Release Notes for Cisco ASR 901 Series Aggregation Services Router for Cisco IOS Release 15.2(2)SNH1

October 2012

OL-28112-01

This release notes is for the Cisco ASR 901 Series Aggregation Services Router for Cisco IOS Release 15.2(2)SNH1 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.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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 • A901-4C-FT-D • A901-6CZ-FT-D[1] • A901-6CZ-FT-A[2]	• A901-12C-F-D • A901-4C-F-D • A901-6CZ-F-D[1] • 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.

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.

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.

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 15.2(2)SNH1 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 15.2(2)SNH1, RELEASE
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Wed 10-Oct-12 19:48 by prod_rel_team
```

New and Changed Information

New Hardware Features in Release 15.2(2)SNH1

The Cisco IOS Release 15.2(2)SNH1 introduces four new variants of the Cisco ASR 901 10G Series Aggregation Services Router. The four SKUs of the router are as follows:

- A901-6CZ-FT-D (Ethernet + TDM with DC Power)
- A901-6CZ-FT-A (Ethernet + TDM with AC Power)
- A901-6CZ-F-D (Ethernet only with DC Power)
- A901-6CZ-F-A (Ethernet only with AC Power)

For more details about the Cisco ASR 901 10G router, see the *Cisco ASR 901 10G Series Aggregation Services Router Hardware Installation Guide*.

New Software Features in Release 15.2(2)SNH1

The following features are supported from this release:

ACL-based QoS

The access control list (ACL) based QoS feature provides classification based on source and destination IP. The current implementation of this feature supports only named ACLs.

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

Inverse Multiplexing over ATM

The Inverse Multiplexing over ATM (IMA) technology is used to transport ATM traffic over a bundle of T1 or E1 cables, known as IMA group. This technology provides a scalable and cost-effective solution to expand WAN bandwidth from T1 speeds, without having to go for DS3 or OC3 circuits. With IMA, you can bundle two or more T1 circuits to effectively gain upward of 3 Mbps speed.

For more information about this feature, see *Inverse Multiplexing over ATM* guide at the following URL:

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

Layer 2 Control Protocol Tunneling

The Layer 2 Control Protocol Tunneling (L2PT) allows tunneling of Ethernet protocol frames across layer 2 switching domains.

For more information about this feature, see *Layer 2 Control Protocol Peering, Forwarding and Tunneling* guide at the following URL:

http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/l2pt.html

TDM Local Switching

The Time-Division Multiplexing (TDM) local switching in E1 mode is supported from Cisco IOS Release 15.2(2)SNH1 onwards. This feature allows switching of Layer 2 data between two circuit emulation (CEM) interfaces on the same router.

For more information about this feature, see *Pseudowire* guide at the following URL:

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

Modified Software Features in Release 15.2(2)SNH1

This section lists the features modified for this release:

Software Licensing

The 10gigUpgrade and Gige4portflexi licenses are available from Cisco IOS Release 15.2(2)SNH1 onwards. The 10gigUpgrade license is required to enable new 10G ports in the Cisco ASR 901 10G router. This license enables the router to function in 1G mode or 10G mode. The Gige4portflexi license is a combination of copper and SFP ports. This license is not tied to any port type.

For more information about this feature, see *Licensing* guide at the following URL:

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

Configuring Ethernet Virtual Connections

The restrictions section of the Ethernet Virtual Connections feature is updated.

For more information about the update, see *Configuring Ethernet Virtual Connections* guide at the following URL:

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

Limitations and Restrictions

Cisco IOS Release 15.2(2)SNH1 for the Cisco ASR 901 Series Aggregation Services Router has the following general limitations and restrictions:

Note For limitations and restrictions that are specific to features, see the respective feature guide.

- QinQ configuration for Layer3 is not possible with pop1 rewrite. However pop2 configured routed QinQ is supported.
- Default xconnect MTU is 9216.
- For interoperability with other routers for an xconnect session, ensure that the MTU on both PE routers is same before the xconnect session is established.
- VLAN IDs 4093, 4094, and 4095 are reserved for internal usage.

ACL

- Loopback feature should not be enabled when L2 Control Protocol Forwarding is enabled.
- Following IOS keywords are not supported on Cisco ASR 901—match-any, ip-options, logging, icmp-type/code, igmp type, dynamic, reflective, evaluate.
- Ingress PACL and RACL supports TCP/UDP port range; Egress ACL does not support port range.
- Sharing access lists across interfaces is not supported.
- ACL is not supported on Management port (FastEthernet) and serial interfaces.
- Devices in the management network (network connected to Fast Ethernet port) cannot be accessed from any other port. If the default route is configured on Cisco ASR 901 to fast ethernet interface (Fa0/0), all the routed packets will be dropped. However, this configuration could keep CPU busy and affect overall convergence.

Clocking

- External interfaces like BITS and 1PPS have only one port—they work either as an input interface or output interface at a given time.
- The *line to external* option for external SSU is not supported.
- ToD is not integrated to the router system time. ToD input or output reflects only the PTP time, not the router system time.
- Revertive and non-revertive modes work well only with two clock sources.
- BITS cable length option is supported via **`platform timing bits line-build-out`** command.
- There is no automatic recovery from OOR Alarms. It has to be manually cleared using **`clear platform timing oor-alarms`** command.
- If copper Gigabit Ethernet port is selected as the input clock source, the link should be configured as a IEEE 802.3 link-slave, using **`synce state slave`** command.
- BITS reports LOS only for AIS, LOS and LOF alarms.
- Loop timing is not supported in E1/T1 controllers. (IOS Command—**`clock source line`**). However, the clock can be recovered from T1/E1 lines and used to sync system clock using the IOS command **`network-clock input-source <prio> controller <E1/T1> 0/x.`**

IEEE 1588v2 (PTP)

- Ordinary clock slave and master mode is supported.
- Unicast Direct and Unicast Negotiation modes are supported; Multicast mode is not supported.
- PTP slave supports both single and two-step modes. PTP master supports only two-step mode.
- VLAN 4093 is used for internal PTP communication; do not use 4093 in your network.
- Loopback interface is used in Cisco ASR 901 router instead of ToP interface for configuring 1588 interface/IP address.
- The **`output 1pps`** command is not supported. Alternately, you can use the **`no input 1pps`** command.
- Sync and Delay request rates should be above 32pps, the optimum value being 64pps.
- Clock-ports even when configured as slave-only, start off as master. So the initial or reset state of the clock always shows as master. This implies that the master should have higher priority (priority1, priority2) for the slave to accept the master.

Supported Hardware

Table 3 shows the SFP modules supported on the Cisco ASR 901 Router:

Table 3 SFPs Supported on the Cisco ASR 901 Router

• CWDM-SFP-1470	• GLC-T
• CWDM-SFP-1490	• GLC-ZX-SM
• CWDM-SFP-1510	• GLC-ZX-SMD
• CWDM-SFP-1530	• GLC-ZX-SM-RGD
• CWDM-SFP-1550	• SFP-10G-ER
• CWDM-SFP-1570	• SFP-10G-LR
• CWDM-SFP-1590	• SFP-10G-LR-X
• CWDM-SFP-1610	• SFP-10G-SR
• DWDM-SFP-XXXX[1]	• SFP-10G-SR-X
• GLC-BX-U and GLC-BX-D[2]	• SFP-10G-ZR
• GLC-EX-SMD	• SFP-GE-L
• GLC-LH-SMD	• SFP-GE-S
• GLC-LX-SM-RGD	• SFP-GE-T
• GLC-SX-MMD	• SFP-GE-Z
• GLC-SX-MM-RGD	

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.

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-SNAPSHOT-MIB
- CISCO-SNMP-TARGET-EXT-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
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-FLASH-MIB
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-IP-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-TS-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-SMI-MIB
- NOTIFICATION-LOG-MIB
- UDP-MIB
- OSPF-MIB
- PerfHist-TC-MIB
- RFC1213-MIB
- RMON2-MIB
- RMON-MIB
- SNMP-FRAMEWORKMIB
- SNMP-TARGET-MIB
- SNMPv2-MIB
- SNMPv2-SMI
- SNMPV2-TC
- TCP-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:

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 15.2(2)SNH1, choose **15.2** from the first drop-down list, **2** from the second drop-down list, and **SNH1** 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 15.2(2)SNH1, 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 15.2(2)SNH1.

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.
CSCtn32463	There is no command restriction in applying a service policy to Ethernet Virtual Connection (EVC) on the egress.
CSCtn71094	The **no int vlan 1** command deletes VLAN 1.
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.
CSCts80072	The MPLS forwarding-table counters are not getting incremented.
CSCts80090	Reserved VLANs are not blocked.
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.
CSCtw98202	IP service-level agreement (SLA) echo and jitter is not supported over xconnect.
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.

Bug ID	Description
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.
CSCty27927	The bandwidth remaining percent limits traffic to configured value. To configure QoS scheduler, use the **qos-config scheduling-mode Min-BW-Guarantee** command under the interface where the queuing policy is configured. This command allows the per-class rate to use any unutilized bandwidth beyond the configured minimum guaranteed bandwidth.
CSCty95886	The file copy function is not detecting errors properly.
CSCtz09377	Some virtual circuits are going down when several xconnect sessions with Connectivity Fault Management (CFM) is configured.
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.
CSCtz69403	IPv6 traffic is not getting dropped with link-local as source address.
CSCtz82423	The copper small form-factor pluggable (SFP) link is not coming up during online insertion.
CSCtz82918	IPv6 addresses are not sent in addresses Cisco Discovery Protocol (CDP) TLV.
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.

Bug ID	Description
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.
CSCua60361	The 6PE related commands should be hidden, as they are not supported.
CSCua81678	The following error message is displayed for /128 prefix: “Reached Maximum Number of IPv6 Hosts”.
CSCua84571	Load balancing is not working with different streams having symmetrical addresses.
CSCua88693	The **verify** command is not supported on usbflash0 device. Workaround: Copy the file to “flash” file system; verify the image, and then copy the file to usbflash.
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.
CSCub17763	The IMA interface is not coming up.
CSCub56206	The egress object is missing from SVI interface after reload of the router.
CSCub71746	Alarm Indication Signal (AIS) is visible momentarily at T1 controller of CE1 while reverting back to primary.

Bug ID	Description
CSCuc15639	Connectivity Fault Management (CFM) session, with 100ms continuity-check interval, is not stable.
CSCuc22630	The router fails to recognize USB when its removed immediately after insertion. Workaround: After inserting the USB, wait for a few seconds, and then remove it.
CSCuc38512	It is not possible to compress the file system when the last file is deleted. Workaround: Back up all the files to TFTP server or USB device and erase the file system. This will reclaim the deleted file space.
CSCuc38706	The router may hang or reset if an IOS file is not specified in the **boot system flash usbflash0:** command. Workaround: Ensure that proper IOS file is present in the usbflash0 device and the file name is mentioned.
CSCuc62493	The GLC-ZX-SMD SFP is not getting detected in 10G AC (A901-6CZ-Fx-A) SKUs.

Closed Caveats

This section provides information about the closed caveats for the Cisco ASR 901 router running Cisco IOS Release 15.2(2)SNH1.

Bug ID	Description
CSCtg47129	The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication. Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link: http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html
CSCtr66435	The counters are showing incorrect values for Layer 2 NNI and User-to-Network Interface (UNI) interfaces.
CSCts78165	Reconfiguring EVCs of mixed type on a GigabitEthernet interface fails.
CSCts82314	Junk values are displayed for class-default counters.
CSCtt28873	The configuration validation routine is not covering all illogical configurations.
CSCtw77870	QoS assertion fails and traceback is observed after deleting the policy-map attached to a MLPPP interface.
CSCtx14499	Traceback occurs after issuing **show license status** and **license save** commands.
CSCty04056	Error occurs while trying to clear the Onboard Failure Logging (OBFL) information.
CSCty77530	802.1Q Tunneling (QinQ) is not able to support multiple NNI ports.
CSCtz27856	Layer 2 traffic is failing with QinQ encapsulation between NNI interfaces over EVC.

Bug ID	Description
CSCua84167	The link connected over GigabitEthernet 0/11 is not coming up.
CSCub02378	PTP is not working after reloading the master/slave router.

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*

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 15.2(2)SNH1