

Software Management Operations

- Revision History, on page 1
- Overview, on page 1
- Upgrading or Downgrading of CP and UP, on page 3

Revision History

Note Revision history details are not provided for features introduced before release 21.24.

Revision Details	Release
Support is extended for N-4 backward compatibility of software releases.	21.26
Support is extended for N-3 backward compatibility of software releases.	21.25
Support is extended for N-2 backward compatibility of software releases.	21.24.1
First introduced.	Pre 21.24

Overview

CUPS supports backward compatibility of software releases on Control Plane (CP) and User Plane (UP). The feature allows seamless upgrade/downgrade of the software from/to one previous release (N-1)/two previous releases (N-2)/three previous releases (N-3)/four previous releases (N-4). The functionality includes support for the following:

- N-1/N-2/N-3 /N-4 compatibility of software releases on two CPs in ICSR mode—allows seamless upgrade of CPs from one version to another in CP 1:1 redundancy scenario.
- N-1/N-2/N-3 /N-4 compatibility of software releases on two UPs in ICSR mode—allows seamless upgrade of UPs from one version to another in UP 1:1 redundancy scenario.
- N-1/N-2/N-3/N-4 compatibility of software releases between CP and UP—allows seamless upgrade of the associated CP or UP from one version to another.

- N-1/N-2/N-3/N-4 compatibility of software releases between CP and UP with multi-Sx—allows seamless upgrade of the associated CP or UP from one version to another in multi-Sx scenario.

Important Contact your Cisco Account representative for procedural assistance prior to upgrading or downgrading your software versions.

Version Exchange between CP and UP

Version/release information is exchanged when CP and UP pairs. The release information exchange also occurs when the CP pairs with a Standby CP or UP pairs with a Standby UP (in 1:1 redundancy scenario) through the heart beat message exchanged between Active and Standby.

When incompatible releases are paired, an Alarm (SNMP Trap) is raised. For details, see *SNMP Trap* section.

To indicate the peer version during the exchange of release information, the following new IE is included in the association request and heartbeat request messages.

Information Elements	P	Condition / Comment								IE Length	IE ID
Peer Version	O	Used to specify the peer GR/PFCP version and StarOS version								4 bytes	245
		Bits									
	Octets	8	7	6	5	4	3	2	1		
	1 to 2	Peer Version IE Type = 245 (decimal)									
	3 to 4	Length = n bytes									
	5 to 8	Peer GR/PFCP Version									
	9 to 12	StarOS GR Version									
	13 to 13	StarOS Version String Length									
	Variable Length	StarOS Version String Value									

SNMP Traps

The following SNMP traps are raised when pairing is done with an incompatible release.

SNMP Trap	Description
SRPPeerUnsupportedVersion	The Active/Standby CP/UP in higher version raises the SNMP trap when the peer is in a version lower than N-4.
SRPPeerUnsupportedVersionClear	The Active/Standby CP/UP in higher version raises the SNMP trap to clear the SRPPeerUnsupportedVersion.
SxPeerUnsupportedVersion	The CP/UP in higher version raises the SNMP trap when the peer is in a version lower than N-4.

SNMP Trap	Description
SxPeerUnsupportedVersionClear	The CP/UP in higher version raises an SNMP trap to clear the SxPeerUnsupportedVersion.

Limitations

The following are the known limitations of the feature:

- When the peer version is determined to be lower than the supported N-4 version, the association/pairing is allowed. However, functional aspect of the same isn't guaranteed.

Caution Don't attempt to upgrade from incompatible versions. Contact your Cisco Account representative for the upgrade path and steps.

SNMP traps are raised by the node on the latest version with respect to the StarOS version. For details, see the *SNMP Trap* section of this chapter.

- From release 21.24.1, RCM is checkpoint agnostic to enable support for future UP releases. Currently RCM does not support N-4 compatibility and only supports N-1 compatibility.

Upgrading or Downgrading of CP and UP

The following Maintenance Operating Procedure (MOP) outlines the steps necessary to Upgrade or Downgrade a Control Plane and User plane from previous release (N-1)/(N-2)/(N-3)/(N-4) to or from the latest N release.

Important Contact your Cisco Account representative for procedural assistance prior to upgrading or downgrading your software versions.

The following are the Upgrade options:

- **Only CP Upgrade**: When requirement is to upgrade only the CP, and the UP must remain intact.
- **Only UP Upgrade**: When requirement is to upgrade only the UP, and the CP must remain intact.
- **Both CP and UP Upgrade**: When requirement is to upgrade both CP and UP. In this case, upgrade the CP first and then the UP or the other way around.

Health Checks

Perform the following health checks after every operation of upgrade, downgrade, or reload of chassis.

1. Check the Service Redundancy Protocol (SRP) information on the Active chassis to avoid issues during an SRP switchover and decide if proactive analysis must be done before the SRP switchover. Use the following CLI commands:
   - **srp validate-configuration srp validate-switchover**

- **show srp info**

The following is a sample output.

```
Peer Configuration Validation: Complete
Last Peer Configuration Error: None
Last Peer Configuration Event: Wed Mar 18 15:34:02 2019  (1602 seconds ago)
Last Validate Switchover Status: None
Connection State: Connected
```

Check the following parameters:

- **Peer Configuration Validation: Complete**—If it shows "In Progress", you must wait and then execute the **show srp info** again after 15 seconds (approximately).
- **Last Peer Configuration Error: None**—If you see "Peer Checksum Validation Failure", then it indicates that there are configuration differences between Active and Standby chassis that must be fixed.
- **Last Validate Switchover Status: None**—The output must show as "None". And, output should be *Remote Chassis - Ready for Switchover (XX seconds ago)* when the **srp validate-configuration** and **srp validate-switchover** CLI commands are triggered.
- **Connection State: Connected**—The output must show as "Connected".

2. Check subscriber count on both Active and Standby chassis.

   After sessions are up, execute **show subscribers summary | grep Total** CLI command in the Active chassis. The following is a sample output.

   ```
   show subscribers summary | grep Total
      Total Subscribers:  100
   ```

   On Standby chassis, execute **show srp checkpoint statistics | grep allocated** CLI command. The following is a sample output.

   ```
   show srp checkpoint statistics | grep allocated
      Current pre-allocated calls:  100
   ```

3. Check the status of the license by executing **show license information** CLI command. It should be in "Good (Redundant)" and not in "Expired" state.
4. Check the Session Recovery Status by executing the **show session recovery status verbose** CLI command. The following is a sample output.

   ```
   Session Recovery Status:
     Overall Status        : Ready For Recovery
     Last Status Update    : 7 seconds ago

                 ----sessmgr---  ----aaamgr----  demux
    cpu state    active standby  active standby  active  status
   1/0  Active     8      1        8      1        17     Good
   ```

5. Verify all the SessMgrs are in Standby-Connected state on Standby chassis by executing **show srp checkpoint statistics | grep Sessmgrs** CLI command. The following is a sample output.

   ```
   Number of Sessmgrs:        1
   Sessmgrs in Active-Connected state:  0
   Sessmgrs in Standby-Connected state: 8
   Sessmgrs in Pending-Active state:    0
   ```

6. Verify the status of all the cards to see if they are in Active or Standby state. The following is a sample output.

```
show card table

Slot          Card Type              Oper State  SPOF  Attach
----------- ---------------------- ----------- ----- ------
1: VC        5-Port Virtual Card     Active        -
```

7. Execute **show task resources | grep -v good** CLI command and its output must only display the total number of SessMgrs and sessions.
8. Execute the **show crash list** CLI command to check if there were any new crashes.
9. Execute the **show service all** CLI command to verify that the state is displayed as "Started" and not "Initialized".

Build Upgrade

Backup Configuration

1. Back up the current configuration—save current configuration, that will be used in case of downgrade, which probably has all the features and configuration present until now.
2. Collect the **show support details** on both Active and Standby chassis before making any changes or Upgrade.
3. Perform Health Checks.

Upgrade Procedure

1. Perform chassis Health Checks on both the nodes.
2. On the secondary chassis (ICSR), which is in Standby state, change boot priority with N build.
3. Reload to latest 21.xx.xx build.
4. Do the new configuration change on Standby chassis (For example, any new CLI, license, or configuration changes.).
5. Do Health Check on the reloaded chassis. Check for any crashes or errors.

Perform Switchover

1. Before SRP switchover from Active to Standby on both chassis, check:
   a. On Active chassis: **show subscriber summary | grep Total**
   b. On Standby chassis: **show srp checkpoint statistics | grep allocated**

Note The count must be same for both.

   c. On Active and Standby chassis: **show sx peer**

For example:

```
|||||  Sx Service                                                    No of
|||||  ID                                                                 Restart
|||||  |                                                  Recovery              |
Current    Max        Peer
vvvvv  v     Group Name    Node ID         Peer ID     Timestamp             v
Sessions   Sessions   State
----- ---- ----------------- ------------------------- ------------------- ------
--------- --------- --------
CAAXD  22    CPGROUP21   209.165.200.225   50331649    2021-03-17:02:33:55    0
    0          0      NONE

Total Peers:    1
```

Note Peer state must be Active and associated. Peer ID must match on both the chassis.

d. On Standby chassis: **show srp checkpoint statistics | grep Sessmgrs**

Note "Number of Sessmgrs" must be equal to the "Sessmgrs in Standby- Connected state".

e. On Active chassis:

1. **srp validate-configuration**: This CLI command is for initiating a configuration validation check from the ACTIVE chassis. If the validation doesn't have any error, output of this CLI command is blank.
2. **srp validate-switchover**: Validates both Active and Standby chassis are ready for a planned SRP switchover. If chassis is ready for switchover, then the output of this CLI command is blank.
3. **show srp info | grep "Last Validate Switchover Status"** : Output of this CLI command must be as follows.

   ```
   Last Validate Switchover Status: Remote Chassis - Ready for Switchover
   ```

4. **show srp info debug**: Active and Standby chassis must have the same output.

2. On Active chassis: **srp initiate-switchover**
   - **a.** Perform chassis Health Checks on both the nodes. Also check Step 1a and Step 1c under the *Performing Switchover* section. There can be a difference of 5%.
   - **b.** Perform call testing since new sessions are serviced on the new Active chassis.
   - **c.** Upgrade the old Active as mentioned in Step 2 through Step 5 under the *Upgrade Procedure* section.

CP Upgrade

This section describes the procedure for CP-only upgrade.

1. Perform Health Check procedure on both CP nodes as mentioned in the Health Checks, on page 3 section.

2. Perform Upgrade on Standby CP as mentioned in the Build Upgrade, on page 5 section.

Note If the context names on CP and UP are different, then execute **debug pgw pfd-mgmt** CLI command on the upgraded CP before making it Active.

3. Perform Health Check on both chassis, and then do CP switchover to the upgraded chassis.
4. Verify that the new chassis is taking the new sessions, there are no new crashes, or session drop due to error scenarios. Do Health Check on both the CP and UP.
5. Upgrade the new Standby CP as mentioned in the Build Upgrade, on page 5 section.

UP Upgrade

This section describes the procedure for UP-only upgrade.

1. Perform Health Check procedure on both the UP nodes as mentioned in the Health Checks, on page 3 section.
2. Perform Upgrade on Standby UP as mentioned in the Build Upgrade, on page 5 section.
3. Do "sx-peer configuration" on the upgraded Standby chassis.
4. Perform Health Check on both the UP nodes, and then do UP switchover.
5. Upgrade the new Standby UP as mentioned in the Build Upgrade, on page 5 section.

CP and UP Upgrade

This section describes the procedure for upgrading the CP first and then upgrading the UP, or the other way round.

Upgrading CP First

1. Perform Health Check procedure on both CP and UP, as mentioned in the Health Checks, on page 3 section.
2. Perform Upgrade on Standby CP as mentioned in the Build Upgrade, on page 5 section.

Note If the context names on CP and UP are different, then execute **debug pgw pfd-mgmt** CLI command on the upgraded CP before making it Active.

3. Perform Upgrade on Standby UP as mentioned in the Build Upgrade, on page 5 section.
4. Upgrade both Standby CP and UP to N build.
5. Perform Health Check on both chassis, and then do CP switchover to the upgraded chassis.
6. Verify that the new chassis is taking the new sessions, there are no new crashes, or session drop due to error scenarios.

7. Perform Health Check on both the UP nodes, and then do UP switchover.
8. Perform Health Check on newly Active UP. Verify that there are no call drops, and data is flowing through the new chassis.
9. Upgrade new Standby CP and UP as mentioned in the Build Upgrade, on page 5 section.

Upgrading UP First

1. Perform Health Check and build transfer procedure on both CP and UP.
2. Perform Upgrade on Standby UP as mentioned in the Build Upgrade, on page 5 section.
3. Do "sx-peer configuration" on the upgraded Standby chassis.
4. Perform Health Check on both the UP nodes, and then do UP switchover.
5. Perform Upgrade on new Standby UP as mentioned in the Build Upgrade, on page 5 section.
6. Perform Upgrade on Standby CP as mentioned in the Build Upgrade, on page 5 section.
7. Perform Health Check on both the CP nodes, and then do CP switchover.

Note If the context names on CP and UP are different, then execute **debug pgw pfd-mgmt** CLI command on the CP.

8. Upgrade new Standby CP chassis. Perform Health Check.
9. Perform Health Check on both the Active and Standby UP.
10. If everything is working as expected, then do the configuration changes on the Standby CP first. Then do the similar changes on the Active CP and execute **push config-to-up all** CLI command. New changes are pushed to the new Active UP.

Downgrade Procedure

Downgrade – Both CP and UP

If there are new configurations and/or configuration changes needed on CP as part of Upgrade, then follow the steps to upgrade the UP first.

1. Do Health Check on both CP and UP.
2. Change boot priority to the N-1/N-2/N-3/N-4 build on the Standby UP. Reload Standby UP.
3. Do "sx-peer configuration" on downgraded Standby UP.
4. Do Health Check on both the UP nodes and then do UP switchover.
5. Perform Step 1 to Step 3 on new Standby UP.
6. Change boot priority to N-1/N-2/N-3/N-4 build on the Standby CP. Reload the Standby CP.

Note If the context names on CP and UP are different, then execute the **debug pgw pfd-mgmt..** CLI command on the CP.

7. Load the configuration that has been saved in Step 1 mentioned in *Backup Configuration* section in Build Upgrade, on page 5.
8. Do Health Check on both CP nodes and then do the CP switchover.
9. Perform Step 6 and Step 7 to downgrade old Active.
10. On Active CP, execute **push config-to-up all** CLI command so that changes in the configuration are pushed to the UP.

Downgrade – CP Only

Perform Step 6 through Step 10 mentioned in the *Downgrade – Both CP and UP* section.

Downgrade – UP Only

Perform Step 1 through Step 5 mentioned in the *Downgrade – Both CP and UP* section.