Release Notes for Cisco ASR 901 Series Aggregation Services Router for Cisco IOS Release 15.3(2)S

March 2013

OL-29265-01

This release notes is for the Cisco ASR 901 Series Aggregation Services Router for Cisco IOS Release 15.3(2)S and contains the following sections:

Introduction

The Cisco ASR 901 Series Aggregation Services Router is a cell-site access platform specifically designed to aggregate and transport mixed-generation radio access network (RAN) traffic. The router is used at the cell site edge as a part of a 2G, 3G, or 4G RAN.

The Cisco ASR 901 router helps enable a variety of RAN solutions by extending IP connectivity to devices using Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), Node Bs using High Speed Packet Access (HSPA) or Long Term Evolution (LTE), base transceiver stations (BTSs) using Enhanced Data Rates for GSM Evolution (EDGE), Code Division Multiple Access (CDMA), CDMA-2000, EVDO, or WiMAX, and other cell-site equipment.

Cisco Systems, Inc.
www.cisco.com

It transparently and efficiently transports cell-site voice, data, and signaling traffic over IP using traditional T1 and E1 circuits, as well as alternative backhaul networks such as Carrier Ethernet and DSL, Ethernet in the First Mile (EFM), and WiMAX. It also supports standards-based Internet Engineering Task Force (IETF) Internet protocols over the RAN transport network, including those standardized at the Third-Generation Partnership Project (3GPP) for IP RAN transport. Custom designed for the cell site, the Cisco ASR 901 router features a small form factor, extended operating temperature, and cell-site DC input voltages.

Table 1 lists the Cisco ASR 901 router model versions.

Table 1   Cisco ASR 901 Router Models

TDM + Ethernet Version	Ethernet Version
• A901-12C-FT-D[1]	• A901-12C-F-D[1]
• A901-4C-FT-D[1]	• A901-4C-F-D[1]
• A901-6CZ-FT-D[1]	• A901-6CZ-F-D[1]
• A901-6CZ-FT-A[2]	• A901-6CZ-F-A[2]

1. DC power
2. AC power

Note Some of the Cisco ASR 901 models have port based licensing. For more details, see the Licensing chapter in Cisco ASR 901 Series Aggregation Services Router Software Configuration Guide.

System Specifications

Table 2 lists the supported system configurations for the Cisco ASR 901 router:

Memory Details

Table 2 lists the memory available for Cisco ASR 901 router.

Table 2   Cisco IOS Release 15.3(2)S Memory Details

Platform	Software Image	Flash Memory	DRAM Memory	Runs From
Cisco ASR 901 Series Aggregation Services Router TDM version	asr901-universalk9-mz	128 MB	512 MB	RAM
Cisco ASR 901 Series Aggregation Services Router, Ethernet version	asr901-universalk9-mz	128 MB	512 MB	RAM

Determining the Software Version

To determine the image and version of Cisco IOS software running on your Cisco ASR 901 router, log in to the router and enter the **show version** command in the EXEC mode:

```
Router> show version
Cisco IOS Software, 901 Software (ASR901-UNIVERSALK9-M), Version 15.3(2)S, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Mon 25-Mar-13 13:13 by prod_rel_team

ROM: System Bootstrap, Version 15.2(2r)SNI, RELEASE SOFTWARE (fc1)
```

New and Changed Information

New Hardware Features in Release 15.3(2)S

There are no new hardware features in Cisco IOS Release 15.3(2)S.

New Software Features in Release 15.3(2)S

The following features are supported from this release:

Configuring Y.1564 to Generate Ethernet Traffic

Y.1564 is an Ethernet service activation or performance test methodology for turning up, installing, and troubleshooting Ethernet-based services. This test methodology allows for complete validation of Ethernet service-level agreements (SLAs) in a single test. Using traffic generator performance profile, you can create the traffic based on your requirements. The network performance like throughput, loss, and availability are analyzed using Layer 2 traffic with various bandwidth profiles.

For more information about this feature, see Configuring Y.1564 for Ethernet Traffic Generation section of the *Configuring Ethernet OAM* feature guide at the following URL:

http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/oam.html

Ethernet Synthetic Loss Measurement in Y.1731

The Ethernet Synthetic Loss Measurement in Y.1731 feature allows you to measure the Frame Loss Ratio (FLR) in the network, that is, the ratio of frames lost to frames sent, using synthetic frames.

For more information about this feature, see the *ITU-T Y.1731 Performance Monitoring* feature guide at the following URL:
http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/y1731pm.html

EVC Default Encapsulation

Cisco IOS Release 15.3(2)S introduces support for EVC default encapsulation on the Cisco ASR 901 router. This feature matches and forwards all the ingress traffic on the port. The default service instance on a port is configured using the **encapsulation default** command.

For more details, see the following URLs:

- http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/swevc.html (*Configuring Ethernet Virtual Connections*)
- http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/oam.html (*Configuring Ethernet OAM*)

Hot Standby Pseudowire Support for ATM and TDM Access Circuits

The Hot Standby Pseudowire Support for Inverse Multiplexing over ATM (IMA) feature improves the availability of pseudowires by detecting failures and handling them with minimal disruption to the service. This feature allows the backup pseudowire to be in a "hot standby" state, so that it can immediately take over if the primary pseudowire fails.

For more information about this feature, see *Configuring Pseudowire* feature guide at the following URL: http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/pseudowire.html

Microwave ACM Signaling and EEM Integration

The Microwave ACM Signaling and EEM Integration feature enables the microwave radio transceivers to report link bandwidth information to an upstream Ethernet switch and take action on the signal degradation to provide optimal bandwidth.

For information about this feature, see *Microwave ACM Signaling and EEM Integration* feature guide at the following URL:
http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/mw_acm.html

Multi-UNI MEPs in the Same VPN

Effective with Cisco IOS Release 15.3(2)S, services are configured such that two or more bridge domains (BDs) are used to achieve UNI isolation and backhauling towards provider edge (PE) device. Local MEPs (with up direction) need to be configured on the UNIs (with the associated BDs) to monitor the service backhaul connection.

For more information about this feature, see Configuring Multi-UNI CFM MEPs in the Same VPN section of the *Configuring Ethernet OAM* feature guide at the following URL:
http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/oam.html

OSPFv3 MIBs

The OSPFV3-MIB is supported from Cisco IOS Release 15.3(2)S onwards. This MIB module is for OSPF version 3.

For more information about this MIB, see *Cisco ASR 901 Series Aggregation Services Router MIB Specifications* guide at the following URL:

http://www.cisco.com/en/US/docs/wireless/asr_901/mib/reference/asr_mib.html

Remote Loop-Free Alternate - Fast Reroute for EoMPLS

The Remote Loop-Free Alternate - Fast Reroute for EoMPLS feature is introduced.

For more information about this feature, see *Remote Loop-Free Alternate - Fast Reroute* feature guide at the following URL:
http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/remote_lfa-frr.html

Traffic Engineering - Fast Reroute for EoMPLS

The Traffic Engineering - Fast Reroute for EoMPLS feature is introduced.

For more information about this feature, see *MPLS Traffic Engineering - Fast Reroute Link* feature guide at the following URL:
http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/mpls_te-frr.html

Y.1731 Performance Monitoring

Y.1731 Performance Monitoring feature provides standards-based Ethernet performance monitoring as outlined in the ITU-T Y-1731 specification and interpreted by the Metro Ethernet Forum (MEF).

For more information about this feature, see the *ITU-T Y.1731 Performance Monitoring* feature guide at the following URL:
http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/y1731pm.html

Modified Software Features in Release 15.3(2)S

This section lists the features modified for this release:

Combo Port Media Type Select

Starting with Cisco IOS Release 15.3(2)S, the Cisco ASR 901 router supports selection of combo ports as the media type. A combo port is considered as a single interface with dual front ends (an RJ-45 connector and an SFP module connector).

For more details, see *Configuring Gigabit Ethernet Interfaces* guide at the following URL:

http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/gige_intf.html

Configurable MTU on Physical Interface

Starting with Cisco IOS Release 15.3(2)S, the Cisco ASR 901 router supports modification of MTU size on physical interface.

For more details, see *Configuring Gigabit Ethernet Interfaces* guide at the following URL:

http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/gige_intf.html

Disabling MAC Address Learning on an Interface or Bridge Domain

Starting with Cisco IOS Release 15.3(2)S, you can control MAC address learning on an interface or VLAN to manage the available MAC address table space by controlling which interfaces or VLANs can learn MAC addresses.

For more details, see Disabling MAC Address Learning on an Interface or Bridge Domain section of the *Configuring Ethernet Virtual Connections* feature guide at the following URL:
http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/swevc.html

Layer 3 Ping in Customer EVC

Starting with Cisco IOS Release 15.3(2)S, pop 2 configuration is supported on layer 2 and layer 3 operations. Additionally, it is supported on GigabitEthernet and port channel interfaces.

For more details, see L3 PING in customer EVC section of the *Configuring Ethernet Virtual Connections* feature guide at the following URL:
http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/swevc.html

Sub-second Link OAM Timers

Starting with Cisco IOS Release 15.3(2)S, the Cisco ASR 901 router supports sub-second OAM timers.

For more details, see the *Configuring Ethernet OAM* feature guide at the following URL:

http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/oam.html

TCAM in Cisco ASR 901 Router

Effective with Cisco IOS Release 15.3(2)S, the Ternary Content Addressable Memory (TCAM) is allocated and deallocated dynamically, which improves both feature scalability and the efficiency of usage of TCAM.

For more details, see *Configuring QoS* guide at the following URL:

http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/qos.html

Supported Hardware

Table 3 and Table 4 shows the SFP modules supported on the Cisco ASR 901 routers:

Table 3   SFPs Supported on the Cisco ASR 901 1G Router

• CWDM-SFP-1470	• GLC-LX-SM-RGD
• CWDM-SFP-1490	• GLC-SX-MMD
• CWDM-SFP-1510	• GLC-SX-MM-RGD
• CWDM-SFP-1530	• GLC-T
• CWDM-SFP-1550	• GLC-ZX-SM
• CWDM-SFP-1570	• GLC-ZX-SMD
• CWDM-SFP-1590	• GLC-ZX-SM-RGD
• CWDM-SFP-1610	• SFP-GE-L
• DWDM-SFP-XXXX[1]	• SFP-GE-S
• GLC-BX-U and GLC-BX-D[2]	• SFP-GE-T
• GLC-EX-SMD	• SFP-GE-Z
• GLC-LH-SMD	

1.   40 wavelengths

2.   These SFPs (GLC-BX-U and GLC-BX-D) should be connected back to back to bring the interface link up.

Table 4   SFPs Supported on the Cisco ASR 901 10G Router

• SFP-10G-ER	• SFP-10G-SR
• SFP-10G-LR	• SFP-10G-SR-X
• SFP-10G-LR-X	• SFP-10G-ZR

Note   For information on how to configure SFPs, see the *Cisco ASR 901 Series Aggregation Services Router Software Configuration Guide.*

Supported MIBs

The Cisco ASR 901 router supports the following MIBs:

• BGP4-MIB	• CISCO-STP-EXTENSIONS-MIB
• BRIDGE-MIB	• CISCO-SYSLOG-MIB
• CISCO-ACCESSENVMON-MIB	• CISCO-TC

- CISCO-CAR-MIB
- CISCO-CDP-MIB
- CISCO-CEF-MIB
- CISCO-CLASS-BASED-QOS-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-DATA-COLLECTION-MIB
- CISCO-DOT3-OAM-MIB
- CISCO-EIGRP-MIB
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENTITY-ASSET-MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB
- CISCO-ENVMON-MIB
- CISCO-FLASH-MIB
- CISCO-IETF-PW-MIB
- CISCO-IETF-PW-TC-MIB
- CISCO-IF-EXTENSION-MIB
- CISCO-IMAGE-MIB
- CISCO-IPSLA-ETHERNETMIB
- CISCO-MEMORY-POOL-MIB
- CISCO-NETSYNC-MIB
- CISCO-NTP-MIB
- CISCO-OSPF-MIB
- CISCO-PING-MIB
- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-MIB

- ENTITY-MIB
- ETHERLIKE-MIB
- HCNUM-TC
- IANAifType-MIB
- IEEE8021-CFM-MIB
- IF-MIB
- IMA-MIB
- INT-SERVE-MIB
- IP-FORWARD-MIB
- IP-MIB
- MPLS-LDP-MIB
- MPLS-LSR-MIB
- MPLS-VPN-MIB
- NOTIFICATION-LOG-MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-FLASH-MIB
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-IP-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-TS-MIB
- OSPF-MIB
- OSPFv3-MIB
- PerfHist-TC-MIB
- RFC1213-MIB
- RMON2-MIB
- RMON-MIB

- CISCO-PTP-MIB
- CISCO-QUEUE-MIB
- CISCO-RESILIENT-ETHERNET-PROTOCOL -MIB
- CISCO-RTTMON-MIB
- CISCO-SENSOR-ENTITY-MIB
- CISCO-SMI-MIB
- CISCO-SNAPSHOT-MIB
- CISCO-SNMP-TARGET-EXT-MIB

- SNMP-FRAMEWORKMIB
- SNMP-TARGET-MIB
- SNMPv2-MIB
- SNMPv2-SMI
- SNMPV2-TC
- TCP-MIB
- UDP-MIB
-

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats, severity 2 caveats are less serious, and severity 3 caveats are the least serious of these three severity levels. Only select severity 3 caveats are listed.

This section contains the following topics:

- Using Bug Toolkit
- Open Caveats
- Resolved Caveats

Using Bug Toolkit

The Caveats section only includes the bug ID and a short description of the bug. For details on the symptoms, conditions, and workaround for a particular bug you must use the Bug ToolKit. This section explains how to use the bug toolkit and has the following topics:

- Search Bugs
- Save Bugs
- Save Search
- Retrieve Saved Search or Bugs
- Export to Spreadsheet

Search Bugs

This section explains how to use the Bug ToolKit to search for a specific bug.

Step 1 Go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

You are prompted to log into Cisco.com. After successful login, the Bug Toolkit page opens.

Step 2 Click **Launch Bug Toolkit**.

Step 3 To search for a specific bug, enter the bug ID in the **Search for Bug ID** field and click **Go** in the **Search Bugs** tab.

To search for bugs in a specific release, enter the following search criteria:

- Select Product Category—Select **Routers**.

- Select Products—Select the required product from the list. For example, to view bugs for Cisco ASR 901, choose **Cisco ASR 901 Series Aggregation Services Router** from the list.

- Software Version—Choose the required Cisco IOS version from the drop-down lists. For example, to view the list of outstanding and resolved bugs in Cisco IOS Release 15.3(2)S, choose **15.3** from the first drop-down list, **2** from the second drop-down list, and **S** from the third drop-down list.

- Search for Keyword(s)—Separate search phrases with boolean expressions (AND, NOT, OR) to search within the bug title and details.

- Advanced Options—You can either perform a search using the default search criteria or define custom criteria for an advanced search. To customize the advanced search, select **Use custom settings for severity, status, and others** and provide the following information:

  - Severity—Select the severity level.

  - Status—Select **Open**, **Fixed**, or **Terminated**.

    Select **Open** to view all the open bugs. To filter the open bugs, clear the Open check box and select the appropriate sub-options that appear below the Open check box. The sub-options are New, Held, More, Open, Waiting, Assigned, Forwarded, Postponed, Submitted, and Information Required. For example, if you want to view only new bugs in Cisco IOS Release 15.3(2)S, select **New**.

    Select **Fixed** to view fixed bugs. To filter fixed bugs, clear the Fixed check box and select the appropriate sub-options that appear below the Fixed check box. The sub-options are **Resolved** or **Verified**.

    Select **Terminated** to view terminated bugs. To filter terminated bugs, clear the Terminated check box and select the appropriate sub-options that appear below the terminated check box. The sub-options are **Closed**, **Junked**, and **Unreproducible**. Select multiple options as required.

  - Advanced—Select the **Show only bugs containing bug details** check box to view only those bugs that contain detailed information, such as symptoms and workarounds.

  - Modified Date—Select this option if you want to filter bugs based on the date on which the bugs were last modified.

  - Results Displayed Per Page—Select the appropriate option from the list to restrict the number of results that appear per page.

Step 4 Click **Search**. The Bug Toolkit displays the list of bugs based on the specified search criteria.

Save Bugs

This section explains how to use Bug ToolKit to save the bugs retrieved by your search in a specific release.

Step 1 Perform a search.
Repeat Step 1 through Step 3 in the "Search Bugs" section on page 9.

Step 2 Select the check boxes next to the bug you want to save in the Search Results page and click **Save Checked**.

The Save Bug Settings area appears under the Search Bugs tab.

Step 3 Specify group settings in the **Place in Group** field.

- Existing Group—Select an existing group.

- Create New Group—Enter a group name to create a new group.

Existing groups have their group notification options already set. If you select an existing group, go to Step 5.

Step 4 Specify the following email update (group notification) options.

- No emailed updates—Select if you do not want to receive email updates.

- Yes, email updates to—Enter your email address.

  - On a schedule—Specify the frequency of email delivery.

Step 5 Click **Save Bug**.

The Bug ToolKit saves the selected bugs in the specified group.

Save Search

This section explains how to use Bug ToolKit to save your search after searching for the bugs in a specific release.

Step 1 Perform a search.
Repeat Step 1 through Step 3 in the "Search Bugs" section on page 9.

Step 2 Click **Save Search** in the Search Results page to save your search with the specified criteria.

The Save Search Settings area appears under the My Notifications tab.

Step 3 Enter a name for your search in the **Search Name** field.

Step 4 Specify group settings in the **Place in Group** field.

- Existing Group—Select an existing group.

- Create New Group—Enter a group name to create a new group.

Existing groups have their group notification options already set. If you select an existing group, go to Step 6.

Step 5 Specify the following email update (group notification) options.

- No emailed updates—Select if you do not want to receive email updates.

- Yes, email updates to—Enter your email address.

  - On a schedule—Specify the frequency of email delivery.

Step 6 Click **Save Search**.

The Bug ToolKit saves your search in the specified group.

Retrieve Saved Search or Bugs

This section explains how to use Bug ToolKit to retrieve a saved search or bugs.

Step 1 Go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl and click **Launch Bug Toolkit**.

You are prompted to log into Cisco.com.

Step 2 Click **My Notifications** tab.
My Notifications tab displays the Group Name, Summary, and Actions.

Step 3 Click the group in the Group Name column. The group contains saved search and bugs.

Step 4 Retrieve saved search or bugs.

- Click the saved search name to display the Search Results page.

- Click the saved bug to display details or hover your mouse pointer over the Info link.

The My Notifications tab also provides option to delete bug, delete search, delete group, edit group notifications (in the Actions column), move selected saved search or bugs to different group, and to export saved bugs in all the groups to a spreadsheet.

Export to Spreadsheet

The Bug ToolKit provides the following options to export bugs to a spreadsheet:

- Click **Export All to Spreadsheet** link in the Search Results page under the Search Bugs tab. Specify file name and folder name to save the spreadsheet. All the bugs retrieved by the search is exported.

- Click **Export All to Spreadsheet** link in the My Notifications tab. Specify file name and folder name to save the spreadsheet. All the saved bugs in all the groups is exported.

If you are unable to export the spreadsheet, log into the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1-800-553-2447).

Open Caveats

This section provides information about the open caveats for the Cisco ASR 901 router running Cisco IOS Release 15.3(2)S.

Bug ID	Description
CSCtk33675	The service instance configuration is rejected when the encapsulation is set to default for double-tagged traffic.
CSCtl70431	The "no rewrite" option is not working on interfaces configured with encapsulation dot1q.
CSCtn18900	Service policy classification based on inner Virtual LAN p-bits is not working.
CSCtn71094	The **no int vlan 1** command deletes VLAN 1.

Bug ID	Description
CSCtn79746	The **show ethernet service instance statistics** command is not displaying any statistics.
CSCto96840	A CLI restriction is required for Dual Rate Three Color (2R3C) on parent class in Hierarchical Quality of Service (HQoS).
CSCtq26793	Some ports are not getting bundled with the port channel because of attribute mismatch, such as flow-control.
CSCtr05566	The Multiprotocol Label Switching (MPLS) traffic fails when port channel encapsulation is not equal to the bridge domain on the core.
CSCtr70228	High CPU utilization is observed while performing save or copy operation.
CSCts66081	Ingress VLAN translation failure occurs when entries exceed 3000.
CSCts80090	The reserved VLANs are not blocked on the router.
CSCts84679	The circuit emulation (CEM) interface displays wrong configuration in the **show running-configuration** command output, when pw-class is configured.
CSCts85484	Traceback occurs after executing **rep preempt segment segid** command.
CSCts92808	Weighted Random Early Detection (WRED) counters are not working for discard class 0.
CSCtw52497	The interface drops all ingress packets when you reload the router with write erase, and copy the saved configuration to the running configuration.
CSCtw69021	Maximum bandwidth guarantee for Multilink Point-to-Point Protocol (MLPPP) interface is not working for 64-byte size frames in Low Latency Queuing (LLQ).
CSCtx12366	The servo is accepting more than 64PPS Sync in static unicast.
CSCtx22010	SyncE is not supported for the Copper SFPs: GLC-T and SFP-GE-T
CSCtx34208	Clock selection fails for SyncE when interface media-type is SFP.
CSCtx54735	High CPU utilization and traceback is observed while doing copy and paste of 16 E1 controllers unconfigurations.
CSCtx77374	Input errors are increasing when serial interface flaps. This issue is observed on a serial interface that is part of a multilink interface, when keepalive is disabled.
CSCty04070	Traffic fails and continuous traceback is observed, when xconnect is configured on an untagged EVC.
CSCty95886	The file copy function is not detecting errors properly.
CSCtz16522	The Two-Way Active Measurement Protocol (TWAMP) session-reflector packet truncation fails.
CSCtz34776	Random IP/UDP packets sent to LB interface are getting punted to CPU.
CSCtz38207	Router is rebooting continuously due to failed fans.
CSCtz48755	We recommend the use of minimum 1 sec (or above) hello timer for Hot Standby Router Protocol (HSRP) and Virtual Redundancy Router Protocol (VRRP). With this configuration, we support a maximum of 50 sessions.

Bug ID	Description
CSCtz69403	IPv6 traffic is not getting dropped with link-local as source address.
CSCtz81384	The Layer 2 ATM/IMA interface and its permanent virtual circuits (PVCs) are not coming up when operations, administration and maintenance (OAM) is configured.
CSCtz90417	When the router boots up, the following traceback is displayed: "%LICENSE-2-VLS_ERROR: 'VLSsetPersistencePath' failed with an error - rc = 212 - 'Error[212]:"

There is no functionality impact, it can be safely ignored. |
| CSCtz90437 | When the router boots up, it displays the following traceback messages: "*Mar 19 23:45:24.371: %LICENSE-2-UNRECOVERABLE: The IOS license storage on this device was not recovered. UDI=A901-12C-FT-D:FHAK1234567

*Mar 19 23:45:24.375: Following corrupted license storage was un-recoverable : lic0:/lservrc.pri

*Mar 19 23:45:24.375: -Traceback= 265C5A8z 60DC228z 60D97C8z 60D9F64z 580B534z 580573Cze"

These tracebacks may also appear while trying to install a license.

There is no functionality impact, it can be safely ignored. |
| CSCua19178 | Packet drops are seen with IPv6 fragmentation. |
| CSCua34320 | The OSPFv3 keeps old router-id even after changing the loopback address. |
| CSCua34389 | Manual tunnel having MPLS configuration with dynamic option in the following sequence does not set up targeted ldp session resulting in tunnel staying down. shut/no shut of the tunnel brings back the targeted Label Distribution Protocol (LDP) session up.

```
interface Tunnel108
ip unnumbered Loopback0
mpls label protocol ldp
mpls ip
tunnel source Loopback0
tunnel destination 36.36.36.36
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 dynamic
```

The issue is not observed when tunnel mode is configured ahead of tunnel destination, |
| CSCua40707 | The commands related to MPLS and MPLS-TE/FRR are applicable only to SVI interfaces though they can be enabled globally.

Thus configuring the MPLS commands on the GigabitEthernet interface or port-channel is not supported. |
CSCua49491	The MPLS traffic engineering counters are not supported.
CSCua51628	The OSPFv3 bidirectional forwarding detection (BFD) flaps after an interface is shut in a port-channel bundle.
CSCua81678	The following error message is displayed for /128 prefix: "Reached Maximum Number of IPv6 Hosts".

Bug ID	Description
CSCua82917	In remote LFA FRR, the recovery takes more than 80 ms.
CSCua84571	Load balancing is not working with different streams having symmetrical addresses.
CSCua88693	The **verify** command is not supported for the USB flash in the Cisco ASR 901 10G router.
CSCua98165	The IPv6 BFD packets should be mapped to Queue 6 on egress interface.
CSCua99910	MAC address table (MAC learning) failures can be seen with more than 31000 MAC Addresses in certain conditions. So it is safe to assume the platform supports 31000 MAC addresses.
CSCub12715	The "pura_cef_ipv6_route_create_update:Reached Maximum Number of Prefixes supported by platform.Additional Prefixes will not be programmed" message is displayed when the primary path is shut/unshut in a redundant convergent setup.
CSCub71746	Alarm Indication Signal (AIS) is visible momentarily at T1 controller of CE1 while reverting back to primary.
CSCuc15639	Connectivity Fault Management (CFM) is not supported with 100 ms interval.
CSCuc22630	The router fails to recognize USB when its removed immediately after insertion.
CSCuc25878	The UBR transmits at a lower rate when all five class of service (CoS) Private Virtual Circuits (PVCs) are configured.
CSCuc33942	The Cisco ASR 901 10G interface is coming up after changing the shut/no shut configuration in startup-configuration.
CSCuc39560	IPv6 traffic drop occurs globally when IPv4 VRF is configured on the same SVI with "ip vrf definition".
CSCuc52851	The "%QOS-6-POLICY_INST_FAILED:" error message is displayed when service-policy is applied under a multilink interface.
CSCuc85033	The untagged Ethernet Virtual Circuit (EVC) port is not supported for spanning tree.
CSCuc95900	Traffic is receiving two VLAN tags, instead of three for QinQ with pop 2.
CSCud04703	In Zero Touch Provisioning, the Cisco ASR 901 router is not able to connect to the CE server using option-43 template, when source interface is passed as a parameter.
CSCud05125	In traffic generator, the receiver (Rx) counter is incrementing even after the EVC mismatch.
CSCud14278	Border Gateway Protocol (BGP) flap is observed between PEs when traffic from CE side is oversubscribed towards PE.
CSCud16558	High convergence time is observed when "shut" operation is performed on fast re-route (FRR) configured with port channels. This issue can be resolved with BFD.
CSCud20997	The Ethernet Over MPLS (EoMPLS) pseudowire redundancy fails when backup pseudowire is active in TE-FRR backup path.

Bug ID	Description
CSCud21775	In Zero Touch Provisioning, the Cisco ASR 901 10G router is using wrong Unique Device Identifier (UDI) event-id to make connection to the CE.
CSCud24655	CPU hog is observed when primary path is "shut" in an LFA FRR set up with 1000 prefixes.
CSCud29184	The **show version** command is not giving the image name when the boot system variable is set as: **boot system flash** *image-name*.
CSCud32961	Error occurs when any label entry is crossing the 3500 range.
CSCud33913	In Zero Touch Provisioning, the VLAN discovery is not supported for encapsulation dot1ad.
CSCud37655	The xconnect MTU is not used for traffic filtering.
CSCud53474	The combo interface is going down after the channel group configuration.
CSCud71334	The mac-address flap control is putting all ports into "err-disabled" state, in some cases.
CSCud74577	The CPU process for IP SLA continues to run even after stopping the traffic generator.
CSCud75293	The **show rom-monitor** command is not showing upgraded ROMMON version in IOS mode.
CSCud79202	The **show inventory** command is displaying the PID of SFP-SX-MM as GLC-SX-MM.
CSCud89083	The router displays "soc_counter_sync: counter thread not responding" error, under heavy CPU usage.
CSCue11410	The incremental-SPF configuration is causing micro loops during convergence, in IGP IS-IS.
CSCue11688	The VRF routes are leaked from the adjacent VRF with a particular IP:nn pattern.
CSCue18282	CPU hog and traceback is observed when scale configuration is pushed from CE server to the router.
CSCue22409	Connectivity Fault Management (CFM) continuity check message (CCM) packets are tagged with egress interface tag, instead of CFM configured interface tag.
CSCue53113	In combo-ports, the traffic is flowing only to a single direction when the media-type is RJ-45.
CSCue54634	Traffic outage and pstorm errors are observed when port channel is configured and unconfigured multiple times.
CSCue67669	It is not possible to configure default encapsulation only on the CE facing interface. This brings down the CFM session.
CSCue68363	Pseudowire Emulation Edge to Edge (PWE3) statistics shows wrong values after the Resource Reservation Protocol-Trafic Extension (RSVP-TE) primary path failure.
CSCue72819	Traceroute is not working when Connectivity Fault Management (CFM) up Maintenance Endpoint (MEP) is configured with default encapsulation under xconnect.

Bug ID	Description
CSCue75664	Traceroute fails when CFM maintenance intermediate point (MIP) is configured with default encapsulation.
CSCue80587	The throughput statistics is active even after completing the IP SLA schedule.
CSCue88662	Un-configuring or changing the split-horizon for bridge-domain fails.
CSCue91862	Peering is not working for untagged EVC when service instance is configured with default encapsulation.
CSCue94536	The port channel interface flaps when lacp max-bundle is configured and unconfigured.
CSCuf06812	Invalid encapsulation type warning is displayed when EVC is configured under port channel.
CSCuf16106	Traceroute is not working when CFM down MEP is configured with default encapsulation.
CSCuf21682	High reconvergence is observed for global traffic in Remote Loop Free Alternate (LFA).
CSCuf30394	The combo port interfaces are not coming up when one end is in auto-select mode and the other end in SFP mode.
CSCuf35663	The Multiple Spanning Tree Protocol (MSTP) interoperability is not working with Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP), and the port is blocked.
CSCuf48503	Higher latency is observed for middle priority queue.
CSCuf51632	The 10G in 1G mode is using the default Maximum Transmission Unit (MTU) of 1518.
CSCuf54567	BGP label carrying information (RFC 3107) is not working when ECMP and EoMPLS is configured.
CSCuf26488	Traffic drops for Equal Cost Multipath (ECMP) prefixes after neighbour discovery (ND) expires on both the links.
CSCuf49860	Configuration of backup peer on primary xconnect, after bringing up remote peer backup results in flap.

Resolved Caveats

This section provides information about the resolved caveats for the Cisco ASR 901 router running Cisco IOS Release 15.3(2)S.

Bug ID	Description
CSCtn32463	There is no command restriction in applying a service policy to Ethernet Virtual Connection (EVC) on the egress.
CSCua28317	The IMA link is not coming up after removing and adding it in loss of frame (LOF) condition.
CSCua72546	The IMA auto-restart feature is not working.
CSCua72557	The IMA test link feature is not working.

Bug ID	Description
CSCud35547	The ECMP is not working when traffic is coming on 2 ingress interfaces.
CSCud60102	An untagged EVC port is moving into blocked state by default.
CSCud64293	The TE-FRR protection is not working when explicit primary path is configured.
CSCud70245	The error message "pstorm_ether_pak_tx" is not formatted properly.
CSCud72473	When the Cisco ASR 901 router is configured as Network Time Protocol (NTP) client, it loses synchronization with the server after some time.
CSCue22998	Ethernet jitter is giving a wrong return code when it is configured through SNMP.
CSCue30216	High convergence time is observed for some global prefixes in remote LFA OSPF setup. This issue is also observed for IS-IS, with 500 prefix global scale.
CSCue54917	The Cisco ASR 901 10G router license is shown as "in use" when the interface is down.

Troubleshooting

The following sections describe troubleshooting commands you can use with the Cisco ASR 901 Series Aggregation Services Router.

Collecting Data for Router Issues

To collect data for reporting router issues, issue the following command:

- **show tech-support**—Displays general information about the router if it reports a problem.

Collecting Data for ROMMON Issues

To collect data for ROMMON issues, issue the following command while in the EXEC mode:

- **show rom-monitor**—Displays currently selected ROM monitor.

Note If you contact Cisco support for assistance, we recommend that you provide any crashinfo files stored in flash memory. For more information about crashinfo files, see http://www.cisco.com/en/US/products/hw/routers/ps167/products_tech_note09186a00800a6743.shtml.

Related Documentation

Documents related to the Cisco ASR 901 Series Aggregation Services Router include the following:

- *Cisco ASR 901 Series Aggregation Services Router Hardware Installation Guide*
- *Cisco ASR 901 Series Aggregation Services Router Software Configuration Guide*
- *Regulatory Compliance and Safety Information for Cisco ASR 901 Series Aggregation Services Routers*
- *Cisco ASR 901 Series Aggregation Services Router Series MIB Specifications Guide*

To access the related documentation on Cisco.com, go to:

http://www.cisco.com/en/US/partner/products/ps12077/tsd_products_support_series_home.html

Services and Support

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Release Notes for Cisco ASR 901 Aggregation Series Router for Cisco IOS Release 15.3(2)S