Release Notes for Cisco ASR 901 Series Aggregation Services Router for Cisco IOS Release 615.6(2)SP6

First Published Date: April 15, 2019

This release notes is for the Cisco ASR 901 Series Aggregation Services Router for Cisco IOS Release 15.6(2)SP6 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.

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

Cisco Systems, Inc.
www.cisco.com

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 1G Router model versions.

Table 1   *Cisco ASR 901 1G Router Models*

Power Source	TDM + Ethernet Version	Ethernet Version
DC Power	• A901-12C-FT-D • A901-4C-FT-D	• A901-12C-F-D • A901-4C-F-D
AC Power	• none	• none

Table 2 lists the Cisco ASR 901 10G Router model versions.

Table 2   *Cisco ASR 901 10G Router Models*

Power Source	TDM + Ethernet Version	Ethernet Version
DC Power	• A901-6CZ-FT-D	• A901-6CZ-F-D • A901-6CZ-FS-D
AC Power	• A901-6CZ-FT-A	• A901-6CZ-F-A • A901-6CZ-FS-A

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 and Memory Details

Table 3 lists the supported system configurations and memory details for the Cisco ASR 901 router:

Table 3   *Cisco IOS Release 15.6(2)SP6 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
Cisco ASR 901 Series Aggregation Services Router, IPsec enabled Ethernet version	asr901sec-universalk9.mz	256 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:

The following example shows output from Cisco ASR 901 router that supports normal IOS software.

```
ASR901_1> show version
Cisco IOS Software, 901 Software (ASR901-UNIVERSALK9-M), Version 15.6(2)SP3, RELEASE
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 14-Apr-19 16:09 by prod_rel_team

ROM: System Bootstrap, Version 15.6(3r)SP6, RELEASE SOFTWARE (fc1)
```

The following example shows output from Cisco ASR 901 Series Aggregation Services Router, IPsec enabled Ethernet version.

```
SANR1> show version
Cisco IOS Software, 901 Software (ASR901SEC-UNIVERSALK9-M), Version 15.6(2)SP3, RELEASE
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 14-Apr-19 16:29 by prod_rel_team

ROM: System Bootstrap, Version 15.6(3r)SP6, RELEASE SOFTWARE (fc1)
```

New and Changed Information

New Hardware Features in Release 15.6(2)SP6

There are no new hardware features in this release.

New Software Features in Release 15.6(2)SP6

There are no new hardware features in this release.

Modified Software Features in Release 15.6(2)SP6

There are no modified features in this release.

Supported Hardware

Table 4 and Table 5 shows the SFP modules supported on the Cisco ASR 901 routers:

Important Notes

- 10G SFPs inserted into 1GE port provides 1GE speed.

- 10G SFPs inserted into 10GE port without a valid license provides only 1GE speed.

- 100M SFP works only with **no negotiation auto** command.

- If 1G SFP is used to connect a 10G port to a 1G port, you do not have to explicitly configure the **no negotiation auto** command to bring up the link.

- Effective with Cisco IOS Release 15.4(3)S, the auto-select feature is supported on 100M SFPs. However, this feature is not supported on combo ports.

- Remote Fault Indication feature is not applicable for 1G mode in 10GE ports. It applies only to 10G mode in 10GE ports.

- By default dual rate SFP works in 1G mode, to make it work in 100M mode, "no negotiation auto" should be configured.

- Dual rate SFP can be configured in 100M mode when inserted in 1G ports only.

- Dual rate SFP when inserted in 10G ports will work in 1G mode only.

Table 4   SFPs Supported on the Cisco ASR 901 1G and 10G Routers for 1G Mode

• CWDM-SFP-1470	• GLC-SX-MM-RGD
• CWDM-SFP-1490	• GLC-T
• CWDM-SFP-1510	• GLC-ZX-SM
• CWDM-SFP-1530	• GLC-ZX-SMD
• CWDM-SFP-1550	• GLC-ZX-SM-RGD
• CWDM-SFP-1570	• SFP-GE-L
• CWDM-SFP-1590	• SFP-GE-S
• CWDM-SFP-1610	• SFP-GE-T
• CWDM SFP+	• SFP-GE-Z
• DWDM-SFP-XXXX[1]	• GLC-BX40-D-I
• GLC-BX-U and GLC-BX-D[2]	• GLC-BX40-DA-I
• GLC-EX-SMD	• GLC-BX40-U-I
• GLC-LH-SMD	• GLC-BX80-D-I
• GLC-LX-SM-RGD	• GLC-BX80-U-I
• GLC-SX-MMD	• GLC-GE-DR-LX

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 5   SFPs Supported on the Cisco ASR 901 10G Router for 10G Mode

• SFP-10G-ER	• SFP-10G-ZR
• SFP-10G-LR	• SFP-10G-LRM
• SFP-10G-LR-X	• SFP-H10GB-ACU7M
• DWDM-SFP+	• SFP-H10GB-ACU10M
• SFP-H10GB-CU1M	• SFP-10G-BX-D-I
• SFP-H10GB-CU3M	• SFP-10G-BX-U-I
• SFP-H10GB-CU5M	• SFP-10G-BX40-D-I
• SFP-10G-SR	• SFP-10G-BX40-U-I
• SFP-10G-SR-X	

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

Supported MIBs

The Cisco ASR 901 router supports the following MIBs:

• BGP4-MIB	• CISCO-STP-EXTENSIONS-MIB
• BRIDGE-MIB	• CISCO-SYSLOG-MIB
• CISCO-ACCESSENVMON-MIB	• CISCO-TC
• CISCO-CAR-MIB	• ENTITY-MIB
• CISCO-CDP-MIB	• ETHERLIKE-MIB
• CISCO-CEF-MIB	• HCNUM-TC
• CISCO-CLASS-BASED-QOS-MIB	• IANAifType-MIB
• CISCO-CONFIG-COPY-MIB	• IEEE8021-CFM-MIB
• CISCO-CONFIG-MAN-MIB	• IF-MIB
• CISCO-DATA-COLLECTION-MIB	• IMA-MIB
• CISCO-DOT3-OAM-MIB	• INT-SERVE-MIB
• CISCO-EIGRP-MIB	• IP-FORWARD-MIB
• CISCO-ENHANCED-MEMPOOL-MIB	• IP-MIB

- CISCO-ENTITY-ALARM-MIB
- CISCO-ENTITY-ASSET-MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB
- CISCO-ENVMON-MIB
- CISCO-FLASH-MIB
- CISCO-IETF-PW-MIB
- CISCO-IETF-PW-TC-MIB
- CISCO-IF-EXTENSION-MIB
- CISCO-IMAGE-MIB
- CISCO-IPSLA-ETHERNETMIB
- CISCO-MEMORY-POOL-MIB
- CISCO-NETSYNC-MIB
- CISCO-NTP-MIB
- CISCO-OSPF-MIB
- CISCO-PING-MIB
- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-MIB
- 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

- MPLS-LDP-MIB
- MPLS-LSR-MIB
- MPLS-VPN-MIB
- NOTIFICATION-LOG-MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-FLASH-MIB
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-IP-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-TS-MIB
- OSPF-MIB
- OSPFv3-MIB
- PerfHist-TC-MIB
- RFC1213-MIB
- RMON2-MIB
- RMON-MIB
- SNMP-FRAMEWORKMIB
- SNMP-TARGET-MIB
- SNMPv2-MIB
- SNMPv2-SMI
- SNMPV2-TC
- TCP-MIB
- UDP-MIB
- CISCO-IPSEC-FLOW-MONITOR-MIB
- CISCO-IPSEC-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:

- Bug Search Tool
- Open Caveats
- Resolved Caveats

Bug Search Tool

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 Search Tool.

Use the following link to access the tool: https://tools.cisco.com/bugsearch/search

You will be prompted to log into Cisco.com. After successful login, the Bug Search Tool page opens. Use the Help link in the Bug Search Tool to obtain detailed help.

Open Caveats

There are no open caveats for the Cisco ASR 901 router running Cisco IOS Release 15.6(2)SP6.

Caveat ID Number	Description
CSCvp11753	When remote end of PW flaps, traffic via PW is stopped

Resolved Caveats

This section provides information about the resolved caveats for the Cisco ASR 901 router running Cisco IOS Release 15.6(2)SP6.

Caveat ID Number	Description
CSCux22473	IPv6 Tracking for route learned from IBGP Neighbor is Down.
CSCux68796	IOS-XE Router - High CPU When Handling get-next on "entStateStandby" MIB
CSCuz74957	Cisco IOS and IOS XE Software ISDN Interface Denial of Service Vulnerability
CSCuz99865	IPSec MIB queries returns wrong tunnel count
CSCva00765	crash after no ipv4 multicast multitopology command
CSCva64842	Observing kernel: EXT2-fs error while moving between polaris and MCP_DEV
CSCve56559	Incorrect Track Resolution Metric for GRE Tunnel

Caveat ID Number	Description
CSCve57830	SUBALTNAME DECODE fails for APIC_EM self-signed cert when validating server identity
CSCve89361	Crash in SISF while processing IPv6 packet
CSCvf11776	VRRPv3 with VRRS remains NOT READY after shutdown Port-channel IF.
CSCvf36269	Cisco IOS and IOS XE Software Network Plug-and-Play Certificate Validation Vulnerability
CSCvf73552	VRRP non-zero authentication data on 16.3.3
CSCvf96294	MIB counter for IPSec tunnels does not decrement under high tunnel scale and churn
CSCvg06142	'ipsm Tunnel Entry' and 'Crypto IKMP' memory leak due to IKE tunnel entry not deleted
CSCvg37952	Cisco IOS XE Software ISR4400 Series IPsec Denial of Service Vulnerability
CSCvh54672	VRRP doesnt work over Port-channel L3 interface
CSCvh72848	"no track resolution ip route" and "default track resolution ip route" not working
CSCvh83319	Interop vrrp doesnt work between cedge and vedge
CSCvi83306	Crash with IOSXE-WATCHDOG: Process = IPv6 RIB Event Handler
CSCvj02910	Reload removing ipv6 VRRP group
CSCvj61307	Cisco IOS XE Software Command Injection Vulnerability
CSCvj73544	ospf routing loop for external route with multiple VLINKs/ABRs
CSCvj86790	RIP does not send updates on unnumbered interfaces after reload of ISR 4k
CSCvj98575	Cisco IOS and IOS XE HSRPv2 Information Leak Vulnerability
CSCvk03910	OSPF neighbor stuck in loading after VSS switchover
CSCvk56331	Initial contact in IKEv1 phase 2 rekey (QM1) causes all crypto sessions to drop
CSCvk71047	Router fails to reserve necessary ports for VPN traffic (UDP 500 & 4500) for ISAKMP
CSCvm00765	BFD crash on imitating traffic loss
CSCvm02572	Router crashes on SSH connection with "login on-failure log" enabled
CSCvm28421	ASR901-ESMC padding is having non-zero random values which is causing duplicate QL-TLV
CSCvm40496	iBGP PE-CE When Route-Reflect enable VRF import all Route Target.
CSCvm51112	"clear crypto sa vrf MyVrf" triggers crash after updating pre-shared-keys
CSCvm55465	BGP updates missing ISIS advertising-bits led to LDP label purge on peer.
CSCvm62554	BGP multipath feature drops a path from list after BGP update event
CSCvm76070	Not able to enable the CLI http-status-code-ignore
CSCvm92116	Bulk-sync failure due to bgp router-id interface Loopback0

Caveat ID Number	Description
CSCvm93603	IP change on dialer-int does not trigger a correct "local cryto entpt"in DMVPN
CSCvm95236	BGP update not properly processed by inbound route-map
CSCvn07060	Redistributed metric is not be applied if it is in narrow-style
CSCvn28017	ISR4331 Routers May Crash When "eigrp default-route-tag" Configured on IPv4 AF
CSCvn59020	Modified EIGRP timers on Virtual-Template put all associated Vi interfaces into passive mode
CSCvm10698	ASR901 "qos-config scheduling-mode min-bw-guarantee" command is there still shaper works as policer

Troubleshooting

The following sections describe troubleshooting commands you can use with the 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:

- Cisco ASR 901 1G Router home page: http://www.cisco.com/en/US/partner/products/ps12077/tsd_products_support_series_home.html

- Cisco ASR 901 10G Router home page:
  http://www.cisco.com/c/en/us/support/routers/asr-901-10g-series-aggregation-services-routers/tsd-products-support-series-home.html

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.

- To obtain general networking, training, and certification titles, visit Cisco Press.

- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.