Release Notes for StarOS™ Software Version 21.6.6

First Published: May 21,2018
Last Updated: May 21, 2018

Introduction

These Release Notes identify changes and issues related to this software release. This emergency release is based on release 21.6.5 These release notes are applicable to the ASR 5500, VPC-SI and VPC-DI platforms.

Release Package Version Information

Software Packages	Version
StarOS packages	21.6.6 build 69648

Descriptions for the various packages provided with this release are located in Release Package Descriptions.

Feature and Behavior Changes

The following features and/or behavior changes have been introduced in this emergency release.

Refer to the *Release Change Reference* for a complete list of feature and behavior changes associated with the software release on which this emergency release is based.

S2B Handover Behavior

CSCvj35194

Applicable Products(s) or Functional Area: P-GW and SAE-GW

Feature Default: Disabled – Configuration Required

Feature Changes

When P-GW receives an S2B handover session request for an existing APN with a different PAA (IP Address), the existing session is cleared and a new session is either accepted or rejected, based on the operator configuration. The S2B handover behavior is CLI controlled.

Note:

- When the CLI is enabled, an existing LTE/S2B session is released only if:
    - There are no dedicated bearers present
    - It is a non-eMPS session

    - It is a non-emergency session

- All sessions are released for a given APN with multiple PDN connections.
- For an IMS PDN when CLI is enabled and configured as “allow” then existing call is released with no cause code specified in Delete Bearer Request.

Command Changes

egtp s2b-ho-paa-mismatch

To configure the S2B handover behavior at P-GW when there is a PAA mismatch for a given APN, a new keyword **s2b-ho-paa-mismatch** is added to the **egtp** command in the P-GW Service Configuration mode.

When enabled, the configuration is applicable to all APNs. However, the operator must explicitly configure for an IMS APN.

Use the following configuration to handle S2B handover scenario:

configure

context context_name

pgw-service service_name

egtp s2b-ho-paa-mismatch {allow | reject} [ims-only]

no egtp s2b-ho-paa-mismatch

end

NOTES:

- By default, the above configuration is disabled.
- **no**: Disables the S2B handover configuration.
- **allow**: Accepts a new call after clearing the existing LTE/S2B session when the P-GW receives an S2B handover request with a different PAA for the same APN.
- **reject**: Rejects a new call after clearing the existing LTE/S2B session when the P-GW receives an S2B handover request with a different PAA for the same APN.
- **ims-only**: Enables this behavior only for **ims-only** APN.

Performance Indicator Changes

This section provides information regarding show commands and/or their outputs in support of this feature.

show pgw-service all

The output of this command includes the following field:

- S2b HO PAA Mismatch Action

show session subsystem facility sessmgr instance <*instance_number*>

The output of this command includes the following fields:

- 3 GTP-To-S2b HO PAA Mismatch found
- 1 GTP-To-S2b HO PAA Mismatch accepted
- 1 GTP-To-S2b HO PAA Mismatch rejected
- 1 GTP-To-S2b HO PAA Mismatch bypass
- 0 GTP-To-S2b HO PAA Mismatch ho-in-progress
- 4 S2b-To-S2b HO PAA Mismatch found
- 2 S2b-To-S2b HO PAA Mismatch accepted
- 1 S2b-To-S2b HO PAA Mismatch rejected
- 1 S2b-To-S2b HO PAA Mismatch bypass

Related Documentation

For a complete list of documentation available for this release, go to http://www.cisco.com/c/en/us/support/wireless/asr-5000-series/products-installation-and-configuration-guides-list.html.

Installation and Upgrade Notes

This Release Note does not contain installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

Firmware Updates

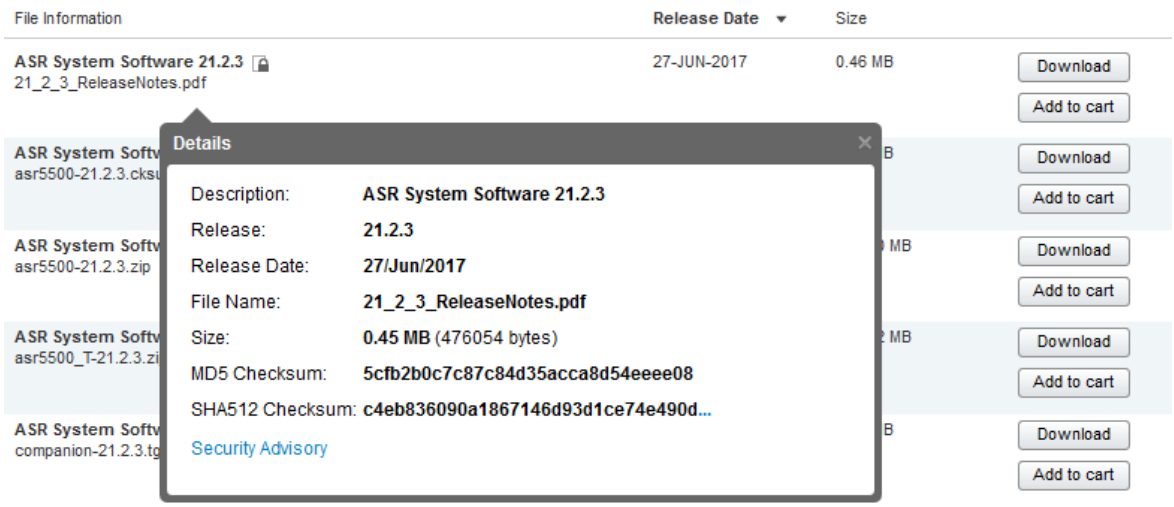
There are no firmware upgrades required for this release.

Software Integrity Verification

To verify the integrity of the software image you have from Cisco, you can validate the SHA512 checksum information against the checksum identified by Cisco for the software.

Image checksum information is available through the following mechanisms:

- **Cisco.com Software Download Details:** To find the checksum, hover the mouse pointer over the software image you have downloaded.



At the bottom you find the SHA512 checksum, if you do not see the whole checksum you can expand it by pressing the "..." at the end.

- **.cksums file:** A file containing software image checksum information is distributed with the image files. The naming convention for this file is:

  <product>-<version>.cksums

  Example: asr5500-21.4.0.cksums

To validate the information, calculate a SHA512 checksum using the information in Table 1 and verify that it matches either the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop please see the table below.

Table 1 – Checksum Calculations per Operating System

Operating System	SHA512 checksum calculation command examples
Microsoft Windows	Open a command line window and type the following command > certutil.exe -hashfile *<filename>.<extension>* SHA512
Apple MAC	Open a terminal window and type the following command $ shasum -a 512 *<filename>.<extension>*

Linux	Open a terminal window and type the following command
	
	$ sha512sum *<filename>.<extension>*
	
	Or
	
	$ shasum -a 512 *<filename>.<extension>*

NOTES: *<filename>* is the name of the file. *<extension>* is the file extension (e.g. .zip or .tgz).	

If the SHA512 checksum matches, you can be sure that no one has tampered with the software image or the image has not been corrupted during download.

If the SHA512 checksum does not match, we advise you to not attempt upgrading any systems with the corrupted software image. Download the software again and verify the SHA512 checksum again. If there is a constant mismatch, please open a case with the Cisco Technical Assistance Center.

Certificate Validation

StarOS software images are signed via x509 certificates. Please view the .README file packaged with the software for information and instructions on how to validate the certificates.

NOTE: Image signing is not currently supported for VPC-SI and/or VPC-DI software packages.

Open Bugs for This Release

The table below highlights the known bugs that were found in, and/or that remain open in this software release.

NOTE: This software release may contain open bugs first identified in other releases. Additional information for all open bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline	Product Found*
CSCvg36262	Split the current MME-Decor related stats for TAU and Attach procedures	mme
CSCvh59780	Sessmgr restart in egtpc event handler path	mme
CSCvh67114	sessmgr restarts at function egtpc_validate_context_ack_rsp_evt	mme
CSCvh82217	sessmgr task restart during MME start Auth procedure.	mme
CSCvi06043	aaamgr restarted multiple times on srp switch-over	pdn-gw
CSCvg95957	Single instance of Bulkstat facility restart seen on active CISCO ASR5500	pdn-gw
CSCvh67681	20% SM CPU increase when Traffic Optim is enabled with 100% heavy session in single event perf test	pdn-gw
CSCvi06491	The default behaviour of diameter encode-supported-features changed in 21.7	pdn-gw
CSCvh64982	Planned SRP switchover followed by switchover due to BGP failure - aaamgr restarts	sae-gw
CSCvf32599	osd-compute reboot leaves CF in booting state: EMCTRL_CARDTYPE_MISMATCH	staros
CSCvh54162	[ePDG] performing iftask restart is causing SF to restart on ultraM with servicemode as epdg	staros
CSCvh68111	The beakerd process has a memory leak	staros
CSCvh83313	IFTASK restarts due to a memory access fault	staros
CSCvi65014	Restart of vpnmgr task adversely affecting the connectivity.	staros

Bug ID	Headline	Product Found*
CSCvh84131	defaut mcdma latency is 0 leading to inefficiency	staros
CSCvh99381	SDR cli output shows all Enaled/Disabled command at all times.	staros
CSCvi44228	Incorrect time format for msg-format rfc5424	staros
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Resolved Bugs for This Release

The table below highlights the known bugs that are resolved in this specific software release.

NOTE: This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline	Product Found*
CSCvi28510	SessMgr memory leak when Xheader insertion with rc4md5 encryption is enabled in charging action	pdn-gw
CSCvj10403	DI - less number of session managers per SF card	staros
CSCvi81094	DInet communication issue with Intel XL710 NIC	staros
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

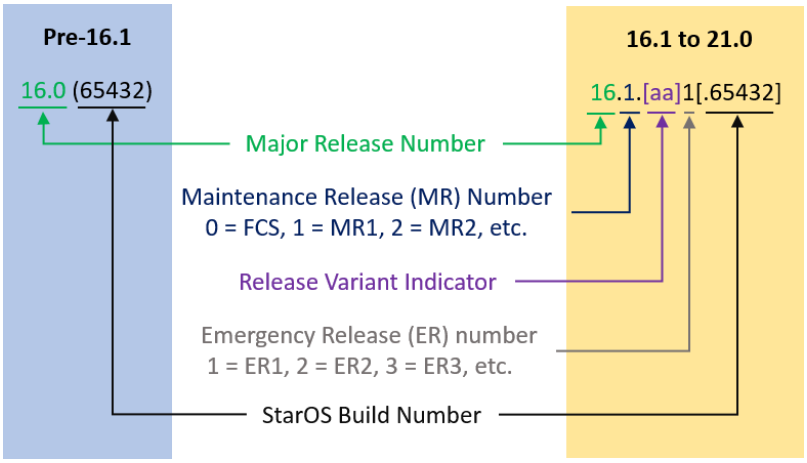
StarOS Version Numbering System

The output of the **show version** command displays detailed information about the version of StarOS currently running on the ASR 5x00 or Cisco Virtualized Packet Core platform.

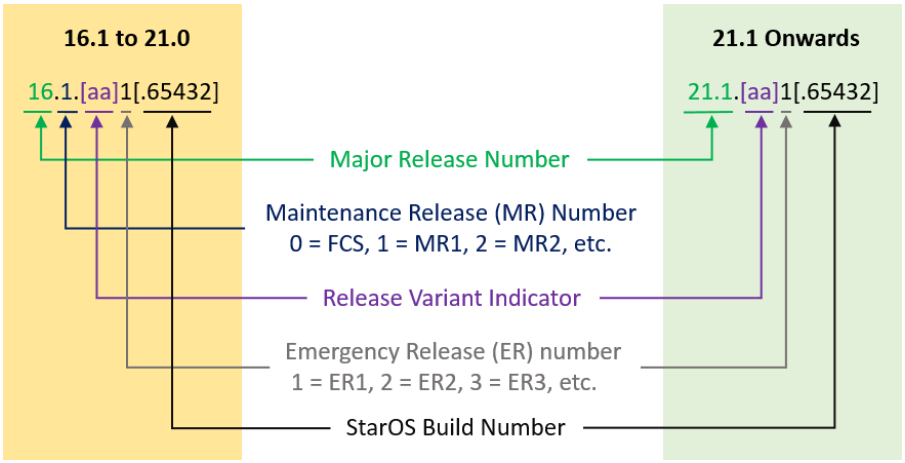
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build number.

From release 16.1 onwards, the output of the **show version** command, as well as the terminology used to describe the Build Version Number fields, has changed. Additionally, **show version** will display slightly different information depending on whether or not a build is suitable for deployment.

The Version Build Number for releases between 16.1 and 21.0 include a major, maintenance, and emergency release number, for example "16.1.2".



The Version Build Number for releases 21.1 and later include a major and emergency release number, for example, "21.1.1".



In either scenario, the appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format will facilitate identifying the changes between releases when using Bug Search Tool to research software releases.

Release Package Descriptions

Table 2 lists provides descriptions for the packages that are available with this release.

Table 2 - Release Package Information

Package	Description
ASR 5500	
asr5500-<release>.bin	A zip file containing the signed ASR 5500 software image, the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
asr5500_T-<release>.bin	A zip file containing the signed, trusted ASR 5500 software image, the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.

Package	Description
VPC-DI	
qvpc-di-<release>.bin	The VPC-DI binary software image which is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-di_T-<release>.bin	The trusted VPC-DI binary software image which is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-di-<release>.iso	The VPC-DI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image.
qvpc-di_T-<release>.iso	The trusted VPC-DI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image.
qvpc-di-template-vmware-<release>.tgz	The VPC-DI binary software image that is used to on-board the software directly into Vmware.
qvpc-di-template-vmware_T-<release>.tgz	The trusted VPC-DI binary software image that is used to on-board the software directly into Vmware.
qvpc-di-template-libvirt-kvm-<release>.tgz	This is an archive that includes the same VPC-DI ISO identified above, but additional installation files for using it on KVM.
qvpc-di-template-libvirt-kvm_T-<release>.tgz	This is an archive that includes the same trusted VPC-DI ISO identified above, but additional installation files for using it on KVM.
qvpc-di-<release>.qcow2.tgz	The VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.
qvpc-di_T-<release>.qcow2.tgz	The trusted VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.
VPC-SI	
qvpc-si-<release>.bin	The VPC-SI binary software image which is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-si_T-<release>.bin	The trusted VPC-SI binary software image which is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-si-<release>.iso	The VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image.
qvpc-si_T-<release>.iso	The trusted VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image.
qvpc-si-template-vmware-<release>.ova	The VPC-SI binary software image that is used to on-board the software directly into Vmware.
qvpc-si-template-vmware_T-<release>.ova	The trusted VPC-SI binary software image that is used to on-board the software directly into Vmware.

Package	Description
qvpc-si-template-libvirt-kvm-<release>.tgz	This is an archive that includes the same VPC-SI ISO identified above, but additional installation files for using it on KVM.
qvpc-si-template-libvirt-kvm_T-<release>.tgz	This is an archive that includes the same trusted VPC-SI ISO identified above, but additional installation files for using it on KVM.
qvpc-si-<release>.qcow2.gz	The VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.
qvpc-si_T-<release>.qcow2.gz	The trusted VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.
StarOS Companion Package	
companion-<release>.tgz	An archive containing numerous files pertaining to this version of the StarOS including SNMP MIBs, RADIUS dictionaries, ORBEM clients. These files pertain to both trusted and non-trusted build variants.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.