Release Notes for Cisco ASR 901 Series Aggregation Services Router for Cisco IOS Release 15.3(3)S1

October 2013

OL-30846-01

This release notes is for the Cisco ASR 901 Series Aggregation Services Router for Cisco IOS Release 15.3(3)S1 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(3)S1 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(3)S1, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Thu 24-Oct-13 13:24 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(3)S1

There are no new hardware features in Cisco IOS Release 15.3(3)S1.

New Software Features in Release 15.3(3)S1

There are no new software features in Cisco IOS Release 15.3(3)S1.

Modified Software Features in Release 15.3(3)S1

There are no modified features in Cisco IOS Release 15.3(3)S1.

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 and 10G Routers for 1G Mode

• 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 for 10G Mode

• SFP-10G-ER	• SFP-10G-SR
• SFP-10G-LR	• SFP-10G-SR-X
• SFP-10G-LR-X	• SFP-10G-ZR
• DWDM-SFP+	• SFP-10G-LRM
• SFP-H10GB-CU1M	• SFP-H10GB-ACU7M
• SFP-H10GB-CU3M	• SFP-H10GB-ACU10M
• SFP-H10GB-CU5M	

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

- CISCO-NTP-MIB
- CISCO-OSPF-MIB
- CISCO-PING-MIB
- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-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
- OSPFv3-MIB
- PerfHist-TC-MIB
- RFC1213-MIB
- RMON2-MIB
- RMON-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

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:

- 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 7.

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 7.

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(3)S1.

Bug ID	Description
CSCtn18900	Service policy classification based on inner Virtual LAN p-bits is not working.
CSCtn71094	The **no interface vlan 1** command deletes VLAN 1.
CSCtn79746	The **show ethernet service instance statistics** command is not displaying any statistics.
CSCto96840	A command 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
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.

Bug ID	Description
CSCtz16522	The Two-Way Active Measurement Protocol (TWAMP) session-reflector packet truncation fails.
CSCtz38207	Router is rebooting continuously due to failed fans.
CSCtz48755	The write operation triggers the flaps for Hot Standby Router Protocol (HSRP). We recommend the use of minimum 1 sec (or above) hello timer for HSRP and Virtual Redundancy Router Protocol (VRRP). With this configuration, we support a maximum of 50 sessions.
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.
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”.
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.

Bug ID	Description
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.
CSCuc39560	IPv6 traffic drop occurs globally when IPv4 VRF is configured on the same SVI with **ip vrf definition**.
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 series 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.
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.

Bug ID	Description
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.
CSCue54634	Traffic outage and pstorm errors are observed when port channel is configured and unconfigured multiple times.
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.
CSCuf21682	High reconvergence is observed for global traffic in Remote Loop Free Alternate (RLFA).
CSCuf48503	Higher latency is observed for middle priority queue.
CSCuf49860	Configuration of backup peer on primary xconnect, after bringing up remote peer backup results in flap.
CSCug61006	Auto-select is not working on the Gigabit Ethernet (0/4) port. For combo ports, shutdown or no shutdown on the interface is mandatory while changing the media type from RJ45 to auto-select and auto-select to RJ45 respectively.
CSCug91477	Strom control filter for the port channel does not show the discarded counters.
CSCue27148	Console hangs when **verify** command is executed on two telnet sessions.
CSCue45003	ASR901 strom control filter does not support current counters value in **show storm** output.
CSCuh51097	Error disable recovery state does not persist for the second time on fiber port even after the error recovery interval.
CSCuh64499	Cisco ASR 901 series router crashes while defaulting the interface.
CSCug92777	On Layer 3, multicast traffic are punted to CPU even when storm control drops all the packets.

Bug ID	Description
CSCuh11698	When more than four ports are connected to a peer where the ports are administratively up, the interface which detects a link up event takes the license first. Hence, the behavior of ports is non predictable. The first port which detects the link up will take the license and the other port may not get a valid license.
CSCui68701	When you insert CWDM or avago type fiber adjacent to GLC-LH-SMD port, the GLC-LH-SMD port goes down.
CSCuj87842	IP connectivity fails on combo ports with copper link after reload.
CSCuh77658	When the router boots up, the Gigabit Ethernet port flaps multiple times.
CSCuh37393	100M SFP support is not available for auto-select medium feature.
CSCuh91973	After reload, incorrect error message is displayed for unsupported SFPs.

Resolved Caveats

This section provides information about the resolved caveats for the Cisco ASR 901 router running Cisco IOS Release 15.3(3)S1.

Bug ID	Description
CSCtx34208	Clock selection fails for SyncE when interface media-type is SFP.
CSCue65843	On executing the **show version** command, an error message stating that Licensing infrastructure is not initialized is displayed.
CSCue90786	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.
CSCuf20395	Tracebacks are seen on the peer device when lacp max-bundle is unconfigured.
CSCug76869	Traceback is seen after configuring EVC with encapsulation range.
CSCug88564	L2CP packets are forwarded within the same bridge-domain and split-horizon group.
CSCuh11479	ASR 901 CFM MIP does not respond with correct tag for LTM encapsulation but uses EVC encapsulation.
CSCuh32439	The traceroute of port channel interface to MIP mac address of egress interface fails when MIP is configured on both the interfaces.
CSCuh34658	Two-way DMM does not work with CFM UP on QinQ pop2 and untagged egress interface.

Bug ID	Description
CSCuh41880	CEM disposition traffic fails on pseudowire failover and xconnect flaps.
CSCuh72606	MLPPP debug infra for Cisco ASR 901 router.
CSCuh95137	When pseudowire switchover is triggered for the VPC circuit, EXP marking fails and all labels are marked as EXP0. This issue is also seen on pseudowire failback.
CSCui09127	As the split-horizon configuration sequence is happening after the VLAN configuration, minimal traffic is sent over the BD's configured with split-horizon during reload.
CSCui09926	MLPPP winpath stats can not be cleared using the **clear counters** command..
CSCui16946	Priority-Tag-EFP configuration is not supported.
CSCui24777	L3 traffic fails with split-horizon configuration on the bridge-domain interface.
CSCui29488	Write memory configuration causes ISIS BFD flap with multicast traffic punting to CPU.
CSCtz34776	Random IP or UDP packets sent to the LB interface are getting punted to CPU.
CSCui30998	CLM discovery is not working because of the missing Slot ID.
CSCui35265	MTU configuration does not get reflected in hardware if we do not have IPv4 address on SVI.
CSCui42671	Convergence number is more than 170ms with scaled bridge-domains.
CSCui44972	Memory leak is found during SNMP poll for PTP MIB.
CSCui46741	Small memory leak is found when accessing certain parts of PTP MIB.
CSCui62019	Router crashes after executing **clear mpls ldp neighbor** command on bootup.
CSCui71922	Split-horizon is not working.
CSCui84281	10G SFP ports show SFP is detected even when the SFP is not present.
CSCuj06552	SFP GLC-EX-SMD is not working properly on the Cisco ASR 901 router.
CSCuj16742	No bind for CEM pseudowire at headend on standby core isolate recovery.
CSCuj28232	TDM psuedowires loose FRR convergence whenever remote end changes VC labels.
CSCuj14237	Stale VFP entry is recreated for forwarding of L2CP, on deleting the encapsulation default EFP configured with L2 protocol forward.
CSCui26581	Memory leak in PTP MIB during SNMP query.
CSCui11515	DMM does not work with CFM UP MEP on UNI as it only considers NNI encapsulation for reply. For example, DMM does not work when we have dot1q without pop on UNI (DMM responder) and dot1q pop 1 on NNI.
CSCui96148	Configuration sequence allows minimal traffic during reload with split-horizon over port-channel interface.
CSCuj19584	Sequence of the output for MIB (entPhysicalDescr) seems to be broken.

Bug ID	Description
CSCuj21759	WP_ERR_NO_FREE_IW_PORT error is observed and L3 ping is failed on MLPPP bundle.
CSCug86309	Copying files from router to another router through Gigabit Ethernet ports encounters timeout and fails.
CSCue75664	Traceroute fails when CFM maintenance intermediate point (MIP) is configured with default encapsulation.

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

Release Notes for Cisco ASR 901 Aggregation Series Router for Cisco IOS Release 15.3(3)S1