Release Notes: Junos® OS Release 15.1X49-D170 for the SRX Series

Release 15.1X49-D170
08 July 2019
Revision 2

Contents

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, EX Series, M Series, MX Series, PTX Series, vSRX, QFabric, QFX Series, SRX Series, and T Series.

These release notes accompany Junos OS Release 15.1X49-D170 for the SRX Series. They describe new and changed features, known behavior, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/software/junos/.

NOTE: Junos OS Release 15.1X49-D170 supports the following devices: SRX300, SRX320, SRX340, SRX345, and High Memory (SRX550M), SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices with host subsystems composed of either an SRX5K-RE-1800X4 (RE2) with an SRX5K-SCBE (SCB2), or an SRX5K-RE-1800X4 (RE2) with an SRX5K-SCB3 (SCB3), and vSRX.

For more details about SRX5400, SRX5600, and SRX5800 devices hardware and software compatibility, please see https://kb.juniper.net/KB30446. If you have any questions concerning this notification, please contact the Juniper Networks Technical Assistance Center (JTAC).

New and Changed Features

This section describes the new features and enhancements to existing features in Junos OS Release 15.1X49-D170 for the SRX Series devices. For information about new and changed features starting in Junos OS Release 15.1X49-D10 through Junos OS Release 15.1X49-D160, refer to the Release Notes listed in the Release 15.1X49 section at Junos OS for SRX Series page.

Release 15.1X49-D170 Software Features

Virtual Routing and Forwarding

- **VRF group in L3VPN traffic (SRX Series and vSRX)**—Starting in Junos OS Release 15.1X49-D170, to support mid-stream routing, VRF undergoes changes for processing a session among a group of MPLS VRF instances in an L3VPN MPLS network. These VRF instances which are logically part of a given L3VPN traffic route are grouped into a VRF group. The VRF groups allows the session to switch from one MPLS VRF to another MPLS VRF.

  VRF group supports the following features:

  - Overlapping in VPN session
  - VRF group Policy
  - VRF group NAT
  - VRF group ALG

  [See Security Policy for Controlling Traffic for VRF Routing-Instance]

Related Documentation

Changes in Behavior and Syntax

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 15.1X49-D170.

Application Identification

- **Security RT logs (SRX Series)**—Starting in Junos OS Release 15.1X49-D170, AppTrack session create, session close, route update, and volume update logs are enhanced to include VRF-name for both Source-VRF and Destination-VRF in syslog.

  [See Application Tracking.]

VPN

- **PKI daemon failover (SRX Series)**—Starting in Junos OS Release 15.1X49-D170, the PKI daemon might fail after RG0 failover on the new node, causing all the IPsec VPNs using the public key infrastructure (PKI) to go down when:
  - A local certificate used for IPsec VPN is revoked by the certificate authority (CA).
  - Certificate revocation list (CRL) check is disabled.
  - CRL is not cleared.

  [See revocation-check (Security PKI) and Understanding Online Certificate Status Protocol and Certificate Revocation Lists.]

- **Encryption algorithm (SRX Series)**—Starting in Junos OS Release 15.1X49-D170, when AES-GCM 128-bit or AES-GCM 256-bit encryption algorithms are configured in the IPsec proposal, it is not mandatory to configure the AES-GCM encryption algorithm in the corresponding IKE proposal.

  [See IPsec VPN Configuration Overview and encryption-algorithm (Security IKE).]

Related Documentation

- New and Changed Features on page 4
- Migration, Upgrade, and Downgrade Instructions on page 14
- Documentation Updates on page 14
- Known Behavior on page 5
- Resolved Issues on page 12

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 15.1X49-D170.

Application Security

- On SRX1500 devices, after you change the revocation configuration of a CA profile, the change cannot be populated to the SSL-I revocation check. We recommend that you change the SSL-I configuration to enable or disable the certificate revocation list (CRL) checking instead of the CA profile configuration. PR1143462

- On SRX1500 devices in a chassis cluster with the Juniper Sky ATP solution deployed, if you disable and then reenable CRL checking of certificate validity, the system does not reenable CRL checking. PR1144280

Authentication and Access Control

- On SRX Series devices, TLS version 1.0 and TLS version 1.1 SSL protocols are blocked because of reported security vulnerabilities. This change might affect users accessing J-Web or the Web authentication GUI, or using dynamic VPN through the Pulse client when using an older Junos OS version or earlier version browsers where TLS version 1.2 protocol is not supported. This change affects Junos OS Release 15.1X49-D100 and later releases. PR1283812

Chassis Clustering

- On SRX550M devices in a chassis cluster, traffic loss for about 10 seconds is observed when there is a power failure on the active chassis cluster node. PR1195025
- On SRX340 and SRX345 devices, half-duplex mode is not supported, because BCM53426 does not support half-duplex mode. BCM5342X SoC port configurations and BCM53426 do not have a QSGMII interface. Only the QSGMII port supports half-duplex mode. PR1149904
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, if you enable IP monitoring on redundancy groups, the feature might not work correctly on the secondary node if the reth interface has more than one physical interface configured on each node, which enables a redundant Ethernet interface LAG. This issue occurs because the backup node will send traffic using the MAC address of the lowest port in the bundle. If the response toward the same MAC address arrives on a different physical port in the bundle, then the internal switch in the SRX Series device will drop the response packets. PR1344173
- During chassis cluster cold synchronization, the GTP-U session is synchronized to the secondary device before the GTP-U tunnel. As a result, the GTP-U tunnel cannot be linked with the corresponding GTP-U flow session. The GTP-U tunnel is not refreshed by the GTP-U traffic until new sessions are created. If an old session does not age out on the primary device, then all the GTP-U traffic goes through fast path and no session creation events are triggered. After the GTP-U timeout period, the tunnels on the secondary device will also age out earlier. PR1353791

Flow-Based and Packet-Based Processing

- On SRX5400, SRX5600, and SRX5800 devices, in a central point architecture, system logs are sent per second per SPU. Hence, the number of SPUs defines the number of system logs per second. PR1126885
- On SRX1500 devices, the log buffer size is increased in event mode. When the log buffer size is 1000, the Packet Forwarding Engine generates log bursts when there are more than 30 entries and then more logs are dropped. PR1133757
- On SRX5400 devices, if a username or a group name contains the following characters: "*" (ASCII 0x2a), "(" (ASCII 0x28), ")" (ASCII 0x29), "\" (ASCII 0x5c), and NUL (ASCII

0x00), the query from the device to the LDAP server might time out, leading to high CPU utilization. PR1157073

- On SRX Series devices, after a user changes some interface configuration, a reboot warning message might appear. The warning message is triggered only when the configuration of the interface mode is changed from route mode to switch or mixed mode. This is a configuration-related warning message and might not reflect the current running state of the interface mode. PR1165345
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, the current Ethernet switching MAC aging uses software to age out bulk learned MAC addresses. You cannot age out a specific MAC address learned at a specific time immediately after the configured age. Theoretically, the MAC address might age out close to two times the configured age-out time. PR1179089
- On SRX300, SRX320, SRX340, SRX345, and SRX1500devices, the command **set system internet-options tcp-mss *value*** does not work in Junos OS Release 15.1X49. PR1213775
- The modem profile is not active until a profile is defined. You need to define a profile before selecting a profile. PR1254427
- On the SRX300, SRX320, SRX340, SRX345, and SRX550M devices, after a certain period of enabling dot1x, multiple first-message EAP frames with the same timestamp are transmitted. However, this does not affect any dot1x functionality. PR1245325
- On SRX Series devices, OSPF over GRE over IPsec is not supported on a device with a standalone central point. PR1274667
- On SRX Series devices, user firewall process useridd retries connecting to the autodiscovery server but fails to connect to the server. Due to this issue, the useridd is unable to handle other messages. Hence, the administrator must remove or deactivate those unused or incorrect user firewall configurations. PR1307851
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, using an SFP-T module can cause an early linkup on connecting a device during the boot process. PR1314167
- FTP using Microsoft NLB does not work correctly in Layer 2 transparent mode. PR1341446

Interfaces and Routing

- On SRX1500 devices, when a 1-gigabit SFP-T transceiver is used on 1-Gigabit Ethernet ports (ge-0/0/12 through ge-0/0/15), the ge- interface does not operate at 100-Mbps speed. PR1133384
- On SRX Series devices, the **show arp** command will show all the ARP entries learned from all interfaces. When Layer 2 global mode is switching, the ARP entries learned from the IRB interface can only show one specific VLAN member port instead of the actual VLAN port learned in the ARP entries. PR1180949
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, use the logical tunnel interface lt-0/0/0 as the destination interface option for an RPM probe server on the device. PR1257502

- If the PPP interface is configured, then traffic received on this interface is sometimes reordered. PR1340417
- When using a crossover cable, the interfaces are down when there is a change from 10 million to 100 million. PR1387978

J-Web

- On SRX550M and SRX1500 devices, there is no option to configure Layer 2 firewall filters from J-Web, irrespective of the device mode. PR1138333
- On SRX Series devices in a chassis cluster, if you want to use J-Web to configure and commit the configurations, you must ensure that all other user sessions are logged out, including any CLI sessions. Otherwise, the configurations might fail. PR1140019
- On SRX1500 devices in J-Web, snapshot functionality (Maintain >Snapshot > Target Media > Disk > Click Snap Shot) is not supported. PR1204587
- On SRX Series devices, DHCP relay configuration under the Configure > Services > DHCP > DHCP Relay page is removed from J-Web in Junos OS Release 15.1X49-D60. The same DHCP relay can be configured using the CLI. PR1205911
- On SRX Series devices, the DHCP client bindings items under the Monitor menu is removed. The same bindings can be seen in the output of the **show dhcp client binding** CLI command. PR1205915
- On SRX Series devices, you cannot create profiles for CL-1/0/0 using J-Web and the CLI. An error message, **interface not found**, is displayed. We recommended using only one LTE mPIM in the supported devices. PR1262543
- On SRX Series devices, when you log in to J-Web and navigate to Monitor>Services>DHCP> DHCP SERVER & DHCP RELAY, and click the Help page icon, the Online Help page displays a 404 error message. PR1267751
- On SRX Series devices, adding 2000 global addresses at a time to the SSL proxy profile exempted addresses can cause the webpage to become unresponsive. PR1278087
- On SRX Series devices, you cannot view the custom log files created for event logging in J-Web. PR1280857
- On SRX Series devices with Junos OS Release 15.1X49-D90 and earlier releases, J-Web does not display the **IDP log locally saved** notification. PR1336341

Layer 2 Ethernet Services

- On SRX1500 devices configured in Ethernet switching mode, only a few MAC entries are shown in the output of the **show ethernet-switching table** command, even after a MAC age-out time. This issue is applicable only when the MAC learning table has more than 17,000 MAC entries. PR1194667
- On SRX300, SRX320, SRX340, and SRX345 devices, you cannot launch the setup wizard after using the reset configuration button when the device is in Layer 2 transparent mode. You can launch the setup wizard by using the reset configuration button on the device when the device is in switching mode. PR1206189

- On SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices, VPLS traffic forwarding stops working after enabling the Ethernet switching configuration. VPLS and Ethernet switching must not be configured together on the same device. We recommend not using the Ethernet switching configuration on these devices when VPLS is enabled. PR1214803
- On SRX345 and SRX550M devices, frames carried with a priority bit on the Tag Protocol Identifier (TPID) will be lost when the packet passes through with Layer 2 forwarding. PR1229021

Platform and Infrastructure

- On SRX5800 devices, if a global SOF policy (all session **service-offload**) is enabled, the connections per second (CPS) will be impacted due to IOC2 limitation. We recommend using an IOC3 card if more sessions are required for SOF or lowering the SOF session amount to make sure the IOC2 is capable of handling it. PR1121262
- On SRX5800 devices, even though the system service REST API is configured and committed, all the configuration changes in this commit do not take effect. This issue occurs because the REST API process fails to come up and the interface IP address is not available during startup. The configuration is not read by the Routing Engine. PR1123304
- On SRX4100 and SRX4200 devices, although the CLI is configurable, the following features are not supported: group VPN, VPN Suite B, and encrypted control links when in a chassis cluster. PR1214410

Unified Threat Management (UTM)

- On SRX Series devices with Sophos Antivirus (SAV) configured, some files that have a size larger than the **max-content-size** might not go into fallback state. Instead, some protocols do not predeclare the content size. PR1005086
- On SRX550M devices using the 12.1X49-D30 release for the enhanced Web filtering feature, performance drop is observed PR1138189
- On SRX1500 devices, when the CPU usage is very high (above 95 percent), there is a possibility that the connection between the AAMW process and the PKI daemon can stop. In this case, the AAMW process remains in an initializing state until the connection is established. PR1142380
- On SRX Series devices, if AAMW is enabled, and SMTP is configured in the AAMW policy with fallback permission enabled under the long network latency between the devices and AWS is running the Juniper Sky ATP service, there might be a file submission timeout error. When sending the timeout error, there is a possibility that the e-mail sent from Outlook might stay in the outbox of the sender, and the receiver might not receive the e-mail. PR1254088
- On SRX Series devices, AAMW-established sessions always use the configured AAMW parameters at the time of session establishment. The configuration changes will not retroactively affect the already established sessions. For example, a session established when the verdict threshold is 5 will always have 5 as the threshold even if the verdict threshold changes to other values during the session lifetime. PR1270751

Upgrade and Downgrade

- When you perform a firmware upgrade or downgrade, a FIPS core file is generated. In Junos OS FIPS mode, the file integrity checking application **veriexec** treats the new updated firmware file as a corrupted Junos OS file. This is an expected behavior by design. PR1268240
- Upgrading from the Junos OS release 15.1X49-D40 to Junos OS release 15.1X49-D120, the GRUB loader stops on node0. PR1347046

User Authentication and Firewall

- On SRX Series devices, firewall authentication cannot retrieve domain information from the access profile configuration. That is because the firewall authentication will not push user domain information to the Juniper Identity Management Service server in case the user authenticates through **web-authentication, pass-through**, or **web-redirect** with an LDAP access profile. PR1281063
- Primary group-domain computers are not supported by the user firewall integration. PR1361512

VPNs

- On SRX Series devices, if an IPsec VPN tunnel is established using IKEv2 because of bad SPI, packet drop might be observed during **CHILD_SA rekey** when the device is the responder for this rekey. PR1129903
- On SRX Series devices, the VPN monitoring feature is not working correctly in JunosOS Release 15.1X49-D40. PR1143955
- On SRX5400, SRX5600, and SRX5800 devices, when CoS is enabled on the st0 interface and the incoming traffic rate destined for the st0 interface is higher than 300,000 packets per second (pps) per SPU, the device might drop some of the high-priority packets internally and shaping of outgoing traffic might be impacted. We recommend that you configure the appropriate policer on the ingress interface to limit the traffic below 300,000 pps per SPU. PR1239021

Related Documentation

- New and Changed Features on page 4
- Migration, Upgrade, and Downgrade Instructions on page 14
- Changes in Behavior and Syntax on page 4
- Known Behavior on page 5
- Resolved Issues on page 12

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 15.1X49-D170.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Application Security

- On SRX Series devices, if you add or remove the application signature in the application firewall (AppFW) with multiple rules, the AppFW might fail to match the application signatures. PR1404161

Chassis Clustering

- On SRX Series devices in a chassis cluster configured with sampling or packet capture, traffic loss is observed when the redundancy group 0 (RG0) fails over from node0 to node1 and returns back to node0. PR1379734

Flow-Based and Packet-Based Processing

- On SRX1500 devices, when the CPU stops the system does not get reset by the watchdog service. PR1361843
- On SRX1500 devices, the activity LEDs for the 1-Gigabit Ethernet or 10-Gigabit Ethernet ports are not working properly. PR1380928
- On SRX Series devices, the flowd process might stop if the **enable-session-cache** command is configured under the **[SSL termination]** hierarchy. PR1407330
- This issue occurs on SRX Series devices in a chassis cluster when using the equal-cost multipath (ECMP) routing between multiple interfaces on both the node0 and node1. If a session is initiated through one node and the ingress traffic comes in through the other node, some packets might get dropped because of frequent reroute between the interfaces.
  As a workaround, avoid using ECMP and ensure the traffic flows to one node0 or node 1. PR1410233

Network Address Translation (NAT)

- This issues occurs on SRX Series devices if UTM Web filtering is configured and an application is configured with the source and destination NAT rule. The nsd process might stop and the Web filtering might not work if the application is deleted or modified. PR1406248

Related Documentation

- New and Changed Features on page 4
- Migration, Upgrade, and Downgrade Instructions on page 14
- Changes in Behavior and Syntax on page 4
- Resolved Issues on page 12
- Documentation Updates on page 14

Resolved Issues

This section lists the issues fixed in hardware and software in Junos OS Release 15.1X49-D170. For information about resolved issues in Junos OS Release 15.1X49-D10 through Junos OS Release 15.1X49-D160, refer to the Release Notes listed in the Release 15.1X49 section.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Application Layer Gateways (ALGs)

- On SRX Series devices, the H.323 protocol voice packets might be dropped. PR1400630

Chassis Clustering

- On SRX Series devices, during GPRS tunneling protocol (GTP) inspection, the GPRS tunneling protocol version 2 (GTPv2) modifies the bearer request packets. Any bearer packets not containing the fully qualified tunnel endpoint identifier information are dropped. PR1399658

Flow-Based and Packet-Based Processing

- On SRX Series devices, OSPF over GRE over IPsec is not supported on a device with a standalone central point. PR1274667
- The fan speed might frequently keep changing between normal and full. PR1316192
- On SRX Series devices, the PKI daemon might stop after RG0 failover. PR1379348
- If you use the TCP proxy, the large file downloads slow down for few seconds. PR1386122
- The SRX320 device might trigger traffic flow while acting as the VRRP backup device, with the Layer 2 link between the devices forwarding the VRRP protocol message. PR1386292
- On SRX Series devices running integrated user firewall, group membership changes are not processed correctly after a user's Windows logon account name is modified while retaining the same distinguished name. PR1394049
- On SRX Series devices, when you switch the interface from family ethernet-switching to family inet or inet6, or vice versa, you might observe traffic loss. PR1394850
- On SRX Series devices, the IPv6 address remains in tentative state after disabling and reenabling the fxp0 interface. PR1394923
- On SRX Series devices, the connection to JIMS fluctuates, resulting in failover. PR1398140
- On SRX4600, SRX5400, SRX5600 and SRX5800 devices, if CPU utilization is high the BGP packets might get dropped. PR1398407
- On SRX1500 devices, the VLAN push function might not work on the encapsulated interfaces. PR1398877

- On SRX Series devices, accessing the management interface fails if the console displays the message **kern.maxfiles limit exceeded by uid 65534, please see tuning(7)**. PR1402242
- On SRX Series devices, in rare conditions the flowd process stops if the IPsec tunnel traffic route is changed. PR1406210

General Routing

- On SRX Series devices, the configuration commit **error: DHCP service may not be de-configured while clients are present** is displayed even though you clear all the DHCP clients. PR1400918

J-Web

- On SRX Series devices, the **Skip to J-web** option does not work if the password contains fewer than 8 characters. PR1371353
- The next-hop IP addresses are not displayed in the routing table on J-Web. PR1398650
- The special characters used in the preshared key are removed after committing the configuration on J-Web. PR1399363
- In J-Web, the error messages related to the Modular Interface Card (MIC) and the physical interface are displayed on the Description. PR1403274
- On SRX Series devices, an mgd core file is seen if the CLI editor is configured using J-Web. PR1404946

Layer 2 Ethernet Services

- On SRX Series devices, a packet is not transited by the IRB interface when Layer 2 learning is in switching mode. PR1218376

Multiprotocol Label Switching (MPLS)

- On SRX550M devices in a chassis cluster, the BGP and OSPF flapped, causing traffic loss and the rpd process to stop. PR1366575

Platform and Infrastructure

- In case failover occurs while the device is handling many concurrent Web authentications, the httpd CPU usage might be high. PR1352133
- On SRX Series devices, the flowd process stops if it goes into a dead loop. PR1403276

Unified Threat Management (UTM)

- On SRX Series devices configured with Web proxy, the whitelist and blacklist functions do not work for HTTPs traffic. PR1401996

Related Documentation

- New and Changed Features on page 4

Documentation Updates

There are no errata or changes in Junos OS Release 15.1X49-D170 for the SRX Series documentation.

Migration, Upgrade, and Downgrade Instructions

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 12.3X48, 15.1X49, 17.3, and 17.4 are EEOL releases. You can upgrade from Junos OS Release 15.1X49 to Release 17.3 or from Junos OS Release 15.1X49 to Release 17.4. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

Upgrade from Junos OS Release 17.4 to successive Junos OS Release, is supported. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

For more information about EEOL releases and to review a list of EEOL releases, see https://www.juniper.net/support/eol/junos.html.

For information about software installation and upgrade, see the Installation and Upgrade Guide for Security Devices.

For information about ISSU, see the Chassis Cluster Feature Guide for Security Devices.

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 4
- Known Behavior on page 5
- Documentation Updates on page 14
- Resolved Issues on page 12

Product Compatibility

This section lists the product compatibility for any Junos OS SRX Series mainline or maintenance release.

- Hardware Compatibility on page 15
- Transceiver Compatibility for SRX Series Devices on page 15

Hardware Compatibility

To obtain information about the components that are supported on the device, and special compatibility guidelines with the release, see the SRX Series Hardware Guide.

To determine the features supported on SRX Series devices in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at https://pathfinder.juniper.net/feature-explorer/.

Transceiver Compatibility for SRX Series Devices

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

Please contact Juniper Networks for the correct transceiver part number for your device.

Finding More Information

For the latest, most complete information about known and resolved issues with the Junos OS, see the Juniper Networks Problem Report Search application at https://prsearch.juniper.net.

For regulatory compliance information about Common Criteria, FIPS, Homologation, RoHS2, and USGv6 for Juniper Networks products, see the Juniper Networks Compliance Advisor.

To access Software Release Notifications for Junos OS Service Releases, visit our Knowledge Center at https://support.juniper.net/support/. You'll need to log in to your Juniper Account. From the Knowledge Center, search by the specific release number, for

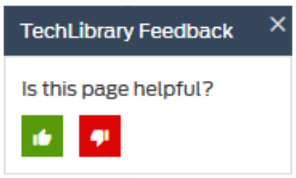
example 17.4R1-S2. Use the Software Release Notifications to download software, and learn about known and resolved issues for specific service releases.

Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos OS feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at https://apps.juniper.net/feature-explorer/.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post sales technical support, you can access our tools and resources online or open a case with JTAC.

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://support.juniper.net/support/warranty/.

- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://support.juniper.net/support/
- Search for known bugs: https://kb.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://support.juniper.net/support/downloads/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://forums.juniper.net
- Open a case online in the CSC Case Management tool: https://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at https://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at https://support.juniper.net/support/requesting-support/.

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

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

To provide a core file to Juniper Networks for analysis, compress the file with the **gzip** utility, rename the file to include your company name, and copy it to **ftp.juniper.net/pub/incoming**. Then send the filename, along with software version information (the output of the **show version** command) and the configuration, to **support@juniper.net**. For documentation issues, fill out the bug report form located at https://www.juniper.net/documentation/feedback/.

Revision History

28, February 2019—Revision 1— Junos OS 15.1X49-D170 – SRX Series.

08, July 2019—Revision 2— Junos OS 15.1X49-D170 – SRX Series.