JUNOS® 10.1 Software Release Notes for Dell™ PowerConnect™ J-SRX Series Services Gateways

Release 10.1R2
13 May 2010

These release notes accompany Release 10.1R2 of the JUNOS Software for Dell PowerConnect J-SRX Series Services Gateways. 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 Software Release Notes for J-SRX Series Services Gateways

Powered by JUNOS Software, 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 Release 10.1 for J-SRX Series Services Gateways

The following features have been added to JUNOS Release 10.1. Following the description is the title of the manual or manuals to consult for further information.

Software Features

Application Layer Gateways (ALGs)

- **DNS doctoring support**—This feature is supported on all J-SRX Series devices.

  Domain Name System (DNS) ALG functionality has been extended to support static NAT. You should configure static NAT for the DNS server first. Then if the DNS ALG is enabled, public-to-private and private-to-public static address translation can occur for A-records in DNS replies.

  The DNS ALG also now includes a maximum-message-length command option with a value range of 512 to 8192 bytes and a default value of 512 bytes. The DNS ALG will now drop traffic if the DNS message length exceeds the configured maximum, if the domain name is more than 255 bytes, or if the label length is more than 63 bytes. The ALG will also decompress domain name compression pointers and retrieve their related full domain names, and check for the existence of compression pointer loops and drop the traffic if one exists.

  Note that the DNS ALG can translate the first 32 A-records in a single DNS reply. A-records after the first 32 will not be handled. Also note that the DNS ALG supports only IPv4 addresses and does not support VPN tunnels.

  [*JUNOS Software Security Configuration Guide*]

Integrated Convergence Services

- **DSCP marking for RTP packets generated by J-SRX Series Integrated Convergence Services**—This feature is supported on J-SRX210 and J-SRX240 devices that have high memory, power over Ethernet capability, and media gateway capability.

  Configure DSCP marking to set the desired DSCP bits for RTP packets generated by J-SRX Series Integrated Convergence Services.

  DSCP bits are the 6-bit bitmap in the IP header used by devices to decide the forwarding priority of packet routing. When the DSCP bits of RTP packets generated by Integrated Convergence Services are configured, the downstream device can then classify the RTP packets and direct them to a higher priority queue in order to achieve better voice quality when packet traffic is congested. Devices running JUNOS Software provide classification, priority queuing, and other kinds of CoS configuration under the Class-of-Service configuration hierarchy.

  Note that the Integrated Convergence Services DSCP marking feature marks only RTP packets of calls that it terminates, which include calls to peer call servers and to peer proxy servers that provide SIP trunks. If a call is not terminated by Integrated Convergence Services, then DSCP marking does not apply.

  To configure the DSCP marking bitmap for calls terminated by Integrated Convergence Services and the address of the peer call server or peer proxy server to which these calls are routed, use the **media-policy** statement in the **[edit services converged-services]** hierarchy level.
  set services convergence-service service-class < name > dscp < bitmap >
  set services convergence-service service-class media-policy < name > term < term-name > from peer-address [< addresses >]
  set services convergence-service service-class media-policy < name > term then service-class < name >

Interfaces and Routing

- **DOCSIS Mini-PIM interface**—Data over Cable Service Interface Specification (DOCSIS) defines the communications and operation support interface requirements for a data-over-cable system. It is used by cable operators to provide Internet access over their existing cable infrastructure for both residential and business customers. DOCSIS 3.0 is the latest Interface standard allowing channel bonding to deliver speeds higher than 100 Mbps throughput in either direction, far surpassing other WAN technologies such as T1/E1, ADSL2+, ISDN, and DS3.

  DOCSIS network architecture includes a cable modem on J-SRX Series Services Gateways with a DOCSIS Mini-Physical Interface Module (Mini-PIM) located at customer premises, and a Cable Modem Termination System (CMTS) located at the head-end or data center locations. Standards-based DOCSIS 3.0 Mini-PIM is interoperable with CMTS equipment. The DOCSIS Mini-PIM provides backward compatibility with CMTS equipment based on the following standards:

  - DOCSIS 2.0
  - DOCSIS 1.1
  - DOCSIS 1.0

  The DOCSIS Mini-PIM is supported on the following J-SRX Series Services Gateways:

- J-SRX210
- J-SRX240

  The DOCSIS Mini-PIM has the following key features:

  - Provides high data transfer rates of over 150 Mbps downstream
  - Supports four downstream and four upstream channel bonding
  - Supports quality of service (QoS)
  - Provides interoperability with any DOCSIS-compliant cable modem termination system (CMTS)
  - Supports IPv6 and IPv4 for modem management interfaces
  - Supports Baseline Privacy Interface Plus (BPI+)
  - Supports Advanced Encryption Standard (AES)

  [*JUNOS Software Security Configuration Guide*]

- **Very-high-bit-rate digital subscriber line (VDSL)**—VDSL technology is part of the xDSL family of modem technologies that provide faster data transmission over a single flat untwisted or twisted pair of copper wires.

  The VDSL lines connect service provider networks and customer sites to provide high bandwidth applications (Triple Play services) such as high-speed Internet access, telephone services like voice over IP (VoIP), high-definition TV (HDTV), and interactive gaming services over a single connection. VDSL2 is an enhancement to VDSL and permits the transmission of asymmetric and symmetric (full-duplex) aggregate data rates up to 100 Mbps on short copper loops using a bandwidth up to 30 MHz. The VDSL2 technology is based on the ITU-T G.993.2 standard.

  The following J-SRX Series Services Gateways support the VDSL2 Mini-Physical Interface Module (Mini-PIM) (Annex A):

  - J-SRX210 Services Gateway
  - J-SRX240 Services Gateway

  The VDSL2 Mini-PIM carries the Ethernet backplane. When the Mini-PIM is plugged into the chassis, the Mini-PIM connects to one of the ports of the baseboard switch.

  The VDSL2 Mini-PIM supports following features:

  - ADSL/ADSL2/ADSL2+ backward compatibility with Annex-A, Annex-M Support
  - PTM or EFM [802.3ah] support
  - Operation, Administration, and Maintenance (OAM) support for ADSL/ADSL/ADSL2+ ATM mode
  - ATM QoS (supported only when the VDSL2 Mini-PIM is operating in ADSL2 mode)
  - MLPPP (supported only when the VDSL2 Mini-PIM is operating in ADSL2 mode)

    - MTU size of 1500 bytes (maximum)
    - Support for maximum of 10 PVCs (only in ADSL/ADSL2/ADSL2+ mode)
    - Dying gasp support (ADSL and VDSL2 mode)

- **Implement the PPPoE-based radio-to-router protocol**—This feature is supported on J-SRX Series.

  JUNOS Release 10.1 supports PPPoE-based radio-to-router protocols. These protocols include messages that define how an external device provides the router with timely information about the quality of a link's connection. There is also a flow control mechanism to indicate how much data the device can forward. The device can then use the information provided in the PPPoE messages to dynamically adjust the interface speed of the PPP links. Use the radio-router statement from the [**set interfaces <unit>**] hierarchy to indicate that metrics announcements received on the interface will be processed by the device.

- **Layer 2 Q-in-Q tunneling**—This feature is supported on J-SRX210, and J-SRX240 devices.

  Q-in-Q tunneling, defined by the IEEE 802.1ad standard, allows service providers on Ethernet access networks to extend a Layer 2 Ethernet connection between two customer sites.

  In Q-in-Q tunneling, as a packet travels from a customer VLAN (C-VLAN) to a service provider's VLAN, a service provider-specific 802.1Q tag is added to the packet. This additional tag is used to segregate traffic into service-provider-defined service VLANs (S-VLANs). The original customer 802.1Q tag of the packet remains and is transmitted transparently, passing through the service provider's network. As the packet leaves the S-VLAN in the downstream direction, the extra 802.1Q tag is removed.

  There are three ways to map C-VLANs to an S-VLAN:

    - All-in-one bundling—Use the **dot1q-tunneling** statement at the [**edit vlans**] hierarchy to map without specifying customer VLANs. All packets from a specific access interface are mapped to the S-VLAN.
    - Many-to-one bundling—Use the **customer-vlans** statement at the [**edit vlans**] hierarchy to specify which C-VLANs are mapped to the S-VLAN.
    - Mapping C-VLAN on a specific interface—Use the **mapping** statement at the [**edit vlans**] hierarchy to map a specific C-VLAN on a specified access interface to the S-VLAN.

  Table 1 on page 7 lists the C-VLAN to S-VLAN mapping supported on J-SRX Series.

Table 1: C-VLAN to S-VLAN Mapping Supported on J-SRX Series Devices

Mapping	J-SRX210	J-SRX240
All-in-one bundling	Yes	Yes
Many-to-one bundling	No	No

Table 1: C-VLAN to S-VLAN Mapping Supported on J-SRX Series Devices *(continued)*

Mapping	J-SRX210	J-SRX240
Mapping C-VLAN on a specific interface	No	No

Integrated bridging and routing (IRB) interfaces are supported on Q-in-Q VLANs for J-SRX210, and J-SRX240 devices. Packets arriving on an IRB interface on a Q-in-Q VLAN are routed regardless of whether the packet is single or double tagged. The outgoing routed packets contain an S-VLAN tag only when exiting a trunk interface; the packets exit the interface untagged when exiting an access interface.

In a Q-in-Q deployment, customer packets from downstream interfaces are transported without any changes to source and destination MAC addresses. You can disable MAC address learning at both the interface level and the VLAN level. Disabling MAC address learning on an interface disables learning for all the VLANs of which that interface is a member. When you disable MAC address learning on a VLAN, MAC addresses that have already been learned are flushed.

[*JUNOS Software Interfaces and Routing Configuration Guide*]

- **Layer 2 Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED)**—This feature is supported on J-SRX100, J-SRX210, and J-SRX240 devices.

  Devices use LLDP and LLDP-MED to learn and distribute device information on network links. The information allows the device to quickly identify a variety of systems, resulting in a LAN that interoperates smoothly and efficiently.

  LLDP-capable devices transmit information in Type Length Value (TLV) messages to neighbor devices. Device information can include specifics, such as chassis and port identification and system name and system capabilities. The TLVs leverage this information from parameters that have already been configured in the JUNOS Software.

  LLDP-MED goes one step further, exchanging IP-telephony messages between the device and the IP telephone. These TLV messages provide detailed information on PoE policy. The PoE Management TLVs let the device ports advertise the power level and power priority needed. For example, the device can compare the power needed by an IP telephone running on a PoE interface with available resources. If the device cannot meet the resources required by the IP telephone, the device could negotiate with the telephone until a compromise on power is reached.

  LLDP and LLDP-MED must be explicitly configured on base ports on J-SRX100, J-SRX210, and J-SRX240 devices. To configure LLDP on all interfaces or on a specific interface, use the **lldp** statement at the [**set protocols**] hierarchy. To configure LLDP-MED on all interfaces or on a specific interface, use the **lldp-med** statement at the [**set protocols**] hierarchy.

  [*JUNOS Software Interfaces and Routing Configuration Guide*]

Manual BIOS upgrade using JUNOS CLI

- This feature is supported on J-SRX100, J-SRX210, and J-SRX240 devices.

  For branch J-SRX Series devices, BIOS is made up of U-boot and JUNOS loader. Apart from this J-SRX240 also has U-shell binary as part of the BIOS.

  On J-SRX100, J-SRX210 and J-SRX240, there is support of Backup BIOS which constitutes a backup copy of U-boot in addition to the active copy from which the system generally boots up.

  Table 2 on page 10 provides details of BIOS components supported for different platforms.

Table 2: Manual BIOS Upgrade components

BIOS Components		J-SRX100	J-SRX210	J-SRX240	
Active	U-boot	Yes	Yes	Yes	
	Loader	Yes	Yes	Yes	
	U-shell			Yes	
Backup	U-boot	Yes	Yes	Yes	

Table 3 on page 10 provides you the CLI commands used for manual BIOS upgrade.

Table 3: CLI Commands for Manual BIOS Upgrade

Active BIOS	Backup BIOS
request system firmware upgrade re bios	**request system firmware upgrade re bios backup**

Procedure for BIOS upgrade

1. **Installing a jloader-srxsme package**

   1. Copy the jloader-srxme signed package to the device.

NOTE: Note that this package should be of the same version as that of the corresponding JUNOS, example, on a device with a 10.1 JUNOS package installed, the jloader-srxsme package should also be of version 10.1.

   2. Install the package using the **request system software add <path to jloader-srxsme package> no-copy no-validate** command.

      root> request system software add /var/tmp/jloader-srxsme-10.1B3-signed.tgz no-copy no-validate

```
Installing package '/var/tmp/jloader-srxsme-10.1B3-signed.tgz' ...
Verified jloader-srxsme-10.1B3.tgz signed by PackageProduction_10_1_0
Adding jloader-srxsme...
Available space: 427640 require: 2674
Mounted jloader-srxsme package on /dev/md5...
Saving state for rollback ...
```

root> show version

```
Model: SRX240h
JUNOS Software Release [10.1B3]
JUNOS BIOS Software Suite [10.1B3]
```

NOTE: Installing the jloader-srxsme package puts the necessary images under directory/boot.

2. **Verifying that images for upgrade are installed**

   - The **show system firmware** command can be used to get version of images available for upgrade. The available version is printed under column **Available version**. The user needs to verify that the correct version of BIOS images available for upgrade.

   root> show system firmware

```
Part              Type           Tag  Current   Available  Status
                                       version   version
 Routing Engine 0  RE BIOS        0    1.5       1.7        OK
 Routing Engine 0  RE BIOS Backup 1    1.5       1.7        OK
 Routing Engine 0  RE FPGA        11   12.3.0               OK
```

3. **BIOS upgrade**

   Active BIOS:

   1. Initiate the upgrade using the **request system firmware upgade re bios** command.

      root> request system firmware upgrade re bios

```
 Part              Type           Tag  Current   Available  Status
                                        version   version
  Routing Engine 0  RE BIOS        0    1.5       1.7        OK
  Routing Engine 0  RE BIOS Backup 1    1.5       1.7        OK
  Perform indicated firmware upgrade ? [yes,no] (no) yes

Firmware upgrade initiated.
```

   2. Monitor the status of upgrade using the **show system firmware** command.

      root> show system firmware

```
 Part              Type            Tag  Current   Available   Status
                                       version   version
Routing Engine 0  RE BIOS         0     1.5       1.7        PROGRAMMING
Routing Engine 0  RE BIOS Backup  1     1.5       1.7        OK
Routing Engine 0  RE FPGA         11    12.3.0               OK
```

      root> show system firmware

```
Part              Type           Tag    Current   Available   Status
                                        version   version
Routing Engine 0  RE BIOS         0     1.5        1.7      UPGRADED
                                                            SUCCESSFULLY

Routing Engine 0  RE BIOS Backup  1     1.5        1.7        OK
Routing Engine 0  RE FPGA         11    12.3.0                OK
```

NOTE: The device must be rebooted for the upgraded active BIOS to take effect.

   Backup BIOS:

   1. Initiate the upgrade using the **request system firmware upgade re bios backup** command.

      root> request system firmware upgrade re bios backup

```
 Part              Type           Tag  Current   Available  Status
                                        version   version
  Routing Engine 0  RE BIOS        0    1.5       1.7        OK
  Routing Engine 0  RE BIOS Backup 1    1.5       1.7        OK
  Perform indicated firmware upgrade ? [yes,no] (no) yes

Firmware upgrade initiated.
```

   2. Monitor the status of upgrade using the **show system firmware** command.

root> show system firmware

```
Part              Type           Tag  Current   Available  Status
                                       version   version
 Routing Engine 0  RE BIOS        0    1.5       1.7        OK
 Routing Engine 0  RE BIOS Backup 1    1.5       1.7        PROGRAMMING
 Routing Engine 0  RE FPGA         11   12.3.0                OK
```

root> show system firmware

```
Part              Type           Tag    Current   Available   Status
                                        version   version
Routing Engine 0  RE BIOS         0     1.5        1.7          OK
Routing Engine 0  RE BIOS Backup  1     1.7        1.7        UPGRADED
                                                            SUCCESSFULLY
Routing Engine 0  RE FPGA         11    12.3.0                OK
```

Network Address Translation (NAT)

- **Increased maximum number of source NAT rules supported**—This feature is supported on J-SRX Series devices.

  JUNOS Release 10.1 increases the number of source NAT rules and rule sets that you can configure on a device. In previous releases, the maximum number of source NAT rule sets you could configure on a device was 32 and the maximum number of rules in a source NAT rule set was 8.

  JUNOS Release 10.1, the maximum number of source NAT rules that you can configure on a device are:

  - 512 for J-SRX100, and J-SRX210 devices
  - 1024 for J-SRX240 devices

  These are systemwide maximums for total numbers of source NAT rules. There is no limitation on the number of rules that you can configure in a source NAT rule set as long as the maximum number of source NAT rules allowed on the device is not exceeded.

NOTE: This features does not change the maximum number of rules and rule sets you can configure on a device for static and destination NAT. For static NAT, you can configure up to 32 rule sets and up to 256 rules per rule set. For destination NAT, you can configure up to 32 rule sets and up to 8 rules per rule set.

Virtual LANs (VLANs)

- **Flexible Ethernet services**—This feature is supported on J-SRX210, and J-SRX240 devices.

  Use flexible Ethernet services encapsulation when you want to configure multiple per-unit Ethernet encapsulations. This encapsulation type allows you to configure any combination of route, TCC, CCC, and VPLS encapsulations on a single physical port. Aggregated Ethernet bundles cannot use this encapsulation type.

  For ports configured with flexible Ethernet services encapsulation, VLAN IDs from 1 through 511 are no longer reserved for normal VLANs.

Related Topics

- Known Limitations in JUNOS Release 10.1 for J-SRX Series Services Gateways on page 20
- Issues in JUNOS Release 10.1 for J-SRX Series Services Gateways on page 23
- Errata and Changes in Documentation for JUNOS Release 10.1 for J-SRX Series Services Gateways on page 37

Changes In Default Behavior and Syntax in JUNOS Release 10.1 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 Software documentation:

Application Layer Gateways (ALGs)

- The following CLI commands have been removed as part of RPC ALG data structure cleanup:
  - **clear security alg msrpc portmap**
  - **clear security alg sunrpc portmap**
  - **show security alg msrpc portmap**
  - **show security alg sunrpc portmap**
- 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>**.

AX411 Access Point

- On J-SRX240 devices managing an AX411 Access Point, when you upgrade from release 10.0x to Release 10.1R2 using the “validate” option, the upgrade might fail during configuration validation. As a workaround, defer the upgrade until the service release with a proper fix becomes available.
- On J-SRX240 devices managing an AX411 Access Point, when you upgrade from release 10.0x to Release 10.1R2 using the “no-validate” option, the upgrade succeeds but the

configuration commit by the management daemon fails and the system might become accessible only through the console. As a workaround, configure the WLAN administration authentication password. If the device is not managing an AX411 Access Point, delete the WLAN configuration.

- On J-SRX240 devices managing an AX411 Access Point, when you load the Release 10.1R2 at manufacturing site or on an empty Compact Flash card or flash memory device, the system might become accessible only through the console. As a workaround, set the WLAN administration authentication password and commit the configuration.
- On J-SRX240 devices managing an AX411 access Point, when you attempt the factory configuration load by using the command “load factory-default” or by pressing the reset button for 15 seconds, the commit fails. As a result, the system continues to use the previous configuration. As a workaround, set the WLAN administration authentication password and commit the configuration.

Chassis Cluster

- The automatic pause timer functionality related to IP address monitoring for redundancy groups has been removed. Instead, a configurable **hold-down-interval** timer for all redundancy groups has been instituted. See the “Configuring a Dampening Time Between Back-to-Back Redundancy Group Failovers” section of the *JUNOS Software Security Configuration Guide*.
- IP address monitoring on redundancy group 0 is now supported.
- The **chassis cluster redundancy-group *group-number* ip-monitoring threshold** CLI command has been removed. Instead, use the **chassis cluster redundancy-group *group-number* ip-monitoring global-threshold** command.
- IP address monitoring on virtual routers is now supported.

Command-Line Interface (CLI)

- On J-SRX Series devices, the **show security monitoring fpc 0** command is now available.

  The output of this CLI command on J-SRX Series devices differs from previous implementations on other devices. Note the following sample output:

  ```
  show security monitoring fpc 0

  FPC 0

  PIC 0

  CPU utilization : 0 %

  Memory utilization : 65 %

  Current flow session : 0

  Max flow session : 131072
  ```

NOTE: When J-SRX Series devices operate in packet mode, flow sessions will not be created and current flow session will remain zero as shown in the sample output above. The maximum number of sessions will differ from one device to another.

- On J-SRX210 devices with Integrated Convergence Services, TDM configuration change might interrupt existing TDM calls if any MPIMs are configured. The voice calls through the MPIM do not work. Run the CLI **restart rtmd** command after making a configuration change to the MPIM ports.
- On J-SRX210 devices with Integrated Convergence Services, registrations do not work when PCS is configured and removed thorough the CLI. The dial tone dissappears when the analog station calls the SIP station. As a workaround, either run the **rtmd restart** command or restart the device.
- 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 (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
    show system storage
    partitions (USB)
    ```
  - Example 2:

    ```
    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
```

Configuration

- On J-SRX100, J-SRX210, and J-SRX240 devices, the current JUNOS Software 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).
- The default values for IKE and IPsec security association (SA) lifetimes for standard VPNs have been changed in this release:
  - The default value for the **lifetime-seconds** configuration statement at the [**edit security ike proposal proposal-name**] hierarchy level has been changed from 3600 seconds to 28,800 seconds.
  - The default value for the **lifetime-seconds** configuration statement at the [**edit security ipsec proposal proposal-name**] hierarchy level has been changed from 28,800 seconds to 3600 seconds.

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.

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.

J-Web

- 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.

WLAN

- While configuring the AX411 Access Point on your J-SRX Series services gateways, 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.

Known Limitations in JUNOS Release 10.1 for J-SRX Series Services Gateways

[accounting-options] Hierarchy

- On 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

- On J-SRX100 devices, there are command-line interface (CLI) commands and J-Web tabs 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 Cluster

On J-SRX Series devices, the following features are not supported when chassis clustering is enabled on the device:

- All packet-based protocols, such as MPLS, Connectionless Network Service (CLNS), and IP version 6 (IPv6)
- Any function that depends on the configurable interfaces:
  - **lsq-0/0/0**—Link services Multilink Point-to-Point Protocol (MLPPP), Multilink Frame Relay (MLFR), and Compressed Real-Time Transport Protocol (CRTP)
  - **gr-0/0/0**—Generic routing encapsulation (GRE) and tunneling
  - **ip-0/0/0**—IP-over-IP (IP-IP) encapsulation
  - **pd-0/0/0**, **pe/0/0/0**, and **mt-0/0/0**—All multicast protocols
  - **lt-0/0/0**—Real-time performance monitoring (RPM)
  - WXC Integrated Services Module (WXC ISM 200)
  - ISDN BRI
  - Layer 2 Ethernet switching

    The factory default configuration for J-SRX100, J-SRX210, and J-SRX240 devices automatically enables Layer 2 Ethernet switching. Because Layer 2 Ethernet switching is not supported in chassis cluster mode, for these devices, if you use the factory default configuration, you must delete the Ethernet switching configuration before you enable chassis clustering.

△ CAUTION: Enabling chassis clustering while Ethernet switching is enabled is not a supported configuration. Doing so might result in undesirable behavior from the devices, leading to possible network instability.

The default configuration for other J-SRX Series devices does not enable Ethernet switching. However, if you have enabled Ethernet switching, be sure to disable it before enabling clustering on these devices too.

For more information, see the “Disabling Switching on J-SRX100, J-SRX210, and J-SRX240 Devices Before Enabling Chassis Clustering” section in the *JUNOS Software 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

- **Maximum concurrent SSH, Telnet, and Web sessions—**On J-SRX210, and J-SRX240 devices, the maximum number of concurrent sessions is as follows:

Sessions	J-SRX210	J-SRX240
ssh	3	5
telnet	3	5
Web	3	5

NOTE: These defaults are provided for performance reasons.

- On J-SRX210 and J-SRX240 devices, for optimized efficiency, we recommend that you limit use of CLI and J-Web to the following numbers of sessions:

Device	CLI	J-Web	Console
J-SRX210	3	3	1

Device	CLI	J-Web	Console
J-SRX240	5	5	1

- On J-SRX100 devices, Layer 3 control protocols (OSPF, using multicast destination MAC address) on the VLAN Layer 3 interface work only with access ports.
- On J-SRX210, and J-SRX240 devices, broadcast TFTP is not supported when **flow** is enabled on the device.

Interfaces and Routing

- 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, bidirection traffic of 20 kbps or above), **keepalives** not get exchanged, and the interface goes down.

NetScreen-Remote

- On J-SRX Series devices, NetScreen-Remote is not supported in JUNOS Release 10.1.

Network Address Translation (NAT)

- The following describes the maximum numbers of NAT rules and rule sets supported:
  - For static NAT, up to 32 rule sets and up to 256 rules per rule set can be configured on a device.
  - For destination NAT, up to 32 rule sets and up to 8 rules per rule set can be configured on a device.
  - For source NAT, the following are the maximum numbers of source NAT rules that can be configured on a device:
    - 512 for J-SRX100, and J-SRX210 devices
    - 1024 for J-SRX240 devices

    These are systemwide maximums for total numbers of source NAT rules. There is no limitation on the number of rules that you can configure in a source NAT rule set as long as the maximum number of source NAT rules allowed on the device is not exceeded.

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 Topics

- New Features in JUNOS Release 10.1 for J-SRX Series Services Gateways on page 3
- Issues in JUNOS Release 10.1 for J-SRX Series Services Gateways on page 23
- Errata and Changes in Documentation for JUNOS Release 10.1 for J-SRX Series Services Gateways on page 37

Issues in JUNOS Release 10.1 for J-SRX Series Services Gateways

- Outstanding Issues In JUNOS Release 10.1 for J-SRX Series Services Gateways on page 23
- Resolved Issues in JUNOS Release 10.1 for J-SRX Series Services Gateways on page 34

Outstanding Issues In JUNOS Release 10.1 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]

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]
- On AX411 Access Points, an access point might not synchronize with the newly associated configuration (by changing or swapping the MAC address) and also might not join the changed cluster when it is associated to a new config block in the WLAN access point configuration. As a workaround, deactivate and activate the access point the following CLI commands:

  ```
  #deactivate wlan access-point < ap-name >
  #commit
  #activate wlan access-point < ap-name >
  #commit
  ```

  [PR/504581]

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, when you upgrade to the latest software image, the interface links do not come up and are not seen in the Packet Forwarding Engine. As a workaround, you can reboot the device to bring up the interface. [PR/399564]
- 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 in a chassis cluster, there might be a loss of about 5 packets with 20 Mbps of UDP traffic on an RG0 failover. [PR/413642]
- 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 in chassis cluster active/active preempt mode, the RTSP session breaks after a primary node reboot and preempt failover. The following common ALGs will be broken: RSH, TALK, PPTP, MSRPC, RTSP, SUNRPC, and SQL. [PR/448870]
- 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]
- On J-SRX100 devices, after primary node reboot and cold synchronization are finished, the chassis cluster auth session timeout age and application name cannot synchronize with the chassis cluster peers. [PR/460181]

Class of Service (CoS)

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

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] [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 MC MAC address because multicast switching is based on the Layer 2 address. [PR/418519]
- On a J-SRX210 on-board 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-SRX240 PoE devices, packet drops are seen on the **lsq** interface when transit traffic with a frame length of 128 bytes is sent. [PR/455714]
- 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]
- GPRS tunneling protocol (GTP) application is supported on well-known ports only. Customized application on other ports is not supported. [PR/464357]

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 and 16-port or 24-port GPIMs, the 1G half-duplex mode of operation is not supported in the autonegotiation mode. [PR/424008]
- 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]

Integrated Convergence Services

The following issues currently exist in J-SRX210 and J-SRX240 devices with Integrated Convergence Services:

- On J-SRX210 devices with Integrated Convergence Services, the call hold feature does not work for Xlite softphones. [PR/432725]
- At least one time slot must be configured for data for voice channels on T1 lines to work. [PR/442932]
- On J-SRX240 devices with Integrated Convergence Services, T1 configuration does not support all the 24 time slots for voice calls. It is limited to 5 time slots or line channels currently. [PR/442934]
- The music-on-hold feature is not supported for SIP phones. [PR/443681]
- The peer call server configuration for the media gateway page in J-Web does not correctly display the port number field when TCP is used as the transport. [PR/445734]
- When you click the **trunk-group** field in J-Web, the configured trunk values are not displayed. [PR/445765]
- Comfort noise packets are not generated when both voice activity detection (VAD) and comfort noise generation are enabled for an FXS station. [PR/448191]
- In J-Web, if you do not configure the class of restriction and a station template, you cannot configure a station. [PR/452439]
- J-Web does not provide support for the SIP template extension inheritance feature. [PR/455787]
- SNMP does not provide support for survivable call server (J-SRX Series SCS) statistics. [PR/456454]
- Consecutive G.711 faxes pass through between two FXS ports fails when originating and terminating sides alternate. [PR/465775]
- When T1 lines for stations or trunks are configured, you might hear a momentary burst of noise on the phone. [PR/467334]

- You must restart the **flow** daemon to commit runtime T1 configuration changes. [PR/468594]
- The SIP-to-SIP simultaneous call capacity is limited to 10 calls. [PR/478485]

Interfaces and Routing

- On J-SRX240 devices, drops in out-of-profile LLQ packets might be seen in the presence of data traffic, even when the combined (data+LLQ) traffic does not oversubscribe the multilink bundle. [PR/417474]
- 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 SRX 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-SRX240 devices, the serial interface maximum speed in extensive output is displayed as 16384 Kbps instead of 8.0 Mbps. [PR/437530]
- On J-SRX Series devices, incorrect Layer 2 circuit replication on the backup Routing Engine might occur when you:
  - Configure nonstop 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 non-standby connection.
  2. Change the configuration to 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 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-SRX210 PoE devices, the G.SHDSL link does not come up with an octal port line card of total access 1000 ADTRAN DSLAM. [PR/459554]
- On J-SRX210 High Memory devices, only six logical interfaces come up on the G.SHDSL ATM interface (including OAM channel). The other two logical interfaces are down. [PR/466296]
- On J-SRX100 and SRX200 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 can not 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 integrated routing and bridging (IRB) interface. As a workaround, enable IGMP snooping to use IGMP over IRB interfaces. [PR/492564]
- On J-SRX100 and 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 due to no ATM connection. [PR/493099]
- 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-SRX210 High Memory devices, the GRE tunnel session is not created properly if the tunnel outgoing interface takes a long time to come up. On T1/E1 interfaces of J-SRX100, J-SRX210, and J-SRX240 devices, traffic through GRE tunnel might not work. As a workaround, first create the physical interface and commit the configuration and then create a GRE tunnel configuration. [PR/497864]
- On J-SRX240 devices, when you activate or deactivate the ATM interface for the VDSL PIM inserted on slots two, three, or four, it might result in a flowd crash due to a bug in the VDSL driver. This problem might not be noticed on J-SRX210 devices. [PR/505347]

J-Web

- On J-SRX Series devices, when the user adds LACP interface details, a pop-up window appears in which there are two buttons to move the interface left and right. The LACP page currently does not have images incorporated with these two buttons. [PR/305885]
- 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 device, 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-SRX Series devices, when J-Web is used to configure a VLAN, the option to add an IPv6 address appears. Only IPv4 addresses are supported. [PR/459530]
- On J-SRX Series devices in J-Web the left-side menu items and page content might disappear when Troubleshoot is clicked twice. As a workaround, click the Configure or Monitor menu to get back the relevant content. [PR/459936]

- 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, in the J-Web interface, the Traceoptions tab in the Edit Global Settings window of the OSPF Configuration page (Configuration>Routing>OSPF Configuration) does not display the available flags (tracing parameters). As a workaround, use the CLI to view the available flags. [PR/475313]
- 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. Navigate to page 1 manually to view the results. [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]

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]
- On J-SRX Series devices with **session-init** and **session-close** enabled, you should not clear sessions manually when too many sessions are in status "used". [PR/445730]

Network Address Translation (NAT)

- On J-SRX240 High Memory devices, in a chassis cluster environment, the secondary node can go to **DB>** mode when there are many policies configured and TCP, UDP, and ICMP traffic matches the policies. [PR/493095]

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 and J-SRX240 devices, the **deactivate poe interface all** command does not deactivate the PoE ports. Instead, the PoE feature can be turned off by using the **disable** configuration option. Otherwise, the device must be rebooted for the deactivate setting to take effect. [PR/426772]
- On J-SRX210 and J-SRX240 devices, reset of the PoE controller fails when the restart chassis-control command is issued and also after system reboot. PoE functionality is not negatively impacted by this failure. [PR/441798]
- On J-SRX210 PoE devices managing AX411 Access Points, the devices 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 Power over Ethernet (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 Acess 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 services gateways reboot, the configuration might not be reflected onto the AX411 Access Points. As a result, the Ax411 Access Point retains the factory default configuration. [PR/476850]

Security

- On J-SRX210 devices in a chassis cluster, 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 (larger than 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 issuing a UTM command:

  the utmd subsystem is not responding to management requests.

  As a workaround, restart the **utmd** process. [PR/436029]

USB Modem

- On J-SRX210, J-SRX100, and J-SRX240 devices, when you restart fwdd at the dial-out side, the umd interface goes down and the call never gets connected. As a workaround, disable the dialer interface and restart the forwarding daemon. Enable the dialer interface when the forwarding daemon is up and running. As a result the dial-out side reconnects with the dial-in side successfully.

  Perform the following steps:

  1. Disable the dialer interface.

     ```
     root@noky# set interfaces dl0 disable
     ```

```
root@noky# commit
```

2. Restart the forwarding daemon.

```
root@noky# run restart forwarding Forwarding Daemon started, pid 1407
root@noky# delete interfaces dl0 disable
root@noky# commit
```

3. Enable the dialer interface.

```
root@noky# delete interfaces dl0 disable
root@noky# commit
```

[PR/480206]

- 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-SRX100, J-SRX210, and J-SRX240 devices, the call terminates if you remove and insert a USB modem. [PR/491820]
- 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 getting 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, 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 three or more zone scenario 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]

WLAN

- On J-SRX Series devices, when WLAN configuration is committed, it takes a while before the configuration is reflected on the access point, depending on the number of virtual access points and the number of access points connected. [PR/450230]
- 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 Release 10.1 for J-SRX Series Services Gateways

The following issues from JUNOS Release 10.0 R1 have been resolved with this release. The identifier following the description is the tracking number in our bug database.

Chassis Cluster

- On J-SRX Series devices configured in a chassis cluster, the following informative messages were erroneously displayed during failover, possibly creating the incorrect impression that errors had occurred:
  - l2ha_set_rg_state: Setting rg state for 1 (MASTER)
  - l2ha_set_rg_state: Setting rg state for 1 (BACKUP)

[PR/498010: This issue has been resolved.]

Flow and Processing

- On J-SRX210 devices, the lowest rate ATM CoS PCR supported was 64 Kbps. The ping operation did not reach an ATM interface with a PCR lower than 64 Kbps. [PR/470994: 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.]

Integrated Convergence Services

- Unable to edit the media gateway IP address field on the peer call server page in J-Web. [PR/445750: This issue has been resolved.]
- The J-Web Call Feature **Add** button did not work. [PR/446422: This issue has been resolved.]
- Was not able to edit the extension number on the J-Web call features page. [PR/447523: This issue has been resolved.]
- When you edited the remote access number in J-Web, the change was not displayed until you refreshed the page. [PR/447530: This issue has been resolved.]
- Caller ID was not displayed on FXS stations for FXO to FXS calls in survivable call server (J-SRX Series SCS) state. [PR/451719: This issue has been resolved.]
- In J-Web, you were not able specify the station type (as either analog or SIP). [PR/452813: This issue has been resolved.]
- On J-SRX210 devices with Integrated Convergence Services, in J-Web, a commit was completed when a trunk group was configured without one or more trunks, but the trunk group configuration was not visible in J-Web or the CLI. [PR/460489: This issue has been resolved.]
- The voice prompt was not played when the user dialed an invalid extension. [PR/472357: This issue has been resolved.]
- The J-SRX210 device allowed the FXS 2 port to be configured as a station and as an FXS trunk concurrently. In this case, the system did not display a commit error. [PR/473561: This issue has been resolved.]
- For SIP trunk to FXO trunk calls routed through the peer call server, the J-SRX Series device removed the called party number in the SIP INVITE messages. [PR/473979: This issue has been resolved.]

Interfaces and Routing

- On J-SRX240 devices, the SNMP null zone counter was not increased when the **reth** interface was put into the null zone. [PR/427256: This issue has been resolved.]
- On J-SRX Series devices, when 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 was taken to effect. [PR/447986: This issue has been resolved.]
- On J-SRX210 PoE devices, the ATM interface on G.SHDSL interface did not go down when the interface was disabled through the **disable** command. [PR/453896: 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, when you entered double quotation marks in the text boxes that accepted characters (for example, protocol name, file name, 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-SRX210, and J-SRX240 devices, in the J-Web interface, Monitor>Switching>Spanning Tree showed a null page when Spanning Tree Protocol was not running on the device. [PR/484202: This issue has been resolved.]
- On J-SRX210, and J-SRX240 devices, wired equivalent privacy (WEP) key validation was not properly executed in J-Web; sometimes an error returned even if the proper validation key was submitted. [PR/486910: This issue has been resolved.]
- On J-SRX Series services gateways using J-Web, the security zone associated to a logical unit other than zero got associated to a logical unit zero. [PR/504026: This issue has been resolved.]

Network Address Translation (NAT)

- On J-SRX210 and J-SRX240 devices, source NAT using interface IP address on the **pp0** interface was not working. Traffic was not forwarded because of NAT translation failure through this interface. [PR/479256: This issue has been resolved.]

Power over Ethernet

- On J-SRX210 and J-SRX240 devices, the output for the **show poe telemetries** command showed the telemetry data in chronological order rather than the preferred reverse-chronological order (most recent data first). [PR/429033: This issue has been resolved.]

USB Modem

- On J-SRX210 Services Gateways with Integrated Convergence Services, when you had USB modem configurations and you removed the USB modem from USB port 1, the device rebooted. [PR/491777: This issue has been resolved.]

Related Topics

- New Features in JUNOS Release 10.1 for J-SRX Series Services Gateways on page 3
- Known Limitations in JUNOS Release 10.1 for J-SRX Series Services Gateways on page 20
- Errata and Changes in Documentation for JUNOS Release 10.1 for J-SRX Series Services Gateways on page 37

Errata and Changes in Documentation for JUNOS Release 10.1 for J-SRX Series Services Gateways

This section lists outstanding issues with the documentation.

Application Layer Gateways (ALGs)

- The following section has been removed from the *JUNOS Software Security Configuration Guide* to reflect RPC ALG data structure cleanup: “Display the Sun RPC Port Mapping Table.”
- The “Verifying the RPC ALG Tables” section of the *JUNOS Software Security Configuration Guide* has been renamed to “Verifying the Microsoft RPC ALG Tables” to reflect RPC ALG data structure cleanup.
- ALG configuration examples in the *JUNOS Software Security Configuration Guide* incorrectly show policy-based NAT configurations. NAT configurations are now rule-based.

Attack Detection and Prevention

The default parameters documented in the firewall/NAT screen configuration options table in the *JUNOS Software Security Configuration Guide* and the J-Web online Help do not match the default parameters in the CLI. The correct default parameters are:

```
tcp {
    syn-flood {
        alarm-threshold 1024;
        attack-threshold 200;
        source-threshold 1024;
        destination-threshold 2048;
        timeout 20;
    }
 }
[edit security screen ids-option untrust-screen]
```

CLI Reference

The “Services Configuration Statement Hierarchy” section in the *JUNOS® Software CLI Reference* refers to the *JUNOS Services Interfaces Configuration Guide*, which has the following error in the sections “Data Size” and “Configuring the Probe”:

- **The minimum data size required by the UDP timestamp probe is identified as 44 bytes. This is incorrect: the minimum data size required by the UDP timestamp probe is 52 bytes.**

Command-Line Interface (CLI)

The following sections have been removed from the *JUNOS Software CLI Reference* to reflect RPC ALG data structure cleanup:

- **show security alg sunrpc portmap**
- **clear security alg sunrpc portmap**

CompactFlash Card Support

- The *JUNOS Software Administration Guide* incorrectly states that JUNOS Software supports a 256-MB CompactFlash card size. JUNOS Software supports only 512-MB and 1024-MB CompactFlash card sizes.

Flow and Processing

- The “Understanding Selective Stateless Packet-Based Services” section in the *JUNOS Software Administration Guide* states: “The following security features are not supported with selective stateless packet-based services—stateful firewall NAT, IPsec VPN, DOS screens, J-flow traffic analysis, WXC integrated security module, security policies, zones, attack detection and prevention, PKI, ALGs, and chassis cluster.” This statement is not correct. With selective packet-mode, traffic that is sent through flow is able to use all of those services, even in a single VR scenario.

- Information about secure context and router context has been removed from the *JUNOS Software Administration Guide* and the *JUNOS Software Security Configuration Guide*. If you want to use both flow-based and packet-based forwarding simultaneously on a system, use the selective stateless packet-based services feature instead. For more information, see “Configuring Selective Stateless Packet-Based Services” in the *JUNOS Software Administration Guide*.

Hardware Documentation

- On J-SRX100 devices, the Alarm LED is off, indicating that the device is starting up.

  Note that when the device is on, if the Alarm LED is off, it indicates that no alarms are present on the device.

- The “Configuring Basic Settings for the J-SRX100 Services Gateway with a Configuration Editor” section in the *J-SRX100 Services Gateway Hardware Guide* contains the following inaccuracies:

  - The documentation incorrectly implies that the management port and loopback address must be defined for the device.
  - The documentation should indicate that the SSH remote access can be enabled.
  - The documentation indicates the CLI command **set services ssh**, which is incorrect. The correct command is **set system services ssh**.

- The J-Web Initial Set Up screenshot shown in the *J-SRX210 Services Gateway Getting Started Guide* and the *J-SRX240 Services Gateway Getting Started Guide* contains the following inaccuracies: The J-Web screenshot incorrectly shows the “Enable DHCP on ge-0/0/0.0” check box as disabled in factory default settings. The J-Web screenshot should indicate the “Enable DHCP on ge-0/0/0.0” check box as enabled in factory default settings.

- The Power over Ethernet section in the *J-SRX210 Services Gateway Hardware Guide* incorrectly states that PoE+ support (IEEE 802.3at standard) is available on all models of J-SRX210 devices.

  The guide should state that

  - PoE (IEEE 802.3 af) support is enabled only on the J-SRX210 Services Gateway PoE model.
  - PoE+ (IEEE802.3 at) support is enabled only on the J-SRX210 Services Gateway with Integrated Convergence Services model.

- 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 EuroDOCSIS 3.0 and DOCSIS J (Japan) models of the DOCSIS Mini-PIM are supported. The guide should state that only DOCSIS 3.0 US model of DOCSIS Mini-PIM is supported.

Installing Software Packages

- The current J-SRX210 documentation 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 Software 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 in both the *root* partition and under the **/var** hierarchy.

- The "Installing Software using the TFTPBOOT Method on the J-SRX100 and J-SRX210 Services Gateway" section in the *JUNOS Software Administration Guide* contains the following inaccuracies:

  - The documentation incorrectly implies that the TFTPBOOT method requires a separate secondary device to retrieve software from the TFTP server.
  - The documentation should indicate that the TFTPBOOT method does not work reliably over slow speeds or large latency networks.
  - The documentation indicates that before starting the installation, you only need to configure the gateway IP, device IP address, and device IP netmask manually in some cases, when actually you need to configure them manually in all cases.
  - The documentation should indicate that on the J-SRX100, J-SRX210, and J-SRX240 devices, only the **ge-0/0/0** port supports TFTP in uboot.
  - Step 2 of the "Installing JUNOS Software Using TFTPBOOT" instructions should mention that the URL path is relative to the TFTP server's TFTP root directory. The instructions should also mention that you should store the JUNOS Software image file in the TFTP server's TFTP root directory.
  - The documentation should indicate that the TFTPBOOT method installs software on the internal flash on J-SRX100, J-SRX210, and J-SRX240 devices.

- The *JUNOS Software Administration Guide* is missing the following information about installing software using USB on J-SRX100, J-SRX210, and J-SRX240 devices:

  You can install or recover the JUNOS Software using USB on J-SRX100, J-SRX210, and J-SRX240 devices. During the installation process, the installation package from the USB is installed on the specified boot media.

Before you begin the installation, ensure the following prerequisites are met:

- U-boot and Loader are up and running on the device.
- USB is available with the JUNOS Software package to be installed on the device.

To install the software image on the specified boot media:

1. Go to the Loader prompt. For more information on accessing the Loader prompt, see “Accessing the Loader Prompt” on page 260 of the *JUNOS Software Administration Guide.*

2. Enter the following command at the Loader prompt:

   Loader>install URL

   Where URL is *file:///package*

   Example:

   Loader>install *file:///junos-srxsme-9.4-200811.0-domestic.tgz*

When you are done, the file reads the package from the USB and installs the software package. After the software installation is complete, the device boots from the specified boot media.

NOTE: USB to USB installation is not supported. Also, on J-SRX100, J-SRX210, and J-SRX240 devices, the software image will always be installed on NAND flash.

Integrated Convergence Services

- The *JUNOS Software Integrated Convergence Services Configuration and Administration Guide* does not include **show** commands for JUNOS Release 10.1.
- On J-SRX210 and J-SRX240 devices with Integrated Convergence Services, the Transport Layer Security (TLS) option for the SIP protocol transport is not supported in JUNOS Release 10.1. However, it is documented in the Integrated Convergence Services entries of the *JUNOS Software CLI Reference Guide*.
- The *JUNOS Software CLI Reference* contains Integrated Convergence Services statement entries for the music-on-hold feature, which is not supported for JUNOS release 10.1.

Interfaces and Routing

- In the *JUNOS Software Interfaces and Routing Configuration Guide,* the “Configuring VDSL2 Interface” chapter incorrectly states that J-Web support for configuring the VDSL2 interface is not available in JUNOS Release 10.1. The J-Web support is available for VDSL2 interfaces in JUNOS Software Release 10.1.
- In the *JUNOS Software Interfaces and Routing Configuration Guide,* the “Configuring G.SHDSL Interface” chapter incorrectly states that J-Web support for configuring the G.SHDSL Interface is not available in JUNOS Release 10.1. The J-Web support is available for G.SHDSL interfaces in JUNOS Software Release 10.1.

J-Web

The following information pertains to J-SRX Series devices:

- **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.
- There is no documentation describing the J-Web pages for media gateways. To find these pages in J-Web, go to **Monitor>Media Gateway**.

Screens

The following information pertains to J-SRX Series devices:

- In the *JUNOS Software Design and Implementation Guide*, the "Implementing Firewall Deployments for Branch Offices" chapter contains incorrect screen configuration instructions.

  Examples throughout this guide describe how to configure screen options using the **set security screen *screen-name*** CLI statements. Instead, you should use the **set security screen ids-option *screen-name*** CLI statements. All screen configuration options are located at the **[set security screen ids-option *screen-name*]** level of the configuration hierarchy.

Related Topics

- New Features in JUNOS Release 10.1 for J-SRX Series Services Gateways on page 3
- Known Limitations in JUNOS Release 10.1 for J-SRX Series Services Gateways on page 20
- Issues in JUNOS Release 10.1 for J-SRX Series Services Gateways on page 23

Hardware Requirements for JUNOS Release 10.1 for J-SRX Series Services Gateways

- Transceiver Compatibility for J-SRX Series on page 42

Transceiver Compatibility for J-SRX Series

We strongly recommend that only transceivers provided by IBM be used on J-SRX Series interface modules. Different transceiver types (long-range, short-range, copper, and so on) can be used together on multiport SFP interface modules as long as they are provided by IBM. We cannot guarantee that the interface module will operate correctly if third-party transceivers are used.

Please contact IBM for the correct transceiver part number for your device.

Related Topics

- New Features in JUNOS Release 10.1 for J-SRX Series Services Gateways on page 3
- Known Limitations in JUNOS Release 10.1 for J-SRX Series Services Gateways on page 20

- Changes In Default Behavior and Syntax in JUNOS Release 10.1 for J-SRX Series Services Gateways on page 15
- Issues in JUNOS Release 10.1 for J-SRX Series Services Gateways on page 23
- Errata and Changes in Documentation for JUNOS Release 10.1 for J-SRX Series Services Gateways on page 37

Dual-Root Partitioning Scheme Documentation for J-SRX Series Services Gateways

Dual-Root Partitioning Scheme

JUNOS Release 10.1 supports dual-root partitions on J-SRX100, J-SRX210, and J-SRX240 devices. Dual-root partition allow the J-SRX Series devices to remain functional if there is file system corruption and facilitate easy recovery of the corrupted file system.

J-SRX Series devices that ship with JUNOS Release 10.1 are formatted with dual-root partitions from the factory. .

NOTE: The dual-root partitioning scheme allows the J-SRX Series devices to remain functional if there is file system corruption and facilitates easy recovery of the corrupted file system. Although you can install JUNOS Release 10.1 on J-SRX100, J-SRX210, and J-SRX240 devices with the single-root partitioning scheme, we strongly recommend the use of the dual-root partitioning scheme.

Selection of Boot Media and Boot Partition

When the J-SRX Series device powers on, it tries to boot the JUNOS Software from the default storage media. If the device fails to boot from the default storage media, it tries to boot from the alternate storage media.

J-SRX100, J-SRX210, and J-SRX240 devices boot from the following storage media (in order of priority):

1. Internal NAND flash (default; always present)
2. USB storage device (alternate)

With the dual-root partitioning scheme, the J-SRX Series device first tries to boot the JUNOS Software from the primary root partition and then from the backup root partition on the default storage media. If both primary and backup root partitions of a media fail to boot, then the J-SRX Series device tries to boot from the next available type of storage media. The J-SRX Series device remains fully functional even if it boots the JUNOS Software from the backup root partition of storage media.

Important Differences Between Single-Root and Dual-Root Partitioning Schemes

Note the following important differences in how J-SRX Series devices use the two types of partitioning systems.

- With the single-root partitioning scheme, there is one root partition that contains both the primary and backup JUNOS Software images. With the dual-root partitioning scheme, the primary and backup copies of JUNOS Software are in different partitions. The partition containing the backup copy is mounted only when required.
- With the dual-root partitioning scheme, when the **request system software add** command is performed for a JUNOS Software package, the contents of the other root partition are erased. The contents of the other root partition will not be valid unless the installation is completed successfully.
- With the dual-root partitioning scheme, after a new JUNOS Software image is installed, add-on packages like **jais** or **jfirmware** should be reinstalled as required.
- With the dual-root partitioning scheme, the **request system software rollback** CLI command does not delete the current JUNOS Software image. It is possible to switch back to the image by issuing the rollback command again.
- With the dual-root partitioning scheme, the **request system software delete-backup** CLI command does not take any action. The JUNOS Software image in the other root partition will not be deleted.

Reinstalling the Single-Root Partition Release Over TFTP

To reinstall JUNOS Software from the boot loader using a TFTP server:

1. Upload the JUNOS Software image to a TFTP server.
2. Stop the device at the loader prompt and set the following variables:
   - **ipaddr**

     ```
     loader> set ipaddr=<IP-address-of-the-device>
     ```
   - **netmask**

     ```
     loader> set netmask=<netmask>
     ```
   - **gatewayip**

     ```
     loader> set gatewayip=<gateway-IP-address>
     ```
   - **serverip**

     ```
     loader> set severip=<TFTP-server-IP-address>
     ```
3. Install the image using the following command at the loader prompt:

   ```
   user@host> install tftp://<server-ip>/<image-path-on-server>
   ```

   For example:

   ```
   loader> install tftp://10.77.25.12/junos-srxsme-9.6R1-domestic.tgz
   ```

   This will format the internal media and install the JUNOS Software image on the media with single-root partitioning.

Reinstalling the Single-Root Partition Release Using USB

To reinstall JUNOS Software from the boot loader using a USB storage device:

1. Format a USB storage device in MS-DOS format.
2. Copy the JUNOS Software image onto the USB storage device.
3. Plug the USB storage device into the J-SRX Series device.
4. Stop the device at the loader prompt and issue the following command:

   user@host> **install file://*<image-path-on-usb>***

   For example:

   loader> **install file:///junos-srxsme-9.6R1-domestic.tgz**

   This will format the internal media and install the JUNOS Software image on the media with single-root partitioning.

Recovery of the Primary JUNOS Software Image with Dual-Root Partitioning Scheme

If the J-SRX Series Services Gateway is unable to boot from the primary JUNOS Software image, and boots up from the backup JUNOS Software image in the backup root partition, a message is displayed on the console at the time of login indicating that the device has booted from the backup JUNOS Software image:

```
login: user
Password:
***********************************************************************
**                                                                   **
**  WARNING: THIS DEVICE HAS BOOTED FROM THE BACKUP JUNOS IMAGE      **
**                                                                   **
**  It is possible that the active copy of JUNOS failed to boot up   **
**  properly, and so this device has booted from the backup copy.    **
**                                                                   **
**  Please re-install JUNOS to recover the active copy in case       **
**  it has been corrupted.                                           **
**                                                                   **
***********************************************************************
```

Because the system is left with only one functional root partition, you should immediately restore the primary JUNOS Software image. This can be done by installing a new image using the CLI or J-Web. The newly installed image will become the primary image, and the device will boot from it on the next reboot.

CLI Changes

This section describes CLI changes when the J-SRX Series device runs JUNOS Release 10.1 with the dual-root partitioning scheme.

- Changes to the Snapshot CLI on page 46
- partition Option with the request system software add Command on page 47

Changes to the Snapshot CLI

On a J-SRX Series device, you can configure the primary or secondary boot device with a “snapshot” of the current configuration, default factory configuration, or rescue configuration. The snapshot feature is modified to support dual-root partitioning. The options **as-primary**, **swap-size**, **config-size**, **root-size**, **var-size**, and **data-size** are not supported on J-SRX Series devices.

With the dual-root partitioning scheme, performing a snapshot to a USB storage device that is less than 1 GB is not supported.

With the dual-root partitioning scheme, you must use the **partition** option when performing a snapshot. If the **partition** option is not specified, the snapshot operation fails with a message that the media needs to be partitioned for snapshot.

The output for the **show system snapshot** CLI command is changed in devices with dual-root partitions to show the snapshot information for both root partitions:

```
user@host> show system snapshot media usb
Information for snapshot on       usb (/dev/da1s1a) (primary)

            Creation date: Jul 24 16:16:01 2009

            JUNOS version on snapshot:

            junos  : 10.1I20090723_1017-domestic

            Information for snapshot on       usb (/dev/da1s2a) (backup)

            Creation date: Jul 24 16:17:13 2009

            JUNOS version on snapshot:

            junos  : 10.1I20090724_0719-domestic
```

NOTE: You can use the **show system snapshot media internal** command to determine the partitioning scheme present on the internal media. Information for only one root is displayed for single-root partitioning, whereas information for both roots is displayed for dual-root partitioning.

NOTE: Any removable media that has been formatted with dual-root partitioning will not be recognized correctly by the **show system snapshot** CLI command on systems that have single-root partitioning. Intermixing dual-root and single-root formatted media on the same system is strongly discouraged.

partition Option with the request system software add Command

A new **partition** option is available with the **request system software add** CLI command. Using this option will cause the media to be formatted and repartitioned before the software is installed.

When the **partition** option is used, the format and install process is scheduled to run on the next reboot. Therefore, it is recommended that this option be used together with the **reboot** option.

For example:

```
user@host>request system software add junos-srxsme-10.1R1-domestic.tgz no-copy
no-validate partition reboot
Copying package junos-srxsme-10.01R1-domestic.tgz to var/tmp/install

Rebooting ...
```

The system will reboot and complete the installation.

⚠ WARNING: Using the **partition** option with the **request system software add** CLI command erases the existing contents of the media. Only the current configuration is preserved. Any important data should be backed up before starting the process.

Dell Documentation and Release Notes

To download the hardware documentation for your product and the JUNOS Software documentation for PowerConnect J-Series J-EX Series products , see the following Dell support website:

http://www.support.dell.com .

To download JUNOS Software documentation for all other PowerConnect J-Series products, see the following Juniper Networks support website: http://www.juniper.net/techpubs/ .

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, seehttp://www.support.dell.com .

Revision History

15 February 2010—Revision 1, JUNOS Release 10.1R1

17 February 2010—Revision 2, JUNOS Release 10.1R1

13 May 2010—Revision 2, JUNOS Release 10.1R2

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

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