Chapter 8

Configuring a Unified In-Service Software Upgrade

This chapter describes how to prepare for and perform a unified in-service software upgrade (unified ISSU) of JUNOSe software on E120 and E320 routers. A unified in-service software upgrade provides a way to upgrade to a higher-numbered release while minimizing the effect of the upgrade on traffic forwarded through the router.

- Unified ISSU Overview on page 401
- Unified ISSU Platform Considerations on page 403
- Unified ISSU Terms That Describe SRP and Line Module Behavior on page 403
- Unified ISSU References on page 404
- Unified ISSU Phases Overview on page 404
- Application Support for Unified ISSU on page 412
- Unexpected Application-Specific Behavior During Unified ISSU on page 418
- Before You Begin a Unified In-Service Software Upgrade on page 430
- Upgrading Router Software with Unified ISSU on page 432
- Halting the Unified ISSU Process and Restoring the Original State of the Router on page 435
- Monitoring a Unified In-Service Software Upgrade on page 437

Unified ISSU Overview

In software releases numbered lower than Release 6.0, all line modules are reloaded when an SRP switchover occurs. This reload disconnects user sessions and disrupts forwarding through the chassis. Stateful SRP switchover was introduced in JUNOSe Release 6.0 to minimize the impact to the router of a stateful switchover from the active SRP module to the standby SRP module. Stateful SRP switchover (high availability) maintains user sessions during the switchover and data forwarding through the router continues to flow with little impact, thus improving the overall availability of the router.

The unified in-service software upgrade (unified ISSU) feature further extends router availability. Unified ISSU enables you to upgrade the router to a higher-numbered software release without disconnecting user sessions or disrupting forwarding through the chassis.

A conventional software upgrade—one that does not use the unified ISSU process—causes a router-wide outage for all users. Only static configurations (stored on the flash card) are maintained across the upgrade; all dynamic configurations are lost. A conventional upgrade takes 30-40 minutes to complete, with additional time required to bring all users back online.

When you perform a unified in-service software upgrade on a router that has one or more modules that do not support unified ISSU, these modules alone are upgraded by means of the legacy, conventional upgrade process. The unsupported modules undergo a cold reboot at the beginning of the unified ISSU process, and are held down until the in-service software upgrade is completed. Connections that pass through the unsupported modules are lost. The interfaces on these modules pass into a down state, which causes the physical layer and link layer to go down during the in-service software upgrade for those modules.

Applications that do not support unified ISSU applications cannot maintain state and configuration with minimal traffic loss across the upgrade to a higher-numbered release. When you attempt a unified in-service software upgrade on a router on which an ISSU-challenged application is configured, the in-service software upgrade cannot proceed.

Router Behavior During a Unified In-Service Software Upgrade

The following behaviors are characteristic of a unified in-service software upgrade.

- Connections that were established before you begin the in-service software upgrade are maintained across the upgrade. Any such connection that was forwarding data continues to do so during and after the upgrade.
- New connections are denied until the upgrade is completed.
- Packet loss during the upgrade is limited. Bandwidth through the modules is reduced, but the impact is minimal.
- Graceful restart protocols do not time out during the in-service software upgrade.
- The in-service software upgrade has a minimal effect on the control and data planes. During the SRP module upgrade phase, forwarding through the fabric is interrupted for about 1 second. During the line module upgrade phase, forwarding through the chassis is interrupted for about 30 seconds.
- Diagnostic software is not run on any modules during a unified in-service software upgrade.

- The router will undergo a cold restart if you attempt to upgrade the software to a lower-numbered version with unified ISSU. The in-service software upgrade must be to a higher-numbered release than the running release.
- Additional memory is consumed during a unified in-service software upgrade. Available memory on a line module might not be sufficient due to the module's configuration. Unified ISSU can detect this limitation during the upgrade procedure and exit the process.

Unified ISSU Platform Considerations

Unified ISSU is supported on E120 and E320 routers.

For information about modules supported on E120 and E320 routers:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support unified ISSU.

Redundant SRP modules are required for unified ISSU support.

Unified ISSU is not supported on the ERX-7xx models, ERX-14xx models, and the ERX-310 router.

Unified ISSU Terms That Describe SRP and Line Module Behavior

Table 46 defines terms relevant to module behavior during a unified in-service software upgrade.

Table 46: Unified ISSU-Related Terms

Term	Meaning
Cold boot	The SRP module or line module loads diagnostics from the flash file system and runs them. When the diagnostics successfully complete, the operational image is loaded from the flash file system and then cold started.
Cold start	The SRP module or line module is initialized from the loaded operational image. The line modules are reloaded and the configuration is read from flash memory. When the line modules are operational, their configuration data is bulk downloaded and their interfaces become operational.
Cold restart	If the active SRP module fails, the standby SRP module assumes the role of active SRP module. When high availability is not configured, the cold restart is similar to the cold start, except that the applications are already loaded into memory on the standby SRP module and ready to be started. The line modules are reloaded.

Table 46: Unified ISSU-Related Terms (continued)

Term	Meaning
Warm restart	If the active SRP module fails, the standby SRP module takes the role of active SRP module. Mirrored configuration data as well as any mirrored volatile data are already resident in memory. The line modules continue to forward data (with a small loss of packets when the fabric is switched from the formerly active SRP module to the newly active SRP module). The protocols and other applications re-initialize from the mirrored data and resynchronize communications with the line modules. When resynchronization is completed, the router resumes normal operations, including updates of any routing tables that result from changes that occurred during the warm restart.

Unified ISSU References

For more information about stateful SRP switchovers see *Chapter 7, Managing High Availability*.

For more information about SRP module redundancy, see *Chapter 6, Managing Modules*.

Unified ISSU Phases Overview

The JUNOSe software includes software modules that operate the following hardware components:

- SRP module
- Line module control plane
- Line module forwarding plane

A unified in-service software upgrade replaces the currently operating software on each of these components with a higher-numbered release. The unified ISSU also upgrades or re-creates the state and configuration data of the configured applications.

Before you begin the in-service software upgrade, you must first prepare the router for the upgrade. See *Before You Begin a Unified In-Service Software Upgrade* on page 430 for more information.

The in-service software upgrade takes place in three phases:

1. Initialization Phase—When you issue the **issu initialize** command, unified ISSU verifies whether all prerequisites for the upgrade have been met. The router is prepared for the upgrade. The configuration that has been mirrored to the standby SRP module is upgraded according to the upgrade release. This phase can last from a few minutes up to 40 minutes depending on the number of software releases across which the router is being upgraded.

2. Upgrade Phase—When you issue the **issu start** command, unified ISSU again verifies whether all prerequisites for the upgrade have been met. During this phase the line module control plane and forwarding plane are upgraded and all three hardware components are resynchronized.

3. Service Restoration Phase—This phase automatically begins without user intervention when the upgrade phase has completed. During this final phase, the router is returned to a normal, runtime state.

The following sections describe these phases in more detail.

Unified ISSU Initialization Phase Overview

When you issue the **issu initialize** command, unified ISSU first verifies whether all requirements for the upgrade are met. The verification process examines the running release, the SRP modules, the line modules, line module redundancy, and the router configuration.

The **issu initialize** command does not interrupt or disrupt any of the runtime operations of the router. The command has no effect on changes of authorization, forwarding, or subscribers (except that the rate of logins might be affected). You cannot manually change the file system redundancy mode from high availability to file synchronization until the unified in-service software upgrade is completed.

NOTE: We recommend that you make no configuration changes after you have issued the **issu initialization** command. As a best practice, ensure that your configuration is complete before you start the software upgrade.

During the initialization phase, you can halt the in-service software upgrade at any time and revert either to a normal SRP module switchover or to the previous state of the router. To stop the unified ISSU process, you must issue the **issu stop** command. If instead you simply exit the CLI session, the unified ISSU initialization phase continues.

The action taken when a requirement is not met depends on the requirement. For some failed verifications, the CLI warns you of the issue and prompts you to proceed or quit the upgrade process. More serious failures cause the CLI to exit the command and provide a message describing the issue.

NOTE: We recommend that you issue the **show issu** command before beginning the in-service software upgrade. The output of the command lists any necessary conditions that are not currently met on the router. You can therefore correct these failures before entering into the upgrade. You can issue the **show issu** command at any time.

NOTE: On E120 and E320 routers, you can hot swap an IOA during the initialization phase without affecting the in-service software upgrade. However, we strongly recommend that you perform any necessary hot swaps before you issue the **issu initialize** command.

If the standby SRP module reloads during the initialization phase, unified ISSU is halted. You must begin again by issuing the **issu initialize** command.

Application Data Upgrade on the Standby SRP Module

Synchronized modules can become unsynchronized because you can change the router configuration at any time until you issue the **issu start** command. When the verification process is completed, unified ISSU starts up the stateful SRP switchover process to maintain synchronization between the active SRP module and the standby SRP module during the SRP module upgrade phase.

NOTE: An SRP switchover from the active SRP module to the standby SRP module at this point in the in-service software upgrade causes a cold restart of the router because the SRP modules are running two different releases. The current release is on the active SRP module and the upgrade release is on the standby SRP module.

The application and configuration data that has been mirrored to the standby SRP module is upgraded as required by the new software release. The CLI displays the progress of the SRP module upgrade.

While data on the standby SRP module is upgraded, any new changes that are mirrored from the primary SRP module to the standby SRP module are also upgraded to the version required by the armed release.

NOTE: This process consumes significant CPU resources on the redundant SRP module and can take a considerable amount of time to complete. Performance of the active SRP module might be affected during the SRP module upgrade.

When the upgrade release has been synchronized to the standby SRP module, stateful SRP switchover is disabled until the in-service software upgrade is completed.

If you configure an application that does not support unified ISSU during the initialization phase, the initialization phase completes, but the **issu start** command subsequently fails.

Line Module Arming

When the upgrade of the application data on the standby SRP upgrade is completed, unified ISSU temporarily arms the line modules with the upgrade release in a backup region of the memory.

NOTE: If a line module reloads at this point, it it is held down for the duration of the upgrade and then undergoes a cold boot to the running release; the line module has no effect on the unified ISSU process.

SNMP Traps

When you issue the **issu initialization** command, the SNMP agent generates a juniSystemIssuStateChange trap with juniSystemIssuState set to initializing. When the unified ISSU initialization is completed, the SNMP agent generates a juniSystemIssuStateChange trap with juniSystemIssuState set to initialized.

Unified ISSU Upgrade Phase Overview

During the upgrade phase, the CLI supports only a reduced set of administrative commands. You cannot interrupt the upgrade phase. The upgrade phase cannot commence if any CLI commands outside of this set are executing when you issue the **issu start** command.

NOTE: Although you can use any CLI session to issue the **issu start** command, we recommend that you issue the command from a session to the management console port. When the standby SRP module switchover takes place, all management network connections through the Ethernet management port are dropped, and you can access the router only through a console port until the service restoration phase is completed.

When you issue the **issu start** command, unified ISSU performs the following operations:

1. Verifies that the unified ISSU requirements on the router are still met.
2. Verifies that the active and standby SRP modules are synchronized. If they are not synchronized, forces a synchronization to ensure that all configuration and file system changes are propagated to the standby SRP module before proceeding with the upgrade.
3. Copies the NVS configuration from a backup memory area to the flash card on the standby SRP module. During the initialization phase, this configuration data was mirrored from NVS on the active SRP module and upgraded as required by the armed release.
4. Upgrades the control plane on each line module at the same time.
5. Switches control from the primary SRP module (running the current release) to the standby SRP module (running the armed upgrade release).
6. Upgrades the forwarding plane on each line module at the same time. The fabric is switched and upgraded.

You can view the status of the router and the progress of the upgrade at any time by issuing the **show issu** command from another terminal session to the router.

NOTE: While a unified ISSU operation is in progress, do not remove the SRP modules or attempt to reset them. Removing the SRP modules anytime during unified ISSU has an adverse impact.

After the unified ISSU operation is completed, issue the **show version** command. The output should indicate the following:

- The formerly active SRP module has rebooted and come up as the new standby SRP module.
- The newly active SRP module indicates that the formerly active SRP has rebooted and has come up as standby SRP module

You can then remove an SRP module after issuing the **halt** command.

Exceptions During the Upgrade Phase

Table 47 describes the behavior of the router during the upgrade phase when certain exceptional events take place outside the context of the in-service software upgrade.

Table 47: Router Response to Undesirable Events During the Upgrade Phase

Event	Router Action
The router reloads.	■ The unified ISSU operation halts. ■ The router undergoes a cold restart. ■ The router boots with the armed upgrade release. ■ The line modules reboot.
The primary SRP module switches over to the standby SRP module.	■ The unified ISSU operation halts. ■ The router undergoes a cold restart. ■ The router boots with the armed upgrade release. ■ The line modules reboot.
The standby SRP module reloads.	■ The unified ISSU operation halts. ■ The router undergoes a cold restart. ■ The router boots with the armed upgrade release. ■ The line modules reboot.
A line module reloads.	■ The line module is held down and prevented from rebooting until the service restoration phase is completed. The line module then undergoes a cold reboot to the running (pre-upgrade) release.
An IOA is hotswapped.	■ Hot swapping is disabled during the upgrade phase. The line module undergoes a cold reboot and hot swapping is reenabled when the service restoration phase is completed,
An application that does not support unified ISSU is configured.	■ This event can take place only before the **issu start** command is issued, because that command disables CLI configuration commands. When you issue the **issu start** command, after configuring such an application, the command exits and generates an error message.

Verification of Requirements

Because some time may have passed since unified ISSU verified the requirements for the upgrade during the initialization phase, unified ISSU reverifies all the same conditions.

Unified ISSU also verifies that no CLI configuration sessions are open, that no scripts or macros are running, and that any SNMP requests or CLI commands in progress complete within 5 seconds.

If any of the required conditions are not met, the CLI either exits the command with an error message or provides an informative message and prompts you to proceed or halt.

When all the conditions are met, the CLI prompts you to proceed. If you continue, then you can subsequently halt the upgrade only by reloading the router. If you exit the command, the router remains in the unified ISSU initialized state.

Upgrade Setup

At this stage all the preconditions have been met. The unified ISSU process shuts down all management interfaces to the router in order to prevent changes in the configuration.

Final preparation for the upgrade phase includes the following actions:

- SNMP—The SNMP agent generates a juniSystemIssuStateChange trap with juniSystemIssuState set to upgrading to indicate that the final phase of the operation has begun. When the trap is issued with this state value, the SNMP agent stops accepting any new SNMP gets or sets and does not issue any further traps.

- CLI—Most CLI commands are disabled. Only **reload**, **show issu**, and **show version** commands are available to you until the service restoration phase completes. These commands are available on the console and are not available to Telnet sessions.

- External events—Externally created events from sources other than the CLI are ignored. These events typically come from user connections, RADIUS servers, SRC software and SDX software, and SNMP, and include login requests, COA requests, multicast join requests, packet mirroring requests, and so on. Logout requests are cached and processed at a later stage.

- Routing protocols—The unified ISSU process prompts you to consider raising the link costs for each routing protocol that is configured on the router. Raising the link cost for routes through the upgrading router enables neighbors to recompute better routes to those destinations. If you choose to raise the link cost, the higher costs can take some time to propagate through the network. Because the router is unable to determine when this has completed, it waits for 2 minutes before proceeding to the next step in the upgrade.

The reason for raising the link cost is that once the upgrade of the line module control plane begins, routing protocol updates cannot be installed in the line modules until that upgrade completes. That period can be in the range 2–15 minutes. During the control plane upgrade, the routing protocols can still accept new routes and communicate with their neighbors but cannot install the routes.

- Routing protocols—The unified ISSU process prompts you to consider raising the link costs for each routing protocol that is configured on the router.

  Once the upgrade of the line module control plane begins, routing protocol updates cannot be installed in the line modules until that upgrade completes. That period can be in the range 2–15 minutes. During the control plane upgrade, the routing protocols can still accept new routes and communicate with their neighbors but cannot install the routes.

  Raising the link cost for routes through the upgrading router enables neighbors to recompute better routes to those destinations that do not pass through the upgrading router. If you choose to raise the link cost, the higher costs can take some time to propagate through the network. Because the router is unable to determine when this has completed, it waits for 2 minutes before proceeding to the next step in the upgrade.

- Unsupported line modules—Any unsupported line modules that are present are held down after the start of this phase when you can no longer gracefully exit from the unified ISSU process. The modules are held down for the duration of the in-service software upgrade and are then undergo a cold boot to the original running release.

- IGMP requests—The router cannot handle IGMP requests for channel changing for IPTV implementations.

Line Module Control Plane Upgrade

At this point, the upgrade release is preserved on each line module in some backup region. When signaled by the active SRP module, all supported line modules simultaneously reload and restart with the new release. Forwarding through the forwarding subsystem on the line modules—through the fabric of the system—is not be affected by the reload.

The line modules then simultaneously recover any application data preserved in memory on the line module and upgrade that data into a format that is understood by the applications running on the new release. This operation can take in the range of 1–10 minutes depending on the size of the data and the upgrade path of the data. Each line module restores its operational state, running the new release with all data upgraded to a version acceptable to the new software.

If the upgrade process fails for any line module, that module undergoes a cold restart, but none of the other line modules is affected.

SRP Module Switchover

At this stage the primary SRP module is running the current release, the redundant SRP module is running the armed release, and the control plane on each supported line module is running the armed release.

When the primary SRP module has verified that all line modules are up, the redundant SRP module takes over control of the router by becoming the active SRP module. The primary, and formerly active, SRP module reboots to the armed release and serves as the standby SRP module.

All applications on the newly active SRP module are restarted. Each application reconstructs itself from the mirrored data, restoring its state and configuration as it was before the switchover. Forwarding through the fabric is interrupted for about one second.

The SRP switchover restarts the routing protocols and triggers a graceful restart because the routes need to be recomputed. This recalculation can take up to 90 seconds. Data continues to be forwarded through routes that were learned before the upgrade of the line module control planes.

Line Module Forwarding Plane Upgrade

While the applications on the SRP module and the line modules reconstruct themselves, they also begin to build up the new state for the forwarding subsystem. All applications on the line module signal the system when they are ready to start the forwarding upgrade.

Because upgrading the forwarding plane affects forwarding through the chassis for up to 30 seconds, unified ISSU does not proceed until the routing protocols have signaled that route reconvergence has completed. Unified ISSU then informs all line modules to simultaneously upgrade their forwarding subsystems.

The line modules then perform the following steps:

1. Halt forwarding through the line modules. Although any links to external devices remain up, incoming data is dropped.
2. Update any changed programmable hardware devices.
3. Update the forwarding subsystem with the new release and upgraded configuration data.
4. Update the routing tables with the reconverged routes.
5. Resume forwarding.

Unified ISSU Service Restoration Phase Overview

This is the final unified ISSU phase. At this point, all three major components of the router—the SRP modules, the line module control planes, and the line module forwarding planes—have been upgraded and forwarding has resumed through the chassis. The following actions take place during this phase:

- The CLI is re-enabled. All commands are made available to users.
- The SNMP agent is restarted and bulk statistics are collected and available for review.

- New login requests and logout requests are processed. The router begins to accept externally created events from sources other than the CLI and SNMP. These events typically come from user connections, RADIUS servers, and SRC software and SDX software, and include login requests, COA requests, multicast join requests, and so on.
- Logout requests that were cached at the start of the in-service software upgrade are processed.
- After the flash memory on the newly active SRP module is updated, stateful SRP switchover is available to the router.

At this point the in-service software upgrade is completed, and the router is restored to normal operation. Any line modules that reloaded during the upgrade phase and were therefore held down are now rebooted to the original running release.

Application Support for Unified ISSU

When an application supports unified ISSU, you can configure the application on the router and proceed with the unified in-service software upgrade with no adverse impact to the upgrade.

Applications that do not support unified ISSU cannot maintain state and configuration with minimal traffic loss across the upgrade. When you attempt the unified in-service software upgrade on a router that is configured with an ISSU-challenged application, the in-service software upgrade is halted and cannot proceed unless you change the configuration. An application that does not support high availability cannot support unified ISSU.

Table 48 indicates which applications support or do not support a unified in-service software upgrade, as well as limitations on their behavior.

Table 48: Application Support for Unified In-Service Software Upgrades

Application	Supported	Unsupported	Notes
Physical Layer Protocols			
DS1	a	–	–
DS3	a	–	–
HDLC	a	–	–
SONET/SDH	a	–	E120 and E320 routers do not support APS.
SONET/SDH VT	–	a	–
Link-Layer Protocols			

Table 48: Application Support for Unified In-Service Software Upgrades (continued)

Application	Supported	Unsupported	Notes
ARP	a	–	ARP entries in the ARP cache do not time out because no ARP aging occurs during unified ISSU. When the unified ISSU is completed, the ARP cache contains the same entries as it had before the unified ISSU began.
ATM	a	–	–
ATM 1483 bulk configuration of dynamic interfaces	a	–	–
ATM bulk configuration of static interfaces	a	–	–
Bridged Ethernet	a	–	–
Cisco HDLC	a	–	–
Ethernet (with and without VLANs)	a	–	–
Frame Relay	a	–	–
PPP	a	–	–
PPPoE	a	–	–
Transparent bridging	a	–	–
Unicast Routing			
Access Routes	a	–	–
BGP	a	–	–
FTP	–	a	–
IP	a	–	–
IPv6	–	a	Unified ISSU does not support IPv6.
IPSec Transport	Not applicable	Not applicable	E120 and E320 routers do not support IPSec.
IPSec Tunnels	Not applicable	Not applicable	E120 and E320 routers do not support IPSec.
IS-IS	a	–	Support only when graceful restart is configured.
OSPF	a	–	Support only when graceful restart is configured.
RIP	a	–	–

Table 48: Application Support for Unified In-Service Software Upgrades (continued)

Application	Supported	Unsupported	Notes
Static Routes	a	–	–
Telnet	a	–	Authentication and command authorizations on Telnet sessions fail during the upgrade phase and Telnet sessions are dropped.

Table 48: Application Support for Unified In-Service Software Upgrades (continued)

Application	Supported	Unsupported	Notes
IPv4 Multicast Routing			
Multicast Routing	a	–	–
ANCP (L2C)	a	–	Unified ISSU can proceed if ANCP is configured. However, ANCP has no graceful restart extensions and therefore it cannot maintain its dynamic state across the upgrade. Consequently, all ANCP sessions are brought down and then restored when the upgrade is completed.
DVMRP	a	–	–
IGMP	a	–	–
PIM	a	–	–
IPv6 Multicast Routing			
Multicast Routing	–	a	Unified ISSU does not support IPv6.
MLD	–	a	Unified ISSU does not support IPv6.
PIM	–	a	Unified ISSU does not support IPv6.
Multiprotocol Label Switching			
MPLS	a	–	–
BGP signaling	a	–	–
LDP signaling	a	–	–
RSVP-TE signaling	a	–	–
Local cross-connects between layer 2 interfaces using MPLS	a	–	–
Policies and QoS			
Policies	a	–	–
QoS	a	–	–

Table 48: Application Support for Unified In-Service Software Upgrades (continued)

Application	Supported	Unsupported	Notes
Remote Access			
AAA	a	–	The following configuration is not supported: The subscriber username and password are on an ATM circuit in Bridged Ethernet over ATM or IP over ATM configurations.
DHCP External Server and Packet Trigger	–	a	–
DHCP Packet Capture	a	–	Configuration of DHCP packet capture does not prevent unified ISSU from proceeding. However, the capturing of packets on the line modules is halted when the unified ISSU upgrade phase commences. Packet capture resumes automatically during the unified ISSU service restoration phase.
DHCP Proxy Client	–	a	–
DHCP Relay Proxy	–	a	–
DHCP Relay Server	–	a	–
DHCPv4 Local Server	a	–	Ensure that DHCP clients have a minimum lease of 120 minutes before you begin unified ISSU to prevent unwanted lease expirations due to the length of the unified ISSU process.
DHCPv6 Local Server	–	a	Unified ISSU does not support IPv6.
L2TP	a	–	Unified ISSU forces an L2TP failover for all established tunnels. L2TP failover resynchronization is required for successful recovery of a tunnel and its sessions following the upgrade.
L2TP Dialout	–	a	–
Local Address Pools	a	–	–

Table 48: Application Support for Unified In-Service Software Upgrades (continued)

Application	Supported	Unsupported	Notes
Local Authentication Server	a	–	–
RADIUS Client	a	–	–
RADIUS Dynamic-Request Server	a	–	
RADIUS Initiated Disconnect	–	a	–
RADIUS Relay Server	–	a	–
RADIUS Route-Download Server	a	–	–
SRC Client	a	–	–
Service Manager	a	–	–
Subscriber Manager	a	–	–
TACACS+	a	–	–
Miscellaneous			
Bulk statistics	a	–	–
Denial of Service (DoS) protection	a	–	–
Firewall	a	–	–
HTTP server	a	–	–
IOA hot swap	–	a	–
J-Flow (IP flow statistics)	a	–	–

Table 48: Application Support for Unified In-Service Software Upgrades (continued)

Application	Supported	Unsupported	Notes
Line Module Redundancy	a	–	When you issue the **issu initialization** command, line module redundancy is made inactive until the upgrade is completed. If a line module in the redundancy group fails during this period of inactivity, unified ISSU holds that module down. The redundant line module cannot take over for the failed line module until the unified ISSU is completed. The primary line modules in the redundancy group must be active for the unified ISSU to proceed. If instead the redundant module is active, validation fails and unified ISSU is halted. You must revert to the primary module in the redundancy group to proceed with the upgrade.
Mobile IP Home Agent	–	a	–
Network Address Translation	a	–	–
NTP	a	–	–
Resource Threshold Monitor	a	–	–
Response Time Reporter	a	–	–
Route Policy	a	–	–
SNMP	a	–	–
Subscriber Interfaces	a	–	–
Tunnels (GRE and DVMRP)	a	–	–
VRRP	a	–	–

Unexpected Application-Specific Behavior During Unified ISSU

This section describes the behavior of applications that vary from the expected behavior during a unified in-service software upgrade.

- AAA Authentication and Authorization Disabled on page 418
- ATM Affected Behaviors on page 418
- DHCP Affected Behaviors on page 419
- DoS Protection State Freeze on page 420
- Ethernet Affected Behaviors on page 420
- FTP Server File Transfers Halted on page 421
- IS-IS Effects on Graceful Restart and Network Stability on page 421
- L2TP Failover of Established Tunnels on page 423
- OSPF Effects on Graceful Restart, Timeouts, and Network Stability on page 423
- PIM Suspended During Unified ISSU on page 425
- Subscriber Logins and Logouts Suspended During Unified ISSU on page 426
- SONET/SDH Behavior During Unified ISSU on page 426
- TACACS+ Services Not Available on page 427
- Interruption in Traffic Forwarding for Layer 3 Routing and Signaling Protocols on page 427
- Recommended Routing Protocol Timer Settings on page 429

AAA Authentication and Authorization Disabled

Authentication and command authorization are temporarily disabled on the serial console connection during the upgrade phase. You can connect to the serial console and issue the **reload**, **show issu**, and **show version** commands without the action of authentication and authorization servers, such as RADIUS or TACACS+.

ATM Affected Behaviors

The following aspects of ATM behavior during unified ISSU are different than the behavior during normal router operations.

ILMI Sessions Not Maintained

The router does not maintain ILMI sessions during a unified in-service software upgrade. The router terminates all ILMI sessions and restarts them during the upgrade. If the ILMI protocol is enabled on any port, you are warned during the initialization phase when unified ISSU is verifying the prerequisites for the upgrade. You can choose to continue the upgrade—and bring down the sessions—or to halt the in-service software upgrade.

OAM CC Effects on VCC

When an ATM VC is configured as an OAM CC source, periodic OAM cells are generated for about 15 seconds. The device configured as the OAM CC sink is likely to declare the VCC down during this time. Unified ISSU generates a warning when it detects an OAM CC source configuration during the initialization phase while unified ISSU is verifying the prerequisites for the upgrade. You can choose to continue or halt the in-service software upgrade

When an ATM VC is configured as OAM CC sink, it cannot receive OAM CC cells generated by the source for about 15 seconds. The OAM CC does not time out and the VCC is not declared down. OAM CC cell generation resumes when the unified ISSU operation is completed.

OAM VC Integrity Verification Cessation

During the unified ISSU operation, verification of OAM VC integrity stops. This verification resumes when the unified ISSU operation is completed.

ATM does not respond to incoming OAM loopback cells during the upgrade for a period of less than 30 seconds. The lack of response might cause ATM peers to declare VCC (VPC) down.

Port Data Rate Monitoring Cessation

The monitoring of ATM port data rates is halted during a unified in-service software upgrade. Monitoring resumes immediately after the unified ISSU operation is completed. The data rates reported by the **show atm interface** command are inaccurate for the period of one configured load interval after unified ISSU is completed.

VC and VP Statistics Monitoring Halts Unified ISSU Progress

A unified in-service software upgrade cannot proceed if VC or VP statistics monitoring is in progress.

DHCP Affected Behaviors

DHCP Common Component Information Suspended

The common DHCP component supports unified ISSU. This component configures option 60 vendor-option strings when you issue the **set dhcp vendor-option** command. The DHCP common component ceases all CLI and SNMP operations when you issue **issu start** command. You can therefore obtain no information about the common DHCP infrastructure until the in-service software upgrade is completed.

DHCP External Server Prevents Unified ISSU Operation

The DHCP external server application does not support unified ISSU. You must completely unconfigure this application from all virtual routers to perform a unified in-service software upgrade.

DHCP Relay and DHCP Relay Proxy Prevent Unified ISSU

The DHCP relay and DHCP relay proxy applications do not support unified ISSU. You must completely unconfigure these applications from all virtual routers to perform a unified in-service software upgrade.

DHCP Packet Capture Halted on Line Modules

The DHCP packet capture application supports unified ISSU in that its configuration does not halt a unified in-service software upgrade. However, packet capture on line modules is halted during the upgrade phase. Packets are not captured and buffered for later forwarding to the SRP module during this phase. Capture resumes automatically during the service restoration phase.

DoS Protection State Freeze

The denial-of-service (DoS) protection application freezes its state when the in-service software upgrade is initiated. Any suspicious control flow, protocol, or priority remains suspicious until unified ISSU completes.

Freezing the DoS protection state prevents any active control flows from interfering with the system while the unified ISSU is in progress. However, no new control flows, protocols, or priorities are monitored for suspicious activity, and no suspicious activity can be detected until the upgrade is completed.

NOTE: Because of this limitation on DoS functionality, we recommend that you do not initiate unified ISSU until all suspicious control flows, protocols, and priorities have been resolved.

When the in-service software upgrade is completed, the DoS protection application resumes attending to all dynamic state that was frozen at the beginning of the unified ISSU process.

Some suspicious control flows might remain in a suspicious list based on your configuration. If the upgrade software version has DoS protection classification algorithms that are better or different than in the previous version, you might want to clear these suspicious control flows to enable the classification algorithms to determine whether the flow is still considered to be suspicious.

Ethernet Affected Behaviors

The following aspects of Ethernet behavior during a unified in-service software upgrade are different than during normal router operations.

ARP Packets Briefly Not Sent or Received

There is a brief period at the end of the upgrade phase when ARP packets are not sent or received. This event can affect ARP entries on attached devices that were in the process of being aged out.

Link Aggregation interruption

During the in-service software upgrade, LACP PDUs are not generated or received for about 15 seconds on Ethernet ports configured with LACP,

This interruption has no effect on the local side of the link because JUNOSe software generates LAC PDU packets every 30 seconds. The link is not declared down unless packets are missed three times. LACP packet generation continues when the unified ISSU operation is completed.

If a device on the other end of the link is configured with the short timeout of one second, then the device is likely to declare the link to be down and remove the link from the LAG bundle.

Port Data Rate Monitoring Halted

The monitoring of Ethernet port data rate is halted during a unified in-service software upgrade. Monitoring resumes immediately after the unified ISSU operation is completed. The data rates reported by the **show interface** command are inaccurate for the period of one configured load interval after unified ISSU is completed.

VLAN Statistics Monitoring Halts Unified ISSU Progress

A unified in-service software upgrade cannot proceed if VLAN statistics monitoring is in progress.

FTP Server File Transfers Halted

During a unified in-service software upgrade, file transfers that involve the FTP server are halted because of the SRP module switchover during the upgrade.

For this reason, the FTP server does not support unified ISSU. You can continue with the in-service software upgrade only when the FTP server is not enabled. You must disable the FTP server to perform the upgrade.

IS-IS Effects on Graceful Restart and Network Stability

IS-IS has the following issues to consider before you begin a unified in-service software upgrade:

- Graceful restart—Required
- Routing around the upgrading router—Optional

Configuring Graceful Restart Before Unified ISSU Begins

You must configure IS-IS graceful restart on the router and on all IS-IS neighbors before you begin the in-service software upgrade. When the unified ISSU process verifies the upgrade requirements during the initialization phase, it detects whether graceful restart is configured. If it is not configured, the CLI displays a warning message and prompts you to proceed or halt. You can stop at this point to configure graceful restart.

If instead you proceed, the in-service software upgrade can complete successfully, but the IS-IS neighbors are likely to break the adjacencies with the upgrading router and consider that routes formerly reached through this router are now unreachable. When the in-service software upgrade completes and the routing protocols restart, the IS-IS neighbors can relearn the routes through the router.

When you issue the **issu start** command, IS-IS lengthens its hello timer values and sends LSPs with the new values. The upgrade proceeds when the IS-IS neighbors have acknowledged the new values.

Configuring Graceful Restart When BGP And LDP are Configured

When BGP, IS-IS, and LDP are all configured on a router on which you will perform a unified in-service software upgrade, ensure that the IS-IS graceful restart timeout is longer than the LDP graceful restart timeout. The IS-IS graceful restart does not complete when the LDP graceful restart timeout is longer than the IS-IS graceful restart timeout. Configure IS-IS graceful timeout with the **nsf t3** command. Configure LDP graceful restart timeout with the **mpls ldp graceful-restart timers max-recovery** command.

Routing Around the Restarting Router to Minimize Network Instability

NOTE: The situation described in this section is very uncommon. This rare circumstance arises when you have redundant uplinks to the core and network topology changes cause routes to go through the upgrading router. In a typical network design, this is not an issue and you do not need to route peers around the upgrading router,

During the unified ISSU upgrade phase, network instability can result if the restarting router goes into an unstable state after the unified ISSU process fails. Some IS-IS traffic loss occurs during the resulting line module resets. For those reasons, you might want IS-IS peers to route around the router that is being upgraded.

You can use the **overload advertise-high-metric issu** command to cause the router to advertise a high metric to its neighbors so that they route around the upgrading router. When you issue the **issu start** command, the router raises the metric to the maximum link cost on all interfaces running IS-IS. The maximum value depends on the metric type. IS-IS neighbors then choose a path with lower metrics to reach any destination that was previously reached through the upgrading router. When unified ISSU is completed, IS-IS reverts the metrics back to the values that were configured before the in-service software upgrade.

When traffic engineering has been configured, the traffic engineering metrics are also increased. New tunnels are not established through the upgrading router and any tunnels undergoing re-optimization in other routers go around the upgrading router.

IS-IS support for unified ISSU does not depend on this configuration. If you do not issue the **overload advertise-high-metric issu** command, the in-service software upgrade can still proceed to successful completion without disrupting IS-IS functionality.

overload advertise-high-metric issu

- Use to cause IS-IS to advertise the maximum link metric on all interfaces to IS-IS neighbors when a unified in-service software upgrade is started.
- Example

  host1(config-router)#**overload advertise-high-metric issu**

- Use the **no** version to send the configured link costs to neighbors during the in-service software upgrade.

L2TP Failover of Established Tunnels

L2TP never declares itself as unified ISSU unsafe. However, unified ISSU forces an L2TP failover for all established tunnels. Successful recovery of a tunnel and its sessions following the in-service software upgrade requires a successful L2TP failover resynchronization, either by the L2TP silent failover method or the L2TP failover protocol.

When the unified ISSU operation attempts to verify the upgrade prerequisites, a warning message is generated if any tunnels are present for which failover resynchronization is disabled.

You can use the **show l2tp tunnel failover-resync disable** command to identify the tunnels referred to by the warning message. The command enables filtering based upon the effective failover resynchronization mechanism:

```
host1#show l2tp tunnel failover-resync disable
L2TP tunnel 2/1 is Up with 1 active session
1 L2TP tunnel found
```

If a successful failover resynchronization cannot be performed for a tunnel following the upgrade, then the tunnel and all of its sessions are subject to disconnection.

L2TP automatically detects a peer L2TP disconnect after the in-service software upgrade is completed by detecting a control channel failure.

When peer LNSs are not configured with PPP keepalives or inactivity timeouts, you must configure an inactivity timeout for L2TP on the LAC. This timeout enables the router to detect a PPP disconnect when signaling has been dropped during the unified ISSU forwarding interruption. In the absence of this configuration, the connection at the LAC and LNS is left as logged in for an extended period of time following the upgrade.

OSPF Effects on Graceful Restart, Timeouts, and Network Stability

OSPF has the following issues to consider before you begin a unified in-service software upgrade:

- Graceful restart—Required
- Dead interval—Required
- Routing around the upgrading router—Optional

Configuring Graceful Restart Before Unified ISSU Begins

You must configure OSPF graceful restart before you begin the in-service software upgrade. When the unified ISSU process verifies the upgrade requirements during the initialization phase, it detects whether graceful restart is configured. If it is not configured, the CLI displays a warning message and prompts you to proceed or halt. You can stop at this point to configure graceful restart.

If instead you proceed, the in-service software upgrade can complete successfully, but the OSPF neighbors are likely to break the adjacencies with the upgrading router and consider that routes formerly reached through this router are now unreachable. When the in-service software upgrade completes and the routing protocols restart, the IS-IS neighbors can relearn the routes through the router.

You must also ensure that the OSPF neighbors have been configured as graceful restart helper routers. During the unified ISSU initialization phase, OSPF graceful restart on the upgrading router cannot verify whether its neighbors are helper routers, and reports that fact by means of the CLI.

Configuring Graceful Restart When BGP And LDP are Configured

When BGP, LDP, and OSPF are all configured on a router on which you will perform a unified in-service software upgrade, ensure that the OSPF graceful restart timeout is longer than the LDP graceful restart timeout. The OSPF graceful restart does not complete when the LDP graceful restart timeout is longer than the OSPF graceful restart timeout. Configure OSPF graceful restart timeout with the **graceful-restart restart-time** command. Configure LDP graceful restart timeout with the **mpls ldp graceful-restart timers max-recovery** command.

Configuring a Longer Dead Interval Than Normal

To prevent OSPF from timing out to the OSPF neighbors, you must configure a dead interval that is longer than the period required for the in-service software upgrade to complete. You must use the value provided by unified ISSU in a warning message displayed during the initialization phase.

Routing Around the Restarting Router to Minimize Network Instability

NOTE: The situation described in this section is very uncommon. This rare circumstance arises when you have redundant uplinks to the core and network topology changes cause routes to go through the upgrading router. In a typical network design, this is not an issue and you do not need to route peers around the upgrading router,

During the unified ISSU upgrade phase, network instability can result if the restarting router goes into an unstable state after the unified ISSU process fails. Some OSPF traffic loss occurs during the resulting line module resets. For those reasons, you might want OSPF peers to route around the router that is being upgraded.

You can use the **overload advertise-high-metric issu** command to cause the router to advertise a high link cost to its neighbors so that they route around the upgrading router. When you issue the **issu start** command, the router raises the link cost to the maximum link cost on all interfaces running OSPF. The higher cost is advertised in the OSPF LSAs. OSPF neighbors then choose a path with lower metrics to reach any destination that was previously reached through the upgrading router. When unified ISSU is completed, OSPF reverts the link costs back to the values that were configured before the in-service software upgrade.

When traffic engineering has been configured, the traffic engineering metrics are also increased. New tunnels are not established through the upgrading router and any tunnels undergoing re-optimization in other routers go around the upgrading router.

OSPF support for unified ISSU does not depend on this configuration. If you do not issue the **overload advertise-high-metric issu** command, the in-service software upgrade can still proceed to successful completion without disrupting OSPF functionality.

overload advertise-high-metric issu

- Use to cause OSPF to advertise the maximum link cost on all interfaces to OSPF neighbors when a unified in-service software upgrade is started.
- Example

  host1(config-router)#**overload advertise-high-metric issu**

- Use the **no** version to send the configured link costs to neighbors during the in-service software upgrade.

PIM Suspended During Unified ISSU

You can minimize PIM traffic loss during the in-service software upgrade by issuing the **ip pim dr-priority** command to set a priority so that PIM neighbors do not forward traffic through the upgrading router. By default, a PIM interface has a priority of one. If you set the priority to one, the lowest possible priority, then the upgrading router is not selected to be a designated router in the PIM network if an interface on another router in that network has a higher priority.

ip pim dr-priority

- Use to set a priority by which a router is likely to be selected as the designated router.
- Example

  host1(config-if)#**ip pim dr-priority 1**

- Use the **no** version to restore the default value, 1.

Subscriber Logins and Logouts Suspended During Unified ISSU

All new subscriber logins are ignored during the upgrade phase. New subscriber logouts are cached and processed after the unified ISSU operation is completed.

Subscriber Statistics Accumulation or Deletion

All subscriber statistics present in the line modules are cleared when the line module forwarding planes are upgraded. For this reason, the router has to read the statistics from the forwarding plane before it is upgraded.

However, forwarding through the line modules continues after that point, until the line module forwarding plane is upgraded. Some statistics can therefore accumulate in the forwarding plane in the interval between these two events. These statistics are not preserved across the upgrade.

Statistics for subscribers that log out during the forwarding plane upgrade are collected and reported before the forwarding plane is reloaded. Statistics are not collected for any subscribers who are connected before you issue the **issu start** command but who log out before the forwarding plane upgrade is completed.

The following subscriber statistics are preserved across the upgrade:

- All policy statistics
- Accounting statistics reported by IP: in bytes, out bytes, in packets, out packets
- Accounting statistics reported by L2TP: in octets, out octets, in packets, out packets
- Accounting statistics reported by PPP: in octets, out octets, in packets, out packets

All other statistics are set to zero, including all statistics belonging to the SNMP generic interface MIB for every interface layer.

SONET/SDH Behavior During Unified ISSU

During a unified in-service software upgrade, several aspects of SONET behavior differ from normal operation.

- SONET APS is not supported.
- During a conventional software upgrade, a SONET loss-of-signal defect lasts more than 2.5 seconds, causing the router to declare an LOS failure. Devices on the remote end of SONET links detect the failure and bring down the link and the dynamic interface stacks built on the link.

  During a unified in-service software upgrade, the LOS does not last more than 2.5 seconds. The remote device detect a momentary LOS but does not perceive this short LOS as a link failure and does not bring the link down,

TACACS+ Services Not Available

During the upgrade phase of unified ISSU, TACACS + services are unavailable. If you have configured AAA authentication for Telnet (with the **aaa new-model command**) this lack of availability affects CLI authentication, authorization, and accounting activities.

Because there is no alternate method of accounting other than TACACS, CLI exec and command accounting does not work during this phase.

Interruption in Traffic Forwarding for Layer 3 Routing and Signaling Protocols

The routing protocols are affected by two interruptions in traffic forwarding caused by the in-service software upgrade during the upgrade phase.

- Switchover from active to standby SRP module—When the active SRP module running the current release switches over to the standby SRP module running the upgrade release, the routing protocols and all other applications restart. A control plane outage of 30–40 seconds prevents the protocols from sending hellos or keepalive messages.

  The protocols must gracefully restart to come back online, recover their routing state on the newly active SRP module, and respond to their peers. Therefore, you must enable graceful restart for all protocols before you begin the in-service software upgrade. All neighbors of the routing protocols must also be configured to support graceful restart.

  A data plane outage of about one second also takes place during the switchover of the fabric from the active primary SRP module to the standby SRP module.

- Upgrade of the forwarding plane for each line module—After the routing protocols reconverge with their peers and rebuild their routing tables, unified ISSU upgrades the forwarding plane on all line modules simultaneously. This upgrade halts forwarding through the chassis. This forwarding outage lasts about 15 seconds.

If capable, routing protocols temporarily lengthen their timers to survive the outages. During the initialization phase, unified ISSU checks for timers that are set too short and whether the protocol enables timer renegotiation. If these checks fail, unified ISSU generates a warning and enables you to reconfigure the protocols before you issue the **issu start** command.

We recommend that you configure timers to be longer than usual for the routing protocols that cannot renegotiate timers. You can use bidirectional forwarding detection (BFD) to quickly detect forwarding interruptions.

Table 49 describes how individual routing protocols behave during a unified in-service software upgrade.

Table 49: Behavior of Routing Protocols During a Unified In-Service Software Upgrade

Protocol	Behavior
BFD	BFD renegotiates its timers as needed. Typically, the timers are lengthened until the SRP module switchover takes place, then shortened for the forwarding plane upgrade, and finally shortened to the original configured values.
BGP	The configured BGP timers are typically long enough to survive the forwarding outages. If, not, unified ISSU generates a warning message. BGP sends out keepalive messages immediately before and immediately after both the SRP module switchover and the forwarding plane restart, independent of the interval since it last sent them.
IS-IS	If necessary, temporarily lengthens the hello timers.
LDP	Unified ISSU warns you if the hello timers or the keepalive timers are not long enough to survive the forwarding plane upgrade. LDP sends out hello messages and keepalive messages immediately before and immediately after both the SRP module switchover and the forwarding plane restart, independent of the interval since it last sent them.
OSPF	OSPF timers are not negotiable between peers. Unified ISSU generates a warning if the hello timers or the keepalive timers are not long enough to survive the forwarding plane upgrade. OSPF begins a graceful restart before the SRP module switchover. When you configure graceful restart before the in-service software upgrade, you must ensure that the graceful restart times are long enough to allow recovery. OSPF sends out hello messages and keepalive messages immediately before and immediately after forwarding plane restart, independent of the interval since it last sent them.
PIM	If necessary, temporarily lengthens the hold times in hello messages. PIM guarantees that at least one hello message with a lengthened hold time is sent to each neighbor. If necessary, increases the join-prune hold time. PIM guarantees that at least one join-prune message with a lengthened hold time is sent to each neighbor.
RIP	RIP timers do not affect unified ISSU.
RSVP-TE	If necessary, temporarily lengthens the graceful restart timers to survive the SRP module switchover. If necessary, lengthens the hello timers to survive the forwarding plane upgrade.

You might want some or all traffic to be routed around the upgrading router rather than accept a forwarding loss during the forwarding interruption. To do so, you must configure your routing protocols appropriately. For example, you might raise the link cost in IS-IS and OSPF, causing their neighbors to seek alternate routes that have lower link costs. In PIM, you can set the priority for the router interface to zero to ensure that the upgrading router is not selected as a designated router.

Recommended Routing Protocol Timer Settings

You can use the default values for many of the routing protocol timers with no adverse effect on a unified in-service software upgrade. For other timers, we recommend particular values, as described in Table 50.

Table 50: Recommended Routing Protocol Timer Settings

Protocol	Timers
BFD	Use the default timers.
BGP	Use the default timers, including graceful restart default timers.
DVMRP	Use the default timers.
IGMP	Use the default timers.
IS-IS	Use the default timers, including graceful restart default timers.
LDP	Use the default timers, including graceful restart default timers, except for the following: ■ Set the hello hold time to at least 901 seconds for a helper or a restarter configuration for a link-level adjacency or for LDP targeted sessions.
OSPF	Use the default timers, including graceful restart default timers, except for the dead interval. Set the OSPF dead interval to at least 301 seconds.
PIM	Set the query interval to at least 210 seconds. ISSU generates a warning for any of the following conditions, but you can ignore the warning without causing a higher FC outage: ■ The current router is a DR. ■ The current router is configured as an Auto RP mapping agent and is chosen as the RP for any group. ■ The current router is an elected or candidate BSR, or if BSR candidate RPs are configured. ■ The graceful restart timer is less than the default value, 30 seconds.
RIP	Use the default timers; graceful restart is not supported. For scaled configurations, such as for 2000 RIP interfaces, use the following values: ■ Flush interval: 600 seconds ■ Holddown time: 260 seconds ■ Invalid interval: 260 seconds ■ Update interval: 60 seconds

Table 50: Recommended Routing Protocol Timer Settings (continued)

Protocol	Timers
RSVP-TE	Use the default timers, including graceful restart default timers, except for the following: ■ For graceful restart, the hello timeout interval is the product of hello misses multiplied by the hello refresh interval. Determine which period is longer, the IC upgrade time or the forwarding upgrade time. Configure the hello refresh and hello miss values so that the hello timeout is greater than the longer of those two periods. ■ For node hellos, the product of the refresh misses multiplied by the hello refresh interval must be great than the FC outage time. For an outage time of less than 30 seconds, for example, configure the following values: ■ Set the node hello refresh interval to 8000. ■ Set the node hello refresh misses to 4.

Before You Begin a Unified In-Service Software Upgrade

The following hardware and software prerequisites must be met for the successful completion of unified ISSU. You can issue the **show issu** command to determine whether the routers meets these requirements.

Hardware Requirements for Unified ISSU

- The E120 or E320 router must support unified ISSU.
- Two SRP modules must be installed in the router.
- All installed combinations of line modules and IOAs must support unified ISSU. Unsupported modules that are online are reloaded during the unified ISSU, with consequent loss of connections and traffic forwarding.

  Do not install IOAs in the chassis while the unified ISSU operation is in process.
- The redundant SRP module must have at least 300 MB of free memory. Depending on their configuration, line modules require up to 75 MB of free memory.

For information about modules supported on E120 and E320 routers:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support unified ISSU.

Software Requirements for Unified ISSU

- The running JUNOSe software release must support unified ISSU.

  You can upgrade to a software version that supports unified ISSU from a software version that does not support unified ISSU only by means of a conventional upgrade. During the conventional upgrade, all line modules are reloaded, all subscribers are dropped, and traffic forwarding is interrupted until the upgrade is completed.

- The armed (upgrade) release must be capable of being upgraded to from the currently running release; it must be higher-numbered than the running release.

- All applications that are configured on the router must support unified ISSU and stateful SRP switchover.

  If one or more unified ISSU-challenged applications are configured and you proceed with a unified in-service software upgrade, the unified ISSU process forces a conventional upgrade on the router. All line modules are reloaded, all subscribers are dropped, and traffic forwarding is interrupted until the upgrade is completed.

  You can avoid this circumstance by removing the configuration for the unified ISSU-challenged applications from the router before you begin the in-service software upgrade.

  See *Application Support for Unified ISSU* on page 412 for information about whether an application supports unified ISSU.

- Stateful SRP switchover must be configured on the router. Use the following commands to configure high availability:

  ```
  host1(config)#redundancy
  host1(config-redundancy)#mode high-availability
  ```

  See *Chapter 7, Managing High Availability* for information about high availability.

The following requirements must be met for traffic forwarding to continue. However, failing to meet these requirements does not halt the unified ISSU operation. The unified ISSU process offers the option to override or ignore these forwarding requirements.

- Graceful restart must be enabled for all configured routing protocols. The unified ISSU operation relies on graceful restart to keep the routing protocols alive through the various stages of the upgrade.

- All connected peers must be configured with graceful restart. Because some protocols cannot themselves confirm peer configuration for graceful restart, you must ensure that the peers are properly configured.

- For applications that exchange keepalive messages with peers, you must ensure that the poll times are adequate to maintain the peering session across any forwarding interruption caused by the unified ISSU operation.

Upgrading Router Software with Unified ISSU

To upgrade your router software by means of unified ISSU, perform the following steps.

1. Disable autosynchronization.

   host1(config)#**disable-autosync**

2. Copy the new release to the router.

NOTE: Be sure to specify the correct software release (.rel) filename for the router you are using, as described in the section *Identifying the Software Release File* in *Chapter 3, Installing JUNOSe Software*.

   host1#**copy /incoming/releases/ftpserver/quebec2.rel R2.rel**

3. Save the current configuration.

   host1#**copy running-configuration** *system2.cnf*

4. Determine whether the router hardware and the software release meet the criteria required for unified ISSU to operate successfully by using one of the following commands:

   host1#**show issu**
   host1#**show issu brief**
   host1#**show issu detail**

5. Arm the primary SRP module with the upgrade release.

   host1#**boot system R2.rel**

NOTE: You must arm any hotfixes that need to be loaded with the new release after you have armed the new release. The hotfixes are supplied when the modules to which they apply are rebooted.

6. Synchronize the NVS file system of the redundant SRP module with that of the primary SRP module.

   host1#**synchronize**

   Because the redundant SRP module is running a different release than the armed release, the module automatically reboots and runs the armed (upgrade) release, R2.rel.

   Wait for the redundant SRP module to boot, initialize, and reach the standby state. At this point, the REDUNDANT LED on the module is illuminated and the ONLINE LED is off. The State field in the **show version** display indicates that the redundant module is in the standby state.

7. Synchronize the file system of the primary module with that of the redundant module.

   The NVS file systems of the two SRP modules are unsynchronized because the redundant SRP module rebooted.

   host1#**synchronize**

8. Reenable autosynchronization.

   host1(config)#**no disable-autosync**

9. Determine whether unified ISSU is in the Idle state and whether all upgrade requirements have been met.

   host1#**show issu**

NOTE: If the results indicate that some requirements are not met, you must correct this situation before proceeding.

10. Ensure that stateful SRP switchover is configured on the router.

    host1#**show redundancy srp**

    If it is not already configured, do so now.

    host1(config)#**redundancy**
    host1(config-redundancy)#**mode high-availability**

11. For each configured protocol on the router and its neighbors, ensure that graceful restart is configured. See the relevant protocol configuration chapters in the JUNOSe document set for information about configuring graceful restart.

12. Begin the initialization phase of the in-service software upgrade.

    host1#**issu initialize**

    The CLI displays the status of the initialization as it proceeds.

13. (Optional) From a different CLI session, display the progress of the initialization.

    host1#**show issu**

    Unified ISSU must be in the Initialized state before you proceed to the next step. The time required for initialization varies with the system load and the complexity of the router configuration.

14. Start the upgrade phase.

    host1#**issu start**

    The router switches to the redundant SRP module running the upgrade release, R2.rel. Significant upgrade milestones are displayed as they occur.

15. When the console indicates that the upgrade is completed, you can verify that the router is back in the idle state and running the upgrade release, R2.rel.

    host1#**show issu**

    You can also verify the status of the SRP modules and line modules, as well as the running and armed releases.

    host1#**show version**

issu initialize

- Use to start the initialization phase of the unified ISSU process.
- This command displays the percentage completion for the process as it takes place.
- Example

  host1#**issu initialize**
  Verifying the ISSU criteria… verified
  Starting the ISSU initializing phase
  Upgrading the standby SRP- This phase can take a long time
  10% completed…

- There is no **no** version.

issu start

- Use to start the upgrade phase of the unified ISSU process after the initialization phase has completed.
- Example

  host1#**issu start**
  Verifying the ISSU criteria… verified
  The system will now enter the upgrading phase. This phase cannot be aborted.
  Do you wish to continue?
  Yes
  Starting the ISSU upgrade phase
  … Upgrading the line card – Control plane
  … Upgrading completed
  Switching from primary SRP to the standby SRP
  The system will resume on the SRP in slot 7 in a few minutes.

- There is no **no** version.

issu stop

- Use to gracefully stop a unified in-service software upgrade and place the process in an idle state.
- You can issue this command only when unified ISSU is in the initialized state. You cannot issue this command after you have issued the **issu start** command to begin the upgrade phase of unified ISSU.
- Example

  ```
  host1#issu stop
  The command will abort the ISSU operation. Do you wish to continue?
  Yes
  Stopping the ISSU upgrade process
  ...reloading standby SRP
  ```

- There is no **no** version.

Halting the Unified ISSU Process and Restoring the Original State of the Router

The options that are available to halt the in-service software upgrade depend on the phase that the upgrade is in when you attempt to halt it. The phase also affects the state of the router after the upgrade is halted.

Halting Unified ISSU During Initialization Phase

During the initialization phase, you can halt the unified ISSU process by issuing the **issu stop** command. This action reloads the redundant SRP module with the armed upgrade release. As a result, unified ISSU is placed in the idle state and the following releases are present on the router:

- Primary SRP module—Running (original) release
- Redundant SRP module—Upgrade release
- Line modules—Running (original) release

After you stop unified ISSU, you can return the router to the state it was in when you began the in-service software upgrade. To roll the router back to its beginning state with the redundant SRP module running the original release, you must perform the following steps to arm the redundant SRP module with the running release:

1. Turn off auto synchronization.

   host1(config)#**disable-autosync**

2. Specify that the router use the running release when it reboots.

   host1(config)#**boot system** *erx_x-y-z.rel*

3. Synchronize the NVS file system of the redundant module with that of the primary module.

   host1#**synchronize**

The redundant SRP module automatically reboots because the armed release (the original release) now differs from the software release it is currently running (the upgrade release).

4. Verify that stateful SRP switchover is enabled.

```
host1#show redundancy
```

Halting Unified ISSU During Upgrade Phase

During the upgrade phase—before the line module and control plane software is upgraded—the unified ISSU process provides an opportunity to cancel the upgrade. If you choose to cancel, the router remains in the unified ISSU initialized state. The CLI command set becomes fully accessible.

If you do not cancel at this point, then the process continues and any line modules that do not support unified ISSU are reloaded. Application sessions are brought down and traffic forwarding is interrupted for the unsupported modules.

If you do cancel in response to the CLI prompt, unified ISSU returns to the initialized state, and the following releases are present on the router:

- Primary SRP module—Running (original) release
- Redundant SRP module—Upgrade release; the module is in the unified ISSU initialized state
- Line modules—Running (original) release

To roll back from the unified ISSU initialized state, you must issue the **issu stop** command. The command reloads the redundant SRP module with the armed release and places unified ISSU in the idle state. As a result, the following releases are present on the router:

- Primary SRP module—Running (original) release
- Redundant SRP—Upgrade release
- Line modules—Running (original) release

After you stop unified ISSU, you can return the router to the state it was in when you began the in-service software upgrade. To roll the router back to its beginning state with the redundant SRP module running the original release, you must perform the following steps to arm the redundant SRP module with the running release:

1. Turn off auto synchronization.

   host1(config)#**disable-autosync**

2. Specify that the router use the running release when it reboots. For

   host1(config)#**boot system** *erx_x-y-z.rel*

3. Synchronize the NVS file system of the redundant module with that of the primary module.

   ```
   host1#synchronize
   ```

   The redundant SRP module automatically reboots because the software release that it is configured to run now differs from the software release it is running.

Monitoring a Unified In-Service Software Upgrade

You can use the **show issu** command to monitor the status of the router with regard to a unified in-service software upgrade.

show issu

- Use to display information about the current status of the router relative to a unified in-service software upgrade and of the upgrade itself.
- Field descriptions
  - ISSU state—State of the upgrade process, idle, initializing, initialized, or upgrading
  - ISSU description—State of the upgrade, including percent complete
  - criteria met—Whether prerequisites for the upgrade have been met and, generally, what errors occurred
  - running release—Filename of JUNOSe software release that is currently running on the SRP modules
  - armed release—Filename of JUNOSe software release that is armed to become the next running release when the router reboots
- Example 1—Displays the current unified ISSU state and identifies the active and armed releases

  ```
  host1#show issu brief

  ISSU state:       initializing
  ISSU description: ISSU initialize is in-progress, 5% complete
  criteria met:     No, upgrade error(s) found
  running release:  release1.rel
  armed release:    release2.rel
  ```

- Example 2—To the information displayed by **show issu brief**, adds a summary table of unified ISSU verification criteria

```
host1#show issu

ISSU state:       idle
ISSU description: ISSU is currently idle
criteria met:     No, upgrade error(s) found
running release:  release1.rel
armed release:    release2.rel

#                  ISSU Activation Criteria Summary                    Met
--   ------------------------------------------------------------   -----------
1    In-Service Software Upgrade ready?                             Yes
2    High-Availability ready?                                       No
3    Line modules ready?                                            Conditional
```

```
4    Configuration conversion support ready?                    Yes
5    CLI sessions ready?                                        Yes
6    Routing applications ready?                                Yes
7    Protocol timers ready?                                     Yes
```

- Example 3—To the information displayed by **show issu**, adds a detailed table of unified ISSU verification criteria that lists mandatory and conditional criteria that have not been met, the impact of this status, and the remedy as reported by router applications and system components that participate in the in-service software upgrade

```
host1#show issu detail

ISSU state:       idle
ISSU description: ISSU is currently idle
criteria met:     No, upgrade error(s) found
running release:  release1.rel
armed release:    release2.rel

#                  ISSU Activation Criteria Summary                 Met
--   ------------------------------------------------------------   -----------
1    In-Service Software Upgrade ready?                             Yes
2    High-Availability ready?                                       No
3    Line modules ready?                                            Conditional
4    Configuration conversion support ready?                        Yes
5    CLI sessions ready?                                            Yes
6    Routing applications ready?                                    Yes
7    Protocol timers ready?                                         Yes

#                      ISSU Criterion Detail                        Met
--   ------------------------------------------------------------   -----------
1    In-Service Software Upgrade ready?                             Yes
2    High-Availability ready?                                       No
->   Problem: The standby SRP must not be running the same releas   No
     e
    Reporting Slot: 6
     Impact: ISSU cannot be performed
     Remedy: boot a release compatible with ISSU on the standby S
     RP
3    Line modules ready?                                            Conditional
->   Problem: Card does not support required memory configuration   Conditional
     : Slot 1, OC3/OC12/DS3-ATM, requires at least 256 MB
    Reporting Slot: 6
     Impact: If you continue, the card will immediately be reset
     and then cold started when ISSU Upgrade completes
     Remedy: data unavailable
->   Problem: Card does not support required memory configuration   Conditional
     : Slot 8, CT3-12, requires at least 256 MB
    Reporting Slot: 6
     Impact: If you continue, the card will immediately be reset
     and then cold started when ISSU Upgrade completes
     Remedy: data unavailable
->   Problem: Card does not support required memory configuration   Conditional
     : Slot 9, CT3-12, requires at least 256 MB
    Reporting Slot: 6
     Impact: If you continue, the card will immediately be reset
     and then cold started when ISSU Upgrade completes
     Remedy: data unavailable
->   Problem: Card does not support required memory configuration   Conditional
     : Slot 10, CT3-12, requires at least 256 MB
```

```
     Reporting Slot: 6
      Impact: If you continue, the card will immediately be reset
      and then cold started when ISSU Upgrade completes
      Remedy: data unavailable
->    Problem: Card not disabled or not online: Slot 1, OC3/OC12/D   Conditional
      S3-ATM, 0/0
     Reporting Slot: 6
      Impact: If you continue, the card will immediately be reset
      and then cold started when ISSU Upgrade completes
      Remedy: If not standby, Wait for card to come online before
      proceeding
->    Problem: Card not disabled or not online: Slot 8, CT3-12, 0/   Conditional
      0
     Reporting Slot: 6
      Impact: If you continue, the card will immediately be reset
      and then cold started when ISSU Upgrade completes
      Remedy: If not standby, Wait for card to come online before
      proceeding
4     Configuration conversion support ready?                        Yes
5     CLI sessions ready?                                            Yes
6     Routing applications ready?                                    Yes
7     Protocol timers ready?                                         Yes
```