Release Notes for Cisco ASR 901 Series Aggregation Services Router for Cisco IOS Release 15.1(2)SNI1

June 2012

OL-27551-01

This release notes is for the Cisco ASR 901 Series Aggregation Services Router for Cisco IOS Release 15.1(2)SNI1, 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 router 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 are introduced in Cisco IOS Release 15.1(2)SNI, with 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 HSPA or 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

Memory Details

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

Table 1 Cisco IOS Release 15.1(2)SNI1 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 15.1(2)SNI1, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Tue 08-May-12 12:09 by prod_rel_team
```

New and Changed Information

New Hardware Features in Release 15.1(2)SNI1

There are no new hardware features in Release 15.1(2)SNI1.

New Software Features in Release 15.1(2)SNI1

There are no new software features in Release 15.1(2)SNI1.

Limitations and Restrictions

Cisco IOS Release 15.1(2)SNI1 for the Cisco ASR 901 has the following limitations and restrictions:

- QinQ configuration for layer 3 is possible only with rewrite pop2 symmetric.
- Layer 2 forwarding is not supported in QinQ configuration, with rewrite pop2 symmetric.
- 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.
- Bridge Domain IDs 4093, 4094, and 4095 are reserved for internal usage.
- In a default configuration, Cisco ASR 901 does not run any spanning-tree protocol. Therefore, all the ports participating in bridge domains are moved to the forward state. To enable MSTP, use the **spanning-tree mode mstp** command in the global configuration mode.
- Cisco ASR 901 does not support VRF on TDM interfaces.

ACL

- 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 work if the encapsulation VLAN id and the bridge domain number are different.
- 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)

- Only ordinary clock is supported.
- Unicast Direct and Unicast Negotiation modes are supported; Multicast mode is not supported.
- Single and two-step modes are supported.
- 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.
- When you configure a loopback address on an interface, make sure that this loopback interface is reachable (using ICMP ping) from remote locations, before assigning the interface to PTP. Once the interface is assigned to PTP, it does not respond to ICMP pings.

T1 Local Switching

- Autoprovisioning is not supported.
- Out-of-band signaling is not supported.
- Port mode local switching is not supported on the CEM interface.
- Interworking with other interface types is not supported.
- The same CEM circuit cannot be used for both local switching and xconnect.
- You cannot use CEM local switching between two CEM circuits on the same CEM interface.

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
- GLC-LH-SM
- GLC-BX-D
- SFP-GE-L
- SFP-GE-S
- SFP-GE-Z
- SFP-GE-T
- SFP-LX-SM
- SFP-SX-MM

For information about 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:

- CISCO-CDP-MIB
- CISCO-CEF-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB
- CISCO-FLASH-MIB
- CISCO-IETF-PW-MIB
- CISCO-IF-EXTENSION-MIB
- CISCO-IMAGE-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-EIGRP-MIB
- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-MIB
- CISCO-RTTMON-MIB
- CISCO-NTP-MIB
- CISCO-SMI-MIB
- CISCO-OAM-MIB
- CISCO-SYSLOG-MIB
- CISCO-CLASS-BASED-QOS-MIB
- CISCO-QUEUE-MIB
- CISCO-CAR-MIB
- CISCO-CAS-IF-MIB
- CISCO-ENTITY-ASSET-MIB
- CISCO-ENVMON-MIB
- ENTITY-MIB
- IANAifType-MIB
- IEEE8021-CFM-MIB
- IF-MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-IP-MIB
- OLD-CISCO-TS-MIB
- CISCO-SNAPSHOT-MIB
- CISCO-PING-MIB
- SNMP-TARGET-MIB
- SNMPv2-CONF
- SNMPv2-MIB
- SNMPv2-SMI
- BGP4-MIB
- OSPF-MIB
- CISCO-OSPF-MIB
- CISCO-STP-EXTENSIONS-MIB
- IP-MIB
- TCP-MIB
- UDP-MIB
- EtherLike-MIB
- BRIDGE-MIB
- INT-SERVE-MIB
- CISCO-RESILIENT-ETHERNET-PROTOCOL-MIB
- EOAM-MIB
- CISCO-NETSYNC-MIB
- CISCO-PTP-MIB
- HCNUM-TC
- PerfHist-TC-MIB
- MPLS-LSR-MIB
- MPLS-LDP-MIB
- MPLS-VPN-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. In the severity 3 category, only select few 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 tool kit. This section explains how to use the bug toolkit and has the following topics:

Search Bugs

The following steps explain 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 15.1(2)SNI1, choose **15.1** from the first drop-down list, **2** from the second drop-down list, and **SNI1** 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 12.2(33)SCD, 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

Complete these steps 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 dialog box 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

Complete these steps to save your search.

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 dialog box 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

Complete these steps 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 the **Export All to Spreadsheet** link in the Search Results page under the Search Bugs tab. Specify a file name and folder name to save the spreadsheet to. All the bugs retrieved by the search are exported.
- Click the **Export All to Spreadsheet** link in the My Notifications tab. Specify a file name and folder name to save the spreadsheet to. All the saved bugs in all the groups are 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 15.1(2)SNI1 and later.

There are no new open caveats for Cisco IOS Release 15.1(2)SNI1.

Resolved Caveats

This section provides information about the resolved caveats for the Cisco ASR 901 router running Cisco IOS Release 15.1(2)SNI1 and later.

Bug ID	Description
CSCua08019	When Cisco ASR901 router was power cycled, NVRAM boot sector got corrupted and the router went to the rommon prompt.

Troubleshooting

Collecting Data for Router Issues

To collect data for reporting router issues, use 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, use 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 Command Reference

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 15.1(2)SNI1