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

August 2012

OL-27680-01

This release notes is for the Cisco ASR 901 Series Aggregation Services Router for Cisco IOS Release 15.2(2)SNG 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 radio access network (RAN). The Cisco ASR 901 includes the following models:

- Cisco ASR 901 Router TDM version (A901-12C-FT-D, A901-4C-FT-D)
- Cisco ASR 901 Router Ethernet version (A901-12C-F-D, A901-4C-F-D)

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

Note Cisco ASR 901 models A901-4C-FT-D and A901-4C-F-D 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 1 lists the supported system configurations for Cisco ASR 901 router:

Memory Details

Table 1 lists the memory available for Cisco ASR 901 router.

Table 1 Cisco IOS Release 15.2(2)SNG 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)SNG, RELEASE
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Fri 17-Aug-12 19:48 by prod_rel_team
```

New and Changed Information

New Hardware Features in Release 15.2(2)SNG

There are no new hardware features in Cisco IOS Release 15.2(2)SNG.

New Software Features in Release 15.2(2)SNG

Cisco ASR 901 router supports the following features from this release:

Bit Error Rate Testing

The BERT feature is used to test the integrity of the physical layer. BERT generates a specific pattern on to the egress data stream of a E1/T1 controller and then analyzes the ingress data stream for the same pattern. The bits that do not match the expected pattern are counted as bit errors.

For more information about this feature, see the *Bit Error Rate Testing* guide at the following URL:
http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/bert.html

Data Collection Manager

This feature provides the ability to periodically transfer selected MIB data from Cisco IOS-based devices to specified Network Management Stations (NMS). The data from multiple MIBs can be grouped into lists, and a polling interval (frequency of data collection) can be configured. All the MIB objects in a list are periodically polled using this specified interval. The collected data from the lists can then be transferred to a specified NMS at a user-specified transfer interval (frequency of data transfer) using TFTP, RCP, or FTP.

For more information about this feature, see *Data Collection Manager* guide at the following URL:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/gdatacol.html#wp1053845

DHCP Client on SVI

DHCP helps you to dynamically and transparently assign reusable IP addresses to clients. The DHCP client retrieves the host information from the DHCP server and configures the SVI interface of the Cisco ASR 901 router. If the DHCP server cannot give the DHCP client the requested configuration parameters from its database, it forwards the request to one or more secondary DHCP servers defined by the network administrator.

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

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

Dying Gasp

ASR901 sends the Dying Gasp PDUs on all the ethernet interfaces on loss of power. This helps neigbouring device to detect the neighbour is down and indicate the management stations. The device rely on short term capacitance which allows the device to function for 8-10ms and send these OAM PDUs.

For more information about this feature, see *Configuring Ethernet OAM* guide at the following URL:

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

Embedded Event Manager Script

Cisco Embedded Event Manager (EEM) has the ability to register with IOS components for specified conditions or thresholds. When those conditions or thresholds occur, EEM is notified and it has to take action. EEM is used to send out notifications through email, syslog, or trap and also takes care of the corrective actions. This can improve network availability by detecting the conditions before an operations staff usually detects the problem, and in some cases it can restore connectivity to the device itself.

For more information about this feature, see *EEM Configuration for Cisco Integrated Services Router Platform* guide at the following URL:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6815/config_guide_eem_configuration_for_cisco_integrated_services_router_platforms.html

Layer 2 Control Protocol Peering and Forwarding

Support was introduced for layer 2 peering and forwarding functionality.

The **l2proto-forward** command was introduced.

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

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

Link Layer Discovery Protocol

To permit the discovery of non-Cisco devices, Cisco ASR 901 supports a vendor-neutral device discovery protocol that is defined in the IEEE 802.1ab standard. Link Layer Discovery Protocol (LLDP) allows network devices to advertise information about themselves to other devices on the network.

For more information about this feature, see *Configuring Link Layer Discovery Protocol* guide at the following URL:

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

Ethernet Loopback

You can use per-port and per VLAN Ethernet loopback to test connectivity at initial startup, to test throughput, and to test quality of service. RFC2544 Latency Testing specifies that the throughput must be measured by sending frames at increasing rate, presenting the percentage of frames received, and reporting the frames dropping rate. This rate is dependent on the frame size. This throughput measurement at traffic generator requires the Ethernet loopback support on the responder.

For more information about this feature, see *Configuring Ethernet OAM* guide at the following URL:

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

Hot Standby Router Protocol and Virtual Router Redundancy Protocol Support

The Hot Standby Router Protocol (HSRP) is a First Hop Redundancy Protocol (FHRP) designed to allow for transparent fail-over of the first-hop IP router. HSRP provides high network availability by providing first-hop routing redundancy for IP hosts on Ethernet, Fiber Distributed Data Interface (FDDI), Bridge-Group Virtual Interface (BVI), LAN Emulation (LANE), or Token Ring networks configured with a default gateway IP address. HSRP is used in a group of routers for selecting an active router and a standby router.

The Virtual Router Redundancy Protocol (VRRP) is an election protocol that dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing several routers on a multi-access link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN.

For more information about this feature, see *Configuring HSRP and VRRP* guide at the following URL:

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

IPv6 Support

IPv6 is introduced on the Cisco ASR 901 router to support Long Term Evolution (LTE) rollouts that provides high-bandwidth data connection for mobile wireless devices. The Cisco ASR 901 router supports IPv6 addressing on Switch Virtual Interface (SVI) and Loopback interfaces.

The CISCO-CONFIG-COPY-MIB and CISCO-FLASH-MIB are supported for IPv6 addressing when either TFTP remote copy protocol (rcp), or FTP is used.

The CISCO-SNMP-TARGET-EXT-MIB was added for the IPv6 over SNMP support feature.

The following MIBs have been modified for the IPv6 over SNMP support feature:

- CISCO-FLASH-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-CONFIG-COPY-MIB

The following features are included in the IPv6 support:

- IPv6 Specification (RFC 2460)
- ICMPv6 (RFC 4443)
- IPv6 Duplicate Address Detection (RFC 4429)
- IPv6 Neighbor Discovery (RFC 4861)
- IPv6 Stateless Address Auto-configuration (RFC 4862)
- IPv4/IPv6 Dual Stack (both IPv4 and IPv6 addressing/forwarding on same VLAN)
- IPv6 Static Routing
- OSPFv3 for IPv6 (RFC 5340)
- IS-IS for IPv6 (RFC 5308)
- Multiprotocol-BGP for IPv6
- BFDv6 (Bidirectional Forwarding Detection for IPv6)+Static (RFC 5881)

- BFDv6+OSPFv3
- BFDv6+BGP
- IPv6 Statistics on interfaces and CLI show commands counters on par with IPv4 counters

For more information about IPv6 Support, see the *IPv6 Support on the Cisco ASR 901 Router* guide at the following URL:
http://www.cisco.com/en/US/docs/wireless/asr_901/Configuration/Guide/ipv6_on_asr901.html

Labeled BGP Support

This feature describes how to add label mapping information to the Border Gateway Protocol (BGP) message that is used to distribute the route on the Cisco ASR 901 Series Aggregation Services Routers. The ASR 901 router also supports the virtual private network (VPN) and virtual routing and forwarding (VRF) over Labeled BGP functionality.

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

Multihop BFD Support

The multihop BFD feature provides subsecond forwarding failure detection for a destination with more than one hop and up to 255 hops. A multihop BFD session is set up between a unique source-destination address pair provided by the client. A session can be set up between two endpoints that have IP connectivity.

The following commands were introduced or modified:

- **bfd-template**
- **bfd map**

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

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

MPLS Traffic Engineering: Fast Reroute Link Protection

This feature describes the Fast Reroute (FRR) link protection and Bidirectional Forwarding Detection (BFD)-triggered FRR feature of Multiprotocol Label Switching (MPLS) traffic engineering (TE). The MPLS TE is supported on the Cisco ASR 901 router to enable only the FRR. The traffic engineering aspects of MPLS TE is currently not supported.

The **asr901-platf-frr enable** command was introduced.

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

Remote Network Monitoring

The Remote Monitoring (RMON) identifies the activity on individual nodes and allows you to monitor all the nodes and their interaction on a LAN segment. RMON allows you to view the traffic that flows through the router and the segment traffic when it has the Simple Network Management Protocol

(SNMP) agent in a router. Combining RMON alarms and events (classes of messages that indicate traffic violations and various unusual occurrences over a network) with existing MIBs allows you to choose where proactive monitoring will occur.

For more information about this feature, see *Configuring RMON Support* feature guide at the following URL: http://www.cisco.com/en/US/docs/ios/12_1/configfun/configuration/guide/fcd301b.html

SNMPv3 Support

Simple Network Management Protocol Version 3 (SNMPv3) is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network.

The security features provided in SNMPv3 are:

- Message integrity—Ensuring that a packet has not been tampered with in-transit.
- Authentication—Determining the message is from a valid source.
- Encryption—Scrambling the contents of a packet to prevent it from being seen by an unauthorized source.

For more information about this feature, see *SNMPv3* feature guide at the following URL: http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html

Two-Way Active Measurement Protocol Responder

The TWAMP-Control protocol is used to start performance measurement sessions. The TWAMP test is used to send and receive performance-measurement probes. You can deploy TWAMP in a simplified network architecture, with the control-client and the session-sender on one device and the server and the session-reflector on another device.

The following commands were introduced or modified:

- **ip sla responder twamp**
- **ip sla server twamp**
- **port**
- **timeout**
- **timer inactivity**
- **show ip sla standards**
- **show ip sla twamp connection detail**
- **show ip sla twamp connection requests**
- **show ip sla twamp session**

For more information about this feature, see *Cisco IOS IPSLA* feature guide at the following URL:

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

Limitations and Restrictions

Cisco IOS Release 15.2(2)SNG 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 (Fast Ethernet) 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

The Cisco ASR 901 router supports the following SFP modules:

- GLC-LX-SM-RGD
- GLC-SX-MM
- GLC-SX-MM-RGD
- GLC-ZX-SM
- GLC-ZX-SM-RGD
- GLC-T
- GLC-FE-100FX-RGD
- SFP-GE-L
- SFP-GE-S
- SFP-GE-Z
- SFP-GE-T
- SFP-LX-SM
- SFP-SX-MM

SFPs supported from Cisco IOS Release 15.2(2)SNG

Cisco IOS Release 15.2(2)SNG introduces support for the following SFPs:

- GLC-BX-U and GLC-BX-D (The SFP GLC-BX-U and GLC-BX-D should be connected back to back to bring the interface link up.)
- GLC-EX-SMD
- GLC-LH-SMD
- GLC-SX-MMD
- GLC-ZX-SMD
- CWDM-SFP-1470
- CWDM-SFP-1490

- CWDM-SFP-1510
- CWDM-SFP-1530
- CWDM-SFP-1550
- CWDM-SFP-1570
- CWDM-SFP-1590
- CWDM-SFP-1610
- DWDM-SFP-XXXX (40 wavelengths)

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-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

- CISCO-FLASH-MIB
- CISCO-IETF-BFD-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
- CISCO-PTP-MIB
- CISCO-QUEUE-MIB
- CISCO-RESILIENT-ETHERNET-PROTOCOL-MIB
- CISCO-RTTMON-MIB
- CISCO-SMI-MIB
- NOTIFICATION-LOG-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
- OSPF-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:

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)SNG, choose **15.2** from the first drop-down list, **2** from the second drop-down list, and **SNG** 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)SNG, 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 12.

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 12.

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)SNG.

Bug ID	Description
CSCtk33675	The service instance configuration is rejected when the encapsulation is set to default for double-tagged traffic.
CSCtl19081	Unconfiguring the network node interface (NNI) port fails. The configuration remains intact and traffic flows without interruption.
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 the 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.
CSCtr66435	The counters are showing incorrect values for Layer 2 NNI and User-to-Network Interface (UNI) interfaces.
CSCtr70228	High CPU utilization is observed while performing save or copy operation.
CSCts66081	Ingress VLAN translation failure occurs when entries exceed 3000.
CSCts78165	Reconfiguring EVCs of mixed type on a GigabitEthernet interface fails.
CSCts80072	The MPLS forwarding-table counters are not getting incremented.
CSCts80090	Reserved VLANs are not blocked.

Bug ID	Description
CSCts82314	Junk values are displayed for class-default counters.
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.
CSCtt14439	The **ping** command fails when all member links are moved from one Multilink Point-to-Point (MLPPP) group to another.
CSCtt28873	The configuration validation routine is not covering all illogical configurations.
CSCtw52497	The interface drops all ingress packets when you reload the router with write erase, and copy the saved configuration to the running configuration.
CSCtw77870	QoS assertion fails and traceback is observed after deleting the policy-map attached to a MLPPP interface.
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.
CSCtx14499	Traceback occurs after issuing **show license status** and **license save** commands.
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.
CSCty04056	Error occurs while trying to clear the Onboard Failure Logging (OBFL) information.
CSCty04070	Traffic fails and continuous traceback is observed, when xconnect is configured on an untagged EVC.
CSCty77530	802.1Q Tunneling (QinQ)is not able to support multiple NNI ports.
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) are configured.
CSCtz16522	The Two-Way Active Measurement Protocol (TWAMP) session-reflector packet truncation fails.

Bug ID	Description
CSCtz27856	Layer 2 traffic is failing with QinQ encapsulation between NNI interfaces over EVC.
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 P rotocol (HSRP) and Virtual Redundancy Router Protocol (VRRP). With this configuration, we support a maximum of 50 sessions.
CSCtz67224	Point-to-Point Protocol (PPP) process stops running.
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.
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.
	`nterface 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 seen when the 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 ASR 901 platform currently doesnot support the MPLS traffic engineering counters.
CSCua51628	The OSPFv3 bidirectional forwarding detection (BFD) flap upon shut on one interface in port-channel bundle.
CSCua60361	6PE related commands need to be hidden.

Bug ID	Description
CSCua81678	Getting the “Reached Maximum Number of IPv6 Hosts” message for /128 prefix.
CSCua84167	The link connected over GigabitEthernet 0/11 is not coming up.
CSCua84571	Load balancing is not working with different streams having symmetrical addresses.
CSCua98165	The IPv6 BFD packets need to 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.
CSCub02378	PTP is not working after reloading the master/slave router.
CSCub12715	The following message is displayed: “pura_cef_ipv6_route_create_update:Reached Maximum Number of Prefixes supported by platform.Additional Prefixes will not be programmed.”
CSCub56206	The egress object is missing from SVI interface after reload of the router.

Closed Caveats

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

Bug ID	Description
CSCts85351	The BITS T1 port configured as OUT sends wrong frame type.
CSCtt20958	An Out Of Range (OOR) alarm is reported on the E1 line network clock source after clearing the Loss of Framing (LoF) alarm.
CSCtt35379	Cisco IOS Software contains a vulnerability in the Border Gateway Protocol (BGP) routing protocol feature. The vulnerability can be triggered when the router receives a malformed attribute from a peer on an existing BGP session. Successful exploitation of this vulnerability can cause all BGP sessions to reset. Repeated exploitation may result in an inability to route packets to BGP neighbors during reconvergence times. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-bgp

Bug ID	Description
CSCtw84664	A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload. Affected devices must be configured to process SIP messages and for pass-through of Session Description Protocol (SDP) for this vulnerability to be exploitable. Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerability. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip
CSCtx41514	The router crash information is not dumped due to machine check exception.
CSCty27927	Bandwidth remaining percent limits traffic to configured value. To configure QoS scheduler, use the **qos-config scheduling-mode Min-BW-Guarantee** command under the 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.
CSCty58300	Cisco IOS Software contains a vulnerability in the Border Gateway Protocol (BGP) routing protocol feature. The vulnerability can be triggered when the router receives a malformed attribute from a peer on an existing BGP session. Successful exploitation of this vulnerability can cause all BGP sessions to reset. Repeated exploitation may result in an inability to route packets to BGP neighbors during reconvergence times. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-bgp

Bug ID	Description
CSCty96049	Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a single DHCP packet to or through an affected device, causing the device to reload. Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcp
CSCtz71758	The Remote Alarm Indication (RAI) alarm is not sent out by the router for T1 circuits, when a T1 circuit receives or detects Alarm Indication Signal (AIS) or Loss Of Framing (LOF) or Loss Of Signal (LOS) alarms.

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)SNG