Alcatel-Lucent

Service Access Switch |Release 7.0 Rev.12

7210 SAS OS Software Release Notes | July 2016

3HE09537AAALTQZZA V7.0.R12 Issue 2

Alcatel·Lucent

Disclaimers

Alcatel-Lucent products are intended for commercial uses. Without the appropriate network design engineering, they must not be sold, licensed or otherwise distributed for use in any hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life-support machines, or weapons systems, in which the failure of products could lead directly to death, personal injury, or severe physical or environmental damage. The customer hereby agrees that the use, sale, license or other distribution of the products for any such application without the prior written consent of Alcatel-Lucent, shall be at the customer's sole risk. The customer hereby agrees to defend and hold Alcatel-Lucent harmless from any claims for loss, cost, damage, expense or liability that may arise out of or in connection with the use, sale, license or other distribution of the products in such applications.

This document may contain information regarding the use and installation of non-Alcatel-Lucent products. Please note that this information is provided as a courtesy to assist you. While Alcatel-Lucent tries to ensure that this information accurately reflects information provided by the supplier, please refer to the materials provided with any non-Alcatel-Lucent product and contact the supplier for confirmation. Alcatel-Lucent assumes no responsibility or liability for incorrect or incomplete information provided about non-Alcatel-Lucent products.

However, this does not constitute a representation or warranty. The warranties provided for Alcatel-Lucent products, if any, are set forth in contractual documentation entered into by Alcatel-Lucent and its customers.

This document was originally written in English. If there is any conflict or inconsistency between the English version and any other version of a document, the English version shall prevail.

Table of Contents

Table of Contents

RELEASE NOTE ORGANIZATION FOR 7210 SAS-D, E, K, M, X, T, AND R6

The following are the major topics covered in these Release Notes:

RELEASE 7210 SAS SUPPORTED HARDWARE

- From 7210 SAS 7.0R10 release, SD card is supported with 7210 SAS-K non-ETR platform.
- 7210 SAS-R6 supports 8GB compact flash (3HE04708AA) and 32GB compact flash (3HE06083AA) from 7.0R6 release.
- From 7.0R7 release, 7210 SAS-K ETR platform is supported.
- From 7.0R6 release, 7210 SAS-R6 supports following 2nd generation IMM (IMM-SAS-R-b) referred as IMMv2.
  - IMM-SAS-R-b 16TX (P/N: 3HE09156AA).
- From 7.0R4 release, 7210 SAS-R6 supports following 2nd generation IMM (IMM-SASR-B) referred as IMMv2.
  - IMM-SAS-R-b 10SFP-1SFP+ (P/N:3HE09152AA)
  - IMM-SAS-R-b 2SFP+ (P/N: 3HE09153AA)
  - IMM-SAS-R-b 4SFP+ (P/N: 3HE09154AA)
  - IMM-SAS-R-b 11cSFP (P/N: 3HE09155AA)

NOTE: IMMv2 works only with SF/CPM-b and cannot co-exist with IMMv1 in the same 7210 SAS-R6 chassis

- From 7.0R4 release 7210 SAS-K is supported.
- 7210 SAS-R6 SF/CPM-b (P/N:3HE08154ABRA02) is supported from 7210 SAS 7.0R3 release and it works with 7.0R3 or higher versions of software release.
  NOTE: SF/CPM-b 3HE08154ABRA01 and 3HE08154ABRA02 can co-exist in the same 7210 SAS-R6 chassis.
- From release 7.0R1, 7210 SAS-R6 supports only SF/CPM-b (P/N:3HE08154ABRA01).
  NOTE: From 7.0R1 SF/CPM (P/N:3HE08154AARA) is not supported.
- All variants of 7210 SAS-R6, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, 7210 SAS-D, and 7210 SAS-E.
- Following USB models from Sandisk are supported:
  - Cruzer Fit – size 4GB and 8GB
  - Cruzer Blade – size 4GB and 8GB

SOFTWARE UPGRADE NOTES

UPGRADE TO 7.0R4 OR LATER RELEASES

- For detailed procedure for upgrading IMMv1 to IMMv2 and bringing up system with IMMv2 7.0R4 or later version of software, refer 7210 SAS Installation Guide.
- From 7.0R4, "*max-ipv6-routes*" CLI is available under "c*onfig>system>res-profile>router*".

UPGRADE TO 7.0R1OR LATER RELEASES

UPGRADE TO SF/CPM-B (P/N:3HE08154ABRA)

Platforms applicable: 7210 SAS-R6

From release 7.0R1, 7210 SAS-R6 supports only SF/CPM-b (P/N:3HE08154ABRA).

7210 SAS-R6 SF/CPM (P/N:3HE08154AARA) and SF/CPM-b (P/N:3HE08154ABRA) cannot co-exist in a single chassis. To upgrade to SF/CPM-b execute the following:

Step 1. Copying required version of the software image using the below methods.

Copy 7.0R1or greater versions of software and config files to cf2: of existing SF/CFM, modify bof.cfg to point to this software. Take out flash cf2: from SF/CFM and put in to SF/CFM-b.

OR

Copy the required images (7.0R1 or higher version) and config files to flash of SF/CPM-b, make sure to bof.cfg point to the required software and config file.

Step 2. Power down the chassis.

Step 3. Remove both (if in use) the SF/CPM and replace both with SF/CPM-b.

Step 4. Plug-in the appropriate connectors (for example: console port connection) to the new SF/CPM- b cards.

Step 5. Power up the chassis.

Step 6. On boot up with SF/CFM-b, "show card" output will display "cpm-sf-b-sas-R6" the correct names for the SF/CPM-b for slot A and B.

NOTES:

- No configuration changes are needed to use SF/CPM-b.
- The upgrade is service affecting.

UPGRADE TO 6.0R6 OR LATER RELEASES

FILTERS

Platforms applicable: 7210 SAS-E

In release 6.0R6, the ACL TCAM allocation scheme has been modified. As part of this change, software allocates only one (1) additional entry for every group of resources allocated for use of ACLs. In previous releases configuration if all ACL entries are used up, it is required to remove one of IP, MAC, or IPv6 entry before upgrading to 6.0R6 release.

UPGRADE FROM 6.0R4 OR PRIOR RELEASES

1830 VWM (CWDM) MANAGEMENT

Platforms applicable: 7210 SAS-M, 7210 SAS-X, 7210 SAS-E

The 7210 SAS release 6.0R5 adds supports for provisioning of cards inserted into the slots available on the 1830 VWM devices. The user must provision the card and card-type (also known as, module type) before the card can be managed by the 7210 SAS after upgrade to 6.0R5 release.

UPGRADE FROM 3.0 RELEASES

NETWORK QOS POLICY

Platforms applicable: 7210 SAS-M (Network mode) and 7210 SAS-X

During upgrade from 3.0 to 4.0 or 5.0 releases following was true:

- For each "network" qos policy of "ip-interface" type in the configuration file, system generated "mpls-lsp-exp-profile-map" policy and was attached to network qos policy. mpls-lsp-exp-profile-map policy id was equal to network qos policy id. "mpls-lsp-expprofile- map" policy was populated with "lsp-exp <lsp-exp-value> profile {in|out}" information. lsp-exp and profile values were copied from corresponding network qos policy of the configuration file.
  In case of upgrade from 3.0 to 6.0 or later releases
- Following console message appears “MINOR: CLI MPLS LSP EXP profile should be configured through the profile map.”

- "profile in|out" configured in "network" qos policy of 3.0 configuration file will be ignored during upgrade. This means user defined 3.0 "profile" definition is lost after upgrade to 6.0 or later releases.
- System attaches default, that is, "mpls-lsp-exp-profile-map" policy id 1 to network qos policy.

Workaround:

- First upgrade from 3.0 to 4.0 or 5.0, save config file then upgrade to 6.0 or later releases.

OR

- After upgrade to 6.0 or later release, user need to configure "mpls-lsp-exp-profile-map" policy and attach to "network" qos policy.

UPGRADE FROM 4.0 OR 5.0 RELEASES

CLI

Platforms applicable: 7210 SAS-M (Network mode) and 7210 SAS-X

- After upgrade to release 6.0 or later releases, system defaults to "ldp-local-fc-enable", CLI "config>qos>ldp-local-fc-enable" is not available from release 6.0.
- Profile parameter [profile {in|out}] under all the Eth-CFM SAA tests (Loopback, Linktrace, 2DM, and 2SLM) was not supported in previous releases and CLI commands has been removed in release 6.0R1. During upgrade profile information, if existed in the config file, will be ignored.

UPGRADE FROM 5.0R1 OR 5.0R2 RELEASES

LAG CONFIGURATION

Platform applicable: 7210 SAS-M and 7210 SAS-X

The 7210 node is allotted a fixed amount of MAC addresses during manufacturing. The base address and the number of MAC addresses is specified on the back of the chassis on the chassis label and also shown in the show chassis command. On 7210 SAS-M or SAS-X, software reserves about 28 addresses for its use to assign MAC addresses to all the ports, system mac etc. MAC addresses are assigned to the LAG using the LAG ID as the offset.

With this allocation scheme, if the total number of MAC addresses is, for e.g 44, then from LAG ID 17 up to the maximum amount of LAG configured, user needs to assign MAC address statically before upgrade to 5.0R3 release, otherwise upgrade to 5.0R3 or later release may fail if system does not have required number of MAC addresses.

Note: The issue will be seen only on nodes which do not have enough MAC addresses, that is, those less than 53 addresses.

From 5.0R3 or later release "show chassis" CLI displays Base MAC address and number of MAC's assigned to node.

DOT1X TUNNELING

Platforms applicable: 7210 SAS-M Network mode and 7210 SAS-X

When "dot1x tunneling" configured on access port, with release 5.0R1 or R2 "admin save" saved "dot1x tunneling" in wrong context of config file. This resulted in errors during next re-boot of node.

Workaround is to modify the saved config so that "dot1x tunneling" appears after "mtu".

Example shown below:

```
port 1/1/1
    ethernet
        mode access
        access
        exit
        mtu 9212
        dot1x
        tunneling
exit
```

UPGRADE TO 5.0R1 OR LATER RELEASES FROM PRIOR RELEASES

ACCOUNTING RECORD NUMBERS

Platforms applicable: 7210 SAS-M, 7210 SAS-X, 7210 SAS-E, 7210 SAS-D

In 5.0R1 release following accounting numbers are modified, new numbers are shown in ( ) netInfIngressOct(52), netInfIngressPkt(53), combinedNetInfIngress(54), accessEgressPkt(55), accessEgressOct(56), combinedAccessEgress(57), combinedNetEgress(58), combinedSvcEgress(59), combinedSvcInEgPkt(60), combinedNetInEgPkt(61)

NON SUPPORTED CLI

Platforms applicable: 7210 SAS-M, 7210 SAS-X, 7210 SAS-E, 7210 SAS-D

In previous releases 7210 SAS was allowing to configure non supported feature CLI's. In 5.0R1 some of the non supported CLI's are removed. In previous releases if user had configured non supported feature CLI, configuration will error out during upgrade to 5.0R1 release. It is recommended to check for non supported CLI by loading config file with 5.0R1 and remove non supported CLI's from config file before final upgrade.

TACACS+

Platforms applicable: 7210 SAS-M, 7210 SAS-X, 7210 SAS-E, 7210 SAS-D

From 5.0R1 tacacs+ "single-connection" option is deprecated. During upgrade following warning message displayed

WARNING: CLI Line:xx "single-connection" This command has been deprecated.

SPLIT HORIZON GROUP NAME

Platforms applicable: 7210 SAS-M, 7210 SAS-X, 7210 SAS-E, 7210 SAS-D

During upgrade to 5.0R1 or later release, if "split-horizon-group <group-name>" CLI, where <group-name> configured with name having spaces, config file execution will error out during upgrade.

Workaround is to edit the config file before upgrading to ensure split horizon group names are with double quotes or no space(s) in the group name.

LOGGING

Platforms applicable: 7210 SAS-M, 7210 SAS-X, 7210 SAS-E, 7210 SAS-D

In 5.0 or later releases , as part of log-id config (configure>log>log-id <num>) needs to have “from change”.

This is necessary for the box to generate config change logger/trap messages, modify configuration file accordingly.

UPGRADE TO 4.0R4 OR LATER RELEASE FROM PRIOR RELEASES

SAP INGRESS QOS

Platforms applicable: 7210 SAS-M, 7210 SAS-X, 7210 SAS-E, 7210 SAS-D

During upgrade to 4.0R4 or later release, the following warning message displayed can be ignored:

MAJOR: CLI #1010 Saps in the system will be re-configured without Sap Indexs, because SAP index file could not be located.

After upgrade to 4.0R4 or higher, it is recommended to save the configuration. When the configuration is saved with 4.0R4 or higher build, sap index file with extension .sdx is automatically generated and saved at a location where the configuration file is stored.

Y.1731 MA NAME

Platforms applicable: 7210 SAS-M, 7210 SAS-X, 7210 SAS-E, 7210 SAS-D

From 4.0R1, Y1731 MA name should be unique across the system. During upgrade to 4.0R1 or Later releases if system finds duplicate names in the configuration file then upgrade to new configuration fails. Before upgrade, it is recommended to modify the configuration file.

Example CLI:

"association 1 format icc-based name "abcdabcdabcd1", name "abcdabcdabcd1" should be unique across system for successful upgrade to 4.0R1 or higher.

UPGRADE TO 1.1R7 OR LATER RELEASES FROM PRIOR RELEASES

SERVICES

Platforms applicable: 7210 SAS-M

In 1.1R7, a default SAP and a dot1q SAP cannot be configured along with enabled egress filters when the SAPs are configured on the same port.

If such a configuration exists in the startup-config, it is recommended that the following procedure is used before performing an upgrade:

Step 1. Create a config file on the cf1 flash which contains the CLI commands to provide basic in-band connectivity and management functions.

Step 2. Add the following command in the startup configuration file. Note that the config-file parameter is the file mentioned in step #1. config>system>boot-bad-exec “cf1:/<config-file>”

Step 3. Follow the Software Upgrade Procedures for 7210 SAS-D, E, K, M, X, and T devices on page 10.

UPGRADE TO 1.1R6 OR LATER RELEASES FROM PRIOR RELEASES

ACL

Platforms applicable: 7210 SAS-M

In 1.1R6, number of egress ACLs is restricted to 256 for combined IP and MAC criteria. If the 7210 SAS M is booted with a configuration file containing more than 256 egress ACLs, the configuration will error out. It is recommended that, in such cases, the following procedure is used before performing an upgrade.

Step 1. Create a config file on the cf1 flash which contains the CLI commands to provide basic in-band connectivity and management functions.

Step 2. Add the following command in the startup configuration file. Note that the config-file parameter is the file mentioned in step #1. config>system>boot-bad-exec “cf1:/<config-file>”

Step 3. Follow the Software Upgrade Procedures for 7210 SAS-D, E, K, M, X, and T devices on page 10.

SOFTWARE UPGRADE PROCEDURES FOR 7210 SAS-D, E, K, M, X, AND T DEVICES

The following sections contain information for upgrading to the 7.0R10 software version. In particular, there are sections that describe the following:

- Standard Software Upgrade Procedure
- Procedure for performing a standard, service-affecting upgrade.

STANDARD SOFTWARE UPGRADE PROCEDURE

This section describes the standard software upgrade procedure which is service-affecting:

- Each software release includes a boot loader (boot.tim) and the software image (both.tim).
- The boot loader initiates the loading of the 7210 SAS OS image based on the boot options file (bof.cfg) settings.

The following steps describe the software upgrade process:

Step 1. Backup existing images and configuration files

New software loads may make modifications to the configuration file which are not compatible with older versions of the software.

Note:

- Alcatel-Lucent recommends making backup copies of the BOOT loader (boot.tim), software image (both.tim) and configuration files, should reverting to the old version of the software be required.

Step 2. Copy 7210 SAS images to cf1:

The 7210 SAS image files both.tim must be copied to the cf1: device on the 7210 SAS node. It is good practice to place all the image files for a given release in an appropriately named subdirectory off the root, for example, cf1:\7.0R12 Copying the boot.tim and other files in a given release to a separate subdirectory ensures that all files for the release are available should downgrading the software version be necessary.

Note: Applicable only to 7210 SAS-D Devices

- The 7210 SAS-D of 64MB flash (part numbers 3HE05676AAAA01, 3HE05676ABAA01, 3HE05677AAAA01, 3HE05677ABAA01 and 3HE06537AAAA01) can accommodate one set of boot.tim and both.tim files, the users are required to overwrite existing files with new files in cf1.With the Enhanced 7210 SAS-D (SAS-D with 128MB flash) supported from 4.0R6, more than one set of boot.tim and both.tim files can be stored on flash.

Step 3. Copy boot.tim to the root directory on cf1:

The BOOT Loader file is named boot.tim. This file must be copied to the root directory of the cf1: device.

Note:

- If it is not possible to overwrite cf1:\boot.tim file, Change the cf1:\boot.tim attributes using **file attrib -r cf1:\boot.tim** command.

Note: Applicable only to 7210 SAS-T and 7210 SAS-K devices

- The 7210 SAS-T and 7210 SAS-K other supported drives such as "cf2:" or "uf1:" can also be used for storing boot.tim image. Note that the valid "bof.cfg" file is in the same drive from where the boot.tim is used. Order of search for boot loader is cf1:/boot.tim, cf2:/boot.tim, uf1:/boot.tim. bof.cfg is read from the drive where boot.tim is loaded.

Step 4. Modify the boot options file to boot the new Image.

The Boot Options File (bof.cfg) is read by the BOOT Loader and indicates primary, secondary and tertiary locations for the image file. The bof.cfg should be modified as appropriate to point to the image file for the release to be loaded. Use the **bof save** command to save the Boot Options File modifications.

Step 5. When upgrading to 7.0R12, execute the **admin reboot upgrade** command. Note that, executing '**admin reboot upgrade**' command system will upgrade the bootrom if required.

Allow the boot sequence to complete and verify that the card comes up.

Step 6. **Applicable only to 7210 SAS-D, E, M, and X devices**
Upgrade the Golden BOOT Loader (only if all of the above steps were successful).

After successfully booting of the new version of 7210 SAS image, upgrade the golden boot loader by executing the **admin update-golden-bootstrap cf1:/boot.tim** command.

Note:

After upgrade to 4.0 or later software images, during next boot, if the user forgets the BOF password and fails to provide a correct password, after three attempts, the system prompts the user to reset the BOF password to factory default. If user accepts BOF password recovery, as a security measure, the system also resets the flash to factory defaults (that is, it removes all the files from the flash except the boot image file (cf1:\boot.tim) and Timos image file (cf1:\both.tim)) and reboots the node with the factory default settings.

Refer the 7210 SAS User Guides and "BOF PASSWORD RECOVERY" in Enhancements section of this document for more details.

SOFTWARE UPGRADE PROCEDURES FOR 7210 SAS-R6

The following sections contain information for upgrading to the 7.0R11 software version. In particular, there are sections that describe the following:

- Standard Software Upgrade Procedure

  Procedure for performing a standard, service-affecting upgrade.

STANDARD SOFTWARE UPGRADE PROCEDURE

This section describes the standard software upgrade procedure which is service-affecting:

- Each software release includes a boot loader (boot.tim) and the software image (cpm.tim and iom.tim).
- The boot loader initiates the loading of the 7210 SAS OS image based on the boot options file (bof.cfg) settings.

The following steps describe the software upgrade process:

Step 1. Backup existing images and configuration files

New software loads may make modifications to the configuration file which are not compatible with older versions of the software.

Note:

- Alcatel-Lucent recommends making backup copies of the BOOT loader (boot.tim), software image and configuration files, should reverting to the old version of the software be required.

Step 2. Copy the 7210 SAS-R6 OS Images to cf2:

The 7210 SAS-R6 image files must be copied to the cf2: device on the 7210 SAS-R6 node. It is a good practice to place all the image files for a given release in an appropriately named subdirectory off the root, for example, cf2:\7.0R12.

Copying the boot.tim and other files in a given release to a separate subdirectory ensures that all files for the release are available for downgrading the software version to be necessary.

Note: The 7210 SAS-R6 drives such as "cf1:" or "uf1:" can also be used for storing boot.tim image. Note that the valid "bof.cfg" file should be in the same drive from where the boot.tim is used. Order of search for boot loader is cf1:/boot.tim, cf2:/boot.tim, and uf1:/boot.tim. bof.cfg is read from the drive where boot.tim is loaded.

Note:

- If it is not possible to overwrite the cf2:\boot.tim file, change the cf2:\boot.tim attributes using file **attrib -r cf2:\boot.tim** command.

Step 3. Copy boot.tim to the Root Directory on cf2:

The BOOT Loader file is named boot.tim. This file must be copied to the root directory of the cf2: device.

Step 4. Modify the Boot Options File to Boot the New Image

The Boot Options File (bof.cfg) is read by the BOOT Loader and indicates primary, secondary and tertiary locations for the image file. The bof.cfg should be modified as appropriate to point to the image file for the release to be loaded. Use the **bof save** command to save the Boot Options File modifications.

Step 5. [Redundant CPMs or CFMs] Synchronize Boot Environment

On systems with Redundant CPMs or CFMs, copy the image files and Boot Options File to the redundant CPM or CFM with "**admin redundancy synchronize boot-env**".

Step 6. Reboot the Chassis

When upgrading to 7210 SAS 7.0R12, execute the admin reboot upgrade command. Note that, executing **'admin reboot upgrade'** command in the system upgrades the bootrom.

Step 7. Verify the Software Upgrade

Allow the boot sequence to complete and verify that all cards are online.
Note: If any card fails to occur online after the upgrade, contact the Alcatel-Lucent Technical Assistance Center for information on corrective actions.
It is recommended to save the configuration "**admin save**" after an upgrade has been performed and the system is operating as expected. This ensures that all configuration is saved in a format that is fully compatible with the newly running release.

Note:

During next boot, if the user forgets the BOF password and fails to provide a correct password, after three attempts, the system prompts the user to reset the BOF password to factory default. If user accepts BOF password recovery, as a security measure, the system also resets the flash to factory defaults (that is, it removes all the files from the flash except the boot image file (cf2:\boot.tim) and Timos image file) and reboots the node with the factory default settings.

RESOLVED ISSUES

NOTE:

- Issues marked as MI might have had a minor impact but did not disturb network traffic
- Issues marked as MA might have had a major impact on the network and might have disturbed traffic
- Issues marked as CR were critical and might have had a significant amount of impact on the network

RESOLVED IN R7.0R12

The following are specific technical issues that have been resolved in Release 7.0R12 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

- When Sandisk Cruzer Fit 8GB USB device with firmware version 1.00 is used to bootup the system or wiring any files into this device fails with previous releases of 7210. In 7.0R12 release, fix is provided. The fix works only after node is upgraded to release 7.0R12 with"admin reboot upgrade" CLI. The user needs to upgrade to 7.0R12 using the following procedure:
  - **Step 1.** Copy "boot.tim" to the boot location (cf1:\ or 1.2x USB drive in uf1:\ or cf2:\ as supported by the respective platform.
  - **Step 2.** Point "bof primary-image" to the TiMOS (both.tim in case of K/E/M/X/T/Mxp and cpm.tim and iom.tim in case of R6/R12) location (for example, compact flash, 1.2x USB device, Network location).
  - **Step 3.** Issue "admin reboot upgrade" command. [228346-MA]
- A port flap on 7210 SAS-R6 can cause the iom-hw bfd sessions running on that port to remain operationally down. This issue is seen rarely on IMMv2 cards. This is resolved in 7.0R8 release. [235150-MA]
- From 7.0R12 on 7210 SAS-R6 an enhancement is provided to power cycle an IMM using "tools perform card <slot_no> power-cycle".[222687-MI]
- In the previous release, LSP flaps due to RSVP refresh timeout when refresh-reduction is enabled on a tagged network interface that has certain port MTU and number of LSPs combination. This issue is resolved in 7.0R12. [224050-MI]
- A node could get blocked for SSH access if that node was regularly polled by a Java script to setup an SSH connection and run some CLI commands. This issue has been resolved. [225118-MI]
- User configured security profile attached to "user-template>tacplus-default" is not saved. However, the functionality works. But subsequent reboot would result in losing this profile and hence the functionality. [231285-MI]
- 7210 SAS-K: SAA two-way-delay measurements occasionally report zero values. There are improvements to this in this release. [230826-MI]
- On 7210 SAS-K, if a VPLS service is bound to an IES service even before creation of that VPLS service, user cannot unbind the VPLS service from that IES service. This issue is resolved in this release. [233064-MI]

- On SAS-R and Mxp, SFP+ port remains in Oper state Up, even after removing the internal port loopback configuration. This issue is resolved. [233234-MI]
- In a rare occurrence, a link flap on ABR node that is stitching LDPoRSVP tunnels can lead to traffic loss on the PWs using this tunnel. This issue is resolved in this release. [234041-MI]

RESOLVED IN R7.0R11

The following are specific technical issues that have been resolved in Release 7.0R11 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

- In previous releases, on 7210 SAS-R6, export prefix-policy per LDP peer was not available. From this release, export-policy per LDP peer can be applied. [221396-MI]
- If an 802.3 LLC frame with a value 0x8809 at control field offset and followed by 0x01/0x02/0x03/0x0A as first byte of payload received on L2 service endpoint such frames were not forwarded. This issue is resolved in this release. This issue is not applicable for 7210 SAS-E and 7210 SAS-K platforms. [221993-MI]
- On 7210 SAS-R6, intermittent issue of central BFD sessions flap with 300msec timeout is resolved in this release. [223097-MA]
- System reboots if the number of meters attached to a SAP is modified to a lower number from higher number, while “monitor service id <n> sap x/y/z rate” output is in-progress. This issue is resolved. [229152-MI]
- With previous 7.0 releases, if 7210 SAS-K system is rebooted with large protocol configuration, sometimes system fails to bootup properly. This issue is resolved. [225697-MA]
- In previous release, efm-oam flaps are rarely seen when the system is configured with more number of efm-oam sessions with 300msec timeout. This issue is resolved. [226237, 203485-MI]
- On 7210 SAS-R6 BFD hw-iom type interface, shutdown generates an incorrect BFD message which causes the OSPF session on the neighbor to stay up till the OSPF hold-down timer expires. This issue is resolved. [212259-MI]

RESOLVED IN R7.0R10

The following are specific technical issues that have been resolved in Release 7.0R10 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

- With 7.0 release, when 7210 SAS-T devices, deployed in a ring topology and PTP is configured in hybrid mode with BC, parallel reboot of all the 7210 SAS-T ring nodes sometimes used to cause few of them not to lock to the PTP master. Workaround for this issue was to reboot the 7210 SAS-T ring nodes in a staged manner. This issue is resolved in 7210 SAS 7.0R10 release. [209601-MA]
- In this release support added to process Y.1731 version-1 DM request packets received on Down MEPs of 7210 SAS-M (network and access-uplink mode), 7210 SAS-T access-uplink mode and 7210 SAS-D. For more information, see Enhancements section. [198278-MI]

- In previous releases of 7210 SAS-T, if mirror-dest id configured with huge value and deleting adding mirror-dest again, might result in node reboot. This issue is resolved in 7.0R10 release. [213367-MA]
- In case of 7210 SAS-R6, IMMs re-boots if non supported CLI “anti-spoof ip” and “statichost ip” commands are configured under SAP context. This issue is resolved in 7.0R10 release. [217945-MI]
- 7210 SAS-K, Dying gasp message were not generated when a static default route is configured, this issue is resolved. [219641-MI]
- In previous releases of 7210 SAS-R6, eth-cfm Linktrace request to MIP failed where MIP was configured in qinq inner tag preserve service. This issue is resolved. [205603-MI]
- In previous release, with IGMP snooping enabled, multicast traffic getting flooded to all ports in the network lag over which the SDP is formed where LAG ports are on same IMM of 7210 SAS-R6, This issue is resolved in 7210 SAS 7.0 R10 release. [MI – 213380].
- In previous releases of 8.0 and from 7.0R4 release, during reboot SDX file was not considered for order in which sap-ingress qos policy applied. During reboot with scaled configuration this can lead to failing of configuration loading. This issue is resolved in 8.0R3 and 7.0R10. This issue is not applicable to 7210 SAS-K. [219365-MA]
- In previous release of 7210 SAS-K, CPU generated L3 packets are not getting remarked as per the remark policy applied on the egress port. This issue is resolved in 7.0R10 release. [222387-MI]
- In previous releases, sometimes IPv6 neighbor solicitation and neighbor advertisement might fail due to the presence of default route in case of 7210 SAS-X, SAS-M. This can be avoided by statically configuring the link local address as neighbor on both the neighboring routers, pointed by default route as nexthop. This issue is resolved in 7.0R10 release. [214070-MI]
- "configure mirror no mirror-dest <>" resulting in following messages on console for SAS-R6 " 1:iomMsg-1:IOM:is_group_empty Getting Group Info Failed; Entry not found” is resolved in 7.0R6 release. [199727-MI]
- 7210 SAS-R6 with releases prior to 7.0R9, IOM UNUSUAL_ERROR (Eg: “Slot x: deallocate_fp_entry_id: deallocate_fp_entry_id: User DOT1AG did not allocate entry y") can be seen when a path flaps in G.8032 ring topology. In some cases, this can also lead to issues with ISIS or any other CPU bound protocol packets being dropped. These issues are resolved in 7.0R9 release.
- In release 5.0, a rare occurrence of eth-ring path’s forwarding state remains in blocking state was seen, even after the path failure is restored. This issue is no more seen with later release, 6.0/7.0/8.0.”
- 7210 SAS-M network mode, 7210 SAS-X, and 7210 SAS-R6 reboots if Eth-ring control SAP is configured in RVPLS service, this is a non supported configuration. From 7.0R9 release, this configuration is not allowed from CLI. [210392-MA]
- With releases prior to 7.0R9, there are very few cases where SAS-K reboots with the following error during bootup, “workQPanic: Kernel work queue overflow”. This issue is resolved in 7.0R9 release. [222576-MA]

RESOLVED IN R7.0R9

The following are specific technical issues that have been resolved in Release 7.0R9 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

- When SAS-R6 is equipped with 2 DC PEMs powered by two different sources and operating at almost equal input voltage, rarely can report spurious power supply failure and clear alarms. This issue is resolved in this release. [211879-MI]
- Under "*config>system>thresholds#*" CLI context "kb-memory-use-alarm" and "kbmemory-use-warn" commands were missing in earlier releases. These commands are available now. [210697-MI]
- In previous releases, packet rate and utilization shown in "monitor port x/y/z rate" command are not accurate, if the polling interval is non-multiple of 10sec. In this release, accuracy of the rates is improved. [211466-MI]
- On SAS-X, if the number of G.8032 rings configured are greater than 22 and the system is upgraded to release 6.0/7.0/8.0, the system crashes. This issue is resolved in this release. [212517-MA]
- On SAS-R6, "show pool" output was showing incorrect CBS and MBS values if the system is brought up in port-scheduler mode. This is resolved in this release. [213033-MI]
- In previous releases, SAM sync performed on 7210 was failing if there was MTU mismatch in the SAS to SAM path and node is managed over IPv6 in-band. This issue is resolved in this release. [214627-MA]
- On 7210 SAS-K, port based remarking stops for other SAP traffic when one of the other SAP on uplink lag or uplink port was deleted. This issue is resolved. [214802-MI]
- On 7210 SAS-K, in previous release, for sap-ingress policy, "default-fc be profile in" was not saved in config file. This issue is resolved in this release. [214918-MI]
- In case of 7210 SAS-R6 and 7210 SAS-T, OAM svc-ping was not working with MPLS path setup using LDP ECMP. This issue is resolved. [205953-MI]

RESOLVED IN R7.0R8

The following are specific technical issues that have been resolved in Release 7.0R8 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

- On 7210 SAS-R6 and 7210 SAS-T, in disabling BFD, associated OSPF or ISIS sessions were brought down. This issue is resolved. [207424-MI]
- On 7210 SAS-R6, if a port on IMM-SAS-R-b 16TX was used as a Test Head port for Y.1564, the output of "monitor port" command for that port would show "Port capacity unknown" against the "Utilization" field. This issue is resolved, and shows the correct value. [207894-MI]
- On 7210 SAS-R6 scaled setup, occasionally, on an event of clearing of IMMv2 cards may disable BGP neighborships even after the cards have come up. This issue is resolved. [211250-MI]
- In release 7.0R7, the 7210 SAS-R6 could not manage a 1830 VWM shelf when connected to the OMC port. The 7.0R8 release addresses this issue. [211252-MA]
- On 7210 SAS-M in access-uplink mode, CFM packets for down-MEPs were not processed when they ingressed a null SAP. This issue is resolved. [210415-MI]

- At times, some of 7210 SAS-T units failed to load image during boot up due to CRC errors. This issue is resolved in 7.0R8. An “admin reboot upgrade” is mandatory. [208504-MA]
- On 7210 SAS-M (in access-uplink mode), 7210 SAS-T (in access-uplink mode) and 7210 SAS-D, a few packet drops in multicast traffic were seen when members were added in or deleted from groups in a VPLS service with IGMP snooping enabled. This issue is resolved. [202716-MI]
- On 7210 SAS-K, the Y.1564 Testhead tool did not check if the packets received on the SAP matched the Mac configured in the profile. The user had to ensure that no other traffic ingress/egress the test SAP, except for testhead traffic. In release 7.0R8, this check is done. [196493-MI]
- On performing a CPM SWO on the 7210 SAS-R6 acting as the VRRP master, the VR Mac would get refreshed that caused a momentary traffic loss. This issue is fixed in 7.0R8. [201638-MI]
- On the 7210 SAS-R6 with IMMv2 cards, IPv6 traffic drops were seen due to failure of neighbor table update. This issue is resolved in 7.0R8. [209998-MA]

RESOLVED IN R7.0R7

The following are specific technical issues that have been resolved in Release 7.0R7 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

- In previous releases, on 7210 SAS-K, multicast IP address in testhead frame-payload was used and the testhead stopped working. Workaround was to re-boot the system. This issue is resolved. [206956-MA]
- In case of 7210 SAS-R6, MBS value displayed in “show pool” output was configured value of "MBS-CBS", this is corrected in 7.0R7 release. [200846-MI]
- In previous releases, system allows to configure unsupported commands on 10Gig port, “configure>port>ethernet# report-alarm signal-fail high-ber”. If the configuration is saved with this command, during subsequent reboot, configuration errors out at this command. This issue is resolved now. [209163-MI]
- In previous release, 7210 SAS-K allows to configure unsupported port command, “configure>port>Ethernet# down-when-looped”. If the configuration is saved with this command, during subsequent reboot configuration errors out at this command. This issue is resolved now. [209907-MI]
- In 7210 SAS 7.0R6 release, 7210 SAS-R6 IMM-v1 network port queue counters were not displayed properly, this issue is resolved. [209596-MI]
- In previous releases for 7210 SAS-K, the console messages were seen after boot up with a config having filters at egress, this issue is resolved.[208432-MI]

RESOLVED IN R7.0R6

The following are specific technical issues that have been resolved in Release 7.0R6 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

- In previous release, 7210 SAS-T SFP (1Gig) ports were not supported as SyncE references when SAS-T hybrid mode, that is, "*configure>system>ptp>clock>freq-source*" set to

"ssu", this issue is resolved. Workaround was to use Fixed copper port or XFP (10Gig) as SyncE reference when SAS-T hybrid mode functionality is used. [201055-MI].

- On 7210 SAS-R6, with port-based scheduler mode enabled, SAP egress QoS policy was used for remarking of CFM packets. In 7.0R6 port egress QoS policy is used. [202802-MI]
- In 7210 SAS-R6, for Queue Packet Forwarded statistics, Packets to octets conversion for frame based accounting takes into account of additional 20 bytes of L1 header. Whereas in previous releases, for Queue Drop statistics, 20 bytes of L1 header length was not considered for Octets conversion. This issue has been resolved in this release. [167508-MI]
- 7210 SAS-K, CBS oversubscription is not supported. In 7.0R6 release software enforces the check. [194548-MI]
- 7210 SAS-K overwriting QoS Policy attached to SAP with other policy, queue priority and weight were not proper, this issue is resolved. [200983-MI]
- In previous release, 7210 SAS-K, Egress Queue Stats “Octets” were counting “ingress encapsulation” rather than “egress encapsulation”. This is resolved. [202305-MI]
- In 7.0R6 release for 7210 SAS-R6, appropriate error messages displayed when attaching a resource profile to a IMM fails. [200853-MI]
- When on-demand or SAA eth-cfm two-way-slm test is initiated from 7210, if the remote device responds with a SLR packet using non-zero initial counter value, 7210 was incorrectly calculating the in-loss and out-loss. This issue is addressed in this release. [195780-MI]
- CPU destined STP/L2PT/PVST traffic incoming on access and uplink ports were using same CPU rate limiters. With this release, separate CPU rate limiters are used for access and uplink ports. [203845-MI]
- IP Multicast is not supported on RVPLS interface, do not configure IGMP or PIM, this can lead to system instability, from 7.0R6 configuration using CLI is not allowed. [204035-MA]
- Issue of UP MEP CCM flaps for qinq-inner-tag preserve epipe service during cpm switch over on 7210 SAS-R6 is resolved. [197354-MI]
- In case of 7210 SAS-R6 and 7210 SAS-T, LDP ECMP did not work when traffic is ingressing the LSR with 3 labels, this issue is resolved. [201237-MI]
- In SAS-K, to set as 'no dot1p-outer' and 'no dot1p-inner' by SNMP in SAP egress policy context was not possible, this issue is resolved. Workaround was to use CLI. [203083-MI]
- In previous release of 7210 SAS-K, for remarking inner tag was remarked with same values as outer tag. In 7.0R6 user configured value is remarked. [197343-MI]

RESOLVED IN R7.0R5

The following are specific technical issues that have been resolved in Release 7.0R5 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

- In previous releases, Egress remarking policy was not applied to CFM messages LBM and LTM forwarded by MIP in VPLS service, but they were sent out with received dot1p values. This issue is corrected in 7.0R5. [202316-MI]
- "configure system ptp clock freq-source" CLI is removed on other 7210 platforms in 7.0R5, only 7210 SAS-T supports this CLI. [202128-MI]

- 7210 SAS-K, DDM temperature and threshold values for 3HE0868CA/CB SFP were shown as zero in the output of show port command, this issue is resolved. [202891-MI]
- From 7.0R5, on 7210 SAS-K, Dual Rate Optical SFP is supported on port 3 (Combo port). [199104-MI]
- 7210 SAS-K, at times, on consecutive insertion and removal of dual rate SFPs 3HE04117AA or 3HE04116AA, messages such as "I2C read errors" were shown on the console. This may render the port to go down and subsequently any insertion or removal of SFPs on other ports can render the ports to go down as well. Work-around is to reboot the box. This is resolved in 7.0R5. [202584-MI]
- 7210 SAS-R6, at times, on consecutive insertion and removal of dual rate SFPs 3HE04117AA or 3HE04116AA, messages such as "I2C read errors" were shown on the console. This may render the port to go down and subsequently any insertion or removal of SFPs on other ports can render the ports to go down as well. Work-around is to "clear card" the slot. This issue is resolved in 7.0R5. [200396-MI]
- In case of hub and spoke 6VPE scenario, OAM VPRN-ping and VPRN-trace for IPv6 from Spoke to Spoke was not working. This issue is resolved. [203285-MI]
- 7210 SAS-R6 with 7.0R4 release, in the lab it is observed that after some network events and MBB, VPLS traffic leaked to other services. This issue is resolved in 7.0R5 release. [202456-MI]
- In previous releases, CLI used to allow unsupported "port aps" command. If user saves this config, it results in a configuration execution failure in next reboot. This issue is resolved in 7.0R5. [202317-MI]
- While responding to SDP keep alive requests, 7210 SAS is using incorrect ttl value (32). This is resulting in keep alive responses not being reached to far-end node if it is beyond 32 hops. This issue is resolved in 7.0R5. [203348-MI]

RESOLVED IN R7.0R4

The following are specific technical issues that have been resolved in Release 7.0R4 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

- In case of SAS-M, SAS-D, 7210 SAS-T, and SAS-X, in Y.1564 test results the average latency values are shown as junk values, if the actual average latency values are in the order of few tens of millisecond. This is resolved in 7210 SAS-7.0R4 release. [193843-MI]
- In a scaled IGMP snooping configuration, few membership report packets may get dropped when the system receives them at a very high rate and consistently for a longer duration. So far, this was seen only in a simulated lab environment. This issue is resolved in 7.0R4 release. [194068-MI]
- In case of SAS-M and SAS-X, in a VPLS service with IGMP-snooping enabled and mrouter configuration on multiple endpoints, very few packet drops may be seen on the mrouter endpoints, whenever a new multicast group is created or deleted due to a first member addition or a last member leave. This issue is resolved in 7210 SAS-7.0R4 release. [194910-MI]
- On SAS-T and SAS-R6, sometimes HW BFD sessions flaps. This issue is resolved in SAS-7.0R4 release. [188145-MA]
- In a VPLS service with PW redundancy and IGMP snooping configuration, multicast traffic is not switched to standby PW during primary failover condition. [198122-MA]

- On SAS-R6, with aggressive efm-oam timer configuration, efm-oam session might flap during tech-support file dumping. This issue is resolved in SAS-7.0R4 release. The minimum efm-oam timer supported is 300msec. [200057-MI]
- Issue of Egress SAP Stats does not work for IP multicast forwarded traffic is resolved in 7.0R4. [185990-MI]
- In case of 7210 SAS-R6, UP MEP did not converge, if endpoint created on port where nondefault qinq etype is configured, this issue is resolved in 7.0R4. [178512]
- 7210 SAS-X and 7210 SAS-M (Network mode), for R-VPLS service high value of Eth-Ring switch over times is resolved in 7.0R4 release. [189948-MI, 189950-MI]
- In case of SAS-R6, SAS-X, and SAS-M, Multicast meter configuration with DSCP classification in Network Port Ingress QoS policy was erroring out. This issue is resolved in 7.0R4. [202391-MI]

RESOLVED IN R7.0R3

The following are specific technical issues that have been resolved in Release 7.0R3 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

- In case of 7210 SAS-R6, If "access egress" qos policy was attached to ports, in software releases 7.0R1 and 7.0R2 any further node reboot or CPM switchover can cause new standby CPM to keep rebooting. In software releases of 6.1R1, 6.1R2, 6.1R3 and 6.1R4, any further node reboot or CPM switchover can erase access egress policy on the new standby CPM. This issue is resolved. [194808-MA]
- In case of 7210 SAS-R6, sometimes few down MEPs were in defect state after cpm switchovers, issue was observed with large number of MEPs configured. This issue is resolved. [194808-MI]
- In 7210 SAS-T network mode we will be able to attach 13 unique remark policies to access port, hybrid port and IP interface. In 7.0R4, CLI check is added to prevent configuration of more than 13 unique remark policy attachment. [191078]
- In 7210 SAS-T network mode, in previous release default access egress policy was not getting programmed when the port mode changed from hybrid to access. This issue is resolved. [191630-MI]
- From 7210 SAS 7.0R3, source-address option in the route-policy to configure pim join-policies to filter (S,G) joins/prunes is allowed. [192725-MI]

RESOLVED IN R7.0R2

The following are specific technical issues that have been resolved in Release 7.0R2 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

- Default external route is not being installed in OSPF DB in MC-LAG Active/Standby switchover scenario. This is resolved. [191081-MI]
- With previous release of 7.0, In case of 7210 SAS-E, Link Local Multicast Data (224.0.0.x) was getting dropped in the service instead of getting flooded if IGMP snooping enabled in VPLS service. This issue is resolved. [185208-MA]
- In case of 7210 SAS-X, in previous release when less than 8 queues were attached to SAP ingress, CBS consumed value is 185 kilo bytes instead of 80 kilo bytes. This is resolved. [191255-MI]

- With previous release, newly booted SAS-T node with no config allowed only 128h meters instead of 256, issue was not observed if booted with config file. Issue is resolved. [190997-MI]
- On 7210 SAS-T and SAS-D, under certain link failure conditions, operational speed of 1Gig fixed copper port downgraded to 10Mbs. This issue is resolved. [184258-MI]
- System allowed to remove a trap-target from a snmp-trap-group even if that particular traptarget is configured under “snmp-dying-gasp”. Execution of such saved configurations errored out. This is resolved. [182398-MI]
- “snmp-dying-gasp” trap may not use system ip address as source-ip, with certain sequence of “snmp-dying-gasp”, source address, and system-ip configurations. This issue is resolved. [188404-MI]
- In case of 7210 SAS-M, configuring LAG without any members, creates a service and adds LAG SAP to service, adding member port to LAG. Now, when SAP is removed, traces were seen with 7210 SAS 7.0R2 release, this issue is resolved in 7.0R2. [191249-MI]

RESOLVED IN R7.0R1

The following are specific technical issues that have been resolved in Release 7.0R1 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

- During earlier release of 7210 SAS-R6 it was recommended to configure max value of 2 for "aclsap-ingress" in "system-res-prof", that is, max of 512 ACL entries. Now, Max value of 4 can be used for "aclsap-ingress" that is, max of 1024 ACL entries. [171858-MA]
- With Tacplus configuration, a non-harmful message "Slot A: aaaUnlockX:semGive failed" is fixed. [182400-MI]
- For 7210 SAS-R6 Egress filter applied to an epipe service “qinq-innertag-preserve”, created to process traffic with more than 2 tags, was not working, this issue is resolved. [165564-MI]
- 7210 SAS-T access-uplink, copying one slope policy to another existing one did not overwrite. Workaround was to delete the second slope policy and then copy. This issue is resolved [163000-MI]
- System was allowing to remove a trap-target from a snmp-trap-group even if that particular trap-target is configured under “*snmp-dying-gasp*”. Execution of such saved configuration errored out. This is resolved. [182398-MI]
- For 7210 SAS-R6 CLI “*qos>queue-mgmt>high-slope*” or “*qos>queue-mgmt>low-slope*” context, if the configured “start-avg” value is higher than the default “max-avg” value, this configuration is saved in wrong order. If a system is rebooted with this saved configuration, configuration execution errors out. This issue is resolved. [190032-MI]
- For SAS-X CLI “*qos>queue-mgmt>high-slope*” or “*qos>queue-mgmt>low-slope*” context, if the configured “start-avg” value is equal to the default “max-avg” value, this configuration is saved in wrong order. If a system is rebooted with this saved configuration, configuration execution errors out. This issue is resolved. [190032-MI]
- In case of SAS-D When port loopback with mac-swap or testhead test is performed on an EPIPE/VPLS service which has SAPs on port 1/1/1 and Lag Id “1”, traffic over these SAPS were forwarded with incorrect VLAN Ids. This issue is resolved. [190223-MA]

- In a “b-vpls” service of SAS-X with the below SAPs combination traffic over these SAPs was forwarded with incorrect VLAN Ids in previous releases.
  port 1/1/1, Lag Id “17” (or)
  port 1/1/2, Lag-Id “18” (or)
  port 1/1/3, Lag-Id “19” (or)
  port 1/1/4, Lag-Id “20” (or)
  port 1/1/5, Lag-Id “21” (or)
  port 1/1/6, Lag-Id “22” (or)
  port 1/1/7, Lag-Id “23” (or)
  port 1/1/8, Lag-Id “24” (or)
  port 1/1/17, Lag-Id “25” (or)”.
  This issue is resolved.[190223-MA]
- With Cpipe configuration present in 7210 SAS-M, USB device was failing to get recognized by the system. This is resolved.” [185134-MA]
- From release 5.0R1 onwards for 7210 SAS-X, there are improvements in rate limiting the CPU destined ICMP traffic.

NEW FEATURES

RELEASE 7.0R12

There are no new items described as features added to 7.0 R12 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

RELEASE 7.0R11

There are no new items described as features added to 7.0 R11 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

RELEASE 7.0R10

The following items describe features added to 7.0 R10 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

7210 SD CARD SUPPORT FOR 7210 SAS-K NON-ETR PLATFORM

Platforms Supported: 7210 SAS-K ETR.

From release 7210 SAS 7.0R10, SD card is supported on 7210 SAS-K non-ETR platform. Support for USB continues as before. In other words, release 7210 SAS 7.0R10 will work with either SD card or USB stick in the rear storage slot.

RELEASE 7.0R9

There are no new items described as features added to 7.0 R9 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

RELEASE 7.0R8

There are no new items described as features added to 7.0 R8 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

RELEASE 7.0R7

The following items describe features added to 7.0 R7 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

7210 SAS-K ETR PLATFORM

Platforms Supported: 7210 SAS-K ETR.

7210 SAS-K ETR is a Ethernet demarcation device targeted for business services, mobile back haul, and vertical and strategic industry segment with support for extended temperature operating range (-40 degree Celsius to +65 degree Celsius). It is a 1G Ethernet demarcation unit capable of serving a single customer or a few.

The following is a brief overview of the product capabilities:

- 1RU, does not have fan (has passive cooling), with an option to use external AC power supply or external DC power supply (both -48V and +24V DC option is supported).

- Supports two power supply unit PINS on the rear panel, providing an option to operate with redundant power supplies (a mix of AC and DC power supply is also allowed) and the capability to log events on power supply failure (requires configuration).
- Provides rack and wall mount options.
- Ethernet Interfaces - 2 x 10/100/100 Base-T ports, 2 x 100/1000 SFP ports and 1 Combo Port (can be used either as an SFP fiber port or RJ45 Copper port).
- Console port for management.
- There are 2 flash drive ports for storage – One on the front panel and other on the rear of the unit. The flash drive port on the rear is internal to the unit and can be secured.
  - The front panel flash drive port is a USB port.
  - The rear panel flash drive port is a SD port and supports SD card for storage.

The feature set supported on the 7210 SAS-K ETR matches the support available on 7210 SAS-K. For more information, see the 7210 SAS-D,E,K Basic System Configuration User Guide.

MULTIPLE STREAM SUPPORT WITH Y.1564 TESTHEAD

Platforms Supported: 7210 SAS-K (ETR and non-ETR).

The 7210 SAS 7.0R7 release supports to generate multiple streams of traffic, for a total of up to ~1Gbps, using Y.1564 testhead OAM tool and validates performance metrics for multiple SAPs.

For more information, see the 7210 SAS-D,E,K OAM and Diagnostics User Guide.

PTP/1588 OC SLAVE AND BC

Platforms Supported: 7210 SAS-R6.

The release 7.0R7 supports use of 1588v2/PTP for frequency and time recovery. It supports both OC slave and BC with IEEE default profile and ITU-T G.8265.1 frequency profile.

The following are some of the restrictions:

- PTP Hybrid mode is not supported.
- Change of clock-type for OC slave to BC or vice-versa requires a reboot of the node for the change to take effect.
- IP source address to use must be configured under *configure> security> source-address> ptp*, before PTP can be used. PTP uses the configured IP address as the source IP address in the PTP messages generated by the node. It is recommended to configure either the system IP address or the loopback IP address for use with PTP.
- In release 7.0R7, when a switch over from active to standby CPM is triggered, PTP on new active CPM takes about 40 minutes to go to a stable, locked state. The downstream slaves using this SAS-R6 observe a similar performance behavior.

For more information, see the 7210 SAS-M,T,X,R6 Basic System Configuration User Guide.

1PPS AND 10MHZ TIMING INTERFACES

Platforms Supported: 7210 SAS-R6.

The release 7.0R7 supports 1pps and 10MHZ to provide only output reference. These interfaces must be used only when PTP is configured and used as a reference. In other words, the output of these interfaces is not recommended to be used without use of PTP.

For more information, see the 7210 SAS-M,T,X,R6 Basic System Configuration User Guide.

RELEASE 7.0R6

The following items describe features added to 7.0 R6 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

7210 SAS-R6 2ND GENERATION IMM 7210 SAS-R6 16T

This release supports the 16 port fixed copper variant of the 2nd generation IMM for 7210 SAS-R6. This IMM provides 20Gbps switching capacity and is non-oversubscribed. The copper port is a RJ.5 interface and supports all the 3 speeds – 10/100/1000Mbps. It provides the same set of services and feature capabilities as the other variants of IMMv2 cards. In addition it supports Synchronous Ethernet on all the ports.

NOTE: On a 7210 SAS-R6 chassis IMMv1 and IMMv2 cannot be used simultaneously. In other words, either all the slots need to be equipped with IMMv1 or all of them need to have IMMv2. A mix and match of IMMv1 and IMMv2 cards is not supported. User must provision the chassis, using the command *configure> system> allow-imm-family*, to either accept IMMv1 or IMMv2 cards. Software checks the equipped cards against the value configured with this command and raise a mis-provisioning alarm if the card type does not match.

NOTE: The increased switching capacity is available for use with current version of SF/CPMs (that is, SF/CPMv2). In other words, there is no need to change the SF/CPM to utilize the increase in bandwidth.

NOTE: Please note that IMMv2 cards are not supported with SF/CPMv1.

Please read the installation guide to know how to install these IMMs. Please read the Basic System Configuration User Guide to know more about how to provision the chassis to accept appropriate IMMs.

G8032 SUPPORT FOR IMMV2 CARDS

Platforms Supported: 7210 SAS-R6 IMMv2 cards.

With this release, support has been added for G8032 on IMMv2 cards. Support provided is very similar to that available on IMMv1 cards and requires similar configuration to utilize the hardware based CCMs and fast-flood-mechanisms.

For more information, please see the 7210 SAS-M,X,T,R6 Basic Systems Configuration User Guide, 7210 SAS-M,X,T,R6 Interfaces Configuration User Guide and 7210 SAS-X,R6 Services User Guide.

Y.1564 TESTHEAD OAM TOOL

Platforms Supported: 7210 SAS-R6 IMMv1 and IMMv2 cards

ITU-T Y.1564 defines the test methodology to be used and parameters to be measured to test service SLA conformance during service turn up. It primarily defines 2 test phases. The first test phase defines service configuration test, which consists of validating whether the service is configured properly. As part of this test the throughput, Frame Delay, Frame Delay Variation (FDV), and Frame Loss Ratio (FLR) is measured for each service. This test is typically run for a short duration. The second test phase consists of validating the quality of services delivered to the end customer and is referred to as the service performance test. These tests are typically run for a longer duration and all traffic is generated up to the configured CIR for all the services simultaneously and the service performance parameters are measured for each the service.

In this release, 7210 SAS-R6 supports service configuration test for user configured rate and measurement of delay, delay variation and loss with the testhead OAM tool. 7210 testhead OAM tool supports bi-directional measurement and it can generate test traffic for only one service at a given time. Testhead OAM tool can be used to perform out-of-service tests for VPLS and Epipe services. It can validate if the user specified rate is available and compute the delay, delay variation and loss for the service under test at the specified rate. It is capable of generating traffic up to about 1Gbps rate. User might need to dedicate the resources of an internal virtual loopback port or a front panel port for use with testhead feature. Additionally, port loopback with mac-swap must be used at both ends and all services or SAPs on the test port will need to be shutdown before using the testhead.

Support is also available in Y.1564 testhead OAM tool for performing CIR/PIR tests in color-aware mode. With this functionality, user can perform service turn-up tests to validate the performance characteristics (delay, jitter and loss) for committed rate (CIR) and excess rate above CIR (that is, PIR rate). The testhead OAM tool uses the in-profile packet marking value and out-of-profile packet marking value, to differentiate between committed traffic and PIR traffic in excess of CIR traffic. Traffic within CIR (that is, committed traffic) is expected to be treated as in-profile traffic in the network and traffic in excess of CIR (that is, PIR traffic) is expected to be treated as out-of-profile traffic in the network, allowing the network to prioritize committed traffic over PIR traffic. The testhead OAM tool allows users to configure individual thresholds for green/in-profile packets and yellow/out-of-profile packets. It is used by the testhead OAM tool to compare the measured value for green/in-profile packets and yellow/out-of-profile against the configured thresholds and report success or failure.

For more information, see 7210 SAS-M,T,X,R6 OAM and Diagnostics Guide and 7210 SAS-M,X,T,R6 Interfaces Configuration User Guide.

NOTE:

- Depending on the IMM variant user might need to assign the internal virtual loopback port resources or the front-panel port resources for use with this functionality. Testhead-loopback port as well as mac-swap loopback port configured for the test, should be in the same line card where test sap is present.
- The user must configure resources for ACL MAC criteria in ingress-internal-tcam using the command *config>system> resource-profile> ingress-internal-tcam> acl-sap-ingress> mac-match-enable*. Additionally they must allocate resources to egress ACL MAC or IPv4 or IPv6 64-bit criteria (using the command *config>system> resource-profile> egress-internaltcam> acl-sap-egress> mac-ipv4-match-enable or mac-ipv6-64bit-enable or mac-ipv4-match-enable*). Testhead tool uses resources from these resource pools. If no resources are allocated to these pools or no resources are available for use in these pools, then testhead will fail to function. Testhead needs a minimum of about 4 entries from the ingress-internal-tcam pool and 2 entries from the egress-internal-tcam pool. If user allocates resources to egress ACLs IPv6 128-bit match criteria (using the command *config> system> resource-profile> egress-internal-tcam> acl-sap-egress> ipv6-128bit-match-enable*), then testhead will fail to function.

PORT LOOPBACK WITH MAC-SWAP

Platforms Supported: 7210 SAS-R6 IMMv1 and IMMv2 cards

This release supports port loopback with MAC swap. When loopback with MAC swap is configured for a SAP, the software enables PHY/MAC loopback on the port where the SAP is configured. All the packets sent out of the port configured for loopback is received back by the

system. On ingress to the system after the loopback, the node swaps the MAC addresses for the specified SAP and service. It only processes packets that match the specified source MAC address and destination MAC address, while dropping packets that do not match. It processes these packets as per the service configuration for the SAP. This is recommended for use with only VPLS and VLL services. In case of 7210 SAS-R6, user might need to assign the resources associated with a virtual loopback port or a front panel port before using this feature. A loopback on the port is expected to be used with an external third-party Ethernet test device. They can be used to diagnose problems with the service provisioning or for testing end-to-end performance metrics for the service.

When the loopback with mac-swap command is executed, it affects all the services and protocols configured on the port as all the packets sent out of the port is looped back, hence exercise extra care when using this command. If multiple saps exist on port, it is recommended to shutdown all the SAPs other than test SAP for which mac-swap is configured. At a time, loopback can be enabled on only one sap.

For more details and recommended procedure of usage please read the 7210 SAS-M,T,X,R6 Interfaces Configuration User Guide and 7210 SAS-M,X,T,R6 OAM and Diagnostics User Guide.

PTP/1588v2 – OC SLAVE

Platforms Supported: 7210 SAS-K

Precision Time Protocol (PTP) is a timing-over-packet technique defined in IEEE 1588-2008. PTP provides the capability to synchronize the network element to a Stratum 1/PRC-traceable source through a network that may or may not be PTP-aware. PTP provides an alternative to Adaptive Clock Recovery (ACR) with the advantages of being a standards-based messaging protocol, having lower bandwidth requirements, and potentially providing better performance. PTP also has the benefit of being able to transport both frequency and phase (time).

The IEEE 1588 functionality is integrated with the existing central clock mechanism. The frequency recovered from the PTP packet stream is made available as one of the input options to the central clock and can be distributed using synchronous Ethernet (syncE) to other nodes.

Following are some of the major functionalities supported:

- Only OC-slave support is available.
- All Ethernet ports support PTP (both fiber and copper, including combo ports).
- Hardware Port-based timestamps is used.
- IEEE 1588 standards based frequency and time profile is available.
- ITU-T G.8265.1 standards based frequency profile is available.
- 7210 SAS-K uses one-step mechanism for PTP message exchanges.

The following are some of the restrictions:

- PTP hybrid mode is not supported in this release.
- PTP OC-Master and BC is not supported in this release.
- Use of PTP timestamps for OAM messages is not supported in this release.

For more information, see the 7210 SAS-D,E,K Basic Systems Configuration User Guide.

LAG SUPPORT – ACTIVE/ACTIVE ON ACCESS-UPLINK PORTS ONLY

Platforms Supported:7210 SAS-K

With this release, support is included for LAG on 7210 SAS-K. LAG with LACP support is available only on access-uplink ports and only active/active mode is supported.

For more information, see the 7210 SAS-D,E,K Interfaces Configuration User Guide.

DEI CLASSIFICATION AND MARKING

Platforms Supported: 7210 SAS-K

DEI based classification is supported for access SAP ingress and access-uplink port ingress. DEI classification can be enabled or disabled per FC. When DEI based classification is enabled, profile assigned by the classification entry is ignored and instead the DEI bit in the packets determines the ingress profile of the packet. DEI bit in the received packet is used to determine the ingress profile for the packet. If in the received packet, DEI = 0, then packet will be considered to be GREEN or in-profile and if DEI = 1, then packet will be considered to be YELLOW or out-of-profile. The profile assigned at the ingress is used to determine WRED slope to apply to the packet at the ingress queuing point. The profile of the packet cannot be reassigned by ingress queue shapers.

DEI based marking is supported on access SAP egress and access-uplink port egress. DEI bit in the outermost VLAN tag of the packet can be marked to carry the profile, assigned by this node to the subsequent nodes in the network. It allows high-priority in-profile packet to be allocated appropriate resources by all the network nodes on the path to the final destination. Similarly, it allows out-of-profile packets to be treated with less preference compared to in-profile packets by all the network nodes on the path to the final destination.

Refer to the 7210 SAS-D,E,K QoS User Guide for more information.

DOT1P MARKING FOR INNER TAG OF QINQ SAP

Platforms Supported:7210 SAS-K

With this release, user has an option to mark the Dot1p values for the inner tag of a QinQ access SAP and QinQ access-uplink SAP independently of the value used for marking the Dot1p bits in the outermost tag. The value can be assigned based on the FC or it can be copied over from the received VLAN tags.

NOTE: DEI bit cannot be marked for inner tag. If user configures the option to copy over the Dot1p values from the received VLAN tag, then the DEI bit is copied over too.

Refer to the 7210 SAS-D,E,K QoS User Guide for more information.

CFM FAULT PROPAGATION

Platforms Supported: 7210 SAS-K

Operators typically deploy many different technologies in the network. These technologies use specific notification methods to indicate or clear faults between peers. There is no native single approach for end-to-end Operation, Administration & Management (OAM). The fault mapping and propagation feature provides the mediation function to bridge the gap between different technologies and provide end-to-end OAM without requiring the operator to select a single OAM tool to run across the entire network. The mapping function is used to communicate and clear faults between the different OAM functions on the same node for a point-to-point service.

In this release, Epipe service can link and propagate or clear faults between endpoints using ETH-CFM with CCM. For instance, an Epipe service could span across the network using 7210 SAS-K for Ethernet access with CFM used for OAM, using 7210 SAS-R6 with pseudowire for

the MPLS segment (T-LDP status signaling used for OAM), and using 7210 SAS-K for Ethernet access at the remote end with CFM used for OAM or Link Loss Forwarding (LLF) used to propagate fault.

Different Ethernet OAM strategies should not overlap the span of each other in order to avoid conflicts that can lead to fault propagation in the direction toward the original fault, a false positive, or worse, a deadlock condition that may require the operator to modify the configuration to escape the condition. For example, overlapping Link Loss Forwarding (LLF) and ETH-CFM fault propagation could cause these issues, as could use of ETH-RDI as an ETH-CFM fault trigger.

NOTE: 7210 SAS-K platform does not support MPLS and hence it does not support use of T-LDP status signaling for OAM. It supports only Ethernet based services and use of CFM for OAM and LLF.

Refer to the 7210 SAS-D,E,K Services and OAM and Diagnostics User Guide for more information.

IP DSCP MARKING

Platforms Supported:7210 SAS-D

With this release, option is available for users to enable marking of IP DSCP values for L2 service packets (that is, packets processed in the context of Epipe and VPLS services) sent out of access port or access uplink port. User has an option to configure either Dot1p marking or IP DSCP marking or both.

NOTE: IP DSCP marking is performed only for IPv4 and IPv6 packets. In addition, the number of VLAN tags in the packet received must match the number of SAP tags to which it is mapped to. If there are more number of tags in the packet, then the IP DSCP value is not modified.

Refer to the 7210 SAS-D,E,K QoS User Guide for more information.

DYING GASP SUPPORT

Platforms Supported: 7210 SAS-K

With this release, support to generate either EFM OAM or SNMP dying gasp is provided, with an option to the user to configure one of them. Dying gasp messages are generated only on power loss event. If EFM OAM is configured, dying gasp is sent out of only access uplink ports which have EFM OAM enabled. If SNMP based dying gasp is configured, the dying gasp is sent to the configured SNMP trap server. If both SNMP based dying gasp and EFM OAM are configured, only SNMP Dying gasp traps are sent to the configured SNMP trap server.

NOTE: On reception of EFM OAM dying gasp message, 7210 SAS-K generates a SNMP trap as before.

Refer to the 7210 SAS-D,E,K Interfaces Configuration User Guide for more information.

ETH-CFM QOS ENHANCEMENT

Platforms Supported: 7210 SAS-K

Service OAM (SOAM) and the associated CFM tools have aligned behaviors with this release. Up and Down MEPs will process the egress QoS policy for packets that are generated from the node. In addition, a new CLI command is introduced to set the priority for LTR messages processed in the context of MIP to provide an option for the user to configure the LTR response priority to be different than the LTM request message.

Refer to the 7210 SAS-D,E,K OAM and Diagnostics User Guide for more information.

RELEASE 7.0R5

There are no new items described as features added to 7.0 R5 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

RELEASE 7.0R4

The following items describe features added to 7.0 R4 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

7210 SAS-R6 2ND GENERATION IMM (IMM-SAS-R-B)

This release supports 2nd generation of IMM on 7210 SAS-R6 (named imm-sas-r-b, and also referred to as IMMv2 below). These IMMs double the switching capacity to 20Gbps per IMM compared to 10Gbps supported with the first generation IMMs (named imm-sas-r). Using the 2nd gen IMMs, the redundant switching capacity of the 7210 SAS-R6 node increases to 120Gbps (full-duplex) from 60Gbps.

The following variants of the IMMv2 are supported in this release:

- IMM - 7210 SAS-R-b 10SFP - 1SFP+IMM variant that supports 10 x 1GE SFP ports and 1 x 10GE SPF+ port. It is a non-oversubscribed card.
- IMM - 7210 SAS-R-b 2SFP+IMM variant that supports 2 x 10GE SFP+ ports. It is a non-oversubscribed card.
- IMM - 7210 SAS-R-b 4SFP+IMM variant that supports 4 x 10GE SFP+ ports. It is an oversubscribed card.
- IMM - 7210 SAS-R-b 22cSFP IMM variant that supports 11 x 1GE SFP port when standard SFP optics are used or supports 22 x 1GE SFP ports when Compact SFP optics are used. User can also use a mix of standard SFP and Compact SFP optics.

NOTES:

- On a 7210 SAS-R6 chassis IMMv1 and IMMv2 cannot be used simultaneously. In other words, either all the slots need to be equipped with IMMv1 or all of them need to have IMMv2. A mix and match of IMMv1 and IMMv2 cards is not supported. User must provision the chassis, using the command configure> system> allow-imm-family, to either accept IMMv1 or IMMV2 cards. Software will check the equipped cards against the value configured with this command and raise a mis-provisioning alarm if the card type does not match.
- The increased switching capacity is available for use with current version of SF/CPMs (i.e. SF/CPMv2). In other words, there is no need to change the SF/CPM to utilize the increase in bandwidth.
- Note that IMMv2 cards are not supported with SF/CPMv1.

In addition to the doubling of the switching capacity, the following improvements are available with second generation IMM:

- Increase in Layer-2 MAC address table entries (FIB in hardware), allowing more number of MAC addresses to be learnt by the node. It allows for larger number of MAC addresses to be learnt per service.
- Increase in IP routing table entries (FIB in hardware), allowing more IPv4 routing entries or IPv6 routing entries per node. It allows the platform to be deployed in a larger network with more number of routes.

- Increase in ingress CAM resource pool, providing a larger number of classification rules and forwarding class per SAP or a larger number of ingress ACLs or get better scaling with other features that use the ingress CAM resource pool.

Please read the 7210 SAS Installation Guide to know how to install these IMMs. Please read the 7210 SAS Basics System Configuration User Guide to know more about how to provision the chassis to accept appropriate IMMs.

7210 SAS-K

7210 SAS-K is an Ethernet demarcation device targeted for business services, mobile backhaul, and vertical and strategic industry segment. It is a 1Giga Ethernet demarcation unit serving a single customer or many.

NOTE: 7210 SAS-K non-ETR variant is supported in this release. Support for ETR variant is not available in this release.

Following is a brief overview of the product capabilities.

- 1RU, fanless unit (passive cooling), with external AC power supply, provides rack, and wall mount options.
- Ethernet Interfaces - 2 x 10/100/1000 Base-T ports, 2 x 100/1000 SFP ports and 1 Combo Port (can be used either as an SFP fiber port or RJ45 Copper port).
- Console port for management.
- 2 USB ports for storage – one on the front panel and other on the rear of the unit; the one on the rear can be secured;
- Provides Ethernet based Epipe and VPLS services using Ethernet QinQ or Dot1q uplinks.
- Provides service differentiation with queuing, hierarchical shaping and scheduling capability on SAP ingress and SAP egress and large packet buffer for burst absorption.
- A rich set of Ethernet OAM tools, such as Y.1731/CFM based LB, LT, SLM, DM. Per SAP loopback with mac-swap, Y.1564 testhead, EFM OAM, and others to allow for quick troubleshooting in case of any customer reported issues, minimizing truck rolls. It provides capability to measure in-service performance parameters such as delay, jitter and loss, using Y.1731/CFM based OAM tools and to perform service activation tests using Y.1564 testhead OAM tool, allowing operators to validate and track SLA compliance.

Major Features Supported on 7210 SAS-K

The following are the major features supported in this release for 7210 SAS-K.

Services

The following service functionality is supported:

- Ethernet based VPLS and Epipe services using access ports and/or access-uplink ports
- RVPLS service (only IPv4) only for in-band management of the device
- Access SAPs – NULL, Dot1q and QinQ encapsulation
- Access-uplink SAPs – QinQ encapsulation

- Service MTU is supported
- DHCP snooping in VPLS service.

QoS

The following is an overview of QoS support available, with more details available in the subsequent paragraphs.

- Access SAP – Per SAP Ingress Queuing and Egress Queuing
- Access Uplink Port – Per Port Ingress and Egress Queuing
- WFQ and Strict Priority scheduling
- 64MB packet buffer memory
- WRED for congestion management – High and Low priority Slope per Queue for in-profile and out-of-profile traffic, Ring and Non-Ring Slope on egress of access-uplink port
- Access SAP Ingress Classification – DSCP and Dot1p only
- Access uplink port Ingress Classification – Dot1p only
- Option to configure queues with configurable FC to queue map and other queue parameters such as CIR/PIR rate, CBS/MBS, priority, weight and WRED slopes.
- Dot1p Marking for Access SAP egress and Access Uplink Port egress (only outermost VLAN tag)
- SAP Ingress policies to define SAP ingress queuing for access SAPs with support for:
  - SAP ingress classification - Dot1p and IPv4 DSCP classification. MAC and IP classification is not available.
  - SAP Ingress Profile Assignment - Option to configure ingress profile (in/out) or option to assign profile based on ingress queue shaper rate.
  - Hierarchical Ingress Shaping (2 levels – per Queue and per SAP).
  - Option to configure queues per SAP, with configurable FC to queue map and other queue parameters such as CIR/PIR rate, CBS/MBS, priority, weight and WRED slopes.
  - Option per SAP to map Unicast traffic and BUM traffic per FC to the same queue or use different queues.
- SAP Egress policies to define SAP egress queuing for access SAPs with support for:
  - Hierarchical Egress Shaping for access SAPs (3 levels – per Queue, per SAP and per port).
  - Option to configure queues per SAP, with configurable FC to queue map and other queue parameters such as CIR/PIR rate, CBS/MBS, priority, weight and WRED slopes.
  - Unicast and BUM traffic uses the same queue per FC.

- Network QoS policies for Access uplink port Ingress and Egress with support for:
  - Dot1p and IPv4 DSCP classification on port ingress.
  - Port Ingress Profile Assignment – Option to configure ingress profile (in/out) or option to assign profile based on configured ingress queue shaper rate.
  - Option to configure ingress and egress queues per port, with configurable FC to queue map and other queue parameters such as CIR/PIR rate, CBS/MBS, priority, weight and WRED slopes.
  - Hierarchical Egress Shaping (2 levels – per Queue, per port).
- SAP Ingress and SAP Egress ACLs (MAC, IPv4 and IPv6 criteria)

OAM and Management Tools

The following OAM tools and Management tools are supported:

- CFM/Y.1731 based Ethernet service OAM tools with support for Down MEP, UP MEP and MIP
- Y.1564 testhead OAM tool for service activation tests.
- Per SAP loopback with mac-swap.
- LLDP.
- EFM OAM (Dying gasp is not supported).
- LLF with NULL SAP.
- SAA and Accounting policies.
- L2CP Tunneling support for EFM, LLDP, and LACP.
- Local Mirroring with support for NULL SAP, Dot1q SAP and Q1.* SAP as mirror destination. Mirror sources can be SAP ingress, SAP egress, Port Ingress and Port Egress.

Network Synchronization

SyncE is supported to provide input reference to system clock or distribute timing reference using syncE. SyncE is support on both fiber and copper ports. On copper ports, 7210 SAS-K can act as a master to distribute timing reference or as a slave to act as timing slave.

Boot Options

7210 SAS-K supports the following options for booting the node:

- Using auto-init/network to download the BOF and images.
- Using USB port at the rear of the chassis (cf1:\).
- Using USB port on the front panel of the chassis (uf1:\).

Features not supported on 7210 SAS-K

The following are some of the features not available on 7210 SAS-K in this release:

- DEI based classification and remarking
- Frame based accounting.
- Dying Gasp (Both EFM OAM and IP SNMP)
- CFM-based Fault Propagation
- NTP Broadcast client server
- PTP
- LAG
- G.8032
- xSTP and 802.1x
- IGMP snooping and MVR

IPv6 SUPPORT IN BASE INSTANCE WITH OSPFv3

Platforms Supported: 7210 SAS-R6

With this release, support has been added for OSPFv3 routing protocol for IPv6 in the base routing instance.

For more information, see 7210 SAS Routing Protocols User Guide, System Management User Guide, and Basic System Configuration User Guide.

6VPE AND 6PE SUPPORT

Platforms Supported: 7210 SAS-R6, 7210 SAS-X, and 7210 SAS-M (network mode only).

This release includes support for IPv6 services with support for IPv6 IES services and IPv6 VPRN services.

7210 can be configured as a Dual-stack router with support for both IPv4 and IPv6 routing. It provides an option to the operator to connect IPv6 networks using the IPv4/MPLS network infrastructure using 6PE tunnels. IPv6 IES IP Interfaces is supported in the base routing instance, with support for routing protocols OSPFv3 and IS-IS for IPv6 and static routing.

In addition, IPv6 VPRN services are supported using 6VPE mechanisms allowing operators to provide IPv6 VPNs. For PE-CE protocols, eBGP for IPv6 and static routing is supported.

For more information, see the 7210 SAS Services User guide, Routing Protocols User Guide, System Management User guide, and Basic System Configuration User Guide.

MULTIPLE INSTANCES OF IS-IS

Platforms Supported: 7210 SAS-R6, 7210 SAS-X, 7210 SAS-M, and 7210 SAS-T (network mode only).

On 7210 SAS-X and 7210 SAS-R6, support to instantiate more than one instance of IS-IS has been added. It allows for configuration of smaller network routing domains such that routing information can be separated in a large network with large number of nodes. Smaller routing domains allows the use of network devices with smaller IPv4 FIB capacity to be used in network deployments.

On 7210 SAS-M and 7210 SAS-T, supports for only a single IS-IS instance and user has an option to use an instance ID other than zero (which is the default). IT allows operators to use 7210 SAS-M and 7210 SAS-T to be used in network where multiple instances of IS-IS is deployed and the instance ID is not zero.

For more information, see the 7210 SAS M,X,T,R6 Routing Protocols User Guide.

MULTIPLE LDP LSR-ID (ALSO KNOWN AS) LDP LOCAL LSR-ID)

Platforms Supported: 7210 SAS-R6, 7210 SAS-X, 7210 SAS-M and 7210 SAS-T (network mode only).

The multiple LDP LSR-ID feature provides the ability to configure and initiate multiple T-LDP sessions on the same system using different LDP LSR-IDs. In the current implementation, all T-LDP sessions must have the LSR-ID match the system interface address. This feature will continue to allow the use of the system interface but also any other loopback interface or local interface address on a per T-LDP session basis. Note that LDP control plane will not allow more than a single T-LDP session with the same local LSR ID to two different LSR-IDS on the same remote node.

An SDP of type LDP will use the source address configured as the local LSR-ID for the T-LDP session to the peer matching a specific SDP far-end address. If no targeted session has been explicitly pre-provisioned to the far-end node under LDP, then the SDP will auto-establish one using the system interface address as the LSR-ID.

An SDP of type RSVP must have the local LSR-ID as the destination of the RSVP LSP from the peer. The local LSR-ID must be a local interface which is not a loopback if CSPF is enabled on the RSVP LSP.

The multiple LDP LSR-ID also provides the ability to use the LDP local interface address instead of the system address as the LSR-ID for the LDP adjacency to the peer over the local interface. In this case, the transport interface will automatically be set to use the same local interface address. This feature can be configured for any I-LDP session. When used as such, the I-LDP transport address parameter is ignored and the session is forced to use the interface as transport-address.

For more information, see the 7210 SAS M,T,X,R6 Routing Protocols and MPLS User Guide.

ETH-CFM PRIMARY VLAN SUPPORT FOR DOWN MEP

Platforms Supported: 7210 SAS-R6, 7210 SAS-X, and 7210 SAS-T (network mode only).

This release extends CFM primary VLAN support to Down MEPs on an Ethernet SAP in an Epipe and VPLS service MEPs. This allows operator to use ETH-CFM tools for fault diagnosis and troubleshooting services when a SAP aggregate a set of VLANs (for example: Dot1q Default SAP).

For more information, see the 7210 SAS M,T and the 7210 SAS-X,R6 Services User Guide.

CFM UP MEP IN VPLS SERVICE

Platforms Supported: 7210 SAS-R6 – IMMv2 (imm-sas-r-b) only.

With this release, support for UP MEP is available in VPLS service. UP MEP allows operators to place a diagnostic point as close to the customer as possible. It allows operators to diagnose fault with services and measure service performance metrics up to the UNI demarcation point. The 7210 UP MEP implementation supports both CFM and Y.1731, including SLM. It can also be used with SAA.

NOTE: Before using UP MEP user needs to configure appropriate amount of resources using the CLI commands under "*config> system> resource-profile>global-res-profile> sf-internal-tcam-resources> eth-cfm> up-mep*". UP MEP feature shares resources with G8032, therefore if upgrading from a previous release, the user must ensure enough resources are available for use with UP MEP.

NOTE: Support is only available on IMMv2 cards. IMMv1 cards do not support this feature.

For more information about ETM CFM and UP MEPs, see the 7210 SAS-X,R6 Services User Guide, 7210 SAS-M,T,X,R6 Basic System Configuration User Guide and 7210 SAS-M,T,X,R6 OAM and Diagnostics User Guide.

BI-DIRECTIONAL MIPS FOR EPIPE SERVICE

Platforms Supported: 7210 SAS-R6

Support for CFM MIP (Maintenance Intermediate Point) is available for use with SAPs and SDPs in an Epipe service. MIPs are useful to operators to diagnose and localize faults by using CFM linktrace and loopback messages. In earlier releases, Ingress MIP was supported only in a VPLS service for SAPs and spoke-SDPs. Ingress MIP responds only to messages that ingress the node. For Epipe service, 7210 SAS implements a MIP which responds to both messages that ingress the node and messages that egress the node (also known as Bidirectional MIP).

Note: Epipe MIPS require resource to be configured for down-mep and up-mep under "configure system resource-profile".

For more information, see the 7210 SAS-X,R6 Services User Guide and 7210 SAS-M,T,X,R6 OAM and Diagnostics User Guide.

TIMING INTERFACES - BITS, 1PPS, 10MHZ

Platforms Supported: 7210 SAS-T (both access-uplink and network mode).

With this release, support is available for BITS interface ports on 7210 SAS-T for use as a input reference or to distribute system clock. User has an option to use either or both BITS1 or BITS2 port. However, BITS1 and BITS2 can be used either as input or output should not be used as one input and the other as output.

This release also supports 1pps and 10MHZ to provide only output reference. These can be used only when PTP is configured and used as a reference. In other words, the output of these interfaces is not recommended to be used without use of PTP.

For more information, see the 7210 SAS-M,T,X,R6 Basic System Configuration User Guide.

TIMING INTERFACES - BITS

Platforms Supported: 7210 SAS-R6.

With this release, support is available for BITS1 interface ports on 7210 SAS-R6 for use as a input reference or to distribute system clock. User has an option to use only BITS1 port (BITS2 port is not supported) BITS1 port can be configured either input or output, should not be used one as input and other as output. For redundancy user can use BITS1 port from active CPM and BITS1 port from standby CPM.

For more information, see the 7210 SAS-M,T,X,R6 Basic System Configuration User Guide.

AUTO-INIT ENHANCEMENTS

Platforms Supported: 7210 SAS-X, 7210 SAS-M, 7210 SAS-T, 7210 SAS-E, 7210 SAS-D (both network mode and access-uplink mode, as applicable).

In prior releases, for the first time boot, user did not have an option to modify some of the BOF parameters, such as link speed, uplink VLAN ID, etc. when using the DHCP based auto-init process. With this release, user is provided an option to configure some of the BOF parameters, such as link speed, link auto-negotiation setting, link duplex setting, uplink ports numbers to

use, and uplink VLAN ID to use. The user provided values are then used to configure the uplink ports appropriately before using DHCP to obtain the BOF from the network with the image and configuration location (as before).

In prior releases, during the first time boot, if DHCP failed to get back responses auto-init would not attempt to load software images (Timos software – both.tim) available from the flash (as shipped from manufacturing). With this release, the bootloader software uses the images (Timos software – both.tim) on the flash to boot the node and present a login prompt to the user. User can then login and use the CLI command 'autoinit stop' to stop the auto-init process and continue with configuration of the node. If the user does not use this command, then the node will reboot and attempt auto-init all over again, going through this process all over again.

For more information, see the 7210 SAS-M,T,X,R6 Basic System Configuration User Guide.

LDP ECMP – ONLY LSR LSPS

Platforms Supported: 7210 SAS-R6 and 7210 SAS-T (network mode only).

This release includes support for LDP ECMP for LSR LSPs only. It provides an option of load-balancing traffic across multiple LSPs at node which is acting as an LSR. LDP ECMP is not supported on a LER node.

The ECMP resources in hardware are shared with IP ECMP feature. Before using LDP ECMP at a LSR node, user needs to allocate ECMP resources and enable it using the CLI command *configure> system> resource-profile> global-resource-profile> router> ldp-ecmp-routes* on 7210 SAS-R6 and the CLI command *configure> system> resource-profile> router> ldp-ecmp-routes* on 7210 SAS-T. For more information about resource usage, see the 7210 SAS-M,T,X,R6 Basic System Configuration User Guide.

NOTE: LDP software will install ECMP paths as long as hardware resources are available for the /32 prefixes. Software will install only a single path after it runs out of ECMP resources in hardware (as long as the number of prefixes is less than the supported system limit for number of LDP /32 prefixes).

For more information about LDP ECMP, see the 7210 SAS MPLS User Guide.

ETHERTYPE FOR DOT1Q ENCAPSULATION PORT

Platforms Supported: 7210 SAS-R6, 7210 SAS-X, 7210 SAS-M, 7210 SAS-T, and 7210 SAS-D (both network mode and access-uplink mode, as applicable).

In prior releases, the ethertype for Dot1q encapsulated port was defined by the system to be 0x8100 and it could not be modified. With this release option is provided to configure the Ethertype for the dot1q encapsulated port. The configured ethertype is used to match with the ethertype present in the outermost tag of the packet received on a dot1q encapsulated port. If there is a ethertype match the packet is identified as a tagged packet and the VLAN ID in the outermost tag is used to map the traffic to one of the SAPs configured on the port. If there is no ethertype match, the packet is identified to be an untagged packet and mapped to the dot1q default SAP or dot1q explicit null SAP, if configured.

NOTE: The Ethertype used to match the inner tag's Ethertype value for a packet received on a QinQ encapsulated port is system defined and set to 0x8100. This feature does not allow user to configure this value.

Following are some of the restrictions:

- Configuration of dot1q etype is supported for access ports and hybrid ports. On hybrid ports, it applies to all traffic (that is, traffic mapped to SAPs and network IP interfaces). It is not supported for network ports.
- In access-uplink mode, Dot1q-preserve SAPs cannot be configured on ports configured to use dot1q ethertype other than 0x8100. In other words, use of dot1q ethertype value of 0x8100 is mutually exclusive to configuration of dot1q-preserve SAPs on a Dot1q port. The converse is also true.
- The maximum number of unique dot1q-etypes configurable per node is limited. The resources needed for configuration of dot1q-etype is shared by the default dot1q-etype, default qinq-etype and user configured values for qinq-etype. In other words, the number of unique dot1q-etypes allowed decreases, if the number of unique qinq-etype configured is more. The converse is also true.

For more information, see the 7210 SAS-D,E,K Interfaces Configuration User Guide and 7210 SAS-M,T,X,R6 Interfaces Configuration User Guide for more information.

LDP Downstream-On-Demand (DoD)

Platforms Supported: 7210 SAS-R6, 7210 SAS-X, 7210 SAS-M and 7210 SAS-T (network mode only).

This feature adds support for Downstream-on-Demand (DoD) label allocation as per RFC 5036. This feature can be enabled on a link-level LDP session and thus will apply to prefix labels only, not service labels. In this release, the 7210 SAS nodes can request a label for the FEC prefix corresponding to the LSR-ID of the LDP DoD neighbor and can reply to label requests from its DoD neighbor for any FEC it has activated.

NOTE: Only LDP DoD single hop is supported. Multi-hop support is not available. In other words, 7210 SAS nodes only replies to label which are available locally and does not forward a label binding request to its downstream neighbor if the labels have not been activated locally.

For more details, see the 7210 SAS-M,T,X,R6 MPLS User Guide.

Multi-Segment Psuedowire Routing (Dynamic MS-PWs)

Platforms Supported: 7210 SAS-R6, 7210 SAS-X, 7210 SAS-M and 7210 SAS-T (network mode only).

In Release 7.0R1, the 7210 SAS-X and 7210 SAS-R6 platforms supported PW switching as one method for providing inter-domain VLL services. This was achieved by configuring the PW-switching points at the S-PEs between domains, as well as the PW endpoints on the T-PEs.

Release 7.0R4 introduces dynamic MS-PW routing and signaling in which the switching points are automatically instantiated in the S-PEs, as described in draft-ietf-pwe3-dynamic-ms-pw-13.txt. The path of the MS-PW is dynamically signaled end-to-end by T-LDP, using PW routing information installed in the S-PEs by MP-BGP. Per-PW configuration is only required at the endpoints of the MS-PW in the T-PEs.

This release includes the following elements of dynamic MS-PWs:

- Generalized ID FEC (FEC129) with AII Type 2.
- Dynamic Multi-segment PW signaling using T-LDP.
- Dynamic Multi-segment PW routing with MP-BGP, using the MS-PW NLRI.
- OAM using VCCV-Ping and VCCV-Trace on dynamic MS-PWs.

Dynamic MS-PWs are supported for Epipe VLL services. Dynamic and static routes, as well as explicit paths for MS-PWs are supported. Dynamic MS-PWs may be established across LDP or RFC 3107 labeled BGP SDPs. PW redundancy is supported so that dynamic MS-PWs may be used as a part of a set of PWs used for PW redundancy, including MC-LAG. Diverse routes for the active and standby MS-PWs can be achieved by using explicit paths or dynamically using a BGP route distinguisher.

PW routing is configured under the new CLI structure: "*confg>service>pw-routing*", while spoke-SDPs using dynamic MS-PWs are configured at T-PEs under "*config>service>epipe>spoke-sdp-fec*".

NOTE: 7210 SAS-R6 and 7210 SAS-X support both S-PE and T-PE functionality. 7210 SAS-M and 7210 SAS-T (network mode) platforms support only T-PE functionality.

For more information, see the 7210 SAS-M,T Services User guide and 7210 SAS-X,R6 Services User Guide.

PORT-BASED EGRESS QUEUES

Platforms Supported: 7210 SAS-R6 (IMMv2 only).

This release introduces port-based egress queues on 7210 SAS-R6 with only IMMv2 cards. It supports per FC based shaping and scheduling on egress of an access or hybrid port, in lieu of per SAP egress queues. It is useful in deployments where the node is acting as an Ethernet aggregation node providing Ethernet transport, providing an option to simplify the QoS provisioning and mechanisms implemented on the node. With this feature enabled software creates 8 queues per access port and all the SAPs configured on that port uses those 8 queues. In case of a hybrid port, all the SAPs configured on the hybrid port uses the per port network egress queues.

NOTE: 7210 SAS-R6 IMMv1 does not support this feature.

The user needs to enable port-based egress queuing on access ports by using the CLI command *configure> system> resource-profile> global-resource-profile> port-scheduler mode*. This is a per node setting. In other words, when this mode is enabled software creates 8 egress queues on all the ports (that is, network ports, hybrid ports and access ports) in the system. It is mutually exclusive to use of per SAP egress queues.

For more information about the port-based egress queues and the shaping and scheduling behavior, see the 7210 SAS-X,R6 QoS User Guide.

ETH-CFM QOS ENHANCEMENT

Platforms Supported: 7210 SAS-R6, 7210 SAS-X, 7210 SAS-T, 7210 SAS-M, 7210 SAS-D (both network mode and access-uplink mode for all applicable platforms).

Service OAM (SOAM) and the associated CFM tools have aligned behaviors with this release. Up and Down MEPs will process the egress QoS policy for packets that are generated from the node. MPLS EXP bits are properly parsed and sent to the ETH-CFM application, these are new default behaviors.

NOTE: This behavior is not implemented for 7210 SAS-M Down MEPs and 7210 SAS-K Down and Up MEPs. In addition on all platforms MIPs do not provide an option to set the priority for LTR response.

For more information, see the 7210 SAS-M,T,X,R6 OAM and Diagnostics User Guide.

MULTI-HOP BFD FOR BGP

Platforms Supported: 7210 SAS-R6, 7210 SAS-X and 7210 SAS-T (network mode only).

In this release, multi-hop BFD is supported for MP-BGP sessions used to exchange VPRN routes in a VPRN service. This allows for faster detection of failure and support faster convergence. For example, it could be used to track BGP RR failure when the node has MP-BGP sessions with multiple RR nodes for redundancy. 7210 SAS uses UDP port number 4784 for establishing multi-hop BFD session.

Additionally, this release allows for use of BFD (single-hop session) for eBGP PE-CE routing protocol in an IPv4 VPRN service. With this, operator can use BFD for faster detection of failures in the PE-CE interface and support highly available services.

For more information, see the 7210 SAS-M,T Services User Guide, 7210 SAS-X,R6 Services User Guide and 7210 SAS-M,T,X,R6 Routing Protocols Guide.

ROUTED VPLS (AS A SERVICE)

Platforms Supported: 7210 SAS-R6.

Routed VPLS (R-VPLS) allows a VPLS instance to be bound to an IES IP interface. Within an R-VPLS service, traffic with a destination MAC matching that of the associated IP interface will be routed based on the IP forwarding table; all other traffic will be forwarded based on the VPLS forwarding table. R-VPLS service can be associated with only IES IPv4 interface in the base routing instance. R-VPLS service supports static routing and routing protocols - OSPFv2 and IS-IS. It can be used for providing L3 services to the customer and for in-band management of the node.

Following are some of the restrictions:

- Spoke-SDP or mesh-SDP cannot be configured in the VPLS instance used for R-VPLS.
- IP Multicast and IGMP snooping is not supported in the VPLS instance used with R-VPLS.
- Multiple SAPs on the same port cannot be part of the same VPLS instance when used with R-VPLS.
- Only dynamic ARP is supported. Static ARP entries cannot be configured.
- SAPs configured in the VPLS instance used with R-VPLS cannot be configured on hybrid ports.
- On 7210 SAS-R6, only unicast traffic uses SAP egress queues. BUM traffic sent out of the SAPs in the service uses port-based egress queues. These queues are shared by all the SAPs and are not user configurable.
- On all 7210 platforms, RVPLS SAPs can accept only packets with number of tags exactly matching the number of SAP tags to which the packet is mapped to. In other words, on a NULL SAP in an RVPLS service can accept only untagged and priority tagged packets, a dot1q SAP can accept only singly tagged packets and a Q1.Q2 SAP can accept only doubly tagged packets. Packets with more number of tags are dropped.

For more information, see the 7210 SAS-X,R6 Services User Guide for more information.

1830 CWDM MANAGEMENT USING OMC (R6)

Platforms Supported: 7210 SAS-R6.

This release adds support for management of the 1830 VWM (CWDM) device using the OMC port on 7210 SAS-R6. It supports equipment and inventory management, with support for provisioning of cards inserted into the slots available on the 1830 VWM (CWDM) device. The user must provision the card and card-type (also known as, module type) before the card can be

managed by the 7210 SAS. The 7210 SAS detects and reports mismatch in provisioning of the card. It also detects and reports insertion and removal of the card/module from the slot on the 1830 device.

For more information, see the 7210 SAS Basic System User Guide for more information.

NOTES:

- Up to 4, 1830 CWDM passive devices can be connected and managed using a single OMC port.
- The USB port cannot be used to manage the 1830 VWM device.
- For redundant connectivity to active and standby SF/CPM with the OMC port, a Y-cable is required to connect the 1830 VWM (CWDM) passive device. Please read the 7210 SAS-R6 Installation guide for more information.

For more information on provisioning 1830 CWDM device management, see the 7210 SAS-M,T,X,R6 Basic System Configuration User Guide.

1830 DWDM MANAGEMENT

Platforms Supported: 7210 SAS-X, 7120 SAS-M, 7210 SAS-T, and 7210 SAS-E (both access-uplink and network mode as applicable).

This release introduces support for 1830 VWM (DWDM) device management. It supports both active and passive DWDM device management.

NOTES:

- USB port needs to be used for 1830 DWDM device management on 7210 SAS-E, 7210 SAS-M and 7210 SAS-X.
- OMC port needs to be used for 1830 DWDM device management on 7210 SAS-T. USB port cannot be used on 7210 SAS-T.
- 7210 SAS-R6 does not support management of 1830 DWDM device.

For more information on provisioning 1830 DWDM device management, see the 7210 SAS-M,T,X,R6 Basic System Configuration User Guide and 7210 SAS-D,E,K Basic System Configuration User Guide.

CONFIGURATION ROLLBACK

Platforms Supported: 7210 SAS-R6.

Configuration rollback provides the ability to return the node to a previously saved configuration (a rollback checkpoint) with minimal impact on services:

- No impact in areas of configuration that did not change
- Configuration parameters that changed (or items that changed configuration have dependencies on) are first removed (revert to default) and the previous values are then restored (can be briefly service impacting in changed areas).
- Configuration rollback is useful in case configuration changes are made but the operator later decides not to keep the changes (that is, for experimentation, or when problems are identified in the configuration during actual network operation). Rollback save is not affected by configuration in unsupported branches (the entire config is saved), but after a rollback revert, if the “diff” (between the current operational config and the rollback checkpoint) finds a change in a CLI branch that is in the Rollback Blacklist, then the revert will fail with an error message indicating the offending branch(es).

The Rollback Blacklist is under the CLI commands “config> system>resource-profile commands”.

For more information, see the 7210 SAS-M, T, X, R6 Basic System Configuration User Guide.

RELEASE 7.0R3

There are no new features added to 7.0 R3 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

RELEASE 7.0R2

The following items describe features added to 7.0 R2 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

IPv6 SUPPORT ON NETWORK IP INTERFACE

Platforms Supported: 7210 SAS-R6.

This release includes IPv6 support for only network port IP interface in the routing base instance.

This allows for use of IPv6 in in-band management of the node and for IPv6 transit traffic. IS-IS for IPv6 and static routing is supported.

Please check the 7210 SAS Routing Protocols User Guide, System Management User guide, and Basic System Configuration User Guide for more information.

RELEASE 7.0R1

The following items describe features added to 7.0 R1 of the 7210 SAS-D, 7210 SAS-E, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS.

BGP 3107 OPTIMIZATION – INSTALL LABEL ONLY FOR SERVICES

Platforms Supported: 7210 SAS-M (Network Mode), 7210 SAS-T (Network Mode) and 7210 SAS-X.

In a seamless MPLS deployment, using BGP 3107 transport tunnels access nodes can potentially received 1000s of addresses for service endpoints (PEs) corresponding to all the nodes in the network. On access nodes, it is not possible to accommodate all these routes into the MPLS FIB, though the routes can be held in the BGP RIB. To alleviate this, 7210 provides an option to install only those BGP labeled routes that are needed for services configured on the node.

When this option is enabled, BGP 3107 transport tunnel routes are held in the RIB and one of the following triggers installation of the routes into the MPLS FIB:

- SDP configuration to far-end destination (for Epipe and VPLS services configured on the node) with the option to use BGP 3107 tunnels enabled
- Dynamic SDP-binding (PW) creation when BGP-AD routes are received for an VPLS service configured on the node
- L3 VPN routes are reachable only through BGP 3107 labelled routes

- Configuration of BGP peer with ‘neighbor’ command (typically needed for eBGP session in inter-AS ‘C’ option)

NOTE: This option is recommended for use only on the edge PE devices and not on the nodes acting as the ABR/ASBR. When this option is enabled, IPv4 labelled routes not required for use by services (for example management IPv4 routes not used in services) are not installed in the FIB.

For more information refer to the 7210 SAS-M, T, X, R6 Routing Protocols User Guide, 7210 SAS-M, T Services User Guide and 7210 SAS-X, R6 Services User Guide.

PIM-SM IN BASE INSTANCE WITH IGMPv3

Platforms Supported: 7210 SAS-M (network mode), 7210 SAS-X and 7210 SAS-R6.

With this release support is available for IPv4 multicast with support for PIM and IGMPv3. It allows for efficient distribution of multicast traffic in the access networks. 7210 SAS devices support PIM-SM and PIM-SSM along with IGMPv3 in the base routing instance. Following is the list of supported functionality:

- PIM SM (Sparse Mode) and PIM SSM (Source Specific Multicast) for IPv4 multicast
- IGMP v1, v2, and v3 support with SSM translate
- PIM DR configuration, with support for use of BFD for detection of DR failure in a redundant configuration
- Only unicast routing table is used for RFP checks.
- PIM and IGMP route policies can be used to filter join messages
- PIM RP support – 7210 SAS devices support RP discovery through Static RP configuration, Dynamic RP discovery using BSR protocol and Anycast RP discovery. It is not recommended to configure 7210 SAS device as a RP or as a BSR.
- Static multicast configuration is supported

NOTE: SAP ingress QoS policies for IES interfaces and network port ingress QoS are enhanced to classify multicast traffic and control the amount of traffic accepted. Multicast traffic can be classified only when PIM is enabled on the IES IP interface or the network port IP interface.

Following are some of the restrictions:

- On 7210 SAS devices, on ingress of a port multicast traffic can be processed in the context of either IGMP-snooping (L2 multicast) or l3-multicast, but not both. In other words, it is not possible to configure SAPs on the port, such that one SAP is a receiver for multicast traffic to be processed by IGMP snooping and another is receiver for multicast traffic to be processed by IP/L3 multicast. An option per port will be available to enable one or the other. By default, IGMP snooping is enabled to be backward compatible. User needs to explicitly change this to allow processing of received multicast traffic by IP/L3-multicast.
- If a VPLS SAP is configured on the same port as the port on which IP multicast is enabled, then multicast traffic received on the SAP is dropped. Unicast, Broadcast and unknown-unicast packets received on the SAP are forwarded appropriately. This behavior is true only for VPLS SAPs and does not apply to VPLS SDPs, Epipe SAPs and Epipe SDPs. Refer to the 7210 SAS-M, T, X, R6 Routing Protocols User guide, 7210 SAS-M, T Services User Guide, 7210 SAS-X, R6 Services User Guide, 7210 SAS-M, T QoS Guide and 7210 SAS-X, R6 QoS User Guide for more information.

BGP 3107 LABELED ROUTES FOR L3 VPNs

Platforms Supported: 7210 SAS-M (Network Mode), 7210 SAS-T (Network Mode) and 7210 SAS-X.

In prior release, BGP 3107 transport LSPs was supported only for L2 services. With this release, support is available for L3 services too.

NOTES:

- On 7210 SAS platform only FRR one-to-one is with PHP is supported for RSVP LSPs used with RFC 3107 BGP LSPs.
- BGP for exchange of IPv4 non-labeled routes in the base routing instance is not supported on 7210 SAS. It must not be used.

For more information refer to the 7210 SAS-M, T Services User Guide and 7210 SAS-X, R6 Services User Guide.

MPLS SUPPORT FOR 7210 SAS-T

Platforms Supported: 7210 SAS-T (Network Mode).

This release introduces support for MPLS on 7210 SAS-T. With this support 7210 SAS-T can be used as 1G/10G access aggregation or 10G Demarcation device extending IP/MPLS to the edge of the access network. It provides operators to use IP/MPLS-based transport mechanisms for providing highly available and resilient services. It can support both Layer-2 VPN services and Layer-3 VPN services with per SAP hierarchical ingress policing and per port hierarchical egress shaping/scheduling, along with extensive Ethernet and MPLS OAM support. It provides support for network synchronization capabilities such as syncE and 1588v2/PTP.

7210 SAS-T is a 1.5RU, 19-inch rack mountable, NEBS and ETSI compliant unit, available in 2 variants:

- 7210 SAS-T – Supports standard Temperature range of 0 oC – 40 oC
- 7210 SAS-T ETR – Supports extended temperature range of -40oC to +65oC

Both these variants provide the following support (unless specified otherwise):

- 10 x 10/100/1000 Base-T copper ports, 12 x 100/1000 1G SFP ports and 4 x 10G XFP ports
- Line-rate switching on all the ports
- Redundant hot-swappable power supply (AC, DC -48V, DC +24V), with DC power source failure detection
- Hot-swappable fan tray with 3 fans and fan filter
- 2 alarm-output pin and 4 alarm-input pins, with an option to supply power (+24V) to the alarm-input.
- 3 storage locations – Internal non-replaceable flash (cf1:\) of size 2GB, external field-replaceable flash (cf2:\), and USB (uf1:\) storage device.
- 7210 SAS-T ETR units support Power over Ethernet (PoE) (802.3af) and PoE+ (802.3at). A maximum of up to 60W of power is available for use by connected PoE devices.

NOTES:

- 7210 SAS-T ETR requires use of 200W power supplies.
- 7210 SAS-T can operate in either L2 mode (also known as, access-uplink mode) or MPLS mode (also known as, network mode). User must configure the BOF parameter uplink-mode to network before using the MPLS and MPLS-TP functionality.

The following functionality (only major ones listed) is supported with this release:

- Support Access, Network and Hybrid port mode
- Support the following SAP encapsulations – NULL, Dot1q, Dot1q Explicit NULL, Dot1q Default, Dot1q range SAP, QinQ (including Q1.*, Q1.Q2 and 0.* SAP)
- Service Support
  - Epipe, VPLS, IES and VPRN services
    - Only T-PE functionality is available for Epipe service
  - VPLS service, with support for BGP-AD (auto-discovery)
    - L2PT and BPDU tunneling in VPLS service
    - IGMP (v1 and v2 only) snooping (Layer-2 multicast) and MVR
    - IGMPv3 snooping is not supported
    - DHCP snooping over SAPs
  - Layer-2 control protocol tunneling support for EFM, LLDP, 802.1x, and LACP
  - IES IPv4 services with support for OSPFv2, IS-IS, static routing and VRRP
  - VPRN IPv4 services with support for eBGP, OSPFv2, and static as PE-CE routing protocols
  - RVPLS service is not supported in this release
- MPLS Support
  - MPLS support for Epipe, VPLS and VPRN services
  - RSVP-TE with FRR (one-to-one and facility with PHP), primary & secondary LSPs with hot standby, SRLG, admin-groups, and others.
  - LDP
  - LDP over RSVP
  - BGP 3107 labeled routes for only L2 VPN and L3 VPN services

NOTE: For BGP 3107 and LDP-over-RSVP only FRR one-to-one is supported.

- PBB support
  - Native Ethernet mode supported
  - SDPs are not supported in PBB service (a.k.a PBB-VPLS is not supported)
  - PBB Epipe and PBB VPLS services supported
  - PBB BEB and PBB BCB functionality supported

Other VPLS features are also inherited by the PBB implementation: VPLS Management (FIB and SAP), L2PT, BPDU translation, ACLs, Mirroring, and QoS capabilities.

Following redundancy and high-availability mechanism are supported in both I-VPLS and B-VPLS services – LAG, mVPLS/xSTP, MC-LAG. G8032 support is available in PBB B-VPLS for use with PBB Epipe service only.

For more information refer to the 7210 SAS-M, T Services User Guide.

- MPLS-TP Support

See the section on MPLS-TP in the release notes and the user guide for more information

- IPv4 Routing Support
  - IPv4 forwarding support with static routing and support for OSPFv2 and IS-IS routing protocols.
  - VRRP support for IPv4 interfaces in IES IPv4 and VPRNv4 services
  - IPv6 addressing and forwarding is not supported (both for services and management of the node).
  - In BGP address family, only vpn-ipv4, ipv4-labeled routes (BGP RFC3107), IPv4 (only for PE-CE routing in VPRNv4 services) and l2-vpn families are supported. BGP IPv4 family is not supported in the base routing instance.
  - Supports route policies for management and control of distribution of routing information
  - DHCP (IPv4) relay support for IES and VPRN services
  - IPv4 multicast is not supported.
  - BFD - This release supports BFD on IPv4 IP interfaces and MPLS-TP LSPs. 7210 SAS-T implements BFD support in hardware and supports 10ms minimum timers for BFD sessions for IPv4 IP interfaces configured on a port. BFD sessions for IPv4 IP interfaces configured on a LAG, the 7210 SAS-R6 supports centralized sessions with a minimum timer of 100ms. BFD support is available for use with following:
    - Static routes
    - OSPFv2
    - IS-IS for IPv4
    - VRRP for IPv4 on IES, VPRN and network ports
    - RSVP-TE
    - MPLS-TP

- QOS and ACL Support
  - 8 Forwarding classes
  - SAP ingress QoS with hierarchical policing (2 levels - per FC, per SAP)
  - Port egress QoS with 8 queues per port, with hierarchical shaping (2 levels - per FC, per port egress shaper)
  - Network IP interface and network port ingress policing (only per FC)
  - Access port, Network port and Hybrid port egress queues with 8 queues per port, per port shaping and scheduling
  - Port based scheduling for access ports, hybrid ports and network ports, with support Strict-priority scheduling (SP), WDRR, WRR or hybrid (i.e. a mix where some queues are configured in SP and some other queues are configured in WDRR or WRR).
  - SAP ingress classification supports MAC criteria, IPv4 criteria, and IPv6 criteria (as applicable)
  - Egress marking using Dot1p, IPv4 DSCP and MPLS EXP (as applicable) [NOTE: unlike 7210 SAS-M, 7210 SAS-T, requires use of remarking policies for configuring egress FC to priority bit marking).
  - Supports 2 modes for buffer allocation – per node MBS pool and per port MBS pool
  - In per port MBS pool, user has an option to allocate larger amount of buffers towards the per port MBS pool by decommissioning ports which are not used to deploy any services.
  - SAP ingress and egress ACLs, Network port IP interface ingress and egress ACLS are supported, with MAC criteria, IPv4 criteria and IPv6 criteria (as applicable).
  - IPv6 match criteria supported only for Epipe and VPLS services in both QoS classification and ACLs.
- Network Synchronization support
  - Supports Synchronous Ethernet on SFP ports, XFP ports and fixed copper ports.
    - User must use SFPs and XFPs that support syncE to make use of the syncE support
    - Fixed copper ports can be used to either distribute frequency (master) or recover frequency (slave)
  - PTP/1588v2 support is available. Support for OC-slave and BC is provided with 1588-default and ITU-T G.8265.1 (frequency) profile.
  - BITS, 1pps, ToD and 10MHz interfaces are not supported in this release.

- High Availability and Reliability Support
  - Hot-swappable Redundant Power supplies
  - Hot-swappable Fan try with 3 fans, with notification for a single fan failure
  - LAG with active/active and active/standby support
  - MC-LAG support (server support)
  - G8032 with the capability to use 7210 SAS-T as interconnection nodes in a major-ring/sub-ring topology
  - STP, RSTP, MSTP with mVPLS/xSTP support
  - MPLS FRR - facility with PHP and one-to-one support
  - MPLS primary and secondary LSPs, with hot-standby secondary LSP support
  - Active/Standby PW in Epipe and VPLS services
  - VRRP (IPv4) support in IES and VPRN services
  - MPLS-TP linear protection for MPLS-TP LSPs and Active/Standby PW for MPLS-TP PWs
  - Fault propagation support in Epipe service (For example: LLF, and others.)
  - BFD support with 10ms timers for faster failure detection
- OAM support
  - Supports EFM OAM with support for EFM OAM dying gasp message or a SNMP dying gasp message on loss of power.
  - Supports LLDP
  - CFM/Y.1731 Down MEP, UP MEP, Ingress MIP only for VPLS, Ingress and Egress MIP for Epipe (see user guide for MEP support per service and different service objects).
  - CFM and Y.1731 based OAM tools – Supports CCM, Linktrace, Loopback, 2-DM, 1-DM, 2-SLM, AIS, and RDI.
  - MPLS OAM tools for Epipe, VPLS and VPRN services (example – lsp-ping, vccv-ping, vprn-ping, mac-ping, and others.).
  - Mirroring support – Option to use remote mirroring using MPLS SDPs as mirror destination or local mirroring using NULL SAP or dot1q SAP as mirror destination
  - Port loopback with MAC swap is supported
  - Y.1564 testhead OAM tool for service performance measurement before service turn-up
  - TWAMP
  - 1830 VWM device management for CWDM devices is supported

- Accounting, Security and Management support
  - Per SAP ingress and egress accounting records
  - Per network IP interface and network port accounting records
  - Out-of-band Ethernet management port is available with IPv4 support
  - Support for Dot1x is available
  - SNMP (including v3 support), SSH, Telnet, NTP, and others are supported
  - RADIUS & TACACS+ supported
  - User profiles are supported
  - Software defines a policy which is used for CPU protection and it is not user configurable.
  - Supports Autoinit, which allows operators to deploy the nodes faster. 7210 SAS-T provides the following boot options:
    - Using Autoinit
    - Using internal flash (cf1:\)
    - Using external flash (cf2:\)
    - Using USB port (uf1:\)

When shipped from factory the device is configured to use autoinit by default. For more information reference on how to use the various options to boot the 7210 SAS-T device to the 7210 SAS-T Installation Guide and 7210 SAS-T Basics System Configuration Guide.

For more information refer to the all the 7210 SAS-M, T User Guides.

MPLS-TP SUPPORT ON 7210 SAS-T (NETWORK MODE)

Platforms Supported: 7210 SAS-T (network mode).

This release introduces the MPLS Transport Profile (MPLS-TP) on 7210 SAS-T. MPLS-TP is intended to allow MPLS to be operated in a similar manner to existing transport technologies with static configuration of transport paths (that is, no requirement for a dynamic control plane), in-band proactive and on-demand operations and maintenance (OAM), and protection mechanisms that do not rely on a control plane (For example: RSVP-TE) to operate. 7210 SAS-T can operate both as an LER and LSR for MPLS-TP LSPs, and as a T-PE for MPLS-TP PWs. It can therefore act as a node within an MPLS-TP network. 7210 supports MPLS-TP for only Epipe, VPLS services and on Ethernet ports only.

NOTE: 7210 SAS-T can operate in either L2 mode (also known as, access-uplink mode) or MPLS mode (also known as, network mode). The user must configure the BOF parameter uplink-mode to network before using the MPLS and MPLS-TP functionality.

In this release, bidirectional co-routed MPLS-TP LSPs and PWs is supported. MPLS-TP identifiers, OAM and protection mechanisms defined in IETF RFCs are supported. This includes:

- MPLS-TP identifiers for nodes, LSPs, and PWs
- OAM and protection using the MPLS-TP Generic Associated Channel (G-ACh) with both IP and non-IP encapsulation (as applicable)
- Proactive CC for MPLS-TP LSPs using BFD
- On-Demand CV for MPLS-TP LSPs and PWs using LSP Ping/Trace and VCCVPing/Trace

- Linear protection for MPLS-TP LSPs, with the ability to configure a working path and a protect path for each LSP
- Static PW status signaling, (RFC 6478), with support for PW redundancy and MC-LAG (7210 node acts a T-PE only in this scenario)
- Active/standby dual homing into IES/VPRN/VPLS service configured on the 7x50 and 7210 node acting as the T-PE. (**NOTE**: The 7210 node does not support termination of MPLS-TP PW into a IES/VPRN Service).

MPLS-TP also introduces the capability to configure an unnumbered MPLS-TP interface type with a unicast, multicast or broadcast next-hop MAC address and without a configured IP address. MPLS-TP LSPs can also use conventional numbered and unnumbered IP interfaces.

For more information refer to the 7210 SAS-M,T services user guide, 7210 SAS-M, T, X, R6 OAM and Diagnostics User Guide, 7210 SAS-M, T, X, R6 Router Configuration User Guide and 7210 SAS-M, T, X, R6 MPLS User Guide.

LAG ACTIVE/STANDBY OPERATION WITHOUT LACP

Platforms Supported: 7210 SAS-M (Network Mode), 7210 SAS-T (Network Mode), 7210 SAS-X and 7210 SAS-R6.

The active/standby decision for LAG member links is a local decision driven by pre-configured selection-criteria. In releases prior to release 7.0.R1, this decision was communicated to the remote system using LACP signaling. This release provides an alternative mechanism that is applicable to connections with LACP non-capable devices based on the “disable-transmitter” function at the port-member level. As a consequence, the transmit laser will be switch off for all LAG members in standby. On switchover (active-links failed), the laser will be switched on and all LAG members will become active. This mode of operation works in conjunction with MC-LAG support available on 7210 SAS-M, T, X, R6 (in Network Mode).

For more information refer to the 7210 SAS-M, T, X, R6 Interfaces User Guide.

ROUTED VPLS (AS A SERVICE)

Platforms Supported: 7210 SAS-M (network mode) and 7210 SAS-X.

Routed VPLS (R-VPLS) allows a VPLS instance to be bound to an IES IP interface. Within an R-VPLS service, traffic with a destination MAC matching that of the associated IP interface will be routed based on the IP forwarding table; all other traffic will be forwarded based on the VPLS forwarding table. R-VPLS service can be associated with only IES IPv4 interface in the base routing instance. R-VPLS service supports static routing and routing protocols - OSPFv2 and IS-IS. It can be used for in-band management of the node or for providing L3 services to the customer.

Following are some of the restrictions:

- Spoke-SDP or mesh-SDP cannot be configured in the VPLS instance used for R-VPLS
- IP Multicast and IGMP snooping is not supported in the VPLS instance used with R-VPLS
- Multiple SAPs on the same port cannot be part of the same VPLS instance when used with R-VPLS
- Only dynamic ARP is supported. Static ARP entries cannot be configured.
- SAPs configured in the VPLS instance used with R-VPLS cannot be configured on hybrid ports.

Refer to the 7210 SAS-M, T Services User Guide and 7210 SAS-X, R6 Services User Guide for more information.

NOTE: On 7210 SAS-R6, R-VPLS feature is supported as BETA only. It cannot be used for deployment in production networks. In addition to the restrictions listed above, per SAP egress queues and egress marking is not supported on 7210 SAS-R6.

MIXED MODE LSPS IN A SDP

Platforms Supported: 7210 SAS-M (Network mode), 7210 SAS-T (Network mode), 7210 SAS-X and 7210 SAS-R6.

The mixed-LSP (Also known as, mixed mode LSPs) SDP allows for a maximum of two LSP types to be configured within an SDP: a primary LSP type and a backup LSP type. This feature allows either of the following:

- RSVP LSP as primary LSP within an SDP with LDP LSP as backup LSP. In case of failure of all RSVP LSP paths associated with the SDP, the backup LDP LSP is used.
- LDP LSP can be configured as primary LSP with BGP 3107 LSPs configured as backup LSP. In case of failure of LDP LSP the backup BGP 3107 LSP is used.

At any given time, the service manager programs only one type of LSP. This LSP is used to forward service packets. The service manager will program the NHLFE(s) for the active LSP type, preferring the primary LSP over the backup LSP. If the primary LSP is not configured or if the configured primary LSP goes down, software will program the backup LSP.

The behavior of the RSVP/LDP SDP is as follows - If the primary RSVP LSP is not configured or if the configured primary RSVP LSP goes down, software will program the backup LDP LSP. When one or more RSVP LSPs become available, the service manager reverts back to the RSVP LSP type at the expiry of the “sdp-revert-time” timer or the failure of the LDP LSP, whichever comes first. The service manager then re-programs accordingly. If the “infinite” value is configured, then the SDP reverts to the RSVP LSP type only if the LDP LSP failed. Note however, that LDP uses a tunnel down damp timer which is set to three (3) seconds by default. When the LDP LSP fails, the SDP will revert to the RSVP LSP type after the expiry of this timer. For an immediate switchover, this timer must be set to zero (0).

Note the following difference in behavior of the LDP/BGP SDP compared to that of an RSVP/LDP SDP. For a given /32 prefix, only a single route will exist in the routing table: the IGP route or the BGP route. Thus, either the LDP FEC or the BGP label route is active at any given time. The impact of this is that the tunnel table needs to be re-programmed each time a route is deactivated and the other is activated. Furthermore, the SDP revert-time cannot be used since there is no situation where both LSP types are active for the same /32 prefix.

Refer to the 7210 SAS-M, T Services User Guide and 7210 SAS-X, R6 Services User Guide for more information.

ETHERNET CRC ETHERNET MONITORING

Platforms Supported: 7210 SAS-D, 7210 SAS-T (Access-uplink and Network mode), 7210 SAS-M (Access-uplink and Network mode), 7210 SAS-X, and 7210 SAS-R6.

This release supports the capability to monitor the CRC error rate on Ethernet ports (these are errors seen in received traffic from a remote Ethernet source). It is possible for two independent thresholds to be set, one for signal-degrade and one for signal-failure. If the error rate reaches the signal-degrade threshold, a log message will be raised. If the signal-failure threshold is reached, the associated Ethernet port is declared down. A port that is taken out of service due to

signal-failure will remain in an operationally down state until an administrator enables the port by manually performing a shutdown/no shutdown operation on the associated port configuration. This should only be used when sufficient redundancy is available for the connection reachable through a given Ethernet port. Care should be taken when determining the threshold to be used for the signal-degrade and signal-failure levels as setting these parameters at a low threshold could result in false detection of a problem.

Refer to the 7210 SAS-E, D Interfaces User Guide, 7210 SAS-M, T, X, R6 Interfaces User Guide for more information.

DEI CLASSIFICATION AND MARKING

Platforms Supported: 7210 SAS-D, 7210 SAS-T (Access-uplink and Network mode), 7210 SAS-M (Access-uplink and Network mode), 7210 SAS-X, and 7210 SAS-R6.

DEI based classification is supported on access port, Access-uplink ports, Network ports and Hybrid ports. DEI classification can be enabled or disabled per port. DEI bit in the received packet is used to determine the ingress profile for the packet. If in the received packet, DEI = 0, then packet will be considered to be GREEN or in-profile and if DEI = 1, then packet will be considered to be YELLOW or out-of-profile. The profile assigned at the ingress can be used to enable color-aware metering with SAP ingress policing, network port ingress policing and access-uplink port ingress policing. The profile of the packet can be reassigned by ingress meters/policers when policing is used on SAP ingress. When policing is used, the final profile of the packet is determined by the meter/policers, based on the configured CIR/PIR rates. If a packet is below CIR rate, it is assigned green/in-profile and if it exceeds the CIR rate and is below the PIR rate, it is assigned yellow/out-of-profile.

On 7210 SAS-X, the behavior remains the same, when ingress policing is used, but it is different when ingress queuing is used. When SAP ingress queuing is used, the profile assigned to the packet by user configuration cannot be reassigned by the ingress meters/policers or by ingress queue rate shapers. Hence, user assigned profile is the final profile assigned to the packet.

The final profile assigned at ingress is used by egress to determine the WRED slope to use. The WRED slope determines whether the packet is eligible to be assigned a buffer and can be queued up on egress queue for transmission. On 7210 SAS-X, the behavior remains the same, when ingress policing is used, but it is different when ingress queuing is used. When SAP ingress queuing is used, the ingress profile is used to determine the WRED slope to use at ingress (access SAPs), in addition to egress (access SAPs and network/hybrid port).

NOTE: Ingress queuing is supported only on 7210 SAS-X and Ingress policing is supported on 7210 SAS-D/M/T/X/R6.

DEI based marking is supported on access ports, access-uplink ports, hybrid ports and network ports. DEI bit in the outermost VLAN tag of the packet can be marked to carry the profile, assigned by an operator's trusted node at the ingress to the operator's network, to the subsequent nodes in the network. It allows high-priority in-profile packet to be allocated appropriate resources by all the network nodes on the path to the final destination. Similarly, it allows out-of-profile packets to be treated with less preference compared to in-profile packets by all the network nodes on the path to the final destination.

Following are some of the restrictions:

- DEI based classification cannot be configured for IP interfaces. MPLS EXP based classification will continue to be available as before.

Refer to the 7210 SAS-E, D QoS User Guide, 7210 SAS-M, T QoS User Guide, 7210 SAS-X, R6 QoS User Guide, 7210 SAS-E, D Interfaces User Guide, and 7210 SAS-M, T, X, R6 Interfaces User Guide for more information.

VLL SPOKE SWITCHING (ALSO KNOWN AS SWITCHING-PE (S-PE)) SUPPORT FOR EPIPE SERVICE USING MPLS

Platforms Supported: 7210 SAS-X and 7210 SAS-R6.

The VLL Spoke Switching feature, also called Switching-PE (S-PE) functionality, provides the user with the ability to create a Epipe service by cross-connecting two spoke SDPs. In this release, only Manual Pseudowire Stitching/Switching is supported for Epipe service. The objective of this feature is t

o allow the scaling of Epipe and VPLS services in a large network in which the otherwise full mesh of PE devices would require thousands of Targeted LDP sessions per PE node.

Services with one SAP and one spoke SDP are created normally on the PE; however, the target destination of the SDP is the 7x50/7210 SAS PW switching node instead of what is normally the remote PE. In addition, the user configures a VLL service on the PW switching node using the two SDPs.

The PW switching node acts in a passive role with respect to signaling of the PWs. It waits until one or both of the PEs sends the label mapping message before relaying it to the other PE. This is because it needs to pass the Interface Parameters of each PE to the other. A PW switching point TLV is inserted by the switching PW to record its system address when relaying the label mapping message. This TLV is useful in a few situations:

- It allows for troubleshooting of the path of the PW especially if multiple PW switching points exist between the source PE and destination PE.
- It helps in loop detection of the T-LDP signaling messages where a switching point would receive back a label mapping message it had already relayed.
- The switching point TLV is inserted in PW status messages when they are sent end-to-end or from a PW switching node towards a destination PE.

PW OAM is supported for the manual switching PWs and allows the PW switching node to relay end-to-end PW status notification messages between the source and destination PE. The PW switching node can generate a PW status notification and to send it to source PE or destination PE by including its system address in the PW switching point TLV. This allows a source/destination PE to identify the origin of the PW status notification message.

NOTE: Epipe S-PE functionality is not supported on 7210 SAS-M Network Mode and 7210 SAS-T Network Mode.

Refer to the 7210 SAS-X, R6 Services User Guide for more information.

VLL spoke switching (also known as Switching-PE (S-PE)) support for Epipe service using MPLS-TP

Platforms Supported: 7210 SAS-R6.

The VLL Spoke Switching feature, also called Switching-PE (S-PE) functionality, provides the user with the ability to create an Epipe service by cross-connecting two spoke SDPs. In this release, only Manual Pseudowire Stitching/Switching is supported for Epipe service. 7210 SAS device acting as the S-PE can stitch two MPLS-TP PWs or a MPLS-TP PW and an IP/MPLS static PW. With this functionality, 7210 SAS-R6 can act as a gateway between MPLS-TP access network and IP/MPLS network.

MPLS PW OAM is supported between the endpoints of the service, encompassing both the MPLS-TP PW segment and IP/MPLS PW segment, if any. MPLS-TP LSP OAM is supported only for the MPLS-TP LSP segment.

NOTES:

- In the IP/MPLS domain, MPLS LSP can be setup dynamically, but the MPLS PW needs to be configured statically.
- S-PE/Stitching between static PW and a dynamic PW is not supported.

Refer to the 7210 SAS-X, R6 Services User Guide for more information.

Configuration Rollback

Platforms Supported: 7210 SAS-R6 (BETA only).

Configuration rollback provides the ability to return the node to a previously saved configuration (a rollback checkpoint) with minimal impact on services:

- No impact in areas of configuration that did not change
- Configuration parameters that changed (or items that changed configuration have dependencies on) are first removed (revert to default) and the previous values are then restored (can be briefly service impacting in changed areas).

Configuration rollback is useful in case configuration changes are made but the operator later decides not to keep the changes (i.e., for experimentation, or when problems are identified in the configuration during actual network operation). Rollback save is not affected by configuration in unsupported branches (the entire config is saved), but after a rollback revert, if the "diff" (between the current operational config and the rollback checkpoint) finds a change in a CLI branch that is in the Rollback Blacklist, then the revert will fail with an error message indicating the offending branch(es). The Rollback Blacklist is as follows:

- CLI commands under the *config> system>resource-profile* commands

Refer to the 7210 SAS-M, T, X, R6 System Management User Guide for more information.

Fault Propagation – LLF with dot1q/qinq SAPs on access ports

Platforms Supported: 7210 SAS-D, 7210 SAS-T (Access-uplink mode) and 7210 SAS-M (Access-uplink mode).

In releases prior to release 7.0R1, LLF was supported only with NULL SAP configured in an Epipe service. With this release, LLF support is added which provides an option to bring down an access port configured with dot1q or qinq encapsulation when the access-uplink port goes down. The SAPs on the dot1q port could be configured in either Epipe or VPLS services.

For more information refer to the 7210 SAS-D, E OAM and Diagnostics User Guide and 7210 SAS-M, T, X, R6 OAM and Diagnostics User Guide.

OSPFv2 AS PE-CE PROTOCOL

Platforms Supported: 7210 SAS-T (Network mode), 7210 SAS-X and 7210 SAS-R6.

With this release, OSPFv2 is available for use as PE-CE protocol in a VPRNv4 service. Following support is available:

- Supports receiving CE routes using OSPFv2 and distribution of those routes using MP-BGP to remote CE routers in the VPRN service as type 5 LSA ("AS-external routes").
- Supports "Super Backbone" functionality, which allows for distribution of OSPF routes to remote CE routers in the same VPRN service, as type-3 inter-area routes instead of AS-external routes. It allows remote CE routers to differentiate between actual AS-external routes and internal routes (that is, the internal routes for sites that are reachable over the VPN service).
- Supports "Sham Links" to allow remote CE routers to use the backbone VPRN service as the primary link for connectivity and a backdoor link for secondary connectivity.
- Supports use of "DN" bit and VPN route tags to allow loop detection and prevention
- Option is available to use BFD with OSPFv2 for faster detection of failure of the PE-CE interface
- Supports multiple OSPF instances per node, with a single OSPF instance per VPRNv4 service.
  NOTE: Only a single instance continues to be supported in the base routing instance.
- Graceful restart helper mode is supported

NOTE: OSPFv2 PE-CE routing protocol is not supported on 7210 SAS-M in network mode.

For more information refer to the 7210 SAS-M, T Services User Guide, 7210 SAS-X, R6 Services User Guide and 7210 SAS-M, T, X, R6 Routing protocol User Guide.

LAYER-2 CONTROL PROCESSING (L2CP) FOR EPIPE AND VPLS SERVICE

Platforms Supported: 7210 SAS-D, 7210 SAS-T (Access-uplink and Network mode), 7210 SAS-M (Access-uplink and Network mode), 7210 SAS-X, and 7210 SAS-R6.

With release 7.0R1, L2CP support has been extended to allows for transparent forwarding of untagged LACP, EFM OAM, LLDP, and 802.1x control packets received on an access port using a dot1q default SAP or a dot1q explicit NULL SAP on a dot1q encapsulated port or a 0.* SAP on a QinQ encapsulated port. When using a QinQ uplink or a dot1q uplink, the control packets are tagged with configured uplink SAP tags. Hence, to the upstream (from customer towards the core) nodes in the network, they appear as tagged packets and are forwarded transparently (if it is a 7210 and also 7x50). When using MPLS uplinks, the control packets are encapsulated in MPLS.

The difference with respect to earlier releases is that, in earlier releases to tunnel LACP, EFM OAM, LLDP, and 802.1x frame the only option available was NULL access SAP configured in an Epipe service. As mentioned above with release 7.0R1, we have additional options available, i.e. dot1q explicit null SAP, dot1q default SAP, and 0.* SAP, for an Epipe service.

In a VPLS service, similar support is available and these L2 control protocol packets are flooded out of all the other SAPs in the service and are encapsulated on egress with the appropriate SAP tags. Hence, it is recommended to use this feature very carefully and only when a VPLS service is used to emulate an end-to-end Epipe service (i.e. an Epipe configured using a 3-point VPLS Service, with one access SAP and 2 access-uplink SAP/SDPs for redundant connectivity). In other words, if the VPLS service is used for multipoint connectivity, it is not recommended to use this feature.

Refer to the 7210 SAS-E, D Services User Guide, 7210 SAS-M, T Services User Guide and 7210 SAS-X, R6 Services User Guide for more information.

MANAGEMENT ACCESS FILTER (MAF) IP CRITERIA ENHANCEMENT – SUPPORT MATCH OF SOURCE TCP/UDP PORT AND FRAGMENT FIELDS

Platforms Supported: 7210 SAS-D, 7210 SAS-T (Access-uplink and Network mode), 7210 SAS-M (Access-uplink and Network mode), 7210 SAS-X, and 7210 SAS-R6.

With this release, Management Access Filter (MAF) IP criteria has been extended to include match for TCP/UDP source port number and IP fragment. This allows operator greater granularity to define policies that identify the traffic that needs to be filtered or processed.

Refer to the 7210 SAS-E, D System Management User Guide and 7210 SAS-M, T, X, R6 System Management User Guide for more information.

SUPPORT BI-DIRECTIONAL MIPS FOR EPIPE ONLY

Platforms Supported: 7210 SAS-D, 7210 SAS-M (Access-uplink mode), and 7210 SAS-T (Access-uplink mode).

With this release support for CFM MIP (Maintenance Intermediate Point) is available for use with access and access-uplink SAPs in an Epipe service. MIPs are useful to operators to diagnose and localize faults by using CFM linktrace and loopback messages. For Epipe service, 7210 SAS implements a MIP which responds to both messages that ingress the node and messages that egress the node (also known as Bidirectional MIP).

NOTE: In earlier releases, Ingress MIP was supported only in a VPLS service for SAPs. Ingress MIP responds only to messages that ingress the node.

For more information, see the 7210 SAS-D, E and 7210 SAS-M, T Services User Guide and 7210 SAS-M, T, X, R6 OAM and Diagnostics User Guide.

BFD FOR BGP AND MULTIHOP BFD

Platforms Supported: 7210 SAS-M (Network mode).

In this release, multi-hop BFD is supported for MP-BGP sessions used to exchange VPRN routes in a VPRN service. This allows for faster detection of failure and support faster convergence. For example, it could be used to track BGP RR failure when the node has MP-BGP sessions with multiple RR nodes for redundancy. The 7210 SAS uses UDP port number 4784 for establishing multi-hop BFD session.

Additionally, this release allows for use of BFD (single-hop session) for eBGP PE-CE routing protocol in an IPv4 VPRN service. With this, operator can use BFD for faster detection of failures in the PE-CE interface and support highly available services.

For more information refer to the 7210 SAS-M, T Services User Guide for more information.

SUPPORT IP AND MAC CRITERIA FOR ACCESS SAP INGRESS QOS CLASSIFICATION

Platforms Supported: 7210 SAS-D, 7210 SAS-T (Access-uplink and Network mode), 7210 SAS-M (Access-uplink and Network mode), 7210 SAS-X, and 7210 SAS-R6.

In prior releases, use of MAC and IP criteria in an access SAP ingress QoS policy was mutually exclusive. With this release option is available for simultaneous use of both IP and MAC criteria in a single policy for access SAP ingress classification. It allows user to differentiate L2 packets based on MAC header fields and IP packets based on IP header fields on a single SAP and prioritize L2 and IP traffic as per their needs (for example L2 control traffic such as LACP, CCMs can be prioritized over IP user traffic).

To enable this feature user will need to allocate resources with the CLI command *configure>system> ingress-internal-tcam> qos-sap-ingress-resource> ipv4-mac-match-enable*, before associating a SAP ingress policy that has both IPv4 and MAC criteria to an access SAP. The 7210 QoS user guide has more details on resource consumption when this option is enabled.

For more information refer to the 7210 SAS-D, E QoS User Guide, 7210 SAS-M, T QoS User Guide and 7210 SAS-X, R6 QoS User Guide.

SUPPORT IPV4 PRECEDENCE IN ACCESS SAP INGRESS QOS CLASSIFICATION

Platforms Supported: 7210 SAS-D, 7210 SAS-T (Access-uplink and Network mode), 7210 SAS-M (Access-uplink and Network mode), 7210 SAS-X, and 7210 SAS-R6.

This release supports use of IPv4 and IPv6 precedence value for access SAP ingress QoS classification. It provides flexibility of using either IPv4/v6 DSCP or IPv4/v6 precedence values for differentiating and prioritizing customer traffic.

In a single classification entry can either match IP DSCP field or match IP precedence field, but not both. A single policy can contain a mix of entries such that some match IP DSCP field and some others match IP precedence field.

To enable IP precedence, at a minimum resources need to be allocated using any one of the following commands:

configure>system> ingress-internal-tcam> qos-sap-ingress-resource> ipv4-mac-match-enable or configure>system> ingress-internal-tcam> qos-sap-ingress-resource> ipv4-match-enable or configure>system> ingress-internal-tcam> qos-sap-ingress-resource> mac-match-enable or configure>system> ingress-internal-tcam> qos-sap-ingress-resource> ipv6-ipv4-match-enable.

IPv4 precedence classification entries are allocated resources from the chunks/slices allocated to any one of the above. The 7210 QoS user guide has more details on resource consumption when this option is enabled. IPv4 precedence classification entries can be configured in SAP ingress policies created using either the parameter ‘ip-criteria any’ or ‘ip-criteria dscp-only’ and IPv6 precedence classification entries can be configured in SAP ingress policies created using either the parameter ‘ipv6-criteria any’ or ‘ipv6-criteria dscp-only’.

For more information refer to the 7210 SAS-D, E QoS User Guide, 7210 SAS-M, T QoS User Guide and 7210 SAS-X, R6 QoS User Guide.

TWO-WAY ACTIVE MEASUREMENT PROTOCOL (TWAMP)

Platforms Supported: 7210 SAS-R6.

Two-Way Active Measurement Protocol (TWAMP) provides a standards-based method for measuring the round-trip IP performance (packet loss, delay and jitter) between two devices. TWAMP uses the methodology and architecture of One-Way Active Measurement Protocol (OWAMP) to define a way to measure two-way or round-trip metrics.

There are four logical entities in TWAMP: the control-client, the session-sender, the server, and the session-reflector. The control-client and session-sender are typically implemented in one physical device (the “client”) and the server and session-reflector in a second physical device (the “server”) with which the two-way measurements are being performed. The 7210 SAS device acts as the server only.

For more information refer to the 7210 SAS-M, T, X, R6 OAM and Diagnostics User Guide.

ENHANCEMENTS

RELEASE 7.0R12

There are no new items described as enhancements added to the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS for release 7.0R12.

RELEASE 7.0R11

There are no new items described as enhancements added to the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS for release 7.0R11.

RELEASE 7.0R10

The following item describe enhancements added to the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS release 7.0R10.

- In release 7210 SAS 7.0R10 support added to process Y.1731 version-1 DM request packets received on Down MEPs of 7210 SAS-M (network and access-uplink mode, VPLS and Epipe service), Epipe service on 7210 SAS-T access-uplink mode and 7210 SAS-R6. On 7210 SAS-D support was added from 7.0R6. Rest of the platforms except 7210 SAS-E, Y.1731 version-1 DM supported from beginning.
  7210 nodes supports reception of v1 messages, processes it as a v0 message, and respond back with v1. In other words, v1 messages are not generated by the node nor any v1 specific TLV or message content processed by the node.
  Note that for 7210 SAS-D and 7210 SAS-T access-uplink mode user need to configure CLI "configure eth-cfm system enable- dmm-version-interop" to process version-1 DM packets.
- TCP window size for FTP and SCP connections has been increased to 65536 Bytes from this release.
- 7210 boot process can be interrupted in the bootloader by any key press received on the console port. From 7.0R10, if no valid password entered within 30sec then it continue the boot process automatically. This enhancement ensures that the boot process will automatically continue if it was unintentionally interrupted by induced external electrical noise on RS232-console wires or operator error.

RELEASE 7.0R9

There are no new items described as enhancements added to the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS for release 7.0R9.

RELEASE 7.0R8

The following item describe enhancements added to the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS release 7.0R8.

FC SUPPORT WITH Y.1564 TESTHEAD

Platforms Supported: 7210 SAS-K (ETR and non-ETR).

With this release, Y.1564 testhead OAM tool provides validation of performance metrics for not only multiple SAPs, but multiple FCs of a single SAP or a mix-n-match of both.

For more information, see the 7210 SAS-D,E,K OAM and Diagnostics User Guide.

RELEASE 7.0R7

There are no new items described as enhancements added to the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS for release 7.0R7.

RELEASE 7.0R6

The following item describe enhancements added to the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS release 7.0R6.

Y.1731/CFM DMM VERSION 1 MESSAGE PROCESSING

Platforms Supported: 7210 SAS-D.

With this release, support has been added to process CFM/Y.1731 version 1 DM messages.

Refer to the 7210 SAS-D,E,K OAM and Diagnostics User Guide for more information.

ETH-CFM QoS ENHANCEMENTS

Platforms Supported: 7210 SAS-X, 7210 SAS-R6, 7210 SAS-T, 7210 SAS-M, 7210 SAS-D (both access-uplink mode and network mode for 7210 SAS-M and 7210 SAS-T)

In previous release, Service OAM (SOAM) and the associated CFM tools have aligned behaviors with this release. Up and Down MEPs will process the egress QoS policy for packets that are generated from the node. With this release the following enhancements are available:

- A new CLI command (mip-ltr-priority) is introduced to set the priority for LTR processed in the context of MIP. It provides an option for the user to configure the LTR response priority to be different than the LTM request message.
- Added support for PW configured to use vc-type-vlan. The Dot1p bits of the Ethernet header in the payload encapsulated by MPLS packets now uses the value specified in the ccm-ltm-priority or the priority specified during the test using the SAA/OAM tool. It is supported for both Down and Up MEPs configured on the SDP.
- Refer to the 7210 SAS-M,X,T,R6 OAM and Diagnostics User Guide, 7210 SAS-D,E,K OAM and Diagnostics User Guide, 7210 SAS-M, T Services User Guide, 7210 SAS-X,R6 Services User Guide and 7210 SAS-D,E,K Services User Guide for more information.

RELEASE 7.0R5

There are no new items described as enhancements added to the 7210 SAS-D, 7210 SAS-E, 7210 SAS-K, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS for release 7.0R5.

RELEASE 7.0R4

The following item describe enhancements added to the 7210 SAS-D, 7210 SAS-E, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS release 7.0R4.

MIP CREATION USING DEFAULT MODE FOR VPLS SERVICE

Platforms Supported: 7210 SAS-D, 7210 SAS-M, 7210 SAS-T, 7210 SAS-X, SAS-R6 (in both access-uplink mode and network mode as applicable).

With this release, configuration of ingress MIPs in a VPLS service using the default mode is supported. This allows user to create MIPs without explicitly creating lower level MEPs. In 7210 use of default MIPs consumes lesser resources in the ingress-internal-tcam resource pool than explicit MEPs. Explicit MEPs are instantiated only when lower MEPs are configured.

PTP HYBRID MODE

Platforms Supported: 7210 SAS-T (both access-uplink and network mode).

With this release, support is available for PTP in hybrid mode where SyncE or BITS can be used for frequency recovery.

Functionality can be enabled using CLI "*configure>system>ptp>clock>freq-source ssu*". when changing from pure PTP mode to Hybrid mode or vice versa, reboot is required after saving config changes.

Note that SFP (1Gig) ports and Fixed Copper ports should not be used as SyncE references for SAS-T hybrid mode that is, Only XFP (10Gig) ports can be used as SyncE references. However, SFP (1Gig) ports or Fixed Copper ports or XFP (10Gig) ports can be used as SyncE master ports for down stream slaves.

For more information, see the 7210 SAS-M,T,X,R6 Basic System Configuration User Guide.

RELEASE 7.0R3

There are no new items described as enhancements added to the 7210 SAS-D, 7210 SAS-E, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS for release 7.0R3.

RELEASE 7.0R2

There are no new items described as enhancements added to the 7210 SAS-D, 7210 SAS-E, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS for release 7.0R2.

RELEASE 7.0R1

The following item describe enhancements added to the 7210 SAS-D, 7210 SAS-E, 7210 SAS-M, 7210 SAS-X, 7210 SAS-T, and 7210 SAS-R6 OS release 7.0R1.

GENERATION OF Y.1731 AIS MESSAGE ON PORT DOWN

This feature provides an optional capability that allows the 7210 SAS-T access-uplink to generate Y.1731 AIS messages based on the port's operational state. By default, MEP exchanges CCM messages with the peer MEPs associated with it and generates AIS messages only when the CFM defect/fault detected on the MEP is of higher priority than the user configured defect. With this feature, the system tracks the operational state of the port on which a Down MEP is configured and sends out AIS messages when the port operational state changes

to down. Through appropriate configuration, it allows the operator to disable generation of CCMs for the MEP and instead use only the port's operational state for generation of AIS messages.

Note that it is recommended to disable CCM's while using generation of AIS message on port down.

FACILITY ALARM SUPPORT

Platforms Supported: 7210 SAS-E, 7210 SAS-D, 7210 SAS-T, 7210 SAS-M, 7210 SAS-X, and 7210 SAS-R6 (in both Access-uplink and Network mode, as applicable)

Facility alarms provide a useful tool for operators to easily track and display the basic status of their equipment facilities. The CLI "show system alarms" command displays current facility alarm conditions and recently cleared alarms without searching event logs or monitoring various card and port show commands to determine the health of managed objects in the system such as cards and ports. The SR OS alarm model is based on RFC 3877 and uses the RFC 3877 ALARM-MIB.

For more information refer to the 7210 SAS-D, E System Management User Guide and 7210 SAS-M, T, X, R6 System Management User Guide.

MPLS-TP EPIPE PW/SPOKE TERMINATION INTO A VPLS SERVICE

Platforms Supported: 7210 SAS-R6

With release 7.0R1, MPLS-TP support has been extended for MPLS-TP Epipe PW/spoke termination into a VPLS service (only VPLS service and not I-VPLS, B-VPLS, Routed VPLS and M-VPLS). It allows 7210 SAS-R6 to be used as a gateway between MPLS-TP and IP/MPLS network, with the MPLS-TP Epipe PW used in the access network to backhaul service traffic up to the IP/MPLS edge and terminated in to a VPLS service.

For more information, see the 7210 SAS-X, R6 Services User Guide.

KNOWN LIMITATIONS

The following are specific technical limitations that exist in Release 7.0R11 of 7210 SAS OS. The topics are arranged alphabetically.

ACLs

- At CPM MAF, src-port (front panel port) based filtering does not work for packets received on RVPLS interface. [196845]
- Egress Filter counters does not work for IES service in access-uplink mode SAS-M and SAS-D, however, ACL functionality works fine. [108134]
- The doubly tagged packet ingress on Q.* sap egresses with 3 tags on the Q1.Q2 sap. Such packet not identified as an IP packet as a result will not match the IP ACL on egress. [112850]
- Traffic on dot1q saps can hit egress filter entry attached to ":0" or "0.*" or "*" sap on same port if dot1q traffic matches and matching entry not configured on dot1q sap. The workaround is to configure matching entry with action or an entry with default action forward or drop on dot1q sap. [113270]
- With default action "drop", if CPU bound packet does not match none of the entry match criteria, these packets are still forwarded to CPU. The workaround for this is, configure a entry criteria with match any and action drop as the last entry in the IP-filter.
- A filter entry action value configured as action should force the filter to pick up the default action configured for the filter. This does not work. It is recommended to explicitly configure the action for each filter entry. [76620]
- MACs that are already learned do not age out after a filter is added to drop packets from those MACs. [73370]
- In an ingress MAC filter policy, the etype and frame-type match criteria do not match packet fields in those packets received with more than one VLAN tag. [72839]
- IP filter match criteria option-present cannot be used to match packet fields for traffic on IES interfaces. [73188]
- Egress SAP statistics and egress ACLs/filters cannot be enabled on a SAP when the port on which it is created has a default SAP configured for 7210 SAS-E.
- In case of 7210 SAS-E, an ingress IP filter policy, Layer 3 and Layer 4 match criteria (such as, src-ip, dst-ip, srcport, dst-port, etc.) do not match packet fields in those packets received with more than one VLAN tag. [72839]
- In case of 7210 SAS-E, a MAC or IP filters applied on a SAP in an IGMP snooping-enabled VPLS service will not be able to block IGMP control packets. [80612]
- From 7210 SAS 6.0 releases, TTL=1 and TTL=255 IP packets would get accounted under SAP stats and these type of packets hit the egress matching ACL's entries.
- When remarking is enabled, remarking occurs on :0,:*,0.* and null SAPs. Accordingly, the egress MAC filter matches that dot1p bit used for re-marking, even though the packets egressing these SAPs do not have a VLAN tag. [161648]
- On SAP ingress use of SAP ingress QoS policy with MAC criteria is mutually exclusive to use of ACLs with IPv6 criteria. [137396]

- Ingress IP ACL cannot be applied for DHCP broadcast packets. [180423]
- The user has to make sure at least 1 ACL entry is free for the ACL re-numbering or copy functionality to work. [164279]
- Time of day policies cannot be combined with IPv6 ACLs.
- In SAS-E Filter logging is not supported. [73135]
- For SAS-X Maximum of 1024 IP Filter and 1024 MAC Filter entries are supported, but CLI allows creation of 8k MAC entries. [105669] [105900]

CLI

- Non-printable 7-bit ASCII characters (for example, French letters with accents) are not allowed inside the various description fields. These characters were accepted for some description fields prior to Release 5.0. When upgrading to Release 5.0.R1 or later, the user must ensure that the configuration file does not contain any non-printable 7-bit ASCII characters that might have been in any description field prior to Release 5.0. Configurations that do not comply may result in failed config “exec” in CLI and/or during system bootup. User can use “exec -syntax” command to detect if any unprintable characters exist in the current configuration. [99519] [93998]
- The “detail” option for “admin save” command is not supported. Default values under any CLI context can be viewed by using “info detail” command.
- In case of access-uplink 7210 SAS-M, T, D, E, the CLI commands under the context config>router for the management routing instance are not supported. [101636]

CES

- TDM ports cannot participate in a split horizon group (although it is user configurable). TDM ports is not a supported feature. [101695]
- In Cpipe service of type CESoPSN, if the port is configured for ACR then channel group #1 must be configured in a service and must be operationally up.Channel group #1 is used as the master tributary for deriving adaptive clock using ACR.

DHCP

- The DHCP broadcast packets are sent to CPU even if DHCP relay is shut down on IES. It is recommended to delete configuration instead of keeping shut down. [161115]
- DHCP packets received over a SDP cannot be identified and option-82 inserted by the node cannot be removed by the node, in the downstream direction. Therefore, if this behavior is not required by the user, the user should not enable DHCP snooping if the DHCP server is reachable over the SDP (either spoke-sdp or meshsdp).

IGMP SNOOPING

- In case of 7210 SAS-E, on an IGMP snooping-enabled VPLS service, the 7210 SAS-E does not support multicast forwarding statistics. The show service id service-id mfib statistics command output will always show zero value counters. [81173]
- In case of 7210 SAS-M and T network mode, X and R6, in a VPLS service, when IGMP snooping is enabled, the multicast replication is based on Layer 2 MAC addresses.
- In case of 7210 SAS-M and T network mode, X and R6, IGMPv3 is not supported.

- IGMP snooping is not supported for control word enabled SDP in vpls service.
- In case of 7210 SAS-M and T network mode, X and R6, if single -tagged multicast packets arrive on a null SAP belonging to a VPLS service with IGMP snooping enabled, they are forwarded based on the MFIB if the entry is present, else they are dropped. The same is applicable for double-tagged multicast packets arriving on a Dot1q SAP. [87551]
- IGMP Snooping on sdp with vc type "vc-vlan" requires static configuration.
- On SAS-M, SAS-X, SAS-D SAS-T Default sap (:* sap) does not participate in igmp-snooping process. The following packets are flooded in the service when received on * sap: IGMP General Queries, IGMP Reports/Joins, and Registered and Unregistered Multicast Data Packets. [109045]
- On SAS-E Default sap (:* sap) does not participate in igmp-snooping process. Igmp query sent on default sap is flooded to all the saps and not learned in MFIB. If there is no entry for the group, igmp report sent on default sap is flooded to all the saps and not learned in MFIB. If there is an entry for the group then report follows the MFIB and data forwarded to only that port.
- Registered Multicast Data packets sent on default sap follows MFIB.
- Un-Registered Multicast Data packets sent on default sap gets flooded in the service. [112586]
- On SAS-E Flushing out 2047 groups learned in a single VPLS service (by executing a shut on igmp-snooping command) can cause Dot1ag to flap under loaded CPU conditions. [84904]

IP

- "allow-directed-broadcast" is not supported. [122203]
- The ping ip-address detail command should report the interface on which the ping reply was received. This information does not display in the output. [76887]
- IP packets that need fragmentation are not forwarded. However, if the ARP is not resolved for the next-hop, only the first packet is fragmented and sent out as soon as the ARP is resolved. Only CPU-generated packets are fragmented. [76353]

LAG

- For a LAG configuration with more than one port, every other jumbo frame is dropped. The solution is to increase the MBS from the default value of 128Kbits to 144Kbits for two port LAGs. [73552]
- **F**or a LAG configuration with more than one port, if a meter configuration does not specify a CBS value, some packets may be marked yellow and be treated accordingly when buffer management begins.The solution is to increase the CBS setting whenever the CIR configured for the meter is greater than 1Gbps. For a LAG with two ports, a CBS value of 64Kbits is recommended. [72497]
- When all the member ports of a LAG are removed and added back, the stats for a SAP on that LAG, belonging to a VPLS or an Epipe service, is reset to zero. [73439]
- In case of 7210 SAS-E, Dot1q tagged LACP packets received on dot1q SAP are dropped instead of forwarding them transparently. [154370]

- LACP and CFM protocol packets count are not shown in the output packets column of the show lag lag-id statistics command. Packet count for tunneled LACP pdus are not shown in port statistics. [77986]
- In 7210 SAS-R6, lag-hashing is not done for BUM traffic in a SAP-SAP case, all the traffic is sent out of the flood-port, "show lag <id> detail" displays flood port.
- In an LAG, if port is down due no lacp packets received from other end then unlearned traffic sent on other active ports of lag is also flooded on the oper down port.

MANAGEMENT

- The system becomes unresponsive and reboots when the file version check boot.tim command is issued simultaneously from multiple Telnet sessions. Simultaneous execution of this command should be avoided. [76543]
- If an ongoing FTP is aborted, the console and Telnet become unresponsive for a duration that depends on the size of the file being transferred. [76734,74294]
- Max value that can be set for svcVRouterId snmp mib object is 66. [127090]
- SNMP operations on some unsupported SNMP MIBs might succeed.
- snmp dying gasp trap for snmpv1 trap server is not supported. [125543]
- An asterisk "*" indicating an unsaved configuration change may not be displayed after changing some of the parameters under some contexts such as the system and log contexts, (for example, **A:ALU-7210>config>system or A:ALU-7210>config>log*). Additionally, the Change Since Last Save field in the show system information command output may not be updated. [61271]

MPLS

- FRR support with LDPoRSVP or BGP 3107 will not be sub-50ms.
- The operational state of LDP will go down with the reason code "IOM Failure" if the number of /32 prefixes learnt go beyond 1000 for SAS-M, 1500 for SAS-X and SAS-R6. [98085]
- A small amount of traffic loss is seen for any MBB event for traffic sent at line rate with a configuration of 200 or more LSPs. [95811]
- Implicit NULL (PHP) must be configured to use LDPoverRSVP tunnel.
- For 3107 L2 services if BGP transport is LDP then LDPoRSVP is not supported, in such configuration sdp will remain down.
- LDP-over-RSVP transport is not supported for BGP SDPs (RFC 3107). SDPs configured in this manner will become operationally up but no traffic will be forwarded. [146172]
- LSR PHP Node copies the tunnel label exp values to single vc-label packets destined to Egress LER but doesn't remark vc-label exp values. [108939]
- FRR failover time for unlearned traffic (such as broadcast, unknown-unicast, and multicast traffic types) will not be under sub-50ms.
- In case of 7210 SAS-R6, packet drops are seen during global revert MBB in case of SAP, primary path and FRR path reside on different IMM's. [177662, 177643].

MIRROR

- For 7210 SAS-D, up to 10 Uplink access SAPs can be ingress mirrored. [114247]
- For Access-uplink mode M, T, D, E, when port egress is mirror source , mirrored traffic would contain additional service internal tag.
- For Access-uplink mode M, T, D, E, in case of dot1q mirror destination, when sap ingress is mirror source and single priority tagged packet is mirrored, mirrored packet would not contain priority tag.
- For 7210 SAS-E, mirrored traffic using dot1q sap, profile assignment and hence dot1p remarking does not work. For FC be, profile is ignored and treated as in-profile always. For other FCs, profile is ignored and treated as out-of-profile always. [141252]
- For 7210 SAS-E, packets that get dropped due to egress queue drops are mirrored when port egress mirroring is enabled.
- For 7210 SAS-E, a mirrored packet contains the internal service VLAN ID (that is significant internally to the 7210 SAS-E) when ingress mirroring is configured for an IES SAP. [75852]
- For 7210 SAS-R6, if mirror is enabled on a network port, then mirror traffic carries an extra VLAN tag. This issue exists with SAS-R6 IMMv1 only. [165270]
- In case of 7210 SAS-R6, unlearnt service packets egressing out of network port with MPLS header gets mirrored without MPLS header. This issue exists with SAS-R6 IMMv1 only. [174014]
- In case of 7210 SAS-R6, additional mirrored packet sent when both ingress and egress are used as source in case of unlearnt traffic. This issue exists with SAS-R6 IMMv1 only. [175208]
- For 7210 SAS-R6, egress mirrored frames are copies of the frame as ingressed, any modifications made to a frame at egress, such as VLAN tag, TPID, L3 TTL decrements, and others are not seen at the mirror destination.
- For 7210 SAS-X, only egress rate command can be used on mirror destination. sap-egress qos policy cannot be used with mirror destination (null sap).
- For 7210 SAS-E, packets that get dropped due to egress filters are mirrored when port egress mirroring is enabled.

OAM

- It is not recommended to enable LLF on both the SAPs simultaneously of an EPIPE service, it can lead to unrecoverable fault loops.
- The 7210 SAS-M Down MEP CFM packets does not follow QoS policies.
- In case of 7210 SAS-R6, Up MEP on SAP in Epipe Service CFM reply messages egressing from SDP binding are sent with exp value 7 when remarking is disabled. [202804]
- CFM reply packets are always taken as in-profile while re-marking even when request packet is classified to out-profile. [202687]

- Up Mep on Null or * sap with egress sap dot1q/qinq, following is the behavior. [202717]
  - CCM message: by default Dot1p bits set to 0. If remarking is enabled in egress sap then takes configured dot1p.
  - Other messages: EPIPE service in SAS-R6, SAS-X, SAS-M and SAS-T (network mode only) by default Dot1p bits is set to 0. If remarking is enabled in egress sap, then the configured dot1p is taken.
- In Testhead jitter and latency values are provided only when the test traffic encapsulation is same as test SAP, for example, Q1.Q2 doubly tagged traffic is used if test sap is of Q1.Q1 encapsulation. [152369]
- On 7210 SAS-D, Mirror and Testhead functionality cannot be configured at the same time. [163084]
- For 7210 SAS-D, the show eth-cfm mep mep-id domain md-id association ma-id command will not display CCM ERROR, CCM XCON frames in its output.
- For 7210 SAS-D, the show eth-cfm mep mep-id domain md-id association ma-id remote-mep rmep-id command will not display some TLVs and details.
- On the 7210 SAS-D platform, even if a SAP is administratively shutdown, the hardware state machine receives and processes the CCM packets sent by remote peers and the CFM MEP remains up and shows no CCM defect.[126719]
- Under a high CPU load, ETH CFM defect reporting and clearing may be delayed.
- In case of Access-uplink mode M, T and D, when a SAP has UP MEP configured on it, the CFM frames would use the forwarding path of the service. This causes the “Ingress Stats” of SAP Statistics to increment when UP MEP sends packets. These packets are also counted in “Ingress Drop Stats”, if SAP’s “statistics ingress counter-mode” set to default that is, “in-out-profile-count”. [141370]
- In case of 7210 SAS-D, M, T, the 7210 SAS does not display the remote MEP's MAC address in the display output of the CLI show command "**show eth-cfm mep *mep-id* domain *md-id* association (ma-id) all-remote-mepids**"
- In case of 7210 SAS-D, M, T, the ETH-CFM CCM Sequence Check for out-of-sequence CCMs and Last CCM Sequence Number tracking is not done for received CCMs.
- In case of 7210 SAS-D, M, T, the ETH-CFM CCMs with incorrect DMAC are not dropped by hardware.
- In case of 7210 SAS-D, M, T, the ETH-CFM CCMs transmitted will always have the Sequence Number as zero.
- In case of 7210 SAS-D, M, T, the ETH-CFM CCMs with invalid Data TLV-s, Invalid Port/Interface TLV-s do not cause CCM Errors
- In case of 7210 SAS-D, M, T, and R6, the show eth-cfm mep *mep-id* domain *md-id* association *ma-id* command would not display Last CCM Rx-Time, Last CCM Seq Number, CCM Tx Count.
- Before configuring any port as “loopback-svc-port”, it’s always recommended to remove any configurations made on this port, and ensure it has only default configurations.
- Test head test port is not supported when port mode is configured as access uplink (these ports show up in show port display as "l2up"). [150123]
- Test head marker packets etype is always set to 0x0800, user defined etype in test head profile is not carried in marker packets. [153288]

- Test head marker packets does not carry any Layer 4 info defined in test head profile, any qos/filter applied on a sap based on Layer 4 fields will not take effect for markerpackets. [153414]
- For modifying saps from service, internal mac swap loop back port, test head loop back port it is recommended to deconfigure mac-swap loop back configuration. [150496, 150403]
- With UP MEP, removing all lag member ports "defMacStatus" is not reported, "defRemoteCCM's" on both ends are reported. [136119]
- When SAP in the parent MVPLS instance goes into STP blocked state, the associated SAP in the child VPLS instance is shut down. This prevents any packets from being generated in the host path. In 7210, CCM-s are hardware generated and hence the CCM state m/c works properly. However, the LB-s and LT-s, which are generated and processed in software, stops working.[109722]
- In a spoke SDP with the control word configuration enabled, vccv-ping from the remote end does not return a response when the LSP is shutdown. [80905]
- If SAP is configured as static mrouter port, port loop back with mac swap does not work in unregistered multicast traffic. Unregistered multicast traffic that is sent out of the SAP is not looped back but registered/learned multicast is looped back. [130327]

ROUTING

- "configure router bgp family" by default is set to "ipv4". It needs to be configured to "vpnipv4"for VPRN configuration.[122553]
- When the BGP routes fails to get installed due FIB is full, BGP Peer goes operationally down.
- OSPFv2/v3 would operationally go down on exceeding the FIB limit.[144137]

QOS

- In case of 7210 SAS-D, DSCP can be remarked only for packets received with number of tags matches to tags configured on ingress SAP.
- Access-Egress policy enabled with dscp remarking will remark DSCP bits in data packets egressing out of L2 SAPs (VPLS/Epipe/I-BVPLS/B-VPLS). It is recommended not to enable DSCP remark for ports carrying L2 SAPs. [121134]
- In case of 7210 SAS-R6, when SAP remarking is not enabled for L2 service SAPs and port remark is enabled, Port Remarking for L2 service does not work if ingress is null/*/0/cp-1 SAP and egress is dot1q/q1.*/q1.q2. or Ingress is spoke-ether and egress is q1/q1.*/q1.q2 SAPs or svc-sap-type qinq-inner-tag-preserve. Workaround is to use SAP egress policy for remarking. [170807,168509]
- In case of oversubscription of 7210 SAS-R6 IMM bandwidth, higher priority packets may get dropped.
- For 7210 SAS-D from 6.0R2 release, 7210 SAS-D per port total available buffer is 146KB compared to 157KB in previous releases. The shared portion of buffer available has reduced from 89KB to 78KB. [159987].

- For 7210 SAS-D, with a slope policy, queue depths for lower priority queues do not get limited to max average when the scheduler is in strict mode and if lower priority queue is not serviced by scheduler due to high traffic on higher priority queue. [111651]
- Meter buckets are re-initialized when the rate value is modified. Rate values are modified by explicitly changing the rate values using the appropriate CLI command or by changing the adaptation rule. [84395]
- When a port is congested, a small amount of excess traffic is sent out of the lower priority queues. The amount of excess traffic depends on the packet sizes. [111644, 111664]
- For 7210 SAS-E, there is a small difference in the actual rate of traffic egressing out of a port for a given egress rate limit value. The difference in the actual rate is affected by the size of the packet. For example, it is noted that for an egress rate limit value of 40Mbps, the difference is approximately 2Kbps to 150Kbps for packets sizes between 100 bytes to 9212 bytes.
- A maximum of 15 network QoS policies of type ipinterface with unique mapping of FC to EXP values can be created, and these policies must be shared among 32 IP interfaces.
- If a network QoS policy with classification based on match of a Dot1p value ‘0’ is associated to a network port, which has IP interfaces using either a null or a dot1q:0 encapsulation, any untagged IP packet received on the network IP interface will get classified to the FC designated by this rule. The same behavior is applicable to a null SAP when it receives untagged packet.[98819]
- With a slope policy, queue depths for queues 1 to 7 for a port do not get limited to max-average when the scheduler is in strict mode. [85063]
- If an IP interface is configured on a hybrid port, following is the behavior.
  - IP interface on q.* encap, single tagged packets gets proper classification and policing
  - IP interface on 0.* encap, up to two tag packets gets classification and policing properly as per the config
  - IP interface on q1.*, and q1 interface, q1.q1 packets gets proper classification, but q1.q2 does not
- PBB: Ingress classification on B-SAP using I-TAG PCP bits and egress remarking of ITAG PCP bits is not supported. [123642]
- In case of 7210 SAS-X and 7210 SAS-R6, for VPRN L3 SAP, per SAP egress remarking is not supported. It is recommended to use port based egress remarking. If DSCP is used with port based egress marking, then L2 SAP traffic is also marked. Therefore, when having a mix of L2 and L3 SAPs on the port, it is recommended to use only Dot1p based marking.
- In 7210 SAS-R6 CIR oversubscription is not supported both at Aggregate Level and Port Level (ERL). Queue and Aggregate CIR rates should be configured such that bandwidth is available to each level to service all Committed Information rates at each level. [175278]
- During congestion in the system , and if a queue is not able to get shared buffers to hold at least number of packets equal to weight configured, then the configured weights cannot be guaranteed. [163712]
- For 7210 SAS-X, the overridden CBS of a queue can only be greater than the CBS defined in the sap-ingress qos policy. [160811]

- For 7210 SAS-X, when an ERL lesser than 700Mb is applied on a 1G port and when two queues are in the PIR scheduling loop, traffic is seen in low priority queues even though there are drops in high priority queues. [152374]
- All untagged packet received on null access sap or null encap network port is classified to a fc that is associated with an entry with a match criteria set to dot1p value of "0". [98819]
- For 7210 SAS-X, Queue CIR/PIR minimum value can be set to 26kbps. Configuring lesser value results in traffic stops on egress.[102578]
- In case of 7210 SAS-X, higher Cir-Level queue's PIR traffic may affect lower Cir-level queue's CIR traffic when port egress-rate or sap egress agg-rate-limit configured. Similar issue of higher CIR queue rate affected by lower CIR queue rate seen, if queue's at same CIR level and difference between CIR values of the queues is larger. This issue is seen where egress-rate or sap egress agg-rate-limit configured value closer to sum of queue CIR's value configured. [111002, 111657,126359]
- In case of 7210 SAS-X, egress queue drop counters count only tail drop packets and WRED drops are not counted. [109298]
- For 7210 SAS-X, when 2 or more SAP queues are in the same pir level but having different weights, traffic distribution may not be as per pir weight of the queues. This behavior was observed in case of higher bandwidth allocated to one or more higher level queues of the same SAP.[107013]
- For 7210 SAS-X, when Traffic is egressing out of network port for vpls/epipe services, traffic is rate-shaped without taking MPLS or dot1q header into account on network-port. This leads to actual traffic throughput more than configured queue rate (CIR and PIR). The workaround is to take the network-header into account while configuring the queue CIR and PIR. This behavior is also with egress-rate configured on the port. In case of vprn service, MPLS header accounted for rate-shaping or egress-rate.[101713]
- For 7210 SAS-X, when traffic is sent from dot1q-sap to null-sap, the actual throughput is less than the configured queue CIR/PIR. The workaround is to take the dot1q-header into account while configuring the queue CIR and PIR. This behavior is same with egress-rate configured on the port. [102176]
- Only the outermost tag is marked with dot1p bits when remarking on egress is enabled for QinQ access SAPs. [108010]
- When configuring network QoS policy using SNMP, it is recommended to first create policy specifying type of policy (ip-interface or port type) and then modify policy to set user defined or default values of the policy. [123171]

SECURITY

- If the system IP address is not configured, RADIUS user authentication will not be attempted for in-band RADIUS servers unless a source address entry for RADIUS exists.
- SNMP access cannot be authorized for users by the RADIUS server. RADIUS can be used to authorize access to a user by FTP, console, or both.
- If the first server in the list cannot find a user the server will reject the authentication attempt. In this case, the 7210 node does not query the next server in the RADIUS server list and denies access. If multiple RADIUS servers are used, the software assumes they all have the same user database.

- If the TACACS+ start-stop parameter option is enabled for accounting, every command will result with two commands in the accounting log.
- If TACACS+ is first in the authentication order and a TACACS+ server is reachable, the user will be authenticated for access. If the user is authenticated, the user can access the console and has the rights assigned to the default TACACS+ authenticated user template **config>system>security>user-template tacplus_default**. Unlike RADIUS, TACACS+ does not have fine granularity for authorization to define if the user has only console or FTP access. The 7210 SAS OS supports a default template for all TACACS+ authenticated users.
- If TACACS+ is first in the authentication order and the TACACS+ server is not reachable, the authorization for console access for the user is checked against the user's local or RADIUS profile if configured. If the user is not authorized in the local/RADIUS profile, the user is not allowed to access the box. Note that inconsistencies can arise depending on certain combinations of local, RADIUS and TACACS+ configurations. For example, if the local profile restricts the user to only FTP access, the authentication order is TACACS+ before local, the TACACS+ server is **up** and the TACACS+ default user template allows console access, an authenticated TACACS+ user will be able to log into the console using the default user template because TACACS+ does **not** provide granularity in terms of granting FTP or console access. If the TACACS+ server is **down**, the user will be denied access to the console as the local profile only authorizes FTP access. [39392]
- If a source-address entry is configured for inband RADIUS servers, the source address (IP address) is used as the NAS IP address, otherwise the IP address of the system interface is used.
- In defining RADIUS Vendor Specific Attributes (VSAs), the TiMetra-Default-Action parameter is required even if the TiMetra-Cmd VSA is not used [13449]

TIMING

- On 7210 (except SAS-K platform), NTP time correction can't happen if system time is set to beyond +/- 32 years of NTP time.
- In case of 7210 SAS-D fixed copper port as SyncE reference is supported with port speed as 1 Gbps and Auto negotiation is ON or Limited.
- Ethernet ports that use dual-rate fiber SFPs cannot participate in a Synchronous Ethernet Network.
- Applying the command "debug sync-if-timing" on a second qualified reference has no effect.
- SyncE Reference switch is based on LOS and not based on signal degradation.
- Ethernet ports that use copper SFPs cannot participate in a Synchronous Ethernet Network.
- Standby CPM takes around 10-15 seconds to update sync-if-timing status after CPM switch over. [169225]

SERVICES

- It is NOT recommended to configure MC-LAG without LACP and MC-LAG with LACP on same node, it may take more for traffic to converge in some failure cases. [192846]

- In case of PW switching, mismatch in control-word configured on static segment results in packet corruption. [186952]
- Multicast data packets with ttl=1 are not forwarded in service when MVR is configured. [143559]
- SHG can be configured either in “mvr vpls-service” or “user vpls-service”, but not in both.
- The system accepts packets with sizes exceeding the port MTU by 4 bytes, as listed in below scenario if egress port has proper MTU to transmit these extra bytes.
  - 1522 byte (includes 4 byte FCS) single vlan tagged or 1526 byte (includes 4 byte FCS) double vlan tagged packets received on null sap is forwarded where ingress is null port and egress is dot1q/qinq port.
  - 1526 byte (includes 4 byte FCS) double vlan tagged packet received on dot1q sap is forwarded where ingress port is dot1q and egress is qinq port. [75221]
- A MAC will not age out as long as STP BPDUs from that source are received, although data traffic is not present. [71658]
- When qinq etype (x) is configured on a port and a sap q1.q2 is created, q1.q2 tagged traffic mapped to this sap only if the outer tpid is (x) and inner tpid is 0x8100.If q1.* sap exists on same port then traffic mapped to q1.* sap if the outer tpid is (x).
- All R-VPLS ies interfaces by default chassis mac is assigned, different mac can be configured using CLI “interface <intf-name> mac”. [139425]
- R-VPLS service not supported with *.* Saps. [140881]
- For R-VPLS service, mac address resolved by ARP is also learnt in L2 FDB table; hence ARP ages out upon FDB entry age out.
- In R-VPLS operational IP MTU is set to least of participating SAP’s MTU. SAP MTU is Port MTU – DLC header, wherein DLC header is 14 Bytes for NULL port, 18 Bytes for dot1q port and 22 Bytes for qinq port.[141391]
- A service configured with 'svc-type any" and null-sap to null-sap allows packets up to 1514 including 4 byte FCS if the port MTU is default value of 1514. Workaround is to increase the port MTU from default value of 1514. [116239]
- In VPLS and VLL services, port MTU checks are performed only at the ingress. [92910]
- In case of access-uplink mode SAS-M, T, D, E, an Epipe service, traffic is not switched if the source MAC is a multicast or broadcast address [71437]
- For SAS-E, when a ARP request is received for an address configured for an IP interface in a VPLS service, the first ARP reply is sent to all the SAPs, instead of the SAP on which the request arrived. [94288]
- For SAS-E, MAC address learning rate is slow for certain sized packets. The average learning rate is approximately 200 MAC addresses per second. The learning rate for packets with sizes of 80 and 260 have been determined to be lower than this average. [77067]
- For SAS-E, Layer 4 load balancing for broadcast, multicast and unlearned unicast traffic is not supported. [72425]
- In 7210 SAS-M configured in network mode, temporary data loop around 10-20 msec during revertive mode of 8032. [129307]

- Source BMAC, B-SA learnt in B-VPLS service starts aging only after C-SA associated with B-SA are aged out in case of I-VPLS. In case of PBB-EPIPE, B-SA is not aged out once it is learnt.
- PBB I-tag etype is not configurable, Its value is 0x88e7. PBB B-Tag etype is not configurable Its value is 0x8100
- A set of source MAC addresses are learned on a spoke SDP. If this traffic ceases to come onto this spoke SDP, and if the same traffic (the source MACs) is received on another spoke SDP that is in STP discarding state, then the MACs do not age out. [77996]
- Traffic from a B-VPLS SAP to a I-VPLS SAP matches the p-bit on the B-header instead of the customer dot1p bit when a MAC filter is applied on the B-SAP. [158408]
- For network mode 7210 SAS-M, SAS-T, SAS-X and SAS-R6, processing of ingress BUM traffic on a SAP or spoke-SDP configured in a VPLS service use support egress resources. This results in traffic drops for egress traffic out of the port on which SAPs or Spoke-SDP is configured, if BUM traffic contributes to greater than or equal to 50% of port bandwidth. Depending on the packet size and ingress BUM traffic rate, different amount of drops are observed on different platforms. Contact an ALU representative for more information. This issue is not applicable to 7210 SAS devices configured in Access-uplink mode. [85380, 215022]
- PBB packets with UCA (Use Customer Address) bit set are not forwarded. [113909]
- For epipe service of "svc-sap-type qinq-inner-tag-preserve", the priority of the first tag in the packet egressing will always be 0 unless remarking is enabled.
- For epipe service of "svc-sap-type qinq-inner-tag-preserve", Ingress and Egress IP classification and filter will not work if more than 2 tags are received.
- Traffic that hits a blackhole route in a VPRN Service, would not get accounted under filter statistics. [125527]
- Fragmentation is not supported for IP Packets received on L3 SAP of vprn service [121145]
- When packet is received on a SAP, the service MTU check includes the length of the packet and the SAP delineation encapsulation overhead (that is, 4 bytes for a dot1q tag or 8 bytes for a QinQ SAP). Similarly, when a packet is received on a SDP Binding (also known as PW) is of type vc-vlan, the service MTU check includes the length of the encapsulated packet along with the vc-vlan encapsulation length. If the packet length is greater than the service-mtu, that packet is dropped.
  Note: This limitation is not applicable to 7210 SAS-K. On 7210 SAS-K, service-mtu includes the length of the packet excluding the service delineation. For more information, see the Services User Guide.
- With service-mtu-check disabled, a null SAP allows 4 bytes more than the port MTU for tagged traffic (excluding FCS); a dot1q SAP allows 8 bytes more than the port MTU for tagged traffic (excluding FCS); and a dot1q-star SAP allows 4 bytes more than the port MTU for un-tagged traffic and 8 bytes more than the port MTU for tagged traffic (excluding FCS).
- In case of 7210 SAS-X, max 63 saps can be configured on Hybrid port. [150473]
- SAS-X only - Discard unknown on b-vpls service is not supported. [122038]

STATISTICS

- SAP ingress meters (counters) are incremented for packets dropped by a filter on that SAP. [70878]
- Packets with CRC errors are accounted for in the ingress meter calculations. [80966]
- Packets discarded as the result of a discard unknown-source and discard-unknown configuration are accounted for in the ingress meter calculations. [84842]
- Egress sap statistics not supported for VLAN range SAPS
- On access ports, protocol packets of EFM, LACP, Dot1x, and DWL are counted as part of SAP statistics if NULL SAP, Dot1q Explicit NULL SAP, or Dot1q Default SAP is configured on an access port. [95361]
- Non-routable traffic received on access IP interface not accounted in sap stats. [137643]
- For 7210 SAS-E, for SAPs, if egress filter and egress statistics are enabled together then egress filter counters cannot be used to obtain count of packets matching the egress filter entry. However, egress filter functions appropriately. If the user needs to obtain a count of packets matching the egress filter entry, the egress statistics must be disabled with the no packetsforwarded-count command in the SAP context where the egress filters are in use. [93524]
- For 7210 SAS-E, Accounting records can only count packets or octets at a given time. This is configurable by the user. The configuration is also used to change the behavior for statistics collection.
- For 7210 SAS-E, the monitor service id service-id sap sap-id rate command displays statistics in either packet or octet mode based on the accounting record configured. The utilization rate shows the appropriate values only when operating in octet mode
- TTL=1 and ARP packets are not accounted in a vprn L3 SAP Statistics.
- Packets larger than port MTU are learned and are accounted for by rate limiters. However, they are dropped as expected. [73497]
- Accounting statistics for a spoke SDP in a VPLS service show extra egress packets when the destination to which the traffic stream is being sent is already learned, but actual packets on the wire are correct. The percentage of error depends upon the packet sizes, FDB size, rate of traffic and the duration of the traffic.[81608/94306]
- IGMP packets sent out of a SAP or spoke SDP are not accounted in SAP or spoke SDP egress statistics. If they are received from a peer and forwarded out of a SAP or spoke SDP, they are accounted. [88332]
- Ingress SDP statistics are accounted against the primary spoke SDP, even if traffic is received on other secondary spoke SDP. [93627].
- When continuous traffic is flowing through sap, "Ingress Drop Stats" may not display proper results if sap "statistics ingress counter-mode" is "in-out-profile-count"
- In 7210 SAS-R6, Queue drop statistics on dot1q/qinq L3 VPN sap case, vlan tag length of 4byte is not considered for octet conversion.
- In case of access-uplink mode 7210 SAS-M, SAS-T, SAS-D, egress ACL stats are not working in a null-star service for null Star,0.* sap,:* sap,:0 sap, however ACL functionality works. [122804]
- For 7210 SAS-X, CPU traffic bypasses egress scheduler policies and is not counted in egress queue counters statistics. [105180]

- For 7210 SAS-X, queue rate calculation is frame based. When traffic is egress or ingress out of a queue, the configured queue rate accounts for IFG and preamble of the frame.[103790]
- For 7210 SAS-X, egress queue stats "Octet Count" output may not count network-header bytes in case of network port or dot1q header bytes and in case of null to dot1q sap. [109272]
- In case of 7210 SAS-X BUM traffic received on a sap are accounted in egress queue counts of the source sap. [106158]

STP

- STP BPDUs received on uplink sap hits the unicast meter instead of multi-point meter. [128453]

SYSTEM

- The below mentioned issue and workaround is applicable to SAS-M and SAS-E units manufactured before 15-Dec-2013. For any alarm-box with open-circuit-voltage greater than 12VDC, the ESD/lightning protection circuit inside SAS-M or SAS-E may cause unexpected leakage current on the alarm contacts output. To overcome this design limitation, the customer can add ¼ watt resistors (matching resistor values on the three wires) to limit the leakage current. Depending on the remote device, try these resistor values from high to low in the following sequence: 33K, 22K, 16K, 9.1K, 6.8K, 5.1K and 3.9K.
- It is recommended to shutdown 10 Gig MDA before physically removing it from 7210 SAS-M chassis. If 10 Gig MDA is removed without shutdown in some cases fixed 10 Gig ports 1/1/25 and 1/1/26 flap. [144816]For SAS-D and SAS-T, the Fixed Copper ports cannot operate in 1Gig mode with auto negotiation disabled. [75345, 113818]
- When performed "file dir" on empty drive (cf1 or uf1), shows "MINOR: CLI File Not Found "uf1:"." [178197]
- After reboot for about 15 minutes, card temperature readings are not displayed in 7210 SAS-D.
- OAM DNS lookups do not work correctly unless the full DNS name is provided. [54239, 54689]
- Inserting and removing SFPs in rapid succession causes the "SFP/XFP Checksums do not match" message to be displayed on the CLI session. If this message appears, execute a shutdown command followed by a no shutdown command on the offending port to resolve the issue. [76935]
- BOF password configured by user gets reset in case 7210 rebooted with "boot.tim" version (prior to 4.0) which does not support BOF password. [145037]
- The number of files in the root directory is limited to 100. As a possible workaround, create a directory in the root directory and use that to save/store files. [75227]
- There is currently no show command to display the current values of password hash settings. [32747]
- When the password aging option is enabled, the reference time is the time of the last boot, and not the current time. The password expiry is also reset on every reboot. [64581]

- A port LED may glow if a 1Gig fiber SFP is inserted (without connecting a cable) with 100Mbps speed configured. (Note: 100Mbps mode is not supported for 1Gig Fiber SFPs excepting dual-rate fiber SFPs and copper SFPs). [85620]
- After 497 days, system up-time will wrap around due to the standard RFC 1213 MIB-II 32-bit limit.
- Dual rate SFPs (3HE04116AA and 3HE04117AA) connected to GigE SFP require autonegotiation to be disabled to operate in 1G mode. [78737]
- **default.cfg** is a file name reserved by the system. Do not create a file with this name in the root directory. [76972]
- CLI “file dir” does not start to list when number files are more than 700+ files on flash cf1
- If an ongoing FTP is terminated, the console and Telnet are unresponsive for a duration depending on the size of the file being transferred. [76734, 74294]
- For 7210 SAS-E, the link state of fixed copper ports remain in their current state even after a system reboot is initiated, but traffic is not forwarded. They are initialized during system startup. [76466]
- In case of SAS-E, SAS-M, SAS-X, SAS-T, the user is recommended to protect the out-of-band (OOB) Ethernet management interface to avoid high CPU utilization when high-rate of traffic (For example, High rate of traffic due to DoS attach, high rate of broadcast traffic due to network miss configuration, and so on) is received on that interface. The system does not rate-limit ingress traffic on the OOB port and users should use other mechanisms to achieve this process. Management Access filters can be used to filter traffic destined to CPU. It uses CPU resources and cannot be used to drop high-rate of ingress traffic on the OOB port.
- In case of 7210 SAS-E, SAS-M, SAS-X, SAS-T, It is recommended to shutdown external CF (cf2) or USB (uf1) using CLI “file shutdown <>” before they are physically removed from the system. If removed without shutdown, following error messages may appear. CONSOLE:PLATFORM:UMASS_BBB_Send_Command Bulk Transfer Failed UTC CRITICAL: LOGGER #2002 Base A:PLATFORM:UNUSUAL_ERROR.
- In case of 7210 SAS-M, ports used as "no-service-ports" in bof should not be used in configuration, else execution of configuration file errors out. [120103]
- LED's on vwm-shlef controller turns "Green" when configured shelf-id matches with rotary-id, but sometimes it shows "Amber". Executing “show system vwm-shelf” OR “show system vwm-shelf id” turns LED to "Green" if configured shelf-id matches with rotary-id.
- Quick insert and removal of USB may report flash-device failure, allow 15-30sec settling time to avoid these flash-device-false failure messages.
- When the show service fdb-mac command is executed through the console while the MDA is initializing (and when traffic is coming into the box), a software crash could occur. To avoid this anomaly, wait until the MDA is initialized and the ports are up before issuing the command. [74051]
- The 7210 SAS-R6 BFD sessions created after BFD scaling limit is reached are not coming up even if existing active BFD sessions are deleted, workaround is to shutdown/no shutdown BFD. [181225]

KNOWN ISSUES

The following are specific technical issues and limitations that exist in Release 7.0R11 of 7210 SAS devices. The topics are arranged alphabetically.

NOTE:

- Issues marked as MI might have had a minor impact but did not disturb network traffic.
- Issues marked as MA might have had a major impact on the network and might have disturbed traffic.
- Issues marked as CR were critical and might have had a significant amount of impact on the network.

ACLs

- Egress filter counter does not increment for action drop on SAS-R6 IMMv2, however filter functionality works fine. [190140-MI]
- IPv4 or IPv6 ingress ACL configured on network interface filters matching MPLS encapsulated IPv4 or IPv6 service traffic. [199826-MI]
- For 7210 SAS-E, egress Packets not be dropped when IP filter is configured on QinQ Uplink SAP with QinQ etype is configured to non default values on the port. [112881]
- In 7210 SAS-E, egress Ip/Mac filters action not work on 0.* SAP for Epipe and Vpls service. [114263]
- For 7210 SAS-E, ingress and egress filters do not block STP packets when STP is enabled in a service. [75921]
- For 7210 SAS-E, a **mgmt-access-filter** with a **deny-host-unreachable** action sends “Destination Net Unreachable” instead. [73676]
- For 7210 SAS-E, an egress filter applied to drop all traffic on a port also drops EFM loopback traffic. [82782]
- If dot1q and * sap created on same port but belonging to different services, traffic matching dot1q sap hits the ingress filter attached to * sap only if no ingress filter attached to dot1q sap. This issue happens in network mode 7210 SAS-M, X, T and R6. [109037-MA].
- When Q1.Q2 and Q1.* sap are configured on the same port, traffic sent with Q1.Q2 tag hits ingress filter attached to Q1.* sap. This issue happens in network mode 7210 SAS-M, X, T and R6. [109133-MA]
- For 7210 SAS-E, an IP filter applied at SAP ingress to filter IGMP packets does not work.

CLI

- During 7210 SAS-R6 boot, while editing the bof params line “or Type 'auto' to retrieve BOF configuration through DHCP” appears. Auto option is not supported in 7210 SAS-R6 and Auto option should not be used, if used it may create boot loop. [213627-MI]
- Following are some of the known issues with CLI Rollback on 7210 SAS-R6:
  - ERROR seen while doing Rollback revert for a management access filter. [188689]
  - Rollback failed for maximum routes in VPRN. [187417]
- There are some unsupported CLI and CLI options displayed in the CLI command set.

- Some of the show, monitor, and tools CLI command output displays unsupported fields and modules.
- The output of the **tools dump** command is not aligned properly when issued from a Telnet session. [76876-MI]
- The 7210 SAS-R6 does not support BGP RR functionality, though the CLI is available.
- 7210 SAS-X, CLI "monitor port" output is not 100% accurate all time. [110978-MI]

CES

- Commands executed quickly after provisioning a T1/E1 MDA would get delayed response due to the MDA initialization (given that the commands needed IOM/MDA routines to be called such as **show port**). [94277-MI]
- SAP ingress statistics in a CPIPE service does not increment when LOS is reported on a DS1/E1 port. [98828-MI]
- Provisioning m24-100fx-1gb-sfp MDA (which is pre-provisioned as MDA1) on MDA2 can lead to undesired behavior especially when a CES card is installed in the MDA 2 slot. [97786-MI]
- TDM ports cannot participate in a split horizon group (although it is user configurable). It is not a supported feature. [101695-MI]

IGMP SNOOPING

- In an IGMP snooping enabled VPLS service, if the IP interface is removed and added back, multicast traffic between spoke SDPs may not resume towards one or more spokes. The spoke SDPs mentioned here are configured for the M-router port. The work-around is to remove the static M-router configuration and add it back; or execute a shutdown command and a no shutdown command of the spoke SDPs. [91856-MI]
- In a scaled setup with spoke SDPs configured as M-router port multicast traffic for some services is not forwarded over some spokes when the LAG flaps. Remove and reconfigure the M-router port for the spoke SDP restores the traffic. [97851-MI]
- In 7210 SAS-E, when more than 2047 (S,G) joins are received in a scaled setup, it might result in hash collisions in the multicast forwarding. In such cases, learned groups can be removed/added back, with messages appearing on the console. (95345)
- On an IGMP snooping-enabled VPLS service, the 7210 SAS-E does not support multicast forwarding statistics. The **show service id** *service-id* **mfib** statistics command output will always show zero value counters. [81173]

IP

- For RVPLS IP forwarding ARP is closely bound to FDB entry, ARP entry will be removed if MAC in FDB ages out. Traffic will not be forwarded till ARP resolved. To avoid traffic loss it is recommended to configure FDB timeout be greater than or equal to ARP timeout. This issue is not applicable for 7210 SAS-K. [190982-MI]
- SNMP query of the vRtrActiveArpEntries object does not return the correct value. The CLI reports the correct number of ARP entries. [80788-MI]
- 7210 SAS-E does not support secondary IP interfaces. However, these are configurable through SNMP, and should be avoided. [76848].

- When ARP is cleared, few packets from a single flow IP traffic gets load balanced in case ECMP is enabled. [156758-MI]
- With ECMP enabled, mac-ping and eth-cfm loopback test fails for LDP based SDP bindings. [161380-MI]
- 7210 SAS does not support Sub Second hello timer for VRRP
- In SAS-T and SAS-R6 with IMMv1, if IPv4/UDP or IPv6/UDP packets with UDP destination port value equal to 3784 and IP TTL value NOT equal to 255 or 1, that are received on any L2 service or L3 interface are not forwarded. [184471-MA]
- In 7210 SAS-R6, directly connected active routes take considerable amount of time to come up. [171954-MI]
- In 7210 SAS-R6, reducing the interval/timeout timers much below default values is not recommended for OSPF, IS-IS, BGP, LDP and RSVP to ensure stability under transitional events like a CFM switchover. [56792, 58891-MI]

LAG

- For 7210 SAS-K, it is recommended to have max of 2 LAG and 2 ports in Uplink LAG even though CLI allows to configure. [207440-MI, 207653-MI]
- LAG mode change from access to uplink or uplink to access is not supported when ports are associated to LAG group. CLI does not throw error, but can lead to system issues [207736-MI, 206954-MI]
- With LSP over lag, traffic is sent out on a port added to the LAG sub-group which is in stand-by mode, workaround is to shut/no shut of LAG. [159334-MI]
- If in a two-port LAG containing two sub-groups with one port each, a **shutdown** on the port belonging to the active sub-group will flap the LAG. This happens only if the LAG is associated with an IP interface. [85967-MI]

MANAGEMENT

- SNMP walk of vRtrConfEntry shows the vpls-management and management instance as active even though these are not currently supported. [76832-MI]
- SNMP query of the following operational rates does not return the correct values. The value returned is 0. CLI reports correct operational values. [76853-MI].
  - tAccessEgressQueueOperPIR
  - tAccessEgressQueueOperCIR.
- If a source-address is configured for NTP, and if the system is rebooted with an older time set (using **admin set-time**), NTP takes a few iterations to synchronize for the first time. [86897-MI]
- The CLI allows the user to specify a TFTP location for the destination for the **admin save** and **admin debug-save** commands which will overwrite any existing file of the specified name. [18554-MI]
- The 7210 SAS does not support storing more than 500 events for log destinations memory and SNMP. Although, the CLI and MIB allows up to 1024 to be configured, it is recommended not to exceed 500.

- SNTP broadcast packets are not processed when they are received with an all-ones address. They are processed if they are received with sub-net broadcast address. [73662]
- LACP flaps when starting an SSH server (no shutdown of SSH server). [75648]
- If there are NTP broadcast client configurations over the **management** routing-instance, and if the out of band eth-management port is disabled, on configuring an NTP server and removing it will remove the broadcast client configurations as well. [101255-MI]

MPLS

- For 7210-R6, packet drops are observed in VPLS/VPRN service when traffic switched over to MBB path. [178203-MA]
- In case of 7210 SAS-R6, FRR timings are greater than 50ms when saps are also configured on a hybrid port. [178443-MA].
- In case of 7210 SAS-R6, modifying the LDP hello timers while the hello adjacency is up does not come into effect, until the adjacency bounces. However, after two High Availability switchovers, the active CPM or CFM starts using the new timer value. [112617-MI]
- Tools perform router MPLS CSPF command does not accept SRLG group name having alpha characters [155853-MI]
- Tools perform router MPLS command does not work for SRLG group names having numeric character length of more than 10. [156220-MI]
- The **show router rsvp interface** *interface-name* **detail** command displays incorrect Auth Rx Seq Num and Auth Tx Seq Num values. [86903-MI]

MIRROR

- 7210 SAS-R6, egress mirror also mirrors ingress ip multicast data packets. This issue exists with SAS-R6 IMMv1 only. [189812-MI]
- Ingress QoS policies applied for forwarded traffic will also be reflected on its mirrored traffic, if mirror destination is a null SAP. [73951-MI]
- Log events are not generated for mirror application. [72100]

OAM

- In case of SAS-K, Broadcast/multicast traffic dropped on VPLS service where Mac Swap with loopback is enabled. [202211-MI]
- 7210 SAS-K, packets generated by testhead OAM tool are sent in the service even if it does not match the ethertype configured on the port on which the test SAP is configured. [195790-MI]
- On SAS-R6, Epipe MIPS require resource to be configured for "down-mep" and "up-mep" under "configure system resorce-profile". [202895-MI]
- In case of UP MEP, until peer MAC is learnt in VPLS service all CFM packets are sent with dot1p value "0".[201342-MI]
- 7210 SAS-R6 UP MEP CCM messages are sent with dot1p 0 in VPLS service when UP MEPs are configured on SAPs and egress is SAP. [201177-MI]
- 7210 SAS-K, CFM 1-DM test results are not proper. [199552-MI]

- 7210 SAS-K, CFM 2-DM tests fails to work when we configure disable-learning in a VPLS service. [198054-MI]
- 7210 SAS-K, CFM CCM packets not processed when the received CCM packet does not have End TLV. [195613-MI]
- Y.1731 version-1 DM request packets received on Down MEPs are not processed in case of SAS-M. This works on Up MEPs. [200963-MI]
- In case of 7210 SAS-D, recommended minimum value for EFM OAM timers is tx-interval of 500ms and a multiplier of 4. Even though CLI allows for lesser values, it is not supported -MI.
- EFM-OAM sessions flap under the following conditions in case of 7210 SAS-D and 7210 SAS-E:
  - Using timers less than the default values,
  - STP packets that need to be forwarded in the slow-path (CPU-based forwarding) are incoming at a rate >64kbps, and
  - The CPU utilization is > 80% [76129-MA]
- ICMP pings with higher packet sizes sent at higher rates will fail. [77611-MI]
- The "vlan 0" for CLI "*configure>eth-cfm domain < > association < > bridge-identifier < >*" is not supported. [169536-MI]
- Eth-CFM convergence fails; when llf is enabled on the LAG SAP and Lag shut and no-shut is done, or box is admin saved and rebooted. **Workaround**: Remove and add back MEPs. [116513-MA]
- The ETH-CFM defect is not reported on booting the 7210 SAS with a configuration that has the ETH-CFM session over a LAG with no member ports. [100813-MI]
- It is not recommended to use fault-propagation when the service entities (for example, SAP and SDP binding) are configured on a LAG. A LAG flap can result in CFM defect being raised which in turn results in a false fault propagation event. This issue is seen only when CCM timers of less than 10 seconds are in use. This configuration is not blocked in CLI but it is highly recommended that users do not use fault propagation with LAG when using CCM timers of less than 10 seconds. [150233-MA]
- On 7210 SAS-D and SAS-T, on a given SAP in any service, in order to use Y.1731 2-DM, it is recommended to configure only one Y.1731 MEP, or configure MAC Address for each MEP created on the same SAP otherwise, 2-DM may not work properly. Except 2-DM, other functionalities are not affected even if there are multiple MEP's. [118015-MI]
- For EFM OAM with timers less than the default values can result in EFM flaps due to events such as STP topology change, clearing FDB, or adding and removing ports to a LAG. It is recommended to use the default timers, tx-interval=10 and multiplier=5 or above. [81218, 82228-MI]
- For 7210 SAS-E, under a heavy load condition, CFM/EFM/LACP/Eth-ring may flap due to any of the following triggers [74223, 106782]:
  - Executing a **clear fdb** or a **show fdb** command.
  - Transferring large files using FTP onto the flash.
  - Mac moves occur at a rate of approximately 40 macs/sec.

- For 7210 SAS-E, CFM packets generated from the CPU are assigned to FC BE. Hence, there may be CFM flaps if the egress BE queue is congested.
- On PBB Epipe SAP, if the UP MEP is configured, it is recommended to enable CCM, with CCM disabled loopback, linktrace, DM, and SLM tests fails. [136751-MI]
- For QinQ saps (q1.q2, q.* and 0.*), dot1ag loopback reply messages (LBR) will take the priority from configuration field ccm-ltm-priority (config=>service=>vpls=>sap=>eth-cfm=>mep=>ccm-ltm-priority) instead of using the priority of corresponding Loopback message (LBM) received. Note that this is applicable only when box is in 7210 SAS-M access-uplink mode. For network mode, LBR will have same priority as corresponding LBM. [109767-MI]
- When FRR with facility backup kicks in and the merge point is the LSR with implicit null is 1 hop away, lsp-ping/trace does not work. [108025-MI]
- ETH-CFM Down MEP session on standby pseudowire does not come up in a VLL/VPLS pseudowire redundancy configuration. In case of standby becomes active ETH-CFM session comes up. [100594, 148081 -MI]
- LSP-trace fails over bypass tunnel when the LER is the PLR in FRR Facility backup configuration. [109165-MI]
- In case of 7210 SAS-R6, by default dot1p bit set as "0" for up mep packets (ccm,lt,lb,2dm,2slm,1dm, eth-test) when they are egressing on sap. Workaround is to configure remark policy at sap egress. [183978-MI]
- OAM "lsp-ping and trace" fails for ACH type "none" when configured on unnumbered-mpls-tp interfaces with "multicast/broadcast" static-arp. [180659-MI]
- For **mac-ping** and **mac-trace** when used with the **fc** and **return-control** options, do not use the egress queue as specified by the **fc** option. [82306-MI]
- In case of 7210 SAS-T, the Y.1564 testhead, when configured to use internal-loopback-ports, latency will not be computed when frame size is greater than 9000 bytes. Same test works fine with front panel port used as loopback ports. [177164-MI]
- For 7210 SAS-X, when port loopback with MAC swap is used, packets received on the test SAP (after going the test SAP loop) do not use SAP ingress queues. Only SAP ingress meters are used.
- Using **mac-populate** and **mac-purge** simultaneously on several VPLS services (for example, 64) could result in instability of the router. To avoid this anomaly, it is recommended to carry out this operation per VPLS service. [79690-MI]
- The timestamps are all 0s when **cpe-ping** is performed with SAA. [81726-MI]

QoS

- In 7210 SAS-R6 RVPLS service the L2 unicast traffic is taking port based remarking, where as it is supposed to take sap-based remarking. [203154-MI]
- In 7210 SAS-R6, if a LAG has more than 1 port from the same IMM then while attaching a queue-policy to the primary-port make sure the ‘total CBS under that policy multiplied by the no. of ports in the lag’ doesn’t exceed max CBS value(140MB) available CBS value (140- MMU Configured CBS). [202780-MI]
- 7210 SAS-K, fragmented packets may be received upon changing the autoneg capability of remote device from 100Mbps to 1Gbps. [197188-MI]

- 7210 SAS-K, traffic having mixed frame sizes and also for Jumbo frames deviation in shaper rates may be seen. [193169/195681-MI]
- 7210 SAS-K, classification based on inner Dot1p is not supported, though the CLI command match-inner-dot1p is available.
- 7210 SAS-K, a max of 200 queues for Ingress and 200 queues for Egress are supported. Allocations available in tools dump system-resources. The software does not enforce this check. It is not recommended to exceed this number at anytime.
- 7210 SAS-K, frame based accounting feature is not supported even though CLI command is available. [190211-MI]
- 7210 SAS-K, configuring Egress Rate less than 10Kbits/sec is not supported. [196558-MI]
- 7210 SAS-K, Max MBS for Queue supported is up to 11.5 MB even though configuration is available from CLI. [198927-MI]
- 7210 SAS-T network mode Dot1p remarking is not working for traffic ingressing I-SAP and egressing out of PBB B-SAP. [182552-MI]
- Ingress qos resources are not getting freed up when the ingress qos policy is removed from the SAP with tod-suite configured. [141896-MI]
- The maximum entry-id value for the IP/MAC-criteria in the SAP ingress policy context is restricted to 63 although the CLI allows up to 64. Entry-id 64 should not be specified. [76790/76964-MI]
- When remarking is enabled on access egress for a Dot1q port, the Dot1p bits in the outer customer tag get remarked when the traffic is sent out of a Dot1q default SAP. Similarly, when remaking is enabled on access egress of NULL encap port, Dot1q bits in the outer customer tag get remarked when traffic is sent out of a NULL SAP. The workaround: In the case of a NULL SAP, remarking can be disabled to preserve the Dot1p bits. [86818-MI]. This is not applicable to 7210 SAS-K.
- 7210 SAS-M in "access-uplink" mode, by modifying the ethernet mode of 10Gport from "access uplink" to "access" and back to "access uplink", default shaper on 10G port gets configured to 1Gig. After this operation 10G port egress only 1Gig traffic.
  Workaround: Apply and removal of non-default "network-queue" qos policy to 10G port corrects the issue, "configure port <port-no> ethernet access uplink queue-policy <name>". [151008-MI]
- When mac-criteria dot1p-only is used as the classification criteria for a B-SAP and when resources are allocated from an IPv4 or IPv6 TCAM slice, the unlearnt traffic from B-SAP to I-SAP hits the multicast meter even if an unknown meter is configured for that FC in the policy. This issue does not occur if the TCAM slice is of type MAC. [152477-MI]
- The slope policy attached to a hybrid port under the access-egress context will be ignored as it is unsupported. [161469-MI]
- L2PT tunneled STP packets do not have the appropriate MPLS EXP bits set. They are set to zero. [90580-MI]

- In case of 7210 SAS-R6, in rare occasions queue buffers not released during below operations while traffic flowing over SAP or network port, this can result in configuration failures and console messages.
  - attaching user defined queue policy
  - modification of queue scheduler mode, cbs, mbs values
  - port down
  - LAG port removal
  - SAP delete

  It is recommended to carry out the above configuration changes after stopping traffic.

  The configuration failures can be re-covered by rebooting line card.

  In case of SAP delete, it is recommended to shutdown SAP before deletion. [168529-MI]
- In case of 7210 SAS-T, during heavy congestion in the system such that shared buffers are utilized completely and schedular mode is strict, line rate traffic may not be achieved for all sizes of packet. [164543]
- In 7210 SAS-T access-uplink mode, inner tag dot1p not getting remarked when egress is qinq sap and ingress is dot1q sap. [163616]
- telnet, ftp, ssh, radius, and tacplus are egressing on NC queue. [162022-MI]
- In 7210 SAS-X, it is not recommended to oversubscribe the 1.3GB buffer using ingress or egress queues. Oversubscription can result in traffic loss whenever new queues (ingress or egress) are created in HW due to events like enabling ingress queues on a SAP, adding a new link to a LAG SAP. [132888-MI]
- Ingress queue configurations is not supported through TOD. [149711, 149712-MI]
- In 7210 SAS-X, when scheduler-mode of the port is changed from sap-based to fc-based or vice versa, the traffic on the port may be disrupted for 2-3 seconds. [111643-MI]
- In 7210 SAS-X, when port scheduler mode is "fc-based" and multiple SAPs are configured on that port, and when one of the SAP consumes high bandwidth either due to queues to CIR levels, PIR weight, or CIR rate, remaining PIR traffic among rest of the SAPs having default SAP egress qos policy may not be fairly distributed. [107446-MI]
- In 7210 SAS-X, when egress rate command is used on network port, queues are not getting the expected rate for the following conditions:
  - When traffic flows from null sap to out of network port.
  - When queue rate is close to ERL rate.

  [109689-MI] [111255-MI]
- In 7210 SAS-X, during configuration oversubscription of queue CIR may result in undesirable behavior of shaper and scheduler. Oversubscription of CIR is not recommended. [101715-MI]
- The actual traffic rate may fluctuate from the configured CIR and PIR for the queue. The average rate is as per the operational rate but the rate may fluctuate around +/- 55-60kbps from the configured rate. [102303-MI]
- When the multiple queues have traffic flowing and the queues having same cir-level have very less pir bandwidth to share among them or when pir-weight ratio is very high for the

queues under same cir-level, it is seen that traffic is not shared among same cir-level queues as per the configured pir-weight for the queues.

- Under a network port policy with Dot1p classification, traffic for classifiers with **out-profile** will be momentarily marked **in-profile** when some other classifier with profile **in** is changed to **out**. [85482-MI]
- In 7210 SAS-E, if a port on which egress-rate port limiting is enabled and is mirrored on the egress, then for packets less than 768 bytes, the rate of traffic seen on the mirror destination port is not the same as that on the mirrored source port. [83168]
- In 7210 SAS-E, when the queue on egress is within the CBS limit, the allocation of buffers is purely based on packet arrival time regardless of the packet's in-profile or out-profile state. This can sometimes cause unequal distribution of queue's CIR/PIR to the various ingressing traffic using the same queue. As a workaround, configure an aggressive slope policy for yellow packets. [74730]

TIMING

- In case of 7210 SAS-T, PTP hybrid mode with BC is deployed in a topology where a 2-way master/slave relationship exists, if master's time information changes drastically during reboot or initialization then sometimes few of them not to lock to the PTP master. This issue is not observed if all nodes in topology are 7210 nodes. Workaround for this issue is enable PTP only after its master is stabilized or reboot the nodes in a staged manner. [220749-MI]
- In case of 7210 SAS-T, PTP hybrid mode is configured, PTP shut/no shut can result in 1-PPS frequency not proper. A node reboot will resolve this issue. [220367-MA]
- 7210 SAS-R6, when a switch over from active to standby CPM is triggered, PTP on new active CPM takes about 40 minutes to go to a stable, locked state. The downstream slaves using this SAS-R6 observe a similar performance behavior. [210553, 201629-MA]
- "IEEE 1588/PTP Clock Recovery Event Statistics" of CLI "show system PTP statistics" gets reset after PTP shut/no shut. [150062-MI]
- With PTP configured, it is not recommended to remove system IP, this can result in PTP flaps. If system IP is shutdown when PTP uses system IP as source, the PTP sessions continue to use the system IP. [143255-MI]
- For 7210 SAS-X, when 1588 PTP slaves connected to upstream SASX as a 1588 BC, "Packet Loss" counter on slave increments every two minutes for CLI "show system ptp statistics". This does not affect frequency or time recovery. [147821-MI]
- For 7210 SAS-X, system deriving clock from 10 gig port with XFP (3HE00566CAAA01) does not move to holdover state when the master Dut is admin rebooted. Power cycle of the master Dut works fine. [105269-MA]
- For 7210 SAS-X, syncE not supported on the following SFP's.
  - Dual Rate SFP's: 3HE04116AA and 3HE04117AA
  - Fast Ethernet SFP's: 3HE00869AB, 3HE01454AAAA02 and 3HE00024AAAA02

SERVICES

- Eth-Ring switch over times are greater than 50ms with link failure which is farthest from the RPL node and more than 20 services protected by Eth ring. [187004-MI]

- 7210 SAS-K, maximum 4 Access-Uplink ports are supported on the node, even though CLI allows configuration of 5 access-uplink ports.
- In 7210 SAS-R6, STP state of saps on root bridge are incorrect after Clear Card and SWO in succession. [172199-MI]
- Dot1p priority is not preserved for RSTP packets forwarded by the node (for example doubly tagged STP packets received on a SAP). The dot1p is remarked to 7. Additionally, these packets are not matched against egress filter policies. [71855/75921-MI]
- When a time-range is expected to be active, a delay of up to 8 seconds can be expected for an associated filter policy on either ingress or egress. [161652-MI]
- Changing the **fdb-table-size** on multiple services simultaneously (for example, by a script) may affect MAC learning in some services. [82362-MI]
- There may be a small amount of traffic flow between services when LSPs are removed and added back within a very short duration, or when the LSPs are cleared under a given SDP. [84963-MI]
- On same Hybrid port if FRR for LSP and G8032 for SAP is configured, traffic switch over times observed for FRR and G8032 protected entities are high.[162771-MA]
- In case of PBB BCB (B-SAP to BSAP) packet, C-SA (customer mac) is learned in ivpls service when ivpls, isid matches transit packet's id.

  Note: a small amount of C-SA (up to a maximum of few hundreds) are learnt and not all C-SA are learnt. [129525-MI]
- When SAS is configured as PE, in igmp enabled vpls service if spoke sdp is blocked due to reception of standby bit from connected MTU and then moves to forwarding statel There would be multicast data traffic loss till the next set of query/report is received. [121470-MI]
- PBB-packets received on B-SAP forwarded to epipe SAP if B-SA MAC matches "backbone-dest-mac" configured in pbb-epipe service. Packets with other B-SA MAC are dropped. [113910-MI]
- For SDP configured with vc-type vlan and "no vlan-vc-tag", tag value is carried as 0. In case vlan-vc-tag is configured, the proper tag is carried. [162708]
- In case of 7210 SAS-R6, service with L2PT/BPDU translation enabled, when CPM switchover happens, no xStp packets get translated in 4 seconds. Due to which xSTP flaps and a loop is created. [171060-MI]

STATISTICS/AC COUNTING

- In case of SAS-R6 IMMv2, if terminated MPLS service packets has broadcast or multicast dest mac, then port ingress stats packet count does not increment. [201634-MI]
- In 7210 SAS-D and 7210 SAS-E, when * sap and other encap saps exist on same port, if egress statistics enabled on * sap and egress statistics disabled on the other saps, other saps egress packets are counted as part of * sap egress statistics. Similar behavior is observed with *.* or 0.* saps. [127452-MI]
- Attaching accounting-policy on SAS-D L2 Uplink SAP is not supported and should not be configured, however, CLI commands exists. [111897-MI]

STP

- If a large number of MAC addresses exists in the VPLS FDB and the entire FDB is flushed and relearned, there may be a period of when RSTP BPDUs are not sent. A partial workaround is to configure fdb-table-size limits. [40532-MI]
- For 7210 SAS-E, if an ingress CPU forwarded RSTP/L2PT/PVST packet rate exceeds 64kbps, RSTP flaps. On 7210 SAS-M, if an ingress CPU forwarded RSTP/L2PT/PVST packet rate exceeds 128kbps on access, or 200kbps on network port, RSTP may flap. [73189]
- If 7210 SAS-Ms are connected in a ring topology with LAG configuration and FRR, when ring is broken, STP flaps for some service is observed. [95969-MI]
- RSTP convergence fails if **force-vlan-vc** is enabled on a mesh SDP. [94928-MA]

SYSTEM

- 7210 SAS-K, booting through port 3 is supported in fiber mode (SFP) only. [202510-MI]
- 7210 SAS-K, 100FX SFPs are not supported.
- 7210 SAS-K, Copper SFP is supported only in 1Gig mode in port 1 and 2.
- 7210 SAS-K, Copper SFP is not supported on port 3.
- In 7210 SAS-D, if port is not shut before loopback is configured, speed is always set to auto negotiated speed. If port is shut before loopback then speed set to 1Gbps. [114904-MI]
- 7210 SAS-D, sometimes "[iomMsg-1]soc_phyctrl_loopback_set: u=0 p=3 TIMEOUT" console message appears when port internal loopback is enabled/disabled on Copper SFP port. [115784-MI]
- 7210 SAS-D, snmpwalk reports redundant power-supply status. [113827-MI]
- In certain scenarios, traffic drops are seen during source learning when copper ports are operating in half duplex modes. Once learned, there are no other observed drops. [75875-MI]
- The system time MIB object stiDateAndTime is the UTC time and should not include the time zone offset in SNMP **get** and **set** requests. [66553-MI]
- During auto-config, if a DHCP relay packet for an unrelated DHCP session is received by the system, the system may be non-responsive. [76811-MI].
- When using 100FX SFPs, autonegotiation should be disabled. [99132-MI]
- The system saves core dumps at the URL specified in the BOF, while coming up. Specifying a remote location as a core file destination has two issues.
  - If a remote URL is specified, and if the uplinkA cannot be brought up, saving the core dump may not succeed, even if uplinkB is up.
  - If uplinkA's BOF is configured to use DHCP, the IP address acquired by DHCP is not released by the system after saving the core file.

  Thus, it is recommended to configure the core file destination to be the local flash (cf1). [76764, 76736-MI].
- Internal loopback of port does not work when loopbacked port speed is set to 100Mb and autoneg is turned off. [113995-MI]
- In certain scenarios (such as Cu SFP connected to Fixed Cu), the show port command does not display the MDI/MDX value as expected. Functionality is not affected. [76765-MI]

- For dual rate fiber SFPs to operate successfully, both sides should be configured with the correct speeds. [82194-MI]
- During auto-config, if a DHCP relay packet for an unrelated DHCP session is received by the system, the system may be non-responsive. [76811].
- In case 7210 SAS-E, M, D, applying large router policy configurations (2000 to 3000+ lines) at one time, can cause protocols such as LACP, EFM, to flap. [83787]
- The statistics and the utilization rate displayed by the **monitor port rate** CLI command for a given time interval does not match the actual count and rate received by the system in that time interval. [83757]
- During AutoInit using DHCP, it is recommended to store proper bof, config files in defined location. In lab scenario, it is observed that, through DHCP if 7210 SAS fetches the ip address, but bof or config file is not stored in defined location, after several DHCP request or replies, DHCP starts failing. A reboot of 7210 SAS is required to recover from DHCP failures. [131915]
- Control protocols may flap when the **file copy** command is initiated, using FTP, from the system if the specified FTP server is not reachable. This happens under loaded CPU conditions. Before initiating the **file copy** command using FTP, verify that the FTP server is reachable. [76566].
- In a scaled configuration with STP enabled, when on an event (such as a network LAG flap) causes an enormous amount of traps sent out of the 7210, STP may flap. [95969-MI]
- 10Gig alarms, “no-frame-lock” and “high-ber”, are not supported on the 7210 although they are configurable.
- The **configure port** *port-id* **ethernet report-alarm** command option **no-frame-lock** or **high-ber** are allowed to be configured but they are not supported. This command is applicable only for 10G ports.
- In loaded CPU conditions and scaled configurations, CPU spikes may cause STP to flap. This was seen in one condition when CPU spiked due to link down event and was processing 16K OSPF routes. [84889-MA]
- In loaded CPU conditions and scaled configurations, CPU spikes may cause LAGs to flap. This was seen under the following events:
  - Addition and deletion of an OSPF interface in non-backbone area. [84537-MI]
  - Addition and deletion of port (or LAG port) to ip-interface. [84165/86007-MI]
  - Enabling an SSH server. [84166-MI]
    The workaround or to lessen the chances of flaps occurring in this case, it is suggested to enable the **preserve-key** option before enabling SSH.

HARDWARE

- Only one port LEDs is used to indicate port status and link activity. If the LED is lit steady, it indicates link up. If the LED is blinking, it indicates link activity.