone2 then permit source-nat pool p1
  The correct text is as follows:
  user@host# set security policy from-zone zone1 to-zone zone2 policy zone1_to_zone2 then permit
- The “Using NAT and the H.323 ALG to Enable Incoming Calls” example uses the old NAT version. The example has been revised to use the new NAT version in Junos OS Release 10.4.
- The “Configuring Static NAT for Incoming SIP Calls” example incorrectly states the command to configure static NAT as **set security nat interface ge-0/0/2.0 static-nat 1.1.1.3/32 host 10.1.1.3/32**. The example has been reworked in Junos OS Release 10.4.

Errata for the Junos OS Hardware Documentation

This section lists outstanding issues with the hardware documentation.

Quick Start Guides

- The following J-SRX Series Quick Start Guides erroneously provide an IP address of 192.168.1/24 in the "Part 4: Ensure That the Management Device Acquires an IP Address" section:
  - *J-SRX100 Services Gateway Quick Start Guide*
  - *J-SRX210 Services Gateway Quick Start Guide*
  - *J-SRX240 Services Gateway Quick Start Guide*

  The correct IP address in this section is 192.168.1.0/24.

J-SRX100 Services Gateway Hardware Guide

- The output for the **show chassis hardware** and **show chassis hardware detail** commands is incorrectly documented for the Routing Engine field. The following table provides details of the guide, section, incorrect output, and corrected output for these commands.

Section	Incorrect Value in the Hardware Guide	Correct Value Displayed in the Command Output
Monitoring the J-SRX100 Services Gateway Chassis Using the CLI	RE-J-SRX100-HM	RE-J-SRX100H
Locating the J-SRX100 Services Gateway Component Serial Number and Agency Labels	RE-J-SRX100-HIGHMEM	RE-J-SRX100H

- The "Understanding Built-In Ethernet Ports" section in the *J-SRX100 Services Gateway Hardware Guide* erroneously states the following:

  The services gateway acts as a DHCP client out of the built-in Ethernet ports. If the services gateway does not find a DHCP server within a few seconds, the device acts as a DHCP server and assigns an IP address as 192.168.1.1/24. With the device temporarily acting as a DHCP server, you can manually configure it with the J-Web interface.

  The correct information for this section is as follows: The services gateway acts as a DHCP client on port fe-0/0/0, and ports fe-0/0/1 to fe-0/0/7 act as a DHCP server.

- The "Upgrading the J-SRX100 Services Gateway Low Memory Version to a High Memory Version" section in the *J-SRX100 Services Gateway Hardware Guide* is missing the following information:

  The J-SRX100 Services Gateway High Memory model is shipped with the license key.

J-SRX210 Services Gateway Hardware Guide

- The output for the **show chassis hardware** and **show chassis hardware detail** commands is incorrectly documented for the Routing Engine field. The following table provides details of the guide, section, incorrect output, and corrected output for these commands.

Section	Incorrect Value in the Hardware Guide	Correct Value Displayed in the Command Output
Monitoring the J-SRX210 Services Gateway Chassis Using the CLI	RE-J-SRX210-LOWMEM	RE-J-SRX210B
Locating the J-SRX210 Services Gateway Component Serial Number and Agency Labels	RE-J-SRX210-LOWMEM	RE-J-SRX210B

- The "Understanding Built-In Ethernet Ports" section in the *J-SRX210 Services Gateway Hardware Guide* erroneously states the following:

  The services gateway acts as a DHCP client out of the built-in Ethernet ports. If the services gateway does not find a DHCP server within a few seconds, the device acts as a DHCP server and assigns an IP address as 192.168.1.1/24. With the device temporarily acting as a DHCP server, you can manually configure it with the J-Web interface.

  The correct information for this section is as follows: The services gateway acts as a DHCP client on port ge-0/0/0 and ports ge-0/0/1 and fe-0/0/2 to fe-0/0/7 act as a DHCP server.

- **Installing Software Packages**—The current *J-SRX210 Services Gateway Hardware Guide* does not include the following information:

  On J-SRX210 devices, the **/var** hierarchy is hosted in a separate partition (instead of the *root* partition). If Junos OS installation fails as a result of insufficient space:

  1. Use the **request system storage cleanup** command to delete temporary files.
  2. Delete any user-created files both in the *root* partition and under the **/var** hierarchy.

J-SRX240 Services Gateway Hardware Guide

- The output for the **show chassis hardware** and **show chassis hardware detail** commands is incorrectly documented for the Routing Engine field. The following table provides details of the guide, section, incorrect output, and corrected output for these commands.

Section	Incorrect Value in the Hardware Guide	Correct Value Displayed in the Command Output
Monitoring the J-SRX240 Services Gateway Chassis Using the CLI	RE-J-SRX240-LM	RE-J-SRX240B
Locating the J-SRX240 Services Gateway Component Serial Number and Agency Labels	RE-J-SRX240-POE	RE-J-SRX240H-POE

- The "Understanding Built-In Ethernet Ports" section in the *J-SRX240 Services Gateway Hardware Guide* erroneously states the following:

  The services gateway acts as a DHCP client out of the built-in Ethernet ports. If the services gateway does not find a DHCP server within a few seconds, the device acts as a DHCP server and assigns an IP address as 192.168.1.1/24. With the device temporarily acting as a DHCP server, you can manually configure it with the J-Web interface.

  The correct information for this section is as follows: The services gateway acts as a DHCP client on port ge-0/0/0, and ports ge-0/0/1 to ge-0/0/15 act as a DHCP server.

- The "J-SRX240 Services Gateway (High Memory with DC Power Supply Model) Compliance Statements for Network Equipment Building System (NEBS)" section in the *J-SRX240 Services Gateway Hardware Guide* incorrectly states that the battery return connection is to be treated as a Common DC return (DC-C), as defined in GR-1089-CORE.

  The guide should state that the battery return connection is to be treated as an Isolated DC return (DC-I), as defined in GR-1089-CORE.

- The *J-SRX240 Services Gateway Hardware Guide* is missing information about the following statements and data:

  - The "J-SRX240 Services Gateway Site Electrical Wiring Guidelines" section should include the following statement:

    For devices with AC power supplies, an external surge protective device (SPD) must be used at the AC power source.

  - The "General Electrical Safety Guidelines and Warnings" section should include the following statements:

    

    WARNING: Use copper conductors only.

    Waarschuwing Gebruik alleen koperen geleiders.

    Varoitus Käytä vain kuparijohtimia.

Attention Utilisez uniquement des conducteurs en cuivre.

Warnung Verwenden Sie ausschließlich Kupferleiter.

Avvertenza Usate unicamente dei conduttori di rame.

Advarsel Bruk bare kobberledninger.

Aviso Utilize apenas fios condutores de cobre.

¡Atención! Emplee sólo conductores de cobre.

Varning! Använd endast ledare av koppar.

- The “Grounding the J-SRX240 Services Gateway” section should list the following as tools and the parts required for grounding the J-SRX240 device:
  - Grounding cable for your device—The grounding cable must be minimum 14 AWG (2 mm^2), minimum 90ºC wire, or as permitted by the local code.
  - Grounding lug—Ring-type, vinyl-insulated TV14-6R lug or equivalent for your grounding cable.
  - Washers and 10-32x.25-in. screws to secure the grounding lug to the protective earthing terminal.
  - Phillips (+) screwdrivers, numbers 1 and 2.
- The “Grounding the J-SRX240 Services Gateway” section should include the following information in the grounding instructions step:

  Step 6 - Secure the grounding cable lug to the grounding point with the screw. Apply between 6 lb-in. (0.67 Nm) and 8 lb-in. (0.9 Nm) of torque to the screws.
- The “J-SRX240 Services Gateway Installation Safety Guidelines and Warnings” section should specify that the J-SRX240 Services Gateway can be installed as customer premises equipment (CPE) only.
- The “J-SRX240 Services Gateway (High Memory with DC Power Supply Model) Compliance Statements for Network Equipment Building System (NEBS)” section should specify the following statement:

  The battery return connection is to be treated as an Isolated DC return (DC-I), as defined in GR-1089-CORE.
- The “J-SRX240 Services Gateway Installation Instructions Warning’ section in Appendix J-SRX240 Services Gateway Installation Safety Guidelines and Warnings should specify the following statements:
  - Before you make any crimp connections, coat all conductors (frame ground, battery, and battery return) with an appropriate antioxidant compound. Before you connect unplated connectors, braided strap, and bus bars, bring them to a bright finish and coat them with an antioxidant compound. You do not have to

prepare tinned, solder-plated, or silver-plated connectors or other plated connection surfaces before connecting them, but make sure such surfaces remain clean and free of contaminants. To provide a permanent low-impedance path, tighten all raceway fittings.

- An electrical conducting path shall exist between the device chassis and the grounding conductor, or between the chassis and the metal surface of the enclosure or rack in which the device is mounted. Electrical continuity shall be provided by the use of thread-forming-type, unit-mounting screws that remove any paint or nonconductive coatings and establish metal-to-metal contact. Any paint or other nonconductive coatings shall be removed on the surfaces between the mounting hardware and the enclosure or rack. The surfaces shall be cleaned and an antioxidant applied before installation.

J-SRX Series Services Gateways for the Branch Physical Interface Modules Hardware Guide

- The *J-SRX Series Services Gateways for the Branch Physical Interface Modules Hardware Guide* erroneously lists the maximum MTU (bytes) for the Serial Mini-PIM as 1504. The correct value for this section is 2000.
- The "DOCSIS Mini-Physical Interface Module" chapter in the *J-SRX Series Services Gateways for the Branch Physical Interface Modules Hardware Guide* erroneously states that the EuroDOCSIS 3.0 and the DOCSIS J (Japan) models of the DOCSIS Mini-PIM are supported. The guide should state that only the DOCSIS 3.0 U.S. model of the DOCSIS Mini-PIM is supported.

Related Documentation

- New Features in Junos OS Release 10.3 for J-SRX Series Services Gateways on page 4
- Known Limitations in Junos OS Release 10.3 for J-SRX Series Services Gateways on page 24
- Issues in Junos OS Release 10.3 for J-SRX Series Services Gateways on page 29

Hardware Requirements for Junos OS Release 10.3 for J-SRX Series Services Gateways

- Transceiver Compatibility for J-SRX Series Devices on page 50

Transceiver Compatibility for J-SRX Series Devices

We recommend the use of transceivers compatible with the Junos OS. We cannot guarantee that the interface module will operate correctly if tranceivers are not compatible with the Junos OS. Please contact Dell for the correct transceiver part number for your device.

Stream Control Transmission Protocol Overview

Stream Control Transmission Protocol (SCTP) is an IP Transport Layer protocol. SCTP is a reliable transport protocol operating on top of a connectionless packet network such as IP and supports data transfer across the network in single IP or multi-IP cases. SCTP provides the following services:

- Aggregate Server Access Protocol (ASAP)
- Bearer Independent Call Control (BICC)
- Direct Data Placement Segment chunk (DDP-segment)
- Direct Data Placement Stream session control (DDP-stream)
- DPNSS/DASS 2 extensions to IUA Protocol (DUA)
- Endpoint Handleescape Redundancy Protocol (ENRP)
- H.248 Protocol (H248)
- H.323 Protocol (H323)
- ISDN User Adaptation Layer (IUA)
- MTP2 User Peer-to-Peer Adaptation Layer (M2PA)
- MTP2 User Adaptation Layer (M2UA)
- MTP3 User Adaptation Layer (M3UA)
- Q.IPC
- Reserved
- Simple Middlebox Configuration (SIMCO)
- SCCP User Adaptation Layer (SUA)
- Transport Adapter Layer Interface (TALI)
- v5.2 User Adaptation Layer (V5UA)

SCTP can transport signaling messages to and from Signaling System 7 (SS7) for 3G mobile network through M3UA, M2UA or SUA. SCTP is a packet-based transport protocol. SCTP provide reliable and secure transport, minimized end-to-end delay, short failover time in case of network failures and both sequence and no-sequence transport.

Configuration Overview

You should configure at least one SCTP profile to enable the security device to perform stateful inspection on all SCTP traffic. The stateful inspection of SCTP traffic will drop some anomalous SCTP packets. The SCTP firewall supports deeper inspection:

- **Packet filtering**—The profile configuration of drop packets for special SCTP payload protocol and M3UA service enables packet filtering.
- **Limit-rate**—Controls the packets rate of SCCP in M3UA service.

The SCTP deeper inspection requires the following steps:

- Creating an SCTP profile
- Configuring the filtering and limiting parameters
- Binding the SCTP profile to a policy

NOTE: The policy should permit SCTP traffic.

Upgrade and Downgrade Instructions for Junos OS Release 10.3 for J-SRX Series Services Gateways

In order to upgrade to Junos OS Release 10.3 or later, your device must be running Junos OS Release 10.1R2 or later.

For additional upgrade and download information, see the *Junos OS Administration Guide for Security Devices* and the *Junos OS Migration Guide*.

Junos OS Release Notes for Dell PowerConnect J-EX Series Ethernet Switches

New Features in Junos OS Release 10.3 for J-EX Series Ethernet Switches

New features in Release 10.3 of Junos OS for J-EX Series Ethernet switches are described in this section.

Not all J-EX Series software features are supported on all J-EX Series Ethernet switches in the current release. For a list of all J-EX Series software features and their platform support, see the software overview information in the Dell PowerConnect J-EX Series Ethernet Switch Complete Software Guide for Junos OS at http://www.support.dell.com/manuals.

New features are described on the following pages:

Access Control and Port Security

- **Captive portal authentication functionality enhancements**—Limitations on captive portal authentication functionality are removed. Captive portal functionality no longer requires that a routed VLAN interface (RVI) be created or that the switch's DHCP gateway IP address be configured as the IP address of the RVI.

Captive portal authentication can now be configured on the same interface with both 802.1X and MAC RADIUS authentication. Authentication fallback is enabled on an interface on which more than one type of authentication is configured. Captive portal authentication is supported on J-EX4200 switches.

- **MAC RADIUS authentication on J-EX8200 switches**—All MAC RADIUS authentication functionality available on J-EX4200 switches is extended to J-EX8200 switches.
- **Additional 802.1X features support on J-EX8200 switches**—Support for the following features related to 802.1X that are available on J-EX4200 switches is extended to J-EX8200 switches:
  - Static MAC bypass of authentication
  - Guest VLANs
  - Per-user firewall filters
  - Voice VLAN assignments
  - Vendor-specific attributes (VSAs)

Layer 2 and Layer 3 Protocols

- **IPSec support for OSPFv3**—IPSec can be used to secure OSPFv3 interfaces and protect OSPFv3 virtual links by authenticating and encrypting each IP packet of a data stream.
- **IGMP snooping EXCLUDE modes**—IGMP snooping now supports IGMPv3 EXCLUDE and EXCLUDE NULL modes.
- **Layer 2 protocol tunneling**—L2PT on J-EX Series Ethernet switches now supports unidirectional link detection (UDLD)

Management and RMON

- **Remote performance monitoring (RPM) enhancements**—To specify timestamping of RPM probes icmp-ping, icmp-ping-timestamp, udp-ping, and udp-ping-timestamp, you can configure hardware timestamps on the requester.
- **SNMP MIB enhancements**—Power supply MIB definitions have been introduced for monitoring and managing power on a J-EX Series Ethernet switch.

Packet Filters

- **Firewall filters with dynamic TCAM allocation on J-EX8200 switches**—Dynamic allocation of ternary content addressable memory (TCAM) to firewall filters is supported on J-EX8200 switches.
- **Firewall filter IPv6 support on J-EX8200 switches**—Firewall filters for IPv6 traffic are now supported on J-EX8200 switches.

Related Documentation

- Changes in Default Behavior and Syntax in Junos OS Release 10.3 for J-EXSeries Ethernet switches on page 54
- Limitations in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 54

- Outstanding Issues in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 57
- Resolved Issues in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 60
- Errata in Documentation for Junos OS Release 10.3 for J-EX Series Ethernet switches on page 63

Changes in Default Behavior and Syntax in Junos OS Release 10.3 for J-EX Series Ethernet Switches

Interfaces

- The default for the PoE management mode has been changed from static mode to class mode.

Related Documentation

- New Features in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 52
- Limitations in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 54
- Outstanding Issues in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 57
- Resolved Issues in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 60
- Errata in Documentation for Junos OS Release 10.3 for J-EX Series Ethernet switches on page 63

Limitations in Junos OS Release 10.3 for J-EX Series Ethernet Switches

This section lists the limitations in Junos OS Release 10.3R2 for J-EX Series Ethernet switches.

Access Control and Port Security

- When you have configured more than 1024 supplicants on a single interface, 802.1X authentication might not work as expected and the 802.1X process (**dot1xd**) might fail.
- The RADIUS request sent by a J-EX Series Ethernet switch contains both Extensible Authentication Protocol (EAP) Identity Response and State attributes.
- When an external RADIUS server goes offline and comes back online after some time, subsequent captive portal authentication requests might fail until the **authd** daemon is restarted. As a workaround, configure the revert interval—the time after which to revert to the primary server—and restart the **authd** daemon.

Bridging, VLANs, and Spanning Trees

- On J-EX Series Ethernet switches, configuring more than 64,000 MAC address clone routes in a single VLAN causes the Routing Engine to create core files and reboot.

Class of Service

- On J-EX8200 switches, classification of packets using ingress firewall filter rules with forwarding-class and loss-priority configurations does not rewrite the DSCP or 802.1p

bits. Rewriting of packets is determined by the forwarding-class and loss-priority values set in the DSCP classifier applied on the interface.

- On J-EX4200 switches, the traffic is shaped at rates above 500 Kbps, even when the shaping rate configured is less than 500 Kbps.

Firewall Filters

- On J-EX4200 switches, when interface ranges or VLAN ranges are used in configuring firewall filters, egress firewall filter rules take more than 5 minutes to install.
- On J-EX4200 switches, IGMP packets are not matched by user-configured firewall filters.

Hardware

- If you press the reset button on the Switch Fabric and Routing Engine (SRE) module in a J-EX8208 switch without taking the module offline first (using the CLI), the fabric planes in the module might not come back online.

Infrastructure

- On J-EX Series Ethernet switches, an SNMP query fails when the SNMP index size of a table is greater than 128 bytes, because the Net SNMP tool does not support SNMP index sizes greater than 128 bytes.
- On J-EX Series Ethernet switches, the **show snmp mib walk etherMIB** command does not display any output, even though the **etherMIB** is supported. This occurs because the values are not populated at the module level—they are populated at the table level only. You can issue **show snmp mib walk dot3StatsTable**, **show snmp mib walk dot3PauseTable**, and **show snmp mib walk dot3ControlTable** commands to display the output at the table level.
- When you issue the **request system power-off** command, the switch halts instead of turning off power.
- In the J-Web interface, the Ethernet Switching monitoring page might not display monitoring details if there are more than 13,000 MAC entries on the switch.
- In the J-Web interface, changing the port role from Desktop, Desktop and Phone, or Layer 2 Uplink to another port role might not remove the configurations for enabling dynamic ARP inspection and DHCP snooping.
- On J-EX8200 switches, if IS-IS is enabled on routed VLAN interfaces (RVIs), IS-IS adjacency states go down and come up after a graceful Routing Engine switchover (GRES).
- Momentary loss of an inter-Routing Engine IPC message might trigger the alarm that displays the message **Loss of communication with Backup RE**. There is no functionality affected.

Interfaces

- J-EX Series Ethernet switches do not support queued packet counters. Therefore, the queued packet counter in the output of the **show interfaces *interface-name* extensive** command always displays a count of 0 and is never updated.
- The following message might appear in the system log:

  ```
  Resolve request came for an address matching on Wrong nh nh:355,
  type:Unicast...?
  ```

  You can ignore this message.
- On J-EX4200 switches, when port mirroring is configured on any interface, the mirrored packets leaving a tagged interface might contain an incorrect VLAN ID.
- On J-EX8200 switches, port mirroring configuration is not supported on a Layer 3 interface with the output configured to a VLAN.
- On J-EX8200 switches, when an egress VLAN that belongs to a routed VLAN interface (RVI) is configured as the input for a port mirroring analyzer, the analyzer incorrectly appends a dot1q (802.1Q) header to the mirrored packets or does not mirror any packets at all. As a workaround, configure a port mirroring analyzer with each port of the VLAN as egress input.
- The following interface counters are not supported on routed VLAN interfaces (RVIs): local statistics, traffic statistics, and transit statistics.
- J-EX Series Ethernet switches do not support IPv6 interface statistics. Therefore, all values in the output of the **show snmp mib walk ipv6IfStatsTable** command always display a count of 0.
- The **show interfaces *interface-name* detail | extensive** command might display double counting of packets or bytes for the transit statistics and traffic statistics counters. You can use the counter information displayed under the **Physical interface** section of the output.

J-Web Browser Support

- **J-Web Browser Support for Your Dell PowerConnect J-Series Devices**—To access the J-Web interface for all platforms, your management device requires the following Windows operating system and browsers:
  - Operating System: Microsoft Windows XP Service Pack 3
  - Browser: Microsoft Internet Explorer version 7.0 or Mozilla Firefox version 3.0

  

  NOTE: Other browser versions may work but are not supported.

  

  NOTE: Only English-version browsers are supported.

NOTE: For both J-SRX and J-EX devices, the browser and the network must support receiving and processing HTTP 1.1 GZIP compressed data.

Layer 2 and Layer 3 Protocols

- On J-EX8200 switches, ensure that the **bfd-liveness-detection** timers are set no lower than 500 milliseconds.

Related Documentation

- New Features in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 52
- Changes in Default Behavior and Syntax in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 54
- Outstanding Issues in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 57
- Resolved Issues in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 60
- Errata in Documentation for Junos OS Release 10.3 for J-EX Series Ethernet switches on page 63

Outstanding Issues in Junos OS Release 10.3 for J-EX Series Ethernet Switches

The following are outstanding issues in Junos OS Release 10.3R2 for J-EX Series Ethernet switches. The identifier following the description is the tracking number in our bug database.

Access Control and Port Security

- On J-EX Series Ethernet switches, when you enable and disable IPv6 on the management interface (**me0**), the management information is not displayed in the **show lldp local-information** command output. [PR/503955]
- On J-EX4200 switches, EAP-TTLS authentication with a server-reject-vlan configuration might not work. [PR/506918]

Bridging, VLANs, and Spanning Trees

- If you modify MSTP configuration and VLAN membership for an interface, those changes can result in an inconsistent MSTP membership for that interface. As a workaround, restart the Ethernet switching process (eswd) after committing the configuration. [PR/525507]

Infrastructure

- On J-EX8200 switches, when IGMP snooping is enabled on an interface, the IPv6 multicast Layer 2 control frame is not forwarded to other interfaces in the same VLAN. [PR/456700]
- If you configure a large number of VLANS and aggregated Ethernet interfaces and commit the configuration, the forwarding process (**pfem**) utilization stays at 80 percent

for more than 60 minutes. As a result, the aggregated Ethernet interfaces cannot be used until the **pfem** usage reduces to normal limits. [PR/544433]

- When an IGMP version 3 group-specific report is sent to a VLAN in a J-EX4200 switch, the switch sends back the Group and Source-Specific Queries (GSSQ) message to the intended receivers only, instead of flooding the message to all members of that VLAN. This problem occurs because the switch uses the standard forwarding database (FDB) lookup scheme to send out the GSSQ message and does not flood the VLAN. [PR/560945]
- On J-EX8200 switches, the routing protocol process might crash because some PIM-enabled interfaces are reusing SNMP indexes, which disables interfaces and IPv6 routing instances. [PR/561042]

Interfaces

- On J-EX8200 switches, aggregated Ethernet interfaces might go down and come back up for a few minutes while the switch is updating many routes. [PR/416976]
- On J-EX8200 switches, when a firewall filter is applied on the loopback (**lo0**) interface, the switch stops generating local ARP requests for transit traffic. As a workaround, do the following:
  - Create firewall filters to block known unwanted traffic to the Routing Engine, and then accept all other traffic.
  - Create firewall filters for specific hosts and all local subnets, and then discard all other traffic.

  [PR/486443]

J-Web Interface

- In the J-Web interface, you cannot commit some configuration changes in the Ports Configuration page and the VLAN Configuration page because of the following limitations for port mirroring ports and port mirroring VLANs:
  - A port configured as the output port for an analyzer cannot be a member of any VLAN other than the default VLAN.
  - A VLAN configured to receive analyzer output can be associated with only one port.

  [PR/400814]
- J-Web does not provide a way to upload a Junos OS package to the backup Routing Engine. As a workaround, use the CLI command **request system software** add to upload Junos OS packages to the switch. For details, see "Installing Software on a J-EX8200 Switch with Redundant Routing Engines (CLI Procedure)" in the *Dell PowerConnect J-Series Ethernet Switch Complete Software Guide for Junos OS Release 10.3.* [PR/402109]
- If an SRE module, RE module, SF module, line card, or Virtual Chassis member is in offline mode, the J-Web interface might not update the dashboard image accordingly. [PR/431441]

- In the J-Web interface, in the Port Security Configuration page, you are required to configure **action** when you configure **MAC limit** even though configuring an **action** value is not mandatory in the CLI. [PR/434836]
- In the J-Web interface, in the OSPF Global Settings table in the OSPF Configuration page, the Global Information table in the BGP Configuration page, or the Add Interface window in the LACP Configuration page, if you try to change the position of columns using the drag-and-drop method, only the column header moves to the new position instead of the entire column. [PR/465030]
- When you have a large number of static routes configured and if you have navigated to pages other than page 1 in the Route Information table in the J-Web interface (**Monitor > Routing > Route Information**), changing the **Route Table** to query other routes refreshes the page but does not return to page 1. For example, if you run a query from page 3 and the new query returns very few results, the Results table continues to display page 3 and shows no results. To view the results, navigate to page 1 manually. [PR/476338]
- In the J-Web interface, the dashboard does not display the uplink ports or uplink module ports unless transceivers are plugged into the ports. [PR/477549]
- The J-Web interface Static Routing page might not display details on entries registered in the routing table. [PR/483885]
- An IPv4 static route that has been configured using the CLI might not be displayed when you select **Configure > Routing > Static Routing** in the J-Web interface. [PR/487597]
- In the J-Web interface, the auto-complete feature might not be disabled in the password field. As a workaround, you can disable the auto-complete feature in the browser. [PR/508425]
- In the J-Web interface, the **Software Upload and Install Package** option might not display a warning message when there are pending changes to be committed. [PR/514853]
- For a Virtual Chassis configuration member, the J-Web Chassis View displays the assembly model number (for example, F1NYY) instead of the chassis model number (for example, EX4200-24T). As a workaround, use the CLI command **show chassis hardware** to display correct model numbers. [PR/539977]
- When you use an https connection in the Microsoft Internet Explorer browser to save a report from the View Events page (**Monitor > Events and Alarms > View events**) in the J-Web interface, the following error message is displayed:

  ```
  Internet Explorer was not able to open the Internet site
  ```

  [PR/542887]
- In the J-Web interface, when you use an https connection in the Microsoft Internet Explorer browser, you cannot upload (**Maintain > Config Management > Upload**) or download (**Maintain > Config Management > History > Configuration History**) a configuration file. As a workaround, use an http connection.

  [PR/551200]

- If you have accessed the J-Web interface using Microsoft Internet Explorer, you might not be able to commit a configuration when an SSL certificate has been added to the switch using the CLI editor (**Configure >CLI tools > CLI Editor**). As a workaround, you can use Firefox to commit configurations. [PR/552629]
- On J-EX8200 switches when no line cards are inserted, the Monitor Interface page in the J-Web interface might display an error message. You can ignore the error message. [PR/562454]
- J-Web has not been tested with and does not currently support the following browsers: Microsoft Internet Explorer version 8, Mozilla FireFox version 3.6, and Google Chrome. [PR/563908]
- The J-Web dashboard might not automatically refresh after navigation for J-EX Series switches. [PR/566359]
- If you have accessed the J-Web interface using an https connection through the Microsoft Internet Explorer Web browser, you might not be able to download and save reports from some pages on the **Monitor**, **Maintain**, and **Troubleshoot** tabs. Some affected pages are at these locations:
  - **Maintain > Files > Log Files > Download**
  - **Maintain > Config Management > History**
  - **Maintain > Customer Support > Support Information > Generate Report**
  - **Troubleshoot > Troubleshoot Port > Generate Report**
  - **Monitor > Events and Alarms > View Events > Generate Report**
  - **Monitor > Routing > Route Information > Generate Report**

  As a workaround, you can use the Mozilla Firefox Web browser to download and save reports using an https connection. [PR/566581]

Related Documentation

- New Features in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 52
- Changes in Default Behavior and Syntax in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 54
- Limitations in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 54
- Resolved Issues in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 60
- Errata in Documentation for Junos OS Release 10.3 for J-EX Series Ethernet switches on page 63

Resolved Issues in Junos OS Release 10.3 for J-EX Series Ethernet Switches

The following are the issues that have been resolved since Junos OS Release 10.2R1 for J-EX Series Ethernet switches. The identifier following the descriptions is the tracking number in our bug database.

Bridging, VLANs, and Spanning Trees

- On J-EX Series Ethernet switches, when the VLAN with the lowest-numbered VLAN ID is down, the **show ntp associations** command output displays the following message:

  ```
  /usr/bin/ntpq: write to localhost failed: No route to host
  ```

  [PR/466595: This issue has been resolved.]

- On J-EX Series Ethernet switches, in a scaled environment with more than 4000 VLANs, MVRP advertisements might not be sent intermittently when the VLAN membership is modified. [PR/475701: This issue has been resolved.]

- On J-EX Series Ethernet switches, having a large number of VSTP instances and RSTP instances might cause continuous changes in the topology. As a workaround, reduce the number of VSTP instances to fewer than 190. [PR/504719: This issue has been resolved.]

Infrastructure

- On J-EX Series Ethernet switches, MAC addresses not present in the forwarding database (FDB) because of hash collision are not removed from the Ethernet switching process (**eswd**). These MAC addresses do not age out of the Ethernet switching table even if traffic is stopped completely and are never relearned when traffic is sent to these MAC addresses, even when there is no hash collision. As a workaround, clear those MAC addresses from the Ethernet switching table. [PR/451431: This issue has been resolved.]

- On J-EX8200 switches, the system log messages from the line cards display the timestamp in UTC, instead of the time zone specified in the CLI configuration. [PR/494892: This issue has been resolved.]

- On J-EX Series Ethernet switches, the **/var** directory appears full after some files in the **/var/log** directory are deleted. To avoid this problem, use the **clear log** *filename* command to clear the log files, instead of deleting them manually. [PR/496298: This issue has been resolved.]

- On J-EX8200 switches, the **show pfe statistics traffic multicast fpc** *fpc-slot dev-number* command takes a long time to display output, and the output shows incorrect values. [PR/506031: This issue has been resolved.]

Interfaces

- In a Q-in-Q tunneling configuration that includes aggregated Ethernet interfaces (LAGs), after a **pfem** process restart, the member interfaces in the VLAN might be incorrectly set. [PR/527117: This issue has been resolved.]

J-Web Interface

- In the J-Web interface, the procedure of uploading a software package to the switch might not work properly if you are using the Microsoft Internet Explorer Web browser version 7. [PR/424859: This issue has been resolved.]

- In the J-Web interface, interfaces configured with **no-flow-control** might be displayed in the Link Aggregation Configuration page. [PR/437410: This issue has been resolved.]

- In the J-Web interface, in the OSPF Configuration page (**Configuration > Routing > OSPF**), the Traceoptions tab in the Edit Global Settings window does not display the available flags (tracing parameters). As a workaround, use the CLI to view the available flags. [PR/475313: This issue has been resolved.]
- In the J-Web interface, the OSPF Monitoring page might display an error message if there are multiple interfaces or neighbors detected in an autonomous system. [PR/502132: This issue has been resolved.]
- On J-EX4200 switches, you might not be able to upgrade the switch to Junos OS Release 10.3 using the J-Web interface from a release prior to Junos OS Release 10.2. As a workaround, upgrade the switch using the CLI. [PR/509073: This issue has been resolved.]
- In the J-Web interface, the PoE configuration page and Monitoring PoE page might not display in the Microsoft Internet Explorer Web browser version 7. [PR/516048: This issue has been resolved.]
- In the J-Web interface, when you are assigning interfaces to a VLAN using the in-band management option, EZSetup might display only interfaces in which transceivers have been inserted. [PR/521632: This issue has been resolved.]
- If RIP, BGP, OSPF, and DHCP are not configured on a switch, the "feature not configured" validation message masks the **Commit**, **Help**, and **Logout** menu options if you are using the Mozilla Firefox Web browser. As a workaround, refresh the J-Web interface. [PR/528346: This issue has been resolved.]
- In the J-Web interface when you select **Monitor > Switching > Ethernet Switching**, the MAC learning log might not display information. [PR/535200: This issue has been resolved.]
- J-EX Series Ethernet switches do not support the J-Web interface. [PR/561871: This issue has been resolved.]
- J-EX4200 switches with an SFP+ line card installed do not properly display the J-Web dashboard chassis view. [PR/564307: This issue has been resolved.]

Layer 2 and Layer 3 Protocols

- If a J-EX8200 switch receives an IGMP packet of unknown type, the switch might flood the packet on all interfaces, including the ingress interface from which the packet was received. [PR/502248: This issue has been resolved.]

Related Documentation

- New Features in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 52
- Changes in Default Behavior and Syntax in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 54
- Limitations in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 54
- Outstanding Issues in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 57
- Errata in Documentation for Junos OS Release 10.3 for J-EX Series Ethernet switches on page 63

Errata in Documentation for Junos OS Release 10.3 for J-EX Series Ethernet Switches

This section lists outstanding issues with the documentation.

Infrastructure

- Options **ip** and **ip6** for the **show pfe statistics** command are not supported on J-EX Series Ethernet switches. Support for those options on the switches might be incorrectly indicated in the documentation.

Related Documentation

- New Features in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 52
- Changes in Default Behavior and Syntax in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 54
- Limitations in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 54
- Outstanding Issues in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 57
- Resolved Issues in Junos OS Release 10.3 for J-EX Series Ethernet switches on page 60

Dell Documentation and Release Notes

To download the hardware documentation for your product and the Junos OS documentation for PowerConnect J-Series J-EX Series and J-SRX Series products , see the following Dell support website: http://www.support.dell.com/manuals.

If the information in the latest release notes differs from the information in the documentation, follow the release notes.

Requesting Technical Support

For technical support, see http://www.support.dell.com .

Revision History

22 November 2010—Revision 2, Junos Release 10.3R2